



**UNIVERSIDAD PEDAGOGICA
NACIONAL**

Educadora de educadores

ESTUDIO DE BASES DE GRÖBNER Y ALGUNAS APLICACIONES BÁSICAS

Daniel Eduardo Silva Amazo

Universidad Pedagógica Nacional

Facultad de Ciencia y Tecnología

Licenciatura en Matemáticas

Bogotá

2024

ESTUDIO DE BASES DE GRÖBNER Y ALGUNAS APLICACIONES BÁSICAS

Daniel Eduardo Silva Amazo

Trabajo de grado presentado como
requisito para optar por el título de
Licenciado en Matemáticas

Asesor:

José Leonardo Ángel Bautista

Prof. Departamento de Matemáticas UPN

UNIVERSIDAD PEDAGÓGICA
NACIONAL

Educa Universidad Pedagógica Nacional *adores*

Facultad de Ciencias y Tecnología

Licenciatura en Matemáticas

Bogotá

2024

Agradecimientos

Quiero agradecerte Nataly por acompañarme en todo este camino y apoyarme en los momentos que más lo requerí. También agradezco a Leonardo Ángel, mi asesor, por la paciencia para guiarme, aconsejarme y corregirme las veces que fue necesario. Por último dedico este trabajo a mi hija Paula por ser la motivación que me mantiene en pie cada día para seguir luchando por mis sueños, con esto quiero demostrarte que los sueños se cumplen y hay que trabajar duro por ellos.

UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

Resumen

Una cuestión interesante al estudiar ideales de un anillo de polinomios, sobre un anillo específico, consiste en determinar un conjunto de generadores para tal ideal. En el caso univariable se conoce que todo ideal es principal (como consecuencia del algoritmo de la división); sin embargo, en el caso multivariable, aunque no existe un único camino para abordar el problema, las bases de Gröbner se constituyen en una respuesta útil para abordar otros asuntos. Particularmente, las bases de Gröbner se distinguen como un conjunto especial de generadores que poseen la propiedad de que el término principal de cualquier polinomio en el ideal es divisible por el término principal de al menos uno de los polinomios que conforman dicha base.

En este trabajo se reconstruyen algunos de los elementos que conforman la teoría de bases de Gröbner partiendo de estructuras algebraicas iniciales como lo son los grupos y anillos. Posteriormente, se resalta la utilidad de estas mediante el estudio de algunas de sus aplicaciones como el determinar si un polinomio del anillo pertenece al ideal (Ideal membership), problemas de optimización, el k -coloreado de grafos, la resolución de sudokus y aplicaciones en la criptografía.

Adicionalmente, en los últimos capítulos del trabajo se muestra cómo el uso de software de cálculo simbólico como CoCoA, Singular, Wolfram Mathematica e inteligencia artificial como ChatGPT y Julius AI se constituye en una herramienta eficiente para encontrar una base de Gröbner o en la construcción de algoritmos que lo permitan.

Finalmente, se resalta que este trabajo es producto de una reconstrucción de parte de la teoría existente que se alimenta de ejemplos nuevos y una reflexión sobre la necesidad de incluir ciertos objetos en el estudio. En tal sentido, se enfatiza en que este trabajo no es exhaustivo en relación con el tema y pretende constituirse en un documento de referencia para quien quiera iniciar un estudio al respecto.

Palabras claves

Base de Groebner, anillo de polinomios, ideal

UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

Tabla de Contenido

1. Introducción	2
2. Algunos conceptos previos	10
2.1. Grupos	10
2.1.1. Subgrupos	24
2.2. Anillos	33
2.2.1. Subanillos	38
2.2.2. Ideales	39
2.2.3. Factorización de elementos en un anillo	57
2.3. Polinomios	61
2.3.1. Ideales en $(F[x], +, \cdot)$	76
2.3.2. Polinomios en varias variables	80
2.4. Ideales en $A[x_1, x_2, \dots, x_n]$	101
3. Bases de Gröbner	104
3.1. Base de Gröbner definición y caracterización.	104

3.2. S-polinomios y el algoritmo de Buchberger	113
3.3. Bases de Gröbner reducidas	126
4. Uso de IA y software especializado	130
4.1. CoCoA	130
4.2. Singular	135
4.3. ChatGPT	137
4.4. Julius	139
5. Algunas aplicaciones	142
5.1. Uso de bases de Gröbner en problemas de optimización	142
5.2. El problema k -coloreado	151
5.3. Criptografía (Polly Cracker)	167
6. Conclusiones	172
Referencias	176

UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

Tabla de figuras

2.1. Cuadrado base	17
2.2. Rotación ρ_2	18
2.3. Rectas de reflexión	18
2.4. Reflexión con respecto a la recta m_3	19
2.5. rotación de 180° y reflexión respecto a μ_1	19
4.1. Ejemplo anillo cociente en CoCoA	131
4.2. Arimética de polinomios en CoCoA	131
4.3. Algoritmo de la división CoCoA un solo divisor	132
4.4. Algoritmo de la división CoCoA varios divisores	133
4.5. Ejemplo base de Gröbner en CoCoA	134
4.6. Ejemplo orden de términos en CoCoA	134
4.7. Ejemplo cálculo de una base de Gröbner en SINGULAR	136
4.8. Interacción con Julius AI	140
5.1. Ejemplo cálculo de una base de Gröbner en intersección de una esfera y un plano.	143

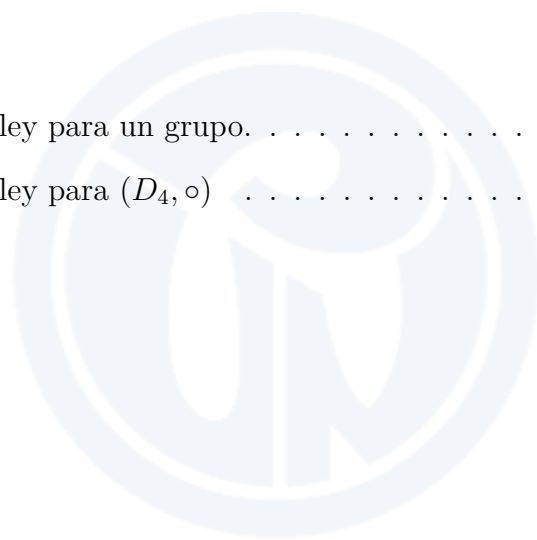
5.2. Sistema de ecuaciones	150
5.3. Grafo de seis vértices	152
5.4. Grafo dos colores, solución	152
5.5. Grafo enumeración de vértices	153
5.6. Grafo no 2-coloreable	155
5.7. Grafo de n vértices	156
5.8. Grafo con un subgrafo cíclico	158
5.9. Ejemplo grafo de 8 vértices	159
5.10. Ejemplo grafo 3-coloreado	161
5.11. Grafo no 3-coloreable	161
5.12. Shidoku	162
5.13. Shidoku Solución	164
5.14. Uso de Wolfram Mathematica para encontrar una base de Gröbner	165
5.15. Uso de chatGPT para enlistar polinomios	166
5.16. Intersección	171

UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

Índice de tablas

2.1. Tabla de Cayley para un grupo.	12
2.2. Tabla de Cayley para (D_4, \circ)	20



UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

Introducción

La necesidad de extender el algoritmo de la división estudiado en un anillo de polinomios en una variable con coeficientes en un anillo, a un anillo de polinomios en varias variables se constituye en una motivación para estudiar la teoría de bases de Gröbner. Particularmente, debido a que en el caso multivariado no existe una forma canónica de ordenar los términos de un polinomio conduciendo a que existan diferentes cocientes y residuos para una misma división. Ahora bien, en el caso de anillos de polinomios en una variable establecer si un polinomio p es divisible por otro q es equivalente a determinar si p pertenece al ideal generado por q ; siguiendo esta idea, bajo la teoría de bases de Gröbner es posible encontrar una base para un ideal de un anillo de polinomios en varias variables, cuyas características permiten establecer de una manera eficiente si un polinomio del anillo pertenece al ideal, de forma similar a como en álgebra lineal se determinan bases especiales para los espacios vectoriales.

Además de sus aplicaciones directas al estudio de los ideales en anillos de polinomios, las bases de Gröbner también son utilizadas para resolver problemas en otras ramas de las matemáticas como la teoría de grafos, optimización, criptografía,

entre otros, ya que es posible crear algoritmos que pueden ser implementados en diferentes lenguajes de programación una vez se haya modelado el problema en el lenguaje de la teoría de anillos.

Específicamente, el propósito de este documento consiste en describir de una manera más detallada las consideraciones a tener en cuenta en el algoritmo de la división en polinomios en varias variables y cómo estas conducen al problema del **ideal membership** (pertenencia a un ideal). En este punto se hace necesario aclarar que a lo largo de este trabajo sólo se consideraron los anillos conmutativos con identidad y en el caso particular de los anillos de polinomios, se estudió aquellos cuyos coeficientes pertenecen a anillos Noetherianos.

Posteriormente, se parte de la teoría de bases de Gröbner, mostrando ejemplos y contraejemplos, ideas claves, identificando resultados y pruebas para algunos teoremas que lo sustentan, esto con el objetivo de dar solución a este problema de pertenencia. Además, se estudia uno de los algoritmos para la construcción de bases de Gröbner y se utilizan algunas tecnologías digitales como CoCoA, Singular e inteligencia artificial (IA) para implementar tal algoritmo y resolver algunos problemas de aplicación relacionados con el problema de coloración de Grafos, resolución de Sudokus, Sistema de encriptación Barkee y Polly Cracker. De este modo, el trabajo está dividido en cuatro capítulos de la siguiente manera:

En el **primero** de ellos, se lleva a cabo una revisión exhaustiva de los conceptos fundamentales del álgebra abstracta, tales como grupos, anillos, subanillos e ideales, los cuales son esenciales para el desarrollo posterior del estudio. Se incluyen

resultados importantes, como el hecho de que si H es un subgrupo normal de un grupo $(G, *)$, entonces el conjunto cociente G/H forma un grupo. De manera análoga, en el contexto de anillos e ideales, si I es un ideal de un anillo cualquiera $(A, +, \cdot)$, el cociente A/I , con la operación de suma heredada, puede extenderse de forma natural para dotarlo de una estructura de anillo. Asimismo, se aborda un análisis formal de los polinomios en una variable, con especial énfasis en el algoritmo de la división y en el comportamiento de los ideales dentro de un anillo de polinomios.

Este análisis sirve de base para destacar la necesidad de introducir un orden sobre los términos de los polinomios puesto que garantizar que el cociente y el residuo sean únicos en el algoritmo de la división no es trivial en el contexto multivariable. La definición de un orden adecuado sobre los términos es, por tanto, crucial para extender los algoritmos algebraicos tradicionales a dominios más complejos y es un elemento fundamental en el desarrollo de las bases de Gröbner.

El **segundo** capítulo está dedicado al estudio detallado de las bases de Gröbner, abordando tanto su teoría fundamental como los procedimientos algorítmicos que permiten su cálculo. Se presentan resultados clave, tales como el hecho de que todo ideal I no nulo en el anillo de polinomios conmutativo $(A[X], +, \cdot)$ posee una base de Gröbner. Este resultado es esencial, ya que garantiza la existencia de un conjunto finito de generadores que permite resolver varios problemas algebraicos.

Asimismo, se expone en profundidad el algoritmo de Buchberger, una de las herramientas más importantes en la teoría de las bases de Gröbner. Este algoritmo se basa en la construcción de los denominados S -polinomios, los cuales se utilizan

iterativamente para refinar un conjunto generador de un ideal hasta convertirlo en una base de Gröbner. Además, se incluye la definición de base de Gröbner reducida, un concepto que implica que los coeficientes de los términos principales de los polinomios generadores son 1, y se discuten los pasos necesarios para obtenerla. Estos resultados constituyen el núcleo teórico para la resolución de sistemas de ecuaciones polinomiales y otros problemas computacionales en álgebra conmutativa.

El **tercer** capítulo se centra en la aplicación de software y algoritmos de inteligencia artificial para el cálculo de bases de Gröbner, destacando las ventajas que ofrece el uso de estas herramientas en comparación con los métodos manuales. Se examinan diversas plataformas de software matemático, como CoCoA, Singular y Mathematica, que permiten no solo la obtención eficiente de bases de Gröbner, sino también la resolución de problemas complejos en álgebra conmutativa y geometría algebraica mediante su implementación.

A lo largo del capítulo, se muestran ejemplos prácticos que evidencian cómo el uso de software optimiza el proceso de cálculo y permite manejar sistemas de ecuaciones polinomiales con múltiples variables de forma más ágil. Además, se discuten las contribuciones recientes en el ámbito de la inteligencia artificial, la cual, a través de algoritmos de optimización y aprendizaje automático, está comenzando a tener un impacto significativo en la mejora de la eficiencia de los cálculos algorítmicos, tanto en el contexto de las bases de Gröbner como en otros dominios matemáticos.

En definitiva, este capítulo demuestra cómo la combinación de herramientas computacionales y avances en IA facilita no solo la resolución de problemas abstrac-

tos, sino también la aplicación directa de estos conceptos a situaciones prácticas y de gran envergadura en diversas áreas de la ciencia y la ingeniería.

El **cuarto** y último capítulo se enfoca en ilustrar las aplicaciones de la teoría de bases de Gröbner en diversos campos de las matemáticas y otras áreas afines. En primer lugar, se aborda el problema del k -coloreado y se establece un paralelismo con la resolución de Sudokus, mostrando cómo las bases de Gröbner permiten modelar y resolver problemas de este tipo mediante sistemas de ecuaciones polinomiales. A lo largo del capítulo, se ejemplifica la practicidad de las bases de Gröbner en la resolución eficiente de sistemas algebraicos no lineales, optimización y criptografía, destacando su relevancia en áreas como la teoría de códigos y los sistemas de seguridad criptográficos.

Esta sección resalta la versatilidad y poder de las bases de Gröbner, que no solo encuentran aplicaciones teóricas en el álgebra conmutativa y la geometría algebraica, sino también en problemas computacionales y prácticos, brindando soluciones eficientes a desafíos complejos en distintas disciplinas.

UNIVERSIDAD PEDAGÓGICA
NACIONAL

Educadora de educadores

Justificación

Uno de los grandes problemas que existe en matemáticas consiste en establecer métodos que permitan solucionar ecuaciones o sistemas de ecuaciones polinómicas en diferentes estructuras. Sin embargo, para lograr tal objetivo no es suficiente con entender las expresiones algebraicas inmersas en los sistemas de ecuaciones, sino que es necesario ahondar en el estudio de la estructura sobre la que se trabaja para poder identificar propiedades de la estructura, relaciones entre diferentes objetos del álgebra para así lograr proponer métodos que sean apropiados, eficientes y efectivos. Por ejemplo, cuando estudiamos sistemas de ecuaciones lineales se identifica la necesidad de reconocer la noción de sistemas equivalentes, vectores independientes o dependientes (en un espacio vectorial determinado) o espacios solución, llegando así a establecer métodos o algoritmos de solución como la eliminación Gaussiana, la factorización de matrices, la regla de Cramer, entre otros objetos y conceptos del álgebra.

Particularmente, bajo la propuesta curricular de los primeros cursos de álgebra en la Universidad, se observa que no se propone el estudio de muchas herramientas

que permitan abordar la solución de ecuaciones o sistemas de ecuaciones no lineales, con varias variables o con muchas ecuaciones. Bajo esta perspectiva, surge el interés de ahondar en el estudio de teorías u objetos del álgebra que permitan complementar el acervo de conocimientos al respecto. En tal sentido, con base en la experiencia vivida en cursos como teoría de grupos y en diferentes conversaciones desarrolladas con integrantes del grupo de álgebra, se considera la posibilidad y pertinencia de estudiar parte de la teoría de anillos de polinomios en varias variables, de determinar relaciones entre sistemas de ecuaciones polinomiales e ideales y de abordar teorías como la de bases de Gröbner para buscar formas equivalentes de solucionar los sistemas mencionados.

A partir de una consulta preliminar sobre bases de Gröbner se observa que tal teoría, parte de diferentes algoritmos para construir bases más simples para el ideal de un anillo de polinomios, contribuye a construir un escenario bajo el cual la solución de sistemas de ecuaciones se puede abordar de una forma más estructurada, simple e incluso admitiendo el uso de programas que reducen el número o complejidad de los cálculos a desarrollar. Por otro lado, también se observa su utilidad para abordar problemas aplicados, por ejemplo, de teoría de grafos, optimización o criptografía.

Por otro lado, se considera que un estudio de este tipo puede contribuir a fortalecer diferentes competencias de un futuro profesor de matemáticas, por ejemplo las relacionadas con procesos de indagación e investigación en matemáticas, de comunicación y redacción de un discurso, y claramente las relacionadas con el conocimiento disciplinar ya que se investigan y estudian conceptos u objetos de las matemáticas de manera formal y rigurosa.

Objetivos

Objetivo general

El presente trabajo tiene como objetivo estudiar algunos elementos de la teoría de bases de Groebner, abordando sus fundamentos y algunas de las posibles aplicaciones en los diversos campos de las matemáticas.

Objetivos específicos

- Estudiar un Algoritmo para encontrar una base de Groebner para el ideal generado por un conjunto finito de polinomios dado.
- Analizar una forma de implementar las bases de Groebner para solucionar sistemas de ecuaciones algebraicos.
- Estudiar algunas aplicaciones de las bases de Groebner en temas de geometría algebraica o matemática recreativa.

Algunos conceptos previos

2.1. Grupos

A partir del estudio de algunos sistemas numéricos, como los enteros, racionales y reales, se observa la aparición de una estructura algebraica común llamada grupo. Esta estructura está formada por un conjunto no vacío y una operación interna definida en él que satisface ciertas propiedades. Además, se resalta la importancia de esta estructura en el estudio posterior de otras estructuras como la de anillo, campo y espacio vectorial. A continuación, se presentan algunas definiciones y resultados (algunos con demostración) que serán empleados posteriormente. Si se desea profundizar en tales desarrollos, puede consultarse (Hungerford, 2012) o (Fraleigh, 2003).

Definición 2.1.1. Si G es un conjunto no vacío, una **operación binaria** sobre G , es una función $*$: $G \times G \rightarrow G$ que asocia a cada par (g_1, g_2) de $G \times G$ un elemento de G el cual denotaremos por $g_1 * g_2$.

Esta definición permite crear operaciones sobre conjuntos no sólo numéricos

sino más generales, surgiendo así lo que llamaremos una estructura algebraica.

Ejemplo 2.1.1. *A continuación se ilustran algunos ejemplos de operaciones binarias:*

- Sea $A = \{a, b\}$ y $G = \wp(A) = \{\emptyset, \{a\}, \{b\}, A\}$. La unión (\cup) y la intersección (\cap) de conjuntos son operaciones binarias sobre G .
- En $M_2(\mathbb{R})$, el conjunto de las matrices de tamaño 2×2 con entradas en \mathbb{R} , se define la operación $*$ como:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae & bf \\ cg & dh \end{pmatrix}$$

donde cada producto en las componentes se realiza en \mathbb{R} .

- Tomando $\mathbb{R}_n[x]$ como el conjunto de los polinomios de grado n en la indeterminada x y con coeficientes reales, la suma usual no es una operación binaria, ya que la suma de dos polinomios de grado n puede dar como resultado un polinomio de grado menor o igual que n . Sin embargo, la suma usual de polinomios si es una operación binaria sobre $\mathbb{R}_{\leq n}[x]$, el conjunto de polinomios de grado menor o igual a n .
- Si $F = \{f \mid f : \mathbb{R} \rightarrow \mathbb{R}\}$ denota el conjunto de las funciones con dominio \mathbb{R} y valor real, entonces la suma y producto definidas por:

$$(f + g)(x) := f(x) + g(x)$$

$$(f \cdot g)(x) := f(x) \cdot g(x)$$

para todo $x \in \mathbb{R}$.

- $a * b := a^2 + 2ab + b^2$ es una operación binaria sobre \mathbb{N} , \mathbb{Z} , \mathbb{Q} y \mathbb{R} . Aquí el signo $+$ denota la suma usual, ab denota el producto usual de a por b y a^2 es el producto de a consigo mismo.
- Si G es un conjunto finito, podemos describir una operación binaria sobre G escribiendo todos los valores de $g_1 * g_2$ en una tabla de Cayley¹ para la operación. Por ejemplo, si $G = \{a, b, c\}$ tenemos:

Tabla 2.1: Tabla de Cayley para un grupo.

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Aquí, para $g_1, g_2 \in G$, $g_1 * g_2$ es el elemento en la fila de g_1 y en la columna de g_2 , a modo de ejemplo, $b * c = a$.

Notación: De aquí en adelante la expresión $(G, *)$ representará una estructura algebraica conformada por un conjunto G y una operación binaria $*$ definida en él.

Dada una operación definida sobre un conjunto, existen propiedades que rigen su comportamiento (la forma de hacer cálculos) y permiten generar diferentes estructuras. A continuación, se menciona la definición de algunas propiedades clásicas:

¹Una tabla de Cayley es un arreglo rectangular que describe los resultados de la operación entre dos elementos de un grupo, fue introducida por Arthur Cayley en su artículo llamado *On The Theory of Groups, as depending on the symbolic equation $\theta^n = 1$* . (Fraleigh, 2003)

Definición 2.1.2. Considere la estructura $(G, *)$, se dice que:

i) $*$ es **asociativa** en G , si para todo $g_1, g_2, g_3 \in G$

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3.$$

ii) $*$ es **conmutativa** en G , si $g_1 * g_2 = g_2 * g_1$ para todo $g_1, g_2 \in G$

iii) Un elemento $e \in G$ es un **elemento neutro**² de G con respecto a la operación $*$, si para cualquier elemento a de G se tiene que $a * e = e * a = a$.

iv) Sea e un elemento neutro de $(G, *)$. Un elemento $a \in G$ es un elemento **invertible** de G con respecto a la operación $*$, si existe un elemento $a' \in G$ de tal manera que $a * a' = e = a' * a$. Al elemento a' se le llamará el **inverso** de a .

Ejemplo 2.1.2. Los siguientes ejemplos ilustran la definición anterior:

- Sobre \mathbb{N} la suma y producto usual son operaciones asociativas y conmutativas, 0 es el elemento neutro y no hay elemento invertible para algún $n \in \mathbb{N}$ con $n \neq 0$.
- En $(\mathbb{Z}, +)$ (suma usual), 0 es el elemento neutro de \mathbb{Z} con respecto a $+$, -1 es el inverso del elemento 1 y en general, para un elemento $a \in \mathbb{Z}, a \neq 0$, su inverso es $-a$ con respecto a $+$.

²Obsérvese que en esta definición el elemento neutro satisface la propiedad conmutativa, sin embargo, esto no es en general un requisito en algunas operaciones, es decir, existen propiedades que se suplen al comportamiento de una operación pero a un sólo lado y allí se hablará de elemento neutro a derecha o a izquierda, por ejemplo. En este documento no se trabajará con tales definiciones.

- Si sobre \mathbb{Z} definimos la operación binaria $*$ así:

$$a * b = ab + 1$$

Entonces $*$ no es asociativa, en efecto:

$$\begin{aligned}(a * b) * c &= (ab + 1) * c \\ &= (ab + 1)c + 1 \\ &= abc + c + 1\end{aligned}$$

Pero,

$$\begin{aligned}a * (b * c) &= a * (bc + 1) \\ &= a(bc + 1) + 1 \\ &= abc + a + 1\end{aligned}$$

- Todo número real distinto de cero es un elemento invertible bajo el producto y la suma usual.
- El producto usual de matrices no es conmutativo en $M_{m \times n}(\mathbb{R})$ (matrices de tamaño $n \times m$ con entradas en los reales).
- La operación binaria definida en la tabla de Cayley del ejemplo 1.1.1, es conmutativa, lo podemos verificar viendo que es simétrica con respecto a la diagonal principal.

El siguiente teorema brinda información relevante acerca de un conjunto sobre el cual se ha definido una operación binaria.

Teorema 2.1.1. *Dada $(G, *)$ con $*$ asociativa. Si existe un elemento identidad en G con respecto a $*$ entonces este elemento es único. Además, cada elemento invertible tiene un único inverso.*

Demostración. Sean e y e' identidades de G , entonces. $e' * e = e$ (e' es identidad) y $e' * e = e'$ (e es identidad) luego $e' = e$.

Sea u un elemento invertible en G con u' y u'' dos inversos de u , entonces:

$$u'u = e$$

$$(u'u)u'' = eu''$$

$$u'(uu'') = u''$$

$$u'e = u''$$

$$u' = u''$$

□

Las propiedades y resultados mencionados conducen al estudio de una estructura común en matemáticas y que puede ser relevante para el lector, la de grupo. Esta estructura está compuesta de un conjunto y una operación que satisface las propiedades que se mencionan a continuación.

Definición 2.1.3. *Decimos que $(G, *)$ es un grupo si:*

- i) $*$ es asociativa en G .
- ii) G tiene un elemento identidad con respecto a $*$.
- iii) Todo elemento $a \in G$ es invertible.

Si además $*$ es una operación conmutativa entonces decimos que $(G, *)$ es un **grupo abeliano** o **conmutativo**.

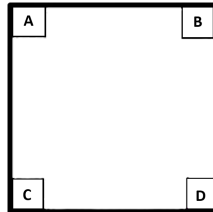
Bajo esta definición y considerando el **ejemplo 2.1.2** se afirma que $(\mathbb{Z}, +)$ es un grupo abeliano. Otros ejemplos de grupos son los siguientes:

Ejemplo 2.1.3. .

- $(\mathbb{R}, +)$, $(\mathbb{R} - \{0\}, \cdot)$, (\mathbb{Q}^+, \cdot) , $(\mathbb{Q}, +)$.
- $(M_n(\mathbb{R}), +)$, donde $M_n(\mathbb{R})$ representa el conjunto de matrices de tamaño $n \times n$ con coeficientes en \mathbb{R} y $+$ la suma usual de matrices (componente a componente).
- $(\mathbb{Z}_n, +_n)$, donde $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$ y $+_n$ es la suma modulo n .
- (D_n, \circ) , Grupo de simetrías un n -ágono regular, también llamado **Grupo diédrico**

Como caso particular el grupo (D_4, \circ) correspondiente a las simetrías de un cuadrado.

Sea el cuadrado de vértices $\{A, B, C, D\}$ tal como se muestra en la figura:

Figura 2.1: *Cuadrado base*

La posición inicial o base, que se muestra en la figura, servirá como punto de referencia para el análisis. A partir de esta disposición, se realizan dos tipos de movimientos: rotaciones en sentido contrario a las manecillas del reloj, identificadas por la letra ρ , y reflexiones, que se representarán con la letra μ .

Las rotaciones serán las siguientes:

ρ_0 : rotación de 0° .

ρ_1 : rotación de 90° .

ρ_2 : rotación de 180° .

ρ_3 : rotación de 270° .

Por ejemplo, si al cuadrado base se le aplica ρ_2 se obtendrá como resultado el cuadrado que se muestra a continuación:

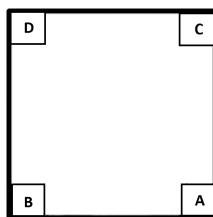


Figura 2.2: Rotación ρ_2

Por otro lado, si sobre el cuadrado base se trazan las rectas m_1, m_2, m_3 y m_4 como se muestra en la **figura 1.3**.

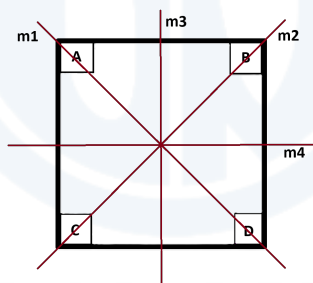


Figura 2.3: Rectas de reflexión

Podemos nombrar las siguientes reflexiones: *ducadores*

μ_1 reflexión con respecto a la recta m_1 .

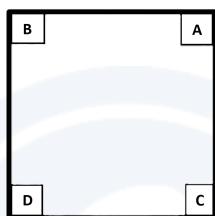
μ_2 reflexión con respecto a la recta m_2 .

μ_3 reflexión con respecto a la recta m_3 .

μ_4 reflexión con respecto a la recta m_4 .

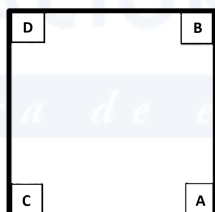
Aquí por ejemplo, al reflejar el cuadrado con respecto a la recta m_3 , es decir, aplicar sobre él la reflexión μ_3 se obtiene el cuadrado que se muestra en la figura 2.4.

Figura 2.4: Reflexión con respecto a la recta m_3



La expresión $\mu_i \circ \rho_j$ denotará que al cuadrado base se le aplicará primero ρ_j y seguidamente se aplicará la reflexión μ_i , por ejemplo, $\mu_1 \circ \rho_2$ significará que primero se rota el cuadrado base 180° y luego se refleja con respecto a la recta μ_1 obteniendo así el cuadrado de la figura 2.5:

Figura 2.5: rotación de 180° y reflexión respecto a μ_1



Observando el cuadrado resultante, se puede notar que se obtiene el mismo

resultado si al cuadrado base, se aplica μ_2 , esto quiere decir que $\mu_1 \circ \rho_2 = \mu_2$.

La tabla de Cayley para (D_4, \circ) es mostrada en la tabla 2.2.

Tabla 2.2: Tabla de Cayley para (D_4, \circ)

\circ	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	μ_3	μ_4
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	μ_3	μ_4
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	μ_3	μ_4	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	μ_4	μ_3
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	μ_4	μ_3	μ_1	μ_2
μ_1	μ_1	μ_4	μ_2	μ_3	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	μ_3	μ_1	μ_4	ρ_2	ρ_0	ρ_1	ρ_3
μ_3	μ_3	μ_1	μ_4	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
μ_4	μ_4	μ_2	μ_3	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

En esta tabla se pueden identificar cuatro grandes subconjuntos, a saber, si se aplica primero rotaciones y seguidamente rotaciones se obtiene como resultado una rotación. Por otro lado, si se aplica primero una reflexión y después una rotación o de forma contraria, si primero se rota el cuadrado y después se refleja, el resultado será una reflexión. Por último si se realiza una reflexión seguida de otra reflexión, se obtendrá una rotación.

- (S_n, \circ) , grupo de permutaciones de n elementos. En particular, si $n = 3$ se tiene el grupo (S_3, \circ) , en el cual $\sigma_0, \sigma_1, \sigma_2$ son las permutaciones definidas de la siguiente manera:

$$\sigma_i : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$$

tal que,

$$\begin{array}{lll} \sigma_0(1) = 1, & \sigma_1(1) = 2, & \sigma_2(1) = 3 \\ \sigma_0(2) = 2, & \sigma_1(2) = 3, & \sigma_2(2) = 1 \\ \sigma_0(3) = 3, & \sigma_1(3) = 1, & \sigma_2(3) = 2 \end{array}$$

Note que, $(\sigma_1 \circ \sigma_2)(1) = 1$, $(\sigma_1 \circ \sigma_2)(2) = 2$, $(\sigma_1 \circ \sigma_2)(3) = 3$, esto es, $\sigma_1 \circ \sigma_2 = \sigma_0$, de igual forma, $\sigma_2 \circ \sigma_1 = \sigma_0$, por lo tanto, $\sigma_1^{-1} = \sigma_2$ y $\sigma_2^{-1} = \sigma_1$.

Un resultado que quizá pueda parecer interesante al lector, es que las estructuras (S_3, \circ) y (D_3, \circ) , están definidas sobre conjuntos con tres elementos y las operaciones cumplen las mismas propiedades algebraicas en sus respectivas estructuras, esto significa que ellas son isomorfas³

Al estudiar estructuras algebraicas con una sola operación existen dos notaciones clásicas, una multiplicativa y una aditiva. Bajo la notación multiplicativa, en la estructura $(G, *)$, en lugar de escribir $a * b$ se escribe ab , y si un elemento a tiene inverso, este es denotado por a^{-1} . Por otro lado, en el caso de notación aditiva se expresa la operación como $a + b$ en lugar de ab y se denotará como $-a$ al elemento invertible de a .

³Dos estructuras son isomorfas si existe una función biyectiva f entre ellas que preserva las operaciones entre los objetos de cada estructura, es decir, $f(a * b) = f(a) *' f(b)$ donde $a, b \in (G, *)$ y $f(a), f(b) \in (G', *')$. Para más información se puede consultar (Hungerford, 2012) o (Saracino, 2008).

Esta distinción en la notación, ya sea multiplicativa o aditiva, facilita la comprensión y comunicación de las operaciones dentro del contexto algebraico en el que se trabaja.

Nota: De aquí en adelante se usará la notación multiplicativa cuando $*$ sea una operación binaria general o cuando se hable del producto sobre una estructura conocida.

Dicha notación multiplicativa nos permite definir las potencias de un elemento de un grupo, así:

Definición 2.1.4. Sea $(G, *)$ un grupo y $x \in G$, las potencias de x se definen como sigue:

$$i) x^0 = e.$$

$$ii) x^n = xxx \cdots x \text{ (} n \text{ factores) si } n > 0.$$

$$iii) x^{-n} = (x^{-1})^n = x^{-1}x^{-1}x^{-1} \cdots x^{-1}, \text{ si } n > 0.$$

De esta definición se sigue:

Teorema 2.1.2. Sea $(G, *)$ un grupo, $x \in G$ y $m, n \in \mathbb{Z}$, entonces:

$$i) x^m x^n = x^{m+n}.$$

$$ii) (x^n)^{-1} = x^{-n}.$$

$$iii) (x^m)^n = x^{mn} = (x^n)^m.$$

Demostración. .

i) Si m, n son ambos positivos, por la asociatividad de $*$ se tiene que:

$$x^m x^n = \underbrace{xxx \cdots x}_m \cdot \underbrace{xxx \cdots x}_n = \underbrace{xxx \cdots x}_{m+n} = x^{m+n}$$

Si m, n son ambos negativos, esto es, $m = -r$ y $n = -s$ con $r, s > 0$. Así por definición y por el caso anterior se sigue:

$$x^m x^n = x^{-r} x^{-s} = (x^{-1})^r (x^{-1})^s = (x^{-1})^{r+s} = x^{-(r+s)} = x^{-r-s} = x^{m+n}$$

Finalmente, si $m = -r < 0$ y $n > 0$ con $r > n$.

$$x^m x^n = x^{-r} x^n = (x^{-1})^r (x^{-1})^{-n} = (x^{-1})^{r-n} = x^{-(r-n)} = x^{-r+n} = x^{m+n}$$

ii) Note que $x^n x^{-n} = x^{n-n} = x^0 = e$ luego $(x^n)^{-1} = x^{-n}$.

iii)

$$(x^m)^n = \underbrace{x^m x^m x^m \cdots x^m}_n = x^{\overbrace{m + m + m + \cdots + m}^n} = x^{mn} = x^{nm} = (x^n)^m$$

Educadora de educadores

□

2.1.1. Subgrupos

En algunos de los ejemplos de grupos que han sido mencionados hasta ahora se hace evidente la existencia de una relación de contención, por ejemplo, $(\mathbb{Z}, +)$ está contenido en $(\mathbb{Q}, +)$ el cual a su vez está contenido en $(\mathbb{R}, +)$ haciendo las respectivas restricciones a la operación $+$. A estos grupos que están contenidos en otro grupo se les denominan subgrupos.

Definición 2.1.5. Sea $(G, *)$ un grupo y H un subconjunto no vacío de G que es cerrado⁴ bajo la operación $*$. Si $(H, *)$ es en sí mismo un grupo, entonces se dice que $(H, *)$ es un **subgrupo** de $(G, *)$. Por simplicidad, se denotará esta relación por $H \leq G$.

Antes de seguir ejemplificando subgrupos, un teorema que es muy útil para determinar si una subestructura es un subgrupo de un grupo dado, es el siguiente:

Teorema 2.1.3. Sea $(G, *)$ un grupo y H un subconjunto de G . $H \leq G$ si y sólo si:

- i) H es cerrado para $*$.
- ii) El elemento identidad de $(G, *)$ está en H .
- iii) para todo $a \in H$, $a^{-1} \in H$.

Ejemplo 2.1.4. Algunos ejemplos de subgrupos son los siguientes:

- Sea (\overline{F}, \cdot) el grupo de funciones reales no nulas con la operación de multiplicación definida en el **ejemplo 2.1.2**. Si \overline{C} denota el conjunto de todas las

⁴Cerrado en este contexto significa que para cualesquiera $a, b \in H$ se cumple que $a * b \in H$

funciones reales no nulas y continuas, entonces $\overline{C} \subseteq \overline{F}$.

- Sea $(G, *)$ un grupo y a un elemento fijo de G , consideremos el conjunto:

$$H_a = \{x \in G \mid ax = xa\}$$

- i) H_a es cerrado bajo la operación en G pues si $x_1, x_2 \in H_a$ entonces

y

$$ax_1 = x_1a$$

$$ax_2 = x_2a$$

luego,

$$\begin{aligned} a(x_1x_2) &= (ax_1)x_2 \\ &= (x_1a)x_2 \\ &= x_1(ax_2) \\ &= x_1(x_2a) \\ &= (x_1x_2)a \end{aligned}$$

esto implica que $x_1x_2 \in H_a$.

- ii) Por otro lado, si e es el elemento identidad de G entonces $ea = ae$ y por tanto $e \in H_a$.

iii) Finalmente, si $x \in H_a$ entonces:

$$ax = xa$$

$$x^{-1}(ax) = x^{-1}(xa)$$

$$(x^{-1}a)x = a$$

$$x^{-1}a(xx^{-1}) = ax^{-1}$$

$$x^{-1}a = ax^{-1}$$

Así $x^{-1} \in H_a$.

Por i), ii) y iii) podemos concluir entonces que H_a es un subgrupo de G .

- Del mismo modo que el ítem anterior, el conjunto

$$Z(G) = \{z \in G \mid zx = xz \text{ para todo } x \in G\}$$

forma un subgrupo con la operación binaria definida sobre G . Este subgrupo es llamado el **centro de G** y consiste en todos los elementos que conmutan con cualquier elemento de G . Además se tiene que $Z(G) \neq \emptyset$ pues el elemento identidad de G siempre pertenece al centro de G .

Otros resultados usados para caracterizar un subgrupo H de un grupo $(G, *)$ son los siguientes:

Teorema 2.1.4. Sea H un subconjunto no vacío de un grupo $(G, *)$. $H \leq G$ sí y sólo sí $ab^{-1} \in H$ para todo $a, b \in H$.

Demostración. (\Rightarrow) Es claro que si $H \leq G$ y $b \in H$ entonces $b^{-1} \in H$, al ser H cerrado bajo $*$ se tiene que $ab^{-1} \in H$ para todo $a \in H$.

(\Leftarrow) Como H no es vacío, entonces existe $a \in H$ y por tanto $aa^{-1} = e \in H$, esto implica que si $b \in H$ entonces $eb^{-1} = b^{-1} \in H$, así, si $a, b \in H$ se cumple que $a(b^{-1})^{-1} = ab \in H$. Se concluye entonces en virtud del **teorema 1.1.2** que $H \leq G$. □

Teorema 2.1.5. *Sea $(G, *)$ un grupo y $H \subseteq G$ finito y no vacío. Si H es cerrado para $*$ entonces $H \leq G$.*

Demostración. Suponga que $h \in H$, se quiere mostrar que $h^{-1} \in H$. Como H es cerrado, entonces todas las potencias de h están en H , esto es, $h^n \in H$ para todo $n \in \mathbb{Z}$ □

Ejemplo 2.1.5. *Los siguientes ejemplos buscan ilustrar el teorema anterior:*

- Sea $H \subset M_2(\mathbb{R})$ el conjunto de matrices de la forma $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ tales que $ac \neq 0$, entonces (H, \cdot) es un subgrupo de $(GL_2(\mathbb{R}), \cdot)$, el grupo de matrices invertibles de tamaño 2×2 con el producto usual. Lo anterior se da ya que:

$$ab^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} e & f \\ 0 & h \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} h & -f \\ 0 & e \end{pmatrix} = \begin{pmatrix} ah & -af + be \\ 0 & ce \end{pmatrix}$$

donde $he \neq 0$ puesto que $h \neq 0$ y $e \neq 0$. Así mismo $ah \neq 0$ y $ce \neq 0$ y por tanto, concluimos que $ab^{-1} \in H$

- La estructura $(2\mathbb{Z}_n = \{y \in \mathbb{Z}_n \mid y = 2x, x \in \mathbb{Z}_n\}, +_n)$ es un subgrupo de $(\mathbb{Z}_n, +_n)$. Sea $y \in 2\mathbb{Z}_n$. Por definición, existe $x \in \mathbb{Z}_n$ tal que $y = 2x$; así, si z es el inverso de x en \mathbb{Z}_n , se tiene que $2z \in 2\mathbb{Z}_n$ y $x + z \cong 0 \pmod{n}$. De lo anterior, $2x + 2z = 2(x + z) \cong 0 \pmod{n}$, por lo tanto $2z$ es el inverso de y en $2\mathbb{Z}_n$. Ahora, sea $y_1 = 2k \in 2\mathbb{Z}_n$ entonces $y_1 + 2z = 2k + 2z = 2(k + z) \in 2\mathbb{Z}_n$.
- $(U_n = \{z \in \mathbb{C} \mid z^n = 1\}, \cdot)$ es un subgrupo de (\mathbb{C}, \cdot) .

Demostración. Por el teorema de Euler y el teorema de Moivre se pueden escribir los elementos de U_n de la forma $z = \cos(m\frac{2\pi}{n}) + i\text{sen}(m\frac{2\pi}{n})$ donde $m = 0, 1, \dots, n-1$, luego U_n es finito, además es no vacío pues si $m = 0$, $1 = \cos(0) + i\text{sen}(0) \in U_n$. También es cerrado pues

$$\begin{aligned} z_1 z_2 &= \left[\cos\left(m_1 \frac{2\pi}{n}\right) + i\text{sen}\left(m_1 \frac{2\pi}{n}\right) \right] \left[\cos\left(m_2 \frac{2\pi}{n}\right) + i\text{sen}\left(m_2 \frac{2\pi}{n}\right) \right] \\ &= \cos\left((m_1 + m_2) \frac{2\pi}{n}\right) + i\text{sen}\left((m_1 + m_2) \frac{2\pi}{n}\right) \\ &= \cos\left(m_3 \frac{2\pi}{n}\right) + i\text{sen}\left(m_3 \frac{2\pi}{n}\right) \end{aligned}$$

donde $m_3 = m_1 + m_2$. Así U_n es cerrado para el producto y en virtud del teorema 2.1.5 $U_n \leq \mathbb{C}$. □

Si (G, \cdot) es un grupo y $H \leq G$, por el **teorema 2.1.4**, $ab^{-1} \in H$ para todo $a, b \in H$. Así, se puede definir una relación entre los elementos de G de la siguiente manera:

Si $a, b \in G$ se dice que $a \sim_R b$ si y sólo si $ab^{-1} \in H$

Teorema 2.1.6. *La relación \sim_R es una relación de equivalencia en G .*

Demostración. Se debe demostrar que \sim_R es reflexiva, simétrica y transitiva:

- Sea $a \in G$ como $H \leq G$, $aa^{-1} = e \in H$ y por lo tanto $a \sim_R a$.
- Si $a \sim_R b$ entonces $ab^{-1} \in H$, dado que $H \leq G$ entonces $(ab^{-1})^{-1} \in H$ pero $(ab^{-1})^{-1} = ba^{-1}$, así tenemos que $b \sim_R a$.
- Si $a \sim_R b$ y $b \sim_R c$ entonces $ab^{-1} \in H$ y $bc^{-1} \in H$, como H es cerrado bajo la multiplicación $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$, esto implica que $a \sim_R c$.

Las tres condiciones anteriores permiten concluir que \sim_R es una relación de equivalencia en G . □

Esta relación de equivalencia determina una partición G/\sim_R del grupo $(G, *)$, cuyos elementos se caracterizan a continuación:

Teorema 2.1.7. $G/\sim_R = \{Ha : a \in G\}$ con $Ha = \{ha \mid h \in H\}$.

Demostración. Primero se demostrará que G/\sim_R es un partición.

- Si $x \in [a]_{\sim_R} \cap [b]_{\sim_R}$ ⁵ entonces por definición de clase de equivalencia $x \sim_R a$ y $x \sim_R b$, ahora, dado que \sim_R es una relación simétrica, de las relaciones $x \sim_R a, x \sim_R b$ se concluye que $xa^{-1} \in H$ y $bx^{-1} \in H$. Al ser estos últimos dos productos elementos de H y dado que H es un subgrupo de G se tiene debido a la asociatividad y a la cerradura de H que $(bx^{-1})(xa^{-1}) = ba^{-1} \in H$, es decir,

⁵ $[a]_{\sim_R}$ denota el conjunto de todos los $x \in G$ relacionados con a

$a \sim_R b$ y en conclusión $[a]_{\sim_R} = [b]_{\sim_R}$. Observe que lo que se acaba de demostrar es la proposición contra recíproca de: si $b \notin [a]_{\sim_R}$ entonces $[a]_{\sim_R} \cap [b]_{\sim_R} = \emptyset$.

- Como \sim_R es reflexiva entonces $a \in [a]_{\sim_R}$ para todo $a \in G$ y por lo tanto $G \subseteq \bigcup_{a \in G} [a]_{\sim_R}$. Por otro lado, si $x \in \bigcup_{a \in G} [a]_{\sim_R}$ entonces $x \in [a]_{\sim_R}$ para algún $a \in G$ luego, por definición de clase $x \in G$ y en consecuencia $\bigcup_{a \in G} [a]_{\sim_R} \subseteq G$. Se concluye así que $G = \bigcup_{a \in G} [a]_{\sim_R}$.

Ahora se quiere demostrar que la clase $[a]_{\sim_R} = Ha$. Sea $x \in [a]_{\sim_R} \in G / \sim_R$ entonces $x \sim_R a$ luego $xa^{-1} \in H$, esto implica que $xa^{-1} = h$ para algún $h \in H$, o lo que es equivalente, $x = ha$, por lo tanto $x \in Ha$.

Note que todos los argumentos aquí son reversibles, en el sentido en que son doble implicación, obteniendo así lo que se desea demostrar.

□

Al conjunto Ha del teorema anterior se le denomina clase lateral a derecha de G .

De forma análoga, se define la relación:

$a \sim_L b$ sí y sólo sí $a^{-1}b \in H$, que genera una partición de G cuyos elementos son los conjuntos de la forma $aH = \{ah \mid h \in H\}$ y son llamados clases laterales a izquierda de G .

En notación aditiva las clases laterales izquierda y derecha se escribirán $a + H$ y $H + a$ respectivamente.

Ejemplo 2.1.6.

- Sea (D_4, \circ) y $H = \{\rho_0, \mu_1\}$. Las clases laterales a izquierda de D_4 con respecto a H son:

$$\rho_0 H = \{\rho_0, \mu_1\}$$

$$\mu_1 H = \{\mu_1, \rho_0\}$$

$$\rho_1 H = \{\rho_1, \mu_4\}$$

$$\mu_2 H = \{\mu_2, \rho_2\}$$

$$\rho_2 H = \{\rho_2, \mu_2\}$$

$$\mu_3 H = \{\mu_3, \rho_3\}$$

$$\rho_3 H = \{\rho_3, \mu_3\}$$

$$\mu_4 H = \{\mu_4, \rho_1\}$$

- Sean $G = (\mathbb{Z}, +_{12})$ y $H = \{4, 8, 0\}$, entonces las clases laterales a derecha de H son:

$$H +_{12} 0 = \{4, 8, 0\}$$

$$H +_{12} 4 = \{4, 8, 0\}$$

$$H +_{12} 8 = \{4, 8, 0\}$$

$$H +_{12} 1 = \{5, 9, 1\}$$

$$H +_{12} 5 = \{5, 9, 1\}$$

$$H +_{12} 9 = \{5, 9, 1\}$$

$$H +_{12} 2 = \{6, 10, 2\}$$

$$H +_{12} 6 = \{6, 10, 2\}$$

$$H +_{12} 10 = \{6, 10, 2\}$$

$$H +_{12} 3 = \{7, 11, 3\}$$

$$H +_{12} 7 = \{7, 11, 3\}$$

$$H +_{12} 11 = \{7, 11, 3\}$$

- Sea $G = \{e, a, a^2, b, ab, a^2b\}$ donde e es el elemento identidad, $a^3 = e$, $b^2 = e$,

$ba^i = a^{-i}b$ y $i \in \mathbb{Z}$. Tomemos $H = \{e, b\}$, los cocientes derechos son:

$$He = \{e, b\} = Hb$$

$$Ha = \{a, a^2b\} = Ha^2b$$

$$Ha^2 = \{a^2, ab\} = Hab$$

Los cocientes izquierdos de H son:

$$eH = \{e, b\} = bH$$

$$aH = \{a, ab\} = abH$$

$$a^2H = \{a^2, a^2b\} = a^2bH$$

Nótese del ejemplo anterior que no siempre las clases laterales izquierdas son iguales a las derechas, sin embargo, existen un tipo especial de subgrupos los cuales permiten esta igualdad, estos son definidos a continuación:

Definición 2.1.6. Sea $(G, *)$ un grupo y $H \leq G$. Si toda clase lateral a derecha es también una clase lateral a izquierda, esto es, $aH = Ha$ para todo $a \in G$, se dice que $(H, *)$ es un **subgrupo normal** del grupo $(G, *)$ y se denotará por $H \trianglelefteq G$.

Se tiene así que el subgrupo $(\{e, b\}, \cdot)$ del ejemplo anterior no es normal en $(\{e, a, a^2, b, ab, a^2b\}, \cdot)$.

Ejemplo 2.1.7. Los siguientes subgrupos son normales:

- $(H = \{4, 8, 0\}, +_{12})$ del grupo $(\mathbb{Z}, +_{12+})$ en el ejemplo 2.1.6.

- $(n\mathbb{Z}, +)$ como subgrupo de $(\mathbb{Z}, +)$.
- $H = \{0\} \times \mathbb{Z}_2 = \{(0, 0), (0, 1)\}$ en $(\mathbb{Z}_3 \times \mathbb{Z}_2, +)$ donde $+$ es la suma componente a componente.

Con un subgrupo normal H en G , además de tener la particularidad de que las clases laterales derechas e izquierdas sean iguales, se tiene que la estructura $(G/H, +)$ con $+$ definida por: $(a + H) + (b + H) = (a + b) + H$, es un grupo, lo que da lugar entonces a la siguiente definición.

Definición 2.1.7. Si H es un subgrupo normal de G entonces diremos que $(G/\sim_L, +) = (G/\sim_R, +)$ es el **grupo cociente aditivo** y lo notaremos como G/H .

2.2. Anillos

En la sección anterior exploramos una de las estructuras fundamentales en álgebra: los grupos. Ahora centraremos nuestro estudio en anillos, que son estructuras más “robustas”, en tanto en estas se consideran dos operaciones que se relacionan. Esta característica permite tener un conjunto de propiedades adicionales que conducen a resultados relevantes para nuestro objetivo.

Los anillos son herramientas esenciales en matemáticas que permiten abstraer la naturaleza algebraica de sistemas numéricos clásicos como \mathbb{Z} , \mathbb{Q} , \mathbb{R} en las que se estudian y utilizan las operaciones de suma y multiplicación. Es así, que a partir del estudio de anillos, se pueden generalizar nociones como la de divisibilidad, factorización y otras estructuras para así utilizarlas en diferentes áreas de las matemáticas

como criptografía, geometría algebraica y álgebra lineal. Es decir, los anillos son fundamentales tanto en la teoría como en aplicaciones prácticas en diversas ramas matemáticas. Dicho esto, procedemos a dar la definición formal de anillo.

Definición 2.2.1. *Sea A un conjunto no vacío. Si en A se han definido dos operaciones binarias denotadas por $+$ y \cdot , tal que:*

- $(A, +)$ es un grupo abeliano.
- \cdot es asociativa.
- \cdot distribuye con respecto a $+$, es decir, para cuales quiera $a, b, c, d \in A$ se tiene que:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot d = b \cdot d + c \cdot d$$

se dice que A junto con las operaciones tiene estructura de **anillo**, es decir $(A, +, \cdot)$ es un anillo.

Si existe un elemento neutro para la operación \cdot , este se llamará identidad y se se dirá entonces que $(A, +, \cdot)$ es un **anillo con identidad** y si la operación \cdot es conmutativa diremos que $(A, +, \cdot)$ es un **anillo conmutativo**.

Nota: Por costumbre a la operación $+$ se le llama suma y a la operación \cdot multiplicación, la identidad será denotada por 1 en caso que esta exista.

Una vez más los conjuntos numéricos fundamentales son útiles para ejemplificar lo que es un anillo:

Ejemplo 2.2.1. *Algunos ejemplos de anillos son:*

- Los conjuntos \mathbb{Z} , \mathbb{Q} , \mathbb{R} y \mathbb{C} forman anillos si sobre ellos se definen la suma y producto usuales.
- Sea X un conjunto no vacío y $\wp(X)$ su conjunto de partes, entonces las estructuras $(\wp(X), \Delta, \cap)$ y $(\wp(X), \cup, \cap)$ son anillos.
- $(M_n(\mathbb{R}), +, \cdot)$ es un anillo no conmutativo, ya que dadas dos matrices cuadradas A y B , en general $AB \neq BA$.
- \mathbb{Z}_n con la suma y producto módulo n es un anillo conmutativo y con unidad.
- $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$ con la suma y producto usual de enteros es un anillo conmutativo sin unidad.

Nota: De aquí en adelante se usará la notación $+$ y \cdot como las operaciones suma y producto módulo n cuando se trabaje sobre \mathbb{Z}_n .

Algunas propiedades básicas familiares en los conjuntos numéricos son válidas también para los anillos en general:

Teorema 2.2.1. *Dado el anillo $(A, +, \cdot)$ se cumple:*

1. $0 \cdot a = a \cdot 0 = 0$

2. $a \cdot (-b) = (-a) \cdot b = -(ab)$

3. $(-a)(-b) = a \cdot b$

Demostración. .

1.

$$a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) \quad \text{Propiedad distributiva}$$

$$a \cdot 0 + \cancel{a \cdot 0} = \cancel{a \cdot 0} \quad \text{Definición de elemento neutro}$$

$$a \cdot 0 = 0 \quad \text{Sumando } -a \cdot 0 \text{ a ambos lados de la ecuación}$$

2.

$$a \cdot (-b) + a \cdot b = a \cdot (-b + b) \quad \text{Propiedad distributiva}$$

$$= a \cdot 0 \quad \text{definición de inverso aditivo}$$

$$= 0 \quad \text{ítem 1}$$

Luego $a \cdot (-b)$ es el opuesto de $a \cdot b$, esto es, $a \cdot (-b) = -(a \cdot b)$

Del mismo modo,

$$(-a) \cdot b + a \cdot b = (-a + a) \cdot b$$

$$= 0 \cdot b$$

$$= 0$$

entonces $(-a) \cdot b = -(a \cdot b)$

UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

3. Note que:

$$\begin{aligned} (-a) \cdot (-b) + a \cdot (-b) &= (-a + a) \cdot (-b) \\ &= 0 \cdot (-b) \\ &= 0 \end{aligned}$$

Luego $(-a) \cdot (-b) = -(a \cdot (-b))$, por el numeral 2 tenemos que $-(a \cdot (-b)) = -(-(a \cdot b))$ y por definición $-(-(a \cdot b))$ es el inverso de $-(a \cdot b)$, es decir, $-(-(a \cdot b)) = a \cdot b$ y por lo tanto, $(-a) \cdot (-b) = a \cdot b$

□

A continuación se introducen algunos tipos especiales de anillos los cuales serán relevantes en resultados posteriores.

Definición 2.2.2. Sea $(A, +, \cdot)$ un anillo con identidad 1.

- Un elemento $u \neq 0 \in A$ es llamado **una unidad** de A , si existe $x \in A$ tal que $ux = xu = 1$. Si todo elemento $u \in A$ es una unidad, entonces se dirá que $(A, +, \cdot)$ es un **anillo de división** y si además $(A, +, \cdot)$ es conmutativo, se dirá que es un **campo**.
- Dos elementos distintos de cero $a, b \in A$ se llaman **divisores de cero** si $ab = 0$.
- Si $(A, +, \cdot)$ es conmutativo y no tiene divisores de cero, se dice que es un **dominio de integridad**.

Los siguientes ejemplos ilustran esta definición.

Ejemplo 2.2.2. .

- Como $2 \cdot 3 = 0$ en $(\mathbb{Z}_6, +, \cdot)$, 2 y 3 divisores de cero, mientras que 4 no es unidad de \mathbb{Z}_6 .

En general, los divisores de cero en $(\mathbb{Z}_n, +, \cdot)$ son aquellos que no son primos relativos con n , esto conduce a concluir que si p es primo, \mathbb{Z}_p es un anillo de división, más aún, es un campo.

- 2 es unidad en $(\mathbb{Z}_5, +, \cdot)$, puesto que $2 \cdot 3 = 1$.
- Observe que \mathbb{Z}_2 es un dominio de integridad, sin embargo, $M_2(\mathbb{Z}_2)$ no lo es, pues:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

2.2.1. Subanillos

De igual forma a cómo se hizo con los grupos, en las siguientes secciones se estudiarán subconjuntos de anillos que también tengan estructura de anillo, es decir, subestructuras. Entre ellos se encuentran subconjuntos especiales que serán una base concreta del propósito de este estudio.

Definición 2.2.3. Sea $(A, +, \cdot)$ un anillo con identidad y S un subconjunto no vacío

de A . Se dice que S es un **subanillo** de $(A, +, \cdot)$ si $(S, +, \cdot)$ es un anillo.

Antes de ejemplificar algunos subanillos, a partir de la definición de anillo, se infiere de forma directa el siguiente resultado:

Teorema 2.2.2. *Sea $(A, +, \cdot)$ un anillo con unidad 1 y $\emptyset \neq S \subseteq A$, S es un subanillo de $(A, +, \cdot)$ si y sólo si:*

i) $(S, +)$ es subgrupo de $(A, +)$.

ii) $ab \in S$ para todo $a, b \in S$

Ejemplo 2.2.3. .

- El conjunto $2\mathbb{Z}$ es subanillo de $(\mathbb{Z}, +, \cdot)$. En general $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$ con n un entero fijo, es un subanillo de los enteros.

- El subconjunto S de todas las matrices de la forma $\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$ es un subanillo de $(M_n(\mathbb{R}), +, \cdot)$.

Existe un tipo de subanillo especial que es fundamental para el propósito de este estudio y el cual llamaremos ideal, dada su relevancia, su estudio se dispone en la siguiente sección.

Educadora de educadores

2.2.2. Ideales

Los ideales son un tipo de subanillo con la característica de que al tomar un elemento en él y multiplicarlo bien sea a izquierda o derecha con un elemento del

anillo del cual este es subanillo, el producto es absorbido por el subanillo, es decir, este producto es un elemento del subanillo.

Estos subanillos son importantes en la teoría de anillos, ya que, por un lado su papel es similar al de los subgrupos normales para los grupos, y por otro ellos permiten abordar nociones como la de elementos primos, elementos irreducibles, entre otras.

Definición 2.2.4. Dado I un subanillo de $(A, +, \cdot)$, se dice que:

- I es un **ideal izquierdo** de $(A, +, \cdot)$, si $ax \in I$ para todo $a \in A$ y todo $x \in I$.
- I es un **ideal derecho** de $(A, +, \cdot)$, si $xa \in I$ para todo $a \in A$ y todo $x \in I$.
- I es un **ideal bilátero** de $(A, +, \cdot)$, o simplemente un **ideal**, si I es un ideal derecho e izquierdo de $(A, +, \cdot)$.

De esta definición y del teorema 2.2.2 se sigue que:

Teorema 2.2.3. Si $\emptyset \neq I \subseteq A$ entonces I es un ideal de $(A, +, \cdot)$ si y sólo si se cumplen las condiciones:

- i) Para cualesquiera $x_1, x_2 \in I$, se tiene que $x_1 - x_2 \in I$.
- ii) Si $x \in I$ y $a \in A$ entonces $ax = xa \in I$.

Ejemplo 2.2.4. .

- Algunos de los ideales más conocidos son algunos tipos de subconjuntos de

números enteros. Sea $n \in \mathbb{N}$ fijo, el siguiente conjunto:

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

es un ideal de $(\mathbb{Z}, +, \cdot)$ ya que si $k_2 \in \mathbb{Z}$, $nk_1 \in n\mathbb{Z}$ entonces

$k_2 \cdot nk_1 = n(k_1k_2) \in n\mathbb{Z}$. En general, todos los ideales en \mathbb{Z} son de la forma $n\mathbb{Z}$.

- El conjunto I de matrices de la forma $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ es un ideal izquierdo de $(M_2(\mathbb{R}), +, \cdot)$.

En efecto, considere $X = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ y $A = \begin{pmatrix} c & d \\ e & f \end{pmatrix}$ entonces $AX = \begin{pmatrix} c & d \\ e & f \end{pmatrix}$

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ca + db & 0 \\ ea + fb & 0 \end{pmatrix} \in I.$$

Note que $XA = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} c & d \\ e & f \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix} \notin I$.

- $M_n(k\mathbb{Z})$ para un entero k fijo, es un ideal de $(M_n(\mathbb{Z}), +, \cdot)$.

Demostración. como las entradas de las matrices en $M_n(k\mathbb{Z})$ son elementos del conjunto $k\mathbb{Z}$, entonces estas tienen la forma kz para algún entero z . Así, si consideramos las matrices $A \in M_n(k\mathbb{Z})$ y $B \in M_n(\mathbb{Z})$, donde,

$$A = \begin{pmatrix} kz_{11} & kz_{12} & \cdots & kz_{1n} \\ kz_{21} & kz_{22} & \cdots & kz_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ kz_{n1} & kz_{n2} & \cdots & kz_{nn} \end{pmatrix} \text{ y } B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

obtendremos como resultado

$$AB = \begin{pmatrix} \sum_{h=1}^n kz_{1h}b_{h1} & \sum_{h=1}^n kz_{1h}b_{h2} & \cdots & \sum_{h=1}^n kz_{1h}b_{hn} \\ \sum_{h=1}^n kz_{2h}b_{h1} & \sum_{h=1}^n kz_{2h}b_{h2} & \cdots & \sum_{h=1}^n kz_{2h}b_{hn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{h=1}^n kz_{nh}b_{h1} & \sum_{h=1}^n kz_{nh}b_{h2} & \cdots & \sum_{h=1}^n kz_{nh}b_{hn} \end{pmatrix}$$

y factorizando k en cada una de las sumatorias tenemos:

$$AB = \begin{pmatrix} k \sum_{h=1}^n z_{1h}b_{h1} & k \sum_{h=1}^n z_{1h}b_{h2} & \cdots & k \sum_{h=1}^n z_{1h}b_{hn} \\ k \sum_{h=1}^n z_{2h}b_{h1} & k \sum_{h=1}^n z_{2h}b_{h2} & \cdots & k \sum_{h=1}^n z_{2h}b_{hn} \\ \vdots & \vdots & \ddots & \vdots \\ k \sum_{h=1}^n z_{nh}b_{h1} & k \sum_{h=1}^n z_{nh}b_{h2} & \cdots & k \sum_{h=1}^n z_{nh}b_{hn} \end{pmatrix}$$

Como dentro de cada sumatoria se tiene productos de enteros, entonces cada una de las entradas de AB es un elemento de $k\mathbb{Z}$. Así se concluye que

$AB \in M_n(k\mathbb{Z})$; de forma similar se prueba que $BA \in M_n(k\mathbb{Z})$, y por lo tanto $M_n(k\mathbb{Z})$ es un ideal de $(M_n(\mathbb{Z}), +, \cdot)$. \square

En general, dado un ideal I de un anillo $(A, +, \cdot)$, se tiene que

$M_n(I) := \{[a_{ij}] | a_{ij} \in I\}$ es un ideal de $(M_n(A), +, \cdot)$.

- Sea F el conjunto de todas las funciones de valor real definidas sobre \mathbb{R} . El

subconjunto $I = \{f \in \mathbb{R} \mid f(0) = 0\}$ es un ideal de $(F, +, \cdot)$.

Demostración. $I \leq F$ pues si $h_1, h_2 \in I$ entonces $(h_1 - h_2)(0) = h_1(0) - h_2(0) = 0 - 0 = 0$ luego $h_1 - h_2 \in I$. Ahora, sean $f \in F$ y $g \in I$ entonces $fg(0) = f(0)g(0) = f(0) \cdot 0 = 0 = g(0)f(0) = gf(0)$. Luego $gf = fg \in I$ \square

- Sea $(A, +, \cdot)$ conmutativo e I un ideal, el conjunto

$$\sqrt{I} = \{x \in A \mid x^n \in I \text{ para algún } n \in \mathbb{Z}\}$$

es un ideal de $(A, +, \cdot)$.

Demostración. Sean $x_1, x_2 \in \sqrt{I}$, existen $n_1, n_2 \in \mathbb{Z}$ tales que $x_1^{n_1}, x_2^{n_2} \in I$, luego $(-x_2)^{n_2} \in \sqrt{I}$ pues $(-x_2)^{n_2} = -x_2^{n_2}$ si n es impar y $(-x_2)^{n_2} = x_2^{n_2}$ si n es par, así, en cualquiera de los casos al ser I un ideal, $(-x_2)^{n_2} \in I$. Tomando $n = n_1 + n_2$ se tiene que $(x_1 - x_2)^n = \sum_{k=0}^n \binom{n}{k} x_1^{n-k} (-x_2)^k$ esto es porque $(A, +, \cdot)$ es conmutativo (pruébese esto). Como cada uno de los factores $\binom{n}{k} x_1^{n-k} (-x_2)^k \in I$ e I es un ideal, entonces $(x_1 - x_2)^n \in I$, por lo tanto $x_1 - x_2 \in \sqrt{I}$. Así se concluye que $\sqrt{I} \leq A$.

Ahora, sean $x \in \sqrt{I}$ y $a \in A$ entonces existe $n \in \mathbb{Z}$ tal que $x^n \in I$, como I es ideal entonces $a^n x^n = (ax)^n \in I$ y en consecuencia $ax \in \sqrt{I}$. \square

El conjunto \sqrt{I} se llama el radical de I .

Todo $(A, +, \cdot)$ tiene al menos dos ideales, a saber, $\{0\}$ y el mismo A , estos ideales son llamados **ideales triviales**.

Se tiene entonces el siguiente resultado para anillos con identidad:

Teorema 2.2.4. *Sea I un ideal de $(A, +, \cdot)$ con identidad 1 , si $1 \in I$ entonces $I = A$.*

Demostración. Sea $a \in A$, si $1 \in I$ entonces $1 \cdot a = a \in I$, luego $A \subseteq I$ y por lo tanto, $A = I$. \square

Teorema 2.2.5. *Sea $(A, +, \cdot)$, el conjunto $S = \{I \subseteq A \mid I \text{ es un ideal de } (A, +, \cdot)\}$ es un conjunto parcialmente ordenado con respecto a la contención \subset .*

Una técnica común en matemáticas para la creación de nuevos conjuntos es emplear las operaciones entre conjuntos como la unión y la intersección; por tanto, cabe preguntarse si la unión o intersección, de dos ideales también es un ideal.

Teorema 2.2.6. *Sean $(A, +, \cdot)$ y $\{I_i\}_{i \in N}$ una familia de ideales de $(A, +, \cdot)$, el conjunto $\bigcap_{i \in N} I_i$ es un ideal de $(A, +, \cdot)$.*

Demostración. Si $x \in \bigcap_{i \in N} I_i$ y $a \in A$ entonces $x \in I_i$ para todo $i \in N$, como cada I_i es un ideal, entonces $ax \in I_i$ y por lo tanto $ax \in \bigcap_{i \in N} I_i$. De manera similar $xa \in \bigcap_{i \in N} I_i$. \square

Este resultado conduce a la siguiente definición.

Definición 2.2.5. *Sea X un subconjunto de $(A, +, \cdot)$ y $\{I_i\}_{i \in N}$ la familia de todos los ideales en $(A, +, \cdot)$ que contienen a X , entonces $\bigcap_{i \in N} I_i$ es llamado el **ideal generado por X** . Denotado por $\langle X \rangle$.*

*Un ideal generado por un sólo elemento a es llamado **ideal principal** y este se*

denotará simplemente por $\langle a \rangle$

Un **anillo de ideales principales** es un anillo en el cual todo ideal es principal.

Teorema 2.2.7. Sea $(A, +, \cdot)$ un anillo, $a \in A$ y $X \subseteq A$.

i) El ideal principal $\langle a \rangle$ consiste de todos los elementos de la forma:

$$ra + as + na + \sum_{i=1}^m r_i a s_i \text{ tales que } r, s, r_i, s_i \in A, m \in \mathbb{Z}^+, \text{ y } n \in \mathbb{Z}.$$

ii) Si A es un anillo con unidad entonces $\langle a \rangle = \left\{ \sum_{i=1}^m r_i a s_i \mid r_i, s_i \in A, m \in \mathbb{Z}^+ \right\}$.

Un resultado inmediato del teorema es el siguiente:

Colorario 2.2.1. Si $(A, +, \cdot)$ es un anillo conmutativo con identidad y

$X = \{a_1, \dots, a_n\} \subset A$ entonces:

$$\langle a_1, \dots, a_n \rangle = \left\{ \sum_{i=1}^n r_i a_i \mid r_i \in A \right\}$$

Ejemplo 2.2.5. Considere $A = \mathbb{Z}$, entonces por la conmutatividad de \mathbb{Z} se tiene lo siguiente:

$$\begin{aligned} \langle 3 \rangle &= \left\{ \sum_{i=1}^n r_i \cdot 3 \cdot s_i \mid r_i, s_i \in \mathbb{Z}, n \in \mathbb{Z}^+ \right\} \\ &= \left\{ 3 \sum_{i=1}^n r_i s_i \mid r_i, s_i \in \mathbb{Z}, n \in \mathbb{Z}^+ \right\} \\ &= \{3k \mid k \in \mathbb{Z}\} \\ &= 3\mathbb{Z}. \end{aligned}$$

y

$$\begin{aligned}
 \langle 4, 6 \rangle &= \{r_1 \cdot 4 + r_2 \cdot 6 \mid r_1, r_2 \in \mathbb{Z}\} \\
 &= \{2(r_1 \cdot 2 + r_2 \cdot 3) \mid r_1, r_2 \in \mathbb{Z}\} \\
 &= \{2k \mid k \in \mathbb{Z}\} \\
 &= \langle 2 \rangle
 \end{aligned}$$

Aquí, dado que 2 y 3 son primos relativos entonces el menor entero positivo que podemos escribir como combinación lineal de ellos es 1, esto nos permite afirmar que para cualquier entero k podemos encontrar enteros r_1 y r_2 de tal manera que $k = r_1 \cdot 2 + r_2 \cdot 3$.

Como se vio anteriormente, se pueden construir ideales utilizando la intersección de conjuntos. Ahora definiremos nuevos ideales a partir de la unión.

Definición 2.2.6. Sea $\{I_i\}_{i \in \mathbb{N}}$ una familia de ideales de $(A, +, \cdot)$. Definimos la suma de la familia, denotada por $\sum_{i \in \mathbb{N}} I_i$, como el ideal generado por el conjunto $\bigcup_{i \in \mathbb{N}} I_i$, esto es:

$$\sum_{i \in \mathbb{N}} I_i = \left\{ \sum_{k=1}^n a_k \mid a_k \in \bigcup_{i \in \mathbb{N}} I_i, n \in \mathbb{Z}^+ \right\}$$

En el caso particular de una familia finita:

$$I_1 + I_2 + \cdots + I_n = \left\{ \sum_{j=1}^n a_j \mid a_j \in I_j \right\}$$

Ejemplo 2.2.6. .

- En $(\mathbb{Z}, +, \cdot)$,

$$\langle m \rangle + \langle n \rangle = \langle \text{mcd}(m, n) \rangle$$

donde, $\text{mcd}(m, n)$ denota al máximo común divisor entre m y n .

Demostración. Si $x \in \langle m \rangle + \langle n \rangle$ entonces $x = a + b$ tal que $a \in \langle m \rangle$ y $b \in \langle n \rangle$, es decir, $x = km + pn$ con $k, p \in \mathbb{Z}$. Si $d = \text{mcd}(m, n)$, $d|m$ y $d|n$ en consecuencia, $d|x$ y por tanto $x \in \langle d \rangle$,

Recíprocamente, si $x \in \langle d \rangle$, $x = ds$ pero como d se puede escribir como combinación lineal de m y n , $x \in \langle m \rangle + \langle n \rangle$. \square

Como casos particulares,

$$\langle 2 \rangle + \langle 3 \rangle = \langle 1 \rangle = \mathbb{Z}$$

$$\langle 12 \rangle + \langle 8 \rangle = \langle 4 \rangle = 4\mathbb{Z}$$

De esta forma, se observa que todo ideal en \mathbb{Z} es principal.

- En el anillo de matrices $(M_n(\mathbb{Z}), +, \cdot)$

$$M_n(\langle m \rangle) + M_n(\langle n \rangle) = M_n(\langle m \rangle + \langle n \rangle) = M_n(\langle \text{mcd}(m, n) \rangle)$$

Definición 2.2.7. Sea $\{I_i\}_{i \in N}$ una familia finita de ideales de un anillo $(A, +, \cdot)$.

Definimos el producto de la familia como el ideal generado por el conjunto:

$$\{x_1 x_2 \cdots x_n \mid x_i \in I_i\}$$

Del teorema 2.2.7 se tiene que:

$$I_1 I_2 \cdots I_n = \left\{ \sum_{j=1}^m x_{1j} \cdots x_{nj} \mid x_{ij} \in I_i, 1 \leq i \leq n, m \geq 1 \right\}$$

Ejemplo 2.2.7. .

- En $(\mathbb{Z}, +, \cdot)$

$$\begin{aligned} \langle 2 \rangle \langle 3 \rangle \langle 5 \rangle &= \left\{ \sum_{j=1}^m x_{1j} x_{2j} x_{3j} \mid x_{1j} \in \langle 2 \rangle, x_{2j} \in \langle 3 \rangle, x_{3j} \in \langle 5 \rangle, m \geq 1 \right\} \\ &= \left\{ \sum_{j=1}^m (2q)(3r)(5s) \mid q, r, s \in \mathbb{Z}, m \geq 1 \right\} \\ &= \left\{ 30 \sum_{j=1}^m qrs \mid q, r, s \in \mathbb{Z}, m \geq 1 \right\} \\ &= \langle 30 \rangle \end{aligned}$$

- En $(\mathbb{Z}, +, \cdot)$,

$$\langle m \rangle \langle n \rangle = \langle mn \rangle$$

Demostración. Si $x \in \langle m \rangle \langle n \rangle$ entonces $x = a_1 b_1 + \cdots + a_t b_t$, donde $a_i \in \langle m \rangle$ y $b_i \in \langle n \rangle$, con $i = 1, 2, \dots, t$. Entonces, $x = k_1 m s_1 n + \cdots + k_t m s_t n$, con $k_i, s_i \in \mathbb{Z}$ y por tanto, $x \in \langle mn \rangle$. Recíprocamente, si $x \in \langle mn \rangle$, entonces $x = kmn$, con $k \in \mathbb{Z}$, de donde, $x = kmn \in \langle m \rangle \langle n \rangle$. \square

La propiedad distributiva se satisface también para la suma y producto de ideales.

Teorema 2.2.8. Si J, I_1, I_2, \dots, I_n son ideales de un anillo $(A, +, \cdot)$ entonces:

- $J(I_1 + \cdots + I_n) = JI_1 + \cdots + JI_n$
- $(I_1 + \cdots + I_n)J = I_1J + \cdots + I_nJ$

A partir de la definición de producto de ideales y del resultado anterior aparecen ideales en los cuales sus elementos tienen un comportamiento similar a los primos en los números enteros, dando paso así a los siguientes ideales:

Definición 2.2.8. Se dice que un ideal P de $(A, +, \cdot)$ es un **ideal primo** si $P \neq A$ y para cualesquiera ideales I, J de $(A, +, \cdot)$ se tiene que:

$$\text{Si } IJ \subset P \text{ entonces } I \subset P \text{ o } J \subset P$$

A continuación, algunos ejemplos de ideales primos.

Ejemplo 2.2.8. .

- $\langle 3 \rangle$ es un ideal primo en $(\mathbb{Z}, +, \cdot)$, pues si $\langle k \rangle$ y $\langle n \rangle$ son dos ideales cualquiera en $(\mathbb{Z}, +, \cdot)$ de modo que $\langle k \rangle \langle n \rangle \subset \langle 3 \rangle$ entonces kn es múltiplo de 3, es decir, $3|kn$, al ser 3 un número primo entonces $3|k$ o $3|n$, esto implica que $\langle k \rangle \subset \langle 3 \rangle$ o $\langle n \rangle \subset \langle 3 \rangle$.
- $24\mathbb{Z}$ no es un ideal primo de $(\mathbb{Z}, +, \cdot)$ porque $6\mathbb{Z} \cdot 8\mathbb{Z} = 48\mathbb{Z} \subset 24\mathbb{Z}$ pero $6\mathbb{Z} \not\subset 24\mathbb{Z}$ y $8\mathbb{Z} \not\subset 24\mathbb{Z}$.

En este ejemplo es de notar dos cosas:

1. No existe un ideal en $(\mathbb{Z}, +, \cdot)$ distinto de \mathbb{Z} , que sea mayor a $\langle 3 \rangle$ con respecto al orden dado por la contención, es decir, no existe un ideal $\langle m \rangle$ de manera que $\langle 3 \rangle \subset \langle m \rangle \subset \mathbb{Z}$. Esto es porque todo múltiplo de 3 debe ser múltiplo de m y el único valor de m que satisface este orden es $m = 1$, pero $\langle 1 \rangle = \mathbb{Z}$.
2. El ideal $48\mathbb{Z}$ lo hemos factorizado como el producto de los ideales $6\mathbb{Z}$ y $8\mathbb{Z}$.

Estas dos propiedades no sólo se cumplen en $(\mathbb{Z}, +, \cdot)$ sino que pueden estudiarse de manera general en otros anillos. El numeral 2, por ejemplo, permite visualizar que, tal como se hace con los números enteros positivos, es posible factorizar ideales y extender la idea de factorización a los elementos en un anillo.

Para seguir esta línea, tenemos el siguiente resultado:

Teorema 2.2.9. Si P es un ideal en un anillo $(A, +, \cdot)$, $P \neq A$ y para todo $a, b \in A$ se satisface:

Si $ab \in P$ implica que $a \in P$ o $b \in P$

entonces P es un ideal primo de $(A, +, \cdot)$.

Demostración. Sean I, J ideales de $(A, +, \cdot)$ tales que $IJ \subset P$. Suponga que $I \not\subset P$ y $J \not\subset P$, entonces existen $x_1 \in I$ y $x_2 \in J$ tales que $x_1 \notin P$ y $x_2 \notin P$. Sin embargo, como $x_1x_2 \in IJ$ se tiene que $x_1x_2 \in P$ y por la hipótesis del teorema $x_1 \in I$ o $x_2 \in J$, siendo esto una contradicción, se concluye entonces que P es un ideal primo. \square

Nota: La recíproca es válida sólo si $(A, +, \cdot)$ es un anillo conmutativo.

Ejemplo 2.2.9. .

- $\langle p \rangle$ es un ideal primo de $(\mathbb{Z}, +, \cdot)$ si y sólo si p es primo.

Demostración. (\Leftarrow) Sea p un entero primo y $a, b \in \mathbb{Z}$ tales que $ab \in \langle p \rangle$ entonces ab es múltiplo de p , como p es primo entonces $p|a$ o $p|b$, es decir, $\langle a \rangle \subset \langle p \rangle$ o $\langle b \rangle \subset \langle p \rangle$. En virtud del teorema anterior, $\langle p \rangle$ es un ideal primo.

(\Rightarrow) Suponga que p no es primo, entonces existen enteros m y n de modo que $m|p$ y $n|p$ \square

- $\mathbb{Z} \times \{0\}$ es un ideal primo de $\mathbb{Z} \times \mathbb{Z}$ con la suma y producto componente a componente, ya que:

Si $(a, b)(c, d) = (ac, bd) \in \mathbb{Z} \times \{0\}$ entonces $bd = 0$ y como tanto b como d son enteros entonces $b = 0$ o $d = 0$. Para el caso en que $b = 0$ se tiene que $(a, b) \in \mathbb{Z} \times \{0\}$ y en el caso en que $d = 0$, $(c, d) \in \mathbb{Z} \times \{0\}$.

Definición 2.2.9. Un ideal I de $(A, +, \cdot)$ es llamado un **ideal maximal** si $I \neq A$ y además para cualesquier ideal J de $(A, +, \cdot)$ se cumple que:

$$\text{Si } I \subseteq J \subseteq A \text{ entonces } J = I \text{ o } J = A$$

En concordancia con lo dicho en la reflexión del ejemplo 2.2.8 se tiene entonces que en $(\mathbb{Z}, +, \cdot)$ el ideal $\langle 3 \rangle$ es maximal. Ahora, se ejemplificarán más ideales de este tipo.

Ejemplo 2.2.10. .

- Si $(F, +, \cdot)$ es como en el ejemplo 2.1.1 (funciones con dominio \mathbb{R} y valor real), entonces el ideal $I = \{f \in F \mid f(0) = 0\}$ es maximal.

Demostración. Suponga que J es un ideal de $(F, +, \cdot)$ tal que $I \subset J$, tomemos $g \in J - I$ entonces $g(0) \neq 0$. Así, existe un $h \in F$ tal que

$$h(0) = \frac{1}{g(0)}$$

se sigue entonces que $g(0)h(0) = 1$ y si 1_F denota la identidad en $(F, +, \cdot)$, la función $1_F - gh \in I$ pues $(1_F - gh)(0) = 0$, luego $1_F - gh \in J$. Como $gh \in J$ porque J es ideal, $(1_F - gh) + gh = 1_F \in J$ y por tanto, en virtud del teorema 2.2.4, se debe tener que $J = F$. \square

- Sea $S = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R} \right\}$ el subanillo de $(M_2(\mathbb{R}), +, \cdot)$, el ideal $I =$

$$\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \text{ es maximal.}$$

Demostración. Sea J un ideal de $(S, +, \cdot)$ tal que $I \subset J$, si $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in J - I$ tenemos que $d \neq 0$ y por tanto,

$$\begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{d} \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in J$$

Como $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I$, tenemos que

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in J$$

Así, $J = S$. □

Hay una relación estrecha entre ideales primos e ideales maximales, sin embargo se hace necesario introducir un par de resultados que ayudarán a ver tal relación.

Como se mencionó en el inicio de esta sección, los ideales dentro de un anillo tienen un rol similar a los subgrupos normales, note que como I es conmutativo, entonces I es un subgrupo normal de $(A, +)$ y en consecuencia $(A/I, +)$ es un grupo, esto permite extender este cociente a un anillo.

Teorema 2.2.10. *Sea I un ideal de un anillo $(A, +, \cdot)$, el grupo cociente aditivo A/I es un anillo con multiplicación dada por:*

$$(a + I)(b + I) = ab + I$$

Demostración. Se empezará demostrando que la multiplicación está bien definida:

Suponga que $a' + I = a + I$ y $b' + I = b + I$, esto implica que $a - a' \in I$ y a su vez $b - b' \in I$. Por otro lado observe que:

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' \\ ab - a'b' &= (a - a')b + a'(b - b') \end{aligned}$$

Por lo tanto, $ab - a'b' \in I$, es decir, $ab + I = a'b' + I$.

Se dijo anteriormente que $(A/I, +)$ es un grupo, ahora,

$$\begin{aligned} [(a + I)(b + I)](c + I) &= (ab + I)(c + I) \\ &= (ab)c + I \\ &= a(bc) + I \\ &= (a + I)[(b + I)(c + I)] \end{aligned}$$

Así, \cdot es asociativa.

Finalmente, se validan las propiedades distributivas como sigue:

$$\begin{aligned}
 (a + I)[(b + I) + (c + I)] & \\
 &= (a + I)[(b + c) + I] \\
 &= a(b + c) + I \\
 &= (ab + ac) + I \\
 &= (ab + I)(ac + I) \\
 &= (a + I)(b + I) + (a + I)(c + I)
 \end{aligned}$$

La otra distributiva se prueba de manera similar. □

Como $2\mathbb{Z}_6$ es un ideal de $(\mathbb{Z}_6, +_6, \cdot)$, entonces se puede usar para visualizar el teorema:

Ejemplo 2.2.11. *Los elementos de $\mathbb{Z}_6/2\mathbb{Z}_6$ son:*

$$0 +_6 2\mathbb{Z}_6 = 0 +_6 \{0, 2, 4\} = \{0, 2, 4\}.$$

$$1 +_6 2\mathbb{Z}_6 = 1 +_6 \{0, 2, 4\} = \{1, 3, 5\}.$$

$$2 +_6 2\mathbb{Z}_6 = 2 +_6 \{0, 2, 4\} = \{0, 2, 4\}.$$

$$3 +_6 2\mathbb{Z}_6 = 3 +_6 \{0, 2, 4\} = \{1, 3, 5\}.$$

$$4 +_6 2\mathbb{Z}_6 = 4 +_6 \{0, 2, 4\} = \{0, 2, 4\}.$$

$$5 +_6 2\mathbb{Z}_6 = 5 +_6 \{0, 2, 4\} = \{1, 3, 5\}$$

Así, algunos de los productos nos quedan:

$$(0 +_6 2\mathbb{Z}_6)(4 +_6 2\mathbb{Z}_6) = 0 \cdot 4 +_6 2\mathbb{Z}_6 = 0 +_6 2\mathbb{Z}_6$$

$$(2 +_6 2\mathbb{Z}_6)(3 +_6 2\mathbb{Z}_6) = 2 \cdot 3 +_6 2\mathbb{Z}_6 = 0 +_6 2\mathbb{Z}_6$$

$$(4 +_6 2\mathbb{Z}_6)(2 +_6 2\mathbb{Z}_6) = 4 \cdot 2 +_6 2\mathbb{Z}_6 = 2 +_6 2\mathbb{Z}_6$$

$$(3 +_6 2\mathbb{Z}_6)(3 +_6 2\mathbb{Z}_6) = 3 \cdot 3 +_6 2\mathbb{Z}_6 = 3 +_6 2\mathbb{Z}_6$$

Los ideales primos se relacionan con el anillo cociente $(A/I, +, \cdot)$ de la siguiente manera:

Teorema 2.2.11. $(A/I, +, \cdot)$ no tiene divisores de cero si y solo si I es primo.

De igual forma, los ideales maximales están relacionados con el anillo cociente $(A/I, +, \cdot)$ mediante el siguiente teorema.

Teorema 2.2.12. Sea I un ideal de un anillo con identidad $(A, +, \cdot)$.

- Si I es maximal y $(A, +, \cdot)$ es conmutativo, entonces el anillo cociente $(A/I, +, \cdot)$ es un campo.
- Si el anillo cociente $(A/I, +, \cdot)$ es un anillo de división, entonces I es maximal.

Finalmente, como resultado de este teorema se obtiene la relación entre ideales primos e ideales maximales.

Colorario 2.2.2. Si $(A, +, \cdot)$ es conmutativo con identidad, entonces todo ideal primo I de $(A, +, \cdot)$ es maximal.

A modo de ejemplo, todo ideal $\langle p \rangle$ con p primo en \mathbb{Z} es maximal.

Existe un conjunto de anillos especial en términos de las propiedades que tienen sus ideales, por ejemplo, el si son finitamente generados o existen condiciones de cadena para los ideales. Lo que permitirá la posibilidad de trabajar con algoritmos de la división en anillo de polinomios con coeficientes en este tipo de anillos. Particularmente tenemos los anillos Noetherianos.

2.2.3. Factorización de elementos en un anillo

Como se mencionó en las observaciones al **ejemplo 2.2.8**, los elementos de un anillo se pueden factorizar si este cumple ciertas propiedades. Se iniciará primero definiendo la división o divisibilidad entre elementos del anillo para luego dar paso al concepto de factorización.

Definición 2.2.10. Sea $(A, +, \cdot)$ conmutativo y $a, b \in A$. Se dice que a **divide a** b (notado por $a|b$), si $a \neq 0$ y existe $x \in A$ de modo que $ax = b$.

Decimos que a y b son asociados si $a|b$ y $b|a$.

Observe que en la definición no se exige que el anillo tenga elemento identidad, esto implica que en un anillo $(A, +, \cdot)$, no siempre se tiene que a es asociado con sí mismo.

Ejemplo 2.2.12. .

- En $(\mathbb{Z}_6, +, \cdot)$ 2 y 4 son asociados, pues $2 \cdot 2 = 4$ y $4 \cdot 2 = 2$.

El siguiente teorema muestra la relación entre divisibilidad e ideales principales.

Teorema 2.2.13. Sean $(A, +, \cdot)$ conmutativo con identidad y $a, b, u \in A$.

- i) $a|b$ si y sólo si $\langle b \rangle \subseteq \langle a \rangle$.
- ii) a y b son asociados si y sólo si $\langle a \rangle = \langle b \rangle$.
- iii) u es una unidad si y sólo si $u|r$ para todo $r \in A$.
- iv) u es una unidad si y sólo si $\langle u \rangle = A$.

Demostración. .

i) (\Rightarrow) Sea $b' \in \langle b \rangle$ entonces en virtud del teorema 2.2.7, b' es múltiplo de b , esto lo podemos escribir como: $b' = by$ con $y \in A$. Como $a|b$ entonces existe $x \in A$ tal que $ax = b$ y en consecuencia $b' = (ax)y$, es decir, b' es múltiplo de a y por tanto $b' \in \langle a \rangle$.

(\Leftarrow) Como $\langle b \rangle \subseteq \langle a \rangle$ entonces $b \in \langle a \rangle$ lo cual implica que $b = ax$ para algún $x \in A$, por lo tanto $a|b$.

ii) Consecuencia inmediata de i).

iii) (\Rightarrow) Como u es unidad entonces existe $x \in A$ tal que $ux = 1$, luego, si $r \in A$ $u(xr) = r$, es decir, $u|r$.

(\Leftarrow) Si $u|r$ para todo $r \in A$, en particular $u|1$, esto implica que existe $x \in A$ tal que $ux = 1$, luego, u es unidad.

iv) Si u es unidad por iii) $u|1$ y como $1|u$ entonces 1 y u son asociados, por ii) $\langle u \rangle = \langle 1 \rangle$, pero $\langle 1 \rangle = A$.

□

Como consecuencia de *ii*) las únicas unidades en \mathbb{Z} son 1 y -1 .

La noción de número primo se extiende desde los enteros a anillos en general como sigue:

Definición 2.2.11. Sea $(A, +, \cdot)$ con identidad. Se dice que un elemento $x \in A$ es irreducible si:

- $x \neq 0$ y x no es una unidad de A .
- Si $x = ab$ entonces a es unidad o b es unidad.

Adicionalmente, un elemento $p \in A$ se dice primo si:

- $p \neq 0$ y p no es una unidad de A .
- si $p|ab$ entonces $p|a$ o $p|b$.

Los siguientes son ejemplos de elementos primos y elementos irreducibles:

Ejemplo 2.2.13. .

Educadora de educadores

- Considere el subanillo $(J = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}, +, \cdot)$ del anillo $(\mathbb{R}, +, \cdot)$ y la función $f : J \rightarrow \mathbb{Z}$ tal que $f(a + b\sqrt{10}) = a^2 - 10b^2$ entonces:

i) $f(uv) = f(u)f(v)$ para todo $u, v \in J$ y $f(u) = 0$ si y sólo si $u = 0$.

ii) u es una unidad en J si y sólo si $f(u) = \pm 1$.

iii) $2, 3, 4 + \sqrt{10}$ y $4 - \sqrt{10}$ son elementos irreducibles en J .

iv) $2, 3, 4 + \sqrt{10}$ y $4 - \sqrt{10}$ no son elementos primos en J .

Demostración. .

i) Sean $u = a_1 + b_1\sqrt{10}$ y $v = a_2 + b_2\sqrt{10}$ entonces $uv = (a_1a_2 + 10b_1b_2) + (a_2b_1 + a_1b_2)\sqrt{10}$ luego, $f(uv) = (a_1a_2 + 10b_1b_2)^2 - 10(a_2b_1 + a_1b_2)^2$, por otro lado, $f(u) = a_1^2 - 10b_1^2$ y $f(v) = a_2^2 - 10b_2^2$, así, $f(u)f(v) = (a_1^2 - 10b_1^2)(a_2^2 - 10b_2^2)$.

ii) (\Rightarrow) Si $u = a_1 + b_1\sqrt{10}$ es una unidad en $(J, +, \cdot)$ entonces existe $v = a_2 + b_2\sqrt{10}$ tal que $uv = 1$. Por el ítem anterior se tiene que $f(u)f(v) = 1$, al ser esta una multiplicación de enteros la única forma de que la igualdad se cumpla es que $f(u) = f(v) = \pm 1$.

(\Leftarrow) Suponga que $u = a + b\sqrt{10}$ y $f(u) = \pm 1$, tome $v = a + (-b)\sqrt{10}$, observe que:

$$uv = (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2 = \pm 1$$

Si $uv = 1$ entonces el inverso de u es v , y si $uv = -1$ entonces $-v$ es el inverso de u . Por lo tanto, u es una unidad.

Los ítems iii) y iv) se dejan al lector.

□

2.3. Polinomios

En diferentes cursos de matemáticas se han trabajado polinomios como expresiones algebraicas y son utilizadas en la construcción de ecuaciones o en análisis de funciones. Sin embargo, no es usual trabajar con la estructura de anillo asociada al conjunto de polinomios con coeficientes en otro anillo. En esta sección se abordan los polinomios haciendo énfasis en esta mirada algebraica de estructuras.

Definición 2.3.1. Sea $(A, +, \cdot)$ un anillo conmutativo con unidad.

- Un **polinomio en la variable x** con coeficientes en A se define como la suma formal:

$$a(x) = \sum_{k=0}^{\infty} a_k x^k$$

con $a_k \in A$, donde el conjunto soporte $S_a := \{a_k \mid a_k \neq 0\}$ es finito.

- El conjunto de polinomios en la variable x con coeficientes en el anillo $(A, +, \cdot)$ se denotará por $A[x]$.
- El **polinomio cero** es el polinomio tal que $a_k = 0$ para todo $k \in \mathbb{N}$.

Además, sobre $A[x]$ se puede definir la siguiente función:

Definición 2.3.2. Dado el conjunto de polinomios $A[x]$ con coeficientes en el anillo $(A, +, \cdot)$ y $a(x) \in A[x]$. El **grado de $a(x)$ con respecto a la variable x** es la

imagen de $a(x)$ mediante la función $gr : A[x] \rightarrow \mathbb{N} \cup \{-\infty\}$ dada por:

$$gr(a(x)) = \begin{cases} n := \max\{i \mid a_i \in S_a\} & \text{si } a(x) \neq 0 \\ -\infty & \text{si } a(x) = 0 \end{cases}$$

$a_n \in S_a$ se llamará el **coeficiente principal** de $a(x)$.

Note que esta función se encuentra bien definida dado a que si $a(x) \neq 0$, se tiene que $S_a \neq \emptyset$ y finito, luego el conjunto de subíndices es finito y por lo tanto está acotado superiormente, existiendo así un i máximo. Adicionalmente, como el máximo es único entonces para cada $a(x)$ existe un único n .

Ejemplo 2.3.1. .

- $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ son el conjunto de polinomios con coeficientes en \mathbb{Z} , \mathbb{Q} y \mathbb{R} respectivamente.
- Para el polinomio $a(x) = 1 + 2x + 0x^2 - 3x^3 + 5x^4 + 0x^5 + 0x^6 + \dots + 0x^n + \dots \in \mathbb{Z}_6[x]$, $S_a = \{a_0 = 1, a_1 = 2, a_3 = -3, a_4 = 5\}$, $gr(a(x)) = 4$ y el coeficiente principal es 5.

Las operaciones de adición y multiplicación sobre el anillo $(A, +, \cdot)$ pueden ser extendidas a $A[x]$ de la siguiente manera:

Definición 2.3.3. *Dados*

$$a(x) = \sum_{k=0}^{\infty} a_k x^k, \quad b(x) = \sum_{k=0}^{\infty} b_k x^k \in A[x]$$

Entonces el polinomio adición es definido por

$$c(x) = a(x) + b(x) = \sum_{k=0}^{\infty} c_k x^k$$

donde,

$$S_c = \{c_k = a_k + b_k \mid c_k \neq 0\}$$

De manera similar se define el producto de dos polinomios como sigue:

$$d(x) = a(x)b(x) = \sum_{n=0}^{\infty} d_n x^n$$

donde,

$$S_d = \left\{ d_n = \sum_{i=0}^n a_i b_{n-i} \mid n \text{ es el máximo entero tal que } a_k, b_k = 0 \text{ para } k > n \right\}$$

Por otro lado, $d_k = 0$, si $k > n$.

Teorema 2.3.1. Si $(A, +, \cdot)$ es un anillo, $(A[x], +, \cdot)$ es un anillo.

Demostración. Sean $a(x) = \sum_{i=0}^{\infty} a_i x^i, b(x) = \sum_{j=0}^{\infty} b_j x^j, c(x) = \sum_{k=0}^{\infty} c_k x^k \in A[x]$. Para demostrar que $(A[x], +)$ es un grupo abeliano es suficiente con probar que $+$ es asociativa, existe un elemento neutro respecto a $+$ y todo elemento $a(x) \in A[x]$ tiene

inverso aditivo.

- Asociatividad:

$$\begin{aligned}
 & [a(x) + b(x)] + c(x) \\
 &= \left[\sum_{i=0}^{\infty} a_i x^i + \sum_{j=0}^{\infty} b_j x^j \right] + \sum_{k=0}^{\infty} c_k x^k && \text{Definición de polinomios} \\
 &= \sum_{m=0}^{\infty} (a_m + b_m) x^m + \sum_{k=0}^{\infty} c_k x^k && \text{Definición de } + \\
 &= \sum_{l=0}^{\infty} (a_l + b_l + c_l) x^l && \text{Definición de } + \\
 &= \sum_{i=0}^{\infty} a_i x^i + \sum_{l=0}^{\infty} (b_l + c_l) x^l && \text{Asociatividad de } A \text{ y definición de } + \\
 &= \sum_{i=0}^{\infty} a_i x^i + \left[\sum_{j=0}^{\infty} b_j x^j + \sum_{k=0}^{\infty} c_k x^k \right] && \text{Definición de } +
 \end{aligned}$$

- El polinomio cero es el elemento neutro de la suma, pues:

$$\begin{aligned}
 a(x) + 0(x) &= \sum_{k=0}^{\infty} a_k x^k + \sum_{j=0}^{\infty} 0 x^j && \text{Definición de polinomio} \\
 &= \sum_{m=0}^{\infty} (a_m + 0) x^m && \text{Definición de } + \\
 &= \sum_{m=0}^{\infty} a_m x^m && \text{Propiedad modulativa en } A \\
 &= a(x) && \text{Definición de polinomio}
 \end{aligned}$$

- El inverso del polinomio $a(x)$ en relación con la operación $+$ está dado por

$$-a(x) = \sum_{k=0}^{\infty} (-a_k)x^k \text{ donde cada } -a_k \text{ es el inverso de } a_k \text{ en } (A, +, \cdot)$$

- Finalmente, como $(A, +)$ es abeliano, de manera directa se verifica que $(A[x], +)$ también lo es.

A continuación se prueban la asociatividad para el producto y la propiedad distributiva del producto respecto de la suma.

■

$$\begin{aligned} & \left[\left(\sum_{i=0}^{\infty} a_i x^i \right) \left(\sum_{j=0}^{\infty} b_j x^j \right) \right] \left(\sum_{k=0}^{\infty} c_k x^k \right) \\ &= \left[\sum_{n=0}^{\infty} \left(\sum_{i=0}^n a_i b_{n-i} \right) x^n \right] \left(\sum_{k=0}^{\infty} c_k x^k \right) && \text{Definición de } \cdot \\ &= \sum_{s=0}^{\infty} \left[\sum_{n=0}^s \left(\sum_{i=0}^n a_i b_{n-i} \right) c_{s-n} \right] x^s && \text{Definición de } \cdot \\ &= \sum_{s=0}^{\infty} \left(\sum_{i+j+k=s} a_i b_j c_k \right) x^s && \text{Asociatividad y distributiva de } A \\ &= \sum_{s=0}^{\infty} \left[\sum_{m=0}^s a_{s-m} \left(\sum_{j=0}^m b_j c_{m-j} \right) \right] x^s && \text{Propiedad distributiva de } A \\ &= \left(\sum_{i=0}^{\infty} a_i x^i \right) \left[\sum_{m=0}^{\infty} \left(\sum_{j=0}^m b_j c_{m-j} \right) x^m \right] && \text{Definición de } \cdot \\ &= \left(\sum_{i=0}^{\infty} a_i x^i \right) \left[\left(\sum_{j=0}^{\infty} b_j x^j \right) \left(\sum_{k=0}^{\infty} c_k x^k \right) \right] && \text{Definición de } \cdot \end{aligned}$$

■

$$\begin{aligned}
& a(x) \cdot [b(x) + c(x)] \\
&= \sum_{i=0}^{\infty} a_i x^i \cdot \left[\sum_{j=0}^{\infty} b_j x^j + \sum_{k=0}^{\infty} c_k x^k \right] && \text{Definición de polinomio} \\
&= \sum_{i=0}^{\infty} a_i x^i \cdot \left[\sum_{m=0}^{\infty} (b_m + c_m) x^m \right] && \text{Definición de } + \\
&= \sum_{n=0}^{\infty} \sum_{i=0}^n a_i (b_{n-i} + c_{n-i}) x^i && \text{Definición de } \cdot \\
&= \sum_{n=0}^{\infty} \sum_{i=0}^n (a_i b_{n-i} + a_i c_{n-i}) x^i && \text{Distributiva de } A \\
&= \sum_{n=0}^{\infty} \sum_{i=0}^n a_i b_{n-i} x^i + \sum_{n=0}^{\infty} \sum_{i=0}^n a_i c_{n-i} x^i && \text{Asociativa en } A \\
&= a(x)b(x) + a(x)c(x) && \text{Definición de } \cdot
\end{aligned}$$

□

Nota: Por simplicidad, de aquí en adelante en vez de escribir el polinomio

$$a(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 x^0 + a_1 x + \cdots + a_n x^n + 0x^{n+1} + 0x^{n+2} + \cdots$$

se escribirá

$$a(x) = a_0 x^0 + a_1 x + \cdots + a_n x^n$$

entendiendo $a_k = 0$ para $k > n$.

Se puede observar que dependiendo de las características del anillo $(A, +, \cdot)$,

resultados (propiedades) usuales de la suma y producto en $\mathbb{R}[x]$ no se tienen en $A[x]$, por ejemplo, al utilizar la multiplicación de polinomios el grado del polinomio resultante no necesariamente es la suma de los grados de los polinomios multiplicados, como sucede en $\mathbb{Z}_8[x]$, $(4x^2+x)(2x^2+1) = 2x^3+4x^2+x$. El siguiente teorema menciona la condición necesaria para analizar el grado del producto de dos polinomios.

Teorema 2.3.2. (Propiedades de la función grado) Si $(A, +, \cdot)$ es un anillo y $a(x), b(x) \in A[x]$ entonces:

$$i) \quad gr(a(x) + b(x)) \leq \max[gr(a(x)), gr(b(x))].$$

$$ii) \quad gr(a(x)b(x)) \leq gr(a(x)) + gr(b(x)).$$

iii) Si $(A, +, \cdot)$ es un dominio de integridad, $(A[x], +, \cdot)$ es un dominio de integridad y por tanto

$$gr(a(x)b(x)) = gr(a(x)) + gr(b(x)).$$

Demostración. Sean $a(x) = \sum_{i=0}^{\infty} a_i x^i$ y $b(x) = \sum_{j=0}^{\infty} b_j x^j$, elementos de $A[x]$ tal que $n = gr(a(x))$ y $m = gr(b(x))$.

i) Por la definición de grado se tiene que $a_i = 0$ para $i > n$ y $b_j = 0$ si $j > m$, luego para $k > \max(m, n)$ se tiene que $a_k + b_k = 0$. Por lo tanto, $gr(a(x) + b(x)) \leq k$.

ii) Suponga que $k > m + n$, por la definición del producto de polinomios se sabe que el coeficiente de x^k en $a(x)b(x)$ viene dado por la expresión:

$$d_k = \sum_{i=0}^k a_i b_{k-i}$$

para $i \leq n$ se tiene $k - i \geq k - n > m$, por lo tanto $b_k = 0$ y en consecuencia:

$$d_k = 0 + \sum_{i=n+1}^k a_i b_{k-i}$$

Ahora, por definición de grado si $i > n$ entonces $a_i = 0$. Se puede así concluir que $d_k = 0$ y por lo tanto $gr(a(x)b(x)) \leq n + m$ ya que d_k no está en el soporte de $a(x)b(x)$.

iii) Sean $a(x), b(x) \in A[x]$ tales que $b(x)q(x) = 0$. El coeficiente principal de este producto es de la forma $a_n b_m$ con $a_n, b_m \in A$, como A es un dominio de integridad, si $a_n \neq 0$ y $b_m \neq 0$ entonces $a_n b_m \neq 0$, así el se debe tener que $a_n = 0$ o $b_m = 0$ implicando que $p(x) = 0$ o $q(x) = 0$, es decir, $A[x]$ es un dominio de integridad.

□

Si $(F, +, \cdot)$ es un campo, no necesariamente $(F[x], +, \cdot)$ es un campo, no obstante, el hecho de que F sea un campo permite abordar nociones como el algoritmo de la división en $(F[x], +, \cdot)$ ya que en este algoritmo se necesita dividir coeficientes principales entre dos polinomios, por tanto, se debe garantizar que dichos coeficientes tengan inversos multiplicativos.

Teorema 2.3.3. Algoritmo de la división en $(F[x], +, \cdot)$. Dados $(F, +, \cdot)$ un campo y $a(x), b(x) \in F[x]$. Si $b(x) \neq 0$ entonces existen únicos polinomios $q(x), r(x) \in F[x]$ tal que

$$a(x) = q(x)b(x) + r(x)$$

donde, $r(x) = 0$ o $gr(r(x)) < gr(b(x))$. A $q(x)$ se le denomina cociente y a $r(x)$ residuo.

Demostración. ⁶ Sean $a(x) = a_0 + a_1x + \dots + a_nx^n$ y $b(x) = b_0 + b_1x + \dots + b_mx^m$ elementos de $F[x]$ tales que $a_n, b_m \neq 0$ y $n > 0$. Considere $S = \{a(x) - s(x)b(x) \mid s(x) \in F[x]\}$, si $0 \in S$ entonces existe un $s(x)$ tal que $a(x) - s(x)b(x) = 0$ de donde, $a(x) = s(x)b(x)$ y tomando $q(x) = s(x)$ y $r(x) = 0$ estaría demostrada la propiedad. Si por el contrario, $0 \notin S$ entonces sea $r(x)$ un elemento de mínimo grado en S , entonces $a(x) - s(x)b(x) = r(x)$ y en consecuencia $a(x) = q(x)b(x) + r(x)$ para algún $q(x) \in F[x]$. Se probará ahora que $gr(r(x)) < gr(b(x)) = m$.

Suponga que

$$r(x) = c_t x^t + c_{t-1} x^{t-1} \dots + c_1 x + c_0$$

con $c_j \in F$ y $c_t \neq 0$.

Si $t \geq m$, entonces $a(x) - q(x)b(x) - (c_t/b_m)x^{t-m}b(x) = r(x) - (c_t/b_m)x^{t-m}b(x)$, este último se puede ver de la forma $r(x) - (c_t x^t + \text{términos de menor grado})$, el cual es un polinomio de grado menor que t , el grado de $r(x)$. Sin embargo, el lado izquierdo de la ecuación puede ser escrito como sigue:

$$a(x) - [q(x) + (c_t/b_m)x^{t-m}]b(x)$$

estando así en S y este hecho contradice que $r(x)$ sea un polinomio de menor grado

⁶Demostración tomada de (Fraleigh, 2003)

escogido en S .

Se concluye así que el grado de $r(x)$ debe ser menor que m , el grado de $b(x)$.

Para la unicidad: Suponga que existen $r_1(x)$, $r_2(x)$, $q_1(x)$, $q_2(x)$ tales que

$$a(x) = q_1(x)b(x) + r_1(x)$$

y

$$a(x) = q_2(x)b(x) + r_2(x)$$

restando se obtiene que

$$[q_1(x) - q_2(x)]b(x) = r_1(x) - r_2(x)$$

debido a que $gr(r_1(x)), gr(r_2(x)) < gr(b(x))$ se sigue $gr(r_1(x) - r_2(x)) < gr(b(x))$ y para que esto pueda suceder se debe tener que $q_1(x) - q_2(x) = 0$, de donde, $q_1(x) = q_2(x)$ y por lo tanto $r_1(x) - r_2(x) = 0$ o lo que es lo mismo $r_1(x) = r_2(x)$. \square

Los siguientes ejemplos tienen como objetivo ilustrar la forma de conseguir los polinomios $r(x)$ y $q(x)$ del teorema inmediatamente anterior empleando el clásico método para dividir.

Ejemplo 2.3.2. *División de polinomios una variable:*

- Considere los polinomios $a(x) = 3x^3 + 2x^2 - 5x + 4$ y $b(x) = x^2 - 2$ en el anillo

$(\mathbb{R}[x], +, \cdot)$.

El cociente de $a(x)$ entre $b(x)$ se halla mediante la siguiente división larga:

$$\begin{array}{r}
 3x^3 + 2x^2 - 5x + 4 \quad \Big| \quad x^2 - 2 \\
 \underline{- 3x^3 \qquad \qquad + 6x} \qquad \Big| \quad 3x + 2 \\
 \qquad \qquad \qquad 2x^2 \quad + x + 4 \\
 \qquad \qquad \qquad \underline{- 2x^2 \qquad \qquad + 4} \\
 \qquad \qquad \qquad \qquad \qquad \qquad x + 8
 \end{array}$$

Se tiene entonces que $q(x) = 3x + 2$ y $r(x) = x + 8$

- En $\mathbb{Z}_5[x]$ considere los polinomios

$$a(x) = x^4 + 2x^3 + 2x^2 + 4x + 4$$

y

$$b(x) = x^2 + 3x + 3$$

Para hallar $q(x)$ y $r(x)$ se procede a realizar la división obteniendo:

Educadora de educadores

- Si $F = \mathbb{Q}$, $E = \mathbb{C}$ y $\alpha = i$, se tiene $\phi_i(x^2 + 1) = 0$, luego i es un cero de $x^2 + 1$.

Los ceros de un polinomio permiten encontrar factores lineales en un polinomio dado (si los hay) para lograr así una factorización de este (si es posible), como lo enuncia el siguiente teorema:

Teorema 2.3.4. (teorema del factor). Sea $(F, +, \cdot)$ un subcampo de un campo $(E, +, \cdot)$. Un elemento $\alpha \in F$ es un cero de $a(x) \in F[x]$ si y sólo si $x - \alpha$ es un factor de $a(x)$, esto es, $a(x) = (x - \alpha)b(x)$ para algún $b(x) \in F[x]$.

Demostración. (\Rightarrow) Suponga que $\alpha \in F$ es un cero de $a(x)$. Se sabe que por el algoritmo de la división existen $q(x), r(x) \in F[x]$ tal que $a(x) = (x - \alpha)q(x) + r(x)$ donde $r(x) = 0$ o $gr(r(x)) < 1$. Si $gr(r(x)) < 1$ entonces $r(x) = c$ para algún $c \in F$, luego $a(x) = (x - \alpha)q(x) + c$. Aplicando la evaluación en α , como α es un cero de $a(x)$ se tiene $\phi_\alpha((x - \alpha)q(x) + c) = 0$, de donde $c = 0$. Se concluye entonces que $a(x) = (x - \alpha)q(x)$.

(\Leftarrow) Si $(x - \alpha)$ es un factor de $a(x)$ entonces $a(x) = (x - \alpha)b(x)$ para algún $b(x) \in F[x]$. Luego, aplicando la evaluación en α queda $\phi_\alpha((x - \alpha)b(x)) = (\alpha - \alpha)b(\alpha) = 0 \cdot b(\alpha) = 0$. □

El siguiente es un ejemplo de aplicación del teorema del factor para dividir polinomios.

Ejemplo 2.3.4. .

- Considere en $(\mathbb{Z}_5[x], +, \cdot)$ el polinomio $x^4 + 3x^3 + 2x + 4$.

$$\begin{array}{r}
 x^4 + 3x^3 + 2x + 4 \quad \left| \begin{array}{l} x + 4 \\ \hline x^3 + 4x^2 + 4x + 1 \end{array} \right. \\
 \underline{-(x^4 + 4x^3)} \\
 4x^3 \\
 \underline{-(4x^3 + x^2)} \\
 4x^2 + 2x \\
 \underline{-(4x^2 + x)} \\
 x + 4 \\
 \underline{-(x + 4)} \\
 0
 \end{array}$$

Luego, $a(x) = (x + 4)(x^3 + 4x^2 + 4x + 1)$.

Aunque se ha factorizado el polinomio $a(x)$, note que $\alpha = 1$ también es un cero del polinomio $x^3 + 4x^2 + 4x + 1$ y por tanto, se puede aplicar el teorema del factor:

$$\begin{array}{r}
 x^3 + 4x^2 + 4x + 1 \quad \left| \begin{array}{l} x + 4 \\ \hline x^2 + 4 \end{array} \right. \\
 \underline{-(x^3 + 4x^2)} \\
 4x + 1 \\
 \underline{-(4x + 1)} \\
 0
 \end{array}$$

Así, $a(x) = (x + 4)^2(x^2 + 4)$.

Una vez más se puede aplicar el teorema del factor al polinomio $x^2 + 4$.

$$\begin{array}{r}
 x^2 \qquad \qquad \qquad + 4 \quad \left| \begin{array}{l} x + 4 \\ x + 1 \end{array} \right. \\
 \hline
 -(x^2 \quad + 4x) \\
 \hline
 \qquad \qquad \qquad x \quad + 4 \\
 \qquad \qquad \qquad -(x \quad + 1) \\
 \hline
 \qquad \qquad \qquad \qquad \qquad \qquad 0
 \end{array}$$

Por lo tanto, $a(x) = (x + 4)^3(x + 1)$.

Otro teorema que relaciona un polinomio con sus ceros en un campo $(F, +, \cdot)$, es el siguiente.

Teorema 2.3.5. *Un polinomio $a(x) \in F[x]$ con $(F, +, \cdot)$ un campo, distinto de 0 y de grado n puede tener a lo sumo n ceros.*

Demostración. Si $\alpha_1 \in F$ es un cero de $a(x)$, entonces $a(x) = (x - \alpha_1)q_1(x)$ donde $gr(q_1(x)) = n - 1$. Un cero $\alpha_2 \in F$ de $q_1(x)$ resulta en una factorización $a(x) = (x - \alpha_1)(x - \alpha_2)q_2(x)$. Continuando con este proceso, se llega a que $a(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)q_r(x)$, donde $q_r(x)$ ya no tiene ceros en F . Como $gr(a(x)) = n$ entonces a lo sumo n factores de la forma $(x - \alpha_i)$ pueden aparecer en la ecuación anterior y en consecuencia $r \leq n$. Además si $b \in F$ y $b \neq \alpha_i$ para $i = 1, 2, \dots, r$ se tiene que

$$\phi_b(a(x)) = (b - \alpha_1)(b - \alpha_2) \cdots (b - \alpha_r)q_r(b) \neq 0$$

Así, ninguno de los $(b - \alpha_i)$ o $q_r(b)$ son cero (por construcción) y por lo tanto, los r elementos α_i son todos los ceros de $a(x)$ en $(F, +, \cdot)$. \square

Al polinomio $q_r(x)$ de la anterior demostración se le conoce con el nombre de polinomio irreducible. Para ampliar este concepto, se presenta la siguiente definición.

Definición 2.3.5. *Un polinomio no constante $a(x) \in F[x]$, se dice que es un **polinomio irreducible en $F[x]$** o que es irreducible sobre F si $a(x)$ no puede ser expresado como un producto de dos polinomios $b(x), c(x) \in F[x]$ ambos de menor grado que $\text{gr}(a(x))$. Si $a(x) \in F[x]$ no es irreducible sobre F entonces se dice que es **reducible sobre F** .*

Note que en la anterior definición se enfatiza en que el polinomio sea irreducible sobre F , esto se hace debido a que un polinomio puede ser irreducible sobre un campo $(F_1, +, \cdot)$ pero reducible sobre otro campo distinto $(F_2, +, \cdot)$. Los siguientes son ejemplos de este hecho.

Ejemplo 2.3.5. .

- *El polinomio $x^2 + 4$ es irreducible sobre \mathbb{Q} , sin embargo, es reducible sobre \mathbb{C} pues $x^2 + 4 = (x + 2i)(x - 2i) \in \mathbb{C}[x]$.*
- *El polinomio $a(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$ es irreducible, pues por el teorema del factor, si fuese reducible existiría $\alpha \in \mathbb{Z}_5$ tal que $\phi_\alpha(a(x)) = 0$, no obstante, $\phi_0(a(x)) = 2$, $\phi_1(a(x)) = 1$, $\phi_2(a(x)) = 1$, $\phi_3(a(x)) = 3$ y $\phi_4(a(x)) = 3$.*

2.3.1. Ideales en $(F[x], +, \cdot)$

Una observación que surge a partir del algoritmo de la división en un anillo de polinomios sobre un campo, es que si al dividir $a(x)$ entre $b(x)$ se obtiene un residuo

cero, entonces $a(x) \in \langle b(x) \rangle$, debido al colorario 2.2.1. En esta sección se presentan un par de resultados que involucran ideales de polinomios.

Se ha dicho ya que todo ideal en $(\mathbb{Z}, +, \cdot)$ es principal, sin embargo, esto no pasa en $(\mathbb{Z}[x], +, \cdot)$, es decir, no todo ideal $I \subset \mathbb{Z}[x]$ es principal, por ejemplo, si se toma un $p \in \mathbb{Z}$ primo, el ideal $\langle p, x \rangle$ no es principal, dado que al suponer lo contrario, debe existir $a(x) \in \mathbb{Z}[x]$ tal que $\langle p, x \rangle = \langle a(x) \rangle$, así, por el colorario 2.2.1, existe un $q(x) \in \mathbb{Z}[x]$ tal que $q(x)a(x) = p$ y $gr(q(x)a(x)) = gr(p) = 0$, en consecuencia $gr(a(x)) = 0$, $a(x) \in \mathbb{Z}$ y $a(x)|p$. Así, $a(x) = \pm 1$ o $a(x) = \pm p$.

En el primer caso se tiene que $\langle p, x \rangle = \mathbb{Z}[x]$, por lo tanto deben existir $m(x), n(x) \in \mathbb{Z}[x]$ de manera que $1 = pm(x) + xn(x)$, observe que para que esto pueda suceder, el polinomio $xn(x)$ debe anularse con el producto de $pm(x)$, así en $m(x)$ debe existir un término independiente $m_0 \in \mathbb{Z}$ de manera que $1 = pm_0$ lo que resulta en una contradicción debido a que $p \nmid 1$.

En el segundo caso se tendría $\langle p, x \rangle = \langle p \rangle$, lo que implica que $x = pq(x)$ con $q(x) \in \mathbb{Z}[x]$, así, $q(x)$ debe ser de la forma q_0x , con $q_0 \in \mathbb{Z}$, de lo contrario se obtendría un polinomio con potencias de x distintas a 1, por lo tanto se sigue la igualdad $1 = pq_0$ lo cual es imposible.

Por lo anterior, se sigue un teorema que permite caracterizar ideales principales de $(F[x], +, \cdot)$:

Teorema 2.3.6. *Si $(F, +, \cdot)$ es un campo, entonces todo ideal en $(F[x], +, \cdot)$ es principal.*

Demostración. Sea I un ideal de $(F[x], +, \cdot)$. Si $I = \{0\}$ entonces $I = \langle 0 \rangle$, si por el contrario $I \neq \{0\}$, tome un $b(x) \in I$ cuyo grado sea mínimo. Si $gr(b(x)) = 0$ entonces $b(x) \in F$ y por lo tanto es una unidad, en consecuencia $I = \langle 1 \rangle = (F[x], +, \cdot)$, siendo I principal. Por otro lado, si $gr(b(x)) \geq 1$, tome cualquier elemento $a(x) \in I$, entonces por el algoritmo de la división $a(x)$ se puede escribir como sigue:

$$a(x) = b(x)q(x) + r(x)$$

con $gr(r(x)) = 0$ o $gr(r(x)) < gr(b(x))$, $q(x), r(x) \in I$. Ahora, como $a(x), b(x) \in I$ se concluye gracias a la definición de ideal que $a(x) - b(x)q(x) = r(x) \in I$ y como $b(x)$ es un elemento de mínimo grado en I y es distinto de 0, $r(x) = 0$. Por lo tanto $a(x) = b(x)q(x)$ y $I = \langle b(x) \rangle$. \square

El siguiente resultado relaciona los ideales principales de $(F[x], +, \cdot)$ con sus ideales maximales.

Teorema 2.3.7. *Un ideal $\langle a(x) \rangle \neq \{0\}$ de $(F[x], +, \cdot)$ es maximal si y solo si $a(x)$ es irreducible sobre F .*

Demostración. (\Rightarrow) Suponga $\langle a(x) \rangle \neq \{0\}$ que es un ideal maximal de $(F[x], +, \cdot)$. Entonces $\langle a(x) \rangle \neq F[x]$, luego $a(x) \notin F$. Sea $a(x) = b(x)q(x)$ una factorización de $a(x)$ en $F[x]$. Como $\langle a(x) \rangle$ es un ideal maximal, entonces también es un ideal primo, luego como $a(x) = b(x)q(x) \in \langle a(x) \rangle$ se tiene que $b(x) \in \langle a(x) \rangle$ o $q(x) \in \langle a(x) \rangle$, esto es, cualquiera de los dos tiene a $a(x)$ como factor, pero entonces no se tendría que $gr(b(x)) < gr(a(x))$ y $gr(q(x)) < gr(a(x))$. Esto muestra que $a(x)$ es irreducible sobre

F .

(\Leftarrow) Si $a(x)$ es irreducible sobre F , suponga que I es un ideal tal que $\langle a(x) \rangle \subset I \subset F[x]$. Ahora, I es un ideal principal debido al teorema anterior, luego existe un $b(x) \in F[x]$ tal que $I = \langle b(x) \rangle$. Como $a(x) \in I$ se sigue que $a(x) = b(x)q(x)$ para algún $q(x) \in F[x]$. Sin embargo, como $a(x)$ es irreducible entonces o bien $b(x)$ es de grado 0 o $q(x)$ es de grado 0. Si $gr(b(x)) = 0$ entonces $b(x) \in F$ y es una unidad, por lo tanto $\langle b(x) \rangle = I = F[x]$. Si $gr(q(x)) = 0$ entonces $q(x) = c \in F$ y en consecuencia $b(x) = \frac{1}{c}a(x) \in \langle a(x) \rangle$, luego, $I = \langle a(x) \rangle$. Así, tener que $\langle a(x) \rangle \subset I \subset F[x]$ es imposible y se concluye que $\langle a(x) \rangle$ es maximal. \square

Este teorema permite afirmar que, por ejemplo, el ideal $\langle x^2 + 1 \rangle$ es maximal en $\mathbb{R}[x]$ y de igual manera, los ideales generados por los polinomios dados en el ejemplo 2.3.5 son maximales. Además, también permite concluir que si $a(x)$ es irreducible entonces $(F[x]/\langle a(x) \rangle, +, \cdot)$ es un campo, en virtud del teorema 2.2.12.

Ejemplo 2.3.6. .

- Sea $x^2 + c \in \mathbb{Z}_3[x]$, si $\alpha \in \mathbb{Z}_3$ es una raíz de $x^2 + c$ en $F[x]$ entonces $\alpha = 0, 1$ o 2 , es decir, $0^2 + c = 0$ o $1^2 + c = 0$ y $2^2 + c = 0$, lo cual se puede resumir en que $c = 0$ o $1 + c = 0$. De aquí se puede afirmar que si $c = 0$ o $c = 2$ el polinomio $x^2 + c$ es reducible en $\mathbb{Z}_3[x]$ debido al teorema del factor. Por lo tanto, $x^2 + 1$ es un polinomio irreducible en \mathbb{Z}_3 y en consecuencia $\mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$ es un campo.
- Sea $a(x) = x^2 + cx + 1 \in \mathbb{Z}_5[x]$, usando el teorema del factor para encontrar

factores lineales de $a(x)$, tomando $x = 0, 1, 2, 3$ o 4 se llega a:

$$2 + c = 0, 2c = 0, 3c = 0, 2 + 4c = 0$$

luego, $c = 0, 2, 3$. Así, $\mathbb{Z}_5[x]/\langle x^2 + x + 1 \rangle$ y $\mathbb{Z}_5[x]/\langle x^2 + 4x + 1 \rangle$ son campos.

Finalmente, los dos teoremas anteriores permiten demostrar que dado cualquier polinomio no constante en la variable x existe un campo en el cual este polinomio tenga un cero.

Teorema 2.3.8. *Sea $(F, +, \cdot)$ un campo y $a(x) \in F[x]$ un polinomio no constante, entonces existe un campo $(E, +, \cdot)$ que contiene a $(F, +, \cdot)$ y $\alpha \in E$ tal que $\phi_\alpha(a(x)) = 0$.*

La demostración de este resultado se puede encontrar, por ejemplo, en (Fraleigh, 2003).

2.3.2. Polinomios en varias variables

Siguiendo la idea utilizada para definir un anillo de polinomios en la variable sobre un anillo $(A, +, \cdot)$, se puede definir, de forma recursiva, un anillo en dos variables. Particularmente se define el anillo $((A[x_1])[x_2], +, \cdot)$ como el anillo de polinomios en la variable x_2 con coeficientes en $A[x_1]$. Se puede demostrar que $((A[x_1])[x_2], +, \cdot)$ y $((A[x_2])[x_1], +, \cdot)$ son isomorfas, esto es, son iguales como estructura (para ampliar esta idea, el lector puede referirse a (Hungerford, 2012)). Además, si

$T_{x_1, x_2} = \{x_1^i x_2^j \mid i, j \in \mathbb{N}\}$, un polinomio $a(x_1, x_2) \in (A[x_1])[x_2]$, puede ser visto como

una expresión formal $\sum_j^\infty \sum_i^\infty a_{ij} x_1^i x_2^j$ con $a_{ij} \in A$, en otras palabras los elementos de T_{x_1, x_2} se convierten en una base para los polinomios en las variables x_1, x_2 . Denotando al conjunto de las expresiones formales sobre la base T_{x_1, x_2} como $A[x_1, x_2]$ se puede demostrar que hay un isomorfismo entre $((A[x_1])[x_2], +, \cdot)$ y $(A[x_1, x_2], +, \cdot)$.

Este tratamiento recursivo puede extenderse para definir anillos de polinomios en las variables x_1, x_2, \dots, x_n como el construido a partir del anillo de polinomios con las $n - 1$ variables x_1, x_2, \dots, x_{n-1} , es decir, $((A[x_1, x_2, \dots, x_{n-1}])[x_n], +, \cdot)$, no obstante, es más fácil trabajar con el anillo isomorfo $(A[x_1, \dots, x_n], +, \cdot)$, de expresiones tomadas con base T_{x_1, x_2, \dots, x_n} y coeficientes en A .

Sin embargo, para definir bien los elementos del anillo $(A[x_1, x_2, \dots, x_n], +, \cdot)$ es conveniente incluir las siguientes definiciones:

Definición 2.3.6. Sean x_1, x_2, \dots, x_n variables y $(A, +, \cdot)$ un anillo.

- Un **monomio** definido a partir de x_1, \dots, x_n es un producto formal de la forma $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, donde $\alpha_i \in \mathbb{N}$ para $i = 1, 2, \dots, n$. Al conjunto T_{x_1, \dots, x_n} de todas los monomios de esta forma se le llamará base canónica de $A[x_1, x_2, \dots, x_n]$ el cual es el conjunto de todas las expresiones formales

$$\sum_{\alpha_1} \sum_{\alpha_2} \cdots \sum_{\alpha_n} a_{\alpha_1, \dots, \alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \text{ de elementos de } T_{x_1, \dots, x_n} \text{ con coeficientes en } A.$$

Un **término** definido a partir de x_1, \dots, x_n es el producto entre un elemento $a \in A$ y un monomio.

Un **polinomio** definido a partir de x_1, \dots, x_n es una suma de finita de términos, esto es, la suma formal

$$a(x_1, \dots, x_n) = \sum_{\alpha_1}^{\infty} \sum_{\alpha_2}^{\infty} \cdots \sum_{\alpha_n}^{\infty} a_{(\alpha_1, \dots, \alpha_n)} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

donde el soporte $S_c = \{a_{(\alpha_1, \alpha_2, \dots, \alpha_n)} \in A \mid (\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0\}$ es finito.

- El grado de un monomio se define como:

$$gr_m(x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}) = \sum_{i=1}^n \alpha_i$$

- El grado de $a(x_1, \dots, x_n) = \sum_{\alpha_1} \sum_{\alpha_2} \cdots \sum_{\alpha_n} a_{(\alpha_1, \dots, \alpha_n)} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in A[x_1, \dots, x_n]$ es definido como:

$$gr(a(x_1, x_2, \dots, x_n)) = \text{máx}[gr_m(x_1^{\alpha_1} \cdots x_n^{\alpha_n})]$$

Ejemplo 2.3.7. Sean x, y variables y $A = \mathbb{Z}$. El polinomio

$$a(x, y) = (10x^3)y^4 - (5x^3 - x^2)y^2 + (3x^2 + 2x + 1)y + (-3x^4 + 1)$$

es un elemento de $(\mathbb{Z}[x])[y] \sim \mathbb{Z}[x, y]$.

Observe que $a(x, y)$ se puede escribir como elemento de $(\mathbb{Z}[y])[x]$ como sigue:

$$a(x, y) = (-3)x^4 + (10y^4 - 5y^2)x^3 + (y^2 + 3)x^2 + (2y)x + (y + 1)$$

y a su vez, como combinación de los elementos $x^3y^4, x^3y^2, x^2y^2, x^2y^0, xy, x^0y, x^4y^0, x^0y^0 \in T_{x,y}$.

$$a(x, y) = 10x^3y^4 - 5x^3y^2 + x^2y^2 + 3x^2 + 2xy + y - 3x^4 + 1$$

El grado de $a(x, y)$ es:

$$\text{máx}[gr(x^3y^4), gr(x^3y^2), gr(x^2y^2), gr(x^2y^0), gr(xy), gr(x^0y), gr(x^4y^0)] = 7$$

Para simplificar la notación, al monomio $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ se denotará como X^α , entendiendo a X como el vector (x_1, x_2, \dots, x_n) y a α como $(\alpha_1, \alpha_2, \dots, \alpha_n)$. Cuando $\alpha = (0, 0, \dots, 0)$ se tiene que $X^\alpha = 1$. De esta manera, en vez de escribir $a(x_1, x_2, \dots, x_n) \in A[x_1, x_2, \dots, x_n]$, se escribirá $a(X) \in A[X]$. Así mismo, la expresión

$\sum_{\alpha_1=0}^{\infty} \sum_{\alpha_2=0}^{\infty} \cdots \sum_{\alpha_n=0}^{\infty} a_{(\alpha_1, \dots, \alpha_n)} x^{\alpha_1} \cdots x_n^{\alpha_n}$ será simplificada por $\sum_{i=1}^k a_i X^{\alpha_i}$ ya que S_a es finito.

La aritmética de polinomios en varias variables se puede extender a partir de la operaciones entre monomios como sigue:

Definición 2.3.7. Sean $aX^\alpha, bX^\beta \in A[x_1, x_2, \dots, x_n]$.

- Se dice que aX^α es semejante a bX^β notado por $aX^\alpha \sim bX^\beta$, si $X^\alpha = X^\beta$, es decir, si $\alpha_i = \beta_i$ para $1 \leq i \leq n$.

- Si $aX^\alpha \sim bX^\beta$ entonces la suma de términos se define por:

$$aX^\alpha + bX^\beta = (a + b)X^\alpha$$

- El producto de términos está dado por:

$$aX^\alpha \cdot bX^\beta = abX^{\alpha+\beta}$$

donde $\alpha + \beta = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$.

- La suma de $a(X), b(X) \in A[X]$, se define por:

$$\begin{aligned} a(X) + b(X) &= \sum_{i=1}^n a_i X^{\alpha_i} + \sum_{j=1}^m b_j X^{\beta_j} \\ &= \sum_{k=1}^{\max(m,n)} (a_k X^{\alpha_k} + b_k X^{\beta_k}) \end{aligned}$$

Sobre entendiéndose que si $m < n$ entonces $b_k = 0$ para $k > m$. En el caso en que $n < m$ entonces $a_k = 0$ para $k > n$.

Educadora de educadores

- El producto $a(X) \cdot b(X) \in A[X]$ es:

$$\begin{aligned}
 a(X) \cdot b(X) &= a(x_1, \dots, x_n) \cdot b(x_1, \dots, x_n) \\
 &= \sum_{i=0}^n (a_i X^{\alpha_i} \sum_{j=1}^m b_j X^{\beta_j}) \\
 &= \sum_{i=0}^n \sum_{j=0}^m (a_i b_j X^{\alpha_i} X^{\beta_j}) \\
 &= \sum_{i=0}^n \sum_{j=0}^m (a_i b_j X^{\alpha_i + \beta_j})
 \end{aligned}$$

Nota: De aquí en adelante, un polinomio $a(X) \in A[X]$ se considerará como una expresión sin términos semejantes, por ejemplo, el polinomio $a(x, y) = 2xy^2 - 5xy^2 \in \mathbb{Z}[x, y]$ se reducirá a $a(x, y) = -3xy^2$.

Con estas operaciones así definidas se puede probar que $(A[x_1, x_2, \dots, x_n], +, \cdot)$ es un anillo isomorfo a $((A[x_1, x_2, \dots, x_{n-1}])[x_n], +, \cdot)$ véase (Hungerford, 2012).

Una de las cuestiones que naturalmente aparece es: ¿sigue funcionando el algoritmo de la división cuando se tiene un anillo de polinomios en varias variables? es decir, dados polinomios $a(X), b(X) \in A[X]$, con $gr(b) \leq gr(a)$ ¿existen únicos polinomios q y r de manera que $a = qb + r$ y $gr(r) < gr(b)$? La respuesta corta a esta pregunta es **no** pues como se verá más adelante, para poder dividir polinomios se debe definir un orden para los monomios y como resultado se obtiene un cociente y residuo que depende del orden.

Ejemplo 2.3.8. .

- Sean $a(x, y) = 4x^2y^3 + 3xy^2$ y $b(x, y) = x^2 + y^2$ polinomios en $\mathbb{R}[x, y]$, el cociente de $a(x, y)$ entre $b(x, y)$ al ordenar de forma descendente ambos polinomios con respecto a las potencias de la variable x , se obtiene al dividir el término mayor con respecto al orden escogido $a(x, y)$ con el término de mayor de $b(x, y)$ y proceder a multiplicar este cociente por cada uno de los términos de $b(x, y)$, para finalmente sustraer el polinomio resultante de $a(x, y)$.

El algoritmo finaliza si el grado del polinomio resultante con respecto a la variable x es menor al grado de $b(x, y)$, de lo contrario, se divide el término mayor del polinomio resultante entre el término mayor de $b(x, y)$. El cociente de esta división será la suma de todos los cocientes parcialmente obtenidos en cada división parcial y el residuo será el polinomio obtenido después de la última resta:

$$\begin{array}{r|l} 4y^3x^2 + 3y^2x & x^2 + y^2 \\ - 4y^3x^2 & - 4y^5 \\ \hline & 3y^2x - 4y^5 \end{array}$$

$q(x, y) = 4y^3$ y el residuo $r(x, y) = 3y^2x - 4y^5$.

Así como se realizó la división con respecto al orden determinado por la variable x , también se puede hacerlo ordenando los monomios con respecto a las

potencias de y para obtener:

$$\begin{array}{r|l}
 4x^2y^3 + 3xy^2 & y^2 + x^2 \\
 - 4x^2y^3 & \hline
 3xy^2 - 4x^4y & 4x^2y + 3x \\
 - 3xy^2 & \\
 \hline
 - 4x^4y - 3x^3 &
 \end{array}$$

$$q(x, y) = 4x^2y + 3x, \quad r(x, y) = -4x^4y - 3x^3.$$

Se puede notar en ambos casos que $gr(b(x, y)) < gr(a(x, y))$ y el residuo $r(x, y)$ no es un polinomio de menor grado que el de $b(x, y)$, además, tampoco existen únicos $q(X)$ y $r(X)$ tales que $a(X) = q(X)b(X) + r(X)$ lo que permite concluir que no se satisface el algoritmo de la división como fue planteado para el caso de una variable.

Lo anterior se da, entre otras cosas porque $(A[X], +, \cdot)$, no es un dominio de integridad y por otro lado, T_{x_1, \dots, x_n} no es un conjunto totalmente ordenado, como sucede para una sola variable, donde $T_x = \{x^0, x, x^2, \dots\}$ es totalmente ordenado por la función grado. Por ejemplo, si se piensa en los monomios x^2y^4 y x^3y^3 , a priori no es posible decidir cuál es mayor puesto que ambos tienen grado 6.

Para resolver este problema y a su vez también poder realizar una división, se deben ordenar los monomios. Hay varias formas de ordenación, por ejemplo, podemos ordenar los monomios de forma ascendente o descendente según el grado del monomio y en caso de que se tengan monomios del mismo grado se procede a ordenar con respecto a una variable.

Suponga que se desea ordenar el polinomio de $\mathbb{Z}[x, y]$:

$$a(x, y) = x^2 + 4xy^2 + 7xy + 5x + y^2 + 2$$

Para cada término tomamos su grado,

$$gr_m(x^2) = 2, gr_m(4xy^2) = 3, gr_m(7xy) = 2, gr_m(5x) = 1, gr_m(y^2) = 2, gr_m(2) = 0$$

El orden en forma descendente según el grado queda:

$$4xy^2 > y^2, x^2, 7xy > 5x > 1$$

Ahora, para poder comparar los tres términos de segundo grado se ordena de forma descendente con respecto a la variable x para obtener:

$$4xy^2 > x^2 \succ 7xy \succ y^2 > 5x > 1.$$

Este orden recibe el nombre de **Lexicográfico graduado**.

Como se ha dicho antes, existen más ordenaciones distintas a la aquí mostrada, algunas de estas no servirán para el objetivo de este trabajo y por lo tanto se definen las condiciones que debe satisfacer un orden para que sea admisible y algunos ejemplos de estos ordenes.

Definición 2.3.8. .

- **Un orden admisible de los monomios** en T_X es un orden total $<_{T_X}$ sobre los elementos de T_X que satisface las siguientes dos condiciones:
 - i) Si $X^\alpha \neq 1$ entonces $1 <_{T_X} X^\alpha$ para todo $X^\alpha \in T_X$.
 - ii) Si $X^\alpha <_{T_X} X^\beta$ entonces $X^\alpha X^\gamma <_{T_X} X^\beta X^\gamma$ para todo $X^\gamma \in T_X$.

- Dado un orden admisible $<_{T_X}$ en T_X y $a(X) \in A[X]$, se dice que un monomio X^α es el **monomio principal** de $a(X)$ respecto a $<_{T_X}$, si X^α es el máximo de los monomios que aparecen en $a(X)$ y es denotado por $MP(a(X))$, el **coeficiente principal**, $CP(a(X))$, es el coeficiente que acompaña a al monomio principal en $a(X)$ y el **término principal** es $TP(a(X)) = CP(a(X)) \cdot MP(a(X))$.

En el siguiente ejemplo se definen algunos ordenes admisibles

Ejemplo 2.3.9. .

- Se define el orden **lexicográfico** ($<_l$) sobre T_X como:

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} <_l x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$$

sí y solo sí existe un i de manera que $\alpha_i < \beta_i$ y $\alpha_k = \beta_k$ para $1 \leq k < i$.

Teorema 2.3.9. El orden lexicográfico ($<_l$) es un orden admisible:

Demostración. .

- i) Definiendo $1 = x_1^0 x_2^0 \cdots x_n^0$, si $X^\alpha \neq 1 \in T_X$ se tiene que existe un $\alpha_j \in \{\alpha_1, \cdots, \alpha_n\}$ tal que $\alpha_j \neq 0$, por lo tanto, se puede tomar

$\alpha_i = \min\{\alpha_j \in \{\alpha_1, \dots, \alpha_n\} \mid \alpha_j \neq 0\}$. Así $\alpha_i > 0$ y $\alpha_k = 0$ para $1 \leq k < i$, por lo tanto, $1 <_l X^\alpha$.

ii) Si $X^\alpha <_l X^\beta$ entonces existe $i \in \{1, 2, \dots, n\}$ tal que $\beta_i > \alpha_i$ y $\beta_k = \alpha_k$ para $1 \leq k < i$. Luego, para todo $\gamma_k \in \mathbb{N}$, $k \in \{1, 2, \dots, n\}$ se tiene que $\beta_k + \gamma_k > \alpha_k + \gamma_k$ y si $i \neq k$ $\beta_i + \gamma_i = \alpha_i + \gamma_i$. Por lo tanto:

$$x_1^{\alpha_1 + \gamma_1} x_2^{\alpha_2 + \gamma_2} \dots x_n^{\alpha_n + \gamma_n} <_l x_1^{\beta_1 + \gamma_1} x_2^{\beta_2 + \gamma_2} \dots x_n^{\beta_n + \gamma_n}$$

$$X^{\alpha + \gamma} <_l X^{\beta + \gamma}$$

$$X^\alpha X^\gamma <_l X^\beta X^\gamma$$

□

- El orden **lexicográfico inverso** es el definido por:

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} <_{\text{inv}} x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}$$

sí y sólo si existe $i \in \{1, \dots, n\}$ tal que $\alpha_i > \beta_i$ y $\alpha_k = \beta_k$ para $1 \leq k < i$.

- El orden **lexicográfico graduado inverso** es el definido por:

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} <_{\text{ginv}} x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}$$

sí y solo sí $gr(x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}) < gr(x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n})$ o, si

$gr(x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}) = gr(x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n})$ entonces existe un i de manera que

$\alpha_i > \beta_i$ y $\alpha_k = \beta_k$ para $i < k \leq n$.

- Si $a(x, y, z) = 3x^4z - 2x^3y^4 + 7x^2y^2z^3 - 8xy^3z^3 \in \mathbb{Q}[x, y, z]$, $a(x, y, z)$ se encuentra ordenado en forma descendente respecto a $<_l$, además:

$$MP(a(x, y, z)) = x^4z, CP(a(x, y, z)) = 3, TP(a(x, y, z)) = 3x^4z.$$

El orden de $a(x, y, z)$ en forma descendente respecto al orden graduado lexicográfico inverso ($<_{l_{inv}}$) es :

$$a(x, y, z) = -2x^3y^4 + 7x^2y^2z^3 - 8xy^3z^3 + 3x^4z$$

Aquí,

$$MP(a(x, y, z)) = x^3y^4, CP(a(x, y, z)) = -2, TP(a(x, y, z)) = -2x^3y^4.$$

Nótese que a partir de la definición del orden lexicográfico se tiene que $x_n <_l x_{n-1} <_l \dots <_l x_3 <_l x_2 <_l x_1$. Usualmente se acostumbra a identificar las variables x_1, x_2, x_3 con x, y, z respectivamente, entonces bajo el orden lexicográfico se tiene que $z <_l y <_l x$, no obstante, en ocasiones se necesita justamente la relación inversa tal como se ejemplifica en 2.3.8, en ese caso se puede hacer la distinción $x_1 = z$, $x_2 = y, x_3 = x$ o utilizar el orden lexicográfico inverso.

Ahora ya se tienen todos los ingredientes para poder formular un algoritmo de la división en el anillo $(A[X], +, \cdot)$. Sin embargo, para una mayor comprensión, se

hará un análisis del proceso de división en una variable tomando como referencia el ejemplo 2.3.2.

Suponga que se desea dividir el polinomio $x^4 - 3x^3 + 2x^2 + 4x$ entre $x^2 - 2x + 3$ pero esta vez en $\mathbb{Q}[x]$.

El primer paso es dividir el término principal x^4 del dividendo y dividirlo entre el término principal del divisor x^2 , esto es $\frac{x^4}{x^2} = x^2$, luego multiplicamos este cociente por cada uno de los términos del divisor, esto es:

$$x^2(x^2 - 2x + 3) = x^4 + 2x^3 + 3x^2,$$

el siguiente paso es restar este último polinomio del dividendo tal como se muestra a continuación:

$$\begin{array}{r} x^4 - 3x^3 + 2x^2 + 4x - 1 \quad \Big| \quad x^2 - 2x + 3 \\ -x^4 + 2x^3 - 3x^2 \\ \hline -x^3 - x^2 + 4x - 1 \end{array}$$

Ahora se procede a dividir el término principal del residuo entre el término principal del divisor y se obtiene como resultado $\frac{-x^3}{x^2} = -x$, se multiplica este por cada uno de los términos del divisor y se resta del residuo obtenido anteriormente así:

$$\begin{array}{r} x^4 - 3x^3 + 2x^2 + 4x - 1 \quad \Big| \quad x^2 - 2x + 3 \\ -x^4 + 2x^3 - 3x^2 \\ \hline -x^3 - x^2 + 4x \\ x^3 - 2x^2 + 3x \\ \hline -3x^2 + 2x - 1 \end{array}$$

Se repite el proceso dividiendo $\frac{-3x^2}{x^2} = -3$

$$\begin{array}{r}
 x^4 - 3x^3 + 2x^2 + 4x - 1 \quad | \quad x^2 - 2x + 3 \\
 -x^4 + 2x^3 - 3x^2 \\
 \hline
 -x^3 - x^2 + 4x \\
 x^3 - 2x^2 + 3x \\
 \hline
 -3x^2 + 2x - 1 \\
 3x^2 - x + 4 \\
 \hline
 x + 3
 \end{array}$$

Este algoritmo termina cuando el término principal del divisor, en este caso x^2 , no divide al término principal del residuo, es decir, x .

Lo anterior motiva a la siguiente definición la cuál permite generalizar el algoritmo para el caso de múltiples variables:

Definición 2.3.9. .

- Dados $a, b, c \in A[X]$ con $c \neq 0$ y el conjunto T_X ordenado bajo un orden admisible $<_{T_X}$, se dice que a se **reduce** a b módulo c en un paso, escrito como

$$a \xrightarrow{c} b,$$

si y sólo si $TP(c)$ divide a un término no cero $a_i X^\alpha$ que aparece en a y

$$b = a - \frac{a_i X^\alpha}{TP(c)} c$$

- Dados a, b y c_1, c_2, \dots, c_s polinomios en $A[X]$, con $c_i \neq 0$, $1 \leq i \leq s$, se dice

que a es **reducido** a b modulo $C = \{c_1, c_2, \dots, c_s\}$, denotado como

$$a \xrightarrow{C}_+ b,$$

si y sólo si existe una secuencia de índices $i_1, i_2, \dots, i_t \in \{1, \dots, s\}$ y una secuencia de polinomios $b_1, \dots, b_{t-1} \in A[X]$ de modo que:

$$a \xrightarrow{c_{i_1}} b_1 \xrightarrow{c_{i_2}} b_2 \xrightarrow{c_{i_3}} \dots \xrightarrow{c_{i_{t-1}}} b_{t-1} \xrightarrow{c_{i_t}} b$$

- Un polinomio $r \in A[X]$ es llamado **reducido** con respecto al conjunto de polinomios distintos de cero $C = \{c_1, c_2, \dots, c_s\}$, si $r = 0$ o ningún término que aparece en r es divisible por ninguno de los $TP(c_i), i = 1, \dots, s$, en otras palabras, r no puede ser reducido módulo C .
- Si $a \xrightarrow{C}_+ r$ y r es reducido con respecto C , entonces r es llamado el **residuo** de a con respecto a C .

Con lo anterior se justifican las divisiones mostradas en el **ejemplo 2.3.8**, pues como se mostrará en el siguiente ejemplo, hay una equivalencia entre la reducción y la división. Además, con la definición anterior también se puede dividir un mismo polinomio entre otros varios a la vez.

Ejemplo 2.3.10. .

- Sean los polinomios $a(x) = 6x^4 + 13x^3 - 6x + 1$, $c(x) = 3x^2 + 5x - 1$ en $(\mathbb{Q}[x], +, \cdot)$. $a(x)$ se reduce a $b(x) = 3x^3 + 2x^2 - 6x + 1$ mediante $c(x)$ si se

- Sean $a(x) = -3x^5 + 11x^3 - 46x^2 + 32$, $c(x) = -3x^2 - 6x + 8$ entonces $a \xrightarrow{C} b = 0$

con:

$$b_1 = -3x^5 + 11x^3 - 46x^2 + 32 - \frac{-46x^2}{-3x^2}(-3x^2 - 6x + 8)$$

$$b_1 = -3x^5 + 11x^3 + 92x - \frac{272}{3}$$

$$b_2 = -3x^5 + 11x^3 + 92x - \frac{272}{3} - \frac{11x^3}{-3x^2}(-3x^2 - 6x + 8)$$

$$b_2 = -3x^5 - 22x^2 + \frac{364}{3}x - \frac{272}{3}$$

$$b_3 = -3x^5 - 22x^2 + \frac{364}{3}x - \frac{272}{3} - \frac{-22x^2}{-3x^2}(-3x^2 - 6x + 8)$$

UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

$$\begin{aligned}
b_3 &= -3x^5 + \frac{496}{3}x - \frac{448}{3} \\
b_4 &= -3x^5 + \frac{496}{3}x - \frac{448}{3} - \frac{-3x^5}{-3x^2}(-3x^2 - 6x + 8) \\
b_4 &= 6x^4 - 8x^3 + \frac{496}{3}x - \frac{448}{3} \\
b_5 &= 6x^4 - 8x^3 + \frac{496}{3}x - \frac{448}{3} - \frac{6x^4}{-3x^2}(-3x^2 - 6x + 8) \\
b_5 &= -20x^3 + 16x^2 + \frac{496}{3}x - \frac{448}{3} \\
b_6 &= -20x^3 + 16x^2 + \frac{496}{3}x - \frac{448}{3} - \frac{16x^2}{-3x^2}(-3x^2 - 6x + 8) \\
b_6 &= -20x^3 + \frac{400}{3}x - \frac{320}{3} \\
b_7 &= -20x^3 + \frac{400}{3}x - \frac{320}{3} - \frac{-20x^3}{-3x^2}(-3x^2 - 6x + 8) \\
b_7 &= 40x^2 + 80x - \frac{320}{3} \\
b &= 40x^2 + 80x - \frac{320}{3} - \frac{40x^2}{-3x^2}(-3x^2 - 6x + 8) \\
b &= 0
\end{aligned}$$

Note que si

$$\begin{aligned}
u(x) &= \frac{-46x^2}{-3x^2} + \frac{11x^3}{-3x^2} + \frac{-22x^2}{-3x^2} + \frac{-3x^5}{-3x^2} + \frac{6x^4}{-3x^2} + \frac{16x^2}{-3x^2} + \frac{-20x^3}{-3x^2} + \frac{40x^2}{-3x^2} \\
&= x^3 - 2x^2 + 3x + 4
\end{aligned}$$

Se tiene que:

$$a(x) = u(x)c(x)$$

Considere $(\mathbb{Q}[x, y], +, \cdot)$, el polinomio $a(x, y) = x^3y^3 + 2y^2$ el conjunto

$C = \{c_1(x) = 2xy^2 + 4y^2 + 3x, c_2(x) = y^2 - 2y - 2\}$ y el orden lexicográfico con $x < y$.

Se desea calcular $b(x, y)$ tal que $a \xrightarrow{C} b$:

Primero encontramos los b_i :

$$b_1 = x^3y^3 + 2y^2 - \frac{x^3y^3}{2xy^2}(2xy^2 + 4y^2 + 3x)$$

$$b_1 = -2x^2y^3 + 2y^2 - \frac{3}{2}x^3y$$

$$b_2 = -2x^2y^3 + 2y^2 - \frac{3}{2}x^3y - \frac{-2x^2y^3}{2xy^2}(2xy^2 + 4y^2 + 3x)$$

$$b_2 = 4xy^3 + 2y^2 - \frac{3}{2}x^3y + 3x^2y$$

$$b_3 = 4xy^3 + 2y^2 - \frac{3}{2}x^3y + 3x^2y - \frac{4xy^3}{2xy^2}(2xy^2 + 4y^2 + 3x)$$

$$b_3 = -8y^3 + 2y^2 - \frac{3}{2}x^3y + 3x^2y - 6xy$$

$$b_4 = -8y^3 + 2y^2 - \frac{3}{2}x^3y + 3x^2y - 6xy - \frac{-8y^3}{y^2}(y^2 - 2y - 2)$$

$$b_4 = -14y^2 - \frac{3}{2}x^3y + 3x^2y - 6xy - 16y$$

$$b_5 = -14y^2 - \frac{3}{2}x^3y + 3x^2y - 6xy - 16y - \frac{-14y^2}{y^2}(y^2 - 2y - 2)$$

$$b = b_5 = -\frac{3}{2}x^3y + 3x^2y - 6xy - 44y - 28.$$

Nuevamente, haciendo:

$$q_1 = \frac{x^3y^3}{2xy^2} + \frac{-2x^2y^3}{2xy^2} + \frac{4xy^3}{2xy^2}$$

$$q_1 = \frac{1}{2}x^2y - xy + 2y.$$

$$q_2 = \frac{-8y^3}{y^2} + \frac{-14y^2}{y^2}$$

$$q_2 = -8y - 14$$

Se tiene que $a(x, y) = (2xy^2 + 4y^2 + 3x)q_1 + (y^2 - 2y - 2)q_2 + b$.

Este ejemplo permite observar un resultado que generaliza el algoritmo de la división y el cual es enunciado en el siguiente teorema:

Teorema 2.3.10. *Dado $a \in A[X]$, un conjunto de polinomios $C = \{c_1, c_2, \dots, c_s\} \subseteq A[X]$ tal que cada c_i es distinto de cero y un orden admisible para los monomios \langle_{TX} . Entonces existen polinomios $q_1, q_2, \dots, q_s, r \in A[X]$ tales que:*

$$a = q_1c_1 + q_2c_2 + \dots + q_sc_s + r$$

Con r reducido respecto a C y

$$MP(a) = \max \left[\max_{1 \leq i \leq s} (MP(q_i) \cdot MP(c_i)), MP(r) \right]$$

Demostración. A continuación se indicarán las ideas principales de la demostración, el lector interesado puede revisar la prueba completa de este en (Adams y Loustau-nau, 1994).

- Los polinomios q_i se obtienen mediante la reducción de a en el conjunto C , es decir, se tiene una secuencia de polinomios c_i tales que a se reduce a r . Observe que a medida que se hace la reducción a un paso, los términos principales de los cocientes (en la definición los b_i), van desapareciendo y se crea una cadena descendiente donde $TP(b_{i+1}) < TP(b_i)$, como esta relación es un buen orden el algoritmo debe parar.
- Por el orden mencionado en el ítem anterior cuando ya no sea posible seguir haciendo las reducciones a un paso el $MP(r) \leq MP(a)$

□

Note que como consecuencia de este teorema se tiene que $a-r \in \langle c_1, c_2, \dots, c_s \rangle$ y por lo tanto, si $r = 0$, $a \in \langle c_1, c_2, \dots, c_s \rangle$, sin embargo, el recíproco no es cierto, es decir, si a pertenece al ideal generado por $C = \{c_1, \dots, c_s\}$ no necesariamente el residuo de la reducción de a módulo C es cero como se hace evidente en el siguiente ejemplo.

Ejemplo 2.3.11. Sean $a = y^2x - x \in \mathbb{Q}[x, y]$, $C = \{yx - y, y^2 - x\} \subset \mathbb{Q}[x, y]$ Usando el orden lexicográfico graduado tenemos que:

$$y^2x - x \xrightarrow{yx-y} y^2 - x \xrightarrow{y^2-x} 0$$

luego $y^2x - x = y(yx - y) + (y^2 - x)$, así, $y^2x - x \in \langle yx - y, y^2 - x \rangle$.

Sin embargo, si la reducción se realiza cambiando el orden de los c_i tenemos

$$y^2x - x \xrightarrow{y^2-x} x^2 - x$$

Note que $r = x^2 - x$ ya está reducido respecto a C , sin embargo, haciendo esta reducción no es posible determinar si $y^2x - x$ pertenece o no al ideal $\langle C \rangle$.

De la primera parte del ejemplo se tiene que $a \in \langle C \rangle$. Además, se puede probar que $\langle C \rangle = \langle yx - y, y^2 - x, x^2 - x \rangle$, es decir, se incluye el polinomio obtenido en la segunda parte del ejemplo como elemento generador; así, cambiando el orden de los polinomios de este nuevo generador de $\langle C \rangle$ siempre se obtendrá el mismo residuo al hacer una reducción. En el siguiente capítulo se ahondará en las características de este conjunto de generadores en particular.

El problema que este ejemplo trata de presentar recibe el nombre de **ideal membership** y consiste en que dado un $a \in A[X]$ y un ideal $I \subset A[X]$, se debe decidir si $a \in I$ o no. Este problema se trata de solucionar encontrando un “mejor” conjunto generador de I y será abordado más adelante.

2.4. Ideales en $A[x_1, x_2, \dots, x_n]$

En esta sección se abordarán algunos hechos sobre los ideales en $A[x_1, \dots, x_n]$. Para esto, se hace necesario recordar que a partir del corolario 2.2.1 se tiene que el

ideal generado por el conjunto de polinomios $\{c_1, \dots, c_s\} \subset A[X]$ es de la forma:

$$\langle c_1, \dots, c_s \rangle = \left\{ \sum_{i=1}^s u_i c_i \mid u_i \in A[X], i = 1, \dots, s \right\}$$

La primera observación es que, a diferencia de lo que sucede con un anillo de polinomios en una variable, si se tiene un anillo de polinomios en varias variables sobre un campo, este no es anillo de ideales principales.

Por ejemplo, el ideal $I = \langle x, y \rangle \subset \mathbb{Q}[x, y]$, no es principal pues de lo contrario existiría un $p \in \mathbb{Q}[x, y]$ tal que $\langle x, y \rangle = \langle p \rangle$, $x = u_1 p$ y $y = u_2 p$; así, el grado de $u_1 p$ respecto a la variable x es 1 y el grado de u_2 respecto a y es 1 también, con lo que grado de p debe ser a lo más 1 y se puede concluir que p es de la forma:

$$p = c_0 + c_1 x + c_2 y + c_3 xy$$

con $c_0, c_1, c_2, c_3 \in \mathbb{Q}$. De aquí, $x = u_1 p = u_1(c_0 + c_1 x + c_2 y + c_3 xy)$ y por tanto $c_3 = 0$. Como $c_0 + c_1 x + c_2 y \in \langle x, y \rangle$, $c_0 = 0$. Finalmente, $y = u_2(c_1 x + c_2 y)$ de donde $c_1 = 0$ y en consecuencia $x = u_1(c_2 y)$ lo cual es una contradicción.

Otro resultado sobre los ideales en $A[X]$ y útil para nuestro propósito es el conocido como el teorema de la base de Hilbert el cuál se enuncia a continuación:

Teorema 2.4.1. *En el anillo $(A[X], +, \cdot)$ se tiene que:*

- *Si I es un ideal de $A[X]$, entonces existen polinomios $c_1, \dots, c_s \in A[X]$ tales que $I = \langle c_1, c_2, \dots, c_s \rangle$.*

- Si $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n \subseteq \dots$ es una cadena ascendente de ideales de $A[X]$, entonces existe $N \in \mathbb{N}$ tal que $I_N = I_{N+1} = I_{N+2} = \dots$.

En otras palabras, este teorema afirma que todo ideal en $A[X]$ es finitamente generado y que dado un ideal I siempre se podrá encontrar un ideal maximal que lo contenga.

Es de resaltar que un ideal $I \subset A[X]$ puede tener diferentes bases, es decir, diferentes conjuntos de polinomios c_1, c_2, \dots, c_s que lo generen, por el ejemplo, $\langle x, y \rangle = \langle x + y, y \rangle$, ya que si $a(x, y) \in \langle x, y \rangle$ entonces $a(x, y) = u_1(x, y)x + u_2(x, y)y$, para $u_1(x, y), u_2(x, y) \in A[x, y]$, pero este también puede ser visto como $a(x, y) = u_1(x, y)(x + y) + [u_1(x, y) - u_2(x, y)]y$, es decir, $\langle x, y \rangle \subseteq \langle x + y, y \rangle$, por otro lado, si $b(x, y) \in \langle x + y, y \rangle$, $b(x, y) = u_1^*(x, y)(x + y) + u_2^*(x, y)y = u_1^*(x, y)x + [u_1^*(x, y) + u_2^*(x, y)]y$ obteniéndose así la otra contención.

Para finalizar, es importante mencionar que el estudio de ideales en $(F[X], +, \cdot)$ abarca muchos otros temas aparte de los que se trabajan en este documento, por ejemplo, su uso para la factorización, es por esto que se omiten resultados que tal vez puedan interesar al lector pero que podrá encontrar en cualquier bibliografía sobre álgebra abstracta como, por ejemplo, la que se encuentra relacionada en este documento.

Bases de Gröbner

3.1. Base de Gröbner definición y caracterización.

El algoritmo de la división trabajado en el capítulo anterior es el que finalmente permite abordar el objeto de estudio de este trabajo, las bases de Gröbner, y mediante el uso de esta herramienta se tendrá como una de sus aplicaciones el resolver el problema del **ideal membership** mencionado también en el capítulo anterior.

Ahora si, finalmente se tienen todas las herramientas para poder definir las bases de Gröbner como sigue. De aquí en adelante se entenderá que el anillo de coeficientes de todo anillo de polinomios es conmutativo, con identidad y Noetheriano.

Definición 3.1.1. *Sea I un ideal de $(A[X], +, \cdot)$. Un conjunto de polinomios $G = \{g_1, g_2, \dots, g_t\} \subset I$ es llamado una **base de Gröbner** para I si y sólo si para todo $c \in I$, $c \neq 0$, existe un $i \in \{1, 2, \dots, t\}$ tal que $MP(g_i)$ divide a $MP(c)$. En general si $I = \langle G \rangle$ entonces se dirá simplemente que G es una base de Gröbner.*

Ejemplo 3.1.1.

- Es evidente que si $a(x) \in \mathbb{Q}[x]$ entonces $G = \{a(x)\}$ es una base de Gröbner para el ideal $I = \langle a(x) \rangle$.
- $G = \{x, y\} \subset \mathbb{Q}[x, y]$ es una base de Gröbner respecto al orden lexicográfico $(<_l)$

Demostración. (Por contradicción). Suponga que existe un $c \in \mathbb{Q}[x, y]$ tal que $x \nmid MP(c)$ y $y \nmid MP(c)$, se tendría entonces que $c \in \mathbb{Q}$ y como $\frac{1}{c} \in \mathbb{Q}$ por definición de ideal se sigue que $1 = \frac{1}{c} \cdot c \in \langle x, y \rangle$ obteniendo así la contradicción: $\langle x, y \rangle = \mathbb{Q}[x, y]$ por el teorema 2.2.4. \square

- $G = \{g_1 = x + z, g_2 = y - z\} \subset \mathbb{Q}[x, y, z]$, es una base de Gröbner respecto a $(<_l)$.

Demostración. Para $c \in I$ se tiene que $c = h_1(x + z) + h_2(y - z)$ para algunos $h_1, h_2 \in \mathbb{Q}[x, y, z]$ o de forma equivalente $c = h_1x + h_2y + h_1z - h_2z$.

Si $MP(h_1) \geq MP(h_2)$ se tendrá que $MP(c) = MP(h_1)x$ esto debido al orden lexicográfico, luego $x \mid MP(c)$.

Considere ahora, $MP(h_1) < MP(h_2)$. Si $MP(h_1) = 0$ entonces

$MP(c) = MP(h_2)y$ por el orden lexicográfico y por tanto $MP(c)$ es divisible por y .

Si $MP(h_1) \neq 0$ entonces $MP(h_2)$ contiene a una potencia de x , de lo contrario $MP(c) = MP(h_1)x$, así $MP(c)$ en consecuencia debe contener una potencia de x .

Los dos casos anteriores conducen a que $MP(c)$ es divisible bien sea por x o y . \square

- El ideal I generado por los polinomios dados en el ejemplo 2.3.11 no forman una base de Gröbner con respecto al orden lexicográfico, pues $c = 4xy + 7x + 4y^2 = 2xy^2 + 3x + 4y^2 - 2x(y^2 - 2y - 2)$ es un elemento de I , pero $4xy$ no es divisible por $2xy^2$ o y^2 .
- Sean $g_1 = x + z$, $g_2 = -x + y \in \mathbb{Q}[x, y, z]$, considere el orden $<_l$, $I = \langle g_1, g_2 \rangle$ y $G = \{g_1, g_2\}$. Entonces G no es una base de Gröbner para I pues $c = y + z \in I$ y $MP(c) = y$ no es divisible por $MP(x + z) = x$ o $MP(-x + y) = -x$.

Se darán ahora otras caracterizaciones para una base de Gröbner, sin embargo, por simplicidad se definirá el siguiente conjunto:

Definición 3.1.2. Sea $S \subset A[X]$ se define el **ideal de términos principales de S** como el ideal ideal generado por los términos principales de los polinomios en S , esto es:

$$T(S) = \langle TP(S) \rangle, \text{ donde, } TP(S) = \{TP(s) \mid s \in S\}$$

Teorema 3.1.1. Sea I un ideal no cero de $A[X]$ y $G = \{g_1, \dots, g_t\} \subset I$. Las siguientes afirmaciones son equivalentes:

- i) G es una base de Gröbner para I .
- ii) $c \in I$ si y sólo si $c \xrightarrow{G} 0$.
- iii) $c \in I$ si y sólo si $c = \sum_{i=1}^t h_i g_i$ con $MP(c) = \max_{1 \leq i \leq t} [MP(h_i) \cdot MP(g_i)]$.

iv) $T(G) = T(I)$.

Demostración. ¹ i) \Rightarrow ii). (\Rightarrow) Sea $c \in A[X]$. Por el **Teorema 2.3.10**, existe un $r \in A[X]$ reducido respecto de G , tal que $c \xrightarrow{G}_+ r$. Así, se tiene que $c - r \in I$ y en consecuencia $c \in I$ si y sólo si $r \in I$, en particular, si $r = 0$ entonces $c \in I$.

(\Leftarrow) Si $c \in I$ y $r \neq 0$ entonces $r \in I$ y por i) existe un $i \in \{1, \dots, t\}$ tal que $TP(g_i)$ divide a $TP(r)$. Esto contradice el hecho de que r es reducido con respecto a G . Por lo tanto, $r = 0$ y $c \xrightarrow{G}_+ 0$.

ii) \Rightarrow iii). (\Rightarrow) Para $c \in I$, sabemos por hipótesis que $c \xrightarrow{G}_+ 0$ y por tanto por el teorema 2.3.10 tenemos que $c = \sum_{i=1}^t h_i g_i$.

(\Leftarrow) Si $c = \sum_{i=1}^t h_i g_i$ entonces por el colorario 2.2.1 $c \in I$.

iii) \Rightarrow iv). Como $G \subseteq I$ entonces $T(G) \subseteq T(I)$. Ahora, sea $c \in I$, entonces por hipótesis $c = \sum_{i=1}^t h_i g_i$, así se tiene que

$$TP(c) = \sum_i TP(h_i)TP(g_i)$$

donde la suma está sobre todos los i tal que $MP(c) = MP(h_i)MP(g_i)$. Por lo tanto $T(I) \subseteq T(G)$.

iv) \Rightarrow i). Si $c \in I$ entonces $TP(c)$ está en $T(G)$ y por lo tanto,

$$TP(c) = \sum_{i=1}^t h_i TP(g_i)$$

¹Tomado de (Adams y Loustaunau, 1994)

Para algún $h_i \in A[X]$, al expandir el lado derecho de esta igualdad, se tiene que cada término es divisible por algún $TP(g_i)$, entonces $TP(c)$, el único término al lado izquierdo es también divisible por algún $TP(g_i)$

□

Como corolario de este teorema se tiene:

Colorario 3.1.1. Si $G = \{g_1, \dots, g_t\}$ es una base de Gröbner para el ideal I , entonces $I = \langle g_1, \dots, g_t \rangle$.

Demostración. Como cada $g_i \in I$ entonces $\langle g_1, \dots, g_t \rangle \subseteq I$. Por otro lado, si $c \in I$ por el teorema anterior $c \xrightarrow{G}_+ 0$, y en consecuencia $c \in \langle g_1, \dots, g_t \rangle$, es decir,

$I \subseteq \langle g_1, \dots, g_t \rangle$.

□

Note que hasta el momento se ha definido y caracterizado lo que es una base de Gröbner para un ideal $I \subset A[X]$, sin embargo, una de las cuestiones que naturalmente aparece es: ¿para todo ideal existe una base de Gröbner? Con objeto de responder a esta pregunta, se presentan los siguientes resultados:

Teorema 3.1.2. Sea I un ideal generado por un conjunto de términos S y $c \in A[X]$. Entonces $c \in I$ si y sólo si para cada término aX^α que aparece en c existe otro término $bX^\beta \in S$ que divide a aX^α . Más aún, existe un subconjunto finito S_0 de S tal que $I = \langle S_0 \rangle$.

Demostración. (\Rightarrow) Si $c \in I$ entonces $c = \sum_{i=0}^l u_i a_i X^{\alpha_i}$ con $u_i \in A[X]$, $a_i X^{\alpha_i} \in S$.

Al expandir el lado derecho se hace evidente que cada término que aparece en c es

divisible por un término $a_i X_i^\alpha \in S$.

(\Leftarrow) Si para cada término aX^α que aparece en c existe un término $bX^\beta \in S$ que divide a aX^α entonces cada uno de estos $aX^\alpha \in I = \langle S \rangle$ y en consecuencia $c \in I$.

Finalmente, para probar la última afirmación del teorema, se parte de que I es finitamente generado por un conjunto S' , debido al teorema de la base de Hilbert.

Por lo acabado de demostrar, cada término aX^α que aparece en cada polinomio $c = \sum_{i=0}^k u_i a_i X_i^\alpha$ de S' es divisible por un $bX^\beta \in S$, así, se puede escribir entonces $c = \sum_{i=0}^k u'_i b_i X_i^\beta$, escogiendo $S_0 = \{bX^\beta \mid c = \sum_{i=0}^k u'_i b_i X_i^\beta\}$ se obtiene un subconjunto finito de S generador de I . \square

Colorario 3.1.2. *Todo ideal $I \subseteq A[X]$ distinto de cero tiene una base de Gröbner.*

Demostración. Por el teorema anterior el ideal de términos principales $T(I)$ es finitamente generado por un conjunto el cual podemos asumir $\{TP(g_1), \dots, TP(g_t)\}$ con $\{g_1, \dots, g_t\} \subseteq I$. Si se toma $G = \{g_1, \dots, g_t\}$, entonces $T(G) = T(I)$ y por consiguiente, G es una base de Gröbner para I por el teorema 3.1.1. \square

El hecho de que exista una base de Gröbner para cualquier ideal I permite encontrar en algunas ocasiones una representación de los polinomios en I que es “más amigable” para trabajar como se evidencia en el siguiente ejemplo:

Ejemplo 3.1.2. .

- Sea $I = \langle x^2 + 2x, x^2 - 4 \rangle \subset \mathbb{Q}[x]$. Si $c \in I$ entonces para algunos $u_1, u_2 \in \mathbb{Q}[x]$

se tiene que:

$$\begin{aligned} c &= u_1(x^2 + 2x) + u_2(x^2 - 4) \\ &= u_1(x + 2)x + u_2(x + 2)(x - 2) \\ &= [u_1x + u_2(x - 2)](x + 2). \end{aligned}$$

Luego, $c \in \langle x + 2 \rangle$ si y sólo si $c \xrightarrow{x+2} 0$. Así, por el teorema 3.1.1, $\langle x + 2 \rangle$ es una base de Gröbner para I y por el colorario 3.1.2, $\langle x^2 + 2x, x^2 + 4 \rangle = \langle x + 2 \rangle$.

- Sean $G = \{g_1, \dots, g_t\} \subset F[x]$ con $(F, +, \cdot)$ un campo y $d = \text{MCD}(g_1, \dots, g_t)$. Entonces G es una base de Gröbner para $I = \langle G \rangle$ si y sólo si existe un $a \neq 0 \in F$ tal que $ad \in G$.

Demostración. (\Rightarrow). Por propiedades del MCD, se tiene que existen $h_i \in F[x]$ de tal manera que $d = h_1g_1 + h_2g_2 + \dots + h_tg_t$, es decir, $d \in \langle G \rangle$, por lo tanto, $TP(d)$ es divisible por $TP(g_k)$ para algún $g_k \in G$. Por otro lado, como $d|g_i$ para todo $1 \leq i \leq t$ entonces $gr(d) \leq gr(g_i)$, sin embargo, si $gr(d) < gr(g_i)$, G no sería una base de Gröbner y por lo tanto se debe tener que $gr(d) = gr(g_i)$ para todo i . Por lo tanto, $g_i = c_id$, con $c_i \in F$. \square

- Sean $I = \langle d \rangle$ un ideal principal de $(F[X], +, \cdot)$ y $G = \{g_1, \dots, g_t\} \subseteq I$ con $(F, +, \cdot)$ un campo. $G \subseteq I$ es una base de Gröbner para I si y sólo si $cd \in G$ para algún $c \in F$ tal que $c \neq 0$.

Demostración. (\Rightarrow). Como $G \subseteq I$ entonces $d \in \langle G \rangle$, al ser G una base de

Gröbner, existe $g_k \in G$ tal que $MP(g_k) | MP(d)$. Por otro lado, como $g_k \in I$ se tiene que $g_k = cd$ con $c \in F[X]$. Si $gr(c) > 0$ entonces $gr(g_k) > gr(d)$ pues $(F, +, \cdot)$ es un campo, así se tendría que $MP(g_k)$ no dividiría a $MP(d)$, lo cual es una contradicción. Por lo tanto $gr(c) = 0$ y en consecuencia $c \in F$.

(\Leftarrow). Si $p \in I$ entonces $p = ud$ y como $cd \in G$ entonces $p = \frac{1}{c}u(cd)$, la conclusión se sigue inmediatamente del ítem iii) del Teorema 3.1.1. \square

- Sea $\{g_1, \dots, g_t\} \subseteq F[X]$ y $0 \neq h \in F[X]$. $\{g_1, \dots, g_t\}$ es una base de Gröbner si y sólo si $\{hg_1, \dots, hg_t\}$ es una base de Gröbner.

Demostración. (\Rightarrow). Obsérvese que si $c \in \langle hg_1, \dots, hg_t \rangle$ entonces $c = \sum_{i=1}^t u_i hg_i$ y en consecuencia $c \in \langle g_1, \dots, g_t \rangle$ y al ser esta una base de Gröbner entonces $MP(c)$ es divisible por $MP(g_k)$ para algún $k \in \{1, 2, \dots, t\}$. De esta forma $MP(hg_k)$ divide al máximo de los monomios principales de los $u_i hg_i$ y este máximo es $MP(c)$, además, como $h|c$, entonces $MP(h) | MP(c)$, $MP(c)$ es divisible por $MP(hg_k)$ y por lo tanto, $\langle hg_1, \dots, hg_t \rangle$ es una base de Gröbner.

(\Leftarrow). Sea $c \in \langle g_i \rangle$ luego $c = \sum u_i g_i$, $ch = \sum hu_i g_i$, $hc \in \langle hg_i \rangle$ como esa es base de G , existe hg_k tal que $MP(hg_k) | MP(hc)$ Como $\{hg_1, \dots, hg_t\}$ es una base de Gröbner, por el ítem iii) del Teorema 3.1.1, $c \in \langle hg_1, \dots, hg_t \rangle$ si y sólo si $c = \sum_{i=1}^t u_i hg_i$ con $MP(c) = \max_{1 \leq i \leq t} [MP(u_i)(hg_i)]$, como $(F, +, \cdot)$ es un campo $MP(c)$ también puede ser visto como

$\max_{1 \leq i \leq t} [MP(u_i h)MP(g_i)]$. Por otro lado, obsérvese que $c \in \langle g_1, \dots, g_t \rangle$ y nuevamente por el Teorema 3.1.1 $\{g_1, \dots, g_t\}$ es una base de Gröbner. \square

A partir del Teorema 3.1.1 se puede observar que la **Definición 3.1.1** es equivalente a decir que si G es una base de Gröbner entonces ningún polinomio en el ideal I es reducido respecto de G , sin embargo, se puede hacer una apreciación más general partiendo desde $A[X]$, esto se hace caracterizando una base de Gröbner mediante el teorema que se presenta a continuación y cuya demostración el lector la podrá encontrar de forma más detallada en (Adams y Loustaunau, 1994):

Teorema 3.1.3. *Sea $G = \{g_1, \dots, g_t\} \subset F[X]$ donde cada $g_i \neq 0$. G es una base de Gröbner si y sólo si para todo $c \in F[X]$ el residuo de la división por G es único.*

Demostración. (\Rightarrow) Suponga que $c \xrightarrow{G}_+ r_1$ y $c \xrightarrow{G}_+ r_2$, como $c - r_1$ y $c - r_2$ están ambos en $\langle G \rangle$ entonces $r_1 - r_2 \in G$ y por tanto, $r_1 - r_2$ se reduce a cero módulo G debido al teorema 3.1.1, es decir, $r_1 - r_2 = 0$, por tanto, $r_1 = r_2$.

(\Leftarrow) Ahora se busca demostrar que se cumple el segundo ítem del teorema 3.1.1. Si $c \in \langle G \rangle$ entonces basta mostrar que $c \xrightarrow{G}_+ r$ con $r = 0$. \square

Este último resultado aunque parece generalizar la caracterización de una base de Gröbner, extendiéndola a todo el anillo $(F[X], +, \cdot)$, no es muy eficiente para encontrar una base de Gröbner G para un ideal dado, pues se debería verificar que para todos los elementos de $F[X]$, los cuales pueden ser infinitos, el residuo de la división con G es único sin importar el orden de los elementos de G , además, dependiendo del cardinal de G , la reducción se puede tornar tediosa pues es necesario tener en cuenta todos los distintos ordenes de G en que se puede realizar dicha división. No obstante, si se pueden descartar subconjuntos de $F[X]$ que no formen

una base de Gröbner, por ejemplo, el conjunto $G = \{yx - y, y^2 - x\}$ no es una base de Gröbner, pues como se vio en el **ejemplo 2.3.11**, $y^2x - x \xrightarrow{G}_+ 0$ y $y^2x - x \xrightarrow{G}_+ y^2 - x$.

3.2. S-polinomios y el algoritmo de Buchberger

En la sección anterior se definió lo que es una base de Gröbner y se afirmó que todo ideal admite una, sin embargo, no se mencionó cómo encontrarla a partir de un ideal dado. Esta sección se enfoca en estudiar un algoritmo para poder hallar una base de Gröbner para un ideal $I \subset F[X]$, a partir de este punto, sólo se consideraran anillos de polinomios cuyos coeficientes se encuentran en un campo F .

Teniendo en la cuenta el último teorema de la sección anterior (**Teorema 3.1.3**), puede suceder que cuando se hace la división de $c \in F[X]$ entre los elementos de G , algún término aX^α que aparece en c sea divisible por $MP(g_i)$ y $MP(g_j)$ para algunos $g_i, g_j \in G$ con $i \neq j$. Suponga que se decide reducir c entre g_i se obtendrá el polinomio $h_1 = c - \frac{aX^\alpha}{TP(g_i)}g_i$, por otro lado, si en lugar de reducir por g_i se elige g_j el resultado será $h_2 = c - \frac{aX^\alpha}{TP(g_j)}g_j$. De aquí se sigue la expresión $h_2 - h_1 = \frac{aX^\alpha}{TP(g_i)}g_i - \frac{aX^\alpha}{TP(g_j)}g_j$ la cual motiva a la siguiente definición y de la que desprende un resultado útil para hallar la base de Gröbner buscada.

Definición 3.2.1. Sean $g_1, g_2 \in F[X]$ distintos de cero y $L = \text{mcm}(MP(g_1), MP(g_2))$ respecto a un orden $<_T$. El polinomio:

$$S(g_1, g_2) = \frac{L}{TP(g_1)}g_1 - \frac{L}{TP(g_2)}g_2$$

es llamado el S – polinomio de g_1 y g_2 .

Para ilustrar esta definición se propone el siguiente ejemplo:

Ejemplo 3.2.1. .

- Sean $g_1 = 3x^2yz - y^3z^3$, $g_2 = xy^2 + z^2 \in \mathbb{Q}[x, y, z]$ y \prec_l .

Entonces, $L = \text{mcm}(x^2yz, xy^2) = x^2y^2z$ y

$$\begin{aligned} S(g_1, g_2) &= \frac{x^2y^2z}{3x^2yz}(3x^2yz - y^3z^3) - \frac{x^2y^2z}{xy^2}(xy^2 + z^2) \\ &= -xz^3 - \frac{1}{3}y^4z^3 \end{aligned}$$

- Considérense los polinomios del ítem anterior y el orden lexicográfico graduado.

El S -polinomio sería:

$$\begin{aligned} S(g_1, g_2) &= \frac{xy^3z^3}{-y^3z^3}(-y^3z^3 + 3x^2yz) - \frac{xy^3z^3}{xy^2}(xy^2 + z^2) \\ &= 3x^3yz - z^2 \end{aligned}$$

- Para el conjunto $G = \{x^4y + 2xy^3 + 5x^3, x^2y^2 - 3xy, xy^4 + xy^2\} \subset \mathbb{Z}_7[x, y]$ y el

orden $<_{lq}$, se tienen los siguientes S – polinomios.

$$\begin{aligned} S(x^4y + 2x^3y + 5x^3, x^2y^2 - 3xy) &= \frac{x^4y^3}{x^4y}(x^4y + 2x^3y + 5x^3) - \frac{x^4y^3}{x^2y^2}(x^2y^2 - 3xy) \\ &= x^4y^3 + 2x^3y^3 + 5x^3y^2 - x^4y^3 + 3x^3y^2 \\ &= 2x^3y^3 + x^3y^2 \end{aligned}$$

$$\begin{aligned} S(x^4y + 2x^3y + 5x^3, xy^4 + xy^2) &= \frac{x^4y^4}{x^4y}(x^4y + 2x^3y + 5x^3) - \frac{x^4y^4}{xy^4}(xy^4 + xy^2) \\ &= x^4y^4 + 2x^3y^4 + 5x^3y^3 - x^4y^4 - x^4y^2 \\ &= 2x^3y^4 + 6x^4y^2 + 5x^3y^3 \end{aligned}$$

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

Un par de resultados acerca de los S – polinomios y para los cuales el lector podrá encontrar su demostración en (Adams y Loustaunau, 1994) son los siguientes dos teoremas:

Teorema 3.2.1. *Dados $c_1, c_2, \dots, c_s \in F[X]$ tales que $MP(c_i) = MP(c_j) \neq 0$ para todo $i, j = 1, \dots, s$ y dado $c = \sum_{i=1}^s f_i c_i$, con $f_i \in F$. Si $MP(c) < MP(c_i)$, entonces c es una combinación lineal de $S(c_i, c_j)$, cuyos coeficientes pertenecen a F .*

Como se dijo antes, la definición 3.2.1 proporciona un método para encontrar una base de Gröbner mediante el teorema que sigue a continuación y cuya prueba se encuentra con más detalle en (Adams y Loustaunau, 1994), el cual es conocido como teorema de Buchberger en reconocimiento al matemático austriaco Bruno Buchberger.

Teorema 3.2.2. *Sea $G = \{g_1, \dots, g_t\} \subset F[X]$ tal que cada $g_i \neq 0$. G es una base de Gröbner si y sólo si para todo $i \neq j$ se tiene que:*

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

Demostración. (\Rightarrow). Si $G = \{g_1, \dots, g_t\}$ es una base de Gröbner para $I = \langle g_1, \dots, g_t \rangle$, entonces $S(g_i, g_j) \xrightarrow{G}_+ 0$ para todo $i \neq j$ por el teorema 3.1.1, debido a que $S(g_i, g_j) \in I$.

(\Leftarrow). Se usará el ítem *iii*) del teorema 3.1.1 para probar que G es una base de Gröbner. Sea $c \in I$, entonces este puede ser escrito de muchas maneras como combinación lineal de los g_i . Por ejemplo:

$$c = \sum_{i=1}^t h_i g_i, \text{ con } X = \max_{1 \leq i \leq t} (MP(h_i)MP(g_i)).$$

Si $X = TP(c)$ se termina la demostración. De lo contrario, si $X < TP(C)$ se debe encontrar otra representación de c con un X más pequeño lo cual conducirá a una contradicción. \square

Ejemplo 3.2.2. .

- Se verá que $G = \{y^3 - 2y, xy - 2y, x^2 - 2y^2\}$ es una base de Gröbner considerando el orden lexicográfico.

Calculando los S – polinomios se obtiene:

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

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

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

Ahora, el siguiente paso corresponde a verificar que cada uno de los S –

polinomios es reducido a cero respecto de G .

$$\begin{aligned}
 r_1 &= 2y^3 - 2xy - \frac{2y^3}{y^3}(y^3 - 2y) \\
 &= 2y^3 - 2xy - 2y^3 + 4y \\
 &= -2xy + 4y \\
 r_2 &= -2xy + 4y - \frac{-2xy}{xy}(xy - 2y) \\
 &= -2xy + 4y + 2xy - 4y \\
 &= 0.
 \end{aligned}$$

Así, $S(y^3 - 2y, x^2 - 2y^2) \xrightarrow{G} 0$.

Del mismo modo,

$$S(y^3 - 2y, xy - 2y) \xrightarrow{xy-2y} -4xy + 2y^5 \xrightarrow{xy-2y} 2y^5 - 8y \xrightarrow{y^3-2y} -8y + 4y^3 \xrightarrow{y^3-2y} 0$$

y

$$S(xy - 2y, x^2 - 2y^2) = -2xy + 2y^3 \xrightarrow{xy-2y} -2y^3 + 4y \xrightarrow{y^3-2y} 0.$$

- Retómese el conjunto $G = \{x^4y + 2xy^3 + 5x^3, x^2y^2 - 3xy, xy^4 + xy^2\}$ del ejemplo 3.2.1 y sus S -polinomios obtenidos.

Como,

$$6x^2y^2 + 4xy^3 \xrightarrow{G} 4xy^3 + 4xy$$

se concluye que G no es una base de Gröbner para $\langle G \rangle$.

Para hallar una base de Gröbner usando este teorema, se debe reducir cada S – *polinomio* en G y si el residuo no es cero, se agrega este residuo al conjunto de generadores. Se debe repetir este proceso hasta que todos los S – *polinomios* posibles se reduzcan a cero.

Ejemplo 3.2.3. .

- Sea $I = \langle g_1 = xy - x, g_2 = x^2 - y \rangle \subset \mathbb{Q}[x, y], <_{lginv}$.

$$\begin{aligned} S(g_1, g_2) &= \frac{x^2y}{xy}(xy - x) - \frac{x^2y}{x^2}(x^2 - y) \\ &= (x^2y - x^2) - (x^2y - y^2) \\ &= y^2 - x^2. \end{aligned}$$

Como

$$y^2 - x^2 \xrightarrow{x^2-y} \left[y^2 - x^2 - \frac{-x^2}{x^2}(x^2 - y) = y^2 - y \right]$$

entonces,

$$y^2 - x^2 \xrightarrow{G} y^2 - y,$$

luego, haciendo $g_3 = y^2 - y$, al ser este residuo no cero, se debe agregar al conjunto generador G , quedando:

$$G_1 = \{xy - x, x^2 - y, y^2 - y\}.$$

Obsérvese que el hecho de haber agregado a g_3 hace que $S(g_1, g_2) \xrightarrow{G} 0$.

Veamos ahora si los otros S – polinomios también se reducen a cero:

$$\begin{aligned} S(g_1, g_3) &= \frac{xy^2}{xy}(xy - x) - \frac{xy^2}{y^2}(y^2 - y) \\ &= xy^2 - xy - xy^2 + xy \\ &= 0. \end{aligned}$$

Por otro lado,

$$\begin{aligned} S(g_2, g_3) &= \frac{x^2y^2}{x^2}(x^2 - y) - \frac{x^2y^2}{y^2}(y^2 - y) \\ &= (x^2y^2 - y^3) - (x^2y^2 - x^2y) \\ &= -y^3 + x^2y. \end{aligned}$$

Aplicando el algoritmo de la división (Teorema 2.3.8):

$$\begin{aligned} r_1 &= -y^3 + x^2y - \frac{x^2y}{xy}(xy - x) \\ &= -y^3 + x^2y - x^2y + x^2 \\ &= -y^3 + x^2. \end{aligned}$$

$$\begin{aligned} r_2 &= -y^3 + x^2 - \frac{x^2}{x^2}(x^2 - y) \\ &= -y^3 + x^2 - x^2 + y \\ &= -y^3 + y. \end{aligned}$$

Educadora de educadores

$$\begin{aligned}
 r_3 &= -y^3 + y - \frac{-y^3}{y^2}(y^2 - y) \\
 &= -y^3 + y + y^3 - y^2 \\
 &= -y^2 + y.
 \end{aligned}$$

$$\begin{aligned}
 r_4 &= -y^2 + y - \frac{-y^2}{y^2}(y^2 - y) \\
 &= -y^2 + y + y^2 - y \\
 &= 0.
 \end{aligned}$$

Luego, $S(g_2, g_3) \xrightarrow{G_1} 0$ y en consecuencia G_1 es una base de Gröbner para el ideal dado.

- Se encontrará una base de Gröbner para el ideal $I = \langle x^2y + z, xz + y \rangle \subseteq \mathbb{Q}[x, y, z]$ con respecto a $<_{lg}$.

El primer paso es calcular el S – polinomio:

$$\begin{aligned}
 S(x^2y + z, xz + y) &= \frac{x^2yz}{x^2y}(x^2y + z) - \frac{x^2yz}{xz}(xz + y) \\
 &= x^2yz + z^2 - x^2yz - xy^2 \\
 &= -xy^2 + z^2.
 \end{aligned}$$

Como se puede observar el $TP(-xy^2 + z^2) = -xy^2$ no es divisible por ninguno de los términos principales de $x^2y + z$ y $xz + y$ por lo tanto, $-xy^2 + z^2$ es reducido respecto a este par de polinomios y en este caso debe ser agregado al

conjunto generador, quedando este último de la siguiente manera:

$$G_1 = \{-xy^2 + z^2, x^2y + z, xz + y\}$$

Ahora, calculando los correspondientes S – polinomios para G_1 se obtiene:

$$\begin{aligned} S(-xy^2 + z^2, xz + y) &= \frac{-xy^2z}{-xy^2}(-xy^2 + z^2) - \frac{-xy^2z}{xz}(xz + y) \\ &= -xy^2z + z^3 + xy^2z + y^3 \\ &= y^3 + z^3 \end{aligned}$$

El cual es reducido respecto de G_1 y por tanto, se deberá añadir a este. Antes, se calculará el otro S – polinomio.

$$\begin{aligned} S(-xy^2 + z^2, x^2y + z) &= \frac{-x^2y^2}{-xy^2}(-xy^2 + z^2) - \frac{-x^2y^2}{x^2y}(x^2y + z) \\ &= -x^2y^2 + xz^2 + x^2y^2 + yz \\ &= xz^2 + yz. \end{aligned}$$

El lector podrá verificar que este último polinomio puede ser reducido a cero respecto de G_1 y en consecuencia no se añadirá a G_1 . En este punto tenemos la siguiente base de Gröbner:

$$G_2 = \{-xy^2 + z^2, x^2y + z, xz + y, y^3 + z^3\}$$

- Se encontrará una base de Gröbner para el ideal $I = \langle x^2y+z, xz+y \rangle \subseteq \mathbb{Q}[x, y, z]$ con respecto a $<_{inv}$.

Calculando el correspondiente S – polinomio se tiene:

$$\begin{aligned} S(z + x^2y, xz + y) &= \frac{xz}{z}(z + x^2y) - \frac{xz}{xz}(xz + y) \\ &= xz + x^3y - xz - y \\ &= x^3y - y \end{aligned}$$

El siguiente paso es verificar si este S – polinomio es reducido respecto de I

$$\begin{aligned} r_1 &= x^3y - y - \frac{x^3y}{x^2y}(x^2y + z) \\ &= x^3y - y - x^3y - xz \\ &= -xz - y \end{aligned}$$

$$\begin{aligned} r_2 &= -xz - y - \frac{-xz}{xz}(xz + y) \\ &= -xz - y + xz + y \\ &= 0 \end{aligned}$$

Como se observa que el S – polinomio es reducido a 0 respecto del conjunto generador, se concluye que $\{x^2y + z, xz + y\}$ es una base de Gröbner para I .

El procedimiento mostrado en este ejemplo se puede resumir en el siguiente pseudo-código:

Algorithm 1 Algoritmo para calcular una base de Gröbner

Entrada: $F = \{f_1, \dots, f_s\} \subseteq A[X]$ con $f_i \neq 0$ ($1 \leq i \leq s$).

Salida: $G = \{g_1, \dots, g_t\}$, una base de Gröbner para $\langle f_1, \dots, f_s \rangle$.

Inicio: $G := F$, $G^* := \{\{f_i, f_j\} \mid f_i, f_j \in G\}$

Mientras $G^* \neq \emptyset$ **hacer**

Escoja cualesquiera $\{f, g\} \in G^*$

$G^* := G^* - \{\{f, g\}\}$

$S(f, g) \xrightarrow{G}_+ h$, donde h es reducido con respecto a G

Si $h \neq 0$ **entonces**

$G^* := G^* \cup \{\{u, h\} \mid \text{para todo } u \in G\}$

$G := G \cup \{h\}$

Fin Si

Fin Mientras

El siguiente teorema prueba que en efecto del algoritmo de Buchberger se obtiene una base de Gröbner:

Teorema 3.2.3. *Dado $F = \{f_1, \dots, f_s\} \subseteq A[X]$ con $f_i \neq 0$ ($1 \leq i \leq s$), el algoritmo de Buchberger producirá una base de Gröbner para el ideal $I = \langle f_1, \dots, f_s \rangle$.*

Demostración. Primero se mostrará que el algoritmo termina en un número finito de pasos (Por contradicción). Suponga que este no termina, a medida que el algoritmo

progresas, se estará construyendo la cadena estrictamente creciente

$$G_1 \subset G_2 \subset G_3 \cdots$$

cada G_i será obtenido a partir de G_{i-1} añadiendo a este algún $h \in I$ y este h es una reducción distinta de cero con respecto a G_{i-1} de un S -polinomio de dos elementos de G_{i-1} , como h es reducido, se tiene que $TP(h) \notin TP(G_{i-1})$ y en consecuencia se tiene la cadena estrictamente ascendente de ideales

$$TP(G_1) \subset TP(G_2) \subset TP(G_3) \cdots$$

contradiciendo así el ítem ii) del teorema de la base de Hilbert (Teorema 2.4.1).

Ahora, suponga que el algoritmo termina en un conjunto $G = \{g_1, g_2, \dots, g_t\}$, se tiene entonces que $F \subseteq G \subseteq I$ y por tanto $I = \langle f_1, f_2, \dots, f_s \rangle \subseteq \langle g_1, g_2, \dots, g_t \rangle \subseteq I$. Así, G es un conjunto generador para I y además, si $g_i, g_j \in G$ entonces $S(g_i, g_j) \xrightarrow{G}_+ 0$ por construcción. Por lo tanto G es una base de Gröbner para I por el teorema 3.2.2. \square

Una observación que resulta del ejemplo anterior es que un mismo ideal I puede distintas bases de Gröbner dependiendo del orden escogido. En particular, para un ideal habrá un tipo especial de bases de Gröbner llamado bases reducidas, lo que simplificará aún más cualquier cálculo que se realice en I . En la siguiente sección se trabajará alrededor esta cuestión.

3.3. Bases de Gröbner reducidas

A partir del Teorema 3.2.3 se puede observar que uno de los principales problemas que surge, es la cantidad de elementos que aparecen en la base, pues, a esta se le irán añadiendo S – *polinomios* cada vez que estos no se reduzcan respecto de la base inicial. Para optimizar este algoritmo se procede a reducir la base como se verá a lo largo de esta sección:

Definición 3.3.1. Una base de Gröbner $G = \{g_1, \dots, g_t\}$ es **mínima** si para todo $i \in \{1, 2, \dots, t\}$ se tiene que $CP(g_i) = 1$ y para todo $i \neq j$ $MP(g_i) \nmid MP(g_j)$.

De esta definición, se desprende que la base de Gröbner hallada en el primer ítem del ejemplo 3.2.2 es una base mínima, de igual forma que lo es la base G_1 hallada con el algoritmo de Buchberger en el primer ítem de ejemplo 3.2.3.

Un primer resultado que se sigue a partir de esta definición es que toda base de Gröbner es mínima o se puede reducir para encontrar una base mínima, tal como se afirma en el siguiente teorema:

Teorema 3.3.1. Sea $G = \{g_1, \dots, g_t\}$ una base de Gröbner para un ideal I . Para obtener una base de Gröbner mínima desde G , se deben quitar del conjunto generador todos los g_i para los cuales existe un $j \neq i$ de manera que $MP(g_j) \mid MP(g_i)$. Finalmente se debe dividir cada g_i que quedó en la base por su coeficiente principal.

Demostración. Sea $c \in I$, como G es una base de Gröbner entonces existe un $g_i \in G$ tal que $MP(g_i) \mid MP(c)$, si $MP(g_j) \mid MP(g_i)$ para algún $g_j \in G$, se tiene

que $MP(g_j)|MP(c)$ y por tanto, $G_1 = G - \{g_i\}$ es una base de Gröbner también. Al repetir este proceso para G_1 se obtendrá una nueva base G_2 y así sucesivamente hasta que ya no exista un j tal que $MP(g_j)|MP(g_i)$, Si se le llama G_k a la última base obtenida y se divide cada elemento de esta entre su monomio principal, resultará una base mínima. \square

El siguiente ejemplo muestra como hallar una base mínima.

Ejemplo 3.3.1. Para $I = \langle y^2 + yx + x^2, y + x, y \rangle$, se puede verificar mediante el algoritmo de Buchberger que una base de Gröbner respecto del orden lexicográfico es:

$$G = \{y^2 + yx + x^2, y + x, y, x, x^2\}$$

Sin embargo, el monomio principal de $y+x$ divide al monomio principal de y^2+yx+x^2 y por lo tanto, se puede prescindir de este en el conjunto generador obteniendo:

$$G_1 = \{y + x, y, x, x^2\}$$

nuevamente, $MP(x)|MP(x^2)$, retirando este último de G_1 se llega a:

$$G_3 = \{y + x, x, y\}$$

finalmente, retirando $x + y$ se tiene:

$$G_4 = \{x, y\}.$$

Obsérvese que también se podría minimizar G a $\{y + x, x\}$.

Este ejemplo permite ver que cuando se minimiza G se obtienen bases del mismo tamaño, es decir, cada base mínima tiene la misma cantidad de generadores. Esto no es una casualidad, sino que es una generalidad para cualquier base G .

Teorema 3.3.2. Si $G = \{g_1, \dots, g_t\}$ y $G' = \{g'_1, \dots, g'_s\}$ son bases de Gröbner mínimas para un ideal I , entonces $s = t$ y después de enumerar convenientemente, se tiene que $TP(g_i) = TP(g'_i)$ para todo $i = 1, 2, \dots, t$.

A pesar de que las bases de Gröbner mínimas tienen la misma cantidad de elementos no son iguales, como se evidencia en el ejemplo 3.3.1. Por lo tanto, para lograr la unicidad se necesita de una condición especial en los polinomios de la base de Gröbner.

Definición 3.3.2. Una base de Gröbner $G = \{g_1, \dots, g_t\}$ es llamada una **Base de Gröbner reducida**, si para todo $g_i \in G$ se tiene que $CP(g_i) = 1$ y g_i es reducido respecto de $G - \{g_i\}$. En otras palabras, todo término distinto de cero que aparece en g_i no es divisible por el término principal de algún g_j , con $j \neq i$.

A la luz de esta definición la base mínima $\{y + x, x\}$ no es reducida, mientras que $\{x, y\}$ sí es una base de Gröbner reducida.

Para construir una base de Gröbner reducida a partir de una base mínima se puede hacer lo siguiente:

Si $G = \{g_1, \dots, g_t\}$ es una base de Gröbner mínima para I , considere $H_1 = G - \{g_1\}$ y $g_1 \xrightarrow{H_1}_+ h_1$, entonces $H_2 = H_1 \cup \{h_1\}$ es una base Gröbner para I .

reduciendo g_2 con respecto a H_2 se obtendrá un h_2 el cual se debe añadir a $H_2 - \{g_2\}$, obteniendo así, $H_3 = (H_2 - \{g_2\}) \cup \{h_2\}$, repitiendo este proceso hasta reducir g_t a un h_t , se obtendrá la base Gröbner reducida $H = \{h_1, h_2, \dots, h_t\}$.



UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

Uso de IA y software especializado

En la actualidad existen algunas herramientas tecnológicas que permiten el cálculo de Bases de Gröbner. Software de suscripción como Wolfram Mathematica, Maple o Macaulay2, tienen incorporadas dentro de sus múltiples herramientas, el cálculo de Bases de Gröbner.

En esta sección se abordarán CoCoA y SINGULAR las cuales son aplicaciones de software libre que aunque no son tan poderosas como las antes mencionadas permiten también encontrar entre otras cosas bases reducidas. Adicionalmente, se trabajara con IA tales como chatGPT y Julius mostrando sus ventajas y posibles desventajas.

4.1. CoCoA

Educadora de educadores

A continuación se muestran algunos ejemplos de instrucciones en el software CoCoA para el trabajo aritmético de polinomios y además el cálculo de una Base de Gröbner. Para los detalles de instalación del software el lector puede dirigirse al manual de (CoCoA Team, 2024) el cual se encuentra en la pagina web:

<https://sites.google.com/view/cocoa-cocoalib>.

En CoCoA los anillos de polinomios con que se puede trabajar son aquellos con coeficientes en:

```
ZZ: #Anillo de enteros.
QQ: #Anillo de racionales.
ZZ/(N): #Anillo cociente de enteros.
R: #Anillo de números reales.
QQ[i]: #Anillo de complejos.
```

Si R es un anillo e I es un ideal, entonces el comando R/I crea el anillo cociente correspondiente.

Figura 4.1: *Ejemplo anillo cociente en CoCoA*

```
# Use R:= ZZ/(5)[x,y], Lex;
# I:= Ideal(4*x^2-3*y, 2*x-y);
# ReducedGBasis(I);
[x +2*y, y^2 +2*y]
#
```

El siguiente ejemplo muestra como hacer operaciones aritméticas de polinomios en $\mathbb{Z}_5[x, y]$:

Figura 4.2: *Aritmética de polinomios en CoCoA*

```
# Use R:=ZZ/(5)[x,y];
# F:=4*x^2-3*x+1;
# G:=5*x^2+4*y^2-3;
# F+G;
-x^2 -y^2 +2*x -2
# F-G;
-x^2 +y^2 +2*x -1
# F*G;
x^2*y^2 -2*x*y^2 -2*x^2 -y^2 -x +2
# F/G;
--> ERROR: Inexact division (i.e. quotient does not exist in ring or monoid)
--> [CoCoALib] RingElem / RingElem
--> F/G;
--> ^
#
```

Como observación, las multiplicaciones deben estar obligatoriamente indicadas por el operador $*$, por ejemplo, se debe escribir $3*x*y$ en lugar de $3xy$. Además, observe que CoCoA arrojó un error al momento de hacer la división, esto se debe a que la división no es un elemento del anillo, no obstante, si se desea saber el cociente y residuo de dicha división, se debe usar otro comando. Por otro lado, recuérdese que para poder dividir se hace necesario indicar el orden de los términos y al no haberlo indicado CoCoA utiliza el orden Lexicográfico graduado inverso por defecto, sin embargo, también admite los órdenes:

```
Lex; #Lexicográfico.
DegLex; #Lexicográfico graduado.
DegRevLex; #Lexicografico graduado inverso.
Xel; #lexicográfico inverso.
```

Figura 4.3: Algoritmo de la división CoCoA un solo divisor

```
# Use R:=ZZ/(5)[x,y], Lex;
# F:=4*x^2-3*x+1;
# G:=5*x^2+4*y^2-3;
# DivAlg(F,[G]);
record[quotients := [0], remainder := -x^2 +2*x +1]
# DivAlg(G,[F]);
record[quotients := [0], remainder := -y^2 +2]
# |
```

Suponga que se desea realizar la división de $x^2y + x^2 - xy - y^2$ respecto de $\{y^2 - x, xy - y, x^2 - x\} \subset \mathbb{Q}[x, y]$ con el orden lexicográfico. Se utiliza entonces el comando DivAlg y como primera entrada el polinomio a reducir, luego se enlistan los polinomios del conjunto:

Figura 4.4: Algoritmo de la división CoCoA varios divisores

```
# Use R:=QQ[x,y], Lex;
# DivAlg(x^2*y+x^2-x*y-y^2,[y^2-x,x*y-y,x^2-x]);
record[quotients := [-x*y -x -y^3 -y^2 +y, 0, 0], remainder := y^5 +y^4 -y^3 -y^2]
# DivAlg(x^2*y+x^2-x*y-y^2,[x*y-y,y^2-x,x^2-x]);
record[quotients := [x +y, -x, 0], remainder := 0]
# |
```

Note que CoCoA no realiza la reducción sino que va realizando las divisiones según el orden en que se escriban los polinomios.

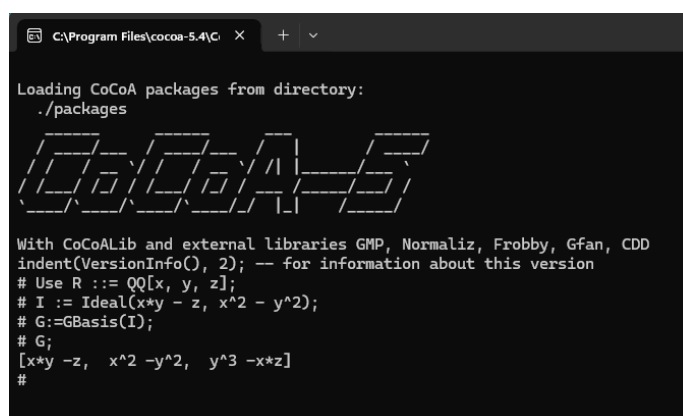
CoCoA también permite el cálculo de bases de Gröbner, el siguiente pseudo-código ejemplifica su uso para esta tarea:

```
Use R ::= QQ[x,y,z]; # Define el anillo de polinomios con
coeficientes en Q.
I := Ideal[x*y^2 - z^2, x^2*y + z, x*z + y]; # Define el ideal
de polinomios.
G := GBasis(I); # Calcula una base de Gröbner.
G; # Muestra la base de Gröbner.
```

Utilizando este algoritmo se tendrá como resultado la base $G = \{xy - z, x^2 - y^2, y^3 - xz\}$ tal como se muestra en la imagen a continuación:

Educadora de educadores

Figura 4.5: Ejemplo base de Gröbner en CoCoA



```

C:\Program Files\cocoa-5.4\Cocoa X + v
Loading CoCoA packages from directory:
./packages

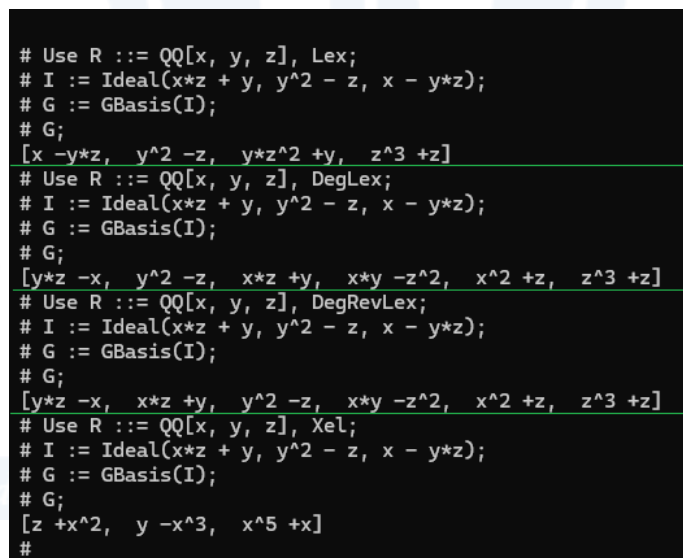
CoCoA-5

With CoCoALib and external libraries GMP, Normaliz, Frobbly, Gfan, CDD
indent(VersionInfo(), 2); -- for information about this version
# Use R := QQ[x, y, z];
# I := Ideal(x*y - z, x^2 - y^2);
# G:=GBasis(I);
# G;
[x*y -z,  x^2 -y^2,  y^3 -x*z]
#

```

Cambiando el orden se obtiene lo siguiente:

Figura 4.6: Ejemplo orden de términos en CoCoA



```

# Use R := QQ[x, y, z], Lex;
# I := Ideal(x*z + y, y^2 - z, x - y*z);
# G := GBasis(I);
# G;
[x -y*z,  y^2 -z,  y*z^2 +y,  z^3 +z]
# Use R := QQ[x, y, z], DegLex;
# I := Ideal(x*z + y, y^2 - z, x - y*z);
# G := GBasis(I);
# G;
[y*z -x,  y^2 -z,  x*z +y,  x*y -z^2,  x^2 +z,  z^3 +z]
# Use R := QQ[x, y, z], DegRevLex;
# I := Ideal(x*z + y, y^2 - z, x - y*z);
# G := GBasis(I);
# G;
[y*z -x,  x*z +y,  y^2 -z,  x*y -z^2,  x^2 +z,  z^3 +z]
# Use R := QQ[x, y, z], Xel;
# I := Ideal(x*z + y, y^2 - z, x - y*z);
# G := GBasis(I);
# G;
[z +x^2,  y -x^3,  x^5 +x]
#

```

Se puede usar el software para encontrar una base de Gröbner reducida cambiando el comando `GBasis()` por `ReducedGBasis()`.

Nota: En los casos que fueron trabajados con CoCoA los comandos `GBasis()` y `ReducedGBasis()` producen la misma base de Gröbner como resultado.

4.2. Singular

Al igual que CoCoA, SINGULAR es un software libre dedicado al álgebra computacional de polinomios. Entre sus funciones se tiene el cálculo de bases de Gröbner.

En SINGULAR se encontrarán dos tipos de órdenes preestablecidos, globales y locales. Se sugiere al lector remitirse al manual en cual se encuentra en la pagina web (<https://www.singular.uni-kl.de/>) para ver la definición de estos. A continuación se listan los órdenes globales:

```
lp; #Lexicográfico.
rp; #Lexicográfico inverso.
dp; #Lexicográfico reverso graduado.
Dp; #Lexicográfico graduado.
wp; #Lexicográfico "pesado" reverso.
Wp; #Lexicográfico pesado.
```

Los órdenes locales son:

```
ls; #Lexicográfico negativo.
ds; #Lexicográfico reverso graduado negativo.
Ds; #Lexicográfico graduado negativo.
```

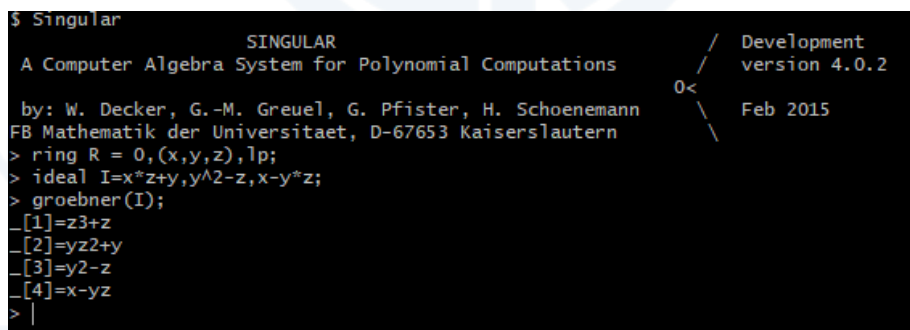
La siguiente lista de instrucciones es un ejemplo para el cálculo de una base de Gröbner en SINGULAR.

```
ring R = 0, (x,y,z), lp;
ideal I = x*z+y; y^2-z,x-y*z;
groebner(I);
```

En la primera línea se define el anillo R, el 0 se usa para indicar que los coeficientes pertenecen a \mathbb{Q} . (x, y, z) son las indeterminadas del anillo de polinomio y lp es el orden lexicográfico.

En la segunda línea se genera el ideal I, para luego mostrar la base de Gröbner mediante el comando groebner(I).

Figura 4.7: Ejemplo cálculo de una base de Gröbner en SINGULAR



```
$ Singular
SINGULAR
A Computer Algebra System for Polynomial Computations
by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann
FB Mathematik der Universitaet, D-67653 Kaiserslautern
Development
version 4.0.2
0<
Feb 2015
> ring R = 0, (x,y,z), lp;
> ideal I=x*z+y,y^2-z,x-y*z;
> groebner(I);
_[1]=z3+z
_[2]=yz2+y
_[3]=y2-z
_[4]=x-yz
> |
```

En la anterior imagen se observa como resultado la base $G = \{z^3 + z, yz^2 + y, y^2 - z, x - yz\}$, la cual coincide con la arrojada en CoCoA (Figura 4.6).

4.3. ChatGPT

Se inició una conversación con ChatGPT desde cero, es decir, sin que hubiesen interacciones previas de un usuario con esta herramienta, el objetivo es analizar qué tan útil puede resultar el uso de una (IA) al trabajar en matemáticas, específicamente con bases de Gröbner. A continuación se copia la interacción con (ChatGPT, 2024):

Usuario: Hola, deseo calcular una base de Gröbner para el ideal generado por los polinomios $x^2 + y, y^2 - z, x - yz$, en el anillo $\mathbb{Q}[x, y, z]$. ¿Me puedes ayudar?

ChatGPT: ¡Hola! Claro que sí, te puedo ayudar a calcular una base de Gröbner para el ideal generado por los polinomios $f_1 = x^2 + y, f_2 = y^2 - zy, f_3 = x - yz$, en el anillo $\mathbb{Q}[x, y, z]$.

La base de Gröbner es un conjunto de polinomios generadores del ideal que tienen ciertas propiedades que hacen que sean "más simples" para realizar cálculos en álgebra computacional, como resolver sistemas de ecuaciones o realizar operaciones ideales.

Para calcular la base de Gröbner, se utiliza un algoritmo como el de Buchberger, el cual encuentra una base de Gröbner con respecto a un orden monomial dado. Un orden monomial comúnmente utilizado es el orden lexicográfico o el orden de grado total.

Vamos a proceder a calcular la base de Gröbner utilizando el algoritmo de Buchberger para los polinomios f_1, f_2 y f_3 en el anillo $\mathbb{Q}[x, y, z]$.

Voy a hacer los cálculos y te daré la base de Gröbner en breve.

*It seems like I can't do more advanced data analysis right now. Please try again later. However, you can still compute the Gröbner basis using tools like ****SymPy**** (si estás programando en Python) o ****Mathematica****. Si necesitas ayuda con cómo usar estas herramientas para calcular la base de Gröbner, estaré encantado de guiarte.*

La primera observación para resaltar es que, al parecer, al usarse una versión gratuita de ChatGPT no se pueden hacer cálculos avanzados, sin embargo, una alternativa propuesta por la (IA) es el de generar un código de Python para resolver el problema:

```
from sympy import symbols, groebner

# Definir las variables y los polinomios
x, y, z = symbols('x y z')
f1 = x**2 + y
f2 = y**2 - z
f3 = x - y*z

# Calcular la base de Gröbner
G = groebner([f1, f2, f3], x, y, z, domain='QQ')

# Mostrar la base de Gröbner
G
```

El cual al ser compilado arroja como resultado:

$$\text{GrobnerBasis}((x + z^4, y + z^3, z^6 - z), (x, y, z))$$

Esta es en efecto una base de Gröbner para $\langle x^2 + y, y^2 - z, x - yz \rangle$ usando el orden lexicográfico.

4.4. Julius

El propósito es ahora analizar el comportamiento de una IA llamada **Julius AI** que tiene como característica el estar diseñada principalmente para el análisis de datos y cálculos matemáticos.

Se procede a generar con **(AI, 2024)** la misma interacción que con chatGPT:

UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

Figura 4.8: Interacción con Julius AI

The screenshot shows a chat conversation. The user asks: "Hola, deseo calcular una base de Gröbner para el ideal generado por los polinomios $x^2+y, y^2-z, x-yz$, en el anillo $\mathbb{Q}[x,y,z]$. ¿Me puedes ayudar?". Julius responds with a code block for calculating the Gröbner basis using Sympy, a code explanation, and the resulting basis.

```

</> Calculated Gröbner Basis for Polynomials
Python
1 from sympy import symbols, groebner
2
3 # Definimos las variables
4 x, y, z = symbols('x y z')
5
6 # Definimos los polinomios
7 polynomials = [x**2 + y, y**2 - z, x - y*z]
8
9 # Calculamos la base de Gröbner
10 G = groebner(polynomials, x, y, z)
11
12 # Mostramos la base de Gröbner
13 G
Code Explanation
This code snippet defines three polynomials and computes their Gröbner basis using the sympy library.
Code Output
<summary>GroebnerBasis([x + z**4, y + z**3, z**6 - z], x, y, z, domain='ZZ', ord... Show more
The base de Gröbner para el ideal generado por los polinomios  $x^2 + y, y^2 - z, x - yz$  en el anillo  $\mathbb{Q}[x, y, z]$  ha sido calculada exitosamente. Aquí está la base de Gröbner:
Summary ^
GroebnerBasis([x + z**4, y + z**3, z**6 - z], x, y, z, domain='ZZ', order='lex')
Esta base de Gröbner es un conjunto de polinomios que genera el mismo ideal y tiene propiedades útiles para resolver sistemas de ecuaciones polinómicas.

```

La primera impresión es que al igual que ChatGPT genera un código en Python, el cual coincide exactamente con el arrojado por la otra IA, no obstante, lo compila dentro de la conversación. Por otro lado no hace explicaciones sobre la teoría de bases de Gröbner como si lo hace ChatGPT.

Se puede observar que ambas IA dan solución al problema planteado, sin embargo, Julius es más ventajosa ya que permite ejecutar código dentro de su entorno

haciendo que su solución sea más completa e inmediata.

Por otro lado, una fuerte desventaja de Julius frente a ChatGPT es que sólo permite un máximo de 8 interacciones al usuario por día en su versión gratuita, mientras que en ChatGPT se permite un número ilimitado.

En conclusión, las dos IA además de dar una solución específica generan un código en Python modificable que permite aprender algo de programación para posteriormente resolver problemas más complejos.

A través de estas interacciones se puede ahondar en la teoría de bases de Gröbner en relación con los caminos que proponen las IA y el tipo de problemas que pueden resolver, por lo pronto la intención del trabajo no es hacer un análisis exhaustivo de cómo el uso de herramientas tecnológicas abordan estos problemas y simplifican procesos de cálculo matemático.

UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

Algunas aplicaciones

Como se mencionó al final del ejemplo 2.3.10 uno de los primeros problemas que apareció con respecto al algoritmo de la división es el del ideal membership y aunque no se dijo en su momento, como consecuencia del teorema 3.1.1 se ha resuelto este problema debido a que si G es una base de Gröbner para I entonces $c \in I$ si y sólo si $c \xrightarrow{G} 0$. En esta sección se pretende abordar otra aplicación de las bases de Gröbner y para ello se involucrarán ejercicios comunes en otros contextos de las matemáticas.

5.1. Uso de bases de Gröbner en problemas de optimización

Educadora de educadores

El lector estará familiarizado de sus cursos de cálculo con el concepto de optimización, el siguiente ejemplo es uno de los problemas típicos que se aborda en esta área de las matemáticas:

Ejemplo 5.1.1. *Encuentre el punto sobre la curva C de intersección de la esfera*

$x^2 + y^2 + z^2 = 9$ y el plano $x - y + 3z = 6$ que está más alejado del plano xy .

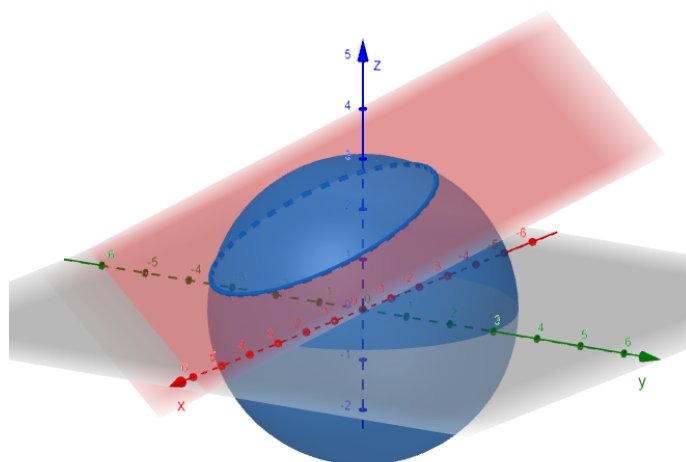


Figura 5.1: Ejemplo cálculo de una base de Gröbner en intersección de una esfera y un plano.

Solución: Para solucionar este problema se puede hacer uso de los multiplicadores de Lagrange y resolver el sistema:

$$\begin{cases} 2x\lambda + \mu & = 0 \\ 2y\lambda - \mu & = 0 \\ 2z\lambda + 3\mu & = 0 \\ x^2 + y^2 + z^2 - 9 & = 0 \\ x - y + 3z - 6 & = 0. \end{cases}$$

Aunque este problema se puede resolver con una manipulación algebraica adecuada, el lector advertirá que este tipo de problemas sera complejo dependiendo de la forma

de la función a optimizar y de la cantidad de restricciones que se tengan.

Si se suman las dos primeras ecuaciones llegaremos al sistema equivalente:

$$\begin{cases} x + y & = 0 \\ x^2 + y^2 + z^2 - 9 & = 0 \\ x - y + 3z - 6 & = 0 \\ 2x\lambda + \mu & = 0 \\ 2z\lambda + 3\mu & = 0. \end{cases}$$

El cual al sumar la primera ecuación con la tercera y hacer la sustitución $y = -x$ en la segunda ecuación se tiene el sistema:

$$\begin{cases} x + y & = 0 \\ 2x^2 + z^2 - 9 & = 0 \\ 2x + 3z - 6 & = 0 \\ 2x\lambda + \mu & = 0 \\ 2z\lambda + 3\mu & = 0. \end{cases}$$

Finalmente, despejando una de las variables en la segunda ecuación y sustituyéndola en la tercera ecuación se tienen las soluciones: $x = \frac{6}{11} \pm \frac{9}{22}\sqrt{14}$, $y = -\frac{6}{11} \pm \frac{9}{22}\sqrt{14}$, $z = \frac{18}{11} \pm \frac{3}{11}\sqrt{14}$.

Obsérvese que al ir resolviendo el sistema lo que se está haciendo es encontrar

un conjunto de polinomios cuyas raíces sean las mismas que los del problema inicial y en la medida que estos tengan una expresión más sencilla, el problema se simplificará. Es de allí que una propuesta para la solución de este sistema será la de definir el ideal $I = \langle 2x\lambda + \mu, 2y\lambda - \mu, x^2 + y^2 + z^2 - 9, x - y + 3z - 6 \rangle$ y encontrar una base de Gröbner reducida para I , generando así un conjunto de polinomios que faciliten los cálculos. Ahora se formalizará esta idea y después se retomará este ejemplo.

Haciendo un estudio similar al que se realizó en el caso de una variable, se define la función de evaluación en el caso multivariable.

Definición 5.1.1. Sea $(A, +, \cdot)$ un subcampo de un campo $(E, +, \cdot)$. La función evaluación en varias variables es definida por:

$$\begin{aligned} \phi_{X_0} : A[X] &\rightarrow A \\ a(X) &\rightarrow \phi_{X_0}(a(X)) = a(X_0) \end{aligned}$$

Aquí $X_0 = (a_1, a_2, \dots, a_n)$, esto es, una n -tupla de elementos de A , en otras palabras, X_0 es un elemento de A^n y este último recibe el nombre de **espacio afín**. En el caso en que $a(X_0) = 0$ se dice que X_0 es una raíz del polinomio $a(X)$.

Una consecuencia que al lector le pueda parecer interesante es que la función evaluación permite generar una conexión entre los polinomios y el conjunto que contiene sus raíces que (por lo general representado por un lugar geométrico), esto es, para cada polinomio $a(X) \in A[X]$ se puede definir $V(a(X))$ como el conjunto de todas las soluciones de la ecuación $a(X) = 0$, es decir, el conjunto de todas sus raíces. Así, si por ejemplo, $A = \mathbb{R}$ y $a(x, y) = x^2 + y^2 - 4$, entonces $V(x^2 + y^2 - 4)$ es

el circunferencia de radio 2 sobre el plano xy centrado en el origen. Formalmente:

Definición 5.1.2. Sean $(A, +, \cdot)$ un campo, $(A[X], +, \cdot)$ su anillo de polinomios en n variables y $a(X) \in A[X]$.

- **La variedad definida por $a(X)$ es el conjunto:**

$$V(a(X)) = \{X_0 = (a_1, \dots, a_n) \in A^n \mid a(X_0) = 0\}$$

- Si $F = \{f_1, f_2, \dots, f_s\} \subset A[X]$ entonces **la variedad definida por F es:**

$$V(F) = \{(a_1, \dots, a_n) \in A^n \mid f_i(a_1, \dots, a_n) = 0, \text{ para todo } i = 1, 2, \dots, s\}$$

Teorema 5.1.1. Sea $(A, +, \cdot)$ un campo y $F = \{f_1, \dots, f_s\} \subset A[X]$ entonces:

$$V(F) = \bigcap_{i=1}^s V(f_i)$$

Demostración. Obsérvese que $(a_1, \dots, a_n) \in V(F)$ si y sólo si $f_i(a_1, \dots, a_n) = 0$ para todo $i \in \{1, \dots, s\}$, y esto es equivalente a decir que $(a_1, \dots, a_n) \in V(f_i)$ para todo i , lo cual equivale también a que $(a_1, \dots, a_n) \in \bigcap_{i=1}^s V(f_i)$. \square

Ejemplo 5.1.2. .

- Sea $F = \{x^3 - 5x^2 + 7x - 3, x^3 - 6x^2 + 11x - 6\}$ entonces $V(F) = \{1, 3\}$, por otro lado, $V(x^3 - 5x^2 + 7x - 3) = \{1, 3\}$ y $V(x^3 - 6x^2 + 11x - 6) = \{1, 2, 3\}$ luego $V(x^3 - 5x^2 + 7x - 3) \cap V(x^3 - 6x^2 + 11x - 6) = \{1, 3\} \cap \{1, 2, 3\} = \{1, 3\}$.

- Como $V(2x - y - 3) = \{(x, 2x - 3)\}$ y $V(x - y - 2) = \{(x, x - 2)\}$ entonces $(x, y) \in V(2x - y - 3) \cap V(x - y - 2)$ si y sólo si $(x, y) = (x, x - 2) = (x, 2x - 3)$ luego $x - 2 = 2x - 3$ y en consecuencia $x = 1$ y $y = -1$, por lo tanto $V(2x - y - 3, x - y - 2) = \{(1, -1)\}$.

Para ver cómo el uso de variedades puede ayudar a la resolución de sistemas de ecuaciones considérese $V(I)$ con $I = \langle f_1, f_2, \dots, f_s \rangle$, es decir, las soluciones del sistema infinito:

$$f_i = 0, f \in I; \quad (5.1)$$

y compare con las soluciones del sistema finito:

$$f_1 = 0, f_2 = 0, \dots, f_s = 0. \quad (5.2)$$

Es claro que toda solución en (5.1) es también solución de (5.2).

Ahora, si $(a_1, \dots, a_n) \in A^n$ es solución del sistema (5.2) y $f \in I$ entonces $f(a_1, \dots, a_n) = 0$ ya que $f = \sum_{i=1}^s u_i f_i$, para algunos $u_i \in A[X]$. Por lo tanto, esta será una solución del sistema (5.1). Se tiene así que $V(I) = V(f_1, \dots, f_s)$, además se sabe que si $\{f'_1, \dots, f'_t\}$ es otro conjunto generador del ideal I entonces $V(I) = V(f'_1, \dots, f'_t)$. Esto quiere decir que las soluciones del sistema $f_1 = 0, \dots, f_s = 0$ son las mismas soluciones de $f'_1 = 0, \dots, f'_t = 0$, luego, una variedad no está determinada por un conjunto particular de ecuaciones si no que está determinada por un ideal. Por lo que se puede usar las bases de Gröbner para encontrar una “mejor” representación para I y obtener una “mejor” para $V(I)$.

Ejemplo 5.1.3.

- Retomando el ejemplo de optimización el cual inició esta discusión (Ejemplo 5.1.1), Tómesese $I = \langle 2x\lambda + \mu, 2y\lambda - \mu, x^2 + y^2 + z^2 - 9, x - y + 3z - 6 \rangle$, usando CoCoA para hallar una base reducida se tiene:

$$G = \left\{ x - \frac{63}{4}\mu + \frac{15}{4}, \lambda + \frac{11}{12}\mu - \frac{1}{4}, y + \frac{63}{4}\mu - \frac{15}{4}, z + \frac{21}{2}\mu - \frac{9}{2}, \mu^2 - \frac{6}{11}\mu + \frac{5}{77} \right\}$$

O equivalentemente el sistema:

$$\begin{cases} x - \frac{63}{4}\mu + \frac{15}{4} = 0 \\ \lambda + \frac{11}{12}\mu - \frac{1}{4} = 0 \\ y + \frac{63}{4}\mu - \frac{15}{4} = 0 \\ z + \frac{21}{2}\mu - \frac{9}{2} = 0 \\ \mu^2 - \frac{6}{11}\mu + \frac{5}{77} = 0 \end{cases}$$

Obsérvese que las demás variables sólo dependen de μ , por lo tanto, resolviendo para μ en la última ecuación (la cuál es una cuadrática) se obtiene: $\mu = \frac{21 \pm 2\sqrt{14}}{77}$ y al hacer la respectiva sustitución se obtiene el mismo resultado que se había anticipado. A saber:

$$x = \frac{12 \pm 9\sqrt{14}}{22}, y = -\frac{12 \pm \sqrt{14}}{22}, z = \frac{18 \mp 3\sqrt{14}}{11}.$$

- Suponga que se desea encontrar la intersección entre la recta $x = \frac{1}{2}$ y la circunferencia $x^2 + y^2 = 4$.

Se debe resolver el sistema:

$$\begin{cases} 2x - 1 = 0 \\ x^2 + y^2 - 4 = 0 \end{cases}$$

Usando CoCoA para calcular una base de Gröbner reducida del ideal $I = \langle 2x + 1, x^2 + y^2 - 4 \rangle$ se tiene que $g_1 = x + \frac{1}{2}$, $g_2 = y^2 - \frac{15}{4}$.

Solucionando ahora el sistema $g_1 = 0$, $g_2 = 0$ se tiene $x = -\frac{1}{2}$, $y = \pm \frac{\sqrt{15}}{2}$

- Para hallar la intersección entre las curvas $x^2 + y^2 = 5$, $x^5 + y^2 = 33$, $x^3 - 5xy = -2$. Se plantea el sistema:

$$\begin{cases} x^2 + y^2 - 5 = 0 \\ x^5 + y^2 - 33 = 0 \\ x^3 - 5xy + 2 = 0 \end{cases}$$

Se considera el ideal $I = \langle x^2 + y^2 - 5, x^5 + y^2 - 33, x^3 - 5xy + 2 \rangle$ y se obtiene la base de Gröbner $G = \{x - 2, y - 1\}$ con respecto $<_l$.

Así se tiene que la solución es $x = 2, y = 1$ como lo muestra la siguiente figura:

Educadora de educadores

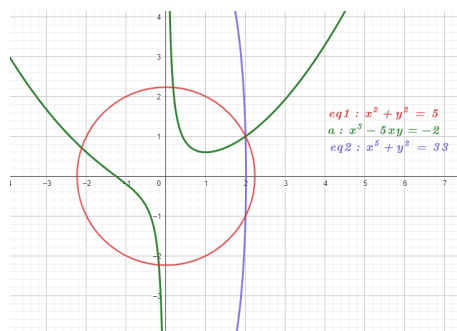


Figura 5.2: Sistema de ecuaciones

- Aunque el sistema:

$$\begin{cases} x^2 + y^3 - 1 = 0 \\ -xy + x - y^2 = 0 \end{cases}$$

Se transforme a

$$\begin{cases} x - y^4 - y^2 + y - 1 = 0 \\ y^5 - y^4 + y^3 - y^2 + 2y - 1 = 0 \end{cases}$$

y este último parezca más complejo de resolver a simple vista, obsérvese que la segunda ecuación solo se encuentra en la variable y , luego, se podría usar un método numérico como Newton-Raphson para aproximar la solución y ya con y fijo, la primera ecuación es trivial.

Usando Julius AI para generar el código en python para dicho método numérico, se obtuvo después de la cuarta iteración que $y = 0,5974970086825179$, por lo tanto, una aproximación a la solución del sistema es:

$$x = 0,8869565769 \quad y = 0,5974970086825179$$

- La base de Gröbner reducida usando $<_l$ asociada al sistema de ecuaciones lineales

$$\begin{cases} x + 4y - z - 6 = 0 \\ 2x + 5y - 7z + 9 = 0 \\ 3x - 2y + z - 2 = 0 \end{cases}$$

es $G = \{x - 1, y - 2, z - 3\}$. Con esta se puede determinar que la solución al sistema es $x = 1, y = 2, z = 3$

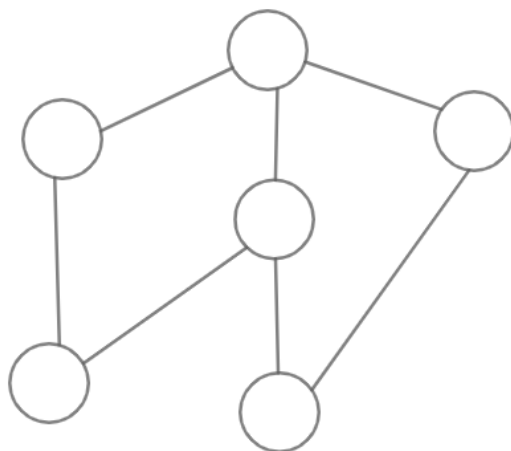
El lector estará tentado a pensar que si finalmente se usará un software para calcular las bases de Gröbner ¿porqué no usarlo en primera instancia para resolver el sistema de ecuaciones? pero justamente el punto aquí es que la mayoría de estos software utilizan el método de las bases de Gröbner para solucionarlos.

5.2. El problema k -coloreado

Otro contexto dónde las bases de Gröbner pueden ser de utilidad es en la teoría de grafos ya que uno de los problemas más famosos en esta área de las matemáticas es el conocido como el problema de la k -coloración. En el cuál se desea colorear los n vértices de un grafo con k colores de manera que dos vértices adyacentes (unidos por una misma arista) no queden con el mismo color. A modo de ejemplo, supóngase

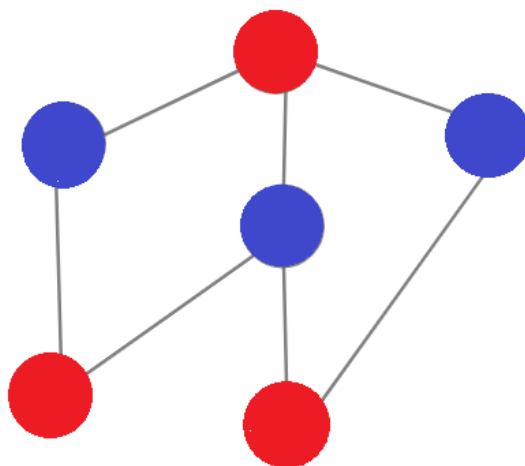
que se desea colorear el grafo de la figura 5.3 con los colores rojo y azul.

Figura 5.3: *Grafo de seis vértices*



Después de unos pocos intentos, el lector podrá encontrar la siguiente solución:

Figura 5.4: *Grafo dos colores, solución*



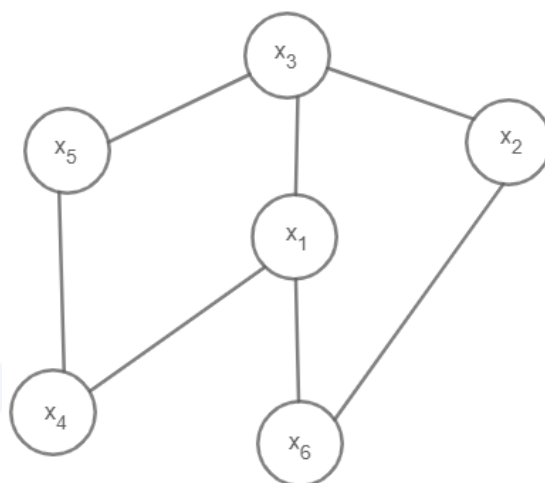
Y aunque a simple vista para este caso el problema pueda parecer trivial,

esto se puede complicar a medida que tanto el número de vértices, aristas y colores aumente, tal como se verá más adelante.

Una solución algebraica para este problema de los dos colores consiste en:

1. Utilizar los números 1 y -1 para los colores, por ejemplo, al color azul le corresponderá el -1 y al rojo el 1.
2. Hacer corresponder las variables x_i de $(\mathbb{C}[x_1, \dots, x_n], +, \cdot)$ con cada uno de los distintos n vértices (Ver figura 5.5).

Figura 5.5: Grafo enumeración de vértices



Obsérvese que la forma en que se hace la correspondencia entre vértices y variables es aleatoria. Ahora, como cada vértice tendrá uno de los dos posibles colores (1 y -1) se tiene que para todo i :

$$x_i^2 - 1 = 0$$

Por otro lado, también se tiene que:

$$x_i^2 - x_j^2 = 0 \quad (5.3)$$

$$(x_i - x_j)(x_i + x_j) = 0 \quad (5.4)$$

Luego, si el color de x_i es diferente al color de x_j entonces $x_i - x_j \neq 0$ y en consecuencia $x_i + x_j = 0$.

El siguiente paso es tomar el ideal I generado por los n polinomios de la forma $x_i^2 - 1$ y por los polinomios $x_i + x_j$ siempre y cuando los vértices x_i y x_j sean adyacentes.

Para este caso en particular el ideal es:

$$I = \langle x_1^2 - 1, x_2^2 - 1, x_3^2 - 1, x_4^2 - 1, x_5^2 - 1, x_6^2 - 1, x_1 + x_3, x_1 + x_4, x_1 + x_6, x_2 + x_3, x_2 + x_6, x_3 + x_5, x_5 + x_4 \rangle$$

Calculando ahora una base de Gröbner reducida para I se obtiene como resultado:

$$G = \{x_4 - x_6, x_3 - x_6, x_2 + x_6, x_5 + x_6, x_1 + x_6, x_6^2 - 1\}$$

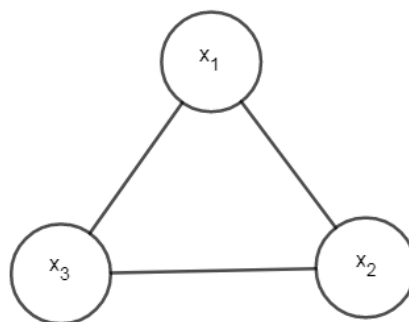
Claramente G sugiere que al asignarle un color al vértice x_6 se puede encontrar el color de los demás vértices pues todos los polinomios en G tienen como variable a x_6 . Así si a x_6 le asignamos el color rojo (1) entonces x_1 debe ser de color azul dado que $x_1 + x_6 \in G$, de forma análoga x_5 y x_2 deben ser de color azul. Continuando con la asignación x_3 y x_4 deben ser de color rojo debido a que los polinomios $x_3 - x_6$ y

$x_4 - x_6$ pertenecen a G .

Con esta configuración de colores mencionada se obtiene el grafo de la figura 5.3.

Una pregunta que naturalmente surge es ¿todos los grafos se pueden 2-colorear? Si la respuesta es no ¿Qué condiciones deben cumplirse para que un grafo sea 2-coloreable?

Figura 5.6: Grafo no 2-coloreable



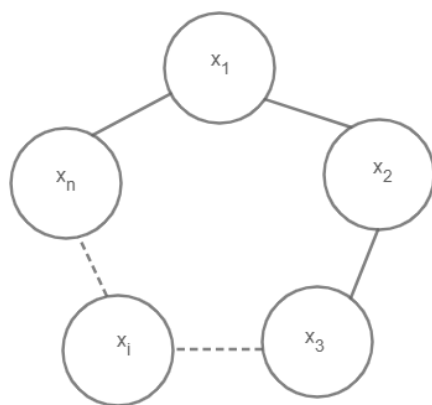
Obsérvese que el grafo de la figura 5.6 no es 2-coloreable ya que al asignar un color a x_1 los vértices x_2 y x_3 tendrán un color distinto a este, pero al haber sólo dos colores x_2 y x_3 deben compartir el mismo color, sin embargo, estos dos vértices son adyacentes.

Visto de forma algebraica, este grafo genera al sistema:

$$\begin{cases} x_1 + x_2 = 0 \\ x_2 + x_3 = 0 \\ x_3 + x_1 = 0 \end{cases}$$

el cual no tiene solución distinta a la trivial.

Figura 5.7: Grafo de n vértices



Se puede verificar que cualquier grafo “cíclico”, como el de la figura 5.7, con un número impar de vértices no es 2-coloreable ya que el sistema generado es de la forma:

Educadora de educadores

$$\left\{ \begin{array}{l} x_1 + x_2 = 0 \\ x_2 + x_3 = 0 \\ \vdots \\ x_{n-1} + x_n = 0 \\ x_n + x_1 = 0 \end{array} \right.$$

para el cual, sustituyendo x_1 de manera recursiva en las primeras $n - 1$ ecuaciones se tiene:

$$\left\{ \begin{array}{l} x_2 = -x_1 = (-1)x_1 \\ x_3 = -x_2 = -(-x_1) = (-1)^2x_1 \\ x_4 = -x_3 = -(-1)^2x_1 = (-1)^3x_1 \\ \vdots \\ x_n = (-1)^{n-1}x_1 \end{array} \right.$$

Como n es impar, supóngase que es de la forma $2k + 1$ para algún entero k . La última de las ecuaciones anteriores lleva a

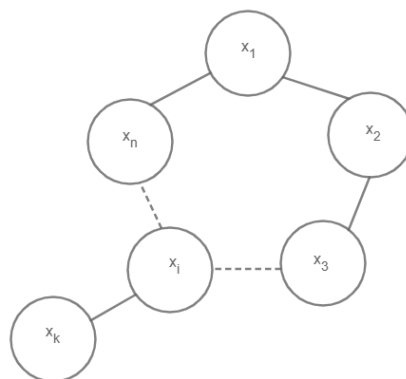
$$x_n = (-1)^{n-1}x_1 = (-1)^{2k}x_1 = x_1$$

lo cual es una contradicción pues x_n y x_1 son adyacentes.

Nótese que si a un grafo cíclico se le añade otro vértice que no pertenezca al ciclo pero que este relacionado con alguno de ellos, el sistema seguirá siendo incon-

sistente dado que esta nueva ecuación no aporta ninguna modificación con respecto a las variables del ciclo.

Figura 5.8: Grafo con un subgrafo cíclico



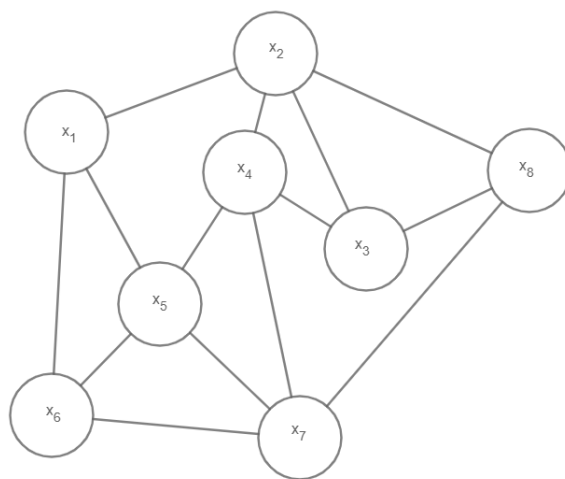
Lo anterior se puede resumir en el siguiente teorema:

Teorema 5.2.1. *Si un grafo contiene al menos un subgrafo cíclico con un número de vértices impar, entonces no es 2-coloreable.*

Ahora, supóngase que se desea colorear el siguiente grafo usando 3 colores manteniendo la condición de que dos vértices adyacentes no queden del mismo color.

NACIONAL

Educadora de educadores

Figura 5.9: Ejemplo grafo de 8 vértices

Siguiendo la misma idea del caso anterior, los colores serán representados por las raíces cúbicas de la unidad, $1, \xi, \xi^2$.

Al asignar a cada vértice un color, se debe cumplir entonces que:

$$x_i^3 - 1 = 0, \text{ para } 1 \leq i \leq 8. \quad (5.5)$$

Como $x_i^3 = x_j^3$ se sigue:

$$x_i^3 - x_j^3 = 0$$

$$(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$$

Si x_i y x_j tienen distinto color entonces $x_i - x_j \neq 0$ y en consecuencia se tiene que:

$$x_i^2 + x_i x_j + x_j^2 = 0 \quad (5.6)$$

Tómese ahora el ideal I generado por cada polinomio de la ecuación (5.5) y por los polinomios en la ecuación (5.6) siempre y cuando x_i y x_j estén conectados por una arista.

Para este caso:

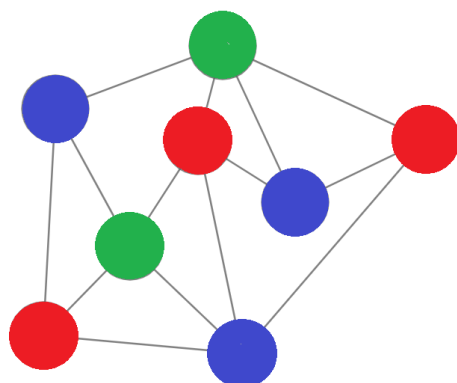
$$I = \langle x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_4^3 - 1, x_5^3 - 1, x_6^3 - 1, x_7^3 - 1, x_8^3 - 1, x_1^2 + x_1 x_2 + x_2^2, \\ x_1^2 + x_1 x_5 + x_5^2, x_1^2 + x_1 x_6 + x_6^2, x_2^2 + x_2 x_3 + x_3^2, x_2^2 + x_2 x_4 + x_4^2, x_2^2 + x_2 x_8 + x_8^2, x_3^2 + x_3 x_4 + x_4^2, \\ x_3^2 + x_3 x_8 + x_8^2, x_4^2 + x_4 x_5 + x_5^2, x_4^2 + x_4 x_7 + x_7^2, x_5^2 + x_5 x_7 + x_7^2, x_6^2 + x_6 x_7 + x_7^2, x_7^2 + x_7 x_8 + x_8^2 \rangle$$

La base de Gröbner reducida es:

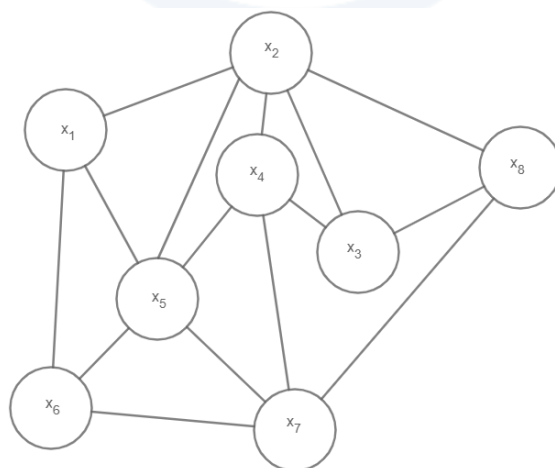
$$G = \{x_1 - x_7, x_2 + x_7 + x_8, x_3 - x_7, x_4 - x_8, x_5 + x_7 + x_8, x_6 - x_8, x_7^2 + x_7 x_8 + x_8^2, x_8^3 - 1\}$$

Note que existe un único polinomio en una sola variable, $x_8^3 - 1$, luego se puede escoger un color arbitrario para x_8 , rojo por ejemplo. Como el polinomio $x_7^2 + x_7 x_8 + x_8^2$ pertenece al ideal, entonces x_7 y x_8 están unidos y deben tener colores diferentes, sea azul el color asignado para x_7 . El polinomio $x_6 - x_8$ indica que estos dos vértices tienen el mismo color, luego x_6 es rojo como a su vez x_4 también lo es. x_1 y x_3 son azules pues $x_1 - x_7$ y $x_3 - x_7$ están en el ideal.

Por lo anterior, se verifica que el grafo se puede 3-colorear como sigue:

Figura 5.10: *Ejemplo grafo 3-coloreado*

Nótese que a diferencia que en el caso de dos colores, aquí se tiene un grafo tanto con ciclos pares como impares, sin embargo, el grafo se pudo 3-colorear. Por otro lado, si se le añade otra arista al grafo anterior uniendo los vértices x_2 y x_5 el grafo no es 3-coloreable:

Figura 5.11: *Grafo no 3-coloreable*

En este caso al ideal I del grafo anterior se debe añadir el polinomio generador

$x_2^2 + x_2x_5 + x_5^2$, al hacer esto y calcular la base de Gröbner se tiene que 1 pertenece a esta, lo que genera la ecuación inconsistente $1 = 0$, implicando que el sistema no tiene solución.

Ahora se explorará en un rompecabezas lógico muy popular relacionado con el problema de la k -coloración, el Shidoku, cuyo objetivo es el mismo que en el Sudoku: rellenar la cuadrícula con números de tal forma que no se repita ningún número en ninguna fila, columna o bloque. En este caso, se usan los números del 1 al 4, y en lugar de 9 bloques de 3×3 , la cuadrícula de Shidoku se divide en 4 bloques de 2×2 .

Figura 5.12: *Shidoku*

			4
4		2	
	3		1
1			

Un Shidoku puede ser pensado como grafo de 16 vértices, uno por cada casilla, el cual se desea colorear con los números 1, 2, 3 y 4, se invita al lector a representar gráficamente el grafo del Shidoku en la figura 5.12. Los vértices adyacentes a uno fijo, son aquellos que se encuentran en su misma fila, columna y caja 2×2 .

Aplicando una vez más el método para colorear grafos, se procede a enumerar los vértices de izquierda a derecha y hacia abajo, obteniendo las ecuaciones:

$$x_i^4 - 1 = 0, 1 \leq i \leq 16$$

y teniendo en cuenta que $x_i - x_j \neq 0$, si estos son vértices adyacentes.

$$(x_i^2 + x_j^2)(x_i + x_j) = 0$$

tal que

$$(i, j) \in \{(1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (1, 9), (1, 13), (2, 3), (2, 4), (2, 5), (2, 6), (2, 10), (2, 14), (3, 4), (3, 7), (3, 8), (3, 11), (3, 15), (4, 7), (4, 8), (4, 12), (4, 16), (5, 6), (5, 7), (5, 8), (5, 9), (5, 13), (6, 7), (6, 8), (6, 10), (6, 14), (7, 8), (7, 11), (7, 15), (8, 12), (8, 16), (9, 10), (9, 11), (9, 12), (9, 13), (9, 14), (10, 11), (10, 12), (10, 13), (10, 14), (11, 12), (11, 15), (11, 16), (12, 15), (12, 16), (13, 14), (13, 15), (13, 16), (14, 15), (14, 16), (15, 16)\}$$

Hasta aquí tenemos entonces 72 polinomios que generarán el ideal. Además nótese que hasta aquí se estaría resolviendo un Shidoku vacío, el cual tendrá varias soluciones; surge de aquí la pregunta de ¿cómo es la base de Gröbner y qué información proporciona esta cuando un grafo se puede k -colorear de distintas maneras? Por el momento sólo interesará cuando el Shidoku tiene solución única o no tengan solución.

Obsérvese que en el Shidoku de la figura 5.12 se tienen unas casillas ya solucionadas, es decir, vértices ya coloreados los cuales pueden ser pensados como condiciones iniciales dando origen a los polinomios:

$$x_4 - 4, x_5 - 4, x_7 - 2, x_{10} - 3, x_{12} - 1, x_{13} - 1.$$

No obstante, no se pueden introducir estos polinomios así directamente al conjunto generador, debido a que el método indica que los colores que se usan son las raíces de la unidad, por lo tanto se ha decidido realizar la identificación: $1 \rightarrow 1, 2 \rightarrow -1, 3 \rightarrow i, 4 \rightarrow -i$.

Así los anteriores polinomios son transformados en:

$$x_4 + i, x_5 + i, x_7 + 1, x_{10} - i, x_{12} - 1, x_{13} - 1.$$

Al utilizar el software Mathematica¹ para encontrar la base de Gröbner correspondiente (ver figura 5.14) se obtiene:

$$G = \{1 + i^2, 1 + x_{16}, -i + x_{15}, i + x_{14}, -1 + x_{13}, -1 + x_{12}, i + x_{11}, -i + x_{10}, 1 + x_9, -i + x_8, 1 + x_7, -1 + x_6, i + x_5, i + x_4, -1 + x_3, 1 + x_2, -i + x_1\}.$$

Haciendo la correspondiente asignación de colores dada en G , la solución del Shidoku es:

Figura 5.13: *Shidoku Solución*

3	2	1	4
4	1	2	3
2	3	4	1
1	4	3	2

¹Wolfram Mathematica es un software de suscripción muy utilizado en por matemáticos debido a su potente manejo de lenguaje simbólico algebraico.

```

In[ ]:= polynomials = {
  x1^4 - 1, x2^4 - 1, x3^4 - 1, x4^4 - 1, x5^4 - 1, x6^4 - 1,
  x7^4 - 1, x8^4 - 1, x9^4 - 1, x10^4 - 1, x11^4 - 1, x12^4 - 1,
  x13^4 - 1, x14^4 - 1, x15^4 - 1, x16^4 - 1,
  (x1^2 + x2^2) * (x1 + x2), (x1^2 + x3^2) * (x1 + x3), (x1^2 + x4^2) * (x1 + x4),
  (x1^2 + x5^2) * (x1 + x5), (x1^2 + x6^2) * (x1 + x6), (x1^2 + x9^2) * (x1 + x9),
  (x1^2 + x13^2) * (x1 + x13), (x2^2 + x3^2) * (x2 + x3), (x2^2 + x4^2) * (x2 + x4),
  (x2^2 + x5^2) * (x2 + x5), (x2^2 + x6^2) * (x2 + x6), (x2^2 + x10^2) * (x2 + x10),
  (x2^2 + x14^2) * (x2 + x14), (x3^2 + x4^2) * (x3 + x4), (x3^2 + x7^2) * (x3 + x7),
  (x3^2 + x8^2) * (x3 + x8), (x3^2 + x11^2) * (x3 + x11), (x3^2 + x15^2) * (x3 + x15),
  (x4^2 + x7^2) * (x4 + x7), (x4^2 + x8^2) * (x4 + x8), (x4^2 + x12^2) * (x4 + x12),
  (x4^2 + x16^2) * (x4 + x16), (x5^2 + x6^2) * (x5 + x6), (x5^2 + x7^2) * (x5 + x7),
  (x5^2 + x8^2) * (x5 + x8), (x5^2 + x9^2) * (x5 + x9), (x5^2 + x13^2) * (x5 + x13),
  (x6^2 + x7^2) * (x6 + x7), (x6^2 + x8^2) * (x6 + x8), (x6^2 + x10^2) * (x6 + x10),
  (x6^2 + x14^2) * (x6 + x14), (x7^2 + x8^2) * (x7 + x8), (x7^2 + x11^2) * (x7 + x11),
  (x7^2 + x15^2) * (x7 + x15), (x8^2 + x12^2) * (x8 + x12), (x8^2 + x16^2) * (x8 + x16),
  (x9^2 + x10^2) * (x9 + x10), (x9^2 + x11^2) * (x9 + x11), (x9^2 + x12^2) * (x9 + x12),
  (x9^2 + x13^2) * (x9 + x13), (x9^2 + x14^2) * (x9 + x14), (x10^2 + x11^2) * (x10 + x11),
  (x10^2 + x12^2) * (x10 + x12), (x10^2 + x13^2) * (x10 + x13), (x10^2 + x14^2) * (x10 + x14),
  (x11^2 + x12^2) * (x11 + x12), (x11^2 + x15^2) * (x11 + x15), (x11^2 + x16^2) * (x11 + x16),
  (x12^2 + x15^2) * (x12 + x15), (x12^2 + x16^2) * (x12 + x16), (x13^2 + x14^2) * (x13 + x14),
  (x13^2 + x15^2) * (x13 + x15), (x13^2 + x16^2) * (x13 + x16), (x14^2 + x15^2) * (x14 + x15),
  (x14^2 + x16^2) * (x14 + x16), (x15^2 + x16^2) * (x15 + x16),
  x4 + i, x5 + i, x7 + 1, x10 - i, x12 - 1, x13 - 1};

(* Calcular la base de Gröbner *)
gbasis = GroebnerBasis[polynomials, {x1, x2, x3, x4, x5, x6, x7, x8, x9, x10, x11, x12, x13, x14, x15, x16},
  MonomialOrder -> Lexicographic];

gbasis

Out[ ]:= {1 + i^2, 1 + x16, -i + x15, i + x14, -1 + x13, -1 + x12, i + x11, -i + x10, 1 + x9, -i + x8, 1 + x7, -1 + x6, i + x5, i + x4, -1 + x3, 1 + x2, -i + x1}

```

Figura 5.14: *Uso de Wolfram Mathematica para encontrar una base de Gröbner*

Nota: Se ha decidido usar Mathematica debido a que es visualmente más amigable en su interfaz a la hora de la escritura con respecto a CoCoA. Por otro lado, también se ha aprovechado la IA para generar los polinomios y ordenarlos en forma de lista debido a la cantidad.

Figura 5.15: Uso de chatGPT para enlistar polinomios



Claramente el Shidoku además de ser un caso particular del problema de 4-colorear un grafo, también lo es de un Sudoku, dónde se tiene una cuadrícula de tamaño 9×9 con cajas de 3×3 que se desea 9-colorear.

Se hace evidente también que la generalización del problema del k -coloreado consiste en resolver el sistema que contiene las n ecuaciones de la forma $x_i^k - 1 = 0$, una por cada vértice del grafo, y tantas de la forma $\frac{x_i^k - x_j^k}{x_i - x_j} = 0$ como aristas que este

tenga.

5.3. Criptografía (Polly Cracker)

Esta sección tiene como objetivo dar una mirada muy superficial al uso de las bases de Gröbner en Criptografía, para una investigación más detallada el lector puede referirse a (Albrecht, Farshim, Faugere, y Perret, 2011).

Como es sabido, criptografía es el estudio de los métodos de cifrado de mensajes de manera que se proteja la información enviada por el emisor y sea recibida de forma privada por el receptor. De este modo, se llama **Criptosistema** a un algoritmo que realice la labor de encriptar y desencriptar mensajes.

Los criptosistemas se pueden separar en dos grandes grupos: Los de **clave privada o simétricos** caracterizados por usar una misma clave tanto para encriptar como desencriptar los mensajes, algunos ejemplos de ellos son el cifrado Cesar o el cifrado Hill, por otro lado, están los cifrados de **clave pública o asimétricos** los cuales usan dos claves, una para encriptar y otra para desencriptar, entre los cuales se encuentra el cifrado Polly Cracker el cuál se ilustra a continuación:

Ejemplo 5.3.1. Sea $K = \mathbb{Z}_2$, supóngase que Bob desea enviar el mensaje $m = 1 \in K$ a Alice. Ella necesita una clave pública (que cualquiera podría conocer) para que Bob encripte su mensaje, en el caso Polly Cracker esta clave es un conjunto aleatorio de polinomios pertenecientes a un ideal I sobre el anillo $\mathbb{Z}_2[x, y, z]$.

Supóngase que Alice escoge los siguientes polinomios, elementos de $\mathbb{Z}_2[x, y, z]$:

$$f_1 = x^2 + y$$

$$f_2 = x^3 + z$$

$$f_3 = xy + z$$

Además supóngase que $I = \langle f_1, f_2, f_3 \rangle$. Como clave privada Alice debe escoger un $\gamma \in V(I)$, esto lo podría realizar usando una base de Gröbner G para I :

$$G = \{xy + z, x^2 + y, y^2 + xz\}$$

Solucionado la ecuación

$$x^2 + y = 0$$

Si $x = 0$ entonces $y = 0$, si $x = 1$ se deduce también que $y = 1$, por lo tanto, las posibles soluciones son de la forma $(0, 0, z)$ o $(1, 1, z)$, ahora, usando la ecuación $xy + z$, se obtienen las soluciones $(0, 0, 0)$ y $(1, 1, 1)$.

En este ejemplo tómese $\gamma = (1, 1, 1)$.

Ahora, para encriptar el mensaje, Bob toma un $h \in I$ y realiza la suma $c := h + m$

$$c = x^3 + xy + 1$$

Este será el mensaje encriptado que enviará a Alice. Para desencriptar el mensaje, Alice deberá evaluar este polinomio en γ , es decir, calcular $c(1, 1, 1)$ y así obtendrá el mensaje enviado por Bob.

En este ejemplo, por simplicidad se tomó el cuerpo finito $(\mathbb{Z}_2, +, \cdot)$ y el posible mensaje a enviar es o bien 0 o 1, sin embargo, para un alfabeto de 26 caracteres puede pensarse en \mathbb{Z}_{29} , haciendo una correspondencia entre cada letra del alfabeto con un número entre 0 y 28 añadiendo símbolos especiales como espacios, puntos, guiones, etc. Para los números sobrantes.

El uso de un cuerpo finito asegura que los coeficientes y las operaciones permanezcan dentro de un conjunto controlado de valores, evitando que los polinomios “crezcan” demasiado y que los cálculos sean ineficientes. Además, los cuerpos finitos hacen que los problemas de descifrado (como la reducción de bases de Gröbner) sean computacionalmente difíciles, lo cual da seguridad al criptosistema.

Otro método de encriptación es el conocido como Barkee, para explicar su funcionamiento se sigue la idea de (de La Torre Fernández, 2016) donde se toma $F \subset K[X]$, finito y $<_T$ un orden de términos, se denominará como forma normal de $a(X) \in K[X]$ respecto de F , a un polinomio mónico $\hat{a}(X)$ que satisfaga las condiciones:

$$\text{i) } \text{Sop}(\hat{a}(X)) \cap \{\alpha + \mathbb{N}^n : aX^\alpha \in TP(F)\} = \emptyset.^2$$

²En su trabajo de grado el autor hace referencia a la intersección de $\text{Sop}(\hat{a}(X))$ con el conjunto $IN_{\leq}(F) + \mathbb{N}^n$, no obstante esto es un error puesto que $IN_{\leq}(F)$ es un conjunto de términos principales, es decir, es de diferente naturaleza que \mathbb{N}^n estando la operación “+” mal definida y por tanto la intersección mencionada es vacía de forma trivial.

ii) Existe $h(X) \in \langle F \rangle$ tal que $\hat{a}(X) = a(X) + h(X)$.

Esta forma normal servirá para encriptar el mensaje que Bob desea enviar a Alice de la siguiente manera:

Ejemplo 5.3.2. Alice usa como clave pública el conjunto de polinomios en $\mathbb{Q}[x, y]$ con el orden lexicográfico ($<_l$):

$$F = \{f_1 := 3x^2y^2 - 5xy + 4, f_2 := 5x^3y - 3x\}$$

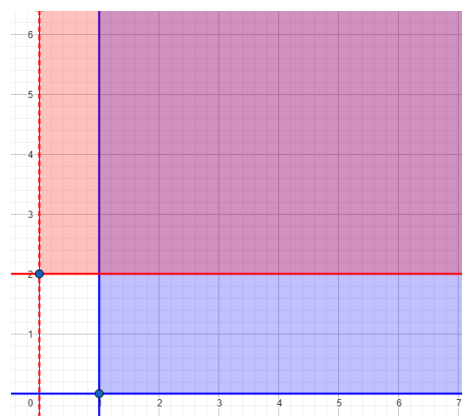
y un conjunto de formas normales N de tal manera que su soporte tenga intersección vacía con el conjunto $\{\alpha + \mathbb{N}^2 : aX^\alpha \in TP(G)\}$, aquí, G es la base de Gröbner reducida para el ideal $I = \langle F \rangle$.

La base de Gröbner reducida es:

$$G = \left\{ x + \frac{9}{80}y - \frac{13}{40}, y^2 - \frac{2}{9}y + \frac{64}{9} \right\}$$

Aquí $TP(G) = \{x, y^2\}$ y por tanto el soporte de las formas normales deben tener intersección vacía con:

$$\{(1, 0), (0, 2)\} + \mathbb{N}^2 = \{(1 + n, n), (n, 2 + n) : n \in \mathbb{N}\}$$

Figura 5.16: *Intersección*

La figura anterior muestran la región donde se encuentran las parejas ordenadas del conjunto anterior, allí se pueden apreciar las posibles potencias para las formas normales, es decir, $(0,0), (0,1)$ por lo tanto, Alice puede escoger la forma $N = \{y\}$.

Supóngase que Bob quiere enviar el número 8 como mensaje, entonces toma el polinomio $m := 8y$ y una combinación lineal de los polinomios de F (que puede ser cualquiera), por ejemplo, $h := 3yf_1 - 4yf_2$ y envía a Alice

$$h + m = -20x^3y^2 + 9x^2y^3 - 15xy^2 - 12xy + 20y$$

Finalmente, Alice para descryptar el mensaje sólo debe reducir el polinomio $h + m$ con respecto a G .

Conclusiones

Las bases de Gröbner se constituyen en una herramienta fundamental para el estudio de ideales en la teoría de anillos de polinomios en varias variables, ya que si un ideal es generado por una de ellas, entonces para todo elemento del ideal su término principal (bajo un orden determinado) es divisible por el término principal de algún elemento de la base, lo cual conlleva, de cierta forma, a extender el algoritmo de la división a anillos de polinomios en varias variables.

Una de las ventajas que ofrecen las bases de Gröbner es la existencia de un mecanismo para decidir si un polinomio dado f , perteneciente a un anillo de polinomios $(A[X], +, \cdot)$, es miembro de un ideal $I \subset A[X]$. Este problema, conocido como el **Ideal Membership Problem**, es fundamental en álgebra computacional y la obtención de una base de Gröbner para un ideal permite resolverlo de manera eficiente. Otra de las ventajas de tales bases consiste en la posibilidad de abordar algunas aplicaciones en otras ramas de las matemáticas, por ejemplo, relacionados con sistemas de ecuaciones polinómicas, optimización de funciones en varias variables sobre un campo, análisis de sistemas criptográficos o teoría de grafos.

Para encontrar una base de Gröbner G de un ideal I en un anillo de polinomios $(A[X], +, \cdot)$, se debe definir un orden para los términos de los polinomios en este anillo, luego encontrar los S -polinomios de los generadores de I y con ayuda de la reducción verificar si el residuo es cero, de lo contrario añadir este S -polinomio al conjunto de generadores, lo que se constituye en el algoritmo de Buchberger. Es en este punto donde el análisis del algoritmo de la división en el anillo juega un papel importante, ya que se ve la necesidad de establecer un orden para los términos del polinomio atendiendo a las diferentes variables y de abordar conceptos como la reductibilidad; estas observaciones llevan a que, por ejemplo, se identifique la no unicidad de la división (e.d. del cociente y del residuo).

Lo anterior pone de manifiesto la necesidad de contar con un conocimiento sólido de algunos elementos relacionados con la teoría de grupos, la teoría de anillos, la teoría de anillos de polinomios y de identificar algunas relaciones que se presentan entre ellas. Al respecto, el autor de este trabajo es consciente de que no es suficiente con acudir a la literatura especializada y tomar de manera aislada las definiciones y teoremas ya demostrados, sino que para lograr una adecuada construcción teórica es pertinente profundizar en el estudio de los temas, reconstruir una línea temática exaltando las dificultades, los problemas matemáticos que llevan a la construcción de los conceptos, construir ejemplos propios y reconstruir algunas de las demostraciones.

En esta dirección, el desarrollo de este trabajo de grado le permitió al autor asumir la tarea de un matemático al reconstruir parte de una teoría, fortaleciendo competencias relacionadas con la investigación, comunicación, lectura, escritura y síntesis de información matemática, las cuales son habilidades que pueden mejorar

la formación integral de un profesor de matemáticas.

Adicionalmente, aunque se es consciente de que a nivel escolar (en educación básica y media), en general, no se trabajan dichos conceptos de la manera formal en que son expuestos en el trabajo, el hecho de abordar con el nivel de profundidad mostrado en este documento temas propios de las matemáticas permite fortalecer la formación matemática y el reconocimiento de conexiones entre diversos temas y ampliar la comprensión de algunos conceptos y objetos que son trabajados en la escuela, por ejemplo, todo lo relacionado con polinomios, el algoritmo de la división, mecanismos para solucionar sistemas de ecuaciones, aplicaciones de las matemáticas en diversos contextos, lo que, a su vez, permitirá hallar y proponer distintas formas de abordar los contenidos en la escuela sin que resulte un despropósito para el aprendizaje de los futuros estudiantes.

Otro elemento que fue fundamental en el desarrollo del trabajo consiste en el uso de diferentes herramientas tecnológicas como Software de cálculo simbólico (CoCoA, Singular, Wolfram Mathematica) o inteligencia artificial (ChatGPT, Julius IA), las cuales permiten de manera eficiente y eficaz implementar los algoritmos estudiados, desarrollar ejemplos, desarrollar escritos en lenguajes especializados (LaTeX). Este conocimiento de la tecnología enriquece el estudio mismo de las matemáticas y permite el desarrollo de otras competencias pertinentes a la época actual en la que vivimos como el lograr una comunicación asertiva de ideas para una transmisión efectiva de conocimientos. Además, evidenciar que el uso de IA resulta útil en la resolución de problemas matemáticos me encaminan a llevarlas al aula y usarlas como un instrumento de enseñanza.

El haber podido entender para posteriormente reconstruir los fundamentos de una teoría matemática enriqueció mi pasión por las matemáticas y espero que el uso de una herramienta especializada para la comunicación en matemáticas como es el editor de texto LaTeX me haya permitido expresar de manera efectiva las ideas plasmadas en este trabajo.

Finalmente, se recalca que en este documento se abordan algunas ideas relacionadas con la teoría de bases de Gröbner pero no es exhaustivo y existen diferentes caminos para continuar el trabajo, por ejemplo, estudiar otros algoritmos para la construcción de bases de Gröbner, establecer si el algoritmo estudiado puede ser mejorado, identificar comportamientos o propiedades de las bases de Gröbner en anillos de polinomios sobre anillos diferentes a los abordados (por ejemplo sobre el anillo de los números dobles, duales, campos de característica finita, matrices,), estudiar implicaciones del algoritmo de la división en anillos de polinomios para tareas como la descomposición de elementos, estudiar el uso de otras tecnologías digitales relacionadas con bases de Gröbner.

UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

Referencias

- Adams, W. W., y Loustaunau, P. (1994). *An introduction to gröbner bases* (Vol. 3). American Mathematical Society.
- AI, J. (2024). *Respuesta generada por la inteligencia artificial julius ai*. Descargado de <https://julius.ai/> (Accedido el 14 de diciembre de 2024)
- Albrecht, M. R., Farshim, P., Faugere, J.-C., y Perret, L. (2011). Polly cracker, revisited. En *International conference on the theory and application of cryptology and information security* (pp. 179–196).
- ChatGPT. (2024). *Respuesta generada por el modelo de lenguaje gpt-3.5 de openai*. Descargado de <https://chat.openai.com/> (Accedido el 14 de diciembre de 2024)
- CoCoA Team. (2024). *Cocoa manual: Computations in commutative algebra* [Manual de software informático]. Descargado de <http://cocoa.dima.unige.it/manual.html> (Accedido el 14 de diciembre de 2024)

- de La Torre Fernández, P. (2016). *Criptografía con bases de gröbner* (Tesis de Master no publicada). Universidad de La Laguna, Santiago de La Laguna, Tenerife. (Trabajo de Grado)
- Fraleigh, J. B. (2003). *A first course in abstract algebra*. Pearson Education India.
- Hungerford, T. (2012). *Algebra*. Springer.
- Saracino, D. (2008). *Abstract algebra a first course*. WAVELAND PRESS, INC.



UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores

Índice alfabético

- Anillo, 34
- de división, 37
 - con identidad, 34
 - Conmutativo, 34
 - de ideales principales, 45
- Base de Gröbner, 104, 124
- mínima, 126
 - Reducida, 128
- Campo, 37
- Cerrado, 24
- Clase
- de equivalencia, 29
 - Lateral a derecha, 30
 - Lateral a izquierda, 30
- Divisor de cero, 37
- Dominio de integridad, 37
- Grupo, 15
- abeliano, 16
- Centro de un, 26
- Cociente aditivo, 54
- de permutaciones, 20
 - diédrico, 16
 - partición de un, 29
- Ideal, 40
- Bilátero, 40
 - Derecho, 40
 - Izquierdo, 40
 - Maximal, 52
 - Primo, 49, 51
 - isomorfas, 21
- Operación binaria, 10
- Polinomio
- en una variable, 61
 - en varias variables, 82
 - S-, 114
- Subanillo, 39

Subgrupo, 24

Subgrupo normal, 32

Tabla de Cayley, 12

unidad, 37



UNIVERSIDAD PEDAGOGICA
NACIONAL

Educadora de educadores