Un estudio de la relación de divisibilidad en la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$

Leidy Lizeth Castro Daza
Leidy Gisselle Sánchez Fúquene

Universidad Pedagógica Nacional
Licenciatura en Matemáticas
Bogotá D.C.
2016

Un estudio de la relación de divisibilidad en la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$

Leidy Lizeth Castro Daza
Cc.1026557391 Cód. 2011240019

Leidy Gisselle Sánchez Fúquene
Cc.1076656181 Cód. 2011140067

Trabajo de grado presentado ante el Departamento de Matemáticas asociado a un grupo de investigación.

Director:
Juan Carlos Ávila Mahecha

Codirector:
Yeison Alexander Sánchez Rubio

Universidad Pedagógica Nacional
Bogotá D.C Julio 2016

Agradecimientos

Agradecemos de manera especial al profesor Yeison Sánchez quien gracias a su dedicación hizo posible el desarrollo de este trabajo de grado, así como por los grandes aportes a nuestra formación como maestras.

Agradecemos a los profesores del grupo de Álgebra, en particular al profesor Juan Carlos Ávila por su apoyo para la realización de esta monografía.

1.Información General	
Tipo de documento	Trabajo de grado
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central
Título del documento	Un estudio de la relación de$\mathbb{Z}[\sqrt{-5}]$ divisibilidad en la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$
Autores	Castro Daza, Leidy Lizeth; Sánchez Fúquene, Leidy Gisselle
Director	Ávila Mahecha, Juan Carlos; Sánchez Rubio, Yeison Alexander
Publicación	Bogotá. Universidad Pedagógica Nacional, 2016. 88 p.
Unidad Patrocinante	Universidad Pedagógica Nacional
Palabras Claves	Extensión cuadrática, anillo conmutativo con unidad, divisibilidad, números primos e irreducibles, proceso de analizar

2.Descripción

El trabajo de grado elaborado se fundamentó en el proceso matemático de analizar en la estructura. En teoría de números este proceso se ve reflejado en el estudio de la relación de divisibilidad y el concepto de primo o de irreducible, pues permite la descomposición de un elemento a partir de elementos previamente ya caracterizados.

En este sentido, el interés del trabajo de grado titulado "Un estudio de la relación de divisibilidad en la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$" se centra en el estudio de la descomposición en esta estructura, que conlleva a ampliar las nociones de divisibilidad, unidades, asociados, números irreducibles y factorización única, además del estudio de algunos aspectos de la teoría de los números enteros en esta extensión cuadrática.

3.Fuentes

Ángel, L., Luque, C., & Sánchez, Y. (2014). *El proceso matemático de analizar en teoría de números: una aproximación desde la relación de divisibilidad.* XII Coloquio regional de matemáticas y II Simposio de Estadística.

Cox, D.(1989). *Primes of the forme $x^2 + ny^2$: Fermat, class field theory and complex*

multiplication. New York: Wiley-Interscience Publication.

Hagedorn, T. (s,f). *Primes of the form $x^2 + ny^2$ and the geometry (convenient) numbers.* The college of New Jersey.

Ivorra C. (s.f). Álgebra. Valencia: Universidad de Valencia.

Jiménez, H. (2006). *Estudio algebraico de los números Duales.* Bogotá: Universidad Pedagógica Nacional.

Luque, C., Jiménez, H. & Fonseca, J. (s.f). *¿Es necesaria la Propiedad Reflexiva en la Definición de Orden?*

Pérez, E. (2005). *Estructuras Algebraicas.* Bogotá: Universidad Pedagógica Nacional.

Pollar, H. (1965). *The theory of algebraic numbers.* New York: Cornell University.

Ravenna, G. (2008). Estructuras algebraicas. La Plata: Universidad de la Plata.

Zhang, Y. (2006). Representing primes as $x^2 + 5y^2$: an inductive proof that Euler missed. China: National University of Singapore.

4.Contenidos

En el primer capítulo se estudia la estructura algebraica de la extensión $\mathbb{Z}[\sqrt{-5}]$, así como el establecimiento de un orden con base en una función σ de $\mathbb{Z}[\sqrt{-5}]$ a $\mathbb{N}$, similar a la norma definida en los enteros Gaussianos. Esta función a su vez permitió definir el conjunto de los elementos de $\mathbb{N}$ que son imagen directa de $\mathbb{Z}[\sqrt{-5}]$ por la función σ, conjunto que se notará Σ.

En Σ se define una operación multiplicación, a partir de la cual es posible definir una relación de divisibilidad, la cual se relaciona con la divisibilidad en $\mathbb{Z}[\sqrt{-5}]$. Razón por la cual será de gran utilidad en el estudio de la divisibilidad de la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$. Así pues, este trabajo de grado dedica los dos siguientes capítulos al estudio de los elementos que pertenecen a Σ. y al estudio de la divisibilidad en esta estructura.

Por último, el cuarto capítulo usa los resultados obtenidos en los capítulos previos para estudiar algunas propiedades de la divisibilidad en $\mathbb{Z}[\sqrt{-5}]$ como la existencia de un algoritmo de la división y la posibilidad de cálculo del máximo común divisor de dos

elementos dados; así como para llevar a cabo el proceso de analizar en este superconjunto con vías a determinar el cumplimiento de un teorema análogo al teorema fundamental de la aritmética (TFA).

5.Metodología

Para la elaboración de esta monografía inicialmente se realizó una revisión documental basada principalmente en trabajos de grado del departamento de matemáticas de la Universidad Pedagógica Nacional, dirigidos por profesores del grupo de Algebra. Seguidamente se hizo un estudio de la estructura algebraica y de orden de la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$ con las operaciones suma y multiplicación. Posteriormente haciendo uso de herramientas tecnológicas tales como hojas de cálculo, programadores en lenguaje Pascal y macros de Excel se estudiaron los elementos de la estructura con el fin de realizar conjeturas y verificaciones en torno a la relación de divisibilidad y la caracterización de elementos tales como unidades, asociados y elementos irreducibles.

Una vez realizada las conjeturas y sus correspondientes verificaciones se demostraron algunas de ellas haciendo uso de razonamientos por inducción y contradicción, además de la realización de pruebas basadas en teoremas análogos en estructuras usuales y no usuales tales como el conjunto de los números naturales, enteros y enteros gaussianos.

6.Conclusiones

El conjunto $\mathbb{Z}[\sqrt{-5}]$ es un dominio de integridad, que no cumple la propiedad de existencia de inversos multiplicativos, lo que justificó el estudio de la divisibilidad en este superconjunto, en el cual se definió una relación $\preccurlyeq$ basada en una función σ de $\mathbb{Z}[\sqrt{-5}]$ a $\mathbb{N}$ la cual resultó ser un orden parcial que cumple la propiedad de monotonía con la multiplicación.

Dada la existencia de elementos no comparables mediante la relación $\preccurlyeq$ se define la relación $\approx$ en $\mathbb{Z}[\sqrt{-5}]$ tal que $z \approx w$ si y solo si $\sigma(z) = \sigma(w)$. Esta relación es de equivalencia y

permite definir el conjunto cociente $\mathbb{Z}[\sqrt{-5}]/\approx$, donde $\approx$ es una congruencia para la multiplicación y existe un orden total compatible con la operación.

Dada la función σ, se define el conjunto Σ de los elementos de $\mathbb{N}$ que son imagen directa de $\mathbb{Z}[\sqrt{-5}]$ por la función σ, conjunto en el cual la multiplicación es una operación, en tanto que σ es una función multiplicativa. Gracias a esto fue posible definir una relación de divisibilidad por medio de la cual se caracterizaron elementos distinguidos como: el 0, el 1, los elementos irreducibles y los compuestos. Nótese que como $\Sigma \subset \mathbb{N}$ entonces la descomposición en Σ se sigue de la descomposición en $\mathbb{N}$, con lo que se tiene que existe descomposición en termino de irreducibles, sin embargo no es única.

La cantidad de descomposiciones de un compuesto en Σ se puede calcular hallando su descomposición en $\mathbb{N}$ y fijándose en los factores primos p congruentes con 2, 3, o 7 módulo 20, los cuales al agruparse en parejas forman distintas factorizaciones en término de irreduicbles.

En la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$ con las operaciones suma y multiplicación, se define una relación de divisibilidad por medio de la cual se ejemplifica el proceso de matemático de analizar mediante la caracterización de elementos distinguidos; como el $(0,0)$, las unidades, lo números irreducibles y los números compuestos. En esta estructura se prueba que todo compuesto se puede factorizar como producto finito de irreducibles y se muestra que el número de descomposiciones de un elemento dado no es único, pues existen al menos tantas factorizaciones diferentes para un z dado, salvo por asociados, como descomposiciones tenga $\sigma(z)$ en Σ.

El anillo $\mathbb{Z}[\sqrt{-5}]$ mostró un ejemplo de una estructura en la que las nociones de primo e irreducible no son equivalentes, como si sucede en los conjuntos usuales. Esto permitió ampliar la idea de primo a un constructo mucho más elaborado, el cual se relaciona con la existencia de descomposición única.

Elaborado por:	Leidy Lizeth Castro Daza, Leidy Gisselle Sánchez Fúquene.
Revisado por:	Juan Carlos Ávila.

Fecha de elaboración del Resumen:	24	07	2016

Índice general

Introducción

En el marco del los proyectos de investigación del grupo de Álgebra alrededor del proceso matemático de analizar, se propuso dar participación a los estudiantes de la Licenciatura en Matemáticas de la UPN para que ellos vivenciaran la actividad matemática asociada al proceso de construcción del conocimiento matemático; por lo cual se ofreció a los estudiantes un espacio académico de asistencia libre llamado Seminario de Álgebra, cuya propuesta fue estudiar el proceso matemático de analizar ejemplificado desde la descomposición en subconjuntos y superconjuntos de $\mathbb{Z}$.

A partir del trabajo realizado en este espacio, se tuvo la oportunidad de reconocer las matemáticas, en particular la teoría de números, como el producto de ideas que evolucionan a lo largo del tiempo. Más aún, fue posible ver a las matemáticas como una ciencia no plenamente formada, razon por la cual, entre otras cosas, surge la motivación de las autoras de estudiar la relación de divisibilidad en la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$.

Para comenzar a dar una idea de lo que este trabajo de grado recopila en sus cuatro capítulos, cabe notar que a lo largo de la historia "las buenas ideas matemáticas difícilmente pasan de moda, aunque la forma de implementarlas puede sufrir cambios espectaculares". Tal es el caso de la noción de número primo en los números naturales, que los griegos desarrollaron en lo que hoy se conoce como una teoría de números pura, donde se reconoce a un número primo como aquel que siendo diferente de la unidad, solo es posible expresarse como el producto de él mismo y la unidad. Esta idea luego evoluciona con el surgimiento de la teoría algebraica de números, en la cual el concepto de número primo evoca a un constructo mucho más elaborado.

Así pues, este trabajo intenta responder, en la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$, a cuestionamientos que han sido de interés a en el estudio de la teoría de números, dentro de los que se encuentran: ¿Que son unidades?, ¿Qué es un número primo?, ¿Cuántos números primos existen?, ¿Cómo se puede identificar que un número es primo?¿Todo número que no sea primo se puede expresar como producto de primos y de ser así, de manera única?.

Con tal fin, el presente documento expone el proceso matemático de analizar en una estruc-

tura, ejemplificado desde la relación de divisibilidad, por medio de la cual se se evidencia la descomposición de un elemento en $\mathbb{Z}[\sqrt{-5}]$ a partir de elementos previamente caracterizados en este superconjunto. Para lo cual, se hizo necesario el estudio de la estructura algebraica de dicha extensión, así como el establecimiento de un orden con base en una función σ de $\mathbb{Z}[\sqrt{-5}]$ a $\mathbb{N}$, similar a la norma definida en los enteros Gaussianos. Esta función a su vez permitió definir el conjunto de los elementos de $\mathbb{N}$ que son imagen directa de $\mathbb{Z}[\sqrt{-5}]$ por la función σ, conjunto que se notará Σ. Trabajo que será abordado en el primer capítulo.

En Σ se define una operación multiplicación, a partir de la cual es posible definir una relación de divisibilidad, la cual se relaciona con la divisibilidad en $\mathbb{Z}[\sqrt{-5}]$. Razón por la cual será de gran utilidad en el estudio de la divisibilidad de la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$. Así pues, este trabajo de grado dedica los dos siguientes capítulos al estudio de los elementos que pertenecen a Σ y al estudio de la divisibilidad en esta estructura.

Por último, el cuarto capítulo usa los resultados obtenidos en los capítulos previos para estudiar algunas propiedades de la divisibilidad en $\mathbb{Z}[\sqrt{-5}]$ como la existencia de un algoritmo de la división y la posibilidad de cálculo del máximo común divisor de dos elementos dados; así como para llevar a cabo el proceso de analizar en este superconjunto con vías a determinar el cumplimiento de un teorema análogo al teorema fundamental de la aritmética (TFA).

Objetivos

Objetivo General

Desarrollar un estudio relacionado con la relación de divisibilidad, la descomposición y otros aspectos tratados usualmente en la Teoría de Números en la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$.

Objetivos Específicos

- Estudiar las operaciones y propiedades en la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$.
- Con base en el tratamiento dado a los enteros Gaussianos, $\mathbb{Z}[i]$, definir y estudiar una función $\sigma : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$, similar a la norma definida en $\mathbb{Z}[i]$.
- Definir un orden en $\mathbb{Z}[\sqrt{-5}]$ compatible con la multiplicación de esta estructura con base en σ.
- Estudiar el conjunto $\Sigma = \sigma_!(\mathbb{Z}[\sqrt{-5}])$, con la operación multiplicación.
- Desarrollar el proceso de analizar en Σ con base en la relación de divisibilidad.
- Estudiar en $\mathbb{Z}[\sqrt{-5}]$ una relación homóloga a la divisibilidad en $\mathbb{Z}$.
- Establecer relaciones entre la divisibilidad en $\mathbb{Z}[\sqrt{-5}]$ y Σ.
- Desarrollar el proceso de analizar en $\mathbb{Z}[\sqrt{-5}]$ con base en la relación de divisibilidad en este conjunto y las relaciones establecidas en Σ.

Capítulo 1

El conjunto $\mathbb{Z}[\sqrt{-5}]$

En este capítulo se tiene el interés de caracterizar el superconjunto $\mathbb{Z}[\sqrt{-5}]$ como una extensión cuadrática de los números enteros. Por ello se definen las extensiones cuadráticas de $\mathbb{Z}$ y se determina la estructura que estas poseen con las operaciones suma y multiplicación. Lo anterior con el fin estudiar la estructura particular $\big(\mathbb{Z}[\sqrt{-5}], +, \cdot\big)$, en la cual se espera que la divisibilidad no sea trivial y con esto los conceptos de unidad, elemento irreducible y primo. También se estudiará la estructura de orden en este superconjunto, estudio partir del cual surge la función σ como elemento clave para el estudio de la divisibilidad en $\mathbb{Z}[\sqrt{-5}]$.

1.1. Extensiones cuadráticas de $\mathbb{Z}$

Las extensiones cuadráticas de $\mathbb{Z}$, las cuales se notarán como $\mathbb{Z}[k]$, son conjuntos formados por números de la forma $(a + bk)$ con $k \notin \mathbb{Z}$, y $k^2, a, b \in \mathbb{Z}$, con las operaciones suma y multiplicación, definidas de la siguiente manera:

Sean $p, q \in \mathbb{Z}[k]$, tal que $p = (a + bk)$ y $q = (c + dk)$, su suma es:

$$p + q = (a + bk) + (c + dk) = ((a + c) + (b + d)k)$$

y su producto es:

$$pq = (a + bk)(c + dk) = \big((ac + bdk^2) + (ad + bc)k\big)$$

Un ejemplo de una extensión cuadrática de $\mathbb{Z}$ es el conjunto $\mathbb{Z}[i]$ donde $i^2 = -1$ denominado el conjunto de los *Enteros Gaussianos*, obsérvese que como $i \notin \mathbb{Z}$ se esta ampliando $\mathbb{Z}$ a un conjunto que incluye a $\sqrt{-1}$ y a números de la forma $a + bi$ con las operaciones suma y multiplicación definidas como sigue:

$$(a + bi) + (c + di) = ((a + c) + (b + d)i)$$

$$(a+bi)(c+di) = ((ac-bd)+(ad+bc)i)$$

Si ahora $k^2 = 0$, con $k \neq 0$, a los números de la forma $a+bk$ con $k \notin \mathbb{Z}$, y $a, b \in \mathbb{Z}$ se les llama el conjunto de los *Números Gaussianos Duales*.

En cada uno de los ejemplos presentados anteriormente la notación usada para hacer referencia a un $z \in \mathbb{Z}[k]$ admite pensar que el producto bk y la suma $a+bk$, corresponden a las operaciones usuales en los números enteros, lo cual es incorrecto, pues $k \notin \mathbb{Z}$. De manera que para evitar esos desaciertos y simplificar la notación se define a continuación una función f biyectiva entre $\mathbb{Z}[k]$ y $\mathbb{Z} \times \mathbb{Z}$ para copiar la estructura de $(\mathbb{Z}[k], +, \cdot)$ en las parejas.

$$f \colon \mathbb{Z}[k] \to \mathbb{Z} \times \mathbb{Z}$$

$$(a+bk) \to (a,b)$$

Por tanto en adelante se representará al elemento $a+bk$ como la pareja (a,b), además se notará al conjunto $\mathbb{Z} \times \mathbb{Z}$ como $\mathbb{Z}[k]$ y las definiciones de suma y multiplicación que se usarán son las que resultan de la copia mediante la función f, es decir:

Definición 1.1. Sean $(a,b),(c,d) \in \mathbb{Z}[k]$ la suma se define como,

$$(a,b)+(c,d) = ((a+c),(b+d))$$

Definición 1.2. Sean $(a,b),(c,d) \in \mathbb{Z}[k]$ la multiplicación se define por,

$$(a,b)(c,d) = \big((ac+bdk^2),(ad+bc)\big)$$

Además se dirá que dos elementos de $\mathbb{Z}[k]$ son iguales, si son iguales componente a componente, es decir,

Definición 1.3. Sean $(a,b),(c,d) \in \mathbb{Z}[k]$ son iguales si y sólo si $a = c$ y $b = d$.

Nótese que $(\mathbb{Z}[k], +, \cdot)$ y $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ son isomorfos mediante f.

1.1.1. Propiedades de la suma en $\mathbb{Z}[k]$

A continuación se demuestran algunas propiedades que satisfacen el conjunto $\mathbb{Z}[k]$ con la operación suma.

Teorema 1.1. Para todo $(a,b),(c,d),(d,e)$, elementos de $\mathbb{Z}[k]$, se cumple que:

$$(a,b)+((c,d)+(e,f)) = ((a,b)+(c,d))+(e,f)$$

Demostración.

$(a,b)+((c,d)+(e,f))$

$=(a,b)+((c+e),(d+f))$	Por definición 1.1
$=((a+(c+e)),(b+(d+f)))$	Por definición 1.1
$=(((a+c)+e),((b+d)+f))$	Por propiedad asociativa de $(\mathbb{Z},+)$
$=((a+c),(b+d))+(e,f))$	Por definición 1.1
$=((a,b)+(c,d))+(e,f)$	Por definición 1.1

Por tanto $(\mathbb{Z}[k],+)$ cumple la propiedad asociativa. □

Teorema 1.2. Para todo $(a,b),(c,d)\in\mathbb{Z}[k]$ se cumple que:

$$(a,b)+(c,d)=(c,d)+(a,b)$$

Demostración.

$(a,b)+(c,d)=((a+c),(b+d))$	Por definición 1.1
$=((c+a),(d+b))$	Por propiedad conmutativa de $(\mathbb{Z},+)$
$=(c,d)+(a,b)$	Por definición 1.1

Como $(a,b)+(c,d)=(c,d)+(a,b)$ entonces $(\mathbb{Z}[k],+)$ cumple la propiedad Conmutativa. □

Teorema 1.3. En $\mathbb{Z}[k]$ existe un elemento (x,y) tal que para todo $(a,b)\in\mathbb{Z}[k]$, se cumple que $(a,b)+(x,y)=(a,b)$

Sean $(a,b),(x,y)\in\mathbb{Z}[k]$ tales que $(a,b)+(x,y)=(a,b)$, entonces,

$((a+x),(b+y))=(a,b)$	Por definición 1.1
$a+x=a$ y $b+y=b$	Por definición 1.3
$x=0$ y $y=0$	Existencia de inversos en $(\mathbb{Z},+)$

Demostración. El elemento $(0,0)$ cumple que $(a,b)+(0,0)=(a+0,b+0)=(a,b)$. Al número $(0,0)$ se le denomina el elemento Neutro de la suma en $\mathbb{Z}[k]$. □

Teorema 1.4. En $\mathbb{Z}[k]$ para todo $(a,b)\in\mathbb{Z}[k]$ existe un (x,y) tal que:

$$(a,b)+(x,y)=(0,0)$$

Sean $(a,b),(x,y)\in\mathbb{Z}[k]$ tales que:

$(a,b)+(x,y)=(0,0)$

$((a+x),(b+y))=(0,0)$	Por definición 1.1
$a+x=0$ y $b+y=0$	Por definición 1.3
$x=-a$ y $y=-b$	Existencia de inversos en $(\mathbb{Z},+)$

Demostración. El elemento $(-a,-b)\in\mathbb{Z}[k]$ cumple que $(a,b)+(-a,-b)=(a+(-a),b+(-b))=(0,0)$. El elemento $(-a,-b)$ es el inverso aditivo de (a,b). □

Lo anterior demuestra que la estructura $(\mathbb{Z}[k],+)$ es un *grupo abeliano.*

1.1.2. Propiedades de la multiplicación en $\mathbb{Z}[k]$

Ahora se estudiarán las propiedades que cumple la estructura $\mathbb{Z}[k]$ con la operación multiplicación.

Teorema 1.5. Para todo $(a,b),(c,d),(d,e)$ elementos de $\mathbb{Z}[k]$, se cumple que:

$$((a,b)(c,d))\,(e,f)=(a,b)\,((c,d)(e,f))$$

Demostración.

$((a,b)(c,d))\,(e,f)$

$=((ac+bdk^2),(ad+bc))\,(e,f)$	Por definición 1.2
$=(((ac+bdk^2)e+(ad+bc)fk^2)\,,((ac+bdk^2)f+(ad+bc)e))$	Por definición 1.2
$=((a(ce+dfk^2)+bk^2(cf+de))\,,(a(cf+de)+b(ce+dfk^2)))$	Por propiedad distributiva de $(\mathbb{Z},+,\cdot)$
$=(a,b)\,((ce+dfk^2),(cf+de))$	
$=(a,b)\,((c,d)(e,f))$	Por definición 1.2

Por tanto $\mathbb{Z}[k]$ con la multiplicación cumple la propiedad asociativa. □

Teorema 1.6. Para todo $(a,b),(c,d)\in\mathbb{Z}[k]$ se cumple que:

$$(a,b)(c,d)=(c,d)(a,b)$$

Demostración.

$(a,b)(c,d) = ((ac + bdk^2), (ad + bc))$ Por definición 1.2
$= ((ca + dbk^2), (cb + da))$ Conmutatividad en $(\mathbb{Z}, +, \cdot)$
$= (c,d)(a,b)$ Por definición 1.2

Como $(a,b)(c,d) = (c,d)(a,b)$ entonces $\mathbb{Z}[k]$ con la multiplicación cumple la propiedad Conmutativa. □

Teorema 1.7. Existe un $(x,y) \in \mathbb{Z}[k]$ tal que para todo $(a,b) \in \mathbb{Z}[k]$ se cumple:

$$(a,b)(x,y) = (a,b)$$

Demostración. El elemento $(1,0)$ cumple que:

$$\begin{gathered}(a,b)(1,0) \\ = ((a1 + b0k^2), (a0 + b1)) \\ = ((a+0), (0+b)) = (a,b)\end{gathered}$$

A $(1,0)$ se le denomina el elemento Neutro de la multiplicación en $\mathbb{Z}[k]$. □

Para el caso de la propiedad existencia inversos multiplicativos, es posible afirmar que estas extensiones cuadráticas no cumplen dicha propiedad. Obsérvese que todo elemento $(a,0)$ con $a \neq \pm 1$ no tiene inverso multiplicativo, pues de existir un inverso (c,d) debe cumplirse que:

$$(a,0)(c,d) = (1,0)$$

de modo que $(ac, ad) = (1,0)$ y por igualdad de parejas ordenadas $ac = 1$, lo que sucede únicamente si $a = c = \pm 1$.

Teorema 1.8. Para todo $(a,b), (c,d), (e,f) \in \mathbb{Z}[k]$ se cumple que:

$$(a,b)\left[(c,d) + (e,f)\right] = \left[(a,b)(c,d)\right] + \left[(a,b)(e,f)\right]$$

Demostración.

$(a,b)\left[(c,d) + (e,f)\right]$
$= (a,b)\left[(c+e), (d+f)\right]$ Por definición 1.1
$= \left[(a(c+e) + b(d+f)k^2), (a(d+f) + b(c+e))\right]$ Por definición 1.2
$= \left[(ac + ae + bdk^2 + bfk^2), (ad + af + bc + be)\right]$ P. distributiva en $(\mathbb{Z}, +, \cdot)$
$= \left[((ac + bdk^2) + (ae + bfk^2)), ((ad + bc) + (af + be))\right]$ P. asociativa en $(\mathbb{Z}, +)$

$= [(ac + bdk^2), (ad + bc)] + [(ae + bfk^2), (af + be)]$ Por definición 1.1
$= [(a, b)(c, d)] + [(a, b)(e, f)]$ Por definición 1.2

Lo que demuestra que $\mathbb{Z}[k]$ cumple la propiedad distributiva de la multiplicación con respecto a la suma. □

En síntesis, como la estructura algebraica determinada por la operación suma sobre $\mathbb{Z}[k]$ es un grupo abeliano y la estructura algebraica determinada por la operación multiplicación sobre $\mathbb{Z}[k]$ es un semigrupo conmutativo con unidad, además de que la multiplicación distribuye con respecto a la suma, se concluye que la estructura algebraica de $(\mathbb{Z}[k], +, \cdot)$ es un anillo conmutativo con unidad.

Teorema 1.9. $\mathbb{Z}[k]$ con la suma y la multiplicación es un anillo conmutativo con identidad.

Además, atendiendo al no cumplimiento de la propiedad de existencia de inversos multiplicativos se puede afirmar que este anillo no tiene estructura de Campo, lo que es coherente con la idea de estudiar la relación de divisibilidad en estos superconjuntos.

Ahora, si bien los $\mathbb{Z}[k]$ no contienen a los números enteros, contienen un conjunto que es completamente isomorfo, motivo por el cual son superconjuntos de $\mathbb{Z}$. Para hacer una prueba de ello se debe hallar un subconjunto $\mathcal{Z}$ de $\mathbb{Z}[k]$, tal que entre $\mathcal{Z}$ y $\mathbb{Z}$ exista un isomorfismo. Con este fin recuérdese que la pareja (a, b) se puede ver como el elemento $a + bk$, de manera que si se hace $b = 0$ este queda de la forma $a + 0k$, así pues, es de intuirse que el subconjunto de los elementos $(a, 0)$ que pertenecen a $\mathbb{Z}[k]$ es isomorfo a los números enteros. Atendiendo a esto se enuncia el siguiente teorema.

Teorema 1.10. El conjunto $\mathcal{Z} \subset \mathbb{Z}[k]$ definido por $\mathcal{Z} = \{z \in \mathbb{Z}[k] : z = (a, 0)\}$ con las operaciones suma y multiplicación definidas en $\mathbb{Z}[k]$ es isomorfo al anillo de los números enteros.

Demostración. Sea la función g definida como:

$$\begin{aligned} g : \mathbb{Z} &\longrightarrow \mathcal{Z} \\ a &\longrightarrow (a, 0) \end{aligned}$$

Nótese que:

- $g(a + b) = (a + b, 0) = (a, 0) + (b, 0) = g(a) + g(b)$
- $g(ab) = (ab, 0) = (a, 0)(b, 0) = g(a)g(b)$

Por lo tanto la función g es un homomorfismo entre $\mathbb{Z}$ y $\mathcal{Z}$. Como esta función es biyectiva, g es además un isomorfismo. □

Lo anterior permite asegurar que los números de la forma $(a, 0)$ que pertenecen a $\mathbb{Z}[k]$ se operan y comportan en términos de propiedades igual que los números enteros.

1.2. La estructura $(\mathbb{Z}[\sqrt{-5}], +, \cdot)$

En la sección anterior se demostró que $\mathbb{Z}[k]$ con las operaciones suma y multiplicación es un anillo conmutativo con unidad, sin embargo, dependiendo del valor que se le de a k^2 pueden darse diferentes estructuras de anillo, por ejemplo, puede suceder que la estructura sea un dominio de integridad como en el caso de los *Enteros Gaussianos* o que por el contrario como ocurre con los *Números Gaussianos Duales* no se cumpla la propiedad cancelativa de la multiplicación debido a la existencia de elementos divisores de cero[1], que para este caso corresponden a los números de la forma $(0, b)$ para cualquier entero $b \neq 0$, donde $(0, b)(0, a) = (0, 0)$.

Por tanto uno de los propósitos de esta sección es averiguar cómo es la estructura de anillo para el caso $k^2 = -5$, esto es, la estructura $\left(\mathbb{Z}[\sqrt{-5}], +, \cdot\right)$; para ello se estudiará el cumplimiento de la propiedad cancelativa de la multiplicación, la cual junto con las propiedades de anillo conmutativo con unidad alude a una estructura de dominio de integridad.

En este sentido, supóngase que $z_1, z_2, z_3 \in \mathbb{Z}[\sqrt{-5}]$ con $z_1 = (a, b), z_2 = (s, t), z_3 = (u, v)$ y $(a, b) \neq (0, 0)$. Si

$$z_1 z_2 = z_1 z_3$$

entonces,

$$z_1(z_2 - z_3) = (0, 0)$$

donde

$$z_2 - z_3 = ((s - u), (t - v)) = (c, d)$$

entonces

$$z_1(z_2 - z_3) = (a, b)(c, d) = (0, 0)$$

$$((ac - 5bd), (ad + bc)) = (0, 0)$$

[1] Jiménez, H. (2006). *Estudio algebraico de los números Duales*. Bogotá: Universidad Pedagógica Nacional, p. 12

por la definición 1.3 se tiene

$$ac - 5bd = 0 \quad \text{y} \quad ad + bc = 0 \tag{1.1}$$

multiplicando por d, c las igualdades respectivamente, resulta

$$acd = 5bd^2 \quad \text{y} \quad acd = -bc^2$$

restando estas igualdades

$$b\left(c^2 + 5d^2\right) = 0$$

es decir que $b = 0$ o $(c^2 + 5d^2) = 0$ por propiedades de los Números Enteros. Si $(c^2 + 5d^2) = 0$ entonces

$$(c, d) = (0, 0)$$

de donde resulta:

$$\begin{aligned} c = 0 \quad &\text{y} \quad d = 0 \\ s - u = 0 \quad &\text{y} \quad t - v = 0 \\ s = u \quad &\text{y} \quad t = v \end{aligned}$$

por definición 1.3

$$z_2 = z_3$$

Si $b = 0$, por ecuación (1.1) se tiene:

$$ac = 0 \text{ y } ad = 0$$

como $a \neq 0$ entonces $c = 0$ y $d = 0$, por tanto

$$\begin{aligned} s - u = 0 \quad &\text{y} \quad t - v = 0 \\ s = u \quad &\text{y} \quad t = v \end{aligned}$$

por definición 1.3

$$z_2 = z_3$$

Así pues, se puede formular el siguiente teorema.

Teorema 1.11. Para todo $z_1, z_2, z_3 \in \mathbb{Z}[\sqrt{-5}]$ con $z_1 \neq (0, 0)$, si $z_1 z_2 = z_1 z_3$ entonces $z_2 = z_3$.

Teniendo en cuenta que este anillo cumple la propiedad cancelativa de la multiplicación, se enuncia el siguiente teorema cuya demostración es inmediata.

Teorema 1.12. El conjunto $\mathbb{Z}[\sqrt{-5}]$ con las operaciones suma y multiplicación es un dominio de integridad.

1.2.1. En búsqueda de un orden en $\mathbb{Z}[\sqrt{-5}]$

El presente aparte se ocupa de indagar si $\mathbb{Z}[\sqrt{-5}]$ es un anillo ordenado. Para ello alúdase inicialmente el hecho de que los números enteros son un dominio de integridad totalmente ordenado, debido a que en $\mathbb{Z}$ existe un subconjunto $\mathbb{Z}^+$ de números positivos el cual satisface las siguientes condiciones:

i $(\forall a, b \in \mathbb{Z}^+)\,[(a+b \in \mathbb{Z}^+) \wedge (ab \in \mathbb{Z}^+)]$

ii $(\forall a \in \mathbb{Z})\,(a \in \mathbb{Z}^+ \quad \veebar \quad a = 0 \quad \veebar \quad -a \in \mathbb{Z}^+)]$

Conjunto a partir del cual se define la relación $\leqslant$ que es un orden total en $\mathbb{Z}$, tal que para dos números enteros x, y cualesquiera se cumple:

1. $(a < b) \leftrightarrow (b - a \in \mathbb{Z}^+)$
2. $(a \leqslant b) \leftrightarrow (a < b \quad \vee \quad a = b)$

De modo que la expectativa radica en la posibilidad de hallar en el superconjunto $\mathbb{Z}[\sqrt{-5}]$ un orden total compatible con las operaciones, lo que es equivalente al interrogante acerca de la existencia de un conjunto de números positivos distinto del conjunto vacío.

Teorema 1.13. En $\mathbb{Z}[\sqrt{-5}]$ no existe un subconjunto P de números positivos.

Demostración. Supóngase que existe $P \subset \mathbb{Z}[\sqrt{-5}]$, $P \neq \emptyset$ el cual satisface las siguientes condiciones:

I $(\forall z, w \in P)\,[(z+w \in P) \wedge (zw \in P)]$

II $\left(\forall z \in \mathbb{Z}[\sqrt{-5}]\right)\,(z \in P \quad \veebar \quad z = (0,0) \quad \veebar \quad -z \in P)]$

Si $(1,0) \notin P$ por la condición II, $(-1,0) \in P$, y por I $(-1,0)(-1,0) = (1,0) \in P$, lo que es una contradicción, por tanto $(1,0) \in P$. Ahora como $(1,0) \in P$, por inducción sobre m, para todo $m \in \mathbb{Z}^+$, $(m,0) \in P$. Además, dado que $(0,x) \neq (0,0)$ por II $(0,x) \in P \quad \veebar \quad (0,-x) \in P$.

- Si $(0,x) \in P$ entonces $(0,x)(0,x) = (-5x^2, 0) \in P$, lo que es absurdo dado $(5x^2, 0) \in P$ pues $5x^2 \in \mathbb{Z}^+$. Por tanto $(0,x) \notin P$.
- Si $(0,-x) \in P$ entonces $(0,-x)(0,-x) = (-5x^2, 0) \in P$, lo que es absurdo dado que $(5x^2, 0) \in P$ pues $5x^2 \in \mathbb{Z}^+$. Luego $(0,-x) \notin P$.

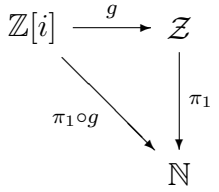
En consecuencia la suposición inicial es falsa y el teorema se cumple. □

Como se ha demostrado que en $\mathbb{Z}[\sqrt{-5}]$ no existe un conjunto de números positivos análogo al subconjunto $\mathbb{Z}^+$ de los números $\mathbb{Z}$, entonces no es posible definir una relación de orden inducida por P que sea total y compatible con las operaciones. Por tanto la idea ahora será hacer uso del hecho de que los números naturales poseen un orden total, para así, abordar el problema de definir un orden en $\mathbb{Z}[\sqrt{-5}]$ que sea compatible con la multiplicación, el cual será útil para el estudio de la divisibilidad en este superconjunto. Con este fin se expone a continuación el tratamiento que a este problema se da en el conjunto de los *Enteros Gaussianos*.

En este superconjunto para todo elemento z existe un elemento $\bar{z}$ que se denomina el *conjugado de* z, de modo que $z\bar{z} = (a^2 + b^2, 0)$. Esto motiva definir las funciones g, π_1 así:

$$\begin{array}{rcl} g : \mathbb{Z}[i] & \longrightarrow & \mathcal{Z} \\ (a,b) & \mapsto & (a^2+b^2, 0) \end{array} \qquad \begin{array}{rcl} \pi_1 : \mathcal{Z} & \longrightarrow & \mathbb{N} \\ (x,0) & \mapsto & x \end{array}$$

y con esto el diagrama



evidencia la posibilidad de definir una función $\gamma = \pi_1 \circ g$ tal que:

$$\begin{array}{rcl} \gamma : \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ (a,b) & \mapsto & a^2 + b^2 \end{array}$$

que permite caracterizar a cada elemento de $\mathbb{Z}[i]$ mediante un número natural, por medio del cual se define la relación $\preceq$ en $\mathbb{Z}[i]$ tal que:

$$(a,b) \preceq (c,d) \text{ si y solo si } \gamma((a,b)) < \gamma(c,d) \text{ o } (a,b) = (c,d)$$

relación que resulta ser un orden compatible con la operación multiplicación. Con base en esta idea a continuación se hace un tratamiento similar para el caso $\mathbb{Z}[\sqrt{-5}]$.

1.2.2. La función σ

Definición 1.4. El conjugado de un número $z = (a,b) \in \mathbb{Z}[\sqrt{-5}]$ es $\bar{z} = (a,-b)$

Definición 1.5. Sea $\sigma : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{N}$ de modo que:

$$\sigma((a,b)) = a^2 + 5b^2$$

A $\sigma(z)$ se le llama la σ-norma de z, la cual cumple las siguientes propiedades:

Teorema 1.14. Para todo $z, w \in \mathbb{Z}[\sqrt{-5}]$ se cumple que:

i) $\sigma(z) > 0$ para cualquier $z \neq (0,0)$

ii) $\sigma(z) = 0$ sí y solo si $z = (0,0)$

iii) $\sigma(zw) = \sigma(z)\sigma(w)$

iv) $\sigma(z) \leq \sigma(zw)$ con $w \neq (0,0)$

Demostración. La parte *i)* se cumple gracias a la definición de la función σ.

Para la parte *ii)* es evidente que si $z = (0,0)$ entonces $\sigma(z) = 0$, por tal razón se demostrará que si $\sigma(z) = 0$ entonces $z = (0,0)$. Supóngase que $z = (a,b)$ con $(a,b) \neq (0,0)$, por definición de la función σ se cumple que $\sigma(z) = a^2 + 5b^2$, y por definición del superconjunto $\mathbb{Z}[\sqrt{-5}]$ se tiene que $a, b \in \mathbb{Z}$, por lo tanto $\sigma(z) > 0$ esto por propiedades en los enteros; pero por hipótesis $\sigma(z) = 0$ lo cual es una contradicción dada la ley de la tricotomía en $\mathbb{N}$, entonces $z = (0,0)$.

Ahora pues, con el fin de demostrar *iii* hágase $z = (a,b),\ w = (c,d)$, por la definición de multiplicación en $\mathbb{Z}[\sqrt{-5}]$ y aplicando la función σ se tiene:

$$\begin{aligned}
\sigma(zw) &= \sigma((a,b)(c,d)) \\
&= \sigma(ac - 5bd, ad + bc) \\
&= (ac - 5bd)^2 + 5(ad + bc)^2 \\
&= (ac)^2 - 10acbd + (5bd)^2 + 5(ad)^2 + 10adbc + 5(bc)^2 \\
&= c^2\left(a^2 + 5b^2\right) + 5d^2\left(a^2 + 5b^2\right) \\
&= \left(a^2 + 5b^2\right)\left(c^2 + 5d^2\right) \\
&= \sigma(z)\sigma(w)
\end{aligned}$$

La cuarta parte se cumple gracias a *i), ii)* y *iii).* □

Ya definida la función σ e indicadas algunas de sus propiedades, a continuación se establece la siguiente relación en $\mathbb{Z}[\sqrt{-5}]$ inducida por σ.

Definición 1.6. Para todo z, w en $\mathbb{Z}[\sqrt{-5}]$ se dice que:

$$z \preceq w \text{ sí y solo si } \sigma(z) < \sigma(w) \text{ o } z = w$$

Teorema 1.15. La relación $\preceq$ es una relación de orden.

Demostración. Se procederá a probar que $\preceq$ es reflexiva: sea $z \in \mathbb{Z}[\sqrt{-5}]$, como $z = z$ para todo $z \in \mathbb{Z}[\sqrt{-5}]$, por definición 1.6 $z \preceq z$.

Transitiva: sean $z, w, r \in \mathbb{Z}[\sqrt{-5}]$ de tal manera que $z \preceq w$ y $w \preceq r$, de aquí por la definición 1.6 se tienen los siguientes casos:

Caso 1: $\sigma(z) < \sigma(w)$ y $\sigma(w) < \sigma(r)$.
Por transitividad de la relación $<$ en $\mathbb{N}$ se tiene que $\sigma(z) < \sigma(r)$ y por la definición 1.6 se concluye que $z \preceq r$.

Caso 2: $\sigma(z) < \sigma(w)$ y $w = r$.
Como $w = r$ sustituyendo se tiene que $\sigma(z) < \sigma(r)$ y por la definición 1.6 se obtiene que $z \preceq r$.

Caso 3: $z = w$ y $\sigma(w) < \sigma(r)$.
Como $z = w$ sustituyendo se tiene que $\sigma(z) < \sigma(r)$ y por la definición 1.6 se obtiene que $z \preceq r$.

Caso 4: $z = w$ y $w = r$.
Por transitividad en de la igualdad en $\mathbb{N}$ se tiene que $z = r$ y por definición 1.6 $z \preceq r$.

Así pues, se puede afirmar que la relación $\preceq$ es transitiva.

Antisimétrica: sean $z, w \in \mathbb{Z}[\sqrt{-5}]$ de tal manera que $z \preceq w$ y $w \preceq z$. Supóngase ahora que $z \neq w$, como $z \preceq w$ y $w \preceq z$, entonces por la definición de la relación se puede afirma que $\sigma(z) < \sigma(w)$ y $\sigma(z) < \sigma(w)$ lo cual es una contradicción, esto teniendo en cuenta la ley de la tricotomía en los números naturales, lo que permite concluir que $z = w$.

Así pues, queda demostrado que la relación $\preceq$ es una relación de orden en $\mathbb{Z}[\sqrt{-5}]$. □

Habiendo demostrado que $\preceq$ es una relación de orden, es natural cuestionarse si esta es compatible con la multiplicación, y por otro lado si ordena totalmente el conjunto. Con este fin se enuncia el siguiente teorema.

Teorema 1.16. *Monotonía de la multiplicación en* $\mathbb{Z}[\sqrt{-5}]$. Para todo $w, x, z \in \mathbb{Z}[\sqrt{-5}]$, si $w \preceq z$ y $x \neq (0, 0)$ entonces $wx \preceq zx$.

Demostración. Si $w \preceq z$, entonces por definición 1.6 se tienen los siguientes casos:

Caso 1: $\sigma(w) < \sigma(z)$.
Como $\sigma(w) < \sigma(z)$ y $x \neq (0,0)$, por teorema 1.14 parte i $\sigma(x) > 0$. Así pues, por propiedad de la monotonía de la relación $<$ en $\mathbb{N}$ se cumple que $\sigma(w)\sigma(x) < \sigma(z)\sigma(x)$. Ahora, como la función σ es multiplicativa (teorema 1.14 parte ii) entonces $\sigma(wx) < \sigma(zx)$. Finalmente usando la definición 1.6 se comprueba que $wx \preceq zx$.

Caso 2: $w = z$.
Si $w = z$ por propiedades de la igualdad en $\mathbb{N}$ se tiene que $wx = zx$ y por definición 1.6 $wx \preceq zx$. □

Así pues, la relación $\preceq$ es monótona con la multiplicación, sin embargo como era de esperarse, el orden inducido por la función σ no cumple la propiedad de monotonía de la suma, por ejemplo: sea $z = (1,1)$ y $w = (-2,1)$ se cumple que $z \preceq w$, pues $\sigma(z) < \sigma(w)$, ahora, si $x = (2,0)$ entonces $z + x = (3,1)$ y $w + x = (0,1)$, pero $w + x \preceq z + x$ pues $\sigma(0,1) < \sigma(3,1)$.

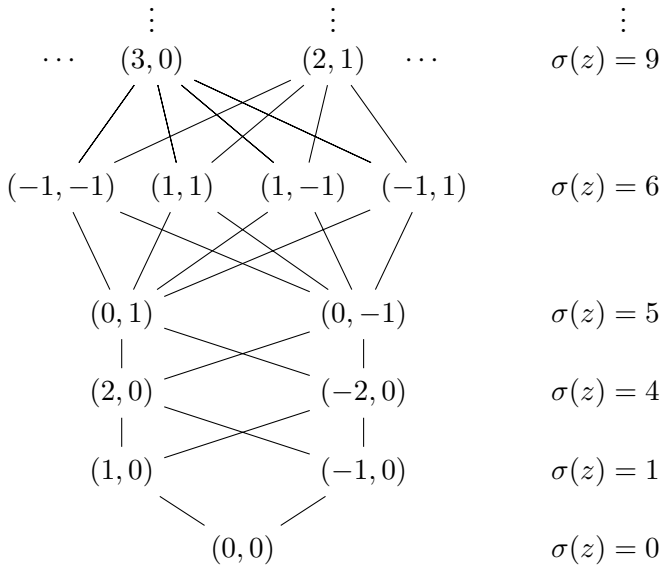


Figura 1.1: Diagrama de Hasse bajo la relación $\preceq$

Ahora queda por determinar si este superconjunto es totalmente ordenado mediante la relación $\preceq$. En este sentido, obsérvese que el diagrama de Hasse de la figura 1.1 elaborado a partir del orden establecido mediante la función σ permite afirmar, por ejemplo, que $(1,0) \preceq (0,-1)$ pues $\sigma(1,0) < \sigma(0,-1)$. Sin embargo, esto no implica que siempre sea posible comparar dos elementos mediante esta relación de orden, pues, por ejemplo dados los elementos $(3,0)$ y $(2,1)$, evidentemente diferentes, se tiene que $\sigma(3,0) = \sigma(2,1) = 9$ lo que implica que no

es posible afirmar que $(3,0) \preceq (2,1)$ o que $(2,1) \preceq (3,0)$. Lo anterior demuestra que el superconjunto $\mathbb{Z}[\sqrt{-5}]$ mediante la relación $\preceq$ es parcialmente ordenado.

1.2.3. La relación $\approx$ y el semigrupo cociente $(\mathbb{Z}[\sqrt{-5}]/\approx, *)$

Dada la existencia de elementos que no se pueden comparar se buscará definir un conjunto donde se tenga un orden total. Para ello se incluyen los siguiente teoremas:

Teorema 1.17. Sean z, w elementos no comparables de $\mathbb{Z}[\sqrt{-5}]$ entonces $\sigma(z) = \sigma(w)$.

Demostración. Supógase que $\sigma(z) \neq \sigma(w)$ entonces se debe cumplir que $\sigma(z) < \sigma(w)$ o $\sigma(z) > \sigma(w)$, es decir que z y w se pueden comparar mediante $\preceq$ lo que es una contradicción, por tanto $\sigma(z) = \sigma(w)$. □

Teniendo en cuenta el teorema anterior se define la siguiente relación en el conjunto $\mathbb{Z}[\sqrt{-5}]$.

Definición 1.7. Dos elementos $z, w \in \mathbb{Z}[\sqrt{-5}]$ están relacionados mediante $\approx$ si y solo si $\sigma(z) = \sigma(w)$.

Teorema 1.18. la relación $\approx$ es una relación de equivalencia.

Demostración. Sean $z, w, r \in \mathbb{Z}[\sqrt{-5}]$ por definición 1.7 $z \approx z$. Si $z \approx w$ por definición 1.7 $\sigma(z) = \sigma(w)$ por lo tanto $w \approx z$. Por último si $z \approx w$ y $w \approx r$ por definición 1.7 y transitividad de la relación de igualdad en $\mathbb{N}$ $\sigma(z) = \sigma(z)$ lo implica que $z \approx r$. Así pues, $\approx$ es una relación de equivalencia. □

Esta relación de equivalencia lleva a pensar en el cociente resultante entre el conjunto $\mathbb{Z}[\sqrt{-5}]$ y la relación $\approx$, así como en el interrogante de si esta relación de equivalencia es una congruencia para la multiplicación. Dicho lo anterior, el conjunto cociente $(\mathbb{Z}[\sqrt{-5}]/\approx)$ que se genera a partir de la relación $\approx$ es:

$$\mathbb{Z}[\sqrt{-5}]/\approx = \{[z] : z \in \mathbb{Z}[\sqrt{-5}]\}$$
$$[z] = [w] \text{ si y solo si } z \approx w$$

Ahora , para responder al interrogante de si la relación $\approx$ es una congruencia para la multiplicación hay que tener en cuenta que cada elemento $[z]$ de $\mathbb{Z}[\sqrt{-5}]/\approx$ tiene varios nombres o representantes, así pues, es necesario demostrar que la operación multiplicación en el cociente está bien definida, es decir, que su resultado no depende de la elección del representante.

Teorema 1.19. La relación $\approx$ es una congruencia para la multiplicación en $\mathbb{Z}[\sqrt{-5}]$.

Demostración. Para esto basta con probar que si $[z] = [z']$ y $[w] = [w']$ entonces $[zw] = [z'w']$. Así pues, si $[z] = [z']$ y $[w] = [w']$, entonces $z \approx z'$ y $w \approx w'$. Dado lo anterior por definición 1.7 se tiene $\sigma(z) = \sigma(z')$ y $\sigma(w) = \sigma(w')$ y como consecuencia de la monotonía de la multiplicación en $\mathbb{N}$ y de la propiedad multiplicativa de la función σ se tiene que $\sigma(zw) = \sigma(z'w')$, es decir que $zw \approx z'w'$ por definición 1.7, por tanto $[zw] = [z'w']$. □

De lo anterior se tiene que en $\mathbb{Z}[\sqrt{-5}]/\approx$ existe una operación bien definida notada como $*$ tal que $[z]*[w] = [zw]$ la cual hereda las propiedades de la multiplicación de $\mathbb{Z}[\sqrt{-5}]$, es decir, estructura de semigrupo conmutativo con unidad. Por el contrario, no se puede considerar la suma entre clases como una operación, pues por ejemplo $[(3,0)] = [(2,1)]$ sin embargo $[(3,0)] + [(1,0)] \neq [(2,1)] + [(1,0)]$.

Véase que la importancia de estudiar este cociente, radica en que al definir una relación de orden similar a $\preceq$ en donde los elementos son clases, trae como consecuencia el establecimiento de un orden total en $\mathbb{Z}[\sqrt{-5}]/\approx$, pues se reúnen en una misma clase aquellos elementos que correspondían a los no comparables.

Este orden es el resultante de la relación $\precapprox$ definida como:

$$[z] \precapprox [w] \text{ si y solo si } z \preceq w \text{ o } z \approx w$$

Teorema 1.20. La relación $\precapprox$ es un orden total.

Demostración. Supóngase por contradicción que existen $[z], [w] \in \mathbb{Z}[\sqrt{-5}]/\approx$ que no se pueden comparar mediante la relación $\precapprox$, es decir,

$$[z] \not\precapprox [w] \text{ y } [w] \not\precapprox [z]$$

Por la definición de la relación $\precapprox$ se tiene que:

$$z \not\preceq w \text{ y } z \not\approx w \tag{1.2}$$

$$w \not\preceq z \text{ y } w \not\approx z \tag{1.3}$$

De la primera parte de (1.2) y (1.3) se sabe que $z \approx w$ y de la segunda parte que $z \not\approx w$ lo cual es una contradicción, por lo tanto $[z] \precapprox [w]$ o $[w] \precapprox [z]$. □

En definitiva, como la multiplicación es una operación en $\mathbb{Z}[\sqrt{-5}]/\approx$ y las relaciones $\preceq$ y $\approx$ son monótonas con la multiplicación en $\mathbb{Z}[\sqrt{-5}]$ se puede afirmar que la relación $\precapprox$ es un orden total compatible con la operación definida entre clases.

1.2.4. El conjunto Σ de las σ-normas

En la figura 1.1 del diagrama de Hasse bajo la relación $\preceq$ se puede ver que las primeras imágenes de la función σ son 0,1,4,5,6,9, es decir que elementos como 2 o 3 no tienen preimagen en $\mathbb{Z}[\sqrt{-5}]$, esto es que no existen enteros x, y tales que $\sigma((x,y)) = 2$ o 3. Lo anterior motiva definir el conjunto de los elementos de $\mathbb{N}$ que son imagen directa de $\mathbb{Z}[\sqrt{-5}]$ por la función σ, es decir,

$$\sigma_! \left(\mathbb{Z}[\sqrt{-5}]\right) = \left\{a \in \mathbb{N} : \sigma(z) = a \text{ con } z \in \mathbb{Z}[\sqrt{-5}]\right\}$$

conjunto que en adelante se notara como Σ.

$$\Sigma = \sigma_! \left(\mathbb{Z}[\sqrt{-5}]\right)$$

Ahora considérese la estructura $(\Sigma, \cdot)$ donde $\cdot$ es el producto usual en $\mathbb{N}$. Para comenzar se verificará que $\cdot$ es cerrada en Σ, para ello alúdase al hecho de que la función σ es multiplicativa, esto es, dados dos elementos $a, b \in \Sigma$ donde $a = \sigma(z)$ y $b = \sigma(w)$ se tiene que $\sigma(z)\sigma(w) = \sigma(zw)$, lo que implica que $a \cdot b \in \Sigma$. Así pues $\cdot$ es una operación en Σ.

Retomando resultados de la sección anterior nótese que a cada clase de $\mathbb{Z}[\sqrt{-5}]/\approx$ le corresponde a una única σ-norma y a cada σ-norma le corresponde una única clase, lo que sugiere la existencia de un isomorfismo entre $(\mathbb{Z}[\sqrt{-5}], *)$ y $(\Sigma, \cdot)$, por lo cual se presenta el siguiente teorema.

Teorema 1.21. La estructura $(\mathbb{Z}[\sqrt{-5}]/\approx; *)$ es isomorfo al conjunto $(\Sigma, \cdot)$

Demostración. Sea la función h tal que:

$$\begin{array}{rcl} h : (\mathbb{Z}[\sqrt{-5}]/\approx; *) & \longrightarrow & (\Sigma; \cdot) \\ [z] & \mapsto & \sigma(z) \end{array}$$

Véase que efectivamente h con la operación multiplicación es un homomorfismo: Sean $[z], [w] \in \mathbb{Z}[\sqrt{-5}]/\approx$ se tiene que

$$\begin{aligned} h([z] * [w]) &= h([zw]) \\ &= \sigma(zw) \\ &= \sigma(z)\sigma(w) \\ &= h([z]) \cdot h([w]) \end{aligned}$$

Así pues, h con la operación multiplicación es un homomorfismo, y dado que es también biyectiva entonces h es además un isomorfismo, por lo tanto $(\mathbb{Z}[\sqrt{-5}]/\approx; *) \cong (\Sigma; \cdot)$ $\square$

Gracias al isomorfismo anterior es posible afirmar que el conjunto Σ con la operación multiplicación es un semigrupo conmutativo con unidad. También como era de esperarse se tiene que el orden definido en el cociente es el mismo orden de los naturales.

Teorema 1.22. Sean $z, w \in \mathbb{Z}[\sqrt{-5}]$, $[z] \precapprox [w]$ si y solo si $\sigma(z) \leq \sigma(w)$.

Demostración. Como $[z] \precapprox [w]$ por la definición de esta relación se tiene que $z \preceq w$ o $z \approx w$. Ahora, por la definición 1.6 y 1.7 se obtiene $\sigma(z) \leq \sigma(w)$

Como la demostración a derecha usa únicamente definiciones entonces la demostración a izquierda se hace devolviendo en este razonamiento. □

El cumplimiento de los teoremas anteriores da paso al estudio del conjunto $\mathbb{Z}[\sqrt{-5}]/\approx$, a partir del conjunto Σ, tarea que será abordada en el siguiente capítulo.

Capítulo 2

Caracterización del conjunto Σ

En este capítulo lo que se busca es establecer cuándo un número natural pertenece a Σ, propósito para el cual se buscó solucionar la ecuación diofántica $a = x^2 + 5y^2$. Por ejemplo, al intentar solucionar $2 = x^2 + 5y^2$ se puede ver que los posibles candidatos x, y son los naturales que den el menor resultado posible, es decir:

$$1^2 + 5(0^2) = 1; \quad 2^2 + 5(0^2) = 4; \quad 0^2 + 5(1^2) = 5$$

de esto se tiene que la ecuación $2 = x^2 + 5y^2$ no tiene solución, de donde se concluye que $2 \notin \Sigma$. Debido a la cantidad de cálculos necesarios para solucionar esta ecuación se diseñó un software que, por medio de la recursión, indica los a tales que alguna de las posibles combinaciones de x, y cumple que $a = x^2 + 5y^2$.

Gracias a este sofware se hallaron los primeros naturales que pertenecen al conjunto Σ, los cuales se presentan en la tabla 2.1

a	$[(x, y)]$	a	$[(x, y)]$
0	$[(0, 0)]$	16	$[(4, 0)]$
1	$[(1, 0)]$	20	$[(0, 2)]$
4	$[(2, 0)]$	21	$[(1, 2)]$
5	$[(0, 1)]$	24	$[(2, 2)]$
6	$[(1, 1)]$	25	$[(5, 0)]$
9	$[(2, 1)]$	29	$[(3, 2)]$
14	$[(3, 1)]$	30	$[(5, 1)]$

Tabla 2.1: Primeros $a \in \mathbb{N}$ tales que $a \in \Sigma$.

Una vez hecho esto, lo siguiente que se hizó fue empezar a clasificar los elementos que per-

tenecen a Σ para evidenciar alguna regularidad. Una de las primeras clasificaciones fue un arreglo módulo 4 que se muestra en la tabla 2.2, en la cual los elementos en negrilla son aquellos que no pertenecen a Σ. De esta tabla se puede observar que los elementos que no pertenecen a Σ son más fáciles de caracterizar, esto debido a que ninguna de las columnas de la tabla permite afirmar que todos sus elementos pertenecen a Σ. Sin embargo, sí es posible conjeturar que los elementos de la forma $4k+3$ no pertenecen al conjunto de las σ-normas.

$4k$	$4k+1$	$4k+2$	$4k+3$
0	1	**2**	**3**
4	5	6	**7**
8	9	**10**	**11**
12	**13**	14	**15**
16	**17**	**18**	**19**
20	21	**22**	**23**
24	25	**26**	**27**
28	29	30	**31**

Tabla 2.2: Arreglo de $\mathbb{N}$ módulo 4

De manera que una vía para caracterizar el conjunto Σ es la de averiguar qué elementos no pertenecen al codominio de la función σ. A continuación se presenta la prueba de la conjetura mencionada.

Teorema 2.1. Si $a \equiv 3 \mod 4$ entonces $a \notin \Sigma$.

Demostración. Sea $x, y \in \mathbb{Z}$, tanto x como y pueden ser de la forma $2m$ o $2m+1$, por tanto $x^2 = 4m^2$ o $x^2 = 4m^2+4m+1$, es decir que $x^2 \equiv 0, 1 \mod 4$[1] y $5y^2 \equiv 0, 1 \mod 4$. Así pues, luego de hacer todas las combinaciones de $x^2 + 5y^2$, se obtiene que $\sigma((x, y))$ es congruente con

$$0, 1, 2 \mod 4$$

Lo anterior permite concluir que no existe en el conjunto Σ elementos congruentes con 3 mód 4. □

Aunque ya se han caracterizado infinitos naturales que no pertenecen a Σ, aun existen más sin caracterizar. Con el fin de continuar con este proceso, se procede a duplicar el módulo 4 con la intención de preservar la columna que ya no pertenecen al conjunto Σ e intentar incluir los otros elementos que están en negrilla en alguna columna módulo 8.

[1]Esta notación hace referencia a que $x^2 \equiv 0 \mod 4$ o $x^2 \equiv 1 \mod 4$

0	1	**2**	**3**	4	5	6	**7**
8	9	**10**	**11**	**12**	**13**	14	**15**
16	**17**	**18**	**19**	20	21	**22**	**23**
24	25	**26**	**27**	**28**	29	30	**31**
32	**33**	**34**	**35**	36	**37**	**38**	**39**
40	41	**42**	**43**	**44**	45	46	**47**
48	49	**50**	**51**	**52**	**53**	54	**55**
56	**57**	**58**	**59**	**60**	61	**62**	**63**

Tabla 2.3: Arreglo de $\mathbb{N}$ módulo 8

Obsérvese que mediante el arreglo mostrado en la tabla 2.3 se halla que los elementos de la forma $8k+2, 8k+3$ y $8k+7$ no pertenecen a Σ, de los cuales, los elementos de la forma $8k+3$ y $8k+7$ están incluidos en los elementos de la forma $4k+3$. Por tanto, el nuevo caso que surge mediante este arreglo corresponde a los números de la forma $8k+2$. A continuación se presenta la prueba de esta conjetura.

Teorema 2.2. Si $a \equiv 2 \mod 8$ entonces $a \notin \Sigma$.

Demostración. Análogo al caso anterior, para todo $x, y \in \mathbb{Z}$ se tiene que $x^2 \equiv 0, 1, 4 \mod 8$ y $5y^2 \equiv 0, 5, 4 \mod 8$. Por tanto, luego de hacer todas las posibles combinaciones de $x^2 + 5y^2$, se obtiene que los residuos modulo 8 de $\sigma(x, y)$ son:

$$0, 1, 4, 5, 6 \mod 8$$

Lo anterior permite afirmar que no existe $a \in \Sigma$ tal que $a \equiv 2, 3, 7 \mod 8$. De estos casos los $\equiv 3, 7 \mod 8$ están incluidos en la congruencia 3 módulo 4, por lo tanto, queda demostrado que para todo $a \equiv 2 \mod 8$, $a \notin \Sigma$. □

Nuevamente al duplicar el módulo, resulta una conjetura basada en un arreglo módulo 16, proceso que puede ser reiterado aparentemente infinitas veces.

Teorema 2.3. Si $a \equiv 12 \mod 16$ entonces $a \notin \Sigma$.

Demostración. En un arreglo módulo 16, todo cuadrado perfecto es congruente con $0, 1, 4, 9$ mód 16, por tanto, cinco veces un cuadrado perfecto es congruente con $0, 5, 4, 13 \mod 16$. Al hacer todas las combinaciones posibles de $x^2 + 5y^2$, estas resultan congruentes con

$$0, 1, 4, 5, 6, 8, 9, 13, 14 \mod 16$$

entonces, se puede afirmar que los elementos

$$a \equiv 2, 3, 7, 10, 11, 12, 15 \mod 16$$

no pertenecen a Σ. De estos casos las congruencias $2, 10 \mod 16$ están incluidas en el caso $8k+2$ y las congruencias $3, 7, 11, 15 \mod 16$ están contenidas en el caso $4k+3$, por lo tanto el nuevo caso que emerge de este arreglo es el de los elementos de la forma $16k+12$, es decir que los elementos $a \equiv 12 \mod 16$ no pertenecen a Σ. □

Teorema 2.4. Si $a \equiv 8 \mod 32$ entonces $a \notin \Sigma$.

Demostración. La demostración es análogo a la ralizada en los casos anteriores □

Teniendo en cuenta los teoremas anteriores es posible conjeturar que para todo módulo de la forma $4(2^t)$ con $t \in \mathbb{N}$ existe un $m \in \mathbb{N}$ tal que los $a \equiv m \mod 4(2^t)$ cumplen que $a \notin \Sigma$, donde cada una de estas congruencias caracteriza nuevos elementos que no pertenecen a Σ y m corresponde al valor indicado en la siguiente tabla.

t	Caso
0	$a \equiv 3 \mod 4\,(2^0)$
1	$a \equiv 2 \mod 4\,(2^1)$
2	$a \equiv 12 \mod 4\,(2^2)$
3	$a \equiv 8 \mod 4\,(2^3)$

Tabla 2.4: Primeros casos donde $a \notin \Sigma$

Ahora, mediante la exploración y haciendo uso de la conjetura se halla que cuando $t = 4$ y $t = 5$ existen dos casos más, módulos 64 y 128. De modo que si $a \equiv 48 \mod 64$ o $a \equiv 32$ mód 128 entonces $a \notin \Sigma$. Teniendo en cuenta los 6 casos enunciados surgen dos teoremas como resultado de la organizacion de estos mediante la siguiente tabla.

0	$3 \mod 4$	$2 \mod 8$
1	$12 \mod 16$	$8 \mod 32$
2	$48 \mod 64$	$32 \mod 128$
⋮	⋮	⋮
k	$3(4^k) \mod 4^{k+1}$	$2(4^k) \mod 2(4^{k+1})$

Tabla 2.5: Generalización de casos

Así pues, la tabla 2.5 permite enunciar los siguientes teoremas. Para su demostración a continuación se demuestra el siguiente lema.

Lema 2.1. Si $m \in \Sigma$ y $m = 4l$ entonces $l \in \Sigma$.

Demostración. Como $m \in \Sigma$ y $m = 4l$ entonces $4l = x^2 + 5y^2$. Con el fin de demostrar que $l \in \Sigma$ se analizarán cuatro casos atendiendo a la paridad de los x, y.

- Supógase que $x = 2t + 1$ y $y = 2s + 1$ entonces $x^2 = 4k + 1$ y $5y^2 = 4r + 1$, por tanto $4l = 4z + 2$ lo que implica una contradicción pues $4 \nmid 4z + 2$, entonces x, y no son simultaneamente impares.
- Supóngase $x = 2t + 1$ y $y = 2s$ entonces $x^2 = 4k + 1$ y $5y^2 = 4r$, por tanto $4l = 4z + 1$ lo que es una contradicción pues $4 \nmid 4z + 1$, en conclusión no se cumple que x, y sean impar, par respectivamente.
- Supóngase que $x = 2t$ y $y = 2s + 1$ entonces $x^2 + 5y^2 = 4z + 1$. Como $4 \nmid 4z + 1$, no se cumple que x, y sean par e impar respectivamente.
- Si x, y pares entonces $x^2 + 5y^2 = 4t^2 + 20s^2$ es decir que $4l = 4(t^2 + 5s^2)$ lo que implica que $l = t^2 + 5s^2$ por lo tanto $l \in \Sigma$.

Por lo tanto si $m = 4l$ entonces $l \in \Sigma$. □

Teorema 2.5. Para todo $k \in \mathbb{N}$, si $m \equiv 3(4^k) \mod 4^{k+1}$ entonces $m \notin \Sigma$.

Demostración. Se razonará por inducción. Si $k = 0$ entonces por el teorema 2.1 si $m \equiv 3 \mod 4$ entonces $m \notin \Sigma$. Supóngase ahora que se cumple para $k = n$, es decir,

$$m \equiv 3(4^n) \mod 4^{n+1} \Rightarrow m \notin \Sigma.$$

Para demostrar que se cumple para $k = n + 1$ se razonará por contradicción. Supóngase que $m \in \Sigma$ y $m \equiv 3(4^{n+1}) \mod 4^{n+2}$. Como $m \equiv 3(4^{n+1}) \mod 4^{n+2}$ entonces:

$$\begin{aligned} m &= 3(4^{n+1}) + 4^{n+2}l \\ m &= 4\left(3(4^n) + 4^{n+1}l\right) \end{aligned} \tag{2.1}$$

Como $m \in \Sigma$ y por (2.1) $m = 4t$ con $t = 3(4^n) + 4^{n+1}l$ entonces por el lema 2.1 $t \in \Sigma$. Ahora, por hipótesis de inducción $t \notin \Sigma$, lo que resulta una contradicción, esto implica que $m \notin \Sigma$. El razonamiento anterior permite concluir que para todo $k \in \mathbb{N}$, si $m \equiv 3(4^k) \mod 4^{k+1}$ entonces $m \notin \Sigma$. □

Teorema 2.6. Para todo $k \in \mathbb{N}$, si $m \equiv 2(4^k) \mod 2(4^{k+1})$ entonces $m \notin \Sigma$.

Demostración. Análogo al caso anterior se razonará por inducción. Si $k = 0$ entonces por el teorema 2.2 si $m \equiv 2 \mod 8$ entonces $m \notin \Sigma$. Supóngase ahora que se cumple para $k = n$, es decir,

$$m \equiv 2(4^n) \mod 2(4^{n+1}) \Rightarrow m \notin \Sigma.$$

Para demostrar que se cumple para $k = n + 1$ se razonará por contradicción. Supóngase que $m \in \Sigma$ y $m \equiv 2(4^{n+1}) \mod 2(4^{n+2})$, entonces:

$$\begin{aligned} m &= 2(4^{n+1}) + 2(4^{n+2})l \\ m &= 4\left(2(4^n) + 2(4^{n+1})l\right) \end{aligned} \tag{2.2}$$

Como $m \in \Sigma$ y por (2.2) $m = 4t$ con $t = 2(4^n) + 2(4^{n+1})l$ entonces por el lema 2.1 $t \in \Sigma$. Ahora, por hipótesis de inducción $t \notin \Sigma$, lo que resulta una contradicción, esto implica que $m \notin \Sigma$. El razonamiento anterior permite concluir que para todo $k \in \mathbb{N}$, si $m \equiv 2(4^k) \mod 2(4^{k+1})$ entonces $m \notin \Sigma$. □

Los dos teoremas anteriores permiten hallar infinitos números enteros que no pertenecen a Σ, sin embargo, resta por responder el interrogante de si estos son los únicos elementos que no pertenecen al conjunto de las σ-normas o si por el contrario, hacen falta otros por caracterizar.

Nótese que los m caracterizados por el teorema 2.6 corresponden a elementos múltiplos de dos puesto que:

$$\begin{aligned} m &\equiv 2(4^n) \mod 2\left(4^{n+1}\right) \\ m &= 2(4^n) + 2\left(4^{n+1}\right) l \\ m &= 2\left(4^n + 4^{n+1}l\right) \end{aligned}$$

Caso similar ocurre con los elementos m caracterizados por el teorema 2.5 cuando $n \geq 1$,

$$\begin{aligned} m &\equiv 3(4^n) \mod 4^{n+1} \\ m &= 3(4^n) + 4^{n+1}l \\ m &= 4\left(3(4^{n-1}) + 4^n l\right) \end{aligned}$$

De modo que los teoremas anteriores con las condiciones enunciadas caracterizan elementos que no pertenecen a Σ que resultan ser pares, salvo el caso del teorema 2.5 cuando $k = 0$ donde resulta que $m \equiv 3 \mod 20$.

Teorema 2.7. Sea $k, r, m \in \mathbb{N}$ con $k \geq 1$ si $m \equiv 3(4^k) \mod 4^{k+1}$ o $m \equiv 3(4^r) \mod 4^{r+1}$ entonces m es par.

Haciendo uso de software se logró evidenciar que con estos dos teoremas se han caracterizado todos elementos pares que no pertenecen a Σ. Lo anterior sugiere la búsqueda de elementos que no pertenecen a Σ que sean impares y no sean congruentes con 3 módulo 4. Un primer elemento con estas características es el número 13 el cual es impar y es congruente con 1 módulo 4. Dado que $13 \notin \Sigma$ entonces existen más elementos que no pertenecen a Σ que no han sido caracterizados.

Con el objetivo de caracterizar estos elementos se elaboró un arreglo módulo 5 como se muestra en la tabla 2.6, del cual se halla que los naturales que no pertenecen al conjunto de las σ-normas son aquellos de la forma $5k+2$ y $5k+3$, hecho que permite enunciar el siguiente teorema.

$5k$	$5k+1$	$5k+2$	$5k+3$	$5k+4$
0	1	**2**	**3**	4
5	6	**7**	**8**	9
10	**11**	**12**	**13**	14
15	16	**17**	**18**	**19**
20	21	**22**	**23**	24
25	**26**	**27**	**28**	29
30	**31**	**32**	**33**	34

Tabla 2.6: Arreglo de $\mathbb{N}$ módulo 5

Teorema 2.8. Si $a \equiv 2, 3 \mod 5$ entonces $a \notin \Sigma$.

Demostración. En un arreglo módulo 5 los cuadrados perfectos están dados por:

$$\begin{gathered}(5k+1)^2 \equiv 1 \mod 5 \\ (5k+2)^2 \equiv 4 \mod 5 \\ (5k+3)^2 \equiv 4 \mod 5 \\ (5k+4)^2 \equiv 1 \mod 5 \\ (5k)^2 \equiv 0 \mod 5\end{gathered}$$

Por tanto, para todo $x, y \in \mathbb{Z}$ se tiene que $x^2 \equiv 0, 1, 4 \mod 5$ y $5y^2 \equiv 0 \mod 5$. En consecuencia los $a \in \Sigma$ son congruentes con:

$$0, 1, 4 \mod 5$$

Esto permite afirmar que en el conjunto Σ no existen elementos a tales que $a \equiv 2, 3 \mod 5$ □

Reiterando la busqueda con uso de softtware, se halla otro elemento que no pertenece a Σ que no está caracterizado por los teoremas 2.5, 2.6 o 2.7. Este elemento es el número 65, pues 65 no es múltiplo de 4, no es múltiplo de 2 y es equivalente con 0 módulo 5. Lo anterior sugiere la realización de un arreglo módulo 25, como se muestra en la tabla 2.7, la cual presenta negrilla los elementos que no pertenecen a Σ en la que se han suprimido las columnas correspondientes a los elementos $m \equiv 2, 3 \mod 5$, que son elementos $m \notin \Sigma$ previamente caracterizados por el teorema 2.7.

0	1	4	5	6	9	**10**	**11**	14	**15**	16	**19**	20	21	24
25	**26**	29	30	**31**	**34**	**35**	36	**39**	**40**	41	**44**	45	46	49
50	**51**	54	**55**	56	**59**	**60**	61	64	**65**	**66**	69	70	**71**	**74**
75	**76**	**79**	80	81	84	**85**	86	89	**90**	**91**	94	**95**	96	**99**
100	101	**104**	105	**106**	109	**110**	**111**	**114**	**115**	116	**119**	120	121	**124**
125	126	129	**130**	**131**	134	**135**	**136**	**139**	**140**	141	144	145	**146**	149
150	**151**	**154**	**155**	**156**	**159**	**160**	161	164	**165**	166	169	**170**	**171**	174
175	**176**	**179**	180	181	184	**185**	**186**	189	**190**	**191**	**194**	**195**	196	**199**
200	201	**204**	205	206	**209**	**210**	**211**	214	**215**	216	**219**	**220**	**221**	224
225	**226**	229	230	**231**	**234**	**235**	**236**	**239**	**240**	241	244	245	246	249
250	**251**	254	**255**	256	**259**	**260**	261	**264**	**265**	**266**	269	270	**271**	**274**
275	276	**279**	280	281	**284**	**285**	**286**	289	**290**	**291**	294	**295**	**296**	**299**

Tabla 2.7: Arreglo de $\mathbb{N}$ módulo 25

Obsérvese que en la tabla se hallan dos columnas en las que todos sus elementos no pertenecen a Σ, muchos de los cuales no han sido caracterizados. Estos elementos son los resaltados en color gris, correspondientes a los naturales de la forma $25k + 10$ y $25k + 15$. Lo que permite formular el siguiente teorema.

Teorema 2.9. Para todo $m \in \mathbb{N}$, si $m \equiv 10, 15 \mod 25$ entonces $m \notin \Sigma$

Demostración. En un arreglo módulo 25 los posibles residuos cuadráticos son los elementos congruentes con

$$0, 1, 4, 6, 9, 11, 14, 16, 19, 21, 24 \mod 25$$

de modo que $5y^2 \equiv 0, 5, 20 \mod 25$, por tanto los posibles residuos resultantes de la combinación $x^2 + 5y^2$ con $x, y \in \mathbb{Z}$ son congruentes con

$$0, 1, 4, 5, 6, 9, 11, 14, 16, 19, 20, 21, 24 \mod 25$$

en donde se concluye que los elementos que no pertenecen a Σ son los congruentes con

$$2, 3, 7, 8, 10, 12, 13, 15, 17, 18, 19, 22, 23 \mod 25$$

de los cuales los $m \equiv 2, 7, 12, 17, 22 \mod 25$ son congruentes con 2 módulo 5 y por tanto están contenidos en el teorema 2.7 al igual que los elementos congruentes con $3, 8, 13, 18, 23$ mód 25 que son congruentes con 3 módulo 5. En este sentido, los nuevos casos que surgen del arreglo módulo 25 son los referentes a los números de las formas $25k + 10$ y $25k + 15$ lo cual permite concluir que los $a \equiv 10, 15 \mod 25$ no pertenecen a Σ. □

Podría pensarse que con este teorema se han caracterizado todos los elementos que no pertenecen a Σ que son múltiplos de 5, sin embargo muchos de los elementos que se muestran en negrilla (elementos que no pertenecen a Σ) son múltiplos de 5 que no son congruentes con $10, 15 \mod 25$. Lo anterior sugiere la formulación del siguiente teorema resultante de multiplicar por 5 la congruencia anterior.

Teorema 2.10. Para todo $m \in \mathbb{N}$, si $m \equiv 75, 50 \mod 125$ entonces $m \notin \Sigma$

La demostración de este teorema es análoga a la del teorema inmediatamente anterior. Estos últimos tres teoremas permiten conjeturar que para todo módulo de la forma 5^{k+1} con $k \in \mathbb{N}$ existe un $m \in \mathbb{N}$ tal que para todo $a \equiv m \mod 5^{k+1}$ se cumple que $a \notin \Sigma$, donde m corresponde al valor indicado en la tabla 2.8. Cabe recalcar que cada una de estas congruencias caracteriza nuevos elementos que no pertenecen a Σ.

k	m	mód 5^{k+1}
0	$2, 3$	mód 5^1
1	$10, 15$	mód 5^2
2	$50, 75$	mód 5^3
$\vdots$	$\vdots$	
n	$3\left(5^n\right), 2\left(5^n\right)$	mód 5^{n+1}

Tabla 2.8: Generalización de casos módulo 5^{k+1}

De modo que análogo a los sucedido anteriormente con las congruencias de la forma 4^{k+1} es posible generalizar estos casos en un teorema. Para su demostración se prueba primero el siguiente lema.

Lema 2.2. Si $m \in \Sigma$ y $m = 5l$ entonces $l \in \Sigma$.

Demostración. Como $m \in \Sigma$ entonces existen $x, y \in \mathbb{N}$ tales que $x^2 + 5y^2 = 5l$, por lo tanto $x^2 = 5(l - y^2)$ esto implica que x es múltiplo de 5. Sea $x = 5t$ entonces $25t^2 + 5y^2 = 5l$ por lo tanto $5t^2 + y^2 = l$, es decir que $l \in \Sigma$. □

Teorema 2.11. Para todo $m, k \in \mathbb{N}$, si $m \equiv 3(5^k), 2(5^k) \mod 5^{k+1}$ entonces $m \notin \Sigma$

Demostración. Se razonará por inducción. Si $k = 0$ entonces por el teorema 2.7 si $m \equiv 2, 3$ mód 5 entonces $m \notin \Sigma$. Supóngase ahora que se cumple para $k = n$, es decir,

$$m \equiv 3(5^n),\ 2(5^n) \mod 5^{n+1} \Rightarrow m \notin \Sigma.$$

Para demostrar que se cumple para $k = n + 1$ se razonará por contradicción. Supóngase que $m \in \Sigma$ y $m \equiv 3(5^{n+1}), 2(5^{n+1}) \mod 5^{n+2}$, entonces:

$$\begin{aligned} m = 3(5^{n+1}) + 5^{n+2}l \quad &\text{o} \quad m = 2(5^{n+1}) + 5^{n+2}l \\ m = 5(3(5^n) + 5^{n+1}l) \quad &\text{o} \quad m = 5(2(5^n) + 5^{n+1}l) \end{aligned} \tag{2.3}$$

Como $m \in \Sigma$ y por (2.3) $m = 5t$ y por el lema 2.2 $t \in \Sigma$. Ahora, por hipótesis de inducción $t \notin \Sigma$, lo que resulta una contradicción, esto implica que $m \notin \Sigma$. El razonamiento anterior permite concluir que para todo $k \in \mathbb{N}$, si $m \equiv 3(5^k),\ 2(5^k) \mod 5^{k+1}$ entonces $m \notin \Sigma$. □

Lo anteriormente expuesto permite afirmar que si m es congruente con alguna de las siguientes congruencias, entonces $m \notin \Sigma$

$$\begin{aligned} m &\equiv 3(4^k) \mod 4^{k+1} \\ m &\equiv 2(4^k) \mod 2(4^{k+1}) \\ m &\equiv 3(5^k), 2(5^k) \mod 5^{k+1} \end{aligned}$$

Sin embargo el recíproco de la afirmación anterior no es cierta, ya que por ejemplo el elemento 209, que no pertenece a Σ, no corresponde con ninguna de las congruencias presentadas anteriormente; pues no es par, ni múltiplo de 5 y resulta que $65 \equiv 1 \mod 4$ y $65 \equiv 0 \mod 5$. Esto alude a la existencia de otros elementos que no pertenecen a Σ, los cuales no cumplen las congruencias enunciadas. De modo que se hizo necesaria una minuciosa observación y exploración, mediante la cual se ha logrado observar que los elementos que restan por caracterizar son algunos de los múltiplos de las potencias impares de los primos enteros $11, 13, 17, 19$ o de primos como $31, 37, 53, 59$ que resultan ser congruentes con $11, 13, 17, 19$ módulo 20. Para demostrar esta observación es necesario formalizar primero lo que significa que un número sea residuo cuadrático módulo p, establecer algunas de sus propiedades y enunciar resultados de la teoría de números como la Ley de la reciprocidad cuadrática.

Definición 2.1. Sea p un primo impar y a un entero, si la congruencia $x^2 \equiv a \mod p$ tiene solución, se dice entonces que a es un residuo cuadrático módulo p.

Esta idea de residuo cuadrático no es nueva, pues se ha venido usando desde los primeros teoremas que caracterizan a los elementos que no pertenecen a Σ. Ahora, para facilitar el estudio de los residuos cuadráticos se introduce la notación debida a *Legendre*.

Definición 2.2. Sea $p > 0$ un primo impar y a un número entero. Se define el símbolo de Legendre $\big(a/p\big)$ como:

$$\big(a/p\big) = \begin{cases} 1 \text{ si } a \text{ es un residuo cuadrático módulo } p \\ -1 \text{ si } a \text{ no es un residuo cuadrático módulo } p \\ 0 \text{ si } p \mid a. \end{cases}$$

Entre algunas propiedades importantes se encuentran:

Teorema 2.12. Sea p un primo impar y a, b enteros cualesquiera. Entonces:

i) $\big(a/p\big)\big(b/p\big) = \big(ab/p\big)$

ii) $\big(-1/p\big) = (-1)^{\frac{p-1}{2}}$

Este teorema se demuestra haciendo uso del criterio de Euler [2]. A continuación se presenta un teorema que permite hallar el carácter cuadrático de cualquier primo impar p.

Teorema 2.13 (Ley de la reciprocidad cuadrática)**.** Sean p y q primos impares distintos se cumple que:

$$\big(p/q\big)\big(q/p\big) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$$

Esta ley fue descubierta por primera vez por Euler y posteriormente redescubierta por Legendre quien la demostró parcialmente.[3] Teniendo en cuenta los resultados anteriores, a continuación se demuestra el siguiente teorema.

Teorema 2.14. $\big(-5/p\big) = 1$ si y solo si $p \equiv 1, 3, 7, 9 \mod 20$

[2] El criterio de Euler establece que $\big(a/p\big) \equiv a^{\frac{p-1}{2}} \mod p$, su demostración al igual que la del teorema 2.12 se puede consultar en: Jiménez, L., Gordillo, J. & Rubiano, G. (2004). *Teoría de números para principiantes.* Bogotá: Universidad Nacional de Colombia, Pg:158.

[3] La prueba completa de esta ley se puede encontrar en: Ivorra C. (s.f). *Álgebra* , Valencia: Universidad de Valencia, Pg:250.

Demostración. Como $\big(-5/p\big) = 1$ haciendo uso de los teoremas 2.12 y 2.13, se tiene que:

$$\begin{aligned}\big(-5/p\big) &= \big(-1/p\big)\big(5/p\big)\\ &= (-1)^{\frac{p-1}{2}}\big(5/p\big)\\ &= (-1)^{\frac{p-1}{2}}\big(p/5\big)(-1)^{\frac{(p-1)}{2}\frac{(5-1)}{2}}\\ &= (-1)^{\frac{p-1}{2}}\big(p/5\big)(-1)^{p-1}\end{aligned}$$

además

$$\big(p/5\big) = \begin{cases} 1 \text{ si } p \equiv 1 \mod 5\\ 1 \text{ si } p \equiv 4 \mod 5\\ -1 \text{ si } p \equiv 2 \mod 5\\ -1 \text{ si } p \equiv 3 \mod 5\end{cases}$$

y como

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } p \equiv 1 \mod 4\\ -1 \text{ si } p \equiv 3 \mod 4\end{cases}$$

y $(-1)^{p-1} = 1$ para cualquier p, entonces

$$\big(-5/p\big) = \begin{cases} 1 \text{ si } p \equiv 1 \mod 4 \text{ y } p \equiv 1 \mod 5\\ 1 \text{ si } p \equiv 1 \mod 4 \text{ y } p \equiv 4 \mod 5\\ 1 \text{ si } p \equiv 3 \mod 4 \text{ y } p \equiv 2 \mod 5\\ 1 \text{ si } p \equiv 3 \mod 4 \text{ y } p \equiv 3 \mod 5\end{cases}$$

Resolviendo el primer sistema de congruencias lineales, como $p \equiv 1 \mod 5$, entonces $p = 5k + 1$ donde k es un número entero. Sustituyendo en la segunda congruencia se obtiene,

$$\begin{aligned}5k + 1 &\equiv 1 \mod 4\\ 5k &\equiv 0 \mod 4\\ k &\equiv 0 \mod 4\end{aligned}$$

y como $k \equiv 0 \mod 4$, entonces $k = 4s$ y $p = 5(4s) + 1 = 20s + 1$ donde s es un entero, por tanto:

$$p \equiv 1 \mod 20$$

De manera análoga para el segundo sistema, como $p \equiv 4 \mod 5$, entonces $p = 5k + 4$. Sustituyendo en la segunda congruencia se obtiene,

$$\begin{aligned}5k + 4 &\equiv 1 \mod 4\\ 5k &\equiv -3 \mod 4\\ k &\equiv 1 \mod 4\end{aligned}$$

entonces $k = 4s + 1$ donde s es un entero y $p = 5(4s + 1) + 4 = 20s + 9$, por tanto:

$$p \equiv 9 \mod 20$$

Luego de solucionar los cuatro sistemas de congruencias se tiene finalmente que

$$\big(-5/p\big) = \begin{cases} 1 \text{ si } p \equiv 1 \mod 20 \\ 1 \text{ si } p \equiv 9 \mod 20 \\ 1 \text{ si } p \equiv 7 \mod 20 \\ 1 \text{ si } p \equiv 3 \mod 20 \end{cases}$$

Así pues se tiene que si $p \mid x^2 + 5y^2$ y $(x, y) = 1$, entonces $p \equiv 1, 3, 7, 9 \mod 20$.

La implicación a izquierda de este teorema se puede obtener devolviéndose en la prueba. □

Teorema 2.15. Sea p primo en $\mathbb{N}$ con $p \neq 2, 5$ si $p \mid x^2+5y^2$ y $(x, y) = 1$ entonces $p \equiv 1, 3, 7, 9$ mód 20.

Demostración. Inicialmente se debe probar que si $p \mid x^2 + 5y^2$ y $(x, y) = 1$ entonces y resulta ser primo relativo con p lo que alude a la existencia del inverso multiplicativo módulo p de y.

Supóngase que $(p, y) \neq 1$, entonces $(p, y) = d$ lo que implica que $d \mid p$ y $d \mid y$. Dado que p es primo, $d = p$ y por tanto $p \mid y$.

Ahora pues, como $p \mid y$ entonces $5y^2 \equiv 0 \mod p$ y como $x^2 \equiv -5y^2 \mod p$, por transitividad de la congruencia, $x^2 \equiv 0 \mod p$, es decir que $p \mid x$ lo que implica que $(x, y) = p$. Esto es una contradicción, por lo tanto $(p, y) = 1$.

Como y tiene inverso multiplicativo módulo p, existe z tal que $yz \equiv 1 \mod p$. Esto implica que $(xz)^2 \equiv -5 \mod p$, es decir que $(-5/p) = 1$ y por el teorema 2.14 $p \equiv 1, 3, 7, 9 \mod 20$ □

Teniendo como insumo el teorema 2.15 a continuación se demuestra el siguiente teorema que caracteriza los elementos que no pertenecen a Σ que hacen falta por caracterizar.

Teorema 2.16. Sea $a, p \in \mathbb{N}$ con $p \equiv 11, 13, 17, 19 \mod 20$ y p^r la mayor potencia que divide a a, si r es impar entonces $a \notin \Sigma$.

Demostración. Supóngase por contradicción que $a \in \Sigma$ y cumple las condiciones dadas, es decir, p^r es la mayor potencia que divide a a donde r es impar y $p \equiv 11, 13, 17, 19 \mod 20$. Como $a \in \Sigma$, $a = x^2+5y^2$ con $x, y \in \mathbb{N}$, así pues se tienen 3 casos para los valores que pueden tomar x, y.

- **Caso i.** Si $x, y \neq 0$
  Como $p \equiv 11, 13, 17, 19 \mod 20$ por el teorema 2.15 $(x, y) \neq 1$, lo que implica que $(x, y) = d$, así pues deben existir $m, n \in \mathbb{N}$ tales que $md = x$ y $nd = y$ con $(m, n) = 1$. Ahora pues, como $p^r \mid a$ entonces $p \mid x^2 + 5y^2$, es decir, $p \mid d^2(m^2 + 5n^2)$.

  Por definición de número primo en $\mathbb{N}$ se tiene que $p \mid d^2$ o $p \mid m^2 + 5n^2$. Si $p \mid m^2 + 5n^2$, como $(m, n) = 1$ por el teorema 2.15 $p \equiv 1, 3, 7, 9 \mod 20$ lo que corresponde a una contradicción pues $p \equiv 11, 13, 17, 19 \mod 20$, de modo que que $p \mid d^2$ y por lo tato $p \mid d$. Sea p^t la mayor potencia que divide a d, es decir que $d = p^t k$ con $(k, p) = 1$ entonces $d^2 = p^{2t}k^2$. Ahora como $p \nmid m^2 + 5n^2$ entonces $p^r \nmid m^2 + 5n^2$ por lo tanto $p^r \mid d^2$.

  Como p^r es la mayor potencia que divide a a, es entonces también la mayor potencia que divide a d^2, por lo tanto $p^2 t = p^r$, de modo que $r = 2t$, pero por hipótesis r es impar, lo que alude a una contradicción, por tanto $a \notin \Sigma$.

- **Caso ii.** Si $x = 0$
  Como $p \mid a$ entonces $p \mid 5y^2$. Ahora, por definición de primo en $\mathbb{N}$ y como $p \equiv 11, 13, 17, 19 \mod 20$ entonces $p \mid y^2$ lo que implica que $p \mid y$.

  Sea p^t la mayor potencia que divide a y, es decir que $y = p^t k$ con $(k, p) = 1$ entonces $5y^2 = p^{2t}(5k^2)$ y $(5k^2, p) = 1$ de modo que la mayor potencia que divide a a es p^{2t} lo que es una contradicción pues r es impar.

- **Caso iii.** Si $y = 0$
  Como $p \mid x^2$ entonces $p \mid x$. Sea $t \in \mathbb{N}$ tal que $p^t \mid x$ con $p^t k = x$ y $(p, k) = 1$ entonces $x^2 = p^{2t}k^2$. Lo anterior es una contradicción pues la mayor potencia de p que divide a a es impar.

Como conclusión de los tres casos anteriores $a \notin \Sigma$. □

Ya culminada la prueba del teorema 2.16, se diseñó un programa el cual comparaba el conjunto de los elementos que no pertenecen a Σ con el conjunto de los elementos caracterizados por los teoremas 2.5, 2.6, 2.11, 2.16, el cual mostró que dichos conjuntos eran iguales, por lo cual es posible conjeturar que estos 4 teoremas permiten caracterizar a todos los elementos que no pertenecen a Σ. Ahora se procede a verificar si estos teoremas son necesarios para la caracterización de estos elementos.

Con este fin se hizo una exploración, mediante la cual se verificó que los elementos caracterizados por el teorema 2.11 se pueden también caracterizar por los teoremas 2.5, 2.6 o

2.16, como se puede observar en tabla 2.9. De manera que se excluirá el teorema 2.11 de las condiciones necesarias y suficientes para caracterizar los $m \notin \Sigma$.

$m \notin \Sigma$	Teorema 2.11	Teorema 2.5	Teorema 2.6	Teorema 2.16
10	$\equiv 10 \mod 25$		$\equiv 8 \mod 32$	
15	$\equiv 15 \mod 25$	$\equiv 3 \mod 4$		
35	$\equiv 10 \mod 25$	$\equiv 3 \mod 4$		
40	$\equiv 15 \mod 25$		$\equiv 8 \mod 32$	
50	$\equiv 50 \mod 125$		$\equiv 2 \mod 8$	
60	$\equiv 10 \mod 25$	$\equiv 12 \mod 16$		
65	$\equiv 15 \mod 25$			$13 \cdot 5$
75	$\equiv 75 \mod 125$	$\equiv 3 \mod 4$		
85	$\equiv 10 \mod 25$			$17 \cdot 5$
90	$\equiv 15 \mod 25$		$\equiv 2 \mod 8$	
95	$\equiv 10 \mod 25$	$\equiv 3 \mod 4$		$19 \cdot 5$
110	$\equiv 10 \mod 25$			$11 \cdot 10$

Tabla 2.9: Casos a los que pertenecen los elementos del teorema 2.10

Ahora, se debe determinar si los teoremas 2.5, 2.6, 2.16 son independientes, para ello basta con averiguar si existen elementos que solo puedan ser caracterizados mediante una y solo una de las condiciones enunciadas.

Con este fin obsérvese, que la tabla 2.9 también permite verificar que dado un elemento que no pertenece a Σ, si este se encuentra bajo la caracterización del teorema 2.5, no cumple la congruencia del teorema 2.6; lo que sugiere que los dos conjuntos formados por los elementos caracterizados por estos teoremas son disyuntos, como se demuestra a continuación.

Teorema 2.17. Sea $j, k \in \mathbb{N}$, $\forall m \notin \Sigma$, $m \equiv 3(4^j) \mod 4^{j+1}$ sí y solo si $m \not\equiv 2(4^k) \mod 2(4^{k+1})$

Demostración. Supóngase que $m \equiv 2(4^k) \mod 2(4^{k+1})$ como $m \equiv 3(4^j) \mod 4^{j+1}$ entonces

$$m = 4^{j+1}l + 3(4^j) \tag{2.4}$$
$$m = 2(4^{k+1})t + 2(4^k) \tag{2.5}$$

igualando (2.4) y (2.5) resulta:

$$2(4^{k+1})t + 2(4^k) = 4^{j+1}l + 3(4^j)$$

Según la ley de la tricotomía se presentan los siguientes casos:

Caso 1: Si k=j entonces

$$\begin{aligned} 4^k[2(4t)+2] &= 4^k[4l+3] \\ 2(4t)+2 &= 4l+3 \end{aligned}$$

lo que es una contradicción pues $4l+3$ es un número impar.

Caso 2: Si $j<k$ con $k=j+r$ entonces

$$\begin{aligned} 4^{j+r}[2(4t)+2] &= 4^j[4l+3] \\ 2(4^r)[4t+1] &= 4l+3 \end{aligned}$$

Lo que resulta una contradicción pues $4l+3$ es impar.

Caso 3: Si $k<j$ con $j=k+s$ entonces

$$\begin{aligned} 4^k[2(4t)+2] &= 4^{k+s}[4l+3] \\ 2[4t+1] &= 4^s[4l+3] \\ 4t+1 &= 2,4^{s-1}[4l+3] \end{aligned}$$

Lo que resulta una contradicción pues $4t+1$ es impar. Esto permite concluir que la suposición inicial es falsa, por tanto si $m \equiv 3(4^j) \mod 4^{j+1}$ entonces $m \not\equiv 2(4^k) \mod 2(4^{k+1})$. La implicación a izquierda se demuestra de manera análoga. □

Para probar que el teorema 2.16 es independiente de los teoremas 2.6 y 2.5, es necesario mostrar que existe un elemento que únicamente puede ser caracterizado por el teorema 2.16. Para ello obsérvese que el elemento 319 el cual no pertenece a Σ, cumple que $319 = 29 \cdot 11$, por tanto es caracterizado por el teorema 2.16, y como este no es par ni es congruente con 3 módulo 4, entonces no es caracterizado por los otros dos teoremas

Finalmente para mostrar que los teoremas 2.5 y 2.6 son independientes del teorema 2.16, se tiene como ejemplo que existen números como 3 y 2 congruentes con 3 mód 4 y 2 mód 8 respectivamente, los cuales no pueden escribirse como múltiplos de elementos congruentes con $11, 13, 17, 19$ módulo 20.

En resumen los teoremas 2.5, 2.6 y 2.16 son necesarios y suficientes para caracterizar los elementos que no pertenecen a Σ. Esto conduce a enunciar el teorema 2.18, cuya demostración es inmediata.

Teorema 2.18. Sea $m \in \mathbb{N}$ si m cumple alguno de los siguientes criterios entonces $m \notin \Sigma$.

i) Para algún $k \in \mathbb{N}$, $m \equiv 3(4^k) \mod 4^{k+1}$

ii) Para algún $k \in \mathbb{N}$, $m \equiv 2(4^r) \mod 2(4^{r+1})$

iii) Existe p factor primo de m tal que $p \equiv 11, 13, 17, 19 \mod 20$ y p^k con k impar la mayor potencia que divide a m

A pesar de que el recíproco de este teorema se ha verificado por medio software; no se tiene aun una prueba que justifique que para todo m, si $m \notin \Sigma$ entonces m cumple alguno de los ítems del teorema 2.18. Véase que la importancia de esta conjetura es que establece la pertenencia de un elemento en el conjunto Σ.

Conjetura 2.1 (Criterio de pertenencia)**.** Sea $m \in \mathbb{N}$, si $m \notin \Sigma$ entonces m cumple alguno de los siguientes criterios:

i) Para algún $k \in \mathbb{N}$, $m \equiv 3(4^k) \mod 4^{k+1}$

ii) Para algún $k \in \mathbb{N}$, $m \equiv 2(4^r) \mod 2(4^{r+1})$

iii) Existe p factor primo de m tal que $p \equiv 11, 13, 17, 19 \mod 20$ y p^k con k impar la mayor potencia que divide a m

Capítulo 3

Proceso de Analizar en Σ

En el estudio de una estructura algebraica el proceso de analizar se presenta de dos maneras: análisis *en* la estructura y análisis *de* la estructura el primero entendido como descomponer un elemento del conjunto en términos de otros a partir de relaciones, operaciones y propiedades definidas entre ellos, los cuales son identificados como elementos distinguidos; esto se puede ejemplificar en la descomposición en factores primos de un número en el conjunto de los números naturales o de los números enteros. El segundo entendiendo como la descomposición de la estructura a partir de sus subestructuras; por ejemplo las particiones de un conjunto[1].

En los números naturales mediante la operación multiplicación, se define una relación de divisibilidad con la cual es posible identificar tres elementos especiales: el cero, la unidad y los primos. El cero es especial en tanto que, además de ser el módulo para la suma, todo elemento número natural lo divide. Por otro lado la unidad al ser el módulo para la multiplicación, se considera distinguido pues divide a todo número natural. Finalmente, los primos en $\mathbb{N}$ se definen como aquellos que siendo distintos de la unidad son divisibles únicamente por ellos mismos y la unidad. Estos últimos son considerados especiales, entre otras cosas, porque todo elemento del conjunto se puede expresar como producto de primos de manera única.

Así pues, el presente capítulo tiene como propósito presentar el proceso matemático de analizar en $(\Sigma, \cdot)$, el cual se estudiará mediante una relación de divisibilidad definida a partir de la operación multiplicación. Dicho proceso es puesto en evidencia mediante la descomposición de elementos del conjunto en términos de otros previamente caracterizados, análogo al proceso que se realiza en los números naturales.

[1] Ángel, L., Luque, C., & Sánchez, Y. (2014). *El proceso matemático de analizar en teoría de números: una aproximación desde la relación de divisibilidad.* XII Coloquio regional de matemáticas y II Simposio de Estadística.

En este sentido, para llevar a cabo esta tarea se define a continuación una relación de divisibilidad en Σ.

Definición 3.1. Sean $a, b \in \Sigma$, se dice que a divide a b, denotado por $a \mid_{\Sigma} b$ si y sólo si existe un $c \in \Sigma$ tal que $ac = b$.

En este conjunto hay diferencias con respecto a los números naturales, una diferencia es que en Σ no se tiene suma, mientras que si se cuenta con un orden el cual como ya se demostró coincide con el orden de los naturales y con el orden definido en el cociente $\mathbb{Z}[\sqrt{-5}]/\approx$.

Ahora como $\Sigma \subset \mathbb{N}$ se puede decir que si $a \mid_{\Sigma} b$ entonces $a \mid b$ lo cual indica que la primera relación está contenida en la otra. Con respecto a las propiedades de la divisibilidad definida en Σ véase que esta relación es reflexiva, pues el 1 pertenece a Σ, además hereda la propiedad antisimétrica de la divisibilidad en $\mathbb{N}$ y dado que la multiplicación en Σ es asociativa, esta relación resulta transitiva.

Lo que se quiere mirar ahora es si se cumple el teorema fundamental de la aritmética (TFA), es decir, si todo número compuesto se puede expresar como el producto de factores primos y de manera única. Para estudiar el cumplimiento de este teorema en Σ, lo primero que se tiene que hacer es caracterizar algunos elementos.

En Σ el 0 sigue siendo un elemento distinguido ya que este anula para la multiplicación, de manera que todo elemento en Σ lo divide. El 1 nuevamente como neutro para la multiplicación en Σ juega un papel importante pues cumple que $\forall a \in \Sigma$, $1 \mid_{\Sigma} a$, por lo cual se le denomina unidad. Ahora, de acuerdo con la definición de primo en $\mathbb{N}$, los elementos $4, 6$ y 9 son primos en Σ, pues sus divisores en $\mathbb{N}$ no pertenecen a Σ debido a que $2 \equiv 2 \mod 8$ y $3 \equiv 3 \mod 5$.

Obsérvese que en este conjunto el elemento 36 se puede descomponer como:

$$36 = 4 \cdot 9 = 6 \cdot 6$$

lo cual muestra que la factorización no es única, más aún, se tiene que,

$$6 \mid_{\Sigma} 4 \cdot 9$$

sin embargo, no se cumple que:

$$6 \mid_{\Sigma} 4 \text{ o } 6 \mid_{\Sigma} 9$$

Es decir que en Σ los elementos que tienen exactamente dos divisores no cumplen una de las principales características que tienen los primos, la cual coincide con la definición de primo en teoría algebraica de números, es decir

$$\text{Siempre que } p \mid ab \text{ entonces } p \mid a \text{ o } p \mid b$$

En los conjuntos usuales las definiciones dadas de primo son equivalentes, sin embargo en Σ los elementos como $6, 4$ y 9 que no cumplen la condición anterior y tienen exactamente dos divisores se denominaran *irreducibles*, esto en tanto que ellos no se pueden expresar como el producto de otros dos sin usar la unidad y a ellos mismos.

Definición 3.2. Un elemento r en Σ es irreducible si y solo sí tiene exactamente dos divisores.

Nótese que todo primo es irreducible, pero como ya se mostró en el ejemplo anterior, en Σ no todo irreducible es primo. Es por esto que en lugar de hacer una caracterización en términos de primos e irreducibles, se hablará de manera general de elementos irreducibles en Σ y dirá que un elemento es primo refiriendose a los primos de los naturales.

Para caracterizar los elementos irreducibles en Σ, obsérvese que los primeros candidatos son los primos de $\mathbb{N}$ que también pertenecen a Σ. Supóngase que se cumple que existen primos p en $\mathbb{N}$ tales que $p \in \Sigma$. Ahora como en $\mathbb{N}$ los números primos son congruentes con 1 o 3 módulo 4 y por el teorema 2.1 se tiene que los $p \equiv 3 \mod 4$ no pertenecen a Σ entonces p debe ser congruente con 1 módulo 4. La exploración anterior motiva a la presentación del siguiente teorema.

Teorema 3.1. Sea p primo en $\mathbb{N}$, si $p \in \Sigma$ entonces $p \equiv 1 \mod 4$

Sin embargo, el recíproco de este teorema no es cierto, pues no todo primo entero congruente con 1 módulo 4 pertenece a Σ. Por ejemplo, $13 \equiv 1 \mod 4$, pero por el teorema 2.8 como $13 \equiv 3 \mod 5$ entonces 13 no pertenece a Σ. Por lo tanto este teorema se considera una condición necesaria pero no suficiente para caracterizar los primos de $\mathbb{N}$ que pertenecen a Σ.

Con el propósito de encontrar una condición necesaria y suficiente que caracterice cuáles primos de los naturales pertenecen a Σ, obsérvese que en un arreglo módulo 20 lo primos congruentes con 1 módulo 4 son congruentes con $1, 5, 9, 13, 17$ módulo 20. De estos primos los congruentes con 13 y 17 módulo 20 no pertenecen a Σ por el teorema 2.16. Lo anterior sugiere que los primos p enteros que pertenecen a Σ son los $p \equiv 1, 5, 9 \mod 20$, teorema que fue inicialmente conjeturado por Euler(Leonhard Euler, 1707–1783) producto de generalizaciones de resultados de Fermat (Pierre de Fermat, 1601–1665) sobre la solución de las ecuaciones[2] $p = x^2 + y^2$ y $p = x^2 + 3y^2$.

Teorema 3.2. Para todo p primo en $\mathbb{N}$, $p \in \Sigma \Leftrightarrow p \equiv 1, 5, 9 \mod 20$

[2]Cox, D.(1989). *Primes of the forme $x^2 + ny^2$: Fermat, class field theory and complex multiplication.* New York: Wiley-Interscience Publication. pg 26

Demostración. Dada la doble implicación de este teorema se comenzará demostrando a derecha es decir: para todo p primo impar en $\mathbb{N}$, sí $p \in \Sigma$ entonces $p \equiv 1, 5, 9 \mod 20$. Como $p \in \Sigma$, entonces $p = x^2 + 5y^2$ para $x, y \in \mathbb{Z}$. Por tanto se presentan los siguientes casos:

- Par-Par. Sean $x = 2k$ y $y = 2m$ entonces:

$$\begin{aligned} p &= 4k^2 + 20m^2 \\ p &= 4(k^2 + 5m^2) \end{aligned} \tag{3.1}$$

  de la igualdad (3.1) se tiene que p es par, lo que lleva a una contradicción, por lo tanto no existe ningún primo en el caso par-par.

- Impar-Par. Sean $x = 2k + 1$ y $y = 2m$ entonces:

$$\begin{aligned} p &= (2k+1)^2 + 20m^2 \\ p &\equiv (2k+1)^2 \mod 20 \\ p &\equiv 4(k(k+1)) + 1 \mod 20 \\ p &\equiv 4t + 1 \mod 20 \end{aligned}$$

  Ahora pues, dado que t es el producto entre dos números consecutivos, entonces los posibles casos en un arreglo módulo 5 son:

$$\begin{aligned} p &\equiv 4((5x-1)5x) + 1 \mod 20 \\ p &\equiv 4((5x-2)(5x-1)) + 1 \mod 20 \\ p &\equiv 4((5x-3)(5x-2)) + 1 \mod 20 \\ p &\equiv 4((5x-4)(5x-3)) + 1 \mod 20 \\ p &\equiv 4((5x-5)(5x-4)) + 1 \mod 20 \end{aligned}$$

  reescribiendo estas congruencias se tiene:

$$\begin{aligned} p &\equiv 4((5x-1)5x) + 1 \mod 20 \\ p &\equiv 4(5x(5x-3)) + 9 \mod 20 \\ p &\equiv 4(5x(5x-5)) + 20 + 5 \mod 20 \\ p &\equiv 4(5x-2)(5x-5) + 9 \mod 20 \\ p &\equiv 4((5x-5)(5x-4)) + 1 \mod 20 \end{aligned}$$

  de donde resultan las siguientes congruencias

$$\begin{aligned} p &\equiv 9 \mod 20 \\ p &\equiv 5 \mod 20 \\ p &\equiv 1 \mod 20 \end{aligned}$$

sin embargo el primer elemento que pertenece a $\mathbb{N}$ que es de la forma $4(k(k+1))+1$ y congruente con 5 módulo 20 es el 25 por lo tanto los primos en ese caso resultaran siendo únicamente los congruentes con 1 o 9 módulo 20.

- Par-Impar. Sean $x = 2k$ y $y = 2m+1$ entonces:

$$\begin{aligned} p &= (2k)^2 + 5(2m+1)^2 \\ p &= 4k^2 + 20m(m+1) + 5 \\ p &\equiv 4k^2 + 5 \quad \text{mód } 20 \end{aligned}$$

y en un arreglo módulo 5 se tiene

$$\begin{aligned} p &\equiv 4(5x)^2 + 5 \quad \text{mód } 20 \\ p &\equiv 4(5x+1)^2 + 5 \quad \text{mód } 20 \\ p &\equiv 4(5x+2)^2 + 5 \quad \text{mód } 20 \\ p &\equiv 4(5x+3)^2 + 5 \quad \text{mód } 20 \\ p &\equiv 4(5x+4)^2 + 5 \quad \text{mód } 20 \end{aligned}$$

de donde resultan las siguientes congruencias

$$\begin{aligned} p &\equiv 5 \quad \text{mód } 20 \\ p &\equiv 9 \quad \text{mód } 20 \\ p &\equiv 1 \quad \text{mód } 20 \end{aligned}$$

- Impar-Impar Sean $x = 2k+1$ y $y = 2m+1$ entonces:

$$\begin{aligned} p &= (2k+1)^2 + 5(2m+1)^2 \\ p &= 4k(k+1) + 1 + 5[4m(m+1)+1] \\ p &= 4k(k+1) + 20m(m+1) + 6 \end{aligned} \tag{3.2}$$

de la igualdad (3.2) resulta que:

$$\begin{aligned} p &\equiv 4k(k+1) + 6 \quad \text{mód } 20 \\ &\wedge \\ p &\equiv 2 \quad \text{mód } 4 \end{aligned}$$

lo que es una contradicción pues no existe ningún primo entero impar congruente con 2 módulo 4.

Por lo tanto para todo p primo en $\mathbb{Z}$, si se tiene que $p \in \Sigma$ entonces $p \equiv 1, 5, 9 \mod 20$.

Ahora se procederá a demostrar que para todo p primo en $\mathbb{N}$, si:

$$p \equiv 1, 5, 9 \mod 20 \rightarrow p \in \Sigma$$

Se razonará por contradicción, supóngase que $p \notin \Sigma$, por lo tanto p debe cumplir alguna de las siguientes congruencias, según el criterio de pertenencia.

i) Para algún $k \in \mathbb{N}$, $p \equiv 3(4^k) \mod 4^{k+1}$

ii) Para algún $k \in \mathbb{N}$, $p \equiv 2(4^r) \mod 2(4^{r+1})$

iii) Existe q factor primo de p tal que $q \equiv 11, 13, 17, 19 \mod 20$ y q^k con k impar la mayor potencia que divide a p

El tercer ítem corresponde de inmediato a una contradicción, pues por hipótesis p es primo y $p \equiv 1, 5, 9 \mod 20$. Ahora si p cumple el ítem 2 por el teorema 2.7 p seria par, lo que es una contradicción pues p es primo impar.

Finalmente, dado que p es primo se descarta el caso i) cuando $k > 0$, pues p resultaría ser par. Si $k = 0$ se tiene que $p \equiv 3 \mod 4$ lo cual resulta una contradicción, pues $p \equiv 1 \mod 4$ ya que por hipótesis $p \equiv 1, 5, 9 \mod 20$.

Así pues, para todo p primo en $\mathbb{N}$, si $p \equiv 1, 5, 9 \mod 20$ entonces $p \in \Sigma$. □

En la demostración anterior se uso el criterio de pertenencia el cual no ha sido demostrado, sin embargo esto no afecta la validez del teorema ya que este se encuentra probada por otra vía en el documento de Ying Zhang,[3], lo que ratifica su veracidad.

De manera que los primos en $\mathbb{N}$ que son congruentes con $1, 5, 9$ módulo 20 son irreducibles en Σ. No obstante, estos elementos no son los únicos irreducibles, pues por ejemplo, $6 \in \Sigma$ y como $2, 3 \notin \Sigma$ entonces 6 es irreducible en Σ. De ahí que otros candidatos a ser irreducibles son aquellos resultan del producto de dos números primos $p, q \in \mathbb{N}$ tales que $p, q \notin \Sigma$ y $pq \in \Sigma$.

Como los primos enteros que no pertenecen a Σ, de acuerdo con el teorema 3.2, son los $p \equiv 2, 3, 7, 11, 13, 17, 19 \mod 20$ entonces la tarea es averiguar cuáles productos de estos elementos pertenecen a Σ. Un primer caso que se deberá estudiar es el de los cuadrados de

[3]Zhang, Y. (2006) *Representing primes as $x^2 + 5y^2$: an inductive proof that Euler missed.* National University of Singapore, China.

los $p \equiv 2, 3, 7, 11, 13, 17, 19 \mod 20$, pues se sabe que todo entero al cuadrado pertenece a Σ. Ahora, por el teorema 2.16 es posible afirmar que dados p, q primos diferentes en $\mathbb{N}$ si $p \equiv 11, 13, 17, 19 \mod 20$ entonces $pq \notin \Sigma$, entonces no se tendrá en cuenta este caso. De modo que un segundo caso que se deberá estudiar es el de los posibles productos entre el 2 y los primos $p \equiv 3, 7 \mod 20$.

Para el caso de los cuadrados de los $p \equiv 2, 3, 7, 11, 13, 17, 19$ se demuestra el siguiente teorema.

Teorema 3.3. Si p primo en $\mathbb{N}$ con $p \equiv 2, 3, 7, 11, 13, 17, 19 \mod 20$, entonces p^2 es irreducible en Σ.

Demostración. Dado el elemento $(p, 0)$ se tiene que $\sigma((p, 0)) = p^2 + 0^2$ de modo que $p^2 \in \Sigma$. Ahora, como en $\mathbb{Z}$ los únicos divisores de p^2 son $1, p$ y p^2, pero por el teorema 3.2 como $p \equiv 2, 3, 7, 11, 13, 17, 19 \mod 20$, entonces $p \notin \Sigma$. Luego p^2 únicamente es divisible por él mismo y la unidad, de modo que si $p \equiv 2, 3, 7, 11, 13, 17, 19 \mod 20$, entonces $p^2 \in \Sigma$ y p^2 es irreducible en Σ. □

El segundo caso que se estudiará es el relacionado con los productos de los primos enteros p, q diferentes, tales que p y q sean congruentes con $2, 3$ o 7 módulo 20, del cual surge el siguiente teorema.

Teorema 3.4. Sean p, q primos diferentes en $\mathbb{N}$, si p y q son congruentes con $2, 3$ o 7 módulo 20 entonces $pq \in \Sigma$.

Demostración. Para demostrar que $pq \in \Sigma$ se deberá mostrar que pq no cumple alguno de los ítems del criterio de pertenencia los cuales se enuncian a continuación.

i) Para algún $k \in \mathbb{N}$, $m \equiv 3(4^k) \mod 4^{k+1}$

ii) Para algún $k \in \mathbb{N}$, $m \equiv 2(4^s) \mod 2(4^{s+1})$

iii) Existe r factor primo de m tal que $r \equiv 11, 13, 17, 19 \mod 20$ y r^k con k impar la mayor potencia que divide a m

Para esta demostración se tendrán en cuenta los siguientes 5 casos.

- Caso 1. Si $p \equiv 3 \mod 20$ y $q \equiv 7 \mod 20$ entonces $pq \equiv 1 \mod 20$ y a su vez $pq \equiv 1 \mod 4$. Si pq cumpliera el ítem i) se tendría que para $k > 0$ pq sería par y si $k = 0$ entonces $pq \equiv 3 \mod 4$, lo que es una contradicción pues $pq \equiv 1 \mod 4$. Ahora, si pq

cumpliera el ítem ii) pq sería par lo implica una contradicción pues $pq \equiv 1 \mod 4$. Por último, si pq cumplieran el ítem iii) resultaría una contradicción en tanto que p y q son primos congruentes con 3 y 7 módulo 20 respectivamente. De modo que $pq \in \Sigma$ por el criterio de pertenencia.

- Caso 2. Si $p \equiv 2 \mod 20$ y $q \equiv 3 \mod 20$. Como el único primo equivalente con 2 módulo 20 es el 2 entonces entonces $pq = 2q$ donde $2q \equiv 6 \mod 20$ y por lo tanto $2q \equiv 2 \mod 4$. Sí $2q$ cumpliera el ítem i) del criterio de congruencia se tendría para $k > 0$ que $2q \equiv 0 \mod 4$ o si $k = 0$ resultaría que $2q \equiv 3 \mod 4$ lo cual es una contradicción pues $2q \equiv 2 \mod 4$. Ahora, si $2q$ cumpliera el ítem ii) se tendría que $2q \equiv 2(4^k) \mod 2(4^{k+1})$ entonces $q \equiv 4^k \mod 4^{k+1}$ por tanto si $k = 0$ resultaría que $q \equiv 1 \mod 4$ y si $k > 0$ q sería par lo cual es una contradicción pues $q \equiv 3 \mod 4$. Por último, si $2q$ cumpliera el ítem iii) resultaría una contradicción en tanto que $q \equiv 3$ mód 20. De modo que $pq \in \Sigma$ por el criterio de pertenencia.

- Caso 3. Si $p \equiv 2 \mod 20$ y $q \equiv 7 \mod 20$, entonces $pq = 2q$ donde $2q \equiv 6 \mod 20$. Esta demostración es análoga al caso anterior.

- Caso 4. Si $p \equiv 3 \mod 20$ y $q \equiv 3 \mod 20$ entonces $pq \equiv 9 \mod 20$ de modo que $pq \equiv 1 \mod 4$, por tanto este caso es análogo al caso 1, entonces $pq \in \Sigma$ gracias al criterio de pertenencia.

- Caso 5. Si $p \equiv 7 \mod 20$ y $q \equiv 7 \mod 20$ entonces $pq \equiv 9 \mod 20$ de modo que $pq \equiv 1 \mod 4$, por tanto este caso es análogo al caso 1.

De manera que dados p, q primos en $\mathbb{N}$, si p y q son congruentes con $2, 3$ o 7 módulo 20 entonces $pq \in \Sigma$. □

Como $pq \in \Sigma$ y por el teorema 3.2 $p, q \notin \Sigma$ entonces pq es irreducible en Σ. La conjetura de este teorema fue hecha inicialmente por Fermat, quien la comunicó en una carta enviada a sir Kenelm Digby en 1658, en la cual admite que no la pudo probar. Cabe aclarar que la prueba aquí mostrada no es del todo valida en tanto que usa el criterio de pertenencia, sin embargo puede consultar otra demostración en el documento referenciado anteriormente.

Así pues, un elemento $a \in \Sigma$ es irreducible si y sólo si cumple uno de los siguientes ítems.

i) a primo en $\mathbb{N}$ y $a \equiv 1, 5, 9 \mod 20$

ii) $a = p^2$ con p primo en $\mathbb{N}$ y $p \equiv 2, 3, 7, 11, 13, 17, 19 \mod 20$

iii) $a = pq$ con p, q primos diferentes en $\mathbb{N}$ y p, q congruentes con $2, 3$ o 7 módulo 20.

Como todo elemento irreducible en Σ tiene alguno de estos factores primos de $\mathbb{N}$, entonces esto garantiza que no hay mas irreducibles en Σ. Ahora, todo número diferente de l y el 0 se puede expresar en termino de irreducibles, pues la descomposición en Σ se obtiene de la descomposición de los naturales, solo falta por responder el interrogante de si la factorización es única, para ello se muestra la siguiente tabla.

#	Descomposición en $\mathbb{N}$	$p \equiv 1,5,9$ mód 20	$p \equiv 11,13,17,19$ mód 20	$p,q \equiv 2,3,7$ mód 20	Descomposición en Σ
945	$3^3 \cdot 5 \cdot 7$	5		$3^3, 7$	$* 5 \cdot 9 \cdot 21$
966	$2\dot{3} \cdot 7 \cdot 23$			$2,3,7,23$	$* 6 \cdot 161$ $* 14 \cdot 69$ $* 46 \cdot 21$
1445	$5 \cdot 17^2$	5	17^2		$* 5 \cdot 17^2$
6480	$2^4 \cdot 3^4 \cdot 5$	5		$2^4, 3^4$	$* 5 \cdot 4^2 \cdot 9^2$ $* 5 \cdot 6^4$
12126	$2 \cdot 3 \cdot 43 \cdot 47$			$2 \cdot 3 \cdot 43 \cdot 47$	$* 6 \cdot 2021$ $* 86 \cdot 141$ $* 94 \cdot 129$
175329	$3^2 \cdot 7 \cdot 11^2 \cdot 23$		11^2	$3^2, 7, 23$	$* 121 \cdot 9 \cdot 161$ $* 121 \cdot 21 \cdot 69$
4734366	$2 \cdot 3 \cdot 7 \cdot 13^2 \cdot 29$	29	13^2	$2,3,7,23$	$* 29 \cdot 13^2 \cdot 6 \cdot 161$ $* 29 \cdot 13^2 \cdot 21 \cdot 46$ $* 29 \cdot 13^2 \cdot 14 \cdot 69$

Tabla 3.1: Algunas descomposiciones en factores irreducibles de elementos de Σ

Como se observa en la tabla la factorización en Σ no siempre es única, por ejemplo, el número 966 tiene tres factorizaciones diferentes en Σ, pero hay números que a pesar de ser mas grandes como el 1445 que tienen factorización única. Por tanto la pregunta ahora es cuándo un número tiene factorización única en Σ, para ello obsérvese que usa la descomposición en $\mathbb{N}$ para hacer la descomposición en Σ y que son los factores primos con $p \equiv 2,3,7 \mod 20$ los que al combinarse generan descomposiciones diferentes; mientras que los $p \equiv 1,5,9 \mod 20$ y los p^2 con $p \equiv 11,13,17,19 \mod 20$ se mantienen en la descomposición en Σ.

Lo anterior se tiene, dado que no es posible multiplicar los $p \equiv 1,5,9 \mod 20$ con un natural para generar otros irreducibles y con esto distintas factorizaciones, como también sucede con los p^2 cuando $p \equiv 11,13,17,19 \mod 20$, como se demuestra a continuación.

Teorema 3.5. Sea p primo en $\mathbb{N}$ si $p \equiv 1,5,9 \mod 20$ y $pa \in \Sigma$ entonces $a \in \Sigma$

Demostración. Como $p \in \Sigma$ y $pa \in \Sigma$ entonces $p = x^2 + 5y^2$ y $pa = m^2 + 5n^2$. Por tanto:

$$\begin{aligned} p^2a &= (m^2 + 5n^2)(x^2 + 5y^2) \\ &= (mx)^2 + 5(nx)^2 + 5(my)^2 + 25(ny)^2 \end{aligned}$$

Como $p \mid m^2 + 5n^2$ entonces $p \mid y^2(m^2 + 5n^2)$, además $p \mid n^2(x^2 + 5y^2)$, de esto resulta que $p \mid (y^2(m^2 + 5n^2) - n^2(x^2 + 5y^2))$ por lo tanto:

$$\begin{aligned} p &\mid (my)^2 + 5(ny)^2 - (nx)^2 - 5(ny)^2 \\ p &\mid (my)^2 - (nx)^2 \\ p &\mid (my - nx)(my + nx) \end{aligned}$$

Dado que p es primo $p \mid (my - nx)$ o $p \mid (my + nx)$. Si $p \mid (my - nx)$ como:

$$\begin{aligned} p^2a &= (mx)^2 + 5(nx)^2 + 5(my)^2 + 25(ny)^2 \\ &= (mx)^2 + 10(mxny) + 5(nx)^2 + 5(my)^2 - 10(mxny) + 25(ny)^2 \\ &= (mx + 5ny)^2 + 5(my - nx)^2 \end{aligned}$$

entonces $p \mid 5(my - nx)^2$ por tanto $p \mid (mx + 5ny)$, luego,

$$\begin{aligned} p^2a &= \left(\left(\frac{mx + 5ny}{p}\right)^2 + 5\left(\frac{my - nx}{p}\right)^2\right)p^2 \\ a &= \left(\left(\frac{mx + 5ny}{p}\right)^2 + 5\left(\frac{my - nx}{p}\right)^2\right) \end{aligned}$$

como $p \mid (my - nx)$ y $p \mid (mx + 5ny)$ entonces $a \in \Sigma$.

Si $p \mid (my + nx)$ como:

$$\begin{aligned} p^2a &= (mx)^2 + 5(nx)^2 + 5(my)^2 + 25(ny)^2 \\ &= (mx)^2 - 10(mxny) + 25(ny)^2 + 5(my)^2 + 10(mxny) + 5(nx)^2 \\ &= (mx - 5ny)^2 + 5(my + nx)^2 \end{aligned}$$

Análogo al caso anterior como $p \mid (my + nx)$ entonces $p \mid (mx - 5ny)$, luego,

$$\begin{aligned} p^2a &= \left(\left(\frac{mx - 5ny}{p}\right)^2 + 5\left(\frac{my + nx}{p}\right)^2\right)p^2 \\ a &= \left(\left(\frac{mx - 5ny}{p}\right)^2 + 5\left(\frac{my + nx}{p}\right)^2\right) \end{aligned}$$

como $p \mid (my + nx)$ y $p \mid (mx - 5ny)$ entonces $a \in \Sigma$. □

Nótese que este teorema permite afirmar que los primos $p \equiv 1, 5, 9 \mod 20$ no pueden ser factores de algún otro irreducible en Σ, porque como $pa \in \Sigma$ entonces $a \in \Sigma$, lo que conlleva a que pa es compuesto.

De la tabla 3.1, también es posible observar que los cuadrados de los $p \equiv 11, 13, 17, 19 \mod 20$ no generan distintas descomposiciones. Por ejemplo 1445 se puede descomponer unicamente como $5 \cdot 17^2$ pues estos p no tienen ninguna forma de mezclarse de manera que formen otro irreducible. Esto gracias al siguiente teorema, que se muestra precedido de lema 3.1 necesario para su demostración.

Lema 3.1. Si $p \mid x^2 + 5y^2$ y $p \nmid d$ donde $(x, y) = d$ entonces $p \equiv 1, 3, 7, 9 \mod 20$

Demostración. Como $p \mid x^2 + 5y^2$ y $(x, y) = d$ entonces $p \mid d^2 \left(\left(\frac{x}{d}\right)^2 + 5\left(\frac{y}{d}\right)^2 \right)$ y como $p \nmid d$ entonces $p \mid \left(\frac{x}{d}\right)^2 + 5\left(\frac{y}{d}\right)^2$ por tanto $p \equiv 1, 3, 7, 9 \mod 20$ gracias al teorema 2.15. □

Teorema 3.6. Sea p primo en $\mathbb{N}$ si $p \equiv 11, 13, 17, 19 \mod 20$ y $p^2 a \in \Sigma$ entonces $a \in \Sigma$

Demostración. Como $p \equiv 11, 13, 17, 19 \mod 20$ entonces $p \neq 2, 5$. Ahora como $p^2 a \in \Sigma$ entonces $p^2 a = x^2 + 5y^2$, luego $p \mid x^2 + 5y^2$. Sea $(x, y) = d$ si $p \nmid d$ entonces $p \equiv 1, 3, 7, 9$ mód 20 por el lema 3.1 lo cual resulta una contradicción, lo que implica que $p \mid d$ entonces,

$$\begin{aligned} p^2 a &= \left[\left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2 \right] p^2 \\ a &= \left[\left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2 \right] \end{aligned}$$

por tanto $a \in \Sigma$. □

Como $p^2 a$ cumple el teorema 3.6 entonces $a \in \Sigma$ de donde se tiene que $p^2 a$ es compuesto. Ahora, obsérvese que los $p \equiv 11, 13, 17, 19 \mod 20$ no pueden formar irreducibles diferentes de ellos mismos al cuadrado, como se prueba a continuación.

Teorema 3.7. Si $p \equiv 11, 13, 17, 19 \mod 20$ y $a \in \Sigma$ entonces $ap \notin \Sigma$

Demostración. Se razonará por contradicción. Supóngase que $ap = m^2 + 5n^2$, como $a \in \Sigma$ existen $x, y \in \mathbb{N}$ tales que $a = x^2 + 5y^2$. Sea $(m, n) = d$ si $p \nmid d$ por el teorema 3.6 $p \equiv 1, 3, 7, 9$ mód 20 lo que es una contradicción, por lo tanto $p \mid d$. Supóngase ahora que p^s es la mayor

potencia de p que divide a d con $s > 0$ luego,

$$\begin{aligned}(x^2+5y^2)p &= p^{2s}\left(\left(\frac{m}{p^s}\right)^2+5\left(\frac{n}{p^s}\right)^2\right)\\ (x^2+5y^2) &= p^{2s-1}\left(\left(\frac{m}{p^s}\right)^2+5\left(\frac{n}{p^s}\right)^2\right)\end{aligned}$$

Sea $k=(x,y)$ si $p \nmid k$ por el lema 3.1 $p \equiv 1,3,7,9 \mod 20$ lo que es una contradicción, por lo tanto $p \mid k$. Así pues sea p^h la mayor potencia que divide a k entonces se tiene

$$p^{2h}\left(\left(\frac{m}{p^h}\right)^2+5\left(\frac{n}{p^h}\right)^2\right) = p^{2s-1}\left(\left(\frac{m}{p^s}\right)^2+5\left(\frac{n}{p^s}\right)^2\right) \tag{3.3}$$

Se sabe que $(\frac{x}{p^h},\frac{y}{p^h})=\frac{k}{p^h}$ por lo tanto $p \nmid \frac{k}{p^h}$ de igual manera $(\frac{m}{p^s},\frac{n}{p^s})=\frac{d}{p^s}$ de donde $p \nmid \frac{d}{p^s}$. De (3.3) resultan dos casos, si $s \leq h$ entonces $p \mid \left(\frac{m}{p^s}\right)^2+5\left(\frac{n}{p^s}\right)^2$ y por el lema 3.1 resulta que $p \equiv 1,3,7,9 \mod 20$ lo cual es una contradicción. Si $s > h$ entonces $2s > 2h$ y $2s-1 > 2h$ por lo tanto $p \mid \left(\frac{m}{p^h}\right)^2+5\left(\frac{n}{p^h}\right)^2$ y por el lema 3.1 resulta que $p \equiv 1,3,7,9 \mod 20$ lo cual es una contradicción. En conclusión $ap \notin \Sigma$. □

Con esto se tiene que para hacer una factorización en Σ, los $p \equiv 11,13,17,19 \mod 20$ necesariamente deben estar elevados al cuadrado. Para el caso de los pq con $p,q \equiv 2,3,7 \mod 20$ sucede algo similar, pues ellos deben agruparse en pares. Por ejemplo, 12126 se descompone en $\mathbb{N}$ como $2 \cdot 3 \cdot 43 \cdot 47$ donde resulta que cada factor es congruente con 3 o 7 módulo 20. Para hacer la factorización en Σ se agrupan estos elementos en dos parejas, de modo que resultan 3 combinaciones diferentes, de donde se tiene que existen 3 factorizaciones distintas.

Por último se tiene que los pq con $p,q \equiv 2,3,7 \mod 20$ no generan otros irreducibles al agruparse con otros elementos, como se demuestra a continuación.

Teorema 3.8. Si $ba \in \Sigma$ y $b=pq$ con $p,q \equiv 2,3,7 \mod 20$ entonces $a \in \Sigma$.

Demostración. Como $ba \in \Sigma$ y $b=pq$ con $p,q \equiv 2,3,7 \mod 20$, por los teoremas 3.3 y 3.4 $pq \in \Sigma$ entonces $ba=x^2+5y^2$ y $pq=m^2+5n^2$. Por tanto:

$$\begin{aligned}p^2q^2a &= (m^2+5n^2)(x^2+5y^2)\\ &= (mx)^2+5(nx)^2+5(my)^2+25(ny)^2\end{aligned}$$

Como $p \mid m^2+5n^2$ y $q \mid m^2+5n^2$ entonces $pq \mid y^2(m^2+5n^2)$, además $pq \mid n^2(x^2+5y^2)$, de esto resulta que $pq \mid (y^2(m^2+5n^2) - n^2(x^2+5y^2))$ por lo tanto:

$$\begin{aligned} p &\mid (my)^2+5(ny)^2-(nx)^2-5(ny)^2 \\ p &\mid (my)^2-(nx)^2 \\ p &\mid (my-nx)(my+nx) \end{aligned}$$

De igual forma se cumple que $q \mid (my-nx)(my+nx)$. Dado que p, q son primos se tiene que $p \mid (my-nx)$ o $p \mid (my+nx)$ y $q \mid (my-nx)$ o $q \mid (my+nx)$.

Si $p \mid (my-nx)$ y $q \mid (my-nx)$ entonces $pq \mid (my-nx)$ como:

$$\begin{aligned} p^2q^2a &= (mx)^2+5(nx)^2+5(my)^2+25(ny)^2 \\ &= (mx)^2+10(mxny)+5(nx)^2+5(my)^2-10(mxny)+25(ny)^2 \\ &= (mx+5ny)^2+5(my-nx)^2 \end{aligned}$$

entonces $p \mid 5(my-nx)^2$ y $q \mid 5(my-nx)^2$ por tanto $pq \mid (mx+5ny)$, luego,

$$\begin{aligned} p^2q^2a &= \left(\left(\frac{mx+5ny}{pq}\right)^2+5\left(\frac{my-nx}{pq}\right)^2\right)p^2q^2 \\ a &= \left(\left(\frac{mx+5ny}{pq}\right)^2+5\left(\frac{my-nx}{pq}\right)^2\right) \end{aligned}$$

como $pq \mid (my-nx)$ y $pq \mid (mx+5ny)$ entonces $a \in \Sigma$.

Si $p \mid (my+nx)$ y $q \mid (mx-5ny)$ es análogo al caso anterior.

Si $q \mid (my+nx)$ y $p \mid (mx-5ny)$ como:

$$\begin{aligned} p^2q^2a &= (mx)^2+5(nx)^2+5(my)^2+25(ny)^2 \\ &= (mx)^2-10(mxny)+25(ny)^2+5(my)^2+10(mxny)+5(nx)^2 \\ &= (mx-5ny)^2+5(my+nx)^2 \end{aligned}$$

Como $q \mid (my+nx)$ y $p \mid (mx-5ny)$ entonces $p \mid (mx-5ny)^2$ y $q \mid 5(my+nx)^2$ por lo tanto $p \mid (mx-5ny)$ y $q \mid (my+nx)$ lo que implica que $pq \mid (mx-5ny)$ y $pq \mid (my+nx)$ luego,

$$\begin{aligned} p^2q^2a &= \left(\left(\frac{mx-5ny}{pq}\right)^2+5\left(\frac{my+nx}{pq}\right)^2\right)p^2q^2 \\ a &= \left(\left(\frac{mx-5ny}{pq}\right)^2+5\left(\frac{my+nx}{pq}\right)^2\right) \end{aligned}$$

como $pq \mid (my+nx)$ y $pq \mid (mx-5ny)$ entonces $a \in \Sigma$.

Si $p \mid (mx+5ny)$ y $q \mid (mx+5ny)$ es análogo al caso anterior. □

En síntesis, como se podía observar desde la tabla, los números en Σ que tienen diferentes factorizaciones, son aquellos cuya descomposición en $\mathbb{N}$ tiene factores primos congruentes con $2, 3$ o 7 módulo 20, donde estos se pueden agrupar por parejas de diferentes maneras.

Capítulo 4

Divisibilidad en $\mathbb{Z}[\sqrt{-5}]$

En teoría de números un aspecto importante, tal y como se realizó en el capítulo anterior, es la posibilidad de establecer un teorema análogo al TFA, objetivo para el cual es necesario el estudio de la divisibilidad. Es por esto que se estudiarán algunas propiedades de la relación de divisibilidad en $\mathbb{Z}[\sqrt{-5}]$, la existencia de un algoritmo de la división, la posibilidad de cálculo del máximo común divisor, el estudio de elementos distinguidos y con ello la descomposición en este anillo.

Con este fin a continuación se define la relación ser divisor de, basada en la definición que de esta relación se tiene en los números enteros.

Definición 4.1. Sean $z, w \in \mathbb{Z}[\sqrt{-5}]$, se dice que z divide a w, denotado por $z \mid w$ si y sólo si existe un $q \in \mathbb{Z}[\sqrt{-5}]$ tal que $zq = w$.

Ejemplo 4.1.

$$\begin{aligned} (3,0) \mid (9,0) \quad &\text{porque} \quad (9,0) = (3,0)(3,0) \\ (7,2) \mid (7,2) \quad &\text{porque} \quad (7,2) = (7,2)(1,0) \\ (2,1) \mid (9,0) \quad &\text{porque} \quad (9,0) = (2,1)(2,-1) \end{aligned}$$

Los ejemplos anteriores, podrían mostrar que averiguar si un número es divisor de otro en $\mathbb{Z}[\sqrt{-5}]$ es una tarea fácil, sin embargo, esta conlleva a un trabajo más elaborado que en los números enteros, pues se requiere la solución de un sistema de ecuaciones. Por ejemplo, para verificar si efectivamente $(2,1)$ divide a $(9,0)$ se debe encontrar un elemento $(a,b) \in \mathbb{Z}[\sqrt{-5}]$ de tal manera que:

$$(2,1)(a,b) = (2a - 5b, a + 2b) = (9,0)$$

y dada la definición de igualdad de elementos en $\mathbb{Z}[\sqrt{-5}]$, se obtiene el siguiente sistema de ecuaciones

$$\begin{aligned} 2a - 5b &= 9 \\ a + 2b &= 0 \end{aligned}$$

de modo que el problema se reduce a encontrar los elementos a, b enteros que satisfagan el sistema, los cuales son $a = 2$ y $b = -1$.

Así pues, para estudiar la divisibilidad en este conjunto se hizo necesario un programa que hallará los divisores de un elemento dado de $\mathbb{Z}[\sqrt{-5}]$. De manera general dado un (c, d) hallar sus divisores (a, b) implica por medio de ciclos encontrar la solución del siguiente sistema de ecuaciones.

$$\begin{aligned} c &= ax - 5by \\ d &= bx + ay \end{aligned}$$

en donde, por regla de Cramer se tiene

$$x = \frac{\begin{vmatrix} c & -5b \\ d & a \end{vmatrix}}{\begin{vmatrix} a & -5b \\ b & a \end{vmatrix}} = \frac{ac + 5bd}{\sigma((a, b))}$$

$$y = \frac{\begin{vmatrix} a & c \\ b & d \end{vmatrix}}{\begin{vmatrix} a & -5b \\ b & a \end{vmatrix}} = \frac{ad - bc}{\sigma((a, b))}$$

De modo que el programa busca los (a, b) por medio de la recursión tales que $x, y \in \mathbb{Z}$. Teniendo este recurso lo siguiente que se hizo fue estudiar algunas de las propiedades de la relación definida.

4.1. Propiedades de la divisibilidad en $\mathbb{Z}[\sqrt{-5}]$

En Σ la relación de divisibilidad es un orden al igual que en conjuntos usuales como los naturales, esto motiva el estudio del cumplimiento de las propiedades reflexiva, antisimétrica y transitiva de la divisibilidad en $\mathbb{Z}[\sqrt{-5}]$.

Teorema 4.1. $z \mid z$ para todo $z \in \mathbb{Z}[\sqrt{-5}]$

Demostración. Sea $z = (a, b)$, como $(a, b)(1, 0) = (a, b)$ entonces $(a, b) \mid (a, b)$ □

Teorema 4.2. Para todo $z, w, v \in \mathbb{Z}[\sqrt{-5}]$ si $z \mid w$ y $w \mid v$ entonces $z \mid v$

Demostración. Dado que $z \mid w$ y $w \mid v$ entonces existen $q, r \in \mathbb{Z}[\sqrt{-5}]$ tales que $w = zp$ y $v = wr$ de lo cual se tiene que $v = (zp)r$ y por la propiedad asociativa de la multiplicación en $\mathbb{Z}[\sqrt{-5}]$ se tiene que $v = z(pr)$. Luego por la definición 4.1 se concluye que $z \mid v$ □

La relación $\mid$ no resulta anti-simétrica pues si $z \mid w$ y $w \mid z$ no siempre $z = w$. Por ejemplo $(-a, -b) \mid (a, b)$ y $(a, b) \mid (-a, -b)$ pero $(a, b) \neq (-a, -b)$. Por lo cual esta relación no es un orden.

Otras propiedades que cumple la relación $\mid$ se sintetizan en el siguiente teorema.

Teorema 4.3. Sean $w, v, z \in \mathbb{Z}[\sqrt{-5}]$ se cumple que:

1. Si $z \mid w$ entonces $z \mid wv$.
2. $z \mid w$ sí y solo si $vz \mid vw$.
3. Si $z \mid w$ y $z \mid v$ entonces $z \mid (sw + tv)$.

Demostración.

1. Como $z \mid w$ por definición 4.1 existe $t \in \mathbb{Z}[\sqrt{-5}]$ tal que $w = zt$, por propiedades de la igualdad y asociatividad de la multiplicación en $\mathbb{Z}[\sqrt{-5}]$ se tiene que $wv = z(tv)$ por tanto $z \mid wv$

2→. Si $z \mid w$ entonces por definición 4.1 existe t tal que $w = zt$, ahora por propiedades de la igualdad y asociatividad de la multiplicación en $\mathbb{Z}[\sqrt{-5}]$ se tiene que $vw = (vz)t$ de donde se concluye que $vz \mid vw$

← . Si $vz \mid vw$ por definición 4.1 existe un $t \in \mathbb{Z}[\sqrt{-5}]$ tal que $vw = (vz)t$, ahora por las propiedades asociativa y cancelativa de la multiplicación en $\mathbb{Z}[\sqrt{-5}]$ se tiene que $w = zt$ y por lo tanto $z \mid w$

3. Como $z \mid w$ y $z \mid v$ por definición 4.1 existen $q, r \in \mathbb{Z}[\sqrt{-5}]$ tales que $w = zq$ y $v = zr$ por propiedades de la igualdad se tiene $sw = s(zq)$ y $tv = t(zr)$. Sumando las igualdades

anteriores se obtiene $sw + tv = s(zq) + t(zr)$ y por lo tanto $sw + tv = z(sq + tr)$ de donde se concluye que $z \mid sw + tv$. □

Ahora, véase que la divisibilidad en Σ tiene una relación con la divisibilidad definida en $\mathbb{Z}[\sqrt{-5}]$, pues al ser σ una función multiplicativa esta hereda la divisibilidad, es decir, como:

$$\sigma((a,b))\sigma((x,y)) = \sigma((c,d))$$

entonces $\sigma((a,b)) \mid_{\Sigma} \sigma((c,d))$, lo que sugiere el siguiente teorema.

Teorema 4.4. Para todo $z, w \in \mathbb{Z}[\sqrt{-5}]$, se tiene que si $z \mid w$ entonces $\sigma(z) \mid_{\Sigma} \sigma(w)$

Demostración. Sean $z, w \in \mathbb{Z}[\sqrt{-5}]$ tales que $z \mid w$, entonces por definición 4.1 existe $q \in \mathbb{Z}[\sqrt{-5}]$ de tal manera que $zq = w$, aplicando la función σ y teniendo en cuenta que esta es multiplicativa por el teorema 1.14 parte *iii*, se tiene:

$$\begin{aligned} \sigma(zq) &= \sigma(w) \\ \sigma(z)\sigma(q) &= \sigma(w) \\ \sigma(z) &\mid_{\Sigma} \sigma(w) \end{aligned}$$

□

El recíproco del teorema anterior no es cierto. Por ejemplo, $\sigma(2,1) = 9$ y $\sigma(0,3) = 45$, además se sabe que $9 \mid 45$; pero $(2,1) \nmid (0,3)$ porque si lo dividiera tendría que existir un (x,y) tal que:

$$(2,1)(x,y) = (2x - 5y, x + 2y) = (0,3)$$

de donde:

$$\begin{aligned} 2x - 5y &= 0 \\ x + 2y &= 3 \end{aligned}$$

de modo que:

$$\begin{aligned} 2x - 5y &= 0 \\ -2x - 4y &= -6 \end{aligned}$$

por lo tanto se obtiene:

$$3y = 2$$

ecuación que no tienen solución en $\mathbb{Z}$. Sin embargo, lo anteriormente mostrado no implica que no exista un elemento con σ-norma igual a 9 que divida $(0,3)$, por ejemplo $(3,0) \mid (0,3)$

pues $(3,0)(0,1) = (0,3)$. De modo que de existir este elemento, la tarea es determinar cuáles de los posibles elementos w, cuya σ-norma es n y $n \mid \sigma(z)$, dividen a z. Con esto, el teorema anterior sugiere una forma para encontrar los divisores de un elemento dado.

Por otro lado, la siguiente tabla contiene los divisores del elemento $(2,4)$, de la cual es posible observarse que para todo w que lo divide, $\sigma(w) \leq \sigma((2,4))$. Por lo cual se presenta el siguiente teorema que relaciona nuevamente la divisibilidad con la σ-norma.

w	$\sigma(w)$
$(1,0)$ $(-1,0)$	1
$(2,0)$ $(-2,0)$	4
$(-1,1)$ $(1,-1)$	6
$(3,-1)$ $(-3,1)$	14
$(1,2)$ $(-1,-2)$	21
$(2,4)$ $(-2,-4)$	84

Tabla 4.1: Divisores de $(2,4)$ y sus σ-norma

Teorema 4.5. Sean $z, w \in \mathbb{Z}[\sqrt{-5}]$ si $w \neq (0,0)$ y $z \mid w$ entonces $\sigma(z) \leq \sigma(w)$

Demostración. Por el teorema 4.1 se tiene que si $z \mid w$ entonces $\sigma(z) \mid_{\Sigma} \sigma(w)$, por tanto $\sigma(z) \mid \sigma(w)$. Ahora, como $\sigma(z)$ y $\sigma(w)$ son números naturales entonces por propiedades de la divisibilidad en $\mathbb{N}$ se tiene que $\sigma(z) \leq \sigma(w)$. □

La importancia del teorema anterior es que cualquier $w \in \mathbb{Z}[\sqrt{-5}]$ con $w \neq (0,0)$ solo admite un número finito de divisores, pues de no ser así entraría en contradicción con el principio del buen orden. Este hecho es muy importante porque, entre otras cosas, justifica el estudio del máximo común divisor.

Antes de estudiar esta propiedad, se comenzará por analizar la posibilidad de exportar el algoritmo de la división del dominio entero al superconjunto en estudio, lo que de cumplirse asegurará la existencia de una división entre elementos de $\mathbb{Z}[\sqrt{-5}]$ con cociente y residuo único. Lo anterior permitirá determinar si la extensión estudiada es un anillo euclideo, además

de ser base de resultados como la formulación de un algoritmo de euclides para calcular el máximo común divisor.

4.1.1. Algoritmo de la división

El anillo $\mathbb{Z}$ es un **anillo euclidiano**[1] pues existe una función δ definida sobre este dominio con rango en los naturales, tal que $\delta(a) \leq \delta(ab)$ para $b \neq 0$ y cumple además que para cualesquiera a, b con $b \neq 0$ en $\mathbb{Z}$ se tiene la descomposición

$$a = qb + r \text{ donde } q, r \in \mathbb{Z} \text{ y } \delta(r) < \delta(b)$$

Donde δ es la función valor absoluto.

De modo que para exportar el algoritmo de la división al superconjunto en estudio, se observa que en $\mathbb{Z}[\sqrt{-5}]$ la función candidata es la función σ indicada en la definición 1.5, pues como se demuestra en el teorema 1.14 cumple que:

$$\sigma(z) \leq \sigma(zw) \text{ con } w \neq (0,0)$$

Por tanto, para que el anillo $\mathbb{Z}[\sqrt{-5}]$ sea un anillo euclidiano con la función σ resta cumplirse que para todo $w, z \in \mathbb{Z}[\sqrt{-5}] - \{0,0\}$ existan $q, r \in \mathbb{Z}[\sqrt{-5}]$ tales que[2]:

$$w = zq + r \text{ con } r \prec z \tag{4.1}$$

Con el fin de estudiar el cumplimento de esta propiedad se tendrán en cuenta los siguientes casos.

Caso 1: Si w, z son tales que $w \prec z$.

Existen los elementos $q = (0,0)$ y $r = w$ tales que:

$$w = zq + r \text{ donde se cumple } r \prec z \text{ pues } r = w.$$

Por tanto, en este caso se cumple la propiedad indicada en (4.1).

Caso 2: Si w, z son tales que $z \prec w$. Este caso se subdivide en los siguientes casos:

i) Sea $w = (a, b)$, y $z = (c, 0)$.

[1]Pérez, E.(2005). *Estructuras Algebraicas*. Bogotá: Universidad Pedagógica Nacional. p, 156

[2]La relación $\prec$ es tal que $r \prec z$ si y solo si $\sigma(r) < \sigma(z)$, definición 1.6.

ii) Sea $w = (a, b)$, y $z = (c, d)$ con $d \neq 0$.

Nótese que el segundo caso se reduce al primero pues $z\bar{z} = (c^2 + 5d^2, 0)$ y como se tiene que[3]

$$\frac{w}{z} = \frac{w\bar{z}}{z\bar{z}}$$

entonces hallar los q, r que cumplan (4.1) es lo mismo que hallar los s, t tales que:

$$\begin{aligned} w\bar{z} &= (z\bar{z})\, s + t \text{ con } \sigma(r_1) < \sigma(z\bar{z}) \\ (ac + 5bd, bc - ad) &= (a^2 + 5b^2, 0)s + t \text{ con } \sigma(r_1) < \sigma(z\bar{z}) \end{aligned}$$

Por tanto se procede a estudiar el segundo caso. Sea $w = (a, b)$, y $z = (c, 0)$ se deben hallar $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tales qué:

$$(a, b) = (c, 0)(q_1, q_2) + (r_1, r_2) \tag{4.2}$$

y que cumplan:

$$\sigma((r_1, r_2)) < c^2. \tag{4.3}$$

Gracias a la definición 1.3 (igualdad en $\mathbb{Z}[\sqrt{-5}]$), se puede usar el algoritmo de la división[4] en $\mathbb{Z}$ para hallar los números enteros que satisfagan (4.2), así:

$$\begin{aligned} a &= cq_1 + r_1 \\ b &= cq_2 + r_2. \end{aligned}$$

Obsérvese ahora que el sistema de ecuaciones anterior tiene infinitas soluciones, para cada una de las cuales es posible afirmar que:

$$\sigma((r_1, r_2)) < 6c^2$$

pues r_i con $i = \{1, 2\}$ cumple que $r_i < c$. De modo que el conjunto $H \subset \mathbb{N}$ formado por las σ-normas de los (r_1, r_2) al ser no vacío tiene elemento mínimo. Por tanto la tarea ahora es hallar el elemento (r_1, r_2) tal que $\sigma(r_1, r_2) \leq a$ para todo $a \in H$ con la esperanza de que este cumpla (4.3).

Ejemplo 4.2. Dividir $(3, 5)$ entre $(2, 0)$. Es decir que se deben hallar q_1, q_2, r_1, r_2 que cumplan que $\sigma(r)$ sea la menor posible y que:

$$\begin{aligned} (3, 5) &= (2, 0)(q_1, q_2) + (r_1, r_2) \\ (3, 5) &= (2q_1 + r_1, 9q_2 + r_2) \end{aligned}$$

[3]Esta igualdad hace referencia a que resultado dividir a w entre z es igual al resultado de dividir a $w\bar{z}$ entre z por su conjugado.

[4]Modificado, pues en $\mathbb{Z}$ se exige que r sea positivo para que q, r sean únicos. En este caso se puede colocar r_1, r_2 negativos.

de lo anterior se tiene

$$3 = 2q_1 + r_1 \quad \wedge \quad 5 = 2q_2 + r_2$$

Por tanto los elementos que cumplen las condiciones indicadas son:

$$q = (1,2), r = (1,1) \text{ o } q = (2,2), r = (-1,1)$$

Sin embargo, a pesar de que se hallaron $(q_1, q_2), (r_1, r_2)$ de manera que $\sigma((r_1, r_2))$ fuera lo menor posible no se cumple que $\sigma((r_1, r_2)) < \sigma((2,0))$ pues

$$\sigma(1,1) = 6 \not< \sigma(2,0) = 4 \text{ y } \sigma(-1,1) = 6 \not< \sigma(2,0) = 4$$

Por tanto, no existen q, r tales que $(3,5) = (2,0)q + r$ con $r \prec (2,0)$.

El ejemplo anterior muestra que no existe una división con residuo para todo w, z tal que w tiene su segunda componente igual a 0. Ahora, como el segundo caso se reduce al primero entonces no existe un algoritmo de la división en $\mathbb{Z}[\sqrt{-5}]$.

Aunque el algoritmo no se cumple, el método mostrado resulta útil en algunos casos para hallar el cociente y el residuo de dividir dos elementos dados, tal y como se muestran en los siguientes ejemplos.

Ejemplo 4.3. Dividir $(1,4)$ entre $(2,0)$. Es decir que:

$$\begin{aligned} (1,4) &= (2,0)(q_1, q_2) + (r_1, r_2) \\ (1,4) &= (2q_1 + r_1, 2q_2 + r_2) \end{aligned} \tag{4.4}$$

Entonces, para hallar $(q_1, q_2), (r_1, r_2)$ tales que $\sigma((r_1, r_2)) < \sigma((2,0))$ se escogerán los q_1, q_2, r_1, r_1 que cumplan la ecuación (4.4), tales que $\sigma((r_1, r_2))$ sea lo menor posible. Estos elementos son:

$$\begin{gathered} 1 = 2(0) + (1) \quad \wedge \quad 4 = 2(2) + (0) \\ \text{o} \\ 1 = 2(1) + (-1) \quad \wedge \quad 4 = 2(2) + (0) \end{gathered}$$

entonces, $r = (1,0)$ o $r = (-1,0)$ pues:

$$\sigma(1,0) = 1 < \sigma(2,0) = 4 \text{ y } \sigma(-1,0) = 1 < \sigma(2,0) = 4$$

lo que conduce a que el cociente y el residuo no son únicos. En la propiedad de existencia del algoritmo de la división que se explicitó, no se pide que q, r sean únicos. Para la unicidad

hay que indicar otra condición, por ejemplo, en los enteros se pide que el residuo sea no negativo en cuyo caso el residuo es único. En $\mathbb{Z}[\sqrt{-5}]$ no es evidente como escoger el residuo, usualmente se escogerá el de menor norma posible; pero en este ejemplo como las normas son iguales se elegirá el de componentes no negativas. Con lo anterior se tiene que:

$$(1,4) = (2,0)(0,2) + (1,0)$$

Ejemplo 4.4. Dividir $w = (5,3)$ entre $z = (2,1)$. De modo que se dividirá $(5,3)(2,-1)$ entre $(2,1)(2,-1)$, de la siguiente manera:

$$\begin{aligned} (5,3)(2,-1) &= (2,1)(2,-1)(q_1,q_2) + (r_1,r_2) \\ (25,1) &= (9,0)(q_1,q_2) + (r_1,r_2) \\ (25,1) &= (9q_1 + r_1, 9q_2 + r_2) \end{aligned}$$

por definición 1.3 (igualdad entre parejas) se obtiene

$$25 = 9q_1 + r_1 \quad \wedge \quad 1 = 9q_2 + r_2 \tag{4.5}$$

Por tanto, se deben hallar q_1, q_2, r_1, r_2 que cumplan la ecuación (4.5) tales que $\sigma((r_1,r_2))$ sea lo menor posible. Estos son:

$$\begin{gathered} (q_1,q_2) = (2,0) \quad , \quad (r_1,r_2) = (7,1) \\ \text{o} \\ (q_1,q_2) = (3,0) \quad , \quad (r_1,r_2) = (-2,1) \end{gathered}$$

donde el residuo el residuo de la división inicial es $w - zq$, pues,

$$\begin{aligned} w\bar{z} &= (z\bar{z})\, q + r \\ \frac{r}{\bar{z}} &= w - zq \end{aligned}$$

donde $q = (2,0)$ o $q = (3,0)$, entonces

$$\begin{aligned} \frac{r}{\bar{z}} &= (5,3) - (2,1)(2,0) = (1,1) \\ \frac{r}{\bar{z}} &= (5,3) - (2,1)(3,0) = (-1,0). \end{aligned}$$

Por tanto $\frac{r}{\bar{z}} = (1,1)$ o $\frac{r}{\bar{z}} = (-1,0)$. Nuevamente el cociente y el residuo no es unico, pues:

$$\sigma(1,1) = 6 < \sigma(2,1) = 9 \text{ y } \sigma(-1,0) = 1 < \sigma(2,1) = 9.$$

es decir que $(1,1) \prec (2,1)$ y $(-1,0) \prec (2,1)$. Para que sean únicos se escogerá el residuo de menor σ-norma, entonces la descomposición con residuo de $(5,3)$ entre $(2,1)$ es:

$$(5,3) = (2,1)(3,0) + (-1,0)$$

En conclusión, como en $\mathbb{Z}[\sqrt{-5}]$ no se cumple la existencia de una división con residuo para todo par de elementos z, w entonces no se cumple la segunda propiedad necesaria para que el dominio $\mathbb{Z}[\sqrt{-5}]$ con la función σ sea un anillo euclidiano.

Teorema 4.6. El dominio $\mathbb{Z}[\sqrt{-5}]$ con la función σ no es un anillo euclidiano.

4.1.2. El máximo común divisor

Dado que en $\mathbb{Z}[\sqrt{-5}]$ no se cuenta con un algoritmo de la división con la función σ, no es posible contar como en el caso de los enteros con un procedimiento eficiente que permita encontrar, en caso de que exista, el máximo común divisor de z, w de $\mathbb{Z}[\sqrt{-5}]$. Pese a esto, a continuación se procede a verificar si a partir de criterios es posible hallar el MCD de dos elementos dados.

Sean $z, w \in \mathbb{Z}[\sqrt{-5}]$, no ambos cero, entonces un $g \in \mathbb{Z}[\sqrt{-5}]$ que cumpla:

i) $g \mid z$ y $g \mid w$

ii) Si $k \mid z$ y $k \mid w$, entonces $k \mid g$

se llamará el Máximo común divisor de z y w. A continuación se presenta un ejemplo en el que haciendo uso de estos criterios se pretende hallar el MCD de dos elementos.

Ejemplo 4.5. Para determinar el máximo común divisor entre $(4, 2)$ y $(6, 0)$ se descompone cada uno de estos elementos, haciendo uso del software, de la siguiente manera.

$$\begin{aligned} z = (4,2) &= (2,1)(2,0) \\ &= (1,-1)(-1,1) \\ &= (1,0)(4,2) \end{aligned} \qquad \begin{aligned} z = (4,2) &= (-2,-1)(-2,0) \\ &= (-1,1)(1,-1) \\ &= (-1,0)(-4,-2) \end{aligned}$$

$$\begin{aligned} w = (6,0) &= (3,0)(2,0) \\ &= (1,1)(1,-1) \\ &= (1,0)(6,0) \end{aligned} \qquad \begin{aligned} w = (6,0) &= (-3,0)(-2,0) \\ &= (-1,-1)(-1,1) \\ &= (-1,0)(-6,0) \end{aligned}$$

De aquí se halla que los divisores comunes de $(4, 2)$ y $(6, 0)$ son:

$$(1,0), (-1,0), (2,0), (-2,0), (1,-1) \text{ y } (-1,1)$$

Ahora, se descomponen estos elementos para averiguar si alguno tiene como divisor a todos los demás.

$$
\begin{aligned}
(1,0) &= (1,0)(1,0) \\
&= (-1,0)(-1,0)
\end{aligned}
\qquad
\begin{aligned}
(2,0) &= (1,0)(2,0) \\
&= (-1,0)(-2,0)
\end{aligned}
\qquad
\begin{aligned}
(1,-1) &= (1,0)(1,-1) \\
&= (-1,0)(-1,1)
\end{aligned}
$$

$$
\begin{aligned}
(-1,0) &= (1,0)(-1,0)
\end{aligned}
\qquad
\begin{aligned}
(-2,0) &= (1,0)(-2,0) \\
&= (-1,0)(2,0)
\end{aligned}
\qquad
\begin{aligned}
(-1,1) &= (1,0)(-1,1) \\
&= (-1,0)(1,-1)
\end{aligned}
$$

De lo anterior se observa que ningún elemento cumple el criterio *ii)*, pues $(2,0) \nmid (1,-1)$ y $(1,-1) \nmid (2,0)$, de modo que para esta pareja de elementos no existe MCD.

Ejemplo 4.6. Determinar el máximo común divisor de $(8,15)$ y $(28,9)$. Con este fin se descompone cada uno de estos elementos, como se muestra a continuación.

$$
\begin{aligned}
(8,15) &= (3,2)(6,1) \\
&= (1,0)(8,15)
\end{aligned}
\qquad
\begin{aligned}
(8,15) &= (-3,-2)(-6,-1) \\
&= (-1,0)(-8,-15)
\end{aligned}
$$

$$
\begin{aligned}
(28,9) &= (3,2)(6,-1) \\
&= (1,0)(28,9)
\end{aligned}
\qquad
\begin{aligned}
(28,9) &= (-3,-2)(-6,1) \\
&= (-1,0)(-28,-9)
\end{aligned}
$$

Obsérvese que para este caso los divisores comunes son $(1,0),(-1,0),(3,2),(-3,-2)$, de donde se tiene que los elementos $(3,2)$ y $(-3,-2)$ son divisibles por los demás, por tanto estos corresponden al MCD entre $(8,15)$ y $(28,9)$.

Así pues con los criterios dados no siempre existe el máximo común divisor de dos números en $\mathbb{Z}[\sqrt{-5}]$. Ahora, se analizará qué sucede si se usa la relación $\prec$ definida en el capítulo 1 para calcular el MCD. En este sentido, se denominará máximo común divisor de $z, w \in \mathbb{Z}[\sqrt{-5}]$ al elemento d_i que pertenece conjunto de divisores comunes $D_{zw} = \{d_1, d_2, d_3 \ldots d_n\}$, que cumple que $d_j \prec d_i$ para todo j, con $1 \leq j \leq n$.

Haciendo uso de esta definición, se observa que en el ejemplo 4.5 no existe MCD pues $(1,-1) \not\prec (-1,1)$ y $(-1,1) \not\prec (1,-1)$, es decir, que en el conjunto de los divisores comunes existen elementos que no se pueden comparar con la relación $\prec$, situación que se repite en el ejemplo 3.6 pues $(3,2) \not\prec (-3,-2)$ y $(-3,2) \not\prec (3,2)$. Lo anterior permite concluir que con esta definición no es posible calcular el MCD de dos elementos dados a menos que se escoja uno de ellos. Lo anterior es viable en tanto que ambos elementos pertenecen a la misma clase definida en el capitulo 1, pues están relacionados mediante $\approx$. Por tanto se elegirá un (a,b)

como representante de la clase, que pertenezca al conjunto de los comunes divisores y que cumpla que $a > 0$ o $b > 0$. Teniendo esto, es posible decir que el máximo común divisor de $(4, 2)$ y $(6, 0)$ es $(1, -1)$ y que el máximo común divisor de $(8, 15)$ y $(28, 9)$ es $(3, 2)$.

4.2. Proceso de Analizar en $\mathbb{Z}[\sqrt{-5}]$

En Σ se definió a los elementos irreducibles como aquellos que tienen exactamente dos divisores. Si se continua con esta definición en $\mathbb{Z}[\sqrt{-5}]$ resultaría que los elementos $(1, 0)$ y $(-1, 0)$ son irreducibes, además resultaría que haciendo productos entre ellos no es posible expresar otros elementos del conjunto. Esto indica que para descomponer elementos de $\mathbb{Z}[\sqrt{-5}]$ en términos de elementos distinguidos es necesario cambiar la noción de número irreducible que proviene del conjunto Σ. Con este fin se estudiará cuáles son los divisores que tiene todo número en $\mathbb{Z}[\sqrt{-5}]$, para dar una noción de primo que recaiga en el número de divisores que tienen estos elementos en la estructura.

Se iniciará observando que $(1, 0)$ y $(-1, 0)$ son divisores comunes de los elementos presentados en los ejemplos anteriores, lo que sugiere que $(1, 0)$ y $(-1, 0)$ son divisores de todos los elementos de $\mathbb{Z}[\sqrt{-5}]$, característica que cumplen el 1 y el -1 en la estructura de los números enteros, los cuales son denominados **unidades**. Tomando como referencia las unidades en las estructuras usuales de los números enteros y naturales, a continuación se define las unidades en el conjunto $\mathbb{Z}[\sqrt{-5}]$.

Definición 4.2. Un elemento u de $\mathbb{Z}[\sqrt{-5}]$ es una unidad si y sólo si para todo $v \in \mathbb{Z}[\sqrt{-5}]$ se cumple que $u \mid v$

De modo que el primer candidato para ser unidad en el $\mathbb{Z}[\sqrt{-5}]$ es el elemento $(1, 0)$, como se prueba a continuación.

Teorema 4.7. El elemento $(1, 0)$ es unidad en $\mathbb{Z}[\sqrt{-5}]$

Demostración. Se debe probar que $(1, 0) \mid (a, b)$ para todo$(a, b) \in \mathbb{Z}[\sqrt{-5}]$. Para ello debe demostrarse que existe la pareja (x, y) tal que:

$$(1, 0)(x, y) = (a, b)$$

Como la pareja $(1, 0)$ es el elemento neutro de la multiplicación, entonces se tiene que:

$$(1, 0)(a, b) = (a, b)$$

De modo que

$$(x, y) = (a, b)$$

Así por definición de divisibilidad $(1, 0)$ divide a todo $(a, b) \in \mathbb{Z}[\sqrt{-5}]$ □

Para encontrar otras unidades en $\mathbb{Z}[\sqrt{-5}]$ se usa la propiedad transitiva de la relación de divisibilidad. De modo que si $(1, 0) \mid (x, y)$ para todo (x, y) en $\mathbb{Z}[\sqrt{-5}]$ y $(r, s) \mid (1, 0)$ entonces haciendo uso del teorema 4.2 se tiene que $(r, s) \mid (x, y)$ para todo $(x, y) \in \mathbb{Z}[\sqrt{-5}]$. Lo que indica que los divisores de $(1, 0)$ son unidades en $\mathbb{Z}[\sqrt{-5}]$.

Así pues, es de interés buscar los números $(a, b) \in \mathbb{Z}[\sqrt{-5}]$ tales que $(a, b) \mid (1, 0)$. Para ello téngase en cuenta de que si $(a, b) \mid (1, 0)$, por definición 4.1 existe $(x, y) \in \mathbb{Z}[\sqrt{-5}]$ tal que:

$$\begin{aligned} (a, b)(x, y) &= (1, 0) \\ ((ax - 5by), (bx + ay)) &= (1, 0) \end{aligned}$$

y por definición 1.3 se obtiene el siguiente sistema de ecuaciones:

$$\begin{aligned} ax - 5by &= 1 \\ bx + ay &= 0 \end{aligned}$$

resolviendo estas ecuaciones haciendo uso de la regla de Cramer se obtiene

$$x = \frac{\begin{vmatrix} 1 & -5b \\ 0 & a \end{vmatrix}}{\begin{vmatrix} a & -5b \\ b & a \end{vmatrix}} = \frac{a}{a^2 + 5b^2}$$

$$y = \frac{\begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix}}{\begin{vmatrix} a & -5b \\ b & a \end{vmatrix}} = \frac{b}{a^2 + 5b^2}$$

Pero estos elementos (x, y) son especiales, debido a que no todo (x, y) en $\mathbb{Z}[\sqrt{-5}]$ tiene inverso multiplicativo, por ello es necesario establecer condiciones para saber cuando $x, y \in \mathbb{Z}$, con este fin, obsérvese que:

$$\begin{aligned} (x, y) &= \left(\frac{a}{a^2 + 5b^2} \, , \, \frac{b}{a^2 + 5b^2} \right) \\ x^2 + 5y^2 &= \left(\frac{a}{a^2 + 5b^2} \right)^2 + 5 \left(\frac{b}{a^2 + 5b^2} \right)^2 \\ x^2 + 5y^2 &= \frac{1}{a^2 + 5b^2} \end{aligned} \tag{4.6}$$

Por lo tanto, al suponer que x, y son enteros, es claro que $x^2 + 5y^2$ es entero, pero para que se cumpla la igualdad (4.6) es necesario que

$$a^2 + 5b^2 = \pm 1 \tag{4.7}$$

En consecuencia, los únicos enteros a, b que cumplen la igualdad (4.7) son $1, 0$ y $-1, 0$. De modo que las unidades en $\mathbb{Z}[\sqrt{-5}]$ son los elementos $(1, 0)$ y $(-1, 0)$ como era de esperarse. Lo anterior se puede resumir en el siguiente teorema que hace uso la relación de la σ-norma con las unidades.

Teorema 4.8. Sea $w \in \mathbb{Z}[\sqrt{-5}]$, w es unidad si y solo si $\sigma(w) = 1$.

Ya habiendo estudiado que elementos dividen a todo elemento del superconjunto, surge la pregunta de si existe algún número que sea divisible por todo $z \in \mathbb{Z}[\sqrt{-5}]$. Para ello nótese que $w(0, 0) = (0, 0)$ de modo que $w \mid (0, 0)$ para todo $w \in \mathbb{Z}[\sqrt{-5}]$. También se cumple que si $(0, 0) \mid w$ entonces $w = (0, 0)$ con lo que se tiene que el único elemento con estas propiedades es el $(0, 0)$.

Continuando con la labor de averiguar cuáles son los divisores que tiene todo número, surge la pregunta de quién divide a un $(a, b) \in \mathbb{Z}[\sqrt{-5}]$ aparte de las unidades, para ello se referirán los ejemplos 4.5 y 4.6, donde se cumple que:

$$\begin{aligned} (1, -1) \mid (-1, 1) \quad &\text{y} \quad (-1, 1) \mid (1, -1) \\ (3, 2) \mid (-3, -2) \quad &\text{y} \quad (-3, -2) \mid (3, 2) \end{aligned}$$

A partir de esto es posible observar que un divisor de un (a, b), diferente de el mismo, es $(-a, -b)$, pues $(a, b) = (-a, -b)(-1, 0)$. Lo anterior motiva a definir la siguiente relación.

Definición 4.3. Sean $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$ el elemento z_1 es **asociado** de z_2 notado por $z_1 \sim z_2$ si y sólo si $z_1 = z_2 u_i$ con u_i una unidad de $\mathbb{Z}[\sqrt{-5}]$.

Teorema 4.9. La relación $\sim$ es una relación de equivalencia.

Demostración. Para todo $z_1 \in \mathbb{Z}[\sqrt{-5}]$, $z_1 = z_1(1, 0)$, por tanto $z_1 \sim z_1$ en consecuencia esta relación cumple la propiedad reflexiva. Ahora, sí $z_1 \sim z_2$ quiere decir que $z_1 = z_2 u_i$ y como existe un u_j tal que $u_i u_j = (1, 0)$, entonces $z_1 u_j = z_2 u_i u_j$ por tanto $z_1 u_j = z_2$, es decir que $z_2 \sim z_1$. Por tanto la relación $\sim$ cumple la propiedad simétrica. La relación es transitiva puesto que si $z_1 \sim z_2$ y $z_2 \sim z_3$ significa que $z_1 = z_2 u_i, z_2 = z_3 u_j$ sustituyendo la segunda en la primera igualdad resulta que $z_1 = z_3 u_j u_i$ donde $u_j u_i = u_k$, por tanto $z_1 = z_3 u_k$. Lo anterior indica que $z_1 \sim z_3$. □

La forma en que se identificaron los asociados de un número permite conjeturar que si $z \mid w$ y $w \mid z$ entonces son z y w son asociados, la pregunta es si el recíproco también se cumple, lo cual se prueba a continuación.

Teorema 4.10. $z \sim w$ si y solo si $w \mid z$ y $z \mid w$..

Demostración. Como $z \sim w$ por definición 4.3 se tiene para un u_i se cumple que $z = wu_i$. Ahora por el teorema 4.9 se tiene que $w \sim z$, por lo tanto $w = zu_j$ entonces $w \mid z$ y $z \mid w$.

Para la demostración a izquierda, como $w \mid z$ y $z \mid w$ por definición 4.1 existen s, t tales que $ws = z$ y $zt = w$, sustituyendo la segunda en la primera igualdad resulta que $z(ts) = z$ de modo que $ts = (1, 0)$. Teniendo en cuenta lo anterior $t \mid (1, 0)$ y $s \mid (1, 0)$, ahora como para todo $r \in \mathbb{Z}[\sqrt{-5}]$ se cumple que $(1, 0) \mid r$ entonces $s \mid r$ y $t \mid r$ esto debido a la propiedad transitiva de la relación de divisibilidad. Ahora por la definición 4.2 s, t son unidades, lo que permite concluir que $z \sim w$ y $w \sim z$. □

Ahora, obsérvese que cuando se hallan los divisores de un elemento w dado, como en el siguiente ejemplo, siempre se halla que si un $z \mid w$ su asociado z_1 también divide a w, por lo que se prueba el siguiente teorema.

Ejemplo 4.7. $(3, -1) \mid (5, 3)$ pues existe $(0, 1)$ tal que $(3, -1)(0, 1) = (5, 3)$.
. $(-3, 1) \mid (5, 3)$ pues existe $(0, -1)$ tal que $(-3, 1)(0, -1) = (5, 3)$.

donde $(3, -1) \sim (-3, 1)$ relación que también se cumple para los elementos $(0, 1), (0, -1)$.

Teorema 4.11. Si $z \mid w$ y $z_1 \sim z$, entonces $z_1 \mid w$.

Demostración. Dado $z_1 \sim z$, entonces por el teorema 4.10 $z_1 \mid z$ y por propiedad transitiva de la relación de divisibilidad, teorema 4.9, se tiene que $z_1 \mid w$. □

Lo anterior permite concluir que el menor número de divisores que puede tener un elemento dado, distinto de las unidades y el $(0, 0)$, son 4; las dos unidades y sus dos asociados. Gracias a esto es posible definir número irreducible en $\mathbb{Z}[\sqrt{-5}]$ de la siguiente manera.

Definición 4.4. Un elemento $w \in \mathbb{Z}[\sqrt{-5}]$ distinto de las unidades es irreducible sí y solo es divisible únicamente por las unidades y sus asociados.

Considérese ahora, los elementos de $\mathbb{Z}[\sqrt{-5}]$ diferentes de las unidades y el $(0, 0)$. Cada uno de estos elementos puede ser clasificado como un número irreducible o un número compuesto, es decir, un número que posee factores diferentes de las unidades y sus asociados. Por tanto se tiene que todo número de $\mathbb{Z}[\sqrt{-5}]$ es $(0, 0)$, unidad, irreducible o compuesto.

Teorema 4.12. Para todo $z \in \mathbb{Z}[\sqrt{-5}]$ con z compuesto, existe un w irreducible en $\mathbb{Z}[\sqrt{-5}]$ tal que $w \mid z$.

Demostración. Como z un número compuesto en $\mathbb{Z}[\sqrt{-5}]$ entonces $z = z_1 z_2$, donde $z_1 \prec z$ y $z_2 \prec z$. Si z_1 o z_2 son irreducibles entonces el teorema queda probado. Si ninguno es irreducible entonces $z_1 = z_3 z_4$ donde $z_3 \prec z_1$ y $z_4 \prec z_1$. Otra vez si z_3 o z_4 son irreducibles, el teorema queda demostrado, si por el contrario ambos son compuestos entonces $z_3 = z_5 z_6$ donde $z_5 \prec z_3$ y $z_6 \prec z_3$. De continuar con el proceso luego de k pasos se tendría que $z_{2k-1} = z_{2k+1} z_{2k+2}$ donde $z_{2k+1} \prec z_{2k-1}$ y $z_{2k+2} \prec z_{2k+1}$. Como con cualquier valor de k se tiene

$$(0,0) \prec z_{2k-1} \prec \cdots \prec z_5 \prec z_4 \prec z_3 \prec z_2 \prec z_1 \prec z$$

lo que equivale a

$$0 < \sigma(k_{2k-1}) < \cdot < \sigma(z_5) < \sigma(z_4) < \sigma(z_3) < \sigma(z_2) < \sigma(z_1) < \sigma(z)$$

entonces el proceso debe terminar pues de lo contrario se contradice el principio del buen orden. De ahí que debe existir un z_{2k-1} irreducible para algún k que con lo que queda demostrado que todo número compuesto en $\mathbb{Z}[\sqrt{-5}]$ posee un factor irreducible. □

Ahora pues, el paso a seguir es caracterizar los elementos irreducibles en $\mathbb{Z}[\sqrt{-5}]$. Dado que el conjunto $\mathcal{Z} = \{z \in \mathbb{Z}[\sqrt{-5}] : z = (a,0)\}$ con las operaciones suma y multiplicación definidas en $\mathbb{Z}[\sqrt{-5}]$ es isomorfo al dominio de los números enteros, teorema 1.10, surge naturalmente la pregunta de si ¿todo número de la forma $(p,0)$, con p primo en $\mathbb{Z}$ es irreducible en $\mathbb{Z}[\sqrt{-5}]$?

Para responder esta pregunta, inicialmente se averiguará si existen números de la forma $(p,0)$ que se puedan expresar como el producto de dos números α, β no unidades de $\mathbb{Z}[\sqrt{-5}]$, o si por el contrario, todo número de $\mathcal{Z}$ con primera componente prima puede ser descompuesto únicamente en términos de las unidades u_i y sus asociados.

La exploración hecha a partir de la búsqueda de divisores, muestra que efectivamente existen elementos $(p,0)$ que son descomponibles. Algunos de estos elementos se muestran en la tabla 4.2.

De modo que el problema ahora es, cuándo un número de la forma $(p,0)$ con p primo en $\mathbb{Z}$ se puede expresar como el producto de dos elementos de $\mathbb{Z}[\sqrt{-5}]$ diferentes de las unidades. La respuesta a esta pregunta está basada en el hecho de que en este anillo, los elementos $(p,0)$ descomponibles se pueden escribir como el producto

$$(p,0) = (x,y)(x,-y) \tag{4.8}$$

z	$z = \alpha\beta$
$(5,0)$	$(0,1)(0,-1)$
$(29,0)$	$(3,2)(3,-2)$
$(41,0)$	$(6,1)(6,-1)$
$(61,0)$	$(4,3)(4,-3)$
$(89,0)$	$(3,4)(3,-4)$
$(101,0)$	$(9,2)(9,-2)$
$(109,0)$	$(8,3)(8,-3)$
$(149,0)$	$(12,1)(12,-1)$
$(181,0)$	$(1,6)(1,-6)$

Tabla 4.2: Elementos $(p,0)$ descomponibles

como se observa en la tabla 4.1, esto implica que

$$p^2 = \sigma(x,y)\sigma(x,-y)$$
$$p^2 = \left(x^2+5y^2\right)^2$$

De modo que para responder al cuándo, se debe averiguar para qué elementos p de $\mathbb{Z}$ existe solución a la ecuación:

$$p = x^2 + 5y^2, \text{ con } x, y \in \mathbb{Z} \tag{4.9}$$

es decir, qué números de la forma $(p,0)$ con p primo en $\mathbb{Z}$ no son irreducibles en $\mathbb{Z}[\sqrt{-5}]$. Con este interés es preciso notar, que el teorema 3.2 demuestra que los primos enteros p que se pueden escribir como (4.9) cumplen que $p \equiv 1,5,9 \mod 20$. De modo que si $p \equiv 1,5,9$ mód 5 entonces $(p,0)$ es compuesto.

Ya habiendo demostrado para qué p primos enteros, $(p,0)$ es reducible, resta responder para qué p primos enteros $(p,0)$ es irreducible en $\mathbb{Z}[\sqrt{-5}]$. Con este fin se presenta el siguiente teorema.

Teorema 4.13. Si p primo en $\mathbb{Z}$ y $p \not\equiv 1,5,9 \mod 20$ entonces $(p,0)$ es irreducible en $\mathbb{Z}[\sqrt{-5}]$.

Demostración. Se razonará por contradicción. Supóngase que $(p,0)$ es compuesto entonces $(p,0) = zw$ con $z, w \in \mathbb{Z}[\sqrt{-5}]$ y z, w distintos de las unidades. Ahora pues, aplicando la función σ se tiene:

$$\begin{aligned} \sigma((p,0)) &= \sigma(zw) \\ \sigma((p,0)) &= \sigma(z)\sigma(w) \\ p^2 &= \sigma(z)\sigma(w) \end{aligned}$$

dado que z, w son diferentes de las unidades entonces $p = \sigma(z)$ lo que implica que $p = x^2+5y^2$ para algún x, y que pertenece a $\mathbb{Z}$, y por el teorema 3.2 $p \equiv 1, 5, 9 \mod 20$ esto resulta en una contradicción con la hipótesis lo que permite concluir que $(p, 0)$ es irreducible en $\mathbb{Z}[\sqrt{-5}]$. □

Es decir, que $(p, 0)$ es irreducible en $\mathbb{Z}[\sqrt{-5}]$ si $p \equiv 2, 3, 7, 11, 13, 17, 19 \mod 20$. Ya habiendo hallado los $(p, 0)$ que son irreducibles en en $\mathbb{Z}[\sqrt{-5}]$, se procederá a estudiar los elementos que resultan de la descomposición de aquellos $(p, 0)$ que son reducibles. Estudiando estos elementos haciendo uso de la tabla 4.2 se halló que todos los elementos que resultan de la descomposición de los $(p, 0)$ con $p \equiv 1, 5, 9 \mod 20$ son irreducibles en $\mathbb{Z}[\sqrt{-5}]$. Esto en tanto que por el teorema 3.2 se conoce que si $p \equiv 1, 5, 9 \mod 20$ entonces existe un (x, y) tal que $\sigma((x, y)) = p$ y dado que ese (x, y) tiene norma prima entonces se conjetura que este a su vez es irreducible.

Una conjetura mas general que la anterior es que todo número en $\mathbb{Z}[\sqrt{-5}]$ cuya norma es irreducible en Σ es irreducible en $\mathbb{Z}[\sqrt{-5}]$, lo cual se prueba a continuación.

Teorema 4.14. Si r un número irreducible en Σ y $w \in \mathbb{Z}[\sqrt{-5}]$, tal que $\sigma(w) = r$, entonces w es irreducible en $\mathbb{Z}[\sqrt{-5}]$.

Demostración. Supóngase que w no es irreducible en $\mathbb{Z}[\sqrt{-5}]$, entonces $w = zt$, donde z y t no son unidades, entonces como $r = \sigma(w)$ y la σ-norma definida es multiplicativa, entonces $r = \sigma(z)\sigma(t)$. Ahora como r es irreducible, entonces $\sigma(z)$ es unidad ó $\sigma(t)$ es unidad, lo cual es una contradicción, puesto que los únicos elementos en $\mathbb{Z}[\sqrt{-5}]$ que tienen σ-norma 1 son las unidades, por tanto w es un número irreducible en $\mathbb{Z}[\sqrt{-5}]$. □

Por tanto los $z \in \mathbb{Z}[\sqrt{-5}]$ tales que $\sigma(z)$ cumple alguno de los siguientes criterios son irreducibles en $\mathbb{Z}[\sqrt{-5}]$.

- $\sigma(z) = p^2$ con $p \equiv 2, 3, 7, 11, 13, 17, 19 \mod 20$
- $\sigma(z) = p$ con $p \equiv 1, 5, 9 \mod 20$
- $\sigma(z) = pq$ con $p \neq q$ y $p, q \equiv 2, 3, 7 \mod 20$

La pregunta que sigue es cuántos irreducibles existen en $\mathbb{Z}[\sqrt{-5}]$ por cada σ-norma, es decir, cuántos elementos tiene cada clase de equivalencia definida a partir de la relación $\approx$. Para ello se usará un programa que halla elementos de $\mathbb{Z}[\sqrt{-5}]$ dada una σ-norma y se tendrá en cuenta que si un (a, b) tiene la norma elegida, sus asociados $(a, b), (-a, -b)$ y sus conjugados $(a, -b), (-a, b)$ pertenecen a la misma clase.

Teniendo en cuenta esto, se observa que el menor número de elementos que puede tener cada clase es dos, en caso que a o b sean iguales a 0, y cuatro en caso que $a, b \neq 0$. También se observa haciendo uso del software, que los únicos irreducibles con σ-norma p^2 no son necesariamente los $(p, 0)$, pues por ejemplo el elemento $(2, 1)$ tiene σ-norma igual a 3^2. Esta característica la cumplen los p^2 tales que $p \equiv 3, 7 \mod 20$, como el primo 43 quien cumple que $43^2 = \sigma((43, 0)) = \sigma((38, 9))$ y el primo 47 quien cumple que $47^2 = \sigma((47, 0)) = \sigma((2, 21))$.

Lo anterior motiva a que se separen en dos casos los irreducibles con σ-norma p^2 de tal manera que queden en un caso los p^2 tal que $p \equiv 11, 13, 17, 19 \mod 20$ y en otro los p^2 con $p \equiv 3, 7 \mod 20$.

Ahora, para hacer más claro el conteo del número de elementos de cada clase, a continuación se presenta una tabla que muestra el irreducible en Σ y sus correspondientes irreducibles en $\mathbb{Z}[\sqrt{-5}]$, en la cual se prescinde de los asociados y de los conjugados. La tabla se organizó de manera tal que fuera posible distinguir las clases que contienen como máximo cuatro irreducibles de aquellas que tienen ocho.

p^2 con $p \equiv 11, 13, 17, 19 \mod 20$		p con $p \equiv 1, 5, 9 \mod 20$	
p^2	(x, y)	p	(x, y)
11^2	(11,0)	5	(0,1)
13^2	(13,0)	29	(3,2)
17^2	(17,0)	41	(6,1)
19^2	(19,0)	61	(4,3)
31^2	(31,0)	89	(3,4)
37^2	(37,0)	101	(9,2)
53^2	(53,0)	109	(8,3)
pq con $p, q \equiv 3, 7 \mod 20$		$2p$ con $p \equiv 2, 3, 7 \mod 20$	
pq	(x, y)	$2p$	(x, y)
$3 \cdot 3$	(2,1), (3,0)	$2 \cdot 2$	(2,0)
$3 \cdot 7$	(1,2), (4,1)	$2 \cdot 3$	(1,1)
$7 \cdot 7$	(7,0), (2,3)	$2 \cdot 7$	(3,1)
$3 \cdot 43$	(2,5), (7,4)	$2 \cdot 13$	(1,3)
$3 \cdot 47$	(4,5), (11,2)	$2 \cdot 43$	(9,1)
$7 \cdot 23$	(6,5), (9,4)	$2 \cdot 47$	(7,3)
$3 \cdot 67$	(14,1), (11,4)	$2 \cdot 67$	(3,5)

Tabla 4.3: Irreducibles en Σ y sus irreducibles en $\mathbb{Z}[\sqrt{-5}]$

De modo que la clase $[z]$ tiene la siguiente cantidad de elementos dependiendo de la forma

de $\sigma(z)$.

- Si $\sigma(z) = p^2$ con $p \equiv 11, 13, 17, 19 \mod 20$ entonces $[z]$ tiene 2 elementos.
- Si $\sigma(z) = p$ con $p \equiv 1, 5, 9 \mod 20$ entonces $[z]$ tiene 4 elementos, salvo por el $(0, 1)$.
- Si $\sigma(z) = pq$ con $p, q \equiv 3, 7 \mod 20$ entonces $[z]$ tiene 6 o 8 elementos.
- Si $\sigma(z) = 2q$ con $p \equiv 2, 3, 7 \mod 20$ entonces $[z]$ tiene 2 o 4 elementos.

Terminado esto, el nuevo interrogante que surge es: ¿se cumple el recíproco del teorema 4.14? es decir, si z un irreducible en $\mathbb{Z}[\sqrt{-5}]$ entonces $\sigma(z)$ es irreducible en Σ. Nótese que de cumplirse esto, se aseguraría que no existen otros irreducibles en $\mathbb{Z}[\sqrt{-5}]$ distintos de los ya caracterizados.

En este sentido, se analizará si dado un $(x, y) \in \mathbb{Z}[\sqrt{-5}]$, cuya σ-norma a es compuesta en Σ, es compuesto en $\mathbb{Z}[\sqrt{-5}]$. Con este fin se debe hallar la descomposición de a en Σ y como siempre es posible encontrar elementos (x_i, y_i) que tengan σ-norma igual a los factores de la descomposición de a, entonces resta por probar que algún (x_i, y_i) divide a (x, y).

Como la cantidad de elementos que pertenecen a una clase cuya σ-norma es irreducible, es finita y además no mayor a 8, entonces se debe encontrar al menos uno de estos elementos que divida a (x, y), como se muestra en los siguientes ejemplos.

Ejemplo 4.8. Dado el elemento $(4, 2)$ donde $\sigma((4, 2)) = 36$ se sabe que $36 = 4 \cdot 9$ donde 4 y 9 son irreducibles en Σ por el teorema 3.3. Nótese que los elementos de $\mathbb{Z}[\sqrt{-5}]$ que tienen σ-norma igual a 9 son:

$\sigma((x, y)) = 9$	
$(3, 0)$	$(-2, -1)$
$(-3, 0)$	$(-2, 1)$
$(2, 1)$	$(2, -1)$

Tabla 4.4: Elementos de $\mathbb{Z}[\sqrt{-5}]$ cuya σ-norma es 9

De los elementos de la tabla el número $(2, 1)$ cumple que $(2, 1) \mid (4, 2)$ pues existe $(2, 0) \in \mathbb{Z}[\sqrt{-5}]$ tal que:

$$(2, 1)(2, 0) = (4, 2)$$

Esto muestra que el elemento $(4, 2)$ es compuesto. Cabe aclarar que $(2, 1)$ no es el único elemento de σ-norma es 9 que divide a $(4, 2)$ y que no todo elemento de la tabla 4.4 divide a (4,2)

Ejemplo 4.9. Dado el elemento $(7,7)$ se tiene que su σ-norma es compuesta en Σ pues $294 = 49 \cdot 6$ donde 49 y 6 son irreducibles en Σ por los teoremas 3.3 y 3.7. Ahora, en $\mathbb{Z}[\sqrt{-5}]$ existe el elemento $(7,0)$ para el cual $\sigma((7,0)) = 49$ y además cumple que $(7,0) \mid (7,7)$ pues existe $(1,1) \in \mathbb{Z}[\sqrt{-5}]$ tal que:

$$(7,0)(1,1) = (7,7)$$

Es decir que el elemento $(7,7)$, cuya σ-norma es compuesta, es compuesto en $\mathbb{Z}[\sqrt{-5}]$. Obsérvese que no todo elemento (x,y) con $\sigma((x,y)) = 49$ divide a $(7,7)$, por ejemplo, $\sigma(2,3) = 49$ pero $(2,3) \nmid (7,7)$ pues de lo contrario debería existir (x,y) tal que $(2,3)(x,y) = (7,7)$ de donde resulta el siguiente sistema de ecuaciones:

$$\begin{aligned} 2x - 15y &= 7 \\ 3x + 2y &= 7 \end{aligned}$$

solucionando el sistema resulta que $49y = -7$ ecuación que no tiene solución en $\mathbb{Z}$. De modo que $(2,3) \nmid (7,7)$.

Los ejemplos anteriores muestran que dado un $(x,y) \in \mathbb{Z}[\sqrt{-5}]$, cuya σ-norma a es compuesta en Σ, es compuesto en $\mathbb{Z}[\sqrt{-5}]$, de donde surge la siguiente conjetura que se asumirá como verdadera; pues no se ha encontrado un contraejemplo que la refute.

Conjetura 4.1 (Criterio de descomposición)**.** Sea $w \in \mathbb{Z}[\sqrt{-5}]$ y $\sigma(w) = b$ si a irreducible en Σ y $a \mid_{\Sigma} b$ entonces existe un $z \in \mathbb{Z}[\sqrt{-5}]$ tal que $\sigma(z) = a$ y $z \mid w$.

Habiendo expuesto esto, resta demostrar que es posible descomponer un número compuesto en $\mathbb{Z}[\sqrt{-5}]$ en termino de factores irreducibles; lo que demuestra en parte la validez del Teorema Fundamental de la Aritmética en este superconjunto, salvo por la pregunta de si la factorización es única. En este sentido se prueba el siguiente teorema.

Teorema 4.15. Todo número $z = (a,b) \in \mathbb{Z}[\sqrt{-5}]$, tal que $\sigma(z) > 1$, puede ser expresado como producto finito de factores irreducibles.

Demostración. Sea $z \in \mathbb{Z}[\sqrt{-5}]$ y $\sigma(z) > 1$ si z es irreducible la demostración termina, si por el contrario z es un número compuesto entonces entonces z tiene un factor irreducible $z_1 \in \mathbb{Z}[\sqrt{-5}]$, esto es $z = z_1 z_2$ para algún $z_2 \in \mathbb{Z}[\sqrt{-5}]$ donde $\sigma(z_2) > 1$. Si z_2 es irreducible la factorización de z se ha logrado, si z_2 es un número compuesto entonces tiene un factor irreducible $z_3 \in \mathbb{Z}[\sqrt{-5}]$, esto es, $z_2 = z_3 z_4$ para algún $z_4 \in \mathbb{Z}[\sqrt{-5}]$ con $\sigma(z_4) > 1$. Si z_4 es irreducible la factorización se ha logrado para z_2 de aquí sigue que $z = z_1 z_3 z_4$. Si por el contrario z_4 no es irreducible es posible continuar con el proceso aplicado a z_2 y así obtener

un tercer factor irreducible z_5 esto es; $z = z_1 z_3 z_5 z_6$ con $z_6 \in \mathbb{Z}[\sqrt{-5}]$ y $\sigma(z_6) > 1$. En general después de k pasos se tiene que:

$$z = z_1 z_3 z_5 \cdots z_{2k-1} z_{2k}$$

donde $z_1, z_3, z_5, \cdots, z_{2k-1}$ son números irreducibles y $z_{2k} \in \mathbb{Z}[\sqrt{-5}]$ con $\sigma(z_{2k}) > 1$ de donde se tiene que:

$$\sigma(z) > \sigma(z_1) > \sigma(z_3) > \cdots > \sigma(z_{2k-1}) > \sigma(z_{2k})$$

y como por el principio del buen orden el conjunto Σ tiene un elemento mínimo, de ahí que solo existe un número finito de elementos de $\mathbb{Z}[\sqrt{-5}]$ cuyas σ-normas son menores que $\sigma(z)$, lo que indica que el proceso debe terminar, es decir, que z_{2k} es irreducible para algún $k \in \mathbb{N}$. En conclusión cualquier número de $\mathbb{Z}[\sqrt{-5}]$ distinto de las unidades y el elemento $(0, 0)$ puede ser expresado como producto de factores irreducibles. □

Nótese que como se tiene descomposición en término de irreducibles, de cumplirse el criterio de descomposición, se tendría que por cada descomposición en Σ existe por lo menos una descomposición en $\mathbb{Z}[\sqrt{-5}]$. Ahora pues, como en Σ la descomposición no es única, entonces la factorización en termino de irreducibles en $\mathbb{Z}[\sqrt{-5}]$ no es única, como se muestra en los siguientes ejemplos:

Ejemplo 4.10. Como $\sigma((11, 13)) = 966$ entonces $966 \in \Sigma$, donde su factorización en $\mathbb{N}$ esta dada por:

$$966 = 2 \cdot 3 \cdot 7 \cdot 23$$

Como ninguno de sus factores primos en $\mathbb{N}$ pertenece a Σ, entonces se hallan los productos resultantes de todas las combinaciones posibles entre $2, 3, 7, 23$ de la siguiente manera:

$$\begin{aligned} 966 &= (2 \cdot 3)(7 \cdot 23) = 6 \cdot 161 \\ 966 &= (2 \cdot 7)(3 \cdot 23) = 14 \cdot 69 \\ 966 &= (2 \cdot 23)(3 \cdot 7) = 46 \cdot 21 \end{aligned}$$

factores que por el teorema 3.4 resultan ser irreducibles en Σ. De modo que 966 tiene tres descomposiciones diferentes en términos de factores irreducibles en Σ.

De cumplirse el criterio de descomposición en $\mathbb{Z}[\sqrt{-5}]$ se tendría que el número $(11, 13)$ tiene tres descomposiciones diferentes en términos de factores irreducibles en $z \in \mathbb{Z}[\sqrt{-5}]$, salvo

por sus asociados[5].

$$\begin{aligned}(11,13) &= (-1,1)(9,-4)\\ (11,13) &= (3,1)(7,2)\\ (11,13) &= (1,-3)(-4,1)\end{aligned}$$

Ejemplo 4.11. El elemento $(0,36)$ tiene σ-norma 6480. Para comenzar se halla la descomposición de este número en $\mathbb{N}$ obteniéndose:

$$6480 = 2^4 \cdot 3^4 \cdot 5$$

Ahora, haciendo uso del teorema 3.2 se sabe que de la descomposición el único primo que pertenece a Σ es el 5. Por el teorema 3.3 los elementos $4, 6$ y 9 son irreducibles en Σ. De modo que solamente es posible reescribir $2^4 \cdot 3^4$ en términos de $4, 6, 9$. Así pues, se obtiene que,

$$\begin{aligned}6480 &= (2^2)^2 \cdot (3^2)^2 \cdot 5 \;=\; 4^2 \cdot 9^2 \cdot 5\\ 6480 &= (2 \cdot 3)^4 \cdot 5 \;=\; 6^4 \cdot 5\end{aligned}$$

entonces las dos distintas factorizaciones posibles en términos de irreducibles en Σ para el número 6480 son $4^2 \cdot 9^2 \cdot 5$ y $6^4 \cdot 5$. De aquí se sigue que el elemento $(0,36)$ tiene como mínimo dos factorizaciones distintas en $\mathbb{Z}[\sqrt{-5}]$.

$$\begin{aligned}(0,36) &= (2,0)(2,0)(3,0)(3,0)(0,1)\\ (0,36) &= (2,0)(2,0)(2,1)(2,-1)(0,1)\\ (0,36) &= (1,1)(1,1)(-1,1)(-1,1)(0,1)\end{aligned}$$

Las observaciones anteriores permiten afirmar que dado un número z compuesto en $\mathbb{Z}[\sqrt{-5}]$, este tiene como mínimo tantas descomposiciones diferentes salvo por asociados, como descomposiciones diferentes tenga $\sigma(z)$ en Σ. Con lo anterior se concluye que en $\mathbb{Z}[\sqrt{-5}]$ no se cumple el Teorema Fundamental de la Aritmética.

[5]por ejemplo para la descomposición $(11,13) = (3,1)(7,2)$ su descomposición asociada es $(11,13) = (-3,-1)(-7,-2)$.

Conclusiones

El conjunto $\mathbb{Z}[\sqrt{-5}]$ es un dominio de integridad, que no cumple la propiedad de existencia de inversos multiplicativos, lo que justificó el estudio de la divisibilidad en este superconjunto, en el cual se definió una relación $\preceq$ basada en una función σ de $\mathbb{Z}[\sqrt{-5}]$ a $\mathbb{N}$, la cual resulto ser un orden parcial que cumple la propiedad de monotonía con la multiplicación.

Dada la existencia de elementos no comparables mediante la relación $\preceq$, se define la relación $\approx$ en $\mathbb{Z}[\sqrt{-5}]$ tal que $z \approx w$ si y solo si $\sigma(z) = \sigma(w)$. Esta relación es equivalencia y permite definir el conjunto cociente $\mathbb{Z}[\sqrt{-5}]/\approx$, donde $\approx$ es una congruencia para la multiplicación y donde existe un orden total compatible con la operación.

Dada la función σ, se define el conjunto Σ de los elementos de $\mathbb{N}$ que son imagen directa de $\mathbb{Z}[\sqrt{-5}]$ por la función σ, conjunto en el cual la multiplicación es una operación, en tanto que σ es una función multiplicativa. Gracias a esto fue posible definir una relación de divisibilidad por medio de la cual se caracterizaron elementos distinguidos como: el 0, el 1, los elementos irreducibles y los compuestos. Nótese que como $\Sigma \subset \mathbb{N}$ entonces la descomposición en Σ se sigue de la descomposición en $\mathbb{N}$ con lo que se tiene que existe descomposición en termino de irreducibles, sin embargo no es única.

La cantidad de descomposiciones de un compuesto en Σ se puede calcular hallando su descomposición en $\mathbb{N}$ y fijándose en los factores primos $p \equiv 2, 3, 7 \mod 20$ los cuales al agruparse en parejas forman distintas factorizaciones.

En la extensión cuadrática $\mathbb{Z}[\sqrt{-5}]$ con las operaciones suma y multiplicación, se define una relación de divisibilidad, por medio de la cual se ejemplifica el proceso matemático de analizar mediante la caracterización de elementos distinguidos; como el $(0, 0)$ las unidades, los números irreducibles y los números compuestos. En esta estructura se prueba que todo compuesto se puede factorizar como producto finito de irreducibles y se muestra que el número de descomposiciones de un elemento dado no es única, pues existen al menos tantas factorizaciones diferentes para un z dado, salvo por asociados, como descomposiciones tenga $\sigma(z)$ en Σ.

El anillo $\mathbb{Z}[\sqrt{-5}]$ mostró un ejemplo de una estructura en la que las nociones de primo e irreducible no son equivalentes, como si sucede en los conjuntos usuales. Esto permitió ampliar la idea de primo a un constructo mucho mas elaborado, el cual se relaciona con la existencia de descomposición única.

Uno de los aprendizajes obtenidos con la realización de este trabajo de grado es que es posible otorgarle cualidad de objeto matemático al número primo, pues tiene distintas nociones, definiciones y representaciones. A medida que se avanza en el estudio de diferentes estructuras la noción de número primo evoluciona, lo que también nos enseña que como maestras, que es necesario estudiar diversos ejemplos para la comprensión de un objeto matemático y no consolarnos con lo ejemplos usuales.

Para futuros trabajos de grado se recomienda continuar con la revisión y demostración de los resultados y conjeturas que quedaron abiertos. También se recomienda estudiar una extensión cuadrática cambiando el k^2 por elementos como el 3 o el 13, cuyas ecuaciones de la forma $p = x^2 + ky^2$ ya han sido estudiadas.

Otro asunto que puede ser de interés para futuros trabajos de grado es el la evolución histórica del tratamiento que se le ha dado a las soluciones de las ecuaciones de la forma $p = x^2 + ny^2$, los cuales han servido de acicate para el desarrollo de la teoría de números, como es el caso de la formulación de la Ley de la reciprocidad cuadrática.

Bibliografía

[1] Ángel, L., Luque, C., & Sánchez, Y. (2014). *El proceso matemático de analizar en teoría de números: una aproximación desde la relación de divisibilidad*. XII Coloquio regional de matemáticas y II Simposio de Estadística.

[2] Beltrán, P. (2014). *Ecuaciones en el mundo discreto: Un estudio sobre las ecuaciones diofánticas*. Bogotá: Universidad Pedagógica Nacional.

[3] Cox, D.(1989). *Primes of the forme $x^2 + ny^2$: Fermat, class field theory and complex multiplication.* New York: Wiley-Interscience Publication.

[4] Hagedorn, T.(s,f). *Primes of the form $x^2 + ny^2$ and the geometry (convenient) numbers*. The college of New Jersey.

[5] Jiménez, H. (2006). *Estudio algebraico de los números Duales*. Bogotá: Universidad Pedagógica Nacional.

[6] Ivorra C. (s.f). *Álgebra*. Valencia: Universidad de Valencia.

[7] Jiménez, L., Gordillo, J. & Rubiano, G. (2004).*Teoría de números para principiantes.* Bogota: Universidad Nacional de Colombia.

[8] Jiménez, H. & Luque, C. (2007). XVII Encuentro de Geometría y sus aplicaciones. V encuentro de aritmética. *El anillo de los números duales*. Bogotá: Universidad Pedagógica Nacional.

[9] Luque, C., Jiménez, H. & Fonseca, J. (s.f). *¿Es necesaria la Propiedad Reflexiva en la Definición de Orden?*. Bogotá: Universidad Pedagógica Nacional.

[10] Luque, C., Mora, L. & Torres, J. (2005). *Estructuras análogas a los números reales*. Bogotá: Universidad Pedagógica Nacional.

[11] Pérez, E.(2005). *Estructuras Algebraicas*. Bogotá: Universidad Pedagógica Nacional.

[12] Pollar, H. (1965). *The theory of algebraic numbers*. New York: Cornell University.

[13] Ravenna, G. (2008). *Estructuras algebraicas*. La Plata: Universidad de la Plata.

[14] Zhang, Y. (2006) *Representing primes as $x^2 + 5y^2$: an inductive proof that Euler missed*. China: National University of Singapore.