UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD DE CIENCIAS QUÍMICAS, FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE MATEMÁTICA

TESIS

LEMA DE DICKSON Y BASES DE GRÖBNER EN IDEALES DE POLINOMIOS

PRESENTADO POR:

Br. WERNER RENAN SALAZAR CALLA

PARA OPTAR AL TÍTULO PROFESIONAL DE LICENCIADO EN MATEMÁTICA

ASESOR: Mg. JOSÉ MOZO AYMA

CO-ASESOR: Dr. EDISON MARCAVILLACA NIÑO DE GUZMÁN

CUSCO - PERÚ

2024

INFORME DE ORIGINALIDAD

(Aprobado por Resolución Nro.CU-303-2020-UNSAAC)

El que suscribe, **Asesor** del trabajo de investigación/tesis titulada: Lema de DICKSON y bases de Gröbner en ideales de polinomios

presentado por: Werner Renan Salazar Calla con DNI Nro.: 72688752 presentado por: ..... con DNI Nro.: ..... para optar el título profesional/grado académico de Licenciado en Matemática

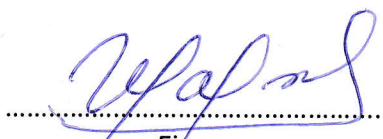
Informo que el trabajo de investigación ha sido sometido a revisión por 1 veces, mediante el Software Antiplagio, conforme al Art. 6° del ***Reglamento para Uso de Sistema Antiplagio de la UNSAAC*** y de la evaluación de originalidad se tiene un porcentaje de 5 **%.**

Evaluación y acciones del reporte de coincidencia para trabajos de investigación conducentes a grado académico o título profesional, tesis

Porcentaje	Evaluación y Acciones	Marque con una (X)
Del 1 al 10%	No se considera plagio.	X
Del 11 al 30 %	Devolver al usuario para las correcciones.	
Mayor a 31%	El responsable de la revisión del documento emite un informe al inmediato jerárquico, quien a su vez eleva el informe a la autoridad académica para que tome las acciones correspondientes. Sin perjuicio de las sanciones administrativas que correspondan de acuerdo a Ley.	

Por tanto, en mi condición de asesor, firmo el presente informe en señal de conformidad y **adjunto** la primera página del reporte del Sistema Antiplagio.

Cusco, 8 de Agosto de 20.24



Firma

Post firma JOSE MOZO AYZA

Nro. de DNI 23884861

ORCID del Asesor 0000-0003-1769-2210

Se adjunta:

1. Reporte generado por el Sistema Antiplagio.
2. Enlace del Reporte Generado por el Sistema Antiplagio: **oid:** 27259:372032180

NOMBRE DEL TRABAJO

Lema de Dickson y bases de Grobner en i deales de polinomios

AUTOR

Werner Renan Salazar Calla

RECUENTO DE PALABRAS

16328 Words

RECUENTO DE CARACTERES

69014 Characters

RECUENTO DE PÁGINAS

63 Pages

TAMAÑO DEL ARCHIVO

555.2KB

FECHA DE ENTREGA

Aug 8, 2024 2:18 PM GMT-5

FECHA DEL INFORME

Aug 8, 2024 2:19 PM GMT-5

5% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 4% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 3% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)
- Bloques de texto excluidos manualmente

Presentación

SEÑOR DECANO DE LA FACULTAD DE CIENCIAS QUÍMICAS, FÍSICAS Y MATEMÁTICAS.

SEÑOR DIRECTOR DE LA ESCUELA PROFESIONAL DE MATEMÁTICA.

SEÑORES DOCENTES MIEMBROS DEL JURADO.

En cumplimiento con las normas y reglamento de grados y títulos establecidos por la Escuela Profesional de Matemática, presento a vuestra consideración el presente trabajo de tesis intitulado: “LEMA DE DICKSON Y BASES DE GRÖBNER EN IDEALES DE POLINOMIOS” con el fin de Optar al Título Profesional de Licenciado en Matemática. Finalmente, espero que el trabajo de investigación explique de manera clara los conceptos y que sirva como antecedente para próximos trabajos de investigación.

Atte. WERNER RENAN SALAZAR CALLA

Dedicatoria

Este es un trabajo de varios meses de esfuerzo y dedicación con el cual pretendo dar fin a cinco años de aprendizaje en mi querida universidad. El presente va dedicado a Renan y Patricia, mis queridos padres, quienes me acompañan en mi camino desde siempre, confían en mí y me dan su apoyo incondicional en todo momento. Ellos son todo para mí.

Gracias infinitas a los dos.

Agradecimientos

Finalizo una de la mejores etapas de mi vida y quiero agradecer a todas las personas que me apoyaron a lo largo de todo este tiempo.

Al profesor José Mozo Ayma y al profesor Edison Marcavillaca Niño de Guzmán, quienes me ayudaron en la realización de este trabajo y de quienes aprendí demasiado, mi más alta estima y reconocimiento para los dos. También extender mi gratitud a los profesores Alejandro Ttito Ttica, Gino Maqui Huaman, Patricio Choque Huaman, Pedro Quispe Sandoval, Felipe Chaparro Lazo, Paulina Taco Llave, Eleuteria Ttito Ttica y todos aquellos que compartieron su conocimiento conmigo en las distintas materias que me enseñaron.

También agradecer a mis compañeros de código Rudy, Naydu, Orlando, Nadia, Kelvin, Malú, Renzo, Kelly, Antony, Jesus, Steven y demás por hacer de este tiempo más maravilloso.

A cada uno de ustedes mi más profunda gratitud. Siempre agradecido con Dios por poner a personas tan maravillosas en mi camino.

Índice

Resumen

El conjunto de polinomios en las n variables $x_1, x_2, \cdots, x_n$ que pertenecen a un cuerpo $\mathbb{K}$ dado y con coeficientes en el mismo cuerpo tiene estructura de anillo y, como en todo anillo, se pueden encontrar subconjuntos I llamados ideales. Los términos de un polinomio pueden ordenarse de manera creciente o decreciente, para esto es necesario introducir una noción de orden dentro del conjunto de monomios en las n variables, al cual se nombrará orden monomial; y con este orden se puede encontrar el elemento "más pequeño" de un conjunto de monomios, el cual se conoce como monomio minimal. Por el lema de Dickson es posible mostrar que todo ideal monomial del anillo de polinomios es finitamente generado. Con estos conceptos asimilados se da a conocer lo que es una base de Gröbner de un ideal I del anillo de polinomios respecto a algún orden monomial dado. El trabajo concluye en que existen bases de Gröbner para todo ideal I de S_n gracias al lema de Dickson. Además, se prueba la existencia de bases de Gröbner mínimas, y la existencia y unicidad de bases de Gröbner reducidas; que siguen siendo bases de Gröbner, solo que con algunas particularidades.

Palabras clave: Ideales, monomios minimales, lema de Dickson, órdenes monomiales, bases de Gröbner.

Abstract

The set of polynomials in the n variables $x_1, x_2, \cdots, x_n$ that belong to a given field $\mathbb{K}$ and with coefficients in the same field has a ring structure and, as in every ring, it is possible find subsets I called ideals. The terms of a polynomial can be ordered in an increasing or decreasing manner. For this it is necessary to introduce a notion of order inside the set of monomials in the n variables, which will be called monomial order; and with this order it is possible find the "smallest" element of a set of monomials, which is known as a minimal monomial. Thanks to Dickson's lemma it is possible to show that every monomial ideal of the ring of polynomials is finitely generated. With these concepts assimilated, what is a Gröbner basis of an ideal I of the ring of polynomials with respect to some given monomial order is revealed. The work concludes showing that in every ideal I of S_n there are Gröbner bases. Furthermore, the existence of minimal Gröbner bases, and the existence and uniqueness of reduced Gröbner bases, are proven; which are still Gröbner bases, with some particularities.

Keywords: Ideals, minimal monomials, Dickson's lemma, monomial order, Gröbner Bases.

Introducción

Del mismo modo que un subconjunto no vacío $\mathfrak{B}$ de un $\mathbb{K}$-espacio vectorial V se dice base cuando $\mathfrak{B}$ genera V y además sus elementos son linealmente independientes, una base de Gröbner de un ideal de polinomios I es un subconjunto finito no vacío de I que genera I y que además posee cierta característica que se mostrará posteriormente.

Ya conocida la definición de base de Gröbner de un ideal I y sabiendo que dicha base está determinada por el ideal líder de I es natural preguntarse: ¿todo ideal I del anillo de polinomios posee una base de Gröbner? El objetivo principal de este trabajo es responder a esta interrogante usando el lema de Dickson, ya que este implica que el ideal líder de I es finitamente generado. Para esto, previamente, se introducen los conceptos de monomio minimal y orden monomial, ya que sin estos es imposible definir lo que es una base de Gröbner. Por consiguiente, antes de cumplir con el objetivo principal de la investigación se tiene que garantizar que siempre es posible encontrar monomios minimales en un conjunto de monomios del anillo de polinomios y también hallar órdenes monomiales en dicho anillo, estos son los objetivos específicos de la investigación.

El presente trabajo inicia con el Capítulo I, en este se da a conocer el planteamiento del problema; es decir, la situación problemática, los problemas y objetivos de la investigación, antecedentes, y demás. Seguidamente, en el Capítulo II se encuentra el marco teórico; es aquí donde se presentan las definiciones, notaciones y proposiciones más básicas para comprender este trabajo, tales como la de anillo, ideal, relación de orden, etc. Posteriormente, el Capítulo III se dedica exclusivamente a lograr los objetivos de la investigación, dando las definiciones necesarias y demostrando los resultados más importantes, tales como el “Lema de Dickson”, “Ideal finitamente generado”, “Orden monomial”, y otros. Finalmente, se dan a conocer las conclusiones de la investigación.

Capítulo I

PLANTEAMIENTO DEL PROBLEMA

1.1. Situación problemática

El conjunto de polinomios en n variables con coeficientes en un determinado cuerpo $\mathbb{K}$ junto con las operaciones usuales de la adición y la multiplicación de polinomios tiene estructura de anillo y se le conoce como anillo polinomial en n variables sobre el cuerpo $\mathbb{K}$. En este anillo, como en cualquier otro, es posible encontrar sub estructuras algebraicas llamados ideales. Sea I un ideal no vacío del anillo polinomial en n variables, una base de Gröbner de I respecto a un orden monomial es un subconjunto finito no vacío de I que verifica ciertas propiedades. El lema de Dickson lleva implícito que todo ideal monomial del anillo de polinomios es finitamente generado, ¿existirá alguna relación entre dicho lema y la existencia de las bases de Gröbner? Considerando dicha pregunta como principal problemática se procederá a realizar la investigación.

1.2. Formulación del problema

1.2.1. Problema general

¿Es posible demostrar la existencia de bases de Gröbner en ideales de polinomios mediante el lema de Dickson?

1.2.2. Problemas específicos

- ¿Existen monomios minimales en subconjuntos de monomios de n variables?
- ¿Existen ordenes monomiales en el anillo polinomial de n variables?

1.3. Justificación de la investigación

Existen algunas aplicaciones de las bases de Gröbner tales como la solución de sudoku (Marcavillaca, 2019) u la optimización restringida a un sistema polinomial (Bances *e*t al., 2014). Antes de comprender o elaborar nuevas aplicaciones de las bases de Gröbner es necesario estudiar qué es una Base

de Gröbner, bajo qué condiciones existen y qué propiedades verifican, es por esto que se desarrolla el presente trabajo. Este es un comienzo a futuras investigaciones más complejas y elaboradas en el campo del álgebra conmutativa y, en específico, las aplicaciones de las bases de Gröbner.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Demostrar que existen bases de Gröbner en ideales de polinomios mediante el lema del Dickson

1.4.2. Objetivos específicos

- Demostrar la existencia de monomios minimales en subconjuntos de monomios de n variables
- Demostrar la existencia de órdenes monomiales en el anillo polinomial de n variables

1.5. Antecedentes empíricos de la investigación

1.5.1. Antecedentes internacionales

Chambi J. (2010), de la Universidad Mayor de San Andrés, presenta el trabajo *Teorema de las bases de Grobner* con el objetivo principal de desarrollar los teoremas de Orden Monomiales para polinomios de n-variables, el Teorema de las Bases de Gröbner y ver la optimización de Bruno Buchberger sobre tal teorema de Gröbner.

García J. (2020), de la Universidad Politécnica de Madrid, realiza el trabajo *Bases de Gröbner y Aplicaciones* con el objetivo de estudiar las Bases de Gröbner, para ello realiza una aproximación matemática desde los conceptos más fundamentales hasta conocer algunas de sus aplicaciones.

Sola V. (2019), de la Universidad de El Salvador presenta el trabajo *INTRODUCCIÓN A BASES ESTÁNDAR Y ALGUNAS APLICACIONES*. Su objetivo principal es exponer detalladamente un estudio introductorio a las bases estándar (de Gröbner) de ideales, demostrando las principales propiedades y algoritmos que permiten estudiar la teoría de ideales desde una perspectiva computacional; y cuyos objetivos específicos son Generalizar el algoritmo de la división de polinomios, en el anillo de polinomios en n indeterminadas, permitiendo introducir las bases de Gröbner y sus propiedades, hacer un estudio de conceptos fundamentales de los anillos de polinomios asociados a un orden monomial cualquiera

y la construcción de formas normales para el cálculo de bases estándar, y desarrollar ejemplos que exhiban la aplicación de las bases estándar.

Diniz P. (2020) de la Universidade Federal de Uberlândia realiza el trabajo *Introdução as Bases de Gröbner* con el objetivo de estudiar las Bases de Gröbner y sus propiedades.

Alcántara D. (2023) de la Universidad de Cantabria presenta el trabajo *BASES DE GRÖBNER* con el objetivo de formular bases de Gröbner de ideales del anillo de polinomios, mostrar el cálculo de estas y algunas aplicaciones.

1.5.2. Antecedentes nacionales

Marca G. (2008), de la Universidad Nacional de Ingeniería, realiza la investigación *Bases de Gröbner con aplicaciones al álgebra conmutativa*. El objetivo de su investigación es discutir algunas principales ideas que envuelven métodos computacionales algebraicos cuya importancia está en la posibilidad de atacar temas clásicos del álgebra conmutativa y geometría algebraica de una manera algorítmica, simplificando cálculos de manera efectiva.

Kong M., Bances R., Medina N., González M., Luna M., y Sánchez R. (2014) de la Pontificia Universidad Católica del Perú, presentan el trabajo de *ALGUNAS APLICACIONES DE LAS BASES DE GRÖBNER*, con el fin de presentar una introducción a las Bases de Gröbner y desarrollar algunas de sus aplicaciones.

Flores L. (2021) de la Universidad Nacional del Altiplano, presenta el trabajo de *BASES DE GRÖBNER Y SU APLICACIÓN EN LA SOLUCIÓN DE SISTEMAS POLINOMIALES*, con el fin de determinar Bases de Gröbner y aplicar a la solución de un sistema de ecuación polinomial

Marcavillaca E. (2019) de la Universidad Nacional de San Antonio Abad del Cusco, presenta el trabajo de *Solución del Sudoku: Utilizando Bases de Gröbner*, con el fin de resolver el Sudoku usando la teoría de las Bases de Gröbner, para esto modela el Sudoku mediante un sistema de ecuaciones polinomiales, luego asocia al Sudoku un ideal en el anillo de polinomios de varias variables. Este ideal será el ideal generado por los polinomios que describen el sistema de ecuaciones, calcula la Base de Gröbner reducida para este ideal. Los generadores de la Base de Gröbner reducida forman un sistema de ecuaciones que es equivalente al sistema original, resolviendo el nuevo sistema se obtiene la solución al Sudoku.

Gimenez P. (2013) de la Pontificia Universidad Católica del Perú, presenta sus notas tituladas *Una introducción a las bases de Gröbner y algunas de sus aplicaciones*, con las cuales pretende ofrecer una introducción elemental a la teoría de bases de Grobner y presentar algunas de sus aplicaciones.

1.6. Metodología de la investigación

1.6.1. Ámbito de estudio

El presente trabajo de investigación se realiza en la Escuela Profesional de Matemática de la Universidad Nacional de San Antonio Abad del Cusco desde mayo de 2022 a febrero de 2023.

1.6.2. Nivel de investigación

Según Hernández et al. (2018), los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes. Es por esto que se considera esta investigación de nivel exploratorio, pues se pretender examinar un tema poco estudiado o novedoso.

1.6.3. Diseño de investigación

El diseño de este trabajo es no experimental porque pertenece al conjunto de estudios que se realizan sin la manipulación deliberada de variables y en los que sólo se observan los fenómenos en su ambiente natural para analizarlos (Hernández *e*t al., 2018).

Capítulo II

MARCO TEÓRICO

2.1. Estructuras algebraicas

Definición 2.1.1. Dado un conjunto no vacío R. Se dice que R es un *anillo*, si en R están definidas las operaciones de adición y multiplicación, denotadas por "$+$" y "$\cdot$", respectivamente, tales que

1. $a + b \in R$; $\forall a, b \in R$,
2. $a + b = b + a$; $\forall a, b \in R$,
3. $(a + b) + c = a + (b + c)$; $\forall a, b, c \in R$,
4. $\exists!\ 0 \in R$ / $a + 0 = a$; $\forall a \in R$,
5. $\exists!\ -a \in R$ / $a + (-a) = 0$; para cada $a \in R$,
6. $a \cdot b \in R$; $\forall a, b \in R$,
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$; $\forall a, b, c \in R$,
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$; $\forall a, b, c \in R$,

(Herstein, 1988).

Si la multiplicación en el anillo R es conmutativa; es decir, si se verifica que $a \cdot b = b \cdot a$, para todo $a, b \in R$, entonces R es un *anillo conmutativo*.

Escolio 2.1.1. Por simplicidad, para la multiplicación de f por g, se emplea la notación fg para denotar al producto de f y g, es decir

$$fg = f \cdot g.$$

Proposición 2.1.1. Sea R un anillo. Si 0 es el elemento neutro para la adición, entonces para todo $a \in R$ se verifica que

$$a \cdot 0 = 0 \cdot a = 0$$

(Herstein, 1988).

Demostración.

Sea a un elemento arbitrario del anillo R y 0 es elemento neutro para la adición en R. Nótese que

$$a \cdot 0 = a \cdot (0 + 0).$$

La condición 8 de la Definición 2.1.1 dice que en un anillo la multiplicación es distributiva respecto a la adición por derecha y por izquierda. Usando la distributividad por izquierda se tendrá que

$$a \cdot 0 = a \cdot 0 + a \cdot 0.$$

Como el elemento neutro para la adición en cualquier anillo es único, es necesario que

$$a \cdot 0 = 0.$$

Análogamente se muestra que

$$0 \cdot a = 0.$$

■

Definición 2.1.2. Sea R un anillo conmutativo. Si existe $1 \in R$ tal que

$$u \cdot 1 = u,$$

para todo u de R, entonces R es un *anillo con unidad*.

Definición 2.1.3 Sea R un anillo. Un subconjunto no vacío I de R es llamado *ideal* del anillo R si satisface las siguientes condiciones:

1. Si $f \in I$, $g \in I$, entonces $f + g \in I$,
2. Si $f \in I$, $g \in R$, entonces $g \cdot f \in I$

(Ene y Herzog, 2011).

Escolio 2.1.2. Para cualquier ideal I de un anillo R se verifica que $0 \in I$, donde 0 es el elemento neutro para la adición en R.

Escolio 2.1.3. R y $\{0\}$ son ideales triviales de cualquier anillo R, donde 0 es el elemento neutro aditivo en R.

Definición 2.1.4. Sea R un anillo conmutativo y $a \in R$, $a \neq 0$. Se dice que a es un *divisor de cero* si existe un $b \in R$, $b \neq 0$, tal que $a \cdot b = 0$ (Herstein, 1988).

Definición 2.1.5. Un anillo conmutativo es un *dominio entero* si no tiene divisores de cero (Herstein, 1988).

Definición 2.1.6. Sea R un anillo. Se dice que R es un *anillo con división* si el conjunto de sus elementos diferentes de cero tienen estructura de grupo con respecto a la multiplicación. (Herstein, 1988).

Definición 2.1.7. Un *cuerpo* es un anillo conmutativo con división (Herstein, 1988).

A los elementos de un cuerpo $\mathbb{K}$ se les denomina escalares. Dentro de los cuerpos más conocidos se encuentran el conjunto de los números reales ($\mathbb{R}$) y el conjunto de números complejos ($\mathbb{C}$) junto con las operaciones usuales de adición y multiplicación.

2.2. Relaciones de orden

En ciertos conjuntos aparece una noción de orden. Sin importar el conjunto con el que se esté trabajando, para referirse a un orden dentro de dicho conjunto se usará el término genérico "preceder". Así, en un conjunto cualquiera E se dirá que los elementos x e y están ordenados si x precede a y o viceversa.

Definición 2.2.1. Sea E un conjunto no vacío. Una relación $\mathcal{R}$ definida en E por

$$x \mathcal{R} y \iff x \text{ precede a } y,$$

es una relación de orden amplio en E si verifica lo siguiente:

1. **Reflexiva** $x \mathcal{R} x, \forall x \in E$,
2. **Antisimétrica** $x \mathcal{R} y \wedge y \mathcal{R} x \Rightarrow x = y$,
3. **Transitiva** $x \mathcal{R} y \wedge y \mathcal{R} z \Rightarrow x \mathcal{R} z$

(Lazo, 1992).

En lo que sigue del trabajo, en lugar de usar el término de "relación de orden amplio", sólo se dirá "relación de orden".

Definición 2.2.2. Sea E un conjunto no vacío. Una relación $\mathcal{R}$ definida en E cumple la *comparabilidad* si para cualesquiera x, y distintos de E se cumple que $x \mathcal{R} y$ o $y \mathcal{R} x$ (Munkres, 1971).

Definición 2.2.3. Sea $\mathcal{R}$ una relación de orden en un conjunto no vacío E. Si $\mathcal{R}$ no verifica la comparabilidad; es decir, existe por lo menos un par de elementos x, y distintos de E tales que no se

cumple que $x \mathcal{R} y$ e $y \mathcal{R} x$, entonces se dice que $\mathcal{R}$ es una relación orden parcial en E o simplemente orden parcial en E.

Definición 2.2.4. Sea E un conjunto no vacío. Si en E se define un orden parcial, entonces se dice que E es un **conjunto parcialmente ordenado**.

Sea A un conjunto diferente del vacío. El conjunto potencia de A, denotado por $P(A)$, es un conjunto parcialmente ordenado por la relación *inclusión*, denotada por $\subset$; es decir, $\subset$ es un orden parcial en $P(A)$.

Definición 2.2.5. Sea $\mathcal{R}$ una relación de orden en un conjunto no vacío E. Si $\mathcal{R}$ verifica la comparabilidad, entonces se dice que $\mathcal{R}$ es un orden total en E.

Definición 2.2.6. Sea E un conjunto no vacío. Si en E se define un orden total, entonces se dice que E es un **conjunto totalmente ordenado**.

El conjunto de los números reales $\mathbb{R}$ es un conjunto totalmente ordenado por la relación *menor o igual que*, denotada por $\leq$, pues esta es un orden total en $\mathbb{R}$.

Se usará la notación $(E, \mathcal{R})$ para denotar un conjunto totalmente ordenado E por el orden total $\mathcal{R}$.

Definición 2.2.7. Sea E un conjunto no vacío. Una relación $\mathcal{R}$ definida en E por

$$x \mathcal{R} y \iff x \text{ precede estrictamente a } y,$$

es una relación de orden estricta en E si verifica lo siguiente:

1. **Irreflexiva** $x \not\mathcal{R} x, \forall x \in E$,
2. **Asimétrica** $x \mathcal{R} y \Rightarrow y \not\mathcal{R} x$,
3. **Transitiva** $x \mathcal{R} y \wedge y \mathcal{R} z \Rightarrow x \mathcal{R} z$

(Lazo, 1992).

Definición 2.2.8. Sea $\mathcal{R}$ una relación de orden estricta en un conjunto no vacío E. Si $\mathcal{R}$ no verifica la comparabilidad, entonces se dice que $\mathcal{R}$ es un orden estricto parcial en E.

Definición 2.2.9. Sea E un conjunto no vacío. Si en E se define un orden estricto parcial, entonces se dice que E es un **conjunto estricto-parcialmente ordenado**.

Definición 2.2.10. Sea $\mathcal{R}$ una relación de orden estricta en un conjunto no vacío E. Si $\mathcal{R}$ verifica la comparabilidad, entonces se dice que $\mathcal{R}$ es un orden estricto total en E.

Definición 2.2.11 Sea E un conjunto no vacío. Si en E se define un orden estricto total, entonces se dice que E es un **conjunto estricto-totalmente ordenado**.

Los conjuntos de los números reales y enteros son conjuntos estricto-totalmente ordenados por la relación de orden *menor que*, denotada por $<$.

Definición 2.2.12 Sean $(A_1, \leq_1)$, $(A_2, \leq_2)$, ..., $(A_n, \leq_n)$ conjuntos totalmente ordenados y las n-uplas

$$a = (a_1, a_2, ..., a_n)$$

$$b = (b_1, b_2, ..., b_n)$$

del producto cartesiano $A_1 \times A_2 \times \cdots \times A_n$. Se define el orden del diccionario u orden lexicográfico en $A_1 \times A_2 \times \cdots \times A_n$, denotado por $\leq$, como

$$a \leq b \Longleftrightarrow (a_1 <_1 b_1) \vee (a_1 = b_1 \wedge a_2 <_2 b_2) \vee ... \vee (a_1 = b_1 \wedge a_2 = b_2 \wedge ... \wedge a_n \leq_n b_n).$$

2.3. Anillo polinomial en n variables sobre un cuerpo $\mathbb{K}$

Para las posteriores definiciones y, en general, en lo que sigue del trabajo, se trabajarán con variables escalares $x_1, x_2, ..., x_n$ de un cuerpo $\mathbb{K}$ dado.

Definición 2.3.1. Sea $\mathbb{K}$ un cuerpo. Un *monomio sobre* $\mathbb{K}$ en un número finito de variables $x_1, \cdots, x_n$ se define como un producto de la forma $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, y se denota por u; esto es

$$u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

donde cada exponente a_i es un entero no negativo. El *grado* de u, denotado por $g(u)$, es la suma de todos los exponentes a_i, es decir

$$g(u) = \sum_{i=1}^{n} a_i.$$

Para este estudio se denotará por M_n al conjunto de monomios en las n variables $x_1, \cdots, x_n$. Así, se definen los conjuntos:

$$M_1 := \{x_1^{a_1} \ / \ a_1 \in \mathbb{Z}_0^+\},$$

$$M_2 := \{x_1^{a_1} x_2^{a_2} \ / \ a_1, a_2 \in \mathbb{Z}_0^+\},$$

$$M_3 := \{x_1^{a_1} x_2^{a_2} x_3^{a_3} \ / \ a_1, a_2, a_3 \in \mathbb{Z}_0^+\},$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$M_n := \{x_1^{a_1} \cdots x_n^{a_n} \ / \ a_1, ..., a_n \in \mathbb{Z}_0^+\}.$$

Definición 2.3.2. Un *término* en las variables $x_1, ..., x_n$ con coeficiente en el cuerpo $\mathbb{K}$ es el producto de un escalar $c \in \mathbb{K}$ y un monomio $u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \in M_n$, y se denota por u'; esto es

$$u' = cu = cx_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}.$$

Al escalar c se le denomina coeficiente del término u'. El grado del término u' es el grado del monomio u que aparece en él; es decir, $g(u') = g(u)$.

Definición 2.3.3. Se define el conjunto de polinomios en las n variables $x_1, ..., x_n$ sobre el cuerpo $\mathbb{K}$, denotado por $\mathbb{K}[x_1, ..., x_n]$, como aquel conjunto que contiene a todas las sumas finitas de términos en las variables $x_1, ..., x_n$ con coeficientes en $\mathbb{K}$; esto es

$$\mathbb{K}[x_1, ..., x_n] := \left\{ \sum_{i=1}^{m} c_i u_i \ / \ c_i \in \mathbb{K}, u_i \in M_n, \ \ \forall i = 1, 2, ..., m \right\}$$

Para denotar un polinomio; es decir, una suma finita de términos en cualquier cantidad entera positiva de variables, se usarán letras minúsculas como f ó g según sea necesario.

Definición 2.3.4. El grado de un polinomio f, denotado por $g(f)$, es el mayor grado de los términos que lo componen.

En el conjunto de polinomios en una variable $x_1 = x$ sobre un determinado cuerpo $\mathbb{K}$, denotado por $\mathbb{K}[x]$, se dice que:

- un polinomio f está **ordenado ascendentemente** si los términos que lo componen están distribuidos de acuerdo al grado de sus términos: comenzando del que tiene menor grado y terminando en el de mayor grado. Este tipo de polinomios tiene la forma

  $$f = c_1 x^{j_1} + c_2 x^{j_2} + c_3 x^{j_3} + ... + c_n x^{j_n},$$

  donde $j_i \in \mathbb{Z}_0^+, \forall i = 1, ..., n$ y $j_1 < j_2 < ... < j_n$.

- un polinomio f está **ordenado descendentemente** si los términos que lo componen están distribuidos de acuerdo al grado de sus términos: comenzando del que tiene mayor grado y terminando en el de menor grado. Este tipo de polinomios tiene la forma

  $$f = c_1 x^{j_1} + c_2 x^{j_2} + c_3 x^{j_3} + ... + c_n x^{j_n},$$

  donde $j_i \in \mathbb{Z}_0^+, \forall i = 1, ..., n$ y $j_1 > j_2 > ... > j_n$.

- un polinomio f de grado n está **completo** si dentro de él existen todos los términos de menor grado a n hasta el término de grado cero, ya sea en orden o no.

Nótese que todo polinomio de $\mathbb{K}[x]$ se puede ordenar de manera ascendente o descendente. Además, se puede agregar los términos que faltan para que sea completo haciendo que estos tengan coeficiente cero. Luego, los polinomios de $\mathbb{K}[x]$ serán de la forma

$$f = c_0 + c_1x + c_2x^2 + ... + c_mx^m = \sum_{k=0}^{m} c_kx^k,$$

donde $g(f) = m$ y cada coeficiente c_k es un escalar de $\mathbb{K}$; es decir,

$$\mathbb{K}[x] = \left\{ \sum_{k=0}^{m} c_kx^k \ \ / \ \ c_k \in \mathbb{K}, \ \ \forall k = 0, 1, 2, ..., m \right\}$$

Dados los polinomios arbitrarios completos y ordenados ascendentemente

$$f = a_0 + a_1x + a_2x^2 + ... + a_mx^m = \sum_{i=0}^{m} a_ix^i \in \mathbb{K}[x],$$
$$g = b_0 + b_1x + b_2x^2 + ... + b_nx^n = \sum_{j=0}^{n} b_jx^j \in \mathbb{K}[x],$$

se definen las operaciones de la adición $(+)$ y la multiplicación $(\cdot)$ en $\mathbb{K}[x]$ de la siguiente manera:

- La adición es un cálculo simple, solo se sumarán los coeficientes de los términos semejantes de f y g, haciendo que los coeficientes para los términos que no existan sean ceros, es decir

$$f + g = \sum_{i=0}^{m} a_ix^i + \sum_{j=0}^{n} b_jx^j$$

$$\boxed{f + g = \sum_{l=0}^{q} (a_l + b_l)x^l, \text{ donde } q \leq \text{máx}\{m, n\}}$$

  La última expresión corresponde a la suma de f y g.

- Para la multiplicación, la expresión correspondiente al producto de los polinomios f y g no es tan fácil de deducir. A continuación, se muestra una deducción de esta.

$$\begin{aligned} f \cdot g =& \sum_{i=0}^{m} a_ix^i \cdot \sum_{j=0}^{n} b_jx^j \\ &= \left(a_0 + a_1x + a_2x^2 + ... + a_mx^m\right) \cdot \left(b_0 + b_1x + b_2x^2 + ... + b_nx^n\right) \\ &= a_0 \left(b_0 + b_1x + b_2x^2 + ... + b_nx^n\right) + a_1x(b_0 + b_1x + b_2x^2 + ... + \\ &\quad b_nx^n) + ... + a_mx^m \left(b_0 + b_1x + b_2x^2 + ... + b_nx^n\right) \end{aligned}$$

$$f \cdot g = \left(a_0b_0 + a_0b_1x + a_0b_2x^2 + ... + a_0b_nx^n\right) + (a_1b_0x + a_1b_1x^2 +$$

$$a_1b_2x^3 + ... + a_1b_nx^{n+1}) + ... + \left(a_mb_0x^m + a_mb_1x^{m+1} +\right.$$

$$a_mb_2x^{m+2} + ... + a_mb_nx^{m+n} \qquad right$$

Usando las propiedades del cuerpo $\mathbb{K}$ en la última igualdad se tendrá que

$$f \cdot g = a_0b_0 + (a_0b_1 + a_1b_0)\,x + (a_0b_2 + a_1b_1 + a_2b_0)\,x^2 + ... + a_mb_nx^{m+n}. \tag{1}$$

Haciendo $a_i = 0, \forall i > m$ y $b_j = 0, \forall j > n$, la ecuación (1) es equivalente a

$$f \cdot g = a_0b_0 + (a_0b_1 + a_1b_0)\,x + (a_0b_2 + a_1b_1 + a_2b_0)\,x^2 + ... +$$

$$(a_0b_{m+n} + a_1b_{m+n-1} + ... + a_mb_n + ... + a_{m+n-1}b_1 + a_{m+n}b_0)x^{m+n}. \tag{2}$$

Nótese que en el producto de f y g el coeficiente correspondiente al monomio $x^l, l = 0, 1, ..., m+n$, es

$$a_0b_l + a_1b_{l-1} + ... + a_lb_0 = \sum_{k=0}^{l} a_kb_{l-k}.$$

Luego, reemplazando cada coeficiente, en (2) se tendrá que

$$f \cdot g = \left(\sum_{k=0}^{0} a_kb_{0-k}\right)x^0 + \left(\sum_{k=0}^{1} a_kb_{1-k}\right)x^1 + \left(\sum_{k=0}^{2} a_kb_{2-k}\right)x^2 + ... + \left(\sum_{k=0}^{m+n} a_kb_{m+n-k}\right)x^{m+n}. \tag{3}$$

Finalmente, (3) es equivalente a

$$\boxed{f \cdot g = \sum_{l=0}^{m+n}\left(\sum_{k=0}^{l} a_kb_{l-k}\right)x^l}$$

La última expresión es la que corresponde al producto de f y g. Este producto también se puede expresar como

$$f \cdot g = \sum_{i=0}^{m} a_ix^i \cdot \sum_{j=0}^{n} b_jx^j = \sum_{l=0}^{m+n} c_lx^l,$$

donde

$$c_l = \sum_{k=0}^{l} a_kb_{l-k}.$$

Escolio 2.3.1. Tanto para la suma y el producto de los polinomios f y g surgirán coeficientes a_i y b_j aparte de los ya conocidos en f y g, los cuales simplemente tomarán el valor de cero para efectos de cálculo.

Proposición 2.3.1. Sea R un anillo y x una variable en R. El conjunto de todos los polinomios en una variable con coeficientes en el anillo R, denotado por $R\,[x]$, es un anillo con las operaciones de adición y multiplicación de polinomios.

Demostración.

Sea R un anillo y x una variable en R, se define el conjunto de polinomios en la variable x con coeficientes en el anillo R, denotado por $R[x]$, como aquel conjunto que contiene a todas las sumas finitas de términos en la variable x con coeficientes en R; esto es que

$$R[x] := \left\{ \sum_{i=1}^{m} c_i u_i \;\; / \;\; c_i \in R, u_i \in M_1, \;\; \forall i = 1, 2, ..., m \right\}.$$

Sean

$$f = a_0 + a_1 x + a_2 x^2 + ... + a_m x^m = \sum_{i=0}^{m} a_i x^i$$
$$g = b_0 + b_1 x + b_2 x^2 + ... + b_n x^n = \sum_{j=0}^{n} b_j x^j$$
$$h = c_0 + c_1 x + c_2 x^2 + ... + c_p x^p = \sum_{k=0}^{p} c_k x^k,$$

polinomios del conjunto de todos los polinomios en la variable x con coeficientes en R, denotado por $R\,[x]$.

En primer lugar, se mostrarán las propiedades correspondientes a la adición para que $R\,[x]$ sea un anillo. Se comenzará mostrando la cerradura de esta operación. La suma de los polinomios f y g está dada por

$$f + g = \sum_{l=0}^{q} (a_l + b_l) x^l, \text{ donde } q \leq \text{máx}\{m, n\}.$$

Como $f, g \in R\,[x]$, los coeficientes a_i, b_j son elementos del anillo R, $\forall i = 0, 1, 2, ..., m$ y $\forall j = 0, 1, 2, ..., n$. Luego, $a_l + b_l \in \mathbb{K}, \;\; \forall l = 0, 1, 2, ..., q$; donde $q \leq$ máx$\{m, n\}$, pues la adición de elementos en el anillo R es cerrada. Por lo tanto, $f + g \in R\,[x]$. Esto muestra que la adición en $R\,[x]$ es cerrada. Nótese también que

$$\begin{aligned} f + g &= \sum_{i=0}^{m} a_i x^i + \sum_{j=0}^{n} b_j x^j \\ &= \sum_{l=0}^{q} (a_l + b_l) x^l, \text{ donde } q \leq \text{máx}\{m, n\}, \end{aligned}$$

puesto que a_l y b_l son elementos del anillo R, se tendrá que

$$\begin{aligned} &= \sum_{l=0}^{q} (b_l + a_l)x^l, \text{ donde } q \leq \text{máx}\{n, m\}, \\ &= \sum_{j=0}^{n} b_j x^j + \sum_{i=0}^{m} a_i x^i \end{aligned}$$

Por consiguiente

$$f + g = g + f;$$

esto muestra la conmutatividad para la adición en $R[x]$. A continuación, se demuestra la asociatividad de la adición en $R[x]$. Véase que

$$\begin{aligned} (f+g)+h &= \left(\sum_{i=0}^{m} a_i x^i + \sum_{j=0}^{n} b_j x^j \right) + \sum_{k=0}^{p} c_k x^k \\ &= \left(\sum_{l=0}^{q} (a_l + b_l)x^l \right) + \sum_{k=0}^{p} c_k x^k, \text{ donde } q \leq \text{máx}\{m, n\}; \\ &= \sum_{s=0}^{r} \left[(a_s + b_s) + c_s \right] x^s, \text{ donde } r \leq \text{máx}\{q, p\}. \end{aligned} \tag{4}$$

Además, que $r \leq \text{máx}\{q, p\}$ y $q \leq \text{máx}\{m, n\}$ implican que $r \leq \text{máx}\{m, n, p\}$. Luego, usando la asociatividad de la adición en el anillo R en (4) se tendrá que

$$(f+g)+h = \sum_{s=0}^{r} \left[a_s + (b_s + c_s) \right] x^s, \text{ donde } r \leq \text{máx}\{m, n, p\}. \tag{5}$$

Análogamente, se puede mostrar que

$$f+(g+h) = \sum_{s=0}^{r} \left[a_s + (b_s + c_s) \right] x^s, \text{ donde } r \leq \text{máx}\{m, n, p\}. \tag{6}$$

Comparando (5) y (6) se tiene que

$$(f+g)+h = f+(g+h).$$

Ahora, supóngase que en $R[x]$ existe un único polinomio

$$e = \sum_{j=0}^{n} e_j x^j$$

tal que para todo f en $R[x]$ implica que

$$f + e = f. \tag{7}$$

En efecto, reemplazando f y e en (7) se tiene que

$$\sum_{i=0}^{m} a_i x^i + \sum_{j=0}^{n} e_j x^j = \sum_{i=0}^{m} a_i x^i,$$
$$\sum_{l=0}^{q} (a_l + e_l) x^l = \sum_{i=0}^{m} a_i x^i, \text{ donde } q \leq \text{máx}\{m, n\}.$$

Como ambas sumas en la última igualdad son iguales, $q = m$; reemplazando se tendrá que

$$\sum_{i=0}^{m} (a_i + e_i) x^i = \sum_{i=0}^{m} a_i x^i.$$

Luego, $a_i + e_i = a_i$, $\forall i = 1, ..., m$. Como $a_i \in R$, $\forall i = 1, ..., m$, y R es un anillo, $e_i = 0$, $\forall i = 1, ..., m$, donde 0 denota al elemento neutro para la adición en el anillo R. Por lo tanto,

$$e = \sum_{i=0}^{m} e_i x^i = \sum_{i=0}^{m} 0 x^i = 0$$

es el elemento neutro para la adición en $R[x]$. Esto muestra la existencia del elemento neutro para la adición en $R[x]$ y que este es el polinomio cuyos coeficientes son todos ceros, el cual se llamará polinomio nulo. Además, como 0 es el elemento neutro para la adición de R, este es único; lo que implica que el polinomio nulo es único. Seguidamente, supóngase que para cada polinomio f de $R[x]$ existe un polinomio

$$f' = \sum_{j=0}^{n} b_j x^j,$$

de $R[x]$, tal que

$$f + f' = e. \tag{8}$$

Reemplazando f, f' y e en (8) se tiene que

$$\sum_{i=0}^{m} a_i x^i + \sum_{j=0}^{n} b_j x^j = \sum_{i=0}^{m} 0 x^i,$$
$$\sum_{l=0}^{q} (a_l + b_l) x^l = \sum_{i=0}^{m} 0 x^i, \text{ donde } q \leq \text{máx}\{m, n\}.$$

Como ambas sumas en la última igualdad son iguales, $q = m$; reemplazando se tendrá que

$$\sum_{i=0}^{m} (a_i + b_i) x^i = \sum_{i=0}^{m} 0 x^i.$$

Luego, $a_i + b_i = 0$, $\forall i = 1, ..., m$. Como a_i es un elemento del anillo de R, para cada $i = 1, ..., m$, y 0 es elemento neutro para la adición en el anillo R, b_i es el elemento simétrico para la adición de a_i; es

decir, $b_i = -a_i$. Por lo tanto,

$$f' = \sum_{i=0}^{m}(-a_i)x^i = -\sum_{i=0}^{m} a_i x^i = -f$$

Así se muestra la existencia del elemento simétrico para la adición en $R[x]$. Además, $f' \in R[x]$ es único para cada $f \in R[x]$, ya que los coeficientes de f' son únicos para los coeficientes de f.

Se acaba de probar todas las propiedades con respecto a la adición para que $R[x]$ sea un anillo. Seguidamente, se prueban las propiedades con respecto a la multiplicación comenzando por la cerradura. El producto de los polinomios f y g está dado por

$$f \cdot g = \sum_{l=0}^{m+n}\left(\sum_{k=0}^{l} a_k b_{l-k}\right)x^l.$$

Como $f, g \in R[x]$, a_i, b_j son elementos del anillo R, $\forall i = 0, 1, ..., m$ y $\forall j = 0, 1, 2, ..., n$. Luego,

$$c_l = \sum_{k=0}^{l} a_k b_{l-k} \in R,$$

$\forall l = 0, 1, 2, ..., m+n$, pues la suma de productos de elementos del anillo R es otro elemento de R. Por lo tanto, $f \cdot g \in R[x]$. Esto muestra que la multiplicación en $R[x]$ es cerrada. A continuación, se muestra la asociatividad de esta operación. Véase que

$$\begin{aligned}(f \cdot g) \cdot h &= \left(\sum_{i=0}^{m} a_i x^i \cdot \sum_{j=0}^{n} b_j x^j\right) \cdot \sum_{k=0}^{p} c_k x^k \\ &= \left[\sum_{l=0}^{m+n}\left(\sum_{k=0}^{l} a_k b_{l-k}\right)x^l\right] \cdot \sum_{k=0}^{p} c_k x^k, \\ &= \sum_{s=0}^{(m+n)+p}\left[\sum_{t=0}^{s}\left(\sum_{k=0}^{t} a_k b_{t-k}\right)c_{s-t}\right]x^s. \end{aligned} \tag{9}$$

Utilizando las propiedades del anillo R se verifica que

$$\begin{aligned}\sum_{t=0}^{s}\left(\sum_{k=0}^{t} a_k b_{t-k}\right)c_{s-t} &= \sum_{t=0}^{s}\left(a_0 b_t + a_1 b_{t-1} + ... + a_{t-1} b_1 + a_t b_0\right)c_{s-t}, \\ &= a_0 b_0 c_s + (a_0 b_1 + a_1 b_0)c_{s-1} + ... + (a_0 b_{s-1} + a_1 b_{s-2} + ...+ \\ &\quad a_{s-2} b_1 + a_{s-1} b_0)c_1 + (a_0 b_s + a_1 b_{s-1} + ... + a_{s-1} b_1 + a_s b_0)c_0, \\ &= a_0(b_0 c_s + b_1 c_{s-1} + ... + b_{s-1} c_1 + b_s c_0) + a_1(b_0 c_{s-1} + b_1 c_{s-2}+ \\ &\quad ... + b_{s-2} c_1 + b_{s-1} c_0) + ... + a_{s-1}(b_0 c_1 + b_1 c_0) + a_s b_0 c_0, \\ &= \sum_{t=0}^{s} a_t\left(b_0 c_{s-t} + b_1 c_{s-t-1} + ... + b_{s-t-1} c_1 + b_{s-t} c_0\right), \\ \sum_{t=0}^{s}\left(\sum_{k=0}^{t} a_k b_{t-k}\right)c_{s-t} &= \sum_{t=0}^{s} a_t\left(\sum_{k=0}^{s-t} b_k c_{s-t-k}\right). \end{aligned} \tag{10}$$

Luego, reemplazando (10) en (9) se tiene que

$$(f \cdot g) \cdot h = \sum_{s=0}^{m+(n+p)} \left[\sum_{t=0}^{s} a_t \left(\sum_{k=0}^{s-t} b_k c_{s-t-k} \right) \right] x^s,$$

$$= \sum_{i=0}^{m} a_i x^i \cdot \left[\sum_{l=0}^{n+p} \left(\sum_{k=0}^{l} b_k c_{l-k} \right) x^l \right],$$

$$= \sum_{i=0}^{m} a_i x^i \cdot \left(\sum_{j=0}^{n} b_j x^j \cdot \sum_{k=0}^{p} c_k x^k \right)$$

$$(f \cdot g) \cdot h = f \cdot (g \cdot h).$$

Otra vez utilizando las propiedades del anillo R se tiene que

$$h \cdot (f+g) = \sum_{k=0}^{p} c_k x^k \cdot \left(\sum_{i=0}^{m} a_i x^i + \sum_{j=0}^{n} b_j x^j \right),$$

$$= \sum_{k=0}^{p} c_k x^k \cdot \left(\sum_{l=0}^{q} (a_l + b_l) x^l \right), \text{ donde } q \leq \text{máx}\{m, n\}$$

$$= \sum_{s=0}^{p+q} \left[\sum_{t=0}^{s} c_t (a_{s-t} + b_{s-t}) \right] x^s, \text{ donde } q \leq \text{máx}\{m, n\}$$

$$= \sum_{s=0}^{p+q} \left[\sum_{t=0}^{s} (c_t a_{s-t} + c_t b_{s-t}) \right] x^s, \text{ donde } q \leq \text{máx}\{m, n\}$$

$$= \sum_{s=0}^{p+q} \left[\sum_{t=0}^{s} c_t a_{s-t} + \sum_{t=0}^{s} c_t b_{s-t} \right] x^s, \text{ donde } q \leq \text{máx}\{m, n\}$$

$$= \sum_{s=0}^{p+m} \left(\sum_{t=0}^{s} c_t a_{s-t} \right) x^s + \sum_{s=0}^{p+n} \left(\sum_{t=0}^{s} c_t b_{s-t} \right) x^s,$$

$$= \sum_{k=0}^{p} c_k x^k \cdot \sum_{i=0}^{m} a_i x^i + \sum_{k=0}^{p} c_k x^k \cdot \sum_{j=0}^{n} b_j x^j,$$

$$h \cdot (f+g) = h \cdot f + h \cdot g.$$

Análogamente se prueba que $(f+g) \cdot h = f \cdot h + g \cdot h$. Esto muestra que la multiplicación es distributiva con respecto a la adición en $R[x]$ por izquierda y derecha. Con esto se termina de probar todas las propiedades de anillo para $R[x]$. Por lo tanto, el conjunto $R[x]$ junto a las operaciones de la adición y multiplicación definidas es un anillo. ■

Nótese que el anillo $R[x]$ está construido sobre el anillo R. Así, si el anillo R está provisto de más propiedades, entonces el anillo $R[x]$ también gozará de más propiedades. Esto conlleva a formular la proposición que se ve a continuación.

Proposición 2.3.2. Sea R un anillo y x una variable en R. Si R es un anillo conmutativo con unidad, entonces $R[x]$ es un anillo conmutativo con unidad.

Demostración.

Anteriormente se probó que el conjunto de polinomios en una variable con coeficientes en un anillo R, denotado por $R\left[x\right]$, es un anillo con las operaciones de adición y multiplicación de polinomios. Ahora, supóngase que R, además de ser sólo un anillo, es conmutativo y tiene unidad. Sea 1 la unidad del anillo R. Supóngase que existe $i \in R[x]$ tal que para $f \in R[x]$ se verifica que

$$f \cdot i = f. \tag{11}$$

Reemplazando f en (11) y usando las propiedades del anillo $R[x]$, se tendrá que

$$\sum_{j=0}^{m} a_j x^j \cdot i = \sum_{j=0}^{m} a_j x^j,$$

$$\left(a_0 + a_1 x + a_2 x^2 + ... + a_m x^m\right) \cdot i = \left(a_0 + a_1 x + a_2 x^2 + ... + a_m x^m\right).$$

$$\left(a_0 \cdot i + a_1 x \cdot i + a_2 x^2 \cdot i + ... + a_m x^m \cdot i\right) = \left(a_0 + a_1 x + a_2 x^2 + ... + a_m x^m\right).$$

$$\left((a_0 \cdot i) + (a_1 \cdot i)x + (a_2 \cdot i)x^2 + ... + (a_m \cdot i)x^m\right) = \left(a_0 + a_1 x + a_2 x^2 + ... + a_m x^m\right).$$

Nótese que $a_j \cdot i = a_j$, $\forall i = 1, ..., m$. Luego, como todo a_j pertenece al anillo con unidad R, $i = 1$; es decir, la unidad de $R[x]$ es el polinomio constante $i = 1$. Esto muestra que el anillo $R[x]$ tiene unidad.

Ahora, como R es anillo conmutativo, la adición y multiplicación en el anillo R son conmutativas. Luego, se tendrá que

$$\begin{aligned} f \cdot g &= \sum_{l=0}^{m+n} \left(\sum_{k=0}^{l} a_k b_{l-k} \right) x^l, \\ &= \sum_{l=0}^{m+n} \left(a_0 b_l + a_1 b_{l-1} + ... + a_{l-1} b_1 + a_l b_0\right) x^l, \\ &= \sum_{l=0}^{n+m} \left(b_0 a_l + b_1 a_{l-1} + ... + b_{l-1} a_1 + b_l a_0\right) x^l, \\ &= \sum_{l=0}^{n+m} \left(\sum_{k=0}^{l} b_k a_{l-k} \right) x^l, \end{aligned}$$

$$f \cdot g = g \cdot f;$$

es decir, la multiplicación en $R[x]$ es conmutativa. Por lo tanto, $R[x]$ es un anillo conmutativo y con unidad. ■

Para una segunda variable y, el conjunto de polinomios en las variables x e y con coeficientes en un anillo conmutativo con unidad R estará denotado por $R\left[x, y\right]$. Los elementos de $R\left[x, y\right]$ serán de la

forma

$$\sum_{i,j}^{m,n} a_{ij}x^i y^j.$$

Dichos elementos pueden reescribirse como

$$\sum_{j=0}^{n}\left(\sum_{i=0}^{m} a_{ij}x^i\right)y^j;$$

es decir, como polinomios en la variable y con coeficientes en $R[x]$. Por lo tanto, el conjunto $R[x,y]$ puede entenderse como $(R[x])[y]$. En virtud de la Proposición 2.3.1, $R[x,y]$ es un anillo y por la Proposición 2.3.2 es conmutativo y con unidad. Así, se enuncia la siguiente proposición.

Proposición 2.3.3. Sea R un anillo conmutativo con unidad y $x_1, x_2, ..., x_n$ son variables que pertenecen a R. El conjunto de todos los polinomios en las variables $x_1, x_2, ..., x_n$ con coeficientes en R, denotado por $R[x_1, x_2, ..., x_n]$, es un anillo conmutativo con unidad, para todo $n \in \mathbb{Z}^+$.

Demostración.

Con las Proposiciones 2.3.1 y 2.3.2 se mostró que la proposición se cumple para una variable.

Supóngase que para k variables la proposición es cierta; es decir, dado un anillo conmutativo con unidad R y $x_1, x_2, ..., x_k$ son variables que pertenecen a R, el conjunto $R[x_1, x_2, ..., x_k]$ es un anillo conmutativo con unidad (hipótesis inductiva). Se tiene que demostrar que la proposición es cierta para $k+1$ variables a partir de la suposición antes hecha. Para esto, igual que para el caso de dos variables que se vio antes de enunciar la proposición, los polinomios de $R[x_1, x_2, ..., x_k, x_{k+1}]$ se escribirán como polinomios en la variable x_{k+1} con coeficientes en $R[x_1, x_2, ..., x_k]$, que es un anillo conmutativo con unidad por la hipótesis inductiva, es decir

$$R[x_1, x_2, ..., x_k, x_{k+1}] = (R[x_1, x_2, ..., x_k])[x_{k+1}].$$

Como los polinomios de $R[x_1, x_2, ..., x_k, x_{k+1}]$ tienen coeficientes en $R[x_1, x_2, ..., x_k]$, que es un anillo por la hipótesis inductiva, $R[x_1, x_2, ..., x_k, x_{k+1}]$ será un anillo. Además, $R[x_1, x_2, ..., x_k]$ es conmutativo y tiene unidad por la hipótesis inductiva, lo que implica que $R[x_1, x_2, ..., x_k, x_{k+1}]$ es conmutativo y tiene unidad, esto por la Proposición 2.3.2. Por el principio de inducción, se concluye que la proposición se cumple para cualquier cantidad entera de variables. ■

La última proposición indica que, dado un anillo conmutativo con unidad, denotado por R, y las n variables $x_1, x_2, ..., x_n$ que pertenecen a R, el conjunto de polinomios en las n variables $x_1, ..., x_n$ con

coeficientes en R, denotado por $R[x_1, ..., x_n]$, tiene estructura de anillo, para todo $n \in \mathbb{Z}^+$; además es conmutativo y tiene unidad.

Nótese que todo cuerpo $\mathbb{K}$ es un anillo conmutativo y con unidad. Lo que se busca con esto, es mostrar que el anillo polinomial en n variables con coeficientes en el cuerpo $\mathbb{K}$, denotado por $\mathbb{K}[x_1, ..., x_n]$, se puede construir sobre un cuerpo y no necesariamente sólo sobre un anillo conmutativo con unidad. Luego, el conjunto de polinomios en las n variables $x_1, ..., x_n$ sobre el cuerpo $\mathbb{K}$ de la Definición 2.3.3 es un anillo conmutativo y con unidad. A partir de ahora, a dicho conjunto se le llamará *anillo polinomial en n variables sobre el cuerpo* $\mathbb{K}$.

Sea $\mathbb{K}$ un cuerpo cualquiera y teniendo las n variables $x_1, ..., x_n$ de $\mathbb{K}$, por simplicidad, se denotará al anillo polinomial en n variables sobre el cuerpo $\mathbb{K}$ por S_n. Es decir,

$$S_n = \mathbb{K}[x_1, ..., x_n].$$

2.4. Ideales en S_n

Definición 2.4.1. Un subconjunto no vacío I de S_n es llamado *ideal* de S_n si verifica las siguientes condiciones:

1. Si $f, g \in I$, entonces $f + g \in I$,
2. Si $f \in I$, $g \in S_n$, entonces $gf \in I$.

(Herzog *et* al., 2018)

Proposición 2.4.1. Sea $\{f_\alpha : \alpha \in \Gamma\}$ un subconjunto no vacío de S_n, donde Γ es un conjunto de índices. El conjunto I de polinomios p de la forma

$$\sum_{\alpha \in \Gamma} g_\alpha f_\alpha,$$

donde cada $g_\alpha \in S_n$ y g_α es nulo, excepto para un número finito de α's, es un ideal de S_n

(Herzog *et* al., 2018).

Demostración.

Sean

$$p = \sum_{\alpha \in \Gamma} g_\alpha f_\alpha \quad \text{y} \quad q = \sum_{\alpha \in \Gamma} h_\alpha f_\alpha,$$

polinomios de I, donde g_α, $h_\alpha \in S_n$ y además g_α y h_α son nulos, excepto para un número finito de α's. Nótese que como S_n tiene estructura de anillo, la suma $g_\alpha + h_\alpha = u_\alpha$ es otro polinomio de S_n y también u_α es nulo, excepto para un número finito de α's. Luego

$$\begin{aligned} p+q &= \sum_{\alpha\in\Gamma} g_\alpha f_\alpha + \sum_{\alpha\in\Gamma} h_\alpha f_\alpha, \\ &= \sum_{\alpha\in\Gamma} (g_\alpha + h_\alpha) f_\alpha, \\ p+q &= \sum_{\alpha\in\Gamma} u_\alpha f_\alpha, \end{aligned}$$

es otro polinomio de I. Además, si r es un polinomio de S_n, entonces el producto $r \cdot g_\alpha = v_\alpha$ es otro polinomio de S_n y también v_α es nulo, excepto para un número finito de α's. Luego

$$\begin{aligned} r \cdot p &= r \cdot \sum_{\alpha\in\Gamma} g_\alpha f_\alpha \\ &= \sum_{\alpha\in\Gamma} (r \cdot g_\alpha) f_\alpha \\ r \cdot p &= \sum_{\alpha\in\Gamma} v_\alpha f_\alpha, \end{aligned}$$

es otro polinomio de I. Por lo tanto, I es un ideal de S_n. ■

El ideal I visto en la Proposición 2.4.1 es llamado *ideal generado por* $\{f_\alpha : \alpha \in \Gamma\}$ y está denotado por $\langle\{f_\alpha : \alpha \in \Gamma\}\rangle$, es decir

$$I = \langle\{f_\alpha : \alpha \in \Gamma\}\rangle.$$

El conjunto $\{f_\alpha : \alpha \in \Gamma\}$ se denomina *sistema de generadores de* I.

En particular, si el sistema de generadores del ideal I es un conjunto finito $\{f_1, f_2, f_m\}$, entonces se escribe

$$I = \langle f_1, f_2, f_m\rangle,$$

e I se denomina *ideal finitamente generado*.

Escolio 2.4.1. Sea I un ideal de S_n. Existe un subconjunto $\{f_\alpha : \alpha \in \Gamma\}$ de S_n tal que

$$I = \langle\{f_\alpha : \alpha \in \Gamma\}\rangle.$$

Capítulo III

BASES DE GRÖBNER EN IDEALES DE S_n

3.1. Monomios minimales y Lema de Dickson

En álgebra generalmente, al momento de hablar de anillos es necesario tener dos operaciones cerradas (adición y multiplicación) en un conjunto. Para el presente estudio, es de fundamental importancia definir una operación en M_n; llamada *división de monomios* que no verifica la propiedad de cerradura.

Definición 3.1.1 (Condición de divisibilidad). Sean dos monomios $u = x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ y $v = x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ de M_n. Se dice que el monomio u divide a v, y se denota por $u|v$, si, y solo si, $a_i \leq b_i$ para cada $i = 1, ..., n$ (Herzog *et* al., 2018).

Sean los monomios

$$u = x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \quad \text{y} \quad v = x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$$

de M_n tales que $u|v$, con la particularidad de que $a_i < b_i$, $\forall i = 1, ..., n$. Luego, si se consideran los monomios u' y v', también de M_n, que resultan de intercambiar los exponentes de la variable x_1 de u y v; es decir,

$$u' = x_1^{b_1}x_2^{a_2}\cdots x_n^{a_n} \quad \text{y} \quad v' = x_1^{a_1}x_2^{b_2}\cdots x_n^{b_n}.$$

será imposible que $u'|v'$ o que $v'|u'$, ya que no se verifica que todos los exponentes de u' son menores o iguales a los de v', ni viceversa (condición de divisibilidad). Lo que se quiere mostrar con esto es que no todo par de monomios en M_n se pueden dividir.

Definición 3.1.2. Si $u = x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ divide a $v = x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$, al resultado de dividir v entre u se le llama *cociente* y es otro monomio $w = x_1^{b_1-a_1}x_2^{b_2-a_2}\cdots x_n^{b_n-a_n}$ de M_n; es decir

$$\frac{v}{u} = \frac{x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}}{x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}} = x_1^{b_1-a_1}x_2^{b_2-a_2}\cdots x_n^{b_n-a_n} = w.$$

Previamente se mostró que la división en M_n no es cerrada, pues no existe el cociente de dos monomios de M_n si no estos no verifican la condición de divisibilidad. El resultado enunciado a continuación es consecuencia de este razonamiento.

Proposición 3.1.1. La división de monomios en M_n es un orden parcial.

Demostración.

Para demostrar esto, se tiene que probar las tres propiedades de relación de orden y seguidamente mostrar porque es parcial.

I. $u|u, \forall u \in M_n$

Dado el monomio $u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \in M_n$. Como $a_i \leq a_i$, para cada $i = 1, ..., n$, se tiene que

$$u|u.$$

II. $u|v$ y $v|u \Longrightarrow u = v$

Dados los monomios

$$u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

$$v = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n},$$

de M_n. Supóngase que $u|v$ y $v|u$. Por la condición de divisibilidad, se tendrá que $a_i \leq b_i$ y $b_i \leq a_i$, para cada $i = 1, ..., n$; y como la relación *menor o igual que*, denotada por $\leq$, es antisimétrica en $\mathbb{Z}_0^+$, $a_i = b_i$, para cada $i = 1, ..., n$. Luego,

$$\begin{aligned} u &= x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}, \\ &= x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}, \\ u &= v. \end{aligned}$$

III. $u|v$ y $v|w \Longrightarrow u|w$

Dados los monomios

$$u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

$$v = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n},$$

$$w = x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n},$$

de M_n. Supóngase que $u|v$ y $v|w$. Por la condición de divisibilidad se tendrá que $a_i \leq b_i$ y $b_i \leq c_i$, para cada $i = 1, ..., n$; y como la relación *menor o igual que*, denotada por $\leq$, es transitiva en $\mathbb{Z}_0^+$, se tendrá que $a_i \leq c_i$, para cada $i = 1, ..., n$. Luego,

$$u|w.$$

Por I., II. y III., la divisón de monomios es una relación de orden en M_n. Y es un orden parcial porque no todos los pares de elementos u, v de M_n son comparables mediante la división de monomios, es decir, no cumplen que $u|v$ o $v|u$. ■

Sea $x_1^{a_1} \in M_1$. El conjunto de divisores de $x_1^{a_1}$, denotado por $Div(x_1^{a_1})$, será el conjunto de todos los monomios en $x_1^{b_1} \in M_1$ tales que $0 \leq b_1 \leq a_1$; es decir

$$Div(x_1^{a_1}) := \left\{ x_1^{b_1} \in M_1 \ / \ 0 \leq b_1 \leq a_1 \right\}.$$

El cardinal de dicho conjunto es $a_1 + 1$, esto significa que el monomio $x_1^{a_1}$ tiene $a_1 + 1$ divisores.

Sea $x_1^{a_1} x_2^{a_2} \in M_2$. El conjunto de divisores de $x_1^{a_1} x_2^{a_2}$, denotado por $Div(x_1^{a_1} x_2^{a_2})$, será el conjunto de todos los monomios en $x_1^{b_1} x_2^{b_2} \in M_2$ tales que $0 \leq b_1 \leq a_1$ y $0 \leq b_2 \leq a_2$; es decir

$$Div(x_1^{a_1} x_2^{a_2}) := \left\{ x_1^{b_1} x_2^{b_2} \in M_2 \ / \ 0 \leq b_1 \leq a_1 \wedge 0 \leq b_2 \leq a_2 \right\}.$$

El cardinal de dicho conjunto es $(a_1+1)(a_2+1)$, esto significa que el monomio $x_1^{a_1} x_2^{a_2}$ tiene $(a_1+1)(a_2+1)$ divisores.

Análogamente, para $x_1^{a_1} \cdots x_n^{a_n} \in M_n$, el conjunto de divisores de este monomio será

$$Div(x_1^{a_1} \cdots x_n^{a_n}) := \left\{ x_1^{b_1} \cdots x_n^{b_n} \in M_n \ / \ 0 \leq b_i \leq a_i; \forall i = 1, ..., n \right\}.$$

El monomio $x_1^{a_1} \cdots x_n^{a_n} \in M_n$ tendrá $\prod_{i=1}^{n} (a_i+1)$ divisores. Esto implica que un monomio en n variables tiene una cantidad finita de divisores.

Definición 3.1.3. Sean M un subconjunto no vacío de M_n y $u \in M$. El monomio u es llamado *monomio minimal* de M si, y solo si,

$$\forall\ v \in M;\ v|u \Longrightarrow v = u$$

(Herzog *e*t al., 2018).

En términos más simples, un monomio u es un monomio minimal de $M \subset M_n$ cuando ningún otro monomio de M, aparte de sí mismo, puede dividirlo.

De la Definición 3.1.3 se deduce que un monomio $u \in M \subset M_n$ no es minimal de M si, y solo si,

$$\exists\ v \in M\ /\ v|u \wedge v \neq u.$$

Esto último es utilizado para mostrar posteriores resultados.

Proposición 3.1.2. Sea M un subconjunto no vacío de M_n. Si M tiene un conjunto finito de monomios minimales $\{u_1, u_2, ..., u_m\}$ y $u \in M$, entonces u puede ser dividido por algún u_i, $i = 1, ..., m$.

Demostración.

Sea M un subconjunto no vacío de M_n que tiene un conjunto finito de monomios minimales $\{u_1, u_2, ..., u_m\}$ y $u \in M$.

- Si $u = u_i$, para algún $i = 1, ..., m$, ya está probada la proposición.
- Si $u \neq u_i$, para todo $i = 1, ..., m$, entonces $\exists\ v_1 \in M\ /\ v_1|u \wedge v_1 \neq u$.
  - Si $v_1 = u_i$, para algún $i = 1, ..., m$, ya está probada la proposición.
  - Si $v_1 \neq u_i$, para todo $i = 1, ..., m$, entonces $\exists\ v_2 \in M\ /\ v_2|v_1 \wedge v_2 \neq v_1$. Como $v_2|v_1$ y $v_1|u$, por la propiedad transitiva de la división de monomios, se tendrá que $v_2|u$.
    - Si $v_2 = u_i$, para algún $i = 1, ..., m$, ya está probada la proposición.
    - Si $v_2 \neq u_i$, para todo $i = 1, ..., m$, entonces $\exists\ v_3 \in M\ /\ v_3|v_2 \wedge v_3 \neq v_2$. Como $v_3|v_2$ y $v_2|u$, otra vez por la propiedad transitiva de la división de monomios, se tendrá que $v_3|u$.

    $\vdots$ $\vdots$ $\vdots$ $\vdots$

Este proceso se repite un número finito n de veces hasta llegar a un $v_n \in M$, que es divisor de u, que ya no puede ser dividido por ningún elemento de M salvo por sí mismo, ya que u tiene un número finito de divisores. Es decir, v_n es un monomio minimal u_i de M, para algún $i = 1, ..., m$, que divide a u. Así queda demostrada la proposición. ■

Seguidamente, se enunciará y demostrará uno de las proposiciones más importantes de este trabajo.

Proposición 3.1.3 (Lema de Dickson). El conjunto de monomios minimales de un subconjunto no vacío M de M_n es finito, $\forall n \in \mathbb{Z}^+$ (Herzog *et* al., 2018).

Demostración.

La demostración se hará por inducción. Para $n = 1$. Supóngase que M es un subconjunto de M_1. Nótese que los elementos de, sea cual sea, M tendrán la forma x_1^n, $n \in \mathbb{Z}_0^+$. Basta con escoger el elemento con menor exponente m de todos los elementos de M, pues este es el único que verifica la condición de monomio minimal en dicho conjunto. Así x_1^m es el único monomio minimal de M y sigue siendo finito.

Para $n = 2$. Si M fuera un subconjunto de M_2, se probará que el número de monomios minimales es finito. Por facilidad, se escogerá $x_1 = x$ y $x_2 = y$. En efecto, supóngase que se tienen infinitos monomios minimales $u_1 = x^{a_1}y^{b_1}, u_2 = x^{a_2}y^{b_2}, ...$ de M, ordenados de tal forma que $a_1 \leq a_2 \leq ....$ Nótese que $a_i \neq a_{i+1}$, ya que si sucede lo contrario, se tendrá que $b_i \leq b_{i+1}$ o $b_i \geq b_{i+1}$, lo que implicará que uno divida al otro y el que puede ser dividido dejaría de ser monomio minimal. Así $a_1 < a_2 < ....$ Como u_i no puede dividir a u_{i+1} por ser monomios minimales de M, necesariamente $b_1 > b_2 > ....$ Esto último implica que M tendrá como máximo $b_1 + 1$ monomios minimales. Así se prueba que $M \subset M_2$ tiene un número finito de monomios minimales.

Supóngase que la proposición es cierta para $n = k-1$, es decir, el conjunto de monomios minimales de un subconjunto no vacío de M_{k-1} es finito. A partir de la anterior suposición se tiene que demostrar que la proposición es verdad para $n = k$. Sea M un subconjunto no vacío de M_k

$$M = \{ux_k^b \in M_k \ / \ b \in \mathbb{Z}_0^+, \ u \in M_{k-1}\},$$

y defínase

$$N = \{u \in M_{k-1} \ / \ \exists b \in \mathbb{Z}_0^+ \text{ tal que } \ ux_k^b \in M\}.$$

Claramente N es diferente del vacío pues M lo es. Por la hipótesis inductiva, el conjunto de monomios minimales de $N \subset M_{k-1}$ es finito. Sean $u_1, u_2, ..., u_m$ los monomios minimales de N. Por la definición de N, se sigue que para cada u_i, $1 \leq i \leq m$, existirá $b_i \in \mathbb{Z}_0^+$ tal que $u_i x_k^{b_i} \in M$. Sea b el mayor entero entre $b_1, b_2, ..., b_m$ y c un entero no negativo menor a b, se define el conjunto $N_c \subset N$ por

$$N_c = \{u \in N \ / \ ux_k^c \in M\}.$$

Nuevamente por la hipótesis inductiva, el conjunto de monomios minimales de $N_c \subset M_{k-1}$ es finito y dichos monomios minimales serán $u_1^{(c)}, u_2^{(c)}, ..., u_{m_c}^{(c)}$. Luego, los monomios minimales de N_0 serán $u_1^{(0)}, u_2^{(0)}, ..., u_{m_0}^{(0)}$, los de N_1 serán $u_1^{(1)}, u_2^{(1)}, ..., u_{m_1}^{(1)}$ y así sucesivamente los monomios minimales de N_{b-1} serán $u_1^{(b-1)}, u_2^{(b-1)}, ..., u_{m_{b-1}}^{(b-1)}$.

Sea un monomio $w = ux_k^r$ de M, donde u es un monomio de M_{k-1} que, por la definición de N, pertenece a dicho conjunto.

- Si $r \geq b$, entonces w es divisible por algún monomio

$$u_1 x_k^{b_1}, u_2 x_k^{b_2}, ..., u_m x_k^{b_m},$$

de M_k, por la proposición anterior.

- Si $0 \leq r < b$, entonces, como $u \in N_r$, w puede ser dividido por algún monomio

$$u_1^{(r)} x_k^r, u_2^{(r)} x_k^r, ..., u_{s_r}^{(r)} x_k^r$$

de M_k por la proposición anterior.

Esto muestra que un monomio $w \in M$ puede ser dividido por uno de los monomios enumerados abajo:

$$\begin{aligned}
&u_1 x_k^{b_1}, u_2 x_k^{b_2}, ..., u_s x_k^{b_s};\\
&u_1^{(0)}, u_2^{(0)}, ..., u_{s_0}^{(0)};\\
&u_1^{(1)} x_n, u_2^{(1)} x_n, ..., u_{s_1}^{(1)} x_n;\\
&\quad \vdots \qquad\quad \vdots \qquad\quad \vdots\\
&u_1^{(b-1)} x_n^{b-1}, u_2^{(b-1)} x_n^{b-1}, ..., u_{s_{b-1}}^{(b-1)} x_n^{b-1}.
\end{aligned}$$

Por lo tanto, cada monomio minimal de M debe estar dentro de la lista anterior de monomios. En conclusión, el conjunto de monomios minimales de un subconjunto M de M_n es finito, $\forall n \in \mathbb{Z}^+$. ■

El Lema de Dickson garantiza que varios procesos dentro de la fundamentación teórica de las Bases de Gröbner terminan después de un número finito de pasos y es por eso que juega un papel fundamental para el desarrollo de este trabajo. Posterior a la siguiente definición, se enunciará y demostrará una consecuencia inmediata del Lema de Dickson.

Definición 3.1.4. Un ideal de S_n recibe el nombre de *ideal monomial* si su sistema de generadores está compuesto solo de monomios (Escudeiro, 2023).

Proposición 3.1.4. Si I es un ideal monomial de S_n y $\{u_\alpha \ / \ \alpha \in \Gamma\}$ su sistema de monomios generadores, entonces existe un subconjunto finito $\{u_{\alpha_1}, u_{\alpha_2}, ..., u_{\alpha_m}\}$ de $\{u_\alpha \ / \ \alpha \in \Gamma\}$ tal que

$$I = \langle u_{\alpha_1}, u_{\alpha_2}, ..., u_{\alpha_m} \rangle$$

(Herzog *e*t al., 2018)

Demostración.

Denótese por M al sistema de monomios generadores $\{u_\alpha \ / \ \alpha \in \Gamma\}$ de I, es decir

$$M = \{u_\alpha \ / \ \alpha \in \Gamma\}.$$

Nótese que $M \subset M_n$. Por el Lema de Dickson, el conjunto de monomios minimales de M es finito, sea este $\{u_{\alpha_1}, u_{\alpha_2}, ..., u_{\alpha_m}\}$. Se mostrará que el conjunto de minimales de M genera el ideal I. Dado un polinomio

$$f = \sum_{\alpha \in \Gamma} g_\alpha u_\alpha, \tag{12}$$

de I, donde $g_\alpha \in S_n$ y además g_α es nulo, excepto para un número finito de α's. Por la proposición 3.1.2 , cada u_α, $\alpha \in \Gamma$, puede ser dividido por algún u_{α_i}, $i = 1, ..., m$. Luego, para cada g_α no nulo se define el polinomio

$$h_\alpha = g_\alpha \frac{u_\alpha}{u_{\alpha_i}}.$$

$$\Rightarrow h_\alpha u_{\alpha_i} = g_\alpha u_\alpha \tag{13}$$

Reemplazando (13) en (12) se obtiene que

$$f = \sum_{\alpha \in \Gamma} h_\alpha u_{\alpha_i}.$$

Por último, sea $f_i \in S_n$ la suma de los h_α's que multiplican a u_{α_i}, se tendrá

$$f = \sum_{i=1}^{m} f_i u_{\alpha_i}.$$

Como f es un polinomio arbitrario de I,

$$I = \langle u_{\alpha_1}, u_{\alpha_2}, ..., u_{\alpha_n} \rangle.$$

■

Al conjunto finito de monomios que generan el ideal I se le llama *sistema de monomios generadores de* I. En palabras más simples, la Proposición 3.1.4 dice que todo ideal monomial es finitamente generado.

Proposición 3.1.5. Sea $I = \langle u_1, u_2, ..., u_m \rangle$ un ideal monomial de S_n. Un monomio u de S_n pertenece a I si, y solo si, u puede ser dividido por algún u_i, $i = 1, ..., m$ (Herzog *e*t al., 2018).

Demostración.

Sea un ideal monomial $I = \langle u_1, u_2, ..., u_m \rangle$ de S_n y u un monomio de S_n. Supóngase que u puede ser dividido por algún u_i, $i = 1, ..., m$. Esto implica que existe el monomio w de S_n tal que

$$\frac{u}{u_i} = w, \text{ para algún } i = 1, ..., m.$$

Luego,

$$u = wu_i \text{ para algún } i = 1, ..., m.$$

Haciendo $f_i = w$ y $f_j = 0$, $\forall j \neq i$, se tendrá que

$$u = \sum_{j=1}^{m} f_j u_j.$$

Por lo tanto, $u \in \langle u_1, u_2, ..., u_m \rangle$.

Para demostrar la recíproca, sea u un monomio de $I = \langle u_1, u_2, ..., u_m \rangle$. Esto es que

$$u = \sum_{i=1}^{m} f_i u_i, \tag{14}$$

donde cada $f_i \in S_n$. Luego, como $f_i \in S_n$, este puede ser escrito como

$$f_i = \sum_{j=1}^{m_i} a_{i_j} v_{i_j}, \tag{15}$$

donde los a_{i_j} son coeficientes no nulos del cuerpo $\mathbb{K}$ sobre el cual se construye S_n y los v_{i_j} son monomios de M_n. Reemplazando (15) en (14) se tendrá

$$u = \sum_{i=1}^{m} \left(\sum_{j=1}^{m_i} a_{i_j} v_{i_j} \right) u_i.$$

De esta última expresión, como u es un monomio, existirán i, j tales que $u = v_{i_j} u_i$. Esto muestra que algún u_i divide a u. ■

Proposición 3.1.6. Sea I un ideal monomial de S_n y $\mathcal{S}$ la colección de todos los sistemas de monomios generadores de I. Existe un único elemento de $\mathcal{S}$ que es mínimo respecto a la inclusión (Herzog *e*t al., 2018).

Demostración.

Existencia. Por la Proposición 3.1.4, existe un sistema de monomios generadores finito para el ideal monomial I. Si este no es mínimo respecto a la inclusión, entonces eliminando los monomios redundantes se obtiene un sistema de monomios generadores de I que es mínimo respecto a la inclusión.

Unicidad. Supóngase que existen dos sistemas de monomios generadores de I que son mínimos respecto a la inclusión

$$\{u_1, u_2, ..., u_m\} \text{ y } \{v_1, v_2, ..., v_n\}.$$

Sea $u_i \in \{u_1, u_2, ..., u_m\}$. Por la Proposición 3.1.5, u_i puede ser dividido por algún $v_j \in \{v_1, v_2, ..., v_n\}$, y por la misma proposición, v_j podrá ser dividido por algún $u_k \in \{u_1, u_2, ..., u_m\}$; esto es que

$$u_k | v_j \text{ y } v_j | u_i. \tag{16}$$

Por la propiedad transitiva de la división de monomios en M_n, u_i podrá ser dividido por u_k. Necesariamente $u_i = u_k$, ya que $\{u_1, u_2, ..., u_m\}$ es mínimo respecto a la inclusión. Reemplazando en (16) se tendrá que

$$u_i | v_j \text{ y } v_j | u_i.$$

Por la propiedad antisimétrica de la división de monomios en M_n, $u_i = v_j$; lo que implica que $u_i \in \{v_1, v_2, ..., v_n\}$. Por lo tanto

$$\{u_1, u_2, ..., u_m\} \subset \{v_1, v_2, ..., v_n\}.$$

Análogamente se prueba que

$$\{v_1, v_2, ..., v_n\} \subset \{u_1, u_2, ..., u_m\}.$$

Luego

$$\{u_1, u_2, ..., u_m\} = \{v_1, v_2, ..., v_n\}, (m = n).$$

Esto muestra que para todo ideal I de S_n existe un único sistema de monomios generadores que es mínimo respecto a la inclusión. ■

A partir de ahora, al sistema de monomios generadores de un ideal I de S_n que es mínimo respecto a la inclusión se le denominará *sistema de monomios generadores mínimo de* I.

3.2. Órdenes monomiales

Definición 3.2.1. Sea S_n el anillo polinomial en n variables sobre un cuerpo $\mathbb{K}$ y M_n el conjunto de monomios también en n variables. Una relación de orden monomial en S_n es un orden total en M_n, denotado por $\leq_{M_n}$, tal que

1. $1 \leq_{M_n} u, \forall u \in M_n$,

2. Si $u <_{M_n} v$ y $w \in M_n$, entonces $uw <_{M_n} vw$,

(Ene y Herzog, 2011).

En lo que sigue del trabajo, en lugar de usar el término de "relación de orden monomial en S_n", sólo se escribirá "orden monomial en S_n".

Escolio 3.2.1. Dados dos números reales a, b y el orden total " menor o igual que" en $\mathbb{R}$, denotada por $\leq$, se dice que $a < b$ cuando $a \leq b$, pero $a \neq b$. Similarmente, dados dos monomios u, v en n variables y un orden total en M_n, denotado por $\leq_{M_n}$, se dirá que $u <_{M_n} v$ cuando $u \leq_{M_n} v$, pero $u \neq v$.

Escolio 3.2.2. La segunda condición de orden monomial $\leq_{M_n}$ en S_n indica que

$$u <_{M_n} v \wedge w \in M_n, \Longrightarrow uw <_{M_n} vw$$

y además es casi trivial que

$$u = v \wedge w \in M_n \Longrightarrow uw = vw.$$

Con esto se quiere mostrar que la segunda condición de orden monomial en S_n implica que

$$u \leq_{M_n} v \wedge w \in M_n \Longrightarrow uw \leq_{M_n} vw.$$

Se usará esto último para mostrar algunos resultados posteriores.

3.2.1. Orden del diccionario

Definición 3.2.1.1 (Orden del diccionario). Dados los monomios

$$u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

$$v = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n},$$

de M_n. Se llama *orden del diccionario* en M_n, denotado por $\leq_{dic}$, a la relación dada por

$$u \leq_{dic} v \Longleftrightarrow (a_1 < b_1) \vee (a_1 = b_1 \wedge a_2 < b_2) \vee ... \vee (a_1 = b_1 \wedge a_2 = b_2 \wedge ... \wedge a_n \leq b_n).$$

Proposición 3.2.1.1. El orden del diccionario en M_n es un orden total en M_n.

Demostración.

Sean dos monomios distintos

$$u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

$$v = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n},$$

de M_n.

- Si $a_1 < b_1$, entonces $u \leq_{dic} v$.
- Si $b_1 < a_1$, entonces $v \leq_{dic} u$.
- Si $a_1 = b_1$, entonces
  - Si $a_2 < b_2$, entonces $u \leq_{dic} v$.
  - Si $b_2 < a_2$, entonces $v \leq_{dic} u$.
  - Si $a_1 = b_1 \wedge a_2 = b_2$, entonces
    - Si $a_3 < b_3$, entonces $u \leq_{dic} v$.
    - Si $b_3 < a_3$, entonces $v \leq_{dic} u$.
    - Si $a_1 = b_1 \wedge a_2 = b_2 \wedge a_3 = b_3$, entonces
      - Si $a_4 < b_4$, entonces $u \leq_{dic} v$.
      - Si $b_4 < a_4$, entonces $v \leq_{dic} u$.

      ⋮ ⋮ ⋮

En general

- Si $a_1 = b_1 \wedge a_2 = b_2 \wedge ... \wedge a_n \leq b_n$, entonces $u \leq_{dic} v$.
- Si $a_1 = b_1 \wedge a_2 = b_2 \wedge ... \wedge b_n \leq a_n$, entonces $v \leq_{dic} u$.

Esto muestra que dados dos monomios en M_n estos dos siempre se pueden comparar con el orden diccionario en M_n. A continuación, se probarán las tres propiedades de relación de orden.

I. $u \leq_{dic} u, \forall u \in M_n$

Dado el monomio $u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \in M_n$. Nótese que

$$a_1 = a_1 \wedge a_2 = a_2 \wedge ... \wedge a_n = a_n;$$

Lo cual es equivalente a que

$$a_1 = a_1 \wedge a_2 = a_2 \wedge ... \wedge a_n \leq a_n;$$

Por lo tanto, $u \leq_{dic} u$.

II. $u \leq_{dic} v$ y $v \leq_{dic} u \Longrightarrow u = v$.

Sean dos monomios

$$u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

$$v = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n},$$

de M_n, tales que $u \leq_{dic} v$ y $v \leq_{dic} u$. El objetivo es probar que $u = v$.

En efecto, supóngase que $u \neq v$; es decir, $u <_{dic} v$ o $v <_{dic} u$.

Si $u <_{dic} v$, entonces

$$(a_1 < b_1) \vee (a_1 = b_1 \wedge a_2 < b_2) \vee ... \vee (a_1 = b_1 \wedge a_2 = b_2 \wedge ... \wedge a_n < b_n).$$

- Si $a_1 < b_1$, entonces $b_1 \not< a_1$; esto implica que $v \not\leq_{dic} u$.
- Si $a_1 = b_1 \wedge a_2 < b_2$, entonces $b_1 = a_1 \wedge b_2 \not< a_2$; esto implica que $v \not\leq_{dic} u$.
- Si $a_1 = b_1 \wedge a_2 = b_2 \wedge a_3 < b_3$, entonces $b_1 = a_1 \wedge b_2 = a_2 \wedge b_3 \not< a_3$; esto implica que $v \not\leq_{dic} u$.

  $\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$
- Si $a_1 = b_1 \wedge a_2 = b_2 \wedge ... \wedge a_n < b_n$, entonces $b_1 = a_1 \wedge b_2 = a_2 \wedge ... \wedge b_n \not< a_n$; esto implica que $v \not\leq_{dic} u$.

Nótese que en todos los casos para que $u <_{dic} v$ se tiene que $v \not\leq_{dic} u$; esto contradice que $v \leq_{dic} u$.

Análogamente, si $v <_{dic} u$, entonces se contradice que $u \leq_{dic} v$. Por lo tanto $u = v$.

III. $u \leq_{dic} v$ y $v \leq_{dic} w \Longrightarrow u \leq_{dic} w$

Sean los monomios

$$u = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n},$$

$$v = x_1^{b_1} x_2^{b_2} \dots x_n^{b_n},$$

$$w = x_1^{c_1} x_2^{c_2} \dots x_n^{c_n}.$$

Supóngase que $u \leq_{dic} v$ y $v \leq_{dic} w$.

- Si $a_1 < b_1$ y
  - $b_1 < c_1$, entonces $a_1 < c_1$. Por lo tanto, $u \leq_{dic} w$.
  - $b_1 = c_1 \wedge b_2 < c_2$, entonces $a_1 < c_1$. Por lo tanto, $u \leq_{dic} w$.
  - $b_1 = c_1 \wedge b_2 = c_2 \wedge b_3 < c_3$, entonces $a_1 < c_1$. Por lo tanto, $u \leq_{dic} w$.

    $\vdots \qquad \vdots \qquad \vdots \qquad \vdots$
  - $b_1 = c_1 \wedge b_2 = c_2 \wedge ... \wedge b_n \leq c_n$, entonces $a_1 < c_1$. Por lo tanto, $u \leq_{dic} w$.
- Si $a_1 = b_1 \wedge a_2 < b_2$ y
  - $b_1 < c_1$, entonces $a_1 < c_1$. Por lo tanto, $u \leq_{dic} w$.
  - $b_1 = c_1 \wedge b_2 < c_2$, entonces $a_1 = c_1 \wedge a_2 < c_2$. Por lo tanto, $u \leq_{dic} w$.
  - $b_1 = c_1 \wedge b_2 = c_2 \wedge b_3 < c_3$, entonces $a_1 = c_1 \wedge a_2 < c_2$. Por lo tanto, $u \leq_{dic} w$.

    $\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$
  - $b_1 = c_1 \wedge b_2 = c_2 \wedge ... \wedge b_n \leq c_n$, entonces $a_1 = c_1 \wedge a_2 < c_2$. Por lo tanto, $u \leq_{dic} w$.

$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$

$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$

- Si $a_1 = b_1 \wedge a_2 = b_2 \wedge ... \wedge a_n \leq b_n$ y
  - $b_1 < c_1$, entonces $a_1 < c_1$. Por lo tanto, $u \leq_{dic} w$.
  - $b_1 = c_1 \wedge b_2 < c_2$, entonces $a_1 = c_1 \wedge a_2 < c_2$. Por lo tanto, $u \leq_{dic} w$.
  - $b_1 = c_1 \wedge b_2 = c_2 \wedge b_3 < c_3$, entonces $a_1 = c_1 \wedge a_2 = c_2 \wedge a_3 < c_3$. Por lo tanto, $u \leq_{dic} w$.

    $\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$
  - $b_1 = c_1 \wedge b_2 = c_2 \wedge ... \wedge b_n \leq c_n$, entonces $a_1 < c_1$. Por lo tanto, $u \leq_{dic} w$.

En conclusión, después de ver todos los posibles casos, se tiene que $u \leq_{dic} w$.

Por I., II. y III., el orden del diccionario $\leq_{dic}$ es una relación de orden en M_n y como además cumple la comparabilidad, es un orden total en M_n. ■

A continuación, se probará que el orden del diccionario $\leq_{dic}$ en M_n es un orden monomial en S_n.

Proposición 3.2.1.2. El orden del diccionario $\leq_{dic}$ en M_n es un orden monomial en S_n.

Demostración.

Para esto se probará las dos condiciones de orden monomial en S_n.

I. $1 \leq_{dic} u, \forall u \in M_n$

Sea un monomio arbitrario

$$u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

de M_n, donde cada exponente a_i es un entero no negativo. Nótese que la unidad de S_n, denotado por 1, es el monomio en el cual todas las variables x_i tienen exponente 0, es decir

$$1 = x_1^0 x_2^0 \cdots x_n^0.$$

Como cada $a_i \in \mathbb{Z}_0^+$, se tendrá que $0 \leq a_i$. Luego, si

- $0 < a_1$, entonces $1 \leq_{dic} u$.
- $0 = a_1$ y
  - $0 < a_2$, entonces $1 \leq_{dic} u$.
  - $0 = a_2$ y
    - $0 < a_3$, entonces $1 \leq_{dic} u$.
    - $0 = a_3$ y

    $\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$

Así sucesivamente, se tendrá que

- Si $0 < a_1 \wedge 0 < a_2 \wedge ... \wedge 0 \leq a_n$, entonces $1 \leq_{dic} u$.

Se acaba de mostrar que sea cual sea el valor de los exponentes enteros no negativos a_i, $1 \leq_{dic} u$. Como u es un monomio arbitrario de M_n, $1 \leq_{dic} u, \forall u \in M_n$.

II. Si $u <_{dic} v$ y $w \in M_n$, entonces $u \cdot w <_{dic} v \cdot w$.

Sean los monomios

$$u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

$$v = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n},$$

$$w = x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n},$$

de M_n. Nótese que

$$u \cdot w = x_1^{a_1+c_1} x_2^{a_2+c_2} \cdots x_n^{a_n+c_n},$$

$$v \cdot w = x_1^{b_1+c_1} x_2^{b_2+c_2} \cdots x_n^{b_n+c_n}$$

son monomios de M_n. Supóngase que $u <_{dic} v$; esto es equivalente a que

$$(a_1 < b_1) \vee (a_1 = b_1 \wedge a_2 < b_2) \vee ... \vee (a_1 = b_1 \wedge a_2 = b_2 \wedge ... \wedge a_n < b_n).$$

- Si $a_1 < b_1$, entonces

$$a_1 + c_1 < b_1 + c_1.$$

Por la definición del orden del diccionario en M_n, $u \cdot w <_{dic} v \cdot w$.

- Si $a_1 = b_1 \wedge a_2 < b_2$, entonces

$$a_1 + c_1 = b_1 + c_1 \wedge a_2 + c_2 < b_2 + c_2.$$

Por la definición del orden del diccionario en M_n, $u \cdot w <_{dic} v \cdot w$.

- Si $a_1 = b_1 \wedge a_2 = b_2 \wedge a_3 < b_3$, entonces

$$a_1 + c_1 = b_1 + c_1 \wedge a_2 + c_2 = b_2 + c_2 \wedge a_3 + c_3 < b_3 + c_3.$$

Por la definición del orden del diccionario en M_n, $u \cdot w <_{dic} v \cdot w$.

⋮ ⋮ ⋮ ⋮ ⋮ ⋮

- Si $a_1 = b_1 \wedge a_2 = b_2 \wedge ... \wedge a_n < b_n$, entonces

$$a_1 + c_1 = b_1 + c_1 \wedge a_2 + c_2 = b_2 + c_2 \wedge ... \wedge a_n + c_n < b_n + c_n.$$

Por la definición del orden del diccionario en M_n, $u \cdot w <_{dic} v \cdot w$.

Por lo tanto, sea cual sea el caso por el cual $u <_{dic} v$, siempre se tendrá que $u \cdot w <_{dic} v \cdot w$.

Por I. y II., el orden del diccionario $\leq_{dic}$ en M_n es un orden monomial en S_n. ■

Se acaba de probar que existe por lo menos un orden monomial en S_n. Similar a este orden monomial, se define el orden del diccionario inverso.

3.2.2. Orden del diccionario inverso

Definición 3.2.2.1 (Orden del diccionario inverso). Dados los monomios

$$u = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

$$v = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n},$$

de M_n. Se llama *orden diccionario inverso* en M_n, denotado por $\leq_{inv}$, a la relación dada por

$$u \leq_{inv} v \iff v \leq_{dic} u.$$

Análogamente al orden del diccionario en M_n, se puede probar que el orden del diccionario inverso $\leq_{inv}$ en M_n es un orden monomial en S_n.

3.2.3. Ideales líder en S_n

Proposición 3.2.3.1. Sea $\leq_{M_n}$ un orden monomial en S_n. Si u y v son monomios distintos de M_n tales que u divide a v, entonces $u <_{M_n} v$ (Herzog *et* al., 2018).

Demostración.

Sean los monomios distintos u y v de M_n tales que u divide a v. Esto implica que existe el cociente $w \in M_n$ tal que

$$\frac{v}{u} = w.$$

Obsérvese que $\frac{v}{u} = w$ es equivalente a que $v = w \cdot u$. Como u y v son distintos, el cociente w es diferente a 1. Además, $1 \leq_{M_n} w$, por la primera condición de orden monomial, por lo que $1 <_{M_n} w$. Luego, por la segunda condición del orden monomial $\leq_{M_n}$, se tiene que

$$1 \cdot u <_{M_n} w \cdot u.$$

Como $1 \cdot u = u$ y $w \cdot u = v$, reemplazando esto en última desigualdad se obtiene que $u <_{M_n} v$. ■

Proposición 3.2.3.2. Sea un orden monomial $\leq_{M_n}$ en S_n. No existe una secuencia infinita decreciente de la forma

$$u_0 \ _{M_n} > \ u_1 \ _{M_n} > u_2 \ _{M_n} > ...,$$

donde $u_0, u_1, u_2, ...$ son monomios (Herzog *e*t al., 2018).

Demostración.

Por contradición. Supóngase que sí existe una secuencia infinita decreciente de monomios $u_0, u_1, u_2, \cdots$ de la forma

$$u_0 \ _{M_n} > \ u_1 \ _{M_n} > u_2 \ _{M_n} > ... \ .$$

Defínase M como el conjunto que contiene a los monomios $u_0, u_1, u_2, ...$ tales que $u_0 \ _{M_n} > \ u_1 \ _{M_n} > u_2 \ _{M_n} > ...$; es decir,

$$M = \{u_0, u_1, u_2, ... \ / \ u_0 \ _{M_n} > \ u_1 \ _{M_n} > u_2 \ _{M_n} > ...\}.$$

Por el Lema de Dickson, el número de monomios minimales de M es finito. Sean $u_{i_1}, u_{i_2}, ..., u_{i_m}$ los monomios minimales de M, donde $i_1 < i_2 < ... < i_m$. Si $j > i_m$, entonces u_j debe dividirse por uno de los monomios minimales, esto por la Proposición 3.1.2. Sea u_{i_k} el minimal que divide a u_j. Por la Proposición 3.2.3.1, $u_{i_k} <_{M_n} u_j$. Sin embargo, ya que $j > i_m \geq i_k$ se tiene que $u_{i_k} \ _{M_n} > \ u_j$, lo que es una contradicción. ■

Definición 3.2.3.1. Dado un orden monomial $\leq_{M_n}$ en S_n y un polinomio distinto de cero

$$f = a_1u_1 + a_2u_2 + ... + a_mu_m$$

de S_n, donde los a_i son escalares de $\mathbb{K}$ distintos de cero y los u_i son monomios tales que

$$u_m \leq_{M_n} u_{m-1} \leq_{M_n} ... \leq_{M_n} u_2 \leq_{M_n} u_1.$$

El **soporte de** f es el conjunto definido por los monomios que aparecen en f y está denotado por $s(f)$.

$$s(f) = \{u_1, u_2, ..., u_m\}.$$

El **líder de** f **con respecto a** $\leq_{M_n}$ es el monomio maximal de $s(f)$ con respecto a $\leq_{M_n}$ y se denota por $\mathcal{L}(f, \leq_{M_n})$.

$$\mathcal{L}(f, \leq_{M_n}) = u_1.$$

El escalar a_1 que acompaña al $\mathcal{L}(f, \leq_{M_n})$ es llamado **coeficiente principal de** f **respecto a** $\leq_{M_n}$ y el término $a_1 u_1$ es llamado **término líder de** f **respecto a** $\leq_{M_n}$.

Escolio 3.2.3.1. Por conveniencia, se define que, para cualquier orden monomial $\leq_{M_n}$ en S_n, el líder del polinomio nulo es 0; es decir, $\mathcal{L}(0, \leq_{M_n}) = 0$, y además

$$\mathcal{L}(0, \leq_{M_n}) <_{M_n} \mathcal{L}(f, \leq_{M_n}),$$

para todo polinomio no nulo f de S_n.

Proposición 3.2.3.3. Sea $\leq_{M_n}$ un orden monomial en S_n. Si f y g son polinomios no nulos de S_n y $w \in M_n$, entonces

1. $\mathcal{L}(fg, \leq_{M_n}) = \mathcal{L}(f, \leq_{M_n})\mathcal{L}(g, \leq_{M_n})$.
2. $\mathcal{L}(wf, \leq_{M_n}) = w\mathcal{L}(f, \leq_{M_n})$.

Demostración.

1. Dado el orden monomial $\leq$ en S_n. Si f y g son polinomios no nulos de S_n, entonces

$$u \leq_{M_n} \mathcal{L}(f, \leq_{M_n}), \quad \forall u \in s(f),$$
$$v \leq_{M_n} \mathcal{L}(g, \leq_{M_n}), \quad \forall v \in s(g).$$

Por la segunda segunda condición del orden monomial $\leq_{M_n}$ en S_n, se tendrá que

$$uv \leq_{M_n} \mathcal{L}(f, \leq_{M_n})v, \quad \forall u \in s(f), \forall v \in s(g);$$
$$\mathcal{L}(f, \leq_{M_n})v \leq_{M_n} \mathcal{L}(f, \leq_{M_n})\mathcal{L}(g, \leq_{M_n}), \quad \forall v \in s(g).$$

Y como $\leq_{M_n}$ es un relación transitiva en M_n,

$$uv \leq_{M_n} \mathcal{L}(f, \leq_{M_n})\mathcal{L}(g, \leq_{M_n}), \forall u \in s(f), \forall v \in s(g).$$

Nótese que

$$s(fg) \subset \{uv \in M_n \ / \ u \in s(f) \wedge v \in s(g)\}.$$

Luego, se tendrá que

$$uv \leq_{M_n} \mathcal{L}(f, \leq_{M_n})\mathcal{L}(g, \leq_{M_n}), \forall uv \in s(fg). \tag{17}$$

Como $\mathcal{L}(f, \leq_{M_n})$ y $\mathcal{L}(g, \leq_{M_n})$ son los elementos maximales de $s(f)$ y $s(g)$, respectivamente, se tendrá que $\mathcal{L}(f, \leq_{M_n})\mathcal{L}(g, \leq_{M_n}) \in s(fg)$. Y por (17), se tendrá que

$$\mathcal{L}(fg, \leq_{M_n}) = \mathcal{L}(f, \leq_{M_n})\mathcal{L}(g, \leq_{M_n}).$$

2. Dado el orden monomial $\leq_{M_n}$ en S_n. Sea f un polinomio no nulo de S_n.

$$u \leq_{M_n} \mathcal{L}(f, \leq_{M_n}), \forall u \in s(f),$$

Si w es un monomio de M_n,

$$wu \leq_{M_n} w\mathcal{L}(f, \leq_{M_n}), \forall u \in s(f),$$

por la segunda condición del orden monomial $\leq_{M_n}$ en S_n. Nótese que

$$s(wf) = \{wu \in M_n \ / \ u \in s(f)\}.$$

Luego, se tendrá que

$$wu \leq_{M_n} w\mathcal{L}(f, \leq_{M_n}), \forall wu \in s(wf), \tag{18}$$

Como $\mathcal{L}(f, \leq_{M_n}) \in s(f)$, $w\mathcal{L}(f, \leq_{M_n}) \in s(wf)$. Por (18), se tendrá que

$$\mathcal{L}(wf, \leq_{M_n}) = w\mathcal{L}(f, \leq_{M_n}).$$

■

Definición 3.2.3.2. Dados un ideal no nulo I y un orden monomial $\leq_{M_n}$ en S_n. El *ideal líder de* I *respecto a* $\leq_{M_n}$ es el ideal monomial generado por $\{\mathcal{L}(f, \leq_{M_n}) \ / \ f \in I, f \neq 0\}$ y está denotado por $\mathcal{L}(I, \leq_{M_n})$. Es decir,

$$\mathcal{L}(I, \leq_{M_n}) = \langle \{\mathcal{L}(f, \leq_{M_n}) \ / \ f \in I, f \neq 0\} \rangle$$

(Herzog *e*t al., 2018).

3.3. Bases de Gröbner

Definición 3.3.1 (Base de Gröbner). Sea I un ideal y $\leq_{M_n}$ un orden monomial en S_n. Una *base de Gröbner de I respecto a* $\leq_{M_n}$ es un conjunto finito $\{g_1, g_2, ..., g_m\}$ de polinomios no nulos de I tales que

$\{\mathcal{L}(g_1, \leq_{M_n}), \mathcal{L}(g_2, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n})\}$ es un sistema de monomios generadores de $\mathcal{L}(I, \leq_{M_n})$(Ene y Herzog, 2011).

Es aquí dónde surge la principal preguntas de la investigación: ¿Todo ideal de S_n tendrá una base de Gröbner?

Proposición 3.3.1. Sea I un ideal no nulo y $\leq_{M_n}$ un orden monomial en S_n. I por lo menos tiene una base de Gröbner respecto a $\leq_{M_n}$.

Demostración.

Supóngase que se tiene un ideal no nulo I y un orden monomial $\leq_{M_n}$ en S_n. El ideal líder de I respecto a $\leq_{M_n}$,

$$\mathcal{L}(I, \leq_{M_n}) = \langle \{\mathcal{L}(f, \leq_{M_n}) \ / \ f \in I, f \neq 0\} \rangle,$$

es un ideal monomial, ya que está generado por monomios. Por la Proposición 3.1.4, $\mathcal{L}(I, \leq_{M_n})$ es finitamente generado, esto implica que existe

$$\{\mathcal{L}(f_1, \leq_{M_n}), \mathcal{L}(f_2, \leq_{M_n}), ..., \mathcal{L}(f_m, \leq_{M_n})\} \subset \{\mathcal{L}(f, \leq_{M_n}) \ / \ f \in I, f \neq 0\}$$

tal que

$$\mathcal{L}(I, \leq_{M_n}) = \langle \mathcal{L}(f_1, \leq_{M_n}), \mathcal{L}(f_2, \leq_{M_n}), ..., \mathcal{L}(f_m, \leq_{M_n}) \rangle,$$

donde $f_1, f_2, \cdots, f_m$ son polinomios no nulos de I. Basta con escoger $\{f_1, f_2, \cdots, f_m\}$ para encontrar una base de Gröbner respecto a $\leq_{M_n}$ para I . ■

Dado un orden monomial en S_n, se muestra la existencia de una base de Gröbner para un ideal no nulo I de S_n, mas no es posible garantizar la unicidad de esta, ya que si $\{f_1, f_2, ..., f_m\} \subset I$ es una base de Gröbner de I, cualquier subconjunto de I que contenga propiamente a $\{f_1, f_2, ..., f_m\}$ será otra base de Gröbner.

Trabajando con un orden monomial en S_n, un conjunto $\{g_1, g_2, ..., g_m\}$ de polinomios no nulos de un ideal I es una base de Gröbner si los líderes de cada g_i, $i = 1, 2, ..., m$ generan el ideal líder de I. Sin embargo, contrario a la noción habitual que se tiene de las propiedades de base de una estructura algebraica, aún no se tiene la certeza de si el subconjunto $\{g_1, g_2, ..., g_m\}$ de I genera el ideal I. A continuación, se enuncia y demuestra una propiedad muy importante de las bases de Gröbner.

Proposición 3.3.2. Sea I un ideal y $\leq_{M_n}$ un orden monomial en S_n. Si $\{g_1, g_2, ..., g_m\}$ es una base Gröbner del ideal I de S_n respecto a $\leq_{M_n}$, entonces $\{g_1, g_2, ..., g_m\}$ es un sistema de generadores de I (Ene y Herzog, 2011).

Demostración.

En efecto, dado un ideal arbitrario no nulo I y un orden monomial $\leq_{M_n}$ en S_n. Supóngase que $\{g_1, g_2, ..., g_m\}$ una base de Gröbner de I respecto a $\leq_{M_n}$.

Sea $f \in \langle g_1, g_2, ..., g_m \rangle$. Luego,

$$f = \sum_{i=1}^{m} f_i g_i,$$

donde cada $f_i \in S_n$. Por la definición de ideal de S_n, $f \in I$.

$$\implies \langle g_1, g_2, ..., g_n \rangle \subset I$$

Por la definición de base de Gröbner se tendrá que

$$\mathcal{L}(I, \leq_{M_n}) = \langle \mathcal{L}(g_1, \leq_{M_n}), \mathcal{L}(g_2, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n}) \rangle.$$

Dado un polinomio no nulo f de I. Por la definición de $\mathcal{L}(I, \leq_{M_n})$, se tendrá que $\mathcal{L}(f, \leq_{M_n}) \in \mathcal{L}(I, \leq_{M_n})$. Luego, por la Proposición 3.1.5, podrá ser dividido por algún $\mathcal{L}(g_{i_0}, \leq_{M_n})$, $i_0 = 1, ..., m$; lo que implica que existirá un monomio u_0 tal que

$$\frac{\mathcal{L}(f, \leq_{M_n})}{\mathcal{L}(g_{i_0}, \leq_{M_n})} = u_0$$

$$\implies \mathcal{L}(f, \leq_{M_n}) = u_0 \mathcal{L}(g_{i_0}, \leq_{M_n})$$

$$\implies \mathcal{L}(f, \leq_{M_n}) = \mathcal{L}(u_0 g_{i_0}, \leq_{M_n}),$$

esto último por la Proposición 3.2.3.3. Sean a_0 y a_{i_0} los coeficientes principales de f y g_{i_0}, respectivamente, defínase el polinomio

$$h^{(1)} = a_{i_0} f - a_0 u_0 g_{i_0},$$

que claramente pertenece a I.

- Si $h^{(1)} = 0$, entonces

$$f = \frac{a_0}{a_{i_0}} u_0 g_{i_0},$$

y así $f \in \langle g_1, g_2, ..., g_m \rangle$.

- Si $h^{(1)} \neq 0$, por como está definido $h^{(1)}$,

$$s(h^{(1)}) = [s(f) \cup s(u_0 g_{i_0})] - \{\mathcal{L}(f, \leq_{M_n})\}.$$

Como $\mathcal{L}(f, \leq_{M_n}) = \mathcal{L}(u_0 g_{i_0}, \leq_{M_n})$ es el mayor monomio de $s(f) \cup s(u_0 g_{i_0})$, se tendrá que

$$\mathcal{L}(f, \leq_{M_n}) \ _{M_n} > \ \mathcal{L}(h^{(1)}, \leq_{M_n}).$$

Ya que $h^{(1)}$ es un polinomio no nulo de I, se repite el mismo proceso que se uso para f. Se escoge g_{i_1}, $i_1 = 1, ..., m$ de tal forma que

$$\mathcal{L}(h^{(1)}, \leq_{M_n}) = \mathcal{L}(u_1 g_{i_1}, \leq_{M_n}),$$

para luego definir el polinomio

$$h^{(2)} = a_{i_1} h^{(1)} - a_1 u_1 g_{i_1},$$

que claramente pertenece a I, donde a_1 y a_{i_1} son los coeficientes principales de $h^{(1)}$ y g_{i_1}.

- Si $h^{(2)} = 0$, entonces

$$h^{(1)} = \frac{a_1}{a_{i_1}} u_1 g_{i_1},$$

y así $h^{(1)} \in \langle g_1, g_2, ..., g_m \rangle$, lo que implicará que $f \in \langle g_1, g_2, ..., g_m \rangle$.

- Si $h^{(2)} \neq 0$, se tendrá que

$$\mathcal{L}(f, \leq_{M_n}) \ _{M_n} > \ \mathcal{L}(h^{(1)}, \leq_{M_n}) \ _{M_n} > \ \mathcal{L}(h^{(2)}, \leq_{M_n});$$

y se define el polinomio $h^{(3)}$ de I. Supóngase que se continúa este procedimiento hasta definir un polinomio $h^{(k)}$ de I.

  - Si $h^{(k)} = 0$, entonces $f \in \langle g_1, g_2, ..., g_m \rangle$.
  - Si $h^{(k)} \neq 0$, se tendrá que

$$\mathcal{L}(f, \leq_{M_n}) \ _{M_n} > \ \mathcal{L}(h^{(1)}, \leq_{M_n}) \ _{M_n} > \ ... \ _{M_n} > \ \mathcal{L}(h^{(k)}, \leq_{M_n}),$$

y se definirá un polinomio $h^{(k+1)}$.

Si se continúa con este proceso, entonces se obtendrá una secuencia infinita decreciente de monomios de la forma

$$\mathcal{L}(f, \leq) \ _{M_n} > \ \mathcal{L}(h^{(1)}, \leq) \ _{M_n} > \ \mathcal{L}(h^{(2)}, \leq) \ _{M_n} > \ ...,$$

lo cual contradice la Proposición 3.2.3.2. Por lo tanto, este proceso terminará en $h^{(m)} = 0$, para algún $m \in \mathbb{Z}^+$, lo que implicará que $f \in \langle g_1, g_2, ..., g_m \rangle$.

$$\Longrightarrow I \subset \langle g_1, g_2, ..., g_m \rangle$$

Por lo tanto $I = \langle g_1, g_2, ..., g_n \rangle$. ■

Proposición 3.3.3. Cada ideal I de S_n es finitamente generado (Ene y Herzog, 2011).

Demostración.

La Proposición 3.3.1 garantiza que todo ideal I de S_n tiene una base de Gröbner, y además esta es finita por definición. Por la Proposición 3.3.2 dicha base de Gröbner (finita) genera I. Esto muestra que I es finitamente generado. ■

Seguidamente, se exhibirán bases de Gröbner con algunas particularidades y se demostrarán sus características con la ayuda de resultados anteriores.

3.3.1. Bases de Gröbner mínimas

Dados un ideal I y un orden monomial $\leq_{M_n}$ de S_n. La Proposición 3.1.6 garantiza que para el ideal monomial $\mathcal{L}(I, \leq_{M_n})$ existe un único sistema de monomios generadores mínimo.

Definición 3.3.1.1 (Base de Gröbner mínima). Sea I un ideal y $\leq_{M_n}$ un orden monomial en S_n. Una base de Gröbner $\{g_1, g_2, ..., g_m\}$ del ideal I es *mínima* respecto a $\leq_{M_n}$ si verifica que

1. $\{\mathcal{L}(g_1, \leq_{M_n}), \mathcal{L}(g_2, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n})\}$ es el sistema de monomios generadores mínimo de $\mathcal{L}(I, \leq_{M_n})$,
2. el coeficiente principal de g_i es 1, para cada $i = 1, 2, ..., m$.

Proposición 3.3.1.1. Todo ideal I de S_n posee una base de Gröbner mínima respecto a un orden monomial dado.

Demostración.

Dado un orden monomial $\leq_{M_n}$ en S_n. Sea I un ideal arbitrario de S_n y $\{g_1, g_2, ..., g_p\}$ una base de Gröbner de I respecto a $\leq_{M_n}$, esto implica que $\{\mathcal{L}(g_1, \leq_{M_n}), \mathcal{L}(g_2, \leq_{M_n}), ..., \mathcal{L}(g_p, \leq_{M_n})\}$ es un sistema de monomios generadores de $\mathcal{L}(I, \leq_{M_n})$ y si este no es mínimo, se eliminan los monomios redundantes hasta tener el sistema de monomios generadores mínimo $\{\mathcal{L}(g_1, \leq_{M_n}), \mathcal{L}(g_2, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n})\}$ de

I (que está contenido en $\{\mathcal{L}(g_1, \leq_{M_n}), \mathcal{L}(g_2, \leq_{M_n}), ..., \mathcal{L}(g_p, \leq_{M_n})\}$). Sea c_i el coeficiente principal de g_i, para cada $i = 1, 2, ..., m$, defínase el polinomio

$$g_i' = c_i^{-1} g_i,$$

que pertenece a I, ya que $g_i \in I$. Nótese que $\{g_1', g_2', ..., g_m'\}$ es una base de Gröbner ya que

$$\{\mathcal{L}(g_1', \leq_{M_n}), \mathcal{L}(g_2', \leq_{M_n}), ..., \mathcal{L}(g_m', \leq_{M_n})\} = \{\mathcal{L}(g_1, \leq_{M_n}), \mathcal{L}(g_2, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n})\}$$

es el sistema de monomios generadores mínimo de $\mathcal{L}(I, \leq_{M_n})$. Además, el coeficiente principal de cada g_i' es 1, esto por como está definido. Luego, $\{\mathcal{L}(g_1', \leq_{M_n}), \mathcal{L}(g_2', \leq_{M_n}), ..., \mathcal{L}(g_m', \leq_{M_n})\}$ es una base de Gröbner mínima de I. Como I es un ideal arbitrario de S_n, todo ideal de S_n posee una base de Gröbner mínima respecto a un orden monomial dado. ■

Existen bases de Gröbner mínimas para un ideal I de S_n, mas no se puede garantizar que estas sean únicas. En efecto, si $\{g_1, g_2, ..., g_m\}, (m > 1)$ es una base de Gröbner mínima del ideal I respecto a un orden monomial $\leq_{M_n}$ en S_n, tal que $\mathcal{L}(g_1, \leq_{M_n}) \leq_{M_n} \mathcal{L}(g_2, \leq_{M_n})$, entonces $\{g_1, g_2 + g_1, ..., g_m\}$.

3.3.2. El algoritmo de la división

Proposición 3.3.2.1 (Algoritmo de la división). Sean $f \in S_n$ y $g_1, g_2, ..., g_m$ polinomios no nulos de S_n. Dado un orden monomial $\leq_{M_n}$ en S_n, existen polinomios $q_1, q_2, ..., q_m$ y r de S_n, tal que

$$f = q_1 g_1 + q_2 g_2 + ... + q_m g_m + r, \tag{19}$$

y verifican las condiciones:

1. $s(r)$ y el ideal $\langle \mathcal{L}(g_1, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n}) \rangle$ son disjuntos;
2. $\mathcal{L}(q_i g_i, \leq_{M_n}) \leq_{M_n} \mathcal{L}(f, \leq_{M_n}), \forall\, i = 1, ..., m.$

La expresión (19) recibe el nombre de forma estándar de f respecto a $g_1, g_2, ..., g_m$ y r se denomina residuo o resto de f respecto a $g_1, g_2, ..., g_m$ (Ene y Herzog, 2011).

Demostración.

En efecto, sea $I = \langle \mathcal{L}(g_1, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n}) \rangle$. Si:

- $s(f) \cap I = \phi$. Haciendo $q_1 = q_2 = ... = q_m = 0$ y $r = f$ se verifica que $s(r) \cap I = \phi$ y

$$\mathcal{L}(q_i g_i, \leq_{M_n}) = \mathcal{L}(0, \leq_{M_n}) \leq_{M_n} \mathcal{L}(f, \leq_{M_n}), \forall i = 1, ..., m.$$

- $s(f) \cap I \neq \phi$. Sea u_0 el monomio maximal respecto a $\leq_{M_n}$ que pertenece a $s(f) \cap I$. Como $u_0 \in I$, por la Proposición 3.1.5, existirá $w_0 \in M_n$ tal que

$$\frac{u_0}{\mathcal{L}(g_{i_0}, \leq_{M_n})} = w_0$$

$$\implies u_0 = w_0 \mathcal{L}(g_{i_0}, \leq_{M_n}), \tag{20}$$

para algún $\mathcal{L}(g_{i_0}, \leq_{M_n}) \in \{\mathcal{L}(g_1, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n})\}$. Sean c_0 y d_{i_0} los coeficientes de u_0 en f y $\mathcal{L}(g_{i_0}, \leq_{M_n})$ en g_{i_0}, respectivamente, esto es que

$$f = ... + c_0 u_0 + ... \tag{21}$$

$$g_{i_0} = d_{i_0} \mathcal{L}(g_{i_0}, \leq_{M_n}) + ... \tag{22}$$

Multiplicando (22) por $c_0 d_{i_0}^{-1} w_0$ y reemplazando (20) en la nueva ecuación se tendrán

$$f = ... + c_0 u_0 + ...$$

$$c_0 d_{i_0}^{-1} w_0 g_{i_0} = c_0 u_0 + ...$$

Defínase el polinomio

$$h_1 = f - c_0 d_{i_0}^{-1} w_0 g_{i_0}. \tag{23}$$

Luego

$$f = c_0 d_{i_0}^{-1} w_0 g_{i_0} + h_1. \tag{24}$$

Si:

  - $s(h_1) \cap I = \phi$. Por la Proposición 3.2.3.3 se tiene que

$$\mathcal{L}(w_0 g_{i_0}, \leq_{M_n}) = w_0 \mathcal{L}(g_{i_0}, \leq_{M_n}) = u_0 \leq_{M_n} \mathcal{L}(f, \leq_{M_n}).$$

    Haciendo $q_{i_0} = c_0 d_{i_0}^{-1} w_0, q_j = 0, \forall j \neq i_0$ y $r = h_1$, (24) es la forma estándar de f con respecto a $g_1, g_2, ..., g_m$ y h_1 es el residuo de f.

  - $s(h_1) \cap I \neq \phi$. Sea u_1 el mayor monomio respecto a $\leq_{M_n}$ entre los monomios pertenecientes a $s(h_1) \cap I$. Por la definición de h_1, $u_0 \notin s(h_1)$ y $u_1 \in s(f)$ o $u_1 \in s(w_0 g_{i_0})$. Si $u_1 \in s(f)$, entonces, por la elección de u_0, se tendrá que

$$u_1 <_{M_n} u_0.$$

Si $u_1 \in s(w_0 g_{i_0})$, entonces $u_1 \leq_{M_n} \mathcal{L}(w_0 g_{i_0}, \leq_{M_n}) = w_0 \mathcal{L}(g_{i_0}, \leq_{M_n}) = u_0$ y como $u_1 \neq u_0$,

$$u_1 <_{M_n} u_0.$$

A partir de esto se afirma que $u_1 <_{M_n} u_0$. Como $u_1 \in I = \langle \mathcal{L}(g_1, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n}) \rangle$, algún $\mathcal{L}(g_{i_1}, \leq_{M_n})$ dividirá a u_1, esto es que existe $w_1 \in M_n$ tal que

$$u_1 = w_1 \mathcal{L}(g_{i_1}, \leq_{M_n}).$$

Luego, se define el polinomio

$$h_2 = h_1 - c_1 d_{i_1}^{-1} w_1 g_{i_1}, \tag{25}$$

donde c_1 es el coeficiente de u_1 en h_1 y d_{i_1} el de $\mathcal{L}(g_{i_1}, \leq_{M_n})$ en g_{i_1}. Luego, reemplazando (23) en (25) y despejando f se tendrá que

$$f = c_0 d_{i_0}^{-1} w_0 g_{i_0} + c_1 d_{i_1}^{-1} w_1 g_{i_1} + h_2. \tag{26}$$

Si:

- $s(h_2) \cap I = \phi$. Nótese que

  $$\mathcal{L}(w_0 g_{i_0}, \leq_{M_n}) = w_0 \mathcal{L}(g_{i_0}, \leq_{M_n}) = u_0 \leq_{M_n} \mathcal{L}(f, \leq_{M_n}),$$
  $$\mathcal{L}(w_1 g_{i_1}, \leq_{M_n}) = w_1 \mathcal{L}(g_{i_1}, \leq_{M_n}) = u_1 \leq_{M_n} \mathcal{L}(f, \leq_{M_n}),$$

  Haciendo $q_{i_0} = c_0 d_{i_0}^{-1} w_0$, $q_{i_1} = c_1 d_{i_1}^{-1} w_1$, $q_j = 0, \forall j \neq i_0, i_1$ y $r = h_2$, (26) es la forma estandar de f con respecto a $g_1, g_2, ..., g_m$ y h_2 es el residuo de f.

- $s(h_2) \cap I \neq \phi$. Se continua con el mismo proceso y se obtiene una secuencia

  $$u_0 \ _{M_n} > \ u_1 \ _{M_n} > u_2 \ _{M_n} > ...,$$

  que terminará en algún monomio u_M por la Proposición 3.2.3.2; y se obtendrá la expresión

  $$f = \sum_{j=0}^{M-1} c_j d_{i_j}^{-1} w_j g_{i_j} + h_M, \tag{27}$$

  donde $s(h_M) \cap I = \phi$ y además

  $$\mathcal{L}(w_0 g_{i_0}, \leq_{M_n}) \leq_{M_n} \mathcal{L}(f, \leq_{M_n}),$$
  $$\vdots \qquad \leq_{M_n} \qquad \vdots \quad ,$$
  $$\mathcal{L}(w_{M-1} g_{i_{M-1}}, \leq_{M_n}) \leq_{M_n} \mathcal{L}(f, \leq_{M_n}).$$

Tomando $q_{i_j} = c_j d_{i_j}^{-1} w_j, \forall j = 1, ..., M-1$, $q_j = 0, \forall j \neq i_j$, $j = 1, ..., M-1$ y $r = h_M$, se tiene que (27) es la forma estandar de f respecto a $g_1, g_2, ..., g_m$ y h_M es su residuo. ■

Proposición 3.3.2.2. Sea I un ideal de S_n y $\{g_1, g_2, ..., g_m\}$ una base de Gröbner I respecto a un orden monomial $\leq_{M_n}$ dado. Un polinomio no nulo f de S_n tiene un único resto respecto a $g_1, g_2, ..., g_m$ (Herzog *e*t al., 2018).

Demostración.

Sea un polinomio no nulo $f \in I = \langle g_1, g_2, ..., g_m \rangle$, donde $\{g_1, g_2, ..., g_m\}$ es una base de Gröbner de I respecto al orden monomial $\leq_{M_n}$. Supóngase que el resto de f respecto a $g_1, g_2, ..., g_m$ no es único. Sean r y r' dos restos distintos de f respecto a $g_1, g_2, ..., g_m$; es decir

$$f = q_1 g_1 + q_2 g_2 + ... + q_m g_m + r, \tag{28}$$

$$f = q_1' g_1 + q_2' g_2 + ... + q_m' g_m + r'. \tag{29}$$

Defínase $q_i'' = -(q_i - q_i') \in S_n$, $\forall i = 1, 2, ..., m$. Haciendo la diferencia de (28) y (29) se obtiene que

$$q_1'' g_1 + q_2'' g_2 + ... + q_m'' g_m = r - r'.$$

De la última ecuación se deduce que $r - r' \in I$. Como $r - r'$ es no nulo, $\mathcal{L}(r - r', \leq_{M_n}) \in \mathcal{L}(I, \leq_{M_n})$. Nótese que $\mathcal{L}(r - r', \leq_{M_n}) \in s(r) \cup s(r')$. Por el algoritmo de la división se sigue que

$$\mathcal{L}(r - r', \leq_{M_n}) \notin \langle \mathcal{L}(g_1, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n}) \rangle,$$

pero como $\mathcal{L}(I, \leq_{M_n}) = \langle \mathcal{L}(g_1, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n}) \rangle$, se llega a una contradicción. Por lo tanto, el resto de f respecto a $g_1, g_2, ..., g_m$ es único. ■

Proposición 3.3.2.3. Sea $\{g_1, g_2, ..., g_m\}$ una base de Gröbner del ideal I de S_n respecto a un orden monomial $\leq_{M_n}$ dado. Un polinomio no nulo f de S_n pertenece a $I = \langle g_1, g_2, ..., g_m \rangle$ si, y solo si, el resto de f respecto a $g_1, g_2, ..., g_m$ es 0 (Ene y Herzog, 2011).

Demostración.

Sea f un polinomio no nulo de $I = \langle g_1, g_2, ..., g_m \rangle$ y considérese

$$f = q_1 g_1 + q_2 g_2 + ... + q_m g_m + r,$$

la forma estándar de f respecto a $g_1, g_2, ..., g_m$. Supóngase que en la expresión estándar de f respecto a $g_1, g_2, ..., g_m$, el residuo r no es 0. Luego

$$r = f - \sum_{i=1}^{m} q_i g_i.$$

Como $f \in I$, $r \in I$; y además $\mathcal{L}(r, \leq_{M_n}) \in \mathcal{L}(I, \leq_{M_n})$, ya que $r \neq 0$. Pero como $\mathcal{L}(r, \leq_{M_n}) \in s(r)$, se tendrá que $\mathcal{L}(r, \leq_{M_n}) \notin \mathcal{L}(I, \leq_{M_n})$ por el algoritmo de la división, lo que es una contradicción. Por lo tanto el resto r de f respecto a $g_1, g_2, ..., g_m$ es 0.

Para mostrar la recíproca, supóngase que el residuo r es nulo. Luego, se tiene que

$$f = \sum_{i=1}^{m} q_i g_i,$$

donde $q_i \in S_n$; esto implica que $f \in I = \langle g_1, g_2, ..., g_m \rangle$. ■

3.3.3. Bases de Gröbner reducidas

Definición 3.3.3.1 (Base de Gröbner reducida). Sea I un ideal y $\leq_{M_n}$ un orden monomial en S_n. Una base de Gröbner $\{g_1, g_2, ..., g_m\}$ del ideal I es *reducida* respecto a $\leq$ si verifica que

1. el coeficiente principal de cada g_i es 1, para cada $i = 1, 2, ..., n$,
2. si $g_i \neq g_j$, $\mathcal{L}(g_i, \leq_{M_n})$ no divide a ningún monomio de $s(g_j)$

(Ene y Herzog, 2011).

Proposición 3.3.3.1. Para cada ideal I de S_n existe una única base de Gröbner reducida respecto a un orden monomial dado (Ene y Herzog, 2011).

Demostración.

Existencia. Dado un orden monomial $\leq_{M_n}$ en S_n, por la Proposición 3.3.1.1, para un ideal arbitrario I de S_n existe una base de Gröbner mínima respecto a $\leq_{M_n}$, sea esta $\{g_1, g_2, ..., g_m\}$. Por la definición de base de Gröbner mínima, el conjunto

$$\{\mathcal{L}(g_1, \leq_{M_n}), \mathcal{L}(g_2, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n})\}$$

es el sistema de monomios generadores mínimo de $\mathcal{L}(I, \leq_{M_n})$, que es único por la Proposición 3.1.6, lo que implica que los elementos $\mathcal{L}(g_i, \leq_{M_n})$, $i = 1, 2, ..., m$, son minimales; es decir, que no se pueden dividir entre ellos.

Sea r_1 el residuo de dividir g_1 respecto a $g_2, g_3, ..., g_m$, es decir que

$$g_1 = q_{1_1} g_2 + q_{1_2} g_3 + ... + q_{1_{m-1}} g_m + r_1,$$

donde $q_{1_i} \in S_n$, $\forall i = 1, ..., m-1$. Nótese que $r_1 \in I$. Como $\mathcal{L}(g_1, \leq_{M_n})$ no puede ser dividido por algún $\mathcal{L}(g_j, \leq_{M_n})$, $j = 2, ..., m$, necesariamente

$$\mathcal{L}(g_1, \leq_{M_n}) \in s(r_1);$$

y esto último implica que $\mathcal{L}(g_1, \leq_{M_n}) = \mathcal{L}(r_1, \leq_{M_n})$. Luego, $\{r_1, g_2, ..., g_m\}$ es una base de Grobner mínima de I con respecto a $\leq_{M_n}$. Como $\mathcal{L}(r_1, \leq_{M_n})$ es el mayor de todos los monomios de $s(r_1)$ respecto a $\leq_{M_n}$, no puede ser dividido por algún $\mathcal{L}(g_j, \leq_{M_n})$, $j = 2, ..., m$; ningún monomio de $s(r_1)$ podrá ser dividido por algún $\mathcal{L}(g_j, \leq_{M_n})$, $j = 2, ..., m$.

Sea r_2 el resto de dividir g_2 respecto a $r_1, g_3, ..., g_m$, es decir que

$$g_2 = q_{2_1} r_1 + q_{2_2} g_3 + ... + q_{2_{m-1}} g_m + r_2,$$

donde $q_{2_i} \in S_n$, $\forall i = 1, ..., m-1$. Nótese también que $r_2 \in I$. Como $\{r_1, g_2, ..., g_m\}$ es una base de Grobner mínima de I, se tendrá que $\mathcal{L}(g_2, \leq_{M_n})$ no puede ser dividido ni por $\mathcal{L}(r_1, \leq_{M_n})$ ni por algún $\mathcal{L}(g_j, \leq_{M_n})$, $j = 3, ..., m$; esto implica que necesariamente $\mathcal{L}(g_2, \leq_{M_n}) = \mathcal{L}(r_2, \leq_{M_n})$. Luego, $\{r_1, r_2, g_3, ..., g_m\}$ es una base de Gröbner mínima de I respecto a $\leq_{M_n}$. Análogamente a r_1 y r_2, se definen los polinomios $r_3, r_4, ..., r_m$ para $g_3, g_4, ..., g_m$, respectivamente; y se obtiene que $\{r_1, r_2, ..., r_m\}$ es una base de Gröbner mínima de I respecto a $\leq_{M_n}$ que cumple con la propiedad de que si $r_i \neq r_j$, entonces $\mathcal{L}(r_i, \leq_{M_n})$ no divide a ningún monomio de $s(r_j)$. Además, se tendrá que el coeficiente principal de cada r_i también es 1, $\forall i = 1, ..., m$; ya que el coeficiente principal de cada g_i es 1, $\forall i = 1, ..., m$ pues $\{g_1, g_2, ..., g_m\}$ es una base de Gröbner mínima de I respecto a $\leq_{M_n}$, y $\mathcal{L}(g_i, \leq_{M_n}) = \mathcal{L}(r_i, \leq_{M_n})$, $\forall i = 1, ..., m$. Esto muestra que $\{r_1, r_2, ..., r_m\}$ es una base de Gröbner reducida de I respecto a $\leq$. Así se prueba la existencia de una base de Gröbner reducida de un ideal I de S_n respecto a un orden monomial dado.

Unicidad. Ahora, supóngase los conjuntos

$$\{g_1, g_2, ..., g_m\} \quad \text{y} \quad \{h_1, h_2, ..., h_n\}$$

son dos bases de Gröbner reducidas para el ideal I de S_n respecto a $\leq_{M_n}$. Por la definición de base de Gröbner reducida se tendrá que para $g_i \neq g_j$, $\mathcal{L}(g_i, \leq_{M_n})$ no divide a ningún monomio de $s(g_j)$, en

particular para $j \neq i$, $\mathcal{L}(g_i, \leq_{M_n})$ no divide a ningún $\mathcal{L}(g_j, \leq_{M_n})$. Análogamente, para $j \neq i$, se muestra que $\mathcal{L}(h_i, \leq_{M_n})$ no divide a ningún $\mathcal{L}(h_j, \leq_{M_n})$. Luego,

$$\{\mathcal{L}(g_1, \leq_{M_n}), \mathcal{L}(g_2, \leq_{M_n}), ..., \mathcal{L}(g_m, \leq_{M_n})\} \quad \text{y} \quad \{\mathcal{L}(h_1, \leq_{M_n}), \mathcal{L}(h_2, \leq_{M_n}), ..., \mathcal{L}(h_n, \leq_{M_n})\}$$

son sistemas de monomios generadores mínimos de $\mathcal{L}(I, \leq_{M_n})$. Por la Proposición 3.1.6, los cardinales de ambos sistemas de monomios generadores son iguales $(m = n)$ y los índices se reordenarán tal que $\mathcal{L}(g_i, \leq_{M_n}) = \mathcal{L}(h_i, \leq_{M_n})$, $\forall i = 1, ..., m$. Supóngase que $g_i - h_i \neq 0$. Nótese que

$$\mathcal{L}(g_i - h_i, \leq_{M_n}) \leq_{M_n} \mathcal{L}(g_i, \leq_{M_n}) \quad \text{y} \quad \mathcal{L}(g_i - h_i, \leq_{M_n}) \in s(g_i) \cup s(h_i).$$

Luego, ningún $\mathcal{L}(g_j, \leq_{M_n})$ dividirá a $\mathcal{L}(g_i - h_i, \leq_{M_n})$, $j \neq i$, esto implica que $\mathcal{L}(g_i - h_i, \leq_{M_n}) \notin \mathcal{L}(I, \leq_{M_n})$; lo que contradice que $g_i - h_i \in I$. Luego, $g_i = h_i$, para $\forall i = 1, ..., m(= n)$; es decir, las bases $\{g_1, g_2, ..., g_m\}$ y $\{h_1, h_2, ..., h_n\}$ son iguales. Esto muestra que para un ideal I de S_n solo existe una base de Gröbner reducida respecto a un orden monomial dado. ■

Conclusiones

1. Gracias al lema de Dickson, en un subconjunto no vacío de monomios en n variables se puede encontrar una cantidad finita de monomios minimales, lo que garantiza la existencia de estos. En particular, para el ideal líder de un ideal I del anillo de polinomios se puede encontrar un sistema de monomios generadores finito, los cuales son minimales; estos minimales a su vez son líderes de ciertos polinomios de I, dichos polinomios conforman una base de Gröbner de I, lo que garantiza la existencia de una base de Gröbner para cualquier ideal I del anillo de polinomios.

2. Se mostró que el orden lexicográfico y el orden lexicográfico inverso verifican las condiciones de orden monomial en S_n. Así que siempre es posible encontrar por lo menos un orden monomial en S_n.

Referencias

Alcántara, D. (2023). *Bases de gröbner*. [Tesis de pregrado, Universidad de Cantabria].

Bances, R., Sánchez Gutiérrez, R. W., Luna Valenzuela, M., González Ulloa, M., Medina García de Correa, N. S., y Kong Wong, M. (2014). *Algunas aplicaciones de las bases de gröbner*. Pontificia Universidad Católica del Perú. Departamento de Ciencias.

Chambi, J. (2010). *Teorema de las bases de gröbner*. [Tesis de pregrado, Universidad Mayor de San Andrés].

Diniz, P. (2020). *Introdução as bases de gröbner*. [Tesis de pregrado, Universidade Federal de Uberlândia].

Ene, V., y Herzog, J. (2011). *Gröbner bases in commutative algebra*. American Mathematical Soc.

Escudeiro, M. (2023). *Um primeiro contato com bases de gröbner e suas aplicações*. Sociedade Brasileira de Matemática: SBM.

Flores, L. (2021). *Bases de gröbner y su aplicación en la solución de sistemas polinomiales*. [Tesis de pregrado, Universidad Nacional del Altiplano].

García de la Cruz García, J. (2020). *Bases de gröbner y aplicaciones*. [Tesis de pregrado, Universidad Politécnica de Madrid].

Gimenez, P. (2013). *Una introducción a las bases de gröbner y algunas de sus aplicaciones*. Pontificia Universidad Católica del Perú. Fondo editorial.

Hernández, R., Fernández, C., y Baptista, P. (2018). *Metodología de la investigación*. McGraw Hill.

Herstein, I. (1988). *Álgebra moderna*. Editorial Trillas México.

Herzog, J., Hibi, T., y Ohsugi, H. (2018). *Binomial ideals*. Springer.

Lazo, S. (1992). *Álgebra moderna*. SOCIEDAD IMPRESORA DE PAPELES LIMITADA.

Marca, G. (2008). *Bases de gröbner y aplicaciones*. [Tesis de pregrado, Universidad Nacional de Ingeniería].

Marcavillaca, E. (2019). *Solución del sudoku: Utilizando bases de gröbner*. [Tesis de pregrado, Universidad Nacional de San Antonio Abad del Cusco].

Munkres, J. (1971). *Topology*. Prentice Hall.

Sola, V. (2019). *Introducción a bases estándar y algunas aplicaciones*. [Tesis de pregrado, Universidad de El Salvador].