UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

SECCIÓN DE MATEMÁTICA.

TEMA:

ANILLOS EUCLIDIANOS Y TEOREMAS FUNDAMENTALES

PRESENTADO POR:

ANDRES MARTINEZ ORELLANA

ANA LUZ MEJIA MUNGUIA

ASESOR DIRECTOR:

MSc. JORGE ALBERTO MARTINEZ GUTIERREZ

PARA OPTAR AL GRADO DE:

LICENCIADO EN MATEMÁTICA

SEPTIEMBRE 2014

SAN MIGUEL, EL SALVADOR, CENTROAMERICA

UNIVERSIDAD DE EL SALVADOR.

RECTOR: ING. MARIO ROBERTO NIETO LOVO.

VICE-RECTORA ACADEMICA: Msc. ANA MARÍA GLOWER DE ALVARADO

SECRETARIA GENERAL: DRA. ANA LETICIA ZAVALETA DE AMAYA

FACULTAD MULTIDISCIPLINARIA ORIENTAL.

DECANO: LIC. CRISTÓBAL HERNÁN RÍOS BENÍTEZ.

VICE-DECANO: LIC. CARLOS ALEXANDER DIAZ.

SECRETARIO: LIC. JORGE ALBERTO ORTEZ HERNÁNDEZ.

ADMINISTRADOR ACADEMICO: LIC. EDWIND JEOVANNY TREJOS CABRERA

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA.

JEFE: M.EST. JOSÉ ENRY GARCÍA.

SECCIÓN DE MATEMÁTICA.

COORDINADOR: ING. DOLORES BENEDICTO SARAVIA.

TRABAJO DE GRADUACION APROBADO POR:

MSc. OSCAR ULISES LIZAMA VIGIL.

Coordinador de Procesos de Graduación.

Depto. Ciencias Naturales y Matemática.

MSc. JORGE ALBERTO MARTINEZ GUTIERREZ.

Asesor Director.

LIC. MARIA OLGA QUINTANILLA DE LOVO.

Tribunal Calificador

LIC. SONIA DEL CARMEN MARTINEZ DE LOPEZ.

Tribunal Calificador.

AGRADECIMIENTOS

A DIOS TODO PODEROSO Por ser mi creador, el motor de mi vida, por no haber dejado que me rinda en ningún momento e iluminarme en el transcurso de mi carrera, porque todo lo que tengo, lo que puedo y lo que recibo es el regalo que él me ha dado.

A mis padres **ELSA MUNGUÍA DE MEJÍA** y **SIPRIAN MEJÍA** por apoyarme en todo momento, por los valores que me han inculcado, y por haberme dado la oportunidad de tener una excelente educación en el transcurso de mi vida, sobre todo por ser un excelente ejemplo de vida a seguir.

A mis **HERMANAS** y **HERMANOS** por llenar mi vida de alegría y amor cuando más lo he necesitado.

A mis abuelitas **ALEJANDRA MEJÍA** y **JOSEFA VÁSQUEZ** por su apoyo estar en los momentos más importantes de mi vida y despertar en mi tanta ternura.

A mi novio **MAURICIO ALVARADO** por ser parte importante de mi vida, por estar siempre apoyándome y por su cariño incondicional.

A **AMIGOS** con quienes compartí gratos momentos de felicidad y tristeza, por apoyarme a culminar mi objetivo, considero su amistad como valiosa y agradezco cada detalle que tuvieron para mi persona.

A mi compañero de tesis **ANDRÉS MARTÍNEZ ORELLANA** por haber sido un excelente compañero de tesis y amigo, por haber tenido la paciencia necesaria y por motivarme a seguir adelante.

A mi querido Asesor Director **Msc. JORGE ALBERTO MARTÍNEZ GUTIÉRREZ** por dirigir nuestro trabajo de grado, por ser un excelente guía y una de las personas que más admiro por su inteligencia, su responsabilidad y su disponibilidad para el trabajo.

Al Tribunal Calificador **Lic. SONIA DEL CARMEN MARTÍNEZ DE LÓPEZ Y LIC. MARIA OLGA QUINTANILLA DE LOVO** por su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia educativa, por su confianza amistad y comprensión fundamentales para la realización de este trabajo.

Un agradecimiento muy especial a la **LIC. MARÍA TRANSITO GUITIERRES REYES** Por su confianza amistad, y comprensión a lo largo de mi carrera.

A todos los **DOCENTES** que contribuyeron en mi educación y formación por toda su dedicación al enseñarme.

Ana Luz Mejía Munguía

A **DIOS TODO PODEROSO** por guiar mis pasos y estar conmigo en todo momento, por muy difícil que fueran las circunstancias a las cuales me enfrentaba cada día de mi vida, pero él siempre estuvo ahí a mi lado y gracias a el he logrado terminar mi carrera, porque siempre me brindo fuerza, sabiduría y valor para poder salir adelante.

A mí querida madre **AMINTA ORELLANA** por estar conmigo siempre apoyándome en todo momento, por compartir conmigo alegrías y tristezas, por sacrificarse tanto para que pudiera llevar acabo mi objetivo y además por enseñarme a perseverar ante las adversidades y por ser muy importante en mi desarrollo profesional, por sus excelentes consejos, su apoyo constante y su amor incondicional en todo momento, el cual me sirvió de guía para poder lograr terminar mi carrera y ser un **LICENCIADO EN MATEMATICA.**

A mi querido padre **REYNALDO MARTINEZ** por todo su apoyo, por sus buenos consejos que han sido tan importantes en mi formación profesional y por hacerme ver que en la vida hay que saber superar todas las adversidades por muy difícil que parezcan.

A mis queridas **HERMANAS**, a mi **HERMANO** por apoyarme incondicionalmente en todo el transcurso de mi carrera, por haberme impulsado siempre a seguir adelante y por hacerme ver que el mayor defecto en la vida es darse por vencido.

A todos mis **FAMILIARES** en general por demostrarme su apoyo incondicionalmente en todo momento, por darme palabras de aliento en los malos momentos y por todos sus buenos consejos.

A mis **COMPAÑEROS/AS** de carrera con quienes compartí gratos momentos de felicidad y tristeza, por apoyarme a culminar mi objetivo, porque nunca me negaron su apoyo incondicional y porque siempre me demostraron su amistad y me impulsaron a seguir adelante, lo cual fue de mucha importancia para lograr mi carrera.

A mi querida y muy apreciada compañera de tesis **ANA LUZ MEJIA MUNGUIA** por haber estado ahí en todo momento, por compartir conmigo alegrías y tristezas, por haber sido una gran compañera y una gran amiga y porque siempre estuvo apoyándome.

A mis **AMIGOS/AS** en general los cuales considero su amistad muy valiosa y agradezco cada detalle que tuvieron para mi persona.

A mi Asesor Director **Msc. JORGE ALBERTO MARTÍNEZ GUTIÉRREZ** por dirigir nuestro trabajo de grado, por ser un excelente guía y una de las personas que más admiro por su inteligencia, su responsabilidad y su disponibilidad para el trabajo.

Al Tribunal Calificador **Lic. SONIA DEL CARMEN MARTÍNEZ DE LÓPEZ Y LIC. MARIA OLGA QUINTANILLA DE LOVO** por su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia educativa..

Un agradecimiento muy especial a la **LIC. MARÍA TRANSITO GUITIERRES REYES** Por su confianza amistad, y comprensión a lo largo de mi carrera.

A todos los **DOCENTES** que contribuyeron en mi educación y formación profesional por toda su dedicación al enseñarme sus conocimientos.

Andrés Martínez Orellana.

ÍNDICE DE CONTENIDOS

BREVE DESCRIPCIÓN DE LA INVESTIGACIÓN

El desarrollo de este trabajo se realizara en tres capítulos, a continuación se hace una breve descripción de lo que se llevará a cabo en cada uno de ellos:

El **Capítulo I** se ha dividido en dos secciones, las cuales se han designado con el nombre de:

- sección I: Elementos de Teoría de Grupos.
- sección II: Elementos de Teoría de anillos.

En la **Sección I** se hace un enfoque teórico de conceptos y propiedades algebraicas tales como:

- grupos.
- Subgrupos.
- Subgrupos Normales.
- homomorfismo de grupos.

En la **Sección II** se hace una breve introducción a la teoría de:

- Anillos.
- Dominios Enteros.
- Campos.
- homomorfismos de anillos.
- ideales.

Lo cual será una base fundamental para poder comprender de una manera más eficiente conceptos y propiedades que se presentaran en el siguiente capítulo.

El Capítulo II se estudia la teoría de anillos de polinomios y teoremas relacionados a los mismos.

El Capítulo III se procede con la parte fundamental de esta investigación, se da desde la perspectiva Euclidiana, se introducirán los conceptos necesarios para comprender la teoría de los anillos euclidianos.

Se estudian los Anillos de Factorización Única, Anillos de Ideales Principales y además se desarrollan las propiedades que debe cumplir un dominio entero para convertirse en un anillo Euclidiano, que es la parte principal de esta investigación.

INTRODUCCIÓN

En el presente trabajo se pretende abordar la teoría de "Anillos Euclidianos y Teoremas Fundamentales", se tratará de conocer y analizar estas estructuras, para lo cual es necesario tener conocimientos básicos de algebra moderna para un mejor aprovechamiento de esta teoría.

Por tanto, surge la necesidad de elaborar este trabajo de la forma más elemental y concisa posible, abriendo una ventana hacia el importante aporte del matemático Euclides. Aunque vale la pena aclarar que los conceptos que aquí se abordaran no son tan sencillos como parecen, razón por la que genera algunas dificultades en los estudiantes.

La aportación de Euclides a las matemáticas no es sencilla de entender por su complejidad y la novedad. Aún sigue siendo una teoría de vanguardia y visionaria por la gran extensión de aplicaciones que tiene en las diferentes ramas de la ciencia contemporánea.

Esta teoría se centra fundamentalmente en el campo del álgebra moderna y algebra abstracta. En matemáticas, los grandes progresos siempre han estado ligados a retos en la capacidad de dar a conocer un poco más en el campo del algebra. En particular, para darnos una idea de la importancia que tiene la teoría de anillos, basta recordar que la teoría de anillos se encuentra inmerso en diferente áreas del algebra moderna. Por otro lado, en este trabajo no se ambiciona ser una biografía de este matemático, ya que eso sería una tarea bastante difícil. Lo que realmente se pretende, es

presentar un trabajo ordenado y formal sobre la obra relacionado a los Anillos de manera que se alcance una mayor comprensión sobre ésta temática y a la vez que sea utilizado como una herramienta de estudio.

No se debe olvidar, por otro lado, que una característica distinta de las matemáticas es su gran unidad, es decir, es imposible hablar de áreas que evolucionen de manera aislada, o como lo dice David Hilbert: "La matemática es en mi opinión un todo indivisible, un organismo cuya vitalidad está condicionada por la conexión de sus partes". Por lo tanto, el desarrollo de una área necesariamente marca su impacto en las otras y todas se retroalimentan entre sí. Es decir, el álgebra no es ajena a esta tendencia y a lo largo de su desarrollo es posible observar su influencia en otras ramas de la matemática y cómo se ha visto beneficiada por los desarrollos de éstas. Sin embargo, a pesar de que sería muy importante enfocarnos un poco a este proceso, no nos es posible revisar en su totalidad esas conexiones del álgebra con otras áreas y sólo se le pide al lector tener en cuenta que el álgebra no ha evolucionado de forma aislada y es posible notar su presencia en todas las matemáticas.

Este trabajo se elaborara con la intención de que pueda servir como una herramienta más a los estudiantes y docentes, el cual se desarrolla de la siguiente manera:

Se presenta un antecedente en el cual se hace énfasis en una breve historia de cómo surge la teoría de anillos y quienes fueron los principales matemáticos que se enfocaron en esta teoría.

Una breve justificación en la cual se detalla el por qué nace la idea de trabajar en la teoría de anillos y para quienes podría servir este trabajo.

Los objetivos generales y específicos que son los que se pretenden lograr al final de este proyecto.

Un marco teórico en el cual se desarrolla toda la teoría necesaria para poder comprender y analizar definiciones, lemas, teoremas, proposiciones, ejemplos del tema de Anillos Euclidianos.

NOTA HISTORICA

Lo novedoso de la geometría analítica es que permite representar figuras geométricas mediante fórmulas de tipo $f\ x,y\ = 0$, donde f representa una función. En particular, las rectas pueden expresarse como ecuaciones polinómicas de grado1, por ejemplo la recta $(2x + 6y = 0)$.

La circunferencia y el resto de cónicas como ecuaciones polinómicas cuadráticas

(La circunferencia $x^2 + y^2 = 4$).

Eso convertía toda geometría griega en el estudio de las relaciones que existen entre polinomios de lineales y cuadráticos. Desde un punto de vista formal, los geómetras de esta época han encontrado una relación fundamental entre la estructura lógica que usaban los geómetras griegos (el plano, la regla, el compás…) y la estructura algebraica del ideal formado por polinomios constantes, lineales y cuadráticos del anillo de polinomios $R[x,y]$, resultando que ambas estructuras son equivalentes.

Este hecho fundamental (no visto con nitidez hasta el desarrollo del algebra y de la lógica matemática entre finales del siglo XIX y principios del siglo XX) resulta fundamental para entender por qué la Geometría de los griegos puede desprenderse de sus axiomas y estudiarse directamente usando la axiomática de Zermelo-Fraenkel, como el resto de la matemática.

El método original de Descartes no es exactamente el que se acaba de explicar. Descartes utiliza solamente el eje de abscisas, calculando el valor de la segunda

componente del punto (x, y) mediante la ecuación de la curva, dándole valores a la magnitud x. Por otro lado, Descartes sólo considera valores positivos de las cantidades x e y, dado que en la época aun resultaban "sospechosos" los números negativos. Como consecuencia, en sus estudios existen ciertas anomalías y aparecen curvas sesgadas. Con el tiempo se aceptaron las modificaciones que muestran el método tal y como lo conocemos hoy en día.

LOS NUEVOS MÉTODOS

La aparición de la Geometría analítica trae consigo una nueva forma de entender la Geometría. El nuevo método algebraico, sustituye el antiguo, el sintético, consiste en establecer unos axiomas y unas definiciones y deducir de ellos los teoremas. El método sintético está a estas alturas casi agotado (Aunque dará algunos resultados interesantes, como la característica de Euler, la naturaleza de estos resultados no es ya tanto Geométrica, como topológica y los resultados realmente importante que se hagan en adelante en el campo de la Geometría ya vendrán de la mano de métodos algebraicos o diferenciales), da paso al método algebraico: estudio de los objetos Geométricos como representaciones en el espacio de ciertas ecuaciones polinómicas, dicho de otro modo, del conjunto de raíces de polinomios.

El método sintético solo volverá abordarse cuando aparezca la Geometría no Euclidea y definitivamente deja de ser un instrumento de investigación Geométrica a

principios del siglo XX, quedando relegado a un conjunto de instrumentos y herramientas para la resolución de problemas, pero ya como una disciplina cerrada.

LOS LÍMITES DEL METODO ALGEBRAICO.

El método algebraico se ve posibilitado por un avance en Algebra hecho durante el siglo XVI, la resolución de las ecuaciones cubicas y de grado4. Esto permite generalizar la Geometría, al estudiar curvas que no son dadas por polinomios cuadráticos, y que no pueden construirse con regla y compás, además de las cónicas, excluyendo la circunferencia, claro. Pero este método que terminará constituyendo una disciplina propia, la Geometría Algebraica tardara aún mucho en salir de unas pocas nociones iniciales prácticamente inalterada desde Descartes, Fermat y Newton. La razón será la imposibilidad de resolver por radicales la ecuación de quinto grado hecho no descubierto hasta el siglo XIX, y el desarrollo de anillos y del algebra conmutativa.

EL CÁLCULO INFINITESIMAL.

El método algebraico tiene otra generalización natural, que es la de considerar una curva no solo como ecuación polinómica si no como una ecuación $f\ x,y\ = 0$ en la que el polinomio es ahora sustituido por una función cualquiera f la generalización de todo esto desde el plano en $\mathbf{R^2}$ al plano en tres dimensiones $\mathbf{R^3}$ se hace de forma natural añadiendo un tercer eje perpendicular (eje Z) a los dos ya considerados y las funciones tomaran la forma $f(x,y,z)$.

Se ve entonces que los aportes fundamentales que realizó Euclides fueron el asociar los anillos con los conjuntos de polinomios y el poder definir Anillos de Polinomios y Euclidianos donde cada uno de ellos debe cumplir sus propias propiedades.

JUSTIFICACION

El estudio de los Anillos Euclidianos puede considerarse como reglas de datos de algún tipo, donde el álgebra que se establezca sobre estos determina la manera en que estos datos pueden combinarse para generar una nueva información (Silvester).

La formulación de un problema concreto en términos del álgebra lineal ha sido y sin duda lo seguirá siendo, uno de los métodos más efectivos para hallar su solución.

Herramientas tales como el determinante, las formas canónicas y transformaciones lineales, entre muchas otras, constituyen decisivamente a facilitar esta labor.

Es por ello que nos dedicaremos al estudio de Anillos Euclidianos que poseen ciertas condiciones adicionales, aparte de las propias definiciones como por ejemplo: anillos de integridad, anillos de factorización única, y anillos euclidianos.

El estudio de anillos de polinomios y euclidianos nos permitirá repasar todas las definiciones y propiedades, como son las operaciones de suma, producto, división, el cálculo de raíces y la factorización desde el punto de vista de su estructura de anillo.

Este nuevo enfoque aclara mucho de los conceptos ya estudiados, considerando propiedades más generales de anillos, y al mismo tiempo dar a conocer nuevos caminos que nos conducirán a resultados bastante fuertes.

OBJETIVOS

Objetivos Generales.

- Documentar de forma introductoria la teoría de Anillos Euclidianos y Teoremas Fundamentales para mostrar su importancia.
- Analizar la teoría de anillos euclidianos y presentar los conceptos que son necesarios para su comprensión.

Objetivos Específicos.

- Mostrar una base de conceptos necesarios y suficientes para comprender los principios de la teoría de los Anillos Euclidianos.
- Estimular el interés de la Teoría de Anillos Euclidianos a estudiantes de matemática.
- Recopilar la información sobre la teoría de Anillos Euclidianos
- Presentar los conceptos necesarios para comprender la teoría de anillos Euclidianos.

CAPÍTULO I

ELEMENTOS INTRODUCTORIOS: ÁLGEBRA ABSTRACTA

SECCION 1: ELEMENTOS DE TEORIA DE GRUPOS

En este capítulo iniciaremos con el estudio de la estructura algebraica conocida **c**omo **"grupo"** que sirven como bloques de construcción fundamentales de la estructura que hoy se llama **Algebra Abstracta**. En capítulos posteriores nos enfocaremos en otros conceptos tales como campos y anillos, con mayor o igual importancia de los que aquí tratamos.

Aparte de que ya se ha hecho tradicional comenzar con el estudio de los grupos, hay razones naturales convenientes para esta elección. Para comenzar, los grupos, como sistema con una sola operación, se prestan a la más simple de las descripciones formales. Sin embargo, a pesar de esta simplicidad de descripción los conceptos fundamentales del algebra tales como homomorfismo, que juegan un papel tan importante en todas las estructuras algebraicas, en realidad en todas las matemáticas, entran aquí en una forma pura y reveladora.

En el **Álgebra Abstracta** tenemos ciertos sistemas básicos que en la historia y en el desarrollo de las matemáticas, han alcanzado posiciones de importancia extraordinaria.

Estos son generalmente conjuntos, con cuyos elementos podemos operar algebraicamente, por lo que entendemos que podemos combinar dos elementos del

conjunto, quizá de varias maneras, para obtener un tercer elemento también del conjunto, además suponemos que estas operaciones algebraicas están sujetas a ciertas reglas que se indican explícitamente en lo que se llaman axiomas o postulados definitorios del sistema.

Nos gustaría subrayar que estos sistemas algebraicos y los axiomas que los definen deben tener cierta naturalidad. Deben surgir de la experiencia que resulta de observar muchos ejemplos; que deben ser ricos en resultados significativos.

GRUPOS

Definición 1.1 Se dice que un conjunto no vacío $\boldsymbol{G}$ es un grupo si en el está definida una operación $(*)$ tal que:

a) $a, b \in G$ implica que $a * b \in G$

b) Dados $a, b, c \in G$ se tiene que $a * (b * c) = (a * b) * c$

c) Existe un elemento identidad $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$

d) Para todo $a \in G$ existe un elemento $b \in G$ tal que $a * b = b * a = e$

Definición 1.2 Se dice que un grupo G es abeliano si $a * b = b * a$, para todo $a, b \in G$

Lema 1.1 Si G es un grupo, entonces:

a) Su elemento identidad es único.

b) Todo $a \in G$ tiene un inverso único $a^{-1} \in G$

c) Si $a \in G,\ a^{-1\ -1} = a$

d) Para $a,\ b\ \in G,\ ab\ ^{-1} = b^{-1}a^{-1}$

e) Si $a,\ b,\ c\ \in G$ y

- $a * b = a * c,$ entonces $b = c$ (propiedad cancelativa)
- $b * a = c * a,$ entonces $b = c$ (propiedad cancelativa)

Prueba (a): Se debe probar que el elemento identidad de un grupo es único, para ello, supóngase que $e * x = x * e = x$ y también que $e' * x = x * e' = x$, para toda $x \in \boldsymbol{G}$.

Comparemos e y e'. En primer lugar tómese e como elemento identidad,

$$e * e' = e' * e = e'$$

Pero considerando e' como identidad tenemos $e * e' = e$. Por tanto,

$$e' = e * e' = e' * e = e$$

y se ha demostrado que la identidad de un grupo es única.

Prueba (b): Sea $a^{-1},\ b^{-1} \in G$ son dos posibles inversos (llamado también simétrico) de a se tiene

$$b^{-1} = b^{-1}\ aa^{-1}\ =\ b^{-1}a\ a^{-1} = a^{-1}$$

$\therefore\ a$ tiene inverso único.

Prueba (c): Si $a^{-1} \in G \Longrightarrow a^{-1}\ a^{-1\ -1}$

$= e$

$= a^{-1}a$ (por definición de inverso)

$\Longrightarrow a^{-1}(a^{-1})^{-1} = a^{-1}a$

$\Longrightarrow (a^{-1})^{-1} = a.$

Prueba (d): $a * b\ \ b^{-1}a^{-1} = a *\ \ b *\ a^{-1} = a *\ e * a^{-1} = a * a^{-1} = e$ y con la definición de inverso $(a * b)^{-1} = b^{-1} * a^{-1}$.

Prueba (e): Probaremos la propiedad de cancelación por la izquierda y por la derecha.

Supóngase que $a * b = a * c$. Entonces existe $a^{-1} \in G$ tal que

$a^{-1} *\ a * b = a^{-1} * (a * c)$

$a^{-1} * a\ * b =\ a^{-1} * a\ * c$ (Ley Asociativa)

$e * b = e * c$, (definición de inverso multiplicativo)

Por la definición de a^{-1} tenemos que $a^{-1} * a\ * b = e * b = b$ y

$a^{-1} * a\ * c = e * c = c$, luego $e * b = e * c$ y por definición de $e \in G$

$b = c$

SUBGRUPOS

Antes de volver al estudio de los grupos, desearíamos cambiar nuestra notación ligeramente. Es molesto seguir usando el $(*)$ para la operación de grupo; de aquí en

adelante prescindiremos de él y en lugar de escribir $a * b$ para $a, b \in G$ denotaremos tal producto simplemente por ab.

En general, no estaremos interesados en subconjuntos arbitrarios de un grupo G pues no reflejan el hecho de que G tiene una estructura algebraica.

Todos los subconjuntos que consideraremos serán de los que tengan propiedades algebraicas derivadas de las de G. Los Subconjuntos más naturales de entre los de tales tipos se introducen en la siguiente.

Definición 1.3 Dado un grupo $(G, *)$ y un subconjunto no vacío H de G, se dice que $(H, *)$ es un subgrupo de $(G, *)$ si y solo si $(H, *)$ es grupo.

Teorema 1.1 Un subconjunto H de un grupo G es un subgrupo, si y sólo si

1. Sea $a, b \in H \implies a.b \in H$
2. Sea $a \in H \implies a^{-1} \in H$

Prueba:

" $\Longrightarrow$ " Las condiciones 1) y 2) son triviales de la definición de subgrupo.

" $\Longleftarrow$ " Como H debe ser un grupo en sí mismo, se puede ver que al cumplirse las dos condiciones, solo queda por demostrar la propiedad asociativa.

En particular, como $H \subseteq G$, se tiene que para todo $x, y, z \in H$, se cumple que

$$x.(y.z) = (x.y).z$$

Lema 1.2 Si H es un subgrupo finito no vacío de un grupo G, y H es cerrado respecto a la multiplicación, entonces H es un subgrupo de G.

Prueba: Sea r el número de elementos de H, de acuerdo al teorema 1.1.2.1, no se necesita otra cosa que demostrar ya que siempre que $a \in H$, entonces $a^{-1} \in H$. Supongamos que $a \in H$; entonces

$$a^2 = aa \in H, a^3 = a^2a \in H, \ldots, a^m \in H,$$

ya que H es, por hipótesis cerrado.

Luego la colección finita de elementos $a,\ a^2,\ a^3, \ldots a^m$, debe estar contenida en H, que es un subconjunto finito de G. Luego debe haber repeticiones en esta colección de elementos; es decir, para algunos enteros r, s con $r > s > 0$, $a^r = a^s$. Basta tomar G, $a^{r-s} = e$(donde e esta en H); como $r - s - 1 \geq 0$, $a^{r-s-1} \in H$ y $a^{-1} = a^{r-s-1}$ ya que $aa^{r-s-1} = a^{r-s} = e$. Por tanto, $a^{-1} \in H$, lo que completa la prueba del lema.

Ejemplo 1: Sea G el grupo de los enteros bajo la adición, H el subconjunto consistente en todos los múltiplos de 5.

Prueba: Por hipótesis se tiene que H es cerrado bajo la multiplicación, siendo esta multiplicación asociativa en G, evidentemente también es asociativa en H.

Sea $a = 5n \in H \Longrightarrow a^{-1} = (5n)^{-1} \in H$

$$5n \in H \Longrightarrow (5n)^{-1} \in H$$

$$\Longrightarrow \ 5n \ \ 5n^{\ -1} = e \in H$$

$$\Longrightarrow \frac{5n}{5n} = e$$

$$\Longrightarrow 1 = e,$$

$\therefore$ Se ha demostrado entonces que H es subgrupo de G.

Teorema 1.2 Sea G un grupo y $a \in G$, entonces el conjunto $H = \{a^n,\ n \in Z\}$ es un subgrupo de G. Además H es el subgrupo de G más pequeño que contiene a.

Prueba: De acuerdo al teorema anterior, es suficiente probar las siguientes propiedades

1. $\forall\ a^n, a^m \implies a^n . a^m \in H.$
2. $\forall\ (a)^n \in H \implies a^{-n} \in H$.

Como $a^n = \underbrace{aa \ldots a}_{\text{n-veces}}$ y $a^m = \underbrace{aa \ldots a}_{\text{m-veces}}$

$$a^n a^m = \underbrace{aa \ldots a}_{\text{n-veces}}\ \underbrace{aa \ldots a}_{\text{m-veces}}$$

$$= \underbrace{aaa \ldots a}_{m+n \text{ veces}}$$

$= a^{m+n} \in H$, así se cumple (1)

Además,

$$a^n a^0 = a^{n+0} = a^n,$$

$$\Longrightarrow a^0 = e$$

Si $a^n \in H$, entonces

$$a^n a^{-n} = a^{n-n} = a^0,$$

y por definición de H, $a^{-n} \in H$, así se cumple (2)

Definición 1.4 Sea G un grupo, H un subgrupo de G; para $a, b \in G$ decimos que a es congruente con b mod H, lo que escribimos: $a \equiv b \; mod \; H$, si $ab^{-1} \in H$.

Lema 1.3 La relación $a \equiv b \; mod \; H$ es una relación de equivalencia.

Prueba: Para poder probar este lema debemos verificar las siguientes tres condiciones: para $a, b, c \in G$

1) $a \equiv a \; mod \; H$
2) $a \equiv b \; mod \; H$, implica que $b \equiv a \; mod \; H$
3) $a \equiv b \; mod \; H$ y $b \equiv c \; mod \; H$**,** esto implica que $a \equiv c \; mod \; H$

Estudiemos una por una, estas condiciones.

1) Para probar $a \equiv a \; mod \; H$ debemos probar usando la definición de congruencia $mod \; H$, que $aa^{-1} \in H$. Como H es un subgrupo de G, $e \in H$, y como $aa^{-1} = e$, entonces $aa^{-1} \in H$ y esto es lo que se nos pedía demostrar.
2) Supongamos que $a \equiv b \; mod \; H$, es decir, supongamos $ab^{-1} \in H$; probaremos que $b \equiv a \; mod \; H$ o lo que es lo mismo decir que $ba^{-1} \in H$.

   Como $ab^{-1} \in H$, es un subgrupo de G, $ab^{-1\;\;-1} \in H$ según (lema 1.1.1.1)

   $ab^{-1\;\;-1} = ba^{-1}$, luego $ba^{-1} \in H$ y $b \equiv a \; mod \; H$.
3) Finalmente, pedimos que sí $a \equiv b \; mod \; H$ y $b \equiv c \; mod \; H$, implica que $a \equiv c \; mod \; H$. La primera congruencia se traduce en $ab^{-1} \in H$, la segunda en $bc^{-1} \in H$; como H es un subgrupo de G,

$$ab^{-1}\ \ bc^{-1}\ = a\ b^{-1}b\ c^{-1} = aec^{-1} = ac^{-1}\ \in H,$$

luego $ac^{-1} \in H$, entonces $a \equiv c\ mod\ H$.

Definición 1.5 Dados dos subgrupos H y K de G, se define su producto como:

$$HK = \ hk: h \in H\ \ y\ k\ \in K\ .$$

Lema 1.4 HK es un subgrupo de G si y solo si $HK = KH$.

Prueba: supongamos primero que $HK = KH$; es decir, que si $h \in H$ y $k \in K$, entonces $hk = k_1h_1$ para algún $k_1 \in K, h_1 \in H$ (no es necesario que $k_1 = k$ o $h_1 = h$). Para probar que HK es un subgrupo, debemos verificar que es cerrado y que todo elemento de HK tiene un inverso en HK. Demostremos, en primer lugar, que es cerrado; supongamos, pues, $x = hk \in HK$ y $y = h'k' \in HK$. Entonces $xy = hkh'k'$, pero como

$$kh' \in KH = HK, kh' = h_2k_2 \text{ con } h_2 \in H \text{ y } k_2 \in K.$$

De donde

$$xy = h\ h_2k_2\ k' = \ hh_2\ \ k_2k'\ \in HK, \text{ y } HK \text{ es cerrado.}$$

Además

$$x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK, \text{ luego } x^{-1} \in HK.$$

Luego HK es subgrupo de G.

Por otra parte, HK es un subgrupo de $\boldsymbol{G}$, entonces para cualquier $h \in H$ y $k \in K$, $k^{-1}h^{-1} \in KH$ y por tanto $kh = (h^{-1}k^{-1})^{-1} \in HK$. Luego $KH \subset HK$.

Si x es ahora un elemento cualquiera de HK, $x^{-1} = hk \in HK$, para algunos

$$h \in H, k \in K,$$

luego

$x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$, luego $HK \subset KH$. luego $HK = KH$.

SUBGRUPOS NORMALES

Definición 1.6 Sea H un subgrupo de G y sea $a \in G$ **(**a un elemento**),** se le denomina clase lateral izquierda al conjunto $Ha = \{ha/\ h \in H\}$.

Definición 1.7 Si G es un grupo y H un subgrupo de G, sea a un elemento cualquiera de G, entonces $aH = \{ha/h \in H\}$ es una clases lateral derecha de H en G.

Definición 1.8 Una clase lateral es una clase lateral izquierda o derecha de algún subgrupo de G. Puesto que $Na = a(a^{-1}Na)$, las clases laterales derechas Na (de N) y las clases laterales izquierdas $a(a^{-1}Na)$ coinciden.

Por tanto, no tiene ningún sentido afirmar que una clase lateral es izquierda o derecha sin antes especificar el subgrupo al que corresponden. En otras palabras: la clase lateral derecha de un subgrupo es igual a la clase lateral izquierda de otro subgrupo diferente. El que una cierta clase lateral sea una clase lateral derecha o izquierda dependerá de que subgrupo que se utilice.

Definición 1.9 Un subgrupo N de G se dice que es un subgrupo normal de $\boldsymbol{G}$ si para toda $a \in G$ y toda $n \in N$, $ana^{-1} \in N$.

Es claro que si representamos por ana^{-1} al conjunto de todos los ana^{-1}, con $n \in N$, entonces N es un subgrupo normal de G si y solo si $ana^{-1} \subset N$ para toda $a \in G$.

NOTACION 1: Usaremos $N \lhd G$ para decir que N es un subgrupo normal de G.

Lema 1.5 Sea N subgrupo de G. Entonces N es un subgrupo normal de G si y solo $gNg^{-1} = N, \forall\, g \in G$.

Prueba: Si N es normal, entonces $gNg^{-1} \subset N$, entonces $N = g(g^{-1}Ng)g^{-1} \subset N$

Por lo tanto $gNg^{-1} = N$ (definición de subgrupo normal)

$\therefore$ La condición suficiente es trivial por definición.

Teorema 1.3 $N \lhd G$ si y solo si toda clase lateral izquierda de N en G es una clase lateral derecha de N en G.

Prueba:

" $\Longrightarrow$ " Si N es un subgrupo normal de G, $\Longrightarrow\ \forall a \in G,\ aNa^{-1} = N$, de donde $aNa^{-1}\ a = Na\ \rightarrow aN = Na$, es decir la clase lateral izquierda aN es la clase lateral derecha Na.

" $\Longleftarrow$ "Supongamos que toda clase lateral izquierda de N en G, es decir para

que $a \in G$, la clase lateral izquierda aN debe ser también la clase lateral derecha.

Como $a = ae \in aN$, cualquiera que sea la clase lateral derecha que resulte ser, aN debe contener al elemento a; pero a esta en la clase lateral derecha Na y dos clases laterales derechas distintas no tienen ningún elemento en común $aN = Na$.

En otras palabras: $aNa^{-1} = Naa^{-1} = N$, y N por tanto es subgrupo normal de $\boldsymbol{G}$.

Corolario 1.1 Si H y K son subgrupos de un grupo abeliano G, entonces HK es un subgrupo de G.

Prueba: Sean $g = xu, h = yv$ donde $x, y \in H$ y $u, v \in K$, dos elementos de HK, entonces aplicando las propiedades asociativas y conmutativas tenemos

$gh^{-1}\ xu\ = (yv)^{-1} =\ xu\ \ v^{-1}y^{-1}\ =\ xy^{-1}\ \ uv^{-1}\ \in HK$, porque al tratarse de subgrupos sabemos que $x, y \in H \Longrightarrow xy^{-1} \in H,\ u,\ v \in K \Longrightarrow uv^{-1} \in K$.

A su vez la relación $gh^{-1} \in HK$ implica que HK es subgrupo.

Definición 1.10 Se define $\frac{G}{N}$ como el conjunto de clases laterales izquierdas de N en G, esto es:

$$\frac{G}{N} = \ aN/a \in G\ .$$

Definición 1.11 Si φ es un homomorfismo de G en $G'(G$ y G' son grupos), entonces el kernel o núcleo de $\varphi, K\ \ \varphi$, se define por

$K\ \ \varphi\ \ =\ \ a \in G\ /\ \varphi\ \ a\ \ = e', e'$es el elemento identidad de $\boldsymbol{G'}$.

Proposición 1.1 El Kernel de φ es un subgrupo normal de G.

Prueba: El núcleo de φ es cerrado $\forall\ a, b\ \in \ker \varphi$

$$\Longrightarrow \varphi\ \ a, b\ \ = \varphi\ \ a\ \ * \varphi\ \ b\ \ = 1H * 1H = 1H,$$

Contiene el elemento identidad $\varphi\ \ 1G\ \ = 1H$

HOMOMORFISMOS DE GRUPOS

Las ideas y resultados de este contenido están muy relacionadas con las del contenido siguiente. Si hay una idea central común a todos los aspectos del álgebra moderna, tal es la noción de homomorfismo. Indicamos con ello una aplicación de un sistema algebraico a un sistema algebraico análogo que preserva la estructura. Precisamos la idea, en lo que a grupos se refiere, en la definición siguiente.

Definición 1.12 Sean $(G, +)\ y\ \ (G,\ *)$ dos grupos, entonces una aplicación $\varphi: (G, +) \rightarrow (G,\ *)$ es un homomorfismo si $\varphi\ \ ab\ \ =\ \ \varphi\ \ a\ \ \varphi\ \ b\ \ $ para todo $a, b\ \in (G, +)$ y $\varphi\ \ a\ ,\ \varphi(b) \in\ \ (G,\ *)$.

Lema 1.6 Supongamos que G es un grupo y que N es un subgrupo normal G; definamos la aplicación $\varphi\ \ a\ \ = Na$ para todo $a \in \boldsymbol{G}$. Entonces, φ es un homomorfismo de G sobre G/N.

Prueba: Sean $x, y \in G$, entonces

$$\varphi\ xy\ = Nxy$$

$$= Nx\,.Ny$$

$$= \varphi\ x\ .\varphi\ y$$

Con esto se prueba que φ es un homomorfismo. Además si $Nx \in G/N$, se tiene que $\varphi\ x\ = Nx$, con $x \in G$. Luego φ es sobre.

Lema 1.7 Si φ es un homomorfismo de G en G', entonces:

a) $\varphi\ e\ = e', e'$: elemento unidad de G'.

b) $\varphi\ a^{-1}\ = \varphi\ a\ ^{-1}$ para todo $a \in G$.

Prueba:

a) Tenemos en primer lugar que $\varphi\ ee\ = \varphi\ e\ \varphi\ e$, además $\varphi\ ee\ = \varphi\ e$, ahora igualando ambas expresiones

$\varphi\ e\ \varphi\ e\ = \varphi\ e$ y por la ley de cancelación $\varphi\ e\ = e'$, e' es identidad.

b) Sea $x\ \in G$, entonces por la parte a)

$$e' = \varphi\ e$$

$$e' = \varphi\ xx^{-1}$$

$$e' = \varphi\ x\ \varphi\ x^{-1}\ ,$$

pero el inverso de $\varphi\ x$ en el grupo G' esta dado por $[\ \varphi\ x\ ]^{-1} = \varphi(x^{-1})$.

SECCION 2: ELEMENTOS DE TEORIA DE ANILLOS.

ANILLOS

Hay ciertos sistemas algebraicos que nos sirven como los bloques de construcción de las estructuras que componen la materia que actualmente llamamos álgebra moderna. Ya hemos aprendido algo de uno de ellos, los grupos. Ahora nuestro propósito es introducir y estudiar un segundo de tales bloques, el constituido por los llamados anillos. El concepto abstracto de grupo tiene su origen en el conjunto de aplicaciones o permutaciones de un conjunto sobre sí mismo. En contraste, los anillos nacen de otra fuente bastante familiar, el conjunto de los enteros. Veremos que están caracterizados de acuerdo a los aspectos algebraicos de los enteros ordinarios de los que pueden considerarse una generalización.

En el próximo párrafo se aclarará que un anillo es completamente diferente de un grupo, ya que es un sistema, en el que hay definidas dos operaciones; estas operaciones comúnmente se llaman adición y multiplicación. Sin embargo, a pesar de las diferencias, el análisis de los anillos seguirá el esquema que establecimos para los grupos. Tendremos los análogos de los homomorfismos, de los subgrupos normales, etc. Ahora pasamos a dar una definición formal de anillo.

Definición 1.13 Un anillo A es un sistema de elementos tal, que es un grupo abeliano para la operación de adición y es cerrado para una operación binaria de multiplicación,

la cual es asociativa y distributiva respecto a la adición. Es decir, para elementos cualesquiera a, b, c del anillo A**,** se tiene

$$a\ bc\ =\ ab\ c,$$

$$a\ b+c\ = ab + ac,$$

$$a + b\ c = ac + bc.$$

Antes de comenzar a estudiar algunas propiedades de los anillos, haremos una pausa para examinar algunos ejemplos. Motivándonos en ellos definiremos varios casos especiales de anillos que son importancia.

Ejemplo 2: Sea R es el conjunto de los enteros positivos, negativos y el cero, donde $(+)$ es la adición usual y $(.)$ la multiplicación usual de los enteros, entonces R es un anillo conmutativo con un elemento unitario.

Ejemplo 1.3: Sea R el conjunto de los enteros pares bajo las operaciones habituales de adición y multiplicación. R es un anillo conmutativo, pero no tiene elemento unitario.

Lema 1.8 Si R es un anillo, entonces para todo $a, b \in R$

1) $a \cdot 0 = 0 \cdot a = 0$
2) $a \cdot\ -b\ =\ -a\ \cdot b = -(a \cdot b)$
3) $-a\ \cdot\ -b\ = a \cdot b$

Si además, R tiene un elemento unitario, 1, entonces

4) $-1 \cdot a = -a$

5) $-1 \cdot -1 = 1$

Prueba:

1) $0a = (0 + 0)a = 0a + 0a \Rightarrow 0a = 0$

2) $a.\ -b + a.\ b = -a + a.b = 0.b = 0$

$$\Rightarrow -a.b = -(a.b).$$

3) $-a\ .\ -b = -\ a.\ -b = --\ a.b = a.b$ (ley de los signos).

4) $(-1).a = 1.(-a) = -a$, por propiedad 2.

5) $-1\ .\ -1 = -\ 1.\ -1 = --\ 1.1 = 1$ se sigue por propiedad 3.

DOMINIOS

Los ejemplos que acabamos de dar en la sección anterior claramente indican que aunque los anillos son una generalización directa de los enteros, ciertos hechos aritméticos a los que estamos acostumbrados en el anillo de los enteros no tienen forzosamente que tener validez en los anillos en general. Por ejemplo, se verá más adelante en la definición **(1.14)** la posibilidad de que $a \cdot b = 0$ sin que ni a ni b sean cero. Existen también ejemplos muy naturales en que $a \cdot b \neq b \cdot a$. Todas estas cosas van en contra de nuestra experiencia previa.

Por simplicidad en la expresión, prescindiremos de aquí en adelante del punto en $a \cdot b$ y escribiremos simplemente este producto como ab.

Definición 1.14 Si R es un anillo conmutativo entonces $\forall a \in R \; tal \; que \;\; a \neq 0$ se dice que es un divisor de cero si existe un $b \in R$, $b \neq 0$, tal que $ab = 0$.

Definición 1.15 Un anillo se dice que es un anillo con división si elementos distintos de cero forman un grupo bajo la multiplicación.

Con el concepto anterior ya podemos dar una definición sobre un dominio, que no es más que una clase especial de anillo.

Definición 1.16 (DOMINIO) Un anillo conmutativo, es un dominio entero si no tiene divisores de cero.

Ejemplo 4 El anillo de los enteros es un ejemplo de dominio entero.

CAMPOS

Definición 1.17 Un cuerpo o Campo es una estructura algebraica en la cual las operaciones llamadas adición y multiplicación se pueden realizar y cumplen las propiedades asociativa, conmutativa y distributiva de la multiplicación respecto de la adición además de la existencia de inverso aditivo, de inverso multiplicativo y de un elemento neutro para la adición y otro para la multiplicación, los cuales permiten efectuar las operaciones.

Definición análoga a la 1.18: Un campo es un Anillo conmutativo con división.

Ejemplos de Campo

Q: es el campo de los números racionales.

R: es el campo de los números reales.

C: es un campo de los números complejos.

HOMOMORFISMOS DE ANILLOS

Al estudiar los grupos vimos que el concepto de homomorfismo resultaba ciertamente fructífero. Esto parece sugerir que apropiadamente un análogo para anillos nos llevaría también hasta importantes ideas. Recuérdese que para los grupos un homomorfismo se definió como una aplicación tal que $\varphi\ ab\ = \varphi\ a\ \varphi\ b\ $. Como un anillo tiene dos operaciones, ¿Qué podría ser una extensión más natural de este tipo de fórmula que se representa en la siguiente definición?

Definición 1.19 Una aplicación φ del anillo R en el anillo R' se dice que es un homomorfismo si para cualesquiera $a, b \in R$ se cumple

1) $\varphi\ a+b\ = \varphi\ a\ + \varphi(b)$,
2) $\varphi\ ab\ = \varphi\ a\ .\varphi(b)$.

Como en el caso de los grupos, hagamos también aquí hincapié en que el $(+)$ y el $(.)$ que aparecen en los primeros miembros de las relaciones (1) y (2) son los de R mientras que el $(+)$ y el $(.)$ que aparecen en los segundos miembros son los de R'.

Una útil observación es la de que un homomorfismo de un anillo R en un anillo R' es, si ignoramos totalmente la multiplicación en ambos anillos, al menos un homomorfismo de R en R' cuando los consideramos como grupos abelianos bajo la respectiva adicione. Por tanto, en cuanto a la adición concierne, todas las propiedades acerca de los homomorfismos de grupos probadas en el capítulo anterior se verifican aquí también. En particular, la mera reformulación del lema (**1.8)** para el caso del grupo aditivo de un anillo nos da:

Teorema 1.4 Si φ es un homomorfismo del anillo R en el anillo R', entonces:

1) $\varphi\ 0\ = 0$
2) $\varphi\ -a\ = -\varphi(a)$ para toda $a \in R$.

Prueba:

1) $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0) = \varphi(0) = 0$
2) $\varphi\ 0\ = \varphi\ a-a\ = \varphi\ a+\ -a\ = \varphi\ a\ + \varphi\ -a\ = 0$ (opuesto aditivo)

$$\Longrightarrow \varphi\ -a\ = -\varphi(a)$$

Ahora bien, en el caso de los grupos, dado un homomorfismo asociamos con este homomorfismo cierto subconjunto del grupo al que llamamos núcleo del homomorfismo. ¿Cuál deberá ser la definición apropiada del núcleo de un homomorfismo entre anillos? Después de todo, los anillos tienen dos operaciones, adición y multiplicación, y podría ser natural preguntar cuál de éstas dos debe singularizarse como base para la definición. Dentro de la definición de cualquier grupo arbitrario está la condición de que el anillo forme un grupo Abeliano bajo la adición. La multiplicación del anillo se dejó con muchas menos restricciones, y por ello, en cierto sentido, mucho menos bajo nuestro control que la adición. Es por esto por lo que es a la adición a la que le damos énfasis especial en el anillo, y damos la siguiente definición.

Definición 1.20 Si φ es un homomorfismo del anillo R en el anillo R' entonces el núcleo de φ, denotado por $I(\varphi)$, es el conjunto de todos los elementos $a \in R$ tales que $\varphi\ a = 0$, el elemento cero de R'.

Lema 1.9 Si φ es un homomorfismo de R en R' con núcleo $I(\varphi)$, entonces:

1) $I(\varphi)$ es un subgrupo de R bajo la adición.
2) Si $a \in I(\varphi)$ y $r \in R$ entonces tanto ar como ra están en $I(\varphi)$.

Prueba. Como φ es, en particular, un homomorfismo de R, como grupo aditivo, en R', como grupo aditivo, en (1) sigue inmediato de nuestros resultados en teoría de grupos.

Para ver (2), supongamos que $a \in I(\varphi)$, $r \in R$. Entonces $\varphi\ a\ = 0$, de modo que $\varphi\ ar\ = \varphi\ a\ \varphi\ r\ = 0\varphi\ r\ = 0$, de acuerdo con lema (1.10).

Análogamente $\varphi\ ra\ = 0$. Luego, por la propiedad definitoria de $I\ \varphi$, tanto ar como ra están en $I\ \varphi$.

IDEALES

Una vez que se han establecido las ideas de homomorfismo y su núcleo para anillos, basadas ambas en nuestra experiencia con los grupos, parece que ha der ser fructuoso establecer también para anillos algo análogo al concepto de subgrupo normal.

Después de haber logrado esto puede esperarse que este análogo conduzca a una construcción sobre anillos semejante a la del grupo cociente de un grupo por un subgrupo normal. Finalmente, si alguien fuera optimista, esperaría que los teoremas de homomorfismos sobre grupos se pudieran aplicar íntegramente a los anillos.

La primera tarea que nos encontramos parece que es la de definir un concepto adecuado de "subgrupo normal" para anillos. Con un poco de intuición esto no resulta tan difícil. Recordemos que los subgrupos normales resultaban no ser otra cosa en el último término que núcleos de homomorfismos, aunque en sus primeras condiciones definitorias no aparecieran los homomorfismos para nada. Entonces, ¿Por qué usar esta observación como clave de nuestra definición para anillos? El lema 1.2.5.9 nos ha proporcionado ya algunas condiciones de las que un subconjunto de anillo debe cumplir para que pueda ser el núcleo de un homomorfismo. Tomamos ahora el punto de vista de

que ya que al menos al presente no tenemos ninguna otra información de que disponer, haremos de las conclusiones del lema 1.9 nuestro punto de partida para nuestra tarea, por lo que definiremos:

Definición 1.21 Un subconjunto no vacío I de R se dice que es un ideal (bilateral) de R si:

1) I es un subgrupo de R bajo la adición.
2) Para todo $i \in I$ y $r \in R$ tanto ir como ri están en I

La condición (2) afirma que I "absorbe" la multiplicación a la derecha y a la izquierda por elementos arbitrarios del anillo. Por esta razón I comúnmente se llama ideal bilateral. Como no tendremos ninguna ocasión de usar algún otro concepto de ideal, solo usaremos la palabra ideal en lugar de ideal bilateral en todo lo que sigue.

Definición 1.22 Un ideal $\boldsymbol{C}$ en un anillo A es un subconjunto no vacío de A con estas propiedades:

1) C es subgrupo aditivo de A.
2) Si $c \in C$ y $a \in A$, entonces $ac, ca \in C$.

Teorema 1.5 En cualquier homomorfismo H de un anillo A**,** el conjunto de elementos que tienen cero por imagen es un ideal en A**.**

Prueba:

1) En general, llamemos C al conjunto de todos los elementos $c \in A$ para los que $H(c) = 0'$, siendo $0'$ el elemento cero en la imagen A'. En tal caso, para cualquier $a \in A$**,** $ac\ H = aH\ \ cH\ = (aH)O'$ y

   $ca\ H = cH\ \ aH\ = 0'$. (Lo que demuestra la parte 1)

2) $c_1H = c_2H = 0'$ esto implica que

$$c_1H - c_2H = (c_1 - c_2)H\ = c_1H - c_2H$$

$$= 0' - 0' = 0'$$(lo que demuestra parte 2).

CAPITULO II

ANILLOS DE POLINOMIOS

Es probable que ya se tenga alguna idea bastante manejable de lo que es un polinomio en x con coeficiente en un anillo R. En cursos anteriores se aprendió a realizar operaciones tales como la suma y la multiplicación de dichos objetos, se ha hecho por mucho tiempo y se sabe lo que significa el Grado de un Polinomio.

Nuestro principal problema es determinar dos aspectos: Explicar qué es un Polinomio y además explicar qué es x. Si definimos un polinomio con coeficientes en un anillo R como una suma formal finita.

$$\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n,$$

donde $a_i \in R$, se verán algunas dificultades. Ciertamente, $0 + a_1 x$ y $0 + a_1 x + 0x^2$ son diferentes como sumas formales, pero queremos considerarlas como el mismo polinomio. Quizá la mejor manera es definir un polinomio como una suma formal infinita

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + \ldots, (a_n \neq 0)$$

donde $a_i = 0$ para todos, o en un número finito de valores de i. Ahora ya no existe el problema de tener más de una suma formal representando lo que deseamos considerar como un solo polinomio.

En este apartado, los polinomios serán estudiados desde el punto de vista de su estructura de Anillo. Este nuevo enfoque aclarara muchos de los conceptos relacionados con lo que se está investigando.

Definición 2.1 Sea A un anillo. Un polinomio en la variable x es una suma formal

$$f\ x\ =\ \sum_{i=1}^{\infty} a_i\, x^i\,,$$

donde $a_i \in A$, para todo $i \geq 0$, y $a_i = 0$, para todo i, excepto un número finito de ellos.

Observación 1. Podemos dar una definición de lo que es un polinomio, sin hacer referencia a la variable $x.(2.24)$

Definición 2.2 Sea A un anillo. Un polinomio sobre A es una sucesión infinita$(a_0, a_1, \dots, a_n, \dots)$ donde $a_i \in A$; para todo i y $a_i = 0$ para casi todos los i.

Una sucesión ($a_0, a_1, \dots, a_n, \dots$) donde casi todos los a_i son iguales a cero, se denomina una sucesión casi nula.

La definición (2.2) es más formal que la definición (2.1) pues no hace uso de la variable x. Sin embargo el símbolo x se ha utilizado para expresar los polinomios desde

hace mucho tiempo y aún se usa en la actualidad. Para mantenernos en esta tradición usaremos la definición (2.1) de polinomios. Si hacemos

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

entonces la variable x es un polinomio en si misma, y deja de ser un objeto desconocido.

En este caso se seguirán denotando los polinomios de la manera clásica

$$f\ x\ = a_n x^n + \cdots + a_1 x + a_0,\ (a_n \neq 0)$$

El conjunto de los polinomios sobre el anillo A lo denotaremos por $A[x]$**.**

Definición 2.3 Sea A un anillo. El anillo de polinomios en la variable x con coeficientes en A y que denotamos por $A[x]$, es el conjunto de ecuaciones formales de la forma

$$f\ x\ = a_n x^n + \cdots + a_1 x + a_0,$$

para cada i que pertenece al anillo A. El elemento a_i se denomina el coeficiente de x^i en $f\ x$, y dos polinomios se consideran iguales si para cada i los coeficientes de x^i son iguales.

Por conveniencia, eliminamos los coeficientes nulos. El polinomio cero tiene todos sus coeficientes igual a cero, y lo denotaremos como 0.

Definición 2.4 El grado de $f\ x$ es el mayor entero n tal que a_n es no nulo, el cual se denota por $gr\ f\ x\ = n$ .Si el grado de $f\ x$ es n entonces escribiremos

$$f\ x\ = \ \sum_{k=0}^{n} a_k\, x^k\ ,\ a_k \neq 0,\ \forall k$$

El coeficiente a_n se denomina coeficiente principal de $f\ x$.

Definición 2.5 Si el coeficiente a_n es igual a 1, entonces decimos que $f\ x$ es un Polinomio Mónico.

Ejemplo 1: $x^4 - 3x^3 + 5x^2 - 2x + 1$.

Observación 1: Si el grado de $f(x)$ es n, entonces $a_k = 0$, para todo $k > n$ y escribimos $f\ x\ = a_n x^n + \cdots +\ a_1 x + a_0$,

Es decir, no se colocan aquellos términos $a_i x^i$ con $i > n$, pues son todos nulos.

Observación 2: Si $f(x)$ es un polinomio constante no nulo, entonces

$$gr\ f\ x\ = 0.$$

Se definen tres operaciones en $A[x]$.

Sean $f\ x\ = a_n x^n + \cdots + a_1 x + a_0$ y $g\ x\ = b_m x^m + \cdots + b_1 x + b_0$, entonces definimos la igualdad, la suma y el producto de $f\ x$ y $g\ x$ de la siguiente manera:

IGUALDAD:

$f\ x\ = g(x)$ Si y solo si $a_i = b_i, \forall\ i$

$$(a_n x^n + \cdots + a_1 x + a_0\ ) = (b_m x^m + \cdots + b_1 x + b_0\ )$$

SUMA:

$$f\ x\ + g\ x\ = a_n x^n + \cdots + a_1 x + a_0\ + (b_m x^m + \cdots + b_1 x + b_0)$$

$$= C_k x^k + \cdots + C_1 x + C_O$$

Donde $C_i = a_i + b_i, \quad a \leq i \leq k$

PRODUCTO:

$$f\ x\ g\ x\ = a_n x^n + \cdots + a_1 x + a_0\ (b_m x^m + \cdots + b_1 x + b_0)$$

$$= \mathrm{C_k x^k} + \cdots + \mathrm{C_1 x} + \mathrm{C_O}$$

Donde $C_s = \ _{i+j}\, a_i b_j$, para todo $0 \leq s \leq k$

Con estas operaciones $A[x]$ es llamado Anillo Conmutativo

Proposición 2.1 Sea A un dominio de integridad. Sean $f(x)$ y $h(x)$ dos polinomios no nulos en $A[x]$ de grado n y m respectivamente, entonces:

i) $gr\ f\ x\ +\ h\ x\ \leq max\ n,m$

ii) $gr\ f\ x\ \ h\ x\ = n + m$

Demostración:

i) Supongamos que $n > m$; entonces el coeficiente principal de $f\ x\ + h(x)$ es igual al coeficiente principal de $f\ x$ y por lo tanto

$$gr\ f\ x\ + h\ x\ = gr\ f\ x\ = n = \max\{n, m\}$$

Por otro lado si suponemos que $n = m$, entonces pueden ocurrir dos casos.

I) La suma de los coeficientes principales de $f(x)$ y $h(x)$ es cero. Luego

$$gr\ f\ x\ + h\ x\ < n$$

II) La suma de los coeficientes principales de $f(x)$ y $h(x)$ es distinta de cero.

En este caso $gr\ f\ x\ + h\ x\ = n$

Luego en cualquiera de los dos casos obtenemos la desigualdad deseada.

ii) Para calcular el grado del producto, sean

$$f\ x\ = a_n x^n + \cdots + a_1 x + a_0$$

y

$$h\ x\ = b_m x^m + \cdots + b_1 x + b_0\ ,$$

entonces hacemos la multiplicación.

$$f\ x\ h\ x\ = C_s x^s + \cdots + C_1 x + C_0\ ,\ \ C_s = \quad_{i+j} a_i b_j$$

Afirmamos que $C_{n+m} \neq 0$. En efecto, se tiene que $C_{n+m} = a_n b_m \neq 0$, pues tanto a_n como b_m son no nulos y A es un dominio entero. Luego por otra parte si $s > n + m$ se tiene

$$C_s = \quad_{i+j} a_i b_j$$

Luego cada término $a_i b_j$ en dicha suma es igual a cero, pues se debe tener $i > n$ o bien $j > m$ lo cual implica que $a_i = 0$ o bien $b_j = 0$.

Por lo tanto $C_s = 0$ para $s > n + m$ y así se ha probado que el grado de $f\ x\ g(x)$ es $m + n$.

Teorema 2.1: El conjunto $A\ x$ de polinomios sobre un anillo A, es un anillo con las operaciones de suma y producto de polinomios. Si A es un anillo conmutativo con unidad, entonces $A\ x$ es un anillo conmutativo con unidad.

Demostración: $A\ x$ cumple las propiedades de grupo, además es conmutativo por lo tanto es un grupo abeliano con la suma de polinomios. El elemento neutro para la suma es el polinomio nulo.

Por hipótesis se tiene que $A\ x$ es un conjunto de polinomios sobre A, y A es un anillo conmutativo con unidad.

Se debe probar que si A es conmutativo con unidad entonces $A\ x$ también lo es.

Si $p\ x = a_n x^n + \cdots + a_1 x + a_0$, entonces el opuesto de $p(x)$ es

$$-p\ x = (-a_n)x^n + \cdots + (-a_1)x - a_0.$$

Con respecto al producto, se demuestra que esta operación es asociativa y satisface las leyes distributivas.

Además, si A es conmutativo, sean $f(x)$ y $h(x)$ dos polinomios en $A\ x$ con

$f\ x = a_n x^n + \cdots + a_1 x + a_0$ y $h\ x = b_m x^m + \cdots + bx + b_0$

Entonces se tiene

$$f(x)\ h\ x = C_s x^s + \cdots + C_1 x + C_0 \quad \text{y}$$

$$h\ x\ f(x) = h_s x^s + \cdots + h_1 x + h_0,$$

en donde $s = m + n$, para todo $0 \leq i \leq s$, obteniendo

$$C_i = \sum_{k+j=i} a_k\, b_j$$

$$= \sum_{k+j=i} b_j a_k$$

$$= d_i$$

Donde

$$d_i = \sum_{k+j=i} b_j a_k$$

Luego $h\ x\ f(x) = f(x)\ h\ x$ por tener todos sus coeficientes iguales

Proposición 2.2 Si el anillo A es un dominio de integridad, entonces el anillo $A[x]$ es un Dominio de Integridad.

Demostración: por hipótesis se tiene que A es un dominio de integridad, lo que se debe probar es que $A[x]$ también lo es.

La prueba se realiza por contradicción, partiendo del hecho de que $A[x]$ es un anillo con unidad, de acuerdo con teorema anterior.

A si, sean $f\ x$ y $h(x)$ dos polinomios en $A[x]$, tal que $f\ x\ h\ x = 0$.

Si $f\ x \neq 0$ y $h\ x \neq 0$, se tiene que $gr\ f \leq gr\ fh = gr\ 0 = 0$ y

$$gr\ h \leq gr\ fh = gr\ 0 = 0,$$

luego, f y h deben ser constantes,

digamos $f(x) = a$, $g(x) = b$, $a, b \in A$,

Luego $ab = 0$ y se tendría que $a \neq 0$ y $b \neq 0$ con $ab = 0$ $(\rightarrow\leftarrow)$ por ser A dominio entero.

Observación 3: Todo Dominio entero se puede sumergir en un cuerpo.

Por lo tanto $A\ x$ tiene su cuerpo de cocientes, el cual también se le llama Cuerpo de Funciones Racionales en x y sus elementos son cocientes de polinomios en $A\ x$.

Teorema 2.2 (algoritmo de la división). Sea K un cuerpo y

$$f\ x\ ,\ h\ x\ \in K\ x\ ,\ h(x) \neq 0,$$

entonces existen polinomios $q(x)\ y\ r(x)$ tales que $f\ x\ = h\ x\ q\ x\ + r(x)$

y se tiene que $r\ x\ = 0\ o\ gr\ r(x)\ < gr\ h(x)$.

Demostración: este teorema se realizara en varios casos.

Si $f\ x\ = 0$, tomamos entonces $q\ x\ = 0$ y $r\ x\ = 0$.

Si $gr(f(x)) < gr(h(x))$, tomamos $q\ x\ = 0$ y $r\ x\ = f(x)$.

Supongamos entonces que $gr(f(x)) \geq gr(h(x))$ y pongamos

$$f\ x\ = a_n x^n + \cdots + a_1 x + a_0$$

y

$$gr\ x\ = b_m x^m + \cdots + b_1 x + b_0$$

Con $n \geq m$.

Podemos usar inducción matemática sobre n para obtener el resultado.

Si $n = 0$, entonces

$$f\ x\ = a_0, h\ x\ = b_0$$

y

$$f\ x\ = a_0 {b_0}^{-1} h\ x\ + 0$$

Tomando $q\ x\ = a_0 {b_0}^{-1}$ y $r\ x\ = 0$, se obtiene el resultado

$$f\ x\ = h\ x\ q\ x\ + r(x).$$

Supóngase que el teorema es cierto para todo polinomio de grado k, con $k < n$,

luego

$$f\ x\ - a_n {b_m}^{-1} x^{n-m} h\ x\ = 0, \text{ si } r(x) = 0$$

es un polinomio de grado menor que n y por la hipótesis de inducción matemática existen $q'(x)$ y $r'(x)$ tales que

$$f\ x\ - a_n {b_m}^{-1} x^{n-m} h\ x\ = h\ x\ q'\ x\ + r'(x)$$

Con $r'\ x\ = 0$ o $gr\ r'\ x\ < gr\ h\ x$

Por lo tanto, se tiene que

$$f\ x\ = h\ x\ q'\ x\ + a_n {b_m}^{-1} x^{n-m} + r'\ x$$

Si tomamos $q\ x\ = q'\ x\ + a_n {b_m}^{-1} x^{n-m}$ y $r\ x\ = r'(x)$ se tiene el resultado

$$f\ x\ = h\ x\ q\ x\ + r(x)$$

Observación 4: Los polinomios $q(x)\ y\ r(x)$ del teorema anterior son llamados respectivamente cociente y resto de la división realizada entre $f\ x$ y $h(x)$.

Definición 2.6 Sea K un cuerpo y $f(x)$, $h(x)$ en $K\ x$. Diremos que el polinomio $f(x)$ es divisible entre $h(x)$, si existe otro polinomio $c(x)$ en $K\ x$, tal que

$$f(x) = h(x)c(x).$$

Ejemplo 2: Sea $f\ x\ = 14x^2 - 5x - 6$ y $h\ x\ = 7x - 6$, encontrar el resto y el cociente.

$$f(x)\big|\underline{h(x)}\ = 14x^2 - 5x - 6\ \big|\underline{7x - 6}$$

$$\underline{-14x^2 + 12x} \qquad 2x + 1$$

$$0 + 7x - 6$$

$$\underline{-7x + 6}$$

$$0$$

,

de donde $f(x) = h(x)q(x)$, entonces $14x^2 - 5x - 6 = (7x - 6)(2x + 1)$, con $q\ x\ = 2x + 1$ y $r\ x\ = 0$.

Definición 2.7 Sea $f\ x$ un polinomio en $K\ x$. Diremos que $f(x)$ es un polinomio irreducible en $K\ x$, o irreducible sobre K, si cada vez que $f\ x\ = h\ x\ c\ x$, entonces $h(x)$ o $c(x)$ es una constante.

Definición 2.8 Un elemento x de un anillo conmutativo R es una unidad si existe $y \in R$ de tal forma que $x.y = 1$, donde 1 es el elemento neutro de $(.)$.

"El polinomio $u(x)$ es una unidad, si y solo si el grado de $u(x)$ es igual al grado de polinomio constante". Luego las unidades de $K\ x$ son precisamente los polinomios constantes (distintos de cero), pues $\text{gr}(c) = 0$.

El problema de determinar cuándo un polinomio es irreducible (que se puede factorizar), es uno de los problemas un poco difíciles en el álgebra y ha sido estudiado desde hace varios siglos. Existen criterios que se pueden aplicar en situaciones especiales, como se ve a continuación:

Veamos mediante un ejemplo como se puede determinar si un polinomio es irreducible, usando las técnicas de la teoría de Anillos.

Ejemplo 3: Demostrar que $f\ x\ = x^2 + 1$ es irreducible en $\mathbb{Q}\ x$.

Demostración: Por definición se sabe que un polinomio es irreducible si no se puede factorizar como el producto de polinomios, es decir

$$f\ x\ \neq p(x)q(x).$$

Supongamos que $f(x)$ se puede escribir como $p(x)q(x)$ esto es,

$$f\ x\ = p(x)q(x), \text{ pero}$$

$$f\ x\ = x^2 + 1$$

$$\Longrightarrow x^2 + 1 = 0$$

$$\Longrightarrow x^2 = -1$$

$$\Longrightarrow x = \pm\ \overline{-1}.$$

Por lo tanto $f\ x\ $ no tiene raíces en $\mathbb{Q}[x]$.

Ahora, si factorizamos $x^2 + 1 = 0$ de tal manera que

$$x^2 + 1 = p(x)q(x),$$

de donde $p\ x\ $ y $q(x)$ son de grado 1

$$x^2 + 1 = 0$$

$$\Rightarrow p\ x\ q\ x\ = 0,$$

entonces como $p\ x\ q\ x\ = 0$ se tiene que

$$p\ x\ = 0\ \text{o}\ q\ x\ = 0,$$

luego $p\ x\ = 0$ es de grado 1, pero esto quiere decir entonces tiene una sola raíz y de la misma forma $q\ x\ = 0$.

De donde obtenemos dos raíces, lo cual no es cierto ya que demostramos anteriormente que

$$f\ x\ = x^2 + 1$$

no tiene solución en $\mathbb{Q}\ x$.

Por lo tanto $f\ x$ es irreducible.

De aquí podemos concluir que un polinomio de grado 2 es irreducible si y solo si no tiene raíces

RAICES DE POLINOMIOS.

Definición 2.9 Sea K un cuerpo. Una extensión F de K es un cuerpo que contiene a K como sub-cuerpo, es decir K es un cuerpo con las mismas operaciones definidas en F.

Ejemplo 4: Los números complejos $\mathbb{C}$ son una extensión de cuerpo de los números reales$\mathbb{R}$.

Observación 5: Si F es una extensión de K y $f(x)$ es un polinomio en $K[x]$, entonces los coeficientes de $f(x)$ están todos en K y por lo tanto en F, luego $f(x)$ esta en el anillo $F\ x$.

Definición 2.10 Sea K un cuerpo, F una extensión de K y

$$f\ x\ = a_n x^n + \cdots + a_1 x + a_0$$

un polinomio en $K\ x$. Entonces si $\lambda \in F$, el valor del polinomio $f(x)$ en el elemento λ, denotado por $f(\lambda)$ es el elemento de F dado por

$$f\ \lambda\ = a_n \lambda^n \ldots a_1\ \lambda + a_0\ .$$

Proposición 2.3 Sea K un cuerpo, F una extensión de $K\ x$, y $\lambda \in F$.

Entonces la función

$$\phi_\lambda : K\ x\ \rightarrow F$$

$$h\ x\ \rightsquigarrow \phi_\lambda\ h\ x\ = h\ \lambda$$

es un homomorfismo de anillos.

La imagen de $f(x)$ bajo ϕ_λ es un cambio de variable de x por λ, o la evaluación de $f(x)$ en λ.

Demostración: Sean $f(x)$ y $h(x)$ dos polinomios en $K(x)$, entonces

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

y

$$h\ x\ = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$$

luego la suma está dada por

$$\phi_\lambda(f\ x\ + h(x))$$

Supongamos $n \geq m$, (el caso n$<$ m es analogo)

$$\phi_\lambda(f\ x\ + h(x)) = \phi_\lambda(a_n x^n + \cdots + a_0 + b_m x^m + \cdots + b_0)$$

$$= \phi_\lambda(a_n x^n + \cdots + (a_m + b_m)x^m + \cdots + (a_0 + b_0))$$

$$= a_n \lambda^n + \cdots + (a_m + b_m)\lambda^m + \cdots + (a_0 + b_0)$$

$$= a_n \lambda^n + \cdots + a_0 + b_m \lambda^m + \cdots + b_0$$

$$= \phi_\lambda\ a_n x^n + \cdots + a_0\ + \phi_\lambda\ a_m x^m + \cdots + b_0$$

$$= \phi_\lambda(f\ x\ + \phi_\lambda(h(x))$$

Con respecto al producto, hagamos

$$f\ x\ h(x) = d_t x^t + d_{t-1}x^{t-1} + \ldots + d_1 x + d_0,$$

Donde $t = n + m$ y

$$d_i = \sum_{k+j=i} a_k b_j , \quad 0 \leq i \leq t$$

Luego de aquí se tiene que

$$\phi_\lambda\ f\ x\ h\ x\ = d_t\lambda^t + d_{t-1}\lambda^{t-1} + \ldots + d_1\lambda + d_0 \qquad (1)$$

y por otro lado

$\phi_\lambda\ f\ x\ \phi_\lambda h\ x$

$$= (a_n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0)(b_m\lambda^m + b_{m-1}\lambda^{m-1} + \ldots + b_1\lambda + b_0$$

$$= d_t\lambda^t + d_{t-1}\lambda^{t-1} + \ldots + d_1\lambda + d_0 \qquad (2)$$

Con $t = n + m$ y

$$d_i = \sum_{k+j} a_k b_j \ , \qquad 0 \leq i \leq t$$

Comparando las expresiones (1) y (2), vemos que ellas son iguales y por lo tanto

$$\phi_\lambda(\ f\ x\ h\ x\ = \phi_\lambda\ f\ x\ )\phi_\lambda h\ x\ .$$

Luego ϕ_λ es un homomorfismo de anillos.

Definición 2.11 Una raíz o un cero de un polinomio $f\ x\ \in K\ x\ $ es un elemento λ en una extensión F de K, tal que $f\ \lambda\ = 0$.

También diremos que el valor de λ anula al polinomio o que λ es una solución de la ecuación $f\ x\ = 0$.

Ejemplo 2.5: Los valores 1 y -1 anulan al polinomio $f\ x\ = x^4 - 1$ en $\mathbb{Q}[x]$, pues $f\ 1\ = 1^4 - 1 = 0$ y $f\ -1\ = 1^4 - 1 = 0$.

Ejemplo 2.6: Sea $f\ x\ = x^2 + 1$ en $\mathbb{Q}\ x\ $. Entonces $i = \ \overline{-1}$ es una raíz de $f\ x\ $, pues $f\ i\ = i^2 + 1 = 0$. notese que i esta en $\mathbb{C}$ pero no en $\mathbb{Q}$.

Teorema 2.3 Sea $f\ x\ $ un polinomio en $K\ x\ ,\ F\ $ una extensión de K y $\lambda \in F$ una raíz de $f\ x\ $. Entonces $f\ x\ $ se factoriza en $F\ x$

$$f\ x\ =\ x - \lambda\ q(x),$$

donde $q(x)$ es un polinomio de grado igual al grado de $f\ x\ $ menos uno.

Demostración: Haciendo la división de $f\ x\ $ entre el polinomio $x - \lambda$ se generan polinomios $q\ x\ $ y $r(x)$ tales que

$$f\ x\ =\ x - \lambda\ q\ x\ + r(x) \qquad (1)$$

Con $r\ x\ = 0$ o $g\ r\ x\ < g\ x - \lambda\ = 1$

Luego el grado de $r\ x\ $ debe ser cero y por lo tanto es un polinomio constante $r\ x\ = \sigma$; con $\sigma \in K$. Haciendo la evaluación de los polinomios en (1) el valor de λ, tenemos que

$$f\ x\ =\ x - \lambda\ q\ x\ + r(x)$$

$$f\ \lambda\ =\ \lambda - \lambda\ q\ \lambda\ + \sigma\ \ \text{(por ser } r\ x\ = 0)$$

$$f\ \lambda\ = 0(q\ \lambda\ ) + \sigma\ ,$$

$f\ \lambda\ = 0\ + \sigma$, pero $\ f\ \lambda\ = 0$ por ser raíz, luego

$$\sigma = 0$$

$$0 = \sigma$$

De donde $\sigma = 0$ por lo tanto en (1) se tiene $f\ x\ =\ x - \lambda\ q\ x$

Un polinomio del tipo $ax + b$ se llama polinomio lineal. Si bien es cierto todo polinomio lineal es irreducible, pues si $ax + b = p\ x\ q\ x\ ,$ entonces la suma de los grados de ellos debe ser igual a 1, por lo tanto $p\ x\ $ o $\ q\ x\ $ es de grado cero, por lo cual es un polinomio constante.

Definición 2.12: Sea $f(x)$ un polinomio en $K\ x$. Diremos que $f(x)$ se factoriza completamente en una extensión F en K, si existen raíces $\lambda_1, \dots, \lambda_t$ en F tal que

$f\ x\ = a_n\ x - \lambda_1\ \ x - \lambda_2\ \ \dots (x - \lambda_t)$, donde $a_n \in K$.

Observación 6: Una de las metas más importantes en la teoría de los polinomios es el poder factorizar cualquier polinomio como un producto de factores lineales. Lamentablemente esto no es posible en cualquier cuerpo K, pues por ejemplo

$$f\ x\ = x^2 + 1$$

no se puede factorizar en $\mathbb{Q}\ x$ como producto de factores lineales, dado que este polinomio no tiene solución en los reales.

Sin embargo siempre se puede hallar una extensión del cuerpo K en donde este problema se resuelve.

Definición 2.13 Una raíz λ de $f(x)$ se dice que tiene multiplicidad K, si

$f\ x\ =\ x - \lambda\ ^k q(x)$ y λ no es raíz $q(x)$.

Teorema 2.4 Sea $f(x)$ un polinomio en $K[x]$ de grado n, entonces $f(x)$ tiene

A lo sumo n raíces en cualquier extensión F de K.

Demostración: (por inducción sobre el grado de $f(x)$).

i) Probamos para $n = 0$

Si $n = 0$, entonces el polinomio $f(x)$ es constante, es decir $f\ x\ = c$, $c \in K$ y no tiene raíces.

Por lo tanto no hay nada que probar.

ii) Ahora probamos para $n = 1$.

Si $n = 1$, entonces la función $f(x)$ es un polinomio lineal, es decir, $f\ x\ = ax + b$, para algunos a y b en K . Sea λ una raíz de $f\ x\ $,

λ es una raíz de $f\ x\ $, entonces $f\ x\ = a\lambda + b$;

$$a\lambda + b = 0$$

$$\Rightarrow a\lambda = -b \Rightarrow \lambda = -b/a,$$

y por lo tanto $\lambda = -b/a$ es una raíz, además es única y se hace referencia al teorema (**2.3**).

iii) Supongamos ahora que el teorema es cierto para todo polinomio de grado menor que n y probemos que se cumple para todo polinomio de grado n.

Sea F una extensión de K, si $f(x)$ no tiene ninguna raíz en f, entonces no hay nada que probar.

Si $f(x)$ tiene una raíz λ en F de multiplicidad m, entonces $f\ x\ = \ x - \lambda\ ^m q(x)$, donde $q(x)$ es de grado $(n - m)$ que no tiene a λ como raíz.

Podemos entonces aplicar la hipótesis de inducción a $q(x)$ para concluir que no tiene mas de $(n - m)$ raíces en F . Como toda raíz de $q(x)$ es una raíz de $f\ x\ $, se deduce entonces que $f\ x\ $ tiene a lo sumo $m + \ n - m\ = n$ raíces en F .

Con esto se ha probado el teorema para polinomios de grado n.

2.1.3 POLINOMIOS SOBRE RACIONALES.

Proposición 2.4 Sea $f(x)$ un polinomio de $grado \leq 3$ en $\mathbb{Q}\ x$, entonces si $f\ x$ es reducible en $\mathbb{Q}\ x$, existe $r \in Q$ tal que $f\ r\ = 0$.

Demostración: Por hipótesis se tiene que $f(x)$ es reducible, entonces existen polinomios $h\ x$ y $g(x)$ en $\mathbb{Q}\ x$ tal que $f\ x\ = h(x)g(x)$ y además $h\ x$ y $g(x)$ no son constantes.

Luego se tiene que

$$3 = grado\ f\ x\ = gradoh\ x\ + grado\ g(x),$$

Por lo tanto el grado de $grado\ h\ x$ $o\ grado\ g(x)$ debe ser igual a uno. Si suponemos que el grado de $h\ x$ es uno, entonces $h\ x\ = ax + b$ con $a, b \in Q$, y luego

$$f\ x\ = (ax + b)g(x).$$

Si $b = 0$, entonces $r = 0$ es raíz de $f(x)$.

$$f\ r\ = ar + b\ g\ r$$

$$\Rightarrow\ ar + 0\ g\ r\ = 0$$

$$\Rightarrow\ ar\ g\ r\ = 0$$

$$\Rightarrow ar = \frac{0}{g\ r}$$

$$\Rightarrow ar = 0\ (a \neq 0)$$

$$\Rightarrow r = 0$$

Si $b \neq 0, \Longrightarrow f\ r\ = \ ar + b\ g\ r\ \Rightarrow\ ar + b\ g\ r\ = 0$

$$\Rightarrow\ ar + b\ = 0/(g\ x\ )$$

$$\Rightarrow ar + b = 0$$

$$\Rightarrow ar = -b$$

$$\Rightarrow r = -b/a$$

Por lo tanto $r = -b/a$ es una raíz de $f(x)$

Definición 2.14 Sea $f\ x\ = a_n x^n + \cdots + a_1 x + a_0$ un polinomio en $\mathbb{Z}[x]$. Se define el contenido o característica de $f(x)$ como el máximo común divisor de los coeficientes $a_0, a_1, \ldots, a_n$.

Usaremos la notación $C(f)$ para representar el contenido de $f(x)$.

Ejemplo 7: Si $f\ x\ = 12x^3 - 6x^2 + 18x$, entonces $C\ f\ =\ 12, 6, 18\ = 6$.

Definición 2.15 Sea $f(x)$ un polinomio con coeficientes enteros. Entonces se dice que $f(x)$ es primitivo (el máximo común divisor de los a_i es igual a 1), si $C\ f\ = 1$.

Ejemplo 8: Sea $f\ x\ = 6x^5 + 3x^4 - 2x^3 + 7x^2 + 5x$, este es un polinomio primitivo, ya que el máximo común divisor de los $a_i = 1$, se ve entonces que el contenido de $f\ x\ = 1$

Definición 2.16: Un polinomio se dice que es Mónico, si el coeficiente de la variable de mayor exponente es 1.

Observación 7: Si $f(x)$ es un polinomio Mónico con coeficientes en Z, entonces $f(x)$ es primitivo.

Ejemplo 9: En $Z\ x$, $4x^2 + 3x + 2$ es primitivo, pero $4x^2 + 6x + 2$ no lo es, pues el 2 no es una unidad en Z**,** es el Máximo Común Divisor de los coeficientes. Claramente, todo irreducible no constante en $Z\ x$ debe ser un polinomio primitivo.

Proposición 2.5 (Lema de Gauss) Sea $f\ x$ un polinomio primitivo en $Z\ x$.

Si $f\ x\ = p\ x\ q\ x$ con $p\ x$, $q\ x$ en $Q\ x$, entonces $f\ x\ = p_1(x)q_1(x)$, donde $p_1(x),\ q_1(x)$ son polinomios con coeficientes enteros. Además

$$p_1\ x\ = \lambda p(x)\ \text{ y }\ q_1\ x\ = \beta q_1\ x\ ,$$

Con λ y β números racionales.

Demostración: Por hipótesis se tiene que $f(x)$ es primitivo en $Z\ x$, entonces se probará que $f(x)$ es irreducible o que se puede factorizar de la forma

$$f\ x\ = p_1(x)q_1(x).$$

Sea $p\ x\ = r_s x^s + \cdots + r_1 x + r_0,\ r_i\ \in\ Q$

$$q\ x\ = t_l x^l + \cdots + t_1 x + r_0,\ t\ \in\ Q$$

Sean m_1 , m_2, el mínimo común múltiplo de los denominadores de $p(x)$ y $q\ x$ respectivamente.

Luego $m_1 p(x)$ y $m_2 q(x)$ son polinomios con coeficientes enteros. Si hacemos

$$C_1 = C(p(x)) \quad \text{y} \quad C_2 = C(q(x))$$

Definamos entonces

$$p_1\ x\ = \frac{m_1}{C_1} p(x)\ \text{ y }\ q_1\ x\ = \frac{m_2}{2} q(x), \text{ luego}$$

$p_1\ x$ y $q_1\ x$ son polinomios primitivos,

y además

$$f\ x\ =\ p(x)\ q\ x$$

$$= \frac{C_1 C_2}{m_1 m_2} p_1\ x\ \ q_1\ x\ ,$$

de tal manera que

$$m_1 m_2 f\ x\ = C_1 C_2 p_1\ x\ \ q_1\ x$$

Como $f\ x$ es monico, el contenido del lado izquierdo es $m_1 m_2$ y por lo tanto

$$m_1 m_2 = C_1 C_2.$$

Luego $f\ x\ = p_1(x) q_1(x)$.

Teorema 2.5 (Criterio de Herstein) Sea $f\ x\ = a_n x^n + \cdots + a_1 x + a_0$ un polinomio con coeficientes enteros. Sea p un número primo, tal que

i) $p | a_i \quad 0 \leq i < n$

ii) $p \nmid a_n$

iii) $p^2 \nmid a_0$

Entonces $f\ x$ es irreducible en $\mathbb{Q}\ x$.

Demostración: Esta prueba se divide en dos casos:

Por hipótesis tenemos que $p | a_i \quad 0 \leq i < n,\ p \nmid a_n$ y $p^2 \nmid a_0$. Lo que se debe probar es que $f(x)$ es irreducible.

Caso I: La prueba se realiza por contradicción. Si $f(x)$ es un polinomio primitivo y además es reducible en $\mathbb{Q}\ x$ entonces por el lema de Gauss se tiene que

$$f\ x\ = h(x)q(x)$$

Con $h(x),\ q(x) \in\ Z[x]$.

Sea $h\ x\ = b_s x^s + \cdots + b_1 x + b_0$, y $q\ x\ = C_t x^t + \cdots + C_1 x +\ C_0$.

Ahora, comparando los coeficientes de grado cero, tenemos que $a_0 = b_0 C_0$

También como $p|a_0$ y $p^2 \nmid a_0$, se tiene $p|b_0 c_0$, pero no puede dividir a ambos.

Luego supongamos que $p|b_0$ y $p \nmid C_0$.

Si $p|b_i$ para todos los i, entonces $p|a_i$ para todos los i, y por lo tanto $f(x)$ no es primitivo.

Supongamos que $p|b_i$, para $0 \leq i < k < s$ y $p \nmid b_k$, luego se tiene

$$a_k = b_k C_0 + b_{k-1} C_1 + \cdots + b_0 C_k$$

y por hipótesis $p|a_k$ entonces $p|\ a_k - (b_{k-1} C_1 + \cdots + b_0 C_k)$ lo cual es una contradicción, ya que $p \nmid C_0$.

Por lo tanto $f\ x$ no es reducible en $\mathbb{Q}\ x$.

CASO II: Si $f\ x$ no es Mónico, hacemos

$$f\ x\ = d f_1\ x\ ,$$

Donde $f_1\ x$ es primitivo con coeficientes enteros. Luego los coeficientes de $f_1\ x$ satisfacen la hipótesis de que p (número primo divide a_i $(0 < i < n)$), además $f_1\ x$ es primitivo entonces cumple que $p \nmid a_n$ y por lo tanto $p \nmid d$.

SUB-CAMPOS

Caracterizamos en esta parte el concepto de sub-campo de un campo dado. Pretendemos establecer que el conjunto de los sub-campos de un campo K es una familia de Moore y retículo completo.

Definición de familia de Moore 2.17: Una familia de Moore sobre un conjunto

$$K = \ 0,1, \dots n-1$$

es una colección de conjuntos L cerrada para la operación de intersección y que contiene K.

Definición de Retículo 2.18: es una estructura algebraica con dos operaciones binarias o bien un conjunto parcialmente ordenado con ciertas propiedades específicas.

Característica De Un Campo

Es importante tener en cuenta que solo los campos finitos tienen característica no nula, esto tiene gran importancia a la hora de resolver la ecuación de la forma

$$x^N - \ x \ = \ 0,$$

pues la característica del campo de las raíces está relacionada con el grado de esta ecuación.

Definición 2.19 Se llama característica de $x \in K - \{0\}$, *car x*, al mínimo entero positivo p tal que $p.x = 0$. El elemento x será de característica nula si y solo si $p.x = 0$ cuando $p = 0$.

Definición 2.20 El sub-campo del campo $(K, +, \cdot)$, generado por el elemento identidad e, recibe el nombre de sub-campo primo de K se representará en adelante por la expresión $(\pi_K, .)$ el sub-campo primo es así, por construcción, el mínimo de K, contenido en cualquier otro sub-campo de K. Esto quiere decir que los elementos mínimos y máximos del retículo completo de los sub-campos de K (familia F_K) son:

$$\min F_K = \pi_K$$

$$\max F_K = K.$$

EXTENSIONES DE CAMPO

En este apartado, se observaran algunas relaciones entre campos como K y F, donde $F \subset K$, ya que K es la extensión (o campo de extensión) de F, y a F se le llama un sub campo de K.

Definición 2.21 Si el campo L es extensión del cuerpo K, puede considerarse el campo L como espacio vectorial sobre el campo K. La dimensión de este espacio vectorial se

llama grado de la extensión y se simboliza por $L : K$ o L/K , símbolos utilizados también para indicar que L es una extensión sobre K y se lee "L sobre K".

A lo largo del trabajo se observaran relaciones entre campos K y F, donde $F \subset K$, se le llama a K una extensión (o campos extensión) de F, y F un sub-campo de K.

Teorema 2.6: Sean $F \subset K \subset L$ tres campos tales que ambas $L:K \ y \ K:F$ son finitas. Entonces L es una extensión finita de F y $L:F = L:K \ L:F$.

Demostración: Se probará que L es una extensión de F mostrando explícitamente una base finita de L sobre F . Al hacerlo se obtendrá el resultado más fuerte afirmando en el teorema, que $L:F = L:K \ K:F$.

Supóngase que $L:K = m$ y $K:F = n$; entonces L tiene una base $v_1, v_2, \dots, v_m$ sobre K y K tiene una base $w_1, w_2, w_3, \dots., w_n$ sobre F. Se probará que los mn elementos $v_i w_j$, donde $i = 1,2, \dots, m$ y $j = 1,2,3, \dots, n$ constituyen una base de L sobre F.

Se empieza por demostrar que, por lo menos, estos elementos generan L sobre F; esto demostrará que L es una extensión finita de F. Sea $a \in L$; dado que los elementos $v_1, v_2, \dots, v_m$ forman una base de L sobre K, se tiene que

$$a = k_1 v_1 +, \dots , + k_m v_n,$$

Donde

$$k_1, k, k_3, \dots., k_n$$

están en K. Puestos que $w_1, w_2, w_3, \dots., w_n$ es una base K sobre F se puede expresar cada k_i como $k_i = f_{i1} v_1 + f_{i2} v_2 + \cdots + f_{in} v_n$, donde f_{ij} están en F.

Sustituyendo esta expresión de los k_i en la expresión anterior de a, se obtiene

$$a = (f_{11}v_1 + f_{12}v_2 + \cdots + f_{1n}v_n)w_1 + \cdots + (f_{m1}v_1 + f_{m2}v_2 + \cdots + f_{mn}v_n)w_n.$$

Por lo tanto, descifrando explícitamente esta suma, se obtiene que

$$a = f_{11}v_1w_1 + f_{12}v_2w_1 + \cdots + f_{1n}v_nw_1 + \cdots + f_{ij}v_jw_i + f_{mn}v_nw_m$$

De esta manera los mn elementos v_iw_j de L, generan L sobre F; por lo tanto $L:F$ es finita y, en efecto $L:F \leq mn$.

Para demostrar que, $L:F = mn$; se necesita solamente probar que los mn elementos v_iw_j anteriores son linealmente independientes sobre F, ya que entonces junto con el hecho de que generan L sobre F, se tendrían que forman una base de L sobre F, de donde por el teorema 1.1.9.1 se llegaría al resultado deseado donde

$$L:F = mn = L:K \quad K:F .$$

Supongamos entonces que para algún b_{ij} en F se tiene la relación

$$0 = b_{11}v_1w_1 + b_{12}v_2w_1 + \cdots + b_{1n}v_nw_1 + b_{21}v_2w_1 + \cdots + b_{2n}v_2w_n + \cdots +$$

$$b_{m1}v_mw_1 + \cdots + b_{mn}v_mw_n ,$$

reduciendo términos en esta suma, se obtiene que $c_1v_1 + c_2v_2 + \cdots + c_nv_m = 0$ donde,

$$c_1 = b_{11}w_1 + \cdots + b_{1n}w_n,\ldots, \quad c_m = b_{m1}w_1 + \cdots + b_{mn}w_n,$$

puesto que los c_i son elementos de K, se tiene que

$$c_1 = c_2 = \cdots = c_m = 0.$$

Por consiguiente, solo la combinación lineal trivial, con todos los coeficientes cero, de los elementos v_iw_j sobre F puede ser cero. Por lo tanto los v_iw_j son linealmente independientes sobre F.

Definición 2.22 Se llama familia Moore (o sistema de Clausura) a todo conjunto $\mathcal{F}$ de partes de un conjunto dado E que tiene las propiedades:

1) $E \in \mathcal{F}$ (Luego es su elemento máximo)
2) Toda intersección (finita o infinita) de partes pertenecientes a $\mathcal{F}$ perteneces a $\mathcal{F}$.

Definición 2.23 Si K es un campo, H sub-campo de K y S una parte cualquiera de K, el mínimo sub-campo V que contiene a H y a S se denomina extensión de H por adjunción de S y se simboliza por $H(S)$.

Evidentemente $H(S) = (HUS)'$, es decir, se trata de la clausura de Moore en la familia de Moore de los sub-campo de K.

Si $\boldsymbol{S}$ tiene un solo elemento, S = {a}, H(S) se dirá extensión simple del campo H.

Proposición 2.6 Si H es un sub-campo de K, S_1, S_2 son dos partes cualesquiera de K, entonces se cumple que:

$$H(S_1 U S_2) = H(S_1)(S_2)$$

Demostración: Por definición se tiene que

$$H(S_1 U S_2) = (\mathrm{H} \cup (H(S_1 \cup S_2)))' \quad \text{(clausura de Moore)}$$

$$H\ S_1\ \ S_2 = H\ S_1 \cup S_2\ \ ' = \mathrm{H} \cup S_1\ ' \cup S_2\ ' \quad \text{(Clausura de Moore)}$$

a) puesto que $H, S_1, S_2 \subseteq H\ S_1\ \ S_2$

$$\Longrightarrow H(S_1 \cup S_2) \subseteq H(S_1)(S_2)$$

b) puesto que $H, S_1 \subseteq H\ \ S_1 \cup S_2 \Rightarrow H\ S_1 \subseteq H\ \ S_1 \cup S_2$

$$\Rightarrow H\ S_1 \subseteq H\ S_1 \cup S_2 \cup S_2 \subseteq H\ S_1 \cup S_2$$

$$\Rightarrow H(S_1)(S_2) \subseteq H\ (S_1 \cup S_2)$$

por lo tanto de a) y b), se tiene que

$$H\ (S_1)(S_2) = H\ S_1 \cup S_2\ .$$

En particular,

$$H\ a_{1,}a_2, \dots, a_n = H\ a_{1,}\ a_2\ \dots(a_n),$$

es decir, se puede reemplazar la adjunción simultánea de n elementos del campo K por n adjunciones sucesivas.

Definición 2.24: Un grupo el cual puede ser generado por un solo elemento se llama grupo cíclico.

Es decir hay un elemento A del grupo G (llamado generador de G) tal que todo elemento de G puede ser expresado como una potencia de A. Si la operación del grupo se denota aditivamente se dirá que todo elemento de G se puede expresar como na, para n entero.

Definición (grupo cíclico) 2.25 Se llama subgrupo cíclico generado por a al subgrupo $a = \{aK \ \ k \in Z\}$.

En otras palabras, G es cíclico con generador A, si $G = \{na/n \in Z\}$. Dado que un grupo generado por un elemento de G es, en sí mismo un subgrupo de G, por definición el único subgrupo de G que contiene a A es el mismo G para ver que este es cíclico.

CAPITULO III

ANILLOS DE IDEALES PRINCIPALES, DE FACTORIZACION UNICA Y ANILLOS EUCLIDIANOS

En este capítulo nos dedicaremos al estudio de algunos anillos especiales que poseen ciertas condiciones adicionales a las propias de la definición de anillo, como lo son Anillos de Ideales Principales, Anillos de Factorización Única y Anillos Euclidianos.

Una de las propiedades fundamentales del anillo de los números enteros es lo que afirma el llamado teorema fundamental de aritmética o teorema de factorización única el cual se enuncia de la siguiente manera: todo número entero puede expresarse de manera única como un producto de número primos.

Este teorema fue demostrado por primera vez por Euclides, aunque la primera demostración completa apareció en las disquicitiones Aritméticae (Este es un libro de teoría de números escrito por el matemático Alemán Carl Friedrich Gauss en 1798 cuando tenía 21 años de edad y publicado en 1801) de Carl Friedrich Gauss.

En este capítulo desarrollamos algunos anillos que poseen propiedades de factorización y divisibilidad, entre ellos se encuentran los Anillos Euclidianos que son a la vez Anillos de Factorización Única, de los cuales nos ocuparemos en el presente capítulo, analizando algunas de sus aplicaciones.

ANILLOS DE IDEALES PRINCIPALES

Iniciamos este capítulo con algunas definiciones muy importantes, las cuales nos servirán como una herramienta para una mejor comprensión de nuestro trabajo.

Definición 3.1 Dos elementos a y b en el anillo R, se dice que son asociados si existe una un unidad u en R tal que $a = bu$

Definición 3.2 Sea D un dominio entero. Decimos que un ideal de este dominio entero D es principal si esta generado por un solo elemento.

$$I = (a) = \text{ ra/r} \in \text{D}$$

Definición 3.3 Un dominio entero para el cual todo ideal es principal es llamado Anillo de Ideales Principales.

Ejemplo 1: Todo campo es un Anillo de Ideales Principales, su demostración es fácil ya que un campo solo tiene 2 ideales. El conjunto de los números enteros es un Anillo de Ideales Principales.

Definición 3.4: Un ideal maximal(o sin divisores) del anillo A es un ideal $\mathfrak{m}$ que no tiene más ideales (o divisores) que A y el mismo, es decir

$\mathfrak{m} \subset \mathfrak{m}' \subseteq A$ implica que $\mathfrak{m}' = A$.

Proposición 3.1 Sea D un Anillo de Ideales Principales. Un elemento $p \in D$ es primo si y solo si (p) es maximal.

Demostración: Por hipótesis se tiene que D es un Anillo de Ideales Principales, además de que p es primo, entonces lo que se debe probar es que p es maximal, la prueba se lleva a cabo por el método de contradicción.

Supóngase que (p) es maximal, entonces no hay nada que probar dado que si (p) es maximal p es un número primo. Por otro lado supóngase que (p) no es maximal, entonces p esta contenido en un ideal maximal (p') . En particular como

$$p \subset (p') \text{ , } p' | p.$$

Se sigue que si $p' | p$, p debe ser igual a tp' es decir $p = tp'$, y como p no divide a p', entonces debe dividir a t. En particular, p' divide a p. Se sigue entonces que $p = tp'$, y como p no divide a p', entonces debe dividir a t.

De donde t seria igual a ps (dicho de otra forma $t = ps$), pero de aquí se tendría que $tp' = 1$, pero esto nos lleva a una contradicción ya que (p') es ideal propio y por lo tanto (p) es maximal.

Luego $t = ps$, de donde $tp' = 1$, pero esto es imposible ya que (p') es un ideal propio.

Definición 3.5: El máximo común divisor (MCD) de dos o más expresiones algebraicas es la expresión algebraica de mayor coeficiente numérico y de mayor grado que está contenida exactamente en cada una de ellas.

Teorema 3.1 Sea D un Anillo de Ideales Principales, entonces el Máximo Común Divisor entre dos elementos a y b cualesquiera siempre existe, además existen elementos x e y en D tales que

$$a, b = ax + by$$

Prueba: Sea I un ideal de D generado por a y b esto es,

$$I = Da + Db$$

Los elementos de I son de la forma $r_1 a + r_2 b$ con r_1 y r_2 en D. Como D es un Anillo de Ideales Principales, el ideal I es principal y por lo tanto existe un elemento d en D, tal que $I = (d)$.

Por hipótesis se sabe que existe d, el cuál es el máximo Común Divisor entre a y b. En efecto, como $a \in I$ y $b \in I$, se tiene que $d|a$ y $d|b$, por otra parte se sabe qué $d \in I$ y por lo tanto d es de la forma

$$d = ax + by$$

para algunos x e y en D.

Sea c un elemento que está en D, tal que $c|a$ y $c|b$,

entonces

$$a = cr \quad \text{y} \quad b = cs,\ r, s \in D$$

$$\Longrightarrow d = cr\ x + (cs)y$$

$$\Longrightarrow d = c(rx) + c(sy)$$

$$\Longrightarrow d = cx + cy,$$

$$\Longrightarrow d = c(rx + sy)$$

$$\Longrightarrow c/d$$

ANILLOS DE FACTORIZACION UNICA

En esta sección estudiaremos los dominios enteros y del problema de la factorización de los elementos de un dominio entero. En el capítulo anterior se mostró que para un campo F, $F[x]$ también es uno de dichos dominios enteros, con factorización única. Para comprender de una manera más clara la idea de un dominio entero arbitrario, a continuación daremos algunas definiciones las cuales son similares

a otras que se dieron anteriormente, ya que es de suma importancia tener estas definiciones que nos servirán como punto de referencia.

Definición 3.6 Un Dominio de Integridad D se dice que es un Anillo de Factorización Única si todo elemento $a \in D$, el cual es diferente de $cero$ y no es una unidad, puede ser factorizado como un producto finito de elementos irreducibles, esto es

$$a = p_1\, p_2 \ \dots \ p_s$$

donde los p_i son irreducibles.

Además si a tiene otra factorización distinta como producto de irreducibles, digamos

$$a = q_1\, q_2 \dots q_t,$$

donde los q_j son irreducibles, entonces $s = t$ y cada uno de los p_i es asociado de algún q_j.

Más adelante en esta sección se prueba el (**teorema 3.2**) el cual dice que todo Anillo de Ideales Principales, es un Anillo de Factorización Única. Además daremos un lema muy importante el cual establece una condición de cadena en ideales, para cualquier Anillo de Ideales Principales.

Ejemplo 2: Si D es un Anillo de Factorización Única, entonces es posible calcular el Máximo Común Divisor en D. En efecto, tomemos a, b en D. Escribimos las descomposiciones en factores irreducibles de ambos elementos de la forma

$$a = p_1 \dots p_n p_{n+1} \dots p_l$$

$$b = p_1 \dots p_n q_1 \dots q_s$$

Donde ningún q_j es producto de un elemento p_i por un elemento p el cual es invertible (que tiene inverso). Así tenemos que $MCD(a,b) = p_1 \ldots p_n$.

Definición 3.7 familia de ideales de R, I_i , $i \geq 1$, tales que

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ \ldots \subseteq I_i \subseteq I_{i+1} \subseteq \ \ldots$$

Lema 3.1 Toda cadena ascendente de ideales I_i , $i \geq 1$ está acotada superiormente por un ideal J de R. Es decir $I_i \subseteq J, \forall\, i \geq 1$.

Demostración: Tomemos $J = \ _{i>1} I_i$

Es evidente que por la forma en la que se ha definido J, esta contiene a todos los I_i . Afirmamos que J es un ideal de R.

En efecto, sean $a, b \ \in J$ y $r \in R$.

Debemos probar entonces que

1. $a \pm b \ \in J$
2. $ra \in J$.

Si $a, b \ \in J$, entonces existen i_1, i_2 , tales que $a \in I_{i1}$ y $b \in I_{i2}$, sin pérdida de generalidad, podemos suponer que $i_1 > i_2$, de donde se tendrá entonces $a \in I_{i1}$, $b \in I_{i1}$ y como I_{i1} es un ideal se tiene

$$a \pm b \in I_{i1} \subseteq J$$

$$ra \in I_{i1} \subseteq J$$

Luego se cumplen las condiciones 1) y 2) y aquí se finaliza la prueba.

Teorema 3.2 (**parte 1**) Todo Anillo de Ideales Principales es un Anillo de Factorización Única.

Demostración: Sea D un Anillo de Ideales Principales y sea a un elemento en D, el cual no es cero, y tampoco es una unidad.

Si a no es irreducible, entonces no hay nada que probar, ya que a es un producto de elementos irreducibles.

Supóngase que a no es irreducible, entonces existe un par de elementos a_1 y a_2 (no unidades) tales que

$$a = a_1 a_2,$$

si tanto a_1 como a_2 son irreducibles, entonces el teorema es cierto.

Ahora tómese a_1 como un elemento no irreducible y hagamos $a_0 = a$, luego se tiene una cadena de dos ideales de tal manera que

$$(a_0) \subsetneq (a_1),$$

continuando de esta manera para los a_i, se tiene una cadena ascendente de ideales, estrictamente contenidos de la forma

$$(a_0) \subsetneq a_1 \subsetneq a_2 \subsetneq \cdots \subsetneq a_n \subsetneq \cdots$$

Como D es un Anillo de Ideales Principales, existe un k, tal que

$$a_n = a_k, \qquad \forall n \geq k.$$

Entonces el elemento a_k es un irreducible, pues si suponemos que $a_k = b_c$, se tendría $a_{k+1} = b$ y por lo tanto la igualdad

$$b = (a_{k+1}) = (a_k),$$

esto implica que b y a_k son asociados. Luego c es unidad.

Además, a_k es un factor irreducible de a y por lo tanto se tiene que

$$a = a_k e,$$

aplicando el mismo razonamiento al elemento e, se concluye que a es un producto de irreducibles. De donde este proceso se termina después de un número finito de pasos, pues si los elementos irreducibles $p_1, p_2, \ldots, p_n, \ldots$ aparecen en la factorización de a, se tendría una cadena ascendente de ideales

$$a \subseteq p_2 \ldots p_n \ldots \subseteq p_3 \ldots p_n \ldots \subseteq \cdots$$

La cual se detiene en algún momento.

Así pues se ha demostrado la primera parte del teorema de Anillo de Factorización Única.

Para poder probar la segunda parte de este teorema, se necesitan algunos resultados previos sobre divisibilidad, los cuales se dan a continuación.

Proposición 3.2 Si a es un elemento irreducible en un anillo de ideales principales D, entonces el ideal (a) es maximal.

Demostración: Por hipótesis se tiene que a es irreducible, lo que se debe probar es que (a) es maximal.

Sea I un ideal de D y supongamos que $(a) \subseteq I \subseteq D$

El ideal I es principal y por lo tanto existe un elemento x en D, tal que $I = (x)$.

Luego

$$a \in a \subseteq x ,$$

y luego existe un elemento $y \in D$, tal que

$$a = xy$$

como a es irreducible, se tiene que x o y es unidad. Si x es una unidad, entonces

$$x = I = D,$$

por otra parte, si y es una unidad, se debe tener que a y x son asociados, luego

$$x = (a)$$

y por lo tanto

$$I = a .$$

En conclusión se tiene que (a) es un ideal maximal.

Con lo que se completa la prueba.

Definición: (ideal primo) 3.8 se dice que un ideal A de un anillo $(R, +, \cdot, \theta)$ es primo si, y solamente si $xy \in A$, implica $x \in A$ o $y \in A$.

Definición 3.9: Diremos que un ideal $I \subset A$ de A es un ideal primo si $I \neq A$ y se verifica la siguiente condición:

El producto de dos elementos del anillo pertenece al ideal si y solo si alguno de los elementos pertenece al ideal, es decir, si

$x, y \in A, xy \in I$ o $y \in I$.

Proposición 3.3 Sea D un Anillo de Ideales Principales y a un elemento en D, tal que $a|bc$, entonces si a es irreducible se tiene que $a|b$ o $a|c$.

Demostración: De acuerdo a la proposición anterior se tiene que el ideal (a) es maximal y por tanto es primo. Luego si $a|bc$, esto implica que $bc \in (a)$, de aquí se tiene que

$$b \in (a) \text{ o } c \in (a),$$

esto es

$$a|b \text{ o } a|c$$

Proposición 3.4 (**Segunda parte del Teorema 3.2**): Sea D un Anillo de Ideales Principales y a un elemento que pertenece a D el cual se factoriza de dos maneras como productos irreducibles

$$a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t, \qquad (1)$$

entonces $s = t$ y cada p_i es un asociado a algún q_j.

Demostración: Comencemos por considerar el elemento p_1 en el lado izquierdo de la ecuación (1) el cual es irreducible y divide al producto $q_1 q_2 \dots q_t$.

Por la proposición anterior se deduce que p_1 divide a alguno de los q_i, digamos $p_1|q_j$, para algún $1 \leq j \leq t$. Luego de acuerdo al ejercicio 6 que dice (si a y b son dos elementos irreducibles, tales que a divide a b, entonces a y b son asociados), se debe tener que p_1 y q_j son asociados, esto es, existe una unidad u_1 tal que

$$p_1 = u_1 q_j,$$

podemos entonces cancelar este elemento en (1) para tener una expresión

$$p_2 p_3 \ldots p_s = u_1 q_1 \ldots q_{i-1} q_{i+1} \ldots q_t \qquad (2)$$

Ahora p_2 divide al producto $u_1 q_1 \ldots q_{i-1} q_{i+1} \ldots q_t$, entonces se debe tener que $p_2|q_h$ con $1 \leq h \leq t$ y $h \neq i$, esto es, dado que p_2 y q_h son asociados, debe existir una unidad u_2, tal que

$$p_2 = u_2 q_h$$

y por lo tanto podemos cancelar p_2 y nos queda

$$p_3 p_4 \ldots p_s = u_1 u_2 q_1 \ldots q_{i-1} q_{i+1} \ldots q_t$$

Continuando de esta manera, podemos cancelar todos los p_i en el lado derecho de (2), después de un numero finito de pasos, hasta obtener una expresión de la forma

$$1 = u q_{i1} \ldots q_{ik} \qquad (3)$$

Con $k = t - s$ y u una unidad.

Como los q_j son irreducibles, no son unidades y por lo tanto en la ecuación (3) se debe tener $k = 0$ o sea $t = s$

ANILLOS EUCLIDIANOS

Hemos señalado varias veces en este trabajo la importancia del algoritmo de la división. Nuestro primer contacto con ellos fue en el algoritmo de división para $\mathbb{Z}$. Este algoritmo se usó de inmediato para probar el importante teorema de que un subgrupo de un grupo cíclico es cíclico, esto es, que tiene un solo generador. El algoritmo de la división para $F[x]$ apareció en el teorema 2.2 y se usó de manera análoga para demostrar que $F[x]$ es un anillos de ideales principales, esto es, que todo ideal en $F[x]$ tiene un solo generador. Ahora bien, una técnica moderna en matemática es tomar varias situaciones claramente relacionadas y tratar de reunirlas extrayendo las ideas importantes que tienen en común. Nos daremos cuenta como la siguiente definición ilustra esta técnica. Comenzando con la existencia del algoritmo veamos que podemos desarrollar, de manera más general en un dominio entero.

Definición 3.10 Una evaluación euclidiana en un dominio entero D es una función v que transforma a los elementos distintos de cero de D en los enteros no negativos tal que se satisfacen las condiciones siguientes:

1) Para todos los $a, b \in D$ con $b \neq 0$ existen q y r en D tales que $a = bq + r$, donde $r = 0$ o $v(r) < v(b)$.
2) Para todos los $a, b \in D$, donde ni a ni b son el elemento nulo (0), $v(a) \leq v(ab)$.

Definición 3.11 Un dominio entero D es un Anillo Euclidiano si existe una evaluación euclidiana en D.

Definición 3.12 Se llama Anillo Euclidiano a cualquier anillo conmutativo R que cumple la propiedad de que a cada $x \in R$ se le puede asignar un entero no negativo $\phi(x)$ tal que:

(i) $\phi\ x\ = 0\ si\ y\ solo\ si, x = 0, el\ elemento\ cero\ de\ R.$

(ii) $\phi(x.y) \geq \phi(z)$ si $x.y \neq 0.$

(iii) $para\ todo\ x, y\ \in R;\ y \neq 0\ \ elemento\ neutro$, existen q, r $\in R,$ tal que

$x = yq + r,\ con\ 0 < \phi\ r\ < \phi\ y$.

Ejemplo 3 Probar que el anillo de los enteros Z con la función $d(x) = x$ es un Anillo Euclidiano. La propiedad 1) de la definición **(3.6)** es consecuencia inmediata de la definición de valor absoluto para números enteros, y la propiedad dos es precisamente el algoritmo de la división para enteros.

Prueba: para probar la propiedad 1), se prueba primero la existencia de $q\ r$ tenemos como un numero entero tal que bq sea mayor de los múltiplos de b menor o igual que a, de tal manera que bq menor o igual que a.

Una vez que se ha obtenido el cociente q, podemos calcular el resto r el cual queda de la siguiente manera

$$r = a - bq$$

Por otra parte si $bq \leq a$, entonces el siguiente múltiplo de q, $b(q+1)$ será estrictamente mayor que a es decir $bq \leq a < b(q+1)$.

Entonces $bq \leq a < b(q+1)$

$$\Longrightarrow bq - bq \leq a - bq < b\ q+1\ - bq$$

$$\Longrightarrow bq - bq \leq a - bq < bq + b - bq$$

$$\Longrightarrow 0 \leq a - bq < b + 0$$

$$\Longrightarrow\ 0 \leq a - bq < b$$

$$\Longrightarrow 0 \leq\ a - bq < b, \text{ como } r = a - bq$$

$$\Longrightarrow 0 \leq r < b$$

Así pues de esta forma se ve que existen enteros q y r tales que $a = bq + r$ con

$$0 < r < b$$

Para la parte 2), Sea Z un anillo euclidiano y $a, b \in Z$. Si b no es unidad en Z entonces

$$v\ a\ < v\ ab\ .$$

Consideremos el ideal $A = \ a \ = \{xa | x \in Z\}$ de Z. Por la condición 1) para anillos euclidianos, $v\ xa\ \leq v\ xab$ para $x \neq 0$ en Z.

Luego el valor $v(a)$ es el mínimo de los valores de v.

Ahora, como el valor de $v(\ ab)$ es máximo en A, todo elemento de A es un múltiplo de ab. En particular, como $a \in A$, a debe ser múltiplo de ab; de donde $a = abx$ para algún $x \in Z$. Como todo esto está teniendo lugar en un dominio entero, de ello se deduce que

$$bx = 1.$$

Luego b es una unidad en Z, en contradicción al hecho de que no es una unidad. El resultado neto de todo es que $v\ a\ < v\ ab\ .$

Teorema 3.3 Todo Anillo Euclidiano R es un Anillo de Ideales Principales**.**

Demostración: Como hipótesis consideremos un ideal I que está en R, $I \neq 0$, lo que se debe probar es que I es un ideal principal.

Para ello consideremos el conjunto $v\ I\ = \ v\ x\ : x \in I - \ 0\ \subset \ 0, 1, 2, 4, \ldots$

Sea $a \in I$ tal que $v\ a\ = Minimo\ v\ I\ $, el cual existe, ya que al ser $0, 1, 2, 4, \ldots$ discreto y bien ordenado. Podemos considerar el Ideal Principal generado por a, es decir (a), el cual está contenido en I. Supongamos que podemos escoger

$$x \in I - (a).$$

Sabemos que existen valores $r, t \in D$ tales que $x = ta + r$, donde $r = 0$ o

$$v(r) < v(a).$$

Pero como x esta en la diferencia de $x \in I - (a)$, lo que significa que $x \in I$ y $x \notin a$, $r \neq 0$. Así pues, se tiene que $r \in D - 0$ es tal que $v(r) < v(a)$, pero

$$r = x - ta \in I,$$

lo cual contradice la minimalidad de $v(a)$.

Luego $I = (a)$.

NOTA 1 Para abreviar se suele hablar de Anillo de Ideales Principales para indicar un Dominio de Integridad con todos sus ideales principales.

Ejemplo 4: Demostrar que el anillo $G = a + bi : a, b \in Z$ es Euclidiano.

Demostración: En primer lugar se debe probar la condición i) del Anillo Euclidiano, la cual establece que:

$$\phi\ x\ = \phi\ a + bi\ = a^2 + b^2$$

$$\phi\ x\ = 0.$$

i) $\phi\ x\ = 0 \Leftrightarrow x = z$; z el elemento identidad de R

" $\Longrightarrow$ "

Sea $x = a + bi$, tal que $\phi\ x\ = 0$

$$\phi\ x\ = 0 \Longrightarrow \phi\ a + bi\ = a^2 + b^2 = 0$$

$$\Longrightarrow a^2 + b^2 = 0$$

$$\Longrightarrow a = 0 \wedge b = 0$$

$$\Longrightarrow x = 0 + 0i = 0$$

" $\Longleftarrow$ " Sea $x = 0$,

$$x = 0 \ \Longrightarrow \phi\ x\ = \phi\ 0$$

$$= \phi\ 0 + 0i$$

$$= 0^2 + 0^2 = 0$$

$\therefore\ \phi\ x\ = 0 \Leftrightarrow x = z = 0$

ii) $\phi\ x.y\ \geq \phi\ x\ \Leftrightarrow xy \neq 0$

" $\Longrightarrow$ "

Esta prueba se lleva a cabo por el método de contradicción, para ello supóngase que $\phi\ x.y\ \geq \phi\ x$ y $xy = 0$.

Sea $x = a + bi$ y $y = c + di$

$$\Longrightarrow xy = (a + bi)(c + di)$$

$$= ac + adi + bci + bdi^2$$

$$= ac + adi + bci + bd(-1)$$

$$= ac + adi + bci - bd$$

$$= \ ac - bd \ + (adi + bci)$$

$$= \ ac - bd \ + (ad + bc)i$$

$$\phi \ xy \ = \ ac - bd \ ^2 + (ad + bc)^2 \geq \ \phi \ x \ = a^2 + b^2$$

$$= (a^2 + b^2)(c^2 + d^2) \geq a^2 + b^2$$

$$= (c^2 + d^2) \geq \frac{(a^2+b^2)}{(a^2+b^2)}$$

$$= c^2 + d^2 \geq 1$$

Por hipótesis se tiene que $xy = 0$,

$xy = 0 \Longrightarrow \ ac - bd \ + \ ad + bc \ i = 0$

$\Longrightarrow ac - bd = 0 \ \wedge \ ad + bc = 0$

$\Longrightarrow ac = bd \wedge \ ad = -bc$ (multiplicando lado izquierdo por d)

$\Longrightarrow adc = bd^2 \wedge \ ad = -bc$ sustituyendo ad el lado izquierdo se tiene

$\Longrightarrow \ -bc \ \ c \ = bd^2$

$\Longrightarrow -bc^2 = bd^2$ por la ley cancelativa en b

$$\Longrightarrow -c^2 = d^2$$

$$\Longrightarrow c^2 + b^2 = 0,$$

Pero esto es una contradicción ya que

$$c^2 + b^2 \neq 0$$

$$\therefore xy \neq 0$$

" $\Longleftarrow$ " Por hipótesis se tiene que $xy \neq 0$

$$xy \neq 0 \Longrightarrow \ ac - bd \ + \ ad + bc \ i \neq 0$$

$$\Longrightarrow ac - bd \neq 0 \ \vee \ ad + bc \neq 0 \qquad (1)$$

Ahora bien, tenemos que

$$\phi \ xy \ = \ ac - bd \ ^2 + (ad + bc)^2 \neq 0 \quad \text{Por (1)}$$

$$= (a^2 + b^2)(c^2 + d^2) \neq 0 \quad \text{Resolviendo se tiene}$$

$$= a^2c^2 + a^2d^2 + b^2c^2 + \ b^2d^2 \neq 0$$

$$= \phi(x)\phi(y) \neq 0$$

$\Longrightarrow \phi(x.y) \geq \phi(x)$; pues $\phi(y) \ \geq 1$ y no puede ser **0.**

$\therefore \phi(x.y) \geq \phi(x) \Leftrightarrow \ xy \neq 0.$

iii) Ahora para probar la existencia del algoritmo Euclidiano, sean dos elementos cualesquiera, tal que

Para todo $\alpha, \beta \in G$ con $\beta \neq 0$, $\exists\ \rho,\ \sigma \in G$ tal que

$$\alpha = \beta\rho + \sigma,$$

Donde $\sigma \neq 0$ o $\phi(\sigma) < \phi(\beta)$,

primeramente probaremos que para $x.y \in \mathbb{C}$, se tiene que $\phi\ xy\ = \phi(x)\phi(y)$.

Sean $x = a + bi$, $y = c + di$

$$\phi\ xy\ = \phi\ \ a + bi\ \ c + di\ \ = \phi\ \ ac - bd\ + \ ad + bc\ i$$

$$= \ ac - bd\ ^2 + \ ad + bc\ ^2$$

$$= \ ac\ ^2 - 2abcd + \ bd\ ^2 + \ ad\ ^2 + 2abcd + \ bc\ ^2$$

$$= \ ac\ ^2 + \ bc\ ^2 + \ bd\ ^2 + \ ad\ ^2$$

$$= \ a + b\ ^2c^2 + \ a + b\ ^2d^2$$

$$= \ a^2 + b^2\ \ c^2 + d^2$$

$$= \phi(x)\phi(y)$$

Ahora sean $\alpha, \beta \in G$ con $\alpha = a_1 + a_2 i,\ \ \beta = b_1 + b_2 i, \beta \neq 0$

$$\frac{\alpha}{\beta} = \frac{(a_1 + a_2 i)}{(b_1 + b_2 i)} = \frac{(a_1 + a_2 i)}{(b_1 + b_2 i)} \cdot \frac{(b_1 - b_2 i)}{(b_1 - b_2 i)}$$

$$= \frac{a_1 b_1 - a_1 b_2 i + a_2 b_1 i + a_2 b_2}{{b_1}^2 + {b_2}^2}$$

$$= \frac{(a_1 b_1 + a_2 b_2)}{{b_1}^2 + {b_2}^2} + \frac{(-a_1 b_2 + a_2 b_1)}{{b_1}^2 + {b_2}^2} i$$

Ahora hagamos

$$r = \frac{a_1 b_1 + a_2 b_2}{{b_1}^2 + {b_2}^2}$$

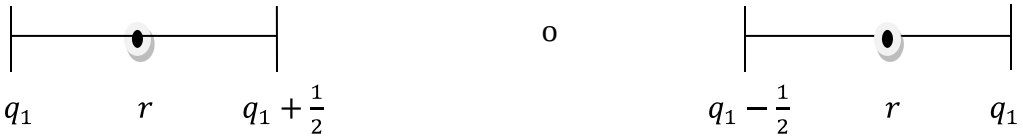
y

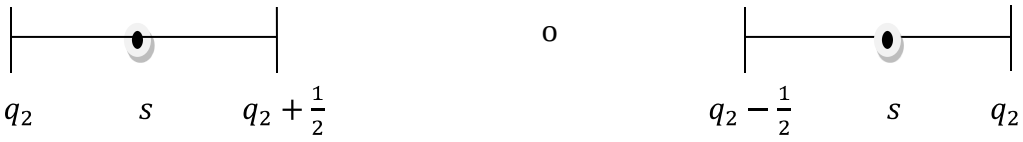
$$s = \frac{-a_1 b_2 + a_2 b_1}{{b_1}^2 + {b_2}^2}$$

y observemos que como $a_1,\ a_2,\ b_1,\ b_2 \in \mathbb{Z}(numeros\ enteros)$, entonces

$r, s \in \mathbb{Q}(numeros\ racionales)$,

De tal manera que para r y s existen $q_1,\ q_2 \in \mathbb{Z}$, tal que:





y definamos $\sigma = q_1 + q_2 i$, además tomemos a $\rho = \alpha - \beta\sigma$ observemos que $\sigma \in G$ y también $\rho \in G$ pues $\alpha, \beta, \sigma \in G$.

Si $\rho = 0$ no habría nada que probar, así que por ello,

Supongamos que $\rho \neq 0$ y probemos que $\phi(\rho) < \phi(\beta)$.

Se tiene por construcción que

$$r - q_1 \leq \frac{1}{2} \text{ y } s - q_2 \leq \frac{1}{2},$$

por lo tanto,

$$\phi\left(\frac{\alpha}{\beta} - \sigma\right) = \phi\left(r + si - q_1 + q_2 i\right)$$

$$= \phi\left(r - q_1 + s - q_2\, i\right)$$

$$= r - q_1^{\,2} + s - q_2^{\,2}$$

$$\leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2$$

$$\leq \frac{1}{4} + \frac{1}{4}$$

$$= \frac{1}{2}$$

Por tanto,

$\phi(\rho) = \phi(\alpha - \beta\sigma) = \phi(\beta)\left(\frac{\alpha}{\beta} - \sigma\right)$, por la primera parte

$$\leq \phi\ \beta\quad \frac{1}{2}$$

$$\phi\ \rho\ \leq \phi\ \beta\quad \tfrac{1}{2}$$

$$\Rightarrow \phi\ \rho\ < \phi\ \beta\ .$$

$$\therefore \forall \alpha, \beta \in G, \exists \sigma, \rho \in G$$

tal que $\alpha = \beta\sigma + \rho, p = 0$ o $\phi(\rho) < \phi(\beta)$

De esta manera se han verificados las propiedades (i), (ii) y (iii) del anillo Euclidiano y por lo tanto se cumplen aquí en este ejemplo.

Así pues, se cumple (iii) y por lo tanto G es un Anillo Euclidiano.

ANEXOS

Después de haber documentado un poco lo que es la teoría de Anillos Euclidianos y sus teoremas fundamentales, se dan a conocer algunas de las aplicaciones en las que es necesario e importante el uso de estos.

1) El método de encontrar el Máximo Común Divisor (MCD) de dos o más elementos en un anillo arbitrario de números enteros, para ello es necesario comprender el concepto de anillos y dominio de ideales principales los cuales se mencionaron anteriormente.

2) Probar que los polinomios son irreducibles.

3) Verificar que tienen una factorización única.

Estos procedimientos que se llevan a cabo a través del método conocido como Algoritmo de Euclides.

El algoritmo de Euclides se describe de la forma siguiente:

Dados los elementos a y b cuyo máximo común divisor se desea encontrar, asumiendo que $a, b > 0$ (el método funciona también si a y b son negativos). Basta trabajar con los valores absolutos de estos números, debido a que

$$MCD\ \ a\ ,\ b\ \ = M.C.D(a, b).$$

Para ello se siguen los siguientes pasos:

a) Se usa el algoritmo de Euclides para obtener $a = q_1 b + r_2$ con $0 < r_1 < b$. Si $r_1 = 0$ entonces $b|a$ y el $M.C.D\ a, b = b$.

b) Si $r_1 \neq 0$, se divide b por r_1 y se produce enteros q_2 y r_2 que satisfacen $b = q_2 + r_2$ con $0 < r_2 < r_1$. si $r_2 = 0$ el proceso termina y

$$M.C.D\ a, b = r_1 .$$

c) Si $r_2 \neq 0$ se procede a dividir r_2 por r_1, obteniendo $r_1 = q_3 r_2 + r_3$ con

$$0 < r_3 < r_2.$$

d) Este proceso continua hasta que algún residuo cero aparece. esto ocurre porque en la frecuencia $b > r_1 > r_2 > \cdots \geq 0$ no pueden haber más de b enteros. Es decir el proceso es finito.

e) En estas circunstancias, el máximo común divisor de a y b no es más que el último residuo diferente de cero obtenido en el proceso anterior.

EJERCICIOS SELECCIONADOS SOBRE ANILLOS DE POLINOMIOS

Algoritmo de Euclides

1) Sean $f\ x = 6x^3 + 3x^2 - 2$ y $h(x) = 2x^2 - 6$ dos polinomios en $Z\ x$.

   Encontrar:

   a) $f\ x + h(x)$

   b) $f\ x\ h\ x$

Solución (a): Sabemos que la suma de polinomios se lleva acabo sumando término a término los coeficientes de las variables que tienen igual exponente, para ello es necesario completar con ceros las partes de donde hace falta alguna variable con el exponente indicado.

$$f\ x\ + h\ x\ =\ 6x^3 + 3x^2 + 0x - 2\ + (0x^3 + 2x^2 + 0x - 6),$$

agregamos las variables faltantes para poder sumarlos y luego lo reescribimos de la forma más usual.

$$6x^3 + 3x^2 + 0x - 2$$

$$\underline{\ 0x^3 + 2x^2 + 0x - 6}$$

$$6x^3 + 5x^2 - 8$$

Por lo tanto $f\ x\ + h\ x\ = 6x^3 + 5x^2 - 8$

Solución (b): Sabemos que la multiplicación de polinomios se lleva acabo multiplicando cada término de un primer polinomio por cada uno de los términos de un segundo polinomio, después de esto se deben asociar los términos que contengan la variable con la misma potencia, para poder efectuar las operaciones de reducción o cancelación de términos semejantes.

$$\begin{aligned} f\ x\ h\ x\ &=\ 6x^3 + 3x^2 - 2\ \ 2x^2 - 6 \\ &= 6x^3\ \ 2x^2 - 6\ + 3x^2\ \ 2x^2 - 6\ - 2\ \ 2x^2 - 6 \\ &= 12x^{3+2} - 36x^3 + 6x^{2+2} - 18x^2 - 4x^2 + 12 \\ &= 12x^5 - 36x^3 + 6x^4 - 18x^2 - 4x^2 + 12 \end{aligned}$$

$$= 12x^5 + 6x^4 - 36x^3 - 22x^2 + 12,$$

Por lo tanto $f\ x\ h\ x\ = 12x^5 + 6x^4 - 36x^3 - 22x^2 + 12$

2) Encontrar el cociente y el resto de la división de los siguientes polinomios en $Q\ x$

a) $f\ x\ = 10x^8 - 2x^2 + 6,\ h\ x\ = x^2 + 2$

$10x^8 + 0x^7 + 0x^6 + 0x^5 + 0x^4 + 0x^3 - 2x^2 + 0 + 6$ | $x^2 + 0x + 2$

$-10x^8 + 0x^7 - 20x^6$ → $10x^6 - 20x^4 + 40x^2$

$-20x^6 + 0x^5 + 0x^4$

$-20x^6 - 0x^5 + 40x^4$

$40x^4 + 0x^3 - 2x^2$

$-40x^4 - 0x^3 - 80x^2$

$-82x^2$

Por lo cual se tiene que el cociente es $q\ x\ = 10x^6 - 20x^4 + 40x^2$ y el resto es

$$r\ x\ = -82x^2$$

b) $4x^5 + 2x^4 - 24x^3 + 18x^2$ | $x^2 + 3x$

$-4x^5 - 12x^4$ → $4x^3 - 10x^2 + 6x$

$-10x^4 - 24x^3$

$10x^4 + 30x^3$

$6x^3 + 18x^2$

$-6x^3 - 18x^2$

0

Por lo cual se tiene que el cociente es $q\ x\ = 4x^5 + 2x^4 - 24x^3 + 18x^2$ y el resto es

$$r\ x\ = 0$$

Ejemplo: Utilizar el algoritmo de Euclides para encontrar el máximo común Divisor de los números 12378 y 3054.

Solución:

Sea $a = 12378\ y\ b = 3054$, entonces aplicando el algoritmo euclidiano tenemos que

$$12378 = 3054(4) + 162$$

$$3054 = 162(18) + 138$$

$$162 = 138(1) + 24$$

$$138 = 24(5) + 18$$

$$24 = 18(1) + 6$$

$$18 = 6(3) + 0,$$

Por lo tanto el $MCD(12378, 3054) = 6$

Ejemplo: Sean los polinomios $a\ x\ = x^5 + 1$ y $b\ x\ = x^3 + 1$, encontrar el máximo común divisor.

Solución:

$$x^5 - 32 = (x^3 - 8)(x^2) + (8x^2 - 32)$$

$$x^3 - 8 = \ 8x^2 - 32 \quad 1/8x \ + \ 4x - 8$$

$$x^3 - 8 = \ x^2 - 4 \quad x \ + \ 4x - 8$$

$$x^2 - 4 = \ 4x - 8 \ (1/4x) + (2x - 4)$$

$$4x - 8 = (2x - 4)(2) \ + \ 0$$

De esto se concluye que el máximo común divisor de los polinomios

$$a \ x \ = x^5 - 32$$

y

$$b \ x \ = x^3 - 8$$

es $2x - 4$.

Antes de dar algunos ejemplos de Anillos Euclidianos, probaremos primero que un Anillo Euclidiano tiene elemento unitario. Esto será un corolario del teorema siguiente el cual es muy importante.

Teorema: en un Dominio Euclidiano *A*, todos sus ideales *I* incluidos en *A* son de la forma $I = Ax$, con $x \in A$.

Demostración: Sea $I \subseteq A$ un ideal cualquiera. Si $I = 0$, ciertamente $I = A \cdot 0$.

Supóngase ahora que $I \neq 0$, y considérese el conjunto

$$v\ a\ : a \in I, a \neq 0\ \subseteq \mathbb{N} \cup \{0\}\ .$$

Como este es un conjunto no vacío de enteros no negativos, por el principio del buen orden Existe un elemento $a \in I, a \neq 0$ tal que $v(a) \leq v(x)$ para toda $x \in I, x \neq 0$.

Ahora bien, para cualquier $b \in I$, por el algoritmo de la división, existen $q, r \in A$ tales que

$b = aq + r$, con $r = 0$ o $v\ r\ < v(a)$,

y observe que la posibilidad $v\ r\ < v(a)$ no se puede dar, ya que como $b \in I$ y $a \in I$, entonces $r = b - aq \in I$ y asi $v(r) \geq v(a)$ por la elección de $a \in I$. Se sigue entonces que $b = aq$ y por lo tanto $I = Aa$ y se ha demostrado que en un dominio Euclidiano todos sus ideales son de la forma $I = Ax$.

Corolario: Todo anillo Euclidiano posee elemento unitario.

Demostración: Si A es Euclidiano, para el ideal $A \supseteq A$, por el teorema anterior, $A = Au$ para algún $u \in A$, es decir todo elemento de A es múltiplo de u.

En particular $u = ue$ para algún $e \in A$.

Ahora para todo $x \in A$, $x = uc$ para algún $c \in A$, y a si

$xe = \ uc \ e = \ ue \ c = uc = x,$

De donde $e = 1 \in A$, por lo tanto todo anillo Euclidiano tiene elemento unitario.

Ejemplo: Sea $i \in \mathbb{C}$ el complejo tal que $i^2 = -1$ y sea

$$Z\ i\ = \{a + bi : a, b \in Z \supseteq \mathbb{C}\}$$

El conjunto $Z\ i\ $ es un anillo con las operaciones de $\mathbb{C}$, ya que si $a + bi,\ c + di \in Z\ i\ ,$ entonces:

$$a + bi\ \ +\ \ c + di\ \ =\ \ a + c\ \ + (b + d)i \in Z\ i$$

y

$$a + bi\ \ \ c + di\ \ =\ \ ac - bd\ \ +\ \ ad + bc\ \ i \in Z\ i$$

El $0 \in i$ es $0 = 0 + 0i$ y el $1 \in Z\ i\ \ $ es $1 + 0i$.

Como las operaciones de $Z\ i\ \ $ son las de $\mathbb{C}$ y como $\mathbb{C}$ es dominio es entero, entonces $Z\ i\ \ $ también lo es.

Para ver que $Z\ i\ \ $ es euclidiano, definimos la norma

$$N : Z\ i\ \ \rightarrow \mathbb{N}$$

Como el modulo del complejo al cuadrado, es decir,

$$N\ \ a + bi\ \ =\ \ a + bi\ ^2 =\ \ a + bi\ \ \ a - bi$$

$$= (a + bi)(a - bi)$$

$$= (a\ a\ - a(bi) + a\ bi\ -\ bi\ ^2)$$

$$= (a^2 - abi + abi - (bi)^2)$$

$$= \ a^2 - abi\ +\ abi - b^2\ -1 \qquad \text{por ser } i^2 = -1$$

$$= \ a^2 - abi\ +\ abi + b^2$$

$$= (a^2 + b^2) +\ -abi + abi$$

$$= a^2 + b^2$$

Claramente,

1) Para cuales quiera u $\in Z\ i\ -\ 0$, se tiene que $N\ u\ \leq N\ uv$.
2) Para probar el algoritmo de la división, sean $u, v \in Z\ i$, $u = a + bi$,

   $v = c + di\ \neq 0$.

Como $v \neq 0$ podemos dividir u entre v en $\mathbb{C}$. Explícitamente,

$$\frac{u}{v} = \frac{uv'}{vv'} = \frac{a + bi\quad c - di}{c + di\quad c + di}$$

$$= \frac{ac + bd}{c^2 + d^2} + \frac{bd - ad}{c^2 + d^2}\,i$$

$$= \alpha + \beta i$$

Donde

$$\alpha = \frac{ac + bd}{(c^2 + d^2)} \in \mathbb{Q}$$

y

$$\beta = \frac{(bd - ad)}{(c^2 + d^2)} \in \mathbb{Q}$$

nótese que $v^{\,2} = c^2 + d^2 \neq 0$ ya que $v \neq 0$.

Ahora, para $\frac{u}{v} = \alpha + \beta i$, con $\alpha, \beta \in \mathbb{Q}$, escójanse $m, n \in Z$ tales que

$$\alpha - m \leq \frac{1}{2} \text{ y } \beta - m \leq \frac{1}{2},$$

de esto se sigue que

$$\begin{aligned} \frac{u}{v} - m + ni &= \alpha + \beta i - m - ni \\ &= \alpha - m + (\beta - n)i \\ &= \alpha - m^{\,2} - \beta - m^{\,2})^{\frac{1}{2}} \\ &\leq \frac{1}{4} + \frac{1}{4}^{\frac{1}{2}} \\ &= \frac{2}{4}^{\frac{1}{2}} = \frac{1}{2}^{\frac{1}{2}} = 1/\sqrt{2}. \end{aligned}$$

Entonces, poniendo $q = m + ni \in Z\,i$, como queremos que $u = vq + r$ en $Z\,i$, necesariamente,

$$r = u - vqZ\ i\ ,$$

y observamos que

$$r\ =\ u - vq\ =\ (v)(\frac{u}{v} - q)\ =\ v\ \ \frac{u}{v} - (m + ni)\ \leq\ v\ \cdot \frac{1}{2}$$

Es decir, $N\ r\ =\ r\ ^2 \leq\ v\ ^2 \cdot \frac{1}{2}$ Y a si $N\ r\ < N(v)$

Como se quería probar.

BIBLIOGRAFIA

- Anillos y sus categorías de representaciones

  M.A. Farinati A.L. Solotar

- ESTRUCTURAS ALGEBRAICAS GRUPOS Y ANILLOS

  PRIMERA EDICIÓN 2009

  Rubén A. Hidalgo

  Departamento de Matemática, Universidad Técnica Federico Santa María,

  Valparaíso,

  Chile.

  E-mail : ruben.hidalgo@usm.cl

  Url : http://docencia.mat.utfsm.cl/~rhidalgo

- Anillos Oswaldo Lezama

  Departamento de Matemáticas

  Facultad de Ciencias

  Universidad Nacional de Colombia

  Sede de Bogotá

  Mayo 30 de 2012

- Una Introducción a las Estructuras Algebraicas Básicas

  Notas para la asignatura ´ Algebra 3

  Profesora Olga Porras

  Departamento de Matemáticas

Facultad de Ciencias

Universidad de los Andes

2 de julio de 2010

- Anillos y Cuerpos

  Luis Arenas

  November 13, 2008

- MODERN ALGEBRA WITH APPLICATIONS

  Second Edition

  WILLIAM J. GILBERT

  University of Waterloo

  Department of Pure Mathematics

  Waterloo, Ontario, Canada

  W. KEITH NICHOLSON

  University of Calgary

  Department of Mathematics and Statistics

  Calgary, Alberta, Canada

- ALGEBRA MODERNA

  FRANK AYRES, JR., Ph. D.

  Formely Professor and head,

  Department of Mathematics

  Dickinson College

- ALGEBRA MODERNA

  I.N Herstein

- ALGEBRA ABSTRACTA

  Primer curso

  Jhn B. Fraleigh

  Departmen of Mathematics

  University if Rhode Island