Universidad del Bío-Bío

Facultad de Educación y Humanidades

Escuela de Pedagogía en Educación Matemática

Dominios de Integridad

Autores: Julio César Jara Fernández
Daniela Alejandra Soto Henríquez
Ximena del Carmen Torres Palma

Profesor Guía: Héctor Fernando Miranda

SEMINARIO PARA OPTAR AL TÍTULO DE PROFESOR DE ENSEÑANZA MEDIA EN EDUACIÓN MATEMÁTICA.

Chillán, Noviembre de 2008

Agradecimientos

Agradecer, hoy y siempre, a mi familia por su amor, comprensión y apoyo primordial que me han otorgado durante este tiempo y que ha sido imprescindible en mi formación como profesional. Además, deseo dar gracias a mis queridos amigos y colegas, con quienes compartí el desarrollo de mi principal proyecto de vida, el ser docente, por su incondicional apoyo, siendo fundamental en este periodo universitario.

Finalmente, mis agradecimientos a los profesores de la Universidad, en especial a nuestro profesor guía, Dr. Fernando Miranda, por su apoyo y oportunas sugerencias.

Ximena

En esta oportunidad, quisiera agradecer a mis compañeras Ximena y Daniela por acompañarme en este desafío de realizar nuestro seminario juntos. Gracias por su comprensión, apoyo y por sobre todo, nuestra gran amistad.

A nuestro profesor guía, Dr. Fernando Miranda, por sus sugerencias, por la facilitación de material y por darnos la libertad y autonomía de ir realizando este seminario según lo que íbamos aprendiendo. De forma muy especial, a mis compañeros Pablo Molina y Paula Verdugo por su gran ayuda en la utilización de LaTeX. Sin su aporte, este seminario no sería lo mismo, por ello les doy las gracias.

A todos mis profesores y profesoras de esta Universidad, que de muchas maneras han incidido en mi formación profesional y personal.

A Leslie. A Vanessa, Andrea y Romina. Y finalmente a Mercedes, Aviano, Anita y Camilo...sin ellos, nada sería lo mismo.

Julio

A mi familia por haberme entregado el apoyo necesario para llevar a cabo esta meta; en especial a mi hermano Camilo, por ser el motor principal que me mantuvo en este desafío, sobre todo en los momentos más difíciles que nos tocó vivir.

Agradezco también a mis compañeros de casa y a mis amigos que siempre tuvieron una palabra de aliento, en los momentos de flaqueza; en especial y con mucho cariño a los *3 mosqueteros* siempre complices y confidentes, gracias por entenderme.

Daniela

Resumen

El presente trabajo, tiene como propósito ordenar ideas para un estudio comprensivo de un tema que en Matemáticas ocupa en lugar transversal en el desarrollo del Algebra y la Teoría de Números. El concepto de Dominio de Integridad, que es nuestro principal objeto de estudio, es un constructo teórico que, al igual que muchos otros conceptos en Matemáticas, presenta una versatilidad y riqueza inagotables para la comprensión e investigación actuales en la disciplina, dentro de sus más abstractas representaciones, y particularmente, en el avance de la Teoría Algebraica de Números.

El hecho de abordar un tema particular de nuestra disciplina, nos permite adquirir la madurez necesaria para trabajar con el resto de los temas que presenta la Matemática en general, muy sofisticados y de alta utilidad para el desarrollo científico y tecnológico, y una comprensión de los temas debe sugerir como consecuencia la habilidad para comunicar resultados y hacerlos comprensibles en su totalidad. Al ser el concepto de Dominio de Integridad un hilo unificador entre teorías y disciplinas, queremos además, proporcionar un documento de estudio válido para quienes quieran emprender su aprendizaje, por curiosidad o por el gusto de hacerlo.

Para ello, hemos enfocado nuestro estudio hacia una construcción de los enteros y sus más importantes conceptos de divisibilidad y factorización, para proseguir con una estructuración de tales propiedades aritméticas en el sentido algebraico. Continuamos con representaciones de Dominios de Integridad conocidos y algunas de sus aplicaciones en la Teoría elemental de Números, teniendo como propósito, estudiarlas desde le punto de vista algebraico. Paa finalizar, se contruye el cuerpo de cocientes de un Dominio de Integridad, tema asociado a los enteros y su incidencia en la formulación de los números racionales.

Abstract

The purpose of this work is to order ideas to a comprehensive study about a subject that in Mathematics has a transversal place in the development of algebra and the Theory of Numbers. The concept Integral domain, our main subject, is a theoretic construct that, like other concepts in Mathematics, present a versatility and unfinished richness to the comprehension and current investigations in the discipline, among its more abstract representations, and especially in the advance of the Theory of Numbers.

To deal with a particular subject of our discipline, allows us to get the maturity needed to work with the rest of the subjects that general Mathematic presents, very sophisticated and highly useful to the scientific and technologic development and at the same time a subject comprehension, must suggest as consequence, the ability to communicate the results and make them comprehensible. The concept of Integral domain unifies theories and disciplines, moreover we want to give a valid document of study to those who want to begin their learning, for curiosity or just because they enjoy it.

For that, we have to focus our study to a construction of integers and their most important concepts of divisibility and factorization, to continue with an organization of such arithmetic properties in the algebraic sense. We continue with representations of the integral domain known and some of their applications in the elemental theory of numbers, having as purpose, study them from the algebraic point of view. To finish, the body of quotients of integral domain must be built, subject related to the integers and its incidence in the formulation of the rational numbers.

ÍNDICE GENERAL

Introducción

La siguiente introducción representa una síntesis de los temas que estudiaremos en profundidad durante el desarrollo de texto. En el damos a conocer los principales conceptos para encaminar nuestro estudio.

De forma previa, adevertiremos al lector conocimientos mínimos acerca de la teoría de grupos, por lo que supondremos conocidas para evitar el regreso infinito de conceptos. Comenzaremos desde la teoría de anillos, del cual extraeremos las siguientes definiciones que darán un sustento general a nuestro estudio posterior.

Definición 0.1 *Un anillo* $(A, +, \cdot)$ *es un conjunto* A *dotado de dos operaciones binarias internas, suma* $(+)$ *y multiplicación* $(\cdot)$*, definidas en* A *tales que se satisfacen los siguientes axiomas:*

- *(R, +) es un grupo abeliano.*
- *La multiplicación definida en R es asociativa.*
- *Para todas las a, b y c R, se cumple la ley distributiva izquierda* $a(b+c) = (ab) + (ac)$ *y la ley distributiva derecha* $(a+b)c = (ac) + (bc)$*.*

Nuestro seminario tendrá como eje central la siguiente definición, la cual es el sustento de la teoría que queremos investigar y comprender.

Definición 0.2 *Un* dominio de integridad *D es un anillo conmutativo $(R, +, \cdot)$ que carece de elementos divisores de cero (tanto por la izquierda como por la derecha).*

A todo dominio de integridad se le puede asociar un cuerpo, llamado Cuerpo de Cocientes, en el cual se sumerge de la misma manera como los números enteros se insertan en los números racionales. Veremos cómo se construye este cuerpo de cocientes y el homomorfismo que permite obtener esta interesante conexión.

Si D es un Dominio de Integridad, no todos los elementos de D poseen un inverso bajo la multiplicación, como es el caso del anillo de los enteros.

Definición 0.3 *Un anillo A puede sumergirse en un anillo A' si existe un isomorfismo de A en A'. (Si R y R' tiene elementos de unidad 1 y $1'$, respectivamente, exigimos además que este isomorfismo lleve de 1 en $1'$). A A' llamaremos sobreanillo o extensión de A si A puede sumergirse en A'.*

Podemos entonces construir un cuerpo que contenga a D, de la misma forma como se construyen las fracciones de números enteros, el cual contiene a Z como un subanillo, el cual lo realizaremos en el desarrollo de este seminario.

Nuestro recorrido continuará netamente en los elementos teóricos particulares de los dominios de integridad. Dado que los enteros presentan una descomposición en factores primos que es única, los dominios enteros como estructuras exponen evidencias aún más abstractas para casos generales. Las definiciones conocidas de la teoría de Números, se nos presentan de la siguiente manera en la teoría algebraica.

Definición 0.4 *Sea D un dominio de integridad y $a, b \in D$. Si existe $c \in D$ tal que $b = ac$, entonces a* divide *a b, o a es un* factor *de b, y se denota $a|b$.*

Definición 0.5 *Un elemento u de un dominio de integridad D es una* unidad *de D, si u divide a 1, esto es, si u tiene inverso multiplicativo en D. Dos elementos $a, b \in D$ son* asociados *en D si $a = bu$, donde u es una unidad en D.*

Definición 0.6 *Un elemento p distinto de cero que no sea unidad de un dominio de integridad D es un* irreducible *de D, si en cualquier factorización $p = ab$ en D, a ó b es unidad.*

Una de las propiedades fundamentales del anillo de los números enteros es que todo entero se expresa de manera única como un producto de números primos. Esta propiedad se generaliza en forma natural a los Dominios de Integridad, originándose así el concepto de Dominio de Factorización Única.

Definición 0.7 *Un dominio de integridad D es un* dominio de factorización única *(DFU) si se satisfacen las siguientes condiciones:*

1. *Todo elemento de D que no sea ni cero ni una unidad, se puede factorizar en un número finito de irreducibles.*

2. *Si $p_1 \cdots p_r$ y $q_1 \cdots q_s$ son dos factorizaciones en irreducibles del mismo elemento de D, entonces $r = s$ y los q_j pueden renumerarse de manera que los p_i y q_i sean asociados.*

Esta definición nos permite tener más de una factorización única en elementos irreducibles de un dominio de integridad D, pero hace referencia a que es un dominio de factorización única si la cantidad de elementos irreducibles en dos factorizaciones distintas, es posible la construcción de elementos asociados tomando de cada una de las factorizaciones un irreducible.

Definición 0.8 *Un dominio de integridad D es un* dominio de ideales principales *(DIP) si todo ideal en D es un ideal principal.*

El concepto de ideal en la teoría de anillos es análogo al de subgrupos en la teoría de grupos. En nuestro estudio, detallaremos aún más sobre las implicancias de estos conceptos, que proporcionan información valiosa acerca de la posibilidad de divisibilidad en estructuras como los enteros.

Para el caso de dominio de integridad, tenemos la siguiente

Definición 0.9 *Sea D un dominio de integridad e I un conjunto tal que $I \subseteq D$. Se dice que I es un* ideal *en D si satisface las siguientes condiciones:*

1. $0 \in I$.
2. *Si $a, b \in I$, entonces $a + b \in I$.*
3. *Si $a \in D$ y $b \in I$, entonces $ab \in I$.*

Definición 0.10 *Sea I un ideal en un dominio de integridad D. Se dice que I es* ideal principal *de D si está generado por un solo elemento, es decir, si es de la forma*

$$(a) = aD = ab/\ b \in D.$$

Nuestro estudio estará dirigido, además, a otros dominios de integridad: definiremos estos casos particulares para obtener mejor información del concepto principal. Existen algunos anillos que gozan de buenas propiedades de factorización y divisibilidad. Entre ellos se encuentran los Dominios Euclidianos, los cuales son a la vez dominios de Factorización única. Los ejemplos más conocidos de un Dominio Euclidiano son los números enteros y los anillos de polinomios con coeficientes neteros, pero también existen otros que no son frecuentemente utilizados, como son los Enteros de Gauss. Haremos un estudio de estos enteros y sus propiedades más relevantes.

Estas definiciones nos permitirán llegar a dos interesantes resultados, pero que en ciertos conjuntos que poseen la estructura de dominio de integridad no se cumplen, los conocidos ejemplos de dominios sin factorización única, que estudiaremos a lo largo de este seminario.

Definición 0.11 *Una* evaluación euclidiana *en un dominio de integridad D es una función v que transforma a los elementos distintos de cero de D, en los enteros no negativos tal que satisfacen las siguientes condiciones:*

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

Un dominio de integridad D es un dominio euclidiano *si existe una evaluación euclidiana en D.*

La siguiente definición es un ejemplo de dominio euclidiano, en donde la función es ahora una norma entera asociada en el plano complejo. Este dominio, el cual fue descubierto por el matemático alemán Carl Friedrich Gauss (1777-1855), en relación al problema de determinar que números enteros positivos se pueden expresar como suma de dos cuadrados.

Definición 0.12 *Un* entero gaussiano *es un número complejo de la forma* $a + bi$ *donde* $a, b \in Z$. *Para un entero gaussiano* $\alpha = a + bi$ *la* norma $N(\alpha)$ *de* α *es* $a^2 + b^2$.

Con estas definiciones, enmarcaremos nuestro estudio hacia nuestro objetivo de situar la estructura de Dominio de Integridad como una importante fuente de información para comprender estructuras algebraicas superiores en jerarquía y como condicionador de una Teoría de Números tendiente hacia la unificación de conceptos por sobre la colección de resultados parciales conocidos antes de su formulación algebraica.

CAPÍTULO 1

Los Números Enteros

En este capítulo, presentamos los números enteros como punto de partida de nuestro estudio. En el extraemos las ideas que motivaron su orígen y sus aspectos axiomáticos, sentando las bases para desarrollar y encauzar el contenido hacia el concepto de dominio de integridad.

Agregamos, además, los elementos que caracterizan los números enteros, tales como las condiciones de divisibilidad, máximo común divisor, la unicidad de la descomposición en factores primos, hasta una prueba del Teorema Fundamental de la Aritmética, dando término con la definición de anillo y algunos aspectos relevantes de esta teoría, clave en la conceptualización abstracta de los enteros como un caso particular de dominio de integridad.

1.1. Construcción de los Enteros

1.1.1. Axiomas de Peano

Los axiomas o postulados de Peano[1] definen de manera exacta al conjunto de los números naturales sin necesidad de otra teoría alguna (por ejemplo Teoría de Conjuntos) y ajena de las definiciones aritméticas de suma o equivalencia, de la siguiente forma:

Básicamente, los naturales se pueden construir a partir de cinco axiomas fundamentales:

i 1 es un número natural, es decir, el conjunto de los N no es vacío.

ii Si $a \in N$, entonces $a + 1 \in N$ (llamado el sucesor de a).

iii 1 no es sucesor de ningún N (primer elemento del conjunto).

iv Si hay dos números naturales a y b tales que sus sucesores son diferentes entonces a y b son números naturales diferentes.

[1] Peano, Giuseppe (1858-1932), Matemático italiano. Estableció la construcción axiomática de los números naturales en el siglo XIX.

v Axioma de inducción: si un conjunto de N contiene al 1 y a los sucesores de cada uno de sus elementos entonces contiene a todos los números naturales.

Los axiomas de Peano tal como fueron escritos (en latín), son los siguientes:

1. El 0 es un número.
2. El sucesor inmediato de un número también es un número.
3. El 0 no es el sucesor inmediato de ningún número.
4. Dos números no tienen el mismo sucesor inmediato.
5. Toda propiedad perteneciente a 0 y al sucesor inmediato de todo número que también tenga esa propiedad pertenece a todos los números (inducción matemática).

Hoy en día, por convenio, el 0 no se considera un número natural, por lo cual dichos axiomas comienzan con el 1.

Teorema 1.1 *La existencia de solo una operación binaria "+" en N que satisface:*

1. $a + 1 = a'$

2. $a + b' = (a + b)'$, *con* $a, b \in N$

Demostración. En primer lugar mostraremos que existe una operación binaria $'+'$ en N que satisface (1) y (2).

Consideremos el conjunto

$S = \{a \in N / a + b$, se puede definir para todos $b \in N$, satisface la condiciones en (1) y (2)$\}$.

Para demostrar que $1 \in S$, para ello definamos

$$1 + b = b' \text{ para cada uno } b \in N.$$

Entonces $1+1 = 1'$ por nuestra definición y $1+b' = (b')' = (1+b)'$ utilizando en repetidas ocasiones nuestra definición, podemos concluir que (i) e (ii) se cumple para $a = 1$, por lo que $1 \in S$.

Sea $a \in S$. Por lo tanto $a + b$ con $b \in N$. Se define como $a' + b = (a + b)'$. Entonces

$$\begin{aligned} a' + 1 &= (a + 1)' && \text{por definición} \\ &= (a')' && \text{note que a} \in S \end{aligned}$$

También

$$\begin{aligned} a' + b' &= (a + b')' && \text{por definición} \\ &= ((a + b)')' && \text{note que a} \in S \\ &= (a' + b)' && \text{por definición} \end{aligned}$$

Por lo que $a' \in S$. Por el axioma (v), se concluye $S = N$. ■

Teorema 1.2 *La operación binaria " + " en N satisface los siguientes enunciados:*

1. *Para todo $a, b, c \in N$, entonces $(a + b) + c = a + (b + c)$ (propiedad asociativa de la adición).*

2. *Para todo $a, b \in N$, entonces se cumple que $a + b = b + a$ (propiedad conmutativa de la adición).*

Demostración. Sean a y b números naturales, y dejemos

$$S = \{c \in N/(a + b) + c = a + (b + c)\}.$$

Entonces por definición de $+$

$$(a + b) + 1 = (a + b)' = a + b' = a + (b + 1).$$

Así, $1 \in S$. Supongamos que $c \in S$. Entonces

$$\begin{array}{rcll} (a + b) + c' & = & ((a + b) + c)' & \text{por definición de } + \\ & = & (a + (b + c))' & \text{note que } c \in S \\ & = & a + (b + c)' & \text{por definición de } + \\ & = & a + (b + c') & \text{por definición de } + \end{array}$$

Entonces $c' \in S$. Por tanto, por el axioma (v), se deduce que $S = N$. Esto demuestra la propiedad asociativa de la adición.

La prueba de (2) es similar y por lo cual fácil de realizar. ■

Teorema 1.3 *Leyes de cancelación para la adición.*

1. $a + u \neq a$.

2. $a + x = a + y \Rightarrow x = y$.

Para todos $a, u, x, y \in N$.

Demostración.

1. Como $u \in N$ entonces por axioma (iii), $u \geq 1$. Supongamos que es 1, entonces

$$\begin{array}{rcll} a + u & = & a + 1 & \text{por Teorema 1} \\ & = & a' & \\ & \neq & a & \end{array}$$

Analogamente si u toma otros valores en N siempre van a ser mayores que a.

2.
   - Caso 1: $x = y+v$, para algunos $v \in N$. Entonces $a+y = a+y \Rightarrow a+y+v = a+y$ lo que contradice el enunciado (i).
   - Caso 2: $y = x+v'$ para algunos $v' \in N$. Entonces $a+x = a+y \Rightarrow a+x = a+x+v'$ lo que contradice el enunciado 1.

■

Teorema 1.4 *El principio del buen orden es un lema que establece que todo conjunto que esté formado únicamente por números naturales tiene un primer elemento. Es decir, que el conjunto de los números naturales es bien ordenado. El primer elemento de los números naturales es 1.*

Demostración. Sea $A \in N$ un conjunto no vacío. Si A no tiene elemento mínimo, entonces existe un conjunto $B = N$.

- 0 debe de estar en B puesto que de no ser así, 0 sería el elemento mínimo de A.
- Si n está en B, entonces $n+1$ también está en B, porque de lo contrario, $n+1$ sería un elemento mínimo de A.

Luego entonces por el principio de inducción matemática, y , pero eso contradice la suposición de que A no era un conjunto vacío. Por lo tanto, A debe tener elemento mínimo. ■

Teorema 1.5 *La existencia de solo una operación binaria $\cdot$ en N que satisface:*

1. $a \cdot 1 = a$
2. $a \cdot b' = a \cdot b + a$

Para todos $a, b \in N$.

Se suele escribir $a \cdot b$ simplemente como ab, que se llama el producto de a por b o el "número que se obtiene de la multiplicación de a por b".

Demostración. La demostración es similar a la del teorema 1.1.1. ■

1.1.2. Los Enteros

Después de haber dado un desarrollo sistemático al conjunto de números naturales N, ahora lo ampliaremos al conjunto números enteros (Z).

La necesidad de ampliar el sistema de números naturales surge del hecho de que una ecuación del tipo $a = x + b$, con $a, b \in N$, no tiene solución en N (por teorema 1.5).

Consideremos el símbolo $\equiv$ como la relación de equivalencia NXN definida por:

$$(a, b) \equiv (c, d) \text{ tal que } a + d = b + c$$

Claramente, $\equiv$ es una relación de equivalencia de NXN. Denotamos la clase de equivalencia de (a,b),$(\overline{a,b})$ y definimos la operación binaria + y $\cdot$ respectivamente como adición y multiplicación respectivamente, en el conjunto de $NXN/\equiv$ de las clases de equivalencia segun las siguientes normas:

$$\begin{aligned}(\overline{a,b})+(\overline{c,d}) &= (\overline{a+c,b+d})\\ (\overline{a,b})(\overline{c,d}) &= (\overline{ac+bd,ad+bc})\end{aligned} \tag{1.3}$$

Estas definiciones de adición y multiplicación están bien definidas, como se puede comprobar de manera sencilla. Notese que $(\overline{1,1})$ es el elemento de la identidad para la adición y $(\overline{1+1,1})$ es el elemento de la identidad para la multiplicación. Puesto que hemos

$$(\overline{a,b})+(\overline{1,1})=(\overline{a+1,b+1})=(\overline{a,b}).$$

y

$$(\overline{a,b})(\overline{1+1,1})=(\overline{a(1+1)+b,a+b(1+1)})=(\overline{a+a+b,a+b+b})=(\overline{a,b})$$

El conjunto $NXN/\equiv$ de clase de equivalencia se denota por Z.

1.2. Divisibilidad en los Enteros

Hasta este punto, consideramos de manera casi natural las operaciones que podemos realizar en este conjunto: las conocemos desde la enseñanza primaria, y a grandes rasgos, podemos decir que en los enteros sabemos sumar, restar y multiplicar. Este hecho se refiere a la cerradura de estas operaciones bajo el conjunto Z, que ya trataremos en detalle en las secciones posteriores.

Una de las dificultades en este conjunto es definir la división, para ello tenemos el siguiente

Teorema 1.6 *Sean a y b dos enteros tal que $b>0$. Entonces, existen únicos enteros q y r que satisfacen*

$$a=qb+r, \qquad 1\leq r<b.$$

El número r en este teorema, es conocido como el *resto no negativo* de a cuando se divide por b. Este resultado es conocido en Aritmética como *Algoritmo de Euclides*.

Demostración. Consideremos $S=\{y/y=a-bx\}$, con $y>0, x\in\mathbf{Z}$, con $S\neq\phi,\ S\subseteq\mathbf{N}$.

Por principio de buen orden en los enteros, existe un elemento minimal r en un conjunto $S\neq\phi$, $S\subseteq\mathbf{N}$, tal que $r=a-bq$, y podemos escribirlo como $a=bq+r$, para un cierto $q\in\mathbf{Z}$.

Veamos que $0 \leq r < b$, para ello, supongamos que $r \geq b$, entonces $r - b \geq 0$. Pero $r - b = a - b(q+1) \in \mathbf{Z}$, del cual realizamos el siguiente análisis

$$\begin{aligned} q+1 &> q \\ b(q+1) &> bq \\ -b(q+1) &< -bq \\ a - b(q+1) &< a - bq \\ r - b &< r \end{aligned}$$

lo cual es una contradicción, pues señala que $r-b$ menor que el elemento minimal, por tanto

$$0 \leq r < b$$

Para probar la unicidad de estos enteros q y r, supongamos que existen q, r y q', r' tales que $bq + r = bq' + r'$, donde $0 \leq r < b$. Entonces $b(q - q') = |r' - r| < b$, de lo cual se desprende que $q = q'$ y $r = r'$. ■

Definición 1.1 *Si el resto de a cuando es dividido por b es cero (en otras palabras, si existe un entero c tal que a = cb) se dice que a en un* múltiplo *de b. Si b* divide *a a, escribimos b|a y decimos que b es un* divisor *de a.*

Claramente podemos observar que siempre en números enteros obtenemos los siguientes resultados:

- $1|a$
- $-1|a$
- $a|0$
- Para cada $a \in \mathbf{Z}$, $a|a$.

Desde la artimética fundamental, conocemos el siguiente resultado, muy útil para nuestras posteriores definiciones de divisibilidad.

Teorema 1.7 *: Supóngase que a, b y c son enteros tal que $b \neq 0$ y $b \neq 0$. Entonces:*

1. *Si $b|a$ y $c|b$, entonces $c|a$.*
2. *Si $b|a$, entonces $bc|ac$.*
3. *Si $c|d$ y $c|e$, entonces , para cualquier m y n enteros, $c|dm + en$.*
4. *Si $a|b$ y $b|a$, entonces $a = \pm b$*

Demostración.

1. Por definición de divisibilidad, obtenemos los siguientes resultados
   - $b|a \Rightarrow a = k_1 b$ (1), con $k_1 \in \mathbf{Z}$.

- $c|b \Rightarrow b = k_2 c$ (2), con $k_2 \in \mathbf{Z}$.

Luego, reemplazamos (2) en (1) y obtenemos la siguiente expresión: $a = k_1 k_2 c \Rightarrow c|a$.

2. Por definición de divisibilidad, solo basta con amplificar por c en ambos lados de la igualdad.

3. Por definición de divisibilidad, $d = ck_1$, con $k_1 \in \mathbf{Z}$ y $e = ck_2$, con $k_2 \in \mathbf{Z}$. Entonces, al amplificar por los enteros m y n en estas igualdades, se obtiene que $dm = ck_1 m$ y $en = ck_2 n$. Al sumar ambas expresiones, tenemos que $dm + en = c(k_1 m + k_2 n)$, concluyendo de este modo que $c|dm + en$.

4. $a|b \Rightarrow b = ak_1$, con $k_1 \in \mathbf{Z}$. Por otra parte, $b|a \Rightarrow a = bk_2$, con $k_2 \in \mathbf{Z}$. Entonces, $b = (bk_1)k_2$; asociamos k_1 y k_2, lo cual implica dos soluciones en $\mathbf{Z}$: $1 = k_1 k_2$ y $-1 = k_1 k_2$, por tanto $b(k_1 k_2) = a$, probando que $a = \pm b$. $\diamond$

■

1.3. Máximo Común Divisor

Entenderemos por *módulo entero*, o simplemente *módulo*, como un conjunto de enteros en el que las operaciones de adición y sustracción son cerradas, en otras palabras, si m y n son enteros en un módulo, entonces $m + n$ y $m - n$ también pertenecen al módulo. Aquel módulo que solo contiene el elemento cero, se conoce como *módulo cero*. El conjunto de todos los enteros forma un módulo, como el conjunto de los enteros que son múltiplos de un entero fijo k.

Teorema 1.8 *En los enteros*

1. *El número 0 pertenece a todos los módulos enteros.*

2. *Sean* a *y* b *enteros pertenecientes a un módulo y sean* m, n *dos enteros arbitrarios. Entonces* $am + bn$ *pertenecen al módulo.*

Demostración.

1. Tomemos cualquier a en un módulo. Entonces $0 = a - a$ está en el módulo.

2. Si a pertenece a un módulo, entonces $2a = a + a$; $3a = 2a + a$; ma también pertenecen al módulo, con m entero. Del mismo modo para b: si b pertenece al módulo, por lo tanto bn pertenece al módulo, con n entero. Según la definición de módulo, para dos elementos de un módulo, las operaciones de adición y sustracción son *cerradas*, único argumento que necesitamos para concluir este teorema.

■

Teorema 1.9 *Sean* a *y* b *dos enteros. Entonces el conjunto de números de la forma* $am+bn$ *forma un módulo.*

Demostración. La demostración de este teorema es trivial y se desprende del resultado anterior. ■

Teorema 1.10 *Cualquier módulo distinto del módulo cero es un conjunto de múltiplos de un entero positivo fijo.*

Demostración. Sea d el menor entero positivo en el módulo. Ante esto, podemos señalar que cada número en el módulo debe ser un múltiplo de d. Supongamos ahora lo contrario: sea n un número en el módulo, el cual no es múltiplo de d. Entonces, por el Teorema 1.2.1, existen enteros q y r tales que:

$$n = dq + r, \qquad 1 \leq r < d$$

A partir de la definición de módulo, vemos que $r = n - dq$ pertenece al módulo y esto contradice la propiedad de minimal definida para d. Por lo tanto, cada elemento del módulo es un múltiplo de d. Se evidencia, además, que cada entero múltiplo de d, pertence al módulo. ■

Usaremos estos resultados para definir el *máximo común divisor*. Primero, se dice que si $k|a$ y $k|b$, se dice que k es un *divisor común* de a y b. Estas características a priori, no son suficientes para definir el *máximo común divisor* como el *mayor* de los enteros positivos que divide de manera simultánea a a y b.

Definición 1.2 *: Sean a y b dos enteros y consideremos el módulo del conjunto de números de la forma am+bn, con m y n enteros arbitrarios. Si esta relación no produce el módulo cero, entonces el número* d *que se ha usado en la demostración del Teorema 1.3.3, se denomina* máximo común divisor *de a y b y se denota por* (a, b).

Teorema 1.11 *El MCD* (a, b) *posee las siguientes propiedades:*

1. *Existen enteros* x *y* y *tales que* $ax + by = (a, b)$.
2. *Dados* $x, y \in \boldsymbol{Z}$, *siempre se tiene que* $(a, b)|ax + by$.
3. *Si* $e|a$ *y* $e|b$, *entonces* $e|(a, b)$.

Demostración.

1. Es consecuencia directa del teorema 1.3.3, por definición de módulo.
2. (a,b) es MCD, por tanto $(a, b)|a$ *y* $(a, b)|b$; entonces existen ciertos $k_1, k_2 \in \mathbf{Z}$ que por definición de divisibilidad en enteros, se tiene que

$$\begin{aligned} a &= (a, b)k_1 \quad / \cdot x, x \in \mathbf{Z} \\ b &= (a, b)k_2 \quad / \cdot y, y \in \mathbf{Z} \end{aligned}$$

   Y multiplicaremos por los números señalados. Luego de esto, obtenemos las siguientes expresiones:

$$ax = (a,b)k_1x$$
$$by = (a,b)k_2y$$

Al sumar ambas expresiones, tenemos que:

$$ax + by = (a,b)\,(k_1x + k_2y) \quad (k_1x + k_2y) \in \mathbf{Z}$$

Sea $(k_1x + k_2y) = \delta$, entonces, concluimos que $ax + by = (a,b)\delta$, y por definición de divisibilidad, entonces

$$(a,b)|ax + by$$

3. Por consecuencia del Teorema 1.3.3.

■

Teorema 1.12 *El MCD de dos números, ambos distintos de cero, es único.*

Demostración. Sean d y d' dos enteros tales que satisfacen la defínción de MCD, entonces $d|d'$ y $d'|d$, lo cual implica que $d = d'$. ■

Teorema 1.13 *Dos enteros a y b, ambos distinto de cero, son primos relativos, si y solo si existen enteros x y y tales que $1 = ax + by$.*

Demostración. Si $(a,b) = 1$, entonces, por Teorema 1.3.3, existen enteros tales que $1 = ax + by$. Si $(a,b) = d$ y $d > 1$, entonces d es el menor entero positivo que puede ser expresado como la forma usada en Teorema 1.3.3. Por lo tanto $1 \neq ax+by$, lo cual contradice nuestra hipótesis. De este modo, hemos probado el teorema. ■

Teorema 1.14 *Sea $d = (a,b)$. Entonces $(\frac{a}{d}, \frac{b}{d}) = 1$.*

Demostración. Si $(\frac{a}{d}, \frac{b}{d}) = k$, con $k \neq 1$, entonces $\frac{a}{d} = ka'$ y $\frac{b}{d} = kb'$; esto es $a = dka'$ y $b = dkb'$. Como $dk|a$ y $dk|b$, se tiene que $d \neq (a,b)$. De ello, podemos concluir que si $d = (a,b)$, entonces $(\frac{a}{d}, \frac{b}{d}) = 1$. ■

1.4. Los Números Primos

Los números primos y sus propiedades fueron estudiados de manera exhaustiva por los matemáticos de la antigua Grecia.

Los matemáticos de la Escuela Pitagórica (500 A.C. a 300 A.C.) estaban interesados en los números por su misticismo y sus propiedades numerológicas. Ellos comprendían la idea de primalidad y estaban interesados en los números perfectos y amigables.

Para el momento en que los *Elementos* de Euclides aparecieron por el 300 A.C., ya habían sido probados varios resultados importantes acerca de los números primos. En el libro IX de los *Elementos*, Euclides plantea el siguiente

Teorema 1.15 *El conjunto de los números primos es infinito.*

Demostración. Supondremos que hay un número primo p que es el último número primo y veremos que eso es imposible. Además, suponiendo que p es el número primo más grande, construyamos otro número q, tal que:

$$q = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p) + 1$$

que es el resultado de multiplicar todos los números primos hasta el último, p; y después sumarle 1.

Evidentemente q no es divisible por ningún primo, pues siempre daría como resto 1. Luego q es divisible sólo por 1 y por sí mismo, es decir, q es primo. Por otra parte q es mayor que p. Luego p no es el mayor número primo. Por tanto no puede existir un número primo que sea el mayor y con esto verificamos la existencia de infinitos números primos. ■

Esta es una de las primeras demostraciones conocidas en la que se utiliza el método de *reducción al absurdo* para establecer la veracidad de ciertos resultados.

Una propiedad importante de los números primos es la siguiente

Definición 1.3 *Si p es primo y $p|ab$, entonces ya sea $p|a$ ó $p|b$ ó ambos.*

Euclides también demuestra el *Teorema Fundamental de la Aritmética*, el cual señala que todo entero puede ser expresado como un producto finito y único de primos.

Teorema 1.16 (Fundamental de la Aritmética) *Todo entero positivo se puede representar de forma única como producto de factores primos. Es decir, para todo $n \geq 2$ existe una factorización única de productos de números primos:*

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_i^{e_i}$$

donde todos los p_i son primos distintos, mientras que los $e^i \geq 0$.

Demostración. Suponga, por contradicción, que existen algunos números enteros que no pueden ser expresados como productos de primos. Sea n el más pequeño de tales enteros. Entonces n no puede ser 1 o primo, así que n tiene que ser un número compuesto. Por tanto $n = ab$ con $1 < a,b < n$. Puesto que n es el entero positivo más pequeño que no es producto de primos, tanto a como b deben ser productos de primos. Sin embargo, un producto de primos multiplicado por un producto de primos es un producto de primos, así que $n = ab$ es un producto de primos. Concluimos que cualquier entero n puede ser expresado como un producto de primos. ■

Cerca del 200 a. c. el griego Eratóstenes ideó un algoritmo para calcular números primos, más conocido como la *criba* de Eratóstenes.

Durante la Edad Media, se da un gran vacío en la historia de las ciencias, por lo que los avances en todas las áreas del conocimiento estaban supeditadas a la fé por sobre el razocionio y el intelecto, razón por la que el desarrollo de la matemática se lleva a cabo, de forma exclusiva, en monasterios y abadías.

1.4.1. Números primos y Criptografía

El teorema Fundamental de la Aritmética es un resultado de existencia: nos dice que para cada número existe una manera de escribirlo como producto de números primos pero no nos señala cómo hacerlo. Si consideramos un número natural "pequeño", digamos 3.780, podemos descomponerlo fácilmente en producto de primos haciendo divisiones sencillas:

$$3780 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7.$$

Se podría pensar que esta operación, ejercicio habitual en la enseñanza general básica, se puede hacer con cualquier número. Esto no es así ni mucho menos. En general, encontrar los números primos que dividen a un número dado es un problema muy difícil, y no sólo desde un punto de vista teórico, sino también computacional; es decir, que ni el computador más potente puede encontrar 4 divisores primos de un número "grande"en un tiempo razonable, tanto es así que muchos métodos de codificación de información usan este hecho.

Los primeros sistemas de transmisión de mensajes secretos se basaban en el intercambio de una clave entre el emisor y el receptor con un contacto directo previo. Esto, en comunicaciones a grandes distancias no era muy práctico ya que hacía necesario que emisor y receptor se junten cada vez que, por motivos de seguridad, obligaban a cambiar la clave. En 1977, Rivest, Shamir y Adleman, científicos del MIT (Masachussests Institute of Technology) en EE.UU, idearon un esquema de cifrado de clave pública. Según este método, llamado RSA por las iniciales de los apellidos de sus creadores, el receptor hace público un número natural "grande", del cual conoce su descomposición en factores primos; este número es usado por el emisor para cifrar sus mensajes. La idea es que aunque todo el mundo tiene acceso a la clave pública y al mensaje cifrado, éste sólo pueden ser descifrado si se conocen los números primos que dividen al número clave. Para que nos hagamos una idea de qué significa "grande", actualmente se considera segura una clave pública dada por un número natural de más de 300 cifras. Por supuesto, a medida que evolucionan las capacidades de los ordenadores, la idea de lo que es un número "grande"va cambiando.

1.4.2. GIMPS

En la última década del siglo de la ciencia, un avance tecnológico revoluciona el mundo de las telecomunicaciones: Internet. Nacida a partir de una idea del ejército americano apenas 20 años antes, la red de redes pasa rápidamente al ámbito universitario y el fenómeno es entonces imparable. Pronto las instituciones de todo el mundo están conectadas y el número de hogares con acceso a Internet crece de manera exponencial. Con millones de ordenadores conectados entre sí, el siguiente paso natural en la búsqueda de primos-récords es la colaboración en Internet. George Woltman, programador y entusiasta de la Teoría de Números,

empieza a finales de 1995 a recopilar toda la información existente relativa a los primos-récords. También crea un programa optimizado para la búsqueda de primos de Mersenne y lo cuelga en la red. Así empieza el proyecto GIMPS (Great Internet Mersenne Prime Search). La idea es que colaboradores de todo el mundo operen sobre una base de datos central. La automatización final del proceso de participación es realizada a finales de 1997 por Scott Kurowski.

Desde entonces, basta con un ordenador personal y un módem para participar en la histórica búsqueda de los números primos.

1.5. Estructura de Anillo

Los ejemplos conocidos de conjuntos de números muestran que debe ser muy importante el estudio de conjuntos, en los que se hayan definido dos operacionees binarias. El sistema mas general de este tipo que estudiaremos aquí, es el de anillo.

Definición 1.4 *Un* anillo $(\Re, +, \cdot)$ *es un conjunto* $\Re$ *junto con dos operaciones binarias* $+$ *y* $\cdot$*, que llamamos suma y multiplicación, definidas en* $\Re$ *tales que se satisfacen los siguientes axiomas:*

- $(\Re, +)$ *es un grupo abeliano.*
- *La multiplicación es asociativa.*
- *Para todas las* $a, b, c \in \Re$*, se cumple la* ley distributiva izquierda $a(b+c) = (ab) + (ac)$ *y la* ley distributiva derecha $(a + b)c = (ac) + (bc)$.

Teorema 1.17 *Si* $\Re$ *es un anillo con identidad aditiva 0 entonces, para cualquier* $a, b \in \Re$*, tenemos*

1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$,
3. $(-a)(-b) = ab$.

Demostración.

1. Si $a \in \Re$, entonces $a0 = a(0 + 0) = a0 + a0$ (según la Ley Distributiva Derecha), y como $\Re$ es un grupo respecto a la adición, esta ecuación implica que $a0 = 0$.

   Análogamente, $0a = (0 + 0)a = 0a + 0a$, usando la Ley Distributiva Izquierda, de donde, también aquí se sigue que $0a = 0$.

2. Para probar que $a(-b) = -(ab)$ debemos mostrar que $ab+a(-b) = 0$. Pero $ab+a(-b) = a(b+(-b) = a(0) = 0$ según el uso de la Ley Distributiva y el resultado de la parte (1) de este lema. Análogamente $(-a)b = -(ab)$.

3. Que $(-a)(-b) = ab$ es en realidad un caso particular de la parte (2); lo remarcaremos porque su análogo en el caso de los números reales ha sido también subrayado en nuestra educación en la escuela. Tenemos con él

$$\begin{aligned} (-a)(-b) &= -(a(-b)) && \text{por la parte (2)} \\ (-a)(-b) &= -(-(ab)) && \text{por la parte (2)} \\ (-a)(-b) &= ab \end{aligned}$$

pues $-(-x) = x$ es una consecuencia del hecho de que en cualquier grupo $(u^{-1})^{-1} = u$.

■

Es necesario que se comprenda que, en el estudio de cualquier tipo de estructura matemática, una idea de importancia básica es el concepto de que dos sistemas que son estructuralmente idénticos, esto es, que uno sea exactamente como el otro, excepto por los nombres. En álgebra, siempre se llama a este concepto isomorfismo. El concepto de que dos anillos sean el mismo, excepto por el nombre de los elementos,nos conduce, como en el caso de los grupos, a la siguiente definición.

Definición 1.5 *un isomorfismo ϕ de un anillo $\Re$ con un anillo $\Re'$ es una función uno a uno que transforma $\Re$ sobre $\Re'$ tal que para todas las $a, b \in \Re$*

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

Entonces, los anillos $\Re$ y $\Re'$ son isomorfos.

Definición 1.6 *Si a y b son dos elementos distintos de cero de un anillo $\Re$ tal que $ab = 0$, entonces a y b son* divisores *de 0. En particular, a es un* divisor izquierdo *de 0 y b es un* divisor derecho *de 0.*

En un anillo conmutativo, todo divisor izquierdo de 0 es también un divisor derecho de 0 y recíprocamente. Así, no hay distinción entre divisores izquierdo y derecho de cero en un anillo conmutativo.

Definición 1.7 *Sea $\Re$ un anillo e I un conjunto, tal que $I \subset \Re$. Se dice que I es un* ideal *en $\Re$ si cumple las siguientes propiedades:*

1. $0 \in I$.
2. *Si $a, b \in I$, entonces $a - b \in I$.*
3. *Si $a \in \Re$ y $b \in I$, entonces $a \cdot b \in I$ (*ideal a derecha*) o $b \cdot a \in I$ (*ideal a izquierda*).*

Con respecto al segundo ítem, aclaramos que un subconjunto de un anillo se dice que es un ideal si forma un subgrupo aditivo con respecto al grupo aditivo abeliano de todo anillo. Para el tercer ítem, simplemente señala que el producto entre los elementos del subconjunto y cualquier elemento del conjunto, pertenece al subconjunto en cuestión.

En el tercer ítem, aclaramos que si $\Re$ es un anillo conmutativo, entonces $a \cdot I = I \cdot a \in I$ y se denomina *ideal invariante*.

Ejemplo 1: Los ideales I del anillo Z_{12} son los siguientes conjuntos:

- $I_1 = \{0\}$
- $I_2 = \{0, 2, 4, 6, 8, 10\}$
- $I_3 = \{0, 3, 6, 9\}$
- $I_4 = \{0, 4, 8\}$
- $I_5 = \{0, 6\}$
- $I_6 = Z_{12}$

donde claramente se observa que las sumas en módulos en cada uno de los subconjuntos forma un subgrupo aditivo abeliano, y que el producto por cualquier elemento de Z_{12} sigue perteneciendo a los ideales señalados.

Podemos identificar que en todo anillo $\Re$ se tienen, al menos, los siguientes ideales: 0 y $\Re$. Se conocen como ideales *impropios*; específicamente el ideal 0 se denomina *trivial*.

Ejemplo 2: A partir del Ejemplo 1, los ideales impropios de Z_{12} son I_1 I_6

Una observación trivial es que si un ideal I de un anillo $\Re$ contiene una unidad u, entonces $I = \Re$. En efecto, por definición de ideal se tiene que $1 = u \cdot u^{-1} \in I$ y si $a \in \Re$, entonces $a = a \cdot 1 \in I$, es decir, todo elemento de $\Re$ está contenido en I.

Teorema 1.18 *Sea $(I_i)_{i\in\Lambda}$ una familia de ideales en un anillo $\Re$. Entonces la intersección de la familia de ideales, definia por $\bigcap_{i\in\Lambda} I_i$ es también un ideal de $\Re$.*

Demostración. Sean $a, b \in \bigcap_{i\in\Lambda} I_i$, $r \in \Re$. Entonces para todo $i \in \Lambda$, $a - b \in I_i$, y $ar(ar) \in I_i$, debido a que los I_i son ideales. De este modo $a - b$ y $ar(ar)$ pertenecen a $\bigcap_{i\in\Lambda} I_i$, probando que esta intersección es un ideal de $\Re$. ■

Definición 1.8 *Sea X un subconjunto de $\Re$ y sea $\Im = I/I$ es un ideal de $\Re$ que contiene a X, donde $\Im \neq$ debido a que $\Re \in \Im$. Sea $A = \bigcap_{I\in\Im} I$. Entonces A es el menor ideal de $\Re$ que contiene a X y se denota por (X). El menor ideal de $\Re$ que contiene un subconjunto X se llama* ideal generado *por X. También se dice que el conjunto X es un* generador *de (X).*

Así, para todo subconjunto X de $\Re$ tenemos que (X) es un ideal de $\Re$, $X \subset (X)$ y si I es un ideal de $\Re$ tal que $X \subset I$, entonces $(X) \subset I$. Otro hecho evidente es que si $X \subset Y \subset \Re$, entonces $X \subset (Y)$, luegoo $(X) \subset (Y)$.

Definición 1.9 *Un ideal I de un anillo $\Re$ se dice que es* finitamente generado *si I es finito.*

Definición 1.10 *Sea I un ideal en un anillo $\Re$. Se dice que I es un* ideal principal *si está generado por un solo elemento, es decir, si es de la forma $(i) = i\Re = \{ir/r \in \Re\}$, donde $i \in \Re$.*

Ejemplo 3: Del Ejemplo 1, podemos señalar que todos los ideales de Z_{12} son ideales principales:

- $I_1 = \{0\}$, donde $(0) = 0Z_{12}$.
- $I_2 = \{0, 2, 4, 6, 8, 10\}$, donde $(2) = 2Z_{12}$.
- $I_3 = \{0, 3, 6, 9\}$, donde $(3) = 3Z_{12}$.
- $I_4 = \{0, 4, 8\}$, donde $(4) = 4Z_{12}$.
- $I_5 = \{0, 6\}$, donde $(6) = 6Z_{12}$.
- $I_6 = Z_{12}$, donde $(1) = Z_{12}$.

La importancia del concepto de ideal es que en él radica la estructura idónea para expresar los hechos más importantes de la existencia de divisibilidad en anillos. Para ejemplificar esto, notemos que si a es un elemento de un anillo A, entonces el ideal $(a) = Aa$ es el conjunto de todos los múltiplos de a. Por lo tanto, si $a|b$ equivale a decir de que $(b) \subset (a)$.

Ejemplo 4: Claramente, a partir del Ejemplo 1, Podemos señalar que, en efecto, 2 divide a 4, pero $(2) = 2Z_{12}$ y $(4) = 4Z_{12}$, luego $(4) \subset (2)$.

Teorema 1.19 *Si A es un dominio de integridad, un ideal P de A es primo sí y sólo sí $P \neq A$ y para todo par de elementos a, b de A, si $ab \in A$ entonces $a \in P$ o $b \in P$.*

Demostración. Si P es primo y $ab \in P$, entonces $(a)(b) \subset (ab) \subset P$, de donde resulta que $(a) \subset P$ o $(b) \subset P$, es decir, $a \in P$ o $b \in P$. De forma recíproca, si $(ab) \subset P$, pero $(a)P$, entonces existe un $a_i \in (a)$. Ahora bien, si $b_i \in (b)$, tenemos que $a_i b_i \in (ab)P$, luego $a_i \in P$ o $b_i \in P$, y debe ser $b_i \in P$, es decir, $(b) \subset P$. ■

Definición 1.11 *Un ideal I de un anillo conmutativo $\Re$ es* maximal *si no existe en $\Re$ ningún ideal propio que contenga a I.*

Definición 1.12 *Un ideal I de un anillo conmutativo $\Re$ es* primo*, si $ab \in I$ para cualquier par de elementos $a, b \in \Re$, entonces $a \in I$ ó $b \in I$.*

Para comprender mejor el concepto de divisibilidad en Z, en particular, y en anillos, en general, se debe tener presente que los ideales principales representan mejor que los propios elementos del anillo cuales son los posibles divisores de un elemento. Esta situación la veremos en detalle, cuando generalicemos la idea de divisibilidad para dominios de integridad.

Definición 1.13 *Si I es un ideal en un anillo $\Re$, entonces, al anillo de las clases laterales $r + I$ bajo las operaciones inducidas es el* anillo cociente *y se denota por $\Re/I$.*

Como veremos en más profunidad en el transcurso de nuestro estudio, esta estructura nos será de gran utilidad para conceptualizar congruencias en el sentido de la teoría elemental de números, puesto que las clases laterales formadas en anillos cocientes son las clases residuales módulo i, donde $(i) = I$.

CAPÍTULO 2

Dominios de Integridad

Una de las propiedades algebraicas más importantes de nuestro sistema numérico usual es que el producto de dos números puede ser 0 sólo si al menos uno de los dos factores es cero. Se suele usar con frecuencia este hecho, incluso de manera inconsciente.

En el siguiente capítulo trataremos la estructura de dominio de integridad, las condiciones en que se puede definir una divisibilidad en elementos de un determionado conjunto e importantes resultados que permitirán reconocer esta generalidad asociada al clásico ejemplo de los números enteros.

2.1. Definiciones

Definición 2.1 *Un* dominio de integridad, dominio íntegro, anillo íntegro*, o sencillamente* dominio*, es un anillo* $(\Re, +, \cdot)$ *que carece de elementos* divisores de cero *por la izquierda y de elementos divisores por la derecha.*

En la literatura matemática antigua se sobreentiende que el anillo es conmutativo y unitario, porque se ignoraba la existencia de anillos no conmutativos que no tuvieran divisores de cero (por la izquierda o por la derecha). Los dominios de Mal´cev son un tipo de anillos no conmutativos que carecen de elementos divisores de cero.

Teorema 2.1 *En el anillo* Z_n *los divisores de* 0 *son precisamente aquellos elementos que no son primos relativos con* n*.*

Demostración. Sea $m \in Z_n$, donde $m \neq 0$, y sea $d \neq 1$ el mcd de m y n. Entonces,

$$m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right) n$$

lo cual da 0 como múltiplo de n. Así, $m(\frac{n}{d}) = 0$ en Z_n, mientras que ni m ni $\frac{n}{d}$ es 0, así que m es un divisor de cero. ■

Teorema 2.2 *Si p es primo, entonces Z_p no tiene divisores de* 0.

Demostración. Sea $m \in Z_p$, donde $m \neq 0$. Entonces $mp = pm = 0$ como múltiplos de p. Como m no tiene factores comunes con p mayores que 1, se prueba que Z_p no tiene divisores de 0. ■

Otra de las importancias del concepto de divisores de 0 se muestra en la siguiente

Definición 2.2 *Sea $\Re$ un anillo y sean $a, b, c \in \Re$. Las Leyes de cancelación valen en $\Re$ si $ab = ac$ con $a \neq 0$, implica $b = c$ y $ba = ca$ con $a \neq 0$ implica $b = c$. Estas son las leyes de cancelación multiplicativas. Es claro que las leyes de cancelación aditiva valen en $\Re$, pues $(\Re, +)$ es un grupo.*

Teorema 2.3 *Las leyes de cancelación valen en $\Re$ si y sólo si $\Re$ no tiene divisores de* 0*, izquierdos ni derechos.*

Demostración. Sea $\Re$ un anillo en el cual se cumplen las leyes de cancelación y supoóngase que $ab = 0$ para elementos $a, b \in \Re$, Debemos probar que $a = 0$ ó $b = 0$. Si $a \neq 0$, entonces $ab = a0$ implica que $b = 0$, por las leyes de cancelación, De forma análoga, $b \neq 0$ implica que $a = 0$, de forma que no puede existir divisores izquierdos ni derechos de 0, si las leyes de cancelación se cumplen.

Por otro lado, supongamos que $\Re$ no tiene divisores izquierdos ni derechos de 0 y supongamos que $ab = ac$ con $a = 0$. Entonces, $ab - ac = a(b - c) =$. Como $a = 0$ y $\Re$ no tiene divisores izquierdos de 0, debemos tener que $b - c = 0$, de modo que $b = c$. Un argumento similar se puede utilizar para el caso análogo con divisores derechos. ■

Así, si los coeficientes de un polinomio pertenecen a un dominio entero, podemos resolver una ecuación polinomial en la cual se pueda factorizar el polinomio en factores lineales, haciendo, como es usual, cada factor igual a 0.

Un dominio de integridad es una estructura que está entre un anillo conmutativo con unitario y un campo, si podemos jerarquizar las estructuras algebraicas. El Teorema 2.3 muestra que las leyes de cancelación para la multiplicación se cumplen en un dominio entero. Hemos visto que Z y Z_p para cualquier primo p son dominios enteros, pero Z_n no es un dominio entero si n no es primo.

Teorema 2.4 *Todo campo F es un dominio de integridad.*

Demostración. Sea $a, b \in F$, supóngase que $a \neq 0$. Entonces, si $ab = 0$ tenemos

$$\left(\frac{1}{a}\right)(ab) = \left(\frac{1}{a}\right)0 = 0$$

Pero entonces,

$$0 = \left(\frac{1}{a}\right)(ab) = \left[\left(\frac{1}{a}\right)a\right]b = 1b = b$$

Hemos mostrado que $ab = 0$ con $a \neq 0$ implica que $b = 0$ en F, de modo que no existan divisores de 0 en F. Es claro que F es un anillo conmutativo con unitario y así, queda probado el teorema. ■

Definición 2.3 *: Sea D un dominio de integridad. Se dice que D es* ordenado *si D contiene un subconjunto D^+ dotado de las siguientes propiedades:*

1. *D^+ es cerrado con respecto a la adición y multiplicación definidas sobre D.*
2. *Para todo $a \in D$ se verifica una, y solo una de las siguientes relaciones:*

$$a = 0 \qquad a \in D^+ \qquad -a \in D^+$$

Los elementos de D^+ se dicen elementos positivos *de D; todos los elementos no nulos de D se dicen elementos* negativos *de D.*

2.2. Dominios de Factorización Única

Definición 2.4 *Sea D un dominio de integridad y $a, b \in D$. Si existe $c \in D$ tal que $b = ac$, entonces a* divide *b (o a es un* factor *de b) y se denota por $a|b$.*

Si nos damos cuenta, esta definición es muy similar a las ya mencionadas para definir cuándo un entero es divisible por otro. Usaremos la simpleza de esos hechos para utilizarlos en una estructura más general.

Definición 2.5 *. Un elemento u de un dominio de integridad D es* una unidad de D *si u divide a 1, esto es, si u tiene inverso multiplicativo en D. Dos elementos $a, b \in D$ son* asociados en D *si $a = bu$, donde u es una unidad en D.*

La condición $a = bu$ para que los elementos $a, b \in D$ sean asociados no es formalmente simétrica, si $a = bu$, entonces $b = au^{-1}$, donde u^{-1} existe y es una unidad de D, ya que u es una unidad de D.

Definición 2.6 *Un elemento p distinto de cero que no sea unidad de un dominio de integridad D es un irreducible de D, si en cualquier factorización $p = ab$ en D, a ó b es unidad.*

Definición 2.7 *Un dominio de interidad D es un* dominio de factorización única *(DFU), si se satisfacen las siguientes condiciones:*

1. *Todo elemento de D que no sea ni 0 ni una unidad, se puede factorizar en un número finito de irreducibles.*
2. *Si $p_1 \cdots p_r$ y $q_1 \cdots q_s$ son dos factorizaciones en irreducibles del mismo elemento de D, entonces $r = s$ y los q_j pueden renumerarse de manera que p_i y q_i sean asociados.*

Teorema 2.5 *Si D es un DFU, entonces la factorización para cualquier elemento en D como un producto finito de factores irreducibles es única salvo el orden o factores que son unidades en D.*

Demostración. Por definición de DFU, $a = p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_n$, donde p_i y q_i son irreducibles, entonces $m = n$, y al renumerar los q_i, tenemos que p_i y q_i son asociados, con $i = 1, 2, \ldots, m$.

Debido a la misma definición, resulta trivial para factorizaciones de elementos irreducibles, y asumimos que esto es verdadero para cualquier elemento de D que puede ser factorizado en s factores irreducibles.

Entonces probaremos que es verdadero para cualquier elemento en D que puede factorizarse en $s + 1$ factores irreducibles.

Sean

$$\begin{aligned} a &= \prod_{i=1}^{s+1} p_i \\ &= \prod_{j=1}^{m} p'_i \end{aligned} \tag{2.1}$$

dos factorizaciones de a en irreducibles, uno de los cuales posee exactamente $s + 1$ factores.

Tenemos que p_i divide el producto de los p'_j, y por tanto, dada la segunda condición de la definición de DFU, p_i debe dividir uno de los elementos $p'_1, p'_2, \ldots, p'_m$. Supongamos que p_1 divide a p'_k, con $1 \leq k \leq m$. Debido a que p'_k es irreducible, entonces p_1 y p'_k son asociados. Entonces $p'_k = up_1$, donde u es una unidad en D, y luego de cancelar el factor común en (2.1), se tiene que:

$$\prod_{i=2}^{s+1} p_i = u \prod_{j=1,\ j\neq k}^{m} p'_j \tag{2.2}$$

En consecuencia, por hipótesis de inducción, las dos factorizaciones en (2.2) pueden diferir solo en el orden de los factores. Debido a que ya sabemos que p_1 y p'_k difieren por una unidad como factor, hemos probado el teorema. ■

Definición 2.8 *Un elemento d en un dominio de integridad D es llamado* máximo común divisor *de los elementos a y b en D si cumple las siguientes propiedades:*

1. *$d|a$ y $d|b$*
2. *Si para algún $c \in D$, tal que $c|a$ y $c|b$, entonces $c|d$.*

Teorema 2.6 *Sea D un DFU y $a, b \in D$. Entonces, existe un máximo común divisor de a y b, que es determinado únicamente, a lo menos, por un factor unidad arbitrario.*

Demostración. Escribamos

$$\begin{aligned} a &= p_1^{e_1} \cdot p_2^{e_2} \cdots p_m^{e_m} \\ b &= p_1^{f_1} \cdot p_2^{f_2} \cdots p_m^{f_m} \end{aligned}$$

donde p_i son irreducibles, e_i y f_i son enteros no negativos, y donde p_i^0 diremos que significa una unidad en D. Señalemos que $g_i = min(e_i, f_i)$, con $i = 1, 2, ..., m$ y $d = p_1^{g_1} \cdot p_2^{g_2} \cdots p_m^{g_m}$. Entonces, claramente $d|a$ y $d|b$. Sea $c \in D$ tal que $c|a$ y $c|b$.

Entonces $c|a$ implica que

$$c = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdots p_m^{\lambda_m}$$

donde λ_i, con $i = 1, 2, ..., m$ son enteros no negativos. Pero entonces $c|a$ y $c|b$ implica, por teormea de DFU, que $\lambda_i \leq e_i$ y $\lambda_i \leq f_i$; $i = 1, 2, ..., m$. En consecuencia, $\lambda_i \leq min(e_i, f_i) = g_i$. Esto prueba que $c|d$, como se deseaba.

Ahora, supongamos que d y d' son dos máximos comunes divisores de a y b. Entonces $d|d'$ y $d'|d$ son asociados, dado que D es un dominio de integridad conmutativo. ■

2.3. Dominios de Ideales Principales

Definición 2.9 *Un dominio de integridad D es un* dominio de ideales principal *(DIP), si todo ideal en D es un ideal principal.*

En el capítulo anterior señalamos brevemente la importancia del concepto de ideal. El hecho de que existan dominios cuyos ideales sean principales, significa que basta limitarse a estudiar sus generadores para conocer propiedades de divisibilidad importantes para los dominios. Consideremos las siguientes afirmaciones, en el ánimo de ejemplificar estas ideas: sabemos que $3|6$ y que $-3|6$. Estas afirmaciones, para efectos de divisibilidad en dominios de integridad son equivalentes, puesto que 3 y -3 son asociados. Podemos resumirla en una sola si consideramos que es el ideal $(3) = (-3)$ el que divide a 6, y podemos escribir $(3)|6$. Podemos pensar que los divisores de un dominio de integridad no son otros elementos del dominio, sino sus ideales.

En el caso de los Dominios de Ideales Principales, cada "divisor ideal" se corresponde con una familia de "divisores reales" asociados, que son sus generadores. Estos "divisores ideales" resultaron escenciales para formular y estructurar una teoría de divisibilidad en anillos de estas características. Como señalamos anteriormente, el concepto moderno de ideal fue construido muy tardiamente en la teoría algebraica de números, y su introducción la debemos a Dedekind[1] a finales del siglos XIX, para formalizar la idea de divisor ideal que no se corresponde con ningún divisor real.

[1] Dedekind, Richard (1832-1916), Matemático alemán. Fue uno de los primeros matemáticos en comprender el significado fundamental de las nociones de grupo, cuerpo, ideal en el campo del álgebra, la teoría de números y la geometría algebraica.

A continuación, demostraremos el siguiente resultado, que integra los conceptos de dominio de factorización única con el de dominio de ideales principales.

Teorema 2.7 *: Todo DIP es un DFU, pero un DFU no necesariamente es un DIP.*

Demostración. Primero, mostraremos que si D es un DIP, entonces D no tiene una cadena infinita de ideales ascendente. Por tanto, sea

$$n_1D \subseteq n_2D \subseteq \dots$$

una cadena de ideales ascendente en D. Sea $N = \bigcup n_iD$ y $m, n \in N$ y $d \in D$. Entonces $m \in n_iD$ $n \in n_jD$ para algunos i, j.

Ahora, como podemos tener las siguientes opciones

$$n_iD \subset n_jD \text{ o } n_jD \subset n_iD$$

con ambos m y n, esto es falso en uno de los dos ideales n_iD y n_jD, supongamos en n_jD, y decimos que $n_jD \subset n_iD$.

Entonces $m - n \in n_iD \subset N$. Además, $nd \in n_iD \subset N$. En consecuencia, N es un ideal en D. Dado que D es DIP, $N = nD$, para algún $n \in D$. Ahora, $n \in N$ implica que $n \in n_kD$ para algún k. Más aún, $N = nD \subset n_kD \subset N$ dado que $N = nD = n_kD$; en consecuencia, $n_kD = n_{k+1}D = \dots$, probando nuestra afirmación.

Siguiendo, mostraremos que cada elemento $n \in D$ es un producto finito de elementos irreducibles. Si n es irreducible, la afirmación es evidente. Nos interesa el caso en que $n = ab$ tal que $a, b \in D$, donde ni a ni b sean unidades en D. Si tanto a y b son productos de elementos irreducibles, también es obvia la afirmación.

Pero, supongamos que a no es un producto de elementos irreducibles, y escribimos que $a = xy$ con $x, y \in D$, donde x no es un producto de elementos irreducibles. Este proceso induce a una cadena de ideales ascendente $(n) \subset (b) \subset (x) \subset \dots$ que continua de forma indefinida si n no es un producto finito de elementos irreducibles. Pero D no posee una cadena ascendente de ideales infinita, por lo que concluimos que n debe ser un producto finito de elementos irreducibles.

Para finalizar, sean

$$n = p_1p_2 \cdots p_r \text{ y } n = q_1q_2 \cdots q_s$$

donde p_j y q_j son irreducibles en D. Entonces tenemos que $p_1|(q_1q_{2s})$, lo cual implica que $p_1|q_{j_1}$ para alguna j_1. Al intercambiar, si es necesario, el orden de las q_j, podemos suponer que $j_1 = 1$ ó $p_1|q_1$. Entonces $q_1 = p_1u_1$ y, como p_1 es un irreducible en D, u_1 es una unidad en D, de modo que p_1 y q_1 son asociados. Tenemos entonces que

$$p_1p_2 \cdots p_r = p_1u_1q_2 \cdots q_s$$

de modo que por las leyes de cancelación en D,

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s$$

Al continuar este proceso, comenzando con p_2 y de forma sucesiva, se obtiene por último

$$1 = u_1 u_2 \cdots u_r q_{r+1} \cdots q_s$$

Como las q_j son irreducibles, debemos tener que $r = s$, con lo cual, la factorización es única, salvo por el orden y cambio por asociados. De este modo, hemos probado que un DIP es un DFU. ■

Para finalizar con este capítulo, extenderemos la noción de dominio de ideales principales bajo el siguiente concepto, que desarrolla una teoría de divisibilidad en dominios de integridad mucho más fina y detallada.

Definición 2.10 *Un anillo $\Re$ es un anillo* noetheriano[2] *si todo ideal de $\Re$ es finitamente generado.*

Evidentemente, todo dominio de ideales principales es un anillo noetheriano.

Teorema 2.8 *: Sea D un dominio de integridad. Son equivalentes:*

1. *D es un anillo noetheriano.*
2. *Para toda cadena ascendente de ideales de D*

   $$I_0 \subset I_1 \subset I_2 \subset I_3 \subset \ldots$$

   existe un número natural n tal que $I_n = I_m$ para todo $m \geq n$.
3. *Toda familia de ideales de D tiene un maximal para la inclusión.*

Demostración.

1. Si $I_0 \subset I_1 \subset I_2 \subset I_3 \subset \ldots$ es una cadena ascendente de ideales de D, es fácil ver que la unión

   $$\bigcup_{i=0}^{\infty} I_i$$

   también es un ideal de D.

   Si D es noetheriano, tiene un generador finito X. Cada elemento de X está en uno de los ideales de I_i, y como X es finito y los ideales forman una cadena, existirá un natural n tal que $X \subset I_n$, pero entonces

   $$\bigcup_{i=0}^{\infty} I_i = (X) \subset I_n$$

   lo que implica que $I_i = I_n$ para todo $i \geq n$. Por tanto (1) implica (2).

[2]Noether, Amalia Emmy (1882-1935), Matemática alemana, reconocida por su trabajo en Álgebra Moderna y Teoría de Números.

2. Si una familia de ideales de D no tuviera maximal, sería posible extraer una cadena ascendente de ideales que contradijera (2). Luego (2) implica (3).

3. Si D tuviera un ideal I que no tenga un generador finito, entonces, dado cualquier elemento $a_0 \in I$, se cumple que $(a_0) \neq I$, luego existe un elemento $a_1 \in I$ tal que $a_1|(a_0)$, luego

$$(a_0) \subset (a_0, a_1) \neq I,$$

y de esta forma podemos conseguir una cadena de ideales

$$(a_0) \subset (a_0, a_1) \subset (a_0, a_1, a_2) \subset \ldots$$

sin que ninguno de ellos sea maximal. Por lo tanto (3) implica (1).

■

CAPÍTULO 3

Dominios de Integridad Especiales

3.1. Dominios Euclidianos

Definición 3.1 *Una evaluación euclideana en un dominio entero D es una función v que transforma a los elementos distintos de cero de D, en los enteros no negativos tal que se satisfacen las condiciones siguientes:*

1. *Para todos los $a, b \in D$ con $b \neq 0$ existen q y r en D tales que $a = bq + r$, donde $r = 0$ o $v(r) \leq v(b)$.*

2. *Para todos los a, $b \in D$, donde ni a, ni b es 0, $v(a) \leq v(ab)$*

Un dominio entero D es un dominio euclideano si existe una evaluación euclideana en D

Ejemplo 3.2 *El anillo de los enteros Z con la función $d(x) = |x|$ es un Dominio Euclideano. La propiedad (1) es consecuencia inmediata de la definición de valor absoluto para números enteros y la propiedad (2) es precisamente el algoritmo de división para los enteros.*

Teorema 3.1 *Todo dominio euclideano es un DIP.*

Demostración. Sea D un dominio euclideano con evaluación euclideana v y sea N un ideal en D. Si $N = \{0\}$, entonces $N = \langle 0 \rangle$ y N es principal. Supóngase que $N \neq \{0\}$. Entonces, existe $b \neq 0$ en N. Escojamos b tal que (b) sea minimal de entre todas las $v(n)$ para $n \in N$. afirmamos que $N = \langle b \rangle$. Sea $a \in N$. Entonces, por la condición (1) para un dominio euclideano, existen q y r en D tales que

$$a = bq + r,$$

donde $r = 0$ o $v(r) < v(b)$. Ahora, $r = a - bq$ y $a, b \in N$, de modo que $r \in N$ puesto que N es un ideal. Así, es imposible que $v(r) < v(b)$ debido a nuestra selección de b. De aquí, $r = 0$, de modo que $a = bq$. Como a es cualquier elemento de N, vemos que $N = \langle b \rangle$. ■

Corolario 3.2 *Un dominio euclideano es un DFU.*

Demostración. Por el teorema anterior, se concluye entonces, que un dominio euclideano es un DIP, y por el Teorema (2,7) un DIP es un DFU. ■

Algunas de las propiedades de los Dominios Euclideanos se relacionan con su estructura multiplicativa. Es necesario aclarar, que la estructura aritmética de un Dominio Euclideano es *intrínsica al dominio* y no se ve afectado de modo alguno por una evaluación euclideana v en el dominio. La evaluación euclideana, no es más que una herramienta que pudiese arrojar alguna luz dobre esta estructura aritmética del dominio. La estructura aritmética de un dominio D está por completo determinada por el conjunto D y las operaciones binarias $+$ y $\cdot$ en D.
Siendo D un Domino Euclideano con evaluación euclideana v, se puede utilizar la propiedad (2) de una evaluación euclideana para caracterizar las unidades de D.

Teorema 3.3 *Para un dominio euclideano con evaluación euclideana v, $v(1)$ es minimal entre todas las $v(a)$ para $a \in D$ distinta de 0 y $u \in D$ es unidad si y sólo si $v(u) = v(1)$.*

Demostración. La condición 2 para v, nos dice que para $a \neq 0$

$$v(1) \leq v(1a) = v(a).$$

Por otro lado, si u es unidad en D, entonces

$$v(u) \leq v(uu^{-1}) = v(1).$$

Así,

$$v(u) = v(1)$$

para una unidad u en D.

En forma recíproca, supóngase que $u \in D$ distinto de cero es tal que $v(u) = v(1)$. Entonces, por el algoritmo de la división, existen q y r en D tales que

$$1 = uq + r,$$

donde $r = 0$ o $v(r) < v(u)$. Pero como $v(u) = v(1)$ es minimal entre todas las $v(d)$ para $d \in D$ distinto de cero, es imposible que $v(r) < v(u)$. De aquí, $r = 0$ y $1 = uq$ de modo que u es unidad. ■

Ejemplo 3.3 *Para Z con $v(n) = |n|$, el mínimo de $v(n)$ para $n \in Z$ distinto de cero, es 1. Es claro que 1 y -1 son los únicos elementos de Z con $v(n) = 1$. Por supuesto, el 1 y el -1 son las unidades de Z.*

Hasta el momento, todo lo demostrado aquí se cumple para todo dominio euclideano. Probaremos ahora algunos resultados clásicos acerca de máximos comunes divisores, en un dominio euclideano.

Definición 3.4 *sea D un DFU. Un elemento $d \in D$ es un máximo común divisor(mcd) de los elementos a y b en D si d/a, d/b y además, c/d para todos los c que dividan a y b.*

Teorema 3.4 *Si D es un DIP y a y b son elementos distintos de cero de D, entonces existe algún mcd de a y b. Más aún, cada mcd de a y b puede espresarse en la forma $\lambda a + \mu b$ para algunos $\lambda, \mu \in D$.*

Demostración. Considérese el conjunto

$$N = \{ra + sb | r, s \in D\}$$

como

$$(r_1 a + s_1 b) \pm (r_2 a + s_2 b) = (r_1 \pm r_2)a + (s_1 \pm s_2)b$$

y

$$t(ra + sb) = (tr)a + (ts)b$$

para $t \in D$, es inmediato que N es un ideal de D. Ahora, $N = \langle d \rangle$ para algún $d \in D$. Entonces, $d|(ra + sb)$ para todas las $r, s \in D$ y, tomando primero $s = 0$ con $r = 1$, y después $r = 0$ con $s = 1$, vemos que $d|a$ y $d|b$. además, si $c|a$ y $c|b$, entonces $c|(ra + sb)$ para todas las $ra + sb$, esto es, $c|n$ para todas las $n \in N$. De aquí que $c|d$. Así, d es un mcd de a y b. Para d, tal como se acaba de constuir, $d \in N$ implica que exiten $\lambda, \mu \in D$ tales que $d = \lambda a + \mu b$. Pero la definición de mcd muestra que si d_1, también es un mcd de a y b, entonces $d|_1$, y $d_1|d$. Así,

$$d_1 = vd = (v\lambda)a + (v\mu)b = \lambda_1 a + \mu_1 b$$

■

En un Dominio Euclideano D, dado cualquier par de elementos a y b, el Máximo Común Divisor entre ellos siempre existe, pues D es un Dominio de Ideales Principales. En los Dominios Euclideanos se puede calcular el mcd mediante un algoritmo, llamado Método de Euclides, el cual depende de las propiedades de la función v.

Teorema 3.5 (Algoritmo Euclideano) *Sea D un dominio euclideano con una evaluación euclideana v y sean a y b elementos de D distintos de cero. Sea r_1 como en la condición* (1) *para una evaluación euclideana, esto es,*

$$a = bq_1 + r_1$$

donde $r_1 = 0$ o $v(r_1) < v(b)$. Si $r_1 = 0$, sea r_2 tal que

$$b = r_1 q_2 + r_2,$$

donde $r_2 = 0$ o $v(r_2) < v(r_1)$. En general, sea r_{i+1} tal que

$$r_{i-1} = r_i q_{i+1} + r_{i+1},$$

donde $r_{i+1} = 0$ o $v(r_{i+1}) < v(r_i)$. Entonces, la sucesión $r_1, r_2, ...$ debe terminar con algún $r_s = 0$. Si $r_1 = 0$, entonces b es un mcd de a y b. Si $r_1 \neq 0$ y r_s es el primer $r_i = 0$, entonces, r_{s-1} es un mcd de a y b.

Demostración. Como $v(r_i) < v(r_{i-1})$ y $v(r_i)$ es un entero no negativo, es claro que llegaremos a alguna $r_s = 0$ después de un número finito de pasos.
Si $r_1 = 0$, entonces $a = bq_1$ y, obviamente, b es un mcd de a y b. Supóngase que $r_1 \neq 0$. Entonces, si $d|a$ y $d|b$, tenemos

$$d|(a - bq_1),$$

de modo que $d|r_1$. Sin embargo, si $d_1|r_1$ y $d_1|b$, entonces

$$d_1|(bq_1 + r_1),$$

de modo que $d_1|a$. Así, el conjunto de divisores comunes de a y b es el mismo conjunto que el conjunto de divisores comunes de b y r_1. Por un argumento similar, si $r_2 \neq 0$, el conjunto de divisores de comunes de b y r_1 es el mismo conjunto que el conjunto de divisores comunes de r_1 y r_2. Continuamos con este proceso y, al final, vemos que el conjunto de divisores comunes de a y b es el mismo conjunto que el conjunto de divisores comunes de r_{s-2} y r_{s-1} donde r_s es el primer r_i igual a 0. Así, un mcd de r_{s-2} y r_{s-1} es también un mcd de a y b. Pero la ecuación

$$r_{s-2} = q_s r_{s-1} + r_s = q_s r_{s-1}$$

muestra que un mcd de r_{s-2} y r_{s-1} es r_{s-1} ■

Ejemplo 3.5 *Hallar el mcd*$(345, 20)$
Aplicando el algoritmo euclideano para la división, tenemos entonces

$$345 = 20 \cdot 17 + 5$$

$$20 = 5 \cdot 4$$

luego el mcd$(345, 20) = 5$

3.2. Dominios y Normas Gaussianas

Un Dominio Euclideano muy especial, es el descubierto por el matemático Alemán Carl Friedrich Gauss[1], en relación al problema de determinar que números enteros positivos se pueden expresar como suma de dos cuadrados.

3.2.1. Enteros Gaussianos

Definición 3.6 *Un Entero Gaussiano es un número complejo* $a + bi$ *donde* $a,b \in Z$. *Para un Entero Gaussiano* $\alpha = a + bi$ *la norma* $N(\alpha)$ *de* α *es* $a^2 + b^2$

Denotaremos por $Z[i]$ al conjunto de todos los enteros gaussianos. El lema siguiente da algunas propiedades básicas de la función norma N en $Z[i]$ y conduce a la demostración de que la función v definida por $v(\alpha) = N(\alpha)$ para $\alpha \in Z[i]$ distinto de cero es una evaluación euclideana en $Z[i]$. Nótese que los enteros gaussianos incluyen todos los racionales enteros, esto es, todos los elementos de Z.

[1]Gauss, Carl Friedrich (1777 - 1855), matemático alemán conocido por sus muy diversas contribuciones al campo de la física,la astronomía tanto teórica como práctica, matemática y física matemática, abarcando prácticamente todas sus ramas.

Lema 3.1 *En $Z[i]$ se cumplen las siguientes propiedades de la función norma N para todas las $\alpha, \beta \in Z[i]$:*

1. $N(\alpha) \geq 0$.
2. $N(\alpha) = 0$ *si y sólo si* $\alpha = 0$.
3. $N(\alpha\beta) = N(\alpha)N(\beta)$

Demostración. Las demostraciones de las propiedades (1) y (2), resultan triviales. Procederemos, entonces, a mostrar las indicaciones para la demostración de la propiedad 3.

Sean $\alpha, \beta \in Z[i]$ tal que $\alpha = a_1 + a_2 i$ y $\beta = b_1 + b_2 i$ donde $a_1, a_2, b_1, b_2 \in Z$. Tenemos:

$$\begin{aligned} N(\alpha, \beta) &= N[(a_1 + a_2 i)(b_1 + b_2 i)] \\ &= N[(a_1 b_1 - a_2 b_2) + (a_1 b_2 + a_2 b_1)i] \\ &= (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_2 b_1) \\ &= (a_1^2 + a_2^2)(b_1^2 + b_2^2) \\ &= N(\alpha)N(\beta) \end{aligned}$$

■

Lema 3.2 $\boldsymbol{Z}[i]$ *es un dominio entero.*

Demostración. Es obvio que $Z[i]$ es un anillo conmutativo con unitario. Es necesario mostrar, ahora, que no hay divisores de 0. Sean $\alpha, \beta \in Z[i]$, usando el Lema (3,1) si hay $\alpha\beta = 0$, entonces

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(0) = 0.$$

Así, $\alpha\beta = 0$ implica que $N(\alpha) = 0$ o $N(\beta) = 0$. De nuevo, por el Lema (3,1), esto implica que $\alpha = 0$ o $\beta = 0$. Así, $Z[i]$ no tiene divisores de cero, de modo que $Z[i]$ es un Dominio Entero ■

Es lógico pensar que, como $Z[i]$ es un subanillo de C donde C es el campo de los números complejos, es obvio que $Z[i]$ no tiene divisores de cero. El argumento en el Lema (3,1) ilustró el uso de la propiedad multiplicativa (3) de la función norma N y evitó salir de $Z[i]$ durante la deducción.

Teorema 3.6 *La función v dada por $v(\alpha) = N(\alpha)$ para $\alpha \in \boldsymbol{Z}[i]$ distinto de cero, es una evaluación euclideana en $\boldsymbol{Z}[i]$. Así, $\boldsymbol{Z}[i]$ es un dominio euclideano.*

Demostración. Nótese que para $\beta = b_1 + b_2 i \neq 0$, se define $N(b_1 + b_2 i) = b_1^2 + b_2^2$, de modo que $N(\beta) \geq 1$. Entonces, para todas las $\alpha, \beta \neq 0$ en $Z[i]$, se tiene $N(\alpha)N(\beta) = N(\alpha\beta)$. Esto prueba la segunda condición para una evaluación euclideana.

Ahora, es necesario probar el algoritmo de la división, primera condición para N. Sea $\alpha, \beta \in Z[i]$, con $\alpha = a_1 + a_2 i$ y $\beta = b_1 + b_2 i$, donde $\beta \neq 0$. Debemos encontrar σ y ρ en $Z[i]$

tales que $\alpha = \beta\sigma + \rho$, donde $\rho = 0$ o $N(\rho) < N(\beta) = b_1^2 + b_2^2$. Hagamos $\sigma = q_1 + q_2 i$ donde q_1 y q_2 son racionales enteros a determinar en Z. Entonces, ρ deberá tener la forma

$$\begin{aligned} \rho &= (a_1 + a_2 i) - (b_1 + b_2 i)(q_1 + q_2 i) \\ &= (a_1 - b_1 q_1 + b_2 q_2) + (a_2 - b_1 q_2 - b_2 q_1) i. \end{aligned}$$

Tenemos que encontrar racionales enteros q_1 y q_2 tales que

$$N(\rho) = (a_1 - b_1 q_1 + b_2 q_2)^2 + (a_2 - b_1 q_2 - b_2 q_1)^2 < b_1^2 + b_2^2$$

esto es,

$$\frac{(a_1 - b_1 q_1 + b_2 q_2)^2}{b_1^2 + b_2^2} + \frac{(a_2 - b_1 q_2 - b_2 q_1)^2}{b_1^2 + b_2^2} < 1$$

Ahora bien, es necesario recordar que

$$\frac{(a_1 - b_1 q_1 + b_2 q_2)^2}{b_1^2 + b_2^2}$$

es precisamente el cuadrado de la distancia d en el plano euclideano, de un punto (q_1, q_2) a la recta l con ecuación $a_1 - b_1 X + b_2 Y = 0$. De manera análoga,

$$\frac{(a_2 - b_1 q_2 - b_2 q_1)^2}{b_1^2 + b_2^2}$$

es el cuadrado de la distancia d' de (q_1, q_2) a la recta l' con ecuación $a_2 - b_2 X - b_1 Y = 0$. Nótese que l es perpendicular a l'. Sea P el punto de intersección estas dos rectas, según se muestra en la figura 1, de la figura se ve que $d^2 + (d')^2$ es el cuadrado de la distancia de (q_1, q_2) a P. Así, debemos mostrar que existe un punto (q_1, q_2) con coordenadas enteras y tal que el cuadrado de la distancia a P es menor que 1. Como P está contenido en el interior o en la frontera de algún cuadrado de lado unitario, tal que ambas coordenadas de cada vértice son enteros, está claro que si se escoge (q_1, q_2) como el punto con coordenadas enteras, más cercano a P, su distancia a P podrá ser a lo más, la mitad de una diagonal del cuadrado, esto es, a lo más $\sqrt{2/2}$ (veáse figura 2). Así, el cuadrado de esta distancia a P es a lo más $\frac{1}{2}$, lo cual es menor que 1.

■

Es necesario hacer notar que se pudo haber probado el algoritmo de la división para la función N de manera exclusivamente algebraica, para lograrlo considere la siguiente sugerencia: Sea $\alpha, \beta \in Z[i]$, tal que $\alpha = a_1 + a_2 i$ y $\beta = b_1 + b_2 i$ y $\beta \neq 0$. Se define $\alpha/\beta = r + si$ en C, para $r, s \in Q$. Ahora considérese q_1 y q_2 enteros racionales en Z, lo más cercanos posible a los números racionales r y s respectivamente.

Se debe mostrar entonces, que para $\sigma = q_1 + q_2 i$ y $\rho = \alpha - \beta\sigma$ se tiene $N(\rho) < N(\beta)$; mediante la demostración de que

$$N(\rho)/N(\beta) = |(\alpha/\beta) - \sigma|^2 < 1.$$

Donde $||$ se define como el valor absoluto usual para los elementos de C.

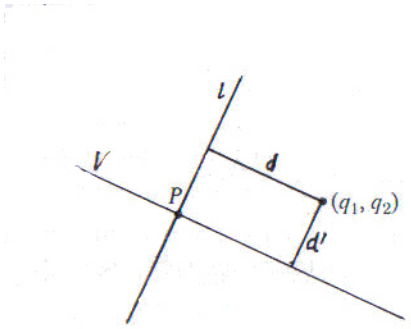

Figura 1

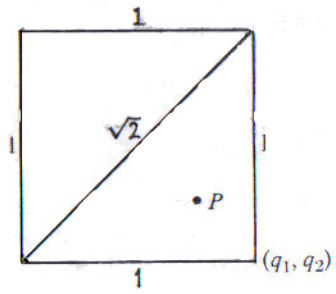

Figura 2

3.2.2. Normas Multiplicativas

Como ya habíamos señalado, para un dominio entero D, los conceptos aritméticos de irreducibles y unidades son intrínsicos al dominio entero mismo y de ninguna manera son afectados por una evaluación o norma, que pueda definirse en el dominio. Sin embargo, una evaluación o norma definida convenientemente puede ayudar a determinar la estructura aritmética de D. Esto se ilustra de manera sorprendente en la teoría de números algebraicos, donde para un dominio de enteros algebraicos se consideran varias evaluaciones diferentes del dominio, cada una cumple su cometido para ayudar a determinar la estructura aritmética del dominio. En un dominio de enteros algebraicos, tenemos esencialmente una evaluación para cada irreducible (salvo asociados) y cada una de dichas evaluaciones da información acerca del comportamiento, en el dominio entero, del irreducible al cual corresponde. Este es un ejemplo de la importancia del estudio de propiedades de elementos en una estructura algebraica, mediante funciones asociadas con ellos.

Procederemos a estudiar dominios enteros que tengan una norma multiplicativa que satisfaga las propiedades de N en $Z[i]$ dadas en el Lema (3,1).

Definición 3.7 *Sea D un dominio entero. Una norma multiplicativa N en D es una función que transforma D en los enteros Z tal que se satisfacen las condiciones siguientes:*

1. $N(\alpha) \geq 0$ *para todas las* $\alpha \in D$.
2. $N(\alpha) = 0$ *si y sólo si* $\alpha = 0$.
3. $N(\alpha\beta) = N(\alpha)N(\beta)$ *para todas las* $\alpha, \beta \in D$.

Teorema 3.7 *Si D es un dominio entero con norma multiplicativa N, entonces $N(1) = 1$ y $N(u) = 1$ para toda unidad u en D. Si, además, toda α tal que $N(\alpha) = 1$ es una unidad en D, entonces un elemento π en D con $N(\pi) = p$ para $p \in Z$ primo, es un irreducible de D.*

Demostración. Sea D un dominio entero con norma multiplicativa N. Entonces,

$$N(1) = N((1)(1)) = N(1)N(1)$$

muestra que $N(1) = 1$. Además, si u es una unidad en D, entonces

$$1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1}).$$

Como $N(u)$ es un entero no negativo, esto implica que $N(u) = 1$.
Supóngase ahora que las unidades de D son precisamente los elementos de norma 1. Sea $\pi \in D$ tal que $N(\pi) = p$ donde p es un primo en Z. Entonces, si $\pi = \alpha\beta$ tenemos

$$p = N(\pi) = N(\alpha)N(\beta),$$

así que $N(\alpha) = 1$ o $N(\beta) = 1$. Por hipótesis, esto significa que α o β es unidad de D. Así, π es un irreducible de D. ■

3.2.3. Ejemplo de un Dominio Sin Factorización Única

Para esta sección, definamos D como el dominio de integridad de ciertos números complejos, tal que

$$D = \{a + b\sqrt{-5} \text{ tal que } a, b \in Z\}$$

y para cada elemento

$$x = a + b\sqrt{-5} \in D$$

definimos su norma gaussiana como

$$N(x) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$$

Se tiene, además, que la norma definida satisface las siguientes condiciones

1. $N(x) = 0$, si y sólo si $x = 0$.
2. $N(xy) = N(x)N(y)$, para todo $x, y \in D$

En este dominio de integridad, es posible encontrar dos factorizaciones en irreducibles distintas para un mismo elemento del conjunto, como por ejemplo

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

Mostraremos que los elementos $3, 7, (1 + 2\sqrt{-5})$ y $(1 - 2\sqrt{-5})$ son irreducibles en D, y que además, no son asociados, para ejemplificar un extraño caso de dominio sin factorización única.

Comenzaremos mostrando que 3 es un irreducible en D. Para ello, si $3 = xy$ tal que $x, y \in D$, se tendrá entonces

$$N(3) = N(x)N(y) = 9$$

Luego, los posibles valores para $N(x)$ son 1, 3 y 9. Si $N(x) = 1$, entonces x es una unidad en D, y se prueba que 3 es un irreducible. Si $N(x) = 9$, tiene como consecuencia que $N(y) = 1$, por tanto y es una unidad en D, y también podemos concluir que 3 es un irreducible.

Veamos qué es lo que ocurre con la posibilidad de que $N(x) = 3$. Si hacemos $x = a+b\sqrt{-5}$, tendremos que

$$3 = N(x) = a^2 + 5b^2$$

lo cual es imposible de resolver para enteros a, b. Mediante esta contradicción, hemos probado que 3 es un irreducible en D. Un análisis análogo es el que se utiliza para mostrar que 7 es un irreducible en D.

Para probar que $1+2\sqrt{-5}$ es un irreducible en D, supongamos nuevamente de que existen ciertos $x, y \in D$ tal que $1 + 2\sqrt{-5} = xy$. Entonces, se tiene que

$$21 = N(1 + 2\sqrt{-5}) = N(x)N(y)$$

Luego, las posibilidades para $N(x)$ son 1,3,7 y 21. Si $N(x) = 1$ ó 27, entonces resulta de que x o y sea una unidad.

Sea $x = a + b\sqrt{-5}$. Entonces, si $N(x) = 3$ ó 7, se tiene una de las siguientes opciones

$$\begin{aligned} 3 &= N(x) = a^2 + 5b^2 \\ 7 &= N(x) = a^2 + 5b^2 \end{aligned}$$

lo cual es imposible solucionar para números enteros. Con ello, hemos mostrado que $1+2\sqrt{-5}$ es un irreducible en D. Un argumento similar es el que se utiliza para probar que $1 - 2\sqrt{-5}$ es un irreducible en D.

Para finalizar, notemos que ninguno de los elementos

$$3, 7, (1 + 2\sqrt{-5}), (1 - 2\sqrt{-5})$$

son asociados.

En efecto, los elementos 3, 7 y $(1+2\sqrt{-5})$ tienen normas distintas, por lo tanto, no puede haber asociados entre ellos. Sin embargo, $(1+2\sqrt{-5})$ y $(1-2\sqrt{-5})$ poseen la misma norma, pero, si existe una unidad u en D tal que

$$(1 + 2\sqrt{-5}) = u(1 - 2\sqrt{-5})$$

obtendremos las siguentes expresiones:

$$1 + 2\sqrt{-5} = 1 - 2\sqrt{-5} \text{ ó } 1 + 2\sqrt{-5} = -1 + 2\sqrt{-5}$$

puesto que las únicas unidades es D son 1 y -1. De este modo, hemos llegado a una contradicción.

Por lo tanto, ninguno de los cuatro elementos señalados son asociados entre si, por lo que D es un dominio de integridad sin factorización única.

3.3. Anillos de Polinomios

En la Teoría Algebraica de Números, los números algebraicos son las raíces de ciertos tipos de polinomios, entonces, es natural comenzar esta exposición con estos tópicos. Nuestro plan en esta sección es comenzar desde los resultados más generales acerca de los números algebraicos. En este proceso de proveer más conocimientos de esto, hemos seleccionado material de algunos aspectos de la teoría de números.

En otras palabras, nos interesaremos en aspectos tales como la divisibilidad, factorización única y polinomios irreducibles, mayormente a interesantes preguntas de las estructuras de anillos y dominios de integridad surgidos en la teoría.

Los polinomios que consideraremos serán aquellos que posean coeficientes enteros, en este caso son llamados polinomios sobre Z, donde Z denota el dominio de los números enteros. Esta colección de polinomios en una indeterminada x es frecuentemente denotada por $Z[x]$.

Definición 3.8 *: Sea A un anillo. El anillo de polinomios en la indeterminada X con coeficientes en A, y que denotaremos por $A[x]$, es el conjunto de expresiones formales de la forma*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

con cada $a_i \in A$. El elemento a_i se denomina el coeficiente de x_i en $f(x)$, y dos polinomios se consideran iguales si para cada i los coeficientes de x_i son iguales.

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

El grado de $f(x)$ es el mayor n tal que a_n es no nulo. Si el grado $(f(x)) = n$ escribiremos $f(x) = \sum_{k=0}^{n} a_k x^k$. El coeficiente a_n se denomina *coeficiente director* de $f(x)$. Si es igual a 1, decimos que $f(x)$ es un *polinomio mónico.*

Asignamos grado$(0) = -\infty$, y por conveniencia en el manejo de fórmulas establecemos que $-\infty < n$ y $-\infty + n = -\infty$ para cualquier $n \in Z^+$.

Se definen dos operaciones en $A[x]$. Sean $f(x) = a_n x^n + ... + a_1 x + a_0$ y $g(x) = b_m x^m + _{....+b_1 x+b_0}$:

- **Suma:** $f(x) + g(x)$ es el polinomio con coeficiente en x^i igual a $a_i + b_i$.
- **Producto:** $f(x)g(x)$ es el polinomio con coeficiente en x^i igual a $a_i b_0 + a_{i-1} b_1 + ... + a_0 b_i$.

Proposición 3.1 *Con estas operaciones, $A[x]$ es un anillo.*

Demostración. Para demostrar que $A[x]$, debemos mostrar en primera instancia, que la suma definida genera un grupo abeliano. En efecto, sean $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ y $g(x) = b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0$ dos polinomios en $A[x]$, tal que $n > m$. Por definición de suma, tenemos que

$f(x) + g(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 + b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0$
$f(x) + g(x) = a_n x^n + a_{n-1}x^{n-1} + ... + (a_m + b_m)x^m + ... + (a_1 + b_1)x + a_0 + b_0$

como los $a_i, b_j \in A$, entonces $a_i + b_j \in A$. Con ello, se muestra que $f(x) + g(x) \in A[x]$.

Claramente se puede mostrar que la suma de los elementos de $A[x]$ es *asociativa* y *conmutativa*. Para ello basta observar que los coeficientes pertenecen al anillo A, de los cuales la suma definida en A es asociativa y conmutativa.

Para mostrar que existe un *elemento neutro* para la suma de polinomios en $A[x]$, nos preguntamos por aquel polinomio $g(x) \in A[x]$ tal que, para todo $f(x) \in A[x]$, sea posible obtener $f(x) + g(x) = f(x)$. Simplemente, por definición de suma de polinomios, tenemos que cada coeficiente en x^i sea $a_i + b_i = a_i$. Como estos coeficientes pertenecen al anillo A, entonces cada uno de los coeficientes b_i de $g(x)$ son iguales a cero. Por tanto, en $A[x]$ existe el elemento neutro, el polinomio cero.

Un análisis similar es el que se realiza para determinar la existencia de los *elementos inversos*. Sean $f(x), g(x)$ polinomios en $A[x]$, entonces $f(x) + g(x) = 0$. Se debe determianr del análisis que en cada uno de los coeficientes de x^i se tiene que $a_i + b_i = 0$. Pero en el anillo A existen elementos inversos, por lo que $a_i = b_i^{-1}$, por lo que en el conjunto $A[x]$ se tienen elementos inversos. Con ello, hemos probado los axiomas de grupo abeliano para $A[x]$.

Nos falta probar que la multiplicación de los elementos de $A[x]$ es *asociativa* y que ésta *distribuye* sobre la suma antes definida. En efecto, sean $f(x) = a_n x^n + ... + a_0$, $g(x) = b_m x^m + ... + b_0$ y $h(x) = c_r x^r + ... + c_0$ elementos en $A[x]$. Tenemos que

$[f(x)g(x)]\, h(x) = [(a_n x^n + ... + a_0)(b_m x^m + ... + b_0)]\, (c_r x^r + ... + c_0)$
$[f(x)g(x)]\, h(x) = (a_n b_m x^{n+m} + ... + a_0 b_0)(c_r x^r + ... + c_0)$
$[f(x)g(x)]\, h(x) = (a_n b_m)c_r x^{n+m+r} + ... + (a_0 b_0)c_0$

Dado que los coeficientes a_i, b_j, c_k pertenecen al anillo A, la multiplicación de estos elementos es asociativa, por lo que podemos reordenar los coeficientes. De esta forma, se puede completar la prueba de que la multiplicación de elementos en $A[x]$ es asociativa.

Del mismo modo, completaremos la prueba de la propiedad distributiva de la multiplicación sobre la suma. Sean $f(x) = a_n x^n + ... + a_0$, $g(x) = b_m x^m + ... + b_0$ y $h(x) = c_r x^r + ... + c_0$ elementos en $A[x]$, tales que $n > m > r$. Tenemos que

$f(x)\,[g(x) + h(x)] = (a_n x^n + ... + a_0)\,[b_m x^m + ... + b_0 + c_r x^r + ... + c_0$

Como la multiplicación de cada uno de los coeficientes se puede distribuir sobre la suma, tenemos que

$f(x)\,[g(x) + h(x)] = (a_n x^n + ... + a_0)b_m x^m + ... + (a_n x^n + ... + a_0)b_0 + (a_n x^n + ... + a_0)c_r x^r + ... + (a_n x^n + ... + a_0)c_0$

del cual podemos asociar de la siguiente manera

$$f(x)\,[g(x) + h(x)] = (a_n x^n + ... + a_0)(b_m x^m + ... + b_0) + (a_n x^n + ... + a_0)(c_r x^r + ... + c_0)$$

y concluímos que

$$f(x)\,[g(x)+h(x)] = f(x)g(x)+h(x)$$

Con ello, hemos realizado una sistematización de la demostración de que $A[x]$, de la cual se puede completar sin mayores dificultades. ■

Teorema 3.8 *Sea A un dominio de integridad y S un subconjunto cualquiera. Entonces $A[S]$ es un dominio de integridad.*

Demostración. La Proposición 3.1 nos señala que si A es un anillo, entonces $A[x]$ también lo es. Aplicándolo a un número finito de veces obtenemos que su A es un dominio de integridad y S es finito, entonces $A[S]$ también lo es. Si S es arbitrario y f, g son dos polinomios no nulos de $A[S]$, entonces los monomios con coeficientes no nulos de f y g contienen un número finito de indeterminadas con exponente no nulo, luego f y g están en un subanillo $A[X]$ con X finito, luego $A[x]$ es un dominio de integridad, luego $f, g \neq 0$. Por lo tanto, $A[S]$ es un dominio de integridad. ■

Teorema 3.9 (Grado del polinomio) *Sea A un anillo unitario y p, q dos polinomios no nulos en $A[x]$ tales que al menos el coeficiente director de uno de ellos no sea un divisor de cero. Entonces $pq \neq 0$, $grad(pq) = grad(p) + grad(q)$ y el coeficiente director del producto es el producto de los coeficientes directores.*

Demostración. Sean $p = \sum_{i=0}^{m} a_i x^i$, $q = \sum_{i=0}^{n} b_i x^i$, con $a_m neq 0 neq b_n$. Entonces $pq = \sum_{k=0}^{m+n}(\sum_{i+j=k} a_i b_j)x^k$ y el coeficiente de x^{m+n} es exactamente $a_m b_n neq 0$, puesto que uno de ellos no es divisor de cero. Por lo tanto $a_m b_n$ es el coeficiente director de pq y su grado es $m+n$. ■

Proposición 3.2 (Algoritmo de división) *. Sea A un anillo, $f(x); g(x) \in A[x]$ con $g(x)$ mónico. Entonces existen unos únicos $q(x); r(x) \in A[x]$ con $grado(r(x)) < grado(g(x))$ tales que $f(x) = g(x)q(x) + r(x)$.*

Nota:

1. Decimos que $g(x)$ divide a $f(x)$ si en lo anterior se obtiene $r(X) = 0$
2. En el caso $A = K$, con K un cuerpo, el algoritmo anterior se tiene siempre, pues el coeficiente líder de $g(x)$ es una unidad.
3. Si $g(x)$ no es mónico, se puede conseguir una pseudo-división de la forma $c \cdot f(x) = g(x)q(x) + r(x)$ con $c \in A$.

Corolario 3.10 *Sea A un anillo y $a \in A$. Entonces para cualquier $f(x) \in A[x]$ existe $q(x) \in A[x]$ tal que*

$$f(x) = (x-a)q(x) + f(a)$$

Corolario 3.11 *Sea $f(x) \in A[x]$ y $a \in A$. Entonces $f(a) = 0$ si y solamente si $x - a$ divide a $f(x)$.*

Teorema 3.12 *Sea A un dominio de integridad y $f(x) \neq 0 \in A[x]$ un polinomio de grado n. Entonces existen a lo más n raíces de $f(x)$ en A.*

Corolario 3.13 *Sea A un dominio de integridad y $f(x), g(x) \in A[x]$ de grado menor o igual que n. Si $f(a) = g(a)$ para $n+1$ valores distintos de $a \in A$, entonces $f(x) = g(x)$.*

Definición 3.9 *Sea $f(x) \in A[x]$ un polinomio no nulo y $a \in A$ una raíz de $f(x)$. Entonces $x - a$ divide a $f(x)$ en $A[x]$.*

Al máximo entero $s > 0$ tal que $(x-a)^s \,|f(x)$ se le llama la *multiplicidad* de a como raíz de $f(x)$.

Se dirá que a es una *raíz simple* de $f(x)$ si $s = 1$. En caso contrario se diría que es *múltiple*.

3.3.1. Factorización

Definición 3.10 *Sea $A[x]$ un anillo de polinomios. Si $f(x), g(x) \in A[x]$, decimos que $f(x)$ divide a $g(x)$, y lo notaremos por $f(x)|g(x)$ si existe $a(x) \in A[x]$ tal que $g(x) = f(x)a(x)$.*

Definición 3.11 *Sean $f(x), g(x) \in A[x]$. Un máximo común divisor de $f(x), g(x)$ es un elemento $d(x) \in A[x]$ tal que*

- *$d(x)/f(x)$ y $d(x)/g(x)$.*
- *Si $v(x)/f(x)$ y $v(x)/g(x)$ entonces $v(x)/d(x)$, con $v(x) \in A[x]$.*

Lo escribiremos como $d(x) = mcd(f(x), g(x))$

Definición 3.12 *Sea $A[x]$ un dominio de integridad de polinomios. Un elemento no nulo $f(x) \in A[x]$ se dice irreducible si $f(x) = u(x)v(x)$, con $u(x), v(x) \in A[x]$ implica que $u(x)$ o $v(x)$ es una unidad en $A[x]$. Dos elementos $f(x), g(x) \in A[x]$ se dicen asociados si existe una unidad $u(x) \in A[x]$ tal que $f(x) = u(x)g(x)$.*

Proposición 3.3 *Sean $f(x), g(x) \in A[x]$. Entonces existe $d(x)$ el máximo común divisor de $f(x)$ y $g(x)$, y podemos encontrar $a(x), b(x) \in A[x]$ tales que*

$$d(x) = a(x)f(x) + b(x)g(x)$$

Demostración. Sabemos que existe $d(x) \in A[x]$ tal que $\langle f(x), g(x)\rangle = \langle d(x)\rangle$. Entonces $d(x)|f(x)$ y $d(x)|g(x)$, y existen $a(x), b(x)$ tal que $d(x) = a(x)f(x) + b(x)g(x)$.

Si $e(x)|f(x)$ y $e(x)|g(x)$ entonces

$$f(x) = e(x)f_1(x) \text{ y } g(x) = e(x)g_1(x) \text{ y}$$
$$d(x) = a(x)f_1(x)e_1(x) + b(x)g_1(x)e(x);$$

de donde $e(x)|d(x)$. ■

Proposición 3.4 *Sea $f(x)$ irreducible en $A[x]$, con $A[x]$ un dominio de integridad de polinomios y consideremos el ideal $I = \langle f(x) \rangle$. Entonces $A[x] = I$ es un cuerpo.*

Demostración. Sea $g(x) + I \neq 0 + I$. Debemos probar que tiene inverso en $A[x] = I$.

Tenemos que $g(x)$ no es múltiplo de $f(x)$. Como existe el máximo común divisor, no puede ser más que 1, dado que $f(x)$ es irreducible. Entonces existen $a(x), b(x) \in A[x]$ tales que

$$1 = a(x)f(x) + b(x)g(x) \text{ y } (g(x) + I)(b(x) + I) = 1 + I$$

■

Lema 3.3 *: Sea $f(x) \in A[x]$ irreducible tal que $f(x)|a(x)b(x)$, con $A[x]$ un cuerpo y $a(x), b(x)$ elementos de $A[x]$. Entonces $f(x)|a(x)$ o $f(x)|b(x)$.*

Demostración. Si $I = \langle f(x) \rangle$, entonces $a(x)b(x) + I = 0 + I$. Como $A[x] = I$ es un cuerpo, $A[x]$ es un dominio de integridad, por lo que $a(x) + I$ o $b(x) + I$ es nulo. ■

Proposición 3.5 *Sea $f(x) \in A[x]$, con $A[x]$ un dominio de integridad. Entonces $f(x)$ se puede escribir como $f(x) = u(x)q_1(x) \cdots q_m(x)$ donde $u(x)$ es una unidad y cada $q_i(x)$ es irreducible.*

Además, esta factorización es única en el sentido de que si $f(x) = v(x)p_1(x) \cdots p_n(x)$ con $v(x)$ unidad y cada $p_i(x)$ irreducible entonces $m = n$ y existe una permutación σ de $\{1, ..., n\}$ tal que $p_i(x) = w_i(x)q_{\sigma(i)}(x)$ con $w_i(x)$ unidad.

Demostración. La existencia de la factorización es por inducción sobre el grado de $f(x)$.

Si $f(x)$ es irreducible, hemos acabado. En otro caso, se puede expresar como producto $f(x) = f_1(x)f_2(x)$, con

$$grado(f(x)) > grado(f_1(x)), grado(f_2(x))$$

Veamos la unicidad. Si $u(x)q_1(x) \cdots q_m(x) = v(x)p_1(x) \cdots p_n(x)$entonces $q_1(x)$ divide a algún $p_i(x)$. Como son irreducibles, existe $w_i(x)$ unidad tal que $q_1(x) = w_i(x)p_i(x)$. Por inducción tenemos el resultado. ■

CAPÍTULO 4

Aplicaciones a la Teoría de Números

Muchas de las aplicaciones del concepto de dominio de integridad se dan en contextos donde los resultados conocidos desde la antigua Grecia eran dispersos y contaban con soluciones superficiales.

Hasta la época de Fermat[1], los métodos utilizados por los matemáticos para las soluciones enteras de ciertos polinomios o ecuaciones diofánticas, se reducían a un conjunto de técnicas y artilugios matemáticos dotados, por supuesto, de un alto nivel de originialidad en su conjetura y presentación, pero carentes de sentido en el ámbito estructural, que pudiera predecir y comprender las situaciones para casos más generales, y no particulares, como lo fueron la búsqueda de ternas pitagóricas o las soluciones enteras que buscaba Fermat para su "última teorema", misterio revelado por Andrew Wiles en el año 1993, en un extenso documento de más de 100 páginas, donde hace uso de los elementos más modernos y avanzados del álgebra y la geometría compleja.

El concepto de dominio de integridad, que surge en la teoría algebraica de forma más tardía, viene a reunir estos resultados parciales, construyendo una hermosa y sofisticada relación entre números enteros, en la mayoría de los casos, con el comportamiento que estos tienen.

En este capítulo, queremos entregar un panormama de cómo el concepto de dominio de integridad viene a ordenar estas situaciones, tales como el Teorema de Pitágoras y la búsqueda de ternas pitágoricas, y un análisis de sus soluciones con dominios de normas gaussianas como una primera aproximación del ibjeto de estudio de la Teoría Algebraica de Números, que es la solución y búsqueda de raíces enteras a ciertos polinomios, así como además, una conceptualización algebraica de la teoría de congruencias.

[1] Fermat, Pierre de (1601-1665), Matemático francés. Es conocido por su trabajo en álgebra, teoría de números y las primeras conceptualizaciones del infinito en cálculo.

4.1. Ternas Pitagóricas

Uno de los teoremas más importantes que conocemos desde la época antigua de la humanidad es el Teorema de Pitágoras, el cual señala que para todo triángulo rectángulo, la suma de los catetos al cuadrado es igual al cuadrado de la hipotenusa, definiendo catetos a los lados adyacentes al ángulo recto, e hipotenusa como el lado opuesto ál vértice donde se forma dicho ángulo. Siendo x y y los catetos y z la hipotenusa, se tiene que:

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

A continuación, realizaremos un estudio sistemático de las ternas pitagóricas integrándolo al concepto de dominio de integridad. Este estudio presenta un orden adecucado para comprender la forma aritmética los resultados conocidos, hasta concluir de forma algebraica[2].

Definición 4.1 *Sean x, y y z números enteros. La terna $\{x, y, z\}$ es una* terna pitagórica *o* triple pitagórico *si satisface la relación $x^2 + y^2 = z^2$.*

Teorema 4.1 *Sea $d = (x, y, z)$ y suponga que $\{x, y, z\}$ es una terna pitagórica. Entonces*

$$\left\{\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right\}$$

es también una terna pitagórica.

Demostración. Dado que d representa el máximo común divisor entre x, y y z, por definición existen enteros α, β, γ tal que

$$x\alpha + y\beta + z\gamma = d$$

y dado que d es divisor común, su cociente genera enteros, digamos x', y', z'.

Entonces

$$\begin{aligned} x\alpha + y\beta + z\gamma &= d \\ x\alpha(\frac{1}{d}) + y\beta(\frac{1}{d}) + z\gamma(\frac{1}{d}) &= 1 \\ \alpha(\frac{x}{d}) + \beta(\frac{y}{d}) + \gamma(\frac{z}{d}) &= 1 \end{aligned}$$

Luego, se tiene que $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}) = 1$, de modo que $\left\{\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right\}$ es una terna pitagórica. ■

Un triple pitagórico $\{x, y, z\}$ que satisface $(x, y, z) = 1$ se dice que es un triple pitagórico *primitivo*. Para encontrar todos los triples pitagóricos es suficiente encontrar todos los triples pitagóricos primitivos.

[2]La secuencia de esta sistematización corresponde a la desarrollada por la profesora María Inés Icaza, Doctora en Matemáticas, Directora del Instituto de Matemática y Física de la Universidad de Talca, en el marco de la primera versión de la Escuela de Verano de Matemáticas (Enero, 2008) realizada en dicha universidad, para la evaluación del curso de Teoría de Números.

Si $\{x, y, z\}$ es un triple pitagórico primitivo, entonces x, y, z son relativamente primos a pares.

Supongamos que x y y son impares; entonces z^2 es par. En efecto, sean $x = 2k_1 - 1$ y $y = 2k_2 - 1$; donde k_1 y k_2 son enteros positivos[3].

Entonces, al elevar al cuadrado estas expresiones, obtenemos

$$x^2 = (2k_1 - 1)^2$$
$$y^2 = (2k_2 - 1)^2$$

cuyos desarrollos son los que a continuación siguen:

$$x^2 = 4k_1^2 - 4k_1 - 1$$
$$y^2 = 4k_1^2 - 4k_2 - 1$$

Al sumar, obtenemos

$$\begin{aligned} x^2 + y^2 &= 4k_1^2 - 4k_1 - 1 + 4k_2^2 - 4k_2 - 1 \\ x^2 + y^2 &= 2\left[2k_1(k_1 - 1) + 2k_2(k_2 - 1) + 1\right] \\ x^2 + y^2 &= 2\xi = z^2 \end{aligned}$$

Mostraremos ahora que z debe ser par. Como $z^2 = 2\xi$, claramente observamos que z^2 debe ser par: si z es impar, el producto entre impares genera un impar, lo cual es una contradicción, por lo que la única opción para z es que sea par.

Podemos concluir, además, que z^2 es divisible por 4. Esto es evidente, por el hecho $z^2 = 2\xi$, del cual podemos decir que $z = \sqrt{2\xi}$, pero como z es par, escribimos $\sqrt{2\xi} = 2n$ donde $n \in Z^+$. Luego $z^2 = 2\xi = 4n^2$, y probamos que $4|z^2$.

Hasta el momento, ya hemos refutado la hipótesis de que los valores de x y y sean pares, cuando se trata de ternas pitagóricas primitivas. La pregunta que debemos formularnos ahora corresponde a qué es lo que sucede cuando ambos números son impares.

Supongamos que x es impar, entonces cabe preguntarnos ¿cuál es el resto que se genera cuando 4 divide a x^2? Veamos: $x = 2k_1 - 1$, para k_1 un entero positivo y $x^2 = 4k_1^2 - 4k + 1$, lo cual implica que $x^2 = 4(k_1^2 - k) + 1$, y al dividir por 4 tenemos que el resto es 1. Situación análoga sucede para el caso de y^2 cuando es divisible por 4.

[3]Excluiremos enteros negativos, pues se tratan de longitudes, donde no se consideran este tipo de valores.

Tenemos entonces lo siguiente:

$$\begin{aligned} x^2+y^2 &= z^2 \\ \frac{x^2+y^2}{4} &= \frac{z^2}{4} \\ \frac{x^2}{4}+\frac{y^2}{4} &= z^2 \\ \left[(k_1^2-k)+1\right]+\left[(k_2^2-k)+1\right] &= z^2 \\ (k_1^2-k+k_2^2-k)+2 &= z^2 \end{aligned}$$

cuyo resto es 2, pero 4 no puede dividir a 2, lo cual es una contradicción, por tanto, x y y no pueden ser impares de forma simultánea.

Como ya hemos desechado dos opciones para los valores de x y y, supongamos que uno de los catetos, digamos x, es par, mientras que y y z son impares, y que $\{x, y, z\}$ es un triple pitagórico primitivo. En consecuencia, podemos escribir

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

y podemos expresarlo de la siguiente forma

$$x^2 = z^2 - y^2 = (z+y)(z-y).$$

Con ello, tenemos que los factores $(z+y)$ y $(z-y)$ son pares. Es muy fácil probar que la suma y diferencia de números impares genera números pares.

Como x y ambos factores son pares, podemos escribir convenientemente la siguiente expresión:

$$\left(\frac{x}{2}\right)^2 = \frac{x^2}{4} = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

Realizamos cambio de variable en los factores, de modo que $r = \frac{z+y}{2}$ y $s = \frac{z-y}{2}$. De este cambio, es evidente señalar que $(r, s) = 1$.

Ante esto, nos resta concluir que r y s deben ser cuadrados perfectos, es decir, existen enteros m y n, con $(m, n) = 1$, tal que $r = m^2$ y $s = n^2$. Como $(\frac{x}{2})^2 = rs$, entonces, tenemos que $\frac{x}{2} = \sqrt{rs}$, pero como $(r, s) = 1$, podemos separar en $\sqrt{r} = m$ y $\sqrt{s} = n$, entonces, r y s deben ser cuadrados perfectos.

Con ello, ya estamos en condiciones de construir las soluciones enteras para los valores de un triple pitagórico primitivo.

En primer lugar, tenemos que $(\frac{x}{2})^2 = rs$, y podemos escribir

$$\begin{aligned} \frac{x}{2} &= \sqrt{rs} \\ \frac{x}{2} &= \sqrt{m^2n^2} \\ \frac{x}{2} &= mn \\ x &= 2mn \end{aligned}$$

conservando la solución positiva, al tratarse de longitudes.

Bajo esta perspectiva, es muy sencillo encontrar los valores de y y z. Como ya hemos expresado anteriormente, teníamos que

$$\begin{aligned} \frac{z+y}{2} &= m^2 \\ \frac{z-y}{2} &= n^2 \end{aligned}$$

Ahora basta encontrar sus soluciones, para ello, despejamos la incógnita z y tenemos que

$$\begin{aligned} z &= 2m^2 - y \\ z &= 2n^2 + y \end{aligned}$$

e igualamos para encontrar el valor de y

$$\begin{aligned} 2m^2 - y &= 2n^2 + y \\ 2m^2 - 2n^2 &= 2y \\ m^2 - n^2 &= y \end{aligned}$$

Para encontrar la forma de los valres de z, simplemente reemplazamos en la ecuación pitagórica, obteniendo

$$\begin{aligned} (2mn)^2 + (m^2 - n^2)^2 &= z^2 \\ 4m^2n^2 + m^4 - 2m^2n^2 + n^4 &= z^2 \\ m^4 + 2m^2n^2 + n^4 &= z^2 \\ (m^2 + n^2)^2 &= z^2 \\ m^2 + n^2 &= z \end{aligned}$$

Desde el punto de vista de las estructuras algebraicas, es posible encontrar soluciones a esta terna utilizando el dominio de integridad de los enteros gaussianos, para el cual asociaremos una norma para z^2. Como sabemos, tenemos la ecuación original $x^2 + y^2 = z^2$ para un triple pitagórico primitivo, el cual podemos factorizar en elementos complejo-conjugados, de la forma

$$\begin{aligned} z^2 &= x^2 - (-1)y^2 \\ z^2 &= (x + yi)(x - yi) \end{aligned}$$

donde asociamos la factorización a normas en el dominio $Z[i]$, de modo que sean $x+yi = N(\alpha)$ y $x - yi = N(\beta)$. Luego tenemos que

$$\begin{aligned} z^2 &= N(\alpha)N(\beta) \\ z &= \sqrt{N(\alpha)N(\beta)} \end{aligned}$$

En este caso, como z es un entero positivo, las normas $N(\alpha)$ y $N(\beta)$ son enteros cuadrados perfectos del dominio $Z[i]$. Entonces $N(\alpha) = (r + si)^2$ y $N(\beta) = (r - si)^2$, y ahora tenemos que

$$\begin{aligned} z &= \sqrt{(r+si)^2(r-si)^2} \\ z &= (r+si)(r-si) \\ z &= r^2 + s^2 \end{aligned}$$

Dado que x, y y z son realtivamente primos a pares, las expresiones $(r+si)$ y $(r-si)$ son irreducibles en $Z[i]$. Por tanto, tenemos en este caso un ejemplo de dominio de factorización única. Realizaremos la siguiente ejemplificación para el triple pitagórico primitivo $\{3, 4, 5\}$, donde es clara la relación $3^2 + 4^2 = 5^2$. Si es posible encontrar una forma cuadrática tal que $5 = r^2 + s^2$ para elementos de la forma $(r + si)$ y $(r - si)$ en $Z[i]$, diremos que 5 tiene factorización distinta de la usual en enteros, $5 = 5 \cdot 1$.

En efecto, podemos escribir $5 = 1^2 + 2^2$, donde 5 no es un irreducible en $Z[i]$ en comparación al conjunto usual Z, por tanto, tiene factorización única en $Z[i]$, a saber, $5 = (1 + 2i)(1 - 2i)$.

4.2. Teoría de Congruencias

La Teoría de Congruencias fue introducida por Gauss, contribuyendo al estudio de la Teoría de Números de forma decisiva. Hasta la época en que estos fueron introducidos en su obra *Disquisitiones Arithmeticae*(1801), los estudios en teoría de números eran más bien sistematizaciones, problemas dispersos y colecciones de algoritmos, por lo que la potencia de los escritos de Gauss proporcionaban las herramientas necesarias para descubrir y comprender una nueva área de estudio en matemáticas.

Definición 4.2 *Si un entero m, distinto de cero, divide la diferencia $a - b$ para los enteros a y b, decimos que a es congruente con b módulo m y escribimos $a \equiv b(mod\ m)$.*

Desde el punto de vista aritmético, la definición de congruencia no es difícil de interpretar. Podemos ejemplificarlo con un hecho muy concreto: cuando decimos que "'son las 5:00 de la tarde al mirar un reloj análogo, nos referimos a que son las 17:00, por lo que la diferencia entre ellas es divisible por 12, y es reflejo de que las horas en el reloj análogo forman un módulo, que es el módulo 12, de modo que $17 \equiv 5(mod\ 12)$.

Desde el punto de vista algebraico, esta división tiene matices más finos que ya hemos dado a conocer en los capítulos anteriores, cuando aparece el concepto de ideal en la teoría algebraica. En ese sentido, podemos elaborar una definición algebraica de congruencia, sin que esta pierda la consistencia obtenida en la teoría aritmética.

Definición 4.3 *Consideremos un dominio de integridad A y un ideal I. Diremos que dos elementos $a, b \in A$ son congruentes módulo I, abreviado $a \equiv a(mod\ I)$, si $a - b \in I$.*

Definición 4.4 *Si $x \equiv y(mod\ m)$, entonces se dice que y es un* residuo *de x módulo m. Un conjunto $x_1, x_2, \ldots, x_m$ se denomina un* sistema completo de residuos *módulo m si para cada entero y existe un único x_j tal que $y \equiv x_j(mod\ m)$.*

Es claro que existe una infinidad de sistemas completos de residuos módulo m, el conjunto $1, 2, \ldots, m-1, m$ sería otro ejemplo de ello.

Un conjunto de m enteros forma un sistema completo de restos módulo m sí y sólo sí no existen dos enteros en el conjunto que sean congruentes módulo m.

Para dos enteros fijos a, m, ambos mayores que cero, el conjunto de todos los enteros x que satisfacen $x \equiv a(mod\ m)$ es la progresión aritmética

$$\cdots, a-3m, a-2m, a-m, a, a+m, a+2m, a+3m, \cdots$$

Este conjunto se llama una *clase de residuos* o *clases de congruencias* módulo m. Existen m distintas clases de residuos módulo m, obteniendo, como ejemplo, al reemplazar sucesivamente $a = 1, 2, 3, \cdots, m$.

Teorema 4.2 *: Si $x \equiv y(mod\ m)$, entonces $(x, m) = (y, m)$.*

Demostración. Por definición de congruencia, tenemos que $y - x = mz$ para algún entero z. Puesto que $(x, m)|x$ y $(x, m)|m$, tenemos que $(x, m)|y$ y en consecuencia que $(x, m)|(y, m)$. De forma análoga, podemos concluir que $(y, m)|(x, m)$, y en virtud del Teorema 1.3.5, tenemos que $(x, m) = (y, m)$. ■

Definición 4.5 *Un sistema reducido de residuos módulo m es un conjunto de enteros r_i tal que $(r_i, m) = 1$, $r_i \not\equiv r_j(mod\ m)$ si $i \neq j$ y tal que cada x primo en m es congruente módulo m para algún elemento r_i del conjunto en cuestión.*

En virtud del Teorema 1.2.2, es claro que un sistema reducido de residuos módulo m se puede obtener mediante la eliminación de los elementos que no son primos relativos con m, a partir de un sistema completo de residuos módulo m. Más aún, para ampliar las relaciones entre teorías y conceptos, todo sistema reducido de residuos módulo m contendrá el mismo número de elementos, que es un número que se denota por $\phi(m)$. Esta es una función, que en la literatura matemática es conocida como la función ϕ de Euler[4].

Definición 4.6 *El número $\phi(m)$ es el número de enteros positivos menores o iguales a m que sean primos relativos con m.*

Teorema 4.3 *Cualquier sistema completo de residuos módulo m forma un grupo abeliano bajo la suma módulo m.*

[4]Euler, Leonhard (1707-1783), Matemático suizo. Además de sus aportes al álgebra y teoría de números, profundizó en la matemática analítica.

Demostración. Comenzaremos usando el sistema completo de residuos $0, 1, 2, ..., m-1$ módulo m. Este sistema es cerrado con respecto a la suma módulo m, mientras que la asociatividad y la conmutatividad es una propiedad inherente a todos los enteros; esto es, si $(a+b)+c = a+(b+c)$ para $a, b, c \in Z$, entonces $a+(b+c) \equiv (a+b)+c(mod\ m)$. El elemento neutro es 0 y pertenece al sistema completo de residuos módulo m. Finalmente, el inverso aditivo de 0 es 0, y el inverso aditivo de cualquier otro elemento a es $m-a$, de los cuales, cada uno de estos inversos es único. ■

Teorema 4.4 *El conjunto Z_m de elementos $0, 1, 2, ..., m-1$ con suma y multiplicación definida en módulo m forma un anillo para todo entero $m > 1$. En particular, Z_m será un dominio de integridad sí y sólo sí m es primo.*

Demostración. En el Teorema 4.3 demostramos que para cualquier sistema completo de residuos módulo m forma un grupo abeliano bajo la adición. La multiplicación es asociativa y la propiedad distributiva de multiplicación módulo m es consecuencia de la correspondientes propiedades de multiplicación usual en Z. De este modo, Z_m es un anillo.

Siguiendo con nuestra demostración, cualquier sistema reducido de residuos módulo m forma un grupo bajo la multiplicación módulo m. Si m es primo, el sistema reducido de residuos de Z_m es $1, 2, ..., p-1$, esto eso, todos los elementos de Z_p excepto 0. Puesto que 0 es el neutro en el anillo, Z_m es un dominio de integridad.

Por otro lado, si m no es primo, entonces m es de la forma $a \cdot b$ con $1 < a \leq b < m$. Entonces, los elementos de Z_m excepto 0 no forma un grupo bajo la multiplicación módulo m, porque no existen elementos inversos para cada elemento a, y con ello, no solución para la congruencia $ax \equiv 1(mod\ m)$. De este modo, Z_m no es un dominio de integridad. ■

En el conjunto de los enteros, se descubrieron muchísimas propiedades y reglas de divisibilidad previo al desarrollo moderno de la teoría de números y del álgebra. Los problemas en que surgen las congruencias eran, practicamente de problemas y desafíos matemáticos entendidos como diversión o pasatiempo en los salones ilustrados de los siglos XVIII y XIX. En ese sentido, Euler y Fermat registraron dos resultados importantísimos en teoría de números, que fueron los primeros en evidenciar la estructura de dominio de integridad en enteros, como ya veremos a continuación.

Teorema 4.5 *(Euler) Si $(a, m) = 1$, entonces*

$$a^{\phi(m)} \equiv 1(mod\ m).$$

Demostración. Sean

$$r_1, r_2, ..., r_{\phi(m)}$$

un sistema reducido de residuos módulo m. Consideremos la coleccion de $\phi(m)$ enteros

$$ar_1, ar_2, ..., ar_{\phi(m)}$$

del cual $(a, m) = 1$. Este conjutno R es también un sistema reducido de residuos módulo m; en efecto, si $(r_i, m) = 1$ para $i = 1, 2, ..., \phi(m)$, entonces es muy fácil verificar que $(ar_i, m) = 1$. En consecuencia, a cada r_i le corresponde un único ar_j tal que $r_i \equiv ar_j (mod\ m)$. De este modo, distintos r_i tendrán diferentes ar_j correspondientes.

Lo anterior significa que los números $ar_1, ar_2, ..., ar_{\phi(m)}$ son los residuos módulo m de $r_1, r_2, ..., r_{\phi(m)}$, pero no necesariamente en el mismo orden. Multiplicando las congruencias generadas con estos residuos, obtenemos

$$\prod_{j=1}^{\phi(m)} (ar_j) \equiv \prod_{i=1}^{\phi(m)} r_i (mod\ m)$$

y en consecuencia

$$a^{\phi(m)} \prod_{j=1}^{\phi(m)} (r_j) \equiv \prod_{j=1}^{\phi(m)} r_i (mod\ m)$$

Ahora $(r_j, m) = 1$, con lo cual podemos cancelar r_j y obtenemos que $a^{\phi(m)} \equiv 1 (mod\ m)$. ■

Teorema 4.6 *(Fermat) Sea p un primo. Si p no divide a a, entonces* $a^{p-1} \equiv 1 (mod\ p)$. *Para todo entero a,* $a^p \equiv a (mod\ m)$.

Demostración. Si p no divide a a, entonces $(a, p) = 1$ y $a^{\phi(p)} \equiv 1 (mod\ p)$. Para encontrar $\phi(p)$, diremos que todos los enteros $1, 2, ..., p-1, p$, con excepción de p, son primos relativos con p. Entonces, tenemos que $\phi(p) = p - 1$, con ello hemos probado la primera parte del teorema.

La segunda parte es una consecuencia inmediata de la anterior demostración, puesto que al multiplicar por a, tenemos

$$\begin{aligned} a^{p-1}a &\equiv 1a (mod\ p) \\ a^p &\equiv a (mod\ p) \end{aligned}$$

demostrando el teorema. ■

De esta forma, ya estamos en condiciones de generar un teorema de congruencia para el conjunto de los enteros, haciendo notar en ella los aspectos de divisibilidad que están presentes en la teoría de dominios de integridad, en particular, y para la teoría de anillos, en general. Nos referimos a los conceptos de ideal y de anillo cociente, los cuales nos aseguran la existencia de la posibilidad de generar divisiones entre enteros y con ello generar congruencias.

Teorema 4.7 *Sean A un subanillo de Z y sea Z/I un anillo cociente, donde I es un ideal en Z. Entonces la función para todo elemento* $a \in A$

$$\begin{aligned} &\phi : A \to Z/I \\ &\phi(a) = a + I \end{aligned}$$

genera congruencias en el subanillo A.

Demostración. La función ϕ transforma los elementos a de A a la forma $a + I = k$, $k \in Z/I \subseteq Z$ para algún $b \in Z$, y decimos que si $(i) = I$, entonces tenemos que $a + bi = k$, lo cual implica que $i|k - a$, expresando en la forma usual $a + I \equiv a(mod\ I)$, o bien $k \equiv a(mod\ i)$, en el sentido aritmético de la definición de congruencia. ■

Estas divisiones generan residuos, por lo que a cada elemento $a \in A$ le corresponde una única equivalencia, muy similar a la definición de sistema completo de residuos, en el sentido de la teoría elemental de números.

Teorema 4.8 *: La función $\phi : A \to Z/I$, con $\phi(a) = a + I$, es un isomorfismo de anillo.*

Para probar que la función mencionada es un isomorfismo, es fácil mostrar que se cumplen $\phi(a + b) = \phi(a) + \phi(b)$ y $\phi(ab) = \phi(a)\phi(b)$ para las operaciones usuales en Z. Dejamos al lector la prueba de ellas, como un ejercicio.

Hasta este punto, hemos realizado un breve recorrido por aspectos de la teoría elemental de números, integrándolas con aspectos del álgebra moderna y cómo los conceptos de anillo y dominio de integridad reúnen estos resultados en favor de una comprensión más exquisita de la teoría.

CAPÍTULO 5

Cuerpo de Cocientes de un Dominio de Integridad

Dado un anillo integro $(A; L, L')$ donde A es un conjunto, L es la ley aditiva y es L' la ley multiplicativa, nos encontramos en general que, aunque la ley aditiva está simetrizada (todo elemento tiene simétrico, diremos también .ºpuesto"por extensión del lenguaje que usamos para la suma) en virtud de la misma definición de anillo, no ocurre lo mismo con la ley multiplicativa L', ya que si ésta también estuviese simetrizada, la estructura de $(A; L, L')$ sería, además, un campo o cuerpo.

La idea que nos planteamos es la de encontrar, para un dominio de integridad A, un cuerpo conmutativo mínimo K que contenga un subanillo isomorfo al dominio A.

Se dice, entonces, que el dominio A está inmerso en el cuerpo K y, obviamente, también estaría inmerso en todos los supercuerpos del cuerpo K. A K se le acostumbra a llamar cuerpo o campo de cocientes del dominio A.

5.1. Producto Cartesiano y Relación de Equivalencia.

Supongamos que A es un dominio de integridad, esto es, un anillo conmutativo, con elemento unidad y sin divisores de cero. Para simplificar, llamemos " $+$ " y " $\cdot$ " las leyes aditiva y conmutativa, respectivamente, y sean 0 y 1 sus respectivos elementos neutros (elementos cero y unidad del anillo).

Consideremos también una parte S de A que sea estable para la ley multiplicativa y que contenga al elemento unidad del anillo, esto es, un submonoide multiplicativo de $A : 1 \in S$ tal que $x, y \in S \rightarrow x \cdot y \in S$.

Definición 5.1 *Una relación es binaria en AXS. Sea el conjunto producto cartesiano*

$$AXS = \{(a,s)/a \in A,\ s \in S\}$$

y definamos en él una relación binaria de la forma

$$(a,s)R(a',b') \Leftrightarrow \exists s_1 \in S \text{ tal que } s_1(s'a - sa') = 0$$

Proposición 5.1 *La relación R es de equivalencia, tal que R es:*

1. *Reflexiva:* $\forall (a,s) \in AXS$

$$sa - sa = 0 \Rightarrow s_1 \in S, s(sa - sa) = 0 \Rightarrow (a,s)R(a,s)$$

2. *Simétrica: Dados* $(a,s),(a',s') \in AXS$, *entonces:*

$$(a,s)R(a',s') \Rightarrow s_1(s'a - sa') = 0, \text{ con } s_1 \in S$$

Del mismo modo, $\exists s_1 \in S$ *tal que*

$$s_1(sa' - s'a) = 0 \Rightarrow (a',s')R(a,s)$$

3. *Transitiva:*

$$(a,s)R(a',s') \Rightarrow \quad \exists s_1 \in S \quad \text{tal que } s_1(s'a - sa') = 0 \tag{5.1}$$
$$(a',s')R(a'',s'') \Rightarrow \quad \exists s_1 \in S \quad \text{tal que } s_1(s''a' - s'a'') = 0 \tag{5.2}$$

Demostración. 3. Multiplicando (5,1) por s_2s'' y (5,2) por s_1s, se tiene:

$$s_1s_2s''(s'a - sa') = 0 \quad \Rightarrow \quad s_1s_2(s's''a - ss''a') = 0$$
$$s_1s_2s(s''a' - s'a'') = 0 \quad \Rightarrow \quad s_1s_2(s''sa' - s'sa'') = 0$$

Entonces

$$s_1s_2(s''s'a - s'sa'') = 0$$

Por lo tanto

$$s_1s_2s'(s''a - sa'') = 0$$

■

Definición 5.2 (Las clases de equivalencia y el conjunto cociente) *Podemos representar por $[a/s]$ a la clase de equivalencia, con representantes (a,s), es decir, al conjunto de todos los pares equivalentes a (a,s):*

$$[a/s] = \{(a',s') \text{tal que } (a',s')R(a,s)\}$$

Y representaremos por $S^{-1}A$ al conjunto cociente, esto es, al conjunto cuyos elementos son las clases de equivalencia

$$S^{-1}A = \{[a/s] \text{ tal que } [a/s] \, clase - equivalencia\}$$

5.2. Estructuración Algebraica del conjunto cociente como Anillo con unitario

Vamos a estructurar algebraicamente el conjunto cociente $S^{-1}A$ definiendo dos leyes internas que llamaremos multiplicación o producto a la ley multiplicativa, que simbolizaremos por $\cdot$ y adición o suma a la ley aditiva que simbolizaremos por $+$, al igual que en el anillo A de partida.

Las propiedades de clausura, asociatividad, conmutatividad y de existencia de elemento neutro se prueban trivialmente en base a las propiedades de las leyes internas que confieren estructura de anillo al conjunto A. Igual de sencillo es la demostración de la propiedad distributiva del producto con respecto a la suma, que mostramos como ejemplo.

Definición 5.3 *Una ley multiplicativa en el conjunto cociente*

$$\forall (a/s'), (a'/s') \in S^{-1}A, (a/s')(a'/s') = (aa'/ss')$$

Proposición 5.2 *Propiedades de la ley multiplicativa en el conjunto cociente:*

1. *Clausura*

$$(a_1/s_1) = (a_1'/s_1'), (a_2/s_2) = (a_2'/s_2') \Rightarrow (a_1a_2/s_1s_2) = (a_1'a_2'/s_1's_2')$$

2. *Asociatividad*

$$\forall (a/s'), (a'/s'), (a''/s'') \in S^{-1}A, \textit{tal que } (a/s')\left[(a'/s')(a''/s'')\right] = \left[(a/s')(a'/s')\right](a''/s'')$$

3. *Conmutatividad*

$$\forall (a/s), (a'/s') \in S^{-1}A, \textit{tal que } (a/s)(a'/s') = (a'/s')(a/s)$$

4. *Elemento Neutro (elemento unidad)*

$$\forall (a/s) \in S^{-1}A, \exists (m/m) \in S^{-1}A, \textit{tal que } (m/m)(a/s) = (a/s)(m/m) = (a/s)$$

Corolario 5.1 *El conjunto cociente es, para la ley multiplicativa, un semigrupo conmutativo con elemento unidad, es decir, un monoide conmutativo.*

Demostración. Esto es efectivo, por las propiedades que cumple la ley multiplicativa.■

Definición 5.4 *Una ley aditiva en el conjunto cociente*

$$\forall (a/s), (a'/s') \in S^{-1}A, \textit{tal que } (a/s) + (a'/s') = ((as' + a's)/ss')$$

Proposición 5.3 *Propiedades de la ley aditiva en el conjunto cociente*

1. *Clausura: Si* $(a_1/s_1) = (a_1'/s_1')$, *y* $(a_2/s_2) = (a_2'/s_2')$ *entonces*

$$((a_1s_2 + a_2s_1)/s_1s_2) = ((a_1's_2' + a_2's_1')/s_1's_2')$$

2. *Asociatividad: Para todo* $(a/s), (a'/s'), (a''/s'') \in S^{-1}A$, *entonces*

$$(a/s) + [(a'/s') + (a''/s'')] = [(a/s) + (a'/s')] + (a''/s'')$$

3. *Conmutatividad: Para todo* $(a/s), (a'/s') \in S^{-1}A$, *entonces*

$$(a/s)(a'/s') = (a'/s')(a/s)$$

4. *Elemento Neutro: Para todo* $(a/s) \in S^{-1}A$, *existe* $(0/m) \in S^{-1}A$, *tal que*

$$(0/m) + (a/s) = (a/s) + (0/m) = (a/s)$$

5. *Elemento Simétrico (opuesto): Para todo* $(a/s) \in S^{-1}A$, *existe* $(-a/s) \in S^{-1}A$ *tal que*

$$(-a/s) + (a/s) = (a/s) + (-a/s) = (0/s)$$

Corolario 5.2 *El conjunto cociente, para la ley aditiva, es un grupo conmutativo.*

Demostración. Efectivamente, también a la vista de las propiedades de la suma. ■

Proposición 5.4 *La ley multiplicativa es distributiva con respecto a la ley aditiva: para todo* $(a/s), (a'/s'), (a''/s'') \in S^{-1}A$, *entonces*

$$(a/s)\left[(a'/s') + (a''/s'')\right] = \left[(a/s)(a'/s') + (a/s)(a''/s'')\right]$$

Corolario 5.3 *Las leyes aditiva y multiplicativa en el conjunto cociente confieren a éste, estructura de anillo conmutativo con elemento unidad.*

Demostración. Por definición de anillo, la estructura algebraica $(S^{-1}A, +, \cdot)$ es, en efecto, un anillo conmutativo con elemento unidad, que llamaremos anillo de fracciones o de cocientes de A por S. ■

Corolario 5.4 *El cero del anillo* $\notin S$.

Demostración. El cero del anillo A no pertenece a pues caso contrario el anillo de cocientes solo contendría la clase $[0/1]$, pues todos los pares de AXS serían equivalentes. ■

5.3. El Cuerpo de Cocientes

Proposición 5.5 *Si A es dominio de integridad y $S = A-\{0\}$, la relación R de equivalencia que determina R es*

$$S^{-1}A = AXS/R$$

y puede expresarse por

$$(a,s)R(a',s') \Leftrightarrow a's = as'$$

Demostración. En efecto, la relación de equivalencia R fue introducida de forma general en la primera definición, mediante la expresión

$$(a,s)R(a',b') \Leftrightarrow \exists s_1 \in S/s_1(s'a - sa') = 0$$

Veamos que, si A es dominio de integridad, la relación R es equivalente a la relación R' definida así:

$$(a,s)R(a',b') \Leftrightarrow s'a - sa' = 0$$

Si $(a,s)R(a',b')$: $(a,s)R(a',b') \Rightarrow \exists s_1 \in S/s_1(s'a-sa') = 0 \Rightarrow s_1(s'a-sa') = 0 \wedge s_1 \neq 0 \wedge A$, con A un dominio de integridad $\Rightarrow s'a - sa' = 0 \Rightarrow s'a = sa' \Rightarrow (a,s)R(a',b')$ ■

Proposición 5.6 *El anillo cociente es un cuerpo si A es dominio íntegro y $S = A - \{0\}$.*

Demostración. En efecto, veamos que, con esta condición, en el anillo conmutativo con elemento unidad de los cocientes, todo elemento, salvo el elemento nulo, es invertible. Entonces, para todo $a/s \in S^{-1}A - \{0/1\}$ se tiene $a/s \neq 0/1$implicando $a \neq 0 \wedge s \neq 0$, pues $s \in S$

$$s/a \in S^{-1}A - \{0/1\} \Rightarrow (a/s)(s/a) = 1/1 \Rightarrow a/s$$

es invertible. ■

Definición 5.5 (Cuerpo de Cocientes) *Si A es un dominio íntegro y $S = A - \{0\}$, entonces el cuerpo $S^{-1}A$ se llama cuerpo de cocientes del dominio de integridad.*

Corolario 5.5 *El dominio de integridad A puede sumergirse en su cuerpo de cocientes, ya que el conjunto $A' = \{(a/1)/\ a \in A - 0\}$ es un subanillo de dicho cuerpo isomorfo al anillo A.*

Proposición 5.7 *Dado un dominio de integridad A, su cuerpo de cocientes, $S^{-1}A$, es el menor para la inclusión que contiene un subanillo isomorfo a A.*

Demostración. En efecto, veamos que de existir un subcuerpo M de $S^{-1}A, M \subseteq S^{-1}A$, que contenga un anillo A' isomorfo a A, dicho subcuerpo M ha de coincidir con $S^{-1}A$. Entonces, para todo $(a/b) \in S^{-1}A$ tal que

$$(a/b) = (a/1)(1/b)\text{con } (a/1),(1/b) \in A' \Rightarrow (a/b) \in M \Rightarrow S^{-1}A \subseteq M$$

Por tanto, $S^{-1}A = M$ ■

Proposición 5.8 *Cualquier cuerpo conmutativo, K, tal que el único subcuerpo del mismo que contenga un subanillo isomorfo a A sea el propio K, es isomorfo a $S^{-1}A$.*

Demostración. En efecto, si llamamos A_1 al subanillo del cuerpo K isomorfo al dominio A, y $S^{-1}A$ a su correspondiente cuerpo de cocientes en K, daremos los siguientes pasos:

1. Probaremos que $S^{-1}A_1$ es isomorfo a $S^{-1}A$.

2. Probaremos que $S^{-1}A$ es isomorfo a K.

Para comenzar, obtendremos que $S^{-1}A_1$ es isomorfo a $S^{-1}A$.

1. Un isomorfismo entre los cuerpos de fracciones:

Sea $g : A \to K$ el homomorfismo inyectivo que existe por hipótesis y llamemos $A_1 = g(A)$, con lo cual $g : A \to A_1$ es isomorfismo y A_1 es también un dominio de integridad.

El cuerpo de fracciones de A_1 será $S_1^{-1}A_1$ donde $S_1 = A_1 - \{0\}$.

en estas condiciones, definimos la correspondencia $h : S_1^{-1}A_1 \to S_1^{-1}A$ por la condición

$$\forall (a/b) \in S_1^{-1}A_1, \text{ entonces } h(a/b) = g^{-1}(a)/g^{-1}(b)$$

y veamos que ha de ser un isomorfismo:

a) Es una aplicación:
Puesto que $b \in A_1 - \{0\} \Rightarrow b \neq 0$por lo cual $g^{-1}(b) \neq 0$, ya que $g > 0$ es un isomorfismo de A en A_1.

$$\begin{aligned} (a/b) = (a'/b') &\Rightarrow ab' = a'b \\ g^{-1}(ab') = g^{-1}(a'b) &\Rightarrow g^{-1}(a)g^{-1}(b') = g^{-1}(a')g^{-1}(b) \\ g^{-1}(a)/g^{-1}(b) = g^{-1}(a')/g^{-1}(b') &\Rightarrow h(a/b) = h(a'/b') \end{aligned}$$

b) Es biyectiva: entonces, probaremos que es inyectiva y sobreyectiva.

- Es inyectiva, pues

$$\begin{aligned} h(a/b) = h(a'/b') &\Rightarrow g^{-1}(a)/g^{-1}(b) = g^{-1}(a')/g^{-1}(b') \\ g^{-1}(a)g^{-1}(b') = g^{-1}(a')g^{-1}(b) \wedge g \text{ isomorfo} &\Rightarrow ab' = a'b \\ &\Rightarrow a/b = a'/b' \end{aligned}$$

- Es sobreyectiva, pues para todo $(c/d) \in S^{-1}A$, y $(c, d) \in A_1 X (A_1 - \{0\})$, entonces existe $(a, b) \in A_1 X (A_1 - \{0\})$ tal que:

$$g(c) = a \wedge g(d) = b \Leftrightarrow g^{-1}(a) = c \wedge g^{-1}(b) = d$$

Entonces, existe

$$(a/b) \in S_1^{-1}A_1$$

tal que

$$h(a/b) = h(g(c)/g(d)) = g^{-1}(g(c))/g^{-1}(g(d)) = a/b$$

c) Es homomorfismo: para todo $(a/b), (a'/b') \in S_1^{-1}A_1$ se tiene

$$\begin{aligned} h(a/b + a'/b') &= h((ab' + a'b)/bb') \\ g^{-1}(ab' + a'b)/g^{-1}(bb') &= \left[g^{-1}(a)g^{-1}(b') + g^{-1}(a')g^{-1}(b)\right]/g^{-1}(b)g^{-1}(b') \\ g^{-1}(a)/g^{-1}(b) + g^{-1}(a')/g^{-1}(b') &= h(a/b) + h(a'/b') \\ h((a/b)(a'/b')) &= g^{-1}(aa')/g^{-1}(bb') \\ g^{-1}(a)g^{-1}(a') &= g^{-1}(b)g^{-1}(b') \\ &= h(a/b)h(a'/b') \end{aligned}$$

2. El isomorfismo entre el cuerpo de fracciones $S_1^{-1}A_1$ y el cuerpo K, definimos:

$$j : S_1^{-1}A_1 \to K, \text{ para todo } (a/b) \in S_1^{-1}A_1, \text{ se tiene } j(a/b) = ab^{-1}$$

y veamos que ha de ser isomorfismo:

a) Es una aplicación: para todo $(a, b) \in A_1X(A_1 - \{0\})$ implica que $ab^{-1} \in K$, puesto que $A_1 \subseteq K$)

$$\begin{aligned} (a/b) = (a'/b') &\to ab' = a'b \qquad \text{multiplicando por } \mathrm{b}^{-1}b'^{-1} \\ ab^{-1} = ab'^{-1} &\to j(a/b) = j(a'/b') \end{aligned}$$

b) Es biyectiva:

- Es inyectiva, pues

$$\begin{aligned} j(a/b) = j(a'/b') &\to ab^{-1} = ab'^{-1} \qquad \text{multiplicando por bb'} \\ ab' = a'b &\to a/b = a'/b \end{aligned}$$

- Es sobreyectiva, pues, para todo $x \in K$, con $x = ab^{-1}$ y definido b, será para todo $m \in K$, con $mb \in K$, y si llamamos $a = mb$, se tiene que

$$m = ab^{-1} \text{ entonces, existe } (a/b) \in K \text{ tal que } j(a/b) = ab^{-1} = m$$

c) Es homomorfismo. Para la ley aditiva se tiene que: para todo $(a/b), (a'/b) \in S_1^{-1}A_1$ se cumple que

$$\begin{aligned} j(a/b + a'/b') &= j((ab' + a'b)/bb') \\ (ab' + a'b)(bb')^{-1} &= ab^{-1} + a'b'^{-1} \\ &= j(a/b) + j(a'/b') \end{aligned}$$

Para la ley multiplicativa, tenemos que para todo $(a/b), (a'/b) \in S_1^{-1}A_1$ entonces

$$\begin{aligned} j((a/b)(a'/b')) &= j(aa'/bb') \\ (aa')(bb')^{-1} &= (ab^{-1})(a'b'^{-1}) \\ &= j(a/b)j(a'/b') \end{aligned}$$

Habida cuenta de que son isomorfismos las correspondencias h y j, también será isomorfismo la correspondencia inversa de cada una de ellas, así como su composición, por lo cual, es isomorfismo $j \circ h^{-1}$:

$$j \circ h^{-1} : S^{-1}A \to K$$

es isomorfo y esto prueba la proposición de unicidad del cuerpo de las fracciones de un dominio de integridad. ■

En Aritmética, claramente, el único cuerpo de cocientes del dominio de integridad Z de los números enteros es el campo Q de los números racionales. De esta forma, es posible construir el cuerpo de los racionales como la mínima estructura que contiene al dominio de los enteros.

CAPÍTULO 6

Conclusiones

A lo largo de nuestro estudio, hemos tenido como objetivo principal situar el concepto de dominio de integridad como un hilo unificador entre la teoría de números y el álgebra abstracta, y como una estructura algebraica de transición entre un anillo y un cuerpo, que en el caso de los números enteros, estas sutilezas se hacen evidentes.

Hemos visto que problemas aritméticos, como encontrar ternas pitagóricas primitivas, quedan resueltos según la estructura en que operan los valores y cantidades que se desean encontrar, o con la construcción de definiciones ad-hoc para lograr el objetivo inicial.

Nos sentimos plenos en desarrollar un tema matemático que, en muchos textos, se presenta de forma muy reducida y además, realizar conjeturas y demostraciones, indagar de forma profunda en sus matices, sus particularidades y el desafío que representó a los matemáticos del pasado generar las definiciones y la teoría subyacente.

El estudio realizado está marcado por la fuerte conceptualización existente, propia del álgebra. Estudiar nuevamente los conceptos, darles el enfoque que motivó nuestro interés en el tema, hacerlo concreto en este seminario de titulación, ha sido una de las actividades académicas que más ha marcado nuestra formación matemática y docente: matemática, porque se necesita una base sólida para desarrollar cada una de las estructuraciones que requiere un tema de este grado de complejidad, y docente, porque no olvidamos que tenemos la responsabilidad de que estos conocimientos, parte de nuestra cultura, sean de acceso y comprensión por el resto de los individuos de nuestra sociedad.

BIBLIOGRAFÍA

[1] A. Pettofrezzo, D. Byrkit. *Introducción a la Teoría de Números*. Editorial Prentice-Hall Internacional, 1972.

[2] J. Fraleigh. *Álgebra Abstracta*. Addison-Wesley Iberoamericana, S.A., 1987.

[3] P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul. *Basic Abstract Algebra*. Cambridge University Press, 1999.

[4] I.N. Herstein. *Álgebra Moderna*. Biblioteca de Matemática Superior. España: Editorial Trillas, 2002.

[5] I.M. Niven, H.S. Zukermann. *An Introduction to the Theory of Numbers*. New York: John Wiley, 1980.

[6] Hua Loo Keng. *Introduction to Number Theory*. Berlin: Springer Verlag, 1982.

[7] C.B. Boyer. *Historia de la Matemática*. Manuales de Ciencia y Tecnología. España: Alianza Editorial, 2003.

[8] C. Ivorra. *Álgebra*. Texto Electónico, obtenido el 15 de marzo de 2008, www.uv.es/ivorra

[9] C. Ivorra. *Teoría de Números*. Texto Electónico, obtenido el 15 de marzo de 2008, www.uv.es/ivorra