UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

INTRODUCCIÓN A LAS ESTRUCTURAS ALGEBRAICAS

MATERIAL DE APOYO A LA DOCENCIA

QUE PARA OBTENER EL TÍTULO DE:

A C T U A R I O

PRESENTA:

FERNANDO DANIEL CAÑADA BAPTISTA

ASESOR: ACT. HARVEY SPENCER SÁNCHEZ RESTREPO

Octubre de 2007

Contenido

Prólogo

En el año 2005 entro en vigor el nuevo plan de estudios de la licenciatura en Actuaría que se imparte en la Facultad de Estudios Superiores Acatlán de la UNAM. Esta actualización se da, principalmente, con la intensión de renovar el proceso enseñanza-aprendizaje y en respuesta a la creciente demanda en los niveles de educación superior.

En apoyo a esta transformación, este material ha sido desarrollado con el objetivo de introducir al alumno de primeros semestres al estudio de las estructuras algebraicas y teoría de ecuaciones. Se presenta en él todos los temas que forman parte del programa de Álgebra Superior II. Con base en la experiencia al impartir las asignaturas de Algebra Superior I y Álgebra Superior II, he encontrado que a pesar de la gran cantidad de bibliografías referentes a la materia, el estudiante no emprende una labor autodidacta para el aprendizaje de los temas, sino que, en general, necesita de un guía para la interpretación de los textos. Debo aclarar que no tengo como objetivo el sustituir con estos apuntes a ningún otro material relacionado al tema. La finalidad es tratar de enunciar de una manera menos estéril proposiciones y resultados de gran profundidad, así como abordar los conceptos de una manera más intuitiva sin perder la esencia de éstos.

El material ha sido escrito en un orden sistemático, de manera que se sugiere la lectura de los capítulos en el orden en el que se presentan.

En el Capítulo 1, de carácter introductorio, se explican las propiedades de las estructuras algebraicas partiendo de las más simples, desde el punto de vista didáctico, como lo son los anillos y los dominios enteros, hasta llegar a la estructura más general que es la de campo. Se incluye también una reseña histórica del *método axiomático* y de las técnicas de demostración mas usadas en el material.

En el Capítulo 2, se tratará el conjunto de los números enteros y se hablará sus principales propiedades y operaciones. La exposición de este capítulo permite que se comprenda el resultado más relevante de la teoría de los números: El Teorema Fundamental de la Aritmética.

En el Capítulo 3, se expone el conjunto de los números complejos. En esta sección se hace una breve reseña de la motivación que permite construir este sistema y en la misma se tratará de desprender a los números complejos de su adjetivo de “imaginarios”. Se hablará también de las principales propiedades y operaciones que se cumplen y de las diversas formas que hay de escribir un número complejo.

En el Capítulo 4, se tratarán los temas relacionados con la teoría de ecuaciones y polinomios. Se define el concepto de polinomio y las operaciones que se pueden hacer con éstos. Se establece, a manera de analogía con el conjunto de los números enteros, el concepto de divisibilidad de polinomios y el cálculo del polinomio máximo común divisor. Se expone también el concepto de raíces de un polinomio y algunas de las técnicas que permiten encontrarlas.

A lo largo del material, se trata de exponer el origen de los conceptos y la motivación de estos. Asimismo, con el objetivo de que el alumno evalúe su aprendizaje, al final de

cada capítulo se incluye una lista de ejercicios los cuales son presentados en orden aleatorio, todo esto con el fin exhibir a las matemáticas como un conocimiento integrado y no como un conjunto de recetas ordenadas.

Se espera que el material sirva tanto a estudiantes universitarios de la licenciatura en Actuaría, como a personas ajenos a ella. Por este motivo, también es posible encontrar los apuntes en el sitio de Internet de educación en línea: http://www.academianet.com.
Agradezco profundamente a María del Carmen González Videgaray por el espacio y apoyo ofrecido.

Agradezco también a mi asesor Harvey Spencer Sánchez Restrepo por sus comentarios, sugerencias y por guiarme en momentos difíciles. Gracias también a todos los profesores que me dedicaron parte de su vida en mi formación como profesionista y que son un ejemplo a seguir.

Gracias a Mahil Herrera Maldonado, Jorge Luis Suárez Madariaga, Pablo Pérez Akaki, Victor Ulloa Arellano por su enseñanza y dedicación a la FES Acatlán y ayudarme en mi formación como docente.

1. Conceptos preliminares

El título de este capítulo expresa, en pocas palabras, los conceptos matemáticos necesarios para la lectura de este material. La primera parte del mismo está encaminada a presentar al estudiante el propósito del método axiomático mientras que la segunda tiene como fin exponer la naturaleza del álgebra moderna. Estos conceptos básicos se ejemplificarán con mayor precisión a lo largo texto.

1.1 Orígenes del método axiomático.

Aproximadamente durante tres mil años hasta comienzos del siglo XIX, la palabra "álgebra" significaba la resolución de ecuaciones polinomiales, generalmente de cuarto o menor grado. A esta parte del álgebra se le conoce como *álgebra clásica*. En las primeras décadas del siglo XX el álgebra se centralizó en el estudio sistemas abstractos y axiomáticos tales como los grupos, anillos y campos, a esto se le conoció como *álgebra moderna* (*o abstracta*)[1].

El término "álgebra moderna" se utiliza en distintos sentidos, sin embargo, probablemente el más común, es denominar con estas palabras (o "matemática moderna") al periodo de la historia de las matemáticas que se extiende desde una fecha que varía bastante según los distintos autores –pero que en cualquier caso no suele ser anterior a Abel, Galois y Cauchy- hasta nuestros días.

Estas "Matemáticas modernas" se identifican esencialmente por las tres "ramas" principales de la axiomática, que son: 1) la extensión de la noción de número y la aparición del "álgebra abstracta"; 2) el nacimiento de las geometrías no Euclideanas de Gauss, Lobatchevski y Bolyai seguido más tarde por las axiomatizaciones de la geometría de Euclides realizadas por Pasch, Peano y sobretodo por Hilbert; 3) el desarrollo de la lógica, con la publicación de la famosa obra de Boole en 1854 y las contribuciones de, entre otros, Frege y Peano, para culminar con el tratado de Russell y Whitehead[2].

Esta axiomatización, sin embargo, no se produjo instantáneamente, sino que tuvieron que pasar bastantes años y discusiones para que se pudiera llegar a un punto de partida que fuera aceptado por la comunidad científica.

La manipulación de expresiones matemáticas, llámense figuras geométricas o símbolos, permitieron un entendimiento más profundo de los hechos matemáticos y de su interdependencia. Esta experimentación se inició con el propósito de establecer relación entre la abstracción y las aplicaciones vitales. Sin embargo, la formulación de una afirmación que se suponía correcta no era suficiente para incorporarla al conocimiento matemático. Para tener certeza de la veracidad de la proposición era necesario que se pudiera deducir de un conjunto de afirmaciones aceptadas como verdaderas con

[1] Leo Corry, *Modern Algebra and The Reise of Mathematical Structures*. Department of Mathematics and Statistics, York University, Canada. 1996.
[2] Jean Piaget, *¿Cómo enseñar matemáticas?*. Traducción al castellano: Jesús Hernández.

anterioridad. Para tener un punto de partida y poder fundamentar las afirmaciones, se propuso un conjunto de afirmaciones que no se demuestran y que se conocen como *axiomas*.

Los historiadores pueden repetir tanto como quieran que Euclides desarrolló la geometría sobre una base axiomática, sin embargo algunos autores señalan que ningún matemático que haya echado una ojeada a los "Elementos" puede estar de acuerdo con ello. Cualquiera que haya contemplado esta obra desde una actitud moderna se da cuenta que hay algo que no encaja bien, pero como desde educación elemental nos han dicho que Euclides propuso el método axiomático, la reacción habitual consiste en hablar de "lagunas"[3].

La axiomática moderna comienza con los *Fundamentos de la Geometría*, de Hilbert. Hilbert enseñó a los matemáticos a pensar axiomáticamente, es decir, a intentar reducir cada teoría a su esquema lógico más estricto.

Puede decirse que la culminación del método axiomático se alcanza en el siglo anterior con Nicolás Bourbaki. Bourbaki comenzó hacia 1940 la publicación de unos *Elementos de Matemáticas* que pretendían exponer sistemáticamente y de manera rigurosa nuestra ciencia. Según la doctrina de Bourbaki[4], la evolución interna de las matemáticas ha ido poniendo de manifiesto la unidad profunda de una ciencia que a principios de siglo no era más que una colección de disciplinas particulares, aunque fuertemente interrelacionadas. La esencia de dicha evolución reside en la sistematización de las relaciones entre las distintas teorías de las matemáticas, y se resume en el método axiomático.

Así, las matemáticas, como una expresión de la mente humana, reflejan la voluntad activa, la razón contemplativa y el deseo de la perfección estética. Sus elementos básicos son la lógica y la intuición, el análisis y la construcción, la generalidad y la individualidad. Aunque diferentes tradiciones realzan aspectos distintos, es sólo la interacción de estas fuerzas antitéticas y la lucha por su síntesis lo que constituye la vida, la utilidad y el valor supremo de la ciencia matemática[5].

1.1.1 Relación entre los axiomas y teoremas.

Como ya hemos señalado, los axiomas son afirmaciones matemáticas que no se demuestran y que son el punto de partida de un conjunto de conocimientos matemáticos.

Un *teorema* es una afirmación que se puede deducir de axiomas o afirmaciones anteriores que han sido demostradas como verdaderas previamente. Un *corolario* es una afirmación que se deduce inmediatamente de un teorema. Un *lema* es una afirmación

---

[3] A. Seidenberg, *"Did Euclid's Ekements Book I Develop Geometry Axiomatically?"* Arch. Hist. Exact. Sc. 14 (1975), 263-296.

[4] Expuesta en su artículo *L'architecture des mathématiques*, recogido en *Les grads courants de la pensée mathématique*, París, 1962, 34-47. Traducción de Nestor Minguez, *Las grandes corrientes del pensamiento matemático*, Buenos Aires, Eudeba, 1962.

[5] Richard Counrant, Herbert Robbins, *¿Qué son las matemáticas?* P. 17, 2006.

intermedia, que se vuelve importante por sí misma, en la cadena de demostración de un teorema.

Con la comprensión de esta relación lógica entre axiomas y teoremas fue posible cuestionar la veracidad incontrovertible de los axiomas y jugar a cambiar alguno para realizar deducciones diferentes a las ya obtenidas. Al primer sistema de conocimientos matemáticos al que se le aplicó este cuestionamiento fue a la geometría[6].

Los axiomas son afirmaciones que lucen verdaderas en las circunstancias y para los fines que se formulan, pero no son inamovibles ni absolutos. En realidad, hay pocos axiomas que se apliquen a las matemáticas en su totalidad, por ejemplo, los "*axiomas de la teoría de conjuntos*", y hay axiomas específicos dentro de las diferentes ramas de las matemáticas. En ocasiones estos axiomas se enuncian formalmente y en ocasiones se encuentran incorporados en definiciones.

1.1.2 Lógica matemática y demostraciones.

Es las secciones precedentes se han tratado brevemente los orígenes del Método Axiomático y de las modificaciones a las que ha sido sometido. En este apartado se da un resumen de algunos resultados de lógica y técnicas de demostración necesarios para el estudio del resto de los apuntes, aclarando que, la intención no es estudiar la lógica matemática, sino introducir (o recordar) algunos términos que aparecen con frecuencia en el material.

La lógica podemos pensarla como el estudio y análisis de los métodos del razonamiento[7]. A lo largo del material nos encontraremos con argumentos para probar ciertos resultados y la lógica provee los métodos para la corrección de estos argumentos. Todas las demostraciones y razonamientos matemáticos se basan en proposiciones, que son enunciados declarativos o cadenas de símbolos inteligibles que se pueden clasificar como verdaderos o falsos. No es necesario saber si una proposición dada es en realidad verdadera o falsa, pero debe ser lo uno o lo otro y no puede ser ambas cosas a la vez. Las proposiciones que siempre son verdaderas se llaman tautologías. Las proposiciones que siempre son falsas se llaman contradicciones o falacias. Algunas proposiciones a veces son verdaderas y a veces son falsas. Desde luego, para que la proposición sea totalmente clara es necesario que se haya establecido el contexto adecuado y que se haya definido adecuadamente el significado de los signos[8].

Existen varias maneras diferentes de formar nuevas proposiciones a partir de proposiciones dadas usando conectivos lógicos.

Si *P* es una proposición, entonces su *negación* es la proposición denotada por "no *P*" que es verdadera cuando *P* es falsa y es falsa cuando *P* es verdadera.

---

[6] Araceli Reyes Guerreo, *Álgebra Superior*, p. 2-4, México, 2005.
[7] Felipe Zaldívar, *Fundamentos de álgebra*, p. 13, México, 2005.
[8] Robert Bartle; Donald Sherbert. *Introducción al análisis matemático de una variable*. Limusa Wiley. Segunda edición. México. 2001.

Si P y Q son proposiciones, entonces su *conjunción* es la proposición denotada por "$P \wedge Q$", que es verdadera cuando tanto P como Q son verdaderas y es falsa en los demás casos.

De manera similar, la *disyunción* de P y Q es la proposición denotada por "$P \vee$ Q" que es verdadera cuando al menos una de ellas es verdadera y falsa cuando ambas son falsas.

Una manera muy importante de formar una nueva proposición a partir de proposiciones dadas es la *implicación* (o *condicional*), denotada por

$$(P \Rightarrow Q), \qquad \text{(si } P \text{ entonces } Q) \qquad \text{o} \qquad (P \text{ implica } Q)$$

En este caso a P se le llama la *hipótesis* y a Q se le llama la *conclusión* de la implicación. En los razonamientos matemáticos, las implicaciones son motivo e gran interés cuando la hipótesis es verdadera, pero no lo son tanto cuando la hipótesis es falsa. El procedimiento aceptado es tomar la proposición $P \Rightarrow Q$ como falsa únicamente cuando P es verdadera y Q es falsa; en los casos restantes la proposición $P \Rightarrow Q$ es verdadera.

Una demostración se dirá que es una *demostración directa* si al afirmar que la hipótesis P de la implicación $P \Rightarrow Q$ implica la conclusión Q se afirma que siempre que la hipótesis P es verdadera, entonces Q es verdadera. La construcción de una demostración directa de $P \Rightarrow Q$ requiere de una cadena de proposiciones $R_1, R_2, \ldots, R_n$ tal que

$$P \Rightarrow R_1, R_1 \Rightarrow R_2, \ldots, R_n \Rightarrow Q$$

La ley del silogismo establece que si $R_1 \Rightarrow R_2$ y $R_2 \Rightarrow R_3$ son verdaderas, entonces $R_1 \Rightarrow R_3$ es verdadera. Esta construcción no suele ser una tarea sencilla; puede requerir intuición y considerable esfuerzo.

Por otro lado, a las demostraciones que se inician con el supuesto de que la conclusión Q es falsa se les llama *demostraciones indirectas*. Hay básicamente dos tipos de demostración indirecta:

i Demostraciones por el contrapositivo. En lugar de demostrar $P \Rightarrow Q$, se puede probar su contrapositivo; es decir *no* $Q \Rightarrow$ *no* P.

ii Demostraciones por contradicción. Este método de demostración hace uso del hecho de que si C es una contradicción (es decir, una proposición que siempre es falsa), entonces las proposiciones

$$P \text{ y } (\textit{no } Q) \Rightarrow C, \quad P \Rightarrow Q$$

son equivalentes. Por tanto, $P \Rightarrow Q$, se establece demostrando que la proposición P y (*no* Q) implica una contradicción.

1.2 Estructuras algebraicas.

En esta segunda parte del capítulo se tratan los conceptos de anillo, dominio entero y campo, que son tan solo algunos ejemplos de estructuras algebraicas. Se enuncian y demuestran algunas de las propiedades más conocidas y esto servirá para deducir otras conceptos más generales en los capítulos siguientes.

Utilizaremos el término "conjunto" y se considerará como sinónimo de "clase", "colección" o "familia", pero estos términos no se definirán así como tampoco se dará una lista de axiomas para la teoría de conjuntos. Por conveniencia usaremos la notación y la terminología de conjuntos elemental. Supongamos que A designa un conjunto. La notación $x \in A$ significa que x está en el conjunto A. Escribiremos $x \notin A$ para indicar que x no está en A.

Un conjunto A es un subconjunto de B si cada elemento de A está también en B. Lo indicaremos escribiendo $A \subseteq B$. Un subconjunto es no vacío si contiene, por lo menos, un elemento.

El concepto de estructura algebraica se gesta a partir de la comprensión de las propiedades básicas de las operaciones de los números y la integración con el concepto de conjunto. El concepto evoluciona al descubrir que existen conjuntos, por ejemplo operaciones geométricas y operaciones de intercambio de objetos, que tienen las mismas propiedades que las operaciones numéricas. Otro componente importante para la evolución del concepto de estructura algebraica es descubrir que existen conjuntos no numéricos, como los polinomios, cuyas operaciones tienen las mismas propiedades que los conjuntos de números[9].

1.2.1 Dominios Enteros y Anillos.

En matemáticas aparecen con mucha frecuencia conjuntos en los cuáles se definen dos operaciones binarias, llamadas suma y producto, que se denotan generalmente por los símbolos + y × respectivamente.

Supondremos que existe un conjunto no vacío D de elementos, a los cuales llamaremos números. Por ***operación binaria*** en un conjunto D se entiende una función B de números de D, con dominio $D \times D$ y codominio D. Por consiguiente, una operación binaria asocia a cada par ordenado (a, b) de elementos del conjunto D con un único $B(a, b)$ de D. Sin embargo en lugar de usar la notación $B(a, b)$, se utilizan las notaciones comunes $a+b$ y ab en la explicación de las propiedades de la adición y multiplicación.

<u>*Definición 1.*</u> Sea D un conjunto de elementos $a, b, c, \ldots$ en el cual la suma $a+b$ y el producto ab de cualesquiera dos elementos a y b (distintos o no) de D están definidos. Entonces, el conjunto D, junto con estas operaciones, es llamado ***dominio entero*** si los siguientes axiomas se cumplen:

Axioma 1. El conjunto de números de D es cerrado bajo la operación suma y la operación multiplicación, es decir, si $a, b \in D$, entonces $a + b \in D$ y $ab \in D$.

---

[9] Araceli Reyes Guerrero, *Álgebra Superior*, pg. 256, México, 2005.

Axioma 2. La suma y la multiplicación de números de *D* es conmutativa, es decir, si $a, b \in D$, entonces

$$a + b = b + a.$$
$$ab = ba.$$

Axioma 3. La suma y la multiplicación de números de *D* es asociativa, es decir, si $a, b, c \in D$, entonces

$$(a + b) + c = a + (b + c).$$
$$(ab)c = a(bc).$$

Axioma 4. En *D* el producto distribuye a la suma, es decir, si $a, b, c \in D$**,** entonces,

$$a(b + c) = ab + ac.$$
$$(a + b)c = ac + bc.$$

Axioma 5. Existe en *D* un elemento neutro para la suma, llamado cero (*0*), tal que para cualquier $a \in D$,

$$a + 0 = 0 + a = a.$$

Axioma 6. Existe en *D* un elemento neutro para la multiplicación, el uno (1), tal que si $a \in D$**,**

$$a1 = 1a = a.$$

Axioma 7. Para cada *a* en *D*, existe en *D* un elemento llamado inverso aditivo que se denota por $-a$, tal que

$$a + (-a) = (-a) + a = 0.$$

Axioma 8. Si $a, b \in D$**,** *a* y *b* son diferentes de cero, entonces $ab \neq 0$.

<u>*Definición 2.*</u> A los elementos *a*, *b* distintos de cero cuyo producto es cero se les llama ***divisores de cero***.

De los axiomas anteriores se pueden deducir todas las leyes usuales del álgebra elemental. Las más importantes se escogen como teoremas. Cabe señalar que las letras *a, b, c, …, x, y, …* representan escalares de *D* a menos que se establezca lo contrario.

Teorema 1. *Si $a + b = a + c$ entonces $b = c$ (con esto se demuestra que el 0 del axioma 5 es único).*

Demostración. Dado $a+b=a+c$, y en virtud del axioma 7, se puede elegir *y* de manera que $y+a = 0$, con lo cual $y+(a+b) = y+(a+c)$, aplicando la propiedad asociativa $(y+a)+b = (y+a)+c$, o sea, $0+b = 0+c$. Pero en virtud del axioma 5, se tiene que $0+b = b$ y que $0+c = c$, o sea, $b = c$. Obsérvese que este teorema demuestra que existe uno y solo un número que tiene la propiedad del *0* en el axioma 5. En efecto, si *0* y *0´* tuvieran ambos esa propiedad, entonces, $0+0´ = 0$ y $0+0 = 0$, por tanto $0´+0=0+0$ y por tanto $0=0´$.

■

Teorema 2. *Dados a, b existe un (único) x tal que a + x = b. Este x se designa por b – a. En particular 0 – a se escribe simplemente –a y se denomina negativo de a.*

Demostración. Dados *a* y *b* se elige *y* de manera que $a+y = 0$ y sea $x = y+b$. Entonces, $a+x = a+(y+b) = 0+b = b$. Por tanto hay por lo menos una *x* tal que $a+x = b$. Pero en virtud del teorema anterior, hay a lo sumo una y sólo una *x* en estas condiciones.

■

Teorema 3*. Dados a, b, se tiene que b – a = b + (-a).*

Demostración. Sea $x = b-a$ y sea $y = b + (-a)$. Se trata de probar que $x = y$. Por definición de *b*-a, $x+a=b$ y

$$y+a = [b+(-a)]+a = b+[(-a)+a] = b+0 = b.$$

Por tanto, $x+a = y+a$, entonces $x = y$.

■

Teorema 4. *El inverso aditivo del inverso aditivo de un número a es a, es decir, -(-a) = a.*

Demostración. Se tiene que $a+(-a) = 0$ por definición de *–a*. Pero esta igualdad dice que *a* es el opuesto de *(-a)*, es decir, que $a = -(-a)$ como lo afirma el teorema.

■

Teorema 5. *Dados a, b, c, se tiene que a(b – c) = ab – ac.*

Demostración. Por Teorema 2 sabemos que existe un *x* tal que $x = b-c$, por tanto, $b = x+c$, luego, $ab = a(x+c) = ax+ac$, y aplicando nuevamente el Teorema 2 tenemos que $ax=ab-ac$ y restituyendo el valor de *x*, tenemos que $a(b-c) = ab-ac$.

■

Teorema 6. *Para toda $a \in D$, $0*a = a*0 = 0$.*

Demostración. Por el axioma 5 se sabe que $a + 0 = 0 + a = a$. Obsérvese también que

$$a(a + 0) = aa + a0 = aa + 0 = aa$$

y como

$$aa + a0 = aa + 0$$

aplicando el Teorema 1 su concluye que $a0 = 0a = 0$.

■

Teorema 7 *(Cancelación para el producto). Si $a, b, c \in D$, $a \neq 0$, y $ab = ac$, entonces $b=c$.*

Demostración. Por hipótesis $ab = ac$, entonces $ab-ac = 0$, de donde $a(b-c) = 0$ y como $a\neq0$, necesariamente $b-c = 0$, es decir, $b = c$.

■

Obsérvese que el teorema 7 es lógicamente equivalente a la afirmación del axioma 8 (¿Por qué?).

Teorema 8. *Si a, b ∈ D, entonces:*

$$(-a)(b) = -(ab)$$
$$(-a)(-b) = ab$$

Demostración. Se deja como ejercicio para el lector.

Frecuentemente, surgen sistemas algebraicos similares a los dominios enteros en los cuales la multiplicación no satisface el axioma 8, o la propiedad conmutativa para el producto, o incluso el axioma 6. Estos sistemas más generales son llamados *anillos*[10]. Así, un anillo es un conjunto *J,* junto con dos operaciones, *x+y* y *xy*, llamadas suma y multiplicación que satisfacen:

i. El conjunto de números de *J* es cerrado bajo la operación suma, y la operación multiplicación, es decir, si $a, b \in J$, entonces $a + b \in J$ y $ab \in J$.

ii. La suma de números de *J* es conmutativa, es decir, si $a, b \in D$, entonces

$$a + b = b + a.$$

iii. La suma y la multiplicación de números de *J* es asociativa, es decir, si $a, b, c \in J$, entonces

$$(a + b) + c = a + (b + c).$$
$$(ab)c = a(bc).$$

iv. En *J* el producto distribuye a la suma, es decir, si $a, b, c \in J$**,** entonces,

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc.$$

Si *xy = yx* para todo *x* e *y* de *J*, se dice que el anillo es ***conmutativo***. Si existe un elemento 1 en *J* tal que $1x = x1 = x$ para todo *x*, se dice que *J* es un ***anillo con unidad***, y 1 es la unidad de K

Ejemplo 1. Sea *A* un conjunto con tres elementos: $A = \{\bar{0}, \bar{1}, \bar{2}\}$ y definamos dos operaciones, a las cuales les seguiremos llamando adición (o suma) y multiplicación (o producto) denotándolas por + y x respectivamente. Tales definiciones las observamos en las siguientes tablas:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

[10] Kenneth Hoffman, Ray Kunze, *Álgebra Lineal*, pg. 139, 1973.

A partir las operaciones ya definidas, se observa en las tablas que se cumple el axioma 1, ya que para cualquiera de las dos operaciones, la operación que se efectúe proporcionará siempre un elemento del conjunto *A*. Es claro también que se cumplen los axiomas 2, 3, y 4 y sólo se hará énfasis en los axiomas 5, 6 y 7. Para el axioma 5, se observa que el neutro aditivo del conjunto *A* es el elemento $\bar{0}$. Para el axioma 7, el inverso aditivo del elemento $\bar{0}$, es $\bar{0}$, mientras que, los inversos aditivos de los elementos $\bar{1}$ y $\bar{2}$ son respectivamente $\bar{2}$ y $\bar{1}$. Por último, para el axioma 6 se observa que el neutro multiplicativo del conjunto *A* es el elemento $\bar{1}$. Con las operaciones así definidas, se verifica que el conjunto *A* es un anillo conmutativo con unidad. Como comentario adicional acerca de este ejemplo, observemos que el axioma 8 también se cumple, ya que para cualesquiera elementos de *A* diferentes de $\bar{0}$, su producto también será distinto de $\bar{0}$, de modo que *A*, junto con las operaciones de suma y multiplicación definidas en las tablas, es también un dominio entero.

Ejemplo 2. Sea *B* conjunto con elementos: $B = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. Como en el ejemplo anterior, se definen dos operaciones, a las cuales les seguiremos llamando adición (o suma) y multiplicación (o producto) denotándolas por + y x respectivamente. Tales definiciones las observamos en las siguientes tablas:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

A partir las operaciones ya definidas, se observa en las tablas que se cumple el axioma 1, ya que para cualquiera de las dos operaciones, el cálculo que se efectúe proporcionará siempre un elemento del conjunto *B*. Del mismo modo, se cumplen los axiomas 2, 3, y 4 y, como en ejemplo 1, sólo se hará énfasis en los axiomas 5, 6 y 7. Para el axioma 5, se observa que el neutro aditivo del conjunto *B* es el elemento $\bar{0}$ mientras que para el axioma 6, el neutro multiplicativo del conjunto *B* es el elemento $\bar{1}$. El axioma 7 también se cumple ya que el inverso aditivo del elemento $\bar{0}$, es $\bar{0}$, mientras que, los inversos aditivos de los elementos $\bar{1}, \bar{2}$ y $\bar{3}$ son respectivamente $\bar{3}$, $\bar{2}$ y $\bar{1}$. Con las operaciones así definidas, se verifica que el conjunto *B* es un anillo conmutativo con unidad. Sin embargo, a diferencia del ejemplo 1, en este conjunto y con estas operaciones, no es posible concluir lo mismo para el caso de dominio entero. Observemos que el axioma 8 no se cumple, ya que para el elemento $\bar{2} \neq \bar{0}$ de *B*, el producto $\bar{2} \times \bar{2}$ es, según la definición, $\bar{0}$. De este modo, el conjunto *B*, junto con las operaciones de suma y multiplicación definidas en las tablas, no forman un dominio entero.

1.2.2 Axiomas de orden (Ordenación de los números).

Este conjunto de axiomas se refiere a un concepto por el que se establece una *ordenación* entre los números de un conjunto dado. Según esta ordenación se puede decidir si un número es mayor o menor que otro. Se introducen aquí las propiedades de

orden, como un conjunto de axiomas referentes al concepto "primitivo" de positivo, para definir después los conceptos de mayor que y menor que a partir del de positivo.

Definición 3. Sea E un conjunto no vacío. Una relación binaria R en E es una relación de orden si se verifica que:

i. $\forall\, x \in E\ xRx$ (Propiedad reflexiva);
ii. $\forall\, x, y, z \in E\ xRy\ \&\ yRz \Rightarrow xRz$ (Propiedad transitiva);
iii. $\forall\, x, y \in E\ xRy\ \&\ yRx \Rightarrow x=y$ (Propiedad antisimétrica).

Observación. Si R verifica (*i*) y (*ii*) se dice que es un preorden. La relación de orden R suele representarse por $\leq_R$ o simplemente por $\leq$.

Definición 4. Una relación de orden $\leq$ en un conjunto E se llama total si $\forall\, x, y \in E$ se tiene que $x \leq y$ o $y \leq x$. Un conjunto totalmente ordenado es un par $(E, \leq)$, donde $E \neq \varnothing$, y $\leq$ es un orden total en E.

Así, suponemos la existencia de una relación $<$ sobre un conjunto dado que establece una ordenación entre los números y que satisface los axiomas siguientes.

Axioma 9. Se verifica una y solo una de las relaciones $x = y$, $x < y$, $x > y$.

Nota: $x > y$ significa lo mismo que $y < x$.

Axioma 10. Si $x > y$, entonces $x + z > y + z$.

Axioma 11. Si $x > y$ e $y > z$, entonces $x > z$ (propiedad transitiva).

Definición 5. Existe un subconjunto no vacío P de E, llamado conjunto de números positivos, que satisface las siguientes propiedades:

i. Si a, b pertenecen a P, entonces $a+b$ pertenece a P.
ii. Si a, b pertenecen a P, entonces ab pertenece a P.
iii. Si a pertenece a D, entonces se cumple exactamente una de las siguientes afirmaciones:

$$a \in P, \qquad a = 0, \qquad -a \in P.$$

Las dos primeras propiedades aseguran la compatibilidad del orden con las operaciones de adición y multiplicación, respectivamente. A la condición *iii* se le conoce como **propiedad de tricotomía**, ya que separa a E en tres tipos de elementos distintos. Establece que el conjunto $\{-a : a \in P\}$ de los números **negativos** no tiene elementos en común con P y, además, que el conjunto E es la unión de tres conjuntos disjuntos.

Definición 6. Un dominio entero D es ordenado si contiene elementos llamados positivos que satisfacen la definición 4.

Teorema 9. *En cualquier dominio entero ordenado todos los cuadrados (a^2) distintos de cero son positivos.*

Demostración. Sea a^2 dado, con $a \neq 0$. Por la propiedad de tricotomía, cualquiera de los dos elementos a, $-a$ son positivos. En el primer caso, a^2 es positivo por el inciso *ii* de la definición 5. En el segundo caso, $(-a)^2 = a^2$ por el teorema 8. Entonces a^2 es positivo.

■

Ahora se pueden definir los símbolos <, >, ≤ y ≥ llamados respectivamente, *menor que, mayor que*, *igual o menor que*, e *igual o mayor que*, de la manera siguiente:

$x < y$ *significa que* $y-x$ *es positivo;*

$x \leq y$ *significa que, o* $x < y$ *o* $x = y$*;*

$y \geq x$ *significa lo mismo que* $x \leq y$.

Teorema 10*. Sean a, b, c elementos en D.*

i. Si $a > b$ y $c > 0$, entonces $ac > bc$.
ii. Si $a > b$ y $c < 0$ entonces $ac < bc$.

Demostración. Se deja como ejercicio para el lector.

Todo lo visto anteriormente nos permite observar que la relación de orden admite una interpretación geométrica simple. Si $x < y$, esto quiere decir que el número x está a la izquierda del número y. Así, los números positivos están a la derecha del cero y los números negativos están a su izquierda. Si $a < b$, un número x satisface las desigualdades $a < x < b$ si y sólo si x está entre a y b.

<u>*Definición 7.*</u> Sea D un dominio entero ordenado. El *valor absoluto* $|a|$ de a es el número 0, si a es 0, y en otro caso es el miembro positivo de la pareja a, $-a$.

Una manera alternativa de expresar esta definición es la siguiente:

$$|a| = +a \text{ si } a \geq 0; \qquad |a| = -a \text{ si } a < 0.$$

1.2.3 Campos (Cuerpos).

La estructura algebraica, más familiar, es la de campo. Se designará por la letra K al conjunto de elementos (números o escalares) que formen parte o que pertenezcan a K. Para tal efecto se supondrá la existencia de dos operaciones, llamadas <u>*adición (+)*</u> y <u>*multiplicación (*)*</u> tales que para cada par de números x, y en K**,** se puede formar la <u>*suma*</u> de x e y que es otro número de K designado por $x+y$, y el producto de x e y que es otro número de K que se designa por $x*y$ o simplemente por xy.

<u>*Definición 8.*</u> El conjunto K con dos operaciones de *suma* y *multiplicación* que cumpla con los siguientes axiomas se dirá que es un campo.

Axioma 1. $\forall\ x, y \in \boldsymbol{K}$ se tiene que $x + y = y + x;\ xy = yx$;

Axioma 2. $\forall\ x, y, z \in \boldsymbol{K}$ se tiene que $x + (y + z) = (x + y) + z;\ x(yz) = (xy)z$;

Axioma 3. $\forall\ x, y, z \in \boldsymbol{K}$ se tiene que $x(y + z) = xy + xz$;

Axioma 4. Existencia de neutros. Existen dos números distintos, el *0* y el *1*, tales que $\forall\ x \in \boldsymbol{K}$ se tiene que $x + 0 = 0 + x = x;\ x*1 = 1*x = x$;

Axioma 5. Existencia de negativos. $\forall\ x \in \boldsymbol{K}$, existe un (único) número $y \in \boldsymbol{K}$ tal que $x + y = y + x = 0$.

Axioma 6. Existencia del recíproco. $\forall\ x \neq 0 \in \boldsymbol{K}$, existe un (único) número $y \in \boldsymbol{K}$ tal que $xy = yx = 1$.

De los axiomas anteriores se puede concluir que un campo también cumple con la definición de dominio entero y con la definición de anillo (probablemente también con la definición de anillo conmutativo con unidad). Así, algunas de las propiedades analizadas en la sección anterior son también propiedades de un campo. Cabe señalar, que los axiomas referentes al orden pueden no cumplirse para un campo dado. Esto se estudiará en el capítulo 3, referente a los números complejos. Ya dicho lo anterior, es posible deducir otras las leyes usuales del álgebra elemental que quizás sean ya conocidas. Las más importantes se escogerán como teoremas y las demostraciones son dejadas como ejercicios para el lector. Una vez más, cabe señalar que las letras *a, b, c, …, x, y, …* representan escalares de *K* a menos que se establezca lo contrario.

Teorema 11. *Dados a, b con* $a \neq 0$, *existe un (único) x tal que* $ax = b$. *La x se designa por b/a o por* $\frac{a}{b}$ *y se denomina cociente de b y a. En particular se tiene que 1/a se escribe* a^{-1} *y se designa como recíproco de a.*

Teorema 12. *Si* $a \neq 0$, *entonces* $b/a = ba^{-1}$.

Teorema 13. *Si* $a \neq 0$, *entonces* $(a^{-1})^{-1} = a$.

Teorema 14. *Si* $ab = 0$, *ó* $a = 0$ *ó* $b = 0$.

Teorema 15. *(a/b) + (c/d) = (ad + bc)/(bd) si b y d no son ambos cero.*

Teorema 16. *(a/b)*(c/d) = (ac/bd) si b y d no son ambos cero.*

Teorema 17. *(a/b)/(c/d) = (ad/bc) si b, c, d no son cero.*

Las demostraciones de estos teoremas se dejan como ejercicio.

■

En resumen, supóngase que se tiene un conjunto *K* de objetos *a, b, c, …, x, y, …* y dos operaciones definidas sobre los elementos de *K* como sigue: la primera operación, llamada adición, asocia a cada par de elementos *x, y* de *K* un elemento *(x+y)* de *K*; la segunda operación, llamada multiplicación, asocia a cada par de elementos *x, y* de *K* un elemento *xy* de *K*; si estas dos operaciones satisfacen los axiomas (1)-(6) enunciados anteriormente, se dirá entonces que el conjunto *K* junto con estas dos operaciones forma un *campo*. Hablando aproximadamente, un campo es un conjunto, junto con algunas operaciones sobre los elementos de éste, que se comportan como la adición, sustracción, multiplicación y división corrientes de los números en el sentido de que obedecen a las 6 reglas del álgebra dadas anteriormente.

Definición 9. Se dirá que un conjunto *K* es un campo ordenado si contiene elementos llamados positivos y además, si satisface la definición 5 y los axiomas de orden.

Ejercicios.

1. Demostrar el Teorema 8.

2. Demostrar el Teorema 10.

3. Demostrar los Teoremas 11, 12, … , 17 referentes a la sección de campos.

4. Demostrar que si *a, b, c, d* son enteros tales que $a>b$ y $c>d$, entonces $a+c > b+d$.

5. Demostrar que si *a, b* son enteros tales que $a < b$, entonces $-a > -b$.

6. Demostrar que si *a, b* son enteros, entonces $a^2 + b^2 \geq 0$.

7. Demostrar que el sistema que contiene únicamente al 0 y al 1, con las operaciones de adición y multiplicación definidas usualmente, con la excepción de que 1+1 = 0 (en lugar de 2) es un dominio entero. ¿Este sistema es también un campo? Justifique su respuesta.

8. Sea *Q* el conjunto de números de la forma $a + b\sqrt{5}$, con *a, b* números enteros. Se definen las operaciones de suma y multiplicación, respectivamente, de la siguiente manera:

$$\left(a + b\sqrt{5}\right) + \left(c + d\sqrt{5}\right) = \left(a + c\right) + \left(b + d\right)\sqrt{5}$$

$$\left(a + b\sqrt{5}\right) \times \left(c + d\sqrt{5}\right) = \left(ac + 5bd\right) + \left(ad + bc\right)\sqrt{5}$$

   Además, de dirá que $a + b\sqrt{5} = c + d\sqrt{5}$ si y sólo si, $a = c$, $b = d$. ¿Es el conjunto *Q*, junto con estas operaciones un dominio entero?

2. Números enteros

El álgebra moderna ha expuesto desde el principio de su existencia una gran riqueza de sistemas matemáticos. Una parte importante de ésta se dedica al estudio y comprensión de los mismos, así como a entender la manera en como se construyen[1]. Como indicamos en el capítulo 1, hay ciertos sistemas algebraicos bi-operacionales, en los cuales se cumplen ciertas propiedades ya estudiadas con anterioridad. Partiendo de éste punto, examinaremos de manera más profunda uno de los conjuntos más conocidos, que es el de los números enteros. La razón por la cual partimos de este punto es porque el concepto abstracto de anillo tiene sus orígenes en este conjunto[2].

2.1 Operaciones y propiedades de los números enteros.

Consideremos el conjunto de los números naturales $\boldsymbol{N} = \{1, 2, 3, \ldots\}$. Recordemos que en este conjunto es un sistema de Peano en el que se definen dos operaciones, suma y multiplicación, las cuales cumplen las propiedades de cerradura, conmutatividad y asociatividad; la existencia del neutro multiplicativo. Recordemos también que la motivación original para la construcción de este conjunto fue el establecer alguna relación entre diversas colecciones de objetos y los números naturales, teniendo así la posibilidad de numerar o contar los objetos considerados. En este sentido, cabe señalar que los números que representan distintas cantidades de elementos no hacen referencia alguna a las características individuales de los objetos contados. Por ejemplo, el número siete es una abstracción de todas las colecciones reales de siete cosas y no depende de ninguna cualidad específica de esas cosas ni de los símbolos usados[3]. A pesar de esto, otras operaciones tan simples como la sustracción, en general no se pueden realizar dentro de éste conjunto. Ante esta situación, surge la necesidad de construir un conjunto que cumpla con un mayor número de propiedades y que nos permita establecer de algún modo alguna relación entre este nuevo conjunto y algunas de las estructuras algebraicas tratadas en el capítulo 1.

Tomando en cuenta lo anterior, consideremos a R como la relación sobre $[\boldsymbol{N}\cup\{0\}]\times[\boldsymbol{N}\cup\{0\}]$ definida como: $(a, b)\mathrm{R}(c, d) \Leftrightarrow a+d = b+c$, donde "+" es la suma usual de números naturales. La relación así definida es una relación de equivalencia (se deja como ejercicio demostrarlo). Esta relación nos permite clasificar el conjunto $[\boldsymbol{N}\cup\{0\}]\times[\boldsymbol{N}\cup\{0\}]$, que por comodidad, a cada clase la vamos a representar como se muestra a continuación: la clase de {(0,0), (1,1), (2,2), …} la representaremos por [0]; la clase de {(1,0), (2,1), (3,2), …} la representaremos por [1], …, la clase de $\{(n, 0), (n+1, 1), \ldots, (n+p, p)\ldots\}$ la representaremos por $[n]$. Estas clases de equivalencia reciben el nombre de <u>*números enteros positivos*</u>, los cuales, en conjunto, denotaremos por $\mathbf{Z}^+$. De forma análoga, a la clase {(0,1), (1,2), (2,3),…} la representaremos por [-1]; {(0,2), (1,3), (2,4),…}, la representaremos por [-2], …, $\{(0, n), (1, n+1), \ldots, (p, n+p)\}$, la representaremos por $[-n]$. Estas clases reciben el nombre de <u>*números enteros negativos*</u>, y se denotarán por $\mathbf{Z}^-$. Así, diremos que un número entero es una pareja de

[1] Garret Birkhoff, Saunders Mac Lane, *A Survey Of Modern Algebra*. 1964.
[2] Herstein, I. N., *Álgebra moderna: Grupos, anillos, campos, teoría de Galois*. 1970.
[3] Richard Courant, Herbert Robbins, *¿Qué son las matemáticas?* 2006

números naturales (m, n) y este número entero será positivo si $m > n$; será cero si $m = n$; o será negativo si $m < n$.

De la unión de los conjuntos $\mathbf{Z}^+$ y $\mathbf{Z}^-$ surge el conjunto de los números enteros. Como es costumbre, se denotará por **Z** a este conjunto donde **Z** = {…-2, -1, 0, 1, 2…}.

Una vez ya definido lo que es un número entero, veamos como podemos operar con enteros. Para esto, sean (m, n), (m', n') números enteros. Considérense los símbolos: + y ×, los cuales denotan, respectivamente, suma y multiplicación. Entonces la suma de enteros se define como:

$$(m, n) + (m', n') = (m+m', n+n')$$

Mientras que la multiplicación se define como:

$$(m, n) \times (m', n') = (mm'+nn', mn'+nm')$$

Con estas operaciones en mente, considérense a *a, b, c* como representantes de cualquier clase de equivalencia de números enteros. Se tiene entonces que los enteros verifican los siguientes:

Axioma 1. El conjunto de números enteros es cerrado bajo la operación suma, y la operación multiplicación, es decir, si $a, b \in Z$, entonces $a + b \in Z$ y $ab \in Z$.

Axioma 2. La suma y la multiplicación de números enteros es conmutativa, es decir, si $a, b \in Z$, entonces

$$a + b = b + a.$$
$$ab = ba.$$

Axioma 3. La suma y la multiplicación de números enteros es asociativa, es decir, si $a, b, c \in Z$, entonces

$$(a + b) + c = a + (b + c).$$
$$(ab)c = a(bc).$$

Axioma 4. En *Z* el producto distribuye a la suma, es decir, si $a, b, c \in Z$**,** entonces,

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc.$$

Axioma 5. Existe en *Z* un elemento neutro para la suma, llamado cero (*0*), tal que para cualquier $a \in Z$,

$$a + 0 = 0 + a = a.$$

Axioma 6. Existe en *Z* un elemento neutro para la multiplicación, el uno (1), tal que si $a \in Z$**,**

$$a1 = 1a = a.$$

Axioma 7. Para cada *a* en *Z*, existe en *Z* un elemento llamado inverso aditivo que se denota por $-a$, tal que

$$a + (-a) = (-a) + a = 0.$$

Axioma 8. Si $a, b \in Z$, a y b son diferentes de cero, entonces $ab \neq 0$.

Teorema 1. *El conjunto de los números enteros, junto con las operaciones de adición y multiplicación dadas anteriormente, constituyen un anillo conmutativo con unidad.*

Observación. El axioma 8 nos dice que en el conjunto de los números enteros no hay divisores de cero, lo cual, según las propiedades abordadas en el Capítulo I, el conjunto de los enteros es también un *dominio entero*.

Se verá ahora, como a partir de los axiomas enunciados anteriormente pueden deducirse otras propiedades que fueron ya tratadas en el Capítulo 1 y que solamente se enunciarán sin proporcionar la demostración.

Teorema 2. *Si $a, b, c \in Z$, y $a + b = a + c$ entonces $b = c$ (con esto se demuestra que el 0 del axioma 5 es único).*

Teorema 3. *Dados $a, b \in Z$ existe un (único) $x \in Z$ tal que $a + x = b$. Este x se designa por $b – a$. En particular $0 – a$ se escribe simplemente $–a$ y se denomina negativo de a.*

Teorema 4. *Dados $a, b \in Z$ se tiene que $b – a = b + (-a)$.*

Teorema 5. *El inverso aditivo del inverso aditivo de un número a es a, es decir, $-(-a) = a$.*

Teorema 6. *Dados $a, b, c \in Z$ se tiene que $a(b – c) = ab – ac$.*

Teorema 7. *Para todo $a \in Z$, $0 \times a = a \times 0 = 0$.*

Teorema 8. *(Cancelación para el producto). Si $a, b, c \in Z$, $a \neq 0$, y $ab = ac$, entonces $b=c$.*

Teorema 9. *Si $a, b \in Z$, entonces:*

$$(-a)(b) = -(ab)$$
$$(-a)(-b) = ab$$

2.1.1 Propiedades de orden de los números enteros.

Otro aspecto importante a considerar de los números enteros, es la posibilidad de enlistarlos de la siguiente manera:

$$\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4\ldots$$

Esta manera de ordenarlos se obtiene a partir de la relación "*menor que*" denotada por el símbolo "<". De esta manera, la afirmación $a < b$, (*a menor que b)* se refiere a que el entero a se encuentra a la izquierda del entero b en la lista descrita anteriormente. De esta manera, la relación $a < b$ se mantiene si y sólo si la diferencia $b – a$ es un entero

positivo. Más aún, cada propiedad de la relación $a < b$ puede ser deducida de las propiedades de clase de los números enteros positivos.

Con estas observaciones, se tiene entonces que

Definición 1. El subconjunto no vacío $\boldsymbol{Z}^+$ de Z satisface las siguientes propiedades:

i. Si a, b pertenecen a $\boldsymbol{Z}^+$, entonces $a+b$ pertenece a $\boldsymbol{Z}^+$.
ii. Si a, b pertenecen a $\boldsymbol{Z}^+$, entonces ab pertenece a $\boldsymbol{Z}^+$.
iii. Si a pertenece a Z, entonces se cumple exactamente una de las siguientes afirmaciones:

$$a \in \boldsymbol{Z}^+, \qquad a = 0, \qquad -a \in \boldsymbol{Z}^+.$$

De esta manera se ha garantizado la existencia de una relación de orden < sobre el conjunto de los enteros, y que además satisface los siguientes axiomas

Axioma 9. Dados $a, b \in \boldsymbol{Z}$, se verifica una y solo una de las relaciones $a = b$, $a < b$, $a > b$.

Axioma 10. Dados $a, b \in \boldsymbol{Z}$, si $a > b$, entonces $a + c > b + c$.

Axioma 11. Dados $a, b, c \in \boldsymbol{Z}$, si $a > b$ y $b > c$, entonces $a > c$.

Así, tenemos entonces que

Definición 2. El conjunto de los números enteros es un conjunto ordenado.

A partir de los axiomas y definiciones dadas anteriormente, se verifica también que los siguientes teoremas se satisfacen para los números enteros

Teorema 10. *En el conjunto de los números enteros, todos los cuadrados (a^2) distintos de cero son positivos.*

Teorema 11*. Sean a, b, c son números enteros.*

i. Si $a > b$ y $c > 0$, entonces $ac > bc$.
ii. Si $a > b$ y $c < 0$ entonces $ac < bc$.

2.1.2 Unidades en los números enteros.

El Axioma 7 nos asegura la existencia de un único elemento en el conjunto de los números enteros, denominado inverso aditivo, para cada elemento en Z, sin embargo podríamos preguntarnos ¿existen elementos en los números enteros tales que mediante la operación multiplicación, se obtenga el neutro multiplicativo? Dicha pregunta será respondida con el siguiente:

Teorema 12. *Los únicos elementos de* ***Z*** *que tienen inverso multiplicativo son -1 y 1.*

Demostración. Es inmediato verificar que el *0* no tiene inverso multiplicativo puesto que $0a = 0 \neq 1$ para cualquier entero *a*. Por otro lado, 1 tiene por inverso al 1, puesto que (1)(1) = 1. Mientras que -1 tiene por inverso multiplicativo al -1 pues (-1)(-1) = 1. Supóngase ahora que $a > 1$. Si *a* tuviera inverso multiplicativo, digamos que $a^{-1} \in Z$ entonces $(a)(a^{-1}) = 1$, ahora a^{-1} no puede ser negativo (¿Por qué?) por lo que $a^{-1} > 0$ y también $a^{-1} \neq 1$ puesto que si $a^{-1} = 1$ entonces $(a)(1) = a$. Por lo tanto $a^{-1} > 1$ y como $a > 1$ y $a^{-1} > 1$ entonces $(a)(a^{-1}) > 1$ lo cual contradice que $(a)(a^{-1}) = 1$. El caso en el que $a < -1$ es análogo al caso anterior.

■

<u>*Definición 3.*</u> En un anillo, a los elementos que tienen inverso multiplicativo se les llama *unidades*. De esta manera, las unidades en los enteros son únicamente el 1 y el -1.

2.1.3 Inducción sobre los números enteros.

Hemos de recordar que en los números naturales, *N*, los cuales con los mismo que los enteros positivos, Z^+, se cumple el principio de inducción. Es posible hacer ver también que Z es un conjunto inductivo, no obstante, es necesario antes hacer una generalización para tener un primer elemento por el cual empezar el principio de inducción.

Para tal caso observemos la siguiente propiedad que resulta ser equivalente al principio de inducción.

Principio del buen orden. Si *A* es un subconjunto no vacío de números naturales entonces *A* tiene un elemento que es menor que todos los demás elementos de *A*.

Teorema 13. *El principio de inducción implica el principio del buen orden.*

Demostración. Sea *A* un subconjunto no vacío de *N* y supongamos que *A* no tiene ningún elemento menor que todos los demás de *A*. Sea *B* el conjunto de todos los números naturales *b* tales que $b < a$ para toda *a* en *A*. Como ningún elemento es menor que sí mismo, *B* está contenido en el complemento A^c de A, como se observa a continuación: i) el 1 está en *B* ya que 1 no está en *A* pues de lo contrario habría un elemento, el 1, menor que todos los demás de *A*. Además, como el 1 es menor que todos los demás naturales, 1 es menor que todos los elementos de *A*, luego, 1 está en *B*. ii) Supóngase que *b* está en *B* (es decir $b < a$ para todo elemento *a* de *A*). Entonces $b+1$ pertenece a *B* también. En efecto, si $b+1$ no perteneciera a *B*, entonces $b+1 \geq a$ para cierta *a* de *A*. Como $b < a$, entonces $b+1 \leq a$, y de ambas desigualdades, $b+1 = a$ está en *A*. Entonces $b+1$ sería un elemento de *A* menor que todos los demás de *A*, contra lo supuesto.

Por todo lo observado anteriormente, según el principio de inducción, $B = N$ y como $B \subset A^c$, resulta que $A^c = N$, por lo tanto $A = \varnothing$, contra la suposición hecha al principio de la demostración.

■

Teorema 14. *El principio del buen orden implica el principio de inducción.*

Demostración. Sea M un subconjunto de N tal que $1 \in M$ y si $n \in M$ entonces $n+1 \in M$. Suponiendo el principio del buen orden se demostrará que $M = N$. Sea M^c el complemento de M en N. Si M^c es no vacío, M^c tiene un elemento mínimo m'. Por consiguiente, ya que $m'-1 < m'$, $m'-1$ no está en M^c, es decir, $m'-1 \in M$. Pero por hipótesis $(m'-1) + 1$ pertenece también a M, es decir, $m' \in M$, lo cual es una contradicción. Luego $M^c = \varnothing$ y $M = N$.

■

Una vez observado lo anterior, si fijamos $n_0 \in Z$, sea el conjunto $Z_{n_0} := \{m \in \mathbf{Z}$ tal que $m \geq n_0\}$ entonces el principio de inducción se cumple empezando por n_0. De manera análoga, el conjunto Z_{n_0} es un conjunto ordenado, es decir, cualquier subconjunto no vacío de Z_{n_0} tiene primer elemento o elemento mínimo.

Ejemplo: Demostrar que para todo entero $n \geq 1$, se cumple la siguiente expresión:

$$1+8+27+\cdots+n^3 = \left[\frac{n(n+1)}{2}\right]^2.$$

Solución: Observamos que la proposición se cumple para $n = 1$, es decir P(1) nos dice que

$$1^3 = \left[\frac{1(1+1)}{2}\right]^2 = \left[\frac{(2)}{2}\right]^2 = [1]^2 = 1.$$

Suponemos que se cumple para $n = k$, es decir, la proposición $P(k)$ es válida, por tanto,

$$1+8+27+\cdots+k^3 = \left[\frac{k(k+1)}{2}\right]^2$$

A esto se le conoce como hipótesis de inducción.

Ahora, lo que queremos demostrar es que también se cumple la expresión para $n = k+1$, por lo que nuestro objetivo será probar que

$$1+8+27+\cdots+k^3 = \left[\frac{k(k+1)}{2}\right]^2$$

se cumple. Para esto, a la hipótesis de inducción (la cual estamos tomando como verdadera), sumamos lo que sería el siguiente término de la suma, es decir, a ambos lados de la ecuación añadimos el término $(k+1)^3$, obteniendo así:

$$1+8+27+\cdots+k^3+(k+1)^3=\left[\frac{k(k+1)}{2}\right]^2+(k+1)^3$$

Observemos que el segundo término de la ecuación anterior es:

$$\left[\frac{k(k+1)}{2}\right]^2+(k+1)^3=\frac{k^2(k+1)^2}{4}+(k+1)^3=\frac{(k+1)^2}{4}\left[k^2+4(k+1)\right]=\frac{(k+1)^2}{4}\left[k^2+4k+4\right]$$

donde

$$\frac{(k+1)^2}{4}\left[k^2+4(k+1)\right]=\frac{(k+1)^2}{4}\left[k^2+4k+4\right]=\frac{(k+1)^2(k+2)^2}{4}=\left[\frac{(k+1)(k+2)}{2}\right]^2$$

Por lo tanto, $1+8+27+\cdots+k^3+(k+1)^3=\left[\frac{(k+1)(k+2)}{2}\right]^2$, que es lo que se quería demostrar.

2.2 Divisibilidad de los números enteros.

En esta sección se abordará el concepto de divisibilidad de enteros. Este concepto es quizás el más importante de los números enteros (y de la *Teoría de números*) ya que partir de él se pueden deducir otras propiedades de suma relevancia. También nos permitirá en un futuro realizar otro tipo de clasificaciones de enteros, algunas de las cuáles han ocupado a grandes matemáticos de distintas épocas.

Definición 4. Si *a, d* son números enteros, decimos que *d divide a* si y sólo si existe un entero *k* tal que *a = dk.*

Visto de otro modo, tenemos que el concepto de divisibilidad menciona que si *a*, y *d* son enteros, con $d \neq 0$, el elemento *d* divide al elemento *a*, lo cual denotaremos por $d \mid a$, sí y sólo si existe un entero *k* tal que $a = kd$ y se dirá que: "*d* es divisor de *a*", o que "*d* es factor de *a*", o que "*a* es múltiplo de *d*", o que "*a* es divisible entre *d*".

El conjunto de divisores (factores) positivos y negativos de un entero *a* se detonará por *Div(a)* y el de los divisores positivos por $Div_+(a)$.

Ejemplos:

1) *-3* divide a *6*, (es decir, $-3 \mid 6$), ya que $6=(-3)(-2)$, donde $k = -2 \in Z$;
2) $7 \mid 56$, pues $56 = (7)(8)$, de igual modo, $7 \mid -56, -7 \mid 56, -7 \mid -56$;
3) *Div (6) = {-6, -3, -2, -1, 1, 2, 3, 6}* y $Div_+(6) = \{1, 2, 3, 6\}$;
4) Todo número entero $d \neq 0$ verifica que $d \mid 0$, pues *0 = (0)(d)*, donde *k=0.* Así el cero tiene infinitos divisores: *Div (0)* = Z -{0};
5) Como caso general del ejemplo 2, $d \mid a$ sí y sólo si $-d \mid a$, pues $a=kd \Leftrightarrow a=(-k)(-d)$. De la misma manera, $d \mid a \Leftrightarrow d \mid -a \Leftrightarrow -d \mid -a$. Se concluye entonces que

$d \mid a \Leftrightarrow |d| \mid |a|$. Este resultado se demostrará como corolario del Teorema 15. De esto se deduce que a cada divisor negativo le corresponde un divisor positivo, y que el número total de divisores, (si es finito) de *a* es el doble del número de divisores positivos.

Teorema 15. *Propiedad transitiva. Si a, b y c son números enteros tales que a | b y b | c, entonces a | c.*

Demostración. Por hipótesis, existen enteros *q* y *r* tales que $b=aq$ y $c=br$. Sustituyendo la primera igualdad en la segunda se obtiene: $c=(aq)r$ y agrupando factores, $c=a(qr)$, por lo tanto $a \mid c$ que es lo que se quería demostrar.

■

Teorema 16. *Si a, b son números enteros y u, u´ son unidades, entonces las dos condiciones siguientes son equivalentes:*

i. *a divide a b;*
ii. *ua divide a u´b.*

Demostración. Se demostrará primero que *i* implica *ii*. Supóngase que $b=aq$; ahora, ya que *u* es unidad, existe u_1 tal que $u\,u_1=1$; por lo tanto, $b=(u\,u_1)b=(u\,u_1)aq=ua(\,u_1q)$ lo que demuestra que *ua* divide *b* y es claro que *b* divide a *u´b* así, por teorema 14, *ua* divide a *u´b*.

Ahora se demostrará que *ii* implica *i*. En este caso tenemos que $u´b=uar$; y como *u´* es unidad, existe $u´_1$ tal que $u´u´_1=1$; por consiguiente, $b=(u´u´_1)b=(u´b)u´_1 =u´_1(uar)=a(uu´_1r)$ lo que prueba que *a* divide a *b*.

■

Corolario. *Si a, b son números enteros, entonces las dos condiciones siguientes son equivalentes:*

i. *a divide a b;*
ii. $|a|$ *divide a* $|b|$.

Un resultado interesante que relaciona las propiedades de divisibilidad y orden en ***Z*** es el siguiente:

Teorema 17. *Si* $a, b \neq 0$, *son enteros y* $a \mid b$ *entonces* $|a| \leq |b|$.

Demostración. Por el corolario anterior, se tiene que $|a| \mid |b|$, es decir, $|b| = |a|q$, con $q \geq 1$. Si $q=1$, $|b|=|a|$. Si $q \neq 1$, entonces $q=1 + q´$ con $q´$ positivo. Por lo tanto, $|b|=|a|(1 + q´)=|a| + |a|q´$, de donde $|b| - |a| = |a|q´ \geq 1$, de donde se observa que la diferencia es positiva y por lo tanto $|b| > |a|$.

■

Teorema 18. *Si $a \mid b$ y $a \mid c$ entonces $a \mid (b+c)$.*

Demostración. Las hipótesis señalan que, por definición, $b=ar$, $c=as$, entonces, $b + c = ar + as = a(r + s)$, de donde se concluye que $a \mid (b + c)$.

■

Teorema 19. *Si $a \mid b$ y c es un entero arbitrario, entonces $a \mid bc$.*

Demostración. Por hipótesis se tiene que $b=ar$, multiplicando por c en ambos lados de la identidad y agrupando factores se tiene que, $bc=a(rc)$.

■

Corolario. *Sean a, b, c enteros tal que $c \mid a$ y $c \mid b$ entonces $c \mid (ar + bs)$ para enteros arbitrarios r, s.*

Cuando se tienen dos números a y b, a los enteros de la forma $ar + bs$, con $r, s \in Z$ se les llaman ***combinaciones lineales*** de a y b.

Ejemplo: Sea $a = 27$ y $b = 6$. Así, 24 es combinación lineal de 27 y 6 ya que existen enteros r y s tales que $27r + 6s = 24$. Por tanto, $27(2) + 6(-5) = 24$.

Corolario. *Un entero c divide a los enteros a y b si y solo si c divide a cualquier combinación lineal de a y b.*

Demostración. El corolario anterior asegura que si c divide a y b, por lo tanto c divide a cualquier combinación lineal de a y b. Inversamente, ya que $a=1a + 0b$, $b=0a + 1b$, a y b son combinaciones lineales de a y b; por lo tanto si c divide a cualquier combinación lineal de a, b, entonces $c \mid a$ y $c \mid b$.

■

Es claro que, en general, dados dos enteros, no cualquier otro entero es combinación lineal de ellos. Por ejemplo 6 no es combinación lineal de 20 y 15, pues si así lo fuera tendríamos: $6=15r + 20s$ y como $5 \mid 15$ y $5 \mid 20$, por el corolario anterior tendríamos forzosamente que $5 \mid 6$, lo cual no es cierto. Es decir, una condición necesaria, para que un entero d sea combinación lineal de a y b es que d sea divisible entre todo divisor común de a y b. En otras palabras, si $e \mid a$ y $e \mid b$ pero e no divide a d, entonces d no es combinación lineal de a y b.

Ejemplo: Hallar todos los enteros a, con $a \neq 1$, tales que $a-1 \mid a^2+5$.

Solución: para resolver este ejercicio, investiguemos primero cuáles son los posibles múltiplos de $a-1$. Para ello, se sabe primero que $a-1 \mid a-1$, luego $a-1 \mid b(a-1)$, para cualquier entero b, y en particular, $a-1 \mid (a+1)(a-1)$. Así, se tiene que $a-1 \mid a^2+5$ y que $a-1 \mid a^2-1$, por lo tanto $a-1$ divide a la diferencia, es decir, $a-1 \mid 6$. Es decir $a-1 \in \{\pm1, \pm2, \pm3, \pm6\}$. Por lo tanto $a \in \{-5, -2, -1, 0, 2, 3, 4, 7\}$, y se concluye verificando que para cada valor de ese conjunto es cierto que $a-1 \mid a^2+5$.

2.2.1 El algoritmo de la división.

Observemos que en general, dados dos enteros *a*, *d*, no siempre es posible encontrar un entero *k* tal que $dk = a$. Si esto ocurre, decimos que *d* (o bien, *k*) no divide exactamente *a*, lo cual se denota por "$d \nmid a$". Por ejemplo, tenemos que en los enteros, $2 \nmid 7$. Sin embargo, como se verá a continuación, cuando esto sucede, siempre es posible encontrar una pareja de enteros *k*, *r*, tales que $a = dk + r$. A tal expresión, se le llamará división con residuo.

Teorema 20. Algoritmo de la división*.Dados a, d* $\in Z$*, con* $d \neq 0$*, existen k, r* $\in Z$*, que verifican:*

$$a = kd + r, con\ 0 \leq r < |d|$$

Además, k y r son únicos. Se dice que k es el <u>cociente</u> y r es el <u>residuo</u> de la división de a por d.

Antes de pasar a la demostración, revisemos algunos ejemplos:

1) Caso: $a > 0, d > 0$. Sean $a = 746$ y $d = 29$. Según el algoritmo de la división:

   $746 = (29)(25)+21$, por tanto $k = 25$, $r = 21$ ya que $0 \leq 21 < |29|$.

2) Caso: $a > 0, d < 0$. Sean $a = 746$ y $d = -29$. Según el algoritmo de la división:

   $746 = (29)(25)+21 = (-25)(-29)+21$, por tanto $k=-25$, $r=21$ ya que $0 \leq 21 < |-29|$

3) Caso: $a < 0, d > 0$. Sean $a = -746$ y $d = 29$. Según el algoritmo de la división:

   $746 = (29)(25)+21$, por tanto, $-746 = -(29)(25)-21$, pero $-21 < 0$

   lo cual es contrario a las condiciones del teorema. De esta manera, se corrige el residuo, y esto se consigue restando y sumando el valor absoluto divisor, que en este caso es 29. Luego:

   $-746 = -(29)(25) -29 +29 -21 = [(29)(-25) -29]+[29-21] = 29(-26) +8$. Por tanto, $k = -26$, $r = 8$ y así $0 \leq 8 < |29|$.

4) Caso: $a < 0, d < 0$. Sean $a = -746$ y $d = -29$. Según el algoritmo de la división:

   $746 = (29)(25)+21$, por tanto, $-746 = -(29)(25)-21$, pero $-21 < 0$

   Se corrige nuevamente como arriba restando y sumando el valor absoluto del divisor -29:

   $-746 = (-29)(25) -29 +29 -21 = [(-29)(25) -29]+[29-21] = (-29)(26) +8$. Por tanto, $k = 26$, $r = 8$ y así $0 \leq 8 < |-29|$.

La conclusión -como veremos en la demostración del teorema- es que para dividir números positivos o negativos por divisores positivos o negativos, basta saber hacerlo para dividendos y divisores positivos y luego corregir el cociente y/o residuo en cada caso.

Observación. Si $0 \leq a < |d|$, entonces $a = 0d + a$ implica $k = 0$ y $r = a$ pues a cumple la condición que tiene que cumplir el residuo.

Demostración del Teorema 20. El teorema consta de dos afirmaciones, la parte existencial, que requiere mostrar que existen k y r en las condiciones del teorema, y luego la unicidad: mostrar que no puede haber dos pares distintos de cociente y residuo para a y d dados.

Existencia: Vamos a probar primero en detalle el caso $a \geq 0;\ d > 0$, ya que, como nos sugieren los ejemplos, los otros casos se reducen a ese.

- Caso $a \geq 0;\ d > 0$:

Aquí, $|d| = d$. La idea intuitiva es considerar los elementos a, $a-d$, $a-2d$, $a-3d$, ...hasta que obtengamos algún elemento menor que d pero aún mayor o igual que cero. Este elemento será el residuo. Formalizamos esta idea de la siguiente manera:

Sea A un subconjunto de $Z_0 := Z^+ \cup \{0\}$ formado por los números de la forma $a - dj$ para algún entero j. Es decir, $A = \{a - dj;\ j \text{ en } Z\} \cap Z_0$. Claramente A es un subconjunto de Z_0 que no es vacío ya que $a = a-0d$ pertenece a A (estamos considerando el caso $a > 0$). Luego, por el principio del buen orden, el conjunto A tiene un elemento mínimo. Llamemos r a ese mínimo. Se tiene que $r \in A$ por un lado, y por otro lado r es menor que todos los demás elementos de A. Como $r \in A$, existe un elemento positivo o cero, llamémoslo k, tal que $r = a-dk$, luego $a = dk + r$. Falta probar que $0 \leq r < d$. Claramente $r \geq 0$ ya que r pertenece a A, que es un subconjunto de Z_0. Si r fuese mayor o igual que d, entonces $r - d \geq 0$ aún. Luego se tendría que el elemento $r-d = a-kd-d = a-(k+1)d$ está también en el conjunto A, pero este es menor que r lo cual es una contradicción ya que r es el mínimo. Así, se concluye que $r < d$.

- Caso $a \geq 0,\ d < 0$:

En este caso $-d > 0$ (y por lo tanto $|d| = -d$) y por el caso analizado anteriormente, existen $k´,\ r´$ tal que $a = k´(-d) + r$ con $0 \leq r´ < |-d|$, entonces $a = (-k´)d + r´$ y por lo tanto $k = -k´$ y $r = r´$.

- Caso $a < 0$:

Para este caso $-a > 0$ y de los casos anteriores, $-a = (k´)d + r´$ con $0 \leq r´ < |d|$. Luego $a = (-k´)d - r´$. Si $r´=0$, se cumple la condición del residuo y obtenemos $k=-k´$ y $r´=r=0$, pero si $r´\neq 0$, entonces $a = (-k´)d - r´ = ((-k)d - |d|) + (|d| - r´)$. Así, $k = -k´ \pm 1$ según si $d < 0$ ó $d > 0$ y $r = |d| - r´$. Se tiene entonces $a = kd + r$ con $0 < r < |d|$ ya que $0 < r´ < |d|$, entonces $-|d| < -r´ < 0$ implica que $|d| - |d| < |d| - r´ < |d|$ pero $|d| - r´ = r$ y luego entonces $0 < r < |d|$.

Unicidad: Supóngase que se tienen dos pares de cocientes y residuos, k, r y k', r'. Se probará entonces que $k = k'$ y $r = r'$. Sin pérdida de generalidad se puede suponer que $r \leq r'$, y luego:

$$a = kd + r = k'd + r' \text{ con } 0 \leq r \leq r' < |d|.$$

Así, $(k - k')d = r' - r$ implica que $d \mid (r' - r)$ y entonces, $|d| \mid (r' - r)$. Como $r' - r \geq 0$ por ser $r' \geq r$, $r' - r \neq 0$, se tiene que $|d| \leq (r' - r)$. Pero $r' < |d|$, luego, $r' - r < |d| - r < |d|$ (ya que $r \geq 0$). Luego no puede ser que $r' - r \neq 0$, es decir tiene que ser $r' = r$.

Se concluye también que $(k - k')d = 0$ y como $d \neq 0$, $k - k' = 0$, es decir, $k = k'$.

■

2.2.2 El Máximo Común Divisor.

Ya hemos visto que el conjunto de divisores de cualquier número entero es finito. Por lo tanto, dados dos números enteros a y b, el conjunto de divisores comunes de a y b es también un conjunto finito pues es la intersección del conjunto de divisores de a con el conjunto de divisores de b. Por consiguiente podemos hablar del siguiente concepto:

<u>Definición 5.</u> *Máximo Común Divisor*. Sean $a, b \in \mathbb{Z}$ no ambos nulos. El máximo común divisor entre a y b es el ***mayor*** de los divisores comunes de a y b.

Observación. Claramente ese número existe ya que la lista de divisores es no vacía (¿Por qué?), finita (por ser a y b no nulos) y es único.

El máximo común divisor entre a y b se denota por: $mcd\ (a, b)$, o bien, por $(a:b)$, entonces:

$$(a : b) \mid a, (a : b) \mid b \text{ y si } d \mid a \text{ y } d \mid b \text{ entonces } d \leq (a : b).$$

Denotaremos en lo sucesivo por $DivCom\ (\{a, b\})$ al conjunto de divisores comunes de a y b, y a $DivCom_+(\{a, b\})$ al conjunto de divisores positivos comunes de a, y b, es decir, en otras palabras:

$$DivCom\ (\{a, b\}) := \{ d \in Z, \text{ tal que } d \mid a \text{ y } d \mid b\} = Div\ \{a\} \cap Div\ \{b\}$$

$$DivCom_+\ (\{a, b\}) := \{ d \in Z, \text{ tal que } d \mid a \text{ y } d \mid b\} = Div_+\{a\} \cap Div_+\{b\}.$$

Ejemplos.

1) $(12 : 18) = 6$;
2) $(12:-35) = 1$ ya que $Div_+\{-35\} = \{1, 5, 7, 35\}$ y $Div_+\{12\} = \{1, 2, 3, 4, 6, 12\}$, entonces, $DivCom_+\{12, -35\} = \{1\}$;
3) $(a : b) = (b : a)$;

4) (a : b) = (-a : b) = (a – b) = (-a : -b) = (|a| : |b|);

5) (a : 1) = 1;

6) $a \neq 0$ se tiene *(a : 0) = |a|;*

7) *b | a* si y sólo si *(a : b) = |b|*

Con objeto de caracterizar de otra manera al máximo común divisor, veremos como se relaciona éste concepto con el de combinación lineal. Recordemos que una combinación lineal de *a, b* son los enteros de la forma: *c = ar + bs*.

En secciones pasadas vimos que una condición necesaria para que un número *c* sea combinación lineal de *a* y *b*, es que *c* sea divisible entre cualquier divisor de común *a* y *b*, en particular, entre el mcd de *a* y *b*. El segundo corolario de la siguiente proposición menciona que ésta condición es también suficiente.

Teorema 21. *Si a y b son números enteros positivos y d = as + bt es combinación lineal positiva mínima, entonces todo divisor de d es también de a y b.*

Demostración. Antes de comenzar con la demostración, entendamos que quiere decir el concepto de combinación lineal positiva mínima. Sea *C* el conjunto de números enteros tales que *C* = {*as + bt* : *as + bt > 0,* con *s, t*¸ números enteros}. Así, el conjunto *C* es el conjunto de combinaciones lineales positivas. Como *a, b* son no nulos, *aa + bb > 0* y por ende el conjunto *C* es no vacío y es un conjunto de números naturales. Por lo tanto, nos interesará el elemento menor del conjunto *C*, y a este número se le llamará *combinación lineal positiva mínima.*

Ahora, sólo nos interesará probar que *d | a* y *d | b*. Según el algoritmo de la división: *a = dq + r* con *$0 \leq r < d$*, como *d = as + bt*, entonces *a = (as+ bt)q + r*, luego *r = a(1 – sq) + b(- tq)* de donde se observa que *r* es combinación lineal de *a* y *b* y como *$0 \leq r < d$* y *d* es combinación lineal positiva mínima, se concluye que *r = 0*, por lo que *d | a*. De manera análoga se demuestra el caso *d | b*.

■

Corolario. *El mcd de dos enteros a, b es la combinación lineal positiva mínima de a y b.*

Demostración. Sea *d´ = (a : b)* y *d = as + bt* combinación lineal positiva mínima. Por la proposición anterior, *d | a* y *d | b* y como d´ es máximo común divisor, entonces *$d \leq d'$*. Ahora como *d´ | a* y *d´ | b*, entonces *d´ | d*, por lo tanto, *$d' \leq d$*, luego entonces *d´ = d*.

■

Corolario*. Un entero c es combinación lineal de a y b sí y sólo si (a : b) = d divide a c.*

Demostración. Sabemos que si *c = am + bn*, entonces, *d | c*. Inversamente, por el corolario anterior, *(a : b)* es la combinación lineal positiva mínima de *a* y *b*, *d = as + bt*. Si *d | c*, por definición, *c= dk*, de donde *c = ask + btk*.

■

2.2.3 Mínimo Común Múltiplo.

Definición 6. Sea $b \in Z$ con $b \neq 0$. El conjunto de múltiplos positivos de b es no vacío pues por *b* es múltiplo de *b*.

Para cualesquiera *a*, *b* números enteros, el conjunto de múltiplos positivos comunes es no vacío, por ejemplo *ab* es un múltiplo común positivo. Por el principio del buen orden, este conjunto tiene un elemento mínimo, al cual llamaremos *mínimo común múltiplo (m. c. m)* y lo denotaremos por $m = [a : b]$. Es decir, se define el *mínimo común múltiplo* de los enteros *a*, *b* como el mínimo valor del conjunto formado por los múltiplos comunes de *a* y *b*, y se denota por *[a : b]*.

Ejemplo. Si $a = 4$ y $b = 6$, los múltiplos comunes positivos de *4* y *6* son $\{4, 8, 12, 16, \ldots\} \cap \{6, 12, 18, \ldots\} = \{12, 24, \ldots\}$, entonces, $[a : b] = [4 : 6] = 12$.

Ejemplo. Si $a = 12$ y $b = 8$, $(a : b) = 4$ y $[a : b] = 24$. Obsérvese que $(12)(8) = (4)(24)$, es decir, $ab = (a : b)[a : b]$. En general esto es cierto.

Teorema 22. *Si a, b son enteros positivos, entonces* $ab = (a : b)[a : b]$.

Demostración. Sea $m = [a : b]$. Como ab es múltiplo común, entonces $m \mid ab$. Sea $d \in Z$ tal que $md = ab$. Probaremos que d es divisor común de *a* y *b*. Como *m* es múltiplo común de *a* y *b*, entonces $m = ar = bs$, de donde $md = ard = bsd = ab$. Como $a \neq 0$ y $b \neq 0$, entonces, $rd = b$ y $sd = a$ lo cual implica que d es divisor común de *a* y *b*.

Veremos ahora que *d* es divisible entre cualquier divisor común de *a* y *b*. Sea d' tal que $d' \mid a$ y $d' \mid b$, entonces $a = d'a'$ y $b = d'b'$. Tenemos al entero $m' = a'b'd' = ab' = a'b$ el cual es múltiplo común de *a* y *b*. Eso implica que $m' = mt$, y luego $mtd' = m'd' = a'd'\, b'd' = md$ y como $m \neq 0$, por la cancelación para el producto es válida, luego $td' = d$ implica $d' \mid d$.

De los dos párrafos anteriores, se sigue que $d = (a : b)$ y por lo tanto, $ab = [a : b](a : b)$. ■

2.2.4 El Algoritmo de Euclides.

En secciones anteriores se han tratado conceptos como el máximo común divisor y el mínimo común múltiplo de dos enteros. Una pregunta interesante sería ¿Existe algún método eficiente que permita calcular estos elementos? Como respuesta provisional tenemos que podemos encontrar el conjunto de divisores positivos comunes y luego seleccionar el mayor de ellos, mientras que en el otro caso, podemos encontrar el conjunto de múltiplos de cada uno de los enteros y seleccionar el más pequeño de los múltiplos comunes. Sin embargo, estos métodos pueden resultar bastante tediosos para enteros de dos dígitos o más.

Un hecho importante acerca del algoritmo de la división es que en la división de un entero por otro, obtenemos un cociente entero y un residuo entero no negativo, el cual

es menor que el divisor. Esta observación, realizada por Euclides (*circa* 300 a.C.) permitió diseñar un algoritmo en el cual mediante divisiones sucesivas, se pudiera determinar el máximo común divisor de dos enteros dados. Veamos como se desarrolla este algoritmo.

Sean *a*, *b* números enteros positivos tal que *a* no sea múltiplo de *b*, entonces en las divisiones sucesivas:

$$\begin{aligned} a &= bq + r_1, & 0 < r_1 < b \\ b &= r_1q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots & \vdots \\ &\vdots & \vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_n. \end{aligned}$$

Ya que $0 < r_n < r_{n-1} < \cdots < r_2 < r_1 < b$ es claro que después de aplicar el algoritmo un número finito de veces obtendremos un residuo de cero.

Ya una vez considerado lo anterior, tenemos que r_n es el máximo común divisor de los enteros *a* y *b*. Pero antes de pasar a la demostración de este hecho, consideremos el siguiente

Lema. *Si a = bq + r, entonces (a : b) = (b : r).*

Demostración. Sea *d=(a : b)* y *d´=*(*b* : *r*). En el primer caso tenemos que *d* divide a cualquier combinación lineal de *a* y *b*, en particular, *d* | *a-bq*, es decir, *d* | *r*. Por tanto, tenemos que *d* es divisor común de *b* y de *r* lo que implica que *d* | *d´*, es decir, *d* ≤ *d´*.

En el segundo caso tenemos que *d´* divide a cualquier combinación lineal de *b* y *r*, en particular, *d* | *bq+r*, es decir, *d* | *a*. Por tanto, tenemos que *d* es divisor común de *a* y de *b* lo que implica que *d´* | *d*, es decir, *d´* ≤ *d*.

De los dos casos, se concluye que *d* = *d´* y por tanto *(a : b) = (b : r).*

■

Teorema 23*. Si a, b son enteros positivos y b no es factor de a, entonces en las divisiones sucesivas:*

$$\begin{aligned} a &= bq + r_1, & 0 < r_1 < b \\ b &= r_1q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots & \vdots \\ &\vdots & \vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_n. \end{aligned}$$

Se obtiene que $r_n = (a : b)$.

Demostración. Como $r_{n-1} = r_n\, q_n$, entonces $(r_n : r_{n-1}) = r_n$. Por el lema anterior, $(r_{n-1} : r_n) = (r_{n-1} : r_{n-2})$, y aplicándolo sucesivamente, $(r_{n-1} : r_n) = (r_{n-1} : r_{n-2}) = (r_{n-1} : r_{n-3}) = \ldots = (a : b) = r_n$.

■

Ejemplo. Calcular *(628 : 40)*. Utilizando el algoritmo de Euclides tenemos que:

628 = 40(15) + 28,

40 = 28(1) + 12,

28 = 12(2) + 4,

12 = 4(3).

Así, *(628 : 40) = 4.*

Ejemplo. Calcular *(2199 : 93)*. Utilizando el algoritmo de Euclides, tenemos que:

2199 = 93(23) + 60,

93 = 60(1) + 33,

60 = 33(1) + 27,

33 = 27(1) + 6,

27 = 6(4) + 3,

6 = 3(2).

Así, *(2199 : 93) = 3.*

Observación. El algoritmo de Euclides no sólo permite calcular el máximo común divisor de dos números enteros, sino también nos proporciona un procedimiento para poder expresarlo como la combinación lineal positiva mínima.

Lema. *Si c es combinación lineal de a y b, y c´ es combinación lineal de c y b, entonces c´ es combinación lineal de a y b.*

Demostración. Por hipótesis, $c = as + bt$, $c´ = ck + bm$. Sustituyendo la primera identidad en la segunda, tenemos que:

$$c´ = (as + bt)k + bm = ask + btk + bm = a(sk) + b(tk + m)$$

así, *c´* es combinación lineal de *a* y *b*.

■

Ahora bien, ya tenemos las herramientas suficientes para encontrar los enteros *s, t* que permitan expresar el máximo común divisor de dos enteros *a, b* como combinación lineal positiva mínima.

Por ejemplo, supongamos *a, b* tal que $(a : b) = r_2$, por el algoritmo de Euclides:

$$a = bq + r_1,$$
$$b = r_1 q_1 + r_2,$$
$$r_1 = r_2 q_2.$$

Entonces:

$$r_2 = b - r_1 q_1,$$
$$r_1 q_1 = aq_1 - bqq_1,$$
$$r_2 = b(1 + qq_1) + a(-q_1).$$

De la misma forma es posible expresar el máximo común divisor de dos enteros para el caso en el que éste se encuentre en más pasos del algoritmo de Euclides.

Ejemplo. Expresar *(628 : 40)* como combinación lineal.

Solución. Utilizando el algoritmo de Euclides tenemos que:

$628 = 40(15) + 28,$

$40 = 28(1) + 12,$

$28 = 12(2) + 4,$

$12 = 4(3).$

Así, $(628 : 40) = 4.$

Despejando los residuos de cada una de las ecuaciones anteriores, tenemos que

$$28 = 628 + 40(-15),$$
$$12 = 40 + 28(-1) = 40 + 628(-1) + 40(15) = 628(-1) + 40(16),$$
$$4 = 28 + 12(-2) = 628 + 40(-15) + 628(2) + 40(-32) = 628(3) + (-47)$$

Por lo tanto los enteros r, s tales que $628r + 40s = (628 : 40)$ son, respectivamente, $r = 3$ y $s = -47$.

2.3 Ecuaciones Diofantinas.

Vamos a aplicar ahora lo estudiado a la resolución de ciertas ecuaciones con coeficientes enteros, llamadas *Ecuaciones Diofantinas*. Se llaman así las ecuaciones con coeficientes enteros de las cuales se buscan soluciones enteras[4]. El nombre se puso por Diofanto de Alejandría (*circa* 275 d.C.) quien fue quien estudió este tipo de problemas en su obra "La Aritmética". Las ecuaciones diofantinas más sencillas son las ecuaciones de la forma: $ax + by = c$, con $a, b, c \in \mathbf{Z}$, donde a, b no son ambos nulos, de las cuales se buscan pares de soluciones enteras.

Observemos que una ecuación de este tipo es la ecuación de una recta en R^2, y que nos estamos preguntando por qué puntos de coordenadas, ambas enteras, pasa esa recta,

[4] Cárdenas, Humberto; Raggi, Francisco; ET. AL. *Algebra Superior*. Trillas. México.1998

Sabemos que el algoritmo de Euclides permite expresar el máximo común divisor de dos enteros como combinación lineal de estos. Es este procedimiento, el que también nos da un método eficiente de encontrar parejas de soluciones *(x, y)* a ecuaciones diofantinas.

Antes de pasar a ecuaciones con estas características, observemos el siguiente resultado, conocido como el primer teorema de Euclides[5]:

Teorema 24. *Si $a \mid bc$ y $(a : b) = 1$, entonces $a \mid c$.*

Demostración. Por hipótesis $1 = as + bt$, multiplicando ambos lados de la identidad por c, $c = asc + btc$. Por hipótesis $a \mid bc$ y $a \mid a$, entonces, a divide a cualquier combinación lineal de a y bc, por lo tanto $a \mid c$.

■

<u>*Definición 7*</u>. Se dice que dos enteros a y b son <u>*primos entre si*</u> o <u>*primos relativos*</u> si $(a : b) = 1$.

Observación. De la definición anterior se sigue que a y b son primos entre si, sí y solo sí $1 = as + bt$.

El resultado anterior es de suma importancia ya que nos permite construir proposiciones tales como

Teorema 25. *Las soluciones enteras de la ecuación:*

$$ax + by = 0 \text{ con } (a : b) = 1 \text{ y } a, b \neq 0$$

$$\text{son } x = -bt \text{ e } y = at$$

Demostración. Es inmediato verificar que $x = -bt$ e $y = at$ es solución a la ecuación. Sólo falta probar que toda solución entera es de esta forma. Si $s = (x, y)$ es solución a la ecuación $ax + by = 0$ tenemos que $ax = -by$, entonces $a \mid by$. Por hipótesis, $(a : b) = 1$, luego $a \mid y$, por lo tanto, $y = at$, entonces, $ax = -bat$, y por la cancelación para el producto, $x = -bt$.

■

Teorema 26. *Una condición necesaria y suficiente para que la ecuación*

$$ax + by = c, \text{ con } a, b, c \in Z$$

tenga solución entera es que $(a : b) \mid c$.

Demostración. Sea $d = (a : b)$, entonces, $d = ar + bs$. Supóngase que $d \mid c$, entonces, $c = dk$, por consiguiente, $c = (ar + bs)k = ark + bsk = a(rk) + b(sk)$. Por lo tanto, $x = rk$, $y = sk$, es una solución a la ecuación.

■

[5] Felipe Zaldívar, *Fundamentos de álgebra*, pg. 151, México, 2005.

Ejemplo. Determinar si la ecuación $16x + 12y = 6$ tiene solución entera, y si es así, exhibirla.

Solución. Sabemos que una condición necesaria y suficiente para que la ecuación diofantina tenga solución, es que $(16 : 12)$ divida a 6, por tanto,

$16 = 12(1) + 4$,
$12 = 4(3)$.

Así, $(16 : 12) = 4$, y como 4 no divide a 6, no es posible una solución entera de la ecuación dada.

Ejemplo. Determinar si la ecuación $696x + 408y = 48$ tiene solución entera, y si es así, exhibirla.

Solución. Sabemos que una condición necesaria y suficiente para que la ecuación diofantina tenga solución, es que $(696 : 408)$ divida a 48, por tanto,

$696 = 408(1) + 288$,
$408 = 288(1) + 120$,
$288 = 120(2) + 48$,
$128 = 48(2) + 24$,
$48 = 24(2)$.

luego, $(696 : 408) = 24$, y como 24 divide a 48, es posible hallar una solución entera a la ecuación.

Ahora, como $24 = 696(-7) + 408(12)$, y $48 = 24(2)$, entonces, $24(2) = 48 = 696(-7)(2) + 408(12)(2) = 48 = 696(-14) + 408(24)$, por lo tanto, $x = -14$ & $y = 24$.

Veamos ahora como conociendo una solución entera de una ecuación diofantina dada, es posible encontrar el conjunto de todas las soluciones.

Teorema 27. *El conjunto de soluciones de enteras (x, y) de la ecuación:*

$$ax + by = c, \text{ con } a, b, c \in Z$$

es de la forma $x = x_0 + u$, $y = y_0 + v$, *en donde* x_0, y_0 *es una solución particular de la ecuación* $ax + by = c$ *y* u, v *son soluciones arbitrarias de la ecuación homogénea asociada* $ax + by = 0$.

Demostración. Sean x_0, y_0, x_1, y_1 soluciones distintas de la ecuación $ax + by = c$. Entonces, $u = x_1 - x_0$, $v = y_1 - y_0$, son soluciones de la ecuación $ax + by = 0$. Esto se verifica fácilmente, ya que

$$\begin{aligned} au + bv &= a(x_1 - x_0) + b(y_1 - y_0) \\ &= ax_1 + by_1 - (ax_0 + by_0) = c - c = 0 \end{aligned}$$

por tanto, $x_1 = u + x_0$ e $y_1 = v + y_0$, siendo u, v solución de la ecuación homogénea $ax + by = 0$.

Sea ahora u, v una solución de $ax + by = 0$. Entonces $x_1 = u + x_0$; $y_1 = v + y_0$ es solución de la ecuación original $ax + by = c$. Esto es sencillo verificarlo ya que

$$ax_1 + bx_1 = a(x_0 + u) + b(y_0 + v)$$
$$= ax_0 + by_0 + au + bv = c + 0 = c.$$

Recordemos que el Teorema 25 nos da un método para encontrar todas las soluciones de la ecuación homogénea

$$ax + by = 0, \text{ con } a, b \in \mathrm{Z},$$

Si $a = 0$, $b = 0$, entonces toda pareja de enteros x, y es solución. Supóngase ahora que $a \neq 0$, o $b \neq 0$. Sea $d = (a : b)$ y por tanto $a = da´$, $b = db´$. Como $d \neq 0$, la ecuación

$$a´x + b´y = 0$$

tiene las mismas soluciones que la ecuación anterior. Entonces, según el Teorema 22, las soluciones son $x = -b´t$, $y = a´t$, con t entero arbitrario.

■

Combinando estos resultados, se obtiene el siguiente

Corolario. *Sean a, b, c enteros tales que a y b no son ambos cero. Supongamos además que $d = (a : b) \mid c$. Sean $a = dk$, $b = dm$. Entonces el conjunto x, y de soluciones enteras de la ecuación*

$$ax + by = c$$

es $x = x_0 - mt$, $y = y_0 + kt$, con t un número entero cualquiera y x_0, y_0 solución particular de $ax + by = c$.

Observación. En caso de que $a = 0$, $b = 0$ y $c \neq 0$, la ecuación no tiene solución. Si $c = 0$, entonces toda pareja de enteros es solución.

Ejemplo. Determinar si la ecuación $696x + 408y = 48$ tiene solución. En caso afirmativo, encontrar el conjunto de todas las soluciones enteras.

Solución. Como se observó en ejemplos anteriores, la ecuación $696x + 408y = 48$ tiene solución entera. Para éste caso, la solución particular x_0, y_0 es respectivamente -14 y 24, mientras que $696 = 24(29)$ y $408 = 24(17)$, por tanto $a´ = 29$, $b´ = 17$ y $x´ = -17t$ e $y´ = 29t$. Por lo tanto el conjunto de soluciones enteras de la ecuación

$$696x + 408y = 48$$

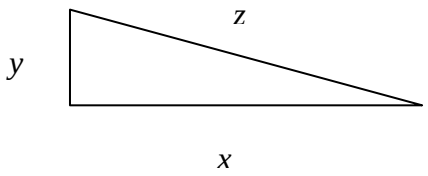
es $x = -14 - 17t$, $y = 24 + 29t$ con t entero arbitrario.

2.4 Números Primos.

Los números se utilizaron para fijar los recuerdos y celebrarlos y para las transacciones comerciales unos 5000 años antes de que se pensase en estudiarlos en sí mismos de forma sistemática. La primea orientación científica al de estudio de los enteros, es decir, el origen de la Teoría de los números, se atribuye generalmente a los griegos. Allá por los años 600 A.C., Pitágoras y sus discípulos efectuaron un estudio completo de los enteros. Fueron los primeros en clasificar los enteros de diversas formas:

Números pares: 2, 4, 6, 8, 10, 12, 14, 16, …
Números impares: 1, 3, 5, 7, 9, 11, 13, …
Números primos: 2, 5, 7, 11, 13, 17, 19, 23, 29,
Números compuestos: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, …

Además de estas clasificaciones, se relacionaron los números enteros con la geometría, realizando una conexión con el teorema de Pitágoras que establece que en todo triángulo rectángulo el cuadrado de la longitud de la hipotenusa es igual a la suma de los cuadrados de las longitudes de los catetos.



$$x^2 + y^2 = z^2$$

Los pitagóricos se interesaron por los triángulos rectángulos cuyos lados eran enteros, denominando a tales figuras como *triángulos pitagóricos*. La correspondiente terna de números (*x*, *y*, *z*) que representan las longitudes de los lados se llama *terna pitagórica*. Algunos ejemplos de estas ternas son los siguientes:

x	*4*	*8*	*12*	*16*	*20*
y	*3*	*15*	*35*	*63*	*99*
z	*5*	*17*	*37*	*65*	*101*

Otra contribución realizada por los griegos, fue la del estudio de los *números perfectos* (esta aportación fue hecha por Euclides) los cuales son llamados así porque se pueden representar como la suma de sus divisores propios (esto es, la suma de todos los divisores positivos menores que él)[6]. De esta manera, el 6 y 24 son números perfectos ya que:

$$6 = 1 + 2 + 3$$

$$24 = 1 + 2 + 4 + 7 + 14$$

[6] La reseña histórica introductoria de la sección de los números primos fue tomada de la obra de T. M. Apostol, *Introducción a la Teoría Analítica de los Números*, Editorial Reverté. España. 1984, pgs.: 1-5

Con estas clasificaciones en mente, profundicemos un poco más acerca de los números primos. Recordemos que el Teorema 19 nos dice que si $a \mid b$ y c es un entero arbitrario, entonces $a \mid bc$. Sin embargo, el caso inverso no es tan inmediato, es decir, si $a \mid bc$, eso no implica que $a \mid b$ o $a \mid c$. Por ejemplo, $6 \mid (3)(4)$, pero 6 no divide a 3 y 6 no divide a 4.

En si, la propiedad $a \mid bc$ implica $a \mid b$ o $a \mid c$ se cumple únicamente cuando a es un número primo, y de hecho, es la propiedad mas importante de los números primos.

A partir de las proposiciones y ejemplos anteriores, se concluye que para a un entero cualquiera distinto de cero, a tiene por lo menos 4 divisores distintos $(\pm 1, \pm a)$.Hay números enteros que tienen únicamente esos 4 divisores y hay otros que tienen más. Esto motiva la separación de los números enteros (distintos de $0, 1, -1$) en dos categorías, la de los números primos y la de los números compuestos.

<u>*Definición 8.*</u> Se dice que un número entero p, distinto de ± 1 es primo si sus únicos divisores son ± 1 y $\pm p$.

Observemos que si p es primo y a un entero entonces $(p:a)$ o bien es p o 1. Por tanto $(p:a) = p \Leftrightarrow p \mid a$.

Teorema 28. *Si un número primo p divide al producto ab de dos enteros, entonces p divide a o bien p divide a b, es decir,*

$$p \mid ab \Rightarrow p \mid a \text{ ó } p \mid b.$$

Demostración. Si $p \mid a$, no hay nada que probar. Si p no divide a entonces $(p : a) = 1$ y por la proposición tenemos que $p \mid b$.

De manera similar se puede demostrar que si un primo p divide a un producto $a_1a_2 \ldots a_n$, entonces p divide al menos a uno de los factores a_i.

■

Teorema 29. *Si p es un entero distinto de ±1 con la siguiente propiedad: si a, b $\in$ Z y p | ab implica que p | a ó p | b, entonces p es cero o p es un número primo.*

Demostración. Supóngase que $p \geq 0$. Sea primero el caso en el que $p > 1$. Si p no fuera primo entonces $p = ab$ con $1 < a < p$, $1 < b < p$. La igualdad anterior prueba que $p \mid ab$ y las desigualdades muestran que p no divide a y p no divide b, es decir, p no cumpliría con "$p \mid ab$ entonces $p \mid a$ ó $p \mid b$" luego entonces, si $p > 1$ y cumple con la propiedad entonces p es primo.

Si $p = 0$, p cumple con la propiedad ya que $0 \mid ab$, entonces $ab = 0$, por lo que $a = 0$ ó $b = 0$, es decir $0 \mid a$ y $0 \mid b$.

■

Cabe señalar que debido a la propiedad anterior, es conveniente considerar que en Z, 0 es primo.

Los números primos son de tal importancia, que a partir de estos se construyen los demás números enteros (a excepción de 1 y -1). Pongamos un ejemplo al respecto. Sabemos que los primeros números primos son 2, 3, 5, 7, 11, 13, … y que los números 4, 6, 8, 9, 10, 12, 14 se pueden expresar como el producto de los primeros cuatro primos positivos, a saber que

$$4 = 2 \times 2;$$
$$6 = 2 \times 3;$$
$$8 = 2 \times 2 \times 2;$$
$$9 = 3 \times 3;$$
$$10 = 2 \times 5;$$
$$12 = 2 \times 2 \times 3;$$

La generalización de este resultado es conocido como el *Teorema Fundamental de la Aritmética*, el cual afirma lo siguiente:

Teorema de Factorización Única. *Todo número entero a, distinto de ±1 se puede expresar en la forma:*

$$a = up_1 p_2 \cdots p_h$$

donde $a = \pm 1$, *y* $p_1, \ldots, p_h$ *son primos positivos. Además, si* $a \neq 0$, *la expresión es única, excepto en el orden de los factores.*

Demostración. Si $a = 0$, hacemos $u = 1$, $h = 1$ y $p_1 = 0$, y obtenemos $a = up_1$. Por tanto bastará con demostrar que se cumple para todo entero $a > 1$. Sea M el conjunto de enteros mayores que 1 que no se pueden descomponer de la forma en como lo plantean las afirmaciones. La mecánica de la demostración es hacer ver que $M = \varnothing$. Supongamos que $M \neq \varnothing$. Entonces por el principio del buen orden, M tiene un elemento menor, al cual llamaremos a. Si a fuera primo, entonces haciendo $h = 1$, $u = 1$ y $a = p_1$ tendríamos una expresión de la forma $a = up$ lo cual contradice que $a \in M$. Por tanto a no es primo, entonces $a = bc$ con $1 < b < a$ y $1 < c < a$. Como a es el elemento menor de M, entonces $b, c \notin M$ y por lo tanto, $b = p_1 p_2 \cdots p_n$ y $c = q_1 q_2 \cdots q_r$. Pero $a = bc = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_r$ que es una expresión de la forma $a = p_1 p_2 \cdots p_h$ y esto contradice una vez mas que $a \in M$. Por lo tanto, necesariamente se tiene que $M = \varnothing$.

Demostraremos ahora la unicidad (quizás excepto en el orden) de descomposiciones en primos positivos. Supóngase que $a = up_1 p_2 \cdots p_h$ y $a = u' q_1 q_2 \cdots q_t$ son dos factorizaciones de a. Es claro que $u = u'$, luego entonces $p_1 p_2 \cdots p_h = q_1 q_2 \cdots q_t$ y como p_1 divide $p_1 p_2 \cdots p_h$, debe entonces suceder que $p_1 \mid q_1 q_2 \cdots q_t$ y como p_1 es primo, entonces p_1 divide a alguna q_i. Supóngase que es q_1, entonces $p_2 \cdots p_h = q_2 \cdots q_t$. De manera análoga se concluye que $p_2 = q_2$. Si $h < t$ llegaríamos a que $q_{h+1} \ldots q_t = 1$ lo cual no es posible. Análogamente sucede lo mismo si $t < h$. Por lo tanto se concluye que $t = h$ y así queda probada la unicidad.

■

2.5 Congruencias.

Gauss introdujo una notación notable que simplifica muchos problemas relativos a la divisibilidad de los enteros. En este sentido creó una nueva rama de la teoría de números llamada *teoría de congruencias*[7], cuyos fundamentos se discutirán en esa sección.

Definición 9. Sean $a, b, d \in Z$, $d \neq 0$. Se dice que *a es congruente a b en modulo d* si y solo si $d \mid (a - b)$. Denotaremos que *a* es congruente a *b* en módulo *d* como: $a \equiv b \pmod{d}$, es decir, $a \equiv b \pmod{d} \Leftrightarrow d \mid (a - b)$.

Ejemplo.

1) $5 \equiv 3 \pmod{2}$, $5 \equiv -1 \pmod{2}$, $13 \equiv 8 \pmod{5}$, $13 \equiv 3 \pmod{5}$;
2) $5 \not\equiv 2 \pmod{2}$;
3) Para todo entero k, $2k \equiv 0 \pmod{2}$, $2k + 1 \equiv 1 \pmod{2}$.

Una manera alternativa de decir que $a \equiv b \pmod{m}$ es que la diferencia $(a - b)$ pertenece al conjunto de múltiplos de *m*. Sin embargo, existe aún otra definición alternativa de congruencia, basada en el hecho de que para cualquier entero *a* dividido por *m*, siempre hay un único residuo. Esta definición alternativa la formulamos de la siguiente manera.

Teorema 30. *Dos enteros a, b son congruentes en módulo m si y solo si dejan o proporcionan el mismo residuo cuando son divididos por* $|m|$.

Demostración. Como $a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{-m}$, será suficiente con probar que $m > 0$.

Supóngase primero que $a \equiv b \pmod{m}$, entonces por definición, $(a - b) = c\,m$. Por el algoritmo de la división sabemos que $b = mq + r$, es decir, *b* deja un residuo *r*, $o \leq r < m$ de la siguiente manera $b - mq = r$. Entonces,

$$a = b + cm = mq + r + c\,m = (q + c)m + r,$$

y esta ecuación indica que *r* es el único residuo de la división de *a* por *m*. Luego entonces *a* y *b* tienen el mismo residuo.

Inversamente, supóngase que $a = qm + r$ y $b = q'm + r$, con el mismo residuo *r*. Entonces $(a - b) = (q - q')m$ es divisible por *m*. Entonces se concluye $a \equiv b \pmod{m}$.

■

Teorema 31. *La relación de congruencia de un número entero fijo m y para enteros a, b, c, es una relación de equivalencia, es decir,*

1) $a \equiv a \pmod{m}$ *(reflexiva)*
2) $a \equiv b \pmod{m}$ *implica* $b \equiv a \pmod{m}$ *(simétrica)*
3) $a \equiv b \pmod{m}$ *y* $b \equiv c \pmod{m}$ *entonces* $a \equiv c \pmod{m}$ *(transitiva)*

Demostración. Se deja como ejercicio para el lector.

[7]George Andrews. *Number Theory*. Saunders Company. USA. 1971

Teorema 32. *Si $a \equiv b \pmod{m}$, entonces para cualquier entero x,*

$$a + x \equiv b + x \pmod{m}, \quad ax \equiv bx \pmod{m}.$$

Demostración. Se deja como ejercicio para el lector.

Observación. Hasta el momento hemos enunciado propiedades de las congruencias que también cumple la relación de igualdad. Sin embargo, en general, no todas las propiedades de la relación igualdad se cumplen para las congruencias. Por ejemplo, la ley de cancelación que se mantiene para las ecuaciones no necesariamente se mantiene para las congruencias. Considérese la congruencia: $24 \equiv 12 \pmod{3}$, esto no implica que $4 \equiv 2 \pmod{3}$. El razonamiento no es válido porque el entero *6*, que fue cancelado, es factor del módulo *3*, entonces la diferencia *24 –12* es divisible por el módulo *3* mientras se mantenga el factor *6*.

Sin embargo, es posible encontrar una ley de cancelación para congruencias de la siguiente manera:

Teorema 33. *Para cualesquiera c, m enteros primos relativos, $ca \equiv cb \pmod{m}$ implica $a \equiv b \pmod{m}$.*

Demostración. Por hipótesis, $ca \equiv cb \pmod{m}$. Esto implica que $m \mid (ca - cb) = c(a - b)$. Como c y m son primos relativos, se concluye que $m \mid (a - b)$. Aplicando la definición de congruencia a esta última igualdad, $a \equiv b \pmod{m}$.

■

Teorema 34. *Si c es primo relativo a m, la congruencia $cx \equiv b \pmod{m}$ tiene solución entera x. Cualesquiera dos soluciones x_1, x_2 son congruentes en módulo m.*

Demostración. Por hipótesis, $(c : m) = 1$, entonces $1 = cs + mt$, para enteros s, t. Multiplicando por b esta última igualdad, se tiene que

$$b = (bs)c + (bt)m$$

donde el último termino es múltiplo de m. Entonces $b \equiv (bs)c \pmod{m}$. Esto sugiere que $x = bs$ sea la solución requerida de $b \equiv xc \pmod{m}$, es decir, $cx \equiv b \pmod{m}$.

Por otro lado supóngase que x_1 y x_2 son soluciones de $cx \equiv b \pmod{m}$, es decir, $cx_1 \equiv b \pmod{m}$ y $cx_2 \equiv b \pmod{m}$. Como la relación de congruencia es una relación de equivalencia, $cx_1 \equiv cx_2 \pmod{m}$ y como c y m son primos relativos, entonces, $x_1 \equiv x_2 \pmod{m}$.

■

Ejemplo. Determinar si la congruencia $23x \equiv 11 \pmod{19}$ tiene solución.

Solución. Como *23* y *19* son primos relativos, ya que $(23 : 19) = 1$, entonces la congruencia tiene solución. Utilizando el algoritmo de Euclides,

$$1 = 23s + 19t = 23(5) + 19(-6),$$
entonces, $11 = 23(5)(11) + 19(-6)(11)$

Por lo que $x = (5)(11)$, es decir, $23(55) \equiv 11 (mod.\ 19)$.

Otra manera alternativa de determinar si una congruencia admite soluciones es el siguiente:

Teorema 35. *La congruencia $ax \equiv c (mod.\ b)$, con a, b, c números enteros; a, b no nulos, admite soluciones enteras sí y sólo si $(a : b) \mid c$.*

Demostración. Supóngase primero que la congruencia $ax \equiv c (mod.\ b)$ tiene solución entera. Eso implica, por definición, que $ax - c = bk$, para algún entero $k \neq 0$. Entonces, $ax + b(-k) = c$, donde se observa que c es combinación lineal de a y b y por tanto $(a : b) \mid c$.

De manera inversa, supóngase que $(a:b) \mid c$. Entonces podemos expresar a la congruencia $ax \equiv c (mod.\ b)$ en los "menores términos" mediante

$$a' = \frac{a}{(a:b)}, b' = \frac{b}{(a:b)}, c' = \frac{c}{(a:b)}$$

Así, llegamos a la congruencia "reducida" $a'x \equiv c' (mod.\ b')$. Obsérvese ahora que, si $(a:b) = as + bt$, entonces, $a's + b't = 1$, es decir, a' y b' son primos relativos y por lo tanto nos encontramos en el caso del teorema 33 y por lo tanto la congruencia $ax \equiv c (mod.\ b)$ tiene solución entera.

■

Un caso importante se da cuando el módulo m es un número primo. En este caso, todos los enteros no divisibles por m son primos relativos a m. Este hecho nos permite hacer el siguiente

Corolario. *Si p es número primo y $c \not\equiv 0$ (mód. p), entonces $cx \equiv b (mod.\ p)$ tiene solución única, módulo p.*

Al igual que el caso de sistemas ecuaciones lineales, donde lo que queremos encontrar son las soluciones simultáneas, podemos construir también "sistemas de congruencias lineales" donde lo que deseamos determinar es la solución común para las congruencias dadas. Sin embargo, un sistema de dos o más congruencias lineales no tiene necesariamente solución, aunque cada una de las congruencias individuales si tenga solución. Por ejemplo, no existe ningún x que satisfaga simultáneamente $x \equiv 1 (mód\ 2)$ y $x \equiv 0 (mód\ 4)$, a pesar de que cada una de ellas, separadamente, tiene solución. En este ejemplo, los módulos 2 y 4 no son primos entre sí. Ahora demostraremos que todo sistema de dos o más congruencias lineales que, separadamente, admiten solución única se puede resolver simultáneamente si los módulos son dos a dos primos entre sí.

Teorema 36. *Si los módulos m_1 y m_2 son primos relativos, entonces las congruencias*

$$x \equiv b_1 (mod.\ m_1),\ x \equiv b_2 (mod.\ m_2)$$

tienen una solución común x. Cualesquiera dos soluciones son congruentes módulo m_1m_2.

Demostración. La primera congruencia tienen solución b_1 y la solución general es $x = b_1 + ym_1$, para cualquier entero y. Esta solución debe satisfacer la segunda congruencia, es decir, $b_1 + ym_1 \equiv b_2 (mod.\ m_2)$, o bien $ym_1 \equiv (b_2 - b_1)(mod.\ m_2)$. Como m_1 es primo relativo a m_2, la congruencia puede ser resuelta mediante el método del teorema 34.

Por otro lado, supóngase que x y x' son dos soluciones dadas de las congruencias simultáneas. Entonces $x - x' \equiv 0 (mod.\ m_1)$ y también es congruente en módulo m_2. Como m_1 y m_2 son primos relativos, esto implica que la diferencia $x - x'$ es divisible por el producto de los módulos m_1m_2, lo que quiere decir que $x \equiv x' (mod.\ m_1m_2)$.

■

Ejercicios.

1. Sean a, b enteros tal que $b \mid a$. Demostrar que $b^n \mid a^n$.

2. Si $a < b$, ¿Cuáles son los valores de q y r en la igualdad $a = bq + r$, con $0 \leq r < |b|$?

3. Si $(a : b) = (a : c) = 1$, entonces $(a : bc) = 1$

4. Probar que cualquier entero a, con $a \neq 1$ y para todo número natural n, se cumple que $a - 1 \mid a^n - 1$.

5. Calcular el máximo común divisor de las siguientes parejas de enteros:

    a) 527, 765;
    b) 361, 1178;
    c) 108, 243;
    d) 156, 1740;
    e) 12321, 8658.

6. Supóngase que $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, y en general $F_n = F_{n-1} + F_{n-2}$ para $n \geq 3$. (F_n es llamado el *n-ésimo* número Fibonacci.). Demostrar que

$$F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$$

7. Demostrar que $x \equiv 7 (mód.\ 12)$ implica que $x \equiv 3 (mód. 4)$

8. Si $d \mid a$, $d \mid bc$ y $(a : b) = 1$, pruébese que $d \mid c$.

9. Si n es entero positivo, probar la identidad algebraica:

$$a^n - b^n = (a - b)\sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

10. Demostrar que, si a, b, c son enteros y $a+b=c$, entonces $a=c-b$.

11. Demostrar que si p es primo, entonces $\sqrt{p}$ no es un número racional.

12. Si $(a : b) = 1$, entonces $(a+b : a-b)$ o es 1 o es 2.

13. Para cada inciso, encontrar los enteros x tales que:

    a) $5x \equiv 4$ (mód. 3).
    b) $7x \equiv 6$ (mód. 5).
    c) $9x \equiv 8$ (mód. 7).
    d) $99x \equiv 100$ (mód. 101).
    e) $81x \equiv 57$ (mód. 117).

14. Demostrar que si $a>0$ y a no es primo, entonces hay un divisor primo p tal que $p \leq \sqrt{a}$.

15. Demostrar que para todo número natural n, $(9n+8 : 6n+5) = 1$.

16. Demostrar que si d es combinación lineal de a y b, y b es combinación lineal de a y c, entonces d es combinación lineal de a y c.

17. Demostrar que si a, b son enteros positivos y $a < b$, entonces $a^2 < b^2$. Encontrar ejemplos de números enteros a, b tales que $a < b$ y $a^2 > b^2$.

18. Demostrar que si $(a : c)=1$, $a \mid m$ y $c \mid m$, entonces $ac \mid m$.

19. Demostrar que si $a > 0$, entonces $(ab : ac) = a(b : c)$.

20. Demostrar que si a, b, c son enteros y $a - b = c$, entonces $a = c + b$.

21. Demostrar que si $(a : c)=d$, $a \mid b$ y $c \mid b$, entonces $ac \mid bd$.

22. Sean $c_1, c_2, ..., c_n$ enteros. Se les llama combinaciones lineales de $b_1, b_2, ..., b_n$ a los enteros de la forma

$$c_1 b_1 + c_2 b_2 + \cdots + c_n b_n$$

    a) Muestre que cada uno de los b_i es combinación lineal de $b_1, b_2, ..., b_n$.
    b) Demuestre que si a divide a los enteros $b_1, b_2, ..., b_n$, entonces a divide a cualquier combinación lineal de $b_1, b_2, ..., b_n$ e inversamente.

23. Probar que:

    a) 86 no es combinación lineal de 96 y 75.
    b) 42 no es combinación lineal de 84 y 76.
    c) 94 no es combinación lineal de 144 y 66.

24. Pruébese que si $d=(a : b)$ y $d=ar + bs$, entonces r y s son primos entre sí.

25. Si $d=(a : b)$ y $a=a´d$, $b=b´d$, pruébese que $a´$ y $b´$ son primos entre sí.

26. Demostrar el siguiente teorema. (Teorema de Fermat): Si a es un entero y p un entero primo, entonces

$$a^p \equiv a(mód.p)$$

Hint: Para un entero primo fijo p, pruebe por inducción sobre a.

27. Sean a, b enteros, y p un entero primo. Demostrar que

$$(a+b)^p \equiv a^p + b^p (\text{mod } p).$$

28. Pruébese que si $c \mid a$ y $(a : b)=1$ entonces $(b : c)=1$.

29. Encontrar el máximo común divisor d, de los enteros 299 y 481 y encontrar los enteros x, y tales que $299x+481y = d$.

30. Demostrar que hay infinidad de números primos.

31. Si a y b son primos entre sí, pruébese que el máximo común divisor de a y bc es igual al máximo común divisor de a y c. (Hint: Probar que el conjunto de divisores comunes de a y bc es el mismo que el conjunto de divisores comunes de a y c.)

32. Encontrar la solución general (si es que existe) de cada una de las siguientes ecuaciones diofantinas:

    a) $2x + 3y = 4$;
    b) $17x + 19y = 23$;
    c) $15x + 51y = 41$;
    d) $10x - 8y = 42$;
    e) $121x-88y = 572$.

33. Demostrar que si p y q son primos distintos entonces $(p : q)=1$.

34. Dados x e y, sean $m=ax+by$, $n=cx+dy$, en donde $ad-bc = \pm 1$. Probar que $(m : n) = (x : y)$.

35. Resolver el siguiente sistema de congruencias:

$$x \equiv 5(mód 7)$$
$$x \equiv 2(mód 12)$$
$$x \equiv 8(mód 13)$$

36. Demuéstrese que si un primo p divide a un producto de enteros $a_, a_2 \cdots a_n$, entonces p divide al menos a uno de los factores a_i.

37. La suma de dos enteros positivos es 5264 y su mínimo común múltiplo es 200340. Determinar ambos enteros.

38. Demuéstrese que si un primo p divide a b^n ($n \in \mathbf{N}$) entonces p divide a b.

39. Un turista y su guía escalaban aterrados la pirámide de Keops en Egipto, perseguidos por un fiero león. El turista subía los escalones de cinco en cinco, el guía de seis en seis y león de siete en siete. En cierto momento, el turista estaba a un solo escalón de la cima (donde estaba su escopeta), el guía a nueve y el león a diecinueve. ¿Cuál es el número mínimo de escalones que debe haber en la pirámide de Keops? Según los datos del problema, ¿Existe solución única?

40. Usando el principio del buen orden demuéstrese que todo entero mayor que 1 es divisible entre un número primo. (Hint: Considérese el conjunto M de enteros mayores que 1 que no tienen un factor primo. Si $M \neq \varnothing$, M tiene un elemento mínimo a, el cual no puede ser primo. Al descomponer a como un producto de dos enteros positivos mayores que 1, estos sí tienen factores primos.)

41. Demuestre que el mínimo común múltiplo de dos números primos entre sí es igual a su producto.

42. Sea d = (826 : 1890). Utilizar el algoritmo de Euclides para calcular d, y expresar entonces d como combinación lineal de 826 y 1890.

43. Demostrar que si a y b son primos entre sí y $a \mid c$ $b \mid c$, entonces $ab \mid c$.

44. Sea $d=(a : b)$ y $a=a'd$, $b=b'd$. Si $a \mid c$ y $b \mid c$, demuestre que $a'b'd \mid c$.

45. Si $k > 0$ demuéstrese que

$$(ka : kb) = k(a : b)$$
$$[ka : kb] = k[a : b].$$

46. Si $b_1, b_2, ..., b_n$ son enteros y $d_i = (b_1 : b_2 : ... : b_i)$ para $2 \leq i \leq n$, demostrar que

$$d_i = (d_{i-1} : b_i).$$

(Este ejercicio nos dice que el concepto de m.c.d. puede ser extendido a conjuntos de más de dos enteros.)

47. Pruébese la afirmación análoga del ejercicio anterior, para el caso del mínimo común múltiplo, para enteros $b_1, b_2, ..., b_n$ distintos de cero.

48. Un turista chino fue de viaje a Nueva York y encontró en una tienda un artículo que valía 11 dólares. Sólo traía monedas de su país, pero el vendedor acordó aceptarlas. Cuando habló por teléfono al banco para averiguar la equivalencia, le respondieron que 11 monedas chinas con hoyos redondos equivalían a 15 dólares, 11 monedas con hoyos cuadrados a 16 dólares y 11 monedas con hoyos

triangulares a 17 dólares. ¿Cuántas monedas de cada tipo se necesitaron para pagar el artículo? ¿Es única esta solución? Justifique su respuesta.

49. Sea *p* un número primo. Demostrar que Z_p es un dominio entero y que de hecho todos los elementos de Z_p tienen inverso multiplicativo, si las operaciones de suma y multiplicación de Z_p de definen de la siguiente manera:

$$a + b = pk + r, \text{con } 0 \leq r < p \text{ ; es decir, } a + b \equiv r(mód.p)$$

$$ab = pk' + s, \text{con } 0 \leq s < p \text{ ; es decir, } ab \equiv s(mód.p)$$

Así, para calcular las sumas y productos de enteros de Z_p sólo dividimos la suma (o la multiplicación) de a y b entre p y el residuo será el resultado de esta operación

50. Para cada inciso, determinar si existen enteros *x* tales que:

a) $6x \equiv 5$ (mód. 4),
b) $10x \equiv 8$ (mód. 6),
c) $12x \equiv 9$ (mód. 6).

3. Números complejos

3.1 Introducción.

Desde muchos años atrás se han escrito páginas y páginas en donde se proclaman las propiedades que tienen los números reales. No obstante, dicho sistema resulta ser insuficiente para la solución de diversos problemas que se presentan con frecuencia, en el álgebra, en las ecuaciones diferenciales y en otras ramas de la matemática[1]. Por este motivo, el campo de los reales tuvo que ser ampliado hasta formar un sistema numérico que hoy en día se conoce como el campo de los complejos. Uno de los principales motivos por los que fueron introducidos estos números es porque no es posible encontrar raíces reales a la ecuación:

$$x^2 + 1 = 0$$

Esta extensión de los números reales fue hecha de manera gradual por importantes personajes que intentaban resolver ciertas ecuaciones algebraicas. Por ejemplo, en 1545, Girolamo Cardano (1501-1576), intentó encontrar dos números cuya suma fuese 10 y cuyo producto fuese 40. Al final escribió $40 = \left(5 + \sqrt{-15}\right)\left(5 - \sqrt{-15}\right)$, resultado que le pareció absurdo. Más adelante, René Descartes (1596-1650), calificó de "imaginarias" las expresiones del estilo de $a + \sqrt{-b}$ (donde a es real y b es real positivo). Este término resulta ser quizá desafortunado ya que como se verá en secciones posteriores, de imaginarias no tienen absolutamente nada. Con frecuencia nos referiremos a la "parte imaginaria" de un número complejo, costumbre que se debe a Descartes. Si bien el concepto de número imaginario incomodaba a muchos matemáticos del siglo XVIII, bastantes de ellos ya habían hecho buen uso de los números complejos en problemas tanto físicos como abstractos[2].

3.2 Operaciones y propiedades.

A mediados del siglo XIX, el matemático irlandés William Rowan Hamilton presentó una formulación de la teoría de los números complejos en la cual un número complejo se define como un par de números reales expresados en determinado orden. Esto podría parecer, a primera vista, un poco artificial dado que lo que deseamos hacer es una extensión de los reales que siga cumpliendo con las operaciones algebraicas convencionales. Sin embargo, hemos de recordar que la definición formal de los números enteros está en términos de parejas de naturales, en las cuales el orden de estos es determinante para identificar el número del cual estamos hablando. De igual modo, los racionales se expresan en términos de parejas de enteros, donde una vez más el orden es importante. Así, la formulación propuesta por Hamilton nos lleva a la siguiente:

---

[1] Michael Spivak, *Cálculo infinitesimal*, 2001, pg. 719.
[2] A. David Wunsch, *Variable compleja con aplicaciones*, 1997, pgs. 6-7.

Definición 1. Un número complejo es la pareja *(x; y)* de números reales donde *x* es llamado componente real mientras que *y* se le llama componente imaginaria.

Se dirá que dos números complejos *(a; b), (c; d)* son iguales si y sólo si $a=c$ y $b=d$.

Al conjunto de números complejos lo denotaremos con la letra ***C***. De este modo,

$$\boldsymbol{C} := \{(x; y) : x, y \text{ son reales}\}$$

Definición 2. La suma de dos números complejos *(a; b), (c; d)* es el número complejo *(a+c; b+d)* obtenido sumando, respectivamente, las primeras y las segundas componentes de los dos números dados.

Definición 3. El producto de dos números complejos *(a; b), (c; d)* es el número complejo *(ac – bd; ad + bc)*.

Teorema 1. *Las operaciones de suma y multiplicación que acabamos de definir satisfacen las leyes conmutativa, asociativa y distributiva.*

Demostración. Solamente demostraremos la propiedad distributiva. Las otras demostraciones son más simples y se dejan como ejercicio para el lector. Si $u=(u_1; u_2)$, $v=(v_1; v_2)$ y $w=(w_1; w_2)$, entonces tenemos

$$\begin{aligned} u(v+w) &= (u_1; u_2)\,(v_1+w_1\,;\, v_2+w_2) \\ &= (u_1v_1 + u_1w_1 - u_2v_2 - u_2w_2;\, u_1v_2 + u_1w_2 + u_2v_1 + u_2w_1) \\ &= (u_1v_1 - u_2v_2;\, u_1v_2 + u_2v_1) + (u_1w_1 - u_2w_2;\, u_1w_2 + u_2w_1) \\ &= uv + uw. \end{aligned}$$

■

A partir de las operaciones anteriores es posible definir la resta y la división de números complejos. Así, restar *b* de *a* significa encontrar un número *x* tal que:

$$b + x = a$$

Tal número –diferencia de *a* y *b*– es único, y la misma definición se extiende a los números complejos:

Definición 4. Restar el número complejo *(c; d)* de *(a; b)* significa hallar el número complejo *(x; y)*, tal que:

$$(c;d) + (x;y) = (a;b)$$

puesto que por definición de adición de números complejos tenemos que:

$$(c;d) + (x;y) = (c + x;d + y)\,,$$

y las incógnitas *x*, *y* deben ser determinadas por las ecuaciones:

$$\begin{aligned} c + x &= a \\ d + y &= b \end{aligned}$$

que admiten la única solución $x = a - c;\ y = b - d$. Por lo tanto la diferencia de *(a; b)* y *(c; d)* es un número unívocamente determinado por:

$$(a;b) - (c;d) = (a - c; b - d)$$

A manera de observación, tenemos que en particular:

$$(a;b) - (a;b) = (0;0)$$

es decir, el número complejo *(0; 0)* representa el mismo papel que el *0* para los números reales.

Con el mismo artificio, salvo modificaciones se define la división de números complejos. Es decir, dividir *a* por un número *b*, significa hallar un número *x* tal que $bx=a$.

Definición 5. Dividir el número complejo *(a; b)* por *(c; d)*, con *(c; d)* distinto de *(0;0)*, significa hallar el número complejo *(x; y)* tal que:

$$(c;d)(x;y) = (a;b)$$

puesto que $(c;d)(x;y) = (cx - dy; cy + dx)$, las incógnitas *x, y* deberán hallarse resolviendo el sistema de ecuaciones:

$$cx - dy = a$$
$$dx + cy = b$$

obteniendo la solución única:

$$x = \frac{ac + bd}{c^2 + d^2};$$

$$y = \frac{bc - ad}{c^2 + d^2};$$

que como puede comprobarse por simple sustitución, satisface el sistema dado. En consecuencia la división *(c; d)* $\neq$ *(0; 0)* nos da el cociente:

$$\frac{(a;b)}{(c;d)} = \left(\frac{ac + bd}{c^2 + d^2}; \frac{bc - ad}{c^2 + d^2} \right).$$

Hasta este momento, los números complejos los hemos definido como parejas de números reales, las cuales, según las definiciones dadas anteriormente, las podemos sumar, restar, multiplicar y dividir. Observemos una característica importante. Cualquier número complejo (*a*; *b*), este lo podemos escribir de la siguiente manera:

$$(a;\ b) = (a;\ 0) + (0;\ b) = (a;\ 0) + (b;\ 0)(0;\ 1)$$

Por comodidad, a los números complejos expresados como pareja de reales, los representaremos con las letras *u*, *v*, *w*, *z*, mientras que, como caso único y especial, al complejo (*0*; *1*) le asignaremos la letra *i* y no se utilizará ninguna otra letra para este número.

Otra propiedad interesante, es que números complejos del tipo (*a*; *0*), es decir, que tienen segunda componente (parte imaginaria) nula, al realizar las operaciones fundamentales entre ellos, seguiremos obteniendo un complejo del mismo tipo, como se puede observar a continuación:

$$(a;0)+(b;0)=(a+b;0)$$

$$(a;0)-(b;0)=(a-b;0)$$

$$(a;0)\times(b;0)=(ab;0)$$

$$\frac{(a;0)}{(b;0)}=\left(\frac{a}{b};0\right)$$

La conclusión, a partir de las observaciones hechas anteriormente, es que si a los números complejos con segunda componente *0*, se les somete a las operaciones de adición, sustracción, multiplicación y división, cualesquiera que sea la cantidad de veces que se repita la operación, el complejo resultante tendrá también su segunda componente *0*, mientras que la primera componente resultará de realizar las operaciones indicadas con las primeras componentes de los complejos dados. Esto significa que los números complejos con segunda componente nula se comportan, sin temor a equivocarnos, como números reales. Así, a los complejos del tipo (*a*; 0) simplemente los escribiremos como *a*. De esta manera, el símbolo "*a*" tendrá dos significados: uno, como símbolo de un número real; y el otro, como símbolo de un número complejo (*a*;*0*).

Hemos conseguido así, una manera alternativa de escribir a un número complejo. Por ejemplo, si *z* representa a un número complejo dado (a; b), entonces *z* puede ser expresado como:

$$z = (a; b) = (a; 0) + (b; 0)(0; 1) = a+bi.$$

A esta forma alternativa de escribir al complejo *z* se le conoce como *forma binómica*[3].

Ya previamente establecido que el conjunto de los números complejos recogen las características establecidas, es importante también comentar que ésta estructura numérica cumple con lo que es una estructura de campo ya que se verifican a partir de las definiciones de las operaciones básicas de adición y multiplicación de números complejos los siguientes axiomas:

Axioma 1: El conjunto de los números complejos es cerrado bajo las operaciones de suma y multiplicación, es decir, si $v, w \in \mathbb{C}$, entonces: $v+w \in \mathbb{C}$ *y* $vw \in \mathbb{C}$.

[3] Notación que se le debe al matemático suizo Leonhard Euler (1707-1783).

Axioma 2: La suma y la multiplicación de números complejos es conmutativa, es decir, si $v, w \in \mathbb{C}$, entonces:

$$v + w = w + v$$
$$vw = wv$$

Axioma 3: La suma y la multiplicación de números complejos es asociativa, es decir, si $u, v, w \in \mathbb{C}$, entonces:

$$(u + v) + w = u + (v + w)$$
$$(uv)w = u(vw)$$

Axioma 4: Existe un número complejo, el *0*, tal que para todo $u \in \mathbb{C}$, tenemos que:

$$u + 0 = 0 + u = u$$
$$u0 = 0u = 0$$

Tenemos también que existe un número complejo, el *1*, tal que para todo $u \in \mathbb{C}$, tenemos que:

$$u1 = 1u = u$$

Axioma 5: Para cada $u \in \mathbb{C}$, existe en $\mathbb{C}$ su inverso aditivo denotado por $-u$, tal que:

$$u + (-u) = (-u) + u = 0$$

Tenemos también que, dado $u \neq 0$, existe en $\mathbb{C}$ su inverso multiplicativo denotado por u^{-1}, tal que:

$$u(u^{-1}) = (u^{-1})u = 1$$

Axioma 6: En $\mathbb{C}$, el producto distribuye a la suma, es decir, si $u, v, w \in \mathbb{C}$, entonces:

$$u(v + w) = uv + uw$$
$$(u + v)w = uw + vw$$

Hemos de observar finalmente que algunas de las propiedades que juegan un papel importante en los reales, desaparecen al extender el campo de $\mathbb{R}$ a $\mathbb{C}$, nos referimos explícitamente al orden[4]. Hasta el momento no se ha definido ninguna relación de la forma $u < v$, si u e v son números complejos cualesquiera. Como se verá en el siguiente teorema, es imposible definir una relación que satisfaga los axiomas de orden.

Teorema 2. *No es posible definir una relación de orden en el campo de los números complejos.*

Demostración. Supóngase que se puede definir una relación de orden $<$ que satisficiera los axiomas de orden 9, 10 y 11. Entonces como $i \neq 0$, se debiera tener que $i > 0$ o $i < 0$. Supongamos que $i > 0$. Entonces, por teorema 9 del capítulo 1, tendríamos que $i^2 > 0$, o $-1 > 0$. Sumando *1* a ambos miembros, obtendríamos que $0 > 1$. Por otro lado,

[4] Tom M. Apostol, *Análisis Matemático*, 1976, pg.. 23.

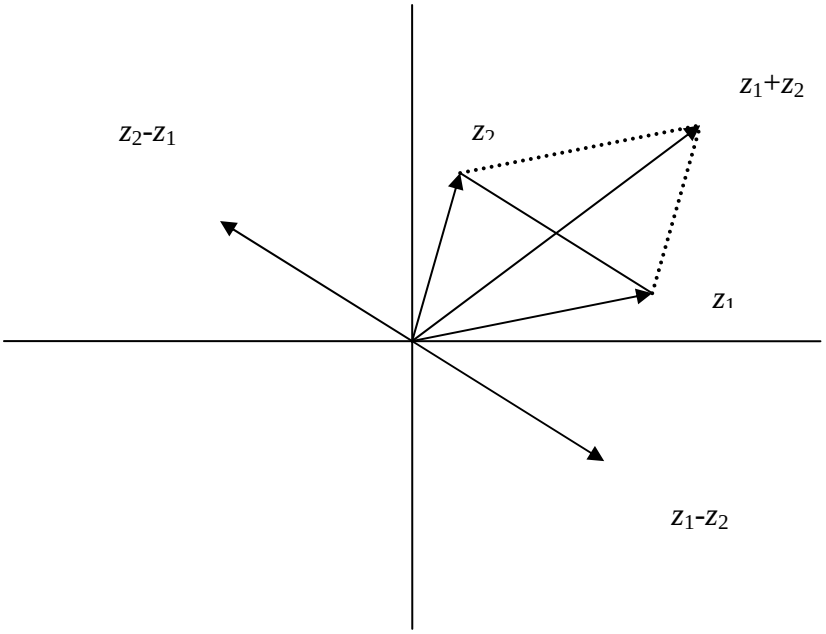
aplicando la definición 5 a *-1 > 0*, hallaríamos *1 > 0*. Tendríamos, pues, que *0 > 1* y también *1 > 0*, que por el axioma 9, es imposible. Así pues, suponer que *i > 0* lleva a una contradicción. Un razonamiento análogo prueba que no es posible que *i < 0*. Por lo tanto, los números complejos no pueden ser ordenados de tal suerte que verifiquen los axiomas 9, 10 y 11.

■

Ante esta situación, no existe una relación de orden que tenga las propiedades usuales con respecto a las operaciones de ℂ. Por ejemplo, usando números reales podemos decir que *2 > 1*, pero dentro de los números complejos no tiene sentido afirmar que *(1+ i) < (2 + 3i)* o que *(2 + 3i) < (1 + i)*. Una desigualdad de la forma $a < b$ siempre implicará que tanto *a* como *b* son números reales. Así los términos positivo y negativo no aplican a los números complejos y el empleo de estas palabras implica que se está hablando de un número real.

Interpretación geométrica de los números complejos.

Puesto que un número complejo $(x; y)$ es un par ordenado de números reales, este puede representarse geométricamente mediante un punto del plano, o por un vector que una al origen (0; 0) con el punto $(x; y)$. Las operaciones de adición y sustracción de números complejos que se acaban de definir tienen una sencilla interpretación geométrica. Si dos números complejos z_1 y z_2 se representan mediante flechas que unen el origen con z_1 y z_2, respectivamente, entonces la suma z_1+z_2 está determinada por la *ley del paralelogramo*. La flecha que une el origen con el punto z_1+z_2 es una diagonal del paralelogramo determinado por *0*, z_1 y z_2, como se ve en la siguiente figura.



La otra diagonal está relacionada con la diferencia de z_1 y z_2. La flecha de z_1 a z_2 es paralela y de igual longitud que la que une *0* con z_2-z_1; la flecha en el sentido opuesto, de z_2 a z_1, se relaciona del mismo modo con z_1-z_2.

Para el caso de la multiplicación y división de números complejos, cabe señalar que cuando multiplicamos *u* por *v* para obtener el producto *uv* la operación que se lleva a cabo con los vectores correspondientes no es una multiplicación escalar (producto punto) ni una multiplicación vectorial (producto cruz), operaciones que quizás son ya conocidas. De manera similar, podemos dividir dos números complejos y también en cierto sentido, sus vectores. Esta operación tampoco tiene equivalente en las operaciones vectoriales que posiblemente ya se conozcan.

3.3 El conjugado y el módulo un número complejo: operaciones y propiedades.

La expresión del número complejo $z = x + iy$ como pareja $z = (x; y)$ quizá nos sugiera la notación para las coordenadas de un punto en el plano *xy*. La expresión $|z| = \sqrt{x^2 + y^2}$ nos indica a su vez la expresión de la distancia pitagórica de dicho punto al origen.

No debe sorprendernos que el plano *xy* (o plano cartesiano) se use a menudo para representar números complejos. Cuando se usa para este propósito se le conoce como plano de Argand, plano *z* o plano complejo[5]. En estas circunstancias, el eje *x*, o eje horizontal, se llama eje de los números reales, mientras que el eje *y*, o eje vertical, se conoce como eje de los números imaginarios.

Otra representación posible de *z* en este plano es en forma de vector. Mostramos $z = x + iy$ como una línea dirigida que comienza en el origen y termina en el punto (*x*, *y*). Así, podemos representar un número complejo como un punto o como un vector en el plano *xy*. Se usarán ambos métodos y a menudo nos referiremos al punto o vector como si se tratase del propio número complejo y no sólo de su representación.

Definición 6. Sea *z* un número complejo escrito en la forma $z = x + iy$, o bien, $z = (x; y)$. Se define el conjugado del número complejo *z*, que se denota por $\bar{z}$, como el número complejo $\bar{z} = x - iy$, es decir el conjugado de *z* sólo difiere en el signo de la componente imaginaria.

Algunas propiedades importantes de los números complejos y los conjugados de los números complejos se enuncian a continuación:

- $z + \bar{z} = (x + iy) + (x - iy) = 2x + (y - y)i = 2x$, es decir, la suma de un número complejo y su conjugado es igual a dos veces la parte real del número complejo, la cual denotaremos por $2\,\mathrm{Re}(z)$.

- $z - \bar{z} = (x + iy) - (x - iy) = (x - x) + (y + y)i = 2yi$, es decir, la resta de un número complejo y su conjugado es igual a dos veces la componente imaginaria del número complejo, la cual denotaremos por $2\,\mathrm{Im}\,g(z)$.

[5] Tom M. Apostol, *Calculus*, 1999, pg. 443.

- $z\bar{z} = (x+iy)(x-iy) = x^2 + y^2$, y a ésta operación se le conoce comúnmente como ***<u>la norma de z</u>***.

- $\bar{\bar{z}} = z$.

- $\overline{(z_1 + z_2)} = \bar{z}_1 + \bar{z}_2$.

- $\overline{(z_1 z_2)} = (\bar{z}_1)(\bar{z}_2)$.

- A partir de las conclusiones anteriores se deduce que la diferencia o el cociente de dos números complejos conjugados es igual, respectivamente, a la diferencia o al cociente de sus conjugados, lo cual se expresa de la siguiente manera:

$$\overline{(z_1 - z_2)} = \bar{z}_1 - \bar{z}_2, \quad \overline{\left(\frac{z_1}{z_2}\right)} = \frac{\bar{z}_1}{\bar{z}_2}.$$

Una observación importante es que los números reales coinciden con sus conjugados y recíprocamente, un número que es igual a su conjugado es un número real. En efecto, si $x + iy = x - iy$, se requiere que *y = -y*, o bien, *y = 0.*

Estas propiedades pueden en ocasiones ahorrarnos trabajo. Consideremos por ejemplo:

$$\frac{1+i}{3-4i} + \frac{1-i}{3+4i} = x + iy$$

Encontrar los números *x, y* puede resultar bastante tedioso. No obstante, observemos que con la ayuda de la ecuación $\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\bar{z}_1}{\bar{z}_2}$, la segunda fracción es el complejo conjugado de la primera. Así, de la deducción de la suma de un número complejo y su conjugado, vemos que *y = 0*, mientras que *x = 2Re((1 + i)/(3 – 4i))* donde la parte real de *(1 + i)/(3 – 4i)* es *(3 – 4)/25 = -1/25*. La respuesta es por tanto *x = -2/25* e *y = 0.*

<u>*Definición 7.*</u> A la raíz cuadrada positiva de la norma de *z* se le llama ***valor absoluto de z o módulo de z***, y se denota por $|z|$ o bien por *mód(z)*. Entonces:

$$mód(x+iy) = mód(z) = |z| = +\sqrt{z\bar{z}} = +\sqrt{x^2 + y^2}.$$

A manera de observación, el módulo de un número complejo es igual al de su conjugado porque:

$$|\bar{z}| = \sqrt{x^2 + (-y)^2} = \sqrt{x^2 + y^2} = |z|$$

El producto de un número complejo por su conjugado es el cuadrado del módulo del número complejo. Obsérvese que $z\bar{z} = x^2 + y^2$. Así pues, $z\bar{z} = |z|^2$.

Teorema 3. *El módulo de un producto es igual al producto de los módulos de sus factores, es decir,*

$$|z_1 z_2 z_3 \cdots z_n| = |z_1||z_2||z_3| \cdots |z_n|$$

Demostración. Consideremos primero el producto dos factores $z' = z_1 z_2$. Tenemos entonces que la norma de z' es:

$$z'\bar{z'} = (z_1 z_2)\overline{(z_1 z_2)} = (z_1 z_2)(\bar{z_1}\bar{z_2}) = (z_1\bar{z_1})(z_2\bar{z_2})$$

entonces $\sqrt{z'\bar{z'}} = \sqrt{z_1\bar{z_1}}\sqrt{z_2\bar{z_2}}$, por tanto $|z'| = |z_1||z_2|$. Consideremos ahora el producto $z'' = z_1 z_2 z_3$, y sea $z' = z_1 z_2$, entonces por lo demostrado anteriormente:

$$|z''| = |z'||z_3| = |z_1||z_2||z_3|$$

y así podemos extender este resultado para el producto de *n* factores.

■

Teorema 4. $|z_1 + z_2 + \cdots + z_n| \le |z_1| + |z_2| + \cdots + |z_n|$ *y la igualdad sólo será válida cuando todos los números* $z_1, z_2, \ldots, z_n$ *sean iguales a cero, o bien, en el caso de que uno de ellos, por ejemplo* $z_1 \neq 0$*, y todos los cocientes* $\frac{z_2}{z_1}, \frac{z_3}{z_1}, \ldots, \frac{z_n}{z_1}$ *sean números reales no negativos.*

Demostración: Obsérvese primero que si $z_1 = a_1 + ib_1$, entonces $a_1 = Re\,(z_1) \le |z_1|$ y la igualdad se da cuando $b_1 = 0$ *y* $a_1 \ge 0$, ya que si $|z_1| = \sqrt{a_1^2 + b_1^2}$, es claro que $a_1 < \sqrt{a_1^2 + b_1^2}$ si $b_1 \neq 0$. Por otra parte si $b_1 = 0$ *y* $a_1 < 0$ entonces $|z_1| = \sqrt{a_1^2} = -a_1$ por tanto $a_1 < -a_1$. Finalmente si $b_1 = 0$ y $a_1 \ge 0$, entonces $|z_1| = \sqrt{a_1^2} = a_1$.

Consideremos ahora la suma de z_1 *y* z_2, por definición de módulo tenemos que:

$$|z_1 + z_2|^2 = (z_1 + z_2)\overline{(z_1 + z_2)} = (z_1 + z_2)(\bar{z_1} + \bar{z_2}) = z_1\bar{z_1} + z_2\bar{z_2} + z_1\bar{z_2} + z_2\bar{z_1} = |z_1|^2 + |z_2|^2 + 2\mathrm{Re}(z_1\bar{z_2})$$

ya que $\bar{z_1}z_2 = \overline{z_1\bar{z_2}}$ y $\overline{z_1\bar{z_2}} + z_1\bar{z_2} = 2\,\mathrm{Re}(z_1\bar{z_2})$, por lo tanto: $\mathrm{Re}(z_1\bar{z_2}) \le |z_1\bar{z_2}| = |z_1||\bar{z_2}| = |z_1||z_2|$ en consecuencia $|z_1 + z_2|^2 \le |z_1|^2 + |z_2|^2 + 2|z_1||z_2| = (|z_1| + |z_2|)^2$ y como el módulo es un número real positivo entonces $|z_1 + z_2| \le |z_1| + |z_2|$ y la igualdad sólo será válida si $\mathrm{Re}(z_1\bar{z_2}) = |z_1\bar{z_2}|$ y por la observación hecha al principio de la

demostración de éste teorema, esto ocurre cuando $z_1\overline{z_2}$ es un número real positivo, es decir, cuando $a_1a_2 + b_1b_2 \geq 0$ y $a_1b_2 - b_1a_2 = 0$. Suponiendo que $z_1 \neq 0$ y $z_1\overline{z_1}$ es un número real positivo, entonces $\frac{\overline{z_1}z_2}{z_1\overline{z_1}} = \frac{z_2}{z_1}$ es un número real positivo.

Recíprocamente si ésta ecuación es verdadera, entonces $\overline{z_1}z_2 = \left(\frac{z_2}{z_1}\right)\left(z_1\overline{z_1}\right)$ será un número real y positivo.

Consideremos ahora la suma de tres términos $z_1 + z_2 + z_3 = (z_1 + z_2) + z_3$. De acuerdo con lo probado anteriormente $|(z_1 + z_2) + z_3| \leq |z_1 + z_2| + |z_3|$ y $|z_1+z_2| \leq |z_1|+|z_2|$ por lo tanto $|z_1 + z_2 + z_3| \leq |z_1| + |z_2| + |z_3|$ y la igualdad sólo será válida si se da simultáneamente que $|z_1+z_2| = |z_1|+|z_2|$ y $|(z_1 + z_2) + z_3| = |z_1 + z_2| + |z_3|$. Veamos en que casos se da ésta situación. Sea $z_1 \neq 0$ la primera igualdad será valida si la razón $\frac{z_2}{z_1}$ es real y positiva. En tal caso, el número $z_1 + z_2 = z_1\left(1 + \frac{z_2}{z_1}\right)$ no es cero y $1 + \frac{z_2}{z_1}$ es un número real positivo. La segunda igualdad exige que $\frac{z_3}{z_1 + z_2} = \frac{z_3}{z_1}\left(1 + \frac{z_2}{z_1}\right)^{-1}$ sea real y positivo, pero $\left(1 + \frac{z_2}{z_1}\right)^{-1}$ es real positivo y $\frac{z_3}{z_1 + z_2}$ es real y positivo, y por lo tanto $\frac{z_3}{z_1}$ es real y positivo.

Razonando de la misma manera, se demuestra el teorema para la suma de más de tres términos.

■

3.4 Existencia de la raíz cuadrada de un número complejo.

Hallar la raíz cuadrada de un número complejo *z* equivale a hallar la solución *v* de una ecuación de segundo grado:

$$v^2 = z$$

Sea $v = a + bi$ y $z = x + yi$, entonces los números reales *a, b* deben ser tales que $(a + bi)^2 = x + yi$, pero $(a + bi)^2 = a^2 - b^2 + 2abi$, en consecuencia, *a* y *b* deben satisfacer el sistema:

$$a^2 - b^2 = x$$
$$2ab = y$$

Ahora, $\left(a^2+b^2\right)^2=\left(a^2-b^2\right)^2+4a^2b^2$ y de ésta última identidad tenemos que $x^2=\left(a^2-b^2\right)^2$ y $y^2=4a^2b^2 \Rightarrow x^2+y^2=\left(a^2-b^2\right)^2+4a^2b^2=\left(a^2+b^2\right)^2$ entonces $\left(a^2+b^2\right)=\sqrt{x^2+y^2}$ tomando la raíz positiva. Despejando a^2 del sistema de ecuaciones, tenemos que $a^2=x+b^2$ y $\left(a^2+b^2\right)=\sqrt{x^2+y^2}$, combinando ambas ecuaciones que $b^2=\dfrac{\sqrt{x^2+y^2}-x}{2}$ y por tanto $a^2=\dfrac{\sqrt{x^2+y^2}+x}{2}$. No obstante es necesario aclarar unas cuestiones. Estas ecuaciones son consecuencias necesarias del sistema de ecuaciones formulado al principio del problema, pero puede suceder que existan soluciones que no lo satisfagan. Para separar las soluciones de $a^2=\dfrac{\sqrt{x^2+y^2}+x}{2}$ que cumplan con el sistema de ecuaciones, debe tomarse en cuenta que $2ab=y$, y en caso de que $y \neq 0$, la ecuación determina el signo de *b* correspondiente a un signo dado de *a*, es decir, *a* y *b* deben tener el mismo signo cuando $y > 0$, y signo contrario cuando $y < 0$.

De acuerdo con esto, las soluciones de la ecuación $v^2=x+yi$ son:

$$v=\pm\left(\sqrt{\frac{\sqrt{x^2+y^2}+x}{2}}+i\sqrt{\frac{\sqrt{x^2+y^2}-x}{2}}\right) \text{ cuando } y > 0$$

$$y\ v=\pm\left(\sqrt{\frac{\sqrt{x^2+y^2}+x}{2}}-i\sqrt{\frac{\sqrt{x^2+y^2}-x}{2}}\right) \text{cuando } y < 0.$$

Ahora bien, cuando $y = 0$, entonces $\sqrt{x^2}=x$ ó $\sqrt{x^2}=-x$ cuando $x > 0$ ó $x < 0$ respectivamente. De aquí se concluye que $a=\pm\sqrt{x}$ y $b = 0$. Si $x > 0$, entonces la ecuación $v^2=x$ tiene dos raíces reales $v=\pm\sqrt{x}$. Por otra parte, si $x < 0$, entonces $a = 0$ y $b=\pm\sqrt{-x}$ y en éste caso la ecuación $v^2=x$ tiene dos raíces imaginarias puras $v=\pm i\sqrt{-x}$.

Finalmente cuando $x = y = 0$, sólo existe la solución trivial $v = 0$.

Ejemplo 1: Resolver la ecuación:

$$X^2=-i$$

Solución: En éste caso, $a = 0; b = -1;$ $\sqrt{a^2+b^2}=1, b<0$, por lo tanto:

$$X=\pm\left(\sqrt{\frac{1}{2}}-i\sqrt{\frac{1}{2}}\right)=\pm\frac{1-i}{\sqrt{2}}$$

Ejemplo 2: Resolver la ecuación:

$$X^2 = -5 + 12i$$

Solución: En este caso *a = -5, b = 12;* $\sqrt{a^2 + b^2} = \sqrt{169} = 13$, $\frac{\sqrt{169} - 5}{2} = 4$;

$\frac{\sqrt{169} + 5}{2} = 9$; *y b>0,* por lo tanto, $X = \pm(2 + 3i)$.

3.5 Ecuaciones de segundo grado con coeficientes complejos.

En el apartado anterior se demostró que todo número complejo tiene raíz cuadrada y a partir de éste resultado podemos calcular las soluciones de ecuaciones de segundo grado con coeficientes complejos. Es decir, la ecuación general de segundo grado $az^2 + bz + c = 0$ con coeficientes *a, b, c* números complejos arbitrarios, puede resolverse por medio de la fórmula general:

$$z = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

la cual se obtiene a partir de las operaciones elementales y de la existencia de la raíz cuadrada.

Ejemplo 3: Resolver la ecuación de segundo grado:

$$iX^2 - (2 + 2i)X + 2 - i = 0$$

Solución: Aplicando la fórmula general tenemos

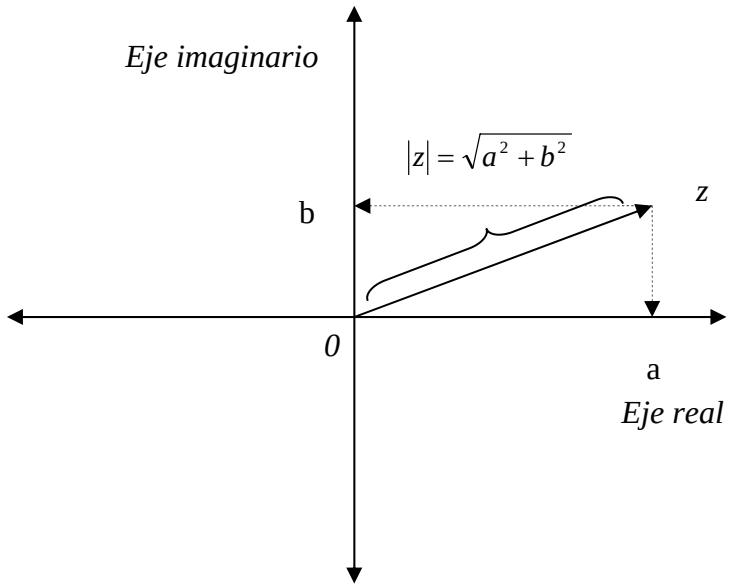
$$X = \frac{2 + 2i \pm \sqrt{-4}}{2i}$$

y tomando $\sqrt{-4} = 2i;$ se hallan las raíces *–i; 2–i.*

3.6 Representación polar de los números complejos.

En la sección 3 se expuso entre otras cosas, que los números complejos se representan gráficamente en el plano de Argand o el plano complejo. Los números complejos de la forma *a+0i* (números reales) están representados por puntos en el eje real. Los números complejos de la forma *0+bi* (números complejos puros) están representados por puntos en el eje imaginario. El punto *0,* junto con *z,* determina un segmento o vector dirigido

$\vec{0z}$, que va del origen *0* al extremo *z*. Las proyecciones del vector que representa a $z = a + bi$ sobre los ejes real e imaginario, son respectivamente, *a y b*, y la longitud del vector $\vec{0z}$ o la distancia de *0 a z* nos da un significado intuitivo del módulo de *z*, $|z| = \sqrt{a^2 + b^2}$.



Por otro lado consideremos dos semirrectas dirigidas l, l' que se cortan en un punto *S*. Entendemos por ángulo entre l, l' - medido de l a l' - y que indicaremos como (l, l'), al ángulo que debe girar l alrededor de *S* para coincidir con l' en posición y dirección, considerándose éste ángulo como positivo o negativo según l rote en el sentido opuesto al que giran las manecillas del reloj o en el mismo sentido que estas giran respectivamente. Desde éste punto de vista, el ángulo (l, l') no está unívocamente determinado sino por el contrario, tiene infinitos valores, cuya vinculación puede establecerse de la siguiente manera: Sea φ el menor ángulo positivo que debe girar l para coincidir con l' en posición y dirección. Si se continúa con la rotación en sentido positivo, volverá a coincidir cuando el ángulo rotado sea φ + 2π (midiendo los ángulos en radianes), nuevamente coincidirá cuando el ángulo sea φ + 4π, y en general, cuando el ángulo sea φ + 2*k*π, siendo *k* un número entero positivo. Así mismo, haciendo rotar l en sentido negativo se obtiene un ángulo cuyo valor absoluto es 2π - φ, las rectas l, l' coinciden en posición y dirección, y lo mismo sucederá después de *k* rotaciones en sentido negativo, es decir, tendremos una magnitud 2*k*π - φ, siendo *k* un número entero positivo. Tomando todos éstos ángulos negativamente, podemos afirmar que l' forma con l los ángulos negativos: φ - 2π, φ - 4π, φ - 6π,…, φ - 2*k*π. Por tanto, la expresión general para el ángulo (l, l') es: φ + 2*k*π, con *k = 0; ±1; ±2;*… un entero arbitrario y φ el menor ángulo positivo entre l y l'.

Los ángulos que difieren en múltiplos de 2π se dicen congruentes en módulo 2π[6]. En éste sentido, tenemos la siguiente congruencia:

[6] James Victor Uspensky, *Teoría de ecuaciones*, 2004, pg. 22.

$$(ll') \equiv -(l'l) (\mathrm{mod}\, 2\pi)$$

Volviendo a la representación geométrica de los números complejos, sea θ el ángulo comprendido entre el eje real y el vector $\vec{0z}$. Este ángulo se le llama argumento a amplitud de *z*. Está definido para $z \neq 0$ y tiene infinitos valores que difieren entre sí en múltiplos de 2π. Si $z = a + bi$, *a* es la proyección de $\vec{0z}$ sobre el eje real. Llamando como *r* al *mód (z)*, entonces $r = \sqrt{a^2 + b^2}$ y de la definición de *cos* θ se desprende que:

$$a = r(\cos\theta)$$

Dado que el ángulo que forman los ejes real e imaginario es $\frac{\pi}{2}$, el ángulo entre $\vec{0z}$ y el eje imaginario será $\frac{\pi}{2} - \theta$ y la proyección de $\vec{0z}$ sobre éste será:

$$b = r\cos\left(\frac{\pi}{2} - \theta\right) = rsen\theta$$

En consecuencia, $z = a + bi$ puede escribirse en la forma $z = r(\cos\theta + isen\theta)$ que es la llamada *forma trigonométrica o polar* de los números complejos.

En general no importa el valor que tome el ángulo θ, no obstante es recomendable elegir el menor valor numérico del argumento. Se tienen entonces que para representar un número complejo *z* en *forma polar* se deben hallar primero el *mód(z)* y luego hallar el ángulo θ de menor valor numérico, tal que:

$$\cos\theta = \frac{a}{r};\ sen\theta = \frac{b}{r};$$

Sin embargo resulta más conveniente en algunas ocasiones determinar el ángulo θ por medio de la tangente y para tal efecto se observan los siguientes casos:

1) Caso en que $a > 0, b > 0$. Se calcula la $\tan\theta' = \frac{b}{a} \Rightarrow \theta' = \tan^{-1}\frac{b}{a}$ y tomamos como $\theta = \theta'$.
2) Caso en que $a > 0, b < 0$. Se calcula la $-\frac{b}{a} > 0$ y $\tan\theta' = -\frac{b}{a} \Rightarrow \theta' = \tan^{-1}\left(-\frac{b}{a}\right)$ y tomamos como $\theta = 2\pi - \theta'$.
3) Caso en que $a < 0, b > 0$. Se calcula la $-\frac{b}{a} > 0$ y $\tan\theta' = -\frac{b}{a} \Rightarrow \theta' = \tan^{-1}\left(-\frac{b}{a}\right)$ y tomamos como $\theta = \pi - \theta'$.

4) Caso en que $a < 0, b < 0$. Se calcula la $\tan\theta' = \frac{b}{a} \Rightarrow \theta' = \tan^{-1}\frac{b}{a}$ y tomamos como $\theta = \pi + \theta'$.

Así, después de haber analizado los casos anteriores, dependiendo del caso en el que se encuentre el número complejo *z*, se tomará el ángulo θ para simplificar los cálculos correspondientes. Supóngase que *s* sea el ángulo medido en radianes, entonces α será el ángulo medido en grados tal que:

$$\alpha = \frac{180s}{\pi} \text{ o bien } s = \frac{\alpha\pi}{180}.$$

Ejemplo 4: Expresar en forma polar el número complejo $z = 1 + i$.

Solución: Aquí $r = |z| = \sqrt{1^2 + 1^2} = \sqrt{2}$, $a = 1$, $b = 1$, y por lo tanto nos encontramos en el caso 1. Entonces $\tan\theta' = \frac{1}{1} \Rightarrow \theta' = \tan^{-1}\frac{1}{1} = \frac{\pi}{4}$ y $\theta = \frac{\pi}{4}$. Así,

$$z = 1 + i = \sqrt{2}\left(\cos\frac{\pi}{4} + isen\frac{\pi}{4}\right).$$

Ejemplo 5: Expresar en forma polar el número complejo $z = 1 - i$.

Solución: Aquí $r = |z| = \sqrt{1^2 + (-1)^2} = \sqrt{2}$, $a = 1$, $b = -1$, y por lo tanto nos encontramos en el caso 2. Entonces $-\left(\frac{-1}{1}\right) > 0$ y $\tan\theta' = -\left(\frac{-1}{1}\right) \Rightarrow \theta' = \tan^{-1}\left(-\frac{-1}{1}\right) = \frac{\pi}{4}$ y tomamos como $\theta = 2\pi - \frac{\pi}{4} = \frac{7\pi}{4}$. Así,

$$z = 1 - i = \sqrt{2}\left(\cos\frac{7\pi}{4} + isen\frac{7\pi}{4}\right)$$

Cabe observar que $1-i$ es el complejo conjugado de $1+i$, y si hubiéramos tomado el ángulo en sentido negativo tendríamos como resultado $z = 1 - i = \sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right) + isen\left(-\frac{\pi}{4}\right)\right) = \sqrt{2}\left(\cos\frac{\pi}{4} - isen\frac{\pi}{4}\right)$ por las propiedades de las funciones coseno y seno, y $z = 1 - i = \sqrt{2}\left(\cos\frac{7\pi}{4} + isen\frac{7\pi}{4}\right) = \sqrt{2}\left(\cos\frac{\pi}{4} - isen\frac{\pi}{4}\right)$.

Por lo tanto el conjugado de un número complejo escrito en forma polar $z = r(\cos\theta + isen\theta)$ es $z = r(\cos\theta - isen\theta) = r(\cos(-\theta) + isen(-\theta))$.

Multiplicación y división de números complejos representados en forma polar.

Sean $u = r(\cos\theta + isen\theta)$ y $v = r'(\cos\theta' + isen\theta')$ dos números complejos expresados en forma polar. Multiplicando y agrupando factores del segundo miembro de la identidad tenemos que:

$$uv = rr'(\cos\theta + isen\theta)(\cos\theta' + isen\theta')$$

Pero $(\cos\theta + isen\theta)(\cos\theta' + isen\theta') = \cos\theta\cos\theta' - sen\theta sen\theta' + i(sen\theta\cos\theta' + sen\theta'\cos\theta)$ y por otra parte:

$$\cos\ \theta\cos\ \theta' - sen\ \theta sen\ \theta' = \cos(\ \theta' + \theta)$$

$$sen\ \theta\cos\ \theta' + \cos\ \theta sen\ \theta' = sen\ (\theta' + \theta)$$

Por lo tanto: $uv = rr'(\cos(\theta' + \theta) + isen(\theta' + \theta))$. *Esto significa que el módulo del producto es el producto de los módulos de los factores y el argumento es la suma de los argumentos.* Por sucesivas aplicaciones de este resultado, ésta regla se extiende a cualquier número de factores. El producto de *n factores*:

$$r_1(\cos\theta_1 + isen\theta_1); r_2(\cos\theta_2 + isen\theta_2); ...; r_n(\cos\theta_n + isen\theta_n)$$

es:

$$(r_1 r_2 \cdots r_n)(\cos\theta_1 + isen\theta_1)(\cos\theta_2 + isen\theta_2)\cdots(\cos\theta_n + isen\theta_n) =$$
$$= (r_1 r_2 \cdots r_n)[\cos(\theta_1 + \cdots + \theta_n) + isen(\theta_1 + \cdots + \theta_n)]$$

En particular, cuando $r_1 = r_2 = \cdots = r_n = r$ y $\theta_1 = \theta_2 = \cdots = \theta_n = \theta$, esta fórmula nos da una importante identidad:

$$[r(\cos\theta + isen\theta)]^n = r^n[\cos(n\theta) + isen(n\theta)]$$

que es conocida como la fórmula de ***De Moivre***[7]. Por supuesto, aquí *n* es un número entero positivo. Sin embargo, como se verá a continuación, es posible hacer la generalización de la fórmula de De Moivre para *n* un número entero negativo.

Obsérvese que:

$$(\cos\theta + isen\theta)^{-1} = \frac{1}{\cos\theta + isen\theta} = \frac{\cos\theta - isen\theta}{\cos^2\theta + sen^2\theta} = \cos\theta - isen\theta = \cos(-\theta) + isen(-\theta)$$

y elevando ambos miembros de la ecuación a la potencia *n*, se obtiene:

$$(\cos\theta + isen\theta)^{-n} = \cos(-n\theta) + isen(-n\theta)$$

[7] Felipe Zaldívar. *Fundamentos de álgebra*. Universidad Autónoma de México, Fondo de Cultura Económica. 2005.

de donde se concluye que la fórmula de De Moivre es también válida para enteros negativos.

Por otro lado, para calcular el cociente de números complejos cuando están escritos en forma polar, se tiene que: Sean $u = r(\cos\theta + isen\theta)$ y $v = r'(\cos\theta' + isen\theta')$ dos números complejos dados en forma polar, entonces el cociente se calcula de la siguiente manera:

$$\frac{u}{v} = \frac{r(\cos\theta + isen\theta)}{r'(\cos\theta' + isen\theta')} = \frac{r}{r'}(\cos\theta + isen\theta)(\cos\theta' + isen\theta')^{-1}$$

pero $(\cos\theta' + isen\theta')^{-1} = \cos(-\theta') + isen(-\theta')$, y de acuerdo con la fórmula de la multiplicación se concluye que:

$$\frac{u}{v} = \frac{r}{r'}(\cos(\theta - \theta') + isen(\theta - \theta'))$$

de aquí se concluye que el módulo del cociente de dos números complejos expresados en forma polar es igual al cociente de los módulos y el argumento es igual a la diferencia de argumentos del dividendo y del divisor.

A partir de la fórmula de De Moivre, se pueden derivar algunas identidades trigonométricas bien conocidas. Por ejemplo tomando *n=2*, $(\cos\theta + isen\theta)^2 = \cos 2\theta + isen2\theta$. Desarrollando el lado izquierdo de la expresión anterior llegamos a $\cos^2\theta + 2i\cos\theta sen\theta - sen^2\theta = \cos 2\theta + isen2\theta$. Igualando las partes correspondientes (real e imaginaria), obtenemos las dos identidades $\cos^2\theta - sen^2\theta = \cos 2\theta$ y $2sen\theta\cos\theta = sen2\theta$.

3.7 Cálculo de raíces de números complejos (potencias fraccionarias).

Por medio de la fórmula de De Moivre es posible representar todas las raíces de la ecuación:

$$v^n = z$$

Donde $z \neq 0$ es un número complejo expresado en forma polar. Sea $z = r(\cos\theta + isen\theta)$ y sea $v = R(\cos\varphi + isen\varphi)$, se tiene entonces que:

$$v^n = R^n(\cos n\varphi + isenn\varphi) = r(\cos\theta + isen\theta) = z$$

Puesto que números complejos iguales deben tener módulos iguales, se concluye que:

$R^n = r$ y por lo tanto $R = \sqrt[n]{r}$ tomando la raíz positiva.

Por otro lado, los argumentos de números complejos iguales difieren solamente en múltiplos de 2π, de modo que:

$$n\varphi = \theta + 2\pi k$$

Siendo *k* un número entero arbitrario. Por lo tanto se concluye que:

$$v = \sqrt[n]{r}\left(\cos\left(\frac{\theta + 2\pi k}{n}\right) + isen\left(\frac{\theta + 2\pi k}{n}\right)\right)$$

proporciona las *n* raíces que resuelven la ecuación $v^n = z$.

Para ésta ecuación, *k* es un entero cualquiera y el número de raíces distintas será sólo de *n*. Para obtener todas estas raíces solo hay que hacer *k = 0; 1; 2;…; n-1*. Para probar ésta afirmación obsérvese lo siguiente. Si *k* es un número entero cualquiera, dividiéndolo por *n* se sabe por el algoritmo de la división de números enteros que:

$$k = nq + l \text{, con } 0 \le l < n \text{, es decir, } l \in \{0,1,\ldots,n-1\}$$

de modo que: $\frac{\theta + (2\pi)k}{n} = \frac{\theta + 2\pi(nq) + (2\pi)l}{n} = \frac{\theta + (2\pi)l}{n} + (2\pi)q$, y por lo tanto:

$$\cos\left(\frac{\theta + (2\pi)k}{n}\right) = \cos\left(\frac{\theta + (2\pi)l}{n} + (2\pi)q\right) = \cos\left(\frac{\theta + (2\pi)l}{n}\right)$$

$$\text{y } sen\left(\frac{\theta + (2\pi)k}{n}\right) = sen\left(\frac{\theta + (2\pi)l}{n} + (2\pi)q\right) = sen\left(\frac{\theta + (2\pi)l}{n}\right)$$

lo que prueba que *k = 0; 1;…; n-1*. Para demostrar que las *n* raíces obtenidas son distintas entre sí, supóngase que k' y k'' son enteros distintos pero que generan las mismas raíces, en ese caso tendremos que:

$$\cos\left(\frac{\theta + (2\pi)k'}{n}\right) = \cos\left(\frac{\theta + (2\pi)k''}{n}\right) \text{ y } sen\left(\frac{\theta + (2\pi)k'}{n}\right) = sen\left(\frac{\theta + (2\pi)k''}{n}\right)$$

Esto sólo será posible si: $\frac{\theta + (2\pi)k''}{n} = \frac{\theta + (2\pi)k'}{n} + (2\pi)q$ siendo *q* un número entero, por lo tanto $k'' = k' + nq \Rightarrow k'' - k' = nq$, es decir que *n* divide a $k'' - k'$, pero $k'' - k' < n$, entonces la única manera de que *n* divida a $k'' - k'$ es que $k'' - k' = 0$, es decir, $k'' = k'$.

La interpretación geométrica de esta ecuación es importante porque puede permitirnos representar fácilmente los puntos del plano complejo que representan las raíces de algún número. Todas las raíces tienen el mismo módulo $\sqrt[n]{r}$. Por lo tanto, pueden representarse sobre un círculo de radio $\sqrt[n]{r}$. Todos los valores que se obtienen por

medio de esta ecuación tienen argumentos distintos. Al aumentar *el valor de k* como se indica en la ecuación, los argumentos aumentan de $\frac{\theta}{n}$ a $\frac{\theta}{n}+\frac{2\pi(n-1)}{n}$ por incrementos de $\frac{2\pi}{n}$. Así, los puntos que representan los diversos valores de $z^{1/n}$, que aparecen sobre el círculo de radio $\sqrt[n]{r}$, están uniformemente distribuidos con una separación angular de $\frac{2\pi}{n}$ [8]. Uno de los puntos (*k = 0)* forma un ángulo de $\frac{\theta}{n}$ con la parte positiva del eje real. Por lo tanto, contamos con suficiente información para representar gráficamente todos los puntos o vectores correspondientes.

Una vez observado lo anterior, podemos dar una definición de *z* elevado a cualquier potencia racional (por ejemplo $(z)^{3/4}$, $(z)^{7/6}$) y, en consecuencia, resolver ecuaciones como $(z)^{3/4}+1=0$. Tal definición es

$$(z)^{n/m}=\left(z^{1/m}\right)^n$$

y combinando los resultados anteriores y el Teorema de Moivre, tenemos que

$$(z)^{n/m}=\left(\sqrt[m]{r}\right)^n\left[\cos\left(\frac{n}{m}\theta+\frac{(2\pi)kn}{m}\right)+isen\left(\frac{n}{m}\theta+\frac{(2\pi)kn}{m}\right)\right],\ k = 0;\ 1;\ 2;\ldots;\ m\text{-}1.$$

Si *n/m* es una fracción irreducible, entonces los valores de *k* de *0* a *m-1* en la ecuación anterior dan como resultado *m* raíces numéricamente distintas. En el plano complejo, dichas raíces se distribuyen uniformemente sobre un círculo de radio $\left(\sqrt[m]{r}\right)^n$. Pero si *n/m* es reducible (es decir, si *n* y *m* tienen factores comunes) entonces, cuando *k* varia de *0* a *m-1*, algunos valores obtenidos tendrán valores numéricamente idénticos. Esto se debe a que la expresión 2π*kn/m* tomará al menos dos valores que difieren en un múltiplo entero de 2π. En el caso extremo de que *n* es divisible entre *m*, todos los valores obtenidos son idénticos. Esto confirma el hecho bien conocido de que *z* elevado a una potencia entera tiene un solo valor. Así, es preciso simplificar al máximo la fracción *n/m* si no queremos perder el tiempo generando raíces idénticas.

Ejemplo 6: Resolver la ecuación $x^4=-4$.

Solución: Siendo $-4=4(\cos\pi+isen\pi)$, entonces:

$$x=\sqrt[4]{4}\left(\cos\left(\frac{\pi+2\pi k}{4}\right)+isen\left(\frac{\pi+2\pi k}{4}\right)\right)\ \text{con } k = 0;\ 1;\ 2;\ 3.$$

Por lo tanto, para obtener las cuatro raíces distintas sólo tenemos que hacer variar a *k* con lo que obtenemos:

[8] A. David Wunsch, *Variable compleja con aplicaciones*, 1997, pg. 31.

$$x_1 = \sqrt{2}\left(\cos\left(\frac{\pi}{4}\right) + isen\left(\frac{\pi}{4}\right)\right) = 1 + i$$

$$x_2 = \sqrt{2}\left(\cos\left(\frac{3\pi}{4}\right) + isen\left(\frac{3\pi}{4}\right)\right) = -1 + i$$

$$x_3 = \sqrt{2}\left(\cos\left(\frac{5\pi}{4}\right) + isen\left(\frac{5\pi}{4}\right)\right) = -1 - i$$

$$x_4 = \sqrt{2}\left(\cos\left(\frac{7\pi}{4}\right) + isen\left(\frac{7\pi}{4}\right)\right) = 1 - i$$

Un caso especial: raíces de la unidad.

La ecuación particular $x^n = 1$ que define a las llamadas *raíces unitarias* de grado *n* es de especial interés[9]. Para éste caso particular se tiene que *r = 1,* y $\theta = 0$, de modo que las *n* raíces distintas de la unidad se obtienen de la fórmula:

$$\cos\left(\frac{2\pi k}{n}\right) + isen\left(\frac{2\pi k}{n}\right)$$

Tomando *k = 0; 1; 2;…; n-1.* Para el caso en que *k = 0* se obtiene la raíz *x = 1*, mientas que las *n-1* raíces restantes se obtienen serán las potencias:

$$w^k; k = 1;2;...;n-1$$

De la raíz $w = \cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$ y sólo se tendrá que aplicar la fórmula de De Moivre para obtenerlas todas.

Ejemplo 7: Hallar las raíces de la ecuación $x^4 = 1$.

Solución: Según lo visto anteriormente se tiene que:

$$x = \sqrt[4]{1}\left(\cos\left(\frac{0 + 2\pi k}{4}\right) + isen\left(\frac{0 + 2\pi k}{4}\right)\right) \text{ con } k = 0; 1; 2; 3.$$

entonces:

$$x_1 = \left(\cos\left(\frac{0}{4}\right) + isen\left(\frac{0}{4}\right)\right) = 1$$

[9] James Victor Uspensky, *Teoría de ecuaciones*, 2004, pg. 30.

$$x_2 = \left(\cos\left(\frac{\pi}{2}\right) + i sen\left(\frac{\pi}{2}\right)\right) = i$$

$$x_3 = \left(\cos\pi + i sen\pi\right) = -1$$

$$x_4 = \left(\cos\left(\frac{3\pi}{2}\right) + i sen\left(\frac{3\pi}{2}\right)\right) = -i$$

Ejercicios.

1. Encontrar los números reales x, y del complejo $z=x+iy$, que cumplan con las siguientes ecuaciones:

   a) $(1+i)z + (3i)\bar{z} = 2+i$;
   b) $z\bar{z} + 2z = 3+i$;
   c) $z\bar{z} + 3(z-\bar{z}) = 4-3i$;
   d) $z\bar{z} + 3(z+\bar{z}) = 7$;
   e) $z\bar{z} + 3(z+\bar{z}) = 3i$.

2. Expresar en forma polar los siguientes números complejos:

   a) $1 - i\sqrt{3}$;
   b) $\sqrt{3} - i$;
   c) i;
   d) $-6i$;
   e) $-1/2 + i\sqrt{3}/2$;
   f) $1/2 - i\sqrt{3}/2$;
   g) $1 - \sqrt{3} - i(1+\sqrt{3})$;
   h) $-4-3i$;
   i) $-2+i$;
   j) $2+\sqrt{3}+i$;

3. Resolver simultáneamente las ecuaciones:

   a) $iz + (1+i)w = 3+i$, $\quad (1+i)\bar{z} - (6+i)\bar{w} = 4$;
   b) $iz - (1+i)w = 3$, $\quad (2+i)z + iw = 4$.

4. Demostrar que la distancia entre los puntos $z_1=r_1(\cos\theta_1+i sen\theta_1)$ y $z_2=r_2(\cos\theta_2+i sen\theta_2)$ viene dada por

$$d^2 = r_1^2 + r_2^2 - 2\cos(\theta_1 - \theta_2).$$

5. Sean z, w números complejos. Demostrar que $|z+w|^2 + |z-w|^2 = 2|z|^2 + 2|w|^2$.

6. Calcular las raíces cuadradas de los números:

a) i ;
b) 15-8i ;
c) $1-i\sqrt{3}$;
d) -3-4i ;
e) $-1+i\sqrt{24}$;
f) $-\frac{1}{2}+i\frac{\sqrt{3}}{2}$;

7. Resolver las siguientes ecuaciones:

a) $x^2-(2+3i)x-1+3i=0$;
b) $(2-2i)x^2-(11+9i)x-16+6i=0$;
c) $x^2-(3-2i)x+5-5i=0$;
d) $(2+i)x^2-(5-i)x+2-2i=0$;
e) $x^2+ix+1=0$.

8. Demostrar que

$$(1+i\sqrt{3})(1+i)(\cos\varphi+isen\varphi)=2\sqrt{2}\left[\cos\left(\frac{7\pi}{12}+\varphi\right)+isen\left(\frac{7\pi}{12}+\varphi\right)\right].$$

9. Dada la igualdad $\sqrt{a+bi}=\pm(\alpha+i\beta)$, ¿cuáles son los valores de $\sqrt{-a-bi}$?

10. Sea $z\neq 0$. Dado $z+\frac{1}{z}=2\cos\varphi$, demostrar que $z^m+\frac{1}{z^m}=2\cos m\varphi$.

11. Si *n* es un entero, demostrar que:

a) $(1+i)^n=2^{\frac{n}{2}}\left(\cos\frac{n\pi}{4}+isen\frac{n\pi}{4}\right)$;
b) $\left(\sqrt{3}-i\right)^n=2^n\left(\cos\frac{n\pi}{6}+isen\frac{n\pi}{6}\right)$;

12. Sean *z*, *w* números complejos, demostrar que: $\left|\frac{z}{w}\right|=\frac{|z|}{|w|}$.

13. Calcular:

a) $i^{2/3}$;
b) $(1+i)^{4/6}$;
c) $\left(2+\sqrt{3}+i\right)^{7/2}$;
d) $\left(1/2-i\sqrt{3}/2\right)^{9/5}$.

14. Sea θ un número real y defínase

$$e^{i\theta}=\cos\theta+isen\theta$$

Demostrar que:

a) Si θ_1 y θ_2 son reales, entonces $e^{i(\theta_1+\theta_2)} = e^{i\theta_1}e^{i\theta_2}$;
b) Demostrar que cualquier número complejo cuyo valor absoluto sea igual a 1 se puede escribir en la forma e^{it}, para algún número real t;
c) Demostrar que cualquier número complejo se puede expresar en la forma $re^{i\theta}$, para algunos números reales r, θ, con $r \geq 0$;
d) Si $z_1 = r_1 e^{i\theta_1}$ y $z_2 = r_2 e^{i\theta_2}$ donde r_1, r_2, θ_1, θ_2 son números reales y r_1, r_2 son mayores o iguales que cero, demostrar que

$$z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}.$$

15. Si $|z| < \frac{1}{2}$, demostrar que la siguiente relación se satisface

$$\left|(1+i)z^3 + iz\right| < \frac{3}{4}.$$

16. Sea z un número complejo cualquiera. Demostrar que:

a) Re(iz) = -Img(z);
b) Img(iz) = Re(z);
c) Re(z^2) = (Re(z))^2 – (Img(z))^2;
d) Img(z^2) = 2(Re(z))(Img(z)).

17. ¿Cuáles de los siguientes enunciados son verdaderos para dos números complejos cualesquiera z_1 y z_2?

a) Re(z_1+z_2) = Re(z_1) + Re(z_2);
b) Re(z_1z_2) = Re(z_1)Re(z_2);
c) Re(βz_1) = βRe(z_1), donde β es real;
d) Img(z_1-z_2) = -Img(z_2- z_1);
e) Img[(z_1-z_2)^2] = -Img[(z_2- z_1)^2];

18. Si $n \geq 0$ es un entero cualquiera ¿cuáles son los cuatro valores posibles de i^n? Demuestre que $i^{n+4} = i^n$. Utilice el resultado anterior para determinar $i^{12,735}$ y $(1+i)^{3074}$ [Sugerencia: calcule primero $(1+i)^2$].

19. Sea $m \neq 0$ un entero. Se sabe que $z^{1/m}$ tiene m valores y que $z^{-1/m}$ también. Para z y m dados seleccionamos al azar un valor de $z^{1/m}$ y uno de $z^{-1/m}$.

a) ¿Es su producto necesariamente igual a 1?;

20. ¿Es siempre posible encontrar un valor de $z^{-1/m}$ tal que, para un valor de $z^{1/m}$ dado, se cumpla que $z^{1/m}\, z^{-1/m} = 1$?

21. Calcular y expresar el resultado en la forma $a+bi$:

a) $(-1+3i)^{-1}$;

b) $i(1+i)(2-i)$;

c) $\dfrac{2+i}{2-i}$;

d) $\dfrac{i}{1+i+\dfrac{i}{1+i+\dfrac{i}{1+i}}}$;

e) $\dfrac{1+i}{i}+\dfrac{i}{1-i}$;

f) $\dfrac{(4+3i)(1-2i)}{7-i}$;

g) $\left(\dfrac{1}{2}+i\dfrac{\sqrt{3}}{2}\right)^3$;

h) $\left(\dfrac{1+i}{\sqrt{2}}\right)^4$;

i) $\left(\dfrac{1-\sqrt{3}-i}{2}\right)^{24}$;

j) $\dfrac{(-1+i\sqrt{3})^{15}}{(1-i)^{20}}+\dfrac{(-1-i\sqrt{3})^{15}}{(1+i)^{20}}$

22. Hallar el módulo de los siguientes números complejos:

a) $-\dfrac{1}{2}+i\dfrac{\sqrt{3}}{2}$;

b) $\dfrac{1-i}{\sqrt{2}}$;

c) $3+4i$;

d) $\left(\dfrac{x+iy}{x-iy}\right)^n$, $n \geq 0$ es entero;

e) $i+\dfrac{(3+4i)(1+i)}{3-4i}$;

f) $\left[\dfrac{(3+4i)(1+i)}{3-4i}\right]^4$;

g) $(1+i)^5$.

4. Polinomios y Teoría de Ecuaciones

El propósito de este capítulo es establecer algunas de las propiedades básicas del álgebra de polinomios sobre un campo. Para tal efecto, se definen las operaciones elementales que se pueden realizar con estos elementos y se establecen algunas analogías con el anillo de los números enteros.

4.1 Operaciones y propiedades.

Definición 1: Sea K un campo. Se define un polinomio sobre K como una función de K en sí mismo, tal que existen elementos $a_0, a_1, \ldots, a_n$ en K tales que

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

para toda t en K, donde a la variable t se le llama indeterminada.

A los elementos $a_0, a_1, \ldots, a_n$ se les llama coeficientes del polinomio, y a los monomios separados $a_n t^n, a_{n-1} t^{n-1}, \ldots, a_1 t, a_0$ se les denomina términos del polinomio.

Si n es el máximo entero tal que $a_n \neq 0$, entonces se dice que *n es el grado de f* y se denota por *grad.* $f = n$. También se dice que a_n es el coeficiente inicial de f y a_0 es el término constante de f.

Los términos con coeficientes iguales a cero usualmente se omiten; mientras que, por otra parte, antes del término inicial pueden agregarse tantos términos con coeficientes nulos como se desee y todos los polinomios así obtenidos son considerados idénticos.

Aún cuando estrictamente hablando, un polinomio debe contener variable t, por cuestión de conveniencia, es costumbre considerar a las constantes distintas de cero como polinomios de grado cero[1].

Sea $g(t) = b_m t^m + b_{m-1} t^{m-1} + \cdots + b_1 t + b_0$ otro polinomio, donde $b_j \in$ K, entonces, la suma del polinomio f y el polinomio g, es el polinomio $f + g$. Si para $n \geq m$ se puede escribir $b_j = 0$ cuando $m < j$, entonces

$$g(t) = 0t^n + 0t^{n-1} + \cdots + 0t^{m+1} + b_m t^m + b_{m-1} t^{m-1} + \cdots + b_1 t + b_0,$$

y se pueden escribir los valores de la suma $f + g$ como

$$(f + g)(t) = (a_n + b_n)t^n + (a_{n-1} + b_{n-1})t^{n-1} + \cdots + (a_1 + b_1)t + a_0 + b_0.$$

Así, $f + g$ es nuevamente un polinomio.

Por otro lado, si $c \in$ K, entonces

[1] James Victor Uspensky, *Teoría de ecuaciones*, 2004.

$$(cf)(t) = ca_n t^n + ca_{n-1}t^{n-1} + \cdots + ca_1 t + ca_0,$$

y por tanto *cf* es también un polinomio.

También se puede considerar el producto de dos polinomios *f* y *g*, denotado por *fg* y

$$(fg)(t) = (a_n b_m)t^{n+m} + \cdots + a_0 b_0$$

de modo que *fg* es un polinomio.

Como observación de naturaleza práctica con respecto a la multiplicación de polinomios, si deseamos por ejemplo, multiplicar los polinomios

$$x^2 - x + 1 \text{ y } x^2 + x + 1$$

La operación usual, aprendida en la enseñanza elemental, sería la siguiente:

$$\begin{array}{llllll} \multicolumn{6}{l}{\left(x^2 - x + 1\right) \times \left(x^2 + x + 1\right)} \\ \hline x^4 & -x^3 & +x^2 & & & \\ & +x^3 & -x^2 & +x & & \\ & & +x^2 & -x & +1 & \\ \hline x^4 & & +x^2 & & +1 & \end{array}$$

Este procedimiento, sobre todo cuando los polinomios que se van a multiplicar contienen demasiados términos, supone un trabajo inútil bastante considerable al escribir potencias de *x*. Esto puede evitarse usando el método de coeficientes separados, que es bastante simple y útil. En éste método, se escriben solamente las sucesiones de los coeficientes de los polinomios que deseamos multiplicar, comenzando con los coeficientes iniciales y sin omitir los coeficientes nulos. Entonces, los coeficientes de uno de los polinomios se multiplican en orden por el primero, segundo, tercero, etc. coeficientes del segundo polinomio, y los renglones de números se disponen uno bajo el otro de tal manera que cada renglón esté desplazado un lugar a la derecha con respecto al precedente. Sumando los números que se encuentran en una misma columna se obtienen los coeficientes ordenados del producto. Finalmente se restituyen las potencias de la indeterminada *x* faltantes.

Por ejemplo, la operación anterior puede ordenarse como sigue

$$\begin{array}{llllll} \multicolumn{6}{l}{\left(1 \quad -1 \quad 1\right) \times \left(1 \quad 1 \quad 1\right)} \\ \hline 1 & -1 & +1 & & & \\ & +1 & -1 & +1 & & \\ & & +1 & -1 & +1 & \\ \hline 1 & 0 & +1 & 0 & +1 & \end{array}$$

De manera que el producto resultante es $x^4 + 0x^3 + x^2 + 0x + 1 = x^4 + x^2 + 1.$

Ejemplo 1. Multiplicar los polinomios

$$x^5 + x^3 - 2x^2 + 3 \text{ y } 2x^4 - 3x^3 + 4x^2 - 1$$

El cálculo se dispone de la siguiente manera

$$\begin{array}{cccccccccc} (1 & 0 & 1 & -2 & 0 & 3) & \times & (2 & -3 & 4 & 0 & -1) \\ \hline 2 & 0 & 2 & -4 & 0 & 6 & & & & & & \\ & -3 & 0 & -3 & 6 & 0 & -9 & & & & & \\ & & 4 & 0 & 4 & -8 & 0 & 12 & & & & \\ & & & & -1 & 0 & -1 & 2 & 0 & -3 & & \\ \hline 2 & -3 & 6 & -7 & 9 & -2 & -10 & 14 & 0 & -3 & & \end{array}$$

Obsérvese que se omitió un renglón nulo, omisión que no altera la operación sí se recorre un lugar más a la derecha el renglón inmediato siguiente.

Por tanto, el resultado de multiplicar los polinomios

$$x^5 + x^3 - 2x^2 + 3 \text{ y } 2x^4 - 3x^3 + 4x^2 - 1$$

es,

$$2x^9 - 3x^8 + 6x^7 - 7x^6 + 9x^5 - 2x^4 - 10x^3 + 14x^2 - 3.$$

Teorema 1. *Sean f y g polinomios tales que f(t) = g(t) para toda* $t \in K$. *Sean* $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$, $g(t) = b_n t^n + b_{n-1} t^{n-1} + \cdots + b_1 t + b_0$. *Entonces* $a_i = b_i$ *para toda i.*

Demostración. Considérese el polinomio $h = f - g$. Luego $h(t) = 0$ para toda $t \in$ K. Hay que probar que $a_i - b_i = 0$ para toda i. Supóngase que esto no es cierto. Sea r el mayor entero tal que $a_r \neq b_r$, entonces para toda t se puede escribir:

$$0 = (a_r - b_r)t^r + \cdots + (a_0 - b_0),$$

de donde dividiendo por t^r,

$$0 = (a_r - b_r) + (a_{r-1} - b_{r-1})t^{-1} + \cdots + (a_0 - b_0)t^{-r},$$

y haciendo que t alcance valores muy grandes (considerando valores reales para t) todos los términos que aparecen a la derecha de $(a_r - b_r)$ tienden a 0, de modo que $a_r - b_r = 0$ lo cual es un contradicción.

■

<u>*Definición 2.*</u> Al polinomio cuyos coeficientes son todos iguales a cero se le llama polinomio nulo o polinomio idénticamente nulo. Por conveniencia se dirá que un polinomio idénticamente nulo es de *grado* $-\infty$.

También se aceptará la convención de que:

$$-\infty + -\infty = -\infty, -\infty + a = -\infty \text{ con } -\infty < a$$

Para todo entero *a* y no se definirá ninguna otra operación con $-\infty$.

Esta convención se hace por el siguiente

Teorema 2. *Sean f y g polinomios con coeficientes en el campo K. Entonces*

$$grad\ (fg) = grad\ f + grad\ g.$$

Demostración. Sean f(t) y g(t) dos polinomios sobre K tales que:

$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$, y $g(t) = b_m t^m + b_{m-1} t^{m-1} + \cdots + b_1 t + b_0$, con $a_n \neq 0$ y $b_m \neq 0$. Entonces

$$f(t)g(t) = a_n b_m t^{n+m} + \cdots + a_0 b_0$$

Como el coeficiente inicial $a_n b_m \neq 0$, se observa que *grad (fg) = n+ m = grad f + grad g*.

Si *f, g*, o ambos, es un polinomio nulo, entonces la convención acerca de $-\infty$ hace que el enunciado sea también válido.

■

4.2 División de Polinomios.

Al igual que en el anillo de los números enteros, se va a definir el concepto divisibilidad de polinomios. Para tales efectos, se hará una pequeña modificación del Algoritmo de la división de números enteros tratado en el Capítulo II. Así, para el residuo, en lugar de considerar el valor absoluto se va a considerar el grado, entendiendo con esto, que el residuo pasa a ser ahora un polinomio. Sin embargo, antes de revisar este algoritmo revisemos lo que significa que un polinomio divida a otro.

<u>*Definición 3.*</u> Si *a(t)* y *b(t)* son dos polinomios con coeficientes en el campo K, tales que $b(t) \neq 0$, entonces se dice que *b(t)* divide a *a(t)* si existe un polinomio *h(t)* tal que *a(t) = b(t)h(t)*.

Con estas operaciones básicas ya definidas, estamos ya en la posición de verificar que el conjunto de los polinomios con coeficientes en el campo K forman una anillo conmutativo con unidad. Se deja para el lector verificar esta afirmación. Cabe señalar que el conjunto de polinomios con coeficientes en K no forman un campo (¿Por qué?).

A continuación se da una lista de teoremas en los cuales no se proporcionan las demostraciones ya que estas son dejadas como ejercicios para el lector.

Teorema 3. *Si b(t) | a(t), entonces grad. b ≤ grad. a.*

Teorema 4. *Si b(t) | a(t), entonces b(t) | a(t)c(t), para todo polinomio c(t) con coeficientes en K, y c(t)≠0.*

Teorema 5. *Si b(t) | a(t) y b(t) | c(t), entonces b(t) | [a(t)+c(t)].*

Teorema 6. *Si b(t) | a(t) y b(t) | c(t), entonces b(t) | [a(t)m(t)+c(t)n(t)].*

Teorema 7. *Si b(t) | a(t) y a(t) | b(t), entonces existe un escalar k en K tal que k≠0 y a(t)=kb(t).*

Algoritmo de la división de polinomios.

Sean $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$, $g(t) = b_m t^m + b_{m-1} t^{m-1} + \cdots + b_1 t + b_0$, polinomios de grado n y m respectivamente, por lo que $a_n \neq 0$, $b_m \neq 0$. Supóngase que $n \geq m$. Eligiendo de forma apropiada una constante c_0, se puede obtener un polinomio $f_1(x)$ tal que

$$f(x) - c_0 x^{n-m} g(x) = f_1(x)$$

que si no es idénticamente nulo, será de grado $n_1 < n$. Para conseguir esto, será suficiente tomar a $c_0 = a_n / b_m$. Mientras sea $n_1 \geq m$, puede encontrarse una constante c_1 tal que

$$f_1(x) - c_1 x^{n_1 - m} g(x) = f_2(x)$$

que si no es idénticamente nulo, será de grado $n_2 < n_1$. Si $n_2 \geq m$, puede repetirse el mismo proceso. Ahora, los grados de los polinomios $f_1(x)$, $f_2(x)$, … forman una sucesión decreciente, de manera que habrá un polinomio $f_{k+1}(x)$ que, o bien, es idénticamente nulo, o es de grado $n_{k+1} < m$.

Reemplazando *f1(x), f2(x), … fk(x)* por su valor, tenemos

$$\begin{aligned}
f(x) - c_0 x^{n-m} g(x) &= f_1(x) \\
f_1(x) - c_1 x^{n_1 - m} g(x) &= f_2(x) \\
f_2(x) - c_2 x^{n_2 - m} g(x) &= f_3(x) \\
\vdots \qquad\qquad \vdots \qquad\quad & \vdots \\
f_k(x) - c_k x^{n_k - m} g(x) &= f_{k+1}(x)
\end{aligned}$$

y sumando estas identidades tenemos que

$$f(x) + \cdots + f_k(x) - (c_0 x^{n+m} + \cdots + c_k x^{n_k - m}) g(x) = f_1(x) + \cdots + f_{k+1}(x)$$

entonces haciendo $(c_0 x^{n+m} + \cdots + c_k x^{n_k - m}) = q(x)$ y $f_{k+1}(x) = r(x)$, tenemos que

$$f(x) - q(x)g(x) = r(x), \text{ implica que } f(x) = q(x)g(x) + r(x).$$

El polinomio *r(x)* es de menor grado que *m* o es un polinomio idénticamente nulo. Los polinomios *q(x)* y *r(x)* se llaman *cociente* y *residuo* de la división de *f(x)* por *g(x)*.

Si el residuo de la división de *f(x)* por *g(x)* es cero, es decir, si

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

donde *q(x)* es un polinomio, se dice que *f(x)* es *divisible* por *g(x)*.

Es sencillo comprobar que sólo puede haber una pareja de polinomios *q(x)*, *r(x)* que satisfacen

$$f(x) = q(x)g(x) + r(x), \text{ y } grad\ r < grad\ g.$$

En efecto, si $f(x) = q(x)g(x) + r(x) = g(x)q_1(x) + r_1(x)$ con *grad r* y *grad* r_1 menores que *grad g*, entonces

$$g(x)\left[q(x) - q_1(x)\right] = r_1(x) - r(x)$$

y por el Teorema *2*,

$$m + grad\left[q(x) - q_1(x)\right] = grad\left[r_1(x) - r(x)\right] < m$$

lo cual sólo es posible si $q(x) - q_1(x) = 0$, en cuyo caso $r_1(x) = r(x)$ y $q(x) = q_1(x)$.

Observación. Si *grad f < grad g*, se toma $q(x) = 0$ y $r(x) = f(x)$.

Ejemplo 2. Dividir $x^8 + x^7 + 3x^4 - 1$ entre $x^4 - 3x^3 + 4x + 1$

Solución. Para efectos prácticos, una vez más se empleará el método de los coeficientes separados, que en esencia es el mismo que se utilizó para la multiplicación de polinomios, salvo ligeras modificaciones para la división. El arreglo del lado izquierdo tendrá los coeficientes del polinomio dividido así como de los polinomios residuos en los renglones inferiores. Por otra parte, el arreglo del lado derecho, en la parte superior, se encontrarán los coeficientes del polinomio divisor, mientras que en la parte inferior se encontrarán los coeficientes del polinomio cociente, es decir, las constantes c_i.

1	*1*	*0*	*0*	*3*	*0*	*0*	*0*	*-1*
-1	*3*	*0*	*-4*	*-1*				
0	*4*	*0*	*-4*	*2*	*0*	*0*	*0*	*-1*
	-4	*12*	*0*	*-16*	*-4*	*0*	*0*	*0*
	0	*12*	*-4*	*-14*	*-4*	*0*	*0*	*-1*
		-12	*36*	*0*	*-48*	*-12*	*0*	*0*
		0	*32*	*-14*	*-52*	*-12*	*0*	*-1*
			-32	*96*	*0*	*-128*	*-32*	*0*
			0	*82*	*-52*	*-140*	*-32*	*-1*
				82	*246*	*0*	*-328*	*-82*
					194	*-140*	*-360*	*-83*

1	*-3*	*0*	*4*	*1*
1	*4*	*12*	*32*	*82*

Entonces,

$$x^8 + x^7 + 3x^4 - 1 = \left(x^4 - 3x^3 + 4x + 1\right)\left(x^4 + 4x^3 + 12x^2 + 3x + 82\right) + \left(194x^3 - 140x^2 - 360x - 83\right)$$

Definición 4. Se dice que *a* es raíz de *f(x)* si *f(a) = 0*. Las raíces de *f(x)* son las soluciones de la ecuación *f(x) = 0*. A las raíces de *f(x)* también se les llama ceros de *f(x)*.

Como caso particular de la división de polinomios, sea *f(x)* un polinomio y $c \in$ K. Existe un polinomio *q(x)* y *r(x) = r*, con $r \in$ K, tales que

$$f(x) = (x - c)q(x) + r.$$

Además, *q(x)* y *r* son únicos. Obsérvese que el residuo *r(x)* es un polinomio de grado menor o igual que 1, es decir, *grad* $r \leq 1$, y por lo tanto es una constante del campo K.

Por otro lado, el residuo de la división por un binomio *x – c*, donde *c* es un escalar de K, puede encontrarse sin realizar la división larga. Esto se observa en el siguiente teorema.

Teorema del Residuo. *El residuo obtenido en la división de f(x) por (x – c) es igual al valor numérico del polinomio f(x) para x = c, es decir, a f(c).*

Demostración. Por ser el polinomio divisor *g(x)* un polinomio lineal, es decir, un polinomio de grado 1, el residuo será una constante *r*. Llamando al cociente como *q(x)*, tenemos la identidad

$$f(x) = (x - c)q(x) + r,$$

al sustituir *x* por *c* en esta identidad, debemos obtener el mismo resultado, es decir, la sustitución de *x* por *c* en *f(x)* debe ser lo mismo que sustituir *x* por *c* en *(x – c)q(x) + r*. Por ser *r* una constante, ésta no se verá afectada por la sustitución y el segundo miembro para *x = c*, será

$$(c - c)q(c) + r = 0q(c) + r = r,$$

mientras que el primer miembro es *f(c)*. Por lo tanto, *r = f(c)*, lo que significa que idénticamente en *x* es

$$f(x) = (x - c)q(x) + f(c).$$

■

Corolario 1. *a es raíz de f(x) si y sólo si (x – a) divide a f(x).*

Corolario 2. *El polinomio lineal x – a divide a (f(x) – f(a)).*

Corolario 3. *Si el polinomio lineal x – a divide a f(x)g(x) entonces x – a divide a f(x) o x – a divide a g(x).*

Ejemplo 3. Demostrar que $f(x) = x^3 + x^2 - 5x + 3$ es divisible por $x + 3$.

Solución. En este caso, $c = -3$, y

$$f(c) = f(-3) = -27 + 9 + 15 + 3 = 0,$$

por lo tanto $f(x)$ es divisible por $x + 3$.

■

Ejemplo 4. ¿En que condiciones $x^n + c^n$ es divisible por $x + c$?

Solución. Al sustituirse $x = -c$ en $x^n + c^n$ tenemos que:

$$(-c)^n + c^n = c^n + c^n = 2c^n, \text{ si } n \text{ es par,}$$

$$\text{y } (-c)^n + c^n = -c^n + c^n = 0, \text{ si } n \text{ es impar,}$$

por lo tanto, $x^n + c^n$ es divisible por $x + c$ si n es impar y si n es par el residuo de la división de $x^n + c^n$ por $x + c$ es $2c^n$.

■

Hemos visto entonces, que es posible obtener por medio del Teorema del residuo, el resto de dividir un polinomio $f(x)$ por el polinomio lineal $(x - c)$. Ahora bien, el cociente de esta división puede determinarse por un procedimiento muy conveniente conocido como *Regla de Ruffini*[2].

El Teorema del residuo afirma que $f(x) = (x - c)q(x) + r$, donde el cociente $q(x)$ es el polinomio $b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0$ y $b_{n-1}, b_{n-2}, ..., b_0$ los coeficientes que se determinarán. Efectuando la multiplicación $(x - c)q(x)$ tenemos que

$$(x - c)q(x) = b_{n-1}x^n + (b_{n-2} - cb_{n-1})x^{n-1} + (b_{n-3} - cb_{n-2})x^{n-2} + \cdots + (b_0 - cb_1)x - cb_0$$

y

$$(x - c)q(x) + r = b_{n-1}x^n + (b_{n-2} - cb_{n-1})x^{n-1} + (b_{n-3} - cb_{n-2})x^{n-2} + \cdots + (b_0 - cb_1)x + r - cb_0$$

Esta última identidad debe ser igual a

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

y para determinar los coeficientes $b_{n-1}, b_{n-2}, ..., b_0$ y r igualamos los coeficientes de las mismas potencias de x y se obtienen el grupo de ecuaciones

$$a_n = b_{n-1}; a_{n-1} = b_{n-2} - cb_{n-1}; \ldots, a_0 = r - cb_0$$

es decir,

---

[2] James Victor Uspensky, *Teoría de ecuaciones*, 2004.

$$b_{n-1} = a_n ; b_{n-2} = a_{n-1} + cb_{n-1} ; \ldots , r = a_0 + cb_0$$

De donde se observa que el cálculo de los coeficientes del polinomio cociente es de naturaleza recurrente y puede ordenarse convenientemente de la siguiente manera

$$\begin{array}{cccccccc} (c) & a_n & a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 \\ & & cb_{n-1} & cb_{n-2} & \cdots & cb_1 & cb_0 \\ \hline & b_{n-1} & b_{n-2} & b_{n-3} & \cdots & b_0 & r \end{array}$$

Las expresiones independientes para $b_{n-1}, b_{n-2}, ..., b_0$ y r que se obtiene por sustituciones sucesivas, son

$$b_{n-1} = a_n ; b_{n-2} = a_n c + a_{n-1} ; b_{n-3} = a_n c^2 + a_{n-1} c + a_{n-2} ; \ldots , b_0 = a_n c^{n-1} + a_{n-1} c^{n-2} + \cdots + a_1 ,$$

y

$$r = a_n c^n + a_{n-1} c^{n-1} + a_{n-2} c^{n-2} + \cdots + a_0 = f(c),$$

en donde la última identidad puede tomarse como una segunda demostración del teorema del residuo.

Ejemplo 5. Encontrar el cociente y el residuo, sin efectuar la división larga, del polinomio

$$3x^6 - 7x^5 + 5x^4 - x^2 - 6x - 8 \text{ por } (x + 2).$$

Solución.

$$\begin{array}{cccccccc} (c = -2) & 3 & -7 & 5 & 0 & -1 & -6 & -8 \\ & & -6 & 26 & -62 & 124 & -246 & 504 \\ \hline & 3 & -13 & 31 & -62 & 123 & -252 & 496 \end{array}$$

Luego entonces, $q(x) = 3x^5 - 13x^4 + 31x^3 - 62x^2 + 123x - 252$ y $r = 496$.

4.3 Polinomio Máximo Común Divisor.

El procedimiento para encontrar el máximo común divisor de dos enteros, estudiado en el Capítulo II, denominado algoritmo de Euclides, nos servirá en esta sección para calcular lo que ahora llamaremos el *máximo común divisor de dos polinomios*. Este procedimiento es esencialmente el mismo, es decir, se harán divisiones sucesivas para determinar el máximo común divisor de dos polinomios dados. Sin embargo, antes de revisar este algoritmo, se presentan algunos conceptos necesarios que garanticen la existencia de éste polinomio[3].

[3] La justificación de éste resultado es tomada de la obra de Manuel Valadez. *Algebra Lineal, Productos Internos y Teoremas de Estructura*. Ediciones Acatlán. México. 1996

Definición 5. Un *ideal* de K, o un *ideal* de polinomios es un subconjunto *J* de K que satisface las siguientes condiciones:

1) El polinomio idénticamente nulo está en *J*,
2) Si los polinomios *f* y *g* están en *J*, entonces *f* + *g* está en *J*,
3) Si el polinomio *f* está en *J* y el polinomio *g* es un polinomio arbitrario de K, entonces *fg* está en *J*.

A partir de esta última condición, se observa que si *c* es un escalar de K y *f* está en *J*, entonces *cf* está también en *J*.

Ejemplo 6. Sean $f_1, f_2, ..., f_n$ polinomios con coeficientes en K. Sea *J* el conjunto de todos los polinomios que se pueden escribir en la forma

$$g = g_1 f_1 + g_2 f_2 + \cdots + g_n f_n$$

Con g_i polinomios con coeficientes en K. Entonces *J* es un ideal.

Esto se verifica fácilmente ya que:

1) El polinomio nulo está en *J*, ya que $0 = 0 f_1 + 0 f_2 + \cdots + 0 f_n$,
2) Si *g* y *h* están en *J*, con $g = g_1 f_1 + g_2 f_2 + \cdots + g_n f_n$ y $h = h_1 f_1 + h_2 f_2 + \cdots + h_n f_n$ entonces,

   $$g + h = g_1 f_1 + \cdots + g_n f_n + h_1 f_1 + \cdots + h_n f_n = (g_1 + h_1) f_1 + \cdots + (g_n + h_n) f_n$$

   implica que *g* + *h* está en *J*,

3) Finalmente, sea *g´* un polinomio cualquiera con coeficiente en K, entonces $g´g = (g´g_1) f_1 + (g´g_2) f_2 + \cdots + (g´g_n) f_n$ implica que *g´g* está en *J*.

Se dice que el ideal *J* que aparece en este ejemplo está generado por $f_1, f_2, ..., f_n$ y se dice que $f_1, f_2, ..., f_n$ es un conjunto de generadores.

Hay que notar que cada uno de los f_i polinomios se encuentran en el ideal *J* ya que

$$f_i = 0 f_1 + \cdots + 1 f_i + \cdots + 0 f_n.$$

Ejemplo 7. El elemento *0* es un ideal. A tal ideal se le conoce como el *ideal nulo*.

Teorema 8. *Sea J un ideal de K. Entonces existe un polinomio g que es un generador de J.*

Demostración. Supóngase que *J* no es el ideal nulo. Sea *g* un polinomio en *J*, el cual no es el polinomio nulo y es de mínimo grado. Se verifica que *g* es un generador de *J*. Sea *f*

cualquier elemento de *J*. Por el algoritmo de la división de polinomios sabemos que existen polinomios *q* y *r* tales que

$$f = gq + r,$$

con *grad r* < *grad g*. Entonces, $r = f - gq$, y por definición se deduce que *r* está también en *J*. Como *grad r* < *grad g* y *g* es de grado mínimo, debe ser entonces que $r = 0$, de donde $f = gq$ y por lo tanto *g* es un generador de *J*.

■

Observación. Sea g_1 un generador no nulo de un ideal *J* y sea g_2 también un generador. Entonces existe un polinomio *q* tal que

$$g_1 = qg_2, \text{ y } grad\ g_1 = grad\ g_2 + grad\ q,$$

de aquí se observa que $grad\ g_2 \leq grad\ g_1$, y simétricamente, se debe tener que existe un polinomio q' tal que

$$g_2 = q'g_1, \text{ y } grad\ g_2 = grad\ g_1 + grad\ q',$$

entonces $grad\ g_1 \leq grad\ g_2$. Por lo tanto, se concluye que $grad\ g_1 = grad\ g_2$, es decir, que los polinomios *q*, q' son constantes.

A partir de ésta observación, se puede escribir entonces

$$g_1 = cg_2, \text{ con } c \text{ alguna constante.}$$

<u>*Definición 6.*</u> Sean $f_1, f_2, ..., f_n$ polinomios no nulos de K. un polinomio *g* se llama <u>*máximo común divisor*</u> de $f_1, f_2, ..., f_n$ si *g* divide a cada f_j y si *h* es otro polinomio que divide a cada f_j, entonces *h* divide a *g*.

Teorema 9. *Sea K un campo y sean $f_1, f_2, ..., f_n$ polinomios no nulos de K. Sea g un generador del ideal J generado por $f_1, f_2, ..., f_n$, entonces g es un máximo común divisor de $f_1, f_2, ..., f_n$.*

Demostración. Como cada f_j pertenece a *J*, existen *n* elementos $q_1, q_2, ..., q_n$ en K tales que para cada $j=1,\ldots,n$, $f_j = q_j g$. De aquí se concluye que *g* divide a cada f_j.

Por otra parte, puesto que *g* pertenece al ideal *J* generado por $f_1, f_2, ..., f_n$, se tiene que

$$g = \sum_{i=1}^{n} g_i f_i, \text{ para } g_i \text{ elementos de K.}$$

Si *h* es otro polinomio que divide a cada f_j, se tendrá entonces que existen $q'_1, q'_2, ..., q'_n$ elementos de K tales que para $j=1,\ldots,n$ $f_j = q'_j h$, quedando entonces que

$$g = \sum_{j=1}^{n} g_j f_j = \sum_{j=1}^{n} g_j (q'_j h) = \sum_{j=1}^{n} (g_j q'_j) h = h \sum_{j=1}^{n} (g_j q'_j)$$

Y por lo tanto h divide a g.

■

Describiremos a continuación un método eficiente que nos permita obtener el máximo común divisor de dos polinomios dados. Sean f y f_1 dos polinomios. Dividiendo f por f_1, sea q_1 el cociente y f_2 el residuo tal que

$$f = f_1 q_1 + f_2,$$

si f_2 no es un polinomio idénticamente nulo, podremos continuar dividiendo f_1 por f_2 obteniendo un cociente q_2 y residuo f_3 tal que

$$f_1 = f_2 q_2 + f_3,$$

nuevamente, si f_3 no es un polinomio idénticamente nulo, la división de f_2 por f_3 lleva a la identidad

$$f_2 = f_3 q_3 + f_4, \ldots, \text{ etc.}$$

Desde que el grado de los polinomios $f_1, f_2, f_3, \ldots$ disminuye y las operaciones pueden continuarse mientras el último residuo obtenido no sea un polinomio idénticamente nulo, se debe llegar a un residuo f_r que divida exactamente al residuo precedente, de manera que tendremos r identidades

$$\begin{aligned}
f &= f_1 q_1 + f_2; \\
f_1 &= f_2 q_2 + f_3; \\
f_2 &= f_3 q_3 + f_4; \\
&\vdots \quad \vdots \quad \vdots \\
f_{r-2} &= f_{r-1} q_{r-1} + f_r; \\
f_{r-1} &= f_r q_r .
\end{aligned}$$

En este procedimiento descrito se observa que f_r es el polinomio máximo común divisor de f y f_1, como lo afirma el Teorema 9.

Al referirnos a f_r como el polinomio que es el máximo común divisor, nos referimos a que f_r es común divisor de f y f_1 y a parte es de grado máximo, es decir, del conjunto de polinomios comunes divisores de f y f_1, f_r es el polinomio con el mayor grado.

Como nota importante, se tiene que si d es otro polinomio divisor común del mismo grado que el polinomio f_r, éste divide a f_r y el cociente es una constante. Luego, hay infinitos divisores comunes de f y f_1 de grado máximo, pero todos ellos son de la forma

$$cf_r,$$

donde *c* es una constante arbitraria. En cuestiones de divisibilidad, los polinomios que difieren únicamente de un factor constante, no pueden ser considerados como esencialmente distintos.

Ejemplo 8. Encontrar el polinomio máximo común divisor de

$$f(x) = x^6 + 2x^5 + x^3 + 3x^2 + 3x + 2 \text{ y } f_1(x) = x^4 + 4x^3 + 4x^2 - x - 2.$$

Solución.

1	*2*	*0*	*1*	*3*	*3*	*2*	→	*f(x)*
-1	*-4*	*-4*	*1*	*2*				
0	*-2*	*-4*	*2*	*5*	*3*	*2*		
	2	*8*	*8*	*-2*	*-4*			
	0	*4*	*10*	*3*	*-1*	*2*		
		-4	*-16*	*-16*	*4*	*8*		
		0	*-6*	*-13*	*3*	*10*	→	$f_2(x)$

1	*4*	*4*	*-1*	*-2*	→	$f_1(x)$
	1	*-2*	*4*		→	$q_1(x)$

Por lo tanto,

$$x^6 + 2x^5 + x^3 + 3x^2 + 3x + 2 = \left(x^4 + 4x^3 + 4x^2 - x - 2\right)\left(x^2 - 2x + 4\right) + \left(-6x^3 - 13x^2 + 3x + 10\right)$$

y continúa el algoritmo ya que no se obtuvo un residuo de cero, entonces

1	*4*	*4*	*-1*	*-2*	→	$F_1(x)$
-1	*-13/6*	*3/6*	*5/3*			
0	*11/6*	*9/2*	*2/3*	*-2*		
	-11/6	*-143/36*	*33/36*	*110/36*		
	0	*19/36*	*19/12*	*19/18*	→	$F_3(x)$

-6	*-13*	*3*	*10*	→	$f_2(x)$
	-1/6	*-11/36*		→	$q_2(x)$

por lo tanto,

$$x^4 + 4x^3 + 4x^2 - x - 2 = \left(-6x^3 - 13x^2 + 3x + 10\right)\left(-\frac{1}{6}x - \frac{11}{36}\right) + \left(\frac{19}{36}x^2 + \frac{19}{12}x + \frac{19}{18}\right)$$

y continúa el algoritmo ya que no se obtuvo un residuo de cero, entonces

-6	*-13*	*3*	*10*	→	$f_2(x)$	
6	*216/12*	*216/18*				
0	*5*	*15*	*10*			
	-5	*-15*	*-10*			
	0	*0*	*0*			

19/36	*19/12*	*19/18*	→	$f_3(x)$
	-216/19	*180/19*	→	$Q_3(x)$

Como se obtiene un residuo de cero, el algoritmo finaliza y por tanto el polinomio máximo común divisor de

$$f(x) = x^6 + 2x^5 + x^3 + 3x^2 + 3x + 2 \text{ y } f_1(x) = x^4 + 4x^3 + 4x^2 - x - 2$$

es,

$$\frac{19}{36}x^2+\frac{19}{12}x+\frac{19}{18}.$$

Cabe señalar que es posible simplificar los cálculos realizados, de manera que se puede evitar trabajar con coeficientes racionales, por ejemplo, si multiplicamos por *6* el polinomio $f_1(x)$, se tendrá que

$$6\,f_1(x)=6x^4+24x^3+24x^2-6x-12,$$

y de ésta manera el residuo $f_3(x)$ estará multiplicado por una constante que para nuestros propósitos no tiene importancia, por lo tanto

6	24	24	-6	-12
-6	-13	3	10	
0	11	27	4	-12
	66	162	24	-72
	-66	-143	33	110
	0	19	57	38

-6	-13	3	10
		-1	-11

→ *este renglón lo multiplicamos por 6 para evitar de nuevo coeficientes racionales*

Esta operación cambia el residuo final a $f_3(x)$ que se obtendría por el procedimiento común y corriente, de manera que se tendrá a $f_3(x)$ multiplicado por una constante.
Se observa que el último renglón, que en éste caso representa a $f_3(x)$, se tiene como factor común a *19*, por lo tanto, podemos tomar al polinomio $f_3(x)$ como

$$x^2+3x+2,$$

Hay que tener en cuenta que en los renglones que se escriben los coeficientes del cociente, los números que ahí aparecen ya no representan dichos coeficientes, pero esto no tiene ya importancia que sólo nos interesan los residuos, y de estos no nos preocupan los factores constantes. Ahora, solo falta por dividir $f_2(x)$ por $f_3(x)$ y se tendrá que

-6	-13	3	10
6	18	12	
0	5	15	10
	-5	-15	-10
	0	0	0

1	3	2
	-6	5

Lo cual finaliza con residuo nulo y por lo tanto el máximo común divisor puede ser también

$$x^2+3x+2.$$

<u>*Definición 7.*</u> Se dice que los polinomios $f_1, f_2,..., f_n$ cuyo máximo común divisor es igual a *1* son <u>*primos relativos.*</u>

4.4 Factorización Única.

A partir del Teorema Fundamental de la Aritmética, es posible obtener una analogía para el anillo de polinomios. Así, el rol que juegan los números primos en el anillo de

los enteros, se sustituye en el anillo de polinomios por los llamados polinomios irreducibles[4].

Definición 8. Un polinomio es llamado *reducible sobre el campo K*, si puede ser factorizado en polinomios de menor grado con coeficientes en el campo K, de lo contrario se le llama *irreducible sobre el campo K*.

El siguiente teorema, considerado como el más importante del álgebra, garantiza que todo polinomio es reducible sobre el campo de los números complejos. La demostración de este teorema, está fuera de los alcances de este material y por tanto sólo se hará uso de la importante afirmación que proporciona.

Teorema Fundamental del Álgebra. *Todo polinomio f con coeficientes en el campo K tiene por lo menos una raíz real o compleja.*

Corolario: *Sea K un campo tal que todo polinomio no constante en K tiene una raíz. Si f es un elemento de K de grado n, entonces existen elementos* $c_1, c_2, ..., c_n$ *y c en K, tales que*

$$f(t) = c(t - c_1)(t - c_2)\cdots(t - c_n).$$

Demostración. Por el corolario del Teorema del residuo, sea $a = c_1$, resulta entonces que

$$f(t) = (t\text{-}c_1)q_1(t), \text{ con grad. } q_1 = n - 1.$$

De manera semejante, sea $a = c_2$, del mismo corolario se concluye que

$$q_1(t) = (t - c_2)q_2(t), \text{ con } grad.\ q_2 = n - 2.$$

Y sustituyendo en la primera identidad, tenemos que

$$f(t) = c(t - c_1)(t - c_2)q_2(t).$$

Es claro que repitiendo el mismo proceso *n* veces se llega a la expresión deseada.

■

Corolario. *Sea f un polinomio de grado n con coeficientes en el campo K, entonces f tiene a lo más n raíces en K.*

Demostración. Supóngase que $c_1, c_2, ..., c_m$ son raíces de *f* en K y que $m > n$. Por el corolario anterior se tiene que

$$f(t) = (t - c_1)(t - c_2)\cdots(t - c_m)g(t),$$

con *g* un polinomio cualquiera de K. Luego entonces $grad.\ f \geq m$, lo cual es una contradicción y por lo tanto se debe tener que $m \leq n$.

■

[4] Serge Lang. *Algebra Lineal*. México. Addison-Wesley Iberoamericana. México. 1986.

Ejemplo 9. El polinomio x^2+1es irreducible sobre el campo de los números racionales.

Solución. Supóngase por el contrario que x^2+1es reducible sobre el campo de los racionales, es decir, que existen números *a, b* tales que

$$x^2+1=(x+a)(x+b)$$

sustituyendo $x = -b$ se tiene que

$$((-b)^2+1)=(-b+a)(-b+b)=0,$$

es decir, $(-b)^2=-1$lo cual es imposible dentro del campo de los números racionales y de hecho sobre cualquier campo ordenado.

Lema. Un polinomio *p(x)* de *grado 3* o *grado 2* es irreducible sobre el campo K a menos que *p(c) = 0* para alguna *c* en K.

Demostración. Cualquier factorización del polinomio *p(x)* en polinomios de menor grado, uno de los factores debe ser un polinomio lineal. Esto es claro ya que el grado del producto de polinomios es la suma de los grados de los factores.

■

Teorema 10. *Sea* $p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ *polinomio con coeficientes enteros. Cualquier raíz racional de p(x) debe tener la forma* $\frac{r}{s}$*, donde* $r \mid a_0$ *y* $s \mid a_n$.

Demostración. Supóngase que *p(x) = 0* para alguna $x=\frac{b}{c}$. Dividiendo *b* y *c* por *(b : c)*, se puede expresar $\frac{b}{c}$ en los menores términos como el cociente $\frac{r}{s}$ donde *(r : s) = 1*, es decir, los enteros *r* y *s* son primos relativos. Sustituyendo $x=\frac{b}{c}$ en *p(x)* y multiplicando por s^n, se tiene que

$$0=s^n p\left(\frac{r}{s}\right)=a_nr^n+a_{n-1}r^{n-1}s+a_{n-2}r^{n-2}s^2+\cdots+a_0s^n,$$

entonces,

$$-a_nr^n=s\left(a_{n-1}r^{n-1}+a_{n-2}r^{n-2}s+\cdots+a_0s^{n-1}\right),$$

es decir, $s \mid a_nr^n$, pero *(s : 1) = 1* entonces $s \mid a_nr^{n-1}$, …, $s \mid a_n$.

De manera similar,

$$-a_0s^n=r\left(a_nr^{n-1}+\cdots+a_1s^{n-1}\right),$$

de donde $r \mid a_0$.

■

Definición 9. Si el coeficiente inicial de un polinomio *f* es igual a *1*, decimos que *f* es un *polinomio mónico*.

Corolario. *Cualquier raíz racional de un polinomio mónico con coeficientes enteros, es un entero.*

A partir del corolario anterior, se observa que es condición necesaria que para que un polinomio sea divisible por un polinomio lineal de la forma $x - a$, el término constante de $p(x)$ debe ser múltiplo del término constante del polinomio $x - a$. Sin embargo esta condición no es suficiente en el sentido de que aún el término constante de $p(x)$ sea múltiplo de la constante a, no es posible afirmar que $p(x)$ sea divisible por $x - a$.

Ejemplo 10. Factorar el polinomio $f(x) = x^3 + 2x^2 - x - 2$ en polinomios de menor grado.

Solución. Por el corolario anterior, si existe una raíz entera del polinomio, forzosamente debe suceder que la raíz entera divida a *-2*, es decir, las posibles raíces enteras del polinomio $f(x)$ son *-1*, *1*, *2*, *-2*. Así, solo se verificará si $f(x)$ se anula para $x = -1$, $x = 1$, $x = 2$, $x = -2$. Así, para $x = 1$,

$$f(1) = (1)^3 + 2(1)^2 - (1) - 2 = 0,$$

y por tanto,

$$f(x) = x^3 + 2x^2 - x - 2 = (x-1)(x^2 + 3x + 2).$$

De igual modo, el polinomio $x^2 + 3x + 2$ es reducible sobre el campo de los números racionales y por tanto, la expresión factorizada de $f(x)$ es

$$f(x) = (x-1)(x+1)(x+2).$$

Teorema 11. *Si el polinomio p(x) es irreducible, entonces p(x) | a(x)b(x) implica que p(x) | a(x) o p(x) | b(x).*

Demostración. Como $p(x)$ es irreducible, el máximo común divisor de $p(x)$ y $a(x)$ es $p(x)$ ó *1*. En el primer caso, $p(x) \mid a(x)$. En el otro caso, es posible escribir

$$1 = s(x)p(x) + t(x)a(x),$$

y luego entonces,

$$b(x) = b(x)s(x)p(x) + b(x)t(x)a(x),$$

Como $p(x)$ divide a $a(x)b(x)$, entonces se tiene que $p(x)$ divide a ambos términos de la derecha de la ecuación y entonces $p(x) \mid b(x)$, que es lo que se quería demostrar.

■

Teorema de Factorización Única. *Cualquier polinomio a(x) no constante con coeficientes en K puede ser expresado como el producto de una constante c y*

polinomios mónicos irreducibles en K. Esta expresión es única excepto en el orden de los factores.

La demostración es análoga a la demostración del Teorema de Factorización Única de números enteros.

■

La derivada formal de un polinomio es de gran utilidad en el estudio de las raíces múltiples[5].

<u>*Definición 10.*</u> Sea $f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ polinomio con coeficientes en K. Se define la derivada formal de *f(t)*, que se denota por $f'(t)$, como sigue

$$f'(t) = a_1 + 2a_2 t + 3a_3 t^2 + \cdots + na_n t^{n-1}.$$

Para $n \geq 1$, se define la *(n+1)– ésima derivada*, $f^{(n+1)}(t)$, como la derivada de *n-ésima derivada*. Con esto queda definida $f^{(n)}(t)$ para todo número natural *n*.

Cabe señalar, que la definición de derivada de un polinomio *f* con coeficientes en K anteriormente expuesta, no hace alusión alguna a la definición de derivada que se presenta en el cálculo diferencial, la cual hace uso del concepto del límite de la función *f(t)*. Es decir, en este caso en particular, cuando tratemos el concepto de derivada formal del polinomio *f(t)*, se estará usando la definición ya presentada y no la del límite del polinomio *f* cuando *t* se aproxima a cero.

<u>*Definición 11.*</u> Si *c* es una raíz del polinomio *f*, la *multiplicidad* de la raíz *c* de *f* es el mayor entero positivo *r* tal que $(x - c)^r$ divide a *f*.

La multiplicidad de una raíz es evidentemente menor o igual al grado de *f*.

Teorema 12. *Sea f(x) un polinomio de grado n > 0 con coeficientes en K, y sea m un número entero positivo. La raíz a es de multiplicidad m de f(x) sí y sólo si se cumplen las siguientes condiciones*

1) $f(a) = f'(a) = \cdots = f^{(m-1)}(a) = 0,$
2) $f^{(m)}(a) \neq 0.$

Observación. Por conveniencia se tiene que $f^{(0)}(a) = f(a)$ y en el caso de que *m = 1*, la condición *1* se reduce a $f(a) = 0$.

Demostración. Afirmación directa. Para *m = 1*, *f(x) = (x – a)g(x)* y *x – a* no divide a *g(x)*. Entonces

$$f'(x) = (x-a)g'(x) + g(x) \text{ y } f'(a) = g(a) \neq 0.$$

[5]Kenneth Hoffman; Ray Kunze. *Álgebra Lineal*. Pearson Prentice Hall. México. 1973.

Supóngase ahora que la afirmación es verdadera para *m* y se demostrará para *m + 1*. Se tiene que $f(x) = (x-a)^{m+1} g(x)$ y *(x – a)* no divide a *g(x)*. Entonces

$$f'(x) = (x-a)^{m+1} g'(x) + (m+1)(x-a)^m g(x) = (x-a)^m \left[(x-a)g'(x) + (m+1)g(x)\right].$$

Es claro que *(x – a)* no divide al segundo factor y por lo tanto, *a* es raíz de multiplicidad *m* de $f'(x)$. Por la hipótesis de inducción aplicada a $f'(x)$, se tiene que

$$f'(a) = f''(a) = \cdots = f^{(m)}(a) = 0 \text{ y } f^{(m+1)}(a) \neq 0.$$

Afirmación recíproca. Para $m = 1$ las condiciones *1) y 2)* afirman que *f(a) = 0*, de donde *f(x) =(x – a)g(x)* y que $f'(a) \neq 0$, es decir, $(x-a)^2$ no divide *f(x)* porque en caso contrario se tendría

$$f(x) = (x-a)^2 g_1(x),$$
$$f'(x) = 2(x-a)g_1(x) + (x-a)^2 g_1'(x)$$

y $f'(a) = 0$, lo que es una contradicción.

Supóngase que la afirmación es verdadera para *m* y se demostrará para *m + 1*. Se parte de que

$$f(a) = f'(a) = f''(a) = \cdots = f^{(m)}(a) = 0 \text{ y } f^{(m+1)}(a) \neq 0.$$

Por la hipótesis de inducción aplicada a $f'(x)$ se concluye que *a* es raíz de multiplicidad *m* de $f'(x)$, así que

$$f'(x) = (x-a)^m g(x) \text{ y } (x-a) \text{ no divide a } g(x).$$

Como *f(a) = 0*, se tiene que para algún $s \geq 1$

$$f(x) = (x-a)^s g_1(x) \text{ y } (x-a) \text{ no divide a } g_1(x).$$

Entonces

$$f'(x) = (x-a)^{s-1}\left[(x-a)g_1(x) + sg_1'(x)\right]$$

y es claro que *(x – a)* no divide al segundo factor. Comparando esta expresión de $f'(x)$ con la anterior vemos que $s = m+1$ y

$$f(x) = (x-a)^{m+1} g_1(x) \text{ y } (x-a) \text{ no divide a } g_1(x).$$

■

Ejemplo 11. La ecuación $f(x) = x^n - nx + n - 1 = 0$; n > 1 se satisface para x = 1. ¿Cuál es la multiplicidad de esta raíz?

Solución. Tenemos que

$$f'(x) = nx^{n-1} - n$$

$$f''(x) = n(n-1)x^{n-2}$$

Luego:

$$f(1) = 0;\ f'(1) = 0;\ f''(1) \neq 0$$

y 1, por lo tanto, es una raíz doble. Así. el polinomio *f(x)* es divisible por $(x-1)^2$ pero no por $(x-1)^3$.

4.5 Solución de Ecuaciones de Tercer Grado.

En las siguientes dos secciones se tratarán los métodos de resolución de ecuaciones de tercer y cuarto grado mediante el empleo de radicales. Nos concentramos principalmente en polinomios de estos grados ante la imposibilidad de extender estos artificios a ecuaciones de quinto o mayor grado[6].

Sea *p(x)* un polinomio de *grado 3* con coeficientes en el campo K. La ecuación polinomial

$$p(x) = a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

tiene las mismas raíces que la ecuación *P(x)*, con

$$P(x) = x^3 + ax^2 + bx + c = 0,$$

Es decir, $P(x) = \frac{1}{a_3}p(x)$. La ecuación *P(x)* puede simplificarse de tal manera que el coeficiente de la indeterminada al cuadrado se anule. Esto se logra haciendo la sustitución

$x = y + k$, siendo k arbitrario.

Por medio de la fórmula de Taylor, calculamos *f(y + k)*, es decir,

$$f(y+k) = f(k) + f'(k)y + \frac{f''(k)}{2}y^2 + \frac{f'''(k)}{6}y^3,$$

Donde

$$f(k) = k^3 + ak^2 + bk + c;\ f'(k) = 3k^2 + 2ak + b;\ \frac{f''(k)}{2} = 3k + a;\ \frac{f'''(k)}{6} = 1.$$

---

[6] Ladislav Kvasz. *The history of Algebra and the Development of the Form of its Language.* Philosophia Mathematica Advance Access. 2006.

Lo que nos interesa entonces es que $\frac{f''(k)}{2} = 0$, es decir, *3k + a = 0*, o bien, $k = -\frac{a}{3}$. Entonces,

$$f'\left(-\frac{a}{3}\right) = b - \left(\frac{a}{3}\right)^2 \text{ y } f\left(-\frac{a}{3}\right) = c - \frac{ab}{3} + \frac{2a^3}{27},$$

Y sustituyendo $k = -\frac{a}{3}$ en $x = y + k$, se tiene que $x = y - \frac{a}{3}$. De esta manera *f(x)* se reduce a *f(y)*, donde $f(y) = y^3 + py + q = 0$ y $p = b - \left(\frac{a}{3}\right)^2$ y $q = c - \frac{ab}{3} + \frac{2a^3}{27}$, donde *f(x)* y *f(y)* tienen las mismas soluciones.

Sea ahora $y = w - \frac{p}{3w}$, entonces, sustituyendo $y = w - \frac{p}{3w}$ en *f(y)*, *f(y)* se reduce a

$$w^3 - \frac{p^3}{27w^3} + q = 0.$$

Multiplicando esta última identidad por w^3, se tiene que

$$\left(w^3\right)^2 + q(w^3) - \frac{p^3}{27} = 0.$$

Sea $w^3 = t$, entonces

$$t^2 + qt - \frac{p^3}{27} = 0$$

se puede resolver como una ecuación de segundo grado. Por tanto

$$t = w^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

tiene dos valores para *t* y *seis* valores para *w* en forma de radicales cúbicos.

Sea $A = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ y $B = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$. Ahora $w^3 = A$, tiene tres posibles valores. Denotando por *u* a estos tres posibles valores, se observa entonces que

$$u = \sqrt[3]{A}; u = z\sqrt[3]{A}; u = z^2\sqrt[3]{A};$$

donde $z = \frac{-1 + i\sqrt{3}}{2}$ es la raíz cúbica imaginaria de la unidad.

De igual manera, los otros tres posibles valores de $w^3 = B$, denotándolos por v, se obtienen de

$$v = \sqrt[3]{B}; v = z\sqrt[3]{B}; v = z^2\sqrt[3]{B};$$

y sustituyendo estos valores en la identidad $y = w - \frac{p}{3w}$ se obtienen *3* pares de soluciones para *y*, pares que se dan en iguales. Por lo tanto, la ecuación polinomial *f(y)* tiene las raíces

$$y_1 = \sqrt[3]{A} + \sqrt[3]{B};$$
$$y_2 = z * \sqrt[3]{A} + z^2 * \sqrt[3]{B};$$
$$y_3 = z^2 * \sqrt[3]{A} + z * \sqrt[3]{B}.$$

A estas identidades se les conoce como las *fórmulas de Cardano* (1501-1576)[7].

Ejemplo 12. Resolver la ecuación cúbica

$$x^3 + 9x - 26 = 0.$$

Solución. Para este caso, $a = 0$, $b = 9$, $c = -26$. Haciendo la sustitución $x = y - \frac{0}{3} = y$ se tiene que

$$x^3 + 9x - 26 = 0 \text{, donde } p = 9 \text{ y } q = -26$$

Ahora, $\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = \sqrt{\frac{\Delta}{108}}$, donde $\Delta = 4p^3 + 27q^2$, entonces $\Delta = 21168$ y en consecuencia $\sqrt{\frac{\Delta}{108}} = \sqrt{\frac{21168}{108}} = \sqrt{196} = 14$, luego entonces $A = 13 + 14 = 27$ y $B = 13 - 14 = -1$ y por lo tanto

$$\sqrt[3]{A} = \sqrt[3]{27} = 3 \text{ y } \sqrt[3]{B} = \sqrt[3]{-1}.$$

Finalmente las soluciones serán

[7] Ladislav Kvasz. *The history of Algebra and the Development of the Form of its Language.* Philosophia Mathematica Advance Access. 2006.

$$x_1 = \left(\sqrt[3]{27} + \sqrt[3]{-1}\right) = 3 - 1 = 2;$$
$$x_2 = \left(3 * \frac{-1+\sqrt{3}i}{2}\right) + \left(-1 * \frac{-1-\sqrt{3}i}{2}\right) = -1 + 2\sqrt{3}i;$$
$$x_3 = \left(3 * \frac{-1-\sqrt{3}i}{2}\right) + \left(-1 * \frac{-1+\sqrt{3}i}{2}\right) = -1 - 2\sqrt{3}i.$$

■

4.6 Solución de ecuaciones de cuarto grado con coeficientes reales.

Con base a lo analizado en la sección anterior, sea *f(x)* un polinomio de *grado 4* con coeficientes reales y

$$f(x) = x^4 + bx^3 + cx^2 + dx + e.$$

A partir de *f(x)* se construye la ecuación polinomial *h(y)* de *grado 3* y

$$h(y) = y^3 - cy^2 + (bd - 4e)y - b^2e + 4ce - d^2.$$

A *h(y)* se le conoce como *ecuación auxiliar*[8] de *f(x).*

Sea α número real y raíz de *h(y)*, es decir,

$$h(\alpha) = \alpha^3 - c\alpha^2 + (bd - 4e)\alpha - b^2e + 4ce - d^2 = 0$$

El artificio para resolver las ecuaciones de *cuarto grado* es completar el cuadrado de la identidad de *f(x)* de la siguiente manera

$$f(x) = 0 \Rightarrow x^4 + bx^3 + cx^2 + dx + e = 0,$$
$$\Rightarrow x^4 + bx^3 = -cx^2 - dx - e,$$
$$\Rightarrow x^4 + bx^3 + \frac{1}{4}b^2x^2 = -cx^2 - dx - e + \frac{1}{4}b^2x^2,$$
$$\Rightarrow \left(x^2 + \frac{1}{2}bx\right)^2 = \left(\frac{1}{4}b^2 - c\right)x^2 - dx - e,$$
$$\Rightarrow \left(x^2 + \frac{1}{2}bx\right)^2 + \left(x^2 + \frac{1}{2}bx\right)\alpha + \frac{1}{4}\alpha^2 = \left(\frac{1}{4}b^2 - c\right)x^2 - dx - e + \left(x^2 + \frac{1}{2}bx\right)\alpha + \frac{1}{4}\alpha^2,$$
$$\Rightarrow \left(x^2 + \frac{1}{2}bx + \frac{1}{2}\alpha\right)^2 = \left(\frac{1}{4}b^2 - c + \alpha\right)x^2 + \left(\frac{1}{2}b\alpha - d\right)x + \left(-e + \frac{1}{4}\alpha^2\right) \text{ ------- (1)}$$

Obsérvese la siguiente relación entre los coeficientes del segundo miembro de esta última identidad

[8] Humberto Cárdenas; Francisco Raggi; ET. AL. *Algebra Superior*. Trillas. México.1998.

$$\left(\frac{1}{2}b\alpha - d\right)^2 - 4\left(\frac{1}{4}b^2 - c + \alpha\right)\left(-e + \frac{1}{4}\alpha^2\right) =$$

$$= d^2 - db\alpha + \frac{1}{4}b^2\alpha^2 + b^2e - \frac{1}{4}b^2\alpha^2 - 4ce + c\alpha^2 + 4\alpha e - \alpha^3 =$$

$$= -\left(\alpha^3 - c\alpha^2 + (bd - 4e)\alpha - b^2e + 4ce - d^2\right) = 0.$$

Así que

$$\left(\frac{1}{2}b\alpha - d\right)^2 = 4\left(\frac{1}{4}b^2 - c + \alpha\right)\left(-e + \frac{1}{4}\alpha^2\right) \text{ ------- (2)}$$

Por otro lado, obsérvese que

$$\left(\frac{1}{4}b^2 - c + \alpha\right)x^2 + \left(\frac{1}{2}b\alpha - d\right)x + \left(-e + \frac{1}{4}\alpha^2\right)$$

Puede ser factorizado como una expresión lineal $Ax + B$ tal que

$$\left(\frac{1}{4}b^2 - c + \alpha\right)x^2 + \left(\frac{1}{2}b\alpha - d\right)x + \left(-e + \frac{1}{4}\alpha^2\right) = (Ax + B)^2$$

De esta manera se escogen los números A, B tales que

$$A^2 = \frac{1}{4}b^2 - c + \alpha;$$

$$B^2 = -e + \frac{1}{4}\alpha^2;$$

$$2AB = \frac{1}{2}b\alpha - d.$$

Si $2AB = -d + \frac{1}{2}b\alpha$, se toman A y B, si $2AB = d - \frac{1}{2}b\alpha$, se toman $-A$ y B. Y de la fórmula (2) se tiene que $4(AB)^2 = \left(\frac{1}{2}b\alpha - d\right)^2$, y entonces la fórmula (1) se puede escribir como

$$\left(x^2 + \frac{1}{2}bx + \frac{1}{2}\alpha\right)^2 = (Ax + B)^2$$

Esta ecuación es equivalente a la ecuación original *f(x)* y se satisface sí y sólo si se cumplen

$$x^2 + \frac{1}{2}bx + \frac{1}{2}\alpha = Ax + B$$

$$x^2 + \frac{1}{2}bx + \frac{1}{2}\alpha = -Ax - B$$

Por lo tanto las raíces de $f(x) = x^4 + bx^3 + cx^2 + dx + e.$ son las soluciones de las ecuaciones

$$x^2 + \left(\frac{1}{2}b - A\right)x + \left(\frac{1}{2}\alpha - B\right) = 0,$$

$$x^2 + \left(\frac{1}{2}b + A\right)x + \left(\frac{1}{2}\alpha + B\right) = 0.$$

Ejemplo 13. Sea $f(x) = x^4 + 4x^3 + x + 1.$ Entonces $b = 4$, $c = 0$, $d = 1$, $e = 1$. Por lo tanto la ecuación auxiliar es

$$h(y) = y^3 - 17 = 0.$$

Se toma $y = \sqrt[3]{17}.$ Ahora, deben cumplirse

$$A^2 = 4 + \sqrt[3]{17},$$
$$B^2 = -1 + \frac{1}{4}\sqrt[3]{17^2},$$
$$2AB = -1 + 2\sqrt[3]{17},$$

que se satisfacen si

$$A = \sqrt{4 + \sqrt[3]{17}},$$
$$B = \sqrt{-1 + \frac{1}{4}\sqrt[3]{17^2}}$$

de aquí, se obtienen entonces las ecuaciones

$$x^2 + \left(2 - \sqrt{4 + \sqrt[3]{17}}\right)x + \left(\frac{1}{2}\sqrt[3]{17} - \sqrt{-1 + \frac{1}{4}\sqrt[3]{17^2}}\right) = 0,$$
$$x^2 + \left(2 + \sqrt{4 + \sqrt[3]{17}}\right)x + \left(\frac{1}{2}\sqrt[3]{17} + \sqrt{-1 + \frac{1}{4}\sqrt[3]{17^2}}\right) = 0$$

cuyas soluciones son las raíces de *f(x)*.

■

Ejercicios.

1. Demostrar los corolarios 1, 2, 3 del Teorema del residuo.

2. Demostrar lo teoremas 3, 4, 5, 6, 7 correspondientes a la sección 4.2

3. Diremos que un polinomio *f(x)* tiene inverso multiplicativo si existe algún *g(x)* tal que *f(x)g(x)* = 1. Demuéstrese que las siguientes afirmaciones son equivalentes:

    a) *f(x)* tiene inverso multiplicativo;
    b) *f(x)* | *1*;
    c) *f(x)* es de grado cero.

4. Supóngase que *f(x)* | *g(x)*. Demuéstrese que toda raíz de *f(x)* es raíz de *g(x)*.

5. Multiplicar los siguientes polinomios:

    a) $x^4 + x^3 + x^2 + x + 1$ por $x^4 + x^3 + x^2 + x + 1$;
    b) $2x^4 - 3x^3 + x - 1$ por $x^3 + 3x^2 - 1$;
    c) $x^4 + 4x^3 - 5x^2 - 2$ por $x^4 - 4x^3 - 5x^2 - 2$;
    d) $x^5 - 3x^4 + x^3 - x + 1$ por $3x^3 + 7x^2 - x + 1$.

6. Dividir los siguientes polinomios:

    a) $x^7 + 3x^6 - 2x^3 + 3x^2 - x + 1$ por $x^4 - x + 1$;
    b) $2x^7 - 3x^6 + x^5 - 3x^4 + 5x^3 - 4x^2 + 2x - 1$ por $2x^3 - 3x^2 + x - 1$;
    c) $x^5 - 3x^2 + 6x - 1$ por $x^2 + x + 1$;
    d) $x^{10} + x^5 + 1$ por $x^2 + x + 1$;
    e) $(x+1)^7 - x^7 - 1$ por $(x^2 + x + 1)^2$.

7. Sin efectuar la división demostrar que:

    a) $x^4 + 3x^3 + 3x^2 + 3x + 2$ es divisible por $x + 2$;
    b) $x^5 - 3x^4 + x^2 - 2x - 3$ es divisible por $x - 3$;
    c) Si *a* y *b* son distintos y *f(x)* es, separadamente, divisible por *x-a* y *x-b*, demostrar que *f(x)* es divisible por *(x-a)(x-b)*;
    d) $2x^4 - 7x^3 - 2x^2 + 13x + 6$ por $x^2 - 5x + 6$;
    e) $2x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2$ por $x^2 + 1$;
    f) $x^6 + 4x^5 + 3x^4 + 2x^3 + x + 1$ por $x^2 + x + 1$.

8. Escríbase un polinomio de tercer grado que tenga como raíces 0, 1, 2.

9. Demuéstrese que *x-a* | *x-b* si, y sólo si, *a = b*.

10. Escríbase un polinomio de cuarto grado que tenga como raíces *i*, *-i*, 1+*i*, 1-*i*.

11. Resolver las siguientes ecuaciones:

a) $x^3 - 6x + 9 = 0$;
b) $x^3 + 9x^2 + 18x + 28 = 0$;
c) $x^3 + 6x + 2 = 0$;
d) $x^3 - 3abx + a^3 + b^3 = 0$;
e) $x^3 - 6ix + 4(1 - i) = 0$.

12. Hállese al polinomio de menor grado que se anula para x = -1, 0, 1 y toma el valor de 1 para x = 2.

13. Hállese al polinomio de menor grado que se anula para x = 0, 2+i, 2-i y toma los valores de 1 y -1 para x = -1y x = 1.

14. Resuélvase $x^4 - (1+2i)x^3 + (-4+i)x^2 + (3+6i)x + 3 - 3i = 0$; dadas las raíces i y $\sqrt{3}$.

15. Hállese al polinomio de menor grado que para x = 0 toma el valor de 1 y tiene las siguientes raíces: 1 y -1 como raíces simples, 2 como raíz doble y -3 como raíz triple.

16. Escribir un polinomio de séptimo grado con 0 y 1 como raíces dobles, -1 como raíz triple y que para x = 2 el polinomio tome el valor de -1.

17. Supóngase que el polinomio $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$ tiene raíces t_1, t_2, …, t_n. ¿Cuáles son las raíces de los siguientes polinomios

a) $f(t) = a_n t^n - a_{n-1} t^{n-1} + \cdots + (-1)^n a_0$;
b) $f(t) = a_0 t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n$;
c) $f(t) = a_n t^n + a_{n-1} b t^{n-1} + a_{n-2} b^2 t^{n-2} + \cdots + a_1 b^{n-2} t + a_0 b^n$?

18. Escríbase un polinomio de tercer grado que tenga como raíces 1, 1+i, 1-i.

19. Encontrar el polinomio máximo común divisor de los siguientes pares de polinomios:

a) $x^5 + x^4 - x^3 - 2x - 1,\ 3x^4 + 2x^3 + x^2 + 2x - 2$;
b) $x^5 - 2x^4 + x^3 + 7x^2 - 12x + 10,\ 3x^4 - 6x^3 + 5x^2 + 2x - 2$;
c) $x^5 + 3x^4 - 12x^3 - 52x^2 - 52x - 12,\ x^4 + 3x^3 - 6x^2 - 22x - 12$;
d) $x^4 - 4x^3 + 1,\ x^3 - 3x^2 + 1$;
e) $3x^6 - x^5 - 9x^4 - 14x^3 - 11x^2 - 3x - 1,\ 3x^5 + 8x^4 + 9x^3 + 15x^2 + 10x + 9$.

20. Sea $A_{n \times n}$ matriz sobre el campo K y sea J el conjunto de todos los polinomios $f(t)$ en $K[t]$ tales que $f(A)=0$. Demostrar que el conjunto J es un ideal.

21. Demostrar que el conjunto J propuesto en el ejemplo 7 es un ideal.

22. Utilizar el algoritmo euclidiano para encontrar los polinomios $M_1(x)$, $M_2(x)$ tal que satisfagan la ecuación $f_1(x)M_2(x) + f_2(x)M_1(x) = \delta(x)$, donde $\delta(x)$ es el polinomio máximo común divisor de los polinomios $f_1(x)$, $f_2(x)$:

    a) $f_1(x) = x^4 + 2x^3 - x^2 - 4x - 2$, $f_2(x) = x^4 + x^3 - x^2 - 2x - 2$;
    b) $f_1(x) = x^6 - 4x^5 + 11x^4 - 27x^3 + 37x^2 - 35x + 35$,
    $f_2(x) = x^5 - 3x^4 + 7x^3 - 20x^2 + 10x - 25$;
    c) $f_1(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$, $f_2(x) = 3x^4 - 4x^3 - x^2 - x - 2$.

23. Utilizar el algoritmo euclidiano para encontrar los polinomios $M_1(x)$, $M_2(x)$ tal que satisfagan la ecuación $f_1(x)M_2(x) + f_2(x)M_1(x) = 1$:

    a) $f_1(x) = x^4 - x^3 + 4x^2 + 4x + 1$, $f_2(x) = x^2 - x - 1$;
    b) $f_1(x) = 2x^4 + 3x^3 - 3x^2 - 5x + 2$, $f_2(x) = 2x^3 + x^2 - x - 1$;
    c) $f_1(x) = x^5 + 5x^4 + 9x^3 + 7x^2 + 5x + 3$, $f_2(x) = x^4 + 2x^3 + 2x^2 + x + 1$.

24. Encontrar un polinomio del menor grado posible que proporcione residuo de:

    a) $2x$ cuando es dividido por $(x-1)^2$; $3x$ cuando es dividido por $(x-2)^3$;
    b) $x^2 + x + 1$ cuando es dividido por $x^4 - 2x^3 + 10x - 7$; $2x^2 - 3$ cuando es dividido por $x^4 - 2x^3 - 3x^2 + 13x - 10$.

25. Sea $\delta(x)$ el polinomio máximo común divisor de los polinomios $f_1(x)$, $f_2(x)$. Supóngase que la relación $f_1(x)M(x) + f_2(x)N(x) = \delta(x)$ se satisface. ¿Cuál es el polinomio máximo común divisor de los polinomios $M(x)$, $N(x)$?

26. Resolver las siguientes ecuaciones:

    a) $x^4 + 2x^3 - 2x^2 + 6x - 15 = 0$;
    b) $x^4 - 4x^3 + 3x^2 + 2x - 1 = 0$;
    c) $x^4 - 6x^3 + 6x^2 + 27x - 56 = 0$;
    d) $x^4 - x^3 - 4x^2 + 4x + 1 = 0$;
    e) $4x^4 - 4x^3 + 3x^2 - 2x + 1 = 0$.

27. De los siguientes polinomios encontrar el polinomio máximo común divisor:

    a) $(x-1)^3(x+2)^2(x-3)(x-4), (x-1)^2(x+2)(x+5)$;
    b) $(x^3-1)(x^2-2x+1)$, $(x^2-1)^3$.

28. Suponiendo demostrado el teorema fundamental del álgebra, demostrar lo siguiente: Si f y g son dos polinomios sobre el campo K, entonces el m.c.d. $(f : g) = 1$ si, y sólo si, f y g no tienen raíces en común.

Para el resto de los ejercicios se necesita la siguiente definición. Si f, g y p son polinomios sobre el campo K con $p \neq 0$, se dice que f es congruente con g en módulo p si (f-g) es divisible por p. Si f es congruente con g módulo p, se escribe

$$f \equiv g \text{ mód } p.$$

29. Demostrar que para todo polinomio no nulo p, la congruencia módulo p es una relación de equivalencia. Es decir:

    a) Es reflexiva: $f \equiv f \text{ mód } p$;
    b) Es simétrica: $f \equiv g \text{ mód } p$, entonces $g \equiv f \text{ mód } p$;
    c) Es transitiva: $f \equiv g \text{ mód } p$ y $g \equiv h \text{ mód } p$ entonces $f \equiv h \text{ mód } p$.

30. Supóngase que $f \equiv g \text{ mód } p$ y $f_1 \equiv g_1 \text{ mód } p$. Demostrar que:

    a) $f+f_1 \equiv g+g_1 \text{ mód } p$;
    b) $ff_1 \equiv gg_1 \text{ mód } p$.

31. Si p es un polinomio irreducible y $fg \equiv 0 \text{ mód } p$, demostrar que $f \equiv 0 \text{ mód } p$ o que $g \equiv 0 \text{ mód } p$. Dar un ejemplo que muestre que esto es falso si p no es irreducible.

32. Si f, g, h y p son polinomios sobre el campo K, $p \neq 0$ y si $f \equiv g \text{ mód } p$ entonces h(f) $\equiv h(g) \text{ mód } p$.

Referencias Bibliográficas

1. Birkhoff, Garrett; Mac Lane Saunders. *A Survey of Modern Algebra*. MacMillan Company New York. USA. 1964.
2. Cárdenas, Humberto; Raggi, Francisco; ET. AL. *Algebra Superior*. Segunda Edición, quinta reimpresión. Trillas. México.1998.
3. Uspensky, James. *Teoría de Ecuaciones*. Limusa Noriega Editores. México. 2004.
4. Wunsch, David. *Variable compleja con aplicaciones*. Segunda edición. Pearson Education. México. 1999.
5. Lang, Serge. *Algebra Lineal*. México. Addison-Wesley Iberoamericana. México. 1986.
6. Hoffman, Kenneth; Kunze, Ray. *Álgebra Lineal*. Pearson Prentice Hall. México. 1973.
7. Reyes, Araceli. *Algebra Superior*. Thompson Learning. México. 2005.
8. Valadez, Manuel. *Algebra Lineal, Productos Internos y Teoremas de Estructura*. Ediciones Acatlán. México. 1996.
9. Apostol, Tom. *Introducción a la Teoría Analítica de los Números*. Reverté. España. 1984.
10. Apostol, Tom. *Análisis Matemático*. Reverté. Segunda edición. España. 2001.
11. Apostol, Tom. *Calculus Volumen I*. Reverté. Segunda edición. España. 1999.
12. Spivak, Michael. *Cálculo Infinitesimal*. Reverté. Segunda edición. España. 2001.
13. Bartle, Robert; Sherbert, Donald. *Introducción al análisis matemático de una variable*. Limusa Wiley. Segunda edición. México. 2001.
14. Zaldívar, Felipe. *Fundamentos de álgebra*. Universidad Autónoma de México, Fondo de Cultura Económica. 2005.

15. Courant, Richard; Robbins, Herbert. *¿Qué son las matemáticas?* Primera edición en español. Fondo de Cultura Económica. México. 2006.
16. Faddeev, D.; Sominskii, I. S. *Problems in Higher Algebra*. W. H. Freeman And Company. San Francisco and London. 1965.
17. Corry, Leo. *Modern Algebra and the Rise of Mathematical Structures.* Basel (Birkhäuser). 1996.
18. Andrews, George. *Number Theory*. Saunders Company. USA. 1971.
19. Whitelaw, Thomas. *An Introduction to Abstract Algebra.* Chapman And Hall Company.
20. Krick, Teresa. *"Números Enteros"*. Notas correspondientes de la materia de álgebra1 de la Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires.