UNIVERSIDAD PEDAGOGICA NACIONAL

Educadora de educadores

Quitian González Jhon Ferney

Estudio de analogías con los números enteros que se pueden evidenciar en un subconjunto de los números irreales

Universidad Pedagógica Nacional
Facultad de Ciencia y Tecnología
Departamento de Matemáticas
Bogotá. D.C.
Mayo del 2018

Estudio de analogías con los números enteros que se pueden evidenciar en un subconjunto de los números irreales

Quitian González Jhon Ferney

Cód: 2014140067
C.C: 1012407445

Trabajo de Grado
Asociado al estudio de un tema específico

Director:
Donado Nuñez Gil Alberto de Jesús

Universidad Pedagógica Nacional
Facultad de Ciencia y Tecnología
Departamento de Matemáticas
Bogotá. D.C.
Mayo del 2018

Dedicado a

Edi, pues este camino no lo he recorrido solo...

1. Información General	
Tipo de documento	Trabajo de Grado
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central.
Título del documento	Estudio de analogías con los números enteros que se pueden evidenciar en un subconjunto de los números irreales.
Autor	Quitian González, Jhon Ferney.
Director	Donado Nuñez, Gil Alberto de Jesús.
Publicación	Bogotá. Universidad Pedagógica Nacional. 2018. 108 p.
Unidad Patrocinante	Universidad Pedagógica Nacional
Palabras claves	NÚMEROS IRREALES. NÚMEROS ENTEROS. SUBCONJUNTO. ANILLO CONMUTATIVO CON IDENTIDAD. ANALOGÍAS

2. Descripción

Este trabajo se propuso con la intención de mostrar algunas analogías entre el conjunto de los números enteros y un subconjunto de los números irreales. El conjunto de los números irreales, es el conjunto de todos los elementos de la forma $a+bj$ donde $a, b \in \mathbb{R}$, $j = j^2$ con $j \neq 1$ y $j \neq 0$.

El conjunto que se consideró, para la realización de las analogías, fue conjunto de todos los elementos $a + bj \in \mathbb{J}$ con $a, b \in \mathbb{Z}$. Este conjunto se notó con ε. Las analogías se centraron en la consideración de la estructura algebraica, las ecuaciones y la divisilibidad.

3. Fuentes

- Apostol, T. (1972). *Calculus.* Volumnen I. Segunda edición. Editorial Revertre.
- Caicedo, J. (2004). *Teoría de Grupos.* Departamento de Matemáticas. Universidad Nacional de Colombia. Sede Bogotá.
- Cano, J. (2015). *Números de la forma* $a+bj$*, donde* $a, b \in \mathbb{R}$ *y* $j^2 = j$ *con* $j \neq 0$ *y* $j \neq 1$. Licenciatura en Matemáticas. Universidad Pedagógica Nacional.
- Fraleigh, J. (1987). *Álgebra abstracta.* Addison-Wesley Ibeoramericana.
- Koshy, T. (2007). *Elementary Number Theory with Aplicattions.*
- Luque, J., Mora, L. & Torres, J. (2006). *Estructuras análogas a los números reales.* Universidad Pedagógica Nacional.
- Muñoz, J. (2002). *Introducción a la teoría de conjuntos.* Cuarta edición. Universidad Nacional de Colombia. Facultad de Ciencias.

4. Contenidos

El documento cuenta con cuatro capítulos. En el capítulo 01 se establece como un capítulo de referencia, en el cual se hace nombramiento de los teoremas y definiciones en el conjunto de los números irreales. En el capítulo 02, se define el conjunto ε y se determinan las propiedades algebraicas de este conjunto. En el capítulo 03 se abordan las ecuaciones en ε. En el capítulo 04, se incluyen algunos desarrollos hechos con base en una definición de divisibilidad análoga a la definición de divisibilidad en $\mathbb{Z}$.

5. Metolodogía

Para el desarrollo del presente documento, se contó con la dirección del profesor, de la Licenciatura en Matemáticas, Alberto Donado. Inicialmente se hizo una revisión documental de la teoría de los números irreales, la teoría de números, la teoría de conjuntos y la teoría de anillos, buscando posibes analogías entre los números enteros y ε. Posterior a ello, se dio un trabajo en el cual se consideraron opciones a seguir, para el establecimiento de las analogías. Finalmente, se dio la elaboración y estructuración del documento.

Todo esto se desarrollo en el primer semestre académico del 2018.

6. Conclusiones

- El anillo de los números enteros es un subanillo del anillo de los números reales. Análogamente, se cumple que el anillo ε es un subanillo del anillo $\mathbb{J}$.
- Tanto el anillo de los números enteros, como el anillo ε cuentan con una cantidad finita de unidades. En ε existen cuatro elementos que son invertibles bajo el producto definido. Mientras que en $\mathbb{Z}$, hay dos unidades.
- El conjunto $\mathbb{Z}$ es un dominio de integridad. En contraste, se tiene que ε no es dominio de integridad. Además, en ε existen tantos divisores de $(0, 0)$ como números naturales.
- El conjunto de los números enteros está contenido propiamente en ε.
- Analogamente, al conjunto $\mathbb{J}$, en el conjunto ε no se puede definir un conjunto de números positivos. En contraste, en el conjunto de los números enteros se define al conjunto de los números positivos.
- Mientras que en $\mathbb{Z}$ las ecuaciones de la forma $ax = b$ tienen a lo sumo una solución, se cumple que en ε, las ecuaciones de la forma $ax = b$, puede que no tengan solución, que tengan única solución o que tengan infinitas soluciones.
- Las ecuaciones cuadráticas en $\mathbb{Z}$ tienen a los sumo dos soluciones. En contraste, las ecuaciones cuadráticas consideradas en ε, pueden no tener solución, tener cuatro (contando multiplicidades) o tener infinitas soluciones.
- En ε la ecuación $ax^n = b$, con $n \in \mathbb{Z}^+$, a lo sumo tiene una solución si n es impar. Si n es par, la ecuación tiene a lo sumo cuatro soluciones (contando multiplicidades).
- Si una ecuación no tiene solución en $\mathbb{Z}$, esta ecuación seguirá sin tener solución considerándola en ε.
- La relación de divisibilidad definida en $\mathbb{Z}$ y en ε son reflexivas y transitivas, pero no son simétricas ni antisimétricas.
- En ε no se cumple un teorema análogo al teorema del algoritmo de la división de $\mathbb{Z}$.
- Los números primos en $\mathbb{Z}$ tienen cuatro divisores (considerando asociados) en ε.
- En ε no se cumple un teorema análogo al teorema fundamental de la Aritmética.

Elaborado por:	Quitian González Jhon Ferney.
Revisado por:	Donado Nuñez Gil Alberto de Jesús.

Fecha de elaboración del resumen	27	04	2018

Índice general

Índice de figuras

Introducción

Considerando al conjunto de los números reales, se tiene que no existe elemento que satisfaga que su cuadrado sea menor a cero. Con base en ello, se da paso a la construcción del conjunto de los números complejos [7, p. 204]. De forma análoga, bajo la consideración que los únicos números reales que son iguales a sus cuadrados son el 0 y el 1, en el año 2015, Cano presenta un documento en el cual se considera un elemento j, tal que $j^2 = j$, $j \neq 0$ y $j \neq 1$, definiendo al conjunto de los números irreales, notado con $\mathbb{J}$ como los elementos $a + bj$ con $a, b \in \mathbb{R}$.

El trabajo de Cano, se desarrolló principalmente en el estudio de la estructura algebraica, ordenada y topológica del conjunto de números irreales. Los resultados, en el estudio del conjunto de los números irreales fueron, en su mayoría, análogos a los resultados del desarrollo teórico que se hace en los números reales, los números complejos y el conjunto $\mathbb{R}^2$. Por lo cual, en el presente documento se considera un subconjunto de los números irreales, el cual notaremos con ε, de tal forma que en este subconjunto se estudien algunos temas análogos a los que se estudian en $\mathbb{Z}$. El conjunto ε es el conjunto de todos los elementos $a + bj \in \mathbb{J}$ tal que $a, b \in \mathbb{Z}$.

En el capítulo 1, se fija un punto de partida, tomando como referente lo realizado por Cano (ver [3]). En este capítulo se hace mención de todas las definiciones y proposiciones, que se han de considerar en el estudio de las analogías entre ε y $\mathbb{Z}$. Se debe mencionar que solo se tuvieron en cuenta algunos capítulos del documento referido, pues hay capítulos que se alejan del fin de este texto. Además, solo se enuncian las proposiciones, sin dar demostración alguna, aunque en algunas proposiciones se hace una breve mención sobre su demostración, pues han de surgir teoremas en el

estudio de analogías entre ε y $\mathbb{Z}$ que han de seguir los mismos razonamientos.

En el capítulo 2, se hace un estudio de las caracteristicas algebraicas de ε, centrándose en dos aspectos. El primero, las propiedades que se han heredado del conjunto de los números irreales. Y el segundo, las comparaciones que se pueden evidenciar con $\mathbb{Z}$. Se ha de comprobar que la estructura algebraica del subconjunto de los números irreales es un anillo conmutativo con identidad, evidenciando que ε no es un dominio de integridad, tiene infinitos divisores de $(0, 0)$ y tiene cuatro elementos invertibles bajo el producto definido.

En el capítulo 3, se hace un estudio de las ecuaciones en ε, definiendo allí las potencias naturales de los elementos de ε. Se demuestra que existen ecuaciones de la forma $ax = b$, que no tienen solución, otras que cuentan con solución única y otras con infinitas soluciones. Así mismo, se muestra que existen ecuaciones de la forma $ax^2 = b$ en ε que no tienen solución, que tienen cuatro soluciones, contando multiplicidades, o que tienen infinitas solucioness. Además, se abordan las ecuaciones de la forma $ax^n = b$ caracterizando el conjunto de soluciones con base en si n es un número par o impar.

En el capítulo 4, se aborda la relación de divisibilidad, un teorema análogo al algoritmo de la división en $\mathbb{Z}$ y una propuesta para definir números primos en ε, conllevando esto a considerar un teorema análogo al teorema fundamental de la Aritmética, evidenciándose que este no se cumple.

Sobre el final del documento, se incluyen las conclusiones de lo desarrollado. Así como la lista de todas las las referencias bibliográficas que se usaron.

Objetivos

Objetivo General

Realizar un estudio de posibles analogías que se evidencien entre un subconjunto de los números irreales y el conjunto de los números enteros.

Objetivos específicos

- Hacer uso de algunos los conceptos, axiomas y teoremas de la teoría de números y teoría de anillos, que permitan evidenciar analogías entre $\mathbb{Z}$ y ε.
- Realizar conjeturas y, de ser posible, demostrarlas o refutarlas.
- Caracterizar al conjunto ε de acuerdo a su estructura algebraica.
- Abordar algunas ecuaciones en ε, dar condiciones para que las soluciones existan y determinar el conjunto de soluciones para dichas ecuaciones.
- Hacer un estudio en el conjunto ε análogo al que se da en $\mathbb{Z}$ en cuanto a la divisibilidad.

Capítulo 1

Los números irreales

Los números complejos son consecuencia de considerar un número, tal que al multiplicarlo por si mismo, el resultado fuese un número negativo. A partir de esta situación se propone un elemento i tal que $i^2 = -1$. Claramente $i \notin \mathbb{R}$. Pero esta idea permite un desarrollo teórico en el cual se evidencia que los números complejos son una extensión de los números reales, pues existe un conjunto $A \subset \mathbb{C}$, tal que $\mathbb{R}$ es isomorfo con A. Otros ejemplos de extensiones de los números reales, son los números duales, los números dobles [6, pp. 109, 129] y los números irreales [3] .

A mediados del año 2015 Julian Cano, partiendo de la premisa que los únicos números reales que son iguales a sus cuadrados son el 1 y el 0, considera un número j (diferente de 0 y 1), tal que este fuese igual a su cuadrado; es decir $j^2 = j$. Claramente, este número j no pertenece al conjunto de los números reales. Con base en ello, define el conjunto de los números irreales, denotado como $\mathbb{J}$.

Definición 1.0.1 *El conjunto $\mathbb{J}$ estará dado por:*

$$\mathbb{J} = \left\{ a + bj : a, b \in \mathbb{R}, j^2 = j, j \neq 0, j \neq 1 \right\}$$

Para facilitar la notación, define al número irreal $a + bj$ como la dupla (a, b) [3, pág. 1]. Por ende define la unidad irreal j como el número irreal $j = (0, 1)$. Como consecuencia de lo anterior, se define que dos elementos $(a, b), (c, d) \in \mathbb{J}$ son iguales si y solo si $a = c$ y $b = d$.

Puesto que los elementos de $\mathbb{J}$ se consideran como parejas ordenadas de números reales, se establece una correspondencia biunívoca entre $\mathbb{J}$ y $\mathbb{R}^2$ [3, p.14]. De esto se tiene que a cada elemento en $\mathbb{J}$ le corresponde un único punto en el plano cartesiano y, del mismo modo, a todo punto en el plano cartesiano le corresponde un único elemento en $\mathbb{J}$. Sea $w = a + bj \in \mathbb{J}$, a este le corresponde una única pareja ordenada $(a, b) \in \mathbb{R}^2$. A la primera componente de (a, b) se le denominará parte real y a la segunda componente, parte irreal. Por lo cual, al eje x del plano cartesiano, le llamará *eje real* y el eje y será el *eje irreal*. Una representación de esto, se evidecia en la Figura 1.1.

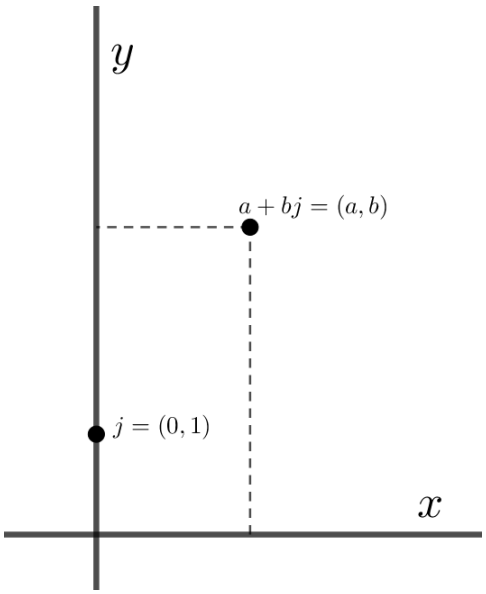

Figura 1.1: Representación de los elementos $(0, 1), (a, b) \in \mathbb{R}^2$ en el plano irreal.

1.1. Estructura algebraica del conjunto de los números irreales

A los números irreales se les dota de dos operaciones binarias: la *suma* ($\oplus$) y el *producto* ($\odot$), partiendo del uso de la suma ($+$) y el producto ($\cdot$) usuales definidos sobre el conjunto de los números reales.

Definición 1.1.1 *Para todo* $(a,b),(c,d) \in \mathbb{J}$ *se define la operación binaria* $\oplus$ *como sigue:*

$$\oplus : \mathbb{J} \times \mathbb{J} \to \mathbb{J}$$

$$((a,b),(c,d)) \mapsto (a,b) \oplus (c,d) = (a+c, b+d)$$

Definición 1.1.2 *Para todo* $(a,b),(c,d) \in \mathbb{J}$ *se define la operación binaria* $\odot$*:*

$$\odot : \mathbb{J} \times \mathbb{J} \to \mathbb{J}$$

$$((a,b),(c,d)) \mapsto (a,b) \odot (c,d) = (a \cdot c, a \cdot d + b \cdot c + b \cdot d)$$

Nota: A partir de esta linea se obviará el símbolo del producto usual de números reales. Para el producto de los números a y b, se notará como ab.

Con base en las dos operaciones, se demuestra [3, p 4] que estas están bien definidas. También, se demuestra que estas cumplen las siguientes propiedades:

- La suma de números irreales es asociativa y conmutativa.
- La suma de números irreales tiene elemento neutro, siendo este (0,0).
- En la suma de números irreales, se verifica la existencia de inversos. Para todo $w = (a,b) \in \mathbb{J}$ existe $-w = (-a,-b) \in \mathbb{J}$ tal que $w \oplus (-w) = (0,0)$.
- $(\mathbb{J}, \oplus)$ tiene estructura algebraica de grupo conmutativo.
- El producto de números irreales es asociativo y conmutativo.
- El producto de números irreales tiene elemento neutro, siendo este (1,0).
- Considerando $\mathbb{J}^* = \mathbb{J} - \{(0,0)\}$, se cumple que el producto en el conjunto $\mathbb{J}^*$ no todos sus elementos tienen inverso. Sea $w = (a,b) \in \mathbb{J}$ si $a \neq 0$ y $a+b \neq 0$, existe $w^{-1} \in \mathbb{J}$ donde $w^{-1} = \left(\frac{1}{a}, -\frac{b}{a(a+b)}\right)$ tal que $w^{-1} \odot w = w \odot w^{-1} = (1,0)$. De esto, se tiene que los elementos $(c,d) \in \mathbb{J}^*$ que no son invertibles bajo $\odot$, son aquellos que cumplen que $c = 0$ o $c = -d$.

- El producto de números irreales distribuye respecto a la suma de números irreales.
- $(\mathbb{J}, \odot)$ tiene estructura algebraica de semigrupo conmutativo con identidad.

Todo lo anterior se sintetiza en el siguiente teorema.

Teorema 1.1.1 *$(\mathbb{J}, \oplus, \odot)$ tiene estructura de anillo conmutativo con identidad.*

Teorema 1.1.2 *Existe un conjunto $H \subset \mathbb{J}$, tal que $(H, \oplus, \odot)$ es isomorfo con $(\mathbb{R}, +, \cdot)$.*

Para demostrar la existencia de un conjunto $H \subset \mathbb{J}$ isomorfo a $\mathbb{R}$, se define el conjunto H como el conjunto de todos los elementos en $\mathbb{J}$ cuya segunda componente fuese igual a cero (0); es decir, H está dado por:

$$H = \{w \in \mathbb{J} : w = (x, 0)\}$$

Con base en la definición de H, se define la función f, como sigue:

$$f : \mathbb{R} \to H$$

$$f(x) = (x, 0)$$

Seguido de ello, se demuestra que f es biyectiva y que $f(w + z) = f(w) \oplus f(z)$ y que $f(w \cdot z) = f(w) \odot f(z)$ para todo $w, z \in \mathbb{R}$. Demostrando así la existencia de un subconjunto de $\mathbb{J}$ que tiene el mismo comportamiento de $\mathbb{R}$.

Definición 1.1.3 *Sea $(a, b) \in \mathbb{J}$ y $\lambda \in \mathbb{R}$, se define el producto por escalar en $\mathbb{J}$ como:*

$$\cdot : \mathbb{R} \times \mathbb{J} \to \mathbb{J}$$
$$\cdot(\lambda, (a, b)) = \lambda \cdot (a, b) = (\lambda, 0) \odot (a, b) = (\lambda a, \lambda b)$$

Teorema 1.1.3 *La estructura $(\mathbb{J}, \oplus, \odot)$ es un espacio vectorial real.*

Teorema 1.1.4 *Los espacios vectoriales reales $\mathbb{J}$ y $\mathbb{R}^2$ son isomorfos* [3, p. 17].

Teorema 1.1.5 *El espacio vectorial real $\mathbb{J}$ es de dimensión 2.*

Teorema 1.1.6 *El conjunto $\mathfrak{B} = \{(1,0), j\}$ es una base para el espacio vectorial real $\mathbb{J}$.*

Teorema 1.1.7 *El conjunto de los unidades*[I] *de $\mathbb{J}$, notada como $\mathfrak{U}(\mathbb{J})$ estará dada por:*

$$\mathfrak{U}(\mathbb{J}) = \{(a,b) \in \mathbb{J} : a \neq 0 \wedge a + b \neq 0\}$$

Teorema 1.1.8 *El conjunto $\mathfrak{U}(\mathbb{J})$, bajo la múltiplicación $\odot$ definida en $\mathbb{J}$ es un grupo conmutativo.*

Teorema 1.1.9 *El conjunto $\mathfrak{D}(\mathbb{J})$ de los elementos divisores de (0,0)*[II] *en $\mathbb{J}$ está dado por:*

$$\mathfrak{D}(\mathbb{J}) = \{(a,b) \in \mathbb{J} - \{(0,0)\} : a = 0 \vee a + b = 0\}$$

Corolario 1.1.1 *La estructura $(\mathbb{J}, \oplus, \odot)$ no es dominio de integridad*[III].

1.2. Orden en $\mathbb{J}$

Con la caracterización algebraica del conjunto $\mathbb{J}$, se prosigue a definir una relación de orden que sea compatible con las operaciones de suma y producto definidas en dicho conjunto. Como primera opción se considera el orden lexicográfico.

Definición 1.2.1 *Sean $w, z \in \mathbb{J}$ con $w = (a,b)$ y $z = (c,d)$, se dice que*

$$w \preceq z \text{ si y solo si } (a < c) \vee (a = c \wedge b \leq d)$$

Teorema 1.2.1 *La relación $\preceq$ es una relación de orden total en $\mathbb{J}$.*

[I] Entiéndase unidades como los elementos u en un anillo R que tienen su inverso bajo la multiplicación definida en R [4, p. 212]

[II] En un anillo R, se define los divisores del elemento 0 (neutro bajo la suma definida en R) a los elementos $a, b \in R$, ambos diferentes de 0, tal que $ab = 0$ [4, p. 216].

[III] Un anillo conmutativo con identidad R, es dominio de integridad, si no contiene divisores de 0.

El anterior teorema implica que $\preceq$ es una relación que es reflexiva antisimétrica y transitiva. Además de ello, se tiene que para cualquier par de elementos en $\mathbb{J}$, estos son comparables bajo la relación $\preceq$, es decir, para todo $w, z \in \mathbb{J}$ se cumple que $w \preceq z$ o $z \preceq w$.

Además de lo anterior, se demuestra que $\preceq$ es compatible con la suma ($\oplus$) definida en $\mathbb{J}$, es decir, que para todo $w, z, t \in \mathbb{J}$, si $w \preceq z$ entonces $w + t \preceq z + t$. Pero esto no se cumple para el producto; es decir, $\odot$ y $\preceq$ no son compatibles. En general, el siguiente teorema, demuestra que no se puede determinar una relación de orden en $\mathbb{J}$ que sea compatible con las operaciones definidas.

Teorema 1.2.2 *En el conjunto $\mathbb{J}$ no existe un conjunto de números positivos*[IV].

La demostración, es análoga a como se demuestra la no existencia de un conjunto de números positivos en los complejos: por reducción al absurdo, considerando el elemento que permitió determinar el conjunto (para el caso de $\mathbb{C}$ el elemento $i = \sqrt{-1}$ y, para $\mathbb{J}$ el elemento j).

En $\mathbb{J}$, sea P el conjunto de los números positivos. Por definción 1.1.1 se tiene que $(0, -1) = -j \neq (0, 0)$, por ende, $j \in P$ o, exclusivamente, $-j \in P$. Supóngase que $-j$ pertenece P, luego $(-j)^2 = (0, 1) = j \in P$. Pero no puede ocurrir que $-j, j \in P$, por lo tanto $-j \notin P$. Lo cual conlleva a considerar que $j \in P$. Sea $(m, -m) \in \mathbb{J}$ con $(m, -m) \neq (0, 0)$. Luego se ha de cumplir, solo uno de los siguientes casos:

- $(m, -m) \in P$. Luego $(m, -m) \odot (0, 1) \in \mathbb{J}$, pero $(m, -m) \odot (0, 1) = (0, 0)$, Pero, por definición $(0, 0) \notin P$. Luego $(m, -m) \notin P$
- $-(m, -m) = (-m, m) \in P$. De forma análoga se tiene que $(-m, m) \odot (0, 1) = (0, 0)$. Luego $-(m, -m) \notin P$.

[IV] En un conjunto M, con dos operaciones, $+$ y $\cdot$ se denomina al conjunto de los números positivos [1, p. 24] al conjunto $M' \subset M$, tal que se cumple que:

- Si $a, b \in M'$ entonces $a + b, a \cdot b \in M'$.
- Sea e el módulo bajo la suma definida. Para todo $b \in M$, con $b \neq e$ se cumple que $b \in M'$ o exclusivamente $-b \in M'$.
- $e \notin M'$.

Como $(m,-m) \neq (0,0)$, $(m,-m) \notin P$ y $-(m,-m) \notin P$, se concluye que no se puede definir un conjunto de números postivos en $\mathbb{J}$.

A pesar del hecho de no poderse definir un orden total en el conjunto $\mathbb{J}$, compatible con $\oplus$ y $\odot$, sí es posible definir un orden parcial en $\mathbb{J}$ y no solo un orden , sino que son dos los que se definen [3, p. 55, 65]. Pero esto, solo se menciona pues no se ha de tener en cuenta para el desarrollo que se hará.

1.3. Conjugado y norma en los números irreales

La finalidad de definir el conjugado en $\mathbb{J}$, radica en buscar una seminorma (como en el caso de los números duales) o una norma como en el caso de los números complejos, para posteriormente dar paso a un estudio de la estructura topológica [3, p. 74]. Por ello, la definición de conjugado surge de la exploración que tuvo en cuenta que se cumpliera las propiedades que se enuncian en el teorema siguente a la definición.

Definición 1.3.1 *Sea $(a,b) \in \mathbb{J}$, se define el conjugado de (a,b), notado como $\overline{(a,b)}$, como:*

$$^{-} : \mathbb{J} \to \mathbb{J}$$

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

Teorema 1.3.1 *Para todo $(a,b),(c,d) \in \mathbb{J}$ y para todo $\alpha \in \mathbb{R}$, se cumple que:*

- $(a,b) \odot \overline{(a,b)} \in \mathbb{R}$.
- $(a,b) = \overline{(a,b)}$ *si y solo si* $(a,b) \in \mathbb{R}$[v].
- $\overline{\overline{(a,b)}} = (a,b)$.
- $\overline{\alpha(a,b)} = \alpha\overline{(a,b)}$.
- $\overline{(a,b) \oplus (c,d)} = \overline{(a,b)} \oplus \overline{(c,d)}$.

[v] En otras palabras, esto es que $b = 0$.

- $\overline{(a,b) \odot (c,d)} = \overline{(a,b)} \odot \overline{(c,d)}$.

Corolario 1.3.1 *La función* $^{-}$ *es una función involutiva*[VI].

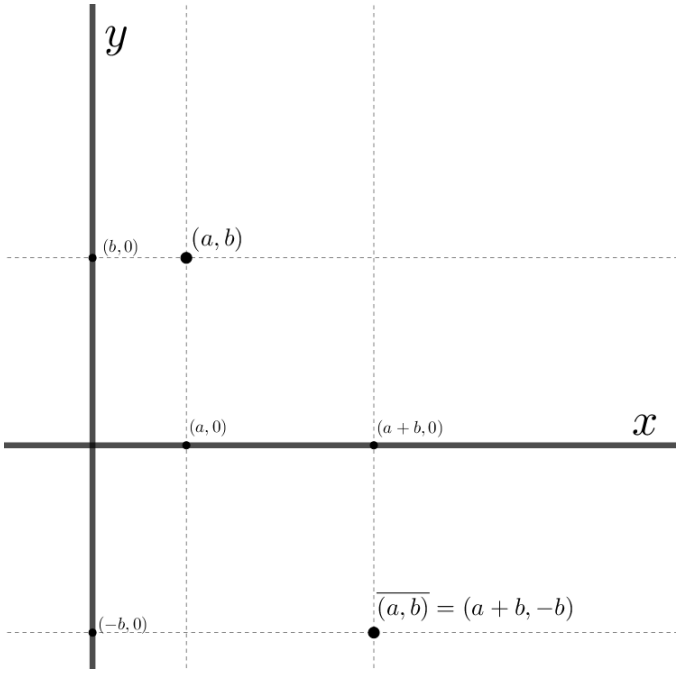

Figura 1.2: El elemento $(a,b) \in \varepsilon$ y su conjugado $\overline{(a,b)} = (a+b,-b)$, en el plano irreal.

Precisando que $(a,b) \odot \overline{(a,b)} = (a(a+b),0)$, se tiene que se cumple $a(a+b) = 0$ sin la necesidad que $(a,b) = (0,0)$. Por lo cual, de poderse, no se define una norma, sino una seminorma. Además, no siempre se cumple que $a(a+b)$ sea mayor o igual a cero. Por lo tanto, se hace una flexibilización en la posible definición de seminorma, con base en el conjugado. Siendo:

$$\big(\mathcal{N}(a,b)\big)^2 = |(a,b) \odot (\overline{a,b})| = |a(a+b)|$$

$$\mathcal{N}(a,b) = \sqrt{|a(a+b)|}$$

Donde $|a(a+b)|$ alude al valor absoluto de $a(a+b)$. Pero a pesar de esta primera definición, se tiene que esta no es una seminorma, especificamente porque no cumple la desigualdad triangular. Un ejemplo que confirma que no se cumple la desigualdad

[VI]Sea $f : A \to A$ es una función involutiva si y solo si $f(f(x)) = x$, para todo $x \in A$. Como consecuencia, se tiene que toda función involutiva es biyectiva.

triangular es:

$$\begin{aligned}\mathcal{N}\big((0,1)\oplus(1,-1)\big) &= \mathcal{N}(1,0)\\ &= 1\\ &> 0\\ &= 0+0\\ &= \mathcal{N}(0,1)+\mathcal{N}(1,-1)\end{aligned}$$

Con lo cual se tiene que $\mathcal{N}\big((0,1)\oplus(1,-1)\big) \nleq \mathcal{N}(0,1)+\mathcal{N}(1,-1)$. Conllevando a que, en general, no se cumple la desigualdad triangular. Por tanto, se concluye que no se puede definir una norma, inducida por el conjugado. Consecuencia de ello, no hay lugar para hablar de distancias en $\mathbb{J}$, partiendo de la definición de conjugado.

Hasta el momento, lo que se ha nombrado es parte del trabajo hecho por Cano (ver [3]). A pesar que su trabajo se extiende hacia otras aspectos de las Matemáticas, estos no se han de nombrar en el presente documento, pues se aleja del interés de lo que se ha de desarrollar.

Capítulo 2

Un subconjunto de los números irreales: ε

En el conjunto de los números irreales $\mathbb{J}$ se pueden evidenciar algunas analogías con $\mathbb{R}$, $\mathbb{R}^2$ y $\mathbb{C}$. Pero, ¿habrá un conjunto en $\mathbb{J}$ de tal forma que en él se evidencien analogías con el conjunto de los números enteros? Dado que el conjunto de números irreales, se puede escribir como el conjunto de duplas con componentes reales, así pues, se considerará el conjunto de todos los elementos de $\mathbb{J}$ tal que sus componentes pertenezcan a $\mathbb{Z}$. A este conjunto se le llamará ε y en él se hará un estudio de análogías con el conjunto de los números enteros.

Definición 2.0.1 *El conjunto ε estará dado por:*

$$\varepsilon = \left\{ a + bj : a, b \in \mathbb{Z}, j^2 = j, j \neq 0, j \neq 1 \right\}$$

Teorema 2.0.1 *El conjunto ε es un subconjunto propio de $\mathbb{J}$.*

Demostración: Debido a que $\mathbb{Z} \subset \mathbb{R}$ y por la definición 2.0.1, se evidencia que todo elemento en ε pertenece a $\mathbb{J}$, luego $\varepsilon \subseteq \mathbb{J}$. Dado que $(\pi, e) \in \mathbb{J}$, pero $(\pi, e) \notin \varepsilon$, se concluye que necesariamente ε es un subconjunto propio de $\mathbb{J}$.

Comparación i de ε con $\mathbb{Z}$: Así como $\mathbb{Z} \subset \mathbb{R}$, se cumple que $\varepsilon \subset \mathbb{J}$.

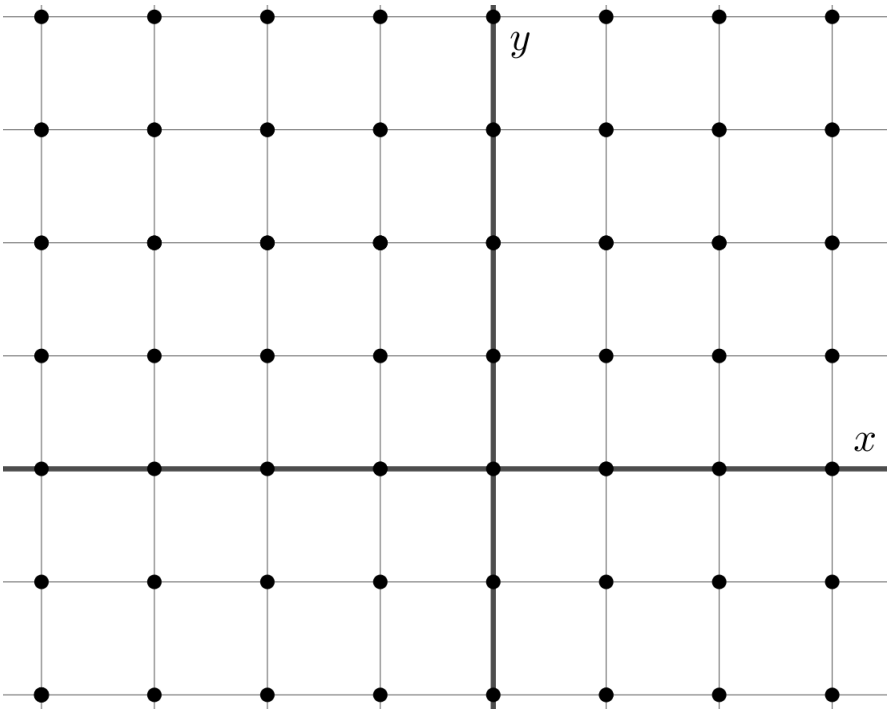

Figura 2.1: Representación de los elementos $(a, b) \in \varepsilon$ en el plano irreal.

2.1. Operaciones inducidas por $\mathbb{J}$ en ε

En el teorema 2.0.1, se demostró que ε es un subconjunto de $\mathbb{J}$. Con las operaciones de $\oplus$ y $\odot$ definidas en $\mathbb{J}$, siendo heredadas a ε, lo que sigue es demostrar que estas operaciones están bien definidas en ε.

Teorema 2.1.1 *La operación $\oplus$ inducida de $\mathbb{J}$ en ε, es una operación bien definida.*

$$\oplus : \varepsilon \times \varepsilon \to \varepsilon$$

$$((a, b), (c, d)) \mapsto ((a, b) \oplus (c, d) = (a + c, b + d))$$

Demostración: Como $a, b, c, d \in \mathbb{Z}$ se tiene que $a+c, b+d \in \mathbb{Z}$, luego $(a+c, b+d) \in \varepsilon$.

Teorema 2.1.2 *La operación $\odot$ inducida de $\mathbb{J}$ en ε, es una operación bien definida.*

$$\oplus : \varepsilon \times \varepsilon \to \varepsilon$$

$$((a, b), (c, d)) \mapsto ((a, b) \odot (c, d) = (ac, ad + bc + bd))$$

DEMOSTRACIÓN: Análogamente al teorema 2.1.1 se tiene que $ac, ad + bc + bd \in \mathbb{Z}$, luego $(ac, ad + bc + bd) \in \varepsilon$.

Nota: Análogamente a $\mathbb{Z}$, se considera en ε que para todo $(a, b), (c, d), (e, f) \in \varepsilon$ la operación $(a, b) \odot (c, d) \oplus (e, f)$ alude a considerar primero $\odot$ y luego $\oplus$; es decir, $(a, b) \odot (c, d) \oplus (e, f) = \big((a, b) \odot (c, d)\big) \oplus (e, f)$.

2.1.1. Estructura algebraica de $(\varepsilon, \oplus, \odot)$

Hasta el momento, se ha demostrado que las operaciones inducidas por $\mathbb{J}$ en ε están bien definidas. Pero ¿qué estructura algebraica tiene la terna $(\varepsilon, \oplus, \odot)$? ¿En qué diferirá de ε? Esto se responderá a continuación.

Teorema 2.1.3 *La estructura $(\varepsilon, \oplus)$ es grupo conmutativo.*

DEMOSTRACIÓN:

- Por teorema 2.0.1, se tiene que $\varepsilon \subset \mathbb{J}$. Por teorema 1.1.1 se cumple que $(\mathbb{J}, \oplus)$ es grupo conmutativo por tanto $(\varepsilon, \oplus)$ hereda la **asociatividad** y **conmutatividad** de $(\mathbb{J}, \oplus)$.

- Dado que (0,0) es neutro en $(\mathbb{J}, \oplus)$ y como $(0, 0) \in \varepsilon$, se tiene que para todo $(a, b) \in \varepsilon$ se cumple que $(a, b) \oplus (0, 0) = (0, 0) \oplus (a, b) = (a, b)$. Por lo tanto $(\varepsilon, \oplus)$ tiene **elemento neutro**, siendo este (0,0).

- Sea $w = (a, b) \in \varepsilon$. Por definición $a, b \in \mathbb{Z}$, luego $-a, -b \in \mathbb{Z}$, por ende $(-a, -b) \in \varepsilon$. Como:

$$\begin{array}{rcll} (a, b) \oplus (-a, -b) & = & (a + (-a), b + (-b)) & \text{Definición de } \oplus \\ & = & (0,0) & \text{Existencia de inversos aditivos en } \mathbb{Z} \end{array}$$

  y dado que $(\varepsilon, \odot)$ es conmutativo, se cumple $(-a, -b) \oplus (a, b) = (0, 0)$. Concluyendo así que $(\varepsilon, \odot)$ goza de la existencia de inversos, teniendo que para todo $w = (a, b) \in \varepsilon$ su inveso es $-w = (-a, -b)$.

Con lo cual se concluye que $(\varepsilon, \oplus)$ es un grupo conmutativo. Con base en que $(\varepsilon, \oplus)$ es un grupo conmutativo, se infiere que también se cumple [2, p. 7]:

- El elemento neutro en $(\varepsilon, \oplus)$ es único.
- Todo elemento en ε tiene un único opuesto bajo la operación $\oplus$.
- Para todo $(a, b) \in \varepsilon$ se cumple que $-(-(a, b)) = (a, b)$.
- Para todos los $(a, b), (c, d), (e, f) \in \varepsilon$, si $(a, b) \oplus (c, d) = (a, b) \oplus (e, f)$ entonces $(c, d) = (e, f)$, esta propiedad se le denomina ley de cancelación a izquierda. Dado que $(\varepsilon, \oplus)$ es conmutativo, también se cumple la ley de cancelación de derecha.

Comparación ii de ε con $\mathbb{Z}$: Así como $(\mathbb{Z}, +)$ es un grupo conmutativo, se cumple que $(\varepsilon, \oplus)$ también lo es.

Teorema 2.1.4 *La estructura $(\varepsilon, \odot)$ es semigrupo conmutativo con unidad.*

Demostración:

1. Por teorema 2.0.1, se tiene que $\varepsilon \subset \mathbb{J}$. Por teorema 1.1.1 se cumple que $(\mathbb{J}, \odot)$ es semigrupo conmutativo con identidad, por tanto $(\varepsilon, \odot)$ hereda la **asociatividad** y **conmutatividad** de $(\mathbb{J}, \odot)$.
2. Dado que (1,0) es neutro en $(\mathbb{J}, \odot)$ y como $(1, 0) \in \varepsilon$, se tiene que para todo $(a, b) \in \varepsilon$ se cumple que $(a, b) \odot (1, 0) = (1, 0) \odot (a, b) = (a, b)$. Por lo tanto $(\varepsilon, \odot)$ tiene **elemento neutro**, siendo este (1,0).

Con lo cual se demuestra que $(\varepsilon, \odot)$ es un semigrupo conmutativo con identidad.

Sea $\varepsilon^* = \varepsilon - \{(0, 0)\}$, se debe notar que en general ε^* no goza de inversos bajo $\odot$. Para ilustrar esto, considérese el elemento $(2, 0) \in \varepsilon$. Si este tuviese inverso, esto significaría que existe $(a, b) \in \varepsilon$ tal que $(2, 0) \odot (a, b) = (1, 0)$[I]. Lo que conlleva a que $(2a, 2b) = (1, 0)$. Pero esto es falso, pues no existe $a \in \mathbb{Z}$ tal que $2a = 1$. Lo cual permite concluir que $(\varepsilon^*, \odot)$ no todos los elementos poseen inverso.

[I]Se omite la otra igualdad, basado en que $(\varepsilon, \odot)$ es conmutativo.

Comparación iii de ε con $\mathbb{Z}$: Así como $(\mathbb{Z}, \cdot)$ es un semigrupo conmutativo con identidad, se cumple que en $(\varepsilon, \odot)$ también lo es.

Teorema 2.1.5 *En ε, se cumple que $\odot$ distribuye respecto a $\oplus$.*

Demostración: Consecuencia directa de los teoremas 1.1.1 y 2.0.1, pues al cumplirse que $\varepsilon \subset \mathbb{J}$, se hereda la distributiva de $\odot$ respecto a $\oplus$.

Teorema 2.1.6 *$(\varepsilon, \oplus, \odot)$ es un anillo conmutativo con identidad.*

Demostración: Es inmediata. Esto debido a los teoremas 2.1.3, 2.1.4 y 2.1.5.

Corolario 2.1.1 *$(\varepsilon, \oplus, \odot)$ es un subanillo*[II] *del anillo $(\mathbb{J}, \oplus, \odot)$.*

Demostración: Como consecuencia del último teorema y de los teoremas 2.0.1 y 1.1.1 se tiene que $(\varepsilon, \oplus, \odot)$ es un subanillo del anillo $(\mathbb{J}, \oplus, \odot)$.

Comparación iv de ε con $\mathbb{Z}$: Así como en $\mathbb{Z}$ se cumple que $\cdot$ distribuye respecto a $+$, también se tiene que en ε se cumple que $\odot$ distribuye respecto a $\oplus$. Además, se cumple que $(\varepsilon, \oplus, \odot)$ y $(\mathbb{Z}, +, \cdot)$ tienen la misma estructura algebraica: anillo conmutativo con identidad. También se cumple que así como $(\mathbb{Z}, +, \cdot)$ es subanillo del anillo $(\mathbb{R}, +, \cdot)$, se cumple que $(\varepsilon, \oplus, \odot)$ es subanillo del anillo $(\mathbb{J}, \oplus, \odot)$.

Teorema 2.1.7 *Existe un conjunto $A \subset \varepsilon$ tal que $(A, \oplus, \odot)$ es isomorfo con $(\mathbb{Z}, +, \cdot)$.*

Demostración: Con base en el teorema 1.1.2, análogamente se define al conjunto A como el conjunto de todos los elementos en ε que cumplen que su segunda componente sea igual a cero; es decir

$$A = \{w \in \varepsilon : w = (x, 0)\}$$

[II] Un subanillo de un anillo $(R, +, \cdot)$, es un conjunto H que satisface:

- $H \subseteq R$.
- H es un anillo bajo las operaciones inducidas por R; es decir, $(H, +, \cdot)$ es un anillo.

Se define f, como sigue

$$f : \mathbb{Z} \to A$$

$$f(x) = (x, 0)$$

Ahora, la demostración se hará en cuatro partes, que son las que se muestran a continuación.

- Sean $x, y \in \mathbb{Z}$ tal que $f(x) = f(y)$. Se tiene que $(x, 0) = (y, 0)$ Con base en la definición 1.0.1, se tiene que $x = y$. Mostrando así que f es **inyectiva**.

- Sea $(x, 0) \in A$. Como $A \subset \varepsilon$ se tiene que $x \in \mathbb{Z}$. Si se considera $f(x)$ se tiene por definición que es igual a $(x, 0)$. Con lo cual se demuestra que f es **sobreyectiva**.

- Sean $x, y \in \mathbb{Z}$. Se tiene que:

$$\begin{aligned} f(x + y) &= (x + y, 0) \\ &= (x, 0) \oplus (y, 0) \\ &= f(x) \oplus f(y) \end{aligned}$$

- Sean $x, y \in \mathbb{Z}$. Se tiene que:

$$\begin{aligned} f(x \cdot y) &= (x \cdot y, 0) \\ &= (x, 0) \odot (y, 0) \\ &= f(x) \odot f(y) \end{aligned}$$

Por lo cual se concluye que f es un isomorfismo de $(\mathbb{Z}, +, \cdot)$ en $(A, \oplus, \odot)$. Lo anterior nos lleva a concluir que existe un conjunto $A \subset \varepsilon$ que se comporta igual que $\mathbb{Z}$. En adelante, abusando un poco del lenguaje, diremos que $\mathbb{Z} \subset \varepsilon$, pero como tal, implicitamente aludiremos a que estamos hablando del conjunto A (ver Figura 2.2).

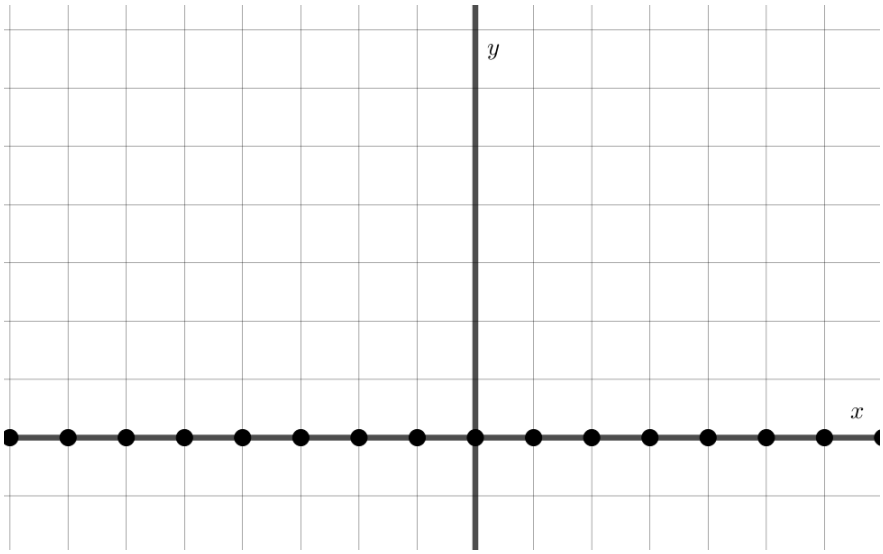

Figura 2.2: Representación en el plano irreal de algunos elementos de $\mathbb{Z}$

Comparación v de ε con $\mathbb{Z}$: Así como $\mathbb{R} \subset \mathbb{J}$, también se cumple que $\mathbb{Z} \subset \varepsilon$. Se debe precisar que al decir que $\mathbb{R} \subset \mathbb{J}$, también se está aludiendo a que existe un subconjunto en $\mathbb{J}$ que es isomorfo a $\mathbb{R}$.

Considérese la cadena de contenencias $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Con los conjuntos $\mathbb{Z}, \mathbb{R}, \mathbb{J}$ y ε, no se puede considerar, de forma similar, una cadena de contenencias, esto debido a que $\mathbb{R} \nsubseteq \varepsilon$ y $\varepsilon \nsubseteq \mathbb{R}$. Dado que $j \in \varepsilon$, y que este es el elemento que satisface que es igual a su cuadrado, pero además es diferente de 0 y de 1, se evidencia que $j \notin \mathbb{R}$. Por otro lado, $\pi \in \mathbb{R}$, pero $\pi \notin \varepsilon$.

2.1.2. Unidades de ε

Como se mencionó previamente, $(\varepsilon, \odot)$ no goza de inversos para todos sus elementos. Por lo tanto surge la pregunta: ¿Cuáles son los elementos invertibles en ε, bajo el producto definido.

Se plantea la situación: Sean $(a, b), (c, d) \in \varepsilon$ tal que:

$$\begin{aligned} (a.b) \odot (c, d) &= (1,0) \\ (ab, ad + bc + bd) &= (1,0) \end{aligned}$$

De la definición 1.0.1 se tiene que $(ab, ad + bc + bd) = (1, 0)$ si y solo si $ab = 1$ y $ad + bc + bd = 0$. Si $ab = 1$ se consideran dos casos:

$$(a = 1 \wedge c = 1) \vee (a = -1 \wedge c = -1)$$

- **Caso 01:** $a = 1$ y $c = 1$. del cual se tiene que:

$$\begin{aligned} ad + bc + bd &= 0 \\ d + b + bd &= 0 \\ d + bd + b + 1 &= 1 \\ d(1 + b) + (1 + b) &= 1 \\ (d + 1)(1 + b) &= 1 \end{aligned}$$

  Lo que conduce a:

$$(d + 1 = 1 \wedge b + 1 = 1) \vee (d + 1 = -1 \wedge b + 1 = -1)$$

  De lo anterior, surge:

  - **Caso a:** $d + 1 = 1$ y $b + 1 = 1$, del cual se tiene que $d = 0$ y $b = 0$.
  - **Caso b:** $d + 1 = -1$ y $b + 1 = -1$, del cual se infiere que $d = -2$ y $b = -2$.

  Teniendo así que:

$$(1, 0) \odot (1, 0) = (1, 0)$$

  Y que

$$(1, -2) \odot (1, -2) = (1, 0)$$

- **Caso 02:** $a = -1$ y $c = -1$, del cual se tiene que:

$$\begin{aligned} ad + bc + bd &= 0 \\ -d - b + bd &= 0 \\ -d + bd - b + 1 &= 1 \\ d(-1 + b) - (-1 + b) &= 1 \\ (d + 1)(b - 1) &= 1 \end{aligned}$$

Lo anterior conllevando a:

$$(d - 1 = 1 \wedge b - 1 = 1) \vee (d - 1 = -1 \wedge b - 1 = -1)$$

Análogamente, surge que:

- **Caso a:** $d - 1 = 1$ y $b - 1 = 1$, del cual se tiene que $d = 2$ y $b = 2$.
- **Caso b:** $d - 1 = -1$ y $b - 1 = -1$, del cual se infiere que $d = 0$ y $b = 0$. Determinando que:

$$(-1, 0) \odot (-1, 0) = (1, 0)$$

Y que

$$(-1, 2) \odot (-1, 2) = (1, 0)$$

Determinando así que hay exactamente cuatro elementos invertibles en ε (ver Figura 2.3). Al conjunto de estos elementos, denominados unidades de ε, se les notará con $\mathfrak{U}(\mathbb{J})$. Como $\varepsilon \subset \mathbb{J}$, se cumple que $\mathfrak{U}(\varepsilon) \subset \mathfrak{U}(\mathbb{J})$, pues todo elemento invertible en ε bajo $\odot$, también es invertible en $\mathbb{J}$. Luego $\mathfrak{U}(\varepsilon)$ está dado por:

$$\mathfrak{U}(\varepsilon) = \big\{(1, 0), (-1, 0), (1, -2), (-1, 2)\big\}$$

Teorema 2.1.8 *Sea* $(a, b) \in \mathfrak{U}(\varepsilon)$ *se cumple que* $\overline{(a, b)} \in \mathfrak{U}(\varepsilon)$

Demostración: Se cumple que $\overline{(1, 0)}, \overline{(-1, 0)} \in \varepsilon$. Esto se debe a que, considerando la segunda condición del teorema 1.3.1, se tiene que $\overline{(1, 0)} = (1, 0)$ y $\overline{(-1, 0)} = (-1, 0)$. Por otro lado, se tiene que $\overline{(1, -2)} = (1 - 2, -(-2)) = (-1, 2)$. Y bajo la consideración de la tercera condición del teorema 1.3.1, se verifica que $\overline{(-1, 2)} = (1, -2)$. Concluyendo así que el conjugado de toda unidad es una unidad.

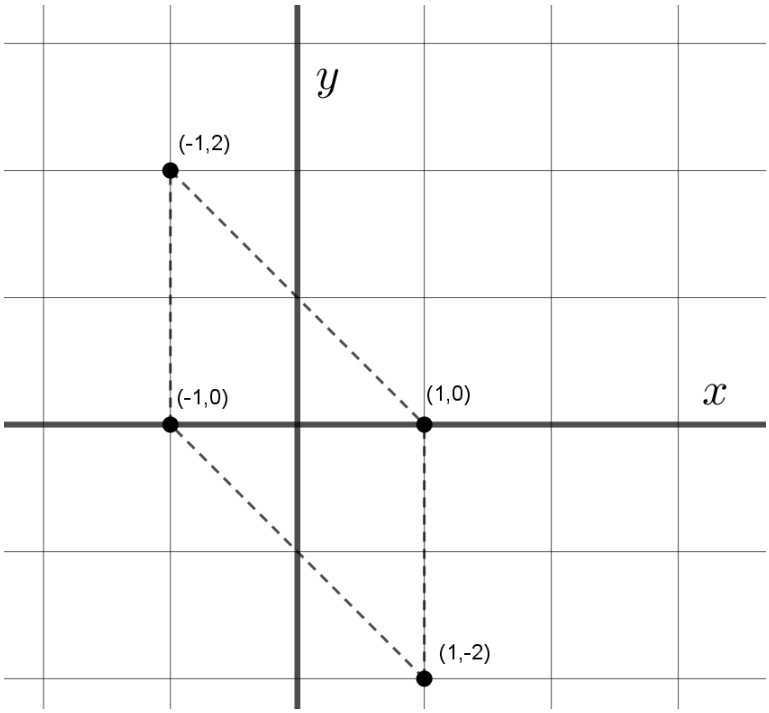

Figura 2.3: Representación en el plano irreal de las unidades de ε

Comparación vi de ε con $\mathbb{Z}$: Tanto $\mathbb{Z}$ como ε tienen una cantidad finita de unidades. Por un lado ε cuenta con cuatro unidades y, por otro lado, $\mathbb{Z}$ cuenta con dos unidades, siendo estas 1 y -1.

El teorema 1.1.8 dice que $(\mathfrak{U}(\mathbb{J}), \odot)$ es un grupo conmutativo, surgiendo así un teorema análogo en $(\mathfrak{U}(\varepsilon), \odot)$, siendo:

Teorema 2.1.9 $(\mathfrak{U}(\varepsilon), \odot)$ *es grupo conmutativo.*

Demostración: A continuación se muestra la tabla de $(\mathfrak{U}(\varepsilon), \odot)$.

$\odot$	(1,0)	(-1,0)	(1,-2)	(-1,2)
(1,0)	(1,0)	(-1,0)	(1,-2)	(-1,2)
(-1,0)	(-1,0)	(1,0)	(-1,2)	(1,-2)
(1,-2)	(1,-2)	(-1,2)	(1,0)	(-1,0)
(-1,2)	(-1,2)	(1,-2)	(-1,0)	(1,0)

Cuadro 2.1: Producto de unidades de ε

Con la tabla 2.1 se evidencia que el producto de unidades de ε está bien definido. Pero, ¿cómo verificar que $(\mathfrak{U}(\varepsilon), \odot)$ es asociativa? Hacer una revisión exhaustiva del

asunto, determinaría si $(\mathfrak{U}(\varepsilon), \odot)$ es o no asociativa, pero sería agotador. Dado que $(\mathfrak{U}(\varepsilon, \odot)$ es de orden 4, de ser grupo conmutativo, este sería isomorfo a $(\mathbb{Z}_4, +)$[III] o exclusivamente isomorfo al cuarto grupo de Klein [4, p. 69].

Como se evidencia $u \odot u = (1, 0)$, para todo $u \in \mathfrak{U}(\varepsilon)$. Si $(\mathfrak{U}(\varepsilon), \odot)$ es isomorfo a cualquier grupo de orden 4, este grupo debe tener dicha propiedad estructural. $(\mathbb{Z}_4, +)$ no tiene dicha propiedad estructural (que cualquier elemento por sí mismo, dé el módulo), pero el cuarto grupo de Klein $(\mathbb{K}, \bullet)$ sí. Por lo tanto, se considera $f : \mathfrak{U}(\varepsilon) \to \mathbb{K}$ tal que

$$f(1, 0) = e$$
$$f(-1, 0) = a$$
$$f(1, -2) = b$$
$$f(-1, 2) = c$$

$\bullet$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Cuadro 2.2: Cuarto grupo de Klein

En la tabla 2.2, se muestra el cuarto grupo de Klein, $(\mathbb{K}, \bullet)$. Con base en esta tabla y la tabla 2.1, con las cuales se verifica, por revisión exhaustiva, que $(\mathfrak{U}(\varepsilon), \odot)$ y $(\mathbb{K}, \bullet)$, son estructuralmente iguales; es decir, son identicos, salvo por los nombres de sus elementos. Luego, $(\mathfrak{U}(\varepsilon), \odot)$ y $(\mathbb{K}, \bullet)$, son isomorfos [4, p. 66]. Lo cual permite decir, que ambos tienen las mismas propiedades estructurales. Concluyendo así que $(\mathfrak{U}(\varepsilon), \odot)$ es grupo conmutativo, pues el cuarto grupo de Klein lo es.

Corolario 2.1.2 *Para todo $u \in \mathfrak{U}(\varepsilon)$ se cumple que $u = u^{-1}$.*

Demostración: Como previamente se dijo, $(\mathfrak{U}(\varepsilon), \odot)$ tiene las mismas propiedades

[III] Se debe aclarar que aquí + no alude a la suma de números enteros, sino a la suma definida en $\mathbb{Z}_4$

estructurales que el cuarto grupo de Klein. De lo cual se tiene que en $\mathfrak{U}(\varepsilon)$ todo elemento es su propio inverso bajo $\odot$ pues esto sucede en $(\mathbb{K}, \bullet)$.

Corolario 2.1.3 *Para todo $u_1, u_2 \in \mathfrak{U}(\varepsilon)$, se cumple que $u_1 \odot u_2 = u_2 \odot {u_1}^{-1}$.*

DEMOSTRACIÓN: Sean $u_1, u_2 \in \mathfrak{U}(\varepsilon)$. Se cumple que $u_1 = {u_1}^{-1}$, luego $u_1 \odot u_2 = {u_1}^{-1} \odot u_2$. Como $(\mathfrak{U}(\varepsilon), \odot)$ conmuta, se concluye finalmente que $u_1 \odot u_2 = u_2 \odot {u_1}^{-1}$.

Comparación [vii] de ε con $\mathbb{Z}$: El conjunto de las unidades de $\mathbb{Z}$ consta de dos elementos, siendo estos -1 y 1. Si se considera este conjunto bajo el producto usual en $\mathbb{Z}$ se puede demostrar que este es isomorfo a $\mathbb{Z}_2$ con la suma allí, definida. Como $(\mathfrak{U}(\varepsilon), \odot)$ consta de cuatro elementos, hubiera sido curioso si este conjunto fuera isomorfo con $(\mathbb{Z}_4, +)$, pues así ambos conjuntos, las unidades de $\mathbb{Z}$ y las unidades de ε, hubieran sido isomorfos a conjuntos cocientes de $\mathbb{Z}$. Pero no fue así, pues se demostró que $(\mathfrak{U}(\varepsilon), \odot)$, es isomorfo al cuarto grupo de Klein $(\mathbb{K}, \bullet)$. Pero esto permite evidenciar la similitud entre las unidades de $\mathbb{Z}$ y ε y es la de cumplir que cada unidad es su propio inverso. Esto sucede tanto con las unidades de ε como con las unidades de $\mathbb{Z}$. De haber sido $\mathfrak{U}(\varepsilon)$ isomorfo con $\mathbb{Z}_4$ no se cumpliría esta propiedad.

Considerando ahora los elementos de $\mathfrak{U}(\varepsilon)$ con la suma $\oplus$ heredada de ε, se determina que esta operación no está bien definida; es decir, que suma de una unidades no es unidad. Considerando $(1,0) \oplus (1,0) = (2,0)$ se evidencia lo dicho previamente. Por lo tanto, se concluye unicamente que $(\mathfrak{U}(\varepsilon), \odot)$ es grupo conmutativo.

2.1.3. Propiedad cancelativa en $(\varepsilon, \odot)$

Considérese en $\mathbb{Z}$ la igualdad $ac = 0$, se infiere que necesariamente $a = 0$ o $c = 0$. Esto se debe a que $\mathbb{Z}$ es un dominio integro[IV]. El corolario 1.1.1, concluye que el anillo $(\mathbb{J}, \oplus, \odot)$ no es un dominio integro. Análogamente, se demostrará que $(\varepsilon, \oplus, \odot)$ también es un dominio no integro.

[IV] También conocido como dominio entero o dominio de integridad.

Teorema 2.1.10 *El conjunto $\mathfrak{D}(\varepsilon)$ de los elementos divisores de (0,0) en ε está dado por:*

$$\mathfrak{D}(\varepsilon) = \{(a,b) \in \varepsilon - \{(0,0)\} : a = 0 \vee a + b = 0\}$$

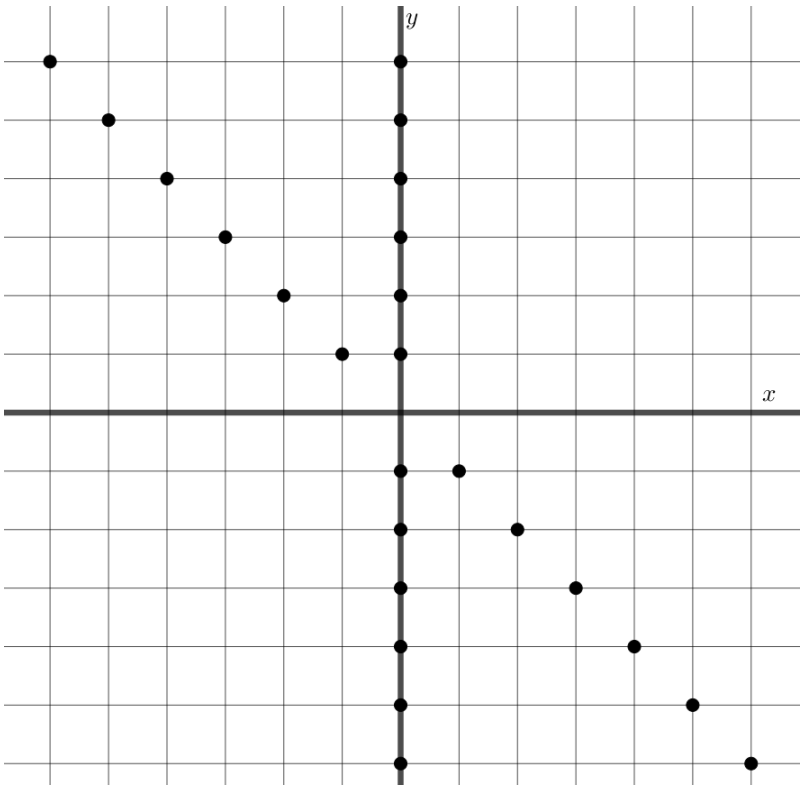

Figura 2.4: Representación en el plano irreal de $\mathfrak{D}(\varepsilon)$

Demostración: Sean $w, z \in \varepsilon$ tal que $w = (a,b)$ y $z = (c,d)$, ambos diferentes de (0,0). El producto $w \odot z$ está dado por:

$$\begin{aligned} w \odot z &= (a,b) \odot (c,d) \\ &= (ac, ad + bc + bd) \end{aligned}$$

Igualando a (0,0), se tiene:

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

De lo cual, por definición 1.1.1, se tiene que $0 = ac$ y $0 = ad + bc + bd$. Como $\mathbb{Z}$ es un dominio de integridad, se cumple que $a = 0$ o $c = 0$. Sin perdida de generalidad,

se dirá que $a = 0$. Lo cual implica que:

$$0 = ad + bc + bd$$

$$0 = bc + bd$$

$$0 = b(c + d)$$

De la misma forma, se concluye que $b = 0$ o $c + d = 0$. Pero no se puede cumplir que $b = 0$, pues esto significaría que $w = (0, 0)$. Luego se tiene que $c + d = 0$. Concluyendo así que los divisores de $(0, 0)$ son los elementos w y z, ambos diferentes de (0,0), tal que: $w = (0, b)$ y $z = (c, -c)$. Algunos de estos elementos se muestran en la Figura 2.4. Se ha de agregar que el conjunto $\mathfrak{D}(\varepsilon)$ tiene tantos elementos como el conjunto de los números naturales; es decir, su cardinal es $\aleph_0$.

Corolario 2.1.4 *La estructura* $(\varepsilon, \oplus, \odot)$ *no es dominio de integridad.*

Demostración: Consecuencia directa del teorema 2.1.10.

Como $(\mathbb{J}, \oplus, \odot)$ no es un dominio de integridad, se tiene que las leyes de cancelación en $(\varepsilon, \odot)$, en general, no son válidas [4, p. 216]. Pues, por ejemplo, si se considera:

$$(0, 0) = (0, 0)$$

$$(0, 5) \odot (3, -3) = (0, 5) \odot (5, -5)$$

Pero $(3, -3) \neq (5, -5)$. Aunque, se puede considerar las leyes de cancelación en un subconjunto de ε, siendo precisos, en el conjunto $\varepsilon^* - \mathfrak{D}(\varepsilon)$. Dada la definición de $\mathfrak{D}(\varepsilon)$ se tiene que:

$$\varepsilon^* - \mathfrak{D}(\varepsilon) = \{(a, b) \in \varepsilon : a \neq 0 \wedge a + b \neq 0\}$$

Teorema 2.1.11 *Para todo* $(a, b), (c, d), (e, f) \in \varepsilon$ *con* $e \neq 0$ *y* $e + f \neq 0$*, si* $(e, f) \odot (a, b) = (e, f) \odot (c, d)$ *entonces* $(a, b) = (c, d)$[v].

[v]Como se enunció el teorema, se demostrará la cancelativa a izquierda de $\odot$ en un subconjunto de ε. No se consideró la cancelativa a derecha, pues de cumplirse la cancelativa de izquierda, se cumple a derecha dado que $(\varepsilon, \odot)$ es conmutativa.

Demostración: Sea:

$$\begin{aligned}(e,f)\odot(a,b) &= (e,f)\odot(c,d) && \text{Hipótesis}\\ (ea, eb+fa+fb) &= (ec, ed+fc+fd) && \text{Definición de producto en } \varepsilon\end{aligned}$$

De donde, por definición 1.1.1, se tiene que: $ea = ec$ y $eb + fa + fb = ed + fc + fd$. Como $e \neq 0$ se tiene que $a = c$ luego:

$$\begin{aligned}eb+fa+fb &= ed+fc+f && \text{Definición 1.1.1}\\ af+be+bf &= cf+de+df && \text{Conmutativa y asociativa en } (\mathbb{Z},+)\\ af+b(e+f) &= cf+d(e+f) && \text{Distributiva en } \mathbb{Z}\\ fa+b(e+f) &= fa+d(e+f) && \text{Sustitución de } a=c\\ b(e+f) &= d(e+f) && \text{Cancelativa de en } (\mathbb{Z},+)\\ b &= d && \text{Cancelativa de en } (\mathbb{Z},+), \text{ dado que } e+f\neq 0\end{aligned}$$

Como $a = c$ y $b = d$, se infiere que $(a, b) = (c, d)$. Concluyendo así la demostración.

Comparación [viii] de ε con $\mathbb{Z}$: Por un lado, $\mathbb{Z}$ es un dominio de integridad. Por otro lado, el conjunto ε no es dominio de integridad, teniendo infinitos divisores del $(0, 0)$. Estos resultados, conllevan a asegurar que en $\mathbb{Z}$ se cumple la propiedad cancelativa y en ε no se cumple.

Teorema 2.1.12 *Se cumple que*

$$\varepsilon^*-\mathfrak{D}(\varepsilon) = \{(a,b)\in\varepsilon : (a>0\wedge b>-a)\vee(a>0\wedge b<-a)\vee(a<0\wedge b<-a)\vee(a<0\wedge b>-a)\}$$

Demostración: Teniendo en cuenta la tautología $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$[VI], se tiene que:

$$\begin{aligned}&\{(a,b)\in\varepsilon : (a>0\wedge b>-a)\vee(a>0\wedge b<-a)\vee(a<0\wedge b<-a)\vee(a<0\wedge b>-a)\}\\ &= \big\{(a,b)\in\varepsilon : (a>0\wedge(b>-a\vee b<-a))\vee(a<0\wedge(b>-a\vee b<-a))\big\}\\ &= \big\{(a,b)\in\varepsilon : (a>0\wedge b\neq -a)\vee(a<0\wedge b\neq -a)\big\}\\ &= \big\{(a,b)\in\varepsilon : (a>0\vee a<0)\wedge b\neq -a\big\}\\ &= \big\{(a,b)\in\varepsilon : a\neq 0\wedge b\neq -a\big\}\\ &= \varepsilon^*-\mathfrak{D}(\varepsilon)\end{aligned}$$

[VI] De la cual se puede consultar la tabla de verdad que la valida en [7, p. 9].

Concluyendo así la demostración. En esencia este teorema muestra que los elementos en ε que no son $(0,0)$ o alguno de sus divisores, pertenecen a uno solo de cuatro subconjuntos de $\varepsilon^* - \mathfrak{D}(\varepsilon)$.

Comparación ix de ε con $\mathbb{Z}$: Considerando $\mathbb{Z} - \{0\}$, se evidencia que este conjunto es la unión dos conjuntos: $\mathbb{Z}^-$ y $\mathbb{Z}^+$ y esto surge de considerar a $\mathbb{Z} - \{0\} = \{a \in \mathbb{Z} : a \neq 0\} = \{a \in \mathbb{Z} : a < 0 \vee a > 0\}$. Con un razonamiento similar, se establece en el teorema 2.1.12 cuatro subconjuntos de $\varepsilon^* - \mathfrak{D}(\varepsilon)$. Graficamente, esto se puede evidenciar en la figura 2.5.

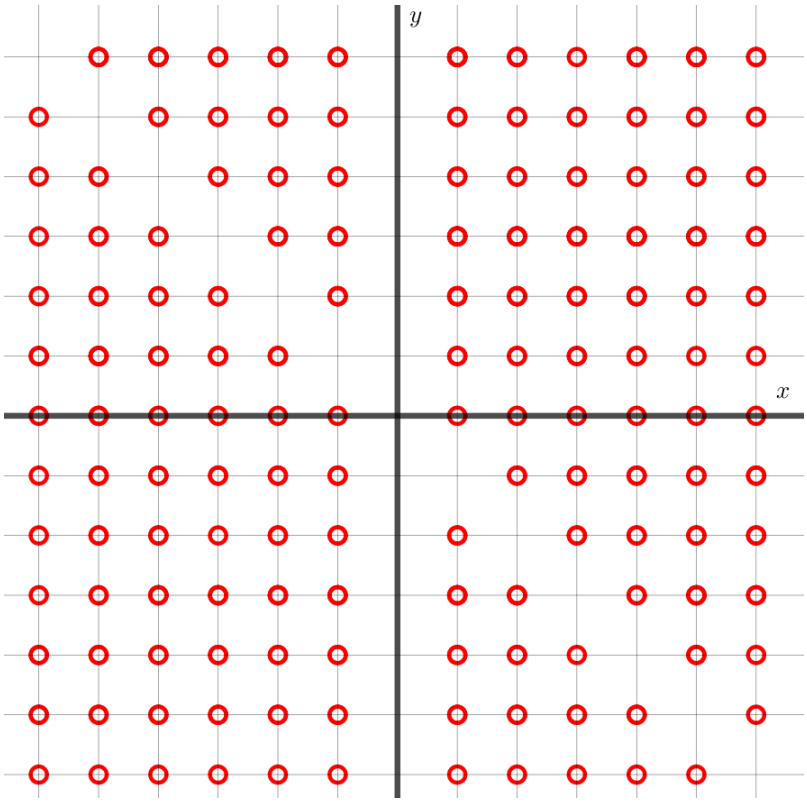

Figura 2.5: Elementos del conjunto $\varepsilon^* - \mathfrak{D}(\varepsilon)$.

2.1.4. Una partición del conjunto ε

Se han considerado los elementos invertibles en $(\varepsilon, \odot)$, los divisores del $(0,0)$, pero surge la duda natural, sobre si un elemento $(a,b) \in \varepsilon$ puede pertenecer a $\mathfrak{D}(\varepsilon)$

y $\mathfrak{U}(\varepsilon)$. De ser así, ¿cuántos elementos satisfacen esto y qué los caracteriza? Será esta la pregunta a responder en lo que sigue.

Teorema 2.1.13 *Se cumple que* $\mathfrak{U}(\varepsilon) \subset \varepsilon^* - \mathfrak{D}(\varepsilon)$.

Demostración: Recordando que $\mathfrak{U}(\varepsilon) = \big\{(1,0),(-1,0),(1,-2),(-1,2)\big\}$, por revisión exhaustiva, para todo $(a,b) \in \mathfrak{U}(\varepsilon)$ se verifica que $(a,b) \neq (0,0)$, que $a \neq 0$ y que $a \neq -b$, por lo tanto, $\mathfrak{U}(\varepsilon) \subseteq \varepsilon^* - \mathfrak{D}(\varepsilon)$. Dado que $\mathfrak{U}(\varepsilon)$ tiene cuatro elementos y $\varepsilon^* - \mathfrak{D}(\varepsilon)$ tantos elementos como números naturales se concluye que $\mathfrak{U}(\varepsilon)$ es un subconjunto propio de $\varepsilon^* - \mathfrak{D}(\varepsilon)$. Concluyendo así la demostración.

Corolario 2.1.5 $\mathfrak{U}(\varepsilon) \bigcap \mathfrak{D}(\varepsilon) = \phi$

Demostración: Del teorema anterior, se verifica que ninguna unidad de ε es divisor de $(0,0)$ y del mismo modo, ningún divisor de $(0,0)$ es una unidad de ε.

Con lo anterior, se da respuesta a la pregunta inicial. Se tiene que no existe $(a,b) \in \varepsilon$ que pertenezca a $\mathfrak{U}(\varepsilon) \bigcap \mathfrak{D}(\varepsilon)$. Luego, se puede pensar en la relación que tienen ε^* y $\mathfrak{D}(\varepsilon)$.

Lema 2.1.1 *Se cumple que* $\mathfrak{D}(\varepsilon) \subset \varepsilon^*$

Demostración: Sea $(a,b) \in \mathfrak{D}(\varepsilon)$. Por definción, se tiene que $(a,b) \neq (0,0)$ y como $\varepsilon^* = \varepsilon - \{(0,0)\}$ se concluye que $(a,b) \in \varepsilon^*$.

Teorema 2.1.14 *Los conjuntos* $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ *y* $\{(0,0)\}$, *determinan una partición de* ε.

Demostración: Para demostrar que dichos conjuntos determinan una partición de ε se debe comprobar que la unión de estos conjuntos es ε y que son disyuntos dos a dos [7, p. 112]. Por lo cual, la demostración se hará en dos partes, que son las que siguen.

- Considérese la unión de los conjuntos $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ y $\{(0,0)\}$, se tiene que:

$$
\begin{aligned}
& \mathfrak{D}(\varepsilon) \bigcup \left(\varepsilon^* - \mathfrak{D}(\varepsilon)\right) \bigcup \{(0,0)\} & \\
= & \left(\mathfrak{D}(\varepsilon) \bigcup \left(\varepsilon^* - \mathfrak{D}(\varepsilon)\right)\right) \bigcup \{(0,0)\} & \text{Asociativa de } \bigcup \\
= & \left(\mathfrak{D}(\varepsilon) \bigcup \varepsilon^*\right) \bigcup \{(0,0)\} & \text{Teorema } A \bigcup (B - A) = B \bigcup A \\
= & \ \varepsilon^* \bigcup \{(0,0)\} & \text{Lema 2.1.1 y Teo } A \subset B \rightarrow A \bigcup B = B \\
= & \ \varepsilon & \text{Dado que } \varepsilon^* = \varepsilon - \{(0,0)\}
\end{aligned}
$$

Con lo cual se demuestra que la unión de $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ y $\{(0,0)\}$ es ε. Como se evidencia, se nombran dos teoremas de operaciones entre conjuntos. Siendo estos $A \bigcup (B - A) = B \bigcup A$ y $A \subset B \rightarrow A \bigcup B = B$, para A, B conjuntos. Estos se pueden consultar en [7], en las páginas 21 y 25, respectivamente.

- A continuación se demostrará que los tres conjuntos son disyuntos dos a dos.

  - Por definición, se tiene que un divisor $(a,b) \in \varepsilon$ de $(0,0)$ cumple que $(a,b) \neq (0,0)$. Como $\{(0,0)\}$ es un conjunto unitario, se verifica que $(0,0) \notin \mathfrak{D}(\varepsilon)$. De la misma forma, también se asegura que para todo $(a,b) \in \mathfrak{D}(\varepsilon)$ se cumple que $(a,b) \notin \{(0,0)\}$. De lo cual se concluye que $\{(0,0)\} \bigcap \mathfrak{D}(\varepsilon) = \phi$.
  - Dado que $\varepsilon^* - \mathfrak{D}(\varepsilon) = \{(a,b) \in \varepsilon : a \neq 0 \wedge a + b \neq 0\}$ se infiere, por definición, que $\left(\varepsilon^* - \mathfrak{D}(\varepsilon)\right) \bigcap \{(0,0)\} = \phi$
  - Por teorema[VII] $A \bigcap \left(B - A\right) = \phi$ se infiere que $\mathfrak{D}(\varepsilon) \bigcap \left(\varepsilon^* - \mathfrak{D}(\varepsilon)\right) = \phi$.

  Concluyendo así que los tres conjuntos, son disyuntos dos a dos.

Finalmente, se ha demostrado que los conjuntos $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ y $\{(0,0)\}$, determinan una partición de ε. En la figura 2.6 se puede evidenciar una representación gráfica de esta partición, donde el $(0,0)$ está representado con $\times$, los elementos $(a,b) \in \mathfrak{D}(\varepsilon)$ se representan con $\bullet$ y, los elementos $(c,d) \in \varepsilon^* - \mathfrak{D}(\varepsilon)$ se representan con $\circ$.

[VII] Ver [7, p. 21].

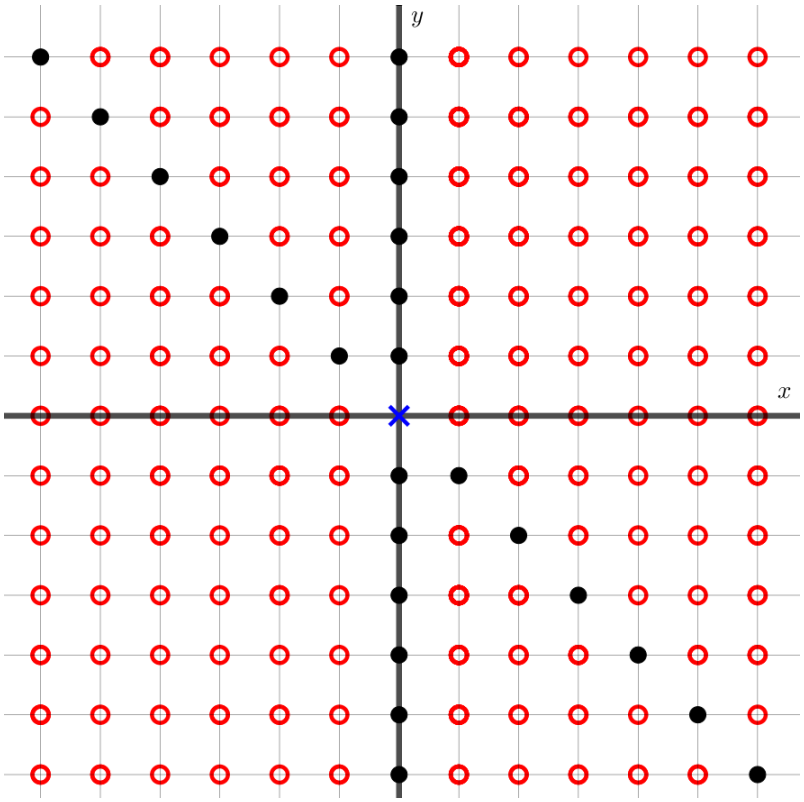

Figura 2.6: Partición del conjunto ε en tres conjuntos: $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ y $\{(0,0)\}$.

Comparación x de ε con $\mathbb{Z}$: Hasta el momento, se ha demostrado que $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ y $\{(0,0)\}$, son tres subconjuntos de ε que determinan una partición de dicho conjunto. Esto es análogo a lo que sucede en $\mathbb{Z}$. Obsérvese que al ser el conjunto vacío, el conjunto de los divisores de 0 en $\mathbb{Z}$, se tiene que la partición en $\mathbb{Z}$ está dada por $\mathbb{Z} - \{0\}$ y $\{0\}$.

2.1.5. El espacio vectorial de ε

El teorema 1.1.3 concluye que $(\mathbb{J}, \oplus, \odot)$ es un espacio vectorial real. Se considera el producto por escalar como sigue:

$$\cdot : \mathbb{R} \times \mathbb{J} \to \mathbb{J}$$
$$\cdot(\lambda, (a,b)) = \lambda \cdot (a,b) = (\lambda, 0) \odot (a,b) = (\lambda a, \lambda b)$$

Si se propusiera heredar este producto por escalar de $\mathbb{J}$ a ε, se evidencia que esté no está bien definido. Sea $(a,b) = (2,3) \in \varepsilon$ y $\pi \in \mathbb{R}$ se tiene que $\pi \cdot (2,3) = (2\pi, 3\pi) \notin \varepsilon$. De lo cual se concluye que $(\varepsilon, \oplus, \odot)$ no es un espacio vectorial real.

Dada la definición de espacio vectorial [4, p. 331], se tiene que el conjunto de los escalares debe ser un campo[VIII]. Por lo cual, no sería lícito considerar a los elementos de $\mathbb{Z}$ como escalares, a pesar de poder verificar las condiciones restantes.

[VIII] Si este campo es el conjunto de los números reales, el espacio vectorial, se denomina un espacio vectorial real.

Capítulo 3

Ecuaciones en ε

En $\mathbb{N}$ no tiene solución la ecuación $5+x=2$. En $\mathbb{Z}$ sí. Pero en $\mathbb{Z}$ no hay solución para la ecuación $2x=3$. ¿Será que en ε las ecuaciones de la forma $a+x=b$ tendrán solución? ¿La ecuaciones de la forma $ax=b$? Si han de tener solución ¿Esta será única? ¿Dependerá de alguna condición de los valores de a y b? En este capítulo se abordarán este tipo de situaciones. Se responderá si las soluciones (de existir) son únicas o no. Además se determinarán las condiciones para las cuales, las ecuaciones tengan solución.

Se debe tener presente que $(\varepsilon, \oplus, \odot)$ tiene estructura de anillo conmutativo con identidad, pues será demasiado útil, como por ejemplo, en el siguiente teorema.

Teorema 3.0.1 *Sean $(a,b),(c,d) \in \varepsilon$ la ecuación $(a,b) \oplus (x_1,x_2) = (c,d)$ tiene solución y esta es única.*

Demostración: Por teorema 2.1.3 se tiene que $(\varepsilon, \oplus)$ es grupo conmutativo y como consecuencia de ello, la ecuación $(a,b) \oplus (x_1,x_2) = (c,d)$ tiene solución y esta es única. La solución estará dada por $(x_1,x_2) = (c-a, d-b)$.

3.1. Ecuaciones de $\mathbb{Z}$ consideradas en ε

Considerando que $\mathbb{Z} \subset \varepsilon$ (por teorema 2.1.7), surge la pregunta sobre si las ecuaciones que no tienen solución en $\mathbb{Z}$, tienen solución en ε. Por ejemplo, considérese

en $\mathbb{Z}$ la ecuación $2x = 3$, esta no tiene solución en dicho conjunto. Pero considérese en ε. Esto sería:

$$(2,0) \odot (x,y) = (3,0)$$
$$(2x, 2y + 0 + 0) = (3,0)$$

Lo cual, por defínción 1.1.1 se reduce a considerar la ecuación $2x = 3$ en $\mathbb{Z}$. Es decir, el ejemplo nos sugiere que si una ecuación no tiene solución en $\mathbb{Z}$, al considerarla en ε está seguirá sin tener solución.

En general, si se considera cualquier ecuación que en $\mathbb{Z}$ no tenga solución, esta seguirá sin tener solución en ε. Estos se debe a que $\mathbb{Z} = \{w \in \varepsilon : w = (x,0)\}$, que $(x,0) \odot (y,0) = (xy,0)$ y que $(x,0) \oplus (y,0) = (x+y,0)$; es decir, la ecuación en $\mathbb{Z}$ se puede expresar como una ecuación en ε cuyos elementos conocidos tienen su segunda componente igual a cero. Lo cual conlleva a una ecuación en las primeras componentes de elementos de ε, llevando de regreso a la ecuación sin solución en $\mathbb{Z}$.

Lastimosamente no sucedió como con $\mathbb{Q}$, donde algunas ecuaciones que no tienen solución en $\mathbb{Z}$ las tienen en $\mathbb{Q}$. Pero, se debe tener en cuenta también la pregunta ¿Si una ecuación tiene solución en $\mathbb{Z}$ tendrá una cantidad diferente de soluciones al considerarse en ε? Se debe precisar que si una ecuación en $\mathbb{Z}$ tiene solución, dicha solución también lo es si se considera esta ecuación en ε. Por ejemplo, si se considera la ecuación $2x = 8$ en $\mathbb{Z}$ la solución es única y está dada por $x = 4$. Pero llevando esta ecuación a ε se tiene que es de la forma $(2,0) \odot (x,y) = (8,0)$ De lo cual se prueba que una solución es $(x,y) = (4,0)$. Pero ¿será está la única solución? Esto se precisará con lo que se ha desarrollar a continuación.

3.2. Ecuaciones en ε de la forma $a \odot x^n = b$

En general, las ecuaciones de la forma $ax^n = b$, con $n \in \mathbb{N}$, no tienen solución en $\mathbb{Z}$. Pero antes de plantear ecuaciones de este tipo en ε se debe hacer la pregunta sobre qué se puede entender por w^n con $w \in \varepsilon$ y $n \in \mathbb{Z}^+$. Con base en la definición

de potencias en $\mathbb{Z}$, análogamente se define potenciación en ε.

Definición 3.2.1 *Sea $(a,b) \in \varepsilon, n \in \mathbb{Z}^+$ se define por recurrencia:*

$$(a,b)^1 = (a,b)$$
$$(a,b)^n = (a,b)^{n-1} \odot (a,b)$$

Teorema 3.2.1 *Sea $(a,b) \in \varepsilon$ se cumple que $(a,b)^n = (a^n, (a+b)^n - a^n)$, para todo $n \in \mathbb{Z}^+$.*

Demostración: Se procederá por inducción.

- Para $n = 1$ se tiene que $(a,b)^1 = (a,b) = (a, a+b-a) = (a^1, (a+b)^1 - a^1)$
- Supóngase que se cumple para n. Por tanto $(a,b)^n = (a^n, (a+b)^n - a^n)$. Ahora considérese $(a+b)^{n+1}$. Se tendra qué:

$$\begin{aligned}
(a+b)^{n+1} &= (a,b)^n \odot (a,b) && \text{Definición 3.2.1}\\
&= (a^n, (a+b)^n - a^n) \odot (a,b) && \text{H. de inducción}\\
&= \left(a^n a, a^n b + \Big((a+b)^n - a^n\Big)a + \Big((a+b)^n - a^n\Big)b\right) && \text{Definición de } \odot\\
&= \Big(a^n a, \cancel{a^n b} + a(a+b)^n - a^n a + b(a+b)^n - \cancel{a^n b}\Big) && \text{Distributiva en } \mathbb{Z}\\
&= \Big(a^n a, (a+b)(a+b)^n - a^n a\Big) && \text{Distributiva en } \mathbb{Z}\\
&= (a^{n+1}, (a+b)^{n+1} - a^{n+1}) && \text{Potenciación en } \mathbb{Z}
\end{aligned}$$

Concluyendo así la demostración.

Ejemplo 3.2.1 *Determine el resultado de $(5,-3)^6$.*

Solución: Consecuencia del teorema 3.2.1, se tiene que

$$(5,-3)^6 = (5^6, (5-3)^6 - 5^6) = (15625, -15561)$$

Teorema 3.2.2 *Sean $(a,b),(c,d) \in \varepsilon$ se cumple que $\big((a,b) \odot (c,d)\big)^n = (a,b)^n \odot (c,d)^n$, para todo $n \in \mathbb{Z}^+$.*

Demostración: De forma análoga al teorema 3.2.1, se procederá por inducción.

- Para $n = 1$ se cumple que $\big((a,b) \odot (c,d)\big)^1 = (a,b) \odot (c,d) = (a,b)^1 \odot (c,d)^1$.

- Supóngase que se cumple para n; esto es, $\big((a,b)\odot(c,d)\big)^n = (a,b)^n \odot (c,d)^n$. Ahora, considerando $\big((a,b)\odot(c,d)\big)^{n+1}$ se tiene que:

$$\begin{aligned}\big((a,b)\odot(c,d)\big)^{n+1} &= \big((a,b)\odot(c,d)\big)^n \odot \big((a,b)\odot(c,d)\big)\\ &= \big((a,b)^n \odot (c,d)^n\big) \odot \big((a,b)\odot(c,d)\big)\\ &= \big((a,b)^n \odot (a,b)\big) \odot \big((c,d)^n \odot (c,d)\big)\\ &= (a,b)^{n+1} \odot (c,d)^{n+1}\end{aligned}$$

Concluyendo así la demostración.

Teorema 3.2.3 *Sea $(a,b) \in \mathfrak{U}(\varepsilon)$, se cumple que $(a,b)^n = (1,0)$, para todo n par positivo.*

Demostración: Dado que n es un número par positivo, se tiene que $n = 2k$ para $k \in \mathbb{Z}^+$. Por inducción, sobre k, se tiene que para:

- $k = 1$ se cumple que $(a,b)^{2\cdot 1} = (a,b)^2 = (1,0)$, pues toda unidad es su inversa bajo $\odot$.
- Ahora, suponiendo que se cumple que $(a,b)^{2k} = (1,0)$, se verifica que $(a,b)^{2(k+1)} = (a,b)^{2k+2} = (a,b)^{2k} \odot (a,b)^2 = (1,0)\odot(1,0) = (1,0)$

Con lo cual se conluye que toda unidad elevada a una potencia par, da como resultado el módulo del producto definido en $\odot$.

Comparación xi de ε con $\mathbb{Z}$: Con la definición de potenciación, se establecieron varios teoremas, de los cuales se evidencian algunas analogías con los números enteros, las cuales son las que siguen.

- Para toda unidad, ya sea en ε o en $\mathbb{Z}$, se cumple que al elevarla a una potencia par, el resultado es la identidad mutiplicativa.
- La potenciación distribuye a derecha respecto al producto. Esto sucede tanto en ε como en $\mathbb{Z}$.

3.2.1. Ecuaciones en ε de la forma $a \odot x = b$

Considérese la ecuación $(5,6)\odot(x,y) = (3,-6)$. ¿Será que está tiene solución en ε? Y la ecuación $(2,6)\odot(x,y) = (6,-6)$ ¿tendrá solución, esta será única? Lo que sigue, nos dirá lo que sucede con estas ecuaciones y con otras bajo la misma estructura.

Luego, por definición 1.1.1 se tiene que $0x = c$, pero como $c \neq 0$ se infiere que no existe $x \in \mathbb{Z}$ que satisfaga la ecuación. Por lo tanto la ecuación $(0, b) \odot (x, y) = (c, d)$ no tiene solución.

Teorema 3.2.4 *Sean $(a, b), (c, d) \in \varepsilon$, la ecuación $(a, b) \odot (x, y) = (c, d)$ no tiene solución si $a \nmid c$.*

Demostración: Si $a \nmid c$ no existe $x \in \mathbb{Z}$ tal que $ax = c$, luego no existe $(x, y) \in \varepsilon$ tal que $(c, d) = (ax, ay + bx + by) = (a, b) \odot (x, y)$.

Considerando la ecuación previa: $(5, 6) \odot (x, y) = (3, -6)$, se concluye que esta no tiene solución, esto debido a que $5 \nmid 3$.

Corolario 3.2.1 *Sean $(a, b), (c, d) \in \varepsilon$, la ecuación $(a, b) \odot (x, y) = (c, d)$ no tiene solución si $a = 0$ y $c \neq 0$.*

Demostración: Como $a = 0$ y $c \neq 0$ se tiene que $a \nmid c$ (pues no existe $x \in \mathbb{Z}$ tal que $0x = c$), por lo tanto, con base en el teorema 3.2.4, se tiene que la ecuación no tiene solución.

Con base en el teorema se tiene que una condición necesaria, para que la ecuación $(a, b) \odot (x, y) = (c, d)$ tenga solución es que $a \mid c$. Esto se ha de tener en cuenta. Pero se debe también considerar que los elementos de ε se pueden caracterizar en tres conjuntos. Siendo estos: $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ y $\{(0, 0)\}$. Con ello también se ha de tener cuidado.

Teorema 3.2.5 *Sea $(a, b) \in \varepsilon$, la ecuación $(a, b) \odot (x, y) = (0, 0)$, tiene infinitas soluciones si $a = 0$ o $a + b = 0$.*

Demostración: Si $a = 0$ y $a+b = 0$, se tiene que $b = 0$. De lo cual se verifica, trivialmente que $(0, 0) \odot (x, y) = (0, 0)$ para cualquier $(x, y) \in \varepsilon$. Ahora, si $a = 0$ o exclusivamente $a + b = 0$, se tiene que (a, b) es un divisor de $(0, 0)$, esto por teorema 2.1.10. Precisando se tiene que:

- Si $a = 0$ y $a + b \neq 0$ se cumple que $b \neq 0$ y que existen inifinitas soluciones de la forma $(x, -x)$, pues $(0, b) \odot (x, -x) = (0, 0)$ (ver Figura 3.1).
- Si $a \neq 0$ y $a + b = 0$, se tiene $a = -b$ y que existen infinitas soluciones a la ecuación de la forma $(x, y) = (0, y)$, pues y puede tomar cualquier valor en $\mathbb{Z}$.

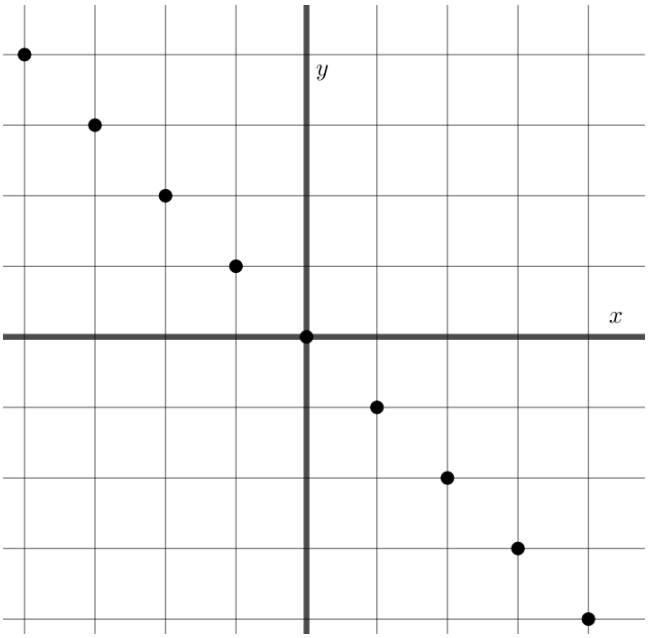

Figura 3.1: Representación en el plano irreal de las soluciones de la ecuación $(0, b) \odot (x, y) = (0, 0)$ con $b \neq 0$.

Concluyendo así, que bajo las condiciones dadas, la ecuación tiene infinitas soluciones.

Teorema 3.2.6 *Sean $(a, b), (c, d) \in \varepsilon$ si $a|c$, $a \neq -b$ y $c = -d$, la ecuación $(a, b) \odot (x, y) = (c, d)$ tiene una única solución en ε.*

Demostración: Dado que $c = -d$, se tiene que:

$$(a, b) \odot (x, y) = (c, d)$$
$$(ax, ay + bx + by) = (c, -c)$$

Luego $ax = c$ y $ay + bx + by = -c$ Como $a \mid c$ se tiene que existe un único $x \in \mathbb{Z}$ que satisface que $ax = c$. Se tiene que x está dado por $\frac{c}{a}$[1]. Con base en ello, se tiene que

$$ay + bx + by = -c$$
$$ay + bx + by + c = 0$$
$$ay + bx + by + ax = 0$$
$$(a + b)(x + y) = 0$$

[1]La división no es una operación bien definida en $\mathbb{Z}$. Pero si se considera en $\mathbb{Z}$ la ecuación $ax = c$ y esta tiene solución se tiene que esta es única y que está dado por la división de c en a, pues por el teorema del algoritmo de la división en $\mathbb{Z}$ el residuo es 0. Por lo tanto, es legal decir que $x = \frac{c}{a}$ pues el resultado de esta división pertenece a $\mathbb{Z}$.

Como $a \neq -b$ se tiene que $a+b \neq 0$. Por tanto, si $x = -y$, se cumple que la ecuación tiene solución. Siendo:

$$(x, y) = \left(\frac{c}{a}, -\frac{c}{a}\right)$$

Para responder a la ecuación que se planteó al inicio de la sección, $(2, 6) \odot (x, y) = (6, -6)$, como se tiene que $6 = -(-6)$, $2 \mid 6$ y $2 \neq -6$, se concluye que la ecuación tiene solución y esta es única. La solución está dada por:

$$(x, y) = \left(\frac{6}{2}, -\frac{6}{2}\right) = (3, -3)$$

Teorema 3.2.7 *Sean $(a, b), (c, d) \in \varepsilon$ si $a = -b$, y $a|c$, la ecuación $(a, b) \odot (x, y) = (c, d)$ tiene infinitas soluciones en ε si y solo si $c = -d$*

Demostración: Como $a = -b$ y $a \mid c$, se tiene que:

- Si la ecuación tiene infinitas soluciones, esto representa que existen infinitos $(x, y) \in \varepsilon$ que satisfacen:

$$\begin{aligned}(a, -a) \odot (x, y) &= (c, d)\\ (ax, ay - ax - ay) &= (c, d)\\ (ax, -ax) &= (c, d)\end{aligned}$$

  De lo cual, por definicion 1.1.1, se infiere que $ax = c =$ y $-ax = d$. Bajo la consideración hecha, y toma cualquier valor en $\mathbb{Z}$, pero se debe cumplir que $c = ax = -(-ax) = -d$, para que existan soluciones de la ecuación y estas sean infinitas Por lo tanto, se cumple que $c = -d$ y que las soluciones a la ecuación $(a, b) \odot (x, y) = (c, d)$, están dadas por el conjunto F, definido como sigue:

$$F = \left\{ \left(\frac{c}{a}, y\right) \in \varepsilon : y \in \mathbb{Z} \right\}$$

- Si $c = -d$, con base a lo anterior, se demuestra que las soluciones a la ecuación son infinitas, siendo F el conjunto de solución.

Corolario 3.2.2 *Sean $(a, b), (c, d) \in \varepsilon$, con $a = -b$ y $a \nmid c$ la ecuación $(a, b) \odot (x, y) = (c, d)$ no tiene solución si $c \neq -d$.*

Demostración: Consecuencia directa del teorema 3.2.7.

Ejemplo 3.2.2 *Determine cuál es el conjunto de soluciones de las ecuaciones de las ecuaciones:*

- $(3,-3)\odot(x,y)=(9,9)$
- $(1,-1)\odot(x,y)=(-4,4)$

SOLUCIÓN:

- Para la ecuación $(3,-3)\odot(x,y)=(9,9)$ se observa que $9\neq -9$, por lo tanto la ecuación no tiene solución en ε.
- Con base en el teorema 3.2.7 y dado que $1=-(-1)\ 1|4$ y $4=-(-4)$ se cumple que la ecuación $(1,-1)\odot(x,y)=(-4,4)$ tiene infinitas soluciones, dadas por:

$$F=\{(-4,y)\in\varepsilon : y\in\mathbb{Z}\}$$

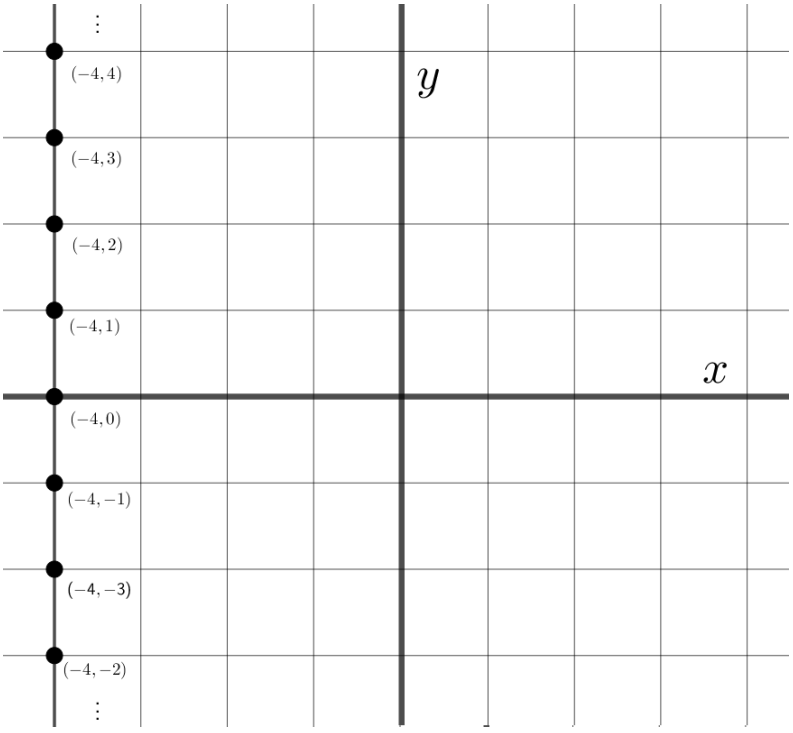

Figura 3.2: Representación en el plano irreal de las soluciones de la ecuación $(1,-1)\odot(c,d)=(-4,4)$.

Teorema 3.2.8 *Sea $(a,b),(c,d)\in\varepsilon$ la ecuación $(a,b)\odot(x,y)=(c,d)$ tiene solución única si $a\neq -b$, $(a+b)|(d+c)$ y $a|c$.*

Demostración: Sea:

$$(a,b) \odot (x,y) = (c,d)$$
$$(ax, ay + bx + by) = (c,d)$$

De lo cual, se tiene que $ax = c$ y $ay + bx + by = d$. Despejando y de la segunda igualdad, se tiene que:

$$ay + bx + by = d$$
$$ay + by = d - bx$$
$$y(a+b) = d - bx$$

Para poder despejar y se primero debe asegurar que $a + b \neq 0$ pero esto se tiene, debido a que $a \neq -b$. Segundo, se debe asegurar que $a + b$ divide a $d - bx$. Como $(a+b)|(d+c)$ se tiene que:

$$\frac{d+c}{a+b} \in \mathbb{Z}$$

Además, como se supone que $x \in \mathbb{Z}$, se tiene que:

$$x = \frac{x(a+b)}{a+b} \in \mathbb{Z}$$

Luego, como la operación resta está bien definida en $\mathbb{Z}$, se cumple que:

$$\frac{d+c}{a+b} - \frac{x(a+b)}{a+b} \in \mathbb{Z}$$

Pero como $ax = c$, se cumple que:

$$\frac{d+c}{a+b} - \frac{x(a+b)}{a+b} = \frac{d+ax}{a+b} - \frac{x(a+b)}{a+b}$$

$$= \frac{d + \cancel{ax} - \cancel{ax} - bx}{a+b}$$

Luego se tiene que

$$\frac{d-bx}{a+b} \in \mathbb{Z}$$

Por ende, tiene lugar decir que:

$$y = \frac{d-bx}{a+b}$$

Como $a|c$ se tiene que $x = \frac{c}{a}$, luego la ecuación $(a,b) \odot (x,y) = (c,d)$ tiene una única solución y esta está dada por:

$$(x,y) = \left(\frac{c}{a}, \frac{d - bx}{a+b}\right) = \left(\frac{c}{a}, \frac{d - b(\frac{c}{a})}{a+b}\right)$$

Corolario 3.2.3 *Sean $(a,b),(c,d) \in \varepsilon$ con $b = 0$, $c \neq 0$, la ecuación $(a,b) \odot (x,y) = (c,d)$ tiene única solución si $a|c$ y $a|d$.*

Demostración: Como $a|c$ se tiene que $a \neq 0$ pues $c \neq 0$. Además, como $a|d$, se tiene que $a|(c+d)$. Luego por teorema 3.2.8, la ecuación tiene solución única y esta es:

$$(x,y) = \left(\frac{c}{a}, \frac{d}{a}\right)$$

Corolario 3.2.4 *Sean $(a,b),(c,d) \in \varepsilon$ tal que $d = 0$, $a \neq -b$, $(a+b)|c$ y $a|c$. La ecuación $(a,b) \odot (x,y) = (c,d)$ tiene solución única.*

Demostración: Esta ecuación es solo una caso particular de las ecuaciones que se plantean en el teorema 3.2.8, con la única variación que $d = 0$. Por lo tanto la solución a la ecuación es única y está dada por:

$$(x,y) = \left(\frac{c}{a}, \frac{-b(\frac{c}{a})}{a+b}\right)$$

Ejemplo 3.2.3 *Determine si la ecuación $(5,9) \odot (x,y) = (40,114)$ tiene solución en ε.*

Solución: Como $5|40$, $5 \neq -9$ y $5+9 = 14|154 = (40+114)$, se concluye que la ecuación tiene solución y esta está dada por:

$$\begin{aligned}(x,y) &= \left(\frac{40}{5}, \frac{114 - 9(\frac{40}{5})}{5+9}\right) \\ &= \left(8, \frac{114-72}{14}\right) \\ &= (8,3)\end{aligned}$$

Se verifica que $(5,9) \odot (8,3) = (40,114)$.

Como se ha evidenciado, la ecuación $(a,b) \odot (x,y) = (c,d)$ puede no tener solución, tener solución única o, tener infinitas soluciones. Y este conjunto de solución, está determinado con las caracteristicas de los números a, b, c y d. Por ejemplo si $a \nmid c$ se tiene que la ecuación no tiene solución. En la tabla 3.1, se realiza una síntesis, de lo desarrollado en esta sección.

Condiciones	**Cantidad de soluciones en ε**	**Resultado del**
$a \nmid c$	No existe solución	Teorema 3.2.4
$a = 0$ y $c \neq 0$	No existe solución	Corolario 3.2.1
$c = d = 0$ y $(a = 0$ o $a + b = 0)$	Infinitas soluciones	Teorema 3.2.5
$a \mid c$, $c = -d$ y $a \neq -b$	Solución única	Teorema 3.2.6
$a \mid c$, $c \neq -d$ y $a = -b$	No existe solución	Corolario 3.2.2
$a \mid c$, $c = -d$ y $a = -b$	Infinitas soluciones	Teorema 3.2.7
$a \mid c$, $a \neq -b$ y $(a + b) \mid (c + d)$	Solución única	Teorema 3.2.8
$a \mid c$, $b = 0$, $a \neq 0$ y $a \mid d$	Solución única	Corolario 3.2.3
$a \mid c$, $d = 0$ $a \neq -b$ y $(a + b) \mid c$	Solución única	Corolario 3.2.4

Cuadro 3.1: Condiciones sobre a, b, c y d para que la ecuación $(a,b) \odot (x,y) = (c,d)$, tenga solución en ε.

Comparación [xii] de ε con $\mathbb{Z}$: Como se ha evidenciado, para que una ecuación de la forma $(a,b) \odot (x,y) = (c,d)$, tenga solución en ε se tiene que a, b, c y d deben cumplir algunas condiciones, además de haber solución, esta puede ser única o haber infinitas. En contraste, en $\mathbb{Z}$, la ecuación de la forma $mx = n$ tiene solución única si y solo si $m \mid n$. No hay más casos en $\mathbb{Z}$.

3.2.2. Ecuaciones en ε de la forma $a \odot x^2 = b$

Sea la ecuación $5x^2 = 20$. En $\mathbb{Z}$ tiene dos soluciones siendo estas $x_1 = 2$ y $x_2 = -2$. Pero la ecuaciones $3x^2 = 1$ y $3x^2 = 24$ no tienen solución en $\mathbb{Z}$. Para que la ecuación de segundo grado $ax^2 = b$ (claramente con $a \neq 0$) tenga solución se debe cumplir que: $\frac{b}{a}$ es un número cuadrado[II]. Si $x_1 \neq 0$ es una solución de la ecuación $ax^2 = b$, se tiene que $x_2 = -x_1$ también es solución. Las soluciones están dadas por:

$$x_1 = \sqrt{\frac{b}{a}} \qquad \text{y} \qquad x_2 = -\sqrt{\frac{b}{a}}$$

[II]Cuando se hable de un número cuadrado c, se alude a que c satisface que es el cuadrado de algún número natural p; es decir, $p^2 = c$. Con lo anterior, se tiene que 0, es un número cuadrado.

Si $b = 0$, se tiene que una solución de la ecuación $ax^2 = b$ es $x = 0$ y esta es única. Esta solución, es de multiplicidad 2, pues se verifica que:

$$x = \sqrt{\frac{0}{a}} = -\sqrt{\frac{0}{a}} = 0$$

Con base en ello y los teoremas 3.2.1 y 3.2.8, se propone el siguiente teorema.

Teorema 3.2.9 *Sea* $(a,b),(c,d) \in \varepsilon$ *la ecuación* $(a,b) \odot (x,y)^2 = (c,d)$ *tiene cuatro soluciones (contando multiplicidades) si* $a \neq -b$ *y*

$$\frac{d+c}{a+b} \ y \ \frac{c}{a}$$

son números cuadrados.

Demostración: Sea:

$$\begin{aligned}
(a,b) \odot (x,y)^2 &= (c,d) \\
(a,b) \odot \Big(x^2, (x+y)^2 - x^2\Big) &= (c,d) \\
\Big(ax^2, a\Big((x+y)^2 - x^2\Big) + b\Big(\cancel{x^2} + (x+y)^2 - \cancel{x^2}\Big)\Big) &= (c,d) \\
\Big(ax^2, (a+b)(x+y)^2 - ax^2\Big) &= (c,d)
\end{aligned}$$

De lo cual, por definición 1.1.1 se tiene que $ax^2 = c$ y $(a+b)(x+y)^2 - ax^2 = d$. Como $\frac{c}{a}$ es un número cuadrado, se tiene que existe $q \in \mathbb{Z}$, se cumple que:

$$\sqrt{\frac{c}{a}} = q$$

Por lo cual se observa que una solución de la ecuación $ax^2 = c$ es $x_1 = q$, pero también $x_2 = -x_1 = -q$ es solución. Entonces, como tal ya se han determinado los valores que toma x, lo cual nos permite reemplazar esto en la ecuación $(a+b)(x+y)^2 - ax^2 = d$. De esto se tiene que:

$$\begin{aligned}
(a+b)(x+y)^2 - ax^2 &= d \\
(a+b)(x+y)^2 - c &= d \\
(a+b)(x+y)^2 &= d+c \\
(x+y)^2 &= \frac{d+c}{a+b}
\end{aligned}$$

Siendo válido este último paso, debido a que $\frac{d+c}{a+b}$ es un número cuadrado, por lo tanto existe $p \in \mathbb{Z}$ tal que:

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

Dado que x toma dos valores, $x_1 = q$ y $x_2 = -q$, se tiene que las cuatro soluciones estarán dadas por:

- Si se considera a $y = p - x_1 = p - q$. Luego la primera solución estará dada por:

$$w_1 = (q, p-q) = \left(\sqrt{\frac{c}{a}}, \sqrt{\frac{d+c}{a+b}} - \sqrt{\frac{c}{a}}\right)$$

- Si se considera a $y = -p - x_1 = -p - q$. Luego la segunda solución estará dada por:

$$w_2 = (q, -p-q) = \left(\sqrt{\frac{c}{a}}, -\sqrt{\frac{d+c}{a+b}} - \sqrt{\frac{c}{a}}\right)$$

- Si se considera a $y = p - x_2 = p + q$. Luego la tercera solución estará dada por:

$$w_3 = (-q, p+q) = \left(-\sqrt{\frac{c}{a}}, \sqrt{\frac{d+c}{a+b}} + \sqrt{\frac{c}{a}}\right)$$

- Si se considera a $y = -p - x_2 = -p + q$. Luego la cuarta solución estará dada por:

$$w_4 = (-q, -p-q) = \left(-\sqrt{\frac{c}{a}}, -\sqrt{\frac{d+c}{a+b}} + \sqrt{\frac{c}{a}}\right)$$

Ejemplo 3.2.4 *Determine cuál de las siguientes ecuaciones tiene solución. De tener solución, diga cuántos y cuáles elementos en ε satisfacen la ecuación.*

- $(2,6) \odot (x,y)^2 = (18, 181)$
- $(2,6) \odot (x,y)^2 = (18, 182)$

Solución: Con base en el teorema 3.2.9 se tiene que:

- Considerando la ecuación $(2,6) \odot (x,y)^2 = (18, 181)$ se observa que

$$\frac{18+181}{2+6} = \frac{199}{8} \notin \mathbb{Z}$$

  Por lo tanto, este número no es un número cuadrado, luego la ecuación no tiene solución.

- Considerando la ecuación $(2,6) \odot (x,y)^2 = (18,182)$ se verifica que $2 \neq -6$ y que

$$\frac{18+182}{2+6} = 25 \text{ y } \frac{18}{2} = 9$$

son números cuadrados. Por ende, las soluciones de la ecuación $(2,6) \odot (x,y)^2 = (18,182)$ están dadas por:

- $w_1 = \left(\sqrt{\frac{18}{2}}, \sqrt{\frac{18+182}{2+6}} - \sqrt{\frac{18}{2}}\right) = (3, 5-3) = (3,2)$
- $w_2 = \left(\sqrt{\frac{18}{2}}, -\sqrt{\frac{18+182}{2+6}} - \sqrt{\frac{18}{2}}\right) = (3, -5-3) = (3,-8)$
- $w_3 = \left(-\sqrt{\frac{18}{2}}, \sqrt{\frac{18+182}{2+6}} + \sqrt{\frac{18}{2}}\right) = (-3, 5+3) = (-3,8)$
- $w_4 = \left(-\sqrt{\frac{18}{2}}, -\sqrt{\frac{18+182}{2+6}} + \sqrt{\frac{18}{2}}\right) = (-3, -5+3) = (-3,-2)$

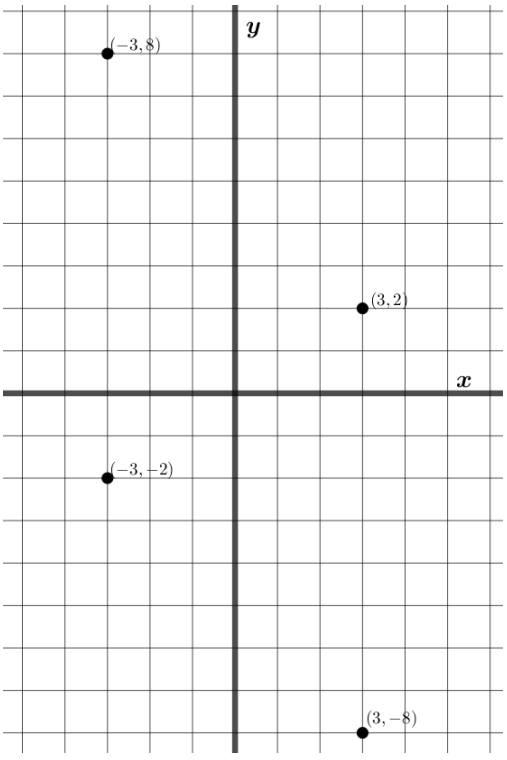

Figura 3.3: Representación en el plano irreal de las soluciones de la ecuación $(2,6) \odot (x,y)^2 = (18,182)$.

Corolario 3.2.5 *La ecuación $(x,y)^2 = (c,d)$ tiene cuatro soluciones, si $d+c$ y c son números cuadrados, siendo estas las soluciones:*

- $w_1 = \left(\sqrt{c}, \sqrt{d+c} - \sqrt{c}\right)$

- $w_2 = \left(\sqrt{c}, -\sqrt{d+c} - \sqrt{c}\right)$
- $w_3 = \left(-\sqrt{c}, \sqrt{d+c} + \sqrt{c}\right)$
- $w_4 = \left(-\sqrt{c}, -\sqrt{d+c} + \sqrt{c}\right)$

DEMOSTRACIÓN: La ecuación $(x, y)^2 = (c, d)$ se puede considerar como una ecuación de la forma $(1, 0) \odot (x, y)^2 = (c, d)$, dado que $(a, b) = (1, 0)$ es la identidad multiplicativa. Considerando el teorema 3.2.9 se tiene que las condiciones se cumplen, por ende la ecuación tiene cuatro soluciones, que son las nombradas.

Ejemplo 3.2.5 *Determine, si es posible las soluciones de las siguientes ecuaciones:*

- $(x, y)^2 = (7, 29)$
- $(x, y)^2 = (16, 0)$
- $(x, y)^2 = (9, 16)$

SOLUCIÓN:

- Se verifica que 29+7 es un número cuadrado, pero 7 no. Por tanto, la ecuación $(x, y)^2 = (7, 29)$ no tiene solución.
- Dado que 16 es un número cuadrado y 16+0=16, se tiene que las soluciones de la ecuación $(x, y)^2 = (16, 0)$ están dadas por:
  - $w_1 = (-4, 0)$
  - $w_2 = (4, 0)$
  - $w_1 = (-4, 8)$
  - $w_2 = (4, -8)$

  Cada una de multiplicidad 2.
- Se verifica que 16 y 16+9 son números cuadrados, por ende la soluciones a la ecuación $(x, y)^2 = (9, 16)$ están dadas por:
  - $w_1 = (3, 2)$
  - $w_2 = (3, -8)$
  - $w_3 = (-3, 8)$

- $w_4 = (-3, -2)$

Corolario 3.2.6 *Sea (m, n) una solución de la ecuación $(a, b) \odot (x, y)^2 = (c, d)$. Se cumple que $(-m, -n)$, también es solución de la ecuación.*

DEMOSTRACIÓN: Como (m, n) es una solución de la ecuación $(a, b) \odot (x, y)^2 = (c, d)$, se cumple que

$$\begin{aligned}(c, d) &= (a, b) \odot (m, n)^2 \\ &= (a, b) \odot \big((-1, 0) \odot (-m, -n)\big)^2 \\ &= (a, b) \odot \big((-1, 0)^2 \odot (-m, -n)^2\big) \\ &= (a, b) \odot \big((1, 0) \odot (-m, -n)^2\big) \\ &= (a, b) \odot (-m, -n)^2\end{aligned}$$

Con lo cual se concluye que $(a, b) \odot (-m, -n)^2 = (c, d)$, luego $(-m, -n)$ también es solución de la ecuación $(a, b) \odot (x, y)^2 = (c, d)$

De forma análoga, se inquiere, sobre si (m, n) es una solución de la ecuación $(a, b) \odot (x, y)^2 = (c, d)$, entonces ¿$\overline{(m, n)}$ es solución de la ecuación? Considerando el tercer ítem del ejemplo 3.2.5, se tiene que $(3, 2)$ es solución de la ecuación $(x, y)^2 = (9, 16)$, Ahora, $\overline{(3, 2)} = (3 + 2, -2) = (5, -2)$, pero $\left(\overline{(3, -2)}\right)^2 = (5, -2)^2 = (25, -16) \neq (9, 16)$. De lo cual se tiene que $\overline{(3, -2)}$, no es solución de la ecuación $(x, y)^2 = (9, 16)$. En general, no se cumple que si (m, n) es una solución de la ecuación $(a, b) \odot (x, y)^2 = (c, d)$, entonces $\overline{(m, n)}$ es solución de la ecuación.

3.2.3. Ecuaciones en ε de la forma $a \odot x^n = b$ con n par

En $\mathbb{Z}$ la ecuación $ax^n = b$ con $b \neq 0$ y n par, se tiene que de existir una solución x_1 esta no es la única pues otra solución es $x_2 = -x_1$. Con base en esto y en lo desarrollado en el teorema 3.2.9 se propone un teorema que alude a las ecuaciones en ε de la forma $a \odot x^n = b$ con n par.

Teorema 3.2.10 *Sea $(a, b), (c, d) \in \varepsilon$ la ecuación $(a, b) \odot (x, y)^n = (c, d)$, con n par, tiene cuatro soluciones, contando mutiplicidades, si $a \neq -b$ y*

$$\frac{d + c}{a + b} \ y \ \frac{c}{a}$$

son las $n-esimas$ potencias de algún $p, q \in \mathbb{Z}$, respectivamente.

DEMOSTRACIÓN: Sea

$$\begin{aligned}(a,b)\odot(x,y)^n &= (c,d)\\ (a,b)\odot\Big(x^n,(x+y)^n-x^n\Big) &= (c,d)\\ \Big(ax^n, a\Big((x+y)^n-x^n\Big)+b\Big(\cancel{x^n}+(x+y)^n-\cancel{x^n}\Big)\Big) &= (c,d)\\ \Big(ax^n,(a+b)(x+y)^n-ax^n\Big) &= (c,d)\end{aligned}$$

De lo cual, por definición 1.1.1 se tiene que $ax^n = c$ y $(a+b)(x+y)^n - ax^n = d$. Como $\frac{c}{a}$ es la $n-esima$ potencia de algún $q \in \mathbb{Z}$, se cumple que:

$$\sqrt[n]{\frac{c}{a}} = q$$

Y se verifica que $x_1 = q$ satisface la ecuación $ax^n = c$, al igual que $x_2 = -q$. Considerando que $ax^n = c$, en la ecuación $(a+b)(x+y)^n - ax^n = d$ se tiene que:

$$\begin{aligned}(a+b)(x+y)^n - ax^n &= d\\ (a+b)(x+y)^n - c &= d\\ (a+b)(x+y)^n &= d+c\\ (x+y)^n &= \frac{d+c}{a+b}\end{aligned}$$

Siendo este último paso válido debido que a $\dfrac{d+c}{a+b} \in \mathbb{Z}$, pues es la $n-esima$ potencia de un $p \in \mathbb{Z}$. Dado que n es par, se verifica que p y $-p$ satisfacen:

$$p^n = \frac{d+c}{a+b} = (-p)^n$$

Por tanto se tiene que y está dado por:

$$y = \pm p - x = \pm\sqrt[n]{\frac{d+c}{a+b}} - x$$

Pero como x toma dos valores $x_1 = q$ y $x_2 = -q$. Se tiene que las cuatro soluciones del ecuación $(a,b)\odot(x,y)^n = (c,d)$ están dadas por:

- Si se considera a $y = p - x_1 = p - q$. Luego la primera solución estará dada por:

$$w_1 = (q, p - q) = \left(\sqrt[n]{\frac{c}{a}}, \sqrt[n]{\frac{d+c}{a+b}} - \sqrt[n]{\frac{c}{a}} \right)$$

- Si se considera a $y = -p - x_1 = -p - q$. Luego la segunda solución estará dada por:

$$w_2 = (q, -p - q) = \left(\sqrt[n]{\frac{c}{a}}, -\sqrt[n]{\frac{d+c}{a+b}} - \sqrt[n]{\frac{c}{a}} \right)$$

- Si se considera a $y = p - x_2 = p + q$. Luego la tercera solución estará dada por:

$$w_3 = (-q, p + q) = \left(-\sqrt[n]{\frac{c}{a}}, \sqrt[n]{\frac{d+c}{a+b}} + \sqrt[n]{\frac{c}{a}} \right)$$

- Si se considera a $y = -p - x_2 = -p + q$. Luego la cuarta solución estará dada por:

$$w_4 = (-q, -p - q) = \left(-\sqrt[n]{\frac{c}{a}}, -\sqrt[n]{\frac{d+c}{a+b}} + \sqrt[n]{\frac{c}{a}} \right)$$

Ejemplo 3.2.6 *Determine cuál de las siguientes ecuaciones tiene solución. De tener solución, diga cuántos y cuáles elementos en ε satisfacen la ecuación.*

- $(4, 8) \odot (x, y)^6 = (62500, -61731)$
- $(4, 8) \odot (x, y)^6 = (62500, -61732)$

SOLUCIÓN: Con base en el teorema 3.2.10, se tiene que:

- Dado que
$$\frac{-61731 + 62500}{4 + 8} = \frac{769}{12} \notin \mathbb{Z}$$
se cumple que la ecuación no tiene solución en ε.

- Considerando la ecuación $(4, 8) \odot (x, y)^6 = (62500, -61732)$, dado que $4 \neq -8$, que $\frac{62500}{4} = 15625 = 5^6$ y que
$$\frac{-61732 + 62500}{4 + 8} = \frac{768}{12} = 64 = 2^6$$
Se concluye que la ecuación tiene cuatro soluciones y estas están dadas por:
  - $w_1 = \left(\sqrt[6]{\frac{62500}{4}}, \sqrt[6]{\frac{-61732+62500}{4+8}} - \sqrt[6]{\frac{62500}{4}} \right) = (5, 2 - 5) = (5, -3)$

- $w_2 = \left(\sqrt[6]{\frac{62500}{4}}, -\sqrt[6]{\frac{-61732+62500}{4+8}} - \sqrt[6]{\frac{62500}{4}}\right) = (5, -2-5) = (5, -7)$
- $w_3 = \left(-\sqrt[6]{\frac{62500}{4}}, \sqrt[6]{\frac{-61732+62500}{4+8}} + \sqrt[6]{\frac{62500}{4}}\right) = (-5, 2+5) = (-5, 7)$
- $w_4 = \left(-\sqrt[6]{\frac{62500}{4}}, -\sqrt[6]{\frac{-61732+62500}{4+8}} + \sqrt[6]{\frac{62500}{4}}\right) = (-5, -2+5) = (-5, 3)$

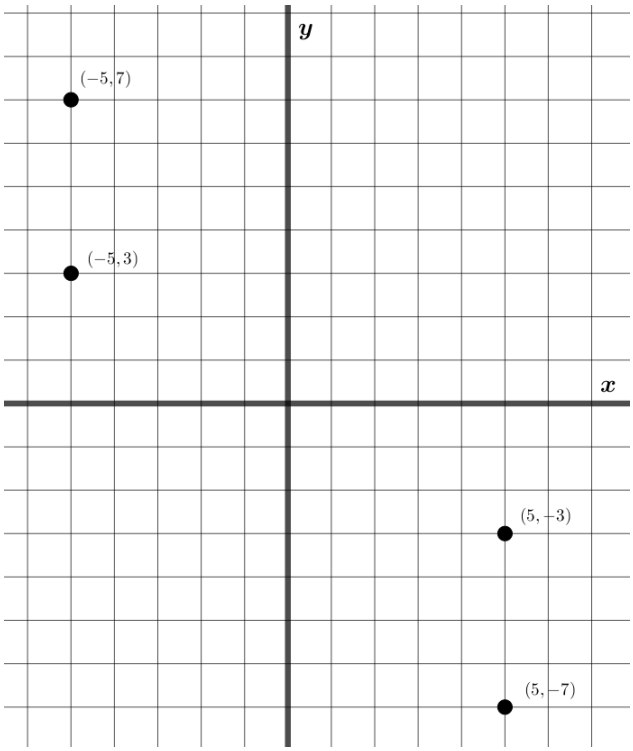

Figura 3.4: Representación en el plano irreal de las soluciones de la ecuación $(4, 8) \odot (x, y)^6 = (62500, -61732)$.

Corolario 3.2.7 *La ecuación $(x, y)^n = (c, d)$ tiene cuatro soluciones, si $d + c$ y c son las $n-$esimas potencias de algún $p, q \in \mathbb{Z}$, respectivamente. Siendo estas las soluciones:*

- $w_1 = \left(\sqrt[n]{c},\ \sqrt[n]{d+c} - \sqrt[n]{c}\right)$
- $w_2 = \left(\sqrt[n]{c}, -\sqrt[n]{d+c} - \sqrt[n]{c}\right)$
- $w_3 = \left(-\sqrt[n]{c},\ \sqrt[n]{d+c} + \sqrt[n]{c}\right)$
- $w_4 = \left(-\sqrt[n]{c}, -\sqrt[n]{d+c} + \sqrt[n]{c}\right)$

Demostración: Análoga a la demostración del corolario 3.2.10, pero considerando el teorema 3.2.10.

Corolario 3.2.8 *Sea (m,n) una solución de la ecuación $(a,b)\odot(x,y)^n=(c,d)$, con n un entero positivo par. Se cumple que $(-m,-n)$, también es solución de la ecuación.*

DEMOSTRACIÓN: Identica a la demostración del corolario 3.2.6, pero bajo la consideración del teorema 3.2.10.

Del corolario anterior, el 3.2.8, se tiene que si un elemento (m,n) es solución de la ecuación $(a,b)\odot(x,y)^n=(c,d)$, entonces $(-m,-n)$ es solución; es decir, el inverso de (m,n) bajo $\odot$ también es solución de la ecuación. Pero esto, va mucho más allá. Haciendo una observación, se tiene que $(-m,-n)=(-1,0)\odot(m,n)$; es decir, $(-m,-n)$ es el producto de (m,n) y una unidad de ε. Observando las soluciones del segundo ítem, de los ejercicios 3.2.4 y 3.2.6, se verifica que si (m,n) es solución, entonces $(m,n)\odot u$ también es solución de la ecuación, para todo $u\in\mathfrak{U}(\varepsilon)$. Esto se ratifica en el siguiente teorema.

Teorema 3.2.11 *Sea (m,n) una solución de la ecuación $(a,b)\odot(x,y)^n=(c,d)$, con n un número par positivo, entonces $(m,n)\odot u$ también es solución de la ecuación, para toda $u\in\mathfrak{U}(\varepsilon)$.*

DEMOSTRACIÓN: Como (m,n) es una solución de la ecuación $(a,b)\odot(x,y)^n=(c,d)$ y puesto que n un número par positivo, se cumple que $u^n=(1,0)$, para cualquier $u\in\mathfrak{U}(\varepsilon)$ y además:

$$\begin{aligned}(c,d)&=(a,b)\odot(m,n)^n\\&=(a,b)\odot\big((1,0)\odot(m,n)\big)^n\\&=(a,b)\odot(u\odot u)^n\odot(m,n)^n\\&=(a,b)\odot\big(u^n\odot u^n\big)\odot(m,n)^n\\&=(a,b)\odot u^n\odot\Big(u^n\odot(m,n)^n\Big)\\&=(a,b)\odot(1,0)\odot\Big(u\odot(m,n)\Big)^n\\&=(a,b)\odot\Big(u\odot(m,n)\Big)^n\end{aligned}$$

Con lo cual se válida que $u\odot(m,n)$ es solución de la ecuación $(a,b)\odot(x,y)^n=(c,d)$. Concluyendo así la demostración.

Comparación xiii de ε con $\mathbb{Z}$: En $\mathbb{Z}$ la ecuación $ax^n = c$ con n un número par, se tiene que la ecuación a lo sumo tiene dos soluciones (considerando multiplicidades. En ε la ecuación $(a,b) \odot (x,y)^n = (c,d)$ con n par, tiene a lo sumo cuatro soluciones (considerando multiplicidades). Algo que caracteriza a ε y a $\mathbb{Z}$ es que si se tiene una solución de la ecuación, se infiere que las demás soluciones están dadas por el producto de dicha solución y las unidades del conjunto respectivo. Esto se demuestra en el teorema 3.2.11.

3.2.4. Ecuaciones en ε de la forma $a \odot x^n = b$ con n impar

Considerando en $\mathbb{Z}$ la ecuación $ax^n = b$ con n impar, se tiene que de tener solución, esta será única. Con base en esta información se propone el siguiente teorema que responde a si la ecuación $(a,b) \odot (x,y)^n = (c,d)$, con n impar tiene solución y si de haberla esta sea única o haya más.

Teorema 3.2.12 *Sea $(a,b),(c,d) \in \varepsilon$ la ecuación $(a,b) \odot (x,y)^n = (c,d)$, con n impar, tiene solución única si $a \neq -b$ y*

$$\frac{d+c}{a+b} \ y \ \frac{c}{a}$$

son las $n-$esimas potencias de algún $p,q \in \mathbb{Z}$, respectivamente.

Demostración: La demostración es análoga a la que se realiza en el teorema 3.2.10, pero como n es impar el valor de x e y están determinados de forma única siendo:

$$(x,y) = \left(\sqrt[n]{\frac{c}{a}}, \sqrt[n]{\frac{d+c}{a+b}} - \sqrt[n]{\frac{c}{a}} \right)$$

Comparación xiv de ε con $\mathbb{Z}$: La ecuaciones de la forma $(a,b) \odot (x,y)^n = (c,d)$, con n impar de tener solución en ε se tiene que esta es única. De forma análoga sucede con $\mathbb{Z}$ y las ecuaciones de la forma $ax^n = b$ con n impar.

3.3. Ecuaciones en ε de la forma $a \odot x^2 \oplus b \odot x \oplus c = 0$

Sea la ecuación $ax^2 + bx + c = 0$, con $a \neq 0$, considerada en $\mathbb{C}$. Esta tiene solución. En $\mathbb{R}$, esta misma ecuación tiene solución bajo la condición que el discriminante[III] sea mayor

[III]Sea la ecuación $ax^2 + bx + c = 0$, con $a \neq 0$, el discriminante está dado por $d = b^2 - 4ac$.

o igual a cero. Pero en $\mathbb{Z}$ esta existe bajo la condición que el discrimiante sea un número cuadrado y además $2a|(-b \pm \sqrt{b^2 - 4ac})$, pues se debe asegurar que:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \mathbb{Z}$$

Ahora, considérese en ε la ecuación:

$$(a, b) \odot (x, y)^2 \oplus (c, d) \odot (x, y) \oplus (e, f) = (0, 0)$$

Si $(c, d) = (0, 0)$, el teorema 3.2.9 determina bajo qué condiciones la ecuación tiene solucion. Ahora, si además de lo anterior, se cumple que $(a, b) = (1, 0)$ el corolario 3.2.5 da las condiciones bajo las cuales la ecuación tiene solución. Considerar que $(a, b) = (0, 0)$ no tiene sentido, pues la ecuación se reduciría a $(c, d) \odot (x, y) \oplus (e, f) = (0, 0)$ y estas ecuaciones se han abordado en una sección previa. Pero qué sucedería si $(e, f) = (0, 0)$. Se tiene que:

$$\begin{aligned}(a, b) \odot (x, y)^2 \oplus (c, d) \odot (x, y) \oplus \cancel{(e, f)} &= (0, 0)\\ (x, y) \odot \big((a, b) \odot (x, y) \oplus (c, d)\big) &= (0, 0)\\ (x, y) \odot \big(ax + c, ay + bx + by + d\big) &= (0, 0)\end{aligned}$$

Ahora, dado que ε no es un dominio integro y bajo el conocimiento de los divisores de (0,0), por teorema 2.1.10, se tienen cuatro casos[IV] Explorando, se tiene que:

- **Caso 01:** Se tiene la posibilidad trivial, que $(x, y) = (0, 0)$. Por lo cual, para toda ecuación de la forma $(a, b) \odot (x, y)^2 \oplus (c, d) \odot (x, y) = (0, 0)$, se tiene que esta es solución.

- **Caso 02:** Que $(ax + c, ay + bx + by + d) = (0, 0)$, de lo cual se tiene que, $ax + c = 0$;

[IV] Dado que ε no es un dominio de integridad y sean $(a, b), (c, d) \in \varepsilon$, tal que $(a, b) \odot (c, d) = (0, 0)$ se cumple alguno de los siguientes casos:

- $(a, b) = (0, 0)$
- $(c, d) = (0, 0)$
- $a = 0$ y $c + d = 0$
- $a + b = 0$ y $c = 0$.

es decir, que $x = -\frac{c}{a}$, luego es necesario que $a \mid c$ y por ende:

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

De lo cual se tienen otros casos:

- Que $a + b = 0$ y $d + c = 0$, luego $a = -b$ y $c = -d$. De lo cual se infiere que independientemente de los valores de y, la solución existe. Pero además de existir la solución, se infiere que hay infinitas soluciones. Con base en el teorema 3.2.7, se concluye que el conjunto de soluciones está dado por:

$$F = \left\{ \left(\frac{-c}{a}, y \right) \in \varepsilon : y \in \mathbb{Z} \right\}$$

- Que $a + b \neq 0$ y $d + c = 0$, luego $a \neq -b$ y $c = -d$. Como $\mathbb{Z}$ es un dominio de integridad, se cumple que $x + y = 0$, luego $x = -y$. De lo cual se tiene que la solución es única y está dada por:

$$(x, y) = (x, -x) = \left(-\frac{c}{a}, \frac{c}{a} \right)$$

- No se da el caso en el cual $a + b = 0$ y $c + d \neq 0$, pues en $\mathbb{Z}$ es falso decir que $0 \cdot a \neq 0$ para todo $a \in \mathbb{Z}$. Luego no hay solución de $0(x + y) = -(c + d)$ si $c \neq -d$.

- Caso en el que se cumple que$(a + b) \mid (d + c)$. Si esto sucede, se tiene que la ecuación tiene solución única y está dada por:

$$y = -\frac{d + c}{a + b} - x = -\frac{d + c}{a + b} + ac$$

  Concluyendo así, que la ecuación tendrá solución única y está dada por:

$$(x, y) = \left(-\frac{c}{a}, -\frac{d + c}{a + b} + ac \right)$$

- **Caso 03:** $(x, y) = (m, -m)$ y $(ax + c, ay + bx + by + d) = (0, n)$, para algunos $m, n \in \mathbb{Z}$ diferentes de cero. Luego

$$(ax + c, ay + bx + by + d) = (0, n)$$
$$(ax + c, -ax + \cancel{bx} - \cancel{bx} + d) = (0, n)$$

Luego $ax + c = 0$ lo cual, como en el caso 02, se condiciona la existencia de solución a que $a \mid c$, de ser así, se tendrá que $x = -\frac{c}{a} = -Y$ (pues se partió del supuesto que la solución sería de la forma $(x, -x)$). Además $-ax + d = n$, esto es $c + d = n$, luego n toma un único valor. Dado que se partió de la suposición que $n \neq 0$ se ha de cumplir que $d \neq -c$. Luego, la ecuación tiene solución única y está dada por:

$$(x, y) = (x, -x) = \left(-\frac{c}{a}, \frac{c}{a}\right)$$

- **Caso 04:** $(x, y) = (0, y)$ y $(ax + c, ay + bx + by + d) = (m, -m)$, para algún $m \in \mathbb{Z} - \{0\}$. De lo cual se tiene que $ax + c = m$, pero como $x = 0$, se tiene que $c = m$. Ahora, considerando la segunda componente de $(ax + c, ay + bx + by + d)$ se tiene que:

$$ay + bx + by + d = -m$$
$$ay + by + d = -c$$
$$y(a + b) = -c - d$$
$$y(a + b) = -(c + d)$$

De forma análoga al caso 02, surgen casos sobre el caso. Siendo:

  - Si $a + b = 0 = c + d$, se cumple que y puede ser cualquier número entero. Luego, el conjunto de solución está dado por:

$$F = \left\{ \begin{pmatrix} 0, y \end{pmatrix} \in \varepsilon : y \in \mathbb{Z} \right\}$$

  - Si $a + b = 0$ y $c + d \neq 0$, luego necesariamente $y = 0$, lo cual conlleva a la solución trivial $(x, y) = (0, 0)$.
  - No se da el caso que $a + b = 0$ y $c + d \neq 0$.
  - Que $(a+b) \mid (c+d)$. De lo cual se concluye que la ecuación tiene solución única

y está dada por:

$$(x, y) = (0, y) = \left(0, -\frac{c+d}{a+b}\right)$$

En resumen, la ecuación de la forma $(a, b) \odot (x, y)^2 \oplus (c, d) \odot (x, y) \oplus = (0, 0)$, siempre tendrá una solución, la trivial $(x, y) = (0, 0)$, pero además existen otras soluciones, bajo ciertas condiciones en a, b, c y d. En la tabla 3.2 se establecen las condiciones y el conjunto de soluciones para cada caso.

Consideraciones sobre el producto $(m, n) \odot (p, q) = (0, 0)$	**Condiciones sobre** a, b, c **y** d	**Conjunto de soluciones en** ε
$(m, n) = (0, 0)$	Ninguna	$\{(0, 0)\}$
$(p, q) = (0, 0)$	$a \mid c$, $a = -b$ y $c = -d$	$\left\{\left(\frac{-c}{a}, y\right) \in \varepsilon : y \in \mathbb{Z}\right\}$
$(p, q) = (0, 0)$	$a \mid c$, $a \neq b$ y $c = -d$	$\left\{\left(-\frac{c}{a}, \frac{c}{a}\right)\right\}$
$(p, q) = (0, 0)$	$a \mid c$ y $(a + b) \mid (d + c)$	$\left\{\left(-\frac{c}{a}, -\frac{d+c}{a+b} + ac\right)\right\}$
$(m, n) = (m, -m)$ y $(p, q) = (0, q)$	$a \mid c$ y $c \neq -d$	$\left\{\left(-\frac{c}{a}, \frac{c}{a}\right)\right\}$
$(m, n) = (0, n)$ y $(p, q) = (p, -p)$	$a + b = 0 = c + d$	$\left\{\left(0, y\right) \in \varepsilon : y \in \mathbb{Z}\right\}$
$(m, n) = (0, n)$ y $(p, q) = (p, -p)$	$(a + b) \mid (c + d)$	$\left\{\left(0, -\frac{c+d}{a+b}\right)\right\}$

Cuadro 3.2: Condiciones sobre a, b, c y d para que en ε tenga solución la ecuación $(x, y)\big((a, b) \odot (x, y) \oplus (c, d)\big) = (0, 0)$.

Como se podrá evidenciar, si en la ecuación $(a, b) \odot (x, y)^2 \oplus (c, d) \odot (x, y) \oplus = (0, 0)$, se cumple que $a \mid c$ y $(a+b) \mid (d+c)$, entonces hay la ecuación tiene al menos tres soluciones, que son las que se enmarcan en la primera, segunda y cuarta fila de la tabla 3.2. Si cumple que $a \mid c$ y $c \neq -d$, se concluye que la ecuación tiene por lo menos dos soluciones, siendo las que se muestran en la primera y tercera fila, de la misma tabla. En general, se tiene que toda ecuación de dicha forma tiene por lo menos una solución (la trivial $(x, y) = (0, 0)$ y a lo sumo cuatro soluciones.

Teorema 3.3.1 *Toda ecuación de la forma*

$$(a, b) \odot (x, y)^2 \oplus (c, d) \odot (x, y) = (0, 0)$$

Tiene por lo menos una solución.

DEMOSTRACIÓN: Lo desarrollado previamente, valida el teorema. Evidenciándose que la solución trivial es $(x, y) = (0, 0)$.

Comparación xv de ε con $\mathbb{Z}$: De la misma forma que cuando se consideró las ecuación de la forma $(a, b) \odot (x, y) = (c, d)$ en ε se tiene que las ecuaciones de la forma $(a, b) \odot (x, y)^2 \oplus (c, d) \odot (x, y) = (0, 0)$ pueden no tener solución, tener solución única o tener infinitas soluciónes. En $\mathbb{Z}$ las ecuaciones cuadráticas tienen a lo sumos dos soluciones. Por lo cual, no hay posible analogía en la cantidad de soluciones de una ecuación.

Aunque una analogía evidente, es la consideración de la solución trivial en la ecuación $(a, b) \odot (x, y) = (c, d)$ en ε, pues esta es el módulo bajo la suma definida. De forma análoga sucede con las ecuaciones de la forma $mx^2 + nx = 0$ en el conjunto de los números enteros, pues la solución trivial es $x = 0$.

Ahora, considerando la ecuación de la forma

$$(a, b) \odot (x, y)^2 \oplus (c, d) \odot (x, y) \oplus (e, f) = (0, 0)$$

Bajo la suposición que $(a, b), (c, d)$ y (e, f) son diferentes de $(0, 0)$ se plantea la conjetura que la ecuación cuenta con a lo sumo cuatro soluciones, contando multiplicidades. Considerando la ecuación, claramente con $(a, b) \neq (0, 0)$, se tiene que

$$\begin{aligned}
(a, b) \odot (x, y)^2 \oplus (c, d) \odot (x, y) \oplus (e, f) &= (0, 0) \\
(a, b) \odot (x^2, (x + y)^2 - x^2) \oplus (cx, cy + cd + dy) \oplus (e, f) &= (0, 0) \\
\Big(ax^2, a\big((x + y)^2 - x^2\big) + bx^2 + b\big((x + y)^2 - x^2\big)\Big) \oplus (cx + e, cy + dx + dy + f) &= (0, 0) \\
\Big(ax^2 + cx + e, (a + b)\big((x + y)^2 - x^2\big) + bx^2 + cx + b(x + y) + f\Big) &= (0, 0)
\end{aligned}$$

Luego, la ecuación tiene solución si $ax^2 + cx + e = 0$ tiene solución en $\mathbb{Z}$. Si está última ecuación tiene solución, a lo sumo tendrá dos soluciones, llamémoslas x_1 y x_2. Estás dos soluciones estarían dadas por:

$$x_1 = \frac{-c + \sqrt{c^2 - 4ae}}{2a} \qquad \text{y} \qquad x_2 = \frac{-c - \sqrt{c^2 - 4ae}}{2a}$$

Ahora, se tiene que:

$$\begin{aligned}(a+b)\big((x+y)^2-x^2\big)+bx^2+cx+b(x+y)+f&=0\\(a+b)\big(\cancel{x^2}+2xy+y^2-\cancel{x^2}\big)+bx^2+cx+bx+by+f&=0\\y^2(a+b)+y(2ax+2bx+b)+(bx^2+cx+bx+f)&=0\end{aligned}$$

Se evidencia en esta última línea una ecuación cuadrática. Por lo cual a lo sumo tendrá dos soluciones. Al estar estas soluciones en términos de x, quien al tomar dos valores x_1 y x_2, permite concluir un total de cuatro soluciones, dos en términos de x_1 y las otras dos, en términos de x_2.

- Considerando primero la solución x_1 se tiene que:

$$y^2(a+b)+y(2ax_1+2bx_1+b)+({bx_1}^2+cx_1+bx_1+f)=0$$

  Considerando $A=a+b$, $B_{x_1}=2ax_1+2bx_1+b$ y $C_{x_1}={bx_1}^2+cx_1+bx_1+f$, se tiene que, de existir, las soluciones estarían dadas por:

$$y_1=\frac{-B_{x_1}+\sqrt{{B_{x_1}}^2-4AC_{x_1}}}{2A}\qquad\text{y}\qquad y_2=\frac{-B_{x_1}-\sqrt{{B_{x_1}}^2-4AC_{x_1}}}{2A}$$

- Analogamente considerando la solución x_2 se tiene que, las dos soluciones en y estarán dadas por:

$$y_3=\frac{-B_{x_2}+\sqrt{{B_{x_2}}^2-4AC_{x_2}}}{2A}\qquad\text{y}\qquad y_4=\frac{-B_{x_2}-\sqrt{{B_{x_2}}^2-4AC_{x_2}}}{2A}$$

  Donde $A=a+b$, $B_{x_2}=2ax_2+2bx_2+b$ y $C_{x_2}={bx_2}^2+cx_2+bx_2+f$.

Concluyendo así, que la ecuación, de tener solución, a lo sumo ha de tener cuatro soluciones. Siendo estas:

- $w_1=(x_1,y_1)$
- $w_2=(x_1,y_2)$
- $w_2=(x_2,y_3)$
- $w_4=(x_2,y_4)$

Se evidencia que, la ecuación $(a,b) \odot (x,y)^2 \oplus (c,d) \odot (x,y) \oplus (e,f) = (0,0)$ tiene a lo sumo cuatro soluciones, pero en contraste con el teorema 3.3.1, se tiene que no se puede asegurar la existencia de por lo menos una solución independientemente de los valores de (a,b), (c,d) y (e,f). Y esto sucede si la ecuación $ax^2 + cx + e = 0$ no tiene solución en $\mathbb{Z}$.

Comparación xvi de ε con $\mathbb{Z}$: En general, las ecuaciones de la forma $(a,b) \odot (x,y)^2 \oplus (c,d) \odot (x,y) \oplus (e,f) = (0,0)$ no se parecen a las ecuaciones de la forma $mx^2 + px + q = 0$ consideradas en $\mathbb{Z}$. Por ejemplo, si $(e,f) = (0,0)$, $a + b = 0 = c + d$, se concluye que existen infinitas soluciones en ε que satisfacen la ecuación. Dichas soluciones son de la forma $(0,y)$, para cualquier $y \in \mathbb{Z}$. En contraparte, las ecuaciones cuadráticas en $\mathbb{Z}$ a lo sumo tienen dos soluciones.

Capítulo 4

Divisibilidad en ε

En el conjunto $\mathbb{Z}$ se dice que a divide a b, si existe $c \in \mathbb{Z}$ tal que $ac = b$. De existir $c \in \mathbb{Z}$, que satisfaga $ac = b$, se tiene que este es único. De esto se tiene que a y c son divisores de b, lo cual es equivalente a decir que b es múltiplo de a y de c [5, p. 70]. Con base en esta definición de la relación de divisibilidad en $\mathbb{Z}$, se definirá de forma análoga la relación de divisibilidad en ε.

Definición 4.0.1 *Sean $(a,b),(c,d) \in \varepsilon$ se dice que (a,b) divide a (c,d) si y solo si existe*[1] *$(e,f) \in \varepsilon$ tal que $(a,b) \odot (e,f) = (c,d)$. Está relación se notará como $(a,b)|(c,d)$.*

Teorema 4.0.1 *Sean $(a,b),(c,d) \in \varepsilon$. Si $(a,b) \mid (c,d)$ entonces $(a,b) \mid \big((c,d) \odot (e,f)\big)$, para todo $(e,f) \in \varepsilon$.*

Demostración: Como $(a,b) \mid (c,d)$, existe $(p,q) \in \varepsilon$ tal que $(a,b) \odot (p,q) = (c,d)$. Ahora, considérese:

$$(c,d) \odot (e,f) = \big((a,b) \odot (p,q)\big) \odot (e,f)$$
$$(c,d) \odot (e,f) = (a,b) \odot \big((p,q) \odot (e,f)\big)$$

Como $(p,q) \odot (e,f) \in \varepsilon$, se cumple que $(a,b) \mid \big((c,d) \odot (e,f)\big)$.

Teorema 4.0.2 *Sean $(a,a_1),(b,b_1),(c,c_1) \in \varepsilon$. Si $(a,a_1) \mid (b,b_1)$ y $(a,a_1) \mid (c,c_1)$ entonces $(a,a_1) \mid (d,d_1) \odot (b,b_1) \oplus (e,e_1) \odot (c,c_1)$, para todo $(d,d_1),(e,e_1) \in \varepsilon$.*

[1] La existencia, no es argumento suficiente para decir que dicho elemento es único. En posteriores secciones, se evidenciará si se cumple que este elemento es único o no.

DEMOSTRACIÓN: Por teorema anterior, se cumple que $(a, a_1) \mid (d, d_1) \odot (b, b_1)$ y $(a, a_1) \mid (e, e_1) \odot (c, c_1)$, para todo $(d, d_1), (e, e_1) \in \varepsilon$. Luego existen $(m, m_1), (n, n_1) \in \varepsilon$, tal que $(a, a_1) \odot (m, m_1) = (d, d_1) \odot (b, b_1)$ y $(a, a_1) \odot (n, n_1) = (e, e_1) \odot (c, c_1)$. Considerando la suma de estos elementos, se tiene que:

$$(a, a_1) \odot (m, m_1) \oplus (a, a_1) \odot (n, n_1) = (d, d_1) \odot (b, b_1) \oplus (e, e_1) \odot (c, c_1)$$
$$(a, a_1) \odot \big((m, m_1) \oplus (n, n_1)\big) = (d, d_1) \odot (b, b_1) \oplus (e, e_1) \odot (c, c_1)$$

Como $(m, m_1) \oplus (n, n_1) \in \varepsilon$, se concluye que $(a, a_1) \mid (d, d_1) \odot (b, b_1) \oplus (e, e_1) \odot (c, c_1)$.

Comparación xvii de ε con $\mathbb{Z}$: Sean $a, b \in \mathbb{Z}$ se denomina combinación lineal [5, p. 71] de a y b, a $\alpha a + \beta b$, para cualquiera $\alpha, \beta \in \mathbb{Z}$. Si $c \mid a$ y $c \mid b$ se infiere que c divide cualquier combinación lineal de a y b. Los dos últimos teoremas evidencian que ocurre de manera análoga en ε.

Ejemplo 4.0.1 *Determine un múltiplo de* $(5, 8)$ *como combinación lineal de* $(15, 50)$ *y* $(40, 103)$.

SOLUCIÓN: Por teorema 3.2.8, se demuestra que existe un único $(c, d) \in \varepsilon$ tal que $(5, 8) \odot (c, d) = (15, 12)$ puesto que $5 \mid 15$, $5 \neq -8$ y $(5 + 8) = 13 \mid 65 = 15 + 50$. Luego se verifica que $(5, 8) \mid (15, 50)$ De forma análoga se verifica que $(5, 8) \mid (40, 103)$. Luego, por teorema 4.0.2 se tiene que $(5, 8)$ divide cualquier combinación lineal de $(15, 50)$ y $(40, 103)$. Especificamente $(1, 0) \odot (15, 50) \oplus (-1, 0) \odot (40, 103) = (-25, -53)$.

Teorema 4.0.3 *La relación de divisibilidad en* ε *es reflexiva.*

DEMOSTRACIÓN: Para todo $(a, b) \in \varepsilon$ se tiene que existe (1,0), tal que $(a, b) \odot (1, 0) = (a, b)$. Con lo cual se demuestra que $(a, b) | (a, b)$.

Teorema 4.0.4 *La relación de divisibilidad en* ε *es transtiva.*

DEMOSTRACIÓN: Sean $(a, b), (c, d), (e, f) \in \varepsilon$. Si $(a, b) \mid (c, d)$ y $(c, d) \mid (e, f)$, entonces existen (m, n), $(p, q) \in \varepsilon$ tal que:

$$(a, b) \odot (m, n) = (c, d)$$
$$(c, d) \odot (p, q) = (e, f)$$

De lo cual se tiene que:

$$\begin{array}{rcll} (a,b)\odot(m,n) & = & (c,d) & \text{Definición de divisibilidad en } \varepsilon \\ \Big((a,b)\odot(m,n)\Big)\odot(p,q) & = & (c,d)\odot(p,q) & \text{Monotonía del producto en } \varepsilon \\ (a,b)\odot\Big((m,n)\odot(p,q)\Big) & = & (c,d)\odot(p,q) & \text{Asociativa del producto en } \varepsilon \\ (a,b)\odot\Big((m,n)\odot(p,q)\Big) & = & (e,f) & \text{Definición de divisibilidad en } \varepsilon \end{array}$$

Dado que $\odot$ es una operación bien definida en ε se tiene que $(m,n)\odot(p,q)\in\varepsilon$. Por lo tanto, $(a,b)\mid(e,f)$. Concluyendo así que la relación de divisibilidad en ε es transitiva.

Es fácil mostrar que, en general, la relación de divisibilidad en ε no es simétrica. Para que la relación sea simétrica debería cumplirse que dados dos elementos de ε si se tiene que uno divide al otro, entonces en sentido contrario también hay divisibilidad; es decir, para todo $(a,b),(c,d)\in\varepsilon$ si $(a,b)\mid(c,d)$ entonces $(c,d)\mid(a,b)$ Según la definición sabemos que la dupla $(3,5)$ divide a $(0,8)$, ya que:

$$\begin{aligned}(3,5)\odot(0,1) &= (0,0+3+5)\\ &= (0,8)\end{aligned}$$

Sin embargo, no se tiene que $(0,8)$ divida a $(3,5)$ ya que cualquier elemento (m,n) de ε al multiplicarse con $(0,8)$ dará como resultado $(0m,8m+0n+8n)=(0,8m+8n)$ cuya primera componente siempre será cero. Por lo tanto, es imposible encontrar un elemento tal que su producto con $(0,8)$ de como resultado $(3,5)$. Luego, la relación no es simétrica. Lo cual tiene como consecuencia que la relación de divisibilidad en ε no sea una relación de equivalencia.

Por otra parte, podría pensarse entonces que cumple la antisimetría. Para que la relación sea antisimétrica deberia cumplirse que para todo par de elementos de ε si se dividen mutuamente entonces estos resultan ser el mismo elemento; es decir, para todo $(a,b),(c,d)\in\varepsilon$, si $(a,b)\mid(c,d)$ y $(c,d)\mid(a,b)$ entonces $(a,b)=(c,d)$.

Si tomamos los elementos $(-4,7)$ y $(-4,1)$ se tiene que: $(-4,7)\odot(1,-2)=(-4,8+7-14)=(-4,1)$ y además $(-4,1)\odot(1,-2)=(-4,-8+1-2)=(-4,7)$. Pero, $(-4,7)$ y $(-4,1)$ son distintos. Por lo tanto, la relación no es antisimétrica. Lo cual tiene como consecuencia que la relación de divisibilidad en ε no sea una relación de orden.

Comparación xviii de ε con $\mathbb{Z}$: La relación de divisibilidad, tanto en ε como en $\mathbb{Z}$, cumple que es reflexiva y transitiva, pero no es simétrica, ni antisimétrica.

4.1. Algoritmo de la división en ε

Sean $a, b \in \mathbb{Z}$, con $b > 0$ el cual se denominará divisor, el teorema del algoritmo de la división determina que existe un único residuo r, que satisface que $0 \leq r < b$, y un único cociente q tal que $bq + r = a$. La demostración de este teorema se puede evidenciar en cualquiera texto de teoría de números, como por ejemplo [5, pp. 65,66], haciendo la demostración en dos partes: demostrando la existencia y demostrando la unicidad de dichos elementos. Aunque se hace evidente, se debe presente que a puede ser igual a 0, pues no hay restricción alguna, esto se menciona, pues será muy útil posteriormente.

Sean $(a, b), (c, d) \in \varepsilon$ no se puede definir un teorema análogo al teorema del algoritmo de la división en $\mathbb{Z}$, esto debido a que no se puede ordenar al conjunto ε; es decir, no se puede precisar si (c, d) es menor o igual a $(0, 0)$ o si es mayor o igual. La demostración que en el conjunto ε no se puede definir una relación de orden compatible con las operaciones definidas, sigue los mismos argumentos que se usaron en el teorema 1.2.2, donde se mostró que en el conjunto $\mathbb{J}$ no existe un conjunto de números positivos.

Se debe tener presente que $\mathbb{Z} \subset \varepsilon$, y preguntarse si al considerar los elementos de $\mathbb{Z}$ en ε se sigue cumpliendo la existencia y unicidad del cociente y residuo para $a, b \in \mathbb{Z}$, con $b > 0$. Los dos siguientes teoremas responderán esto.

Teorema 4.1.1 *Sean $(a, 0), (b, 0) \in \varepsilon$ con $b > 0$, existen unos únicos $(q, q_1), (r, r_1) \in \varepsilon$, con $0 \leq r < b$ y $0 \leq r_1 < b$, tal que* [II] $(b, 0) \odot (q, q_1) \oplus (r, r_1) = (a, 0)$.

Demostración: Por el algoritmo de la división en $\mathbb{Z}$ se asegura que existen únicos q y r, satisfaciendo que $0 \leq r < b$, tal que $bq + r = a$. De manera análoga, se asegura que existen únicos q_1 y r_1, satisfaciendo que $0 \leq r_1 < b$, tal que $bq_1 + r_1 = 0$. Por definición 1.0.1, se

[II] Siguiendo las definiciones en $\mathbb{Z}$, se dirá que $(a, 0)$ corresponde al dividendo, $(b, 0)$ al divisor, (q, q_1) el cociente y (r, r_1) el residuo.

cumple que:

$$(bq + r, bq_1 + r_1) = (a, 0)$$
$$(bq, bq_1) \oplus (r, r_1) = (a, 0)$$
$$(b, 0) \odot (q, q_1) \oplus (r, r_1) = (a, 0)$$

Concluyendo que (q, q_1) y (r, r_1), pues q, q_1, r y r_1 toman valores únicos en $\mathbb{Z}$,verificándose que $q_1 = 0$ y $r_1 = 0$. Concluyendo así la demostración.

Ejemplo 4.1.1 *Sean* $(5, 0)$ *y* $(2, 0)$*, con base en el teorema anterior determine los* $(q, q_1)(r, r_1) \in \varepsilon$*, con* $0 \leq r < 2$ *y* $0 \leq r_1 < 2$*, tal que* $(2, 0) \odot (q, q_1) \oplus (r, r_1) = (5, 0)$

Solución: Con base en el teorema 4.1.1, se tiene que existen únicos elementos $(q, q_1)(r, r_1) \in \varepsilon$ que satisfacen que $(2, 0) \odot (q, q_1) \oplus (r, r_1) = (5, 0)$. Con el apoyo del teorema del algoritmo de la división en $\mathbb{Z}$ se tiene que $q = 2$ y $r = 1$, pues $2 \cdot 2 + 1 = 5$. De la misma forma $q_1 = 0$ y $r_1 = 0$ pues $2 \odot 0 + 0 = 0$. Concluyendo así que $(q, q_1) = (2, 0)$ y que $(r, r_1) = (1, 0)$. Verificándose que $(2, 0) \odot (2, 0) \oplus (1, 0) = (5, 0)$

Con base en el teorema anterior, se muestra que considerando en ε los elementos cuya segunda componente fuera cero, se cumple un teorema análogo al algoritmo de la división en $\mathbb{Z}$. Apresurando las cosas, se diría que al considerar a los elementos de $\mathbb{Z}$ en ε se sigue cumpliendo el algoritmo de la división, pero esto es falso. Si se hace una revisión detallada, se tiene que $a, b \in \mathbb{Z}$ por lo tanto, existen únicos q y r, satisfaciendo que $0 \leq r < b$, tal que $bq + r = a$. Pero, ¿por qué se incluyó en el teorema anterior la condición que $0 \leq r_1 < b$? si r_1 es la segunda componente de un elemento en ε; es decir, el teorema está incluyendo condiciones sobre elementos que no son de $\mathbb{Z}$. El siguiente teorema demostrará que aún considerando elementos de $\mathbb{Z}$, no se cumple un algoritmo de la división en ε, si se excluye la condición que $0 \leq r_1 < b$.

Teorema 4.1.2 *Sean* $(a, 0), (b, 0) \in \varepsilon$ *con* $b > 0$*, existen infinitos* $(q, q_1), (r, r_1) \in \varepsilon$*, con* $0 \leq r < b$*, tal que* $(b, 0) \odot (q, q_1) \oplus (r, r_1) = (a, 0)$.

Demostración: Para asegurar la existencia de los elementos en ε, se hace consideración similar a la del teorema anterior. El argumento para asegurar que q y r son únicos, se debe al teorema del algoritmo de la división en $\mathbb{Z}$. Pero, por otro lado, se se tiene que

$bq_1 + r_1 = 0$, se infiere que q_1 puede tomar cualquier valor en $\mathbb{Z}$ y que $r_1 = -bq_1$. De lo cual se tiene que existen infinitos $q_1, r_1 \in \mathbb{Z}$ que satisfacen que $bq_1 + r_1 = 0$, luego

$$(b, 0) \odot (q, q_1) \oplus (r, -bq_1) = (a, 0)$$

Concluyendo así, que existen infinitos $(q, q_1), (r, -bq_1) \in \varepsilon$, con $0 \leq r < b$, tal que $(b, 0) \odot (q, q_1) \oplus (r, -bq_1) = (a, 0)$.

Ejemplo 4.1.2 *Considere nuevamente el ejemplo 4.1.1, sin tener en cuenta la condición que* $0 \leq r_1 < b$.

SOLUCIÓN: Con base en el último teorema, se tiene que existen infinitos $(q, q_1), (r, r_1) \in \varepsilon$, con $0 \leq r < 2$, tal que $(2, 0) \odot (q, q_1) \oplus (r, r_1) = (5, 0)$. Se tiene que el cociente y el residuo están dados por:

$$(2, q_1) \text{ y } (1, -2q_1), \text{ para } q_1 \in \mathbb{Z}$$

Como se ha establecido, la diferencia entre los dos últimos teoremas, radica en considerar la restricción sobre r_1. Si $0 \leq r_1 < b$ se cumple que se puede hablar de un teorema en ε, análogo al algoritmo de la división en $\mathbb{Z}$, que asegura existencia y unicidad. Si por el contrario, se parte r_1 puede tomar cualquier valor en $\mathbb{Z}$ se cumple un teorema en ε, análogo al algoritmo de la división en $\mathbb{Z}$, que asegura existencia, pero no unicidad.

Ahora, qué sucede si se considera $(a, b), (c, d) \in \varepsilon$, con $b \neq 0$ o $d \neq 0$; es decir, considerar dos elementos en ε de tal forma que por lo menos uno de los dos tiene su segunda componente diferente de cero. ¿Qué condiciones deben cumplir (a, b) y (c, d), para que se cumpla en ε un teorema análogo al algoritmo de la división en $\mathbb{Z}$? ¿Será que existen $(e, f), p, q) \in \varepsilon$ tal que: $(e, f) \odot (c, d) \oplus (p, q) = (a, b)$? ¿Estos elementos serán únicos. Operando, se tiene que:

$$(e, f) \odot (c, d) \oplus (p, q) = (a, b)$$
$$(ec + p, fc + fd + ed + q) = (a, b)$$

Por definición 1.0.1, se tiene que: $ec + p = a$ y $fc + fd + ed + q = b$. Para asegurar que e y c existan y sean únicos, se recurre al algoritmo de la divisibilidad y por ende, se debe condicionar a que $c > 0$ y $0 \leq p < c$. Pero con la igualdad $fc + fd + ed + q = b$, qué condiciones se deben fijar, para que f y q existan y sean únicos? La igualdad se puede

expresar como:

$$\begin{aligned} b &= fc + fd + ed + q \\ b &= d(f+e) + fc + q + ce - ce \\ b &= d(f+e) + c(f+e) + q - ce \\ b + ce &= (d+c)(f+e) + q \\ q &= b + ce - (d+c)(f+e) \end{aligned}$$

Bajo la condiciones propuestas anteriormente, se tiene que e toma un único valor y este se puede determinar con el algoritmo de la división en $\mathbb{Z}$. Se asegura que existen f y q que satisfacen la igualdad $(e,f) \odot (c,d) \oplus (p,q) = (a,b)$, basta con considerar $f = 0$ y $q = b + ce$. Pero, tanto f como q toman infinitos valores, incluso si $c = -d$, quedando que f es cualquier valor en $\mathbb{Z}$ y $q = b + ce$.

Con estos argumentos, se concluye que considerar un algoritmo de la división en ε no es posible, pues se aguera existencia de cociente y residuo, pero no la unicidad, ni siquiera una cantidad finita de posibles residuos y cocientes.

Comparación xix de ε con $\mathbb{Z}$: En $\mathbb{Z}$ se cumple el teorema del algoritmo de la división, el cual asegura que para todo $a, b \in \mathbb{Z}$, con $b > 0$, existen unos únicos q y r, con $0 \leq r < b$, tal que $bq + r = a$. Dado que los elementos de ε no se pueden ordenar, no se habla de un $(c,d) \in \varepsilon$ tal que este sea mayor a (0,0), tal que $(e,f) \odot (c,d) \oplus (p,q) = (a,b)$ con $(e,f), (p,q) \in \varepsilon$ como cociente y residuo respectivamente, con (p,q) menor que (c,d). Incluso obviando el hecho que no existe orden en ε, no se asegura un teorema en ε análogo al teorema del algoritmo de la división en $\mathbb{Z}$, pues solo se asegura la existencia, más no la unicidad.

4.2. Una relación de equivalencia en ε

En $\mathbb{Z}$ bajo la relación de divisibilidad usual es reflexiva y transitiva, pero no es antisimétrica (pues $5 \mid -5$ y $-5 \mid 5$, pero $5 \neq -5$) y no es simétrica (pues $1 \mid 5$, pero $5 \nmid 1$). Igualmente sucede en ε, la relación de divisibilidad definida solo cumple la reflexividad y la transtividad. Pero considerando una nueva relación $\star$ en $\mathbb{Z}$ tal que para $a, b \in \mathbb{Z}$ se cumple que $a \star b$ si y solo si $a|b$ y $b|a$. Esta nueva relación resulta ser una relación de

equivalencia[III], teniendo que para $a \in \mathbb{Z}$ la clase del a, notada como $[a]$, está dada por:

$$[a] = \{a, -a\}$$

Teniendo que todas las clases tienen dos elementos, excepto la clase del 0, que es la clase con un solo elemento. Todo esto da pie para considerar a los elementos a y $-a$ como un solo elemento, siendo este $[a]$. A partir de ello, se define una relación de divisibilidad entre las clases de $\mathbb{Z}/\star$, siendo:

$$[a] \parallel [b] \text{ sii existe } [c] \text{ tal que } [a][c] = [b]$$

Definiendo el producto de las clases como la clase del producto de sus representantes, siendo dicha operación bien definida. Dando paso así, al estudio de una relación de divisibilidad que sea de orden y posteriormente hablar del teorema fundamental de la Aritmética, en adelante abreviado como TFA.

Con base en ello, se define una nueva relación $\diamond$ en ε.

Definición 4.2.1 *Sean $(a,b),(c,d) \in \varepsilon$ se dice que $(a,b) \diamond (c,d)$ si y solo si $(a,b)|(c,d)$ y $(c,d)|(a,b)$.*

Teorema 4.2.1 *La relación $\diamond$ es de equivalencia.*

Demostración: Para que una relación sea de equivalencia, esta debe ser reflexiva simétrica y transtiva.

- **Reflexividad:** Sea $(a,b) \in \varepsilon$ por teorema 4.0.3 se tiene que $(a,b)|(a,b)$, por ende $(a,b) \diamond (a,b)$.
- **Simetría:** Sean $(a,b),(c,d) \in \varepsilon$ tal que $(a,b) \diamond (c,d)$. Por definición se da que:

$$(a,b)|(c,d) \wedge (c,d)|(a,b)$$
$$(c,d)|(a,b) \wedge (a,b)|(c,d)$$

[III]En la teoría de anillos, se determinan estas clases a partir de los asociados. En un dominio integro D, dos elementos $a, b \in D$ son asociados [4, p. 291] si $a = bu$ para alguna unidad u de D. Para todo $c \in \mathbb{Z}$ sus asociados serán c y $-c$, pues las unidades de $\mathbb{Z}$ son 1 y -1. No se tomó una definición de asociados en ε debido a que este conjunto no es un dominio integro y se intenta que toda definición en ε sea fiel a la definición análoga. Por ello, la ruta que se ha tomado, es la de considerar los elementos que se dividen mutuamente.

Este último argumento se valida con el auxilio de la tautología $p \wedge q \longleftrightarrow q \wedge p$. De lo cual se infiere que $(c,d) \diamond (a,b)$.

- **Transitividad:** Sean $(a,b),(c,d),(e,f) \in \varepsilon$. Si $(a,b) \diamond (c,d)$ y $(c,d) \diamond (e,f)$, entonces se cumple que :

$$(a,b) \mid (c,d) \tag{4.1}$$

$$(c,d) \mid (a,b) \tag{4.2}$$

$$(c,d) \mid (e,f) \tag{4.3}$$

$$(e,f) \mid (c,d) \tag{4.4}$$

Por teorema 4.0.4 se tiene que de (4.1) y (4.3) se concluye que $(a,b) \mid (e,f)$. Análogamente, por (4.4) y (4.2) se concluye que $(e,f)|(a,b)$. Demostrando así que $\diamond$ es transitiva.

Finalmente, se concluye que la relación $\diamond$ es una relación de equivalencia.

Dado que $\diamond$ es una relación de equivalencia, esta relación genera una partición en el conjunto ε [4, p. 5]. Y por la defínción de $\diamond$, dos elementos de ε pertenecen a la misma clase, si se dividen mutuamente. La pregunta natural a responder es: ¿Cómo determinar los elementos de la clase de (a,b)? Lo que sigue, responderá a esta interrogante.

Se debe tener en cuenta que los conjuntos $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ y $\{(0,0)\}$ son disyuntos dos a dos, esto por teorema 2.1.14. Por lo cual se determinará la $[(a,b)]$, partiendo del hecho que (a,b) solo puede pertenecer exclusivamente a uno de los tres conjuntos previamente mencionados. Bajo este razonamiento siguen surgiendo preguntas, como por ejemplo, ¿Si $(a,b) \in \mathfrak{D}(\varepsilon)$, todos los elementos de $[(a,b)]$ pertenecerán a $\mathfrak{D}(\varepsilon)$?

4.2.1. La clase del $(0,0)$

El elemento $(0,0)$ es el módulo bajo la operación $\oplus$ en ε (y también en $\mathbb{J}$). Para cualquier $(a,b) \in \varepsilon$ se cumple que $(a,b) \odot (0,0) = (0,0)$. Bajo la definición de divisibilidad $(a,b) \mid (0,0)$. Pero, ¿cuál será la $[(0,0)]$? El siguiente teorema determinará esto.

Teorema 4.2.2 *La* $[(0,0)] = \{(0,0)\}$.

DEMOSTRACIÓN: Se cumple que $(0,0) \in [(0,0)]$[IV]. Ahora, supóngase un elemento $(a,b) \in \varepsilon$, $(a,b) \neq (0,0)$. Si $(a,b) \in [(0,0)]$ se cumpliría que $(0,0)|(a,b)$, pero esto no es posible, dado que no existe $(x,y) \in \varepsilon$ tal que $(x,y) \odot (0,0) = (a,b)$, pues $(x,y) \odot (0,0) = (0,0)$ para todo elemento $(x,y) \in \varepsilon$. Por lo cual se concluye que $(0,0)$ el único elemento de $[(0,0)]$.

4.2.2. La clase del (a,b) con $(a,b) \in \varepsilon^* - \mathfrak{D}(\varepsilon)$

Sea $(a,b) \in \varepsilon^* - \mathfrak{D}(\varepsilon)$ se cumple que $a \neq 0$ y $a \neq -b$, esto por definición. Pero, el lema 2.1.13, establece que $\mathfrak{U}(\varepsilon) \subset \varepsilon^* - \mathfrak{D}(\varepsilon)$. Por lo cual, un punto de partida, es considerar la clase de alguna unidad de ε. Comparando esta situación con $\mathbb{Z}$, se cumple que en $\mathbb{Z}$ las unidades pertenecen a la misma clase, pues estas son 1 y -1. El siguente teorema, mostrará que, de forma análoga a $\mathbb{Z}$ todas las unidades de ε pertenecen a la misma clase.

Teorema 4.2.3 *Bajo la relación $\diamond$, la $[(1,0)]$ es el conjunto $\mathfrak{U}(\varepsilon)$.*

DEMOSTRACIÓN: Para demostrar que $[(1,0)] = \mathfrak{U}(\varepsilon)$ se debe asegurar que todo elemento de la clase de equivalencia pertenece al conjunto de las unidades de ε, y que todo elemento del conjunto de las unidades de ε pertenece a la clase de equivalencia.

- Con base en el teorema 2.1.9 se tiene que $(\mathfrak{U}(\varepsilon), \odot)$ es grupo conmutativo. Por ende, para todo $u \in \mathfrak{U}(\varepsilon)$ se cumple que $w \odot x = (1,0)$ tiene solución y como $w \odot (1,0) = w$, se infiere que $w|(1,0)$ y $(1,0)|w$, concluyendo que $w \diamond (1,0)$. Por lo tanto $w \in [(1,0)]$.
- Sea $(c,d) \in [(1,0)]$, por ende $(c,d)|(1,0)$ es decir, (c,d) es una unidad.

Teorema 4.2.4 *Para todo $(a,b) \in \varepsilon$, con $a \neq 0$ y $a \neq -b$, se cumple que*

$$[(a,b)] = \{(a,b) \odot u : u \in \mathfrak{U}(\varepsilon)\}$$

DEMOSTRACIÓN:

[IV] Sea R una relación de equivalencia, sobre un conjunto A no vacío. Sean $a, b \in A$ se cumple que [7, p.110]:

- $a \in [a]$.
- Son equivalentes las siguientes tres afirmaciones:
  - aRb
  - $a \in [b]$
  - $[a] = [b]$.

- Sea $(c,d) = (a,b) \odot u$ con $u \in \mathfrak{U}(\varepsilon)$. Con base en la tabla 2.1 se evidencia que se cumple que $u \odot u = (1,0)$ para todo $u \in \mathfrak{U}(\varepsilon)$. Por tanto: $(c,d) \odot u = \big((a,b) \odot u\big) \odot u = (a,b)$. De lo cual se tiene que $(a,b)|(c,d)$ y $(c,d)|(a,b)$. Lo que implica que $(c,d) \diamond (a,b)$, concluyendo que $(c,d) \in [(a,b)]$.

- Sea $(c,d) \in [(a,b)]$, por tanto $(c,d) \diamond (a,b)$. De lo anterior se tiene que $(c,d)|(a,b)$ y $(a,b)|(c,d)$, lo cual significa que existen $(m,n),(o,p) \in \varepsilon$ tal que:

$$(a,b) = (c,d) \odot (m,n) \quad \text{y} \quad (c,d) = (a,b) \odot (o,p)$$

Sustituyendo el valor de (c,d) en $(a,b) = (c,d) \odot (m,n)$ se tiene que:

$$\begin{aligned} (a,b) &= (c,d) \odot (m,n) \\ (a,b) &= \Big((a,b) \odot (o,p)\Big) \odot (m,n) \\ (a,b) \odot (1,0) &= (a,b) \odot \Big((o,p) \odot (m,n)\Big) \\ (1,0) &= (o,p) \odot (m,n) \end{aligned}$$

Dándose la cancelación de (a,b) debido a que $a \neq -b$ y consecuencia del teorema 2.1.11. Por lo tanto, al ser $(1,0) = (o,p) \odot (m,n)$, se tiene que $(o,p),(m,n) \in \mathfrak{U}(\varepsilon)$ luego (c,d) es expresado como producto de (a,b) y un elementos de $\mathfrak{U}(\varepsilon)$.

Concluyendo así la demostración.

Corolario 4.2.1 *Sea $(a,0) \in \varepsilon$ con $a \neq 0$, se cumple que*

$$[(a,0)] = \{(a,0),(-a,0),(a,-2a),(-a,2a\}$$

Demostración: Consecuencia directa del teorema anterior, siendo un caso particular, dado que la segunda componente del elemento en ε es cero.

Con base en el corolario anterior se tiene que para cualquier elemento $z \in \mathbb{Z}$ con $z \neq 0$, este divide a elementos en ε que no están en $\mathbb{Z}$. En la tabla 4.1, se evidencian algunos ejemplos de esto.

Teorema 4.2.5 *Para todo $(a,b) \in \varepsilon$, con $a \neq 0$ y $a \neq -b$, se cumple que $c \neq 0$ y $c \neq -d$ para todo $(c,d) \in [(a,b)]$.*

(a,b)	$(a,b)\odot(1,-2)$	$(a,b)\odot(-1,2)$
(1 , 0)	(1 , -2)	(-1 , 2)
(2 , 0)	(2 , -4)	(-2 , 4)
(3 , 0)	(3 , -6)	(-3 , 6)
(4 , 0)	(4 , -8)	(-4 , 8)
(5 , 0)	(5 , -10)	(-5 , 10)
(6 , 0)	(6 , -12)	(-6 , 12)
(7 , 0)	(7 , -14)	(-7 , 14)

Cuadro 4.1: Algunos elementos en $\mathbb{Z}$ y sus múltiplos $(c,d)\in\varepsilon$ con $(c,d)\notin\mathbb{Z}$.

Demostración: El teorema 2.1.9 determina que el conjunto de $\mathfrak{U}(\varepsilon)$ es de cuatro elementos. El teorema 4.2.4 dice que todo elemento $(c,d)\in$ **(a,b)** se puede expresar como producto de (a,b) y un elemento $u\in\mathfrak{U}(\varepsilon)$. La demostración del teorema, se hará por revisión exhaustiva, teniendo en cuenta que si $a\neq 0$ entonces $-a\neq 0$. Luego, sea $(a,b)\in\varepsilon$, con $a\neq 0$ y $a\neq -b$, se cumple que

- Si $u=(1,0)$, se tiene que $(a,b)\odot u=(a,b)=(c,d)$. Por tanto $a=c$ y $b=d$, luego se cumple que $c\neq 0$ y $c\neq -d$.
- Si $u=(1,-2)$, luego $(a,b)\odot u=(a,-2a-b)=(c,d)$. Se tiene que $a\neq -b$ luego $2a\neq -b+a$, por tanto $a\neq 2a+b=-(-2a-b)$. Concluyendo así que $c\neq 0$ y $c\neq -d$.
- Si $u=(-1,0)$, se tiene que $(a,b)\odot u=(-a,-b)=(c,d)$. De lo cual se tiene que $-a=c$ y $-b=d$. Como $a\neq -b$ se tiene que $-a\neq b$. Concluyendo así, que $c\neq 0$ y $c\neq -d$.
- Si $u=(-1,2)$, luego $(a,b)\odot u=(-a,2a+b)=(c,d)$. Como se ha demostrado en un ítem previo que $a\neq 2a+b$ se cumple que $-a\neq -(2a+b)$. Concluyendo así que $c\neq 0$ y $c\neq -d$.

Comparación xx de ε con $\mathbb{Z}$: En sintesis, se tiene que para $(a,b)\in\varepsilon^*-\mathfrak{D}(\varepsilon)$ se cumple que para todo $(c,d)\in[(a,b)]$, es cierto que $(c,d)=(a,b)\odot u$ para algún $u\in\mathfrak{U}(\varepsilon)$ y además $(c,d)\in\varepsilon^*-\mathfrak{D}(\varepsilon)$. Esto sucede de forma análoga en $\mathbb{Z}$.

4.2.3. La clase del (a,b) con $(a,b)\in\mathfrak{D}(\varepsilon)$

Por teorema 2.1.10 se tiene que:

$$\mathfrak{D}(\varepsilon) = \{(a,b) \in \varepsilon - \{(0,0)\} : a = 0 \vee a + b = 0\}$$

De lo anterior, se tiene que los divisores del $(0,0)$ son aquellos elementos $(a,b) \in \varepsilon$ con $(a,b) \neq (0,0)$ que cumplen que su primera componente es igual a cero o que su primera componente es el inverso aditivo (en $\mathbb{Z}$) de la segunda componente. Por lo cual, se ha de determinar las $[(m,-m)]$ y $[(0,n)]$, con $(m,-m),(0,n) \in \mathfrak{D}(\varepsilon)$.

Teorema 4.2.6 *Para todo $(a,b) \in \varepsilon$, si $a = -b$, $(a,b) \neq (0,0)$ se tiene que*

$$[(a,-a)] = \{(a,-a),(-a,a)\}$$

Demostración: Sea $(c,d) \in [(a,-a)]$. De esto, considerando que $[(a,-a)]$ es una clase de equivalencia, se dice que $(a,-a) \in [(c,d)]$ Supongamos que $c \neq -d$. Por ende, por teorema 4.2.5, se tiene que $a \neq -(-a)$, pero esto es falso. Por lo tanto, todos los elementos $(c,d) \in [(a,-a)]$ cumplen que $c = -d$.

Como $c = -d$ se tiene que $(c,-c) \in [(a,-a)]$, de lo cual se dice que $(c,-c)|(a,-a)$ y $(a,-a)|(c,-c)$. De acuerdo a la definición de relación de divisibilidad en ε, se tiene que existen $(x,y),(x',y') \in \varepsilon$ tal que $(a,-a) \odot (x,y) = (c,-c)$ y $(c,-c) \odot (x',y') = (a,-a)$. De lo cual se tiene que $(ax, \cancel{ay} - ax - \cancel{ay}) = (c,-c)$ y $(cx', -cx') = (a,-a)$. Luego, se cumple que

$$ax = c \qquad \wedge \qquad cx' = a$$

Luego $a|c$ y $c|a$. Como $(a,-a) \neq (0,0)$ se tiene que $a \neq 0$ por ende también $c \neq 0$. Por lo cual, necesariamente $c = \pm a$. Por lo tanto $(c,d) = (a,-a)$ o $(c,d) = (-a,a)$. Concluyendo así, que los únicos elementos en $[(a,-a)]$ son $(a,-a)$ y $(-a,a)$.

Teorema 4.2.7 *Para todo $(a,b) \in \varepsilon$, si $a = 0$, $(a,b) \neq (0,0)$ se tiene que*

$$[(0,b)] = \{(0,b),(0,-b)\}$$

Demostración: La demostración es análoga al teorema 4.2.6.

4.3. Los asociados de $(a, b) \in \varepsilon$

Como se indicó previamente, las definiciones que se han de incluir en el estudio del conjunto ε han de ser fieles, en la medida de lo posible, a la definición análoga en $\mathbb{Z}$. Como se aclaró, la definición de asociado, está ligado a la estructura algebraica de un dominio integro. $\mathbb{Z}$ es un dominio integro, pero ε no. Por ende se optó en primera instancia, por la relación $\diamond$, que considera a los elementos en ε que se dividen mutuamente. El siguiente teorema muestra que se pudo hacer uso de la definición de asociado, independientemente que ε no sea un dominio de integridad, pues para todo $(a, b) \in \varepsilon$ se cumple que los elementos de su clase, se expresan como producto de una unidad y (a, b).

Teorema 4.3.1 *Sea $(a, b) \in \varepsilon$, para todo $(c, d) \in [(a, b)]$ se cumple que (c, d) pertenece a uno y solo uno de los siguientes conjuntos: $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ o $\{(0, 0)\}$.*

Demostración: Con base en los teoremas 4.2.5, 4.2.6 y 4.2.7, se demuestra el teorema.

Teorema 4.3.2 *Para todo $(a, b) \in \varepsilon$ se cumple que:*

$$[(a, b)] = \{(a, b) \odot u : u \in \mathfrak{U}(\varepsilon)\}$$

Demostración: Dado que $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ y $\{(0, 0)\}$ determinan una partición en ε, se hará la demostración por casos.

- Si $(a, b) \in \{(0, 0)\}$, es inmediato demostrar que

$$\{(a, b) \odot u : u \in \mathfrak{U}(\varepsilon)\} = \{(0, 0)\} = [(0, 0)]$$

- Si $(a, b) \in \varepsilon^* - \mathfrak{D}(\varepsilon)$, por teorema 4.2.4 se concluye que

$$[(a, b)] = \{(a, b) \odot u : u \in \mathfrak{U}(\varepsilon)\}$$

- Si $(a, b) \in \mathfrak{D}(\varepsilon)$, se cumple solo una de las siguientes opciones:

  - Si $a = 0$ se tiene que

$$\begin{aligned} \{(0, b) \odot u : u \in \mathfrak{U}(\varepsilon)\} &= \{(0, b), (0, b), (0, -b), (0, -b)\} \\ &= \{(0, b), (0, -b)\} \\ &= [(0, b)] \end{aligned}$$

- Si $a = -b$, de lo cual se tiene que:

$$\begin{aligned}\{(a,-a) \odot u : u \in \mathfrak{U}(\varepsilon)\} &= \{(a,-a),(a,-a),(-a,a),(-a,a)\} \\ &= \{(a,-a),(-a,a)\} \\ &= [(a,-a)]\end{aligned}$$

Concluyendo así la demostración.

Corolario 4.3.1 *Para todo* $(a,b) \in \varepsilon$ *se cumple que:*

$$[(a,b)] = \{(a,b),(-a,-b),(a,-2a-b),(-a,2a+b)\}$$

Demostración: Es consecuencia directa del teorema 4.3.1 y del hecho de considerar que las unidades de ε son $(1,0),(-1,0),(1,-2)$ y $(-1,2)$. En el apéndice A, se incluyen algunos elementos de ε y los respectivos elementos de su clase.

Comparación xxi de ε con $\mathbb{Z}$: Partiendo del hecho que $\mathbb{Z}$ es un dominio integro y ε no, se tiene que lo evidenciado con las clases de $(a,b) \in \mathfrak{D}(\varepsilon)$, no es algo que se pueda relacionar con el anillo de los números enteros.

Pero, por otro lado, se ha evidenciado que para todo $(a,b) \in \varepsilon$, este pertenece a uno y solo uno, de los siguentes conjuntos: $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ o $\{(0,0)\}$. Y, con lo desarrollado, se demostró que independientemente de a cual conjunto pertenece (a,b), se tiene que todos los elementos de su clase pertenecen a este mismo conjunto, esto se evidencia en el teorema 4.3.1. Aunque en $\mathbb{Z}$ no se tienen divisores del 0, se cumple que para todo $z \in \mathbb{Z}$ se cumple que todos los elementos de $[z]$ pertenecen al mismo conjunto de la partición de $\mathbb{Z}$, siendo estos conjuntos $z^* = a - \{0\}$ y $\{0\}$. Dado que esta es la partición análoga a la hecha en ε, pues el conjunto de los divisores de 0 en $\mathbb{Z}$ es vacío.

4.4. Compatibilidad de $\diamond$ con $(\varepsilon, \oplus)$ y con $(\varepsilon, \odot)$

Con el paso al cociente de la relación $\diamond$, lo que sigue del proceso, es verificar si operaciones definidas en ε son compatibles[v] con la relacción de equivalencia. Sea $\triangle$ la operación

[v] Sea una relación de equivalencia R en un conjunto P, con la operación $\oslash$ se dice que R es compatible con $\oslash$, si para todo $p, p', q, q' \in P$ se cumple que si pRp' y qRq' entonces $p \oslash qRp' \oslash q'$ [7, p. 113].

obtenida por el paso al cociente de $\oplus$. Está está definida como sigue.

$$\triangle : \varepsilon_{/\diamond} \times \varepsilon_{/\diamond} \to \varepsilon_{/\diamond}$$

$$[(a,b)] \triangle [(c,d)] = [(a,b) \oplus (c,d)]$$

Un problema que surge aquí para demostrar que $\triangle$ está bien definida, es demostrar que $\diamond$ es compatible con $\oplus$, dicho en otras palabras, sin importar el representante de las clases $[(a,b)]$ y $[(c,d)]$ se espera que la suma de dichos representantes pertenezca a $[(a,b) \oplus (c,d)]$.

Considerando esto en $\mathbb{Z}$, se tiene que $5 \in [-5]$, pero $5+5 = 10$ y $5-5 = 0$ y $[0] \neq [10]$. Por lo cual, la suma en $\mathbb{Z}$ no es compatible con la relación de equivalencia que allí se define. De manera análoga sucede con $\oplus$ y $\diamond$. Se cumple que $(4,5) \in [(4,5)]$ y que $(-3,-7), (3,7) \in [(3,7)]$ De lo cual se tiene que:

$$\begin{aligned}
[(4,5)] \triangle [(-3,-7)] &= [(4,5) \oplus (-3,-7)] \\
&= [(1,-2)] \\
&\neq [(7,12)] \\
&= [(4,5) \oplus [(3,7)] \\
&= [(4,5)] \triangle [(3,7)]
\end{aligned}$$

Por lo cual, se concluye que la operación $\oplus$ y la relación de equivalencia $\diamond$ no son compatibles.

Prosiguiendo, se considera $\boxdot$ como la operación obtenida del paso al cociente de $\odot$. Esta operación está definida por:

$$\boxdot : \varepsilon_{/\diamond} \times \varepsilon_{/\diamond} \to \varepsilon_{/\diamond}$$

$$[(a,b)] \boxdot [(c,d)] = [(a,b) \odot (c,d)]$$

Teorema 4.4.1 *La operación $\boxdot$ está bien definida.*

Demostración: Sean $(a,b), (a',b'), (c,d), (c',d') \in \varepsilon$ con $(a,b) \diamond (a',b')$ y $(c,d) \diamond (c',d')$. Dado que $\diamond$ es una relación de equivalencia, se cumple que $(a',b') \in [(a,b)]$ y $(c',d') \in$

$[(c,d)]$. Por teorema 4.3.1, se concluye que

$$(a',b') = (a,b) \odot u_1 \quad \text{y} \quad (c',d') = (c,d) \odot u_2$$

Para algún $u_1, U_2 \in \mathfrak{U}(\varepsilon)$. De esto se tiene que:

$$\begin{aligned}(a',b') \odot (c',d') &= \big((a,b) \odot u_1\big) \odot \big((c,d) \odot u_2\big) \\ &= \big((a,b) \odot (c,d)\big) \odot \big(u_1 \odot u_2\big) \\ &= \big((a,b) \odot (c,d)\big) \odot u_3\end{aligned}$$

Luego se tiene que $(a',b') \odot (c',d') \in [(a,b) \odot (c,d)]$, es decir

$$(a,b) \odot (c,d) \diamond (a',b') \odot (c',d')$$

Como se cumple que $(a,b) \odot (c,d) \diamond (a',b') \odot (c',d')$ y cómo $\diamond$ es una relación de equivalencia, se deduce que $[(a,b) \odot (c,d)] = [(a',b') \odot (c',d')]$; es decir, que el producto de las clases es la clase del producto, sin importar los representantes que se tomen de cada clase. Por lo cual se concluye que $\boxdot$ está bien definida. Quedando así demostrado el teorema.

Teorema 4.4.2 *$(\varepsilon_{/\diamond}, \boxdot)$ es semigrupo conmutativo con identidad.*

Demostración: Sean $[(a,b)], [(c,d)], [(e,f)] \in \varepsilon_{/\diamond}$, se cumple que:

$$\begin{aligned}[(a,b)] \boxdot [(c,d)] &= [(a,b) \odot (c,d)] && \text{Definición de } \boxdot \\ &= [(c,d) \odot (a,b)] && \text{Conmutativa de } \odot \\ &= [(c,d)] \boxdot [(a,b)] && \text{Definición de } \boxdot\end{aligned}$$

Con lo cual se concluye que $(\varepsilon_{/\diamond}, \boxdot)$ es conmutativo. Dado que la operación $\boxdot$ es la operación obtenida del paso al cociente de $\odot$, se deduce que la operación $\boxdot$ hereda las propiedades algebraicas de $\odot$, por lo cual demostrar que $\boxdot$ es asociativa y posee un único módulo (siendo este la [(1,0)] y siendo el único elemento invertibles bajo $\boxdot$) se hace con base en las propiedades algebraicas de $\odot$. Por lo cual se concluye que $(\varepsilon_{/\diamond}, \boxdot)$ es semigrupo conmutativo con identidad.

Comparación xxii de ε con $\mathbb{Z}$: Se tiene que $(\varepsilon_{/\diamond}, \boxdot)$, es un semigrupo conmutativo con identidad. De forma análoga sucede con el producto en $\mathbb{Z}$ inducido en su conjunto cociente. Precisando, se tiene que en $\mathbb{Z}$, que la $[a] = \{1 \cdot a, -1 \cdot a\} = \{a, -a\}$ teniendo que la suma inducida en el conjunto cociente, no es una operación bien definida. De forma análoga sucede en $\varepsilon_{/\diamond}$.

4.5. El conjunto cociente $\varepsilon_{/\diamond}$

Ahora, recordando que la relación $\star$ de equivalencia en $\mathbb{Z}$, es análoga a $\diamond$ en ε, surge la pregunta sobre ¿qué *cara* tienen los elementos de $(\varepsilon_{/\diamond}, \boxdot)$? Pues, se tiene que $(\mathbb{Z}/_{\star}, \cdot)$ es isomorfo a $(\mathbb{N}, \cdot)$[VI]. Una demostración que valida que $(\mathbb{N}, \cdot)$ y $(\mathbb{Z}/_{\star}, \cdot)$ son isomorfos es considerando $f : \mathbb{N} \to \mathbb{Z}/_{\star}$ con $f(a) = [a]$[VII].

Una duda que surge es ¿cuál es el conjunto con el que $(\varepsilon_{/\diamond}, \boxdot)$ es isomorfo? Copiando lo que se hace en $\mathbb{Z}$ se tiene que la función biyectiva va de un subconjunto de ε al conjunto cociente. Ahora, teniendo en cuenta que son cuatro los elementos que hay por clase (excluyendo la del $(0, 0)$ y sus divisores), se espera que los elementos estén distribuidos en cuatro subconjuntos del plano irreal, pues de manera análoga sucede con $\mathbb{Z}$, debido a que los elementos (diferentes de 0) de las clases están en dos conjuntos disyuntos, siendo estos $\mathbb{Z}^-$ y $\mathbb{Z}^+$. Y sí, se tiene previamente esto en ε, pues en la figura 2.5, sugiere algo análogo. Con base en ello, se considera el conjunto ε_1 que está definido como sigue.

$$\varepsilon_1 = \{(a, b) \in \varepsilon : a \geq 0 \wedge b \geq -a\}$$

Como primer paso, se ha de demostrar que para todo $(a, b) \in \varepsilon$ existe un único $(c, d) \in \varepsilon_1$ tal que $(c, d) \in [(a, b)]$. En otras palabras se ha de demostrar que para todo elemento en

[VI] Se ha de aclarar que a pesar que se note con $\cdot$ el producto en $\mathbb{N}$ y el inducido en $\mathbb{Z}/_{\star}$, estas operaciones son diferentes.

[VII] Dada la definición de f, se tiene que esta función cumple que

- Sean $a, b \in \mathbb{N}$ tal que $f(a) = f(b)$, esto es, $[a] = [b]$. Si $a = 0$ se tiene que $b = 0$, pues $\{0\} = [0] = [b]$ Por otro lado, si $a \neq 0$ se tiene que $b \neq 0$ y que $[a] = \{a, -a\} = [b]$. Ahora, no se puede dar que $b = -a$ pues $-a < 0$. Por tanto $a = b$. Demostrando que f es inyectiva.
- Sea $[a]$, por definición se tiene que $a \in \mathbb{Z}$. si $a \geq 0$ se tiene que $f(a) = [a]$. De otro modo, si $a < 0$ se tiene que $f(-a) = [a]$. Demostrando que f es sobreyectiva.
- Ahora, sea $f(a \cdot b) = [a \cdot b] = [a] \cdot [b] = f(a) \cdot f(b)$.

Concluyendo así que f es un isomorfismo.

ε existe un único representante de su clase en ε_1. Considerando la partición evidenciada en el teorema 2.1.14, se tiene el siguiente teorema. Pero, primero se ha de demostrar un lema.

Lema 4.5.1 *Para todo* $(a,b) \in \varepsilon^* - \mathfrak{D}(\varepsilon)$*, si* $(a,b) \in \varepsilon_1$ *se cumple que los elementos* $(c,d) \in [(a,b)]$ *con* $(c,d) \neq (a,b)$ *no pertenecen a* ε_1*.*

Demostración: Como $(a,b) \in \varepsilon^* - \mathfrak{D}(\varepsilon)$ y $(a,b) \in \varepsilon_1$, se infiere que $a > 0$ y $b > -a$. Además, considerando el 4.3.1, se tiene que:

- $(-a,-b) \in [(a,b)]$. Como $a > 0$ se tiene que $-a < 0$, lo cual es argumento suficiente para concluir que $(-a,-b) \notin \varepsilon_1$.
- $(-a, 2a+b) \in [(a,b)]$. De forma análoga, al ítem anterior, se ha de concluir que $-a < 0$ luego, $(-a, 2a+b) \notin \varepsilon_1$.
- $(a, -2a-b) \in [(a,b)]$. Dado que $b > -a$, se cumple que $-b < a$ lo cual conlleva a que $-b - 2a < a - 2a = -a$ De lo cual se concluye que $(a, -2a-b) \notin \varepsilon_1$.

Teorema 4.5.1 *Para todo* $(a,b) \in \varepsilon$ *se tiene que existe un único* $(c,d) \in \varepsilon_1$ *tal que* $(c,d) \in [(a,b)]$*.*

Demostración: Dada la partición de ε en los conjuntos $\mathfrak{D}(\varepsilon)$, $\varepsilon^* - \mathfrak{D}(\varepsilon)$ y $\{(0,0)\}$ se ha de demostrar en tres partes. Siendo:

- Dado que $[(0,0)] = \{(0,0)\}$ y que $(0,0) \in \varepsilon_1$, se demuestra que existe un elemento de la $[(0,0)]$ en ε_1.
- Sea $(a,b) \in \mathfrak{D}(\varepsilon)$. Claramente $(a,b) \neq (0,0)$. Luego se tienen dos casos, los cuales son:
  - Si $a = 0$ Dado que la clase de $(0,b)$ cuenta con dos elementos $(0,b)$ y $(0,-b)$, se tiene que si $b > 0$ entonces $(0,b) \in \varepsilon_1$ demostrando así el enunciado del teorema, para este caso. Ahora, si Si $b < 0$ se tiene que el elemento en ε_1 será $(0,-b)$.
  - Si $a = -b$. De forma análoga se considera que si $a > 0$ entonces $(a,-a) \in \varepsilon_1$. Por otro lado, si $a < 0$ entonces $(-a,a) \in \varepsilon_1$.

  Concluyendo así que para todo $(a,b) \in \mathfrak{D}(\varepsilon)$ existe un elemento en $[(a,b)]$ tal que este elemento pertenece a ε_1.

- Si $(a,b) \in \varepsilon^* - \mathfrak{D}(\varepsilon)$. Por teorema 2.1.12, se cumple que

$$(a > 0 \wedge b > -a) \vee (a > 0 \wedge b < -a) \vee (a < 0 \wedge b < -a) \vee (a < 0 \wedge b > -a)$$

  Considerando los casos, se tiene que:

  - Si $a > 0 \wedge b > -a$, por lema 4.5.1, se tiene que el único elemento de la clase de (a,b) en ε_1 es (a,b).
  - Si $a > 0 \wedge b < -a$. Luego $(a, -2a-b) \in [(a,b)]$. Comprobándose que $(a, -2a-b) \in \varepsilon_1$ pues $-b < a$ implica que $-b-2a < a-2a = -a$. Dado que $(a, -2a-b) \in \varepsilon_1$, el lema 4.5.1, valida que es el único elemento de la clase de (a,b) que pertenece a ε_1.
  - Si $a < 0 \wedge b < -a$, el razonamiento es análogo al segundo ítem, teniendo que $(-a,-b) \in \varepsilon_1$.
  - Si $a < 0 \wedge b > -a$, se razona de forma análoga a los dos últimos ítems, concluyendo que $(-a, 2a+b) \in \varepsilon_1$.

Concluyendo así, la demostración.

Ahora, lo que sigue es demostrar que $\varepsilon_1, \odot$ es isomorfo con $(\varepsilon_{/\diamond}, \boxdot)$. Como se indicó previamente, se definirá la función de forma análoga a como se hace en $\mathbb{Z}$.

Teorema 4.5.2 *Las estructuras* $(\varepsilon_1, \odot)$ *y* $(\varepsilon_{/\diamond}, \boxdot)$ *son isomorfas.*

Demostración: Considérese:

$$f : \varepsilon_1 \to \varepsilon_{/\diamond}$$

$$f((a,b)) = [(a,b)]$$

Como las demostraciones previas, en cuanto a la demostración de isomorfismos refiere, se hará la demostración en tres partes.

- Sean $(a,b),(c,d) \in \varepsilon_1$ tal que $f((a,b)) = f((c,d))$, luego $[(a,b)] = [(c,d)]$ de lo cual se tiene que $(c,d) \in [(a,b)]$. Por lema 4.5.1, se cumple que como $(a,b) \in \varepsilon$ este es elúnico elemento de $[(a,b)]$ que petenece a ε_1. Pero como $(c,d) \in \varepsilon_1$, se concluye que $(a,b) = (c,d)$. Permitiendo esto, concluir que f es inyectiva.

- Sea $[(a,b)] \in \varepsilon_{/\diamond}$. Se tiene que $(a,b) \in \varepsilon$. Con base en el teorema 4.5.1, se concluye que existe $(c,d) \in [(a,b)]$ tal que $(c,d) \in \varepsilon_1$. Luego se tiene que $f((c,d)) = [(c,d)] = [(a,b)]$. Concluyendo así que f es sobreyectiva.

- Sean $(a,b),(c,d) \in \varepsilon_1$, se tiene que:

$$\begin{aligned} f\big((a,b) \odot (c,d)\big) &= \big[(a,b) \odot (c,d)\big] \\ &= [(a,b)] \boxdot [(c,d)] \\ &= f(a,b) \boxdot f(c,d) \end{aligned}$$

Concluyendo así, que $(\varepsilon_1, \odot)$ y $(\varepsilon_{/\diamond}, \boxdot)$ son isomorfos. Una representación de $\varepsilon, \cdot)$ se muestra en la figura 4.1.

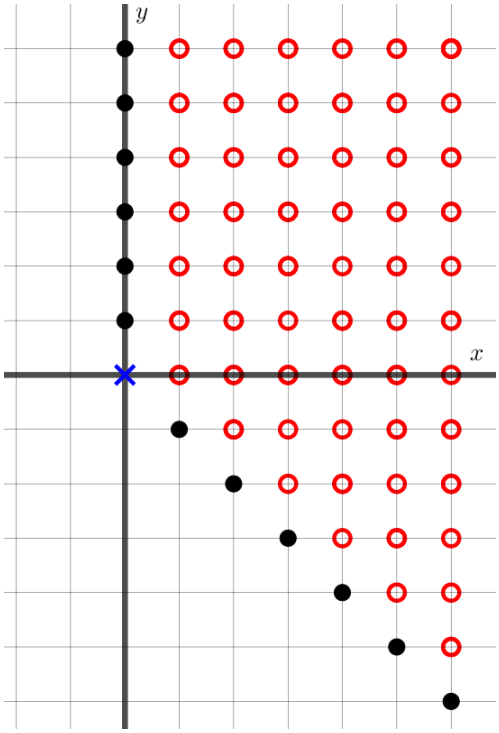

Figura 4.1: Elementos de $(\varepsilon_1, \odot)$: un conjunto isomorfo a $(\varepsilon_{/\diamond}, \boxdot)$.

Comparación xxiii de ε con $\mathbb{Z}$: Como se ha evidenciado, $(\varepsilon_1, \odot)$ y $(\varepsilon_{/\diamond}, \boxdot)$ son isomorfos. Análogamente sucede con $(\mathbb{Z}/_\star, \cdot)$ y $(\mathbb{N}, \cdot)$.
Como se tiene que las sumas definidas en cada conjunto, ε y $\mathbb{Z}$, no son compatibles con la relación de orden que allí se define, se concluye que los conjuntos isomorfos, son estructuralmente iguales (salvo el nombre de sus elementos [4, p. 66]), en cuanto al producto definido se refiere, pues en aspectos aditivos estos conjuntos difieren.

4.6. Una relación de divisibilidad en $\varepsilon_{/\diamond}$

Dando continuación al desarrollo de una relación de divisibilidad análoga a la de los $\mathbb{Z}$, se define la relación $\|$ en $\varepsilon_{/\diamond}$; siendo:

Definición 4.6.1 *Para todo* $[(a,b)], [(c,d)] \in \varepsilon_{/\diamond}$*, se dice que* $[(a,b)] \| [(c,d)]$ *si y solo si existe* $[(e,f)] \in \varepsilon_{/\diamond}$ *tal que* $[(a,b)] \boxdot [(e,f)] = [(c,d)]$.

Teorema 4.6.1 *La relación* $\|$ *es una relación de orden.*

Demostración: Para que una relación sea de orden, debe ser reflexiva, antisimétrica y transitiva. Por ello la demostración se hará en tres partes, que son:

- Para todo $[(a,b)] \in \varepsilon_{/\diamond}$, se cumple que $[(a,b)] \boxdot [(1,0)] = [(a,b)]$: por lo cual se tiene que $[(a,b)] \| [(a,b)]$, concluyendo así que $\|$ es reflexiva.

- Sean $[(a,b)], [(c,d)] \in \varepsilon_{/\diamond}$ tal que $[(a,b)] \| [(c,d)]$ y $[(c,d)] \| [(a,b)]$. Se infiere que $(a,b) \mid (c,d)$ y $(c,d) \mid (a,b)$ y por la definición de $\diamond$, se tiene que $(a,b) \in [(c,d)]$, luego $[(a,b)] = [(c,d)]$ Concluyendo así, que la relación $\|$ es antisimétrica.

- Sean $[(a,b)], [(c,d)], [(e,f)] \in \varepsilon_{/\diamond}$ tal que $[(a,b)] \| [(c,d)]$ y $[(c,d)] \| [(e,f)]$. Por definición se tiene que existen $[(m,n)], [(o,p)] \in \varepsilon_{/\diamond}$ tal que: $[(a,b)] \boxdot [(m,n)] = [(c,d)]$ y $[(c,d)] \boxdot [(o,p)] = [(e,f)]$. De lo cual se cumple que

$$\begin{aligned}
[(e,f)] &= [(c,d)] \boxdot [(o,p)] \\
&= \big([(a,b)] \boxdot [(m,n)]\big) \boxdot [(o,p)] \\
&= [(a,b)] \boxdot \big([(m,n)] \boxdot [(o,p)]\big)
\end{aligned}$$

  Como $\boxdot$ es una operación bien definida sobre $\varepsilon_{/\diamond}$, se cumple que $[(m,n)] \boxdot [(o,p)] \in \varepsilon_{/\diamond}$. Concluyendo así que $[(a,b)] \| [(e,f)]$. Demostrando que $\|$ es transitiva.

Dado que $\|$ es una relación reflexiva, antisimétrica y transitiva, se concluye que $\|$ es una relación de orden.

Se puede evidenciar que demostrar que $\|$ es reflexiva y transitiva, se hizo bajo la misma estructura sobre la cual se demostró que la relación $|$ es una relación en ε que cumple reflexividad y transtividad.

Algo de gran importancia es caracterizar los elementos del conjunto $\varepsilon_{/\diamond}$,de acuerdo al número de divisores. Con base en esto, surgen varias preguntas como:

- Dado un $[(a,b)] \in \varepsilon_{/\diamond}$ ¿cómo determinar sus divisores?
- ¿Cuál es la mínima cantidad de divisores que puede tener un elemento $[(a,b)] \in \varepsilon_{/\diamond}$?
- Dado un $[(a,b)] \in \varepsilon_{/\diamond}$ ¿se puede expresar como un producto de dos elementos distintos de el mismo y las unidades?

Estas y otras preguntas nos dan paso para estudiar, si se puede, una definición de números primos y compuestos en el conjunto $\varepsilon_{/\diamond}$.

4.7. Abordando una definición de números primos en $\varepsilon_{/\diamond}$

En el conjunto $\mathbb{Z}$ se cumple que para todo número entero $n \geq 2$, este es primo, o bien, puede ser expresado como producto de números primos. La factorización en primos, es única, salvo su orden y sus asociados. La anterior proposición, se le conoce como el teorema fundamental de la Aritmética[VIII]. En esta sección se ha de responder la pregunta ¿En $\varepsilon_{/\diamond}$ se da un teorema análogo al TFA? Para responder esto, se ha de considerar, inicialmente, una definición de número primo.

Teniendo presente que $(\varepsilon_{/\diamond}, \boxdot)$ es isomorfo a $(\varepsilon_1, \odot)$. Entonces A partir de este punto, se ha trabajar con los elementos de ε_1, esto en gran medida por aspectos de notación. Luego al considerar a $(a,b) \in \varepsilon_1$ se está considerando a (a,b) y sus asociados[IX] en ε. Evidentemente $(1,0)$ no tiene divisores[X]. Ahora, como $\mathbb{Z} \subset \varepsilon$. se inquiere sobre cuántos

[VIII] Una demostración del TFA, se puede consultar en [5] en las páginas 161 y 162.

[IX] El teorema 4.3.2, permite que se pueda hacer uso de la palabra *asociados*, incluso bajo la consideración que ε no es un dominio de integridad.

[X] Excepto sus asociados.

divisores tiene en ε los números primos de $\mathbb{Z}$.

Considérese p un número primo en $\mathbb{Z}$. Se tiene que p solo tiene dos divisores: él mismo y el 1. Ahora considerando a p como un elemento de ε la pregunta a responder es ¿cuántos divisores tiene $(p, 0)$? Evaluando la sutuación se tiene que los divisores $(a, b), (c, d) \in \varepsilon_1$ de $(p, 0)$, satisfacen que:

$$(a, b) \odot (c, d) = (p, 0)$$

De lo desarrollado en el capítulo 3, se tiene que para que $(p, 0)$ se pueda expresar como producto de (a, b) y (c, d), se debe cumplir que $a \mid p$ y $c \mid p$. como p es primo, sin perdida de generalidad se dirá que $a = p$ y $c = 1$. Luego

$$(p, b) \odot (1, d) = (p, 0)$$
$$(p, pd + b + bd) = (p, 0)$$

Luego se tiene que

$$pd + b + bd = 0$$
$$pd + b(1 + d) + p = p$$
$$p(1 + d) + b(1 + d) = p$$
$$(p + b)(1 + d) = p$$

Ahora, haciendo una retrospectiva, se tiene que si $(m, n) \in \varepsilon_1$ entonces $m \geq 0$ y $n \geq -m$. Especificamente, como se han considerando $(p, b), (1, d) \in \varepsilon_1$ se tiene que $b \geq -p$ y $d \geq -1$. Se evidencia que, posibles valores para b y d es 0, pues $(p+0)(1+0) = p \cdot 1 = p$. Pero otra posibilidad es que $b = -p + 1$ y $d = p - 1$. De lo cual se tiene que:

$$(p, -p + 1) \odot (1, p - 1) = (p, 0)$$

Por lo cual se ve un número los números primos en $\mathbb{Z}$ tienen cuatro divisores (y sus respectivos asociados).

Ahora, sea cual sea la definición de número primo en ε_1, con base en esta definición se ha de determinar si p es primo en ε, partiendo del hecho que p sea primo en $\mathbb{Z}$. Se ha

de optar porque un número primo en $\mathbb{Z}$ sea primo en ε_1. Luego un número primo en ε_1 tendrá exactamente cuatro divisores.

Definición 4.7.1 *Sea* $(a,b) \in \varepsilon_1 - \{(0,0),(1,0)\}$, (a,b) *es un número primo*[XI] *en* ε_1 *si y solo si tiene exactamente cuatro divisores.*

Teorema 4.7.1 *Sea* $(p,0) \in \varepsilon_1$ *con* p *un número primo en* $\mathbb{Z}$*, entonces* $(p,0)$ *es un número primo en* ε*.*

Demostración: La demostración se da bajo los argumentos previos. Se agrega, que los divisores de $(p,0)$ son:

- $(p,0)$
- $(p,-p+1)$
- $(1,0)$
- $(1,p-1)$

Ahora, considerando los divisores de los divisores de $(0,0)$, se responderá a la pregunta sobre cuántos divisores tiene $(m,-m) \in \mathfrak{D}(\varepsilon_1)$. Ejemplificando, se tiene que para $(5,-5)$ es un divisor de sí mismo. Ahora, la ecuación:

$$(5,-5) \odot (x,y) = (5,-5)$$

tiene infinitas soluciones y esto debido al teorema 3.2.7. El conjunto de solución es:

$$F = \{(1,y) \in \varepsilon : y \in \mathbb{Z})\}$$

Ahora, hasta el momento se ha hallado un elemento de ε_1 que se expresa de infinitas formas como producto de números primos. Con lo cual se concluye que en ε_1 no se cumple un teorema análogo al TFA.

[XI]En $\mathbb{Z}$ los números primos se definen como los números mayores o iguales a 2, que tienen exactamente dos divisores. En ε no se cuenta con conjunto de números positivos, por lo cual se ha de flexbilizar la definición, al no considerar a $(0,0)$ y $(1,0)$.

Comparación xxiv de ε con $\mathbb{Z}$: Como se evidenció, se definió número primo en ε_1 teniendo en cuenta la definición de número primo en $\mathbb{Z}$. Pero incluso bajo cualquier otra posible definición de número primo en ε se concluye que no se cumple en ε_1 un teorema análogo al TFA.

Conclusiones

- El anillo de los números enteros es un subanillo del anillo de los números reales. Análogamente, se cumple que el anillo ε es un subanillo del anillo $\mathbb{J}$.
- Tanto el anillo de los números enteros, como el anillo ε cuentan con una cantidad finita de unidades. En ε existen cuatro elementos que son invertibles bajo el producto definido. Mientras que en $\mathbb{Z}$, hay dos unidades.
- El conjunto $\mathbb{Z}$ es un dominio de integridad. En contraste, se tiene que ε no es dominio de integridad. Además, en ε existen tantos divisores de $(0,0)$ como números naturales.
- El conjunto de los números enteros está contenido propiamente en ε.
- Analogamente, al conjunto $\mathbb{J}$, en el conjunto ε no se puede definir un conjunto de números positivos. En contraste, en el conjunto de los números enteros se define al conjunto de los números positivos.
- Mientras que en $\mathbb{Z}$ las ecuaciones de la forma $ax = b$ tienen a lo sumo una solución, se cumple que en ε, las ecuaciones de la forma $ax = b$, puede que no tengan solución, que tengan única solución o que tengan infinitas soluciones.
- Las ecuaciones cuadráticas en $\mathbb{Z}$ tienen a los sumo dos soluciones. En contraste, las ecuaciones cuadráticas consideradas en ε, pueden no tener solución, tener cuatro (contando multiplicidades) o tener infinitas soluciones.
- En ε la ecuación $ax^n = b$, con $n \in \mathbb{Z}^+$, a lo sumo tiene una solución si n es impar. Si n es par, la ecuación tiene a lo sumo cuatro soluciones (contando multiplicidades).
- Si una ecuación no tiene solución en $\mathbb{Z}$, esta ecuación seguirá sin tener solución considerándola en ε.

- La relación de divisibilidad definida en $\mathbb{Z}$ y en ε son reflexivas y transitivas, pero no son simétricas ni antisimétricas.
- En ε no se cumple un teorema análogo al teorema del algoritmo de la división de $\mathbb{Z}$.
- Los números primos en $\mathbb{Z}$ tienen cuatro divisores (considerando asociados) en ε.
- En ε no se cumple un teorema análogo al teorema fundamental de la Aritmética.

Bibliografía

[1] Apostol, T. (1972). *Calculus.* Volumnen I. Segunda edición. Editorial Revertre.

[2] Caicedo, J. (2004). *Teoría de Grupos.* Departamento de Matemáticas. Universidad Nacional de Colombia. Sede Bogotá.

[3] Cano, J. (2015). *Números de la forma* $a + bj$*, donde* $a, b \in \mathbb{R}$ *y* $j^2 = j$ *con* $j \neq 0$ *y* $j \neq 1$. Licenciatura en Matemáticas. Universidad Pedagógica Nacional.

[4] Fraleigh, J. (1987). *Álgebra abstracta.* Addison-Wesley Ibeoramericana.

[5] Koshy, T. (2007). *Elementary Number Theory with Aplicattions.*

[6] Luque, J., Mora, L. & Torres, J. (2006). *Estructuras análogas a los números reales.* Universidad Pedagógica Nacional.

[7] Muñoz, J. (2002). *Introducción a la teoría de conjuntos.* Cuarta edición. Universidad Nacional de Colombia. Facultad de Ciencias.

Apéndice A

Algunas clases de equivalencia de la relación $\diamond$.

(a, b)	(a, b)	$(-a, -b)$	$(a, -2a - b)$	$(-a, 2a + b)$
(1 , 0)	(1 , 0)	(-1 , 0)	(1 , -2)	(-1 , 2)
(1 , 1)	(1 , 1)	(-1 , -1)	(1 , -3)	(-1 , 3)
(1 , 2)	(1 , 2)	(-1 , -2)	(1 , -4)	(-1 , 4)
(1 , 3)	(1 , 3)	(-1 , -3)	(1 , -5)	(-1 , 5)
(1 , 4)	(1 , 4)	(-1 , -4)	(1 , -6)	(-1 , 6)
(1 , 5)	(1 , 5)	(-1 , -5)	(1 , -7)	(-1 , 7)
(2 , 6)	(2 , 6)	(-2 , -6)	(2 , -10)	(-2 , 10)
(2 , 0)	(2 , 0)	(-2 , 0)	(2 , -4)	(-2 , 4)
(2 , 1)	(2 , 1)	(-2 , -1)	(2 , -5)	(-2 , 5)
(2 , 2)	(2 , 2)	(-2 , -2)	(2 , -6)	(-2 , 6)
(2 , 3)	(2 , 3)	(-2 , -3)	(2 , -7)	(-2 , 7)
(2 , 4)	(2 , 4)	(-2 , -4)	(2 , -8)	(-2 , 8)
(2 , 5)	(2 , 5)	(-2 , -5)	(2 , -9)	(-2 , 9)
(2 , 6)	(2 , 6)	(-2 , -6)	(2 , -10)	(-2 , 10)
(3 , 0)	(3 , 0)	(-3 , 0)	(3 , -6)	(-3 , 6)
(3 , 1)	(3 , 1)	(-3 , -1)	(3 , -7)	(-3 , 7)
(3 , 2)	(3 , 2)	(-3 , -2)	(3 , -8)	(-3 , 8)
(3 , 3)	(3 , 3)	(-3 , -3)	(3 , -9)	(-3 , 9)
(3 , 4)	(3 , 4)	(-3 , -4)	(3 , -10)	(-3 , 10)

(a, b)	(a, b)	$(-a, -b)$	$(a, -2a - b)$	$(-a, 2a + b)$
(3 , 5)	(3 , 5)	(-3 , -5)	(3 , -11)	(-3 , 11)
(3 , 6)	(3 , 6)	(-3 , -6)	(3 , -12)	(-3 , 12)
(4 , 0)	(4 , 0)	(-4 , 0)	(4 , -8)	(-4 , 8)
(4 , 1)	(4 , 1)	(-4 , -1)	(4 , -9)	(-4 , 9)
(4 , 2)	(4 , 2)	(-4 , -2)	(4 , -10)	(-4 , 10)
(4 , 3)	(4 , 3)	(-4 , -3)	(4 , -11)	(-4 , 11)
(4 , 4)	(4 , 4)	(-4 , -4)	(4 , -12)	(-4 , 12)
(4 , 5)	(4 , 5)	(-4 , -5)	(4 , -13)	(-4 , 13)
(4 , 6)	(4 , 6)	(-4 , -6)	(4 , -14)	(-4 , 14)
(5 , 0)	(5 , 0)	(-5 , 0)	(5 , -10)	(-5 , 10)
(5 , 1)	(5 , 1)	(-5 , -1)	(5 , -11)	(-5 , 11)
(5 , 2)	(5 , 2)	(-5 , -2)	(5 , -12)	(-5 , 12)
(5 , 3)	(5 , 3)	(-5 , -3)	(5 , -13)	(-5 , 13)
(5 , 4)	(5 , 4)	(-5 , -4)	(5 , -14)	(-5 , 14)
(5 , 5)	(5 , 5)	(-5 , -5)	(5 , -15)	(-5 , 15)
(5 , 6)	(5 , 6)	(-5 , -6)	(5 , -16)	(-5 , 16)
(6 , 0)	(6 , 0)	(-6 , 0)	(6 , -12)	(-6 , 12)
(6 , 1)	(6 , 1)	(-6 , -1)	(6 , -13)	(-6 , 13)
(6 , 2)	(6 , 2)	(-6 , -2)	(6 , -14)	(-6 , 14)
(6 , 3)	(6 , 3)	(-6 , -3)	(6 , -15)	(-6 , 15)
(6 , 4)	(6 , 4)	(-6 , -4)	(6 , -16)	(-6 , 16)
(6 , 5)	(6 , 5)	(-6 , -5)	(6 , -17)	(-6 , 17)
(6 , 6)	(6 , 6)	(-6 , -6)	(6 , -18)	(-6 , 18)
(7 , 0)	(7 , 0)	(-7 , 0)	(7 , -14)	(-7 , 14)
(7 , 1)	(7 , 1)	(-7 , -1)	(7 , -15)	(-7 , 15)
(7 , 2)	(7 , 2)	(-7 , -2)	(7 , -16)	(-7 , 16)
(7 , 3)	(7 , 3)	(-7 , -3)	(7 , -17)	(-7 , 17)
(7 , 4)	(7 , 4)	(-7 , -4)	(7 , -18)	(-7 , 18)
(7 , 5)	(7 , 5)	(-7 , -5)	(7 , -19)	(-7 , 19)
(7 , 6)	(7 , 6)	(-7 , -6)	(7 , -20)	(-7 , 20)