APLICACIONES DE LA TEORÍA DE LAS BASES DE GRÖBNER

JHON SEBASTIAN OVIEDO MELO

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2015

APLICACIONES DE LA TEORÍA DE LAS BASES DE GRÖBNER

JHON SEBASTIAN OVIEDO MELO

Trabajo presentado como requisito parcial para optar al título de
Licenciado en Matemáticas

Asesores
Fernando Andrés Benavides Agredo
Magister en Matemáticas
John Hermes Castillo Gómez
Doctor en Matemáticas

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2015

Nota de Responsabilidad

Todas las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva de los autores.

Artículo 1^{ro} del Acuerdo No. 324 de octubre 11 de 1966 emanado por el Honorable Concejo Directivo de la Universidad de Nariño.

Nota de Aceptación

John Hermes Castillo Gómez
Presidente de Tesis

Fernando Andrés Benavides Agredo
Presidente de Tesis de Tesis

Gilberto García Pulgarín
Jurado

Carlos Arturo Rodríguez Palma
Jurado

San Juan de Pasto, Mayo de 2015

Este trabajo está dedicado a:
Mis padres José Oviedo, Esperanza Melo y a mi familia.
Sebastian

Agradecimientos

Agradezco a Dios por esta oportunidad, por ser mi guía y fortaleza en la realización de este trabajo de grado.

A mi familia, por su apoyo incondicional en cada momento, por la confianza en mi etapa de estudio.

A la universidad de Nariño por contribuir a mi formación académica y personal brindarme la oportunidad de mejorar en cada aspecto de mi vida.

Al departamento de Matemáticas y Estadística, a cada profesor por su valioso apoyo, por la formación matemática recibida.

Al los jurados de evaluación Mg. Gilberto García Pulgarín y Mg. Carlos Arturo Rodríguez Palma por su tiempo, sugerencias y apoyo en la revisión de este trabajo.

A mis asesores Dr. John Hermes Castillo Gómez. y Mg. Fernando Andrés Benavides Agredo, el más sincero agradecimiento por cada consejo, sugerencia, orientación y apoyo en el desarrollo de este trabajo de grado.

Jhon Sebastian Oviedo Melo

Universidad de Narïï¿$\frac{1}{2}$o
Mayo de 2015.

Resumen

En este documento se presenta una introducción a la teoría de las bases de Gröbner desarrollada por Bruno Buchberger en el año 1965 y sus principales aplicaciones en la Teoría de Anillos.

En particular se estudiarán la resolución de los cuatro problemas clásicos de esta teoría. Dados un ideal $I = \langle f_1, f_2, \ldots, f_t \rangle$ y un polinomio f en $K[x_1, x_2, \ldots, x_n]$:

1. Decidir cuando $f \in I$.
2. Determinar polinomios $v_1, v_2, \ldots, v_s \in K[x_1, x_2, \ldots, x_n]$ tales que $f = v_1 f_1 + v_2 f_2 + \cdots + v_s f_s$.
3. Para un ideal $J \in K[x_1, x_2, \ldots, x_n]$, establecer las clases laterales de $K[x_1, x_2, \ldots, x_n]/J$.
4. Encontrar una base para el espacio vectorial $K[x_1, x_2, \ldots, x_n]/J$ sobre K.

Además, se estudiará una aplicación de las bases de Gröbner para construir un algoritmo de decodificación para códigos cíclicos. Adicionalmente se presentarán algunos algoritmos útiles para el análisis de esta teoría con ayuda del Sistema de Álgebra Computacional Discreta GAP, (*Groups, Algorithms, Programming - a System for Computational Discrete Algebra*).

Abstract

In this monograph we present an introduction to the theory of Gröbner bases developed by Bruno Buchberger in 1965 and its main applications in Ring Theory.

In particular, we study the solution of the four classic problems of this theory. Given an ideal $I = \langle f_1, f_2, \ldots, f_t \rangle$ and a polynomial f in $K[x_1, x_2, \ldots, x_n]$:

1. To decide when $f \in I$.
2. To find polynomials $v_1, v_2, \ldots, v_s \in K[x_1, x_2, \ldots, x_n]$ such that $f = v_1 f_1 + v_2 f_2 + \cdots + v_s f_s$.
3. For an ideal J of $K[x_1, x_2, \ldots, x_n]$, to establish the cosets of $K[x_1, x_2, \ldots, x_n]/J$.
4. To determine a basis to the vector space $K[x_1, x_2, \ldots, x_n]/J$ over K.

Also, we study an application of Gröbner bases to construct an algorithm to decode cyclic codes. Additionally, we present some useful algorithms for the study of this theory using the System for Computational Discrete Algebra GAP, (*Groups, Algorithms, Programming - a System for Computational Discrete Algebra*).

Índice general

Introducción

Durante los últimos años en el desarrollo de la ciencia computacional se han llevado a cabo múltiples aportes en diferentes disciplinas. En la matemática encontramos un sin número de herramientas que contribuyen tanto al desarrollo informático como a la evolución del pensamiento matemático. Lo que presentamos en este trabajo es una recopilación detallada de un concepto matemático denominado bases de Gröbner el cual fue dado por Bruno Buchberger en su trabajo de tesis doctoral [2] en honor a su asesor Wolfgang Gröbner quien le planteó la idea de generalizar la teoría de polinomios en una variable. Esta teoría frecuentemente se usa para estudiar problemas en Teoría de Anillos, Geometría Algebraica y algunas aplicaciones en diferentes ramas de la ciencia.

Para resolver sistemas de ecuaciones lineales en Álgebra Lineal se utiliza el método de Gauss-Jordan, a través de la matriz asociada al sistema en su forma escalonada reducida. Este proceso permite encontrar las mismas soluciones del sistema original de una forma "más simple" y eficiente.

Este problema se puede generalizar al estudiar sistemas de ecuaciones no lineales en varias variables, las cuales se pueden ver como elementos en un anillo de polinomios $K[x_1, x_2, \ldots, x_n]$. Hallar el espacio solución de dicho sistema es equivalente a encontrar los generadores "más simples" de un ideal en $K[x_1, x_2, \ldots, x_n]$, donde el ideal considerado está inicialmente generado por los polinomios que constituyen el sistema. En este trabajo se estudiará el procedimiento para obtener un conjunto generador "más simple", el cual se conoce como base de Gröbner para un ideal en $K[x_1, x_2, \ldots, x_n]$. Por ejemplo, para el caso de sistemas de ecuaciones en $K[x]$, utilizando el algoritmo de la división se puede probar que todo ideal es generado por un único polinomio y en consecuencia la solución del sistema original es "más simple".

Otro problema, el cual se conoce como el problema de la membresía de un ideal, consiste en decidir cuando un polinomio pertenece o no a un ideal en el anillo de polinomios $K[x_1, x_2, \ldots, x_n]$. Éste problema ha llamado la atención de los matemáticos durante muchos años.
Una solución para este problema es el concepto de base de Gröbner. Desde ese momento se han realizado múltiples aportes en el estudio de aplicaciones de las bases de Gröbner. Por ejemplo, en la solución de sistemas de ecuaciones, en aplicaciones en la geometría algebraica, en el problema de los tres colores, en programación entera [1, 3], en teoría de códigos, criptografía, ingeniería, física, y más recientemente en biología [9].

Los cuatro problemas fundamentales que se estudian con ayuda de las bases de Gröbner son los siguientes:

Dados un ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$ y un polinomio f en $K[x_1, x_2, \ldots, x_n]$.

1. Decidir cuando $f \in I$.

2. Determinar polinomios $v_1, v_2, \ldots, v_s \in K[x_1, x_2, \ldots, x_n]$ tales que $f = v_1 f_1 + v_2 f_2 + \cdots + v_s f_s$.

3. Establecer las clases laterales de $K[x_1, x_2, \ldots, x_n]/J$ para un ideal $J \in K[x_1, x_2, \ldots, x_n]$ cuyos elementos son de la forma $f + J$, con $f \in K[x_1, x_2, \ldots, x_n]$.

4. Encontrar una base para el espacio vectorial $K[x_1, x_2, \ldots, x_n]/J$ sobre K.

El objetivo general de este trabajo de grado es recopilar de forma ordenada la teoría de las bases de Gröbner junto con sus principales aplicaciones en anillos de polinomios. Para ello se pretende mostrar cómo solucionar los cuatro problemas presentados por medio de bases de Gröbner y dando algunos ejemplos en el sistema de álgebra computacional discreta GAP (*Groups, Algorithms, Programming - a System for Computational Discrete Algebra*).

En el Capítulo 1 se presentan algunas definiciones y resultados de la teoría de grupos y anillos; en particular se dará una exposición breve de las propiedades de los anillos de polinomios. Adicionalmente se expondrá la relación que existe entre el álgebra y la geometría con ayuda del concepto de variedad algebraica de un conjunto de polinomios y sus propiedades. En este contexto se dará una introducción a los problemas fundamentales de la teoría de las bases de Gröbner.

En el Capítulo 2, se estudia la solución de los problemas planteados en el anillo de polinomios en una variable utilizando el algoritmo de la división y la definición de máximo común divisor de polinomios. A continuación, en el Capítulo 3, se analizan estos problemas para polinomios en varias variables iniciando con el caso de polinomios lineales y abordando posteriormente el caso general. Con este objetivo se introduce el algoritmo de la división para polinomios de varias variables. En el Capítulo 4 se presenta el concepto de base de Gröbner, se establece el algoritmo de Bruno Buchberger para el cálculo de bases de Gröbner y las definiciones de base de Gröbner minimal y reducida. En el Capítulo 5 se encuentra la solución a los problemas fundamentales de la teoría de las bases de Gröbner para el anillo de polinomios $K[x_1, x_2, \ldots, x_n]$, así como su aplicación en la decodificación de códigos cíclicos. Finalmente, se presentan las conclusiones de este trabajo y un apéndice donde se muestran algunas de las principales instrucciones y comandos en GAP que se utilizan en esta monografía.

Capítulo 1

Preliminares

En la primera sección de este capítulo se presentan algunas de las definiciones y algunos de los teoremas que se usan en el desarrollo de este trabajo, por ejemplo se definen las estructuras algebraicas de grupo, anillo y campo y algunas de sus propiedades. Además se estudian ciertas propiedades de los anillos de polinomios. En la Sección 1.2 se presentan los problemas que se estudian durante el desarrollo de este trabajo y que se resuelven en los próximos capítulos con la ayuda de las bases de Gröbner. Finalmente en la Sección 1.3, se presenta el Teorema de la base de Hilbert el cual esencialmente sirve para probar que todo ideal en el anillo de polinomios $K[x_1, \ldots, x_n]$ es finitamente generado.

1.1. Nociones básicas

Una de las principales estructuras algebraicas que se estudian en matemáticas es la de grupo, donde se tiene una operación en un conjunto que satisface ciertas propiedades.

Definición 1.1. Un grupo es un conjunto G junto con una operación binaria $*$ en G que se denota por $(G, *)$, tal que :

1. La operación binaria $*$ es asociativa, es decir, $(a * b) * c = a * (b * c)$, para todo $a, b, c \in G$.
2. Existe un elemento $e \in G$ tal que $a * e = e * a = a$, para todo $a \in G$.
3. Para todo $a \in G$, existe un elemento $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$.

Una clase de grupos que merece una atención especial son aquellos cuyos elementos conmutan entre si.

Definición 1.2. Un grupo G es abeliano (conmutativo) si para todo par de elementos a, b de G se cumple la igualdad $a * b = b * a$.

La estructura de grupo permite definir otras estructuras más complejas como las de anillo y campo, cuyas definiciones se presentan a continuación.

Definición 1.3. Un anillo es un conjunto no vacío R con dos operaciones binarias $+$ y $*$ que se denota por $(R, +, *)$ de modo que se cumple lo siguiente:

1. $(R, +)$ es un grupo abeliano.
2. El producto $*$ es asociativo, es decir, $(a * b) * c = a * (b * c)$, para todo $a, b, c \in R$.
3. El producto $*$ es distributivo respecto a la suma, es decir, $(a + b) * c = a * c + b * c$ y $a * (b + c) = a * b + a * c$, para todo $a, b, c \in R$.

A continuación, se exhiben algunas definiciones de casos especiales de anillos que se usarán más adelante.

Definición 1.4. Un anillo se dice que es un anillo conmutativo si $a * b = b * a$, para todo $a, b \in R$.

Definición 1.5. Sea R un anillo y supóngase que existe un elemento $1 \in R$ tal que:

$$a * 1 = 1 * a = a \text{ para todo } a \in R.$$

Entonces diremos que R es un anillo con unitario o con unidad.

Definición 1.6. Sea R un anillo con unidad. Un elemento $a \in R$ se dice que es invertible (o es una unidad), si existe un elemento a^{-1} tal que

$$a * a^{-1} = a^{-1} * a = 1.$$

Más aun, se puede probar que el elemento a^{-1} es único y se denomina el inverso de a.

Definición 1.7. Un anillo R es un anillo con división si es un anillo con unidad, en donde todos los elementos diferentes de cero son invertibles.

Definición 1.8. Un elemento a no nulo de un anillo R se denomina divisor de cero, si existe un elemento no nulo b en R tal que $ab = 0$. Se dice que R es un dominio entero si es un anillo conmutativo que carece de elementos divisores de cero; es decir si $xy = 0$, implica que $x = 0$ ó $y = 0$.

Ahora, a partir de estos conceptos se puede definir una nueva estructura algebraica, la cual se conoce como campo o cuerpo.

Definición 1.9. Un campo K es un anillo conmutativo con unidad, donde todos los elementos diferentes de cero son invertibles. Así, un campo es un anillo con división conmutativo.

Para un estudio más amplio de la teoría de anillos es necesario considerar la noción de ideal.

Definición 1.10. Sea R un anillo y sea $I \subset R$ no vacío. Se dice que I es un ideal derecho de R si satisface las siguientes condiciones:

1. $a + b \in I$, para todo $a, b \in I$.
2. $a * r \in I$, para todo $a \in I$ y $r \in R$.

Definición 1.11. Sea R un anillo y sea $I \subset R$ no vacío. Se dice que I es un ideal izquierdo de R si satisface las siguientes condiciones:

1. $a + b \in I$, para todo $a, b \in I$.
2. $r * a \in I$, para todo $a \in I$ y $r \in R$.

Definición 1.12. Sea R un anillo y sea $I \subset R$ no vacío. Se dice que I es un ideal bilateral de R si es un ideal derecho e izquierdo de R.

En este trabajo estamos interesados en estudiar una familia particular de anillos, la cual se conoce como anillo de polinomios. Un anillo de polinomios en una variable x, es un conjunto formado por polinomios en x, junto con las operaciones de adición y producto usuales entre estos. Más específicamente, se puede definir este conjunto, el cual se denotará $R[x]$, y sus operaciones como sigue:

Definición 1.13. Sea R un anillo. Un polinomio en x es una suma formal $\sum_{i=1}^{\infty} a_i x^i$ donde $a_i \in R$ $\forall i \geq 0$, con $a_i = 0$ excepto para un número finito de subíndices i.

Definición 1.14. Dos polinomios $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ y $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ sobre el anillo R son iguales si y sólo si $a_i = b_i$, para todo $i \geq 0$.

Notación 1.1. $R[x]$ denotará el conjunto de polinomios sobre el anillo R.

Operaciones en $R[x]$

Definición 1.15.

1. Sean $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ y $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$. Se define la suma de $f(x)$ y $g(x)$ como

$$f(x) + g(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0,$$

donde $c_i = a_i + b_i$, $a \leq i \leq k = \text{máx}\{m, n\}$.

2. Sean $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ y $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$. Se define el producto $f(x)g(x)$ como

$$c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0,$$

donde $c_s = \sum_{i+j=s} a_i b_j$, para todo $0 \leq s \leq n + m$.

Teorema 1.1. *El conjunto $R[x]$ tiene estructura de anillo bajo las operaciones de suma y producto entre polinomios. Además, si R es un anillo conmutativo, entonces $R[x]$ es un anillo conmutativo.*

Demostración. Claramente $R[x]$ es un grupo abeliano bajo la suma de polinomios y el neutro es el polinomio nulo 0. Si $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$, el inverso es $-f(x) = (-a_n)x^n + (-a_{n-1})x^{n-1} + \cdots + (-a_1)x + (-a_0) \in R[x]$. La propiedad conmutativa y asociativa se sigue de que los coeficientes de los polinomios están en el anillo R. El producto es asociativo y satisface las leyes distributivas. Supóngase que R es un anillo conmutativo, luego para $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ y $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \in R[x]$, donde $s = m+n$ y para todo $1 \leq i \leq s$ se tiene que

$$f(x)g(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0,$$

donde $c_i = \sum_{r+j=i} a_r b_j$ y

$$g(x)f(x) = d_k x^k + d_{k-1}x^{k-1} + \ldots + d_1 x + d_0,$$

con $d_i = \sum_{j+r=i} b_j a_r$. Luego $f(x)g(x) = g(x)f(x)$. ■

Teorema 1.2. *Si R es un dominio entero, entonces el anillo $R[x]$ es un dominio entero.*

Demostración. Sean $f(x) = \sum_{i=1}^{m} a_i x_i \in R[x]$ con $a_m \neq 0$ y $g(x) = \sum_{i=1}^{n} b_i x_i \in R[x]$ con $b_n \neq 0$. Supóngase que $f(x)g(x) = 0$. Luego de la definición del producto se tiene que $c_{m+n} = a_m b_n = 0$, lo que es una contradicción ya que R es un dominio entero, por tanto se tiene que $a_m = 0$ y $b_n = 0$. ■

Dado un anillo R es posible definir el anillo de polinomios $R[x_1, x_2]$ como el anillo de polinomios en la variable x_2 con coeficientes en el anillo $R[x_1]$. Así, de forma recursiva, se puede definir el anillo de polinomios en n variables $x_1, x_2, \ldots, x_n$ sobre el anillo R, haciendo $R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$.
A continuación se definen algunos conceptos que serán necesarios posteriormente.

Definición 1.16. Se define $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ como un producto potencia, con $\alpha_i \in \mathbb{N}, i = 1, \ldots, n$.

Para un anillo R, el polinomio $f(x_1, x_2, \ldots, x_n)$ de n variables con coeficientes en R se puede ver como una suma de términos de la forma $a x_1^{\beta_1} \cdots x_n^{\beta_n}$, con $a \in R$ y $\beta_i \in \mathbb{N}$[1] para $i = 1, 2, \ldots, n$.

Ejemplo 1.1. Los siguientes son ejemplos de polinomios con coeficientes en el conjunto de los números racionales, $\mathbb{Q}$.

[1] $\mathbb{N} = \{0\} \cup \mathbb{Z}^+$.

- $f = x_1^3 + x_2^3 + x_3$ es un polinomio en 3 variables.
- $g = x_1x_2^2 + x_2x_4^5 - x_3$ es un polinomio en 4 variables.
- $h = 2x + 3y + 5$ es un polinomio en 2 variables.
- $r = 5x^2 + 3yz^3$ es un polinomio en 3 variables.

Con ayuda de GAP se puede definir el anillo de polinomios $\mathbb{Q}[x]$ como sigue. Primero se define la variable x y el anillo $\mathbb{Q}[x]$ con los siguientes comandos:

```
>x:=X(Rationals,"x");
x

>R:=PolynomialRing(Rationals,[x]);
Rationals[x]
```

De esta forma podemos realizar operaciones en $\mathbb{Q}[x]$ en GAP de la siguiente manera. Sean $f(x) = 2x^3 + \frac{3}{4}x^2 + 7x - 1$ y $g(x) = -6x^3 - 6x + 2$, luego $f(x) + g(x)$ y $f(x)g(x)$ se pueden calcular así:

```
>f:=2*x^3+3/4*x^2+7*x-1;
2*x^3+3/4*x^2+7*x-1

>g:=-6*x^3-6*x+2;
-6*x^3-6*x+2

>f+g;
-4*x^3+3/4*x^2+x+1

>f*g;
-12*x^6-9/2*x^5-54*x^4+11/2*x^3-81/2*x^2+20*x-2
```

Es decir

$$f(x) + g(x) = -4x^3 + \frac{3}{4}x^2 + x + 1$$

y

$$f(x)g(x) = -12x^6 - \frac{9}{2}x^5 - 54x^4 + \frac{11}{2}x^3 - \frac{81}{2}x^2 + 20x - 2.$$

Además, GAP da la posibilidad de realizar operaciones con polinomios en varias variables. Por ejemplo, para calcular la suma y el producto de los polinomios $f = \frac{1}{4}x^4y^2 + \frac{2}{3}x^2y - 5xy + 4$ y $g = -\frac{5}{3}x^3y^3 - x^2y^2 + 3xy + 1$ en las variables x y y en el anillo de polinomios $\mathbb{Q}[x, y]$ se procede de la siguiente manera:

```
>x:=X(Rationals,"x");
x

>y:=X(Rationals,"y");
y

>R:=PolynomialRing(Rationals,[x,y]);
Rationals[x,y]

>f:=1/4*x^4*y^2+x^2*2/3*y-5*x*y+4;
1/4*x^4*y^2+2/3*x^2*y-5*x*y+4

>g:=-5/3*x^3*y^3-x^2*y^2+3*x*y+1;
-5/3*x^3*y^3-x^2*y^2+3*x*y+1

>f+g;
1/4*x^4*y^2-5/3*x^3*y^3-x^2*y^2+2/3*x^2*y-2*x*y+5

>f*g;
-5/12*x^7*y^5-1/4*x^6*y^4-10/9*x^5*y^4+3/4*x^5*y^3+25/3*x^4*y^4-2/3*x^4*y^3+1/\
4*x^4*y^2-5/3*x^3*y^3+2*x^3*y^2-19*x^2*y^2+2/3*x^2*y+7*x*y+4
```

Así

$$f + g = \frac{1}{4}x^4y^2 - \frac{5}{3}x^3y^3 - x^2y^2 + \frac{2}{3}x^2y - 2xy + 5$$

y

$$fg = -\frac{5}{12}x^7y^5 - \frac{1}{4}x^6y^4 - \frac{10}{9}x^5y^4 + \frac{3}{4}x^5y^3 + \frac{25}{3}x^4y^4 - \frac{2}{3}x^4y^3 + \\ + \frac{1}{4}x^4y^2 - \frac{5}{3}x^3y^3 + 2x^3y^2 - 19x^2y^2 + \frac{2}{3}x^2y + 7xy + 4.$$

Adicionalmente en GAP también se pueden definir anillos de polinomios en varias variables con coeficientes en anillos (o campos). Por ejemplo, para definir el anillo de polinomios $\mathbb{F}_2[x_1, x_2, x_3]$ en GAP se usa el comando `R:=PolynomialRing(GF(2),[x1,x2,x3]);`, donde `GF(2)` es el campo finito con 2 elementos. En los siguientes capítulos se presentarán otros procedimientos que se pueden realizar en GAP, mayor información se puede encontrar en [4].

1.2. Problemas fundamentales de la teoría de las bases de Gröbner

A continuación se presenta una introducción al concepto de variedad sobre un anillo de polinomios, el cual es fundamental para establecer un puente entre el concepto algebraico y la interpretación geométrica de conjuntos de polinomios. A partir de ahora K denotará un campo.

Definición 1.17. Para un entero positivo n, se define el n-espacio afín como $K^n = \{(a_1, \ldots, a_n) : a_i \in K \text{ para todo } 1 \leq i \leq n\}$.

Ejemplo 1.2. Cuando $K = \mathbb{R}$, $\mathbb{R}^n$ se conoce como el espacio euclídeo n-dimensional.

1.2.1. Forma alternativa de ver un polinomio

Un polinomio f en $K[x_1, x_2, \ldots, x_n]$ determina una función de K^n en K definida por

$$\phi : K^n \to K$$

$$(a_1, a_2, \ldots, a_n) \to f(a_1, a_2, \ldots, a_n).$$

Para todo $(a_1, a_2, \ldots, a_n) \in K^n$, la cual se denomina función de evaluación.

Estas dos formas de identificar un polinomio como sumas de términos y como una función de evaluación permiten por un lado estudiar la estructura algebraica de un polinomio f en $K[x_1, x_2, \ldots, x_n]$ y por otro analizar las características de los puntos $(a_1, a_2, \ldots, a_n)$ que pueden ser evaluados en f. Esta doble identidad de los polinomios es el puente entre el álgebra y la geometría.

Definición 1.18. Para $f \in K[x_1, x_2, \ldots, x_n]$ se define la variedad de f, la cual se denota con $V(f)$, como el conjunto

$$V(f) = \{(a_1, a_2, \ldots, a_n) \in K^n : f(a_1, a_2, \ldots, a_n) = 0\}.$$

En otras palabras, la variedad de f representa el conjunto de puntos en K^n que satisfacen la ecuación $f = 0$.

Definición 1.19. Sean $f_1, f_2, \ldots, f_s \in K[x_1, x_2, \ldots, x_n]$. Se define la variedad de $f_1, f_2, \ldots, f_s$ la cual se denota con $V(f_1, f_2, \ldots, f_s)$, como el conjunto de puntos en K^n que satisfacen el sistema de ecuaciones

$$f_1 = 0,\ f_2 = 0, \ldots, f_s = 0, \tag{1.2.1}$$

es decir

$$V(f_1, f_2, \ldots, f_s) = \{(a_1, a_2, \ldots, a_n) \in K^n : f_i(a_1, a_2, \ldots, a_n) = 0,\ \forall\ 1 \leq i \leq n\}.$$

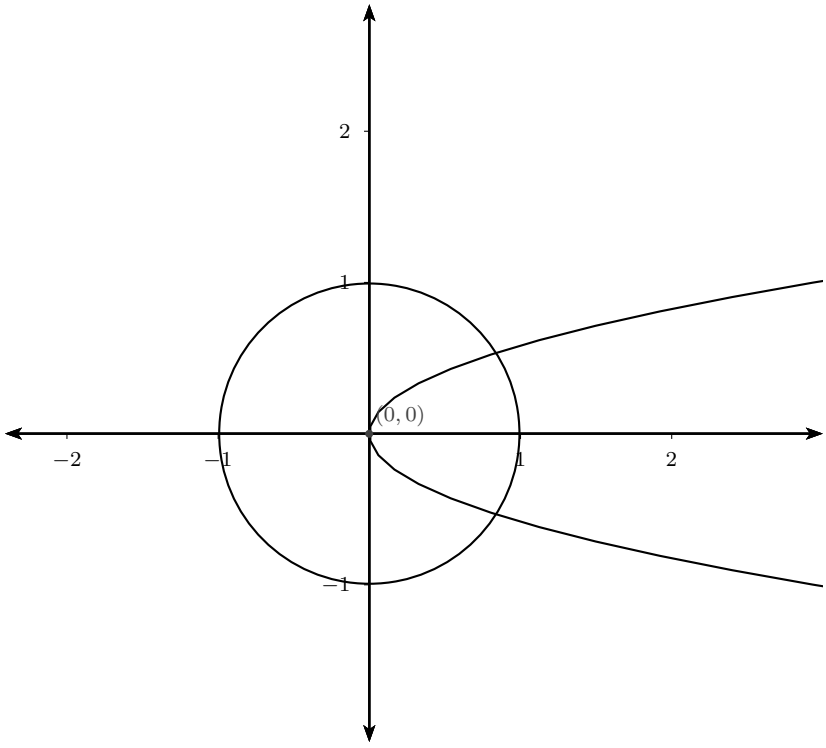

Figura 1.1: Variedad $V(x^2 + y^2 - 1, x - 3y^2)$

Proposición 1.1. *Sean $f_1, f_2, \ldots, f_s$ polinomios en $K[x_1, x_2, \ldots, x_n]$. Entonces $V(f_1, f_2, \ldots, f_s) = \bigcap_{i=1}^{s} V(f_i)$.*

Demostración. En efecto, para $(a_1, a_2, \ldots, a_n) \in V(f_1, f_2, \ldots, f_s)$ se tiene que $f_i(a_1, a_2, \ldots, a_n) = 0$ para cada $1 \leq i \leq n$, por tanto $(a_1, a_2, \ldots, a_n)$ es un punto de la variedad de cada f_i, es decir, $(a_1, a_2, \ldots, a_n) \in \bigcap_{i=1}^{s} V(f_i)$, así $V(f_1, f_2, \ldots, f_s) \subseteq \bigcap_{i=1}^{s} V(f_i)$. Ahora si $(b_1, b_2, \ldots, b_n) \in \bigcap_{i=1}^{s} V(f_i)$, entonces $(b_1, b_2, \ldots, b_n)$ pertenece a cada $V(f_i)$, es decir, $f_i(b_1, b_2, \ldots, b_n) = 0$. Por tanto $(b_1, b_2, \ldots, b_n) \in V(f_1, f_2, \ldots, f_s)$, de ahí que $\bigcap_{i=1}^{s} V(f_i) \subseteq V(f_1, f_2, \ldots, f_s)$, y se sigue la igualdad deseada. ■

Ejemplo 1.3. La variedad $V(x^2 + y^2 - 1, x - 3y^2) \subset \mathbb{R}^2$ es la intersección entre la circunferencia $x^2 + y^2 = 1$ y la parabola $x = 3y^2$ en el plano xy, ver Figura 1.1.

La Definición 1.19 puede extenderse a conjuntos arbitrarios de polinomios en $K[x_1, x_2, \ldots, x_n]$.

Definición 1.20. Para un conjunto $S \subseteq K[x_1, x_2, \ldots, x_n]$ se define la variedad de S, como el conjunto

$$V(S) = \{(a_1, a_2, \ldots, a_n) \in K^n : f(a_1, a_2, \ldots, a_n) = 0, \ \forall\ f \in S\}.$$

Existen varios algoritmos para solucionar sistemas de ecuaciones tales como el Sistema (1.2.1). Algunos dan una solución para casos particulares y otros simplemente dan una aproximación de la solución. La mayoría de estos algoritmos no tienen en cuenta el concepto de variedad, es decir las propiedades geométricas del espacio solución del sistema, al igual que se ignoran sus posibles descripciones alternativas. Para obtener dichas descripciones se puede usar sistemas equivalentes al sistema original, los cuales tienen las mismas soluciones pero son "más fáciles" de resolver. Por ejemplo, para resolver sistemas de ecuaciones lineales, tradicionalmente, se usa el método de Gauss-Jordan, ver Sección 3.1, en el cual se transforma el sistema original por medio de operaciones elementales de matrices para obtener uno nuevo.
Vamos a desarrollar un procedimiento que nos dará la información algebraica y geométrica sobre todo el espacio de solución del Sistema (1.2.1). El método consiste en encontrar una mejor representación para la variedad correspondiente, esto se hará considerando el ideal generado por los polinomios $f_1, f_2, \ldots, f_s$.

Proposición 1.2. *Sean $f_1, f_2, \ldots, f_s$ polinomios en $K[x_1, x_2, \ldots, x_n]$, el conjunto*

$$I = \left\{ \sum_{i=1}^{s} \mu_i f_i \ : \mu_i \in K[x_1, x_2, \ldots, x_n], i = 1, 2, \ldots, s \right\}.$$

es un ideal en $K[x_1, x_2, \ldots, x_n]$. Este ideal se denomina el ideal generado por $f_1, f_2, \ldots, f_s$ y se denota por $\langle f_1, f_2, \ldots, f_s \rangle$.

Demostración. Vamos a probar que $I = \langle f_1, f_2, \ldots, f_s \rangle$ es un ideal en $K[x_1, x_2, \ldots, x_n]$. En efecto si $f, g \in I$, entonces $f = v_1 f_1 + v_2 f_2 + \cdots + v_s f_s$ y $g = t_1 f_1 + t_2 f_2 + \cdots + t_s f_s$ para v_i, t_i polinomios en $K[x_1, x_2, \ldots, x_n]$. Luego $f + g = (v_1 + t_1) f_1 + \cdots + (v_s + t_s) f_s$ y de esta forma $f + g \in I$. Para la segunda condición se tiene que si $f \in I$, entonces $f = v_1 f_1 + v_2 f_2 + \cdots + v_s f_s$ y si h es cualquier polinomio en $K[x_1, x_2, \ldots, x_n]$, entonces $hf = h(v_1 f_1 + v_2 f_2 + \cdots + v_s f_s)$, de donde se sigue que $fh = hf = (hv_1) f_1 + (hv_2) f_2 + \cdots + (hv_s) f_s$, por tanto $hf \in I$. ■

Es preciso señalar que este ideal se puede ver como el conjunto de todas las combinaciones lineales de los polinomios $f_1, f_2, \ldots, f_s$ en $K[x_1, x_2, \ldots, x_n]$ con coeficientes polinomiales.

Definición 1.21. El conjunto $\{f_1, f_2, \ldots, f_s\}$ se denomina un conjunto generador del ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$.

Podemos estudiar la variedad del ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$ la cual se denota como $V(I)$ y se define por

$$V(I) = \{(a_1, a_2, \ldots, a_n) \in K^n : f(a_1, a_2, \ldots, a_n) = 0, \ \forall \ f \in I\}.$$

La variedad anterior define las soluciones de un sistema infinito de ecuaciones polinomiales,

$$f = 0, f \in I. \tag{1.2.2}$$

Por otro lado, si se considera el sistema

$$f_1 = 0, f_2 = 0, \ldots, f_s = 0. \tag{1.2.3}$$

Se puede observar que una solución del Sistema (1.2.2) es solución del Sistema (1.2.3), ya que, si $(a_1, a_2, \ldots, a_n) \in V(I)$, entonces $f(a_1, a_2, \ldots, a_n) = 0$, para todo $f \in I$ y la afirmación se sigue del hecho de que cada $f_i \in I$. Adicionalmente, si $(a_1, a_2, \ldots, a_n) \in K^n$ es una solución del Sistema (1.2.3) y f es cualquier elemento de I, entonces $f = h_1 f_1 + h_2 f_2 + \cdots + h_s f_s$, con $h_i \in K[x_1, x_2, \ldots, x_n]$, de donde $f(a_1, a_2, \ldots, a_n) = h_1(a_1, a_2, \ldots, a_n) f_1(a_1, a_2, \ldots, a_n) + \cdots + h_s(a_1, a_2, \ldots, a_n) f_s(a_1, a_2, \ldots, a_n)$. Así $f(a_1, a_2, \ldots, a_n) = h_1(a_1, a_2, \ldots, a_n)0 + \cdots + h_s(a_1, a_2, \ldots, a_n)0 = 0$, de ahí que $(a_1, a_2, \ldots, a_n) \in V(I)$, y por tanto $V(I) = V(f_1, f_2, \ldots, f_s)$.

Nota 1.1. Un ideal puede tener diferentes conjuntos generadores, inclusive estos conjuntos pueden tener diferente número de elementos.

Ejemplo 1.4. Considere el anillo de polinomios $K[x, y]$, se puede probar que $\langle x, y\rangle = \langle x + y, x\rangle = \langle x + y, x, y\rangle$.
En efecto, claramente $x \in \langle x + y, x\rangle$ y es fácil ver que $y = x + y - 1(x)$, luego $\langle x, y\rangle \subseteq \langle x + y, x\rangle$. De forma elemental se tiene que $\langle x + y, x\rangle \subseteq \langle x, y\rangle$, así $\langle x, y\rangle = \langle x + y, x\rangle$. De igual forma se puede mostrar la tercera igualdad.
Otro hecho a destacar es que a un ideal I de $K[x_1, x_2, \ldots, x_n]$ con dos o más conjuntos generadores distintos con diferente número de elementos, le corresponde una misma variedad, es decir si

$$I = \langle f_1, f_2, \ldots, f_s\rangle = \langle f_1^{'}, f_2^{'}, \ldots, f_t^{'}\rangle,$$

se tiene que

$$V(f_1, f_2, \ldots, f_s) = V(I) = V(f_1^{'}, f_2^{'}, \ldots, f_t^{'}).$$

Así, el sistema $f_1 = 0, \ldots, f_s = 0$ tiene las mismas soluciones que el sistema $f_1^{'} = 0, \ldots, f_t^{'} = 0$. Por lo tanto, la variedad está totalmente determinada por el ideal I y no por el sistema de ecuaciones.

Objetivo. Nuestro objetivo ahora es encontrar el "mejor" conjunto generador para el ideal I, es decir un conjunto generador que ayude a entender la estructura algebraica de $I = \langle f_1, f_2, \ldots, f_s\rangle$ y la estructura geométrica de $V(f_1, f_2, \ldots, f_s)$. A tal conjunto se le denominará una base de Gröbner para el ideal I.

Para abordar este objetivo es necesario considerar la siguiente definición.

Definición 1.22. Para una colección de puntos V del espacio afín K^n, se define el conjunto de polinomios en $K[x_1, x_2, \ldots, x_n]$ que se denota con $I(V)$ al conjunto

$$I(V) = \{f \in K[x_1, x_2, \ldots, x_n] \ : f(a_1, a_2, \ldots, a_n) = 0, \ \forall\ (a_1, a_2, \ldots, a_n) \in V\}.$$

Con respecto al conjunto $I(V)$ se puede probar la siguiente afirmación.

Proposición 1.3. *El conjunto $I(V)$ es un ideal de $K[x_1, x_2, \ldots, x_n]$.*

Demostración. En efecto, para $f, g \in I(V)$ se tiene que $f(a_1, a_2, \ldots, a_n) = 0$ y $g(a_1, a_2, \ldots, a_n) = 0, \forall\ (a_1, a_2, \ldots, a_n) \in V$, luego $(f + g)\ (a_1, a_2, \ldots, a_n) = f(a_1, a_2, \ldots, a_n) + g(a_1, a_2, \ldots, a_n) = 0 + 0 = 0$, de donde se tiene que $f + g \in I(V)$. De igual forma para $h \in K[x_1, x_2, \ldots, x_n]$ y $f \in I(V)$ se tiene que $hf(a_1, a_2, \ldots, a_n) = h(a_1, a_2, \ldots, a_n)f(a_1, a_2, \ldots, a_n) = h(a_1, a_2, \ldots, a_n)0 = 0$ y así $hf \in I(V)$. ■

Es importante notar que este ideal se define por la condición geométrica de que $f \in I(V)$ si y sólo si $f(a_1, a_2, \ldots, a_n) = 0, \forall\ (a_1, a_2, \ldots, a_n) \in V$. Además por el Teorema de la base de Hilbert, el cual se presentará más adelante (ver Teorema 1.3), el ideal $I(V)$ es finitamente generado.

1.2.2. Relación entre álgebra y geometría

Gracias a la construcción del ideal $I(V)$ se puede establecer un puente entre el Álgebra y la Geometría como se indica en el siguiente esquema.

$$\{\text{Subconjuntos de } K[x_1, x_2, \ldots, x_n]\} \longrightarrow \{\text{Variedades de } K^n\}$$

$$\{S\} \qquad\qquad \longrightarrow \qquad\qquad \{V(S)\}.$$

De igual forma se tiene que

$$\{\text{Subconjuntos de } K^n\} \longrightarrow \{\text{Ideales de } K[x_1, x_2, \ldots, x_n]\}$$

$$\{V\} \qquad \longrightarrow \qquad \{I(V)\}.$$

Siguiendo con el objetivo de encontrar el "mejor" conjunto generador es necesario determinar cuando dos conjuntos finitos de polinomios en $K[x_1, x_2, \ldots, x_n]$ dan lugar al mismo ideal. Es decir, dados $f_1, f_2, \ldots, f_s$ y $f_1', f_2', \ldots, f_t' \in K[x_1, x_2, \ldots, x_n]$ con $s \neq t$ decidir cuando $\langle f_1, f_2, \ldots, f_s\rangle = \langle f_1', f_2', \ldots, f_t'\rangle$. Para analizar este punto nos proponemos estudiar los siguientes problemas.

Problemas 1.1. Dados un ideal $I = \langle f_1, f_2, \ldots, f_t\rangle$ y un polinomio f en $K[x_1, x_2, \ldots, x_n]$.

1. Decidir cuando el polinomio $f \in I$. Este problema se conoce como el *problema de membresía de un ideal.*

2. Si $f \in I$, determinar polinomios $v_1, v_2, \ldots, v_s \in K[x_1, x_2, \ldots, x_n]$ tal que $f = v_1 f_1 + v_2 f_2 + \cdots + v_s f_s$.

   Nota 1.2. En este contexto determinar significa construir algoritmos que permitan encontrar tales $v_1, v_2, \ldots, v_s$.

Sea I un ideal en $K[x_1, x_2, \ldots, x_n]$ y $f \in K[x_1, x_2, \ldots, x_n]$. Anteriormente se mostró que el polinomio f determina una función de evaluación de K^n en K definida por

$$\begin{aligned} \phi: K^n &\to K \\ (a_1, a_2, \ldots, a_n) &\to f(a_1, a_2, \ldots, a_n). \end{aligned}$$

Si se restringe esta función a $V(I)$ y consideramos la función de evaluación $V(I) \to K$ definida por $(a_1, a_2, \ldots, a_n) \to f(a_1, a_2, \ldots, a_n),$ para todo $(a_1, a_2, \ldots, a_n) \in V(I)$, es de nuestro interés responder a la siguiente pregunta.

Pregunta 1.1. Para $f, g \in K[x_1, x_2, \ldots, x_n]$, ¿cuándo son iguales las funciones de evaluación $V(I) \to K$ determinadas por los polinomios f y g ?

Para ello es necesario considerar el ideal $I(V(I))$, dado por el conjunto de polinomios en $K[x_1, x_2, \ldots, x_n]$ que se define como

$$I(V(I)) = \{f \in K[x_1, x_2, \ldots, x_n] \ : f(a_1, a_2, \ldots, a_n) = 0, \ \forall \ (a_1, a_2, \ldots, a_n) \in V(I)\}.$$

Si $f - g \in I(V(I))$, entonces $(f - g)(a_1, a_2, \ldots, a_n) = 0,$ para todo $(a_1, a_2, \ldots, a_n) \in V(I)$. Por lo tanto la función $V(I) \to K$ definida por el polinomio $f - g$ es igual a cero. De este modo las funciones de evaluación $V(I) \to K$ determinada por f y g son iguales.

Definición 1.23. Para $f, g \in K[x_1, x_2, \ldots, x_n]$ y J un ideal de $K[x_1, x_2, \ldots, x_n]$, se dice que f es congruente con g módulo J si $f - g \in J$, lo que se denota con $f \equiv g$ mód J. Además se puede probar que la realción $\equiv$ es una relación de equivalencia sobre $K[x_1, x_2, \ldots, x_n]$.

Notación 1.2. El conjunto de clases de equivalencia se denota como $K[x_1, x_2, \ldots, x_n]/J$.

Los elementos de $K[x_1, x_2, \ldots, x_n]/J$ son de la forma $f + J$ y se les llama clases laterales de J, los cuales tienen las siguientes operaciones: para $f, g \in K[x_1, x_2, \ldots, x_n]$ se tiene que $(f + J) + (g + J) = (f + g) + J$ y $(f + J)(g + J) = fg + J$. De esta forma, $K[x_1, x_2, \ldots, x_n]/J$ es un anillo conmutativo con las operaciones de suma y producto definidas anteriormente, el cual se denomina anillo cociente de $K[x_1, x_2, \ldots, x_n]$ por J. También se puede probar que $K[x_1, x_2, \ldots, x_n]/J$ es un espacio vectorial sobre K.
Siguiendo ésta idea nos planteamos estudiar las clases laterales del anillo $K[x_1, x_2, \ldots, x_n]/J$. Para ello nos planteamos resolver los siguientes problemas.

3. Encontrar las clases laterales de $K[x_1, x_2, \ldots, x_n]/J$.
4. Determinar una base para el espacio vectorial $K[x_1, x_2, \ldots, x_n]/J$, sobre K (la cual puede ser o no infinita).

A continuación se presenta el Teorema de la base de Hilbert, el cual demuestra que todo ideal de un anillo de polinomios es finitamente generado. esto implica que cada variedad de un ideal en realidad constituye las soluciones de un conjunto finito de polinomios.

1.3. Teorema de la base de Hilbert

Teorema 1.3. *(Teorema de la base de Hilbert). En el anillo $K[x_1, x_2, \ldots, x_n]$, se cumple lo siguiente*

1. *Si I es un ideal de $K[x_1, x_2, \ldots, x_n]$, existen polinomios $f_1, f_2, \ldots, f_s \in K[x_1, x_2, \ldots, x_n]$ tal que $I = \langle f_1, f_2, \ldots, f_s \rangle$.*
2. *Si $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$ es una cadena ascendente de ideales de $K[x_1, x_2, \ldots, x_n]$, entonces existe un entero positivo N tal que $I_N = I_{N+1} = I_{N+2} \cdots$.*

Observación 1.1. Con respecto al teorema anterior se presentan las siguientes dos definiciones:

1. Un ideal I en R que cumple la condición 1 se denomina un ideal finitamente generado o que tiene un conjunto generador finito.
2. Si un anillo conmutativo R satisface la condición 2 se llama un anillo Noetheriano.

Para la demostración del Teorema 1.3, primero es necesario considerar los siguientes resultados.

Teorema 1.4. *Las siguientes condiciones en un anillo R son equivalentes*

1. *Si I es un ideal de R, existen elementos $f_1, f_2, \ldots, f_s \in R$ tal que $I = \langle f_1, f_2, \ldots, f_s \rangle$.*
2. *Si $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$ es una cadena ascendente de ideales de R, entonces existe un N tal que $I_N = I_{N+1} = I_{N+2} \cdots$.*

En otras palabras R es un anillo Noetheriano si y sólo si todo ideal de R es finitamente generado.

Demostración. Primero supóngase que se cumple la primera condición. Sea

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots,$$

una cadena ascendente de ideales de R. Si se considera la unión de los ideales I_i, esto es $I = \bigcup_{n=1}^{\infty} I_n$ este es nuevamente un ideal de R. Por hipótesis, $I = \langle f_1, f_2, \ldots, f_s \rangle$ con $f_1, f_2, \ldots, f_s \in R$, por tanto para cada $1 \leq i \leq s$, $f_i \in I$ y así existe $N_i \in \mathbb{Z}^+$ tal que $f_i \in I_{N_i}$. Sea $N = \max_{1 \leq i \leq s}\{N_i\}$, de esta forma cada $f_i \in I_N$ y esto implica que $I \subseteq I_N$, i.e $I_k = I_N$, para todo $k \geq N$.

Para la otra implicación se supone lo contrario, que existe un ideal I de R que no es finitamente generado. Sea $f_1 \in I$, luego existe $f_2 \in I \notin \langle f_1 \rangle$. Por lo tanto $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle$, si continuamos este proceso se obtiene una cadena estrictamente ascendente de ideales de R lo cual contradice la segunda condición. ■

Nota 1.3. Para $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_o$ un polinomio no nulo en $K[x]$, a_n es el *coeficiente líder de f* y se denota con $\mathrm{lc}(f) = a_n$.

Teorema 1.5. *Si R es un anillo Noetheriano, entonces $R[x]$ también lo es.*

Demostración. Sea I un ideal de $R[x]$, probemos que I es finitamente generado. Dado un polinomio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_o$ en $R[x]$ con $a_n \neq 0$ y se define el conjunto formado por los coeficientes líderes de todos los polinomios en I; es decir $J = \{r \in R : r \text{ es el coeficiente líder de los polinomios en } I\} \bigcup \{0\}$, tal conjunto J es un ideal de R. En efecto, sean a_n y $b_m \in J$, por definición son los coeficientes líderes de dos polinomios en I, digamos $p_1(x) = a_n x^n + \cdots + a_1 x + a_0$ y $p_2(x) = b_m x^m + \cdots + b_1 x + b_0$, luego $x^m p_1(x) + x^n p_2(x) \in I$, por tanto $a_n + b_m \in J$. Ahora si $r \in R$ entonces $rp_1(x) \in I$ y $ra_n \in J$. Ahora como R es Noetheriano se tiene que existen $f_1, f_2, \ldots, f_s \in I$ tal que sus coeficientes principales generan a J.
Sea N el máximo de los grados de los polinomios $f_1, f_2, \ldots, f_s$. Para cada entero $k < N$, se define a J_k como el subconjunto de R formado por los coeficientes principales de todos los polinomios en I de grado a lo más k. Claramente J_k es un ideal de R, en efecto es fácil ver que es cerrado bajo la suma y para $a \in J_k$ y $r \in R$ $ra \in J_k$. Sea $p(x) \in I$ cuyo coeficiente principal es a y consideremos el polinomio $q(x) = r \in R[x]$. Como I es un ideal de $R[x]$, entonces $q(x)p(x) = rp(x) \in I$, ya que el coeficiente principal de $rp(x)$ es ra. Ahora al ser J_k un ideal de R y por la condición de que R es Noetheriano, existe un número finito de polinomios $q_{k,1}(x), \ldots, q_{k,n_k}(x) \in I$, de tal manera que sus coeficientes principales generen a J_k. Ahora vamos a denotar por I^* al ideal generado por los polinomios

$$f_1, f_2, \ldots, f_s, q_{0,1}(x), \ldots, q_{0,n_0}(x), \ldots, q_{N,1}(x), \ldots, q_{N,n_N}(x).$$

Por construcción se tiene que el ideal $I^* \subset I$ y es finitamente generado. Probemos ahora que $I \subset I^*$. Supóngase lo contrario, que existe un polinomio $h(x) \in I$ pero no está en I^*, podemos escoger a $h(x)$ de menor grado con esta propiedad. Sea $s \in R$ el coeficiente principal de $h(x)$.
Caso 1. Supóngase que el grado de $h(x)$ es al menos N. Como $s \in J$, existen polinomios (monomios) $r_1(x), r_2(x), \ldots, r_s(x) \in R[x]$ tal que $u(x) = \sum_{i=1}^{s} r_i(x) f_i(x) \in I^*$ tiene coeficiente principal s y cuyo grado sea igual al de $h(x)$. Ahora como $h(x) - u(x) \in R$ tiene grado menor que $h(x)$, luego por la minimalidad en la escojencia de $h(x)$ se tiene que $h(x) - u(x) \in I^*$. Así $h(x) \in I^*$, lo cual es una contradicción.
Caso 2. Si el grado de $h(x)$ es $k < N$, luego $s \in J_k$ para algún k. Por lo tanto podemos encontrar polinomios (monomios) $r_{k,j}(x) \in R[x]$ de manera que $v(x) = \sum_{i=1}^{n_k} r_{k,i}(x) q_{k,i}(x) \in I^*$ tiene coeficiente principal s y cuyo grado sea igual al de $h(x)$ y la demostración se sigue de forma similar al Caso 1. ■

Corolario 1.1. *Si R es un anillo Noetheriano, entonces $R[x_1, x_2, \ldots, x_n]$ también lo es.*

Demostración. La demostración se hará por inducción sobre n. Si $n = 1$ entonces por el resultado anterior se cumple la afirmación. Ahora supóngase que $R[x_1, x_2, \ldots, x_n]$ es Noetheriano, luego $R[x_1, x_2, \ldots, x_n][x_{n+1}]$ también lo es nuevamente por el teorema anterior. ■

Así el Teorema de la base de Hilbert se cumple.

Capítulo 2

Polinomios en una variable

Este capítulo se centrará en estudiar la solución de los problemas presentados en el capítulo anterior para el caso del anillo de polinomios $K[x]$ con K un campo. En la Sección 2.1 se presenta el algoritmo de la división para el caso de polinomios en una variable. En la Sección 2.2, se estudia el concepto de máximo común divisor y su importancia en la noción de ideal principal, herramienta que será útil para la solución de los Problemas 1.1 en $K[x]$.

2.1. Algoritmo de la división

En esta sección se estudiarán los polinomios en una variable en el anillo $K[x]$ con K un campo. El algoritmo de la división para éste caso y su implementación en el sistema de álgebra computacional discreta GAP.

Definición 2.1. Para $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ un polinomio no nulo en $K[x]$ con $a_n \neq 0$, se denota con

- $\mathrm{lc}(f) = a_n$ al *coeficiente líder* de f,
- $\mathrm{lt}(f) = a_n x^n$ al *término líder* de f,
- $\mathrm{lp}(f) = x^n$ al *producto potencia líder* de f,
- $\deg(f) = n$ al *grado* de f.

Ejemplo 2.1. Para $f(x) = 2x^4 + 3x^3 - 2x^2 + 1$ en $\mathbb{Q}[x]$ se tiene que $\mathrm{lc}(f) = 2$, $\mathrm{lt}(f) = 2x^4$, $\mathrm{lp}(f) = x^4$ y $\deg(f) = 4$.

Ahora se presenta el algoritmo de la división para el anillo de polinomios $K[x]$.

Teorema 2.1. *(Algoritmo de la división para polinomios en una variable). Dados dos polinomios $f(x)$ y $g(x)$ en el anillo de polinomios $K[x]$, con $g(x) \neq 0$, existen polinomios únicos $q(x)$ (cociente) y $r(x)$ (residuo) en $K[x]$ tales que*

$$f(x) = q(x)g(x) + r(x),$$

con $r(x) = 0$ ó $\deg(r(x)) < \deg(g(x))$.

Demostración. Primero se demuestra la existencia de los polinomios $q(x)$ y $r(x)$. Para ello se aplica el principio de inducción sobre el grado de $f(x)$. Si $f(x) = 0$ o $\deg(f(x)) = 0$, basta tomar $q(x) = 0$ y $r(x) = f(x)$. Supóngase que el teorema se cumple para $f(x)$ con $\deg(f(x)) < n$, ahora para

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

y

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,$$

con $\deg(f(x)) = n$ y $\deg(g(x)) = m$. Si $n < m$, entonces $q(x) = 0$ y $r(x) = f(x)$. Supóngase que $n \geq m$. Considere $q_0(x) = a_n b_m^{-1} x^{n-m}$, donde el cálculo de $a_n b_m^{-1}$ se puede realizar una vez que K es un campo.
Sea

$$r_0(x) = f(x) - q_0(x)g(x).$$

Si $r_0(x) = 0$ ó el $\deg(r_0(x)) < \deg(g(x))$, se toma $q(x) = q_0(x)$ y $r(x) = r_0(x)$.
De otro modo, siguiendo con el proceso anterior cabe notar que los términos que corresponden a la potencia x^n se cancelan por la escojencia de $q_0(x)$, de ahí que $\deg(r_0(x)) < \deg(f(x))$ por tanto aplicando la hipótesis de inducción sobre los polinomios $r_0(x)$ y $g(x)$, existen polinomios $q_1(x), r_1(x) \in K[x]$ en la división de $r_0(x)$ por $g(x)$ tales que

$$r_0(x) = q_1(x)g(x) + r_1(x),$$

con $r_1(x) = 0$ ó $\deg(r_1(x)) < \deg(g(x))$, de donde se obtiene que $f(x) = q_0(x)g(x) + q_1(x)g(x) + r_1(x) = (q_0(x) + q_1(x))g(x) + r_1(x)$. Así tomando $r(x) = r_1(x)$ y $q(x) = q_0(x) + q_1(x)$ se prueba la existencia.
Para probar la unicidad, supóngase que existen polinomios $q_1(x),\ q_2(x),\ r_1(x),\ r_2(x) \in K[x]$ tales que

$$f(x) = q_1(x)g(x) + r_1(x),$$

con $\deg(r_1(x)) = 0$ ó $\deg(r_1(x)) < \deg(g(x))$ y que

$$f(x) = q_2(x)g(x) + r_2(x),$$

con $\deg(r_2)(x) = 0$ ó $\deg(r_2(x)) < \deg(g(x))$. Luego

$$q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x),$$

por tanto

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x). \tag{2.1.1}$$

Comparando los grados podemos ver que como $\deg((q_1(x) - q_2(x))g(x) \geq \deg(g(x))$ y $\deg(r_2(x) - r_1(x)) \leq \text{máx}(\deg(r_1(x)), \deg(r_2(x)))$, entonces se tiene que $\deg((q_1(x) - q_2(x))g(x) > \deg(r_2(x) - r_1(x))$, lo que claramente contradice la igualdad en la Ecuación (2.1.1), entonces se tiene que $r_2(x) = r_1(x)$ y así $q_1(x) = q_2(x)$. ■

Siguiendo con la notación presentada anteriormente, dado los polinomios $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ y $g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$, entonces el primer paso para calcular la división de f por g consiste en restar de f el polinomio $\dfrac{\text{lt}(f)}{\text{lt}(g)}g$. De esta forma se obtiene el polinomio $h = f - \dfrac{\text{lt}(f)}{\text{lt}(g)}g$, el cual es un primer residuo en el proceso de dividir f por g.

Notación 2.1. El polinomio h que se obtiene en el párrafo anterior se denomina una reducción de f por g y el proceso del cálculo de h se denota con

$$f \xrightarrow{g} h.$$

Si $h \neq 0$ con $\deg(h) \geq \deg(g)$, entonces se puede obtener un polinomio h', como una reducción de h por g, es decir

$$h \xrightarrow{g} h'.$$

El proceso de seguir la reducción de los residuos obtenidos al dividir por g se realiza hasta obtener un residuo r que sea cero ó de grado menor que el grado del polinomio g, este proceso se denota con

$$f \xrightarrow{g}_{+} r.$$

Definición 2.2. Sean f y g polinomios en $K[x]$. Se dice que g divide a f sí $f = gt$ para algún $t \in K[x]$.

A continuación se presenta la implementación del algoritmo de la división para polinomios en una variable usando el sistema de álgebra computacional GAP.

Algoritmo 2.1 (Algoritmo de la división en una variable)**.**

```
div:= function(f,g,var)
local q,r,m,n,k,lexord,l,l1,h;
lexord:=MonomialLexOrdering();
q:=Zero(R);
h:=Zero(R);
r:=f;
l:=DegreeIndeterminate(g,var);
l1:=DegreeIndeterminate(r,var);
while (l<=l1) and r<>Zero(R) do
       m:=LeadingTermOfPolynomial(r,lexord);
       n:=LeadingTermOfPolynomial(g,lexord);
       k:=DegreeIndeterminate(m,var)-DegreeIndeterminate(n,var);
       h:=(LeadingCoefficientOfPolynomial(r,lexord)/
          LeadingCoefficientOfPolynomial(g,lexord))*var^k;;
       q:=q+h;
       r:=r-h*g;
      l1:=DegreeIndeterminate(r,var);
od;
return [q,r];
end;
```

Nota 2.1. Es importante notar que al inicio del algoritmo de la división presentado en GAP, primero se debe utilizar el comando `var:=X(K,"var");` donde `var` define la indeterminada a utilizar sobre el campo `K`, al igual que el comando `R:=PolynomialRing(K,[var]);` que construye el anillo de polinomios sobre la indeterminada `var` con coeficientes en `K`.

Ejemplo 2.2. Sean $f = 2x^3 - 2x^2 + 2x + 8$ y $g = -4x^2 + 2x + 8$ en $\mathbb{Q}[x]$. La forma de utilizar el Algoritmo 2.1, en GAP es la siguiente

```
>x:=X(Rationals,"x");
x
>R:=PolynomialRing(Rationals,[x]);
Rationals[x]

>f:= 2*x^3-2*x^2+2*x+8;
2*x^3-2*x^2+2*x+8
```

```
>g:=-4*x^2+2*x+8;
-4*x^2+2*x+8


>div(f,g,x);
[ -1/2*x+1/4, 11/2*x+6 ]
```

Es decir de la división de los polinomios f por g se obtiene el cociente $-\frac{1}{2}x+14$ y el residuo $\frac{11}{2}x+6$.
El proceso que realiza internamente el Algoritmo 2.1 se explica a continuación.
Primero se define la indeterminada y el campo a trabajar con los comandos `x:=X(Rationals,"x");` y `R:=PolynomialRing(Rationals,[x]);` respectivamente.
Primer paso, para $f = 2x^3 - 2x^2 + 2x + 8$ y $g = -4x^2 + 2x + 8$ con el orden usual de polinomios y se hace el cociente $q = 0$ y el residuo $h = 0$, luego se tiene que $r = f$, $l = \deg(g) = 2$ y $ll = \deg(r) = 3$.
Se inicializa el `While:`
$\deg(g) = 2 \leq \deg(r) = 3$ y $r = f$, entonces $m = \mathrm{lt}(r) = 2x^3$, $n = \mathrm{lt}(g) = -4x^2$ y $k = \deg(r) - \deg(g) = 1$ y se calcula

$$h = \frac{\mathrm{lc}(r)}{\mathrm{lc}(g)}x^k = -\frac{x}{2},$$

$$q = q + h = -\frac{x}{2},$$

$$r = r - hg = -x^2 + 6x + 8,$$

con $\deg(r) = 2$. Volvemos al `While:`
$\deg(g) = 2 \leq \deg(r) = 3$ y $r \neq 0$ así, $m = -x^2$, $n = -4x^2$, $k = 0$, luego

$$h = \frac{1}{4},$$

$$q = -\frac{x}{2} + \frac{1}{4},$$

$$r = \frac{11x}{2} + 6,$$

con $\deg(r) = 1$. Finaliza el ciclo ya que $\deg(g) = 2 > \deg(r) = 1$, por tanto el algoritmo da como resultado el cociente y residuo

$$q = -\frac{x}{2} + \frac{1}{4},$$

$$r = \frac{11x}{2} + 6.$$

Ejemplo 2.3. Para $f = 4x^4 - 2x^2 + 5x + 1$ y $g = -4x^2 + 4x - 7$ en $\mathbb{Q}[x]$ si se divide f por g aplicando al algoritmo de la división se tiene que,

```
>div(f,g,x);
[ -x^2-x+5/4, -7*x+39/4 ]
```

el cociente $q = -x^2 - x + \frac{5}{4}$ y el residuo $r = -7x + \frac{39}{4}$.

Ejemplo 2.4. Para $f = 2x^5 - 4x^3 + x^2 - x + 2$ y $g = x^2 + x + 1$ en $\mathbb{Q}[x]$ si se divide al polinomio f por g se tiene que,

```
>div(f,g,x);
[ 2*x^3-2*x^2-4*x+7, -4*x-5 ]
```

el cociente $q = 2x^3 - 2x^2 - 4x + 7$ y el residuo $r = -4x - 5$.

2.2. Máximo común divisor

En esta sección se estudia el problema de encontrar el "mejor" conjunto generador para un ideal en el anillo de polinomios $K[x]$. De esta forma si I es un ideal tal que $I = \langle f_1, f_2, \ldots, f_s \rangle$ se demostrará que este ideal en realidad es generado por un solo elemento, el cual se conoce como el máximo común divisor de los polinomios $f_1, f_2, \ldots, f_s$. Para esto primero se estudia el concepto de máximo común divisor para dos polinomios y luego se extiende para un número arbitrario de polinomios. Además, se presenta la implementación en GAP de un algoritmo para el cálculo del máximo común divisor de dos polinomios de una variable, así como la solución de los Problemas 1.1 para éste caso.

Observación 2.1. Sea $I = \langle f, g \rangle$ y supóngase que $f \xrightarrow{g} h$. Luego $I = \langle h, g \rangle$. En efecto, dado que $f \xrightarrow{g} h$, se tiene que $h = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)} g$ de ahí que $h \in \langle f, g \rangle$. De igual forma $f = h + \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)} g$, de donde $f \in \langle h, g \rangle$. Por lo tanto $\langle f, g \rangle = \langle h, g \rangle$. En general se puede mostrar que si $f \xrightarrow{g}_+ r$, entonces $I = \langle r, g \rangle$.

Utilizando el algoritmo de la división repetidamente se obtiene el siguiente resultado.

Teorema 2.2. *Cada ideal de $K[x]$ se genera por un elemento.*[1]

Demostración. Sea I un ideal no nulo de $K[x]$. Para $g \in I$ con $g \neq 0$ y $\deg(g) = n$ con n la menor potencia posible, se observa que para cualquier $f \in I$ por el algoritmo de la división, ver Teorema 2.1, existen polinomios $q(x)$ y $r(x)$ en $K[x]$ tal que $f(x) = q(x)g(x) + r(x)$, con $r(x) = 0$ ó $\deg(r(x)) < \deg(g(x))$. Si $r(x) \neq 0$, entonces $r(x) = f(x) - q(x)g(x) \in I$ con $\deg(r(x)) < \deg(g(x))$ lo que contradice la escogencia del polinomio $g(x)$. Por lo tanto $r(x) = 0$ y así $f(x) = q(x)g(x)$ de donde se sigue que $I \subseteq \langle g \rangle$, por tanto $I = \langle g \rangle$. ■

Observación 2.2. El polinomio g del teorema anterior es único salvo múltiplos constantes.

[1] Un ideal que se genera por un elemento se denomina ideal principal y un dominio entero en donde cada ideal es principal se denomina Dominio de Ideales Principales (DIP), así por el Teorema 1.2 $K[x]$ es un DIP.

El teorema anterior permite encontrar el mejor conjunto generador para el ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$ a través del polinomio g en $K[x]$. Es decir si se tiene un sistema de ecuaciones $f_1 = 0, f_2 = 0, \ldots, f_s = 0$ con $f_i \in K[x]$ para $1 \leq i \leq s$. El Teorema 2.2 garantiza que $I = \langle f_1, f_2, \ldots, f_s \rangle = \langle g \rangle$, es decir el conjunto solución del sistema anterior es el mismo que el de la ecuación $g = 0$.

Evidentemente ahora surque la siguiente inquietud.

Pregunta 2.1. ¿Cómo calcular el polinomio g del teorema anterior?

Para resolver esta pregunta de la mejor manera dividiremos este proceso en dos partes. Primero se analizará la pregunta cuando el ideal $I = \langle f_1, f_2 \rangle$ con $I \subseteq K[x]$ y después se generalizará para el caso del ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$.

Ahora se presenta una definición que será fundamental para dar respuesta al la pregunta anterior.

Definición 2.3. Sean f_1, f_2 polinomios en $K[x]$ con uno de ellos no nulo. Se denomina el *Máximo Común Divisor* de los polinomios f_1, f_2, el cual se denota como $\mathrm{mcd}(f_1, f_2)$ al polinomio g tal que:

1. g divide a f_1 y a f_2.
2. Si $h \in K[x]$ divide a f_1 y a f_2, entonces h divide a g.
3. $\mathrm{lc}(g) = 1$, es decir g es mónico.

Ahora se muestra un resultado que permite relacionar el ideal $I = \langle f_1, f_2 \rangle$ con el polinomio $\mathrm{mcd}(f_1, f_2)$.

Teorema 2.3. *Sean $f_1, f_2 \in K[x]$, con uno de ellos no nulo, luego el* $\mathrm{mcd}(f_1, f_2)$ *existe y además* $\langle f_1, f_2 \rangle = \langle \mathrm{mcd}(f_1, f_2) \rangle$.

Demostración. Por el Teorema 2.2, existe $g \in K[x]$ tal que $\langle f_1, f_2 \rangle = \langle g \rangle$. Debemos probar que $g = \mathrm{mcd}(f_1, f_2)$. Dado que g es único salvo múltiplos constantes podemos suponer que $\mathrm{lc}(g) = 1$, luego de la igualdad $\langle f_1, f_2 \rangle = \langle g \rangle$ se tiene que $f_1 = h_1 g$ y $f_2 = h_2 g$ con $h_1, h_2 \in K[x]$ de ahí que g divide a f_1 y g divide a f_2. Supóngase ahora que un polinomio $h \in K[x]$ divide a f_1 y a f_2, es decir h divide a cualquier combinación lineal de los polinomios f_1 y f_2, en particular divide a g ya que g está en $\langle f_1, f_2 \rangle$. Entonces, $g = \mathrm{mcd}(f_1, f_2)$. ■

A continuación se muestra una algoritmo para calcular el máximo común divisor de dos polinomios que generen a un ideal. Este procedimiento se conoce como algoritmo Euclídeo.

Lema 2.1. *Sean $f_1, f_2 \in K[x]$, con al menos uno de ellos no nulo, entonces el* $\mathrm{mcd}(f_1, f_2) = \mathrm{mcd}(f_1 - q f_2, f_2)$, *para todo $q \in K[x]$*

Demostración. Primero es preciso notar que $\langle f_1, f_2\rangle = \langle f_1 - qf_2, f_2\rangle$. En efecto, claramente $f_1 - qf_2 \in \langle f_1, f_2\rangle$. Ahora ya que $f_1 = 1(f_1 - qf_2) + qf_2$, entonces $f_1 \in \langle f_1 - qf_2, f_2\rangle$. Ahora aplicando el teorema anterior

$$\langle \text{mcd}(f_1, f_2)\rangle = \langle f_1, f_2\rangle = \langle f_1 - qf_2, f_2\rangle = \langle \text{mcd}(f_1 - qf_2, f_2)\rangle.$$

Dado que el generador de un ideal principal es único salvo múltiplos constantes y que el coeficiente líder del máximo común divisor de dos polinomios, se sigue que $\text{mcd}(f_1, f_2) = \text{mcd}(f_1 - qf_2, f_2)$. ■

Siguiendo la pregunta del cálculo del generador de un ideal en $K[x]$, se va a estudiar para el caso más general de un ideal $I = \langle f_1, f_2, \ldots, f_s\rangle$ con $f_1, f_2, \ldots, f_s \in K[x]$ no todos nulos.

Definición 2.4. Sean $f_1, f_2, \ldots, f_s$ polinomios en $K[x]$ no todos nulos. Se denomina el *Máximo Común Divisor* de los polinomios $f_1, f_2, \ldots, f_s$, que se denota como $\text{mcd}(f_1, f_2, \ldots, f_s)$ al polinomio g tal que

1. g divide a cada f_i con $i = 1, 2, \ldots, s$.
2. Si $h \in K[x]$ divide a cada f_i con $i = 1, 2, \ldots, s$, entonces h divide a g.
3. $\text{lc}(g) = 1$, es decir g es mónico.

De igual forma que en el caso de ideales generados por dos polinomios, se presenta un resultado para la relación entre el ideal $I = \langle f_1, f_2, \ldots, f_s\rangle$ y el $\text{mcd}(f_1, f_2, \ldots, f_s)$.

Teorema 2.4. *Sean $f_1, f_2, \ldots, f_s$ polinomios en $K[x]$ luego.*

1. $\langle f_1, f_2, \ldots, f_s\rangle = \langle \text{mcd}(f_1, f_2, \ldots, f_s)\rangle$.
2. *Si $s \geq 3$, entonces* $\text{mcd}(f_1, f_2, \ldots, f_s) = \text{mcd}(f_1, \text{mcd}(f_2, \ldots, f_s))$.

Demostración. La prueba del item uno se hace de forma similar al Teorema 2.3. Por Teorema 2.2, existe $g \in K[x]$ tal que $\langle f_1, f_2, \ldots, f_s\rangle = \langle g\rangle$. Se debe probar que $g = \text{mcd}(f_1, f_2, \ldots, f_s)$. Dado que g es único salvo múltiplos constantes podemos suponer que $\text{lc}(g) = 1$, como $f_1, f_2, \ldots, f_s \in \langle g\rangle$ se tiene que g divide a cada f_i con $i = 1, 2, \ldots, s$. Para $h \in K[x]$ tal que h divide a cada f_i, se tiene que h divide a cualquier combinación lineal de los polinomios $f_1, f_2, \ldots, f_s$, en particular divide a g, ya que g está en $\langle f_1, f_2, \ldots, f_s\rangle$. De esta manera, se obtiene el resultado deseado.
Por otro lado supóngase que $h = \text{mcd}(f_2, \ldots, f_s)$, luego por la primera parte del teorema $\langle f_2, \ldots, f_s\rangle = \langle h\rangle$, y así $\langle f_1, f_2, \ldots, f_s\rangle = \langle f_1, h\rangle$. Aplicando nuevamente el primer item a los ideales $\langle f_1, f_2, \ldots, f_s\rangle$ y $\langle f_1, h\rangle$ se tiene que $\langle \text{mcd}(f_1, f_2, \ldots, f_s)\rangle = \langle \text{mcd}(f_1, h)\rangle$ y del hecho que el coeficiente líder del máximo común divisor es uno y que genera un ideal principal salvo múltiplos constantes se sigue que $\text{mcd}(f_1, f_2, \ldots, f_s) = \text{mcd}(f_1, h) = \text{mcd}(f_1, \text{mcd}(f_2, \ldots, f_s))$. ■

Observación 2.3. Para calcular el máximo común divisor de los polinomios $(f_1, f_2, \ldots, f_s)$ se procede por inducción por el item dos del Teorema 2.4.

A continuación se presenta el algoritmo Euclídeo que se usa para calcular el máximo común divisor de dos polinomios con ayuda del sistema de álgebra computacional GAP.

Algoritmo 2.2 (Algoritmo Euclídeo)**.**

```
mcd:= function(f1,f2)
local f,g,lexord,r;
lexord:=MonomialLexOrdering();
r:=Zero(R);
f:=f1;
g:=f2;
while g<>Zero(R)do
      r:=QuotientRemainder(f,g)[2];
      f:= g;
      g:= r;
od;
f:=(1/LeadingCoefficient(f))*f;
return f;
end;
```

Ejemplo 2.5. Sean $f_1 = x^3 - 3x + 2$ y $f_2 = x^2 - 1$ en $\mathbb{Q}[x]$. El cálculo del máximo común divisor de los polinomios f_1 y f_2 aplicando el Algoritmo 2.2 se expresa en GAP como

```
>x:=X(Rationals,"x");
x
>R:=PolynomialRing(Rationals,[x]);
Rationals[x]

>f_1:=x^3-3*x+2;
x^3-3*x+2

>f_2:=x^2-1;
x^2-1
```

```
>mcd(f_1,f_2);
x-1
```

Así el máximo común divisor de los polinomios f_1 y f_2 es $x-1$. La prueba de escritorio de este ejemplo se encuentra a continuación.
Se debe recordar que primero se debe definir el anillo de polinomios y la indeterminada a utilizar, ver Nota 2.1. Primer paso, para $f_1 = x^3 - 3x + 2$ y $f_2 = x^2 - 1$ con el orden usual de polinomios hacemos $f = f_1 = x^3 - 3x + 2$, $g = f_2 = x^2 - 1$.
Se inicializa el `While:`

$$x^3 - 3x + 2 \xrightarrow{x^2-1} -2x + 2 = r,$$

$$f = x^2 - 1,$$

$$g = -2x + 2.$$

Nuevamente `While:` y hacemos la división de f por g,

$$x^2 - 1 \xrightarrow{-2x+2} 0 = r,$$

$$f = -2x + 2,$$

$$g = 0.$$

Termina el ciclo `While` y hacemos

$$f = -\frac{1}{2}-2x + 2 = x - 1.$$

Por tanto el $\mathrm{mcd}(f_1, f_2) = x - 1$.

Ejemplo 2.6. Para $f_1 = 2x^2 + 2$ y $f_2 = x^2 + 1$ en $\mathbb{Q}[x]$

```
>mcd(f_1,f_2);
x^2+1
```

El $\mathrm{mcd}(f_1, f_2) = x^2 + 1$.

Ejemplo 2.7. Para $f_1 = x^5 - 2x^4 - x^2 + 2x$, $f_2 = x^7 + x^6 - 2x^4 - 2x^3 + x + 1$ y $f_3 = x^6 - 2x^5 + x^4 - 2x^3 + x^2 - 2x$ en $\mathbb{Q}[x]$, para calcular el $\mathrm{mcd}(f_1, f_2, f_3)$, primero se calcula el $\mathrm{mcd}(f_1, f_2)$ a saber

```
>mcd(f_1,f_2);
x^3-1
```

Sea $h = x^3 - 1$ y finalmente se realiza el cálculo del $\mathrm{mcd}(h, f_3)$

```
>mcd(h,f_3);
x^2+x+1
```

Así el $\mathrm{mcd}(f_1, f_2, f_3) = x^2 + x + 1$.

Es turno ahora de resolver los Problemas 1.1 que se plantearon en el primer capítulo para el caso del anillo $K[x]$.

Solución a los Problemas 1.1. Dados un ideal $I = \langle f_1, f_2, \ldots, f_t\rangle$ y un polinomio f en $K[x]$.

1. Decidir cuando el polinomio $f \in I$. Para solucionar este problema en el anillo de polinomios $K[x]$ primero se calcula el polinomio $g = \mathrm{mcd}(f_1, f_2, \ldots, f_s)$ y se usa el algoritmo de la división de f por g, obteniendo el siguiente resultado

$$f \in I = \langle g\rangle \text{ si y sólo si } f \xrightarrow{g}_+ 0.$$

Ejemplo 2.8. Para el Ejemplo 2.7 si se toma el ideal $I = \langle f_1, f_2, f_3\rangle$ y para el polinomio $f_4 = -x^9+4x^8-2x^7-3x^6+6x^5-10x^4+6x^3-7x^2+15x+1$ se tiene que el $g = \mathrm{mcd}(f_1, f_2, f_3) = x^2 + x + 1$, luego aplicando el Algoritmo 2.1

```
>div(f_4,g,x);
[ -x^7+5*x^6-6*x^5-2*x^4+14*x^3-22*x^2+14*x+1, 0 ]
```

Así el algoritmo devuelve residuo 0 y el cociente $q = -x^7+5x^6-6x^5-2x^4+14x^3-22x^2+14x+1$, por tanto el polinomio $f_4 = -x^9+4x^8-2x^7-3x^6+6x^5-10x^4+6x^3-7x^2+15x+1$ pertenece al ideal $I = \langle f_1, f_2, f_3\rangle$, esto es $f_4 = -x^9+4x^8-2x^7-3x^6+6x^5-10x^4+6x^3-7x^2+15x+1 = qg$. Pero si se toma el polinomio $f_5 = 2x^{10} + 3x^9 + 5x^6 - 8x^5 + x^4 - 3x^3 + 2x^2 + 15x + 1$ aplicando el Algoritmo 2.1 se tiene que

```
>M:=div(f5,g,x);
[ 2*x^8+x^7-3*x^6+2*x^5+6*x^4-16*x^3+11*x^2+2*x-11, 24*x+12 ]
```

Donde $2x^8 + x^7 - 3x^6 + 2x^5 + 6x^4 - 16x^3 + 11x^2 + 2x - 11$ es el cociente y el residuo es $24x + 12$. Por lo tanto el polinomio $f_5 = 2x^{10} + 3x^9 + 5x^6 - 8x^5 + x^4 - 3x^3 + 2x^2 + 15x + 1$ no pertenece al ideal $I = \langle f_1, f_2, f_3\rangle$.

2. Si $f \in I$, determinar los polinomios $v_1, v_2, \ldots, v_s \in K[x]$ tal que $f = v_1f_1 + v_2f_2 + \cdots + v_sf_s$. Los polinomios $v_1, v_2, \ldots, v_s$ se encuentran con el algoritmo de la división, es decir, se hallan a partir de la división de f por $g = \mathrm{mcd}(f_1, f_2, \ldots, f_s)$.
Una forma alternativa de encontrar los polinomios $v_1, v_2, \ldots, v_s$ es modificando el Algoritmo 2.2 como se muestra a continuación. Este nuevo algoritmo da como resultado el máximo común divisor de dos polinomios f_1, f_2 y polinomios v_1, v_2 tales que $\mathrm{mcd}(f_1, f_2) = v_1f_1 + v_2f_2$.

Algoritmo 2.3 (Algoritmo Euclídeo Extendido)**.**

```
mcdextrec:= function(f1,f2,var)
local L,s, S;
if f2<>Zero(R) then
 L:=div(f1,f2,var);
 S:=mcdextrec(f2,L[2],var);
 s:=S[2];
 S[2]:=S[3];
 S[3]:=-L[1]*S[3]+s;
else
  S:=[1/LeadingCoefficient(f1)*f1,1/LeadingCoefficient(f1)*One(R),
     1/LeadingCoefficient(f1)*Zero(R)];
fi;
 return S;
end;
```

Ejemplo 2.9. Siguiendo con el Ejemplo 2.8 se expresará el polinomio $f_4 = -x^9+4x^8-2x^7-3x^6+6x^5-10x^4+6x^3-7x^2+15x+1$ como combinación lineal de los polinomios f_1, f_2, f_3 como se sigue a continuación.
Primero se aplica el Algoritmo 2.3 para los polinomios $f_1 = x^5 - 2x^4 - x^2 + 2x$ y $f_2 = x^7 + x^6 - 2x^4 - 2x^3 + x + 1$, es decir

```
>L:=mcdextrec(f_1,f_2,x);
[ x^3-1, -11/21*x^3-4/7*x^2-1/7*x+5/21, 11/21*x-1 ]
```

Que devuelve el polinomio $L[1] = x^3 - 1$ el cual es el máximo común divisor de los polinomios f_1, f_2 y los polinomios $L[2] = -\frac{11}{21}x^3 - \frac{4}{7}x^2 - \frac{1}{7}x + \frac{5}{21}$ y $L[3] = \frac{11}{21}x - 1$ para expresar a $L[1]$ como combinación lineal de los polinomios f_1 y f_2, como $L[1] = L[2]f_1 + L[3]f_2$, es decir $x^3 - 1 = (-\frac{11}{21}x^3 - \frac{4}{7}x^2 - \frac{1}{7}x + \frac{5}{21})f_1 + (\frac{11}{21}x - 1)f_2$.
Luego nuevamente se utiliza el Algoritmo 2.3 para los polinomios $L[1] = x^3 - 1$ y f_3

```
>LL:=mcdextrec(L[1],f_3,x);
[ x^2+x+1, x^3-2*x^2+x-1, -1 ]
```

Esto devuelve el máximo común divisor de los polinomios f_1, f_2, f_3 es decir

$$g = \text{mcd}(f_1, f_2, f_3) = x^2 + x + 1.$$

Además, proporciona los polinomios que expresan a g como combinación lineal de $L[1]$ y f_3 a través del los polinomios $LL[2] = x^3 - 2x^2 + x - 1$ y $LL[3] = -1$ es decir

$$g = LL[2]L[1] + LL[3]f_3.$$

Ahora reemplazando $L[1]$ por $L[2]f_1 + L[3]f_2$ se tiene que

$$g = LL[2](L[2]f_1 + L[3]f_2) + LL[3]f_3,$$

es decir

$$g = (LL[2]L[2])f_1 + (LL[2]L[3])f_2 + (LL[3])f_3.$$

Por el ejemplo anterior de la división del polinomio f_4 por g se tiene que $f_4 = qg$, donde q es el cociente $q = -x^7 + 5x^6 - 6x^5 - 2x^4 + 14x^3 - 22x^2 + 14x + 1$ reemplazando el polinomio g se tiene que

$$f_4 = q((LL[2]L[2])f_1 + (LL[2]L[3])f_2 + (LL[3])f_3),$$

es decir

$$f_4 = (LL[2]L[2]q)f_1 + (LL[2]L[3]q)f_2 + (LL[3]q)f_3,$$

donde

```
>LL[2]*L[2]*q;
11/21*x^13-65/21*x^12+106/21*x^11+2/21*x^10-61/7*x^9+289/21*x^8-29/3*x^7-22/21\
*x^6-10/3*x^5+14*x^4-250/21*x^3+221/21*x^2-62/21*x-5/21

>LL[2]*L[3]*q;
-11/21*x^11+14/3*x^10-334/21*x^9+533/21*x^8-37/3*x^7-653/21*x^6+1780/21*x^5-10\
7*x^4+1697/21*x^3-857/21*x^2+262/21*x+1

>LL[3]*q;
x^7-5*x^6+6*x^5+2*x^4-14*x^3+22*x^2-14*x-1
```

3. Las clases representativas del elemento $f + I$ en $K[x]/I$ son de la forma $r + I$, donde r es el residuo de la división de f por $g = \text{mcd}(f_1, f_2, \ldots, f_s)$.

   Ejemplo 2.10. Siguiendo con el Ejemplo 2.8 la clase lateral del elemento $f_4 + I$ en $\mathbb{Q}[x]/I$ es de la forma $0 + I$, donde 0 es el residuo de la división de f_4 por $g = \text{mcd}(f_1, f_2, f_3)$ y la clase lateral del elemento $f_5 + I$ en $\mathbb{Q}[x]/I$ es de la forma $24x + 12 + I$, donde $24x + 12$ es el residuo de la división de f_5 por $g = \text{mcd}(f_1, f_2, f_3)$.

4. Las clases laterales que forman una base para el K-espacio vectorial $K[x]/I$ son

$$\{1 + \langle g\rangle, x + \langle g\rangle, \ldots, x^{d-1} + \langle g\rangle\},$$

donde $I = \langle g\rangle$, g es el máximo común divisor de un conjunto finito de polinomios generadores de I y $d = \deg(g)$, es una base para $K[x]/\langle g\rangle$.
En efecto, $\{1 + \langle g\rangle, x + \langle g\rangle, \ldots, x^{d-1} + \langle g\rangle\}$ es linealmente independiente, ya que

$$\alpha_0(1 + \langle g\rangle) + \alpha_1(x + \langle g\rangle) + \cdots + \alpha_{d-1}(x^{d-1} + \langle g\rangle) = 0 = \langle g\rangle,$$

luego por propiedades de clases laterales se tiene que

$$(\alpha_0 + \alpha_1 x + \cdots + \alpha_{d-1}x^{d-1}) + \langle g\rangle = 0 = \langle g\rangle,$$

es decir

$$\alpha_0 + \alpha_1 x + \cdots + \alpha_{d-1}x^{d-1} \in \langle g\rangle,$$

la única posibilidad para que esto ocurra es que

$$\alpha_0 = \alpha_1 = \cdots = \alpha_{d-1} = 0,$$

ya que g tiene grado d y $\langle g\rangle$ contiene a los múltiplos de g.
$\{1+\langle g\rangle, x+\langle g\rangle, \ldots, x^{d-1}+\langle g\rangle\}$ genera al espacio vectorial $K[x]/\langle g\rangle$. En efecto, sea $f(x) \in K[x]$, luego $f(x) + \langle g\rangle \in K[x]/\langle g\rangle$, ahora por el algoritmo de la división se tiene que

$$f(x) = g(x)q(x) + r(x), \text{ con } r(x) = 0 \text{ ó } deg\ r(x) < d.$$

Si $r(x) = 0$, se tiene que $f(x) = g(x)q(x)$, entonces $f(x) = 0$ en $K[x]/\langle g\rangle$ y así $f(x) + \langle g(x)\rangle = \langle g(x)\rangle$, de donde

$$f(x) + \langle g(x)\rangle = 0(1 + \langle g(x)\rangle) + 0(x + \langle g(x)\rangle) + \ldots + 0(x^{d-1} + \langle g(x)\rangle).$$

Si deg $r(x) < d$, con $f(x) = a_o + a_1x + \ldots + a_{d-1}x^{d-1}$, entonces

$$\begin{aligned} f(x) + \langle g(x)\rangle &= (a_o + a_1x + \ldots + a_{d-1}x^{d-1}) + \langle g(x)\rangle \\ &= a_0 + \langle g(x)\rangle + a_1x + \langle g(x)\rangle + \ldots + a_{d-1}x^{d-1} + \langle g(x)\rangle \\ &= a_0(1 + \langle g(x)\rangle) + a_1(x + \langle g(x)\rangle) + \ldots + a_{d-1}(x^{d-1} + \langle g(x)\rangle). \end{aligned}$$

Ejemplo 2.11. Continuando con el ejemplo anterior las clases laterales que forman una base para $\mathbb{Q}[x]/I$ son

$$\{1 + \langle x^2 + x + 1\rangle, x + \langle x^2 + x + 1\rangle\},$$

con $g = \text{mcd}(f_1, f_2, f_3) = x^2 + x + 1$.

Capítulo 3

Polinomios en varias variables

En este capítulo se presenta una generalización de la teoría de polinomios en una variable estudiando el anillo de polinomios en varias variables $K[x_1, x_2, \ldots, x_n]$ con K un campo. A manera de introducción, en la primera sección se estudian los Problemas 1.1 en el caso de polinomios lineales en varias variables y su solución con el método de Gauss-Jordan. Posteriormente, en la Sección 3.2 se introduce el concepto de orden de términos, con el cual se definen el producto potencia líder, el termino líder y el coeficiente líder de un polinomio y se presentan tres ejemplos de orden de términos. Finalmente, en la tercera sección se estudia el algoritmo de la division para polinomios en varias variables.

3.1. Caso lineal

Para el caso en que el sistema dado en la Ecuación (1.2.1), sea un sistema de ecuaciones lineales[1] $f_1 = 0, f_2 = 0, \ldots, f_s = 0$ en el anillo $K[x_1, x_2, \ldots, x_n]$, recordamos que se puede usar el método de Gauss-Jordan a través de la matriz asociada al sistema en su forma escalonada reducida. El método consiste en transformar un sistema de ecuaciones lineales en otro equivalente (que tiene las mismas soluciones) más sencillo de resolver a través de operaciones elementales de fila[2]. Este proceso además permite cambiar el conjunto generador $\{f_1, f_2, \ldots, f_s\}$ de un ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$ por otro más simple. Para ejemplificar mejor este método consideramos el siguiente ejemplo.

Ejemplo 3.1. Sea $f = x - y - 3z = 0$, $g = 2x - 3y - z = 0$ y consideremos el ideal $I = \langle f, g \rangle$, la variedad $V(f, g)$ es la solución del sistema

$$f = x - y - 3z = 0$$

[1] Conjunto de ecuaciones lineales en donde cada ecuación es de primer grado.

[2] Las operaciones elementales de fila son: intercambiar filas, multiplicar una fila por un escalar diferente de cero y sumar un múltiplo de una fila a otra

$$g = 2x - 3y - z = 0.$$

Considere la matriz del sistema

$$\begin{pmatrix} 1 & -1 & -3 \\ 2 & -3 & -1 \end{pmatrix}.$$

Si se denota a f_1 como la fila uno, f_2 como la fila dos se puede transformar la matriz anterior a través de operaciones elementales de fila, es decir

$$\begin{pmatrix} 1 & -1 & -3 \\ 2 & -3 & -1 \end{pmatrix} \xrightarrow{f_2 \to f_2 - 2f_1} \begin{pmatrix} 1 & -1 & -3 \\ 0 & -1 & 5 \end{pmatrix}.$$

Por tanto se obtiene el nuevo sistema

$$f = x - y - 3z$$
$$h = -y + 5z.$$

Utilizando el proceso anterior se puede hacer el cambio (simplificar) del conjunto generador para el ideal $I = \langle f, g \rangle$ a otro. Para esto se observa que $I = \langle f, g \rangle = \langle f, h \rangle$, en efecto el polinomio $h = -y + 5z$ se obtuvo de la resta de la fila dos de la matriz del sistema menos dos veces la fila uno, es decir $h = f_2 - 2f_1 = g - 2f = -y + 5z$, por tanto $h \in I = \langle f, g \rangle$, del mismo modo se tiene que $g = h + 2f = 2x - 3y - z$, luego $g \in \langle f, h \rangle$. De esta forma se simplifica el conjunto generador para I a saber $\{f, h\}$, con el fin de determinar de manera mas fácil la variedad

$$V(I) = V(f, g) = V(f, h) = \{\lambda(8, 5, 1) | \lambda \in \mathbb{R}\}.$$

El proceso de reemplazar el polinomio g por h usando f se puede observar como la reducción de f a h por medio de g, ver la Notación 2.1; es decir

$$f \xrightarrow{g} h.$$

En otras palabras el método básico consiste en sustraer el término líder de un polinomio de otro. Cabe mencionar que existe un cierto orden en las variables en el proceso anterior. Por ejemplo para los polinomios $f = x - y - 3z$ y $g = 2x - 3y - z$, primero se procedió a eliminar la variable x, luego y y finalmente z. Pero si cambiamos el orden en los términos de f y g por $f = -y - 3z + x$ y $g = -3y - z + 2x$ se procederá primero a eliminar la variable y, luego z y posteriormente x.

Utilizando ideas similares a las presentadas en el Capítulo 2 se podrían resolver los Problemas 1.1. En las siguientes secciones de este capítulo se presentan herramientas que serán útiles para resolver los problemas mencionados en el Capitulo 4 de forma general.

3.2. Ordenes de términos

El objetivo de esta sección es presentar las propiedades, características y condiciones para obtener un orden en los términos de un polinomio.

Definición 3.1. Se define el conjunto de productos potencia, en $K[x_1, x_2, \ldots, x_n]$, como la colección de monomios de la forma $x_1^{\beta_1} \cdots x_n^{\beta_n}$ con $\beta_i \in \mathbb{N}$; es decir

$$\mathbb{T}^n = \{x_1^{\beta_1} \cdots x_n^{\beta_n} : \ \beta_i \in \mathbb{N}, \ i = 1, 2, \ldots, n\}.$$

El producto potencia $x_1^{\beta_1} \cdots x_n^{\beta_n}$ se denota por x^β, con $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}$.

Definición 3.2. Para cualquier $x^\alpha, x^\beta \in \mathbb{T}^n$ se define un orden total si exactamente una de las siguientes relaciones se cumplen

$$x^\alpha < x^\beta, \quad x^\alpha = x^\beta \ \text{ ó } \ x^\alpha > x^\beta.$$

En la sección anterior se tuvo en cuenta un cierto orden en las variables, lo que hace que el proceso termine, es decir, que el proceso de reducción se realice en un número finito de pasos. Para esto se necesita un buen ordenamiento entre los productos potencia cuya característica principal es que no exista una cadena descendiente infinita

$$x^\alpha > x^\beta > x^\gamma > \cdots .$$

Un orden que satisface todas estas condiciones se denomina un orden de términos. Estas ideas se ven recopiladas en la siguiente definición.

Definición 3.3. Un orden de términos en $\mathbb{T}^n$ es un orden total $<$ en $\mathbb{T}^n$ que satisface las siguientes condiciones:

1. $1 < x^\alpha$ para todo $x^\alpha \in \mathbb{T}^n$, con $x^\alpha \neq 1$.
2. Si $x^\alpha < x^\beta$, entonces $x^\gamma x^\alpha < x^\gamma x^\beta$, para todo $x^\gamma \in \mathbb{T}^n$.

A continuación se presentan algunos ejemplos de tipos de orden. Se puede probar que estos tipos de orden satisfacen la Definición 3.3.

Definición 3.4. Se define el orden lexicográfico *lex*, con $x_1 > x_2 > \cdots > x_n$ para $x^\alpha, x^\beta \in \mathbb{T}^n$ con $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$

$$x^\alpha < x^\beta,$$

si y sólo si las primeras coordenadas α_i y β_i en α y β, al leer de izquierda a derecha que son diferentes satisfacen que $\alpha_i < \beta_i$.

Ejemplo 3.2. Para el caso de dos variables x_1, x_2 con $x_1 > x_2$ se tiene que

$$1 < x_2 < {x_2}^2 < {x_2}^3 < \cdots < x_1 < x_2x_1 < {x_2}^2x_1 < \cdots < .$$

Es importante señalar que primero se debe definir un orden en las variables, por ejemplo para el caso de x_1, x_2 con $x_1 < x_2$ se tiene que

$$1 < x_1 < {x_1}^2 < {x_1}^3 < \cdots < x_1 < x_1x_2 < {x_1}^2x_2 < \cdots <$$

Definición 3.5. Se define el el orden lexicográfico gradual *deglex* con $x_1 > x_2 > \cdots > x_n$ para $x^\alpha, x^\beta \in \mathbb{T}^n$ con $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$

$$x^\alpha < x^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ o \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \\ \text{y } x^\alpha < x^\beta \text{ con respecto al orden lexicográfico con } x_1 > x_2 > \ldots > x_n. \end{cases}$$

Ejemplo 3.3. Para el caso de dos variables x_1, x_2 con $x_1 > x_2$ se tiene que

$$1 < x_2 < x_1 < {x_2}^2 < x_1x_2 < {x_1}^2 < \cdots < {x_2}^3 < {x_1}^2x_2 < \cdots < .$$

Definición 3.6. Se define el orden lexicográfico gradual inverso *degrevlex* con $x_1 > x_2 > \cdots > x_n$ para $x^\alpha, x^\beta \in \mathbb{T}^n$ con $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$

$$x^\alpha < x^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ o \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \\ \text{y las primeras coordenadas } \alpha_i \text{ y } \beta_i \text{ en } \alpha \text{ y } \beta \text{ al leer de derecha a izquierda que son} \\ \text{diferentes satisfacen que } \alpha_i > \beta_i. \end{cases}$$

Ejemplo 3.4. Para el caso de tres variables x_1, x_2, x_3 con $x_1 > x_2 > x_3$ se tiene que

$$x_1^2x_2x_3 < x_1x_2^3.$$

Proposición 3.1. *Para $x^\alpha, x^\beta \in \mathbb{T}^n$, si x^α divide a x^β entonces $x^\alpha \leq x^\beta$.*

Demostración. Por hipótesis x^α divide a x^β, luego existe $x^\gamma \in \mathbb{T}^n$ tal que $x^\beta = x^\alpha x^\gamma$. Por la primera condición de la Definición 3.3 se tiene que $x^\gamma \geq 1$. Así aplicando la segunda condición se tiene que $x^\beta = x^\alpha x^\gamma \geq x^\alpha$. ■

Teorema 3.1. *Todo orden de términos sobre $\mathbb{T}^n$ es un buen ordenamiento; esto es, para cada subconjunto A de $\mathbb{T}^n$ existe $x^\alpha \in A$ tal que $x^\alpha \leq x^\beta$ para todo $x^\beta \in A$.*

Demostración. Supóngase lo contrario; es decir, que existe un orden de términos que no es un buen ordenamiento, entonces existen $x^{\alpha_i} \in \mathbb{T}^n$, $i = 1, 2, \ldots$ tal que

$$x^{\alpha_1} > x^{\alpha_2} > x^{\alpha_3} > \cdots \tag{3.2.1}$$

Esto define una cadena descendiente de ideales en $K[x_1, x_2, \ldots, x_n]$

$$< x^{\alpha_1} > \subsetneq < x^{\alpha_1}, x^{\alpha_2} > \subsetneq < x^{\alpha_1}, x^{\alpha_2}, x^{\alpha_3} > \subsetneq \cdots \tag{3.2.2}$$

Para notar esto veamos que $< x^{\alpha_1}, \ldots, x^{\alpha_i} > \neq < x^{\alpha_1}, \ldots, x^{\alpha_{i+1}} >$. En efecto, si se da la igualdad $x^{\alpha_{i+1}} \in < x^{\alpha_1}, \ldots, x^{\alpha_i} >$, luego

$$x^{\alpha_{i+1}} = \sum_{j=1}^{i} \mu_j x^{\alpha_j},$$

donde cada μ_j es un polinomio en $K[x_1, x_2, \ldots, x_n]$. Ahora si se expande cada polinomio μ_j como una combinación lineal de productos potencia, entonces cada término de $\mu_j x^{\alpha_j}$ es divisible por algún x^{α_j} con $1 \leq j \leq i$. Así $x^{\alpha_{i+1}}$ aparece como el producto potencia de un término de $\mu_j x^{\alpha_j}$, por lo tanto $x^{\alpha_{i+1}}$ es divisible por algún x^{α_j} con $1 \leq j \leq i$ de donde $x^{\alpha_{i+1}} \geq x^{\alpha_j}$ para algún $1 \leq j \leq i$. Por tanto no se cumple (3.2.1). Así la cadena de ideales es estrictamente creciente en $K[x_1, x_2, \ldots, x_n]$, lo cual es una contradicción con el Teorema de la base de Hilbert, ver Teorema 1.3. ■

Definición 3.7. Para un orden de términos en $K[x_1, x_2, \ldots, x_n]$, se tiene que todo polinomio $f \in K[x_1, x_2, \ldots, x_n]$, con $f \neq 0$, se puede expresar como

$$f = a_1 x^{\alpha_1} + a_2 x^{\alpha_2} + \cdots + a_r x^{\alpha_r},$$

donde $0 \neq a_i \in K$, $x^{\alpha_i} \in \mathbb{T}^n$ y $x^{\alpha_1} > x^{\alpha_2} > \cdots > x^{\alpha_r}$. Se denota con

- $\mathrm{lp}(f) = x^{\alpha_1}$, al *producto potencia líder* de f;
- $\mathrm{lc}(f) = a_1$, al *coeficiente líder* de f;
- $\mathrm{lt}(f) = a_1 x^{\alpha_1}$, al *término líder* de f.

Ejemplo 3.5. Para el polinomio $f = 2x^2yz + 3xy^3 - 2x^3$ con $x > y > z$ se tiene que:

1. Utilizando el orden lexicográfico se puede ver que $\mathrm{lp}(f) = x^3$, $\mathrm{lc}(f) = -2$ y $\mathrm{lt}(f) = -2x^3$.
2. Si utilizamos el orden lexicográfico gradual se observa que $\mathrm{lp}(f) = x^2yz$, $\mathrm{lc}(f) = 2$ y $\mathrm{lt}(f) = 2x^2yz$.
3. Para el orden lexicográfico gradual inverso se tiene $\mathrm{lp}(f) = xy^3$, $\mathrm{lc}(f) = 3$ y $\mathrm{lt}(f) = 3xy^3$.

3.3. Algoritmo de la división

En esta sección se presenta el algoritmo de la división para polinomios en $K[x_1, x_2, \ldots, x_n]$ de cualquier grado el cual es una generalización del caso de una variable. Este algoritmo se puede ver como una extensión del algoritmo de la división en $K[x]$, aunque en realidad este es más que una generalización puesto que permite dividir un polinomio por un conjunto de polinomios en $K[x_1, x_2, \ldots, x_n]$.

Definición 3.8. Sean f, g, h en $K[x_1, x_2, \ldots, x_n]$, con $g \neq 0$. Se dice que f se reduce a h módulo g en un solo paso si $\mathrm{lp}(g)$ divide a un término X no nulo del polinomio f y

$$h = f - \frac{X}{\mathrm{lt}(g)} g.$$

Este procedimiento se denota con

$$f \xrightarrow{g} h.$$

Ejemplo 3.6.

1. Sean $f = 6x^2y - x + 4y^3 - 1$ y $g = 2xy + y^3$ polinomios en $\mathbb{Q}[x, y]$ con el orden de términos *lex*, con $x > y$, luego $\mathrm{lt}(g) = 2xy$ y así

$$f \xrightarrow{g} h,$$

$$\begin{aligned} h &= 6x^2y - x + 4y^3 - 1 - \frac{6x^2y}{2xy}(2xy + y^3) \\ &= 6x^2y - x + 4y^3 - 1 - 3x(2xy + y^3) \\ &= 6x^2y - x + 4y^3 - 1 - 6x^2y - 3xy^3 \\ &= -3xy^3 - x + 4y^3 - 1. \end{aligned}$$

   En este caso observe que el único término de f que es divisible por $\mathrm{lt}(g)$ es $X = 6x^2y = \mathrm{lt}(f)$.

2. Considerando los polinomios del ejemplo anterior con el orden de términos *deglex* con $x > y$ se tiene que ahora que $\mathrm{lt}(g) = y^3$ y así

$$f \xrightarrow{g} h$$

$$\begin{aligned} h &= 6x^2y - x + 4y^3 - 1 - \frac{4y^3}{y^3}(2xy + y^3) \\ &= 6x^2y - x + 4y^3 - 1 - 4(2xy + y^3) \\ &= 6x^2y - x + 4y^3 - 1 - 8xy - 4y^3 \\ &= 6x^2y - x - 8xy - 1. \end{aligned}$$

   En este caso $X = 4y^3$.

Definición 3.9. Sean f, h y $f_1, f_2, \ldots, f_s$ y $F = \{f_1, f_2, \ldots, f_s\}$, polinomios no nulos en $K[x_1, x_2, \ldots, x_n]$. Sea se dice que f se reduce a h módulo F, proceso que se denotará con

$$f \xrightarrow{F}_+ h,$$

sí existe una secuencia de indices $i_1, i_2, \ldots, i_t \in \{1, 2, \ldots, s\}$ y una secuencia de polinomios $h_1, h_2, \ldots, h_{t-1} \in K[x_1, x_2, \ldots, x_n]$ tal que:

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Ejemplo 3.7. Sean $f_1 = yx - y$, $f_2 = y^2 - x$ polinomios en $\mathbb{Q}[x, y]$ con el orden de términos *deglex*, con $y > x$ y $F = \{f_1, f_2\}$, $f = y^2x$, luego

$$f \xrightarrow{F}_+ x.$$

En efecto

$$\begin{aligned} h &= y^2x - \frac{y^2x}{yx}(yx - y), \\ &= y^2x - y(yx - y) \\ &= y^2x - y^2x + y^2 \\ &= y^2. \end{aligned}$$

Ahora

$$\begin{aligned} y^2 \xrightarrow{f_2} y^2 - \frac{y^2}{y^2}(y^2 - x), \\ = y^2 - y^2 + x \\ = x. \end{aligned}$$

Observe que este proceso no siempre da un único resultado, ya que depende del orden con el que se tomen los subíndices i_k en la Definición 3.9. Por ejemplo, observe que en el primer paso del ejemplo anterior se dividió primero con respecto al polinomio f_1 pero también se podría haber hecho la reducción con f_2. Lo cual en este caso proporciona un resultado diferente como se muestra a continuación.

$$\begin{aligned} h &= y^2x - \frac{y^2x}{y^2}(y^2 - x), \\ &= y^2x - x(y^2 - x) \\ &= y^2x - y^2x + x^2 \\ &= x^2. \end{aligned}$$

Luego x^2 no es divisible por ningún producto potencia de f_1. Así

$$f \xrightarrow{F}_+ x^2.$$

Definición 3.10. Un polinomio r se dice que es reducido con respecto a un conjunto de polinomios no nulos $F = \{f_1, f_2, \ldots, f_s\}$, si $r = 0$ o ningún producto potencia que aparece en r es divisible por alguno de los $\mathrm{lp}(f_i)$, para $1 \leq i \leq s$.

Definición 3.11. Si $f \xrightarrow{F}_+ r$ donde r es reducido con respecto a F, luego r se denomina un residuo para f con respecto a F.

El proceso de reducción permite construir el algoritmo de la división en $K[x_1, \ldots, x_n]$. Dados los polinomios $f_1, f_2, \ldots, f_s \in K[x_1, x_2, \ldots, x_n]$ con $f_i \neq 0$, $1 \leq i \leq s$, el proceso de reducción devuelve polinomios $u_1, u_2, \ldots, u_s, r$ en $K[x_1, x_2, \ldots, x_n]$ tal que

$$f = u_1 f_1 + u_2 f_2 + \cdots + u_s f_s + r.$$

De esta forma se construye el algoritmo de la división como sigue.

Algoritmo 3.1 (Algoritmo de la división en varias variables)**.**

```
divvar:= function(f,L,ord)
local r,h,s,bandera,U,i;
U:=[];
i:=1;
while i<=Length(L) do
 Add(U,Zero(R));
 i:=i+1;
od;
h:=f;
r:=Zero(R);
s:=Length(U);
while h<>Zero(R) do
 bandera:=0;
 for i in [1..s] do
  if LeadingTermOfPolynomial(h,ord)/LeadingTermOfPolynomial(L[i],ord) in R then
     bandera:=1;
     U[i]:=U[i]+LeadingTermOfPolynomial(h,ord)/LeadingTermOfPolynomial(L[i],ord);
     h:=h-(LeadingTermOfPolynomial(h,ord)/LeadingTermOfPolynomial(L[i],ord))*L[i];
     break;
 fi;
```

```
 od;
 if bandera=0 then
  r:=r+LeadingTermOfPolynomial(h,ord);
  h:=h-LeadingTermOfPolynomial(h,ord);
 fi;
od;
return [U,r];
end;
```

Teorema 3.2. *(Algoritmo de la división multivariado.) Sea $<$ un orden monomial en $K[x_1, x_2, \ldots, x_n]$ y sea $F = \{f_1, f_2, \ldots, f_s\}$, un conjunto de polinomios en $K[x_1, x_2, \ldots, x_n]$. Luego si f es un polinomio en $K[x_1, x_2, \ldots, x_n]$, el Algoritmo 3.1 produce polinomios $u_1, u_2, \ldots, u_s, r \in K[x_1, x_2, \ldots, x_n]$ tales que*

$$f = u_1 f_1 + u_2 f_2 + \cdots + u_s f_s + r.$$

Con r reducido con respecto a F y

$$lp(f) = \text{máx}(\underset{1 \leq i \leq s}{\text{máx}} (\text{lp}(u_i)\,\text{lp}(f_i)), \text{lp}(r)).$$

Demostración. Primero se observa que el algoritmo se detiene en un determinado momento durante su ejecución. En cada paso del algoritmo el término líder de h se sustrae hasta que esto no se pueda hacer más. Esto es que se produce una secuencia de polinomios $h_1, h_2, \ldots$ de los h's en el algoritmo, donde h_{i+1} es obtenido por la sustracción del término líder de h_i y posiblemente algunos términos más pequeños (en grados), esto es $h_{i+1} = h_i - (\text{lt}(h_i) + \text{términos pequeños})$ esto ocurre ya que se calcula h_{i+1} a partir de h_i por la sustracción de $\frac{\text{lt}(h_i)}{\text{lt}(f_j)} f_j = \text{lt}(h_i) + \text{términos más pequeños}$ (en este caso algún $\text{lp}(f_j)$ divide a $\text{lp}(h_i)$) ó por la resta de $\text{lt}(h_i)$ (cuando $\text{lp}(f_j)$ no divide a $\text{lp}(h_i)$), luego se tiene que para todo i, $\text{lp}(h_{i+1}) < \text{lp}(h_i)$. Así el orden de términos es un buen ordenamiento y la lista de $h_i's$ termina.
Ahora veamos la segunda parte, dado que al iniciar el algoritmo $h = f$ se tiene que en cualquier paso del algoritmo $\text{lp}(h) \leq \text{lp}(f)$. Ahora para cada i, se obtiene un u_i por adición de términos $\frac{\text{lt}(h)}{\text{lt}(f_i)}$, donde $\frac{\text{lt}(h)}{\text{lt}(f_i)} f_i$ cancela el término líder de h, luego se tiene que $\text{lp}(u_i)\,\text{lp}(f_i) \leq \text{lp}(f)$. Además, r es obtenido en la adición por términos $\text{lt}(h)$ y así $\text{lp}(r) \leq \text{lp}(f)$. ■

Ahora presentamos el algoritmo de la división multivariado implementado en GAP, el cual permite dividir un polinomio por una lista de polinomios con respecto a un orden de términos.

Ejemplo 3.8. Si tomamos el Ejemplo 3.7 con $f = y^2x$, $f_1 = yx - y$, $f_2 = y^2 - x$ polinomios en $\mathbb{Q}[x, y]$ con el orden de términos *deglex*, con $y > x$ y $L = \{f_1, f_2\}$, $f = y^2x$, luego, si se divide a f por F, primero con respecto a f_1 y luego con f_2, utilizando el Algoritmo 3.1 se tiene.

```
>x:=X(Rationals,"x"); y:=X(Rationals,"y");
x
y
>R:=PolynomialRing(Rationals,[x,y]);
Rationals[x,y]

>f1:=y*x-y;
x*y-y

>f2:=y^2-x;
y^2-x

>F:=[f1,f2];
[ x*y-y, y^2-x ]

>divvar(y^2*x,F,MonomialGrlexOrdering(y,x));
[ [ y, 1 ], x ]
```

Inicialmente se definen las variables y el anillo de polinomios a utilizar, en este caso utilizamos los comandos `x:=X(Rationals,"x");` `y:=X(Rationals,"y");` y `R:=PolynomialRing(Rationals,[x,y]);` `While:` formamos la lista U de longitud dos con los polinomios nulos, es decir, $U = [0, 0]$. Luego se procede a hacer $h = f = y^2x$, $r = 0$ y a s la longitud de U.
Se inicializa el segundo `While:`
`For:` se pregunta si la división del término líder del polinomio h por el término líder de un polinomio de la lista L está en el anillo R. En este caso podemos observar que efectivamente $\frac{y^2x}{yx}$, donde y^2x es término líder de h y yx es el término líder de $f_1 \in L$. Luego

$$U_1 = 0 + \frac{y^2x}{yx} = y$$

$$h = y^2x - \frac{y^2x}{yx}(yx - y) = y^2.$$

Nuevamente se pregunta si la división del término líder del polinomio h por el término líder de un polinomio de la lista L está en el anillo R. En este caso efectivamente se tiene que $\frac{y^2}{y^2}$, donde y^2 es nuevo término líder de h y y^2 es el término líder de $f_2 \in L$ y así

$$U_2 = 0 + \frac{y^2}{y^2} = 1$$

$$h = y^2 - \frac{y^2}{y^2}(y^2 - x) = x.$$

Termina el ciclo `For` ya que no es posible la división entre el término líder de $h = x$ por ningún término líder de L, por lo cual se procede a escribir a r y a h como

$$r = 0 + x = x$$

$$h = x - x = 0$$

y finaliza el `While`. Así el algoritmo da como resultado

$$U = [y, 1]$$

$$r = x,$$

es decir, al polinomio f lo podemos escribir como combinación lineal de los polinomios de la lista U más el polinomio r, en otras palabras,

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

Nota 3.1. Se debe aclarar que el algoritmo utiliza listas de polinomios, las cuales se manejarán como conjunto en la interpretación.

Ejemplo 3.9. Sean $f_1 = 2y + x + 1$, $f = y^2x + 4yx - 3x^2$ polinomios en $\mathbb{Q}[x, y]$ con el orden de términos *deglex*, con $y > x$ y sea $F = \{f_1\}$. Aplicando el Algoritmo 3.1 se tiene

```
>divvar(f,F,MonomialGrlexOrdering(y,x));
[ [ -1/4*x^2+1/2*x*y+7/4*x ], 1/4*x^3-9/2*x^2-7/4*x ]
```

así la función devuelve el polinomio

$$-\frac{1}{4}x^2 + \frac{1}{2}xy + \frac{7}{4}x$$

y produce el residuo

$$\frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x$$

y así

$$f = \left(-\frac{1}{4}x^2 + \frac{1}{2}xy + \frac{7}{4}x\right)(2y + x + 1) + \left(\frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x\right).$$

Ejemplo 3.10. Para $f_1 = 2xy^2 + 3x + 4y^2$, $f_2 = y^2 - 2y - 2$ y $f = x^3y^3 + 2y^2 \in \mathbb{Q}[x, y]$ con el orden de términos *lex*, con $x > y$ y $F = \{f_1, f_2\}$. Aplicando la función

```
 >divvar(f,F,MonomialLexOrdering (x,y));
[ [ 1/2*x^2*y-x*y+2*y, -8*y-14 ], -3/2*x^3*y+3*x^2*y-6*x*y-44*y-28 ]
```

imprime los polinomios

$$u_1 = \frac{1}{2}x^2y - xy + 2y, u_2 = -8y - 14$$

y el residuo

$$-\frac{3}{2}x^3y + 3x^2y - 6xy - 44y - 28,$$

luego

$$f = \left(\frac{1}{2}x^2y - xy + 2y\right)\left(2xy^2 + 3x + 4y^2\right) + (-8y - 14)\left(y^2 - 2y - 2\right) + \\ + \left(-\frac{3}{2}x^3y + 3x^2y - 6xy - 44y - 28\right).$$

Ejemplo 3.11. Sean $f = x^2y^2 - w^2$, $f_1 = x - y^2w$, $f_2 = y - zw$, $f_3 = z - w^3$ y $f_4 = w^3 - w$ polinomios en $\mathbb{Q}[x, y, w, z]$ esto se traduce como

```
x:=X(Rationals,"x"); y:=X(Rationals,"y");w:=X(Rationals,"w"); z:=X(Rationals,"z");
R:=PolynomialRing(Rationals,[x,y,z,w]);
```

con el orden de términos *lex*, con $x > y > w > z$ y sea $F = \{f_1, f_2, f_3, f_4\}$. Así la función `divvar` aplicada a F resulta

```
F:=[f_1,f_2,f_3,f_4];
[ -y^2*w+x, -w*z+y, -w^3+z, w^3-w ]

divvar(f,F,MonomialLexOrdering (x,y,w,z));
[ [ 0, 0, 0, 0 ], x^2*y^2-w^2 ]
```

devuelve los polinomios $u_1 = 0$, $u_2 = 0$, $u_3 = 0$, $u_4 = 0$ y un residuo $r = x^2y^2 - w^2$, luego $f = r$.

Note que si cambiamos el orden de los polinomios en el conjunto F, se obtienen polinomios cocientes y residuo diferente, es decir

```
F:=[f_1,f_3,f_2,f_4];
[ -y^2*w+x, -w^3+z, -w*z+y, w^3-w ]

divvar(f,[f_1,f_3,f_2,f_4] ,MonomialLexOrdering (x,y,z,w));
[ [ y^4*w+x*y^2, w^23+y*w^19+y^2*w^15+y^3*w^11+y^4*w^7+y^5*w^3,
      w^22+y*w^18+y^2*w^14+y^3*w^10+y^4*w^6+y^5*w^2,
      w^23+w^21+w^19+w^17+w^15+w^13+w^11+w^9+w^7+w^5+w^3+w ], 0 ]
```

devuelve los polinomios $u_1y^4w + xy^2$, $u_2 = w^{23} + yw^{19} + y^2w^{15} + y^3w^{11} + y^4w^7 + y^5w^3$, $u_3 = w^{22} + yw^{18}+y^2w^{14}+y^3w^{10}+y^4w^6+y^5w^2$, $u_4 = w^{23}+w^{21}+w^{19}+w^{17}+w^{15}+w^{13}+w^{11}+w^9+w^7+w^5+w^3+w$, los cuales son los polinomios utilizados para escribir a f como combinación lineal de f_1, f_2, f_3 y f_4 respectivamente y además el algoritmo produce un residuo 0.

Capítulo 4

Bases de Gröbner

En este capítulo se presenta la definición de base de Gröbner y se estudian sus principales propiedades y características. En la Sección 4.2 se estudia el algoritmo propuesto por Bruno Buchberger para el cálculo de una base de Gröbner y finalmente, en la Sección 4.3 presentamos unas clases especiales de bases de Gröbner denominadas bases de Gröbner minimales y bases de Gröbner reducidas, respectivamente.

4.1. Bases de Gröbner

Definición 4.1. Un subconjunto no vacío de polinomios $G = \{g_1, g_2, \ldots, g_t\}$ de un ideal I, se denomina una base de Gröbner para I si para todo $0 \neq f \in I$, existe $i \in \{1, 2, \ldots, t\}$ tal que $\mathrm{lp}(g_i)$ divide a $\mathrm{lp}(f)$.

Es decir si G es una base de Gröbner para I, entonces no hay polinomios no nulos en I reducidos con respecto a G.

Definición 4.2. Para un subconjunto L de $K[x_1, x_2, \ldots, x_n]$ se define el ideal de términos líderes de L como

$$\mathrm{Lt}(L) = \langle \mathrm{lt}(l) \ : \ l \in L \rangle.$$

Este ideal permite caracterizar mejor una base de Gröbner.

Teorema 4.1. *Sean I un ideal no nulo de $K[x_1, x_2, \ldots, x_n]$ y $G = \{g_1, g_2, \ldots, g_t\} \subseteq I$ un conjunto de polinomios no nulos. Las siguientes afirmaciones son equivalentes.*

1. *G es una base de Gröbner para el ideal I.*
2. *$f \in I$ si y sólo si $f \xrightarrow{G}_+ 0$.*
3. *$f \in I$ si y sólo si $f = \sum_{i=1}^{t} h_i g_i$ con $\mathrm{lp}(f) = \mathrm{máx}_{1 \leq i \leq t} (\mathrm{lp}(h_i)\,\mathrm{lp}(g_i))$.*

4. $\mathrm{Lt}(G) = \mathrm{Lt}(I)$.

Demostración. (1) $\Rightarrow$ (2)
Sea $f \in K[x_1, x_2, \ldots, x_n]$, por el algoritmo de la división multivariado, ver Teorema 3.2, existe $r \in K[x_1, x_2, \ldots, x_n]$ reducido con respecto a G tal que $f \xrightarrow{G}_+ r$. Dado que f es una combinación lineal de polinomios de G más el residuo r, se tiene que $f - r \in I$ y así $f \in I$ si y sólo si $r \in I$. Si $r = 0$, entonces $f \in I$. Ahora si $f \in I$ y $r \neq 0$ entonces $r \in I$ y por hipótesis, existe un $i \in \{1, 2, \ldots, t\}$ tal que $\mathrm{lp}(g_i)$ divide a $\mathrm{lp}(r)$. Lo cual es una contradicción con el hecho de que r es reducido con respecto a G. Así $r = 0$ y se cumple que $f \xrightarrow{G}_+ 0$.
(2) $\Rightarrow$ (3)
Sea $f \in I$, y supóngase que $f \xrightarrow{G}_+ 0$. El proceso de reducción de f por G es el que se presenta en el algoritmo de la división multivariado, Ver 3.2 y por tanto existen polinomios $h_1, h_2, \ldots, h_s$ tal que $f = \sum_{i=1}^{t} h_i g_i$ con $\mathrm{lp}(f) = \mathrm{máx}_{1 \leq i \leq t} \left(\mathrm{lp}(h_i)\,\mathrm{lp}(g_i)\right)$.
(3) $\Rightarrow$ (4)
Debemos probar que $\mathrm{Lt}(G) = \mathrm{Lt}(I)$. Claramente $\mathrm{Lt}(G) \subseteq \mathrm{Lt}(I)$, ya que $G \subseteq I$. Para probar la otra contenencia es suficiente mostrar que para todo $f \in I$, $\mathrm{lt}(f) \in \mathrm{Lt}(G)$. Por hipótesis se puede escribir a f como $f = \sum_{i=1}^{t} h_i g_i$ y de esta forma se tiene que

$$\mathrm{lt}(f) = \sum_{i=1}^{t} \mathrm{lt}(h_i)\,\mathrm{lt}(g_i),$$

donde la suma es sobre todos los i que cumplan la condición que $\mathrm{lp}(f) = \mathrm{lp}(h_1)\,\mathrm{lp}(g_i)$. Así $\mathrm{lt}(f) \in \mathrm{Lt}(G)$ y en consecuencia $\mathrm{Lt}(I) \subseteq \mathrm{Lt}(G)$.
(4) $\Rightarrow$ (1)
Por hipótesis $\mathrm{Lt}(G) = \mathrm{Lt}(I)$. Sea $f \in I$. Luego $\mathrm{lt}(f) \in \mathrm{Lt}(G)$, por tanto

$$\mathrm{lt}(f) = \sum_{i=1}^{t} h_i\,\mathrm{lt}(g_i), \tag{4.1.1}$$

para algunos $h_i \in K[x_1, x_2, \ldots, x_n]$. Si se expande la parte derecha de la ecuación (4.1.1) se observa que cada término es divisible por algún $\mathrm{lp}(g_i)$. Por lo tanto $\mathrm{lt}(f)$ también es divisible por algún $\mathrm{lp}(g_i)$, así G es una base de Gröbner para I. ■

Corolario 4.1. *Si* $G = \{g_1, g_2, \ldots, g_t\}$ *es una base de Gröbner para* I*, entonces* $I = \langle g_1, g_2, \ldots, g_t \rangle$.

Demostración. Claramente se da el hecho que $\langle g_1, g_2, \ldots, g_t \rangle \subseteq I$, ya que por definición de base de Gröbner para I, cada g_i está en I. Para la otra inclusión, si $f \in I$, entonces por la parte del Teorema 4.1, $f \xrightarrow{G}_+ 0$. De esta forma $f \in \langle g_1, g_2, \ldots, g_t \rangle$, lo que implica que $I = \langle g_1, g_2, \ldots, g_t \rangle$. ■

Ahora se presenta un resultado que garantiza que todo ideal no nulo de $K[x_1, x_2, \ldots, x_n]$ posee una base de Gröbner.

Primero es necesaria alguna información acerca de la naturaleza de los ideales generados por términos, para esto se muestra el siguiente resultado.

Lema 4.1. *Sean I un ideal generado por un conjunto S de términos distintos de cero y f un polinomio en $K[x_1, x_2, \ldots, x_n]$. Entonces $f \in I$ si y sólo si para cada término X que aparece en f existe un $Y \in S$ tal que Y divide a X. Más aún, existe un subconjunto finito S_0 de S tal que $I = \langle S_0 \rangle$.*

Demostración. Si $f \in I$ se tiene que

$$f = \sum_{i=1}^{l} h_i X_i, \tag{4.1.2}$$

donde $h_i \in K[x_1, x_2, \ldots, x_n]$ y $X_i \in S$. Si se expande la parte derecha de (4.1.2) se puede observar que cada término es divisible por algún término $X_i \in S$, entonces cada término de la izquierda también es divisible por algún $X_i \in S$.
Recíprocamente supóngase que para cada término X que aparece en f existe un término $Y \in S$ tal que Y divide a X. Luego $X = Yh$, con $h \in K[x_1, x_2, \ldots, x_n]$, por tanto $X \in I = \langle S \rangle$ de donde f es una combinación lineal de elementos de S y de esta manera $f \in I$.
Para probar la última afirmación se tiene que por el Teorema la base de Hilbert 1.3, I tiene un conjunto generador finito. Ahora por la primera parte del lema cada término de cada miembro de este conjunto generador, es divisible por algún elemento de S. El conjunto de tales divisores es claramente un conjunto generador para I. ■

Corolario 4.2. *Cada ideal I no nulo de $K[x_1, x_2, \ldots, x_n]$ tiene una base de Gröbner.*

Demostración. Por el lema anterior el ideal de términos líder $\mathrm{Lt}(I)$ tiene un conjunto generador finito, se puede suponer como $\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)\}$, con $g_1, g_2, \ldots, g_t \in I$. Ahora considerando el conjunto $G = \{g_1, g_2, \ldots, g_t\}$, se tiene que $\mathrm{Lt}(G) = \mathrm{Lt}(I)$ y así por el Teorema 4.1 G es una base de Gröbner para I. ■

El Corolario 4.1 prueba que si G es una base de Gröbner para un ideal I, entonces G es un conjunto generador de este ideal. Este hecho permite desligar el concepto de base de Gröbner del de ideal y de esta forma se puede hablar simplemente de una base de Gröbner.

Definición 4.3. Un subconjunto $G = \{g_1, g_2, \ldots, g_t\}$ de $K[x_1, x_2, \ldots, x_n]$ es una base de Gröbner si éste es una base de Gröbner para el ideal $\langle G \rangle$.

Teorema 4.2. *Sea $G = \{g_1, g_2, \ldots, g_t\}$ un conjunto no nulo de polinomios en $K[x_1, x_2, \ldots, x_n]$, entonces G una base de Gröbner si y sólo si para todo $f \in K[x_1, x_2, \ldots, x_n]$ el residuo de la división de f por G es único.*

Para probar este importante teorema, es necesario establecer la siguiente afirmación.

Afirmación 4.1. *Sea G un conjunto no nulo de polinomios en $K[x_1, x_2, \ldots, x_n]$ tal que para todo $f \in K[x_1, x_2, \ldots, x_n]$ el residuo de la división de f por G es único. Si $C \in K$ no nulo, $X \in \mathbb{T}^n$ y $g \in K[x_1, x_2, \ldots, x_n]$, tal que $g \xrightarrow{G}_+ r$, con r reducido con respecto a g, entonces para cada $i \in \{1, \ldots, t\}$ se tiene que $g - CXg_i \xrightarrow{G}_+ r$.*

Sea d tal que $d\,\mathrm{lc}(g_i)$ es el coeficiente de $X\,\mathrm{lp}(g_i)$ en g. se consideran los siguientes casos:
Caso 1. Si $d = 0$, se tiene que el coeficiente de $X\,\mathrm{lp}(g_i)$ en $g - CXg_i$ es $-C\,\mathrm{lc}(g_i) \neq 0$ entonces

$$\begin{aligned} g - CXg_i \xrightarrow{g_i} & g - CXg_i - \frac{-CX\,\mathrm{lt}(g_i)}{\mathrm{lt}(g_i)} g_i \\ &= g - CXg_i + CXg_i \\ &= g \xrightarrow{G}_+ r. \end{aligned}$$

Caso 2. Supóngase que $d = C$. Sea r_1 reducido con respecto a G tal que que $g - CXg_i \xrightarrow{G}_+ r_1$. Como $d = C \neq 0$ se tiene que

$$\begin{aligned} g \xrightarrow{g_i} & g - \frac{CX\,\mathrm{lt}(g_i)}{\mathrm{lt}(g_i)} g_i \\ &= g - CXg_i \\ &= g - CXg_i \xrightarrow{G}_+ r_1 \end{aligned}$$

y como $g \xrightarrow{G}_+ r$, se puede ver $r = r_1$ por la unicidad del residuo.
Caso 3. Supóngase que $d \neq 0$ y $d \neq C$. Sea $h = g - dXg_i$, luego el coeficiente de $X\,\mathrm{lp}(g_i)$ en h es 0, ya que en g aparece el término $dX\,\mathrm{lp}(g_i)$. Como $d \neq 0$ se tiene que

$$\begin{aligned} g \xrightarrow{g_i} h &= g - \frac{dX\,\mathrm{lt}(g_i)}{\mathrm{lt}(g_i)} g_i \\ &= g - dXg_i \end{aligned}$$

y como $d \neq C$, luego

$$\begin{aligned} g \xrightarrow{g_i} & g - CXg_i - \frac{dX\,\mathrm{lt}(g_i) - CX\,\mathrm{lt}(g_i)}{\mathrm{lt}(g_i)} g_i \\ &= g - CXg_i - X(d - C)g_i \\ &= g - CXg_i - dXg_i + CXg_i \\ &= g - dXg_i. \end{aligned}$$

Si $h \xrightarrow{G}_+ r_2$ tal que r_2 es reducido, se tiene que $g \xrightarrow{g_i} h \xrightarrow{G}_+ r_2$ y de esta forma $r_2 = r$ y por lo tanto $g - CXg_i \xrightarrow{g_i} h \xrightarrow{G}_+ r$.

Demostración. Primero supóngase que G es una base de Gröbner. Sea $f \xrightarrow{G}_+ r_1$ y $f \xrightarrow{G}_+ r_2$, con r_1 y r_2 reducidos con respecto a G. Entonces $f - r_1$ y $f - r_2$ están en $\langle G \rangle = \langle g_1, g_2, \ldots, g_t \rangle$, luego

$f - r_2 - (f - r_1) \in \langle G \rangle$, entonces $r_1 - r_2 \in \langle G \rangle$. Como $r_1 - r_2$ es reducido con respecto a G, Por Teorema 4.1 $r_1 - r_2 = 0$, por lo tanto $r_1 = r_2$.
Recíprocamente, supóngase que el residuo de la división de f por G es único y se probará que se satisface la segunda condición del Teorema 4.1. Sea $f \in \langle G \rangle$ tal que $f \xrightarrow{G}_+ r$ donde r es reducido con respecto a G, se debe probar que $r = 0$, luego $f = \sum_{i=1}^{t} h_i g_i$ con $h_i \in K[x_1, x_2, \ldots, x_n]$, como h_i se puede escribir una suma de términos, se obtiene que $f = \sum_{v=1}^{l} C_v X_v g_{i_v}$, donde $C_v \in K$ y $X_v \in \mathbb{T}^n$. Por la Afirmación 4.1 aplicada a $g = f$, se tiene que $f - C_1 X_1 g_{i_1} \xrightarrow{G}_+ r$, de igual forma si se hace $g = f - C_1 X_1 g_{i_1}$ y se aplica nuevamente la Afirmación 4.1 se obtiene que $f - C_1 X_1 g_{i_1} - C_2 X_2 g_{i_2} \xrightarrow{G}_+ r$, es decir $f - (C_1 X_1 g_{i_1} + C_2 X_2 g_{i_2}) \xrightarrow{G}_+ r$, siguiendo este proceso $f - \sum_{v=1}^{l} C_v X_v g_{i_v} \xrightarrow{G}_+ r$ de ahí que $0 \xrightarrow{G}_+ r$ y así $r = 0$. Luego $f \xrightarrow{G}_+ 0$ y por el Teorema 4.1 G es una base de Gröbner. ■

4.2. Algoritmo de Buchberger

En esta sección se estudia el algoritmo de Bruno Buchberger para calcular una base de Gröbner. Además, se presenta una implementación de este algoritmo el cual será programado en el sistema de álgebra computacional discreto GAP. Se mostrarán algunos ejemplos y resultados que permiten caracterizar las bases de Gröbner.

A continuación se presenta la definición de S-polinomio la cual es fundamental en el desarrollo del algoritmo de Buchberger. La idea básica de la construcción de este polinomio ocurre tras el siguiente hecho. Si se toman un ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$ y $F = \{f_1, f_2, \ldots, f_s\}$ el conjunto generador de I de polinomios en $K[x_1, x_2, \ldots, x_n]$, se sabe por la Definición 4.1 que G es una base de Gröbner para I si y sólo si para todo $0 \neq f \in I$, existe $i \in \{1, 2, \ldots, s\}$ tal que $\mathrm{lp}(f_i)$ divide a $\mathrm{lp}(f)$. La dificultad ocurre con los elementos de I cuyos productos potencia líder no sean divisibles por algún $\mathrm{lp}(f_i)$; es decir, si $f \in I$, entonces $f = \sum_{i=1}^{t} h_i f_i$ con $h_i \in K[x_1, x_2, \ldots, x_n]$ $(1 \leq i \leq s)$, por tanto la dificultad sucede cuando el mayor de los $\mathrm{lp}(h_i f_i) = \mathrm{lp}(h_i)\,\mathrm{lp}(f_i)$ es cancelado. La manera más simple para que esto suceda es con el S-polinomio que se define a continuación, pero antes es necesaria establecer la definición de mínimo común múltiplo de dos productos potencia.

Definición 4.4. Sean X, Y dos productos potencia. El mínimo común múltiplo de X, Y que se denota con $\mathrm{lcm}(X, Y)$, se define como el producto potencia L tal que X divide a L y Y divide a L y si Z es otro producto potencia tal que X divide a Z y Y divide a Z, entonces L divide a Z.

Definición 4.5. (S-Polinomio) Sean $f, g \in k[x_1, x_2, \ldots, x_n]$ dos polinomios no nulos. El S-polinomio de f y g se define como

$$S(f, g) = \frac{L}{\mathrm{lt}(f)} f - \frac{L}{\mathrm{lt}(g)} g,$$

donde $L = \operatorname{lcm}(\operatorname{lp}(f), \operatorname{lp}(g))$.

En otras palabras este polinomio está diseñado para que se cancelen los términos líderes de f y g. Para ilustrar este hecho veamos el siguiente ejemplo.

Ejemplo 4.1. Sean $f = 2xy - y$ y $g = 3y^2 - x$ dos polinomios en $\mathbb{Q}[x, y]$ con el orden de términos *deglex*, con $y > x$, luego el mínimo común múltiplo de $\operatorname{lp}(f)$ y $\operatorname{lp}(g)$ es $L = \operatorname{lcm}(\operatorname{lp}(f), \operatorname{lp}(g)) = \operatorname{lcm}(xy, y^2) = y^2x$ y por tanto

$$\begin{aligned} S(f,g) &= \frac{y^2x}{2yx}(f) - \frac{y^2x}{3y^2}(g) \\ &= \frac{y}{2}(f) - \frac{x}{3}(g) \\ &= -\frac{1}{2}(y^2) + \frac{1}{3}(x^2). \end{aligned}$$

Además

$$\begin{aligned} \operatorname{lp}\left(\frac{1}{2}(y)f\right) &= y^2x, \\ \operatorname{lp}\left(\frac{1}{3}(x)g\right) &= y^2x, \end{aligned}$$

el cual se cancela en $S(f, g)$.

Existe otra forma de ver los S-polinomios.
En la división de f por $f_1, f_2, \ldots, f_s$, puede ocurrir que algún término X que aparece en f sea divisible por $\operatorname{lp}(f_i)$ y $\operatorname{lp}(f_j)$ con $i \neq j$, por tanto X es divisible por $L = \operatorname{lcm}(\operatorname{lp}(f_i), \operatorname{lp}(f_j))$, si se reduce f usando f_i se obtiene el residuo

$$h_1 = f - \frac{X}{\operatorname{lt}(f_i)} f_i,$$

si se reduce f usando f_j se tiene el residuo

$$h_2 = f - \frac{X}{\operatorname{lt}_(\, f_j)} f_j,$$

si restamos los residuos h_1 y h_2 se obtiene

$$\begin{aligned} h_2 - h_1 &= f - \frac{X}{\operatorname{lt}(f_j)} f_j - \left(f - \frac{X}{\operatorname{lt}(f_i)} f_i\right) \\ &= \frac{X}{\operatorname{lt}(f_i)} f_i - \frac{X}{\operatorname{lt}(f_j)} f_j, \end{aligned}$$

multiplicando y dividiendo por L se tiene que

$$\begin{aligned} h_2 - h_1 &= L\frac{X}{L(\mathrm{lt}(f_i))}f_i - L\frac{X}{L(\mathrm{lt}(f_j))}f_j \\ &= \frac{X}{L}\left(\frac{L}{\mathrm{lt}(f_i)}f_i - \frac{L}{\mathrm{lt}(f_j)}f_j\right) \\ &= \frac{X}{L}S(f_i, f_j). \end{aligned}$$

Es turno ahora de presentar el Teorema de Buchberger, el cual permite decidir cuando un conjunto finito G de polinomios en $K[x_1, x_2, \ldots, x_n]$ es una base de Gröbner, pero primero es necesario considerar el siguiente lema.

Lema 4.2. *Sean $f_1, f_2, \ldots, f_s$ polinomios en $K[x_1, x_2, \ldots, x_n]$ tales que $\mathrm{lp}(f_i) = X \neq 0$, $(1 \leq i \leq s)$, Sea $f = \sum_{i=1}^{s} c_i f_i$ con $c_i \in K$. Si $\mathrm{lp}(f) < X$, entonces f es una combinación lineal con coeficientes en K de $S(f_i, f_j)$, $1 \leq i < j \leq s$.*

Demostración. Por hipótesis se puede escribir a cada f_i como $f_i = a_i X$+términos pequeños, con $a_i \in K$ y

$$\begin{aligned} f &= \sum_{i=1}^{s} c_i f_i \\ &= c_1 f_1 + c_2 f_2 + \cdots + c_s f_s \\ &= c_1 a_1 (X + \cdots) + c_2 a_2 (X + \cdots) + \cdots + c_s a_s (X + \cdots) \\ &= (c_1 a_1 + c_2 a_2 + \cdots + c_s a_s) X + \cdots \end{aligned}$$

Dado que $\mathrm{lp}(f) < X$, entonces $c_1 a_1 + c_2 a_2 + \cdots + c_s a_s = 0$. Ahora por definición de S-polinomio se tiene que

$$S(f_i, f_j) = \frac{X}{a_i X} f_i - \frac{X}{a_j X} f_j = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j,$$

ya que $L = \mathrm{lcm}\,(\mathrm{lp}(f), \mathrm{lp}(g)) = \mathrm{lcm}(X, X) = X$. Por tanto

$$\begin{aligned} f &= c_1 f_1 + c_2 f_2 + \cdots + c_s f_s \\ &= c_1 a_1 \left(\frac{1}{a_1} f_1\right) + c_2 a_2 \left(\frac{1}{a_2} f_2\right) + \cdots + c_s a_s \left(\frac{1}{a_s} f_s\right) \\ &= c_1 a_1 \left(\frac{1}{a_1} f_1 - \frac{1}{a_2} f_2\right) + (c_1 a_1 + c_2 a_2) \left(\frac{1}{a_2} f_2 - \frac{1}{a_3} f_3\right) + \cdots \\ &+ (c_1 a_1 + c_2 a_2 + \cdots + c_{s-1} a_{s-1}) \left(\frac{1}{a_{s-1}} f_{s-1} - \frac{1}{a_s} f_s\right) + (c_1 a_1 + c_2 a_2 + \cdots + c_s a_s) \frac{1}{a_s} f_s \\ &= c_1 a_1 S(f_1, f_2) + (c_1 a_1 + c_2 a_2) S(f_2, f_3) + \cdots + (c_1 a_1 + c_2 a_2 + \cdots + c_{s-1} a_{s-1}) S(f_{s-1}, f_s). \end{aligned}$$

■

Teorema 4.3. *(Buchberger) Sea $G = \{g_1, g_2, \ldots, g_t\}$ un conjunto no nulo de polinomios en $K[x_1, x_2, \ldots, x_n]$. Luego G es una base de Gröbner si y sólo si para todo $i \neq j$.*

$$S(g_i, g_j) \xrightarrow{G}_+ 0.$$

Demostración. Si $G = \{g_1, g_2, \ldots, g_t\}$ es una base de Gröbner para $I = \langle g_1, g_2, \ldots, g_t\rangle$, luego el $S(g_i, g_j) \in I$ y así por Teorema 4.1 $S(g_i, g_j) \xrightarrow{G}_+ 0$.
Recíprocamente, supóngase que $S(g_i, g_j) \xrightarrow{G}_+ 0$, se usará el Teorema 4.1 para probar que G es una base de Gröbner para I. Considere $f \in I$, luego f puede ser escrito de muchas maneras como combinación de los polinomios g_i, por tanto es posible escribir a f como $f = \sum_{i=1}^{t} h_i g_i$ y utilizando la propiedad de buen orden podemos tomar el menor X tal que

$$X = \max_{1 \leq i \leq t} (\operatorname{lp}(h_i) \operatorname{lp}(g_i)).$$

Si $X = \operatorname{lp}(f)$ el resultado se cumple por la parte tres del Teorema 4.1. Supóngase que $\operatorname{lp}(f) < X$, el objetivo ahora es encontrar una representación de f con un X más pequeño y así llegar a una contradicción. Sea $M = \{i : \operatorname{lp}(h_i) \operatorname{lp}(g_i) = X\}$. Para $i \in M$, se puede escribir a h_i como $h_i = C_i X_i +$ términos menores. Sea $g = \sum_{i \in M} C_i X_i g_i$, ahora para todo $i \in M$ se tiene que $\operatorname{lp}(X_i g_i) = X$, pero $\operatorname{lp}(g) < X$ y por el Lema 4.2 existe $d_{ij} \in K$ tal que

$$g = \sum_{i,j \in M \; i \neq j} d_{ij} S(X_i g_i, X_j g_j).$$

Como $\operatorname{lp}(X_i g_i) = X$ y $\operatorname{lp}(X_j g_j) = X$ con $i, j \in M$, el $\operatorname{lcm}(\operatorname{lp}(X_i g_i), \operatorname{lp}(X_j g_j)) = X$ y así

$$\begin{aligned}
S(X_i g_i, X_j g_j) &= \frac{X}{\operatorname{lt}(X_i g_i)}(X_i g_i) - \frac{X}{\operatorname{lt}(X_j g_j)}(X_j g_j) \\
&= \frac{X}{\operatorname{lt}(X_i)\operatorname{lt}(g_i)}(X_i g_i) - \frac{X}{\operatorname{lt}(X_j)\operatorname{lt}(g_j)}(X_j g_j) \\
&= \frac{X}{\operatorname{lt}(g_i)}(g_i) - \frac{X}{\operatorname{lt}(g_j)}(g_j) \\
&= \frac{X}{X_{ij}}\left(\frac{X_{ij}}{\operatorname{lt}(g_i)}(g_i) - \frac{X_{ij}}{\operatorname{lt}(g_j)}(g_j)\right) \\
&= \frac{X}{X_{ij}}(S(g_i, g_j)),
\end{aligned}$$

con $X_{ij} = \operatorname{lcm}(\operatorname{lp}(g_i), \operatorname{lp}(g_j))$. Por hipótesis $S(g_i, g_j) \xrightarrow{G}_+ 0$, entonces

$$\frac{X}{X_{ij}} S(g_i, g_j) \xrightarrow{G}_+ 0$$

y así

$$S(X_i g_i, X_j g_j) \xrightarrow{G}_+ 0.$$

Esta división produce polinomios h_{ijv} tal que

$$S(X_i g_i, X_j g_j) = \sum_{v=1}^{t} h_{ijv} g_v,$$

donde por Teorema 3.2 se tiene que

$$\begin{aligned} \max_{1\leq v\leq t}(\mathrm{lp}(h_{ijv}), \mathrm{lp}(g_v)) &= \mathrm{lp}(S(X_i g_i, X_j g_j)) \\ &< \max(\mathrm{lp}(X_i g_i), \mathrm{lp}(X_j g_j)) \\ &< \max(X, X) \\ &= X. \end{aligned}$$

Si se sustituye ésta expresión en g y g en f, tenemos

$$f = \sum_{i=1}^{t} h_i^{'} g_i,$$

con $\max_{1\leq v\leq t}(\mathrm{lp}(h_i^{'}), \mathrm{lp}(g_i)) < X$ lo cual contradice la minimalidad de X. ■

De la prueba del teorema anterior se sigue el siguiente corolario,

Corolario 4.3. *Sea $G = \{g_1, g_2, \ldots, g_t\}$ con $g_i \neq 0$ $(1 \leq i \leq t)$. Luego G es una base de Gröbner si y sólo si para todo $i \neq j$ con $1 \leq i < j \leq s$, se tiene*

$$S(g_i, g_j) = \sum_{v=1}^{t} h_{ijv} g_v,$$

donde $\mathrm{lp}(S(g_i, g_j)) = \max_{1\leq v\leq s}(\mathrm{lp}(h_{ijv})\,\mathrm{lp}(g_v))$.

El Teorema de Buchberger nos permite calcular una base de Gröbner siguiendo el siguiente proceso.
Primero se reduce el S-polinomio con respecto a una lista de polinomios y si el residuo r no es cero, entonces se lo adiciona a la lista y se realiza este proceso hasta obtener suficientes polinomios para que todos los S-polinomios sean reducidos a cero.

Ejemplo 4.2. Sean $f_1 = xy - x$, $f_2 = x^2 - y$ polinomios en $\mathbb{Q}[x, y]$ con el orden de términos lex, con $x < y$ y sea $F = \{f_1, f_2\}$, primero determinemos $S(f_1, f_2)$. El mínimo común múltiplo de f_1 y f_2 es $L = \mathrm{lcm}(\mathrm{lp}(f_1), \mathrm{lp}(f_2)) = \mathrm{lcm}(xy, y) = xy$ y por tanto

$$\begin{aligned} S(f_1, f_2) &= \frac{xy}{xy}(f_1) - \left(-\frac{xy}{y}(f_2)\right) \\ &= f_1 + x f_2 \\ &= xy - x + x(x^2 - y) \\ &= x^3 - x. \end{aligned}$$

Aplicando el Algoritmo de la división 3.1 se tiene que $x^3 - x$ es reducido con respecto a F, ya que ningún término líder de f_1 o f_2 divide a un término de $x^3 - x$. Así se adiciona el polinomio $f_3 = x^3 - x$ a $F = \{f_1, f_2\}$, es decir se construye $F^* = \{f_1, f_2, f_3\}$. Nuevamente utilizando el Algoritmo 3.1 se puede observar que $S(f_1, f_2) = x^3 - x \xrightarrow{F^*} 0$, ahora se procede a calcular $S(f_1, f_3)$, donde $L = \text{lcm}(xy, x^3) = x^3y$ es el mínimo común múltiplo de $\text{lp}(f_1)$ y $\text{lp}(f_3)$ entonces,

$$\begin{aligned} S(f_1, f_3) &= \frac{x^3y}{xy}(f_1) - \frac{x^3y}{x^3}(f_3) \\ &= x^2 f_1 - y f_3 \\ &= x^2(xy - x) - y(x^3 - x) \\ &= xy - x^3. \end{aligned}$$

Ahora se aplica el Algoritmo 3.1 para $S(f_1, f_3)$ con respecto a $F^* = \{f_1, f_2, f_3\}$, es decir, $S(f_1, f_3) = xy - x^3 \xrightarrow{F^*}_+ 0$. Finalmente, se calcula $S(f_2, f_3)$ con mínimo común múltiplo de $\text{lp}(f_2)$ y $\text{lp}(f_3)$ $L = \text{lcm}(y, x^3) = x^3y$, entonces

$$\begin{aligned} S(f_2, f_3) &= \frac{x^3y}{-y}(f_2) - \frac{x^3y}{x^3}(f_3) \\ &= -x^3 f_2 - y f_3 \\ &= -x^3(x^2 - y) - y(x^3 - x) \\ &= -x^5 + x^3y - x^3y + x \\ &= -x^5 + x. \end{aligned}$$

Utilizando el Algoritmo 3.1 se puede ver que $-x^5 + x \xrightarrow{F^*}_+ 0$. Por lo tanto, $\{f_1, f_2, f_3\}$ es una base de Gröbner.

Las ideal utilizadas en el ejemplo anterior constituyen un algoritmo presentado por Bruno Buchberger, el cual se implementará en GAP más adelante.

Teorema 4.4. *Dado un conjunto $F = \{f_1, f_2, \ldots, f_s\}$ con $f_i \neq 0$ $(1 \leq i \leq s)$, el algoritmo de Buchberger 4.3 produce una base de Gröbner para el ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$.*

Demostración. Primero es necesario probar que el algoritmo se detiene en un determinado momento durante su ejecución. Supóngase lo contrario, si se construye un conjunto G_i estrictamente más grande que G_{i-1} se obtiene así una secuencia estrictamente infinitamente creciente

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

donde cada G_i se obtiene a partir de G_{i-1} por la adición de algún $h \in I$ a G_{i-1}, donde h es el polinomio reducido no nulo con respecto a G_{i-1} de un S-polinomio de dos elementos de G_{i-1}.

Entonces $\mathrm{lt}(h)$ no pertenece a $\mathrm{Lt}(G_{i_1})$ por ser reducido y así se consigue una cadena estrictamente ascendente de ideales

$$\mathrm{Lt}(G_1) \subsetneq \mathrm{Lt}(G_2) \subsetneq \mathrm{Lt}(G_3) \subsetneq \cdots ,$$

lo cual contradice el Teorema de la base de Hilbert 1.3.
Ahora se puede observar que $G \subset I$ en cada paso del algoritmo. Dado que $g_i, g_j \in I$ se tiene que $S(g_i, g_j) \xrightarrow{G} \in I$, además G es un sistema de generadores de I en cada paso ya que contiene a F, es decir $F \subset G \subset I$. El algoritmo termina cuando $S(g_i, g_j) \xrightarrow{G}_+ 0$ entonces, por el Teorema de Buchberger 4.3, G es una base de Gröbner para I. ■

Es turno ahora de presentar una serie de algoritmos los cuales serán utilizados en el desarrollo y la construcción del algoritmo de Buchberger en GAP.
Primero en necesario calcular el S-polinomio y para ello considerar el cálculo del mínimo común múltiplo de los productos potencia de dos polinomios, el cual se presenta a continuación.

Algoritmo 4.1 (Mínimo común múltiplo de dos productos potencia)**.**

```
lcm:=function(X,Y)
local i,l,L,indets,n,F;
l:=[];
L:=[];
indets := IndeterminatesOfPolynomialRing(R);
n:=Length(indets);
for i in [1..n] do
Add(l,[DegreeIndeterminate(X,i),DegreeIndeterminate(Y,i)]);
od;
for i in [1..n] do
 Add(L,MaximumList(l[i]));
od;
F:=One(R);
for i in [1..n] do
 F:=F*indets[i]^L[i];
od;
return F;
end;
```

Ejemplo 4.3. Sean $X = x^3y^2$, $Y = xy$ dos productos potencia en $\mathbb{Q}[x, y]$. Para calcular el mínimo común múltiplo de X y Y en GAP se hace lo siguiente

```
>x:=X(Rationals,"x"); y:=X(Rationals,"y");
x
y
>R:=PolynomialRing(Rationals,[x,y]);
Rationals[x,y]

>X:=x^3*y^2;
x^3*y^2

>Y:=x*y;
x*y

>lcm(X,Y);
x^3*y^2
```

Ejemplo 4.4. Considere los polinomios $f = xy - x$ y $g = x^2 - y$ en $\mathbb{Q}[x, y]$ con el orden *lex* con $x > y$. El mínimo común múltiplo de los productos potencia lideres de f y g está dado por

```
>lcm(f,g);
x^2*y
```

es decir $\text{lcm}(\text{lp}(f), \text{lp}(g)) = x^2y$.

Algoritmo 4.2 (S-Polinomio)**.**

```
spoly:=function(f,g,ord)
local n,L;
L:=lcm( LeadingMonomialOfPolynomial(f,ord), LeadingMonomialOfPolynomial(g,ord));
return (L/LeadingTermOfPolynomial(f,ord))*f-(L/LeadingTermOfPolynomial(g,ord))*g;
end;
```

Ejemplo 4.5. Para los polinomios $f = xy - x$ y $g = y + 1$ se realiza el cálculo del S-polinomio con respecto al orden de términos *lex* con $y > x$,

```
lex:=MonomialLexOrdering(y,x)
f:=x*y-x;
x*y-x

g:=y+1;
y+1

spoly(f,g,lex);
-2*x
```

Primero se calcula el mínimo común múltiplo de los productos potencia lideres de f y g, es decir $\mathrm{lcm}(\mathrm{lp}(f), \mathrm{lp}(g)) = xy$, $\mathrm{lt}(f) = xy$ y $\mathrm{lt}(g) = y$, entonces

$$\begin{aligned} S(f,g) &= \frac{xy}{xy}(f) - \frac{xy}{y}(g) \\ &= f - xg \\ &= xy - x - x(y+1) \\ &= xy - x - xy - x \\ &= -2x. \end{aligned}$$

Finalmente, utilizando los dos algoritmos anteriores, se puede implementar en GAP el Algoritmo de Buchberger para el cálculo de una base de Gröbner de un ideal I generado por un conjunto de polinomios $F \in K[x_1, \ldots, x_n]$.

Además es necesario utilizar una pequeña función antes de comenzar el algoritmo para formar listas de dos polinomios

```
pair:=function(f,g)
return[f,g];
end;
```

Algoritmo 4.3 (Algoritmo de Buchberger)**.**

```
buchberger:=function(F,ord)
local n,G,G1,h,l,i;
G:=F;
```

```
G1:=ListX( G, G, \<, pair);
while G1<>[] do
  l:=Remove(G1);
  h:=divvar(spoly(l[1],l[2],ord),G,ord)[2];
  if h<>Zero(R) then
    n:=Length(G);
    for i in [1..n] do
      Add(G1,[G[i],h]);
    od;
    Add(G,h);
  fi;
od;
return G;
end;
```

Ejemplo 4.6. Para el Ejemplo 4.2 $f_1 = xy - x$, $f_2 = x^2 - y$ polinomios en $\mathbb{Q}[x, y]$ con el orden de términos lex, con $y > x$. Se define a x y a y como indeterminadas sobre el anillo de polinomios con coeficientes racionales.

```
x:=Indeterminate(Rationals,1);
y:=Indeterminate(Rationals,2);
R:=PolynomialRing(Rationals,[x,y]);
```

Es importante notar que se utilizan estos comandos para definir las indeterminadas y asignarles un orden de aparición[1]. Esto se hace ya que en el algoritmo es necesario llevar cuentas con las indeterminadas. Sea $F = \{f_1, f_2\}$ y $G = F$, luego se forma el conjunto de parejas de polinomios de G a través del comando

```
G1:=ListX( G, G, \<, pair)
```

donde la función calcula parejas diferentes del conjunto G. En este caso se forma el conjunto $G_1 = [f_1, f_2]$. Se inicia el `While` y se elimina una pareja de G_1 quitando a $[f_1, f_2]$ que se ubican en $l = [f_1, f_2]$ y se obtiene que

$$G_1 = \emptyset.$$

Ahora utilizando el Algoritmo 4.2 y el Algoritmo 3.1 se tiene que

$$S(f_1, f_2) \xrightarrow{G}_+ h = x^3 - x.$$

[1] Con el comando `x:=Indeterminate(Rationals,1);` se identifica a x como x_1.

Como h es diferente de 0 se debe hacer el ciclo `For` y de esta forma se adiciona a G_1 las parejas $[f_1, h]$ y $[f_2, h]$ y se aumenta h al conjunto G, es decir

$$G = [f_1, f_2, h].$$

Se regresa al ciclo `While` con $l = [f_1, h]$ y $G_1 = [[f_2, h]]$, es decir se eliminan los polinomios f_1, h de G_1 y se colocan en la lista l. Luego se calcula

$$S(f_1, h) \xrightarrow{G}_+ h = 0.$$

Volvemos al `While` y ahora

$$l = [f_2, h]$$

$$G_1 = \emptyset$$

$$S(f_2, h) \xrightarrow{G}_+ h = 0.$$

Como G_1 es vacío el ciclo `While` termina y se imprime

$$G = [xy - x, x^2 - y, x^3 - x].$$

De esta forma una base de Gröbner para el ideal $I = \langle f_1, f_2 \rangle$ es $G = \{xy - x, x^2 - y, x^3 - x\}$. En GAP se realizan los siguientes comandos

```
f1:=x*y-x;f2:=x^2-y;
x_*x_2-x_1
x_1^2-x_2

G:=[f1,f2];
[ x_1*x_2-x_1, x_1^2-x_2 ]

buchberger(G,MonomialLexOrdering (y,x));
[ x_1*x_2-x_1, x_1^2-x_2, x_1^3-x_1 ]
```

Ejemplo 4.7. Sean $f_1 = y^2 + yx + x^2$, $f_2 = y + x$ y $f_3 = y$ polinomios en $\mathbb{Q}[x, y]$ y el conjunto $F = \{f_1, f_2, f_3\}$ con el orden de términos lex, con $y > x$. La base de Gröbner para el ideal $I = \langle f_1, f_2, f_3 \rangle$ esta dada por el Algoritmo 4.3.
Una vez definido el anillo de polinomios `R:=PolynomialRing(Rationals,[x,y]);` como en el ejemplo anterior, para que GAP de los resultados en términos de x y y en lugar de x_1 y x_2, se puede redefinir las variables como sigue.

```
>x:=X(Rationals,"x"); y:=X(Rationals,"y");
x
```

```
y

>f_1:=y^2+y*x+x^2;
x^2+x*y+y^2

>f_2:=y+x;
x+y

>f_3:=y;
y

>F:=[f_1,f_2,f_3];
[ x^2+x*y+y^2, x+y, y ]

>buchberger(F,MonomialLexOrdering (y,x));
[ x^2+x*y+y^2, x+y, y, -x ]
```

es decir $\{x^2 + xy + y^2, x + y, y, -x\}$ es una base de Gröbner para el ideal $I = \langle f_1, f_2, f_3\rangle$.

Ejemplo 4.8. Sean $f_1 = x^2y + z$, $f_2 = xz + y$ polinomios en $\mathbb{Q}[x, y, z]$ y $F = \{f_1, f_2\}$ con respecto al orden de términos *deglex*, con $x > y > x$. La base de Gröbner para el ideal $I = \langle f_1, f_2\rangle$ está dada por

```
>x:=Indeterminate(Rationals,1);
x_1
>y:=Indeterminate(Rationals,2);
x_2
>z:=Indeterminate(Rationals,3);
x_3
>R:=PolynomialRing(Rationals,[x,y,z]);
Rationals[x_1,x_2,x_3]

>f_1:=x^2*y+z;
x_1^2*x_2+x_3

>f_2:=x*z+y;
x_1*x_3+x_2

>F:=[f_1,f_2,f_3];
```

```
[ x_1^2*x_2+x_3, x_1*x_3+x_2 ]

>buchberger(F,MonomialLexOrdering (x,y,z));
[x_1^2*x_2+x_3, x_1*x_3+x_2, x_1*x_2^2-x_3^2, x_2^3+x_3^3]
```

es decir, $G = \{x^2y + z, xz + y, xy^2 - z^2, y^3 + z^3\}$ es una base de Gröbner para el ideal $I = \langle f_1, f_2\rangle$.

4.3. Bases de Gröbner especiales

En la sección anterior se mostró como calcular una base de Gröbner con ayuda del algoritmo de Buchberger. Sin embargo no se garantiza en ningún momento la unicidad de la base de Gröbner obtenida. Así el objetivo principal de esta sección es mostrar las condiciones necesarias para que se cumpla tal unicidad.

En el Algoritmo 4.3, se puede observar que se toma en cuenta el orden en que aparecen los polinomios en la lista `G`, esto afecta la aplicación del Algoritmo de la división en varias variables 3.1. Además, en el bucle `WHILE` donde se calculan los S-polinomios, se escogió un par de polinomios de la lista `l` para realizar este cálculo. Así que si se cambian cualquiera de estas opciones se podría obtener una base de Gröbner diferente.

Ejemplo 4.9. Para el Ejemplo 4.7 con los polinomios $f_1 = y^2 + yx + x^2$, $f_2 = y + x$ y $f_3 = y$ en $\mathbb{Q}[x, y]$. Si cambiamos el orden del cálculo de los S-polinomios en el Algoritmo 4.3, en ocasiones se puede obtener una base de Gröbner diferente para el ideal $I = \langle f_1, f_2, f_3\rangle$, esto se hace cambiando el orden en los polinomios del conjunto $F = \{f_1, f_2, f_3\}$, a saber $F = \{f_3, f_2, f_1\}$ con el orden de términos lex, con $y > x$, es decir

```
>x:=X(Rationals,"x"); y:=X(Rationals,"y");
x
y

>f_1:=y^2+y*x+x^2;
x^2+x*y+y^2

>f_2:=y+x;
x+y

>f_3:=y;
y
```

```
>F:=[f_3,f_2,f_1];
[ y, x+y, x^2+x*y+y^2 ]

>buchberger(F,MonomialLexOrdering (y,x));
[ y, x+y, x^2+x*y+y^2, -x^2, -x ]
```

Por tanto $\{y, x+y, x^2+xy+y^2, -x^2, -x\}$ es una base de Gröbner para el ideal $I = \langle f_1, f_2, f_3\rangle$ diferente a la que se obtuvo en el Ejemplo 4.7.

Definición 4.6. Una base de Gröbner $G = \{g_1, g_2, \ldots, g_t\}$ se denomina base de Gröbner minimal si para todo i, $\mathrm{lc}(g_i) = 1$ y para todo $i \neq j$, $\mathrm{lp}(g_i)$ no divide a $\mathrm{lp}(g_j)$.

Lema 4.3. *Sea $G = \{g_1, g_2, \ldots, g_t\}$ una base de Gröbner para el ideal I. Si $\mathrm{lp}(g_2)$ divide a $\mathrm{lp}(g_1)$, entonces $\{g_2, \ldots, g_t\}$ es también una base de Gröbner para el ideal I.*

Demostración. Usando la Definición 4.1 se tiene que si $\mathrm{lp}(f)$ es divisible por $\mathrm{lp}(g_1)$, entonces $\mathrm{lp}(f)$ también es divisible por $\mathrm{lp}(g_2)$ y por la misma definición se tiene que $\{g_2, \ldots, g_t\}$ es una base de Gröbner para el ideal I. ■

Como consecuencia del lema anterior, al eliminar todos los polinomios g_i del conjunto $G = \{g_1, g_2, \ldots, g_t\}$ en los cuales se cumpla que $\mathrm{lp}(g_j)$ divida a $\mathrm{lp}(g_i)$ con $j \neq i$ se puede obtener una base de Gröbner minimal.

Corolario 4.4. *Sea $G = \{g_1, g_2, \ldots, g_t\}$ una base de Gröbner para el ideal I. Se obtiene una base de Gröbner minimal para G eliminando todos los g_i para los cuales exista $j \neq i$ tal que $\mathrm{lp}(g_j)$ divide a $\mathrm{lp}(g_i)$ y dividiendo cada polinomio restante en G por su coeficiente líder.*

La última condición se da para asegurar que los polinomios restantes en G sean mónicos.

Proposición 4.1. *Si $G = \{g_1, g_2, \ldots, g_t\}$ y $F = \{f_1, f_2, \ldots, f_s\}$ son bases de Gröbner minimales para el ideal I, entonces $s = t$ y después de una remuneración si es necesario, $\mathrm{lt}(f_i) = \mathrm{lt}(g_i)$ para todo $i = 1, 2, \ldots, t$.*

Demostración. Dado que G es una base de Gröbner para I y $f_1 \in I$, entonces por Definición 4.1, existe un i tal que $\mathrm{lp}(g_i)$ divide a $\mathrm{lp}(f_1)$. Después de reorganizar si es necesario, se puede asumir que $i = 1$. Ahora como F es una base de Gröbner para I, para $g_1 \in I$, existe un j tal que $\mathrm{lp}(f_j)$ divide a $\mathrm{lp}(g_1)$, por tanto $\mathrm{lp}(f_j)$ divide a $\mathrm{lp}(f_1)$ y por la condición de que F es minimal se tiene que $j = 1$ y que $\mathrm{lp}(f_1) = \mathrm{lp}(g_1)$. Como f_2 está en I, entonces existe un i tal que $\mathrm{lp}(g_i)$ divide a $\mathrm{lp}(f_2)$ ya que G es una base de Gröbner. Dado que $\mathrm{lp}(f_1) = \mathrm{lp}(g_1)$ y F es una base de Gröbner minimal se tiene que $i \neq 1$ y después de reorganizar si es necesario, se puede asumir que $i = 2$. Luego como $g_2 \in I$, existe un j tal que $\mathrm{lp}(f_j)$ divide a $\mathrm{lp}(g_2)$, por lo tanto $\mathrm{lp}(f_j)$ divide a $\mathrm{lp}(f_2)$ y por a condición de que F es minimal se deduce que $j = 2$ y que $\mathrm{lp}(f_2) = \mathrm{lp}(g_2)$. Este proceso se realiza para cada polinomio en G y en F llegando a que $s = t$ y se tiene que $\mathrm{lp}(f_i) = \mathrm{lp}(g_i)$ para todo $i = 1, 2, \ldots, t$. ■

A continuación se introduce una nueva noción la cual permite encontrar la unicidad de una base de Gröbner exigiendo ciertas condiciones en los polinomios de la base.

Definición 4.7. Una base de Gröbner $G = \{g_1, g_2, \ldots, g_t\}$ se denomina una base de Gröbner reducida, si para todo i, $\mathrm{lc}(g_i) = 1$ y g_i es reducido con respecto a $G - \{g_i\}$. Esto es, para todo i ningún término no nulo de g_i es divisible por cualquier $\mathrm{lp}(g_j)$ para $j \neq i$.

Es importante notar que una base de Gröbner reducida es también una base de Gröbner minimal. En este punto nuestro objetivo es probar la existencia de una base de Gröbner reducida, para ello se necesita el siguiente resultado.

Corolario 4.5. *Sea $G = \{g_1, g_2, \ldots, g_t\}$ una base de Gröbner minimal para el ideal I. Considere el siguiente proceso de reducción*

$$g_1 \xrightarrow{H_1}_+ h_1, \text{ donde } h_1 \text{ es reducido con respecto a } H_1 = \{g_2, \ldots, g_t\}$$
$$g_2 \xrightarrow{H_2}_+ h_2, \text{ donde } h_2 \text{ es reducido con respecto a } H_2 = \{h_1, g_3, \ldots, g_t\}$$
$$g_3 \xrightarrow{H_3}_+ h_3, \text{ donde } h_3 \text{ es reducido con respecto a } H_3 = \{h_1, h_2, g_4, \ldots, g_t\}$$
$$\vdots$$
$$g_t \xrightarrow{H_t}_+ h_t, \text{ donde } h_t \text{ es reducido con respecto a } H_t = \{h_1, h_2, \ldots, h_{t-1}\}.$$

Luego $H = \{h_1, h_2, \ldots, h_t\}$ es una base de Gröbner reducida para I.

Demostración. Sea G una base de Gröbner minimal, luego se tiene que $\mathrm{lp}(g_i)$ no divide a ningún $\mathrm{lp}(g_j)$, para todo $j \neq i$. Se realizará la prueba para la primera reducción, es decir, supóngase que $g_1 \xrightarrow{H_1}_+ h_1$ donde h_1 es reducido con respecto a $H_1 = \{g_2, \ldots, g_t\}$, luego por el algoritmo de la división 3.2 se tiene que existen $c_2, \ldots c_t \in K[x_1, x_2, \ldots, x_n]$, tales que $g_1 = g_2c_2 + g_3c_3 + \cdots + g_tc_t$, con $\mathrm{lp}(g_1) = \max(\max_{2\leq i\leq t}(\mathrm{lp}(c_i)\,\mathrm{lp}(g_i)), \mathrm{lp}(h_1))$, de donde se tiene que $\mathrm{lp}(g_1) = \mathrm{lp}(h_1)$ por la condición de minimalidad de la base. Siguiendo y de este modo se obtiene que $H = \{h_1, h_2, \ldots, h_t\}$ es una base de Gröbner reducida para I. ■

Teorema 4.5. *(Buchberger) Fijado un orden de términos. Entonces cada ideal no nulo I tiene una única base de Gröbner reducida con respecto a este orden de términos.*

Demostración. Por el corolario anterior se tiene que cada ideal tiene una base de Gröbner reducida, por tanto sólo basta probar la unicidad. Sean $G = \{g_1, g_2, \ldots, g_t\}$ y $H = \{h_1, h_2, \ldots, h_s\}$ bases de Gröbner reducidas para I, entonces G y S son minimales. Por la Proposición 4.1 G y H tienen el mismo número de elementos, es decir $t = s$. Se puede asumir que para cada i, $\mathrm{lt}(g_i) = \mathrm{lt}(h_i)$. Si $g_i \neq h_i$, entonces $g_i - h_i \in I$, entonces por definición de base de Gröbner 4.1, existe j tal que $\mathrm{lp}(h_j)$

divide a $\mathrm{lp}(g_i - h_i)$, así $\mathrm{lp}(g_i - h_i) \geq \mathrm{lp}(h_j)$ y como $\mathrm{lp}(g_i - h_i) < \mathrm{lp}(h_i)$, por tanto $i \neq j$, pero $\mathrm{lp}(h_j) = \mathrm{lp}(g_j)$ divide a un término de g_i o h_i. Esto es una contradicción con el hecho de que H y G son bases de Gröbner reducidas y así $g_i = h_i$. ■

Ejemplo 4.10. Si se consideran los polinomios del Ejemplo 4.6, se puede probar que $\{x^2 - y, x^3 - x\}$ es una base de Gröbner reducida para I.

Capítulo 5

Aplicaciones de la teoría de las bases de Gröbner

En este capítulo se presentan algunas de las principales aplicaciones de la teoría de las bases de Gröbner. El objetivo es dar respuesta a los Problemas 1.1 planteados en el primer capítulo en el caso del anillo de polinomios $K[x_1, x_2, \ldots, x_n]$. Finalmente, en la última sección se estudiará la decodificación de códigos cíclicos con ayuda de la teoría de las bases de Gröbner.

5.1. Aplicaciones elementales de las bases de Gröbner

Sea $F = \{f_1, f_2, \ldots, f_s\}$ un subconjunto de polinomios de $K[x_1, x_2, \ldots, x_n]$. Supóngase que $G = \{g_1, g_2, \ldots, g_t\}$ es una base de Gröbner para el ideal $I = \langle f_1, f_2, \ldots, f_s\rangle$ con respecto a un orden de términos. El Teorema 4.1 expresa el hecho que $f \in I$ si y sólo si

$$f \xrightarrow{G}_{+} 0,$$

lo cual soluciona el *problema de membresía de un ideal*, ver Problemas 1.1. Además este proceso, permite cuando $f \in I$, encontrar $v_1, v_2, \ldots, v_t \in K[x_1, x_2, \ldots, x_n]$ tal que

$$f = v_1 g_1 + v_2 g_2 + \cdots + v_t g_t. \tag{5.1.1}$$

Así, si se utiliza el algoritmo de Buchberger 4.3 se puede hacer un seguimiento a las combinaciones lineales de los f_i's.
Durante el algoritmo para encontrar una base de Gröbner se adiciona un nuevo polinomio g al conjunto inicial, el cual es el residuo no nulo de la división de un S-polinomio por un conjunto $\{h_1, h_2, \ldots, h_l\}$. Esto es

$$g = S(h_v, h_u) - \sum_{i=1}^{l} w_i h_i,$$

para algunos $u, v \in \{1, 2, \ldots, l\}$ y algunos polinomios w_i que son calculados explícitamente durante el algoritmo de la división multivariado.
Además se puede formar una matriz M de tamaño $t \times s$ con polinomios tal que.

$$\begin{bmatrix} g_1 \\ g_2 \\ \cdot \\ \cdot \\ \cdot \\ g_t \end{bmatrix} = M \begin{bmatrix} f_1 \\ f_2 \\ \cdot \\ \cdot \\ \cdot \\ f_s \end{bmatrix}.$$

Luego en la Ecuación (5.1.1) el polinomio f puede ser visto como una combinación lineal de los polinomios $f_1, f_2, \ldots, f_s$

$$f = u_1 f_1 + u_2 f_2 + \ldots + u_s f_s,$$

para $u_1, u_2, \ldots, u_s \in K[x_1, x_2, \ldots, x_n]$. Lo que resuelve el segundo problema planteado, ver Problemas 1.1.
Para ilustrar este hecho se presenta a continuación el siguiente ejemplo.

Ejemplo 5.1. Sean $f_1 = x^2y - y + x$ y $f_2 = xy^2 - x$ polinomios en $\mathbb{Q}[x, y]$, $F = \{f_1, f_2\}$ e $I = \langle f_1, f_2 \rangle$ y considere el orden de términos *deglex*, con $x < y$.

- Pruebe que $f = x^4y - 2x^5 + 2x^2y^2 - 2x^3y - 2x^4 - 2y^3 + 4xy^2 - 3x^2y + 2x^3 - y + 2x$ pertenece a I.
- Encuentre polinomios $v_1, v_2 \in \mathbb{Q}[x, y]$ tal que $f = v_1 f_1 + v_2 f_2$.

Primero se calcula una base de Gröbner para I como sigue

```
buchberger(F,MonomialGrlexOrdering([y,x]));
[ x^2*y+x-y, x*y^2-x, -x^2-x*y+y^2, x^3-2*x+y ]
```

Tomando $f_1 = x^2y - y + x$, $f_2 = xy^2 - x$, $f_3 = -x^2 - xy + y^2$ y $f_4 = x^3 - 2x + y$, se obtiene que $G = \{f_1, f_2, f_3, f_4\}$ es una base de Gröbner para I. Observe que los polinomios f_3 y f_4 se pueden escribir como combinación lineal de los polinomios f_1 y f_2 como se muestra a continuación

$$f_3 = -yf_1 + xf_2$$

y el polinomio f_4 se puede escribir como

$$\begin{aligned} f_4 &= f_2 + xf_3 \\ &= f_2 + x(yf_1 - xf_2) - f1 \\ &= f - 2 + xyf_1 - x^2f_2 - f_1 \\ &= (xy - 1)f_1 + (-x^2 + 1)f_2. \end{aligned}$$

Dado que $\mathrm{lt}(f_2) = xy^2$ es divisible por $\mathrm{lt}(f_3) = y^2$, se puede probar que $H = \{f_3, f_4, f_1\}$ es una base de Gröbner reducida para I, utilizando GAP se tiene

```
>ReducedGroebnerBasis(G,MonomialGrlexOrdering([y,x]));
[ -x^2-x*y+y^2, x^3-2*x+y, x^2*y+x-y ]
```

Así es posible formar la matriz

$$\begin{bmatrix} f_1 \\ f_3 \\ f_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -y & x \\ xy-1 & -x^2+1 \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \end{bmatrix}$$

Sea $f = x^4y - 2x^5 + 2x^2y^2 - 2x^3y - 2x^4 - 2y^3 + 4xy^2 - 3x^2y + 2x^3 - y + 2x$, luego utilizando el Algoritmo 3.1

```
divvar(f,H,MonomialGrlexOrdering(y,x));
[ [ 2*x^2+x-2*y, -2*x^2+x*y-1, 0 ], 0 ]
```

Esta división produce residuo cero, así por Teorema 4.1, se tiene que f pertenece a I.
Además produce polinomios $h_1 = 2x^2 + x - 2y$, $h_2 = -2x^2 + xy - 1$ y $h_3 = 0$, tal que

$$\begin{aligned} f &= h_1f_3 + h_2f_4 + h_3f_1 \\ &= h_1(-yf_1 + xf_2) + h_2((xy-1)f_1 + (-x^2+1)f_2) \\ &= f_1(-yh_1 + h_2(xy-1)) + f_2(-h_2(x^2-1) + xh_1) \\ &= f_1(-2x^2y - 3xy + 2y^2 - 2x^3y + 2x^2 + x^2y^2 + 1) + f_2(2x^4 - x^3y - xy + 2x^3 - 1). \end{aligned}$$

Lo cual soluciona la segunda pregunta.

Para Encontrar las clases laterales de $K[x_1, x_2, \ldots, x_n]/I$, es necesario recordar que $I = \langle G \rangle$ donde $G = \{g_1, g_2, \ldots, g_t\}$ es una base de Gröbner para el ideal I. Además por por el Teorema 4.2 para todo $f \in K[x_1, x_2, \ldots, x_n]$ existe un único elemento $r \in K[x_1, x_2, \ldots, x_n]$ tal que

$$f \xrightarrow{G}_+ r.$$

Definición 5.1. El elemento r anterior el cual es reducido con respecto a G se denomina la forma normal de f con respecto a G que se denota como $N_G(f)$.

Proposición 5.1. *Sean $f, g \in K[x_1, x_2, \ldots, x_n]$. Entonces*

$$f \equiv g (\text{mód } I) \text{ si y sólo si } N_G(f) = N_G(g).$$

Por lo tanto $\{N_G(f) : f \in K[x_1, x_2, \ldots, x_n]\}$ es un conjunto de clases laterales para $K[x_1, x_2, \ldots, x_n]/I$. Además $N_G : K[x_1, x_2, \ldots, x_n] \longrightarrow K[x_1, x_2, \ldots, x_n]$ es $K-$ lineal.

Observación 5.1. Sea G una base de Gröbner para el ideal I y sean $r, f \in K[x_1, x_2, \ldots, x_n]$ con r reducido con respecto a G. Si $f - r \in I$, entonces $f \xrightarrow{G}_+ r$.
En efecto, si $f - r \in I$, entonces $f - r \xrightarrow{G}_+ 0$, es decir $f - r = v_1 g_1 + v_2 g_2 + \cdots + v_t g_t$, para $v_1, v_2, \ldots, v_t \in K[x_1, x_2, \ldots, x_n]$ de donde $f = v_1 g_1 + v_1 g_2 + \cdots + v_t g_t + r$ y del hecho que r es reducido con respecto a G se tiene entonces que $f \xrightarrow{G}_+ r$.

Demostración. Por el Algoritmo 3.2 existe $q \in I$ tal que $f = q + N_G(f)$, donde $q = \sum_{i=1}^{l} h_i g_i$ para $h_i \in K[x_1, x_2, \ldots, x_n]$, luego $f - N_G(f) \in I$. Por tanto $f + I = N_G(f) + I$ en $K[x_1, x_2, \ldots, x_n]/I$. Ahora para $c_1, c_2 \in K$ y para $f_1, f_2 \in K[x_1, x_2, \ldots, x_n]$ se tiene que $c_1(f_1 - N_G(f_1)) + c_2(f_2 - N_G(f_2)) \in I$, es decir $c_1 f_1 - c_1 N_G(f_1) + c_2 f_2 - c_2 N_G(f_2) \in I$, de donde $c_1 f_1 + c_2 f_2 - (c_1 N_G(f_1) + c_2 N_G(f_2)) \in I$ y $c_1 N_G(f_1) + c_2 N_G(f_2)$ es reducido con respecto a G. Por tanto si se aplica la observación anterior se tiene que $N_G(c_1 f_1 + c_2 f_2) = c_1 N_G(f_1) + c_2 N_G(f_2)$ y así $N_G : K[x_1, x_2, \ldots, x_n] \longrightarrow K[x_1, x_2, \ldots, x_n]$ es $K-$ lineal.
Ahora $f \equiv g (\text{mód } I)$ si y sólo si existe $q \in I$ tal que $f = q + g$, luego $N_G(f) = N_G(q) + N_G(g)$. Pero como $q \in I$, entonces $N_G(q) = 0$ y así $N_G(f) = N_G(g)$. Supóngase ahora que $N_G(f) = N_G(g)$, luego $f - g = f - g - N_G(f) + N_G(g) = (f - N_G(f)) - (g - N_G(g) \in I$ y así $f \equiv g (\text{mód } I)$. ■

Ejemplo 5.2. Siguiendo con el Ejemplo 5.1 la clase lateral del elemento $f + I$ en $\mathbb{Q}[x]$ es de la forma $0 + I$, donde 0 es el residuo de la división de f por $G = \{x^2y + x - y, xy^2 - x, -x^2 - xy + y^2, x^3 - 2x + y\}$, dado que

```
>divvar(f,G,MonomialGrlexOrdering(y,x));
[ [ x^2-2*x+2*y-2, 2, -2*y+2, -2*x^2-2*x-3 ], 0 ]
```

Para el polinomio $j = x^{10} + 4x^7y + x^5y^4 - 5x^3y^3 + xy + 2x$, la clase lateral del elemento $j + I$ en $\mathbb{Q}[x]$ es de la forma $7x^2 - 5xy + 7x - 3y + I$, donde $7x^2 - 5xy + 7x - 3y$ es el residuo de la división de j por G, puesto que en GAP se tiene que

```
>divvar(j,G,MonomialGrlexOrdering(y,x));
[ [ x^3*y^3+3*x^5-x^2*y^2+x*y^3+x^3-5*x*y^2+x*y-2*y^2+5*y-3, y^2-5*y+2,
      -2*y+5, x^7+2*x^5+x^3+x ], 7*x^2-5*x*y+7*x-3*y ]
```

Ahora para encontrar una base para el K-espacio vectorial $K[x_1, x_2, \ldots, x_n]/I$ se tiene el siguiente resultado.

Proposición 5.2. *Una base para el K-espacio vectorial $K[x_1, x_2, \ldots, x_n]/I$ consiste de todos los productos potencia $X \in \mathbb{T}^n$, tal que $lp(g_i)$ no divide a X para todo $i = 1, 2, \ldots, t$.*

Demostración. Para cualquier $f \in K[x_1, x_2, \ldots, x_n]$, se tiene que $f + I = N_G(f) + I$ en $K[x_1, x_2, \ldots, x_n]/I$, es decir que cualquier polinomio f se puede escribir como combinación lineal de $N_G(f)$. Además, ya que la forma normal es única, se puede afirmar de que si la $\sum \alpha X + I = 0$ en $K[x_1, x_2, \ldots, x_n]/I$ con $\alpha \in K$ y $X \in \mathbb{T}^n$, entonces dicha suma $\sum \alpha X \in I$. Así por hipótesis se tiene que $\text{lp}(g_i)$ no divide a X para todo $i = 1, 2, \ldots, t$ con lo cual se tiene que cada $\alpha = 0$. ■

Ejemplo 5.3. Continuando con el Ejemplo 5.1, se tiene que la base para $\mathbb{Q}[x,y]/I$ son las clases laterales de $1, x, y, x^2, xy$, es decir

$$\{1+I, x+I, y+I, x^2+I, xy+I\}.$$

Como aplicaciones adicionales

- Dar la tabla de multiplicación en $K[x_1, x_2, \ldots, x_n]/I$.
- Determinar si dos ideales I, J de $K[x_1, x_2, \ldots, x_n]$ son iguales.

Para $f, g \in K[x_1, x_2, \ldots, x_n]$ la clase lateral de f por la clase lateral de g será la forma normal de fg.

$\times$	1	x	y	x^2	xy
1	1	x	y	x^2	xy
x	x	x^2	xy	$-y+2x$	$y-x$
y	y	xy	$xy+x^2$	$y-x$	x
x^2	x^2	$-y+2x$	$y-x$	$-xy+2x^2$	$xy-x^2$
xy	xy	$y-x$	x	$xy-x^2$	x^2

Cuadro 5.1: Tabla de multiplicación de la base $1, x, y, x^2, xy$ para $\mathbb{Q}[x,y]/I$.

Ejemplo 5.4. Para el Ejemplo 5.3 los productos de la base están descritos en el Cuadro 5.1, por ejemplo para las clases $(2x^2+y+I)$ y $(3xy-5+I)$ se tiene que $(2x^2+y)(3xy-5) = 6x^2-10x^2+3xy-5y \equiv 6(xy-x^2)-10x^2+3x-5y = 6xy-16x^2+3x-5y \mod I$), es decir

$$(2x^2+y+I)(3xy-5+I) = 6xy-16x^2+3x-5y+I.$$

Este producto resulta primero de Multiplicar los polinomios y luego reemplazar los productos potencia de cada término utilizando el Cuadro 5.1.

Ahora para determinar si dos ideales I, J de $K[x_1, x_2, \ldots, x_n]$ son iguales; se puede utilizar el Teorema 4.5 en la medida de que I, J son iguales si y sólo si tienen la misma base de Gröbner reducida.
Otra forma de ver este problema es verificar el hecho de que $I = J$ si y sólo si $I \subseteq J$ y $J \subseteq I$, lo cual ya es posible verificar con ayuda del *problema de membresía de un ideal*.

Aplicaciones entre variedades
Considere el mapa de proyección

$$\Pi: \quad \bar{K}^{m+n} \longrightarrow \bar{K}^m$$

$$(a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n) \longrightarrow (a_1, a_2, \ldots, a_m),$$

donde $\bar{K}$ es la clausura algebraica del campo K, es decir, un campo K es algebraicamente cerrado si para cada polinomio $f \in K[x]$ en una variable, la ecuación $f = 0$ tiene una solución en K y que cada campo K esta contenido en un campo $\bar{K}$, en el cual cada elemento de $\bar{K}$ es raiz de un polinomio no nulo en una variable con coeficientes en K, por ejemplo, la clausura algebraica de $\mathbb{R}$ es $\mathbb{C}$.

Definición 5.2. Para un ideal I de $K[x_1, x_2, \ldots, x_n]$ se define el radical de I, que se denota con $\sqrt{I}$, como

$$\sqrt{I} = \{f \in K[x_1, x_2, \ldots, x_n] \ : \ \exists\, e \text{ tal que } f^e \in I\}.$$

Observación 5.2. Sea I un ideal de $K[x_1, x_2, \ldots, x_n]$, luego se tiene

1. $\sqrt{I}$ es un ideal en $K[x_1, x_2, \ldots, x_n]$.
2. $V_K(I) = V_K(\sqrt{I})$.

Se presenta ahora el Teorema de los ceros de Hilbert. Su demostración se puede encontrar en [6].

Teorema 5.1. *(Teorema de los ceros de Hilbert)*

$$I(V_{\bar{K}}(I)) = \sqrt{I},$$

para todo ideal I de $K[x_1, x_2, \ldots, x_n]$.

Proposición 5.3. *Si $S \subset K^n$, entonces $V(I(S))$ es la más pequeña variedad que contiene a S, esto es, si W es cualquier variedad que contiene a S, entonces $V(I(S)) \subseteq W$. Este conjunto se denomina la clausura de Zariski de S.*

Demostración. Sea $W = V(J) \subseteq \bar{K}^n$ una variedad que contiene a S, donde J es un ideal en $K[x_1, x_2, \ldots, x_n]$. Entonces $I(W) \subset I(S)$ y $V(I(S)) \subset V(I(W))$, luego por Teorema 5.1 se tiene que $V(I(W)) = V(\sqrt{J})$, y por Observación 5.2, $V(\sqrt{J}) = V(J) = W$, así $V(I(S)) \subseteq W$. ■

Teorema 5.2. *Sea I un ideal de $K[y_1, y_2, \ldots, y_m, x_1, x_2, \ldots, x_n]$, la clausura de Zariski de $\Pi(V(I))$ es $V(I \cap k[y_1, \ldots, y_m])$.*

Demostración. Sea $V = V(I)$ y $I_y = I \cap k[y_1, \ldots, y_m]$, se debe probar que $\Pi(V) = V(I_y)$.
$\Pi(V) \subseteq V(I_y)$. En efecto, sea $(a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n) \in V$, luego al aplicar la aplicación Π, se tiene que $(a_1, a_2, \ldots, a_m) \in \Pi(V)$. Si $f \in I_y$, entonces $f(a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n) = 0$, ya que $f \in I$ y por tanto $f(a_1, a_2, \ldots, a_m) = 0$ porque f solo contiene las variables $y_1, \ldots, y_m$ y así se cumple la afirmación.
$V(I_y) \subseteq \Pi(V)$. Por la Proposición 5.3 se tiene que $V(I_y) \subseteq V(I(\Pi(V)))$, primero se puede ver que

$I(\Pi(v)) \subseteq \sqrt{I_y}$. Sea $f \in I(\Pi(v))$, luego $f(a_1, a_2, \ldots, a_m) = 0$, para $(a_1, a_2, \ldots, a_m) \in \Pi(V)$, si se observa a f como un elemento de $K[y_1, y_2, \ldots, y_m, x_1, x_2, \ldots, x_n]$, $f(a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n) = 0$, para todo $(a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n) \in V$, por Teorema 5.1, existe un e tal que $f^e \in I$, pero ya que f solo contiene a las variables $y_1, y_2, \ldots, y_m$, y por el hecho de que $f \in \Pi(V)$ se tiene que $f^e \in I_y$, de donde $f \in \sqrt{I_y}$, entonces $V(I_y) = \sqrt{I_y} \subseteq V(I(\Pi(V)))$. ■

5.2. Aplicación de la teoría de las bases de Gröbner para la decodificación de códigos cíclicos

En esta sección se estudiará la utilización de las bases de Gröbner en la Teoría de Códigos, se presenta una breve introducción de los conceptos más importantes y teoremas (sin demostración) en la Teoría de Códigos correctores de errores hasta presentar la decodificación de un código cíclico utilizando bases de Gröbner. El lector interesado puede encontrar las demostraciones y más información sobre la Teoría de Códigos en [8, 7].

5.2.1. Códigos correctores de errores

La Teoría de Códigos busca solucionar los problemas que surgen tras la manipulación y trasmisión de información digital, dichos problemas suelen presentarse como errores en la trasmisión de la información. Los códigos correctores de errores son un mecanismo que permite detectar cuando se ha producido un error y si es posible corregirlo.
Para enviar un mensaje el emisor lo codifica añadiendo algunos símbolos o arreglos mediante alguna regla sistemática, el mensaje codificado es enviado a través de un canal en el cual pueden ocurrir errores, luego el receptor por su parte recibe el mensaje codificado y procede a decodificarlo, es decir, a comparar palabras que estén "más cercanas". Esto se traduce en capacidad de detección y corrección de errores que se han producido en el proceso, con el fin de encontrar el mensaje en su formato original.

Un alfabeto A es un conjunto finito de símbolos los cuales forman los elementos de A. Una palabra es una sucesión finita de elementos de A. El conjunto de palabras que se pueden formar a partir de A se denota como A^*. La longitud de una palabra es el número de símbolos que contiene. El conjunto A^n denota todas las palabras de A de longitud n.

Definición 5.3. Un código es un subconjunto C de A^*, cuyos elementos se denominan palabras código. Si todas las palabras tienen la misma longitud, el código C se denomina un código de bloques y se define el tamaño de C como el número de palabras del código.

Ejemplo 5.5. Sea $A = \{0, 1\}$, $C = \{000, 011, 101, 110\}$, C es un código de bloques de longitud 3 y tamaño 4.

La idea principal de la Teoría de Códigos es dotar al conjunto A con alguna estructura algebraica, por ejemplo, si A contiene q elementos, donde q es la potencia de un número primo, $q = p^n$ para $n > 0$, entonces A se identifica con el campo finito $\mathbb{F}_q$. Durante el resto del capítulo se empleará esta identificación.

A continuación se define el concepto de distancia de Hamming el cual es fundamental para la detección y corrección de errores.

Definición 5.4. Sean $x, y \in A^n$; palabras de longitud n. La distancia de Hamming $d(x, y)$ es el número de coordenadas en que difieren x y y, es decir

$$d(x, y) = \#\{i \ : \ 1 \leq i \leq n, \ x_i \neq y_i\}.$$

La capacidad de detectar y corregir errores de un código C se basa en el siguiente concepto.

Definición 5.5. La distancia mínima de un código C se define como la menor distancia entre sus palabras; es decir

$$d(C) = \text{mín}\{d(x, y) \ : \ x, y \in C, \ x \neq y\}.$$

La siguiente definición presenta el concepto de peso de un código.

Definición 5.6. Para una palabra a de longitud n sobre $\mathbb{F}_q$, se define el peso $w(a)$ como el número de coordenadas distintas de cero.

Definición 5.7. (Código detector de t-errores). Un código C detecta t-errores si cada vez que se envía una palabra código y ocurren entre 1 y t errores durante la transmisión, la palabra resultante no es una palabra código. Un código C detecta exactamente t-errores, si este detecta t errores, pero no detecta $t + 1$ errores (es decir, existe al menos una palabra código la cual cambiando $t + 1$ coordenadas origina una nueva palabra código).

Teorema 5.3. *Un código C detecta exactamente t-errores si y sólo si $d(C) = t + 1$.*

Definición 5.8. (Código corrector de t-errores). Asumiendo que los empates son considerados como errores, un código C corrige t-errores si la decodificación por distancia mínima corrige todos los errores de tamaño t ó menos en cualquier palabra código. Un código C corrige exactamente t-errores, si este corrige t-errores, pero no corrige $(t+1)$-errores. Es decir, todos los errores de tamaño t son corregidos, pero al menos un error de tamaño $t + 1$ es decodificado incorrectamente.

Teorema 5.4. *Un código C corrige exactamente t-errores si y sólo si $d(C) = 2t+1$ ó $d(C) = 2t+2$.*

Corolario 5.1. *$d(C) = d$ si y sólo si C corrige exactamente $\lfloor \frac{d-1}{2} \rfloor$-errores.*

Se estudiarán los códigos lineales, en particular los códigos cíclicos, por lo cual se dan las siguientes definiciones.

Definición 5.9. Un código lineal q-ario de longitud n es un subespacio vectorial $C \subseteq \mathbb{F}_q^n$.

Un código lineal de longitud n y dimensión k, se denomina un $[n, k]$-código. Si además tiene distancia mínima d, se dice que es un $[n, k, d]$-código.

Cabe ahora la pregunta de ¿cómo generar un código? Para dar respuesta se introduce el concepto de matriz generadora.

Definición 5.10. Sea C un código lineal. Una matriz H generadora del código C es una matriz de tamaño $k \times n$ cuyas filas constituyen una base para el código C.

Ejemplo 5.6. Sea $A = \{0, 1\}$, la matriz $H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ genera un código lineal $[3, 2]$-código. En efecto

$$(x_1, x_2) \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = (x_1, x_1 + x_2, x_2),$$

codifica a

$$00 \to 000,\ 01 \to 011,\ 10 \to 110,\ 11 \to 101,$$

formando el código $C = \{000, 011, 110, 101\}$.

Para determinar si una palabra pertenece al código se utiliza el concepto de matriz de control del código.

Definición 5.11. Una matriz H de tamaño $(n - k) \times n$ es una matriz de control del código C si para todo vector $x \in \mathbb{F}_q^n$ se tiene que

$$x \in C \iff Hx^T = 0.$$

Definición 5.12. El síndrome de un vector y se define como

$$S(y) = Hy^T \in \mathbb{F}_q^n.$$

De esta forma el síndrome de un vector y sirve para determinar cuando y pertenece o no al código, dado que $y \in C \iff S(y) = 0$.

Códigos cíclicos

Los códigos cíclicos son un tipo especial de códigos que frecuentemente se usan en la detección y corrección de errores.

Definición 5.13. Un código lineal C de longitud n sobre $\mathbb{F}_q$ es cíclico, si para cada $(c_0, c_1, \ldots, c_{n-1}) \in C$ se tiene que $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.

Sean $\mathbb{F}_q[x]_{(n-1)}$ el espacio vectorial de los polinomios sobre $\mathbb{F}_q$ con grado menor que n y R_n el anillo cociente $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$. Se puede demostrar que

$$\mathbb{F}_q^n \cong \mathbb{F}_q[x]_{(n-1)} \cong R_n.$$

De esta forma se puede identificar a cada vector $(a_0, a_1, \ldots, a_{n-1})$ con el polinomio $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ y con la clase lateral $a_0 + a_1x + \ldots + a_{n-1}x.^{n-1} + \langle x^n - 1\rangle$ en R_n.
Además, se puede probar, que cuando q y n son primos relativos, el polinomio $x^n - 1$ se puede factorizar en polinomios irreducibles distintos y sus raíces forman un grupo cíclico de orden n.

En realidad se puede definir un isomorfismo de espacios vectoriales entre $\mathbb{F}_q^n$ y el anillo cociente R_n, como ya se mencionó arriba, como sigue

$$\phi(C) : \mathbb{F}_q^n \to R_n,$$

tal que $\phi(a_0, a_1, \ldots, a_{n-1}) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$. El siguiente teorema establece un puente entre los códigos cíclicos y los ideales de R_n, la ventaja es que de esta forma se pueden estudiar propiedades en el anillo R_n que tienen su traducción inmediata a los códigos cíclicos.

Teorema 5.5. *Sea $C \subseteq \mathbb{F}_q^n$ un código lineal. Entonces C es cíclico sí y solo si $\phi(C)$ es un ideal de R_n.*

Dado que R_n es un dominio de ideales principales, lo que significa que cada ideal (código cíclico) C es generado por un polinomio $g(x)$, que se denomina polinomio generador de C. Este polinomio $g(x)$ es el único polinomio mónico de menor grado en C. Así

$$C = \{f(x)g(x) : f(x) \in \mathbb{F}_q[x] \text{ y } \deg(g(x)) < n\}.$$

Además, se tienen los siguientes resultados.

Teorema 5.6. *Dado un código cíclico C de longitud n, se cumplen las siguientes afirmaciones.*

1. *Existe un único polinomio mónico $g(x) \in \mathbb{F}_q[x]$ divisor de $x^n - 1$, tal que $C = \langle g(x)\rangle$.*
2. *Si el grado de $g(x)$ es r, entonces C tiene dimensión $n - r$ y*

$$C = \langle g(x)\rangle = \{h(x)g(x) \ : \ deg(h(x)) < n - r\}.$$

3. *Si $g(x) = g_0 + g_1x + \cdots + g_rx^r$, entonces $g_0 \neq 0$ y C tiene matriz generadora*

$$H = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & g_2 & \ldots & g_r & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & g_2 & \ldots & g_r & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & \ldots & g_0 & \ldots & g_r \end{pmatrix}.$$

Definición 5.14. Sea C un código cíclico de longitud n, con polinomio generador $g(x)$ de grado $n-k$, se denomina polinomio de control del código C a

$$h(x) = \frac{x^n - 1}{g(x)} = h_0 + h_1 x + \cdots + h_k x^k.$$

Proposición 5.4. *Para un código cíclico C de longitud n cuyo polinomio de control es $h(x) = h_0 + h_1 x + \ldots + h_k x^k$, luego*

$$H = \begin{pmatrix} h(x) \\ xh(x) \\ \vdots \\ x^{n-k-1}h(x) \end{pmatrix} = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \ldots & h_0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & \ldots & h_k & \ldots & h_0 \end{pmatrix}$$

es una matriz de control de C.

Códigos BCH

Observe que dado que el polinomio generador $g(x)$ de un código cíclico C de longitud n debe dividir a $x^n - 1$, entonces las raíces de $g(x)$ son también son raíces de $x^n - 1$, es decir, raíces n-ésimas de la unidad. Así, se puede identificar un código cíclico especificando su polinomio generador $g(x)$ o, equivalentemente, especificando cuales de las raíces n-ésimas de la unidad son las raíces de $g(x)$. Esto lleva a la construcción de varias familias de códigos, dependiendo en como se escogen las raíces. Los códigos BCH son códigos cíclicos, en los cuales el objetivo es buscar que el código tenga una longitud y distancia designada.

Estos códigos fueron descubiertos independientemente por R.C Bose y D.K Ray-Chaudhuri (1960) y por A. Hocquenghem (1959).

Definición 5.15. Un código BCH de longitud n y distancia designada δ, es un código cíclico cuyo polinomio generador tiene entre sus raíces a $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$, para $b \in \mathbb{N}$ y $2 \leq \delta \leq n$, donde $\alpha \in \mathbb{F}_{q^m}$ es una n-ésima raíz primitiva de la unidad, siendo m el orden multiplicativo de q módulo n, es decir $q^m \equiv 1 \mod n$.

Definición 5.16. Si se toma a $b = 1$, el código se denomina BCH en sentido estricto. Si la longitud n es de la forma $n = q^m - 1$ entonces el código se denomina código BCH primitivo y α es un elemento primitivo de $\mathbb{F}_{q^m}$.

Proposición 5.5. *Un código BCH de distancia designada δ, posee distancia mínima $d \geq \delta$.*

Un polinomio generador de un código BCH está dado por

$$g(x) = \operatorname{lcm}\{m_b(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x)\},$$

donde $m_i(x)$ es el polinomio irreducible de α^i sobre $\mathbb{F}_q$, para $i = b, \ldots, b+\delta-2$. La dimensión del código es $n - \deg g(x)$.
El código BCH de longitud n y distancia designada δ sobre $\mathbb{F}_q$, generado por $g(x)$ se denota con $B_q(n, \delta, \alpha, b)$.

Ejemplo 5.7. Sea $m \in \mathbb{Z}^+$, $n = 2^m - 1$ y $\alpha \in \mathbb{F}_{2^m}$ una raíz primitiva n-ésima de la unidad y $b = 1$. En consecuencia se pueden construir códigos binarios BCH primitivos. Por ejemplo, con $\delta = 2$ se tiene el código

$$C_2 = \{c(x) \in R_n \ : \ c(\alpha) = 0\},$$

donde $R_n = \mathbb{F}_2[x]/\langle x^n - 1\rangle$.
Como $c(x) \in \mathbb{F}_2[x]$, si $c(\beta) = 0$, se tiene que $c(\beta^2) = 0$, por lo tanto

$$C_2 = C_3 = \{c(x) \in R_n \ : \ c(\alpha) = c(\alpha^2) = 0\},$$

donde $C_2 = C_3$ es un código de Hamming de distancia mínima 3 [1]
Para $\delta = 4$, el código que se obtiene es el siguiente

$$\begin{aligned} C_4 &= \{c(x) \in R_n \ : \ c(\alpha) = c(\alpha^2) = c(\alpha^3) = 0\} \\ &= \{c(x) \in R_n \ : \ c(\alpha) = c(\alpha^3) = 0\}. \end{aligned}$$

Los polinomios de C_4 verifican la condición de que $c(\alpha^4) = 0$, así $C_4 = C_5$ cuya distancia mínima es mayor o igual a cinco. La matriz de control de C_4 está dada por

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \ldots & \alpha^{3(n-1)} \end{pmatrix}.$$

Sea $m_1(x) = \mathrm{Irr}(\alpha, \mathbb{F}_2)$[2] el polinomio irreducible de α, $m_3(x) = \mathrm{Irr}(\alpha^3, \mathbb{F}_2)$ el polinomio irreducible de α^3, luego para $m = 4$ se tiene que $n = 15$ y así con ayuda de GAP se puede calcular $m_1(x)$ y $m_3(x)$ como sigue

```
>F:=GF(16);
GF(2^4)

>a:=PrimitiveElement(F);
Z(2^4)

>m1:=MinimalPolynomial(GF(2),a);
x_1^4+x_1+Z(2)^0
```

[1] Un código binario de Hamming de orden k sobre $\mathbb{F}_2$ es un código con matriz de control H_k de orden $k \times n$, cuyas columnas son los elementos de $\mathbb{F}_2^k \backslash \{0\}$ en cualquier orden.

[2] Donde $\mathrm{Irr}(\alpha, \mathbb{F}_2)$ denota el polinomio minimal para α sobre $\mathbb{F}_2$.

```
>m3:=MinimalPolynomial(GF(2),a^3);
x_1^4+x_1^3+x_1^2+x_1+Z(2)^0
```

Es decir,

$$m_1(x) = 1 + x + x^4,$$
$$m_3(x) = 1 + x + x^2 + x^3 + x^4,$$

luego el polinomio generador de C_4 es

$$\begin{aligned} g(x) &= \operatorname{lcm}(m_1(x), m_3(x)) \\ &= (1 + x + x^4)(1 + x + x^2 + x^3 + x^4) \\ &= 1 + x^4 + x^6 + x^7 + x^8. \end{aligned}$$

La dimensión de C_4 es $n - \deg g(x) = 15 - 8 = 7$.
Finalmente, se calcula el código que se obtiene para $\delta = 6$, el código es el siguiente

$$\begin{aligned} C_6 &= \{c(x) \in R_n \ : \ c(\alpha) = c(\alpha^2) = c(\alpha^3) = c(\alpha^4) = c(\alpha^5) = 0\} \\ &= \{c(x) \in R_n \ : \ c(\alpha) = c(\alpha^3) = c(\alpha^5) = 0\}. \end{aligned}$$

Los polinomios de C_6 verifican la condición de que $c(\alpha^6) = 0$, así $C_6 = C_7$ y la distancia mínima es mayor o igual a siete. La matriz de control del código C_6 es

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & ... & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & ... & \alpha^{3(n-1)} \\ 1 & \alpha^5 & \alpha^{10} & ... & \alpha^{5(n-1)} \end{pmatrix}.$$

Para $m_1(x) = \operatorname{Irr}(\alpha, \mathbb{F}_2)$, $m_3(x) = \operatorname{Irr}(\alpha^3, \mathbb{F}_2)$, $m_5(x) = \operatorname{Irr}(\alpha^5, \mathbb{F}_2)$, luego el polinomio generador de C_6 es

$$g(x) = \operatorname{lcm}(m_1(x), m_3(x), m_5(x)).$$

Si se escoge nuevamente a $m = 4$ se tiene que

```
>m5:=MinimalPolynomial(GF(2),a^5);
x_1^2+x_1+Z(2)^0
```

Es decir,

$$m_5(x) = 1 + x + x^2,$$

luego,

$$\begin{aligned} g(x) &= \operatorname{lcm}(m_1(x), m_3(x), m_5(x)) \\ &= (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)(1 + x + x^2) \\ &= 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}. \end{aligned}$$

La dimensión de C_6 es $n - \deg g(x) = 15 - 10 = 5$.

La variedad síndrome de un código cíclico

Sea C un $[n,k]$-código cíclico definido sobre $\mathbb{F}_q$, con polinomio generador $g(x) = f_{i1}f_{i2}\cdots f_{ir}$ y α_{ij} una raíz de f_{ij}, para $j = 1, 2, \ldots, r$, luego se tiene que

$$C = \langle g(x)\rangle = \{c(x) \ : \ c(\alpha_{i1}) = c(\alpha_{i2}) = \cdots = c(\alpha_{ir}) = 0\}.$$

Sea $\alpha \in \mathbb{F}_q^m$ una raíz primitiva de la unidad, donde $\mathbb{F}_q^m$ es una extensión finita sobre $\mathbb{F}_q$, luego cada raíz α_{ij} de $g(x)$ se puede representar como α^{i_j}, con $\{i_1, i_2, \ldots, i_r\} \subseteq \{0, 1, \ldots, n-1\}$. Es posible conocer si una palabra está o no en el código, considerando la matriz

$$H' = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \ldots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \ldots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_r} & \alpha^{2i_r} & \ldots & \alpha^{(n-1)i_r} \end{pmatrix}.$$

Es decir, para un polinomio $f(x) = f_0 + f_1x + \ldots + f_{n-1}x^{n-1} \in \mathbb{F}_q[x]$, se desea saber si $f(x)$ está en C, forzando notación se puede utilizar en lugar del polinomio $f(x)$, el vector $(f_0, f_1, \ldots, f_{n-1})$ y multiplicar

$$H'f(x) = H'(f_0, f_1, \ldots, f_{n-1})^T = \begin{pmatrix} f_0 + f_1\alpha^{i_1} + \ldots + f_{n-1}\alpha^{(n-1)i_1} \\ f_0 + f_1\alpha^{i_2} + \ldots + f_{n-1}\alpha^{(n-1)i_2} \\ \vdots \\ f_0 + f_1\alpha^{i_r} + \ldots + f_{n-1}\alpha^{(n-1)i_r} \end{pmatrix} = \begin{pmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \vdots \\ f(\alpha_r) \end{pmatrix}.$$

Así $f(x) \in C \iff H'f(x) = 0$.

Note que H' no es estrictamente una matriz de control del código C, aunque cumple funciones similares, ya que los valores α^{ti_j} están en $\mathbb{F}_q^m$.

Sea $c \in \mathbb{F}_q^n$ una palabra código y $\tilde{c}$ la palabra recibida, luego $\tilde{c} = c+e$, donde $e = (e_0, e_1, \ldots, e_{n-1})$ $\in \mathbb{F}_q^n$ es el vector error. Si se observa a este vector como el polinomio $e(x) = e_0+e_1x+\ldots+e_{n-1}x^{n-1}$ y si se calcula $H'e(x)^T$, se obtiene un sistema de r ecuaciones relacionadas con el síndrome de $\tilde{c}$, es decir

$$e_0 + e_1\alpha^{i_j} + \ldots + e_{n-1}\alpha^{(n-1)i_j} = s_j, \ j = 1, 2, \ldots, r. \tag{5.2.1}$$

Durante el resto de esta sección se asumirá que la distancia minima de C es $2t-1$ y $w(e) = \tau \leq t$. El siguiente teorema, presenta el hecho de que para un error hay uno y solo un síndrome.

Teorema 5.7. *Sea C un código de distancia $d \geq 2t+1$. Cada error e con $w(e) \leq t$ le corresponde uno y solamente un síndrome s.*

Las soluciones de 5.2.1 se expresarán como puntos en una variedad. Para ello, se consideran los

siguientes polinomios

$$\begin{aligned} f_j &= y_1 z_1^{i_j} + y_2 z_2^{i_j} + \ldots + y_t z_t^{i_j} - x_j,\ j = 1, 2, \ldots, r, \\ h_k &= z_k^{n+1} - z_k,\ k = 1, 2, \ldots, t \ \text{(Polinomio de control de las raíces)}, \\ l_k &= y_k^{q-1} - 1,\ k = 1, 2, \ldots, t \ \text{(Polinomio de control de los coeficientes)}. \end{aligned}$$

Ahora se considera el conjunto

$$F = \{f_j \ : \ j = 1, 2, \ldots, r\} \cup \{h_k \ : \ k = 1, 2, \ldots, t\} \cup \{l_k \ : \ k = 1, 2, \ldots, t\}.$$

Sea I el ideal generado por F y $V(F)$ la variedad definida por F, es decir

$$V(F) = \{p \in \mathbb{F}_{q^m}^{r+2t} \ : \ f_j(p) = h_k(p) = l_k(p) = 0,\ j = 1, 2, \ldots, r,\ k = 1, 2, \ldots, t\} = V(I).$$

El cardinal de $V(I)$ es $(q-1)^t(n+1)^t$, ya que hay $q-1$ puntos para cada l_k de t posibles y $n+1$ puntos de h_k de t posibles. Se denomina a $V(I)$ como la variedad síndrome y a I como el ideal síndrome, además se puede observar que $V(I)$ contiene la información necesaria para decodificar cualquier palabra recibida $\tilde{c}$. En efecto, dado un síndrome $s = H\tilde{c} = He$ con $w(e) = \tau \leq t$, los puntos $p \in V(F)$ que determina la localización y valores correspondiente a e están dados por

$$p(s_1, s_2, \ldots, s_r, 0, \ldots, 0, \alpha^{l_1}, \alpha^{l_2}, \ldots, \alpha^{l_\tau}, *, \ldots, *, \beta_1, \beta_2, \ldots, \beta_\tau), \tag{5.2.2}$$

donde las entradas no nulos de e están localizados en las coordenadas $l_1, l_2, \ldots, l_\tau$ (posiciones) y sus valores en $\beta_1, \beta_2, \ldots, \beta_\tau$ respectivamente, los valores $*$ indican que coordenada puede ser cualquier elemento no nulo de $\mathbb{F}_q$. Para cada síndrome s hay $\binom{t}{n} t!(q-1)^{t-\tau}$, estos puntos se obtienen por la permutación de las variables z y las permutaciones de las variables y.
Ahora se construye el conjunto V_s como el conjunto de los $\binom{t}{n} t!(q-1)^{t-\tau}$ puntos correspondientes a s y S como el conjunto de todos los posibles síndromes no nulos correspondientes a errores con peso a lo más t y se define a $\varepsilon = \bigcup_{s \in S} V_s$. Se puede observar que $|\varepsilon| = \sum_{s \in S} |V_s|$ por ser disjuntos, luego para un peso τ, $|V_s| = (q-1)^\tau \binom{t}{\tau} \tau!(q-1)^{t-\tau}$ y así ε contiene $(q-1)^\tau \sum_{j=1}^{t} \binom{n}{j} \binom{t}{j} j!$ puntos. Toda la información necesaria para decodificar cualquier mensaje recibido está en el conjunto ε. Pero los polinomios de la ecuación 5.2.1 definen una variedad $V(F)$ muy grande.
Para restringir $V(F)$ a ε se adiciona un nuevo polinomio a F, a saber $\binom{t}{2}$ polinomios $z_k z_\lambda \frac{z_k^n - z_\lambda^n}{z_k - z_\lambda}$ $k, \lambda = 1, 2, \ldots, t$ al conjunto F. Luego la variedad correspondiente ahora al conjunto de polinomios es ε. Estos $\binom{t}{2}$ polinomios obligan a las coordenadas z_k y z_λ a ser a lo más una de ellas no nula ó diferentes de cero y distintas. Pero a pesar de todo el cálculo de $V(F)$ es muy costoso, para ello una solución para decodificar usando $V(F)$ es observar que el número de errores es t menos el número de coordenadas nulas en z en el punto p (5.2.2), es decir el primer paso para decodificar es observar que $\tau = t - (t - \tau)$ y que el número de coordenadas nulas de z en p, puede ser calculado al observar las diversas proyecciones de la variedad $V(F)$.

Definición 5.17. Sea $X \subseteq \mathbb{F}_{q^m}^b$. Para cualquier $a \leq b$, se define la proyección de X sobre las primeras a coordenadas por

$$\prod_a(X) = \{p \in \mathbb{F}_{q^m}^a \ : \ \exists \tilde{p} \in \mathbb{F}_{q^m}^{b-a} \text{ tal que } (p, \tilde{p}) \in X\}. \tag{5.2.3}$$

Ahora es posible relacionar los números de errores a la proyección de $V(F)$.

Teorema 5.8. *Sea $\boldsymbol{0}_k$ el vector nulo de $1 \times k$. Dado $\tilde{c} \in \mathbb{F}_q^n$ y su correspondiente síndrome $s = H\tilde{c}$, entonces hay τ errores en $\tilde{c}$ si y sólo si*

$$(s, \boldsymbol{0}_k) \in \prod_{r+k}(V(F)) \ \forall \in k \leq t - \tau$$

y

$$(s, \boldsymbol{0}_{t-\tau+1}) \notin \prod_{r+t-\tau+1}(V(F)).$$

Demostración. Sea s el síndrome correspondiente a un vector error e de peso $\tau \leq t$, luego existe un punto p como en (5.2.2) $\in V(F)$, de esta forma se tiene que $(s, \mathbf{0}_k) \in \prod_{r+k}(V(F))$ para todo $k \leq t - \tau$. Ahora supóngase que $\tilde{p} = (s, \mathbf{0}_{t-\tau+1}) \in \prod_{r+t-\tau+1}(V(F))$, por definición de proyección, existe un punto $\hat{p_0}$ tal que $p_0 = (\tilde{p}, \hat{p_0}) \in V(F)$. Sea

$$\hat{p_0} = (\gamma_1, \gamma_2, \ldots, \gamma_{\tau-1}, \eta_1, \eta_2, \ldots, \eta_t) = (\gamma, \eta).$$

El vector γ no es nulo, ya que si lo fuera implicaría que $s = 0$, es decir $\tilde{c} \in C$. También las coordenadas de γ no son todas distintas, pues si lo fueran representaría un nuevo error y se tendrían dos vectores error distintos con peso $\tau \leq t$ asociados a un solo síndrome s, lo cual contradice el Teorema 5.7. Por lo tanto existen $\gamma_i = \gamma_j$, para algún i, j, con $i \neq j$. Sin perdida de generalidad se puede suponer que $\gamma_i = \gamma_2$ y se toma a

$$\hat{p_1} = (0, \gamma_2, \gamma_3, \ldots, \gamma\tau - 1, \eta_1, \eta_2, \ldots, \eta_t) \text{ si } n_1 + n_2 \neq 0$$

$$\hat{p_1} = (0, 0, \gamma_3, \ldots, \gamma\tau - 1, \eta_1, \eta_2, \ldots, \eta_t) \text{ en otro caso.}$$

Donde se puede observar que $p_1 = (\tilde{p}, \hat{p_1}) \in V(F)$. Si se sigue este proceso se eliminan todas las variables repetidas en γ y se tendrá un vector con coordenadas no nulas distintas que representan a un vector error con peso estrictamente menor que τ que corresponde al síndrome s contradiciendo el Teorema 5.7, por lo tanto $(s, \mathbf{0}_{t-\tau+1}) \notin \prod_{r+t-\tau+1}(V(F))$.
Para la otra implicación supóngase que $(s, \mathbf{0}_k) \in \prod_{r+k}(V(F)) \ \forall \in k \leq t - \tau$ y que $(s, \mathbf{0}_{t-\tau+1}) \notin \prod_{r+t-\tau+1}(V(F))$. Luego $(s, \mathbf{0}_{t-\tau})$ extiende a un punto p en $V(F)$ y usando el argumento anterior se puede relacionar a este punto con un único vector error de peso exactamente τ. ■

Como consecuencia del teorema anterior se tiene el siguiente resultado.

Corolario 5.2. *Sea* $\Gamma = \{p \in V(F) \ : \ p = (s, \boldsymbol{0}_{t-\tau}, *, *, \ldots, *)\}$, *entonces el conjunto* $\prod_{r+t-\tau+1}(\Gamma)$ *contiene exactamente* τ *puntos distintos de la forma* $(s, \boldsymbol{0}_{t-\tau}, \alpha^{l_i})$ *y las posiciones del error correspondiente vienen dadas por* l_i, $1 \leq i \leq \tau$.

El objetivo ahora es desarrollar un método para decodificar códigos cíclicos usando representaciones polinomiales de estas proyecciones. Para esto se presentan algunas nociones y características de la teoría de eliminación.

Teoría de Eliminación

En la teoría de eliminación el objetivo es solucionar un sistema de ecuaciones. Para realizar esto se eliminan variables manipulando las ecuaciones y así encontrar ecuaciones mucho más simples con menos variables.

Definición 5.18. Sea $I = \langle f_1, f_2, \ldots, f_s \rangle$ un ideal de $K[x_1, x_2, \ldots, x_n]$. Se define a I_l como todas las ecuaciones de la forma $f_1 = f_2 = \cdots = f_s = 0$ y donde se eliminan las variables $x_1, \ldots, x_l$, es decir

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

I_l es un ideal de $K[x_{l+1}, \ldots, x_n]$ y se denomina el ideal de eliminación. En efecto, $0 \in I_l$, ya que $0 \in I$ y $0 \in K[x_{l+1}, \ldots, x_n]$, del hecho de que I y $K[x_{l+1}, \ldots, x_n]$ son cerrados bajo la suma, entonces si se suman dos polinomios cualesquiera con variables $x_{l+1}, \ldots, x_n$, el resultado debe ser un polinomio con estas variables. Para $f \in I_l$ y $g \in K[x_{l+1}, \ldots, x_n]$, se tiene que $fg \in I$ y de igual forma $fg \in K[x_{l+1}, \ldots, x_n]$ y así $fg \in I_l$.

Lema 5.1.

$$\prod_{r+k} V(F) = V(I \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]). \tag{5.2.4}$$

Demostración. La prueba se sigue del Teorema 5.2. ■

Es turno de usar la Teoría de las bases de Gröbner como método de decodificar códigos cíclicos. Se escribirá $\mathbb{F}_q[\mathbf{x}, \mathbf{y}, \mathbf{z}]$, donde $\mathbf{x}$ denota las variables $x_1, \ldots, x_r$, $\mathbf{y}$ denota $y_1, \ldots, y_t$ y $\mathbf{z}$ denota las variables $z_1, \ldots, z_t$. Se considerará el orden lexicográfico en $\mathbb{F}_q[\mathbf{x}, \mathbf{y}, \mathbf{z}]$, con $x_1 < \cdots < x_r < z_1 < \cdots < z_t < y_1 < \cdots < y_t$.

Las bases de Gröbner permiten calcular los ideales de eliminación como lo muestra el siguiente teorema.

Teorema 5.9. *Sea* G *una base de Gröbner para el ideal* $I = \langle f_1, f_2, \ldots, f_s \rangle$ *de* $K[x_1, x_2, \ldots, x_n]$ *con respecto al orden de términos definido anteriormente. Entonces*

$$G_k = G \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]$$

es un base de Gröbner del ideal $I \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]$.

Demostración. Se debe probar que para $f \in I \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]$, existe un $g \in G \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]$, tal que $\mathrm{lp}(g)$ divide a $\mathrm{lp}(f)$. Sea $f \in I \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]$, luego como $f \in I$, entonces existe un $g \in G$ tal que $\mathrm{lp}(g)$ divide a $\mathrm{lp}(f)$ y $\mathrm{lp}(f)$ no posee divisores con variables $y_1, y_2, \ldots, y_t$, luego un monomio en las variables $y_1, y_2, \ldots, y_t$ es mayor que uno en $\mathbf{x}, z_1, \ldots, z_k$ por tanto $\mathrm{lp}(g) = \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]$, y así $g \in G \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]$. ■

Note que los ideales de $\langle G_k \rangle$ son ideales de eliminación.
Si se utiliza el Lema 5.2.4 y el Teorema 5.9, se puede reinterpretar el Teorema 5.8 y el Corolario 5.2 de la siguiente forma.

Teorema 5.10. *Dado $\tilde{c}$ y su correspondiente síndrome s, entonces hay τ errores en $\tilde{c}$ si y sólo si para cada $g \in G_k$, se tiene que $g(s, \boldsymbol{0}_k) = 0$, para todo $k \leq t - \tau$ y $g(s, \boldsymbol{0}_{t-r+1}) \neq 0$, para algún $g \in G_{t-r+1}$.*

Corolario 5.3. *Sea $G_{t-r+1} = \{g_1, g_2, \ldots, g_u\}$ y sea $\xi_{t-\tau}$ el vector $(s, \boldsymbol{0}_{t-\tau}, z)$, donde z es una nueva variable. Entonces el ideal $\langle G_{t-\tau+1} \rangle = \langle g_1(\xi_{t-\tau}), g_2(\xi_{t-\tau}), \ldots, g_u(\xi_{t-\tau}) \rangle \in \mathbb{F}_q[z]$ está generado por el polinomio cuyas raíces localizan los errores. Más aún, dicho polinomio está en el conjunto $\{g_1(\xi_{t-\tau}), g_2(\xi_{t-\tau}), \ldots, g_u(\xi_{t-\tau})\}$.*

Demostración. Aplicando el Teorema 5.8, el Corolario 5.2 y el Teorema 5.10 podemos ver que se cumple la primera afirmación. Para completar la prueba es necesario probar que G_{t-r+1} es una base de Gröbner para $\langle G_{t-r+1}(\xi_{t-\tau}) \rangle$, lo cual se cumple con respecto a un orden de términos lexicográfico, en el caso de un ideal cero dimensional, ver [5]. ■

Ejemplo 5.8. Considere el $[15, 5, 7]$-código BCH sobre el campo $\mathbb{F}_2$, con distancia designada $\delta = 6$, ver Ejemplo 5.7. Ya que el número de errores es $t = 3$, entonces se tienen tres variables z y no hay variables y, ya que se trabaja sobre $\mathbb{F}_2$. Con ayuda de GAP se observarán los polinomios que definen la variedad síndrome expresados como en (5.2.1). Para esto primero se definen las variables a utilizar, en este caso

```
>z1:=X(GF(2),"z1");z2:=X(GF(2),"z2");z3:=X(GF(2),"z3");x1:=X(GF(2),"x1");
z1
z2
z3
x1

>x2:=X(GF(2),"x2");x3:=X(GF(2),"x3");
x2
x3
```

Donde $GF(2)$ representa $\mathbb{F}_2$. Luego se define el anillo de polinomios $\mathbb{F}_2[z_1, z_2, z_3, x_1, x_2, x_3]$ por medio del comando

```
>R:=PolynomialRing(GF(2),[z1,z2,z3,x1,x2,x3]);
GF(2)[z1,z2,z3,x1,x2,x3]
```

Por notación se utilizará la variable x_1 para `x1`, x_2 para `x2` y así sucesivamente y se construye el conjunto $F = \{f_1 = z_1+z_2+z_3+x_1, f_2 = z_1^3+z_2^3+z_3^3+x_2, f_3 = z_1^5+z_2^5+z_3^5+x_3, f_4 = z_1^{16}+z_1, f_5 = z_2^{16}-z_2, f_6 = z_3^{16}+z_3\}$. El orden lexicográfico, con $z_3 > z_2 > z_1 > x_3 > x_2 > x_1$, en GAP se obtiene con el comando

```
>lexord:=MonomialLexOrdering([z3,z2,z1,x3,x2,x1]);
MonomialLexOrdering([ z3, z2, z1, x3, x2, x1 ])
```

Luego se calcula la base de Gröbner reducida para F, con respecto al orden `lexord`, con el comando

```
>ReducedGroebnerBasis(F,lexord);
```

Es importante señalar que el cálculo para esta base de Gröbner requiere de algún tiempo, ya que el algoritmo no fue pensado para ser eficiente y si como estrategia para mejorar el aprendizaje del concepto de bases de Gröbner. La base de Gröbner reducida que resulta es

$$
\begin{aligned}
G = \{&x_1^{16}+x_1, x_2^{16}+x_2, x_1^{11}x_2^8+x_1^{14}x_2^2+x_1^6x_2^8x_3\\
&+x_1^5x_2^{10}+x_1^{12}x_2x_3+x_1^9x_2^2x_3+x_1^8x_2^4+x_2^{10}x_3+x_1^5x_2^5\\
&x_1^{15}+x_1^6x_2^8+x_1^{12}x_2+x_1^{10}x_3+x_1^9x_2^2+x_2^{10}+x_1^5x_3^2+x_1^3x_2^4+x_2^5+x_3^3,\\
&z_1^3x_1^3+z_1^2x_1^4+x_1^6+z_1^3x_2+z_1^2x_1x_2+z_1x_1^2x_2+x_1^3x_2+z_1x_3+x_1x_3+x_2^2,\\
&z_1x_1^{13}x_2^8+x_1^{14}x_2^8+z_1x_1^{10}x_2^9+x_1^{11}x_2^9+z_1x_1^{10}x_2^4+x_1^{11}x_2^4\\
&+z_1x_1^3x_2^8x_3^2+x_1^4x_2^8x_3^2+z_1x_1^9x_2x_3^2+x_1^{10}x_2x_3^2+z_1x_2^9x_3^2\\
&+x_1x_2^9x_3^2+z_1^3x_1^5+z_1^2x_1^6+z_1x_1^7+z_1x_2^4x_3^2+x_1x_2^4x_3^2+z_1x_1^4x_2\\
&+z_1^3x_3+z_1^2x_1x_3+z_1x_1^2x_3+x_2x_3, z_1^{16}+z_1, z_1^2x_1^3+z_1z_2x_1^3+z_1x_1^4+z_2^2x_1^3\\
&+z_2x_1^4+z_1^2x_2+z_1z_2x_2+z_1x_1x_2+z_2^2x_2+z_2x_1x_2+x_1^2x_2+x_3, x_1^{13}x_2^8+x_1^{10}x_2^9+x_1^{10}x_2^4\\
&+x_1^3x_2^8x_3^2+x_1^9x_2x_3^2+x_2^9x_3^2+z_1^2x_1^5+z_1z_2x_1^5+z_1x_1^6+z_2^2x_1^5\\
&+z_2x_1^6+x_1^7+x_2^4x_3^2+x_1^4x_2+z_1^2x_3+z_1z_2x_3+z_1x_1x_3+z_2^2x_3+z_2x_1x_3+x_1^2x_3,\\
&z_1^2z_2+z_1^2x_1+z_1z_2^2+z_1x_1^2+z_2^2x_1+z_2x_1^2+x_1^3+x_2, z_2^{16}+z_2, z_1+z_2+z_3+x_1\}.
\end{aligned}
$$

Ahora el objetivo es obtener una base de Gröbner eliminando primero las variables z_2 y z_3 y formar G_1, eliminar la variable z_3 y obtener un conjunto G_2 y finalmente calcular la base con todas las variables. En efecto para las indeterminadas z_1, x_1, x_2, x_3, se construye el anillo de polinomios sobre $\mathbb{F}_2$ en GAP de la siguiente manera

```
>R1:=PolynomialRing(GF(2),[z1,x1,x2,x3]);
GF(2)[z1,x1,x2,x3]
```

Luego se escoge de toda la base G los polinomios con z_1, x_1, x_2, x_3 que pertenezcan a $R1$, utilizando el comando

```
>G1:=Filtered(G, x -> (x in R1)=true);
```

Obteniendo el nuevo conjunto

$$\begin{aligned}G_1 = \{&x_1^{16} + x_1, x_2^{16} + x_2,\\ &x_1^{11}x_2^8 + x_1^{14}x_2^2 + x_1^6x_2^8x_3 + x_1^5x_2^{10} + x_1^{12}x_2x_3 + x_1^9x_2^2x_3\\ &+ x_1^8x_2^4 + x_2^{10}x_3 + x_1^5x_2^5 + x_1^3x_2^4x_3 + x_2^5x_3 + x_1^5 + x_1^2x_2 + x_3,\\ &x_1^{15} + x_1^6x_2^8 + x_1^{12}x_2 + x_1^{10}x_3 + x_1^9x_2^2 + x_2^{10} + x_1^5x_3^2 + x_1^3x_2^4 + x_2^5 + x_3^3,\\ &z_1^3x_1^3 + z_1^2x_1^4 + x_1^6 + z_1^3x_2 + z_1^2x_1x_2 + z_1x_1^2x_2 + x_1^3x_2 + z_1x_3 + x_1x_3 + x_2^2,\\ &z_1x_1^{13}x_2^8 + x_1^{14}x_2^8 + z_1x_1^{10}x_2^9 + x_1^{11}x_2^9 + z_1x_1^{10}x_2^4 + x_1^{11}x_2^4\\ &+ z_1x_1^3x_2^8x_3^2 + x_1^4x_2^8x_3^2 + z_1x_1^9x_2x_3^2 + x_1^{10}x_2x_3^2 + z_1x_2^9x_3^2\\ &+ x_1x_2^9x_3^2 + z_1^3x_1^5 + z_1^2x_1^6 + z_1x_1^7 + z_1x_2^4x_3^2 + x_1x_2^4x_3^2 + z_1x_1^4x_2\\ &+ z_1^3x_3 + z_1^2x_1x_3 + z_1x_1^2x_3 + x_2x_3, z_1^{16} + z_1\}.\end{aligned}$$

Para formar G_2, se utilizan las variables z_2, z_1, x_1, x_2, x_3, eliminando z_3, para esto se forma el anillo sobre $\mathbb{F}_2$ de la siguiente manera

```
>R2:=PolynomialRing(GF(2),[z2,z1,x1,x2,x3]);
GF(2)[z2,z1,x1,x2,x3]
```

Se seleccionan solo los polinomios que tengan las indeterminadas z_2, z_1, x_1, x_2, x_3 que pertenezcan a $R2$, con la función

```
>G22:=Filtered(G, x -> (x in R2)=true);
```

A este conjunto se le añade otra selección para obtener solo los polinomios que no se repiten en G_1 con ayuda de la instrucción

```
>G2:=Filtered(G22, x -> (x in G1)=false);
```

Se obtiene,

$$\begin{aligned}G2 = G_1 \cup \{&z_1^2x_1^3 + z_1z_2x_1^3 + z_1x_1^4 + z_2^2x_1^3 + z2x_1^4 + z_1^2x_2 + z_1z_2x_2 + z_1x_1x_2 + z_2^2x_2 + z_2x_1x_2 + x_1^2x_2\\ &+ x_3, x_1^{13}x_2^8 + x_1^{10}x_2^9 + x_1^{10}x_2^4 + x_1^3x_2^8x_3^2 + x_1^9x_2x_3^2 + x_2^9x_3^2 + z_1^2x_1^5 + z_1z_2x_1^5 + z_1x_1^6 + z_2^2x_1^5\\ &+ z_2x_1^6 + x_1^7 + x_2^4x_3^2 + x_1^4x_2 + z_1^2x_3 + z_1z_2x_3 + z_1x_1x_3 + z_2^2x_3 + z_2x_1x_3 + x_1^2x_3,\\ &z_1^2z_2 + z_1^2x_1 + z_1z_2^2 + z_1x_1^2 + z_2^2x_1 + z_2x_1^2 + x_1^3 + x_2, z_2^{16} + z_2\}.\end{aligned}$$

Finalmente se calcula el conjunto G_3 en el cual intervienen las variables $z_3, z_2, z_1, x_1, x_2, x_3$, así se utiliza el anillo

```
>R3:=PolynomialRing(GF(2),[z3,z2,z1,x1,x2,x3]);
GF(2)[z3,z2,z1,x1,x2,x3]
```

sobre $\mathbb{F}_2$ y utilizando el comando

```
>G33:=Filtered(G, x -> (x in R3)=true);
```

Se escogen los polinomios con estas indeterminadas de G. Nuevamente se añade otra selección para obtener solo los polinomios que no están en G_2 utilizando el comando

```
>G3:=Filtered(G33, x -> (x in G2)=false);
```

Es decir,

$$G3 = G_2 \cup \{z1 + z2 + z3 + x1\}.$$

Sea $a = \alpha$ el elemento primitivo de $\mathbb{F}_{2^4}$, utilizando

```
f:= GF(16);
a:=PrimitiveRoot(f);
```

Se define el campo y la raíz primitiva α, luego se tiene que $\alpha^4 + \alpha + 1 = 0$. Ahora supóngase que la palabra enviada es la palabra $\mathbf{0}$ y se recibe un mensaje con un error en la segunda posición. Luego $s_1 = \alpha$, $s_2 = \alpha^3$ y $s_3 = \alpha^5$. Ya que $\xi_{t-\tau} = (s, \mathbf{0}_{t-\tau}, z)$, entonces $\xi_0 = (s, z)$, es decir $\xi_0 = (\alpha, \alpha^3, \alpha^5, z)$, si se evalúa ξ_0 en $G_1(\xi_0)$ sobre $\mathbb{F}_q[\mathbf{x}, \mathbf{z}]$, utilizando una lista vacía en GAP `S1:=[];` y se calcula el número de polinomios del conjunto G_1 con el comando `Size(G1);` se obtiene un total de siete polinomios. Por notación se define una nueva variable z con el comando

```
>z:=X(GF(2),"z");
```

La evaluación deseada $G_1(\xi_0)$ se da como

```
>for i in [1..7] do
Add(S1,Value(G1[i],[x1,x2,x3,z1],[a,a^3,a^5,z]));
od;
```

El cual adiciona a la lista vacía $S1$ los polinomios de G_1 en las indeterminadas x_1, x_2, x_3, z_1 evaluadas en $\alpha, \alpha^3, \alpha^5, z$, lo que resulta

$$G_1(\xi_0) = S1 = \{0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, z^{16} + z\}$$

$$= \{z^{16} + z\}.$$

De igual forma ocurre para las evaluaciones $G_2(\xi_1)$ y $G_3(\xi_2)$, es decir

$$G_2(\xi_1) = \{0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, \alpha z^2 + \alpha^2 z, z^{16} + z\}$$

$$= \{\alpha z^2 + \alpha^2 z, z^{16} + z\},$$
$$G_3(\xi_2) = \{0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, z + \alpha\}$$
$$= \{z + \alpha\}.$$

Las variedades a $G_1(\xi_0)$ y $G_2(\xi_1)$ contiene a $\mathbf{0}$, confirmando el Teorema 5.10 que hay un error y por el Corolario 5.3 se tiene que $\langle G_3(\xi_2)\rangle$ contiene el polinomio localizador cuya raíz localiza el error $z + \alpha$. Además $G_2(\xi_1)$ está generado por $z(z + \alpha)$.

Ahora supóngase que el mensaje recibido tiene dos errores, en la segunda y cuarta posición. luego $s_1 = \alpha + \alpha^3 = \alpha^9$, $s_2 = \alpha$ y $s_3 = \alpha^2 + \alpha + 1 = \alpha^{10}$, aplicando el método anterior para este nuevo síndrome se forma una lista vacía `S12:=[];` luego

```
>for i in [1..7] do
Add(S12,Value(G1[i],[x1,x2,x3,z1],[a+a^3,a,a^10,z]));
od;
```

Donde se adiciona a la lista $S12$ los polinomios de G_1 en las indeterminadas x_1, x_2, x_3, z_1 evaluadas en $\alpha^9, \alpha, \alpha^{10}$, y se calcula $G_1(\xi_0)$ es decir

$$\begin{aligned} G_1(\xi_0) = S12 = \{&0\alpha, 0\alpha, 0\alpha, \alpha^{13}z^3 + \alpha^7 z^2 + \alpha^2 z,\\ &\alpha^5 z^3 + \alpha^{14} z^2 + \alpha^9 z, z^{16} + z\}\\ &= \{\alpha^{13}z^3 + \alpha^7 z^2 + \alpha^2 z, \alpha^5 z^3 + \alpha^{14} z^2 + \alpha^9 z, z^{16} + z\}. \end{aligned}$$

De forma similar se calcula $G_2(\xi_1)$, lo que resulta

$$\begin{aligned} G_2(\xi_1) = S22 = \{&0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha, 0\alpha,\\ &\alpha^{13}z^2 + \alpha^7 z + \alpha^2, \alpha^5 z^2 + \alpha^{14} z + \alpha^9,\\ &\alpha^9 z^2 + \alpha^3 z + \alpha^{13}, z^{16} + z\}\\ &= \{\alpha^{13}z^2 + \alpha^7 z + \alpha^2, \alpha^5 z^2 + \alpha^{14} z + \alpha^9,\\ &\alpha^9 z^2 + \alpha^3 z + \alpha^{13}, z^{16} + z\}. \end{aligned}$$

La variedad que contiene a $G_1(\xi_0)$ contiene a $\mathbf{0}$, lo cual confirma el Teorema 5.10 que hay dos errores y $\langle G_2(\xi_1)\rangle$ contiene el polinomio localizador, por el Corolario 5.3 los polinomios en $G_2(\xi_1)$ diferentes de $z^{16} + z$ se pueden factorizar de la siguiente manera

$$\alpha^{13}z^2 + \alpha^7 z + \alpha^2 = \alpha^{13}(z + \alpha)(z + \alpha^3),$$
$$\alpha^5 z^2 + \alpha^{14} z + \alpha^9 = \alpha^5(z + \alpha)(z + \alpha^3),$$
$$\alpha^9 z^2 + \alpha^3 z + \alpha^{13} = \alpha^9(z + \alpha)(z + \alpha^3).$$

De esta forma, los localizadores del error son α y α^3.

Finalmente supóngase que el mensaje recibido tiene 3 errores, en la segunda, cuarta y séptima posición. luego $s_1 = \alpha + \alpha^2$, $s_2 = \alpha + \alpha^3$ y $s_3 = \alpha^5$. Ahora se forma una lista vacía `S13:=[];` es decir

```
>for i in [1..7] do
Add(S13,Value(G1[i],[x1,x2,x3,z1],[a+a^2,a+a^3,a^5,z]));
od;
```

Donde se adiciona a la lista $S13$ los polinomios de G_1 en las indeterminadas x_1, x_2, x_3, z_1 evaluadas en $\alpha + \alpha^2, \alpha + \alpha^3, \alpha^5$ y se calcula $G_1(\xi_0)$ es decir

$$\begin{aligned} G_1(\xi_0) = S13 = \{&0\alpha, 0\alpha, 0\alpha, 0\alpha, \alpha^7 z^3 + \alpha^{12} z^2 + \alpha^8 z + \alpha^2, \\ &z^3 + \alpha^5 z^2 + \alpha z + \alpha^{10}, z^{16} + z\}. \\ &= \{\alpha^7 z^3 + \alpha^{12} z^2 + \alpha^8 z + \alpha^2, z^3 + \alpha^5 z^2 + \alpha z + \alpha^{10}, z^{16} + z\}. \end{aligned}$$

La variedad $V(G_1(\xi_0))$ no contiene a $\mathbf{0}$. El Teorema 5.10 confirma que hay 3 errores y $G_1(\xi_0)$ contiene el polinomio localizador, por el Corolario 5.3 los polinomios en $G_1(\xi_0)$ diferentes de $z^{16} + z$ se pueden factorizar de la siguiente manera

$$\alpha^7 z^3 + \alpha^{12} z^2 + \alpha^8 z + \alpha^2 = \alpha^7 (z^3 + \alpha^5 z^2 + \alpha z + \alpha^{10}) = \alpha^7 (z + \alpha)(z + \alpha^3)(z + \alpha^6).$$

Luego los localizadores del error son α, α^3 y α^6.

Conclusiones

- Se presenta una recopilación detallada de la teoría de las bases de Gröbner, la cual se espera que facilite su comprensión y su entendimiento para futuros estudios.
- Se exponen las soluciones a los cuatro problemas fundamentales presentados en los Problemas 1.1 en el anillo de polinomios en una indeterminada. En el caso multivariado con ecuaciones lineales y no lineales se generalizan los resultados a través del concepto de base de Gröbner con la aplicación del algoritmo de la división multivariado y el algoritmo de Buchberger.
- Para códigos cíclicos se presenta un método de decodificación usando la variedad síndrome de un código, la teoría de eliminación y el cálculo de una base de Gröbner para encontrar las posiciones de error.
- Se implementan los algoritmos que aparecen en el estudio de las bases de Gröbner en el sistema de álgebra computacional discreta GAP, los cuales facilitan los cálculos y el desarrollo de la teoría. Cabe resaltar que en este trabajo estos algoritmos se implementan con el animo de que sirvan como una herramienta educacional y que no se pretende con ellos construir algoritmos eficientes, una vez que el estudio de eficiencia de este tipo de algoritmos, como por ejemplo el algoritmo de Buchberger, merecen una dedicación especial.

Apéndice

GAP (Grupos, Algoritmos y Programación) es un sistema de álgebra computacional discreta, con énfasis particular en la Teoría Computacional de Grupos. Fue desarrollado originalmente en el Departamento de Matemática (Lehrstuhl D für Mathematik) de la Universidad Técnica de Aachen, Alemania, entre 1986 y 1997 bajo la dirección del profesor Joachim Neubüser. GAP es gratuito y de código abierto, además de ser un entorno de cálculo algebraico discreto, posee un núcleo implementado en C y dispone aparte de librerías escritas en su propio lenguaje de programación. Se puede encontrar abundante información, manuales, paquetes, foros, y muchos ejemplos en www.gap-system.org.
GAP tiene implementados varios comandos que se utilizaron en el desarrollo de este trabajo. A continuación se presentan algunas de estos comandos, para mayor información se puede leer el manual de GAP [4].

- `> [a..z];`

  Crea una lista de z elementos.

- `> Add(list,i);`

  Adiciona a la lista *list* el elemento i.

- `> Add(list,obj[pos]);`

  Agrega el elemento *obj* a la lista *list* a la posición *pos*.

- `> Length(list);`

  Devuelve la longitud de la lista *list*.

- `> Size(C);`

  Devuelve el tamaño de una colección C.

- `> Lista[i];`

  Presenta el i-ésimo elemento de una lista.

- `> Maximum(list);`

  Devuelve el elemento máximo de la lista *list*.

- `> Minimum(list);`

  Devuelve el elemento mínimo de la lista *list*.

- `> Filtered(list,func);`

  Imprime una lista que contiene los elementos de la lista, para los que la función devuelve verdadero.

- `> Listx(arg1,arg2,...,argn,func);`

  Devuelve una nueva lista construida a partir de los argumentos $arg1, arg2, \ldots, argn$ los cuales pueden ser una lista o colección, una función que devuelve una lista o colección o una función que devuelve verdadero o falso. El ultimo argumento $func$ debe ser una función, que se aplica a los valores de las variables de bucle y se recogen los resultados.

- `> Remove( list[, pos] );`

  Elimina el elemento de la lista *list* ubicado en la posición *pos*.

- `> Value(list,[x],[p]);`

  Evalúa los polinomios de la lista *list* en la variable x, para el valor p.

- `>X(R,"x")` o `> Indeterminate(R,i);` Define la indeterminada x en el anillo R, o define la indeterminada x_i en el anillo R.

- `> PolynomialRing(R,[x]);`

  Se utiliza para definir el anillo de polinomios en la variable x con coeficientes en R.

- `> Zero(R);`

  Imprime El valor nulo del anillo R.

- `> MonomialLexOrdering ([ variable ]);`

  Presenta el orden lexicográfico variables $a > b > \cdots > z$.

- `> MonomialGrlexOrdering([ variable ]);`

  Presenta el orden lexicográfico gradual para determinadas variables.

- `> MonomialGrevlexOrdering ([ variable ]);`

  Ordena las variables mediante el orden lexicográfico gradual inverso.

- `> LeadingTermOfPolynomial(f,ord);`

  Retorna el término líder del polinomio f con respecto al orden de términos ord.

- `> LeadingMonomialOfPolynomial(f,ord);`

  Imprime el producto de potencias líder(lp) de un polinomio f con respecto al orden ord.

- `> LeadingCoefficientOfPolynomial(f,ord);`

  Presenta el coeficiente líder del polinomio f con respecto al ordenamiento ord.

- `> LeadingCoefficient(pol);`

  Devuelve el coeficiente principal del polinomio *pol* en una variable.

- `> IndeterminatesOfPolynomialRing(R);`

  Imprime la variables indeterminadas del anillo R.

- `> DegreeIndeterminate(f,i);`

  Devuelve el grado de la interinidad i del polinomio f.

- `> One(R);`

  Devuelve el valor neutro del anillo R.

- `> QuotientRemainder(f,g);`

  Permite conocer el cociente y residuo de los polinomios f y g en una variable.

- `>GaloisField( p^d )` o `> GF( p^d );` Devuelve el campo de Galois, tomando como argumento los enteros p y d, con p^d.

- `> PrimitiveRoot(R);`

  Imprime la raíz primitiva de un campo finito R.

- `> Ideal (R, [L]);`

  Esta función permite imprimí el ideal generado por la lista de polinomios L sobre el anillo R.

- `> GroebnerBasis (I, ord);;`

  Calcula la base de Gröbner para el ideal I con respecto a el ordenamiento ord.

- `> ReducedGroebnerBasis ( L , ord ) ;`

  Permite calcular la base de gröbner reducida para la lista L con la ordenación ord.

- `> MinimalPolynomial(F,a);`

  Esta función calcula el polinomio irreducible para `a` en el cuerpo `F`.

Referencias

[1] William W. Adams and Philippe Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994. MR 1287608 (95g:13025)

[2] Bruno Buchberger, *Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, Journal of Symbolic Computation **41** (2006), no. 3-4, 475 – 511, Logic, Mathematics and Computer Science: Interactions in honor of Bruno Buchberger (60th birthday).

[3] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, third ed., Undergraduate Texts in Mathematics, Springer, New York, 2007, An introduction to computational algebraic geometry and commutative algebra. MR 2290010 (2007h:13036)

[4] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.6*, 2014.

[5] Patrizia Gianni, *Properties of Gröbner bases under specializations*, Eurocal '87 (JamesH. Davenport, ed.), Lecture Notes in Computer Science, vol. 378, Springer Berlin Heidelberg, 1989, pp. 293–297 (English).

[6] Lev Glebsky and Carlos Jacobo Rubio-Barros, *Una prueba sencilla del teorema de los ceros de Hilbert usando bases de Gröbner*, Lect. Mat. **34** (2013), no. 1, 77–82.

[7] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge Univ. Press, 2003.

[8] John Lopez Santander and Hamilton Ruiz, *La matemática de la teoría de códigos*, Trabajo de grado, Universidad de Nariño, Noviembre 2013.

[9] Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, and Carlo Traverso (eds.), *Gröbner bases, coding, and cryptography*, Springer-Verlag, Berlin, 2009. MR 2590633 (2010i:94007)