UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

UNIDAD DE INVESTIGACIÓN

INFORME FINAL DE PROYECTO DE INVESTIGACIÓN

"BASES DE GRÖBNER APLICADAS A LA CRIPTOGRAFÍA"

AUTORA: RUTH MEDINA APARCANA

(PERIODO DE EJECUCIÓN: Del 01 de junio de 2019

al 31 de mayo de 2020)

(Resolución de aprobación N° 676-2019-R)

Callao, 2020

DEDICATORIA

A la vida... que me permite seguir con mis sueños, mis metas y disfrutar de mi familia, mis amigos, mis colegas.

AGRADECIMIENTOS

Un sincero agradecimiento a todas las personas que de una u otra manera han hecho posible la ejecución y finalización de este proyecto, en especial al profesor Edgar Zárate Sarapura, que siempre me ha brindado su ayuda y consejos de manera incondicional.

Agradezco a la Universidad Nacional del Callao, específicamente al Vicerrectorado de Investigación, que a través del Fondo Especial de Desarrollo Universitario (FEDU) ha financiado de manera parcial la ejecución del presente proyecto.

ÍNDICE

ÍNDICE DE FIGURAS

TABLAS DE CONTENIDO

Pág.

RESUMEN

El proteger la información que se envía por un medio público como internet, es una de las grandes preocupaciones en la actualidad y es uno de los grandes retos mantenerla a salvo; por ello es importante la búsqueda constante de criptosistemas fuertes ante el avance y desarrollo de la tecnología. Hemos trabajado con polinomios en varias variables, porque generarían un algoritmo basado en un problema matemático distinto al de factorización de enteros en números primos, que sea resistente al algoritmo de factorización de Shor y a ordenadores cuánticos, los cuales pronto invadirán nuestro mundo. Para lograrlo, se ha definido un orden y se ha logrado una cierta generalización del algoritmo de división en el anillo de polinomios de varias variables. Como resultado de todo lo anterior se pudo definir las bases de Gröbner reducidas para ideales en dicho anillo que además son únicas y que constituyen la clave secreta para un criptosistema asimétrico, cuya clave pública es un conjunto de generadores. En conclusión, es posible generar un criptosistema basado en polinomios en varias variables cuya clave pública es un conjunto de polinomios generadores de un ideal y su clave secreta es la base de Gröbner reducida, del ideal generado por dicho conjunto de polinomios.
Palabras Claves: criptosistema, clave pública, base de Gröbner

ABSTRACT

Protecting the information that is sent through a public medium such as the internet is one of the great concerns at present and it is one of the great challenges to keep it safe; For this reason, the constant search for strong cryptosystems is important in light of the advancement and development of technology. We have worked with polynomials on several variables, because they would generate an algorithm based on a mathematical problem other than that of factoring integers into prime numbers, which is resistant to Shor's factorization algorithm and quantum computers, which will soon invade our world. To achieve this, an order has been defined and a certain generalization of the algorithm of division in the polynomial ring of several variables has been achieved. As a result of all the above, it was possible to define the reduced Gröbner bases for ideals in said ring that are also unique and that constitute the secret key for an asymmetric cryptosystem, whose public key is a set of generators. In conclusion, it is possible to generate a cryptosystem based on polynomials in several variables whose public key is a set of polynomials that generate an ideal and its secret key is the reduced Gröbner base, of the ideal generated by said set of polynomials.

Keywords: cryptosystem, public key, Gröbner base

INTRODUCCIÓN

Una inquietud que está siempre presente en la vida de todo ser humano es tener protegido sus datos y su información, de observadores no autorizados.

Debido al constante desarrollo y evolución de los medios de comunicación, en especial del internet, los métodos y técnicas para proteger la información, están en una constante mejora, pues todo código secreto seguro, se vuelve inseguro y vulnerable con el tiempo.

La ciencia que se encarga de la protección de la información mediante cifrados y códigos secretos es la Criptografía; y lo hace a través de algoritmos matemáticos. Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la web, la autenticación del usuario y también la del remitente, el destinatario y de la actualidad del mensaje o del acceso, entonces es evidente que los cifrados o encriptados (criptosistemas) de seguridad actuales deben ser lo suficientemente fuertes para acciones como las transacciones por internet y los correos electrónicos; que con el paso del tiempo deberán ser más resistentes a ataques de quienes quieren interceptarla, los cuales también ser fortalecen, por lo que la guerra, se hace implacable.

El criptosistema RSA, que debe su nombre a las iniciales de sus creadores Rives Shamir y Adleman; es el criptosistema más usado en la actualidad, es de clave pública y se basa en la factorización de enteros en números primos grandes, la dificultad es que hasta la actualidad no se conoce ningún algoritmo rápido que haga la factorización, pues la velocidad de resolución de algunos problemas en un ordenador clásico crece de manera exponencial respecto a la cantidad de información.

Con la aparición de los ordenadores cuánticos se tenía la esperanza de obtener factorizaciones rápidas, sin embargo, hasta la actualidad no se ha logrado construir un ordenador cuántico que haga vulnerable al sistema RSA.

En esta investigación nos enfocaremos lograr sistemas criptográficos basados en sistemas de ecuaciones polinomiales de varias variables mediante el uso de las bases de Gröbner presentadas, por Buchberger en 1965, como una alternativa a este problema de crecimiento exponencial.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

Actualmente con el uso masivo de la internet, es fundamental poder mantener nuestros datos y nuestra información valiosa a salvo y segura. Mantener nuestra información fuera del alcance de personas ajenas, es un reto y un problema que perdura con el tiempo, más aún, en estas épocas de aislamiento social, donde todas las comunicaciones y adquisiciones son por medios públicos como lo es la internet que nos permite llegar de una manera rápida y a poco costo.

A lo largo de la historia se han diseñado diferentes procedimientos y algoritmos para proteger la información; pero si existe alguien que necesita o requiere proteger información valiosa por alguna razón, existe también quien quiere romper esa seguridad y busca alcanzarla sin permiso.

Entonces es importante poder proteger la información que se envía por medios inseguros; esta protección de la información la podemos obtener con algoritmos matemáticos fuertes, resistentes a cualquier ataque.

Es así que la criptografía está en constante cambio, mejora y evolución.

Inicialmente para proteger un mensaje, este se transformaba en un mensaje ilegible por medio de una clave. Solo la persona que conocía la clave o podía
detectar la clave podía leerlo. Pero compartir la clave por un medio seguro tenía la misma dificultad que compartir el mensaje, lo que lo convirtió en un método inseguro de usar.

Esta falencia, dio lugar a la llamada criptografía asimétrica por la cual se cuenta con dos claves distintas una para encriptar (clave pública) y otra diferente para desencriptar(clave secreta); actualmente ésta criptografía asimétrica es uno de los pilares de la criptografía actual.

Son muchos los algoritmos basados en la criptografía asimétrica, uno de los más fuertes que hasta hoy perdura es el RSA, creado por Rivest, Shamir y Adleman. Su fortaleza radica en la dificultad de factorizar un entero en primos grandes.

Sabemos que, aunque los primos son en cantidad infinitos, no son fáciles de encontrar, más aún cuando son muy grandes, por lo que requiere tiempo para encontrarlos. Además de ordenadores potentes.

El matemático Peter Shor presentó en 1994 un algoritmo para factorizar enteros grandes en números primos; y se creyó que con este algoritmo se perdería la seguridad en internet. Y así hubiera sido, si es que, para que este algoritmo de Shor fuera efectivo no se requiriera de un ordenador cuántico de miles de q-bits.

Este algoritmo de Shor puede romper algoritmos que tienen como base la factorización y en DLP (problema del logaritmo discreto) es decir puede quebrar también al DSA (Algoritmo de firma digital basado en el logaritmo discreto) y el ECDSA(el algoritmo de firma digital sobre curvas elípticas), y más aún, en tiempo polinomial. La criptografía con curvas elípticas no soluciona el problema como se esperaba.

Hasta hoy, no se cuenta con ordenadores cuánticos, pero se sabe que en un tiempo no muy lejano esto se logrará. Por ello es necesario, encontrar nuevos algoritmos que sean resistentes a ordenadores cuánticos.
Es así como, surge la idea de crear sistemas criptográficos algebraicos basados en polinomios cuya clave pública es un conjunto de polinomios de varias variables que generan un ideal J. Y su fortaleza radica en determinar una base de Gröbner reducida de J.

1.2 Formulación del problema

1.2.1 Problema General

¿Cuál es la forma de obtener algoritmos criptográficos usando bases de Gröbner?

1.2.2 Problemas Específicos

1.-¿Cuáles son las características de una base de Gröbner?
2.-¿Cuáles son las condiciones para que existan las bases de Gröbner?
3.-¿Cuál es la función de las bases de Gröbner en el criptosistema?

1.3 Objetivos

1.3.1. Objetivo General

Describir la forma de obtener un algoritmo criptográfico aplicando bases de Gröbner.

1.3.2. Objetivos Específicos

1. Describir las características de las bases de Gröbner respecto a la relación de orden.
2. Determinar las condiciones de existencia de las bases de Gröbner Reducida.
3. Determinar la función de las bases de Gröbner en el criptosistema.

1.4 Limitantes de la investigación

Uno de los limitantes en esta investigación es que esta no sea ha desarrollado en el anillo de polinomios sobre un cuerpo finito, pues con esta consideración se podrían alcanzar otros resultados importantes.

CAPÍTULO II: **MARCO TEÓRICO**

2.1 Antecedentes

2.1.1 Internacionales

En el ámbito internacional son muchos los antecedentes de uso y estudio de la criptografía, pues desde que existe el hombre, se ha buscado proteger la información.
En la antigüedad, la criptografía era básicamente de uso militar y gubernamental; es así que César el emperador romano, solía proteger su información mediante el llamado Cifrado que lleva su nombre. Sin ahondar mucho señalaremos que después de ello se crearon máquinas mecánicas y electromecánicas para lograr tener a salvo la información, básicamente de tipo militar; y posteriormente con el avance de la ciencia, se ha hecho uso de ordenadores, la electrónica y la computación para conseguir métodos más elaborados y complejos para proteger la información.
Se considera que la criptografía moderna se inicia realmente, con Claude Shannon que es considerado el padre de la criptografía matemática. En 1949 publicó el artículo "Communication Theory of Secrecy Systems" en la Bell System Technical Journal, y poco después el libro Mathematical Theory of Communication, con Warren Weaver. Estos trabajos, junto con los otros que publicó sobre la teoría de la información y la comunicación, establecieron una sólida base teórica para la criptografía y el criptoanálisis. Verdu, S. (1998).
Mencionaremos solo algunos de los investigadores que se le han sucedido después; cuya orientación de su investigación puede contribuir de alguna manera a este proyecto:

Diffie y Hellman (1976) con el fin de resolver el problema de pactar una clave secreta de antemano, dieron lugar a la criptografía de clave pública.
Rives, Shamir y Adleman impusieron el sistema RSA, que se basa en el problema de factorizar enteros en números primos grandes.

Koblitz(1994) en su libro titulado de Teoría de Números y Criptografía en que claramente muestra de manera didáctica la idea de criptografía y métodos básicos de teoría de números para sistemas criptográficos, y también propone usar curvas algebraicas como un modelo de criptografía en clave pública.

En todos estos casos, los criptosistemas están fundamentados en la Aritmética Modular y la Teoría de Números; y la dificultad radica en el tiempo que se requiere para factorizar un entero como producto de números primos grandes, que no es poco y depende mucho del número de cifras de los primos grandes, por lo que se considera que un criptosistema de clave pública es lento. Esta dificultad, esperaba superarse con la aparición de ordenadores cuánticos, pero hasta la actualidad no se ha conseguido, a pesar de haber realizado muchos intentos.

Por otro lado, en 1965, Buchberger introdujo la definición de Bases de Gröbner, presentó un estudio de los ideales del anillo de polinomios mediante las Bases de Gröbner y mostró un algoritmo para calcularlas; luego en el año 2011, Buchberger publicó su libro titulado "Gröbner bases and Aplications", en el que desarrolla una interesante teoría de las bases de Gröbner y como primeras aplicaciones de ésta teoría, desarrolla algoritmos para determinar la pertenencia de un polinomio a un ideal, la igualdad de ideales, muestra métodos para calcular intersección, suma, producto y cociente de ideales, entre otros. Buchberger, B.(2011).

Desde entonces, las Bases de Gröbner se investigan en diversas ramas de la ciencia e ingeniería, por su capacidad de resolver sistemas de ecuaciones polinomiales y la posibilidad de desarrollar algoritmos computacionales.

El hecho de resolver sistemas de ecuaciones polinomiales motiva la idea de aplicar esta teoría a la creación de criptosistemas de clave pública, que sean eficaces, fuertes y resistentes a ordenadores cuánticos.

En esta investigación presentaremos un criptosistema usando la teoría de bases de Gröbner, aprovechando la posibilidad de resolver sistema de ecuaciones de varias variables en el anillo de polinomios.

2.1.2 Nacionales

Los trabajos realizados en el estudio de Bases de Gröbner a nivel nacional, son los siguientes:

Marca (2008) con su tesis titulada:" Bases de Gröbner con aplicaciones al álgebra conmutativa", en la cual que se resume en algunas principales ideas que envuelven métodos computacionales algebraicos y la importancia de tales métodos está en la posibilidad de atacar temas clásicos del algebra conmutativa y geometría algebraica de una manera algorítmica, simplificando cálculos de manera efectiva. Este autor desarrolla las bases de Gröbner y las aplica al álgebra conmutativa, pero no la vincula a la criptografía, como lo haremos en este proyecto de investigación.

Leyva (2016) con su tesis titulada: "Los Sistemas de Ecuaciones Polinomiales y Polinomios Simétricos sobre bases de Gröbner", en la cual se expone la teoría de bases de Gröbner a la solución de sistemas de ecuaciones Polinomiales no lineales y Polinomios simétricos. Este autor aplica las bases de Gröbner para le resolución de Ecuaciones Polinomiales, pero no hace ninguna aplicación a la criptografía. En este proyecto de investigación, desarrollaremos las bases de Gröbner y lo aplicaremos a la criptografía.

2.2 Marco

2.2.1 Teórico

ANILLOS E IDEALES

Definición 2.1: Un anillo es un conjunto no vacío A con dos operaciones, llamadas adición y multiplicación, denotadas respectivamente por "$+$" "$\cdot$", de tal forma que: $(A, +)$ es un grupo abeliano. La multiplicación es asociativa y se cumple la propiedad distributiva. El anillo A se dice conmutativo, si la multiplicación es conmutativa. El anillo A se dice con unidad o unitario si existe un elemento neutro multiplicativo, es decir : $\exists\ 1 \in A: a \cdot 1 = 1 \cdot a = a \forall\ a \in A$. El elemento 1 es llamado elemento unidad del anillo. Un anillo unitario A con $1 \neq 0$ se llama anillo de división si todo elemento $a \in A, a \neq 0,$ tiene inverso multiplicativo, esto es $\exists b \in A\ /\ a \cdot b = b \cdot a = 1$.

Veamos algunos ejemplos:

- $(Z, +, \cdot)$ es un anillo conmutativo con unidad e infinito, mientras que $(Z_n, +, \cdot)$ es un anillo finito, conmutativo con unidad.
- $(Q, +, \cdot), (R, +, \cdot)\ y\ (C, +, \cdot)$ son también anillos conmutativos con unidad infinitos.
- Sea X un conjunto no vacío y $(A, +, \cdot)$ un anillo, si

$$R = \{f : X \to A\ /\ f \text{ es una aplicación}\}$$

entonces R con la suma y el producto "usual" de funciones es un anillo.
Note que R es un anillo conmutativo si A lo es (el recíproco también se cumple) y será un anillo unitario si A tiene elemento unidad. En efecto: Si 1 es el elemento unidad de A, la función $f : X \to A$ definida por $f(x) = 1, \forall\ x \in X$ será el elemento unidad del anillo R.
Sea A un anillo unitario y $U(A) = \{u \in A\ /\ u \text{ es inversible}\}$, no es difícil ver que $(U(A), \cdot)$ es un grupo, llamado el grupo de las unidades del anillo A.
Un anillo $(K, +, \cdot)$ conmutativo con unidad $1 \neq 0$ tal que $U(K) = K \setminus \{0\}$ se llama cuerpo. Veamos algunos ejemplos de cuerpos: los anillos $(Q, +, \cdot), (R, +, \cdot)\ y\ (C, +, \cdot)$ son cuerpos. El conjunto

$$Q[\,i\,] = \{\,a + bi\ /\ a, b \in Q\,\}$$

con la suma y producto usual de los números complejos es un cuerpo, llamado el cuerpo gaussiano. En particular si $(a + bi) \neq 0$,

$$(a + bi)^{-1} = \left(\frac{a}{a^2 + b^2}\right) + \left(\frac{-b}{a^2 + b^2}\right) i$$

Este ejemplo notamos que existen infinitos cuerpos finitos, pues Z_p es un cuerpo, si y solo si p es un número primo.

Definición 2.2: Un anillo A conmutativo y con unidad $1 \neq 0$ se llama dominio de integridad si no tiene divisores de cero, es decir, si $ab = 0$ entonces $a = 0$ o bien $b = 0$.
Proposición 2.1 Sea A un dominio de integridad. Si A es finito, entonces A es un cuerpo.

Prueba. Sea $a \in A, a \neq 0$. Si consideramos la función $f: A \to A$ definida por $f(x) = ax \; \forall \, x \in A$, se tiene que f es inyectiva. En efecto: si $f(x) = f(y)$ entonces $ax = ay$, equivalentemente $a(x - y) = 0$ con $a \neq 0$. Luego siendo A un dominio de integridad $x = y$. Además, como A es finito, f es sobreyectiva. Por lo tanto, para $1 \in A$ existe $b \in A$ tal que $ab = f(b) = 1$.

Definición 2.3:

Un subconjunto no vacío I del anillo $(A, +, \cdot)$ es un ideal, si:

1. $(a - b) \in I \; ; \;\; \forall \, a, b \in I$.
2. $ra, ar \in I \; \forall \, a \in A \; \forall \, r \in I$.

Por ejemplo $nZ = \{nk / k \in Z\}$ es un ideal de Z, y si $(A, +, \cdot)$ un anillo y J un ideal de A. Entonces $M_n(J)$ es un ideal de $M_n(A)$.

En efecto: $M_n(J)$ es no vacío, pues contiene a la matriz nula. Si $(a_{ij}), (b_{ij}) \in M_n(J)$, entonces $(a_{ij}) - (b_{ij}) = (a_{ij} - b_{ij}) \in M_n(J)$ ya que $a_{ij} - b_{ij}$ está en J. Finalmente si $(a_{ij}) \in M_n(A)$ y $(\alpha_{ij}) \in M_n(J)$, entonces $(a_{ij})(\alpha_{ij}) = (c_{ij})$ y $(\alpha_{ij})(a_{ij}) = (d_{ij})$ están en $M_n(J)$ pues:

$$c_{ij} = \sum_{k=1}^{n} a_{ik}\alpha_{kj} = \left(a_{i1}\alpha_{1j} + a_{i2}\alpha_{2j} + \cdots + a_{in}\alpha_{nj}\right) \in J$$

$$d_{ij} = \sum_{k=1}^{n} \alpha_{ik}a_{kj} = \left(\alpha_{i1}a_{1j} + \alpha_{i2}a_{2j} + \cdots + \alpha_{in}a_{nj}\right) \in J$$

Proposición 2.2 Sea $(A, +, \cdot)$ un anillo con unidad. Si I es un ideal propio de A, entonces $I \cap U(A) = \emptyset$.

Prueba. Si existe $u \in I \cap U(A)$, entonces $u \in I$ y para algún $v \in A, uv = vu = 1$, luego $1 = uv \in I$ (pues $u \in I$). Ahora si $a \in A$, entonces $a = a \cdot 1 \in I$ (pues $1 \in I$); es decir $I = A$. Luego el ideal I no es propio.

Definición 2.4: Sistema de generadores de ideales

Si $\{I_\lambda\}_{\lambda \in \Lambda}$ *es una colección arbitraria de ideales de un anillo* A, *entonces* $\bigcap_{\lambda \in \Lambda} I_\lambda$ también es un ideal del anillo A. En particular, si S es un subconjunto no vacío de A, entonces

$$\langle S \rangle = \bigcap {}_{I \text{ ideal de } A \; I \supseteq S} \, I$$

es un ideal del anillo A, llamado ideal generado por S, y S es un generador o sistema de generadores del ideal $\langle S \rangle$.

Definición 2.5:

Si $S = \{a_1, a_2, \ldots, a_n\}$, se dice que el ideal generado por S es finitamente generado y escribimos $\langle S \rangle = \langle a_1, a_2, \ldots, a_n \rangle$, y si $n = 1$ se dice que el ideal es principal.

De otro lado un anillo $(A, +, \cdot)$ se llama anillo de ideales principales, si todo ideal de A es principal. Por ejemplo $(Z, +, \cdot)$ es un anillo de ideales principales.

Proposición 2.3 Sea $(A, +, \cdot)$ un anillo conmutativo con unidad y $S \subseteq A$ no vacío. El ideal generado por S es

$$\langle S \rangle = \{\sum_{i=1}^{n} \quad \{a_i s_i / a_i \in A, s_i \in S, n \in N\} \qquad (1$$

Prueba. Sea I el conjunto que aparece en el lado derecho de (1); es fácil ver que I es un ideal de A (aquí precisamos de la hipótesis de conmutatividad). Como $s = 1 \cdot s$ para todo $s \in S$ tenemos que $S \subseteq I$. Además, si J es un ideal de A que contiene a S, afirmamos que $I \subseteq J$. En efecto: Si $x \in I$, existe $n \in N$ y existen $a_i \in A$, $s_i \in S (\therefore s_i \in J)$ tal que

$$x = \sum_{i=1}^{n} \quad a_i s_i, luego\ x \in J. En\ particular, si\ J = \langle S \rangle\ tenemos\ que$$

$$I \subseteq J = \langle S \rangle = \bigcap_{T\ ideal\ de\ A\ T \supseteq S} T \subseteq I$$

es decir $I = \langle S \rangle$.

Definición 2.6: (HOMOMORFISMOS)

Sean A y A' dos anillos. Un homomorfismo de A en A' es una función $f: A \to A'$ tal que, $\forall a, b \in A$:

(i) $f(a + b) = f(a) + f(b)$

(ii) $f(a \cdot b) = f(a) \cdot f(b)$

Si, además, f es biyectiva se dice que f es un isomorfismo entre A y A'. Si existe un isomorfismo entre los anillos A y A' se dice que estos anillos son isomorfos, lo cual se denota por $A \cong A'$. La siguiente proposición muestra algunas propiedades de este tipo de funciones.

Proposición 2.4 Sea $f: A \to A'$ un homomorfismo de anillos.

1. Si J es un ideal de A' , entonces $f^{-1}(J)$ es un ideal de A.
2. $Ker(f) := \{a \in A / f(a) = 0\}$ es un ideal de A.
3. $Im(f)$ es un subanillo de A'.
4. Si I es un ideal de A, entonces $f(I)$ es un ideal de $Im(f)$
5. f es inyectiva, si y sólo si $Ker(f) = \{0\}$.

La prueba de este resultado lo encontramos en Burton (1970).

Definición 2.7:

Sea A un anillo e I un ideal de A. Si en el conjunto $\frac{A}{I} = \{a + I / a \in A\}$ definimos

$$(a + I) \oplus (b + I) = (a + b) + I,$$

$$(a + I) \odot (b + I) = ab + I \ \forall\ a, b \in A$$

Es fácil ver que $\oplus$ es una operación bien definida en $\frac{A}{I}$ y que $\left(\frac{A}{I},\oplus\right)$ es un grupo abeliano. Por otro lado si $a+I=a'+I$ y $b+I=b'+I$, entonces $a-a'=i_1$ y $b-b'=i_2$ con $i_1, i_2 \in I$, luego
$ab-a'b'=ab-ab'+ab'-a'b'=a(b-b')+(a-a')b'=(ai_2+i_1b') \in I$.
es decir $ab+I=a'b'+I$. Esto demuestra que $\odot$ es otra operación bien definida en $\frac{A}{I}$, y que $\left(\frac{A}{I}, \oplus, \odot\right)$ es un anillo, llamado anillo cociente de A por I.

Si A es un anillo conmutativo, entonces $\frac{A}{I}$ también lo es. Si A es un anillo con unidad 1, entonces $\frac{A}{I}$ también es un anillo con unidad $(1+I)$. Además, la función π: $A \to \frac{A}{I}$ definida por $\pi(a)=a+I \ \forall\, a \in A$ es un homomorfismo sobreyectivo con Ker(π) = I, por lo tanto "I es un ideal de A, si y solamente si, I es el núcleo de algún homomorfismo de anillos". Ahora probaremos el teorema fundamental de homomorfismos de anillos.

Teorema 2.5 (T.F.H.A) Si f: $A \to A'$ es un homomorfismo de anillos, entonces

$$\frac{A}{Ker(f)} \cong Im(f).$$

Prueba. Sabemos que la función $\tilde{f}$: $\frac{A}{Ker(f)} \to A'$ definida por $\tilde{f}(a+I)=f(a) \ \forall\, a \in A$ es un homomorfismo inyectivo de grupos (vea el T.F.H.G).
Ahora como

$$\begin{aligned}\tilde{f}\big((a+I)\odot(b+I)\big) &= \tilde{f}(ab+I)\\ &= f(ab)=f(a)f(b)\\ &= \tilde{f}(a+I)\tilde{f}(b+I) \qquad \forall\, a,b \in I\end{aligned}$$

se tiene que $\tilde{f}$: $\frac{A}{Ker(f)} \to Im(f)$ es un isomorfismo de anillos.
Los siguientes corolarios son consecuencias inmediatas de este teorema.

Corolario 2.1 Si S es un subanillo e I un ideal del anillo A entonces $S+I=\{s+i/s \in S, i \in I\}$ es un subanillo de A, $S \cap I$ es un ideal de A y

$$\frac{S+I}{I} \cong \frac{S}{S \cap I}$$

Corolario 2.2 Sean I, J ideales del anillo A tales que $I \subseteq J$ entonces J/I es un ideal de A/I y

$$\frac{A/I}{J/I} \cong A/J$$

Definición 2.8:
Sea A un anillo y M un ideal propio de A. Se dice que M es un ideal maximal de A si M no está contenido en ningún ideal propio de A. Es decir, si I es un ideal de A tal que $M \subseteq I \subseteq A$, entonces $I = M$ o $I = A$.
Por ejemplo, en el anillo Z, $\langle n \rangle$ es maximal si y solo si n es primo.

Proposición 2.6 Sea A un anillo y M un ideal propio de A, entonces M es maximal si y sólo si $\forall a \in A \setminus M, (M, a) = A$.
Nota:
Usando esta proposición es fácil ver que en el anillo conmutativo $2Z$ (sin elemento unidad), el conjunto $M = 4\ Z$ es un ideal propio de $2\ Z$; más aún M es un ideal maximal de este anillo.
Una relación "$\leq$. en un conjunto no vacío A es un orden parcial en A pues es reflexiva, simétrica y transitiva. En este caso el par $(A, \leq)$ es llamado conjunto parcialmente ordenado.
Sea $(A, \leq)$ un conjunto parcialmente ordenado.

1. Un subconjunto B de A es llamado **cadena** si $\forall\ x, y \in B : x \leq y$ ó $y \leq x$.
2. Una **cota superior** para un subconjunto B de A es un elemento $u \in A$ tal que $b \leq u, \forall\ b \in B$.
3. Un **elemento maximal** de A es un elemento $m \in A$ de modo que si $m \leq x$ para algún $x \in A$, entonces $m = x$.

Lema de Zorn. Si A es un conjunto parcialmente ordenado en el cual toda cadena tiene una cota superior, entonces A posee un elemento maximal.

Teorema 2.7 (Existencia de ideal maximal) Sea A un anillo finitamente generado. Si I es un ideal propio de A entonces existe M ideal propio de A tal que $I \subseteq M$ y
M es maximal.
Prueba. Supongamos que $A = \langle a_1, a_2, \dots, a_n \rangle$. Si

$$A = \{J / J \text{ es ideal propio de } A, I \subseteq J\},$$

entonces $A \neq \emptyset$ pues $I \in A$ y $(A, \subseteq)$ es parcialmente ordenado. Si $\{J_\lambda\}_{\lambda \in \Lambda}$ es una cadena en A, afirmamos que $\tilde{J} = \bigcup_{\lambda \in \Lambda} J\lambda$ es un ideal de A.
Además $\tilde{J}$ es un ideal propio de $A, I \subseteq \tilde{J}$ y $J_\lambda \subseteq \tilde{J}, \forall\ \lambda \in \Lambda$.
En efecto, si $\tilde{J} = A = \langle a_1, a_2, \dots, a_n \rangle$, entonces $a_1 \in J_{\lambda 1}$, $a_2 \in J_{\lambda 2}$, . . . , $a_n \in J_{\lambda n}$; luego existe $k, 1 \leq k \leq n$ tal que $a_1, a_2, \dots, a_n \in J_{\lambda k}$ ($\{J_\lambda\}_{\lambda \in \Lambda}$ es cadena), de donde $A = \langle a_1, a_2, \dots, a_n \rangle \subseteq J_{\lambda_k} \subseteq A$ y por tanto $J_{\lambda_k} = A$, lo cual es imposible. Por lo tanto $\tilde{J} \in A$ y es una cota superior de la cadena $\{J_\lambda\}_{\lambda \in \Lambda}$. luego por el Lema de Zorn, existe M ideal propio de $A, I \subseteq M$ y M es elemento maximal de $(A, \subseteq)$. Afirmamos que M es un ideal maximal de A; en efecto: Sea J un ideal de A con $M \subseteq J \subsetneq A$; luego $J \subsetneq A\ y\ I \subseteq J$, es decir $J \in A$ y $M \subseteq J$, de donde $J = M$.

Corolario 2.3 (Teorema de Krull**)** Si A es un anillo con elemento unidad 1, e I un ideal propio de A, entonces existe un ideal maximal M en A tal que $I \subseteq M$.

Teorema 2.8 Sea A un anillo conmutativo con elemento unidad y M un ideal propio de A, entonces M es maximal si y sólo si A/M es un cuerpo. Herstein(1988).

Definición 2.9:
Sea A un anillo y P un ideal propio de A. P es un ideal primo de A si para todo $a, b \in A$ tal que $ab \in P$ se tiene que $a \in P$ o $b \in P$.
Por ejemplo, en el anillo Z, $\langle p \rangle$ es primo si y solo si p es un número primo.
De otro lado el conjunto $A = Z \times Z$ con las operaciones

$$(a, b) + (x, y) = (a + x, b + y), \qquad (a, b) \cdot (x, y) = (ax, by)$$

es un anillo conmutativo con unidad igual a (1, 1) y tiene divisores de cero.
pues $(n, 0) \cdot (0, m) = (0, 0)$. Si definimos $I = \{(n, 0): n \in Z\}$ es fácil ver que I es un ideal de A.
I es un ideal primo, puesto que si $(a, b) \cdot (x, y) \in I$, entonces $(ax, by) = (n, 0)$, de donde $by = 0$, por lo tanto $b = 0$ o $y = 0$. Así $(a, b) = (a, 0) \in I$ o bien
$(x, y) = (x, 0) \in I$.
I no es un ideal maximal, ya que definiendo $J = \{(n, 2m): n, m \in Z\}$ tenemos que J es un ideal de A y que $I \subsetneq J \subsetneq A$.

Teorema 2.9 Sea A un anillo conmutativo con elemento unidad y P un ideal propio de A, entonces P es un ideal primo si y sólo si A/P es un dominio de integridad. Herstein(1988).

Corolario Sea A un anillo conmutativo con elemento unidad y M un ideal propio de A. Si M es maximal, entonces M es primo.
Nota: El recíproco de este corolario en general es falso.
Más aún el corolario no es cierto si el anillo no tiene elemento unidad, por ejemplo si $A = 2Z$ y $M = 4Z$, sabemos que M es maximal sin embargo no es un ideal primo,
ya que: $2 \in A$ y $2 \cdot 2 = 4 \in M$, pero $2 \notin M$.

Teorema 2.10 Sea A un dominio de ideales principales y sea $\{0\} \subsetneq I \subsetneq A$ un ideal de A, entonces I es maximal si y sólo si I es primo.

Prueba. Sólo falta ver que si $I = \langle a \rangle$ es primo, entonces I es maximal. En efecto: sea $J = \langle b \rangle$ un ideal de A tal que $\langle a \rangle \subseteq \langle b \rangle \subseteq A$, entonces existe $r \in A$ tal que $rb = a \in I$; y por ser I un ideal primo, $r \in I$ ó $b \in I$. Si $r \in I$, existe $s \in A$ tal que $r = sa$, luego $(sa)b = a$, de donde $1 = sb$ con $b \in J$; por lo tanto $1 \in J$ y $J = A$. Si $b \in I$, entonces $J = \langle b \rangle \subseteq I$, así $J = I$, es decir I es maximal.
Es importante recalcar que este teorema nos da una condición necesaria y suficiente para que se cumpla el recíproco del corolario.

DIVISIBILIDAD EN DOMINIOS
En toda esta sección D será un dominio de integridad.
Definición 2.11: Sean $a, b \in D$. Se dice que $a \neq 0$ divide a b, lo cual denotaremos por $a|b$ si existe $c \in D$ tal que $b = ac$. Se dice que a y b son asociados, lo cual denotaremos por $a \sim b$, si existe $u \in U(D)$ tal que $a = bu$. La relacion " $\sim$. es de equivalencia en D.

Definición 2.12: Máximo común divisor.
Sean $a, b, d \in D\backslash\{0\}$. Se dice que $d = mcd(a, b)$ es el máximo común divisor de a y b si

i) $d|a$ y $d|b$,
ii) si $d'|a$ y $d'|b$, entonces $d'|d$.

En un dominio de integridad el mcd es único salvo asociados, ya que si d_1 satisface las condiciones (i) y (ii) entonces $d|a$, $d|b$, $d_1|a$, $d_1|b$ (condición (i)), lo cual implica que $d_1|d$ y $d|d_1$ (condición (ii) sobre d y d_1), de donde $d_1 \sim d$.

Proposición 2.11 Sean $a, b \in D\backslash\{0\}$. Entonces existe $d = mcd(a, b)$ y existen $r, s \in D$ tales que $d = ra + sb$, si y sólo si, $\langle a, b\rangle$ es principal.

Prueba. Supongamos que existe $d = mcd\{a, b\rangle = ra + sb$. Veamos que $\langle a, b\rangle \subseteq \langle d\rangle$: Si $x \in \langle a, b\rangle$, entonces $x = ha + wb$ con $h, w \in D$. Como $d = mcd(a, b)$ se tiene que $d|a$ y $d|b$, luego $d|x$, y esto implica que $x \in \langle d\rangle$. Además, si $x \in \langle d\rangle, x = dt$ para algún $t \in D$, luego $x = rta + stb \in \langle a, b\rangle$. Por lo tanto $\langle a, b\rangle = \langle d\rangle$ es principal.

Recíprocamente, supongamos que $\langle a, b\rangle$ es principal, esto es, $\langle a, b\rangle = \langle d\rangle$ con $d \in D$. Luego existen $r, s \in D$ tales que

$$d = ra + sb. \qquad (2)$$

Por otro lado, como $a \in \langle a, b\rangle = \langle d\rangle$ implica que $a \in \langle d\rangle$ y $d|a$. Análogamente $d|b$. Ahora si $d'|a$ y $d'|b$, por (2), $d'|d$.

Sea $p \in D \setminus \{0\}, p \notin U(D)$.

i) p se llama elemento primo (en D) si dados $a, b \in D$ tales que $p|ab$, se tiene que $p|a$ ó $p|b$.
ii) p de llama elemento irreducible (en D) si dados $a, b \in D$ tales que $p = ab$, se tiene que $a \in U(D)$ o $b \in U(D)$.

Proposición 2.12 Sea $p \in D \setminus \{0\}, p \notin U(D)$. Si p es un elemento primo, entonces p es un elemento irreducible en D.

Prueba. Supongamos que $p = ab$ con $a, b \in D$, entonces $p|ab$, y como p es primo $p|a$ ó $p|b$. Si $p|a$ existe $r \in D$ tal que $a = pr$, de donde $p = (pr)b$ o $rb = 1$ por lo tanto $b \in U(D)$. Si $p|b$ existe $s \in D$ tal que $b = ps$, luego $p = a(ps)$ o $as = 1$ por lo tanto $a \in U(D)$.

Definición 2.13:
Sean $n \in Z$ libre de cuadrados (esto es, no existe $p \in Z^+$ primo tal que $p^2|n$),
$\alpha \in Z[\sqrt{n}] = \{a + b\sqrt{n} : a, b \in Z\}$ y $N : Z[\sqrt{n}] \to R$ definida por
$N(a + b\sqrt{n}) = a^2 - nb^2$. Entonces:

1. $N(\alpha) = \pm 1$, si y sólo si, $\alpha \in U(Z[\sqrt{n}])$.
2. Si $N(\alpha) = \pm p$ con $p \in Z^+$ primo, entonces α es un elemento irreducible en $Z[\sqrt{n}]$.

En efecto**:** Observe que si $\alpha = a + b\sqrt{n}$ y $\alpha = a - b\sqrt{n}$, entonces $N(\alpha) = \alpha\underline{\alpha}$ y $N(\alpha\beta) = \alpha\beta\underline{\alpha\beta} = \alpha\underline{\alpha}\beta\underline{\beta} = N(\alpha)N(\beta)$.

1. Si $N(\alpha) = \pm 1$, esto es $\alpha\underline{\alpha} = \pm 1$, entonces $\alpha \in U(D)$. Recíprocamente, si $\alpha \in U(Z[\sqrt{n}])$, existe $\beta \in Z[\sqrt{n}]$ tal que $\alpha\beta = 1$, luego
$$1 = N(1) = N(\alpha\,\beta) = N(\alpha)N(\beta)$$
y como esta última relación está en Z, implica que $N(\alpha) = \pm 1$.

2. Si $N(\alpha) = \pm p \in Z$ es primo $(\therefore \alpha \neq 0\ y\ \alpha \notin U(Z[\sqrt{n}]))$ y supongamos que $\alpha = \beta\gamma$ con $\beta, \gamma \in Z[\sqrt{n}]$, entonces $\pm p = N(\alpha) = N(\beta)N(\gamma)$ en Z, lo que implica que $N(\beta) = \pm 1$ ó $N(\gamma) = \pm 1$, y así $\beta \in U(D)$ ó $\gamma \in U(D)$.

Definición 2.14:
Un dominio de integridad D se denomina dominio euclidiano si existe una función $\varphi: D \setminus \{0\} \to Z_{\geq 0}$ tales que:

i)Para todo $a, b \in D$ con $b \neq 0$, existen $q, r \in D$ tales que
$$a = bq + r \text{ con } r = 0 \text{ ó } \varphi(r) < \varphi(b).$$
ii)Para todo $a, b \in D \setminus \{0\}$ $\varphi(a) \leq \varphi(ab)$.

La función φ se denomina evaluación euclidiana. Si D es un dominio euclidiano con valuación φ lo denotaremos por (D, φ) y diremos que (D, φ) es un D.E.

Proposición 2.13 Sea (D, φ) un D.E. y sean $a, b \in D \setminus \{0\}$, entonces $b \in U(D)$ si y sólo si $\varphi(a) = \varphi(ab)$.

Prueba. Siempre se tiene que $\varphi(a) \leq \varphi(ab)$, y como $b \in U(D)$, existe $b^{-1} \in D$, luego $\varphi(ab) \leq \varphi((ab)b^{-1}) = \varphi(a)$. Recíprocamente, si $\varphi(a) = \varphi(ab)$, existen $q, r \in D$ tales que
$$a = (ab)q + r\ con\ \ r = 0\ \ \text{ó}\ \ \varphi(r) < \varphi(ab) = \varphi(a).$$

Si $r \neq 0$, entonces $\varphi(r) = \varphi(a(1 - bq)) \geq \varphi(a)$, lo cual es absurdo. Por lo tanto $r = 0$, y así $a = abq$, lo cual implica que $b \in U(D)$.

Lema Si $a = bq + r$, entonces $mcd(a, b) = mcd(b, r)$.

Una de las propiedades más importantes de un dominio euclidiano es que mcd de dos elementos del dominio euclidiano siempre existe, y se puede calcular algoritmo de Euclides, esto es.

Proposición 2.14: (Algoritmo de Euclides)
Sea (D, φ) un D.E. y sean $a, b \in D \setminus \{0\}$. Si $r_0 = a$, $r_1 = b$, aplicando sucesivamente (i) obtenemos $r_2, r_3, \ldots, r_n, r_{n+1}$ definidos por las relaciones:

$$\begin{array}{lll} r_0 = r_1 q_1 + r_2 & \text{con} & r_2 \neq 0\ y\ \varphi(r_2) < \varphi(r_1), \\ r_1 = r_2 q_2 + r_3 & \text{con} & r_3 \neq 0\ y\ \varphi(r_3) < \varphi(r_2) \end{array}$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \quad \text{con} \quad r_n \neq 0 \; y \; \varphi(r_n) < \varphi(r_{n-1}),$$
$$r_{n-1} = r_n q_n + r_{n+1} \quad \text{y} \quad r_{n+1} = 0.$$

Entonces r_n, el último resto no nulo de este proceso es el $mcd(a, b)$.
Un ejemplo bastante conocido de D.E. es el anillo de enteros Z junto con el valor absoluto $|\cdot| : Z \to Z_{\geq 0}$. Otros ejemplos se derivan del siguiente teorema, cuya demostración puede verse en Dummit and Foote (2004).

Teorema 2.15 El dominio de integridad $Z[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in Z\}$ con $\varphi(a + b\sqrt{d}) = |a^2 - db^2|$ es un dominio euclidiano si $d = -2, 1, 2 \; y \; 3$.

Teorema 2.16 Si (D, φ) es un dominio euclidiano, entonces D es un dominio de ideales principales.
Prueba. Sea $I \neq \{0\}$ un ideal de D. Como $\varphi(I \setminus \{0\}) \subseteq Z_{\geq 0}$, por el Principio del Buen Orden, existe $b \in I, b \neq 0$ tal que $\varphi(b) = mín\, \varphi(I \setminus \{0\})$. Afirmamos que $I = \langle b \rangle$. Solo falta ver que $I \subseteq \langle b \rangle$. En efecto: si $a \in I$, siendo $b \neq 0$, existen $q, r \in D$ tales que

$$a = bq + r \; con \; r = 0 \text{ ó } \varphi(r) < \varphi(b).$$

Siendo I un ideal $r = (a - bq) \in I$ (pues $a, b \in I$), luego $r = 0$ ($r \neq 0$ contradice la minimalidad de $\varphi(b)$) de donde $a = bq \in \langle b \rangle$.

Lema Sea D un dominio de ideales principales y sea $p \in D$ no nulo ni unidad, entonces p es primo si y solo si p es irreducible.
Prueba. Sólo falta ver que p es primo, si p es irreducible. En efecto: si $p|ab$, entonces $ab = pc$ con $c \in D$. Como D es un D.I.P , existe $d \in D$ tal que $\langle p, a \rangle = \langle d \rangle$, entonces $p \in \langle d \rangle$, de donde $p = dr$ con $r \in D$, y como p es irreducible $d \in U(D)$ o $r \in U(D)$. Si $d \in U(D)$, entonces $\langle p, a \rangle = D$, luego el $mcd(p, a) = 1$ y $p|ab$, lo que implica que $p|b$. Si $r \in U(D)$, $p \sim d$. Luego $a \in \langle p \rangle = \langle p, a \rangle$, así $p|a$.

Teorema 2.17 Sea D un D.I.P y sea $\{In\}_{n \in Z^+}$ una familia de ideales del dominio D. Si

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots,$$

es fácil ver que $I = \bigcup_{n \in Z^+} I_n$ es un ideal de D. Como D es un D.I.P , existe $a \in D$ tal que $I = \langle a \rangle$, luego existe $n_0 \in Z^+$ tal que $a \in I_{n0}$, así

$$I = \langle a \rangle \subseteq I_{n0} \subseteq I_n \subseteq I,$$

para todo $n \geq n_0$. Por lo tanto $I_n = I_{n0}$, para todo $n \geq n_0$.
Si D es un dominio de ideales principales, hemos probado que toda sucesión ascendente de ideales es estacionaria; un anillo con esta propiedad es llamado Anillo Noetheriano. Atiyah and Macdonald(1989).

Definición 2.15:
Un dominio de integridad D es llamado dominio de factorización única (D.F.U) si
i) cada $a \in D \setminus \{0\}, a \notin U(D)$ puede ser factorizado como un producto finito de elementos irreducibles;
ii) si $a = p_1 \ldots p_n = q_1 \ldots q_m$ son dos factorizaciones de a como en (i), entonces $n = m$ y existe $\sigma \in S_n$ tal que $q_i \sim p_{\sigma(i)}$, para todo $i = 1, 2, \ldots, n$.

Teorema 2.18 Si D es un D.I.P y $a \in D \setminus \{0\}, a \notin U(D)$ entonces a puede ser factorizado como un producto finito de elementos irreducibles.
En efecto: Como $a \in D \setminus \{0\}$ y $a \notin U(D)$, existe p_1 primo tal que $p_1|a$, luego $a = p_1 a_1$ con $a_1 \in D$, de donde $\langle a \rangle \subsetneq \langle a_1 \rangle \subseteq D$. Si $\langle a_1 \rangle = D$, entonces $a = a_1 p_1$ con $a_1 \in U(D)$. Si $\langle a_1 \rangle \subsetneq D$, entonces $a_1 \in D \setminus \{0\}, a \notin U(D)$, luego existe p_2 primo tal que $p_2|a_1$, esto es $a_1 = a_2 p_2$ con $a_2 \in D$ y por lo tanto

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subseteq D.$$

Repitiendo este proceso tenemos

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots \text{ con } a_{k-1} = a_k p_k \text{ y } p_k \text{ primo.}$$

Luego siendo D un D.I.P existe $n \in Z^+$ tal que

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \ldots \subsetneq \langle a_{n-1} \rangle \subsetneq \langle a_n \rangle = D = \langle 1 \rangle$$

Por lo tanto $a = p_1 p_2 \ldots p_{n-1} p_n a_n$ con $a_n \in U(D)$.

Teorema 2.19 Todo D.I.P es un D.F.U
Prueba. Sea D un D.I.P y sea $a \in D \setminus \{0\}, a \notin U(D)$. Por la proposición anterior, a puede ser factorizado como un producto finito de elementos irreducibles. Sólo falta verificar la unicidad de dicha descomposición salvo elementos asociados. Supongamos que

$$a = p_1 \ldots p_n = q_1 \ldots q_m \; con \; n \leq m.$$

Ahora como $p_1|q_1 q_2 \ldots q_m$, entonces $p_1|q_i$ para algún i. Sin pérdida de generalidad, podemos suponer que $p_1|q_1$. Siendo p_1 y q_1 irreducibles $q_1 = p_1 u_1$ con $u_1 \in U(D)$ ($p_1 \sim q_1$), de donde

$$p_2 p_3 \ldots p_n = u_1 q_2 q_3 \ldots q_m.$$

Continuando con este proceso tenemos

$$1 = u_1 \ldots u_n q_{n+1} \ldots q_m$$

donde $q_i = p_i u_i$ con $u_i \in U(D)$, para $i = 1, 2, \ldots, n$ ($p_i \sim q_i$). Como $q_i \in \notin U/(D)$ $n = m$. En general, existe $\sigma \in S_n$ tal que $q_i \sim p_{\sigma i}$ para $i = 1, 2, \ldots, n$.
Sobre un D.F.U también se cumple que elemento primo es equivalente a elemento irreducible (Burton, 1970).

EL ANILLO DE POLINOMIOS EN UNA VARIABLE

Definición 2.16:
Sea A un anillo y $S(A)$ el conjunto de todas las sucesiones en A. Si $f \in S(A)$ y para cada $i \in N$ denotamos $a_i = f(i)$, entonces $f = (a_0, a_1, a_2, \ldots)$. Dada las sucesiones $f = (a_0, a_1, \ldots)$ y $g = (b_0, b_1, \ldots)$ en $S(A)$, definimos:

i) $f + g = (a_0 + b_0, a_1 + b_1, \ldots$

ii) $f \cdot g = (a_0 b_0, a_0 b_1 + a_1 b_0, \ldots, c_n, \ldots) \; donde \; c_n = \sum_{k=0}^{n} a_k b_{n-k}.$

Con estas operaciones es fácil ver que $S(A)$ es un anillo, llamado el anillo de series formales de potencias sobre A. En particular si A es un anillo con elemento unidad 1 y $x := (0, 1, 0, \dots)$, entonces

$$x = (0, 1, 0, \dots)$$

$$x_2 = (0, 1, 0, \dots)(0, 1, 0, 0, \dots) = (0, 0, 1, 0, \dots)$$

$$x_3 = (0, 1, 0, \dots)(0, 0, 1, 0, \dots) = (0, 0, 0, 1, \dots)$$

$$\vdots$$

$$x_n = (0, 0, \dots, \underbrace{0}_{n\ ceros}, 1, 0, \dots)$$

Ahora, para $a \in A$

$$ax^n = (a, 0, 0, \dots)(0, 0, \dots \underbrace{0}_{n\ ceros}, 1, 0, \dots) = (0, 0, \dots \underbrace{0}_{n\ ceros}, a, 0, \dots).$$

Luego, denotando $x^0 = 1$ y $x^1 = x$, el elemento $f = (a_0, a_1, a_2, a_3, \dots)$ de $S(A)$ puede ser escrito en la forma

$$f = (a_0, \dots) + (0, a_1, \dots) + (0, 0, a_2, \dots) + (0, 0, 0, a_3, \dots) + \cdots = \sum_{k=0}^{\infty} a_k x^k$$

Por esta razón, de ahora en adelante, el anillo de series formales de potencias sobre A será denotada por $A[\![x]\!]$, es decir

$$A[\![x]\!] = \left\{ f = \sum_{k=0}^{\infty} a_k x^k : a_k \in A, \forall\, k \geq 0 \right\}$$

Nota:
Sea A un anillo con unidad, la serie formal del anillo $A[[x]]$
se llama polinomio sobre A con indeterminado x, si existe un entero no negativo n tal que $a_k = 0, \forall\, k > n$, es decir

$$f\ es\ un\ polinomio\ sobre\ A \Leftrightarrow f = \sum_{k=0}^{\infty} a_k x^k;\ con\ a_k \in A\ \forall k$$

Notaciones:
Si $A[x]$ denota el conjunto de todos los polinomios sobre el anillo A, es fácil ver que $A[x]$ es un subanillo de $A[[x]]$.
En particular, si A es un anillo conmutativo con unidad, entonces $A[x]$ también es un anillo conmutativo con unidad. Si $f = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio sobre A. El término $a_n \neq 0$ se llama coeficiente principal de f y n se llama el grado del polinomio f. Si este coeficiente principal $a_n = 1$, el polinomio se llama mónico.
Para $f, g \in A[x] \backslash \{0\}$, se cumplen las siguientes propiedades:

- $fg = 0\ o\ gr(fg) \leq gr(f) + gr(g)$.
- La igualdad en $i)$ se da, si A es un dominio de integridad.

- $f+g=0$ *o* $gr(f+g)\leq max\{gr(f),gr(g)\}$

como se ilustra en los ejemplos a continuación se da sobre el anillo $Z_6[x]$

1. Si $f=2x$ y $g=3x$, entonces $fg=0$.
2. Si $f=2x+1$ y $g=3x^2$, entonces $fg=3x^2$, así $2=gr(fg)<gr(f)+gr(g)=3$.
3. Si $f=2x$ y $g=4x$, entonces $f+g=0$.
4. Si $f=2x+1$ y $g=-2x$, entonces $f+g=1$. Por lo tanto $0=gr(f+g)<máx\{gr(f),gr(g)\}=1$.

Si A es un dominio de integridad, entonces $A[x]$ también es un dominio de integridad.
En efecto: Sean $f\neq 0$ y $g\neq 0$ en $A[x]$. Si $gr(f)=n$ y $gr(g)=m$ se tiene que $gr(fg)=n+m$, y por tanto $c_{n+m}\neq 0$ el coeficiente de lugar $(m+n+1)$ del producto fg. Por lo tanto $fg\neq 0$.
Si A es un dominio de integridad, entonces $U(A[x])=U(A)$.
En efecto: Si $f\in U(A[x])$, entonces existe $g\in A[x]$ tal que $fg=1$. Si $f=a_0+a_1x+\cdots+a_nx^n$ y $g=b_0+b_1x+\cdots+b_nx^n$ implica que $a_0b_0=1$, así $a_0\in U(A)$. Por otro lado como $0=gr(fg)=gr(f)+gr(g)\geq gr(f)\geq 0$ se tiene que $gr(f)=0$, así $f=a_0\in U(A)$.

Si $f\in A[x]$ y A' una extensión de A. Un elemento r del anillo A' se llama raíz del polinomio f, si $f(r)=0$. Veamos algunos ejemplos:

1. $f=x^2+x\in Z_6[x]$ posee 4 raíces (en Z_6), pues $f=x(x+1)$ y $f(0)=0$, $f(2)=0, f(3)=0, f(5)=0$.
2. $f=(a,0)x^2\in(Z\times\{0\})[x]$, con $a\neq 0$, posee infinitas raíces en $Z\times Z$, pues $f(0,b)=(a,0)(0,b)^2=(0,0),\forall\, b\in Z$.
3. $f(x)=x^2+x+1\in Z_2[x]$ no tiene raíces en Z_2, pues $f(0)=1, f(1)=1$ y $1\neq 0$.

$f:A\to A$ es una función polinomial si existen $a_0,a_1,\ldots,a_n\in A$ tal que
$$f(r)=a_0+a_1r+\cdots+a_nr^n\,,\forall r\in A.$$

A estas alturas debemos hacer notar la diferencia entre un polinomio y una función polinomial, por ejemplo:

1. $f=3x+5x^2=(0,3,5,0,\ldots)$ es un polinomio de grado 2 sobre R y $f:R\to R$ tal que $f(r)=3r+5r^2\,,\forall\, r\in R$ es una función polinomial sobre R.
2. $f=x^p-x=(0,-1,0,\ldots\ 0,1\underset{\smile}{}_{p+1},0,\ldots)$ es un polinomio (no nulo) de grado p sobre Z_p *y* $f:Z_p\to Z_p$ tal que $f(x)=0,\forall\, x\in Z_p$, es una función polinomial nula sobre Z_p.
3. $f=x^2+x=(0,1,1,0\ldots)\in Z_2[x]$ también es una función polinomial no nula y como $f(x)=x(x+1), f:Z_2\to Z_2$ es la función polinomial nula.

Teorema 2.20 (Algoritmo de la división en el anillo de polinomios)
Sea A un anillo conmutativo con unidad, $f=a_0+a_1x+\cdots+a_nx^n$ y $g=b_0+b_1x+\cdots b_mx^m\in A[x]$. Si $b_m\in U(A)$, existen únicos q y r en $A[x]$ tales que

$$f = gq + r \text{ con } r = 0 \text{ o } gr(r) < gr(g).$$

Prueba. Si $f = 0$ ó $gr(f) < gr(g)$ tomamos $q = 0$ y $r = f$.
Supongamos que $n = gr(f) \geq gr(g) = m$. Si $f_1 = f - x^{n-m}a_n b_m^{-1} g$ entonces $f_1 \in A[x]$ y $f = a_n b_m^{-1} x^{n-m} g + f_1$ con $gr(f_1) < gr(f) = n$.

Si $f_1 = 0$ ó $gr(f_1) < gr(g)$, entonces $q = a_n b_m^{-1} x^{n-m}$ y $r = f_1$. Supongamos que $p = gr(f_1) \geq gr(g) = m$, digamos $f_1 = c_0 + c_1 x + \cdots + c_p x^p$, con $c_p \neq 0$. Si $f_2 = f_1 - x^{p-m}\, c_p b_m^{-1} g$ entonces $f_2 \in A[x]$ y $f_1 = c_p b_m^{-1} x^{p-m} g + f_2$, así

$$f = (a_n x^{n-m} + c_p x^{p-m}) b_m^{-1} g + f_2, \text{ donde } gr(f_2) < gr(f_1) < gr(f) = n.$$

Si $f_2 = 0$ ó $gr(f_2) < gr(g)$, tomamos $q = (a_n x^{n-m} + c_p x^{p-m}) b_m^{-1}$ y $r = f_2$. En caso contrario repetimos el proceso un número finito de veces y obtenemos los polinomios q y f_1 en $A[x]$ tales que $f = qg + f_i$, donde $f_i = 0$ ó $gr(f_i) < gr(g)$; luego tomamos $r = f_i$ tenemos que $f = gq + r$, con $r = o$ ó $gr(r) < gr(g)$. Esto completa la prueba de la existencia. Ahora veamos la prueba de la unicidad. Supongamos que $f = gq + r = gq' + r'$, con $r = 0$ ó $gr(r) < gr(g)$ y $r' = 0$ ó $gr(r\,0) < gr(g)$. Entonces

$$r - r' = (q' - q)g.$$

$$Si\ q - q' = \sum_{k=0}^{l} d_k x^k \neq 0, gr(r - r') = gr((q' - q)g) = gr(q' - q) + gr(g),$$

luego $gr(r - r') \geq\geq gr(g)$. Por otro lado $gr(r - r') \leq max\{gr(r), gr(r')\} < gr(g)$; así $q = q'$ y $r = r'$.
En particular si K es un cuerpo, $K[x]$ es un dominio euclidiano. lo que se logra considerando $gr: K[x]\backslash\{0\} \to Z_{\geq 0}$ que satisface:

(i) Si $f, g \in K[x]$ y $g \neq 0$, entonces $\exists\, q, r \in K[x]$ tal que $f = gq + r$, con $r = 0$ ó $gr(r) < gr(g)$.
(ii) $gr(fg) = gr(f) + gr(g) \geq gr(f)$.

En los siguientes ejemplos se relaciona el polinomio con sus raíces

1. Sea $f = x^2 - 1 \in Z_{15[x]}$; sus raíces son 1, −1, 4 y −4 en Z_{15}, así $f = (x - 1)(x + 1) = (x - 4)(x + 4)$.
2. Sea $f = (a, 0)x^2 \in (Z \times Z)[x]$. Notemos que sus raíces son de la forma $(0, b)\ \forall\ b \in Z$, así f tiene infinitas raíces y $f = [x - (0, b)](a, 0)x$.
3. Sea $f = x^2 + x \in Z_6[x]$. Sus raíces son 0, 2, 3 y 5 en Z_6, así $f = x(x - 5) = (x - 2)(x - 3)$.

Teorema 2.21 Si A es un dominio de integridad y $f \in A[x]$ es tal que $gr(f) = n > 0$, entonces f tiene a lo más n raíces en A.
Trabajando con un polinomio particular se logra un resultado de la teoría de números: Si p es primo, entonces Z_p es un cuerpo. Como $x^p = x\ \forall\ x \in Z_p$, se tiene que $x^p - x = x(x - 1)(x - 2)\ ...\ [x - (p - 1)]$ en Z_p (si p es primo impar), o bien $x^{p-1} - 1 =$

$(x-1)(x-2)\ldots[x-(p-1)]$ en Z_p. Luego, para $x=0$, se tiene $-1=(-1)(-2)\ldots[-(p-1)]$, entonces $(p-1)!=-1$ en Z_p, es decir

$$(p-1)!\equiv -1(mod\ p)$$

resultado conocido como el teorema de Wilson. Apóstol (1984).

Teorema 2.22 (De Gauss) Si D es un dominio de factorización única, entonces $D[x]$ también es un dominio de factorización única. Herstein (1988)

Algunos criterios de irreducibilidad

Teorema 2.23 (Criterio de Eisenstein) Sea D un dominio de factorización única y $f=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$ con $a_n\neq 0$. Si existe $p\in D$ irreducible tales que:

i) $p|a_0, p|a_1, \ldots, p|a_{n-1}$

ii) $p\nmid a_n$ y $p^2\nmid a_0$

entonces el polinomio f no es el producto de dos factores de grado ≥ 1 en $D[x]$. Equivalentemente, f es irreducible en $K[x]$ donde $K=C_f(D)$.

Prueba. Supongamos que existen

$$g=b_0+b_1x+\cdots+b_rx^r\ y\ h=c_0+c_1x+\cdots+c_sx^s\ en\ D[x]$$

con $b_r\neq 0$, $c_s\neq 0$; $1\leq r,s<n$ tal que $f=gh$.
Como $a_0=b_0c_0, p|a_0$ y $p^2\nmid a_0$, implica que: o bien $p|b_0$ y $p\nmid c_0$, ó $p|c_0$ y $p\nmid b_0$.
En el caso que $p|b_0$ y $p\nmid c_0$, puesto que $p\nmid a_n$ y $a_n=b_rc_s$, implica que $p\nmid b_r$ ni $p\nmid c_s$, luego si elegimos $l=min\{i: p\nmid b_i\}\leq r$ vemos que $1\leq l\leq r<n$.
Por lo tanto

$$p|b_0, p|b_1, \ldots, p|b_{l-1}, p\nmid b_l, \ldots \text{ no se sabe } \ldots, p\nmid b_r.$$

Y como $a_l=b_0c_l+b_1c_{l-1}+\cdots+b_{l-1}c_1+b_lc_0$, concluimos que $p|b_lc_0$, así $p|b_l$ o $p|c_0$, una contradicción.
Análogamente en el caso que $p|c_0$ y $p\nmid b_0$, se llega a una contradicción.

Veamos algunos ejemplos

1. Si $p\in Z$ es primo, el polinomio $f=x^n-p\in Q[x]$ es irreducible. Por lo tanto, en $Q[x]$ existen polinomios irreducibles de cualquier grado. Más aún, si $a\in Z\setminus\{\pm 1,0\}$ es libre de cuadrados, entonces $f=x^n+a\in Z[x]$ es irreducible en $Z[x]$.
2. El polinomio $f=\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}$ es irreducible en $Q[x]$], pues
$$f=\frac{1}{9}(2x^5+15x^4+9x^3+3), \frac{1}{9}\in U(Q[x])=Q^*\ \ y\ \ p=3.$$
3. El polinomio $f=10x^{11}+6x^3+6$ es irreducible en $Q[x]$, pero no es irreducible en $Z[x]$, puesto que $f=2(5x^{11}+3x^3+3)$ con $2\in U(Q[x])$, pero 2 es un polinomio irreducible en $Z[x]$.

Si $p\in R[x]$ es irreducible, entonces $gr(p)=1$ o $gr(p)=2$.
En efecto: Si $gr(p)=1$, p es irreducible. Si $gr(p)=2, p=ax^2+bx+c$ es irreducible, si y sólo sí, $\Delta=b^2-4ac<0$. Si $gr(p)\geq 3$, por el teorema fundamental del álgebra, existe $r\in C$ raíz de p.

- Si $r \in R$, entonces $p = (x - r)q$ con $q \in R[x]$, así el polinomio p no es irreducible en $R[x]$.
- Si $r = a + bi \notin R, \underline{r} = a - bi$ también es raíz de p, así $p = (x^2 - 2ax + a^2 + b^2)q(x)$ con $q \in R[x]$ de grado ≥ 1, así el polinomio p no es irreducible en $R[x]$.

Por lo tanto, $gr(p) = 1$ ó $gr(p) = 2$.
Los únicos polinomios irreducibles en $C[x]$ son los polinomios de grado uno. Este es un enunciado equivalente del famoso teorema fundamental del álgebra, que a la letra dice *"Todo $p \in C[x]$ no constante, tiene al menos una raíz en C"*. Por lo tanto, si $p \in C[x]$ tiene grado n, existen $\alpha, \alpha_1, \alpha_2, \ldots \alpha_n \in C$ tal que

$$p = \alpha(x - \alpha_1) \ldots (x - \alpha_n).$$

Por ejemplo, el polinomio $f = x^5 + 2x^3 + (1 + i)$ es irreducible en $Z[i][x]$, pues tomando $p = 1 + i$, que es irreducible en $Z[i]$, vemos que:

$$p|(1 + i), p|2, p \nmid 1 \ \ y \ p^2 \nmid (1 + i)$$

Si $p^2|1 + i, 1 + i = (1 + i)^2\alpha$ algún $\alpha \in Z[i]$, así $1 = (1 + i)\alpha$, es decir $1 + i \in U(Z[i]) = \{\pm 1, \pm i\}$ (¡Absurdo!).

Proposición 2.24 Sea K un cuerpo y $f \in K[x]$ de grado 2 o grado 3, entonces
f es irreducible en $K[x] \Leftrightarrow f$ no tiene raíz en K.

Prueba. Probaremos que, f es reducible en $K[x] \Leftrightarrow \exists\, \alpha \in K : f(\alpha) = 0$. En efecto, si $f = gh$ con $g, h \in K[x]$ tal que $gr(g) \geq 1$ y $gr(h) \geq 1$. Como $gr(f) = gr(g) + gr(h)$ y $gr(f) = 2$ ó 3, implica que $gr(g) = 1$ ó $gr(h) = 1$. noindent Si $gr(g) = 1$, entonces $g = ax + b$ con $a, b \in K$ y $a \neq 0$, entonces existe $-\frac{b}{a} \in K$ tal que $f\left(-\frac{b}{a}\right) = 0$. Si $gr(h) = 1$, entonces $g = cx + d$ con $c, d \in K$ y $c \neq 0$, entonces existe $-\frac{d}{c} \in K$ tal que $f\left(-\frac{d}{c}\right) = 0$. Así, en cualquier caso, existe $\alpha \in K$ tal que $f(\alpha) = 0$. Recíprocamente, si existe $\alpha \in K$ tal que $f(\alpha) = 0$, por el teorema del factor, $f(x) = (x - \alpha)g(x)$ con $g(x) \in K[x]$ de grado 1 ó 2. Así, f es reducible en $K[x]$.

Por ejemplo, sobre Z_2 los polinomios de grado 1 son siempre irreducibles, en este caso son x y $x + 1$; y los polinomios sin raíces en $Z_2[x]$ de grado 2 o grado 3 son: $x^2 + x + 1$, $x^3 + x + 1$ y $x^3 + x^2 + 1$. Por lo tanto

$$x, x + 1, x^2 + x + 1, x^3 + x + 1 \ \ y \ \ x^3 + x^2 + 1$$

son todos los polinomios irreducibles de grado menor o igual a tres en $Z_2[x]$

Proposición 2.25 (Criterio de reducción módulo un primo)
Sea $f = a_0 + a_1x + \cdots + a_nx^n \in Z[x]$ con $a_n \neq 0$. Si existe $p \in Z$ primo tal que $p \nmid a_n$ y $\underline{f} = \underline{a_0} + \underline{a_1}x + \cdots + \underline{a_n}x^n$ es irreducible en $Z_p[x]$, entonces f es irreducible en $Q[x]$.

Prueba. Supongamos que $f = gh$ con $g, h \in Z[x]$ y $\underline{f} = \underline{gh}$. Por la hipótesis, $gr(\underline{g}) = 0$ ó $gr(\underline{h}) = 0$, entonces $\underline{g} = \underline{a} \in U(Z_p[x])$ o $\underline{h} = \underline{b} \in U(Z_p[x])$.
Si $\underline{g} = \underline{a} \in Z_p \backslash \{0\}$, entonces $\underline{f} = \underline{ah}$. Luego, como $p \nmid a_n$,

$$gr(f) = gr(\underline{f}) = gr(\underline{ah}) = gr(\underline{h}) = gr(h),$$

entonces $gr(g) = 0$. Así, $g = \alpha \in U(Q[x])$.
Análogamente, si $gr(\underline{h}) = 0$, entonces $gr(h) = 0$, luego $h = \beta \in U(Q[x])$.

Ilustramos este resultado en los siguientes ejemplos:
1. $f = x^3 - 2x + 3$ es irreducible en $Z[x]$.
En efecto, es cierto que en $Z_2[x]$: $\underline{f} = x^3 + 1$ y $\underline{f}(1) = 0$.
En $Z_3[x]$: $\underline{f} = x^3 - 2x$ y $\underline{f}(0) = 0$.
Más f es irreducible en $Q[x]$, pues tomando $p = 5$, se tiene que $\underline{f} = x^3 + 3x + 3$ no tiene raíces en $Z_5[x]$.
Así, $\underline{f}$ es irreducible en $Z_5[x]$, luego f es irreducible en $Q[x]$ y por lo tanto en $Z[x]$.
2. $f = x^3 - x + 1$ es irreducible en $Z[x]$.
En efecto, $\underline{f} = x^3 - x + 1$ es irreducible en $Z_2[x]$, puesto que
$\underline{f}(0) = \underline{f}(1) = 1$. Así f es irreducible en $Q[x]$ y por tanto es irreducible en $Z[x]$.
3. Si $f = x^4 + 3x + 1 \in Z[x]$, entonces $\underline{f} = x^4 + x + 1 \in Z_2[x]$ no tiene factores de grado 1 ni de grado 3 en $Z_2[x]$, puesto que $\underline{f}(0) = \underline{f}(1) = 1$. Por otro lado si

$$\underline{f} = (x^2 + ax + b)(x^2 + cx + d) \text{ con } a, b, c, d \in Z_2$$

tenemos que:

$$a + c = 0, b + d + ac = 0, ad + bc = 1 \ y \ bd = 1 \ en \ Z_2.$$

Así de la última igualdad $b = d = 1$, por lo tanto $a + c = 0$ y $a + d = 1$ esta es una contradicción; esto nos dice que $\underline{f}$ es un polinomio irreducible en $Z_2[x]$ por lo tanto f es irreducible en $Q[x]$, luego y siendo f mónico, será irreducible en $Z[x]$.

POLINOMIOS EN VARIAS VARIABLES

Definición 2.26. Consideremos las n variables $x_1, x_2, \ldots, x_n$, definimos los siguientes términos:
El producto $x^a = x_1^{a_1} \ldots x_n^{a_n}$ es llamado término de n variables, donde los $a_i \geq 0$ para i=1, 2,…,n; $a = (a_1, \ldots, a_n)$.

El término αx^n es llamado monomio en las variables $x_1, x_2, \ldots, x_n$; donde $\alpha \in K$ y $x = (x_1, x_2, \ldots, x_n)$.
Toda combinación K-lineal de términos de n variables $x_1, x_2, \ldots, x_n$ es llamado un Polinomio en n las variables $x_1, x_2, \ldots, x_n$.

Por ejemplo, $q(x,y,z) = 2x^3y^5z^4 + 4xyz + xz$ es un polinomio en las variables *x, y ,z;* pues es una combinación lineal de los términos $x^3y^5z^4$, xyz , xz.

El conjunto de todos los polinomios en las variables $x_1, x_2, \dots, x_n$ lo denotaremos por $K[x]$ donde $x = (x_1, x_2, \dots, x_n)$. Este conjunto de polinomios, constituye un anillo respecto de la suma y multiplicación usuales, llamado el Anillo de Polinomios en las n variables $x_1, x_2, \dots, x_n$.

Nota: Recordemos que, en el caso de polinomios de una variable la relación de "divisible" es un buen orden, pues tenemos que (x^n) si y sólo si $m \leq n$. Es decir, la relación divisible es isomorfo a la relación de orden en los naturales.

Esta condición se pierde en el caso de polinomios de varias variables pues la relación "divisible"

$$\left(x_1^{a_1}x_2^{a_2}\dots x_n^{a_n}\right)|\left(x_1^{b_1}x_2^{b_2}x_n^{b_n}\right) \Leftrightarrow a_i \leq b_i \text{ para } i = 1, \dots, n$$

no es un buen orden, aunque sí es un orden parcial. Consideremos en N^n ,$\cdot\ |\ \cdot$ el orden parcial siguiente:

$$(a_1, a_2, \dots, a_n)|(b_1, b_2, \dots, b_n) \Leftrightarrow a_i \leq b_i \text{ para } i = 1, \dots, n$$

Así definido $\cdot\ |\ \cdot$ no es un buen orden, es sólo un orden parcial, pero tiene una propiedad que lo acerca a ser un buen orden.

Proposición 2.27 (Lema de Dickson). Para cada $X \subset N^n$ existe un conjunto finito $D \subset X$ finito tal que:

$$\forall x \in X, \exists d \in D \text{ tal que } d\ |x.$$

Prueba. Daremos una demostración por inducción sobre n.
Para $n = 1$: El orden $\cdot\ |\ \cdot$ en N que es un buen orden. Se cumple.
Probaremos primero para N^2. Supongamos que $X \subset N^2$ y sea $(a,b) \in X$.
Suponiendo que $(a,b) \nmid (x,y)$, entonces $x < a$ o $y < b$.
Sean $A_r = \{\ (r,j)|j \in N\ \}$ y $B_r = \{\ (j,r)|j \in N\ \}$.
Restringiendo $\cdot\ |\ \cdot$ a A_r , es isomorfo al buen orden de N. Para cada $r < a$ y $A_r \cap X \neq 0$ consideremos el elemento mínimo d_r de $A_r \cap X$. Análogamente para B_r, cada $r < b$ y $B_r \cap X \neq 0$ consideraremos el elemento mínimo S_r.
Tomando el conjunto D por (a,b) y todos los d_r y S_r, se verifica que D cumple el resultado.
Caso general: Supongamos que el lema es cierto para N^{n-1} y sea $X \subseteq N^n$.
Sea $A_r^j = \{\ (x_1, x_2, \dots, x_n) \in N^n\ /|\ x_j = r\ \}$ y consideremos $(a_1, \dots, a_n) \in X$.
Para cada $j = 1, \dots, n$ y $r < a_j$ consideramos $X \cap A_r^j$. En $X \cap A_r^j$ elegimos D_r^j finito que satisface el lema para $X' = X \cap A_r^j$. Este D_r^j existe por hipótesis de inducción. Luego el conjunto D cumple con el resultado considerando que:

$$D = \{(a_1, a_2, \dots, a_n)\} \cup \bigcup_{j=1}^{n}\bigcup_{r=0}^{a_j-1} D_r^j$$

Nota: Es necesario tener un orden total de términos para obtener un algoritmo de la división de polinomios de varias variables, el orden parcial $\cdot \mid \cdot$ no es suficiente.
Definición 2.27. Un orden de términos $\preccurlyeq$ es un orden total que satisface lo siguiente considerando los términos t, t_1, t_2

1. $1 \preccurlyeq t$, para todo t.
2. $t_1 \preccurlyeq t_2$ implica que $tt_1 \preccurlyeq tt_2$.

Proposición 2.28: Sea A un anillo conmutativo con unidad y sean I_1, I_2, J, J_1, J_2 ideales en A.

1. Las operaciones entre ideales preservan el orden por inclusión:
si $I_1 \subseteq J_1$ y $I_2 \subseteq J_2$ entonces $I_1 \cap I_2 \subseteq J_1 \cap J_2$, $I_1 I_2 \subseteq J_1 J_2$, $I_1 + I_2 \subseteq J_1 + J_2$

2. Dados $I_1 = \langle f_1, \dots, f_r \rangle$, $I_2 = \langle g_1, \dots, g_m \rangle$, entonces
$I_1 I_2 = \langle f_i g_j, i = 1, \dots, r;\ j = 1, \dots, m \rangle$ y $I_1 + I_2 = \langle f_1, \dots, f_r, g_1, \dots, g_m \rangle$.

3. $J(I_1 + I_2) = JI_1 + JI_2$; $J \cap (I_1 + I_2) = J \cap I_1 + J \cap I_2$; $J + J = J$.

4. $I_1 I_2 \subseteq I_1 \cap I_2$.

5. Si $I_1 + I_2 = A$ entonces $I_1 \cap I_2 = I_1 I_2$.

Prueba de 5. Según el punto 4, basta demostrar que $I_1 \cap I_2 \subseteq I_1 I_2$. Como A tiene unitario, tenemos que $I_1 \cap I_2 = (I_1 \cap I_2)A$. Luego:
$I_1 \cap I_2 = (I_1 \cap I_2)(I_1 + I_2) = (I_1 \cap I_2)I_1 + (I_1 \cap I_2)I_2 \subseteq I_2 I_1 + I_1 I_2 = I_1 I_2$.
Nota: Hay una relación importante entre los sistemas de ecuaciones polinomiales y los ideales en $k[x]$. Sea $I \subset k[x]$ un ideal. Podemos considerar soluciones de I, definiendo el conjunto $V(I) \subset k^n$ como sigue:

$$\alpha \in V(I) \Leftrightarrow \forall f \in I, \quad f(\alpha) = 0$$

Proposición 2.29: Dado el siguiente sistema de ecuaciones polinomiales

$$\{f_1(x_1, \dots, x_n) = 0\ f_2(x_1, \dots, x_n) = 0 : f_m(x_1, \dots, x_n) = 0$$

El conjunto de soluciones de este sistema coincide con $V(\langle f_1, \dots, f_m \rangle)$.

La proposición anterior sugiere una aplicación de los ideales a los sistemas de ecuaciones polinomiales: Si $\langle f_1, \dots, f_r \rangle = \langle g_1, \dots, g_m \rangle$, entonces los sistemas $f_i = 0\ (1 \le i \le r)$ y $g_j = 0\ (1 \le j \le m)$ son equivalentes.
Por otro lado, para cada $X \subseteq k^n$ definimos:

$$I(X) = \{f \in k[x_1, \dots, x_n] \ / \ f(\alpha) = 0\ \forall \alpha \in X\}$$

Proposición 2.30: Se tiene los siguientes resultados en $k[x]$:

1. $I(X)$ es un ideal en $k[x]$.
2. $k[x]$ es un anillo de ideales principales.

Una de las preguntas que vamos a responder en el curso es determinar el conjunto $I(V(I))$. Para esto, primero estudiaremos a los ideales en $k[x]$.

IDEALES EN $K[x_1, \dots, x_n]$

Veremos que los ideales en el anillo de polinomios de varias variables tienen un comportamiento diferente. Por ejemplo, en $k[x, y]$tenemos que $\langle x, y\rangle \neq \langle p\rangle$ para todo $p \in k[x, y]$.

En efecto, si $\langle x, y\rangle = \langle p\rangle$, entonces $x, y \in \langle p\rangle$ y $p \neq 1$. Entonces $x = hp$ e $y = gp$. De aquí, $xy = uhp = xgp$ y por lo tanto $yh = xg$. Luego, $h = xq$ y $g = yq$, lo que implica que $p \in k$ y $\langle p\rangle = k[x, y] \neq \langle x, y\rangle$, lo que es una contradicción). Sin embargo, como sucede con la división de los términos, hay algo bueno con los ideales en $k[x_1, \dots, x_n]$. Todo ideal es finitamente generado.

Proposición 2.31: Sea $I \subset K[x]$ un ideal. Entonces:
$J = I \cap k[x_1, \dots, x_n]$ es un ideal en $k[x_1, \dots, x_n]$., llamado ideal de eliminación de las variables $x_1, x_2, \dots, x_{x-1}$.
Existe una relación entre la intersección de dos ideales y los ideales de eliminación.

Proposición 2.32: Sean $I_1 = \langle G_1\rangle$ e $I_2 = \langle G_2\rangle$ ideales de $k[x]$. Introducimos una nueva variable z y consideremos $J = \langle zG_1, (1 - z)G_2\rangle$ como ideal de $k[z, x]$.
Entonces $I_1 \cap I_2 = J \cap k[x]$.
Demostración. Primero demostraremos que $I_1 \cap I_2 \subseteq J$. Sea $f \in I_1 \cap I_2$. Podemos escribir $f = zf + (1 - z)f$. Como zf es combinación de los elementos de zG_1 y $(1 - z)f$ es combinación de los elementos de $(1 - z)G_2$, se sigue que $f \in J$.
Ahora veamos que $J \cap k[x] \subseteq I_1 \cap I_2$. Sea $J \cap k[x]$. La sustitución $z = 1$ demuestra que $f \in I_1$. La sustitución $z = 0$ demuestra que $f \in I_2$.

IDEALES FINITAMENTE GENERADOS

Para ser más didáctica y dar a entender la idea, recordemos lo que sucede con polinomios de una variable: dados los polinomios en una variable $f, p_1, p_2, \dots, p_k \in k[x]$, ¿cómo determinaremos si $f \in \langle p_1, p_2, \dots, p_k\rangle$? Primero, consideremos p = mcd$(p_1, p_2, \dots, p_k)$ = mcd((…mcd (mcd (p_1, p_2), p_3)…), p_k).
Observamos que $\langle p\rangle = \langle p_1, p_2, \dots, p_k\rangle$. En efecto, por el algoritmo de Euclides mcd$(p_1, p_2) \in \langle p_1, p_2\rangle$. Por inducción, $p \in (p_1, \dots, p_k)$. Por otro lado $p|p_i$ y, como consecuencia, $p_i \in \langle p\rangle$. Entonces, por la posición 2.1.7. $\langle p\rangle = \langle p_1, p_2, \dots, p_k\rangle$.
Ya es fácil de responder si $f \in \langle p_1, p_2, \dots, p_k\rangle = \langle p\rangle$. En efecto, $f \in \langle p\rangle$ si y sólo si $p|f$, lo que podemos determinar usando el algoritmo de la división.
Entonces, si queremos ver si $f \in I$ para un ideal $I \subseteq K[x]$, primero, podemos presentar $I = \langle p\rangle$, es decir, encontrar una base buena. Después, determinamos si $f \in \langle p\rangle$ usando el algoritmo de la división. Un procedimiento parecido puede aplicarse para ideales en el anillo de polinomios en varias variables. ($f \in I$ si y sólo si $f \quad (g_1, \dots, g_r) \quad \Rightarrow 0$).

Esta base especial se llama base de Gröbner, la cual vamos a estudiar a continuación.
Fijamos un orden de términos $\preccurlyeq$. Entonces, para cada $g \in k[x_1, \dots, x_n]$ está definido tg(g). Para un ideal $I \subseteq k[x_1, \dots, x_n]$ definimos:

$$TP(I) = \{tp(f) \ / \ f \in I\}$$

Definición 2.28. $\Gamma \subset I$ se llama base de Gröbner de I si para cada $t \in$ TP (Γ) existe g $\in \Gamma$ tal que tg$(g)| t$.

Lema 2.39. Todo ideal I tiene una base de Gröbner finita. Más aún, para cada base de Gröbner Γ de I, tenemos que $I = \langle \Gamma \rangle$. Además

$$f \in I \text{ si y sólo si } f \; \Gamma \Rightarrow 0.$$

Demostración. Por el Lema de Dickson existe $T \subseteq TP\langle I \rangle$ finito tal que $\forall t \in TP(I) \quad \exists \pi \in T, r|t$. Elegimos para cada $t \in T$ un $g \in I$ tal que tp$(g) = t$.
El conjunto de todos estos g forman una base de Gröbner Γ, Tenemos que $\langle \Gamma \rangle \subseteq I$, ya que $\Gamma \subseteq I$. Hay que demostrar que $I \subseteq \langle \Gamma \rangle$. Supongamos que $f \in I$. Por definición de base de Gröbner existe $g \in \Gamma$ tal que $tp(g)|tp(f)$. Entonces $f \quad g \quad \rightarrow f_1$ y $f_1 - f = pg \in I$. De aquí $f_1 \in I$. Luego, $f_1 \quad g_1 \quad \rightarrow f_2 \quad g_2 \quad \rightarrow$ ... y como $\ldots \prec tp(f_2) \prec tp(f_1) \prec tp(f)$, un argumento inductivo muestra que al final obtenemos cero. Ahora, como $f_i - f_{i+1} \in \langle \Gamma \rangle$ tenemos que $f \in \langle \Gamma \rangle$. La última afirmación se sigue por las consideraciones anteriores.

Algunos resultados de Bases de Gröbner

Supongamos que $\emptyset: R_1 \rightarrow R_2$ es un homomorfismo $\emptyset$ de anillos. El homomorfismo tiene el levantamiento natural (que vamos a denotar por el mismo símbolo $\emptyset$) hasta el homomorfismo $\emptyset$: $R_1[x] \rightarrow R_2[x]$, que está definido como $\emptyset(\alpha_1 x^{a_1} + \alpha_2 x^{a_2} + \cdots) = \emptyset(\alpha_1)x^{a_1} + \emptyset(\alpha_2)x^{a_2} + \cdots$.Un elemento $0 \neq b$ del anillo R se llama divisor de cero si existe $0 \neq a \in R$ tal que $ab = 0$.

Proposición 2.40. Consideremos los anillos R_1 , R_2 y sea Γ una base de Gröbner furte para un ideal $I \subseteq R_1[x]$. Si $\emptyset: R_1 \rightarrow R_2$ es un homomorfismo suprayectivo tal que $\emptyset(\alpha)$ no es 0 y tampoco es un divisor de cero para todo $\alpha \in MP(\Gamma)$, entonces $\emptyset(\Gamma)$ es una base de Gröbner fuerte para $\emptyset(I)$.

Demostración. Como $\emptyset$ es suprayectivo, $\emptyset(I)$ es un ideal de $R_2[x]$. El resultado se sigue fácilmente de la siguiente afirmación.
Afirmación**.** Para cada $h \in \emptyset(I)$ existe $f \in I \cap \emptyset^{-1}(h)$ tal que $tp(f) = tp(h)$.
En efecto, la afirmación implica $mp(h)$ que es divisible por $mp\big(\emptyset(g)\big) = \emptyset(mp(g))$ para un $g \in \Gamma$ tal que $mp(g)|mp(f)$. Entonces, basta demostrar la afirmación.

SISTEMAS DE ECUACIONES POLINOMIALES EN n VARIABLES

Unos de los métodos más comunes, que se usa, para resolver un sistema de ecuaciones lineales, es el método de eliminación de Gauss, por el cual un sistema de ecuación lineal como el siguiente:

$$\begin{gathered} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \cdots + a_{1n}x_n = b_1 \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ a_m x_1 + a_{n2}x_2 + a_{n3}x_3 + \cdots + a_{nn}x_n = n \end{gathered}$$

Se “transforma” en otro sistema de ecuaciones equivalentes, que es más fácil de resolver o que es más fácil de describir su conjunto solución, algo como de este tipo:

$$\begin{aligned} C_{11}x_1 + C_{12}x_2 + \cdots + C_{1n}x_n &= d_1 \\ C_{22}x_2 + \cdots + C_{2n}x_n &= d_2 \\ \vdots \qquad\qquad & \vdots \\ C_{nn}x_n &= d_n \end{aligned}$$

Esta transformación se logra mediante la aplicación de operaciones elementales de filas o columnas. Estas operaciones elementales que puede ser de tres tipos: permutación de ecuaciones, multiplicación de una ecuación por un número diferente de cero y sumar una ecuación multiplicada por un número diferente de cero a otra. Estas operaciones nos permiten ir “eliminando” una variable, hasta lograr un sistema en el que se pueda despejar la última variable
Luego reemplazando esta última variable en la ecuación anterior (en la penúltima ecuación), podemos despejar la penúltima variable. Aplicando este resultado en la ecuación anterior a ella, y procediendo de esta manera, hasta hallar el valor de la primera variable y por lo tanto de todas las variables

Para resolver un sistema de ecuaciones polinomiales, queremos generalizar este método de eliminación de Gauss. Para lograrlo, conservaremos las tres operaciones elementales: permutar, sumar y multiplicar una ecuación polinomial por un número un nulo o por un polinomio si fuera necesario.

Sin perder generalidad, consideremos un sistema de ecuación polinomial del siguiente tipo:

$(*)$ $\{f_1(x_1, x_2, \dots, x_n) = 0\ f_2(x_1, x_2, \dots, x_n) = 0\ \vdots\ f_r(x_1, x_2, \dots, x_n) = 0$

Resolver este sistema es hallar los ceros o raíces de todos los polinomios
$f \in J = \langle f_1, f_2, \dots, f_r \rangle$.
Para ilustrar la idea, consideremos:
$R[x, y]$ y el ideal $J = \langle f_1, f_2 \rangle$ donde $f_1(x, y) = x^2 + y^2 - 13$,
$f_2(x, y) = y - 1,5x$. Notar que si $f \in I$, entonces
$f(x, y) = (x^2 + y^2 - 13)h_1(x, y) + (y - 1{,}5x)h_2(x, y)$.
Además, tenemos que $f(2{,}3) = f(-2, -3) = 0$.
Esto significa que los puntos $(2{,}3)$ y $(-2, -3)$ son soluciones del sistema de ecuaciones polinomiales.

$$\{x^2 + y^2 - 13 = 0\ y - 1{,}5x = 0$$

Es decir; el conjunto solución del sistema de dos ecuaciones

$$(1) \qquad \{f_1(x,y) = 0\ f_2(x,y) = 0$$

es el mismo que el conjunto solución del conjunto del sistema de ecuaciones infinito $f(x,y) = 0\ \forall f \in I = \langle f_1, f_2 \rangle$

Nota:

1. Si se tuviera, además de (1), cualquier otro sistema polinomial como:

$$\{h_1(x,y) = 0\ h_2(x,y) = 0$$

que tenga el mismo conjunto solución, es tal que

$$\langle h_1, h_2 \rangle = \langle f_1, f_2 \rangle$$

2. Dado $K[x_1, x_2, \dots, x_n]$ donde $K = C\ o\ R$ y I un ideal tal que $I \subset K[x_1, \dots, x_n]$, podemos definir una relación de equivalencia: "$\sim$" en el conjunto de polinomio de varias variables, así:

$$f \sim h \quad \text{si y sólo si} \quad f - h \in I$$

y considerando que: $f \sim h \leftrightarrow \exists\ q \in I + q\ \ f = h = q$

$$\leftrightarrow f = h + q, \qquad q \in I$$

$$\leftrightarrow h = f - q$$

Entonces $f \sim h \leftrightarrow h = f - q$

Es decir, podemos obtener h, restando que al polinomio f y podemos "reemplazar" h por f.

3. Si $f - h \in I = \langle f_1, f_2, \dots, f_r \rangle$ y $h = 0 \Rightarrow f \in \langle f_1, f_2, \dots, f_r \rangle$

Pero, podría ser que $f \in \langle f_1, f_2, \dots, f_r \rangle$, pero el resto de la división de f por $f_1, f_2, \dots, f_r$ sea diferente de 0.

Veamos un ejemplo:

$f(x,y) = y^2x - x \in Q[x]$, y el $I = \langle f_1, f_2 \rangle\ CQ[xy]$ donde $f_1^x = yx - y$, $f_2 = y^2 - x$. Sea $> x$. Sea $F = \{f_1, f_2\}$ buscando el orden deglex con $y > x$ y el algoritmo de la división, vemos que $f\ f_1 \rightarrow\ y^2 - x\ f_2 \rightarrow\ 0$

Es decir $f\ F \rightarrow\ 0$ y $f = yf_1 + f_2 \in I$.

Si $f\ f_1 \rightarrow\ y^2 - x\ f_2 \rightarrow\ 0$ es $f\ F \rightarrow\ 0$ y $f = yf_1 + f_2 \in I$. Pero si $f\ f_2 \rightarrow\ x^2 - x$ y $x^2 - x$ es reducido con respecto a F. Entonces, el resto de la división de f por F es nulo, $f \in I = \langle f_1, f_2 \rangle$.

Con este procedimiento, el sistema inicial (*) será "simplificado" a otro, con el mismo conjunto de soluciones que el sistema original, pero cuya solución es más fácil de obtener.

La idea, es realizar los intercambios, buscando que el nuevo sistema simplificado este inducido por una base de Gröbner del ideal generado por los polinomios del sistema de ecuaciones polinomiales originales.

4. Diremos que un polinomio es más "simple" que otro si es de menor grado. En polinomios de varias variables necesitamos tener en cuenta todos los exponentes de cada variable (para garantizar unicidad) del monomio de mayor grado. Esto es establecer un "orden". Pues el orden en que se realicen las divisiones puede conducir a resultados distintos.

2.2.2 Conceptual

La intención de proteger información secreta o de alta confidencialidad siempre ha estado presente en nuestras vidas y en nuestra historia desde el Antiguo Egipto, en Roma, en Babilonia, etc. Inicialmente hacer los mensajes o información ilegibles era usada básicamente como una estrategia militar y política, el Cifrado de César que es considerado un ejemplo de criptografía clásica, se basaba en el desplazamiento de las letras del alfabeto o en sustituciones polialfabéticos (varios alfabetos).

Han sido muchos los algoritmos o técnicas que se han creado para garantizar la privacidad de la comunicación por medios inseguros, inicialmente los algoritmos se empleaban sin ordenadores y era relativamente fácil de resolver, pues empleaba una sola clave para cifrar el mensaje y para descifrarlo fueron cambiando.

Luego, Claude Elwood Shannon, a fines del siglo XX, dio a conocer un algoritmo de cifrado, basado en un conjunto de funciones o transformaciones por la cuales un texto simple pasaba a texto ilegible. Este cifrado, diseñado por Shannon, a pesar de ser riguroso, presentaba un inconveniente y éste era que, los interesados en compartir la información debían en algún momento intercambiar la clave (había una única clave) y debían hacerlo por algún medio seguro; pero tener un medio seguro para la intercambiar la clave era tan complicado, como enviar la información.

Una de las grandes motivaciones que dieron pase a una criptografía con dos claves fue el hecho de querer quebrar el sistema de cifrado de la máquina Enigma, (1920), una máquina criptográfica alemana a rotor; cuyas claves fueron descubiertas por Alan Turing, considerado padre de la informática y de la inteligencia artificial; durante la Segunda Guerra Mundial A partir de allí surgieron los ordenadores y esta nueva manera de cifrar la información se basaba en la existencia de problemas matemáticos difíciles de resolver. En 1 976, Whitfiel Diffie y Martin Hellman resolvieron el problema de intercambiar la claves por un medio seguro, pues crearon un protocolo de intercambio de claves y sus ideas fueron adaptadas a un sistema de cifrado con dos tipos de clave; una clave pública, que todos pueden ver y una clave privada, que está oculta.

En la actualidad se consideramos tres tipos de criptografía, la criptografía simétrica o de clave privada, que usa una única clave para cifrar y descifrar; con el inconveniente que se debe intercambiar la clave por un medio seguro. Por ejemplo, DES (Data Encription Standard) y AES (Advanced Encription Standard). Ambos son considerados actualmente como algoritmos de cifrados inseguros, frente al avance y la velocidad de la internet.

La criptografía de clave pública emplea dos claves una clave pública para cifrar el texto y una clave privada para descifrarlo. En este caso no hay necesidad de enviar la clave en secreto, la clave se difunde en internet, todos la ven y todos pueden hacer uso de ella.
La criptografía híbrida, que se caracteriza en combinar las dos anteriores

Los criptosistemas que se consideran actualmente como algoritmos fuertes son basados en el problema matemático difícil de resolver, que es el de factorizar en primos-

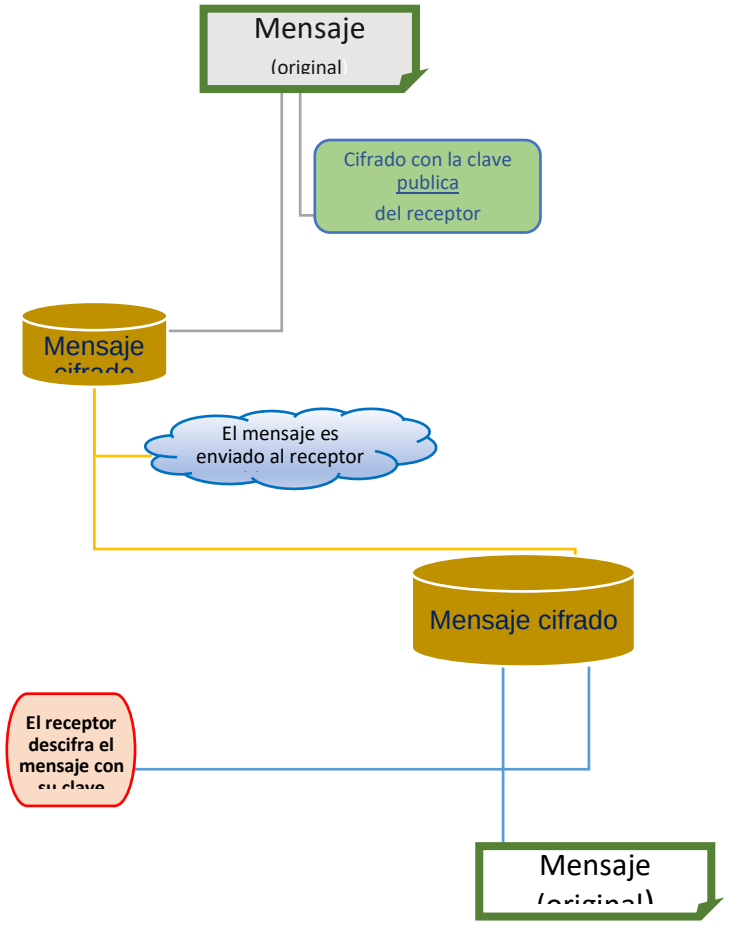
En 1994 Peter Shor presentó un algoritmo que servía para factorizar en números primos en tiempo polinomial con ayuda de un ordenador cuántico. Se pensó que con esto se vulneraría estos criptosistemas fuertes.

Hasta la actualidad no se cuenta con un ordenador cuántico que haría muy efectivo el algoritmo de Shor; sin embargo, en unos cuantos años se espera contar con ellos.

Este hecho hace urgente generar nuevos criptosistemas que no sean vulnerables a este procedimiento de Shor ni a los ordenadores cuánticos; es así que es importante generar nuevos criptosistemas que estén basados en problemas matemáticos difíciles que no involucren la factorización en primos.

Una gran alternativa es trabajar con otro problema difícil en matemática determinar las raíces de polinomios de varias variables.

Fig. 1 Cifrado de clave Pública



Fuente: Elaboración propia

2.3 Definición de términos básicos

- **Criptografía:** La criptografía es un conjunto de técnicas y procedimientos para escribir un mensaje de manera protegida, es decir, escribir un mensaje que solo puede ser leído por quien sea capaz de descifrarlo o hacerlo legible.
  Para algunos la criptografía es la ciencia de cifrar y descifrar información utilizando técnicas que permitan el intercambio de información, por medios públicos y/o inseguros, sólo con las personas o entidades a quienes van dirigidas.

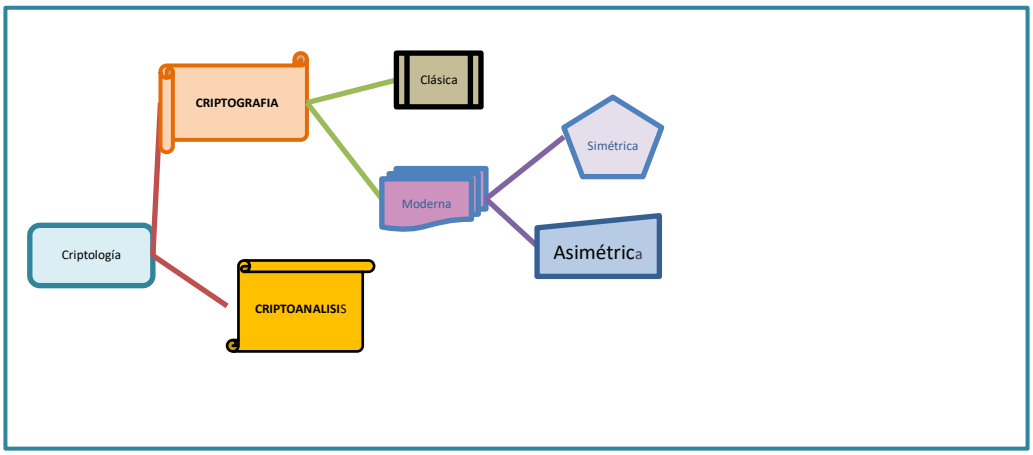
Mediante la criptografía podemos restringir la información a quienes no tienen acceso autorizado(confidencialidad); podemos bloquear la intersección de información, también permite evitar la modificación y la adición de información por agentes externos(Integridad de información), permite verificar si la persona que quiere acceder a la información es quien dice ser(autenticidad del usuario), autenticidad del remitente y también permite verificar que quien recibe el mensaje no puede negar que lo recibió(no repudio en origen) y quien lo envió no pueda negar que lo hizo(no repudio de destino).En otras palabras, la criptografía brinda privacidad, seguridad, confidencialidad, autenticidad y control de acceso, a nuestros recursos y a nuestras transacciones telemáticas. La criptografía puedes ser clásica o moderna.

.

- **Criptografía de clave pública:** La criptografía de clave pública en uno de los tipos de criptografía moderna existentes, como pasamos a describir:
  La criptografía simétrica o de clave privada, usa una única clave para cifrar y descifrar; el gran inconveniente es que se debe intercambiar la clave por un medio seguro, lograr ello es tan complicado como enviar el mensaje por un medio seguro. Por ejemplo, DES (Data Encription Standard) y AES (Advanced Encription Standard); ambos son considerados actualmente como algoritmos de cifrados inseguros, frente al avance y la velocidad de la internet.
  La criptografía asimétrica o de clave pública, emplean dos claves una clave pública para cifrar el texto y una clave privada para descifrarlo. En este caso no hay necesidad de enviar la clave en secreto, la clave se difunde públicamente en internet, todos la ven y todos pueden hacer uso de ella; está vinculada a resolver un problema matemático difícil. Su fortaleza dependerá de la dificultad del problema.
  En la actualidad se estila mucho considerar una criptografía híbrida o mixta que consiste en utilizar ambos tipos de criptografía, pues generalmente los sistemas de clave pública son lentos y demoran en resolver por ello, estos se utilizan para el envío de claves privadas o secretas, mientras que los sistemas de clases privadas se usan para el envío general de los datos encriptados.

- **Criptoanálisis:** es un conjunto de técnicas que se usan para romper los códigos usados para cifrar cierta información. Siempre asociado a alguien interesado en proteger la información hay alguien interesado en conocerla, por lo que la criptografía y el criptoanálisis son inseparables y juntos constituyen la criptología.

Fig. 2 Criptografía y criptosistemas



Fuente: Elaboración propia

- **Criptosistema:** llamado también sistema criptográfico o sistema de cifrado es el conjunto de fundamentos y procedimientos de operación (algoritmo) que se utiliza para el cifrado y descifrado de un mensaje o información, los cuales pueden estar basados en diferentes teorías matemáticas.

  Un criptosistema se compone de dos etapas la primera: encriptar o cifrar el mensaje, es decir convertir un mensaje en ilegible, usando una clave o procedimiento; y la segunda etapa: desencriptar o descifrar el mensaje con una clave (que será secreta) y permite leer el mensaje.

  Para una definición más formal, podemos señalar que un criptosistema es la siguiente quíntupla: (m,c,k,E,D)
  donde m: es el mensaje (original); c: es conjunto de todos los mensajes cifrados (criptogramas); k: el conjunto de claves que se emplean; E el conjunto de transformaciones de cifrado y D: el conjunto de transformación descifrado.
  Entonces, se cumple que Dk(Ek(m))=m.
  Y bueno como lo señalamos líneas arriba, asociado a un sistema criptográfico hay que tener en cuenta que puede ser posible que alguien que no esté autorizado pueda romper el cifrado y acceder a la información secreta, es así que surge el criptoanálisis.

- **Anillo de polinomios en varias variables:** el conjunto que denotaremos por $K[x]$ y está constituido polinomios en las n variables $x_1, x_2, \dots, x_n$ que por simplificar

la escritura denotaremos con $x = (x_1, x_2, \dots, x_n)$, cada uno de estos polinomios en la variables x es una K-combinación lineal de términos en las variables x_1, x_2, $\dots$, x_n. Este conjunto que constituye un anillo respecto de la suma y multiplicación usuales es llamado el anillo de polinomios en n variables.

- **Bases de Gröbner:** Una Base de Gröbner para el ideal I es el conjunto de polinomios no nulos $\Gamma = \{g_1, \dots, g_t\}$ de I tal que para cada $f \in I$ no nulo existe i $\in \{1,2,3, \dots, t\}$ tal que lp(g_i)| $lp(f)$, donde $I \subseteq k[x_1, \dots, x_n]$.

CAPÍTULO III: **HIPÓTESIS Y VARIABLES**

3.1 Hipótesis

3.1.1 Hipótesis General

Las bases de Gröbner permiten determinar algoritmos criptográficos.

3.1.2 Hipótesis Específicas

1. Los sistemas de generadores de un ideal contenido en un anillo de polinomios de varias variables aportan a la construcción de las bases de Gröbner.
2. Bajo condiciones de divisibilidad es posible definir las bases de Gröbner respecto al orden.
3. El funcionamiento del criptosistema está basado en que la clave del criptosistema es el ideal, del cual se conoce la base de Gröbner, lo que permite descifrar el mensaje.

3.2 Definición conceptual de variables

Variable independiente

Base de Gröbner.

Variable dependiente

Criptosistema.

3.3 Operacionalización de variables

Tabla Nº 1

Operacionalización de la variable Independiente

Variable	Dimensión	Indicadores	Índice	Métodos y técnicas
Base de Gröbner	Minimal	Divisibilidad Generalizada para los polinomios en varias variables.	Base de Gröbner reducida	Algoritmo de división generalizado

Tabla Nº 2

Operacionalización de la variable Dependiente

Variable	Dimensión	Indicadores	Índice	Métodos y técnicas
criptosistema	asimétrico	Determinar un algoritmo cuya clave pública y clave secreta se basa en teoría de polinomios.	Criptosistema resistente a la factorización en primos y a un ordenador cuántico.	Resolución de sistemas de ecuaciones polinomiales

CAPITULO IV: DISEÑO METODOLÓGICOS

4.1 Tipo de diseño de investigación.

Este proyecto de investigación es de tipo analítico y descriptivo, no experimental y transversal. Iniciaremos con el estudio de ideales, bases de ideales, resolución de sistemas de ecuaciones algebraicas de varias variables y luego caracterizamos las bases de Gröbner respecto a la relación de orden < Probaremos la existencia de Bases d Gröbner y las bases de Gröbner reducidas.

4.2 Método de investigación

La presente investigación se ha empleado el método deductivo- analítico. Primeramente, hemos establecido un conjunto de premisas generales se ha llegado a conclusiones particulares, es decir, va de lo general a lo particular. Luego, se ha aplicado el método analítico a lo largo de su desarrollo (esto es incluyendo conceptos, definiciones, proposiciones, etc) para llegar a obtener conclusiones que nos permitan determinar la ventaja de aplicar algoritmos de encriptación modernos como el de bases de Gröbner para resolver el problema de ser resistente a los ordenadores cuánticos.

4.3 Población y muestra

Esta investigación tiene como población o universo el conjunto de todos los sistemas criptográficos, que forman parte de la criptografía. La muestra sería los sistemas criptográficos basados en fundamentos algebraicos.

4.4 Lugar de estudio y periodo desarrollado

El estudio se realizó en los ambientes de la Facultad de Ciencias Naturales y Matemática de la Universidad del Callao. Y el período de ejecución de la investigación fue desde el 01 de Junio del 2019 al 31 de Mayo del 2020.

4.5 Técnicas e instrumentos para la recolección de la información

Para la recolección de información se recurrirá a la revisión de bibliografía especializada de libros, artículos de investigación de repositorios de algunas universidades; mediante técnicas como el análisis de contenido, análisis de registro y haremos usos de instrumentos como tablas y/o cuadros.

4.6 Análisis y procesamiento de datos

Este proyecto de investigación se recurrirá a técnicas lógicas como inducción, deducción, análisis y síntesis de la información; y para el procesamiento de datos haremos uso de registro y clasificación de los mismos.

4.7 Si la orientación es hacia un proyecto de inversión

El presente proyecto de investigación no está orientado a proyecto de inversión por el momento.

4.8 Si el proyecto se orienta al impacto ambiental

El presente proyecto de investigación no está orientado al impacto ambiental.

CAPITULO V: RESULTADOS

5.1 Resultados descriptivos

ORDEN DE MONOMIOS EN $K[x_1, \dots, x_n]$

Queremos generar un ordenen este anillo para ello recordemos que en el caso de polinomios de una variable, hemos ordenado los polinomios, ordenando de mayor a menor el exponente de la indeterminada, esto nos fue útil para identificar el término y el coeficiente principales de los polinomios en $K[x]$; sin embargo, para el caso de polinomios de varias variables definiremos un orden análogo.

Sea $M_n = \left\{ x_1^{\beta_1} \dots x_n^{\beta_n} \ / \ \beta_i \in \mathbb{N}, i = 1, \dots, n \right\}$ el conjunto de monomios o productos de potencias de $K[x_1, \dots, x_n]$, donde $x_1^{\beta_1} \dots x_n^{\beta_n} = X^{\beta}$, donde $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$.

El conjunto M_n puede ordenarse de varias maneras, pero es necesario que cumpla algunas propiedades similares al caso de polinomios en una variable como por ejemplo extender las relaciones de divisibilidad, para que llegue a ser un orden total. Es decir, dados cualquier par de elementos x, y se debe cumplir una de las tres condicione
$x < y \quad \vee \quad x = y \quad \vee \quad x > y$; y además, estar bien ordenado.

Definición 5.1.1 Un orden monomial en M_n es un orden total $\preccurlyeq$ que satisface las siguientes condiciones:
1. $1 \preccurlyeq X^{\beta}$ para todo $X^{\beta} \in M_n \backslash \{1\}$ (bien fundado).
2. Si $X^{\alpha} \preccurlyeq X^{\beta}$, entonces $X^{\alpha} X^{\gamma} \preccurlyeq X^{\beta} X^{\gamma}$, para todo $X^{\gamma} \in M_n$ (compatibilidad).

El conjunto numerable M_n es una base para el K-espacio vectorial $K[x_1, \dots, x_n]$, entonces

todo $p \in \mathrm{K}[x_1, \dots, x_n]$ no nulo, puede ser escrito en forma canónica como la suma

$$\sum_{w \in supp(p)} c_w X^w$$

donde $supp(p)$ es subconjunto finito de $\mathbb{N}^n$ que está determinado de manera única, tal que $c_w \in \mathrm{K}\backslash\{0\}$ para todo $w \in supp(p)$. Más aun, para cada $p \in \mathrm{K}[x_1, \dots, x_n]$ definimos el conjunto de monomios que están en p, llamado **soporte de p** ,así:

$$Supp(p) = \{X^w \in M_n \,/\, w \in supp(p)\}$$

Proposición 5.1.1: Dados $X^v, X^w \in M_n$ tenemos que

si X^v divide a X^w entonces $X^v \leq X^w$.

Prueba. Tenemos que existe un $X^\gamma \in M_n$ tal que $X^w = X^v X^\gamma$. Por la primera condición de la definición de orden monomial, tenemos $X^\gamma \geq 1$ y por la segunda condición $X^w = X^v X^\gamma \geq X^v$, lo que concluye la prueba.

Teorema 5.1.2: Un orden monomial en M_n es un buen orden.

Prueba: PDQ. $A \subset M_n$, existe $X^v \in A$ tal que para todo $X^w \in A$, $X^v \leq X^w$.

Procediendo por el absurdo, supongamos que existe un orden monomial que no es un buen orden, entonces, existen $X^{v_i} \in M_n$, $i = 1, 2, \dots$ tales que $X^{v_1} > X^{v_2} > X^{v_3} > \cdots$ Entonces podemos generar una cadena creciente de ideales en $\mathrm{K}[x_1, \dots, x_n]$,así:

$$\langle X^{v_1} \rangle \subsetneq \langle X^{v_1}, X^{v_2} \rangle \subsetneq \langle X^{v_1}, X^{v_2}, X^{v_3} \rangle \subsetneq \cdots$$

donde $\langle X^{v_1}, \dots, X^{v_i} \rangle \neq \langle X^{v_1}, \dots, X^{v_{i+1}} \rangle$, puesto que si son iguales $X^{v_{i+1}} = \sum_{j=1}^{i} q_j X^{v_j}$ siendo q_j un polinomio en $\mathrm{K}[x_1, \dots, x_n], para\ j = 1, \dots, i.$
Como cada q_j como una combinación lineal de productos de potencia, el lado derecho es divisible por algún $X^{v_j}, 1 \leq j \leq i$, entonces $X^{v_{i+1}}$ también es divisible por algún X^{v_j} y $X^{v_{i+1}} \geq X^{v_j}$, $1 \leq j \leq i$ y por la proposición anterior lo cual es una contradicción. Luego la cadena de ideales es estrictamente creciente, entonces $k[x_1, \dots, x_n]$ no es Notheriano.

Definición 5.1.2:
Considerando X=$x_1 x_2 \dots x_n$; $a = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$, definimos el **orden lexicográfico** en M_n (**lex**)con $x_1 > x_2 > \cdots > x_n$ de la siguiente manera:

$X^\alpha < X^\beta$ si y solo si las primeras coordenadas de α y β desde la izquierda que son diferentes cumplen $\alpha_i > \beta_i$.
Consideremos un ejemplo usando el orden lex en $\mathrm{K}[x, y]$ con $x < y$ tenemos

$$1 < x < x^2 < x^3 < \cdots < y < xy < x^2 y < \cdots < y^2 < \cdots$$

Definición 5.1.3:
Considerando que $X = x_1x_2 \dots x_n;\ \alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$, definimos el **orden de grado lexicográfico** en M_n **(deglex)** con $x_1 > x_2 > \cdots > x_n$ así:

$X^\alpha < X^\beta$ si y solo si $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$ ó $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ y $X^\alpha < X^\beta$

con respecto a lex con $x_1 > x_2 > \cdots > x_n$.

Usando el orden de grado lexicográfico delex en $K[x, y]$ con $x < y$, tenemos

$$1 < x < y < x^2 < xy < y^2 < x^3 < x^2y < xy^2 < y^3 < \cdots$$

Definición 5.1.4: Con las mismas condiciones anteriores, definimos el **orden reverso de grado lexicográfico** en M_n **(degrevlex**) con $x_1 > x_2 > x_3 > \cdots > x_n$, asi:

$X^\alpha < X^\beta$ si y solo si $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$ ó $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ y si las primeras coordenadas diferentes de la derecha

Cumplen que $\alpha_i > \beta_i$

Un ejemplo en $k[x_1, x_2, x_3]$ con respecto a degrevlex y $x_1 > x_2 > x_3$ tenemos, $x_1^2x_2\, x_3 < x_1x_1^2$.

Observaciones:
1.Si f es un polinomio denotaremos por lt(f) al término principal, lc(f) al coeficiente principal y por lp(f) al monomio principal de f.

2.Sea el polinomio $f(x, y, z) = x^2y + 2xyz - 7x^3$; tenemos que si el orden es lex con $x > y > z$, entonces $\text{lt}(f) = -7x^3$; $\text{lp}(f) = x^3$; $\text{lc}(f) = -7$. Si el orden es deglex con $x > y > z$, entonces $\text{lt}(f) = 2xyz$; $\text{lp}(f) = xyz$; $\text{lc}(f) = 2$; y si el orden es degrevlex con $x > y > z$, entonces $\text{lt}(f) = x^2y$; $\text{lp}(f) = x^2y$; $\text{lc}(f) = 1$.

4.Un polinomio $f \in k[x_1, \dots, x_n]$ se dice homogéneo todos sus términos tienen el mismo grado total; si f es un polinomio homogéneo, con el orden degrevlex y $x_1 > x_2 > x_3 > \cdots > x_n$ se verifica que x_n divide a f si y solo si x_n divide a lt(f). $f \in \langle x_1, \dots, x_n \rangle$ si, y solo si $\text{lt}(f) \in \langle x_1, \dots, x_n \rangle$.
5. En $k[x, y]$, deglex y degrevlex son el mismo orden.

ALGORITMO DE LA DIVISIÓN EN K$[x_1, \dots, x_n]$
La idea básica del algoritmo será la misma que en el caso de los polinomios de una variable: cuando dividamos f por $f_1, \dots, f_s$ queremos cancelar términos de f usando los términos principales de los $f_i's$ (con los que los nuevos términos introducidos serían menores a los cancelados) y continuar con este proceso hasta que no sea posible más.

Definición 5.1.5 Dados f, g, h, en $k[x_1, \dots, x_n]$ con $g \neq 0$ y fijemos un orden entre los monomios. Decimos que f se reduce a h módulo g en un paso y escribimos

$f \xrightarrow{g} h$ si y solo si lp(g) divide a un término no nulo X de f y $h = f - \frac{X}{\text{lt}(g)}g$.

Veamos algunos ejemplos**:**
1.Sean $f = 2x^3 + x^2y + y^3$, $g = x^2 - xy \in \mathbb{Q}[x, y]$, con el orden lex $x > y$. Escogemos el término $X = 2x^3$ en f y calculamos $h = f - \frac{X}{\mathrm{lt}(g)} g = 2x^3 + x^2y + y^3 - \frac{2x^3}{x^2}(x^2 - xy) = 3x^2y + y^3$.

2. Sean $f = y^2x + 4yx - 3x^2$, $g = 2y + x + 1 \in \mathbb{Q}[x, y]$, con el orden deglex $y > x$. Entonces

$$f \xrightarrow{g} -\frac{1}{2}yx^2 + \frac{7}{2}yx - 3x^2 \xrightarrow{g} -\frac{1}{4}x^3 + \frac{7}{2}yx - \frac{11}{4}x^2 \xrightarrow{g} \frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x$$

En el último polinomio ningún término es divisible por $\mathrm{lp}(g) = y$ y enonces el proceso de división no puede continuar.

Definición 5.1.6: Sea f, h, $f_1, \dots, f_s$ polinomios en $k[x_1, \dots, x_n]$ con $f_i \neq 0$, $1 \leq i \leq s$ y sea $F = \{f_1, \dots, f_s\}$. Decimos que:
f se reduce a h módulo F, escribimos $f \xrightarrow{F} h$, si y solo si existe una secuencia de índices $i_1, i_2, \dots, i_t \in \{1, \dots, s\}$ y una secuencia de polinomios
$h_1, \dots, h_{t-1} \in k[x_1, \dots, x_n]$ tal que

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

Proposición 5.1.3: Sea $f \in k[x_1, \dots, x_n]$.
1. Si $f = 0$ entonces $f \xrightarrow{g} 0$ para todo polinomio $g \in k[x_1, \dots, x_n]$ no nulo.
2. Sean $c \in k$, $c \neq 0$, entonces $f \xrightarrow{c} 0$.
3. Dado $f \xrightarrow{F} h$ y un monomio X entonces $Xf \xrightarrow{F} Xh$.

4. Sea F un conjunto de polinomios no nulos, $f \in F$ y $g \in k[x_1, \dots, x_n]$.
Entonces $fg \xrightarrow{F} 0$.

Probaremos 2. Dado que K es un cuerpo, cualquier término no nulo en $k[x_1, \dots, x_n]$ es dividido por c y luego f se reduce a cero usando el polinomio constante c.

Ejemplo: Sean $f = xy^2 + xy + y^2$, $g = xy + y^2$, $\phi = x \in \mathbb{Q}[x, y]$; con el orden deglex $x > y$. Entonces $f \xrightarrow{\emptyset} xy + y^2 = r$ y $g \xrightarrow{\phi} y^2 = s$ pero $f + g \xrightarrow{\phi} 2xy + 2y^2 \neq r + s$.
Consideremos $f, g_1, g_2 \in k[x_1, \dots, x_n]$, $G = \{g_1, g_2\}$, con g_1, g_2 no nulos tales que

$$f \xrightarrow{g_1} h_1 \xrightarrow{g_2} h_2.$$

Entonces de la primera reducción tenemos:

$$h_1 = f - \frac{X_1}{\mathrm{lt}(g_1)} g_1$$

para algún término no nulo X_1 de f, tal que lp (g_1) divide a X_1, con

$$\mathrm{lp}(f) = \max\left(\quad \mathrm{lp}(h_1), \quad \mathrm{lp}\left(\frac{X_1}{\mathrm{lt}(g_1)}\right)\mathrm{lp}(g_1) \quad \right)$$

Luego, de la segunda reducción:

$$h_2 = h_1 - \frac{X_2}{\mathrm{lt}(g_2)}\, g_2$$

para algún término no nulo X_2 de h_1, tal que lp (g_2) divide a X_2 con

$$\mathrm{lp}(h_1) = \max\left(\mathrm{lp}(h_2), \mathrm{lp}\left(\frac{X_2}{\mathrm{lt}(g_2)}\right)\mathrm{lp}(g_2)\right)$$

Combinando estas dos últimas expresiones obtenemos

$$f = \frac{X_1}{\mathrm{lt}(g_1)}\, g_1 + \frac{X_2}{\mathrm{lt}(g_2)}\, g_2 + h_2 = u_1 g_2 + u_2 g_2 + h_2$$

Con $\mathrm{lp}(f) = \max\left(\mathrm{lp}(u_1)\mathrm{lp}(g_1), \mathrm{lp}(u_2)\mathrm{lp}(g_2), \mathrm{lp}(h_2)\right)$. es decir el proceso de reducción induce una división de f por G. En caso el polinomio h_2 cumpla ciertas condiciones lo llamaremos $resto$ de la división de f por G o $reducido$ respecto a G.

Definición 5.1.7: Un polinomio r es llamado reducido con respecto a un conjunto de polinomios no nulos $F = \{f_1, \dots, f_s\}$ si $r = 0$ o ningún producto de potencias $X \in Supp(r)$ es divisible por algún $\mathrm{lp}(f_i)$, $i = 1, \dots, s$. En otras palabras, r no puede reducirse módulo F a otro polinomio no nulo.

Definición 5.1.8: Si $f \xrightarrow{F} r$ y r es reducido respecto a F, entonces llamamos a r un resto para f con respecto a F.

ALGORITMO DE LA DIVISIÓN EN $k[x_1, \dots, x_n]$

Este proceso de reducción, ahora nos permite definir un algoritmo de la división que imite al caso de polinomios en una variable.

Entrada: $f, f_1, \dots, f_s \in k[x_1, \dots, x_n]$ con $f_i \neq 0$ $(1 \leq i \leq s)$.

Salida: $u_1, \dots, u_s, r$ tal que $f = u_1 f_1 + \cdots + u_s f_s + r$, r es reducido con respecto a $\{f_1, \dots, f_s\}$ y max (lp (u_1) lp (f_1), … , lp (u_s) lp (f_s), lp (r) =lp (f) .

Inicio: $u_1 := 0, u_2 := 0, \dots, u_s := 0, r := 0, h := f$

Mientras $h \neq 0$

Hacer

Si existen i tales que lp (f_i) divide a lp (h),

Entonces

Elegir algún i

$$u_i := u_i + \frac{lt(h)}{lt(f_i)}$$

$$h \coloneqq h - \frac{lt(h)}{lt(f_i)} f_i$$

sino

$$r = r + lt(h)$$

$$h = h - lt(h)$$

Fin
Si
Fin mientras.

Teorema 5.1.4: Dado $F = \{f_1, \dots, f_s\}$ un conjunto de polinomios no nulos y f en $k[x_1, \dots, x_n]$. Entonces, el algoritmo de la división garantiza la existencia de polinomios

$u_1, \dots, u_s, r \in k[x_1, \dots, x_n]$ tales que $f = u_1 f_1 + \cdots + u_s f_s + r$

con r reducido con respecto a F y

$$\text{lp}(f) = \max\left(\max_{1 \le i \le s} (\text{lp}(u_i)\text{lp}(f_i),\ \text{lp}(r)) \right)$$

Además, este algoritmo es equivalente a $f \xrightarrow{F} r$.

Prueba. Observemos primero que el algoritmo termina. En cada iteración del algoritmo, el término principal de h es substraído hasta que ya no es más posible. Así tenemos una secuencia h_1, h_2, … de los $h's$ en el algoritmo donde $\text{lp}(h_{i+1}) < \text{lp}(h_i)$ y, desde que el orden de los términos es bien ordenado, la lista de los $h_i's$ es en realidad finita.

Desde que al comienzo $h = f$, tenemos que en cada iteración del algoritmo $\text{lp}(h) \le \text{lp}(f)$. Ahora, para cada i, obtenemos u_i agregando términos $\frac{\text{lt}(h)}{\text{lt}(f_i)}$, entonces $\text{lp}(u_i)\text{lp}(f_i) \le \text{lp}(f)$. Además, r es obtenido al agregar lt (h) y entonces $\text{lp}(r) \le \text{lp}(f)$,.

Notar que con f escrito como en el teorema anterior, tenemos $f - r \in \langle f_1, \dots, f_s \rangle$. Luego, si $r = 0$, entonces $f \in \langle f_1, \dots, f_s \rangle$. Sin embargo, el converso no es necesariamente cierto; es decir f puede estar en el ideal $\langle f_1, \dots, f_s \rangle$ pero el resto de la división de f por $f_1, \dots, f_s$ no ser cero como comprobaremos en el siguiente ejemplo.

Ejemplo: Sean $f = y^2x - x \in \mathbb{Q}[x, y]$, y el ideal $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[x, y]$, donde $f_1 = yx - y$, $f_2 = y^2 - x$. Sea $F = \{f_1, f_2\}$. Usando el orden deglex $y > x$ con y el algoritmo de la división, vemos que $f \xrightarrow{f_1} y^2 - x \xrightarrow{f_2} 0$, es decir, $f \xrightarrow{F} 0$, $f = yf_1 + f_2 \in I$. Sin embargo, si usamos f_2 primero en el algoritmo de la división entonces $f \xrightarrow{f_2} x^2 - x$, y $x^2 - x$ es reducido con respecto a F. Luego el resto de la división de f por F es no nulo, pero f está en el ideal $\langle f_1, f_2 \rangle$.

Proposición 5.1.6. Un orden de términos es un buen orden.

Prueba. Es fácil de ver que un orden total de términos $\preccurlyeq$ es comparable con $\cdot \mid \cdot$ en el siguiente sentido: Si $t_1 \mid t_2$ entonces $t_1 \preccurlyeq t_2$. Necesitamos demostrar que cada conjunto de términos X no vacío tiene un elemento mínimo. Aplicando el Lema de Dickson y la comparabilidad del orden de términos $\preccurlyeq$, existe $D \subset X$ finito tal que $\forall x \in X \exists d \in D$, d $\preccurlyeq x$. Pero como $\preccurlyeq$ es un orden y D es finito, D contiene un elemento mínimo, digamos m. Ahora es fácil ver que m es un mínimo para X.
Por ejemplo, el orden lexicográfico es un orden de términos.
Otro orden de términos que es interesante: Supongamos que $\alpha_1, \alpha_2, \dots, \alpha_n$ son números reales linealmente independientes sobre $\mathbb{Q}$. Entonces, el mapeo:

$$x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} \to \alpha_1 b_1 + \alpha_2 b_2 + \cdots + a_n b_n$$

es inyectivo e induce un orden de términos.
Si fijamos un orden de términos podemos definir el término principal de un polinomio y desarrollar al algoritmo de la división.
Consideremos un ejemplo. Supongamos que $\preccurlyeq$ es un orden lexicográfico con $y \preccurlyeq x$ y sean $f = x^4 + y^3, g = x^2 + y^2$. El término principal (término más grande respecto de $\preccurlyeq$) de g, es $tp(g) = x^2$. Entonces podemos reducir $f \Rightarrow f_1 = f - x^2 g = -x^2 y^2 + y^3 \Rightarrow f_1 + y^2 g = y^4 + y^3$ y al final obtenemos que $f = (x^2 - y^2)g + (x^4 + y^3)$.

De aquí en adelante vamos a suponer que tenemos un orden de términos fijo.
Dado $f \in k[x]$ denotaremos por tp(f) al término principal de f y por mp(f) al monomio principal de f. Es claro que mp(f) = αtp(f) para un $\alpha \in k$.

Definición 5.1.9. Sean $f, g \in k[x]$ y m un monomio de f. Supongamos que mp(g)|m. El polinomio $f = f - \frac{m}{\text{mp}(g)} g$ se llama reducción en un paso de f por g
y se denota por $f \xrightarrow{g} \tilde{f}$.
El polinomio f se llama terminal por g si mp(g)|m para todos los monomios m de f.

Definición 5.1.10. Sean $G \subset k[x]$ y $f \in k[x]$. Un polinomio $h \in k[x]$ es una reducción de f respecto de G (denotado por $f \xRightarrow{G} h$) si existen polinomios $f = f_0, f_1, \dots, f_k = h$ tales que $f_i \xrightarrow{g} f_{i+1}$ para algún $g \in G$.
Un polinomio h se llama terminal por G si h es terminal por cada $g \in G$.

Proposición 5.1.7: Sea A un anillo conmutativo con unidad y sean I_1, I_2, J, J_1, J_2 ideales en A.

1. Las operaciones entre ideales preservan el orden por inclusión:

si $I_1 \subseteq J_1$ y $I_2 \subseteq J_2$ entonces $I_1 \cap I_2 \subseteq J_1 \cap J_2$, $I_1 I_2 \subseteq J_1 J_2$, $I_1 + I_2 \subseteq J_1 + J_2$

2. Dados $I_1 = \langle f_1, \dots, f_r \rangle$, $I_2 = \langle g_1, \dots, g_m \rangle$, entonces

$I_1 I_2 = \langle f_i g_j, i = 1, \dots, r;\ j = 1, \dots, m \rangle$ y $I_1 + I_2 = \langle f_1, \dots, f_r, g_1, \dots, g_m \rangle$.

3. $J(I_1 + I_2) = JI_1 + JI_2$; $J \cap (I_1 + I_2) = J \cap I_1 + J \cap I_2$; $J + J = J$.

4. $I_1 I_2 \subseteq I_1 \cap I_2$.

5. Si $I_1 + I_2 = A$ entonces $I_1 \cap I_2 = I_1 I_2$.

Prueba de 5. Según el punto 4, basta demostrar que $I_1 \cap I_2 \subseteq I_1 I_2$. Como A tiene unitario, tenemos que $I_1 \cap I_2 = (I_1 \cap I_2)A$. Luego:
$I_1 \cap I_2 = (I_1 \cap I_2)(I_1 + I_2) = (I_1 \cap I_2)I_1 + (I_1 \cap I_2)I_2 \subseteq I_2 I_1 + I_1 I_2 = I_1 I_2$.

Hay una relación importante entre los sistemas de ecuaciones polinomiales y los ideales en k[x].
Sea $I \subset k$[x] un ideal. Podemos considerar soluciones de I, definiendo el conjunto $V(I) \subset k^n$ como sigue:

$$\alpha \in V(I) \Leftrightarrow \forall f \in I, \quad f(\alpha) = 0$$

Proposición 5.1.8: Dado el siguiente sistema de ecuaciones polinomiales

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ f_2(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases}$$

El conjunto de soluciones de este sistema coincide con $V(\langle f_1, \dots, f_m \rangle)$.
La proposición anterior sugiere una aplicación de los ideales a los sistemas de ecuaciones polinomiales: Si $\langle f_1, \dots, f_r \rangle = \langle g_1, \dots, g_m \rangle$, entonces los sistemas $f_i = 0$ $(1 \leq i \leq r)$ y $g_j = 0$ $(1 \leq j \leq m)$ son equivalentes.
Por otro lado, para cada $X \subseteq k^n$ definimos:

$$I(X) = \{ f \in k[x_1, \dots, x_n] \ / \ f(\alpha) = 0 \ \forall \alpha \in X \}$$

Proposición 5.1.9: Se tiene los siguientes resultados en k[x]:
1. $I(X)$ es un ideal en k[x].
2. k[x] es un anillo de ideales principales.

Prueba. Se deja de ejercicio al lector.

Una de las preguntas que vamos a responder en el curso es determinar el conjunto $I(V(I))$. Para esto, primero estudiaremos a los ideales en k[x].

IDEALES EN $k[x_1, \dots, x_n]$
Veremos que los ideales en el anillo de polinomios de varias variables tienen un comportamiento diferente. Por ejemplo, en $k[x, y]$tenemos que $\langle x, y \rangle \neq \langle p \rangle$ para todo $p \in k[x, y]$.
En efecto, si $\langle x, y \rangle = \langle p \rangle$, entonces $x, y \in \langle p \rangle$ y $p \neq 1$. Entonces $x = hp$ e $y = gp$. De aquí, $xy = uhp = xgp$ y por lo tanto $yh = xg$. Luego, $h = xq$ y $g = yq$, lo que implica que $p \in k$ y $\langle p \rangle = k[x, y] \neq \langle x, y \rangle$, lo que es una contradicción). Sin embargo, como sucede con la división de los términos, hay algo bueno con los ideales en $k[x_1, \dots, x_n]$. Todo ideal es finitamente generado.

Proposición 5.1.10: Sea $I \subset k[\mathrm{x}]$ un ideal. Entonces:
$J = I \cap k[x_1, \dots, x_n]$ es un ideal en $k[x_1, \dots, x_n]$., llamado ideal de eliminación de las variables $x_1, x_2, \dots, x_{x-1}$.
Demostración. Se deja de ejercicio al lector.
Existe una relación entre la intersección de dos ideales y los ideales de eliminación.
Proposición 5.1.11: Sean $I_1 = \langle G_1 \rangle$ e $I_2 = \langle G_2 \rangle$ ideales de $k[\mathrm{x}]$. Introducimos una nueva variable z y consideremos $J = \langle zG_1, (1-z)G_2 \rangle$ como ideal de $k[\mathrm{z}, \mathrm{x}]$.
Entonces $I_1 \cap I_2 = J \cap k[\mathrm{x}]$.
Demostración. Primero demostraremos que $I_1 \cap I_2 \subseteq J$. Sea $f \in I_1 \cap I_2$. Podemos escribir $f = zf + (1-z)f$. Como zf es combinación de los elementos de zG_1 y $(1-z)f$ es combinación de los elementos de $(1-z)G_2$, se sigue que $f \in J$.
Ahora veamos que $J \cap k[\mathrm{x}] \subseteq I_1 \cap I_2$. Sea $J \cap k[\mathrm{x}]$. La sustitución $z = 1$ demuestra que $f \in I_1$. La sustitución $z = 0$ demuestra que $f \in I_2$.

IDEALES FINITAMENTE GENERADOS

Dados los polinomios en una variable $f, p_1, p_2, \dots, p_k \in k[\mathrm{x}]$, ¿cómo determinaríamos si $f \in \langle p_1, p_2, \dots, p_k \rangle$? Primero, consideremos $p = \mathrm{med}(p_1, p_2, \dots, p_k) = \mathrm{med}((\dots \mathrm{med}\ (\mathrm{med}\ (p_1, p_2), p_3)\dots), p_k)$.
Observamos que $\langle p \rangle = \langle p_1, p_2, \dots, p_k \rangle$. En efecto, por el algoritmo de Euclides $\mathrm{med}(p_1, p_2) \in \langle p_1, p_2 \rangle$. Por inducción, $p \in (p_1, \dots, p_k)$. Por otro lado $p | p_i$ y, como consecuencia, $p_i \in \langle p \rangle$. Entonces, por la posición 2.1.7. $\langle p \rangle = \langle p_1, p_2, \dots, p_k \rangle$.
Ya es fácil de responder si $f \in \langle p_1, p_2, \dots, p_k \rangle = \langle p \rangle$. En efecto, $f \in \langle p \rangle$ si y solo si $p | f$, lo que podemos determinar usando el algoritmo de la división.
Entonces, si queremos ver si $f \in I$ para un ideal $I \subseteq k[\mathrm{x}]$, primero, podemos presentar $I = \langle p \rangle$, es decir, encontrar una base buena. Después, determinamos si $f \in \langle p \rangle$ usando el algoritmo de la división. Un procedimiento parecido puede aplicarse para ideales en el anillo de polinomios en varias variables. ($f \in I$ si y solo si $f \xrightarrow{(g_1, \dots, g_r)} 0$).
Esta base especial se llama base de Gröbner, la cual vamos a estudiar a continuación.
Fijamos un orden de términos $\preccurlyeq$. Entonces, para cada $g \in k[x_1, \dots, x_n]$ está definido $\mathrm{tg}(g)$. Para un ideal $I \subseteq k[x_1, \dots, x_n]$ definimos:

$$TP(I) = \{tp(f) \ / \ f \in I\}$$

Definición 5.1.11. $\Gamma \subset I$ se llama base de Gröbner de I si para cada $t \in \mathrm{TP}\ (\Gamma)$ existe $\mathrm{g} \in \Gamma$ tal que $\mathrm{tg}(g) | \ t$.

Lema 1. Todo ideal I tiene una base de Gröbner finita. Más aún, para cada base de Gröbner Γ de I, tenemos que $I = \langle \Gamma \rangle$. Además $f \in I$ si y solo si $f \overset{\Gamma}{\Rightarrow} 0$.
Demostración. Por el Lema de Dickson existe $T \subseteq \mathrm{TP}\langle \mathrm{I} \rangle$ finito tal que $\forall t \in TP(I) \quad \exists \pi \in T, r | t$. Elegimos para cada $t \in T$ un $g \in I$ tal que $\mathrm{tp}(g) = t$.
El conjunto de todos estos g forman una base de Gröbner Γ, Tenemos que $\langle \Gamma \rangle \subseteq I$, ya que $\Gamma \subseteq I$. Hay que demostrar que $I \subseteq \langle \Gamma \rangle$. Supongamos que $f \in I$. Por definición de base de Gröbner existe $g \in \Gamma$ tal que $\mathrm{tp}(g) | \mathrm{tp}(f)$. Entonces $f \xrightarrow{g} f_1$ y $f_1 - f = pg \in I$. De aquí $f_1 \in I$. Luego, $f_1 \xrightarrow{g_1} f_2 \xrightarrow{g_2} \dots$ y como $\dots \prec \mathrm{tp}(f_2) \prec \mathrm{tp}(f_1) \prec \mathrm{tp}(f)$, un

argumento inductivo muestra que al final obtenemos cero. Ahora, como $f_i - f_{i+1} \in \langle \Gamma \rangle$ tenemos que $f \in \langle \Gamma \rangle$.
La última afirmación se sigue por las consideraciones anteriores.

Corolario 2: (Teorema de la base de Hilbert).
Todo ideal $I \subseteq k[\mathrm{x}]$ es finitamente generado.
Este teorema afirma que cada sistema infinito de ecuaciones algebraicas es equivalente a un sistema finito. Esto parece a una condición de compacidad. En efecto el Teorema de la base de Hilbert implica la compacidad de k^n en la topología de Zariski que juega un papel importante en geometría algebraica.
Si G genera $I = \langle G \rangle$ y G no es una base de Gröbner para I, puede suceder que $f \in I$ pero que $f \overset{G}{\not\Rightarrow} 0$. Por ejemplo, si $G = \{x^4 + y^3, x^2 + y^2\}$, con el orden lex $y \prec x$. Sabemos que $h = y^4 + y^3 = (x^4 + y^3) + (y^2 - x^2)(y^2 + x^2) \in \langle G \rangle$, pero h es terminal respecto de G. En principio, la reducción de un conjunto G es un análogo del algoritmo de la división. El análogo de los residuos son los polinomios terminales. Haciendo la reducción siempre podemos llegar a un polinomio terminal, porque el orden de términos es un buen orden. También f es "divisible" por un $G \subseteq k[\mathrm{x}]$ si $f \in \langle G \rangle$.
El principio puede suceder que $f \overset{G}{\Longrightarrow} g_1$ y $f \overset{G}{\Longrightarrow} g_2$, donde g_1 y g_2 son terminales y distintos. Sin embargo, cuando G es una base de Gröbner esto no sucede.

Proposición 5.1.12. Sean $G \subseteq k[\mathrm{x}]$ y $g_1, g_2 \in k[\mathrm{x}]$. Si g_1 y g_2 son terminales respecto de G, entonces $\alpha g_1 \pm \beta g_2$ son terminales respecto de G.

Demostración. Como cada g_i es terminal, ningún término de g_i es divisible por un elemento $\mathrm{T}\Gamma(G)$. Por otra parte, todos los términos de $g_1 + g_2$ son términos de g_1 o g_2, de modo que ningún término de $g_1 + g_2$ es divisible por un elemento de $\mathrm{TP}(G)$, lo que implica que $g_1 + g_2$ es terminal respecto de G.

La notación $f \overset{G}{\Longrightarrow} + h$ significa que $f \overset{G}{\Longrightarrow} h$ y h es terminal respecto de G.

Proposición 5.1.13. Sea Γ una base de Gröbner.
1. Si $f \overset{\Gamma}{\Longrightarrow} + g_1$ y $f \overset{\Gamma}{\Longrightarrow} + g_2$, entonces $g_1 = g_2$.
2. $f_1 \overset{\Gamma}{\Longrightarrow} + g$ y $f_2 \overset{\Gamma}{\Longrightarrow} + g$ si y solo si $f_1 + f_2 \in \langle \Gamma \rangle$.

Demostración:
1. Observemos que $g_1 - g_2 \in \langle \Gamma \rangle$ (¿por qué?). Entonces $g_2 \overset{\Gamma}{\Longrightarrow} 0$ por el Lema 3.1.2. Pero $g_1 - g_2$ es terminal por la Proposición 3.1.4. Luego $g_1 - g_2 = 0$.

2. No es difícil ver que si $f \overset{\Gamma}{\Longrightarrow} g$ entonces $f - g \in \langle \Gamma \rangle$ (¿por qué?). Luego, $f_1 \overset{\Gamma}{\Longrightarrow} + g$ y $f_2 \overset{\Gamma}{\Longrightarrow} + g$ implica que $f_1 - g, f_2 - g \in \langle \Gamma \rangle$, . Por lo tanto, $f_1 - f_2 \in \langle \Gamma \rangle$.

El recíproco los demostraremos por contraposición. Supongamos que $f_1 \overset{\Gamma}{\Longrightarrow} g_1$ y $f_2 \overset{\Gamma}{\Longrightarrow} g_2$, $g_1 \neq g_2$. Por la Proposición 3.1.4. $g_1 - g_2$, es terminal y $g_1 - g_2 \notin \langle \Gamma \rangle$. Por lo tanto, $f_1 - f_2 \notin \langle \Gamma \rangle$.
Como una aplicación, consideremos un sistema de ecuaciones polinomiales:

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ f_2(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases}$$

cuyo ideal asociado es $I = \langle f_1, \dots, f_m. \rangle$. Para I construimos una base de Gröbner Γ. La base Γ nos ayudará a responder las siguientes preguntas: ¿El sistema tiene solución? ¿El conjunto de soluciones es finito?

POLINOMIOS SOBRE UN ANILLO Y BASES DE GRÖBNER

A pesar de que nuestro propósito principal es estudiar los polinomios sobre campos, a veces es útil considerar a los polinomios sobre anillos. La utilidad se debe a que los anillos $k[x_1, x_2, \dots, x_n]$ y $k[x_1][x_2, \dots, x_n]$ son isomorfos. En la práctica, cada polinomio $f \in k[x_1, \dots, x_n]$ se puede considerar como elemento de $k[x_1][x_2, \dots, x_n]$; lo que cambia es la representación canónica del polinomio.

Por ejemplo, $f = x^3y^2 + x^3y + x^2y^2 + xy + x + y + 1 \in \mathbb{Q}[x, y]$; si consideramos $f \in \mathbb{Q}[x][y]$ lo escribimos como $f = (x^3+x^2)y^3 + (x^3 + x + 1)y + (x + 1)$.

A continuación, vamos a desarrollar una teoría sobre las bases de Gröbner para polinomios sobre anillos. Sean A un anillo y A[x] el anillo de los polinomios sobre A. Sea $I \subset A$[x] un ideal. Denotaremos por MP(I) al conjunto $\{\text{mp}(f) | f \in I\}$. También tenemos la siguiente definición que es equivalente a la anterior.

Definición 5.1.12

$\Gamma \subset I - \{0\}$ es una base de Gröbner fuerte para I, si para $m \in \text{MP}(I)$ cada existe $g \in \Gamma$ tal que $\text{mp}(g)|m$.

En el caso $A = k$ ambas definiciones son equivalentes, pero para los anillos la divisibilidad de términos y monomios no es lo mismo. También, no todos los ideales de A[x] tienen una base de Gröbner fuerte finita. Pero en el caso de A[x] cuando A es un dominio de ideales principales (DIP)[1] tenemos un análogo del Lema 3.1.2.

Lema 2. Sean A un DIP e $I \subseteq A$[x] un ideal. Entonces I tiene una base de Gröbner fuerte finita Γ. Más aún, $f \in I$ solo si $f \xrightarrow{\Gamma} 0$.

Primero, clarifiquemos, $f \xrightarrow{\Gamma} h$. En este caso, las anteriores sirven también para los polinomios sobre anillos. Pero, en el caso de los anillos la situación es un poco más difícil. Por ejemplo. La proposición 3.1.4. no se satisface para polinomios sobre anillos (¿por qué?). La demostración del Lema 1 es muy parecida a la demostración del Lema 2, pero hay más detalles relacionados con la divisibilidad en el anillo A. Para manejar estos detalles vamos a necesitar varias proposiciones y definiciones.

Definición 5.1.13 Un anillo A se llama Nötheriano si sus ideales satisfacen la propiedad de cadena ascendente, es decir, toda cadena ascendente $I_1 \subseteq I_2 \subseteq \cdots$ de ideales es constante a partir de un $I_n = I_{n+1} = I_{n+2} = \cdots$.

Es posible demostrar que un anillo es Noetheriano si y solo si cada ideal tiene una base (conjunto generador) finita. Luego, el Teorema de Hilbert sobre bases nos asegura que el anillo k[x] es Nötheriano. Sin embargo, nosotros solo necesitaremos el siguiente hecho.

Proposición 5.1.14 Cada dominio de ideales principales (DIP) es un anillo Noetheriano.

Demostración. Supongamos que A es un DIP y $I_1 \subset I_2 \subset \cdots \subset I_x \subset \cdots$ es una cadena ascendente de ideales. Uno puede ver que:

$$I_\infty = \bigcup_{k=1}^{\infty} I_k$$

es un ideal. (En efecto, si $x, y \in I_x$, entonces $x, y \in I_k$ para un k y de modo que $x \pm y \in I_k \subseteq I_\infty$. Las otras propiedades de ideales pueden demostrarse fácilmente).
Como A es un DIP, existe $p \in I_\infty$ tal que $I_\infty = \langle p \rangle$. Pero $p \in I_k$ a partir de un k.
Por lo tanto, $I_\infty = I_k = I_{k+1} = \cdots$.
Recordemos que tenemos fijado un orden de términos. Para $f \in A[\mathrm{x}]$ denotaremos por $\mathrm{tp}(f)$ al término principal de f y por $\mathrm{cp}(f)$ al coeficiente del término principal de f. Para un ideal $I \subset A[\mathrm{x}]$ denotaremos $I(I,t) = \{0\} \cup \{\mathrm{cp}(f) | f \in I \ \mathrm{tp}(f) = t\}$.

Proposición 5.1.15

1. Sea $I \subset A[\mathrm{x}]$ un ideal y t un término, entonces $I(I,t)$ es un ideal en A.
2. Sean $I \subset A[\mathrm{x}]$ un ideal y $t_1 | t_2$ unos términos, entonces $I(I,t_1) \subseteq I(I,t_2)$.

Demostración.

1. Supongamos que $b, c \in I(I,t)$. Entonces $c = \mathrm{cp}(f)$ y $b = \mathrm{cp}(g)$ para algunos $f, g \in I$ con $\mathrm{tp}(f) = \mathrm{tp}(g) = t$. Pero $c \pm b = \mathrm{cp}(f \pm g)$ y $(f \pm g) \in I$ con $\mathrm{tp}(f \pm g) = t$ (si $c \pm b \neq 0$). Tenemos que $c \pm b \in I(I,t)$. También $ab = \mathrm{cp}(ag) \in I(I,t)$ para un $a \in A$.

2. Tenemos que $t_0 = t_0 t_1$ para un término t_0. Sea $b \in I(I,t_1)$. Entonces $b = \mathrm{cp}(f)$ para un $f \in I$ con $\mathrm{tp}(f) = t$. Pero $t_0 f \in I$ y $\mathrm{tp}(t_0 f) = t_0$. Luego $b \in I(I,t_2)$.

Las siguientes definiciones son aplicables para todo orden, parcial, pero nosotros vamos a necesitar un solo orden parcial a saber, la divisibilidad de términos.

Definición 5.1.14. Un conjunto de términos T se llama cadena si par cada $t_1, t_2 \in T$ se tiene que $t_1 | t_2$ o $t_2 | t_1$. En otras palabras, T es totalmente ordenado por $\cdot \mid \cdot$.
Un conjunto de términos T se llama anticadena si para cada $t_1, t_2 \in T$ tenemos que $t_1 | t_2$ o $t_2 | t_1$. En otras palabras, una anticadena es un conjunto de elementos incomparables respecto de $\cdot \mid \cdot$.
El lema de Dickson implica el siguiente resultado,

Proposición 5.1.15. Todas las anticadenas de términos de n variables son finitas.
Demostración. Una anticadena infinita sería una contradicción al Lema de Dickson.

Lema 3 (Lema de König). Sea T un conjunto de términos de n variables. Si todas las cadenas dentro de T son finitas, entonces T es finito.
Prueba. Una cadena $C \subset T$ se llama maximal si no existe otra cadena $C' \subset T$ tal que $C \subseteq C'$. Supongamos que C_1, C_2 son dos cadenas maximales de T.
Denotaremos por $c_i = \mathrm{máx}(C_1)$ al elemento maximal de C_i (estos elementos existen porque cada C_i, es infinito). Uno puede ver que c_1 y c_2 son iguales o incompatibles. (En efecto, si, por ejemplo, $c_1 | c_2$, entonces $C_1 \cup \{c_2\}$ es una cadena, lo que contradice la maximilidad de C_1. Entonces, el conjunto $M = \{\mathrm{máx}(C) | C$ es una cadena maximal de $T\}$

es una anticadena. Por otra parte, $T \subseteq \{t|\exists m \in M, t|m\}$. Pero el conjunto $\{t|\exists m \in M, t|m\}$ es finito.

Demostración. Sea $I \subset A[\mathrm{x}]$ un ideal. Definimos el conjunto de términos $T = \{t|\exists t' \text{tal que } t|t' \wedge I(I,t) \neq I(I,t')\}$. Todas las cadenas de T son finitas por las proposiciones 3.2.4 y 3.2.5. Entonces, por el Lema de König, T es finito $t \in T$. Para sea $I(I,t) = \langle a_t \rangle$. Entonces, existe $g_t \in I$ tal que tp(g_t) = t y cp(g_t) = a_t (¿por qué?). Ahora, $\Gamma = \{g_t|t \in T\}$ es una base de Gröbner fuerte.

HOMOMORFISMO DE ANILLOS BASES DE GRÖBNER

Supongamos que $\emptyset: R_1 \to R_2$ es un homomorfismo $\emptyset$ de anillos. El homomorfismo tiene el levatamiento natural (que vamos a denotar por el mismo símbolo $\emptyset$) hasta el homomorfismo $\emptyset$: $R_1[\mathrm{x}] \to R_2[\mathrm{x}]$, que está definido como $\emptyset(\alpha_1 \mathrm{x}^{a_1} + \alpha_2 \mathrm{x}^{a_2} + \cdots) = \emptyset(\alpha_1)\mathrm{x}^{a_1} + \emptyset(\alpha_2)\mathrm{x}^{a_2} + \cdots$.

Un elemento $0 \neq b$ del anillo R se llama divisor de cero si existe $0 \neq a \in R$ tal que $ab = 0$.

Proposición 5.1.16. Sean R_1 y R_2 anillos, y sea Γ una base de Gröbner fuerte para un ideal $I \subseteq R_1[\mathrm{x}]$. Si $\emptyset: R_1 \to R_2$ es un homomorfismo suprayectivo tal que $\emptyset(\alpha)$ no es 0 y tampoco es un divisor de cero para todo $\alpha \in \mathrm{MP}(\Gamma)$, entonces $\emptyset(\Gamma)$ es una base de Gröbner fuerte para $\emptyset(I)$.

Demostración. Como $\emptyset$ es suprayectivo, $\emptyset(I)$ es un ideal de $R_2[\mathrm{x}]$. El resultado se sigue fácilmente de la siguiente afirmación.

Afirmación**.** Para cada $h \in \emptyset(I)$ existe $f \in I \cap \emptyset^{-1}(h)$ tal que $\mathrm{tp}(f) = \mathrm{tp}(h)$.

En efecto, la afirmación implica $\mathrm{mp}(h)$ que es divisible por $\mathrm{mp}(\emptyset(g)) = \emptyset(\mathrm{mp}(g))$ para un $g \in \Gamma$ tal que $\mathrm{mp}(g)|\mathrm{mp}(f)$. Entonces, basta demostrar la afirmación. Lo haremos por contradicción. Sea $h \in \emptyset(I)$ y supongamos que para todo $f \in I$, con $h = \emptyset(f)$ tenemos que $\mathrm{tp}(h) \neq \mathrm{tp}(f)$. Entre estos f elegimos uno que tiene el menor término principal, digamos f_m. Tenemos que $\emptyset(\mathrm{mp}(f_m)) = 0$. Por otra parte, podemos eliminar $\mathrm{mp}(f_m)$ por un $g \in \Gamma$: $f' = f_m - \frac{\mathrm{mp}(f_m)}{\mathrm{mp}(g)} g$. Pero no $\emptyset\left(\frac{\mathrm{mp}(f_m)}{\mathrm{mp}(g)}\right) = 0$ ($\emptyset(\mathrm{mp}(g))$ es un divisor de cero). Entonces $\emptyset(f') = h$, lo que contradice la minimalidad de f_m.

Proposición 5.1.17. Dado el ideal I en $\mathbb{K}[x_1, \ldots, x_n]$ y sea $\beta = \{f_1, f_2, \ldots, f_r\}$ una base de Gröbner para un ideal I, entonces se cumple que:

1. Si ϕ es un subconjunto finito de polinomios no nulos de I entonces $\beta \cup \phi$ también es base de Gröbner para I.
2. $\psi = \{c_1 f_1, \ c_2 f_2, \ldots, c_r f_r\}$ también es base Gröbner para I.
3. $I = \langle f_1, f_2, \ldots, f_r \rangle$

Prueba. La prueba de estos resultados se obtiene directamente de la definición.

Definición 5.1.15

Un subconjunto $\beta = \{f_1, f_2, \ldots, f_r\}$ de $\mathbb{K}[x_1, \ldots, x_n]$ es una base de Gröbner si y solo es una base de Gröbner para el ideal que genera β, es decir una base de Gröbner para $\langle \beta \rangle$.

Proposición 5.1.18

Sea $\beta = \{f_1, f_2, \ldots, f_r\} \subset \mathbb{K}[x_1, \ldots, x_n]$ y h en $\mathbb{R}[x_1, \ldots, x_n] - \{0\}$, entonces:
β es una base de Gröbner si y solo si $\{hf_1, \ hf_2, \ldots, hf_r\}$ es base de Gröbner.

CÁLCULO DE BASES DE GRÖBNER.

Tenemos que si $F = \{f_1, \dots, f_n\}$ y $f \in \mathbb{K}[x_1, \dots, x_n]$, entonces:

1.- El algoritmo de la división produce polinomios $u_1, u_2, \dots, u_s; r \in \mathbb{K}[x_1, x_2, \dots, x_n]$ tales que

$$f = u_1 f_1 + \cdots + u_s j_j + r$$

con: r reducido respectivo F y

$$lp(f) = max\Big(\max_{1 \le i \le s} \big(|p(u_i)|p(f\ )\big), |lp(x)\Big).$$

2. Tener en cuenta que sí
$X = x_1^{\alpha_1} \dots x_n^{\alpha_n}$, $Y = x_1^{\beta_1} \dots x_n^{\beta_n}$ están en $\mathbb{K}[x_1, \dots, x_n]$
entonces

$mcm(x, y) = x_1^{m_1} \dots x_n^{m_n}$, $mcd(x, y) = x_1^{\rho_1} \dots x_n^{\rho_n}$
donde $m_i = máx\{\alpha_i, \beta_i\}$ y $\rho_i = min\{\alpha_i, \beta_i\}$: $\forall i \in \{1,2, \dots, n\}$.
Mas aún, si x, y satisfacen que $mcd(x, y) = 1$, decimos que
X e Y son relativamente primos.

Definición 5.1.16:
Sean $f, g \in \mathbb{K}[x_1, x_2, \dots, x_n]$ polinomios no nulos y $M = mcm\big(lp(f), lp(g)\big)$. Entonces, el polinomio siguiente:

$$s\big(f,g\big) = \frac{M}{lt(f)} f - \frac{M}{lt(g)} g$$

es llamado **"s-polinomio de f y g"**.

Ejemplo: Sean $f(x, y) = 2yx - y$, $g(x) = 3y^2 - x$ en $Q[x, y]$ con el orden deglex con $y > x$. Entonces:
$L = y^2 x$ y $S(f, g) = \frac{y^2 x}{2yx} f - \frac{y^2 x}{3y^2 g}$

$$S(f, g) = \frac{1}{2} yf - \frac{1}{3} xg = -\frac{1}{2} y^2 + \frac{1}{3} x^2$$

Además: $lp\left(\frac{1}{2} yf\right) = y^2 x = lp\left(\frac{1}{3} xy\right)$.

Nota:
Sean f, g no nulos

1. $f = lt(f)$ y $g = lt(g)$ entonces $S(f, g) = 0$
2. $S(f, g) = S(f, -g)$

Proposición 5.1.19: (Teorema Buchberger)
Sea $G = \{f_1, f_2, \dots, f_t\} \subset \mathbb{K}(x_1, \dots, x_n) - \{0\}$. Entonces G es una base de Gröbner para $I = \langle f_1, f_2, \dots, f_i \rangle$ si y solo si $S(f_i, f_j) \xrightarrow{G} 0$ para $i \neq j$.
Pero entonces, surge una pregunta natural:
¿Cómo calcular las bases de Gröbner para un ideal a partir de un conjunto finito de generadores?

ALGORITMO DE BUCHBERGER

El siguiente algoritmo, llamado Algoritmo de Buchberger, nos permite calcular las bases de Gröbner, de la siguiente manera:

Dados $F = \{f_1, f_2, \dots, f_s\} \subset \mathbb{K}[x_1, \dots, x_n]$ donde $fi \neq 0,\ 1 \leq i \leq s$ obtendremos $G = \{g_1, \dots, g_r\}$ una base de Gröbner pasa $\langle f_1, f_2, \dots, f_r \rangle$.
1°) Llamemos $G \coloneqq F, \mathcal{G} = \{f_i, f_j\} \quad / \quad fi \neq fj$ en $\mathcal{G}$.
2°) Mientras $\mathcal{G} \neq \phi$, hacemos lo siguiente:
1.- Escoger cualquier por $\{f, g\} \in \mathcal{G}$
2.- $\mathcal{G} \coloneqq \mathcal{G} - \{\{f, g\}\}$
$S(f, g) \xrightarrow{G} h$ donde: h es reducido respecto a G
Si $h \neq 0$, entonces
$\mathcal{G} \coloneqq \mathcal{G} \cup \{\{u, h\}/\forall u \in G\}$
$\mathcal{G} \coloneqq \mathcal{G} \cup \{h\}$
Fin si
Fin mientras

Teorema 5.1.20. Dado $\beta = \{f_1, f_2, \dots, f_s\}$ con $f_i \neq 0; \quad \forall i, 1 \leq i \leq s$
El algoritmo de Buchberger produce una base de Gröbner para el ideal $J = \langle f_1, f_2, \dots, f_s \rangle$
Prueba:
Notamos que siguen el algoritmo de Bucberger, cada β_i es $\beta_{i-1} \cup \{h\}$ donde $h \in I$ y es la reducción no nula con respecto a β_{i-1}, de un s-polinomio de dos elementos de β_{i-1}.
Como h es reducido con respecto a β_{i-1}, tenemos que $lt(h) \notin lt(\beta_{i-1})$.
Así si el algoritmo no terminara. Entonces la cadena siguiente es creciente e infinita

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

éste que implicaría que $\mathbb{k}[x_1, \dots, x_n]$ no es Notheriano; lo que es un absurdo.
Observación:
1.Tenemos que $F \subseteq G \subseteq I$, luego $I = \langle f_1, f_2, \dots, f_s \rangle \subseteq \langle g_1, g_2, \dots, g_t \rangle \subseteq I$.
Además, si g_i, g_i son polinomios en G, entonces $S(g_i, g_i) \xrightarrow{G} 0$ por construcción.
2. Las bases de Gröbner obtenidos por el algoritmo de Buchberger no son únicas.

BASES DE GRÖBNER REDUCIDAS

Definición 5.1.17:(Base de Gröbner Reducidas)
Una base de Gröbner $G = \{g_1, g_2, \dots, g_m\}$ es llamado mínima si para todo i, $lc(gi) = 1$ y para todo $i \neq j$ $lp(gi) \nmid$ a $lp(g_j)$.
Nota:
1. Si $G = \{f_1, f_2, \dots, f_t\}$ es una base de Gröbner para un ideal I y si $lp(f_2)|lp(f_1)$ entonces $\{f_2, \dots, f_t\}$ es también base de Gröbner para I.

2. Si $G = \{f_1, f_2, \dots, f_t\}$ es base de Gröbner para I. Una base de Gröbner mínima se obtiene de G eliminando todos los gi tales que $|p(gi)|lp(gi)$ para $j \neq i$. Luego, dividimos los restantes gi por $lc(gi)$.
3. Una base de Gröbner mínima para un ideal, es única.

Definición 5.1.18:
Una base de Gröbner $G = \{g_1, g_2, \dots, g_r\}$ es llamada una base de **Gröbner Reducida** si y solo si para todo $1 \leq i \leq r$, $lc(gi) = 1$ y gi es reducido con respecto a $G - \{gi\}$.
Es decir: Para todo i, ningún término no nulo en gi es divisible por $lp(g_j)$ para todo $j \neq i$.
Nota:
1. Si $F = \{f_1, \dots, f_t\}$ y $H = \{h_1, h_2, \dots, h_r\}$ son base de G mínimas para el ideal entonces $t = r$ y $lt(hi) = lt(gi)\ \forall i = 1, 2, \dots, r$ (reordenando si es necesario).

2. También $G = \{g_1, g_2, \dots, g_r\}$ una base de Gröbner mínima para el ideal I, consideremos el siguiente proceso de reducción:
Si tenemos dos bases de Gröbner mínimos para el ideal J. Además $\{y, x\}$ es reducida y $\{y + x, x\}$ no lo es, pues $y + x \xrightarrow{x} y$.
$g_1 \xrightarrow{F_1} f_1$, donde f_1 es reducido con respecto a $F_1 = \{g_2, \dots, g_r\}$
$g_2 \xrightarrow{F_2} f_2$, donde f_2 es reducido con respecto a $F_2 = \{f_1, g_3, \dots, g_r\}$
$g_3 \xrightarrow{F_3} f_3$, donde f_3 es reducido con respecto a $F_3 = \{f_1, f_2, g_4, \dots, g_r\}$

Luego después obtener
$g_r \xrightarrow{F_r} f_r$ donde f_r es reducido con respecto a $F_r = \{f_1, f_2, \dots, f_r\}$
Entonces:
$F = \{f_1, f_2, \dots, f_r\}$ es una base de Gröbner reducido para I.

Teorema 5.1.21:
Determinado un orden de términos, entonces todo ideal no nulo I tiene una única base de Gröbner reducida respecto a ese orden.

Prueba:
Por el resultado anterior tenemos la existencia, falta ver la unicidad
tenemos coordenados $F = \{f_1, \dots, f_t\}$ y $H = \{g_1, g_2, \dots, g_t\}$ dos bases de Gröbner reducidas para I.

Como F y G son mínimas, entonces para cada i, $lt(fi) = lt(gi)$ y además $lp(fi - gi) < lp(gi)$ supongamos que $gi \neq hi$ para algún i_0; como
$fi_0 - gi_0 \in I$, existe tal que $lp(gj_0)$ divide al $lp(fi_0 - gi_0)$,
$lp(gj_0) \leq lp(fi_0 - gi)$ con $j_0 \neq i_0$ pero $lp(gj_0) = lp(fj_0)$ dividirá a algún término de fi o gi, pero es un absurdo pues G y H son reducidas. Entonces $fi = gi$.

Ejemplo:
Dado $I = \langle f_1, f_2, f_3 \rangle \subset Q[x, y]$ donde $f_1 = y^2 + yx + x^2$; $f_2 = y + x$,
$f_3 = y$. Usaremos el orden lex con $y > x$, podemos calcular una base de Gröbner por I , como sigue:

$$F = \{\ y^2 + yx + x^2, \quad y + x, \quad y, \quad x^2, \quad x\ \}$$

Removiendo $y^2 + yx + x^2, y + x, y, x^2$ obtenemos $\{y, x\}$ y
removiendo $y^2 + yx + x^2, y, x^2$ obtenemos $\{y + x, x\}$.

5.2 Resultados inferenciales

En esta sección mostramos un algoritmo basado en la teoría de uno de los problemas matemáticos más difíciles que es la teoría de polinomios en varias variables. Este criptosistema es asimétrico alternativo a unos de los sistemas mas fuertes como lo es el criptosistema RSA, es un criptosistema de clave publica, fue creado por Ron Rivest, Adi Samir y Leonard Adleman, en 1977 cuya fortaleza está basada en resultados algebraicos de teoría de módulos, en los teoremas de Euler, el teorema de Fermat y la descomposición de un entero grande en números primos grandes. Entiéndase por un numero primo grande aquel número entero que se sabe que es primo y tiene millones de dígitos

LOS CRIPTOSISTEMAS EN POLINOMIOS EN VARIAS VARIABLES

Los criptosistemas de Polly Cracker, es una familia de criptosistemas asimétricos, de clave pública que se fundamenta en la Teoría de Bases de Gröbner de un ideal del anillo de polinomios de varias variables $\mathbb{K}[x_1, x_2, \dots, x_n]$. Consiste en lo siguiente:

Dado un elemento $v \in \mathbb{K}^n$, se considera subconjunto de polinomios de $\mathbb{K}[x_1, x_2, \dots, x_n]$, digamos que consideramos $\{f_1, f_2, \dots, f_r\}$ un conjunto de polinomios tal que $I = \langle f_1, \dots, f_r \rangle$ tales que $v \in V(I)$ es decir que $f(v) = 0\ \forall f \in I$.
Luego $F = \langle f_1, \dots, f_r \rangle$ se toma como la clave pública y $v \in \mathbb{K}^n$ es la clave privada, del receptor.
Si alguien quiere mandar un mensaje m al receptor, debe cifrar ese mensaje usando la clave pública F del receptor.
Para ello elije un polinomio $q \in I = \langle f_1, \dots, f_r \rangle$ y cifra el mensaje m así:

$$M = q + m$$

El receptor lee el mensaje y evalúa M en v , entonces

$$M(v) = q(v) + m = 0 + m = m$$

La fortaleza de este criptosistema se basa en la dificultad de encontrar el cero v tal que $I(v) = 0$, para I que es dado públicamente. Es decir, se basa en resolver el sistema de ecuaciones polinomiales.

El seleccionar el conjunto $F = \{f_1, \dots, f_r\}$ de polinomios debe ser tal que el sistema de ecuaciones polinomiales no sea fácil ni rápidas de calcular en tiempo polinomial.

La idea es construir ideales que produzcan combinaciones tal que sea complicado de calcular sus bases de Gröbner, la seguridad de este sistema criptográfico se basa en la dificultad de calcular bases de Gröbner.

Ahora mostraremos una variación de este criptosistema que consiste en lo siguiente:

CRIPTOSISTEMA DE POLLY CRACKER MODIFICADO

Este es un criptosistema de clave pública basado en las bases de Gröbner de un ideal de anillo de polinomios $\mathbb{K}[x_1, x_2, \dots, x_n]$. Consiste en lo siguiente consideremos un emisor y un receptor. La clave pública la genera de la siguiente manera: Elige los siguientes polinomios al azar: $g_1, g_2, \dots, g_r$ y calcula:

$$fi = g_1 - g_i(v); \text{ para } i = 1,2, \dots, r$$

donde $v \in \mathbb{K}^n$. Entonces la clave pública del receptor es $F = \{f_1, f_2, \dots, f_r\}$ y v será su clave privada.

Como el emisor tiene acceso a $F = \{f_1, f_2, \dots, f_r\}$, lo aplicara para encriptar el mensaje. Digamos que $m \in k$ es el mensaje. Toma F y considera $q_1, q_2, \dots, q_r$ polinomios en $\mathbb{K}[x_1, x_2, \dots, x_n]$ y calcula

$$M = \sum_{i=1}^{r} q_i \, f_i + m$$

M será el mensaje encriptado, que un nuevo polinomio y es enviado públicamente al receptor.

El receptor, una vez recibido el mensaje M, para descifrarlo evalúa M en su clave secreta v.Entonces

$$\begin{aligned} M(v) &= \sum_{i=1}^{r} q_i(v) \, f_i(v) + m \\ &= \sum_{i=1}^{r} q_i(v) \, . \, 0 + m \\ &= m \end{aligned}$$

$M(v) = m$ que el mensaje que el emisor envió.

Ejemplo de Aplicación:

Consideraremos que Betty tiene la siguiente clave privada $v = (1,2) \in \mathbb{R}^2$ y para generar su clave pública considera los siguientes polinomios.

$$g_1(x,y) = xy^2 - y + 2x^2 - 1$$
$$g_2(x,y) = x^2 + xy + 2x + 3$$

Evalúa, $g_1(1,2) = 3$, $g_2(1,2) = 8$. Entonces define

$$f_1(x,y) = g_1(x,y) - g_1(1,2) = xy^2 - y + 2x^2 - 4$$
$$f_2(x,y) = g_2(x,y) - g_2(1,2) = x^2 + xy + 2x - 5$$

Entonces

$$F = \{f_1, f_2\} = \{xy^2 - y + 2x^2 - 4, x^2 + xy + 2x - 5\}$$

es su clave pública.
Betty la comparte su clave pública.
Ahron desea mandarle un mensaje a Betty. El mensaje que Ahron quiere enviar a Betty es $m = 41$.
Para enviar el mensaje a Betty, Ahron utilizará la clave pública de Betty.
Entonces va tomar un par de polinomios, digamos $q_1(x,y) = x^2y$,
$q_2(x,y) = -x \in \mathbb{R}[x,y]$ y encripta el mensaje de la siguiente manera:

$$M = q_1f_1 + q_2f_2 += (x^2y)(xy^2 - y + 2x^2 - 4) + (-x)(x^2 + xy + 2x - 5)$$

Entonces

$$M = x^3y^3 - x^2y^2 + 2x^4y - 4x^2y - x^3 - x^2y - 2x^2 - 5x + 41$$

$$M = x^3y^3 - x^2y^2 + 2x^4y - 5x^2y - x^3 - 2x^2 + 5x + 41$$

Ahora envía este mensaje públicamente.
Betty ve la publicación y para descifrarlos evalúa M en $v = (1,2)$, así:

$$M(1,2) = (1)(8) - (1)(4) + (2)(2) - (5)(2) - 1 - 2 + 5 + 41 = 41$$

$$\therefore M(1,2) = 41 = m$$

En conclusión, el criptosistema algebraico Polly Crackr que fue seguido por Fellows y Koblitz consiste en lo siguiente:
Sea $P = \mathbb{K}[x_1, \dots, x_n]$ un anillo conmutativo polinomios y consideramos los polinomios $f_1, f_2, \dots, f_s \in P$ que $v = (a_1, a_2, \dots, a_n) \in \mathbb{K}^n$ como un cero en común.

Entonces

Clave pública: $f_1, f_2, \dots, f_s$

Clave privada: $(a_1, a_2, \dots, a_n)$

Cifrado: Un texto plano $m \in \mathbb{K}$ es cifrado

Así:

$M = f_1 g_1 + f_2 g_2 + \cdots + f_s g_s$

donde $g_1, g_2, \ldots, g_s \in P$

Descifrado: Se evalúa M en $(a_1, a_2, \ldots, a_n)$ y se obtiene $m = M(a_1, \ldots, a_n)$

Seguridad: El hacker puede romper el cripto sistema si logra calcular la base de Gröbner de $I = \langle f_1, \ldots, f_s \rangle$.

5.3. Otro tipo de resultados de acuerdo con la naturaleza del problema

ATAQUES AL CRIPTOSISTEMA

Este criptosistema de Polly Cracker, presenta algunas debilidades o inconvenientes de seguridad, pues es posible romper su seguridad sin necesidad de la complejidad de usar bases de Gröbner. El criptoanálisis de este criptosistema es posible mediante el uso de ataques que usan teorías algebraicas más simples las bases de Gröbner para romper el sistema. Por ejemplo:

1.Ataque basado en Álgebra Lineal básica

Los hackers saben que se tiene esto:

$$M = m + f_1 g_1 + f_2 g_2 + \cdots + f_s g_s$$

Si consideramos los coeficientes de $g_1, g_2, \ldots, g_s$ como desconocidos y todos los coeficientes de los términos no constantes en la ecuación

$$f_1 g_1 + f_2 g_2 + \cdots + f_s g_s$$

son conocidas. Entonces estamos frente a un sistema de ecuaciones lineales.

Por lo tanto, se podemos resolver.

2.Ataque “inteligente” de Álgebra Lineal

Se puede adivinar los términos t que se tiene en supp (g_i) porque algunos de los términos en t. supp (f_i) se encuentra en Supp (M) si no hay mucha cancelación.

CAPITULO VI: DISCUSIÓN DE RESULTADOS

6.1 Contrastación y demostración de la hipótesis

De la teoría desarrollada en este trabajo, de la información vertida y analizada; y de los resultados obtenidos, hemos podido demostrar la hipótesis planteada al inicio de la investigación, pues hemos mostrado un criptosistema de clave pública, generado a partir de las bases de Gröbner de un ideal del anillo de polinomios de varias variables. Para

ello hemos definido un orden y una divisibilidad en el anillo de polinomios en varias variables, lo mismo que nos ha permitido establecer una base de Gröbner reducida única la cual se usa como clave secreta para descifrar un mensaje encriptado por una clave pública que es un conjunto de polinomios que serán generadores de un ideal I en el anillo de n variables.

6.2 Contrastación de los resultados con otros estudios similares

La seguridad de enviar información por internet es un problema latente actualmente; son muchos y variados los trabajos o investigaciones que se han realizado, se realizaran y se están realizando con este fin. Los sistemas criptográficos que se investigan actualmente son de clave pública o híbridos basados en problemas matemáticos difíciles, como lo es la factorización en números primos grandes, pues la dificultad es lograr los números primos grandes que siempre ha sido un problema. En el presente trabajo el objetivo ha sido mostrar que es posible crear nuevos sistemas criptográficos basados en un problema matemático difícil, diferente de la factorización en números primos; como es el de determinar una base de Gröbner de un ideal en el anillo de polinomios de varias variables resolver sistemas ecuaciones polinomiales. Que es importante de tener pues se trata de conseguir criptosistemas resistentes a ordenadores cuánticos.

6.3 Responsabilidad ética.

La presente investigación ha sido elaborada autora y se ha desarrollado con responsabilidad ética, por ende, la autora se responsabiliza por el contenido de este informe.

CONCLUSIONES

Contar con un sistema finito de generadores de un ideal del anillo de polinomios de n variables, permite determinar un criptosistema diferente a los conocidos, porque su fortaleza no se basa en factorización de enteros en primos, por lo que sería resistente al algoritmo de Shor y por tanto a ordenadores cuánticos.

En el anillo de polinomios de varias variables es posible determinar un cierto orden total, tener una generalización del algoritmo de división para polinomios en n variables, lograr una cierta divisibilidad y poder definir las Bases de Gröbner.

El uso de Bases de Gröbner reducidas nos permite determinar nuevos criptosistemas asimétricos cuya clave pública es un conjunto de polinomios, que serán los generadores de un ideal y cuya base de Gröbner reducida será la clave privada; su fortaleza se encuentra en la dificultad de trabajar con polinomios de varias variables y determinar su base de Gröbner.

RECOMENDACIONES

Es importante seguir buscando criptosistema basados en otros problemas matemáticos difíciles, ya no, basados en factorización de enteros pues con la pronta aparición de ordenadores cuánticos se vería vulnerada la seguridad en internet.

Es importante continuar con el estudio en algoritmo basados en polinomios, con el fin de mejorarlos, pero cuidando que no sea posible vulnerarlo con teorías más sencillas como en el caso estudiado que se conocen ataques con algebra lineal. Poe ejemplo sobre cuerpos finitos aplicando algebra conmutativa.

REFERENCIAS BIBLIOGRÁFICAS

Adams, W., Loustaunau, F. (1996) *An Introduction to Gröbner Bases* . USA: Board.

Buchberger, B.(2011)*Gröbner bases and Aplications*. London: Cambridge University Press.

Buchberger, B., & Winkler, F. (Eds.). (1998). *Gröbner bases and applications* (Vol. 17). Cambridge: Cambridge University Press.

Burton, D. M. (1970). *A first course in rings and ideals* (Vol. 731). Addison-Wesley.

Cox, D. A., Sturnmfels, B. (1998)*Introduction to Gröbner bases. Applications of Computational Algebraic Geometry* Proceedings of Symposia in Applied Mathematics,Vol. 53, AMS, Providence, Rhode Island.

de Frutos Fernández, M. I. (2014). el problema del logaritmo discreto para curvas elípticas y sus aplicaciones criptográficas.

Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (Vol. 3). Hoboken: Wiley.

Escobar Benet, M. (2015). Criptografía en clave pública y privada. RSA.

Faugère, J. C. (2002, July). A new efficient algorithm for computing Gröbner bases without reduction to zero (F 5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation* (pp. 75-83).

Gröbner Bases and Applications. London Mathematical Society Lecture Note Series. Cambridge University Press, 1998.

Herstein, I. N. (1988). *Algebra abstracta* (No. 512.8 H4Y).

Koblitz, N.(1994) A course in *Numbers Theory and Cryptography*. USA:Springer-Verlang.

Koblitz, N., & Menezes, A. J. (2006). *otra mirada a "seguridad demostrable". ii.*

Leyva, Mark. (2016). *"Los Sistemas de Ecuaciones Polinomiales y Polinomios Simétricos sobre bases de Gröbner".* Lima. Universidad Nacional de Ingeniería

Linde Díaz, J. (2019). *Métodos algebraicos en criptografía multivariable* (Doctoral dissertation, Universidad Complutense de Madrid).

Mantilla Cabrera, C. E. (2018). *Análisis de algoritmos criptográficos clásicos vs algoritmos cuánticos* (Master's thesis, Escuela Superior Politécnica de Chimborazo).

Marca, G. (2008):" *Bases de Gröbner con aplicaciones al álgebra conmutativa"* Lima: Universidad Nacional de Ingeniería.

Martin Albrecht and Martin Albrecht. Algorithmic Algebraic Techniques and their Application to Block Cipher Cryptanalysis. PhD thesis, 2010.

Montaño Machacón, J. C. (2015). Algoritmos de encriptación: Análisis del problema de la factorización prima en el método RSA de clave pública-Algoritmo de Shor.

Moreno Centeno, D. (2019). Criptografía Post-cuántica: Implementación de McEliece y una nueva versión.

Oviedo, P. A. (2017). *Fundamentos Matemáticos de Computación Cuántica en el Algoritmo de Shor, para la factorización prima de números enteros* (Doctoral dissertation, UNIVERSIDAD ABIERTA INTERAMERICANA).

Ramió, J. (2006). Libro electrónico de seguridad informática y criptografía, versión 4.1.Disponible en: http://www.criptored.upm.es/guiateoria/gt_m001a.htm

Ramió, J. (2016). Introducción a la seguridad informática y la cristología clásica. Disponible en:http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/leccion1.htm

Scarone Etchamendi, B. (2018). Criptografía post cuántica basada en reticulados: fundamentos teóricos y sistemas de clave pública.

Verdu, S. (1998). Fifty years of Shannon theory. *IEEE Transactions on information theory*, *44*(6), 2057-2078.

Profesora Responsable:

……

Mg. RUTH MEDINA APARCANA

C.D. 1428

ANEXOS

MATRIZ DE CONSISTENCIA

Problema	**Objetivo**	**Hipótesis**	**Operacionalización de Variables**			**Diseño Metodológico**
			Variable	**Dimensión**	**Indicador**	
General ¿Cuál es la forma de obtener algoritmos criptográficos usando bases de Gröbner?	**Objetivo General** Describir la forma de obtener un algoritmo criptográfico aplicando bases de Gröbner	**General** Las bases de Gröbner permiten determinar algoritmos criptográficos.	INDEPENDIENTE Base de Gröbner	Base minimal	Divisibilidad generalizada para los polinomios en varias variables	Es de tipo analítico y descriptivo, no experimental y transversal. Se ha empleado el método deductivo- analítico. Tiene como población o universo el conjunto de todos los sistemas criptográficos, La muestra sería los sistemas criptográficos basados en fundamentos algebraicos
Problemas Específicos **¿**Cuáles son las características de una base de Gröbner? ¿Cuáles son las condiciones para que existan las bases de Gröbner? ¿Cuál es la función de las bases d Gröbner en el criptosistema?	**. Específicos** 1. Describir las características de las bases de Gröbner respecto a la relación de orden. 2.Determinar las condiciones de existencia de las bases de Gröbner. 3.Determinar la función de las bases de Gröbner en el criptosistema.	**Especificas** 1.Los sistemas de generadores de un ideal contenido en un anillo de polinomios de varias variables aportan la construcción de las bases de Gröbner. 2.Bajo condiciones divisibilidad es posible definir las bases de Gröbner respecto al orden. 3. El funcionamiento del criptosistema está basado en que la clave pública del criptosistema es el ideal, del cual se conoce la base de Gröbner.	DEPENDIENTE criptosistema	Clave publica	Criptosistema asimétrico cuya clave pública y clave secreta se basa en teoría de polinomios	