

Los ideales y los retículos de Dedekind en la génesis del álgebra moderna: una visión histórico-epistemológica.

Nelly E. Arias Alonso

Universidad del Valle
Facultad de Educación y Pedagogía
Programa de Licenciatura en Matemáticas y Física
Santiago de Cali
2024

**Los ideales y los retículos de Dedekind en la génesis del álgebra moderna: una visión
histórico-epistemológica.**

Trabajo de Grado para Optar el Título de Licenciada en Matemáticas y Física

Elaborado por
Nelly E. Arias Alonso

Directora
Maribel P. Anacona

Universidad del Valle
Facultad de Educación y Pedagogía
Programa de Licenciatura en Matemáticas y Física
Santiago de Cali
2024

Agradecimientos

Como primera instancia, agradezco a Dios que ha sido mi mayor soporte en este proceso y quien me ha dado la fortaleza y sabiduría para culminar este trabajo.

Agradezco a mis padres Liliana Alonso y Guillermo Arias, a mi hermano Jaiver Arias por todo el sacrificio, amor y apoyo siempre incondicional para conmigo. A mi pareja Anderson Lozano por su paciencia y comprensión, porque siempre recibí de su parte una palabra de aliento para continuar. A mis amigos Yessica Gonzalez y Henry Mestizo por el gran apoyo emocional en cada proceso de mi carrera.

Agradezco muy especialmente a la profesora Maribel Anacona por todo el tiempo de acompañamiento dedicado a este trabajo, sin su gran profesionalismo y calidad humana, nada de esto habría sido posible. De la misma manera agradezco al profesor Guillermo Ortiz por su disponibilidad, comentarios y recomendaciones.

$$r = 1 - \sin \theta$$

Resumen

En este trabajo de grado se realiza un análisis de orden histórico-epistemológico acerca de cómo las nociones de ideal y retículo propuestas por Richard Dedekind gestan los primeros desarrollos que dan paso a la estructuración del algebra. Se inicia identificando el estado de la matemática de la época, luego se exponen las obras más representativas de Dedekind, posterior a esto se expone el problema principal por el cual surge la necesidad de incorporar nuevos dominios numéricos que dan paso a la definición de ideal, para finalmente presentar los elementos que construyen el concepto de *lattice* o retículo. También se expone la relación entre estos dos grandes conceptos en el camino hacia un estructuralismo que luego caracterizará las matemáticas del siglo XX.

Palabras Claves: Ideal, Retículo, Estructura algebraica, Números Naturales, Números Enteros, Conjunto Ordenado.

Abstract

In this degree work, a historical-epistemological analysis is carried out about how the notions of ideal and lattice proposed by Richard Dedekind give rise to the first developments that give way to the structuring of algebra. It begins by identifying the state of mathematics of the time, then the most representative works of Dedekind are exposed, after this the main problem is exposed by which the need arises to incorporate new numerical domains that give way to the definition of ideal, to finally present the elements that build the concept of lattice or reticle. The relationship between these two great concepts is also exposed on the path towards a structuralism that would later characterize the mathematics of the 20th century.

Keywords: Ideal, Lattice, Algebraic Structure, Natural Numbers, Integers, Ordered Set.

Tabla de contenido

AGRADECIMIENTOS:	2
RESUMEN	3
ABSTRACT	3
ÍNDICE DE TABLAS	6
ÍNDICE DE FIGURAS	7
INTRODUCCIÓN	9
CAPÍTULO 1	13
DEDEKIND Y LA EMERGENCIA DEL ESTRUCTURALISMO EN MATEMÁTICAS	13
1.1 ALGUNOS APORTES DE DEDEKIND AL NACIENTE ESTRUCTURALISMO MATEMÁTICO	15
1.2 DEDEKIND Y LA CONSTRUCCIÓN DE LOS REALES	18
1.3 DEDEKIND Y LA ESTRUCTURA DE LOS NÚMEROS NATURALES	21
CAPÍTULO 2	30
EL GERMEN DE LA TEORÍA DE LOS IDEALES DE DEDEKIND	30
2.1 CONCEPTOS BÁSICOS DE LA TEORÍA DE IDEALES	30
2.1.1 <i>Anillo, cuerpo y dominio de integridad</i>	34
2.1.2 <i>El concepto de Ideal</i>	37
2.2 LOS IDEALES DE DEDEKIND: BREVE CONTEXTUALIZACIÓN HISTÓRICA	39
2.2.1 <i>Los números enteros complejos de Gauss</i>	44
2.2.2 <i>Otra generalización de los enteros racionales</i>	51
CAPÍTULO 3	56
UNA MIRADA A LA TEORÍA DE RETÍCULOS DE DEDEKIND	56

3.1 NOCIONES BÁSICAS DE LA TEORÍA DE RETÍCULOS	56
3.1.1 <i>Definición de retículo y algunos ejemplos</i>	64
3.1.2 <i>Retículo algebraico</i>	77
3.1.3 <i>Retículo distributivo y modular</i>	83
3.2 LA TEORÍA DE RETÍCULOS DE DEDEKIND: BREVE CONTEXTUALIZACIÓN HISTÓRICA.....	91
CONCLUSIONES	97
REFERENCIAS BIBLIOGRÁFICAS.....	102

Índice de Tablas

Tabla 1 <i>Doble entrada para el ínfimo.</i>	67
Tabla 2 <i>Doble entrada para el Supremo.</i>	68
Tabla 3 <i>Doble Entrada para el Supremo, Completa.</i>	69
Tabla 4 <i>Doble Entrada para el Ínfimo, Completa.</i>	69
Tabla 5 <i>Verificación de Simetría Respecto a la Diagonal para el Ínfimo.</i>	70
Tabla 6 <i>Verificación de Simetría Respecto a la Diagonal para el Supremo.</i>	71
Tabla 7 <i>Verificación de los Elementos de la Diagonal para el Ínfimo.</i>	72
Tabla 8 <i>Verificación de los Elementos de la Diagonal para el Supremo.</i>	72
Tabla 9 <i>Verificación de Fila y Columna para Elementos Principales, Ínfimo.</i>	73
Tabla 10 <i>Verificación de Fila y Columna para Elementos Principales, Supremo.</i>	74
Tabla 11 <i>Verificación del elemento que devuelve así mismo, Ínfimo.</i>	75
Tabla 12 <i>Verificación del elemento que devuelve así mismo, Supremo.</i>	75
Tabla 13 <i>Supremo para $D6$, $a \vee b = \sup\{a, b\}$.</i>	78
Tabla 14 <i>Ínfimo para $D6$ $a \wedge b = \inf a, b$.</i>	79
Tabla 15 <i>Resumen de equivalencias entre retículo ordenado y retículo algebraico.</i>	80

Índice de Figuras

Figura 1 Relaciones de inclusión en partes de a .	57
Figura 2 Relaciones de inclusión en partes de A , simplificado.	58
Figura 3 Diagrama de Hasse.	59
Figura 4 Diagrama de Hasse para D_{18} .	60
Figura 5 Ejemplo de diagrama de Hasse.	61
Figura 6 Diagrama de Hasse del conjunto A .	63
Figura 7 A relacionado con B .	65
Figura 8 Diagrama de Hasse para D_{12} .	65
Figura 9 Diagrama de Hasse del conjunto A .	67
Figura 10 Diagrama de Hasse para D_6 .	78
Figura 11 Correspondencia entre Retículo Ordenado, y Retículo Algebraico.	80
Figura 12 Diagrama de Hasse del conjunto A .	81
Figura 13 Diagrama de Hasse del conjunto A .	82
Figura 14 Diagrama de Hasse del conjunto A .	84
Figura 15 Diagrama de Hasse de un retículo de cinco elementos llamado M_5 .	85
Figura 16 Diagrama de Hasse de un retículo de cinco elementos llamado N_5 .	86
Figura 17 Diagrama de Hasse de un retículo.	86
Figura 18 Diagrama de Hasse de un retículo donde se señala que no cumple con la distributividad.	87
Figura 19 Diagrama de Hasse para un retículo ordenado ($D_{18};/$) y simplificación de un elemento.	87

Figura 20 *Diagrama de Hasse de un retículo de cinco elementos llamado M5 con puntos definidos.....89*

Figura 21 *Diagrama de Hasse de un retículo de cinco elementos llamado N5 con puntos definidos.....90*

Introducción

Este trabajo de grado pretende identificar cuáles fueron los principales elementos de carácter histórico y epistemológico que aportaron al desarrollo y la estructuración del álgebra, enfocada principalmente en la teoría de ideales y de retículos de Richard Dedekind.

Para desarrollar esta problemática “se considera importante investigar estructuralmente un concepto, es decir, indagar qué tipo de preguntas confieren interés especial al avance de la disciplina y qué tipo de respuestas deberían esperarse” (Corry, 1991, pp. 11-12). Por otro lado, se estudian conceptos fundamentales del álgebra como anillo, ideal y retículo, claves en la matemática de finales del siglo XIX e inicios del siglo XX. Este trabajo de grado se realiza con el propósito de indagar cómo la obra de Dedekind sirvió de base para el proceso de estructuración matemática que tuvo lugar en el siglo XX. En este análisis de carácter histórico se consideran los aportes de algunos matemáticos de la época.

La importancia de reconocer los trabajos, de matemáticos como Dedekind, que dieron paso a la generalización del álgebra a finales del siglo XIX e inicios del siglo XX, consiste principalmente en identificar que este proceso no fue desencadenado *únicamente* por la adaptación del método axiomático que se instauró en la base de la matemática de la época, ni por la formalización de los conceptos de grupo, cuerpo o anillo; sino que se trató también de una corriente estructuralista que atiende al efecto unificador de las teorías matemáticas donde los objetos matemáticos solo son elementos que ocupan una posición y cumplen una función en una estructura, por lo cual no tienen más propiedades que aquellas que las reglas de construcción de la estructura les asignan. Cabe destacar que esta generalización concedió al álgebra la forma de relacionarse con otras áreas de la matemática y otros campos del conocimiento. Diremos entonces que este proceso de estructuración simplificó, generalizó y organizó la matemática.

De manera particular, este trabajo se enfoca en dilucidar los aspectos históricos y epistemológicos que contribuyen a la generalización del álgebra partiendo de la teoría de ideales y de Richard Dedekind, la cual muestra interés en la comprensión del papel primordial que juegan las operaciones, en este caso aritméticas, en su relación con los elementos sobre los que operan. Para ello, establece un procedimiento para extender estas operaciones a nuevos dominios numéricos más amplios sin alterar el concepto aritmético; hasta la propuesta estructural más abstracta, la cual marca un nuevo estilo que privilegia conceptos algebraicos generales (cuerpos, grupos y anillos con operadores, ideales) en lugar de complicados cálculos algebraicos. Al mismo tiempo se consideran las contribuciones matemáticas y epistemológicas de otros matemáticos entorno a estos conceptos, en este período de maduración.

Por tanto, en términos generales, se trata de identificar los elementos de carácter histórico y epistemológico asociados al desarrollo del álgebra desde la teoría de ideales y de retículos de Dedekind. Esto implica de manera particular reconocer el contexto histórico en el que se encontraba el desarrollo del álgebra a finales del siglo XIX y principios del siglo XX, estudiar los aspectos básicos que incidieron en el desarrollo de estas teorías propuestas por Dedekind; y desde una perspectiva estructuralista, analizar de qué manera influyeron los aportes de la teoría de Dedekind en una nueva visión del álgebra.

Para tal efecto, se reconoce desde una visión epistemológica que las matemáticas de finales del siglo XIX se encontraban en una etapa de significativo desarrollo conceptual, debido a los aportes tan adelantados de algunos matemáticos de la época. Los intereses de los algebristas ya no se centraban únicamente en la solución de ecuaciones algebraicas, sino que se iniciaba un periodo de axiomatización y generalización, lo cual incidió en el carácter abstracto del álgebra. En este período, “surgieron las generalizaciones de los sistemas algebraicos cuyas

operaciones satisfacen ciertos axiomas reconocibles e importantes, como los conjuntos con la operación de multiplicación que verifican los axiomas de *grupo*¹ o los conjuntos con una adición y una multiplicación que cumplen los axiomas de *anillo*²” (De la Peña, 2000, pp. 54-55).

Se identifica a Evariste Galois como uno de los principales interesados en el desarrollo del álgebra moderna y de introducir el concepto de cuerpo, que posteriormente sería retomado por Dedekind en un proceso de estructuración matemática. Dedekind no solo trabajó con el concepto de cuerpo y grupo, sino que formuló el concepto de anillo de $\mathbb{Z}$, ideal y dominio; desarrolló la teoría de cuerpo de los números racionales; estableció la continuidad de la recta real definiendo el número real por medio de cortaduras; generalizó el teorema fundamental de la aritmética, entre otros. Con Dedekind se inicia entonces un estilo matemático hacia la formalización y el estudio de las relaciones funcionales entre las diferentes estructuras como interés primordial.

El estudio y desarrollo del presente trabajo permite identificar qué tipo de elementos, desde una perspectiva histórico-epistemológica, influyeron de forma directa en el desarrollo del álgebra de estructuras y el posible impacto que este desarrollo generó en la construcción de la matemática misma. Para ello, fue fundamental analizar principalmente los trabajos y aportes de Dedekind, basándonos esencialmente en “indagar los conceptos matemáticos desde los términos de cuerpo e imágenes del conocimiento, en palabras de Corry, esto es, desde las teorías, hechos, métodos y meta-preguntas que otorgan un interés especial a la investigación” (Corry, 1991, pp. 11-12).

¹ Esta definición se amplía mayormente en el capítulo de preliminares.

² Definición tomada de “los cuadernos de álgebra” de Lezama y ampliada en el capítulo de preliminares.

Para determinar los posibles elementos que influyeron en la formalización del álgebra de estructuras, partiendo de los trabajos de Richard Dedekind (1871), se realizó un análisis de orden epistemológico que involucró el estudio de los principales trabajos algebraicos de la época, así como una consideración del contexto histórico en el cual se desarrollaron.

Teniendo en cuenta lo anterior, se identificaron tres momentos que coinciden con los capítulos del presente trabajo de grado: el primero se centra en clarificar el contexto histórico de la matemática del momento, más específicamente a finales del siglo XIX e inicios del siglo XX. Esta perspectiva proporciona un panorama más claro de cómo se desarrolla un periodo de maduración de las matemáticas que lleva a un tipo de formalización más estructuralista.

El segundo constituye el estudio de las teorías, los elementos y factores que abrieron paso a la génesis de la teoría de los ideales de Dedekind y de qué manera se construyeron los conceptos, las preguntas y los resultados que dieron como respuesta una de las teorías más influyentes en el desarrollo de la matemática moderna. De forma general, nos interesamos por clarificar por qué el punto central de la teoría de ideales de Dedekind se deriva del problema de la factorización única y el problema de la divisibilidad, y cómo estos hallazgos presentan un nuevo panorama en la teoría de números.

El tercero está dedicado al estudio de la teoría de retículos y el reconocimiento en el cambio de los conceptos que se plantearon en ese momento con los conceptos con los que se trabajan en la actualidad, y que confieren interés especial para reflexionar de qué manera Dedekind por medio de sus aportes permitió enriquecer el periodo de maduración y generalización del álgebra.

Capítulo 1

Dedekind y la emergencia del estructuralismo en matemáticas.

El siglo XIX se caracterizó por el rápido desarrollo del conocimiento matemático, se presentaron grandes avances en diversas ramas como la teoría de números, donde se destacan trabajos acerca de los números primos y la ley de reciprocidad cuadrática planteada por Gauss; la relación entre los ceros no triviales de la función zeta de Riemann³ y la distribución de los números primos⁴; la teoría de números enteros algebraicos planteada por Dedekind, la cual extendió el concepto de número primo a otros dominios algebraicos y el desarrollo a profundidad en la teoría de ideales propuesta por Kummer.

La geometría algebraica también vivió grandes avances en este período de tiempo, donde se rescata que las investigaciones hechas con anterioridad por Galois en su teoría de grupos establecieron la conexión entre la teoría de ecuaciones y la teoría de grupos que algunos matemáticos como Poincaré utilizaría para estudiar las propiedades topológicas de las curvas algebraicas y las superficies. Por su parte, Félix Klein usaría estos aportes para enriquecer el campo de la geometría algebraica con sus investigaciones sobre transformaciones de geometría algebraica y el concepto de “grupo de transformaciones”, también estudiaría las funciones elípticas y las superficies de Kummer.

Por su parte, el matemático Julius Weierstrass expone contribuciones importantes al formular una definición rigurosa de límite y continuidad, lo que permitió el desarrollo de la

³ La función zeta de Riemann es una función matemática definida para números complejos. Tiene una serie de propiedades interesantes, una de las cuales es que sus ceros no triviales (es decir, aquellos que no son números negativos enteros) tienen una ubicación especial en el plano complejo. La hipótesis de Riemann afirma que estos ceros se encuentran en una línea vertical conocida como la “línea crítica”. Tienen una relación profunda con la distribución de los números primos y se cree que contienen información valiosa sobre la naturaleza de los números primos.

⁴ Esta hipótesis ha sido un problema abierto en la teoría de números y su resolución es uno de los grandes desafíos matemáticos aún pendientes.

teoría de conjuntos en términos más precisos al cual se destaca principalmente la instauración del método axiomático, la aritmetización del análisis, entre otros. También hubo importantes avances en el campo de la física, como la teoría cuántica y la teoría del caos, que necesitaron de estas herramientas matemáticas avanzadas para su desarrollo.

De la misma manera se consolida la teoría de conjuntos, donde George Cantor se destaca como uno de los principales exponentes de este campo, su trabajo incluyó la introducción de conceptos como los conjuntos numerables e infinitos, así como la demostración de que hay diferentes “tamaños” de infinito⁵, también desarrolló la teoría de conjuntos transfinitos.

Dedekind también se destacó en este campo por sus contribuciones a la teoría de conjuntos, se destacan entre otras, su construcción de los números reales en términos de cortaduras en 1872 y su presentación estructural del conjunto de los números naturales en 1888. Estas y otras contribuciones de Dedekind se presentan con más detalle más adelante.

De otra parte, es importante tener presente que, a finales del siglo XIX, la investigación matemática comienza a ser una actividad regulada y reconocida profesionalmente. En 1897 se creó el primer *Congreso Internacional de Matemáticos* (CIM) en Zúrich, con una participación de 209 matemáticos, el Congreso tuvo por objeto promover las relaciones personales entre los matemáticos de diferentes países y dar cuenta del estado reciente de las diversas ramas de las matemáticas.

⁵ Cantor introdujo el concepto de cardinalidad para comparar el tamaño de los conjuntos. Dos conjuntos tienen la misma cardinalidad si se puede establecer una correspondencia uno a uno entre sus elementos. Por ejemplo, los conjuntos de los números naturales y números enteros tienen la misma cardinalidad, ya que se puede establecer una correspondencia uno a uno entre ellos. Sin embargo, Cantor demostró que no todos los infinitos son iguales, introdujo el concepto de conjuntos no numerables, que son conjuntos infinitos que tienen una cardinalidad mayor que la de los conjuntos numerables. El conjunto de todos los números reales es un ejemplo de un conjunto no numerable. La teoría de Cantor sobre los tamaños de los infinitos revolucionó la comprensión de la infinitud en matemáticas y tuvo profundas implicaciones en diversos campos, como el análisis matemático y la teoría de conjuntos.

En 1899 se inauguró la revista *l'Enseignement mathématique*, cuyo contenido recoge desde entonces la actividad matemática de todo el mundo⁶. El continuo incremento de trabajos de investigación tuvo como consecuencia la aparición de revistas de recopilación, donde se publicaban los resultados, ordenados por temas, de modo que cada especialista pudiera conocer los resultados relevantes obtenidos en su área de trabajo.

En agosto de 1900 se dio el segundo CIM que tuvo lugar en París y donde se consolidaron estos eventos. Fue aquí donde David Hilbert presentó su famosa lista de los 23 problemas matemáticos que, en su opinión, deberán centrar la atención en el siglo XX⁷. Desde entonces se han resuelto completamente 10 de los 23 problemas propuestos por Hilbert, algunos han sido aparentemente resueltos, pero los expertos no han aceptado tales soluciones debido a la ambigüedad que presentan sus enunciados, y otros despiertan gran controversia que aún no se supera totalmente.

Estos grandes avances condujeron a una necesidad de examinar los fundamentos de las matemáticas y revisar con minucia el tema del rigor. Es así como a finales del siglo XIX se comienza a advertir una mirada formalista donde se destaca principalmente la necesidad de concebir la matemática de una forma más abstracta y general. En este proceso de generalización Dedekind desempeña un importante papel que transformará de manera definitiva la forma de concebir las matemáticas.

1.1 Algunos aportes de Dedekind al naciente estructuralismo matemático.

⁶ Fue fundada en 1899 conjuntamente por Henri Fehr de Ginebra y por Charles-Ange Laisant de París como coeditores. La revista está afiliada a la Universidad de Ginebra y es órgano oficial de la *Comisión Internacional de Instrucción Matemática* (ICMI). Publica mayormente artículos sobre revisiones matemáticas, investigación matemática y contribuciones a la historia de las matemáticas.

⁷ El impacto de la lista de problemas anunciada por Hilbert es indicativo de su gran capacidad de visión integrativa dentro de su profesión.

El matemático alemán Julius Wilhelm Richard Dedekind (Brunswick, Alemania, 6 octubre 1831–12 febrero 1916) fue considerado una figura clave en el surgimiento de la matemática conjuntista y estructural del siglo XX principalmente por sus aportes a la teoría de números algebraicos. El padre de Dedekind era Julius Levin Ulrich Dedekind, administrador del Collegium Carolinum en Brunswick. Su madre era Caroline Henriette; tenía tres hermanos mayores; como adulto, nunca usó los nombres de Julius Wilhelm; era descendiente de una familia acomodada, en 1848 estudió en el Collegium Carolinum⁸ de su ciudad natal; en 1850 ingresa con sólidos conocimientos matemáticos a la Universidad de Gotinga⁹ donde conoce al célebre matemático Carl Friedrich Gauss, quien dirige su tesis doctoral *sobre la teoría de las integrales eulerianas*¹⁰ y se convierte en su principal mentor. En 1852 recibe su doctorado y se prepara para presentar su tesis de habilitación¹¹ que era necesaria en Alemania para obtener la *venia docendi*¹².

En 1854 se habilitó como profesor junto con su compañero y amigo Bernhard Riemann. Al morir Gauss, en Gotinga este es sucedido por Gustav Lejeune-Dirichlet, se dice que Dedekind empieza a desarrollar investigaciones de alto nivel gracias a la influencia académica de las nuevas tendencias de las matemáticas que venían de Francia, que Dirichlet ejerció en él, con el

⁸ La Universidad Técnica Carolo-Wilhelmina de Brunswick, abreviado Universidad Técnica de Brunswick o TU Brunswick, es la universidad técnica más antigua de Alemania, siendo fundada en 1745 como Collegium Carolinum y es miembro de la TU9, una sociedad que incluye a los centros técnicos de más renombre de Alemania.

⁹ Para este momento aun no era reconocida como una de las universidades más reconocidas, a pesar de tener a matemáticos como Carl Friederich Gauss y Wilhelm Weber (luego profesor de Hilbert en Königsberg), tenía en esa época un nivel relativamente elemental en los cursos de matemáticas, por lo que, allí se formaban, principalmente docentes de educación media.

¹⁰ En “Über die Theorie der Eulerschen Integrale”.

¹¹ En dicha lección de habilitación mostraba su interés por los fundamentos de la matemática y su orientación reflexiva y sistemática.

¹² Habilitación de enseñanza docente en universidades alemanas, también llamado *privatdozent* (abreviado como PD o Priv.-Doz.) que es el mayor título profesional conferido por algunas universidades europeas, especialmente en los países de habla alemana. En su uso actual, el título indica que el titular tiene permiso para enseñar y supervisar a los estudiantes de grado o de doctorado en la universidad, pero sin la titularidad de una cátedra.

cual estudió teoría de números y otras materias. Para ampliar sus conocimientos, Dedekind abordó el estudio de las funciones abelianas y elípticas de la mano de Riemann con quien compartía enriquecedoras conversaciones diarias acerca de asuntos matemáticos. Tras estas experiencias, en su formación encontró al fin sus principales campos de trabajo: el álgebra y la teoría de números algebraicos.

Con Dedekind se destaca la necesidad de generalizar conceptos y originar nuevos dominios numéricos¹³, esta ampliación de dominios numéricos al adoptar posturas, tales como aceptar que el concepto de sucesor da origen a la adición, la repetición de la adición origina la multiplicación y esta última conduce al concepto de potencia, fue quizás el pilar fundamental en el trabajo matemático de Dedekind¹⁴. Esto muestra que él privilegia las operaciones con relación a los elementos individuales, es decir, predomina principalmente la búsqueda de relaciones conceptuales por encima de laboriosos cálculos. Desde siempre, Dedekind muestra inclinación por una visión estructuralista, siendo esta una corriente poco desarrollada en ese momento¹⁵. Dedekind estuvo fuertemente influenciado por las ideas de Riemann y por el pensamiento formalista de Dirichlet, del cual escucha y estudia sus lecciones sobre teoría de números, famosa por haber puesto el contenido de las *Disquisitiones arithmeticae* de Gauss al alcance de un “gran público” matemático.

Dedekind estudió a profundidad los trabajos de Abel y Galois, y como fruto de esto, fue el primero en impartir clases acerca de las ecuaciones de Galois, un curso de álgebra superior y teoría de Galois, es uno de los primeros en hacer esto: se conserva un manuscrito de sus

¹³ Inicialmente debido a la imposibilidad de realizar operaciones inversas, tales como la sustracción y la división.

¹⁴ Desde la tesis de habilitación que presenta en la universidad de Göttingen, a sus 23 años, Dedekind muestra interés en el tratamiento conceptual de la matemática.

¹⁵ Alrededor de 1860.

lecciones¹⁶ y de él se ha dicho que constituye “el primer tratamiento moderno del tema” en cuyo trabajo destaca principalmente las relaciones en términos de extensiones de cuerpos y a diferencia de sus contemporáneos no se enfoca en el estudio de las soluciones de ecuaciones. Fue además el primero en comprender el concepto fundamental de las nociones de *grupo*, *cuerpo* e *ideal* en el campo del álgebra y la geometría algebraica.

Para mostrar la influencia de Dedekind en la consolidación del álgebra abstracta (estructuralismo algebraico), se trae a colación la figura más destacada de este estructuralismo: Emmy Noether (1882 – 1935). Como lo menciona (Anaconda, 2017), Noether defendió como método general que las diferentes estructuras algebraicas como grupos y cuerpos, y otras estructuras como espacios topológicos, fuesen tratadas en términos de los homomorfismos entre ellas, conceptos que atribuye plenamente a Dedekind, y son probablemente la razón más importante para su famoso eslogan: “todo está basado en Dedekind”.

1.2 Dedekind y la construcción de los reales.

Entre los grandes aportes de Dedekind a las matemáticas, está su famosa construcción de los números reales. En un momento en el cual era absolutamente necesario fundamentar los desarrollos del cálculo y el análisis de un piso firme, Dedekind en 1872 “crea” los números irracionales a partir de un tratamiento netamente aritmético de la recta racional.

Hasta el momento la teoría de límites se apoyaba en evidencias netamente geométricas, pero Dedekind fue mucho más allá al advertir que las propiedades de orden, densidad de los números racionales, hacían posible utilizar este fenómeno para definir los reales y establecer

¹⁶ Dedekind no llegó a publicar este manuscrito, aunque cuidadosamente redactado. De hecho, tardó mucho en publicar contribuciones importantes, ya que este era bastante exigente consigo mismo en lo que a su trabajo como matemático respecta.

todas las operaciones aritméticas y propiedades. Este trabajo tardó muchos años en ser publicado, dado que Dedekind juzgaba fuertemente sus logros, dudaba en publicar sus hallazgos y se especula que era porque no concebía la originalidad de su trabajo al creer que cualquier matemático podía llegar a algo similar, pero solo hasta 1872 en un homenaje a su padre, decidió publicar su famoso artículo llamado “*Continuidad y números irracionales*”. Este artículo resultó ser una contribución importante al estudio de los fundamentos de los números reales $\mathbb{R}$ y la teoría de conjuntos, ya que propone una nueva visión y construcción de los números irracionales y desarrolla la noción de continuidad como una propiedad fundamental de los números reales, y queda caracterizado como un cuerpo de números dotado en un orden lineal continuo. Esta teoría ha sido una contribución fundamental en el campo de las matemáticas y el análisis real.

Para la construcción de los reales Dedekind emplea el concepto de *cortadura*. Una cortadura es una manera de dividir los números racionales en dos conjuntos, de modo que todos los elementos del primer conjunto sean menores que todos los elementos del segundo conjunto. Estos conjuntos no pueden tener elementos comunes y la unión debe ser todo el conjunto de los números racionales $\mathbb{Q}$. Un ejemplo de cortadura es (A_1, A_2) donde la clase $A_1 = \{x \in \mathbb{Q}: x \leq \frac{3}{2}\}$ y la clase $A_2 = \{x \in \mathbb{Q}: x > \frac{3}{2}\}$. Esta cortadura es esencialmente igual a la cortadura (B_1, B_2) donde $B_1 = \{x \in \mathbb{Q}: x < \frac{3}{2}\}$ y $B_2 = \{x \in \mathbb{Q}: x \geq \frac{3}{2}\}$.

Ambas cortaduras tienen la siguiente propiedad: existe un elemento mayor en la primera clase o un elemento menor en la segunda clase. Es decir, existe un elemento separador de las dos clases que es $\frac{3}{2}$. Esta propiedad la satisfacen todas las cortaduras que son producidas por números racionales. Sin embargo, Dedekind prueba que es posible separar el conjunto de los racionales en dos clases que verifican la propiedad de las cortaduras y sin embargo no cumplen con esta última

propiedad. Es decir, no existe un máximo en la primera clase ni un mínimo en la segunda. Tal es el caso de la cortadura (A_1, A_2) donde $A_1 = \mathbb{Q}^- \cup \{x \in \mathbb{Q}: x^2 < 2\}$ y $A_2 = \{x \in \mathbb{Q}: x^2 > 2\}$. Esto pone en evidencia la discontinuidad de los racionales, la existencia de “huecos” en la recta racional. A estas cortaduras que no son producidas por números racionales, Dedekind las denomina “números irracionales”, veamos:

Ahora, cada vez que se da una cortadura (A_1, A_2) que no está determinada por ningún número racional *creamos* un nuevo número, un número *irracional* α , que consideramos como perfectamente definido por esta cortadura (A_1, A_2) ; diremos que el número α corresponde a esta cortadura, o que él determina esta cortadura (1872/1927, p. 8).

Se trata de un acto de “creación” libre para Dedekind, propio de las prácticas matemáticas, que debe cumplir una condición fundamental: el nuevo dominio numérico debe conservar las propiedades del dominio anterior (Arbelaez & Galvez, 2011). Esta condición se conoce como *extensión algebraica*. Es el acto de pasar de un dominio, bien definido estructuralmente, a otro más rico e igualmente bien definido que conserva la estructura algebraica del primero. De esta forma, agrega a los números racionales el nuevo dominio y conforma así el nuevo dominio identificado como el conjunto de los números reales, que identifica con $\mathfrak{R}$.

En este nuevo dominio se verifican las propiedades del conjunto de los números racionales; es decir se trata de un conjunto ordenado unidimensional (I. orden de la recta, II. densidad de los reales; y III. propiedad de la cortadura¹⁸) en el que además se verifica una

¹⁸ Cualquier número $\alpha \in \mathfrak{R}$ produce una *cortadura* $(\mathcal{U}_1, \mathcal{U}_2)$ en el nuevo sistema $\mathfrak{R}$ de los números reales.

propiedad esencial que no tiene el dominio anterior y que caracteriza el nuevo dominio: la *continuidad*.

Al respecto dice Dedekind:

Pero además de estas propiedades el dominio $\mathfrak{R}$ posee también la *continuidad*, i.e., es válido el siguiente teorema: IV. Si el sistema $\mathfrak{R}$ de todos los números reales se subdivide en dos clases, $\mathfrak{U}_1$ y $\mathfrak{U}_2$ tales que cada número α_1 de la clase $\mathfrak{U}_1$ es menor que cada número α_2 de la clase $\mathfrak{U}_2$, entonces existe un y sólo un número α por el cual esa división está determinada (1872/1927, p. 11).

Este axioma garantiza que el nuevo dominio es completo. Es decir, no hay “huecos”. Este axioma tan importante que sólo verifica el conjunto de los reales equivale a decir que si A es un subconjunto no vacío de $\mathfrak{R}$ acotado superiormente en $\mathfrak{R}$, entonces A posee una cota superior en $\mathfrak{R}$.

1.3 Dedekind y la estructura de los números naturales.

Su trabajo sobre los números naturales fue también fundamental en la génesis del estructuralismo. Dedekind ofrece una fundamentación muy rigurosa de los llamados axiomas de Peano y publica en 1888 “*¿Qué son y para qué sirven los números?*”. En esta obra Dedekind explica que los números son abstracciones que utilizamos para representar y contar objetos, así como para medir magnitudes y ordenar elementos, afirma que los números no son entidades físicas ni se limitan únicamente al ámbito de la aritmética, sino que son conceptos mentales y herramientas abstractas que utilizamos para comprender mejor el mundo que nos rodea. En pocas palabras, en este artículo, Dedekind muestra el trasfondo de un análisis filosófico y matemático sobre la naturaleza y utilidad de los números y ofrece una caracterización de la

estructura del conjunto de los naturales. Los trabajos de Dedekind se encuentran en los primeros en mostrar nociones y técnicas de la teoría de conjuntos desde una mirada sistemática.

Como se indica en Reck:

Dedekind trabaja con una ingenua teoría de funciones y a conjuntos los llama “sistemas”—en segundo plano. Esta teoría de fondo es “ingenua” en dos sentidos: no está axiomatizada; permite colecciones arbitrarias de objetos como conjuntos, es decir, Dedekind acepta implícitamente un principio de comprensión sin restricciones (2003).

Teniendo en cuenta lo mencionado anteriormente, analicemos detenidamente la definición 21, 36 y 37 que Dedekind recopila en sus trabajos.

Definición 21. Por una *aplicación* φ de un sistema S se entiende una ley en base a la cual a cada elemento determinado s de S le pertenece una cosa determinada, que se llama la *imagen* de s y se designa con $\varphi(s)$; diremos también que $\varphi(s)$ corresponde al elemento s , que $\varphi(s)$ *resulta*, o es generado, a partir de s mediante la aplicación φ , que s es transformado en $\varphi(s)$ por la aplicación φ . Si T es una parte cualquiera de S , entonces la aplicación φ de S contiene al mismo tiempo una aplicación determinada de T , que nosotros para simplificar indicaremos con el mismo signo φ , es decir la aplicación que a cada elemento t del sistema T le hace corresponder la misma imagen $\varphi(t)$ que posee t como elemento de S ; llamaremos también *imagen* de T al sistema que consiste de todas las imágenes $\varphi(t)$, y lo indicaremos por $\varphi(T)$; con esto queda definido también el significado de $\varphi(S)$. Se puede considerar como ejemplo de una aplicación de

un sistema la asignación de signos o nombres determinados a sus elementos. La aplicación más simple de un sistema es aquella que transforma cada uno de sus elementos en sí mismo: esa será llamada la aplicación *idéntica* del sistema. Por comodidad en los teoremas 22, 23, 24 siguientes, relativos a una aplicación cualquiera φ de cualquier sistema S , indicaremos las imágenes de elementos s y de partes T respectivamente con s' y T' ; además convendremos que las letras latinas minúsculas y mayúsculas sin acento indicaran siempre, respectivamente, elementos y partes del sistema S (1888/1930, p. 132).

La definición de aplicación φ de un sistema (salvo por el término “ley”) empleada por Dedekind corresponde a lo que hoy conocemos una función φ desde un conjunto S .

Definición 36. Sea φ una aplicación, similar²⁰ o no, de un sistema S , y sea $\varphi(S)$ parte de un sistema Z , diremos entonces que φ es una aplicación de S en Z y que S está representado en Z mediante φ . Por lo tanto, cuando $\varphi(S) \subseteq S$ llamamos a φ una aplicación de S en sí mismo, y en este párrafo queremos estudiar las leyes generales de una aplicación de tal género. Al hacer esto usaremos las mismas notaciones que en el § 2, poniendo otra vez $\varphi(S) \subseteq S'$, $\varphi(T) \subseteq T'$. Estas imágenes S' y T' son elementos y partes de S , lo mismo vale para todas cosas designadas con letras latinas. (1888/1930, p. 139)

Notemos que, en esta definición, Dedekind contemplaba intuitivamente la noción de función de un conjunto en otro y la noción de endomorfismo al contemplar funciones cuyo

²⁰ Dedekind hace referencia a una función $1 - 1$ cuando se refiere a una función similar.

espacio inicial y final son el mismo. Si pusiéramos la definición 36 en términos más prácticos y modernos, podríamos interpretarla de la siguiente manera:

Sea φ una función de un conjunto S y sea $\varphi(S)$ parte de un conjunto Z , diremos entonces que φ es una función de S en Z y que S está representado en Z mediante φ . Por lo tanto, cuando $\varphi(S) \subseteq S$ llamamos a φ una función de S en sí mismo, luego decimos que $\varphi(S) = S'$ lo que representa a su vez elementos y partes de S .

Definición 37. K se llama una cadena, cuando $K' < K$. Señalamos explícitamente que este nombre no corresponde de por sí a la parte K del sistema S , sino que solo se le asigna una relación a la aplicación φ , en relación con otra aplicación del sistema S en sí mismo K puede muy bien no ser una cadena (1888/1930, p. 140).

Reescribiendo a términos actuales podríamos presentar la definición 37 en términos más digeridos como: Decimos que K es una cadena si $\varphi(K) \subseteq K$ es decir, si se tiene que $K' \subseteq K$, para lo cual K no es estrictamente cadena por ser parte de S (podría no serlo), sino que es una característica atribuida por la relación de la función φ respecto a otra función del sistema S en sí mismo.

Tomando en cuenta las dos definiciones anteriores y lo mencionado con anterioridad, Dedekind introduce la noción de *infinito simple*. Hasta este momento podemos notar como poco a poco se vislumbra el proceso de conexión entre una definición con otra y que permiten construir un todo más completo, en este caso haciendo referencia a la estructura del conjunto de los números naturales. Veamos:

Definición 71. Un sistema N se llama *simplemente infinito*, cuando hay una aplicación φ de N en sí mismo, tal que N aparece como cadena (44) de un

elemento que no esté contenido en $\varphi(N)$. Llamamos a este elemento, que en lo que sigue queremos denotar con el símbolo 1, el elemento base de N y decimos al mismo tiempo que el sistema N simplemente infinito esta ordenado por la aplicación φ . Si conservamos las cómodas denotaciones anteriores para las imágenes y las cadenas ($\neq 4$), entonces la esencia de un sistema N simplemente infinito consiste en la existencia de una aplicación φ de N y un elemento 1 que cumple las condiciones $\alpha, \beta, \gamma, \delta$:

$$\alpha. N' \subseteq N$$

$$\beta. N = 1_0$$

γ . El elemento 1 no está contenido en N'

δ . La aplicación φ es similar.

Evidentemente se sigue de $\alpha, \beta, \gamma, \delta$, que cada sistema simplemente infinito N es efectivamente un sistema infinito (64), porque es semejante a una parte propia N' de sí mismo²¹ (1888/1930, p. 151).

En esta definición Dedekind afirma que un sistema N es simplemente infinito si existe una función φ sobre N ($\varphi: N \rightarrow N$) y un primer elemento 1²², que cumple con las siguientes condiciones: (i) la imagen de N bajo φ es subconjunto de N ($\varphi(N) \subseteq N$), (ii) a partir del elemento base “1” se tiene N , es decir la comunidad de cadenas tienen a 1 como elemento común y tomadas en su totalidad dan como resultado N , (iii) el elemento base 1 no es elemento de la imagen de N bajo φ ($1 \notin \varphi(N)$); y (iv) φ es una función uno a uno y sobre.

²¹ los ítems anteriores corresponden a los famosos axiomas de Peano, o también conocidos como los axiomas de Dedekind-Peano.

²² aquí el 1 no hace referencia como tal al número 1, realmente el primer elemento puede ser cualquiera

Hasta este punto es importante reconocer que los ítems anteriores corresponden a los famosos axiomas de Peano, o también conocidos como los axiomas de Dedekind-Peano.

Dedekind asume la existencia de conjuntos infinitos, sin hacer uso del axioma del infinito como se haría actualmente. Dedekind hace uso del razonamiento, la prueba inicia suponiendo “la totalidad S de las cosas que pueden ser objetos de mi pensamiento” se selecciona un objeto particular a en S para establecer lo siguiente: la cadena sobre a formada por la función

$$f: x \rightarrow “x \text{ puede ser el objeto de mis pensamientos}”$$

Está contenida en S y como subconjunto, forma un infinito simple. Como era de esperarse este tipo de planteamientos fueron fuertemente criticados por otros matemáticos de la época, quienes argumentaban la falta de coherencia al referirse a “objetos indefinidos” en el plano de los números. Sin embargo, a lo que Dedekind apuntaba por medio de estos razonamientos donde no es relevante la naturaleza del objeto mismo, sino las relaciones con las que este se desenvuelve en un sistema, entonces desde este punto es clave identificar que en sus razonamientos se avistaban ya sus inclinaciones estructuralistas. Esto se ve mayormente reflejado en su definición 73. Veamos:

Definición 73. Si en la consideración de un sistema N simplemente infinito ordenado por una aplicación φ se prescinde por completo de las características específicas de los elementos, se mantiene fundamentalmente su distinción y solo se consideran las relaciones que se establecen mediante la aplicación ordenadora φ , entonces estos elementos se llaman números naturales o números ordinales y también simplemente números, y el elemento base 1 se llama el número base de la sucesión numérica N . Con referencia a esta liberación de los elementos de todo otro contenido (abstracción) se puede denominar con derecho a los números una

creación libre del espíritu humano. Las relaciones o leyes, que se derivaran exclusivamente de las condiciones $\alpha, \beta, \gamma, \delta$ de la *definición 71*, y que por esto son las mismas siempre en todos los sistemas simplemente infinitos ordenados, sean los que fueren los nombres dados ocasionalmente a los elementos particulares (cf.134), conforman el objeto inmediato de la ciencia de los números o aritmética. De los conceptos generales y teoremas del $\S 4$ sobre la aplicación de un sistema en si mismo tomamos inmediatamente los siguientes teoremas fundamentales, donde se entendera por $a, b, \dots m, n \dots$ siempre elementos de N , por lo tanto números; por $A, B, C, \dots$ partes de N ; por $a', b' \dots m', n' \dots A', B', C' \dots$ las imágenes correspondientes, que son generadas por la aplicación ordenadora φ y siempre son a su vez elementos o partes de N ; la imagen n' de un número n se denominara el número siguiente a n (1888/1930, p. 152).

Nótese que particularmente esta definición refuerza lo anteriormente mencionado al afirmar que Dedekind descuida el carácter especial de los elementos, es la abstracción que hace con ellos lo realmente relevante para la concepción de los números naturales, cuyo conjunto es el sistema base de otros conjuntos.

Este novedoso enfoque estructuralista con el que Dedekind presenta el conjunto de los números naturales constituye un gran referente histórico que lo ubica como precursor del estructuralismo matemático. Esto también lo podemos ver en su “*Teorema 132* el cual expresa que todos los sistemas simplemente infinitos son semejantes a la sucesión numérica N y por consiguiente también entre sí” (Dedekind, 1888/1930, p. 172).

Hasta este punto es importante reconocer que, Dedekind en esta visión de los números naturales con un primer elemento y la función sucesor, evidencia que cualquier otro sistema simplemente infinito puede ser isomorfo a esta. Dedekind ofrece una definición de los números naturales muy distinta a la tradicional, proveniente desde la antigüedad griega, en la que prevalecía los entes individuales que la conformaban.

Lo que Dedekind observa es básicamente, que la categoricidad de su noción de “infinito simple” y la definición 73 constituye una estructural presentación del conjunto de los números naturales, aunque no denomine a sus cuatro condiciones $\alpha, \beta, \gamma, \delta$ como “axiomas” ni utilice un modelo de lenguaje formal (Reck, 2003).

Tal como lo expresan Ortiz y Valencia en su artículo:

La importancia de este teorema radica en que es un teorema de categoricidad: todos los modelos de los naturales son isomorfos. Así pues, la categoricidad que Dedekind impone a los naturales implica que estos sean vistos desde una perspectiva estructural, puesto que lo que existe es la estructura que permite expresar los teoremas de la aritmética y, así como los naturales lo hacen (es un modelo de dicha estructura), otro conjunto isomorfo a $\mathbf{N}$ también puede expresar dichos teoremas (2010, p. 44).

Capítulo 2

El germen de la teoría de los ideales de Dedekind.

Con el propósito de que este capítulo sea autocontenido, se presentan en primer lugar algunos conceptos básicos del álgebra, en torno a la noción de *ideal*, que se requieren para el análisis histórico que se realiza posteriormente sobre los trabajos de Dedekind. Para el desarrollo de esta primera parte se retoman como referencia el libro de Marco Panza (Panza, 2007/2019), y los cuadernos de Lezama (Lezama, 2017).

2.1 Conceptos básicos de la teoría de ideales.

Se inicia con una presentación de los conceptos básicos del álgebra hasta llegar a la noción de *ideal*, clave en nuestro estudio. Algunas de las definiciones se ilustran con ejemplos y comentarios para su mejor comprensión.

Definición 2.1: Una operación³² binaria es conocida como *ley de composición interna* en un conjunto E , es una función $*$: $E \times E \rightarrow E$ del producto cartesiano de E con E en E , es decir, se garantiza la cerradura. Así a cada par ordenado (x, y) de elementos de E se le asigna un único elemento de E . La imagen del par (x, y) mediante la función $*$ se denota por $x * y$.

Definición 2.2: Se le llama *magma* a una pareja $\langle E, * \rangle$ compuesta por un conjunto cualquiera E y una operación $*$ definida sobre los elementos de E , una operación de este tipo es conocida como una ley de composición interna.

Ejemplos: $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{N}, \cdot \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{R}, \cdot \rangle$, $\langle \mathbb{C}, + \rangle$, $\langle \mathbb{C}, \cdot \rangle$.

³² En la actualidad el término “operación” conlleva implícitamente a que la relación es clausurativa y uniforme.

Nótese que cualquier conjunto cuya operación sea clausurativa bajo ese conjunto es un *magma*.

Definición 2.3: Un *magma asociativo* se define como una pareja $\langle E, * \rangle$ con una ley de composición interna definida sobre el conjunto E , tal que $\forall x, y, z \in E$ se tiene que $[z * (x * y) = (z * x) * y]$. A un magma asociativo también se le conoce como *semigrupo*.

Ejemplos: $\langle \mathbb{N}, \cdot \rangle, \langle \mathbb{R}, + \rangle, \langle \mathbb{Z}, \cdot \rangle, \langle \mathbb{Q}, + \rangle$.

Definición 2.4: Un *magma conmutativo* se define como una pareja $\langle E, * \rangle$ con una ley de composición interna definida sobre el conjunto E , tal que para $x, y \in E$ se tiene que $(x * y) = (y * x)$.

Ejemplos: $\langle \{-2, 2\}, \cdot \rangle, \langle \mathbb{N}, + \rangle, \langle \mathbb{Z}, \cdot \rangle, \langle \mathbb{Q}, + \rangle$.

Definición 2.5: Se define *monoide* como un magma asociativo y unitario (con un elemento identidad o neutro). Es decir, una pareja $\langle E, * \rangle$ es un monoide si cumple que:

I. $\forall x, y$ perteneciente a E , $x * y$ pertenece a E ;

II. $\forall x, y$ perteneciente a E , $(x * y) * z = x * (y * z)$;

III. Existe en E un elemento e , llamado el elemento *neutro* de $*$ tal que para todo x que pertenece a E , $x * e = e * x = x$.

Ejemplos:

$$\langle \mathbb{N}, + \rangle, \langle \mathbb{N}, \cdot \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{Z}, \cdot \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{Q}, \cdot \rangle$$

Definición 2.6: Se define *monoide conmutativo* a aquel que cumple la conmutatividad para los monoides.

Definición 2.7: Puede entenderse la noción de *grupo* como un monoide con inverso. Es decir, una pareja $\langle E, * \rangle$ es un grupo si cumple que:

- I. $\forall x, y$ perteneciente a E , $x * y$ pertenece a E ;
- II. $\forall x, y, z$ perteneciente a E $(x * y) * z = x * (y * z)$;
- III. Existe en E un elemento e , llamado el elemento *neutro* de $*$ tal que $\forall x$ que pertenece a E , $x * e = e * x = x$;
- IV. $\forall x$, perteneciente a E , existe en E un único elemento x^{-1} llamado elemento inverso de x con respecto a $*$ tal que, $x * x^{-1} = x^{-1} * x = e$.

Ejemplos de grupo:

$$\langle \mathbb{Z}, + \rangle, \langle \{-1, 1\}, \cdot \rangle, \langle \mathbb{Q} - \{0\}, \cdot \rangle, \langle \mathbb{R} - \{0\}, \cdot \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{C}, + \rangle.$$

Ejemplos de NO grupo:

$$\langle \mathbb{N}, + \rangle, \langle \mathbb{C}, \cdot \rangle, \langle \mathbb{Q}, \cdot \rangle.$$

Note que, en $\langle \mathbb{N}, + \rangle$ la definición de grupo no satisface la condición del inverso (ítem IV de la definición anterior), dado que los elementos inversos de $\mathbb{N}$ respecto a la operación suma se encuentran en el dominio de los $\mathbb{Z}$. Por otro lado, $\langle \mathbb{C}, \cdot \rangle$ y $\langle \mathbb{Q}, \cdot \rangle$ no cumplen la definición de grupo porque 0 no es un elemento invertible, luego, si éste es excluido, se tiene que $\langle \mathbb{C} - \{0\}, \cdot \rangle$ y $\langle \mathbb{Q} - \{0\}, \cdot \rangle$ sí poseen estructura de grupo.

Reflexionando acerca del ítem (III) y (IV) en la definición de grupo, podemos notar que el neutro es uno y solamente uno, mientras que el inverso es único, pero no uno solo. Entonces en la noción de elemento neutro no hay una existencia condicionada, es decir $\exists y \forall x$ tal que $B(x, y)$ y el cuantificador existencial actúa sobre el cuantificador universal,

mientras que, para la noción de inverso se aprecia dicha existencia condicionada, puesto que, en este caso $\forall x \exists y$ tal que $B(x, y)$.

Por otro lado, al hablar de estructuras como las de grupo, es ineludible mencionar que esta noción abstracta fue categorizada por los Bourbaki como “La unidad intrínseca de la matemática” que expresa la forma común de diversas teorías matemáticas. Su razón de ser presentó para atender el efecto unificador de las teorías matemáticas tras la instauración del método axiomático.

Las estructuras son constructos resultantes de unas reglas de construcción. En cuanto tales, los axiomas estipulan qué propiedades posee el tipo de estructura que ellos determinan, que son las propiedades de las relaciones definidas entre un conjunto de elementos cuya naturaleza es indiferente (Vélez, 2013).

Definición 2.8: Un grupo $\langle E, * \rangle$ es *conmutativo*, si para cualesquiera elementos x, y que pertenecen a E se cumple la propiedad conmutativa, es decir, $x * y = y * x$, en tal caso decimos que el grupo es *abeliano*.

Ejemplos de grupo abeliano:

$$\langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle, \langle \mathbb{C}, + \rangle$$

Definición 2.9: Sea $\langle E, *, 1 \rangle$ ³³ un grupo y $\emptyset \neq S \subseteq E$. Si S posee estructura de grupo, se dice que es un *subgrupo* de E respecto a la operación $*$ si y solo si, se cumplen las siguientes condiciones:

I. Si x, y pertenece a S entonces $x * y$ pertenece a S ;

³³ La notación $\langle E, *, 1 \rangle$ también denota un grupo, pero se destaca el elemento identidad.

II. Si x pertenece a S entonces x^{-1} pertenece a S .

Ejemplos de subgrupo:

$$\langle \{-1, 1\}, \cdot \rangle, \langle \{1\}, \cdot \rangle$$

Nótese que, $\langle \{1\}, \cdot \rangle$ es subgrupo de $\langle \{-1, 1\}, \cdot \rangle$, por otro lado, $\langle \{-1, 1\}, \cdot \rangle$ y el mismo $\langle \{1\}, \cdot \rangle$ son subgrupos de $\langle \mathbb{Q} - \{0\}, \cdot \rangle$. Sin embargo, $\langle \{-1\}, \cdot \rangle$ no es un grupo.

2.1.1 Anillo, cuerpo y dominio de integridad.

Se presentan a continuación los conceptos fundamentales sobre los cuales se define la noción de *ideal*.

Definición 2.10: Se denomina *anillo* a la terna $\langle E, *, \star \rangle$ compuesta por el conjunto E y dos operaciones definidas $*$ y $\star$ sobre E tales que:

- I. $\langle E, * \rangle$ es un grupo abeliano;
- II. $\langle E, \star \rangle$ es un magma asociativo;
- III. $\star$ es distributiva sobre $*$;
- IV. Si $\star$ es conmutativa el anillo es *conmutativo*;
- V. Si $\star$ tiene elemento neutro E , distinto del elemento neutro de $*$ entonces el anillo es *unitario*.

Ejemplo de anillos:

$$\langle \mathbb{Z}_6, +, \cdot \rangle, \langle \mathbb{Q}, +, \cdot \rangle, \langle \mathbb{R}, +, \cdot \rangle, \langle M_{2 \times 2}(\mathbb{R}), +, \cdot \rangle.$$

Sea $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$, es evidente que este conjunto es cerrado para la suma y el producto, y como estas operaciones son asociativas y conmutativas en $\mathbb{R}$, también lo

son en $\mathbb{Q}(\sqrt{2})$, de la misma manera se comprueba que el producto es distributivo respecto a la suma, además $0 = 0 + 0\sqrt{2}$ y $1 = 1 + 0\sqrt{2}$ que pertenecen a $\mathbb{Q}(\sqrt{2})$, y para todo $x = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ se verifica que $(-x) = (-a) + (-b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, en tanto, $\mathbb{Q}(\sqrt{2})$ es un anillo.

Ejemplo de NO anillo:

$$\langle \mathbb{Z}, \cdot, + \rangle, \langle \mathbb{N}, +, \cdot \rangle.$$

Es importante reconocer que tanto $\cdot$ como $+$ definen dos operaciones de cualquier naturaleza y no únicamente la suma y el producto. Ahora bien, analizando detenidamente la terna $\langle \mathbb{Z}, \cdot, + \rangle$, no posee estructura de anillo porque la operación $+$ que representa $\cdot$ en la definición, no distribuye al producto $\cdot$ que representa a $+$. Es decir, la terna incumple la condición *III* en la definición de anillo.

Por otro lado, la terna $\langle \mathbb{N}, +, \cdot \rangle$ tampoco posee estructura de anillo porque $\langle \mathbb{N}, + \rangle$ no representa un grupo abeliano, y esto se debe a que $\langle \mathbb{N}, + \rangle$ no tiene estructura de grupo porque los elementos inversos de $\mathbb{N}$ no están en $\mathbb{N}$.

Definición 2.11: Se le llama *cuerpo* a un anillo unitario $\langle E, \cdot, + \rangle$ que cumpla las siguientes características:

- I. $\langle E - \{e\}, + \rangle$ es un grupo;
- II. Todos los elementos de E , salvo e son invertibles respecto a $+$;
- III. $\langle E, + \rangle$ Sea un grupo abeliano;
- IV. La operación $\cdot$ sea distributiva sobre $+$;
- V. Si $\cdot$ es además conmutativa en E , entonces el cuerpo es llamado *conmutativo*.

Ejemplos de cuerpo:

$$\langle \mathbb{Q}, +, \cdot \rangle, \langle \mathbb{R}, +, \cdot \rangle, \langle \mathbb{C}, +, \cdot \rangle$$

Ejemplos de NO cuerpo:

$$\langle \mathbb{Q}, \cdot, + \rangle, \langle \mathbb{Z}, +, \cdot \rangle, \langle \mathbb{Z}, \cdot, + \rangle$$

Como ya se mencionó anteriormente $\langle \mathbb{Q}, \cdot, + \rangle, \langle \mathbb{Z}, \cdot, + \rangle$ no poseen estructura de grupo porque la operación suma no distribuye al producto, en tanto, tampoco representan una estructura de cuerpo.

Identifiquemos ahora que la terna $\langle \mathbb{Z}, +, \cdot \rangle$ tampoco es un cuerpo porque los elementos invertibles del conjunto $\mathbb{Z}$ bajo el producto se encuentran en el dominio de los números $\mathbb{Q}$.

Definición 2.12: Un anillo *trivial* o nulo, es aquel que posee un único elemento y su elemento nulo coincide con su elemento identidad.

Definición 2.13: Se dice que $a \in A$ es un *elemento invertible* del anillo A , si existe en A un único elemento que denotado por a^{-1} que cumpla que $aa^{-1} = 1 = a^{-1}a$. El conjunto de todos los elementos invertibles de un anillo A se denota por A^* , entonces, $A^* := \{a \in A | a \text{ es invertible}\}$.

Definición 2.14: Sea A un anillo no nulo, se dice que A es un *anillo de división* si todos los elementos no nulos de A son invertibles.³⁴

Definición 2.15: Un anillo A es *sin divisores de cero* si en su estructura se cumple que, para cualesquiera $a, b \in A$ se tiene que $ab = 0 \leftrightarrow a = 0 \vee b = 0$.

Ejemplos:

³⁴ Un cuerpo es un anillo de división conmutativo

$\mathbb{R}$ es un anillo *sin divisores de cero* porque $\forall a, b \in \mathbb{R}$ tales que $ab = 0 \leftrightarrow a = 0 \vee b = 0$.

$\langle M_{2 \times 2}(\mathbb{R}), +, \cdot \rangle$ es un anillo *con divisores de cero* porque $\exists a, b \in M_{2 \times 2}(\mathbb{R})$ tales que $ab = 0 \leftrightarrow a \neq 0 \wedge b \neq 0$

$$\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Definición 2.16: Un anillo sin divisores de cero se le conoce como *dominio*; si además es conmutativo, se conoce como *dominio de integridad* (DI).

2.1.2 El concepto de Ideal.

Ahora si estamos en condiciones de presentar el concepto fundamental del presente capítulo.

Definición 2.17: Dado A un anillo e I un subconjunto no vacío de A , se dice que I es un *ideal izquierdo* de A , si $x + y \in I$ para todo $x, y \in I$, y además, $ax \in I$ para todo $a \in A$ y todo $x \in I$.

Definición 2.18: Dado A un anillo e I un subconjunto no vacío de A , se dice que I es un *ideal derecho* de A , si $x + y \in I$ para todo $x, y \in I$, y además, $xa \in I$ para todo $x \in I$ y todo $a \in A$.

Definición 2.19: Se dice que I es un *ideal bilatero* o *ideal* de A , si I es un ideal izquierdo y derecho de A .

Definición 2.20: Se dice que el sistema I que cumple las siguientes dos condiciones se considera un ideal:

1. Las sumas y las diferencias de dos números cualesquiera del sistema I son siempre números del mismo sistema I .
2. Todo producto de un número del sistema I por un número del sistema B es un número del sistema I .

Ejemplo:

Si I es un ideal de $\mathbb{Z}$, entonces I es un subgrupo de $\langle \mathbb{Z}, +, 0 \rangle$ y, por lo tanto, está conformado por los múltiplos de algún entero no negativo n , es decir, I es de la forma $n\mathbb{Z}$. Es claro que cada uno de estos conjuntos es un ideal de $\mathbb{Z}$.

Definición 2.21: En un anillo A , tanto A como el conjunto $0 := \{0\}$ se denominan *ideales triviales* del anillo A .

Definición 2.22: Para cualquier anillo A , un ideal no trivial, será un *ideal propio*.

Definición 2.23: Se dice que I es un *ideal primo* de A si para cualesquiera I_1 e I_2 ideales bilateros de un anillo A se tiene que $I_1 I_2 \subseteq I \leftrightarrow I_1 \subseteq I, o, I_2 \subseteq I$.

Definición 2.24: Sea R un DI y sean a, b elementos no nulos de R . El elemento $d \in R$ se dice que es un *máximo común divisor* de los elementos a y b sí:

I. $d|a$ y $d|b$

II. Cada elemento $c \in R$ que divida simultáneamente a y b es también un divisor de d .

Este elemento se denota por $d := m. c. d. (a, b)$.

Definición 2.25: Sea R un DI y sean a, b elementos no nulos de R . Un *mínimo común múltiplo* de a y b es un elemento $c \in R$ tal que:

I. $a|c$ y $b|c$.

II. Cada elemento $f \in R$ tal que $a|f$, y $b|f$ cumple $c|f$.

Este elemento se denota por $c := m. c. m. (a, b)$.

Con todos estos elementos conceptuales claros, estamos en condiciones de revisar desde el punto de vista histórico, los trabajos de Dedekind en torno a la teoría de ideales.

2.2 Los ideales de Dedekind: breve contextualización histórica.

La teoría de los ideales de Dedekind es un intento por generalizar la teoría de los números primos ideales introducida por Ernest Kummer en 1844. Uno de los aspectos más relevantes, relacionados con el estudio de la teoría de cuerpos de números algebraicos, fue la contribución de Dedekind relacionada con el concepto de “ideal”. Este concepto fue desarrollado para abordar el asunto de la factorización única en dominios generalizados de números enteros, desde una perspectiva unificada y general. En las obras de Dedekind se destaca el aspecto metodológico de sus contribuciones. Sus teoremas generalizados sobre factorización fueron siempre formulados en términos de colecciones de números y operaciones entre estas colecciones (especialmente entre ideales) más que en términos de números individuales. “Esta aproximación de Dedekind, en la que se privilegia el estudio de las propiedades de la colección de números frente al número como ente individual, es otro aspecto que da cuenta del pensamiento relacional y estructural de Dedekind” (Anaconda, 2017).

Es importante mencionar que anterior a Gauss, la aritmética se presentaba como una especie de saber constituido por hechos aislados. Es Gauss quien, además de simplificar los aportes de sus predecesores, con su obra “*Disquisitiones Arithmeticae*” en 1801, afianza las bases fundamentales de teoría de números y le otorga una auténtica dimensión científica. No obstante, hasta esa época, la teoría de números era concebida como un tratado únicamente de

enteros. Pero el enfoque de Dedekind consistió principalmente en la formulación de un nuevo marco conceptual y del cual se tiene un progreso más fructífero a través de la introducción de nuevos conceptos, de los cuales su representación no está sujeta a una representación notacional, para obtener la mayor generalidad posible.

Aunque en los libros de aritmética de los *Elementos* de Euclides³⁵ hay evidencia de importantes teoremas que relacionan los números naturales con sus factores primos, fue Gauss el primero en plantear de manera más rigurosa el teorema y presentar una demostración en las *Disquisitiones Arithmeticae*. Este problema es conocido como *el teorema fundamental de la aritmética*, el cual afirma que cada número natural puede ser expresado de manera única (excepto quizás por el orden) como producto de sus factores primos.

Más tarde, al intentar formular leyes de reciprocidad para casos individuales de grados superiores³⁶, Carl Gustav Jacobi consideró enteros complejos que involucraban raíces de unidad de los grados quinto, octavo y duodécimo por separado, y los factorizó mientras asumía las propiedades habituales de los números naturales.

Actualmente, se conoce como *enteros ciclotómicos* a todo θ que es raíz p –ésima primitiva de la unidad de números cuya forma son $a_0 + a_1\theta + \dots + a_n\theta^n$ con $a_i \in \mathbb{Z}$, es decir, un número complejo diferente de 1 tal que $\theta^p = 1$. A partir del estudio de los enteros ciclotómicos, Kummer desarrolló sus aportes a las leyes de reciprocidad superior³⁷. Kummer descubrió que la factorización única no se cumple para estos dominios de números cuando $p \geq 23$, de hecho, solo se cumple para valores de p inferiores a 23, este descubrimiento fue

³⁵ Libros VII y IX

³⁶ Por grados superiores hacemos referencia a ecuaciones de grado mayor a dos.

³⁷ Estas leyes eran vistas por Kummer como pilar fundamental en el estudio de la teoría de números.

publicado en 1844. Durante los años siguientes, Kummer dedicó considerables esfuerzos en desarrollar su teoría de los *números primos ideales*, con el objetivo de revertir este desafortunado hallazgo.

En particular, el trabajo de Dedekind fue inspirado principalmente por su admiración hacia Fermat y Kummer, y por las maravillosas contribuciones que realizó Dirichlet al álgebra, al recopilar en *Disquisitiones arithmeticae* el trabajo de Gauss y analizarlo de manera minuciosa, lo que permitió que todos estos resultados estuvieran al alcance del entendimiento de muchos matemáticos. Dedekind publicó una primera versión del extenso trabajo de Dirichlet acerca de la teoría de los números enteros algebraicos hacia 1862, pero la teoría elaborada hasta ese momento no se encontraba desarrollada de manera tan general, cosa que desilusionó a Dedekind dado que este era exigente a la hora de juzgar sus propios logros.

Por tanto, en 1872 publica una segunda versión de las *Vorlesungen de Dirichlet* (Las conferencias de Dirichlet), en este punto la teoría de los enteros algebraicos se convertía en una teoría de ideales en anillos de enteros en cuyo desarrollo se veía reflejado un lenguaje conjuntista³⁸ y mediante esta transformación se lograba la generalidad deseada por Dedekind. Sin embargo, más adelante, alrededor de 1879 y 1893 se publican dos nuevas versiones de su trabajo, con la intención de tratar integralmente el problema de la descomposición en factores primos únicos en campos de números algebraicos, cuyos métodos se encontraban cada vez más perfeccionados y su punto de partida eran las definiciones de estructuras conjuntistas.

³⁸ Para esta época, los trabajos en álgebra se enfocaban principalmente en el estudio de ecuaciones, desde luego su trabajo poseía para sus contemporáneos un nivel de dificultad mayor, por lo que solo hasta 1890 encontró continuadores.

David Hilbert y Emmy Noether trabajaron en la generalización de estas ideas. Particularmente, el artículo de Noether de 1921 sobre “teoría de ideales en anillos”, convirtió los ideales de números enteros de Dedekind en *ideales*; es decir, subconjuntos definidos axiomáticamente en cualquier conjunto con estructura de anillo. Este trabajo es considerado pionero para el desarrollo del álgebra abstracta.

En un esfuerzo por presentar y clarificar las ideas de Dedekind planteadas en su teoría de los ideales, empezamos por distinguir los conceptos que para la época se interpretaban de una manera diferente a la actual. En un principio, el estudio de la teoría de números giraba en torno a los llamados números *enteros racionales*, que actualmente hace referencia a los números *enteros*³⁹ $\mathbb{Z}$. Dedekind afirma que estos números son *estables* bajo la adición, sustracción y el producto, nótese aquí que Dedekind empieza a caracterizar una de las propiedades de los enteros que ahora conocemos como *propiedad clausurativa*. Dedekind también afirmaba que la teoría de la divisibilidad prioriza la combinación de los números mediante la multiplicación, muestra algunas características al mencionar que no tiene hay divisores de cero; las dos unidades ± 1 dividen a cualquier número, luego, si a es divisible por b , entonces $\pm a$ será también divisible por $\pm b$.

Además, sabemos desde Euclides que: i) un número a es *divisible* por un número b cuando $a = bc$, siendo a, b, c números enteros, ii) que todo número positivo, diferente de la unidad, es un número *primo*, cuando un número es divisible solamente por sí mismo y por la unidad, y iii) es un número *compuesto* si puede expresarse como producto de números primos

³⁹ El conjunto de los enteros $\mathbb{Z}$ forma un anillo con las operaciones de suma y producto.

cuya descomposición es única. Por Euclides sabemos que un número no puede dividir a un producto, si no divide al menos a uno de los factores.

Hacia 1872, Dedekind generaliza la noción de número entero y define un número *entero algebraico* θ como aquel que satisface una ecuación de la forma:

$$\theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \dots + a_{n-1}\theta + a_n = 0$$

de grado finito n y con coeficientes $a_1, a_2, \dots, a_{n-1}, a_n$ todos enteros racionales.

Tal como lo afirma Dedekind:

De esta definición resulta inmediatamente que las sumas, las diferencias y los productos de números enteros son todos también números enteros; por consiguiente, un número entero α se denominará *divisible* por un número entero β , si se tiene que $\alpha = \beta \cdot \gamma$, siendo γ igualmente un número entero. Un número entero ε se llamará una *unidad*, cuando cualquier número entero sea divisible por ε . Por analogía, se debería entender por número *primo* un número entero α que no sea unidad y que sólo tenga como divisores las unidades ε y los productos de la forma $\varepsilon \cdot \alpha$ (1872, p. 32).

El mismo Dedekind explica que en este dominio no existen los números primos, puesto que todo entero que no es una unidad puede ser siempre puesto bajo la forma de un producto de factores, los cuales son números enteros, pero no unidades. Sin embargo, esto se puede resolver si sólo se consideran ecuaciones *irreducibles*. Este sistema es idéntico al sistema de todos los números *enteros racionales* para el caso de la ecuación $\varphi(\theta) = x_0 + x_1\theta$; ó al sistema de los números *enteros complejos* para el caso de la ecuación $\varphi(\theta) = x_0 + x_1\theta + x_2\theta^2$ y $\theta = \sqrt{-1}$.

El problema que se plantea Dedekind es “establecer las leyes generales de la divisibilidad que gobiernan a este sistema”.

Para comprender con mayor claridad el surgimiento de la teoría de ideales de Dedekind es importante reconocer que ésta tiene como interés el problema de la factorización única y el problema de la divisibilidad. La cuestión consiste básicamente en saber si los *enteros algebraicos* se comportan como los enteros racionales en lo que respecta a su descomposición única en factores primos. Ellos surgen al tratar de hallar soluciones enteras a ciertas ecuaciones de la teoría de números, tales como el famoso teorema de Fermat, y aquellas congruencias polinómicas de la forma $x^m \equiv p \pmod{q}$ donde p y q son primos impares y $x, m \in \mathbb{Z}^+$.

2.2.1 Los números enteros complejos de Gauss.

El primer y gran avance hacia la generalización de estas nociones fue realizado por Gauss quien extendió la noción de número entero al dominio⁴⁰ de los números complejos, llamados *enteros complejos* o *enteros gaussianos*. Los enteros complejos se constituyen al introducir los números de la forma $x + y\sqrt{-1}$, donde x e y son números enteros racionales cualesquiera y $\sqrt{-1} = i$; es decir, una raíz de la ecuación cuadrática irreducible $i^2 + 1 = 0$. Modernamente, podemos expresar los enteros complejos o gaussianos como el anillo $\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}\}$.

Gauss probó que las leyes generales de la divisibilidad de estos números son idénticas a las que gobiernan el dominio de los números enteros racionales, y como consecuencia, en 1832

⁴⁰ La palabra *dominio* hace referencia a los anillos conmutativos y unitarios. Esta última condición afirma que el elemento neutro de la primera operación no es el mismo de la segunda. Por ejemplo, los enteros con la suma y el producto forman un dominio. Los números complejos con la suma y el producto también forman un dominio. Un *dominio de integridad*, dominio íntegro, anillo íntegro o dominio entero es un anillo conmutativo que carece de elementos divisores de cero (si $a \cdot b = 0$ entonces $a = 0$ ó $b = 0$). Los enteros con la suma y el producto conforman un dominio de integridad.

dentro de su elaboración planteó una *ley de reciprocidad para residuos bicuadráticos*⁴¹. Esta ley expresa que dado un número primo p , cualquier número q (q primo relativo con p), se llama *residuo cuadrático de p* si existe un entero racional z tal que $z^2 \equiv q \pmod{p}$, es decir, si la diferencia $z^2 - q$ es divisible por p . Además, Gauss probó que esta propiedad es recíproca, esto es, q es residuo cuadrático de p si y solo si p es residuo cuadrático de q ⁴². “El estudio de leyes de reciprocidad se convirtió en la principal motivación directa para el estudio de formulaciones generalizadas de teoremas de factorización única” (Corry, 2004, pp. 81-82).

En el dominio de los números enteros complejos, Dirichlet hace un valioso aporte, al reconocer en las *Disquisitiones Arithmeticae* (Discusiones aritméticas) de Gauss, que las proposiciones generales sobre la composición de los enteros racionales por medio de los números primos prevalecen en los enteros complejos. Esto lo hace por medio de la noción de *norma*, la cual se denota como $N(z)$. Particularmente, si $z = x + yi$ donde x e y son enteros racionales, la *norma de z* se define como $x^2 + y^2$; que también corresponde a la norma de $x - yi$. Es decir, $x^2 + y^2$ es la norma de los dos números conjugados $x + yi$ y $x - yi$.

Se puede verificar que la norma de un producto es igual al producto de las normas de los factores, además para cualquier z dado podemos elegir un número entero complejo q tal que $N(z - q) \leq \frac{1}{2}$; si ahora hacemos que z y $m \neq 0$ sean dos enteros complejos cualesquiera y más aún $w = \frac{z}{m}$, por Euclides sabemos que $z = wm + r$ donde w y r son números enteros complejos, de tal manera que, $N(r) < N(m)$ puesto que r es el residuo de dividir z entre m .

⁴¹ Esta ley fue formulada inicialmente por el prolífico Leonhard Euler en 1783 en una carta a Goldbach, pero fue Gauss quien trece años después la probó. Esta ley también es conocida como Teorema Áureo.

⁴² “Este teorema sobre la reciprocidad cuadrática, también podría extenderse y aplicarse para probar teoremas de reciprocidad análogos para congruencias de grados mayores que dos. Sin embargo, la misma formulación de la ley obligó a Gauss a introducir un tipo particular de factores de los números primos de la forma $4n + 1$; estos factores eran de hecho números complejos” (Corry, *Modern Algebra and the Rise of Mathematical Structures*, 2004).

Observemos que hay cuatro unidades en este nuevo dominio $\pm 1, \pm i$, es decir, cuatro números que dividen a todos los números, cuya norma es igual a uno.

Con base en lo anterior, y extendiendo la analogía de los enteros racionales a los complejos, se define un número *compuesto*, un número *primo* y se puede encontrar *el máximo común divisor* de dos números complejos mediante un número finito de divisiones, de modo que se obtienen leyes generales de divisibilidad que concuerdan con las de los números racionales.

Los números complejos primos y compuestos.

En el siguiente extracto se puede ver cómo Dedekind define de lo que significa que un número entero complejo sea primo o compuesto:

Hay cuatro unidades $\pm 1, \pm i$ esto es, cuatro números que dividen a todos los números y cuya norma es, en consecuencia 1. Cualquier número distinto de cero es un número compuesto, llamado así cuando es el producto de dos factores, ninguno de los cuales es una unidad, o bien es un número primo y tal número no puede dividir un producto a menos que divida a al menos uno de los factores. Todo número compuesto puede expresarse de forma única como un producto de números primos, siempre que, por supuesto, los cuatro primos asociados $\pm q, \pm qi$ se consideren representantes del mismo número primo q (1872/1927, p. 59).

De lo anterior, podemos reconocer que el dominio de los enteros complejos muestra ciertas similitudes con el conjunto de los enteros racionales. Sin embargo, para los números *primos* podemos notar que no todo q primo en el conjunto de los números enteros racionales será también un número primo en $\mathbb{Z}[i]$. Observemos, por ejemplo, el caso del número 2, del cual sabemos que representa un número primo en el conjunto de los números enteros racionales, ya

que solo es divisible por él mismo y por la unidad. Sin embargo 2 no representa un número primo en el conjunto de los enteros complejos dado que este se puede factorizar como $2 = (1 + i)(1 - i)$, donde $(1 + i)$ y $(1 - i)$ no corresponden a unidades en $\mathbb{Z}[i]$.

Luego Dedekind, en su tratado sobre *la teoría de los números enteros algebraicos* propone la construcción del conjunto de los *números primos* q del dominio de los números complejos enteros, veamos con más detalle:

De todos los números primos positivos enteros racionales que son de la forma $4n + 3$ siendo n entero racional se tiene que, cuando $n = 0$, $4(0) + 3$ obtenemos el primo 3; cuando $n = 1$, $4(1) + 3$ obtenemos el primo 7; cuando $n = 2$, $4(2) + 3$ obtenemos el primo 11; cuando $n = 4$, $4(4) + 3$ obtenemos el primo 19; cuando $n = 5$, $4(5) + 3$ obtenemos el primo 23.

Del número $1 + i$, tenemos que $(1 - i) \cdot (1 + i) = -i(1 + i)^2$ donde el producto $(1 - i)(1 + i)$ es equivalente a $1 + 1i - 1i - i^2 = 1 - i^2 = 1 - (-1) = 1 + 1$ del cual, obtenemos el primo 2.

De los factores $x + yi$ y $x - yi$, contenidos en cualquier número primo racional p de la forma $4n + 1$ y cuya norma es $x^2 + y^2 = p$, notamos que cuando $n = 1$, $4(1) + 1$ se obtiene el primo 5 cuya norma puede expresarse como $1^2 + 2^2$; cuando con $n = 3$, $4(3) + 1$ se obtiene el primo 13 cuya norma puede expresarse como $2^2 + 3^2$; cuando $n = 4$, $4(4) + 1$ se obtiene el primo 17 cuya norma puede expresarse como $4^2 + 1^2$.

En síntesis, el conjunto de todos los números primos q del dominio de los números complejos enteros se compone:

- 1) De todos los números primos racionales que (tomados positivamente) son de la forma $4n + 3$;
- 2) Del número $1 + i$, que divide al número primo racional $2 = (1 + i)(1 - i) = -i(1 + i)^2$;
- 3) De los pares de los dos factores $a + bi$ y $a - bi$, contenidos en todo número primo racional p de la forma $4n + 1$, y cuya norma es $a^2 + b^2 = p$ (1872/1927, p. 59).

Es importante mencionar que la congruencia de los números complejos enteros puede definirse de la misma manera que en la teoría de los números enteros racionales, si se tienen z y z' dos números de la forma $x \pm yi$ entonces diremos que son congruentes si se tiene que $z - z'$ es divisible por m , y se simboliza por $z \equiv z' \pmod{m}$. Por ejemplo, $13 \equiv 3 \pmod{5}$ porque 5 divide a la diferencia $13 - 3 = 10$.

En este punto resulta ineludible reflexionar acerca de la genialidad de Dedekind al proponer el desarrollo del conjunto de los números primos en nuevos dominios como los enteros complejos. De lo anterior, podemos decir entonces que Dedekind extiende la noción de número primo planteada por Euclides a otros dominios numéricos a partir de tres condiciones que permite operar con enteros complejos.

El máximo común divisor entre dos números complejos.

Veamos cómo se puede adaptar el algoritmo euclidiano para calcular el máximo común divisor (MCD) de dos números naturales para encontrar el MCD de dos números enteros complejos. Sea $z = -8 + 51i$ y $m = -8 - i$ y encontremos el $MCD(z, m)$.

Paso 1: como $N(z) = 2665 > 65 = N(m)$ comenzamos dividiendo z por m , es decir, empezamos por encontrar los enteros complejos $q_1, r_1 \in \mathbb{Z}[i]$ tal que:

$z = q_1 m + r_1$ y $N(r_1) < N(m)$ para estimar el cociente q_1 , usamos el complejo conjugado de m para dividir z por m :

$$\frac{z}{m} = \frac{-8+51i}{-8-i} = \frac{-8+51i}{-8-i} \cdot \frac{-8+i}{-8+i} = \frac{13-416i}{65} = \frac{13}{65} - \frac{416}{65}i$$

Redondeando las componentes real y compleja de este cociente por separado al entero racional más cercano, obtenemos el entero complejo $q_1 = 0 - 6i$.

Para obtener el resto correspondiente, resolvemos $z = q_1 m + r_1$ por r_1 para obtener:

$$r_1 = z - q_1 m = (-8 + 51i) - (-6i)(-8 - i) = -2 + 3i$$

Esto concluye el primer paso del proceso, dándonos $z = \underbrace{(-6i)}_{q_1} m + \underbrace{(-2 + 3i)}_{r_1}$.

Note que $N(r_1) = 13 < 65 = N(m)$.

Paso 2: a continuación, repetimos este proceso, pero ahora dividimos el divisor anterior m por el resto anterior r_1 para encontrar los enteros complejos q_2 y $r_2 \in \mathbb{Z}[i]$ con $m = q_2 r_1 + r_2$ y $N(r_2) < N(r_1)$:

$$\frac{m}{r_1} = \frac{-8-i}{-2+3i} = \frac{-8-i}{-2+3i} \cdot \frac{-2-3i}{-2-3i} = \frac{13+26i}{13} = 1 + 2i$$

Dado que este cociente ya es un número entero complejo, no es necesario redondear en este paso; simplemente tomamos $q_2 = 1 + 2i$ y establecemos $r_2 = 0$.

Tenga en cuenta que $N(r_2) = 0 < 13 = N(r_1)$.

Habiendo llegado a un resto cero,⁴³ ahora concluimos que el MCD buscado es el resto final distinto de cero r_1 ; esto es, $MCD(z, m) = -2 + 3i$.

Para verificar que $-2 + 3i$ es un divisor común en este ejemplo, podemos desentrañar los resultados de los dos pasos para obtener lo siguiente:

$$\begin{aligned}
 m &= \underbrace{(1 + 2i)}_{q_2} \underbrace{(-2 + 3i)}_{r_1} & z &= \underbrace{(-6i)}_{q_1} \underbrace{(1 + 2i)(-2 + 3i)}_m + \underbrace{(-2 + 3i)}_{r_1} \\
 & & &= [(-6i)(1 + 2i) + 1](-2 + 3i) \\
 & & &= (13 - 6i)(-2 + 3i)
 \end{aligned}$$

Esto verifica que $-2 + 3i$ es de hecho un divisor común de m y z . Pero observe que también podríamos haber escrito estas factorizaciones de la siguiente manera:

$$\begin{aligned}
 m &= (1 + 2i)(-2 + 3i) & z &= (13 - 6i)(-2 + 3i) \\
 &= (1)[(1 + 2i)(-2 + 3i)] & &= (1)[(13 - 6i)(-2 + 3i)] \\
 &= (-i^2)[(1 + 2i)(-2 + 3i)] & &= (-i^2)[(13 - 6i)(-2 + 3i)] \\
 &= \underbrace{(2 - i)}_{-i(1+2i)} \underbrace{(-3 - 2i)}_{i(-2+3i)} & &= \underbrace{(-6 - 13i)}_{-i(13-6i)} \underbrace{(-3 - 2i)}_{i(-2+3i)}
 \end{aligned}$$

Dado que $N(-3 - 2i) = 13 = N(-2 + 3i)$, observe también que ninguno de los dos enteros complejos $-3 - 2i$ y $-2 + 3i$ es mayor que el otro cuando usamos sus normas para compararlos. En otras palabras, también se puede decir que el $MCD(z, m) = -3 - 2i$. De

⁴³ Si hubiéramos obtenido un resto distinto de cero en el paso 2, repetiríamos el proceso hasta obtener cero. Tenga en cuenta que podemos estar seguros de que este proceso se detendrá ya que la norma de estos residuos forma una secuencia decreciente de números enteros racionales no negativos.

hecho, dado que $N(\pm(-2 + 3i)) = N(\pm i(-2 + 3i))$ hay cuatro enteros complejos diferentes que pueden considerarse como el $MCD(z, m)$ en este ejemplo.

Esto puede resultar inquietante al principio, hasta que recordamos que ocurre una situación similar en el conjunto de los números enteros racionales. Por ejemplo, en los enteros positivos, decimos que $MCD(12, 5) = 3$ pero como $12 = (-4)(-3)$ y $15 = (-5)(-3)$ también tendría sentido decir que -3 es un máximo común divisor de 12 y 15. Por supuesto, normalmente evitamos este problema con los números enteros racionales al limitar nuestra atención a los factores enteros positivos. La situación con los números enteros complejos es más complicada simplemente porque una vez que sabemos que $d = MCD(a, b)$ no hay una forma sencilla de decidir cuál de los cuatro números $\pm d, \pm id$ debe tener prioridad como el máximo común divisor, esto se debe a que los cuatro números $1, -1, i, -i$ juegan un papel especial dentro del conjunto de enteros complejos.

La teoría de los enteros algebraicos se convirtió en una teoría de ideales⁴⁴ en anillos de enteros, y mediante esta transformación Dedekind fue logrando la generalidad deseada.

2.2.2 Otra generalización de los enteros racionales.

Dedekind, generaliza el conjunto de los enteros racionales a otros sistemas numéricos, y lo hace estudiando números de la forma $\mathbb{Z}[\theta] = \{x + y\theta : x, y \in \mathbb{Z}\}$ pero para valores $\theta \neq i$.

En cada uno de estos dominios, como es fácil de comprobar, se puede encontrar el máximo común divisor de dos números mediante un número finito de divisiones, y de ahí se sigue inmediatamente que las leyes generales de la divisibilidad coinciden con las que tienen

⁴⁴ Un ideal (en un anillo de números) es un conjunto de infinitos números enteros del anillo, cerrado para la suma y también para la multiplicación por números cualquiera del anillo. Para todo entero k , el conjunto $k\mathbb{Z}$ es un ideal de $\mathbb{Z}$.

lugar para los números racionales. Para Dedekind estos conjuntos pueden tratarse absolutamente de la misma manera que el conjunto de los enteros complejos $\mathbb{Z}[i]$. Sin embargo, en el dominio de los números $x + y\sqrt{-5}$ las leyes generales de la divisibilidad no se cumplen. Este fue el hecho que condujo a Kummer⁴⁵ a la creación de los números ideales⁴⁶.

En el dominio $\mathbb{Z}[\sqrt{-5}]$ falla la facturación única. Un sencillo ejemplo permite verlo. En este dominio se tiene que $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ donde los cuatro factores son primos.

Inicialmente este problema ya había sido abordado por Fermat, en el desarrollo de esta problemática, presenta que un número primo $p = 4n + 1$ puede ser expresado como la suma de dos cuadrados, es decir, interpretado como la hipotenusa de un triángulo rectángulo, pero incluso, llegó aún más lejos, al notar que un producto de dos números de esta forma también se pueden ver como una suma de cuadrados; en su búsqueda por hallar respuestas, en este proceso descubrió tres teoremas sobre la representación de primos impares⁴⁷, mediante las formas $x^2 + y^2$, $x^2 + 2y^2$ y $x^2 + 3y^2$ cuyas demostraciones se basan en un procedimiento conocido como descenso infinito, estos teoremas son:

Teorema 1: Para todo primo impar p se tiene que $p = x^2 + y^2 \leftrightarrow p \equiv 1(mod4)$

Teorema 2: Para todo primo impar p se tiene que $p = x^2 + 2y^2 \leftrightarrow p \equiv 1o3(mod8)$

Teorema 3: Para todo primo impar p se tiene que $p = x^2 + 3y^2 \leftrightarrow p \equiv 1(mod3)$

⁴⁵ A raíz de esta línea de desarrollo, Ernst Edward Kummer (1810-1893) entró en escena con su teoría de los números primos ideales (Corry, Modern Algebra and the Rise of Mathematical Structures, 2004).

⁴⁶ Aunque Kummer fue el primero en trabajar con números ideales y su divisibilidad, fue Dedekind quien realmente los definió y desarrolló su dominio.

⁴⁷ Los primos impares hacen referencia a todo primo diferente de 2

Para valores enteros de x e y ; pero lo único que pudo decir acerca de $x^2 + 5y^2$ es que resulta de multiplicar dos números de la forma $20k + 3$ o $20k + 7$. Por Fermat (1654) también se sabe que, si se multiplican 2 primos que terminan en 3 o 7 y superan en 3 a un múltiplo de 4, entonces su producto está compuesto por un cuadrado y el quíntuple de otro cuadrado.

Fermat estuvo fuertemente inspirado por los aportes de Diofanto⁴⁸, de los cuales podemos rescatar un caso particular en el que expone que 65 puede ser representado como una suma de dos cuadrados, es decir, $7^2 + 4^2$ y $8^2 + 1^2$, lo cual se debe al hecho de que 65 es el producto de 13 y 5 y a su vez cada uno de los cuales es también la suma de dos cuadrados; tal como lo expresa Euclides en su libro X de los *Elementos*: “Si el producto de números primos es un cuadrado, entonces los números enteros mismos son cuadrados”⁴⁹.

De aquí Fermat nota que Diofanto reduce las representaciones de un número como suma de dos cuadrados a sus factores primos, es decir, Diofanto era consciente de la identidad $(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \pm bc)^2$, cuya generalización es conocida actualmente como la identidad de Brahmagupta $(a^2 + b^2)(c^2 + d^2) = (ac - Kbd)^2 + K(ad \pm bc)^2$. Al igual que Fermat, Diofanto inspiró sus trabajos en los aportes de sus antecesores, más específicamente en las famosas ternas pitagóricas, posiblemente desarrolladas por Pitágoras o por sus discípulos⁵⁰, las cuales le permitieron dar solución a casos muy específicos de ecuaciones.

⁴⁸ Nadie estudio a Diofanto como Fermat.

⁴⁹ La prueba de esto puede justificarse de forma directa apelando al teorema de divisibilidad de enteros de Euclides, aunque en su libro de los elementos no se haya resultado de esta manera.

⁵⁰ También hay registros de que los babilónicos registraron alrededor de quince ternas y que posiblemente conocían una formula general para ello.

Mas adelante, Euler dedica gran parte de su vida a estudiar los trabajos de Fermat, de los cuales consigue realizar varias demostraciones por el método de descenso infinito⁵¹ y prueba que $x^2 + 5y^2$ en ocasiones representa un primo p y a veces representa a un primo $2p$, de lo cual conjetura que un primo p es de la forma $x^2 + 5y^2$ si y solo si $p \equiv 1 \pmod{20}$ y que un primo $2p$ es de la forma $x^2 + 5y^2$ si y solo si $p \equiv 3 \pmod{20}$.

Dedekind, sobre la base de la noción de ideal fundó la teoría de números algebraicos considerando las matemáticas como un edificio cuyos cimientos están constituidos por los fundamentos de la teoría de conjuntos, contribuyó a clarificar, de manera esencial, las nociones básicas del álgebra actual, tales como: grupo, anillo, ideal, campo, módulo; en otras palabras, los conjuntos dotados de estructura. De la misma manera, temas que formaron parte de su trabajo matemático fueron los fundamentos de las matemáticas, los números reales, la teoría de Galois.

Richard Dedekind fue considerado como figura clave en el surgimiento de la matemática estructural del siglo XX, su obra ha sido ampliamente estudiada y elogiada hasta el punto de considerarse el “moderno Euclides” por el impacto de sus magníficas contribuciones a la matemática, principalmente en los fundamentos del sistema numérico real y natural, y la teoría de números algebraicos. En particular, Dedekind introdujo varios de los conceptos considerados fundamentales del álgebra moderna: campos, anillos, módulos. También introdujo técnicas que posteriormente fueron desarrolladas por Emmy Noether y por otros matemáticos influyentes de la época, convirtiendo sus trabajos en el núcleo del surgimiento de la imagen estructural del álgebra. Como Noether solía repetir: “ya todo está en Dedekind” al reconocer que sus obras contenían una fuente inagotable de inspiración; se dice que fue gracias a la admiración por

⁵¹ Método de demostración atribuido a Pierre de Fermat, es reconocido como una “variante” del método de reducción al absurdo.

Dedekind que Emmy Noether se apoyó e inspiró en desarrollar su trabajo acerca de su teoría de ideales, aunque en el trabajo de Noether se reconoce un enfoque mucho más "estructural" que el de Dedekind, fue este quien dio el primer paso a la evolución de un "álgebra de estructuras".

Capítulo 3

Una mirada a la teoría de retículos de Dedekind.

Como un tercer gran aporte de los trabajos e investigaciones de Dedekind, nos encontramos con la introducción del concepto de *retículo* y de toda una teoría en torno a él. Para comprender en un sentido amplio esta nueva propuesta teórica de Dedekind, es necesario revisar los aspectos centrales de dicha teoría desde un punto de vista moderno. Por tanto, se presentan a continuación las definiciones y ejemplos que nos ofrecen un panorama global de esta teoría algebraica y la suficiente claridad conceptual para luego abordar los trabajos de Dedekind desde un punto de vista histórico. De igual manera, se presentan estos conceptos matemáticos con el propósito de que el documento sea autocontenido, puesto que no necesariamente hacen parte del currículo universitario.

3.1 Nociones básicas de la teoría de retículos.

Como se sabe, en teoría de conjuntos, un *retículo* es un conjunto parcialmente ordenado en el cual, para cada par de elementos, existen un supremo y un ínfimo. Para comprender bien el sentido de este concepto vamos a desglosar cada uno de los elementos conceptuales que lo rodean.⁶⁶

Iniciamos esta sección recordando el concepto de relación de orden que se plantea en (Burris & Sankappanavar, 1981) para caracterizar los conjuntos parcialmente ordenados.

Veamos:

⁶⁶ En esta sección tomamos como referencia algunos ejemplos y definiciones del canal de Youtube de Alicia Piñeiro (Conjuntos ordenados, redes y álgebras de Boole, 2020)

Definición 3.1 Sea A un conjunto. Una relación binaria $\leq$ definida en A es de *orden parcial* en el conjunto A , si las siguientes condiciones se cumplen en A :

- | | |
|---|---------------|
| (i) $a \leq a$ | Reflexiva |
| (ii) $a \leq b \wedge b \leq a \rightarrow a = b$ | Antisimétrica |
| (iii) $a \leq b \wedge b \leq c \rightarrow a \leq c$ | Transitiva |

a este conjunto parcialmente ordenado también se le conoce como *poset*.

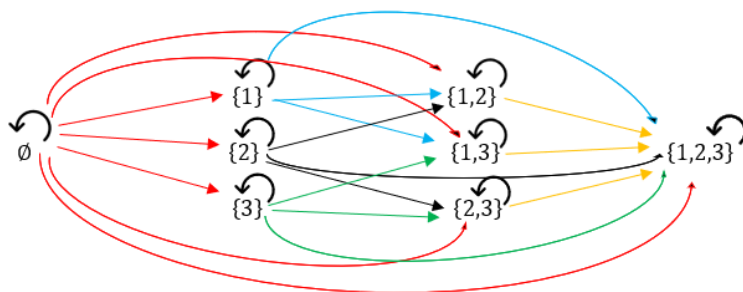
Veamos un ejemplo: sea $A = \{1,2,3\}$. Escribamos el conjunto de partes de A :

$$\wp(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, A\}$$

Consideremos la relación de inclusión en $\wp(A)$ y hagamos el grafico de estas relaciones:

Figura 1

Relaciones de inclusión en partes de A .



Nota. Adaptado de *Relaciones de inclusión en partes de A* , de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

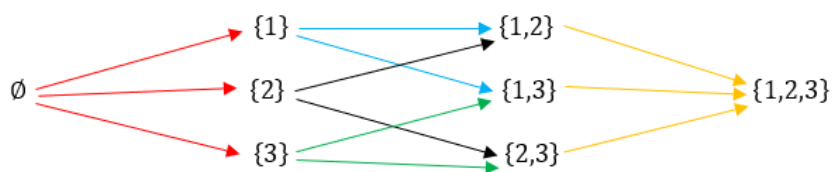
Como se puede observar, la relación dibujada en el grafico anterior es la inclusión, donde expresamos con el “bucle” $\curvearrowright$ que todo conjunto está incluido en sí mismo $a \leq a$, lo cual cumple la propiedad *reflexiva*. Con las flechas indicamos la existencia de un conjunto en otro,

ahora, respecto a la propiedad *antisimétrica*, si un conjunto está incluido en otro y este otro en el primero, esto la definición de igualdad de conjuntos justamente $a \leq b \wedge b \leq a \rightarrow a = b$; además, es importante notar que las flechas van en un único sentido, lo cual cobrará relevancia más adelante. Finalmente notemos que se cumple la propiedad *transitiva* al percibir que, si un conjunto está incluido en otro y este otro en un tercero, entonces el primero estará incluido en el tercero $a \leq b \wedge b \leq c \rightarrow a \leq c$. Por tanto, el $\wp(A)$ es un conjunto *parcialmente ordenado* por la relación de contención.

Pero este diagrama se puede simplificar aún más⁶⁷, con lo que se conoce como *diagrama de Hasse*, el cual consiste en eliminar los “bucles”, ya que, si estamos trabajando con una relación de orden, se sobre entiende que se cumple la reflexividad para cada conjunto, además también eliminamos las aristas transitivas, esto es, aquellas que se pueden obtener a partir de dos o más aristas, con lo cual, las únicas aristas que dibujaríamos serían aquellas que relacionan elementos diferentes. Entonces tendríamos este nuevo gráfico:

Figura 2

Relaciones de inclusión en partes de A, simplificado.



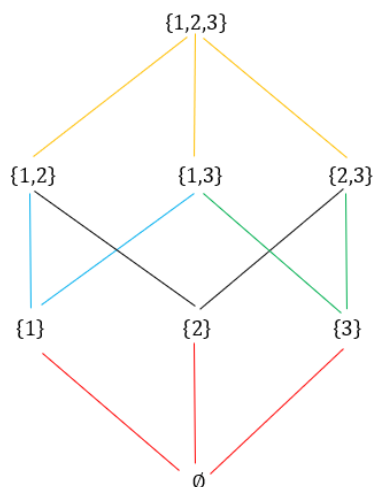
Nota. Adaptado de *Relaciones de inclusión en partes de A, simplificado*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCrfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCrfdafMY).

⁶⁷ Siempre y cuando se tenga la certeza de que estamos trabajando con una relación de orden.

También podemos omitir el sentido de las aristas si se las dibuja de abajo hacia arriba, veamos:

Figura 3

Diagrama de Hasse.



Nota. Adaptado de *Diagrama de Hasse*, de Alicia Piñeiro, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Finalmente, este es la representación del conocido *diagrama de Hasse*. Ahora bien, si un conjunto A además de ser parcialmente ordenado, verifica que para todo a, b en A $a \leq b \vee b \leq a$, entonces decimos que A es *totalmente ordenado*. Es decir, que $\leq$ es un orden total en A , que puede representarse como $(A; \preceq)$ donde el símbolo $\preceq$ significa que “precede”, es decir, el conjunto $(A; \preceq)$ es totalmente ordenado cuando $\forall a, b \in A: (a \preceq b \vee b \preceq a)$. Esto significa que siempre puedo comparar dos elementos cualesquiera del conjunto y establecer si uno es “menor” que el otro, de acuerdo con la relación de orden.

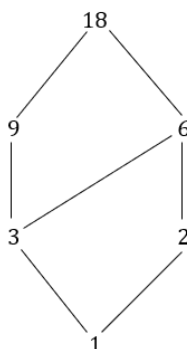
Ejemplo: El conjunto de los números naturales $\mathbb{N}$ con la relación usual de orden $\leq$ es totalmente ordenado. Lo mismo pasa con los enteros, racionales y reales.

De otro lado, si en un conjunto hay elementos que no cumplen que $\forall a, b \in A: (a \leq b \vee b \leq a)$ se dice que los elementos son *incomparables*, veamos un ejemplo:

Consideremos el conjunto $D_{18} = \{x \in \mathbb{N} / x \text{ divide a } 18\}$, por extensión sabemos que el conjunto está formado por $D_{18} = \{1, 2, 3, 6, 9, 18\}$. Ahora, si realizamos el diagrama de Hasse tenemos:

Figura 4

Diagrama de Hasse para D_{18} .



Nota. Adaptado de *Diagrama de Hasse para D_{18}* , de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

El $(D_{18}; /)$ es un conjunto ordenado. Sin embargo, nótese que el 2 y el 3 no están relacionados, entonces decimos que 2 y 3 o 3 y 2 no tienen relación, luego, esta no es una relación de orden total porque se incumple que $\forall a, b \in A: (a \leq b \vee b \leq a)$, dado que, 2 no precede a 3, ni 3 precede a 2. Esto se representa como $3 \parallel 2$, desde luego en el diagrama anterior

también es fácil observar que 9 y 2, 9 y 6 tampoco se relacionan, por tanto, también son incomparables $9 \parallel 2$, $9 \parallel 6$ respectivamente.

Definición 3.2: Sea $(A; \leq)$ un conjunto totalmente ordenado. Un elemento $m \in A$ se llamará *maximal* de A , si $(\forall x \in A)(m \leq x \Rightarrow x = m)$, dicho de otra manera, no puede existir otro elemento delante de un maximal y si existiera sería él mismo. Si el maximal es único, se le conoce como *máximo* o último elemento.

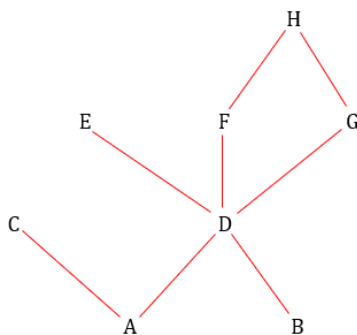
De manera análoga se define el *minimal* de A . Si $(\forall x \in A)(x \leq m \Rightarrow x = m)$. Esto significa que, si hay alguien detrás de un minimal, solo puede ser el propio minimal, entonces los minimales son aquellos elementos que no preceden a ningún otro elemento. Si el minimal es único, se le conoce como *mínimo* o primer elemento.

Si volvemos nuevamente al ejemplo anterior, el único minimal es el 1, puesto que, es el único elemento que no es predecesor de otro, si, por ejemplo, supusiéramos que 6 es minimal, sería fácil determinar que este, está siendo precedido por 2, lo cual incumple la definición de minimal. De la misma manera, es fácil notar que 18 es el único maximal, dado que no está detrás de ningún otro.

Veamos otro ejemplo: consideramos el siguiente diagrama de Hasse,

Figura 5

Ejemplo de diagrama de Hasse.



Nota. Adaptado de *Ejemplo de diagrama de Hasse*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY.

Los minimales serían A y B porque son los únicos elementos que no preceden a ningún otro, y los maximales serían C , E y H porque delante de ellos no hay ningún otro, para este caso particular el maximal no es único, por tanto, no habría un último elemento en este diagrama de Hasse.

Definición 3.3 Sea $(A; \leq)$ un conjunto A ordenado con primer elemento p ⁶⁸, decimos que un *átomo*⁶⁹ son aquellos elementos indivisibles⁷⁰ que se encuentran inmediatamente después del primer elemento. Es decir, $m \in A$ es átomo de $A \leftrightarrow \forall x \in A: ((x \leq m) \rightarrow (x = m) \vee (x = p)) \wedge m \neq p$.

Veamos un ejemplo, si consideramos el conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ con la relación “divisor” y hacemos el diagrama de Hasse.

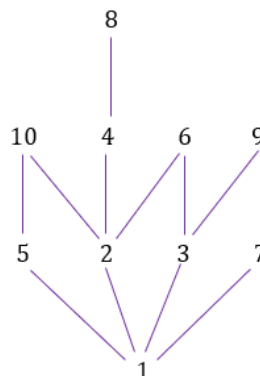
⁶⁸ Que el conjunto A tenga un elemento considerado como primer elemento nos está indicando que este elemento es un minimal y que además es único.

⁶⁹ La palabra átomo aquí también conserva su significado derivado del latín atomus, el cual expresa literalmente que no puede dividirse o “sin división”.

⁷⁰ Es importante resaltar que Dedekind (Dedekind, *Über zerlegungen von zahlen durch ihre grobten gemeinsamen teiler*, 1897) utiliza el término indivisible para referirse a los átomos, estos serían aquellos elementos que son primos relativos entre sí.

Figura 6

Diagrama de Hasse del conjunto A .



Nota. Adaptado de *Diagrama de Hasse del conjunto A*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Notemos que este conjunto tiene primer elemento y es 1, basados en la definición, los átomos serían los elementos que están inmediatamente después del primer elemento, es decir, 5, 2, 3 y 7. Pero, ¿qué tipo de números son estos? Son primos. Si pensamos por ejemplo en 4, notemos que 4 se descompone en 2×2 o el 6 se descompone en 2×3 , mientras que los átomos son números que no se pueden dividir, no los podemos expresar como productos de dos números diferentes, salvo que sean sí mismo y uno, de ahí viene la palabra *átomo*, que son indivisibles.

Definición 3.4: Si se tiene un conjunto ordenado $(A; \leq)$ y $\emptyset \neq B \subseteq A$ llamamos *cota superior* a los elementos que están detrás de todos los elementos del subconjunto. Es decir, sea $s \in A$, decimos que s es cota superior de B si y solo si $\forall x \in B, x \leq s$. El conjunto de cotas

superiores se le conoce como *mayorante*, y la menor⁷¹ de las cotas superiores recibe el nombre de *supremo*. Si el supremo pertenece a B , se llama *máximo* de B .

De manera análoga, se define *cota inferior* a los elementos que están antes de todos los del subconjunto. Es decir, sea $i \in A$, decimos que i es cota inferior de B si y solo si $\forall x \in B, i \leq x$. El conjunto de cotas inferiores se le conoce como *minorante*, y la mayor de las cotas inferiores⁷² recibe el nombre de *ínfimo*. Si el ínfimo pertenece a B , se llama *mínimo* de B .

3.1.1 Definición de retículo y algunos ejemplos

En este momento tenemos todos los prerrequisitos conceptuales para definir el concepto central del capítulo. Veamos:

Definición 3.5: Sea $(A; \leq)$ un conjunto ordenado, se dice que es un *superior semiretículo*, si $\forall a, b \in A: \exists \text{supremo}(a, b)$. De manera análoga se dice que un conjunto ordenado es *inferior semiretículo*, si $\forall a, b \in A: \exists \text{ínfimo}(a, b)$.

Definición 3.6: Un *lattice* o *retículo* es un conjunto ordenado que es a la vez superior e inferior *semiretículo*. En otras palabras, entre todo par de elementos debe existir el supremo y el ínfimo. Al supremo entre un elemento a y un elemento b lo denotamos como $\text{sup}\{a, b\}$ o $a \vee b$ ⁷³ y al ínfimo entre a y b lo denotamos como $\text{inf}\{a, b\}$ o $a \wedge b$.

Nota 1: Existe la propiedad que garantiza que, para un conjunto ordenado $(A; \leq)$ se tiene que $\forall a, b \in A, a \leq b \Leftrightarrow a \vee b = b$. Si pensamos detenidamente en un a relacionado con un b como lo indica el siguiente gráfico.

⁷¹ En el sentido del orden, decimos “menor” a la primera de las cotas superiores o primer elemento del conjunto mayorante.

⁷² Es decir, el último elemento del conjunto minorante.

⁷³ Esta es la representación que Dedekind usa para referirse al supremo.

Figura 7

A relacionado con B.



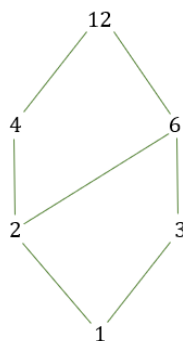
Nota. Adaptado de *A relacionado con B*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Si un a precede a b (desde luego este gráfico puede ser un subconjunto de un conjunto más grande) el supremo entre a y b es b , dado que, b será el menor de las cotas superiores que están delante de él. De la misma manera, el ínfimo de esta relación será a , dado que para todos los elementos que pudieran preceder a a , este sería la mayor de las cotas inferiores. Esto es importante en la medida en que, cada vez que tengamos que determinar si un conjunto ordenado es o no una red, no hará falta estudiar a aquellos elementos que están relacionados entre sí, bastara con analizar que ocurre entre aquellos elementos que no están relacionados, como mencionamos anteriormente, estos elementos suelen llamarse incomparables.

Veamos un ejemplo, analicemos si el conjunto ordenado $(D_{12}; /)$ con la relación “divisor” es un retículo. Sabemos que los divisores de 12 son $D_{12} = \{1, 2, 3, 4, 6, 12\}$ si representamos esto en un diagrama de Hasse, tendremos que:

Figura 8

Diagrama de Hasse para D_{12} .



Nota. Adaptado de *Diagrama de Hasse para D_{12}* , de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Como lo mencionamos anteriormente, no tiene sentido analizar aquellos elementos que están relacionados entre sí, iremos directamente a quienes son incomparables, como es el caso del 2 y el 3, luego para hallar el $\sup\{2,3\}$ observamos las cotas superiores de 2 y 3 que, gracias a la ayuda visual que proporciona el diagrama de Hasse, es fácil notar que hay dos elementos delante de ellos, el 6 y el 12, pero se considera la primera de las cotas superiores, es decir, 6.

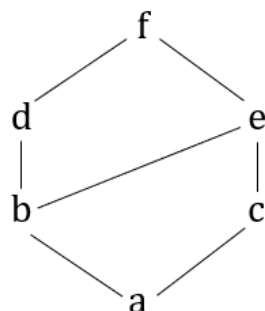
De la misma forma se calcula el $\inf\{2,3\}$: observamos las cotas inferiores de 2 y 3 y es fácil notar que es 1, además es la única. Otro par de incomparables es 4 y 6, es fácil de determinar que $\sup\{4,6\} = 12$, el $\inf\{4,6\} = 2$. También es fácil determinar que 3 y 4 son incomparables y que $\sup\{3,4\} = 12$ y el $\inf\{3,4\} = 1$.

Ahora bien, después de que se han analizado todos los elementos incomparables, se puede deducir que el conjunto inicial es un *retículo*, dado que todo par de elementos en el conjunto tiene supremo e ínfimo.

Veamos otro ejemplo: Sea el conjunto ordenado $A = \{a, b, c, d, e, f\}$ según muestra el siguiente diagrama de Hasse:

Figura 9

Diagrama de Hasse del conjunto A .



Nota. Adaptado de *Diagrama de Hasse del conjunto A*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Ahora construyamos las tablas de doble entrada para $\vee$ el *sup.* y $\wedge$ para el *ínf.*

Tabla 1

Doble entrada para el ínfimo.

$\wedge$	a	b	c	d	e	f
a						
b						
c						
d						
e						
f						

Nota. Adaptado de *Doble entrada para el ínfimo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Tabla 2

Doble entrada para el supremo.

$\vee$	a	b	c	d	e	f
a						
b						
c						
d						
e						
f						

Nota. Adaptado de *Doble entrada para el supremo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Estas tablas son usadas por el propio Dedekind (Dedekind, Über zerlegungen von zahlen durch ihre grobten gemeinsamen teiler, 1897)⁷⁴ para determinar el supremo y el ínfimo.

Para completar la tabla del supremo basta con interpretar del diagrama de Hasse, cuál es el supremo entre cada arista, es decir, el supremo entre a y a , será a . Si pensamos en los elementos a y b , el supremo será b ⁷⁵. Si se piensa en dos elementos incomparables como d y c , seguimos el mismo análisis del ejemplo anterior, revisamos cuales elementos son cotas superiores y vemos que la única cota superior en común entre d y c es f .

⁷⁴ Una traducción aproximada al español sería: "Sobre la descomposición de números por sus máximos factores comunes"

⁷⁵ Si este paso no es claro, se sugiere revisar la nota 1.

Tabla 3

Doble entrada para el supremo, completa.

$\vee$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	b	e	d	e	f
c	c	e	c	f	e	f
d	d	d	f	d	f	f
e	e	e	e	f	e	f
f	f	f	f	f	f	f

Nota. Adaptado de *Doble entrada para el supremo, completa*, de Alicia Piñeiro, 2020,

Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY)

De manera análoga se completa la tabla del ínfimo y se obtiene:

Tabla 4

Doble entrada para el Ínfimo, completa.

$\wedge$	a	b	c	d	e	f
a	a	a	a	a	a	a
b	a	b	a	b	b	b
c	a	a	c	a	c	c
d	a	b	a	d	b	d
e	a	b	c	b	e	e
f	a	b	c	d	e	f

Nota. Adaptado de *Doble entrada para el ínfimo, completa*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY

Definición 3.7: Sea un conjunto ordenado $(A; \leq)$ y una operación $*$ definida en A . Se dice que la relación $*$ es cerrada en A si y sólo si $a * b \in A$, para todos $a, b \in A$.

En otras palabras, una *relación es cerrada* si al operar todo par de elementos en el conjunto, el resultado está en el conjunto. Por ejemplo, la operación “suma” definida en el conjunto de los números naturales es *cerrada*, pero su operación inversa no lo es.

Es fácil identificar en las tablas del ejemplo anterior que las operaciones trabajadas son cerradas, dado que, cada elemento obtenido al realizar el supremo y el ínfimo hacen parte del conjunto inicial.

Definición 3.8: Sea un conjunto ordenado $(A; \leq)$ y una operación $*$ definida en A . Se dice que la operación $*$ es *conmutativa* en A si y sólo si $a * b = b * a \in A$, para todos $a, b \in A$.

Es decir, se trata de una operación que al efectuarse se obtiene el mismo resultado sin importar el orden de los elementos.

Tomando como referencia el ejemplo anterior, para evidenciar si una operación es *conmutativa* en las tablas, debemos marcar la diagonal y verificamos si hay simetría respecto de cada diagonal.

Tabla 5

Verificación de simetría respecto a la diagonal para el ínfimo.

$\wedge$	a	b	c	d	e	f
a	a	a	a	a	a	a
b	a	b	a	b	b	b
c	a	a	c	a	c	c
d	a	b	a	d	b	d
e	a	b	c	b	e	e
f	a	b	c	d	e	f

Nota. Adaptado de *Verificación de simetría respecto a la diagonal para el ínfimo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Tabla 6

Verificación de simetría respecto a la diagonal para el supremo.

$\vee$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	b	e	d	e	f
c	c	e	c	f	e	f
d	d	d	f	d	f	f
e	e	e	e	f	e	f
f	f	f	f	f	f	f

Nota. Adaptado de *Verificación de simetría respecto a la diagonal para el supremo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Para este caso en particular, es sencillo ver que las operaciones *sup* e *ínf* son conmutativas en A .

Definición 3.9: Se define una operación $*$ como *idempotente*, cuando operamos un elemento con sí mismo y el resultado es el mismo elemento. Es decir, se define una *operación idempotente* de un conjunto ordenado $(A; \preceq) \leftrightarrow \forall a \in A: a * a = a$.

Para el caso particular de las tablas, debemos revisar las diagonales y verificar que los elementos en la diagonal sean iguales a los elementos que se están operando.

Tabla 7

Verificación de los elementos de la diagonal para el ínfimo.

$\wedge$	a	b	c	d	e	f
a	a	a	a	a	a	a
b	a	b	a	b	b	b
c	a	a	c	a	c	c
d	a	b	a	d	b	d
e	a	b	c	b	e	e
f	a	b	c	d	e	f

Nota. Adaptado de *Verificación de los elementos de la diagonal para el ínfimo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Tabla 8

Verificación de los elementos de la diagonal para el supremo.

$\vee$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	b	e	d	e	f
c	c	e	c	f	e	f
d	d	d	f	d	f	f
e	e	e	e	f	e	f
f	f	f	f	f	f	f

Nota. Adaptado de *Verificación de los elementos de la diagonal para el supremo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Efectivamente, las operaciones *sup* e *inf* son idempotentes en A .

Definición 3.10: Se define el *elemento neutro* de un conjunto ordenado $(A; \leq)$ como aquel elemento que, al operarlo con otro, nos da siempre el otro elemento como resultado. Es decir, $e \in A$ es elemento neutro $*$ si y sólo si $a * e = a \wedge e * a = a, \forall a \in A$.

En las tablas solo basta con verificar si hay alguna fila o columna que devuelve los elementos en el mismo orden en que estaban.

Tabla 9

Verificación de fila y columna para elementos principales, ínfimo.

$\wedge$	a	b	c	d	e	f
a	a	a	a	a	a	a
b	a	b	a	b	b	b
c	a	a	c	a	c	c
d	a	b	a	d	b	d
e	a	b	c	b	e	e
f	a	b	c	d	e	f

Nota. Adaptado de *Verificación de fila y columna para elementos principales, ínfimo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Tabla 10

Verificación de fila y columna para elementos principales, supremo.

$\vee$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	b	e	d	e	f
c	c	e	c	f	e	f
d	d	d	f	d	f	f
e	e	e	e	f	e	f
f	f	f	f	f	f	f

Nota. Adaptado de *Verificación de fila y columna para elementos principales, supremo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Por tanto, el elemento *neutro* de la operación supremo es el elemento a y el neutro de la operación ínfimo es el elemento f .

Definición 3.11: Se define el *elemento absorbente* de un conjunto ordenado $(A; \leq)$ como el elemento que, al operarlo con cualquier otro, devuelve a sí mismo. Es decir, $n \in A$ es el elemento absorbente de $*$ si y sólo si $a * n = n \wedge n * a = n$, para todo $a \in A$.

Aquí basta con verificar en las tablas, cual es elemento que siempre devuelve a sí mismo, veamos:

Tabla 11

Verificación del elemento que devuelve así mismo, ínfimo.

$\wedge$	a	b	c	d	e	f
a	a	a	a	a	a	a
b	a	b	a	b	b	b
c	a	a	c	a	c	c
d	a	b	a	d	b	d
e	a	b	c	b	e	e
f	a	b	c	d	e	f

Nota. Adaptado de *Verificación del elemento que devuelve así mismo, ínfimo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Tabla 12

Verificación del elemento que devuelve así mismo, supremo.

$\vee$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	b	e	d	e	f
c	c	e	c	f	e	f
d	d	d	f	d	f	f
e	e	e	e	f	e	f
f	f	f	f	f	f	f

Nota. Adaptado de *Verificación del elemento que devuelve así mismo, supremo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

En el supremo es fácil identificar que en la tabla el elemento que siempre da como resultado si mismo es f y para el caso del ínfimo es a . Es decir, al revés de los neutros.

Nota 2: Todo lo anteriormente mencionado, puede resumirse tal como se presenta (Burris & Sankappanavar, 1981) en términos más axiomáticos, decimos que todo *retículo* satisface las siguientes identidades:

$A_1: (a) \ x \vee y \approx y \vee x$ leyes conmutativas
 $(b) \ x \wedge y \approx y \wedge x$

$A_2: (a) \ x \vee (y \vee z) \approx (x \vee y) \vee z$ leyes asociativas
 $(b) \ x \wedge (y \wedge z) \approx (x \wedge y) \wedge z$

$A_3: (a) \ x \vee x \approx x$ leyes de idempotencia
 $(b) \ x \wedge x \approx x$

$A_4: (a) \ x \approx x \vee (x \wedge y)$ leyes de absorción

$$(b)x \approx x \wedge (x \vee y)$$

$$A_5: a \leq b \leftrightarrow a \vee b = b \quad \text{Supremo}$$

$$A_6: a \leq b \leftrightarrow a \wedge b = a \quad \text{Ínfimo}$$

3.1.2 Retículo algebraico

Definición 3.12: Sea un conjunto $A \neq \emptyset$ y dos operaciones binarias cualquiera definidas en A : $\wedge$ y $\vee$, decimos que $(A, \wedge, \vee)$ es un *retículo algebraico* si se cumplen las leyes anteriores⁷⁶, es decir, si las operaciones son cerradas, asociativas, conmutativas, idempotentes y cumple la ley de absorción, en otras palabras, la única diferencia entre un retículo algebraico y un retículo cualquiera, es que el retículo algebraico se está definiendo a partir de las operaciones $\wedge$ y $\vee$ y no con la relación de orden.

Ejemplos: 1) Si se tiene el conjunto $A = \{1,2\}$ entonces $(\wp(A), \cup, \cap)$ es un retículo algebraico, ya que es de amplio conocimiento que la “unión” y la “intersección” de conjuntos cumplen con las leyes ya mencionadas.

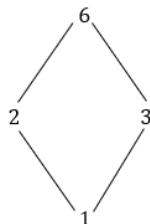
2) Si pensamos en el conjunto $(D_{12}, m.c.d., m.c.m.)$ este sería un retículo algebraico, dado que, las operaciones $m.c.d., m.c.m.$ cumplen con las leyes anteriores.

Luego, si sabemos que un conjunto ordenado que sea retículo cumple con las leyes mencionadas en la nota 2 entonces, *todo retículo ordenado también se puede considerar retículo algebraico*. Ilustremos esto con siguiente ejemplo:

⁷⁶ Las mencionadas en la nota 2.

Figura 10

Diagrama de Hasse para D_6 .



Nota. Adaptado de *Diagrama de Hasse para D_6* , de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Dada un retículo ordenado $(D_6; /)$ definimos dos operaciones que la estructuran en un retículo algebraico. Para tal efecto, primero representamos los divisores de 6 en el diagrama de Hasse sabiendo que $D_6 = \{1, 2, 3, 6\}$

Encontramos el supremo e ínfimo de cada par de elementos y los representamos en sus respectivas tablas

Tabla 13

Supremo para D_6 , $a \vee b = \sup\{a, b\}$

$\vee$	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

Nota. Adaptado de *Supremo para D_6 , $a \vee b = \sup\{a, b\}$* , de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Tabla 14

Ínfimo para D_6 , $a \wedge b = \inf\{a, b\}$.

$\wedge$	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

Nota. Adaptado de *Ínfimo para D_6 , $a \wedge b = \inf\{a, b\}$* , de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Si observamos detenidamente los resultados de las tablas, vemos que, para este caso en particular, los resultados en la tabla del supremo corresponden al *m. c. m* y los resultados en la tabla del ínfimo corresponden al *m. c. d*, por lo tanto, el retículo ordenado $(D_6; /)$ es equivalente a un retículo algebraico, con las operaciones *m. c. m* y *m. c. d*.

Propiedad 1: Si se tiene un retículo algebraico $(A, \vee, \wedge)$. Sea la relación $R = a \leq b \leftrightarrow a \vee b = b$ es una relación de orden. De manera análoga $R = a \leq b \leftrightarrow a \wedge b = a$ es también una relación de orden. Desde luego, para la relación R también se cumple que $\sup\{a, b\} = a \vee b$ y $\inf\{a, b\} = a \wedge b$.

Ejemplo: Dado el retículo algebraico $P(\{a, b, c\}; \cup; \cap)$ encontremos la relación de orden de forma que sea retículo ordenado.

Como ya habíamos mencionado anteriormente cuando un elemento a se va a relacionar con otro b , es decir, $a \leq b \leftrightarrow a \vee b = b$ o $a \leq b \leftrightarrow a \wedge b = a$.

Puedo decir que para dos conjuntos cualquiera A y B , $A \leq B \leftrightarrow A \cup B = B$ pero sabemos por teoría de conjuntos que esto pasa cuando $A \subseteq B$, o sea que la relación que buscamos es la inclusión. De manera análoga $A \leq B \leftrightarrow A \cap B = A$.

Entonces, el retículo algebraico $P(\{a, b, c\}; \cup; \cap)$ es equivalente al retículo ordenado $(P(\{a, b, c\}); \subseteq)$, podemos entonces decir, que todo retículo ordenado cualquiera se puede estructurar algebraicamente, y todo retículo algebraico se puede ordenar, es decir, hay una correspondencia.

Figura 11

Correspondencia entre Retículo Ordenado, y Retículo Algebraico.



Nota. Adaptado de *Correspondencia entre Retículo Ordenado, y Retículo Algebraico*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y algebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Analizamos lo anteriormente mencionado de una manera más clara:

Tabla 15

Resumen de equivalencias entre retículo ordenado y retículo algebraico.

PASAR DE	A	CONOZCO	DEBO OBTENER
Retículo Ordenado	Retículo Algebraico	La relación de orden $\leq$	Las operaciones $\vee$ e $\wedge$: $a \vee b = \sup\{a, b\}$ $a \wedge b = \inf\{a, b\}$
Retículo Algebraico	Retículo Ordenado	Las operaciones binarias $\vee$ e $\wedge$	La relación de orden: $a \leq b \leftrightarrow a \wedge b = a$ $a \leq b \leftrightarrow a \vee b = b$

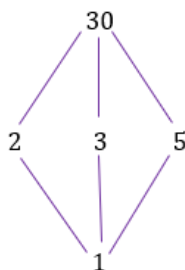
Nota. Adaptado de *Resumen de equivalencias entre retículo ordenado y retículo algebraico*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Definición 3.13 Sea un retículo $(A; \leq)$ con un primer elemento 0_A y un último elemento 1_A , para todo $a \in A$ se dice que es *complemento* y se representa como a' , si cumple que el ínfimo de un elemento a con su complemento a' devuelve el primer elemento y el supremo entre un elemento a y su complemento a' da el último elemento, es decir $a \wedge a' = 0_A$ y $a \vee a' = 1_A$.

Ejemplo: Sea el retículo A con la relación “divide” ($A = 1, 2, 3, 5, 30; /$), hallemos los complementos de los elementos de A , primero realizamos el diagrama de Hasse:

Figura 12

Diagrama de Hasse del conjunto A .



Nota. Adaptado de *Diagrama de Hasse del conjunto A*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY.

Notemos que el complemento de 1 será 30 porque la definición me garantiza que el supremo entre un elemento y su complemento da el último elemento, lo cual es fácil de deducir del diagrama de Hasse que el último elemento es el 30 y el primer elemento es 1, luego $1' = 30$, a lo que es igual que, el $\sup\{1, 30\} = 30$, ahora bien, si pensamos en el complemento de 30 y ubicamos en el diagrama el primer elemento, podemos deducir fácilmente que 1 es el complemento de 30, dado que cumple que $\inf\{1, 30\}$ es 1, esto aplica para todos los conjuntos ordenados, siempre el primer elemento y el último se complementan entre sí. Ahora veamos el complemento del 2, cual o cuales elementos al relacionarlos con 2 tienen supremo 30 e ínfimo 1? Es fácil notar con la ayuda del diagrama de Hasse, que tanto el 3 como el 5 cumplen esta condición, luego $2' = \{3, 5\}$. De manera análoga tenemos que $3' = \{2, 5\}$ y $5' = \{2, 3\}$.

Ahora, analicemos el conjunto ordenado $A = 1, 2, 3, 4$ con la relación $\geq$. Para $(A = 1, 2, 3, 4; \geq)$ tenemos el diagrama de Hasse

Figura 13

Diagrama de Hasse del conjunto A.



Nota. Adaptado de *Diagrama de Hasse del conjunto A*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Es sencillo ver que, $1' = 4$, $4' = 1$ porque como mencionamos anteriormente, el primer y último elemento se complementan entre sí. Ahora bien, ¿cual podría ser $2'$? si analizamos 2 y 3 el supremo sería 2 y el ínfimo sería 3, luego si analizamos 1 y 2, el supremo sería 1, lo cual es cierto, pero el ínfimo sería 2, y ya sabemos que esto no es cierto, ahora, si analizamos 2 y 4, podemos notar que el ínfimo es 4, lo cual es verdadero, pero el supremo sería 2 y nuevamente, esto no es cierto. Luego, deducimos que 2 no tiene complemento para este caso en particular. Bajo el mismo razonamiento es fácil llegar a que 3 tampoco tiene complemento.

Podemos entonces decir que, para un retículo, cada elemento puede tener un único complemento, puede tener más de uno o puede no tener ninguno. En el caso en que cada elemento de un retículo tenga al menos un complemento, diremos que se trata de una *Retículo Complementado*.

3.1.3 Retículo distributivo y modular

Definición 3.14: Sea $(A, \vee, \wedge)$ un retículo, diremos que *el retículo es distributivo* si y solo si:

$$\forall a, b, c \in A: a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

$$\forall a, b, c \in A: a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

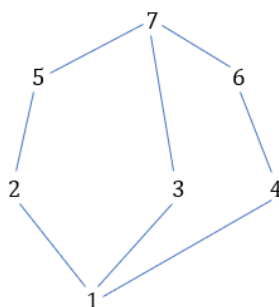
Ejemplo: si tenemos el retículo $P(\{a, b, c\}; \cup; \cap)$ es fácil verificar que se trata de un retículo distributivo, porque por la teoría de conjuntos sabemos que tanto la “unión” como la

“intersección” cumplen con la distributividad. Ahora veamos un ejemplo en el que esto no se cumpla:

Si consideramos el retículo $(A, \leq)$ dado por el siguiente diagrama:

Figura 14

Diagrama de Hasse del conjunto A



Nota. Adaptado de *Diagrama de Hasse del conjunto A*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Usando la definición de retículo distributivo, analizamos 3 elementos del diagrama, luego tenemos:

$$a \vee (b \wedge c) = 2 \vee (3 \wedge 5) = 2 \vee 1 = 2$$

$$(a \vee b) \wedge (a \vee c) = (2 \vee 3) \wedge (2 \vee 5) = 7 \wedge 5 = 5$$

Aquí es fácil ver que para los elementos 2, 3 y 5 no se cumple la distributividad, con esto es suficiente para afirmar que este retículo no es distributivo, sin embargo, si en el caso hipotético en que estos 3 elementos seleccionados hubiesen cumplido con la definición, se tendría que verificar para todos los elementos que componen nuestro conjunto.

Propiedad 2: Para todo retículo distributivo, el complemento, si existe, es único.

De acuerdo con la propiedad 2, si volvemos al ejemplo anterior donde se tiene el retículo $(A = 1, 2, 3, 5, 30; /)$, como ya se ha probado, los elementos 2, 3 y 5 no tienen un complemento único, por tanto, este retículo no es un Retículo Distributivo.

Definición 3.15: Si A es un retículo y $L \neq \emptyset$ es un subconjunto de A tal que para cada par de elementos a, b en L tanto $a \vee b$ como $a \wedge b$ están en L , donde $\vee$ y $\wedge$ son las operaciones de retículos de A , entonces decimos que L con las mismas operaciones (restringidas a L) es un subretículo de A .

Definición 3.16. Dos retículos algebraicos A_1 y A_2 son isomorfos si hay una biyección α de A_1 a A_2 tal que para todo a, b en A_1 se cumplen las siguientes dos ecuaciones:

$$-\alpha(a \vee b) = \alpha(a) \vee \alpha(b)$$

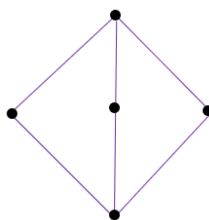
$$-\alpha(a \wedge b) = \alpha(a) \wedge \alpha(b)$$

donde α es llamada isomorfismo.

Propiedad 3 (Teorema de Birkhoff)⁷⁷: Todo retículo o lattice finito es distributivo si y solo si, no contiene ningún subretículo isomorfo a alguno de los siguientes:

Figura 15

Diagrama de Hasse de un retículo de cinco elementos llamado M_5 .

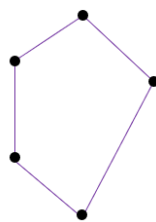


⁷⁷ Tomado de (Burris & Sankappanavar, 1981, p. 14)

Nota. Adaptado de *Diagrama de Hasse de un retículo de cinco elementos llamado M_5* , de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Figura 16

Diagrama de Hasse de un retículo de cinco elementos llamado N_5 .

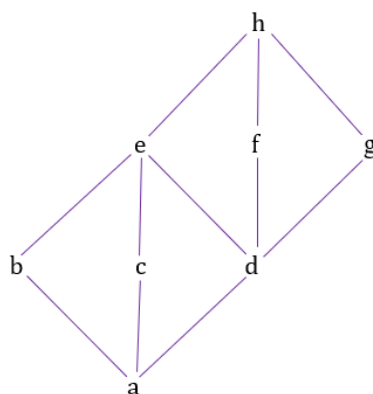


Nota. Adaptado de *Diagrama de Hasse de un retículo de cinco elementos llamado N_5* , de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Ejemplo: Para el siguiente diagrama de Hasse determinemos si corresponde a un retículo distributivo.

Figura 17

Diagrama de Hasse de un retículo.



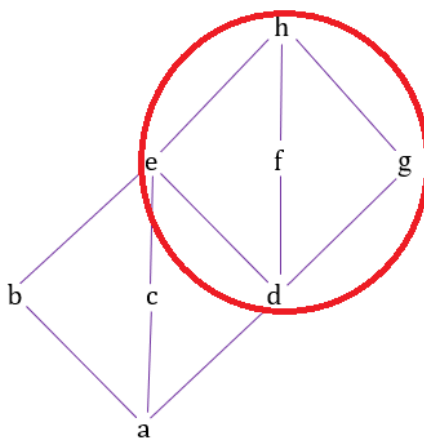
Nota. Adaptado de *Diagrama de Hasse de un retículo*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole,

[youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Al observar el diagrama podemos notar que una parte del diagrama contiene una de las formas mencionadas en la definición, para las cuales no se cumple la distributividad, esto es:

Figura 18

Diagrama de Hasse de un retículo donde se señala que no cumple con la distributividad.

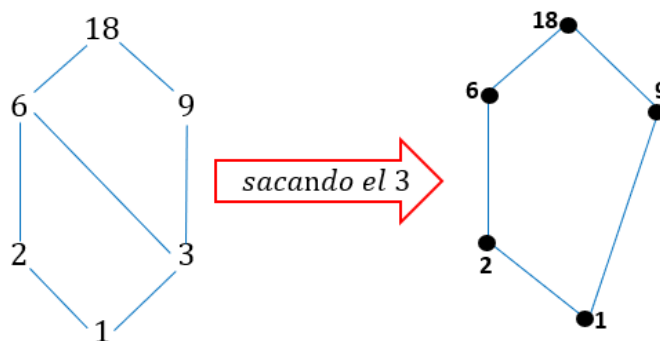


Nota. Adaptado de *Diagrama de Hasse de un retículo donde se señala que no cumple con la distributividad*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Veamos otro ejemplo y hagamos el respectivo análisis, si se considera el retículo ordenado $(D_{18};/)$ y observamos su diagrama de Hasse:

Figura 19

Diagrama de Hasse para un retículo ordenado $(D_{18};/)$ y simplificación de un elemento.



Nota. Adaptado de *Diagrama de Hasse para un retículo ordenado $(D_{18};/)$ y simplificación de un elemento*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Si analizamos el diagrama de Hasse para el retículo $(D_{18};/)$ vemos que es casi similar a aquellas que no son distributivas (diagrama de la derecha), a excepción de un número, entonces ¿se puede afirmar que el diagrama de Hasse de la derecha es subconjunto del diagrama de la izquierda? de ser así, el retículo dado no sería distributivo. Pero ahora, analicemos más profundamente esta situación y notemos que, el retículo $(D_{18};/)$ algebraicamente se corresponde con $(D_{18}; m. c. m; m. c. d.)$ y dado que, las operaciones $m. c. m$ y $m. c. d.$ son distributivas entre sí, esto nos estaría diciendo que el retículo sí sería distributivo. Luego, hemos llegado a una contradicción, ¿a qué se debe esto?

Al considerar el diagrama de la derecha como subconjunto del diagrama inicial y omitir el elemento 3, incumplimos la definición de subretículo, puesto que, si bien podemos tomar menos elementos, se deben mantener los supremos e ínfimos de la red inicial, veamos por qué:

El $\inf\{6, 9\}$ del diagrama de la izquierda es igual a 3.

El $\inf\{6, 9\}$ del diagrama de la derecha es 1.

Por lo cual, el análisis del subretículo fue incorrecto y finalmente el retículo $(D_{18};/)$ sí representa un retículo distributivo.

Finalizamos esta sección presentando la noción de retículo modular.

Definición 3.17: Un retículo *modular* es cualquier retículo que satisface la ley modular:

$$M: x \leq y \rightarrow x \vee (y \wedge z) \approx y \wedge (x \vee z)$$

La ley modular es obviamente equivalente (para retículos) a la identidad

$$(x \wedge y) \vee (y \wedge z) \approx y \wedge ((x \wedge y) \vee z)$$

Ya que $a \leq b$ se cumple si y solo si $a = a \wedge b$. Además, no es difícil ver que cada retículo satisface, entonces para verificar la ley modular basta con verificar la implicación

$$x \leq y \rightarrow y \wedge (x \vee z) \leq x \vee (y \wedge z)$$

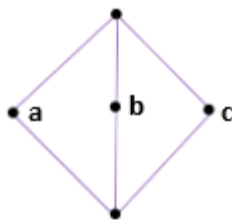
Teorema 3.18: Todo retículo distributivo es un retículo modular.

Si tomamos en cuenta la *definición 3.14*, sabemos que $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, y teniendo en cuenta que $a \vee b = b$ siempre que $a \leq b$.

Como se mencionó en la *propiedad 3* (teorema de Birkhoff) los retículos modulares y distributivos en términos de dos retículos de cinco elementos, representados en las *ilustraciones 15 y 16*.

Figura 20

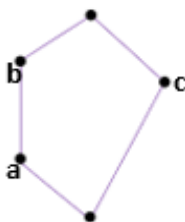
Diagrama de Hasse de un retículo de cinco elementos llamado M_5 con puntos definidos.



Nota. Adaptado de *Diagrama de Hasse de un retículo de cinco elementos llamado M_5 con puntos definidos*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

Figura 21

Diagrama de Hasse de un retículo de cinco elementos llamado N_5 con puntos definidos.



Nota. Adaptado de *Diagrama de Hasse de un retículo de cinco elementos llamado N_5 con puntos definidos*, de Alicia Piñeiro, 2020, Conjuntos ordenados, redes y álgebras de Boole, [youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY](https://www.youtube.com/@matematicamaravillosa?si=SYW85RKHCRfdafMY).

En ninguno de los casos $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ por lo que M_5 y N_5 no son retículos distributivos. Aunque para N_5 podemos notar que $a \leq b$ pero $a \vee (b \wedge c) \neq b \wedge (a \vee c)$ por lo que N_5 no satisface la ley modular a diferencia de M_5 .

Teorema 3.19 (Teorema de Dedekind): Se dice que M es un retículo no modular si N_5 se puede incrustar⁷⁸ en M .

Ejemplo: Si R es un anillo, sea $I(R)$ el conjunto de ideales de R . Se define $\wedge$ y $\vee$ en $I(R)$ por $I_1 \wedge I_2 = I_1 \cap I_2$, $I_1 \vee I_2 = \{i_1 + i_2 : i_1 \in I_1, i_2 \in I_2\}$ entonces bajo estas operaciones $I(R)$ es un retículo.

El ejemplo anterior sin duda es una muestra clara de cómo se vinculan los dos aspectos más relevantes en este trabajo de investigación, se conjugan aquí tanto la definición de ideal como la de retículo basados en conceptos más elementales como el de anillo, veamos entonces que $I(R)$ es retículo o lattice, dado que, ya conocemos con más familiaridad que la intersección entre dos conjuntos $I_1 \cap I_2$ y la suma de elementos de ideales $i_1 + i_2 : i_1 \in I_1, i_2 \in I_2$ cumplen con las leyes expuestas en la *nota 2*, las cuales nos garantizan la definición de retículo.

3.2 La teoría de retículos de Dedekind: breve contextualización histórica.

Estos aportes se encuentran particularmente en dos artículos planteados por Dedekind al finalizar el siglo XIX (Dedekind, *Über zerlegungen von zahlen durch ihre grobten gemeinsamen teiler*, 1897) y (Dedekind, *Ueber die von drei moduln erzeugte dualgruppe*, 1900)⁷⁹, los cuales no tuvieron al principio un gran impacto pero más adelante se les reconocería como fuertes y originales contribuciones a la teoría de retículos, y especialmente al estudio de retículos modulares.

Antes de presentar la noción de retículo en el trabajo de Dedekind, hacemos referencia a la noción de módulo, la cual está en la génesis del concepto de retículo. En su célebre obra de

⁷⁸ El término “incrustar” hace alusión a inclusión.

⁷⁹ Una aproximación a la traducción en el español sería: “Sobre el grupo dual generado por tres módulos”.

1872, Dedekind introdujo la noción de *módulo*, como un “sistema $\mathfrak{a}$ de números reales o complejos α cuyas sumas y diferencias pertenecen a $\mathfrak{a}$ ” (Dedekind, 1872, p. 42). Los *módulos* desempeñan un papel central en la teoría de números de Dedekind.

Para desarrollar la teoría de módulos, Dedekind definió una *relación de divisibilidad* para módulos: un módulo $\mathfrak{a}$ es divisible por un módulo $\mathfrak{b}$ si $\mathfrak{a} \subset \mathfrak{b}$. Esta relación de divisibilidad sienta las bases para nociones aritméticas relacionadas y para la metodología aritmética que prevaleció en muchos de sus trabajos matemáticos. Tienen particular interés para este trabajo las nociones de *mínimo común múltiplo* (m.c.m) y *máximo común divisor* (m.c.d) de módulos: el m.c.m de $\mathfrak{a}$ y $\mathfrak{b}$ es $\mathfrak{a} \cap \mathfrak{b}$, y el m.c.d de $\mathfrak{a}$ y $\mathfrak{b}$ es el módulo compuesto por todos los números $\alpha + \beta$ con α y β recorriendo respectivamente todos los números de $\mathfrak{a}$ y $\mathfrak{b}$.

Aunque las relaciones entre módulos fueron definidas en términos del dominio subyacente no se introdujeron símbolos para ellas sino hacia 1877, cuando Dedekind introdujo símbolos para múltiplo($>$), divisor($<$), m.c.m. ($+$), m.c.d. ($-$). Esto le permitió deducir lo que ahora conocemos como “leyes modulares” en la teoría de retículos.

En 1897 Dedekind estudia los sistemas de números en términos de su máximo común divisor. Este concepto lo quiere extender a dominios que no permiten la descomposición en factores primos. Dedekind comienza investigando con sistemas de tres y cuatro números hasta llegar a sistemas con n elementos generales, llamados *combinaciones*. Dedekind identifica en estos sistemas las propiedades de conmutatividad y asociatividad y las leyes de absorción, y observa que las leyes de idempotencia se derivan de ellas, pero las leyes distributivas no. Todo este ejercicio de generalización lo llevó a la noción de *Dualgruppe*, es decir, retículo⁸⁰.

⁸⁰ Recordar definición 3.6 de la sección anterior.

Un sistema $\mathfrak{A}$ de cosas $\alpha, \beta, \gamma \dots$ es llamado *Dualgruppe*⁸¹, si hay dos operaciones $\pm$ tales que crean a partir de dos cosas α, β dos cosas $\alpha \pm \beta$ que también están en A y que también satisfacen las condiciones de A (Dedekind, 1897).

Posteriormente mostró que esta noción se aplica a diversos dominios y describió cinco nuevos modelos: módulos, ideales, subgrupos de un grupo, campos y puntos de un espacio n -dimensional. (Schlimm, 2011) Esta amplia gama de aplicaciones da cuenta de su fecundidad y utilidad.

Dedekind define una relación de divisibilidad, denotada por $a < b$ o $b > a$ (a divisor de b) y definida por $a + b = a$, $a - b = b$. Esta relación satisface las leyes de una relación de orden parcial. Algunos *Dualgruppen* satisfacen lo que Dedekind llama *Modulgesetz* (ley modular): para tres módulos d, m, p , si $d < m$, entonces:

$$(m + p) - d = m + (p - d).$$

Aunque las leyes distributivas no se verifican en general en los retículos, si se verifican en modelos importantes de la lógica y la teoría de ideales. Este hecho condujo a Dedekind a los *Dualgruppe vom Idealtypus*; es decir, a los retículos distributivos⁸². Y los retículos modulares⁸³, aquellos donde se verifican las leyes modulares, fueron denominados *Dualgruppe vom Modultypus*. (Schlimm, 2011) Es así como Dedekind no sólo dio la definición de retículos, sino que logró avances significativos en el desarrollo de la teoría. De ahí el reconocimiento a los trabajos de Dedekind en el surgimiento del estructuralismo de orden.

⁸¹ El *dualgruppen* al que Dedekind se refiere no hace referencia la definición actual de grupo, sino a la definición de retículo

⁸² Recordar definición 3.14 de la sección anterior

⁸³ Recordar definición 3.16 de la sección anterior

Con las valiosas contribuciones elaboradas por Dedekind a lo largo de su vida como matemático, se marca un estilo estructuralista de forma implícita, que se enfoca en las operaciones entre los elementos de los sistemas en cuestión, más que en los elementos mismos. Mas adelante esta idea la desarrollarán con mayor fuerza los Bourbaki al exponer que “los objetos matemáticos solo son elementos que ocupan una posición y cumplen una función en una estructura, por lo cual no tienen más propiedades que aquellas que las reglas de construcción de la estructura les asignan” (Vélez, 2013, p. 12), de ahí que los Bourbaki le consideraran uno de sus antecesores directos.

En 1894 en una versión de los suplementos de las conferencias de Dirichlet, Dedekind introduce por separado propiedades fundamentales para m.c.m. y m.c.d. para módulos a , b y c , se cumple que:

$$\begin{array}{ll} a + b = b + a & a - b = b - a \\ (a + b) + c = a + (b + c) & (a - b) - c = a - (b - c) \\ a + a = a & a - a = a \end{array}$$

Sobre estas consideraciones, Dedekind expone la noción de *modulgruppe*: si se generan módulos repetidamente formando el máximo común divisor y mínimo común múltiplo, a partir de tres módulos arbitrarios, se obtiene un *modulgruppe* finito, que consta en general de 28 módulos diferentes.

Dedekind observó que el grupo en cuestión en la definición de retículo se reduce a 18 elementos, si sus elementos son ideales en lugar de módulos, de lo cual podemos inferir que Dedekind ya había analizado con detenimiento las estructuras inducidas por m.c.m. y m.c.d., se estima que esta definición alrededor de 1897, Dedekind estudia los sistemas de números en

términos de sus m.c.m. y esto lo hace de la manera más general posible, cuando se encuentra frente a la imposibilidad de descomponer en factores primos en ciertos dominios, este empieza a estudiar los sistemas de tres y cuatro números, luego sistemas formados por n elementos generales conocidos como *combinaciones*. Para estos formula seis leyes fundamentales para las operaciones, las cuales denomina “leyes A”

$$\alpha + \beta = \beta + \alpha$$

$$\alpha - \beta = \beta - \alpha$$

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$

$$(\alpha - \beta) - \gamma = \alpha - (\beta - \gamma)$$

$$\alpha + (\alpha - \beta) = \alpha$$

$$\alpha - (\alpha + \beta) = \alpha$$

Aquí Dedekind también identifica la conmutatividad, la asociatividad y las leyes de absorción, desde luego también se señalan que las leyes idempotentes $\alpha + \alpha = \alpha$ y $\alpha - \alpha = \alpha$ se derivan de ellas, pero las leyes distributivas no, aunque seas ciertas, dado que no son deducibles de las “leyes A”, dado que, las combinaciones de Dedekind son conjuntos de elementos, las operaciones $+$ o $-$ pueden ser también interpretadas como unión e intersección. Dedekind observa que muchos de sus teoremas sobre combinaciones ya habían sido tratados por Schroder en sus trabajos sobre lógica del álgebra, donde este había probado la independencia de las leyes distributivas del sistema de “leyes A”.

Ademas, Birkhoff refuerza la genialidad de Dedekind, señalando que: “la abundancia de este concepto de retículos en matemáticas, no se había mencionado anterior a él. Desde luego, es importante resaltar que, la definición axiomática de una estructura abstracta puede satisfacer sus axiomas en otros dominios matemáticos” (1940).

Como ya se ha mencionado antes, las leyes distributivas no aplicaban a las “leyes A” desarrolladas para retículos, esta es la razón que lleva a Dedekind a introducir la subespecie de

Dualgruppe vom idealtypus. Al exponer modelos adecuados, Dedekind demuestra que estas dos nociones no coinciden, es decir, que las leyes distributivas y modulares para retículos son independientes.

Herbert Mehrtens señala que:

Dedekind podría no haberse dado cuenta que la misma estructura abstracta que subyace sus investigaciones también se aplica a las de Schorder, en el momento en que Dedekind expone su noción de *dualgruppe*, este no menciona que coincide con la noción de cálculo lógico de Schorder. (1979).

Por tanto, si el análisis de Mehrtens es correcto son los axiomas y teoremas lo que pusieron de manifiesto la conexión entre el cálculo, los ideales y los módulos.

Así, en 1900 Dedekind había publicado una caracterización axiomática de retículos, y discutido los ejemplos principales y demostrado los teoremas fundamentales relativos a los retículos modulares; pero no presento este trabajo como el comienzo programático de una nueva e importante teoría, aunque abstracta, la noción de Dualgruppe de Dedekind estaba estrechamente ligada a la de módulos, que esperaba que desempeñaran un papel fundamental en la teoría algebraica de números, sin embargo, el desarrollo posterior no siguió su ejemplo, como es evidente por el hecho de que no aparecen en el libro de texto de álgebra de weber.

Conclusiones

A grandes rasgos podemos notar que los elementos que llevaron a Dedekind al desarrollo de su teorías matemáticas engrana múltiples conceptos y diversos procesos de formación por parte de Dedekind y otros matemáticos influyentes hacia finales del siglo XIX, este fue considerado un punto de inflexión importante en el desarrollo del álgebra, dado que, estos aportes dieron otra mirada al transcurso de la matemática y se abrió camino a un periodo de generalización, es decir, aquí se empezaría a formar el núcleo del futuro del álgebra abstracta. Al mismo tiempo, se creó una nueva teoría algebraica de números, que se convirtió en el hogar temporal del álgebra mientras crecían sus conceptos básicos (Stillwell, John, 1877).

Las matemáticas nunca volverían a ser las mismas después de los aportes de Dedekind dado el impacto y la profundidad de sus trabajos para ese entonces. Pero además del avance al entorno matemático, comprender la evolución histórica-epistemológica de los conceptos y conceptualizaciones fundamentales de la matemática y su interrelación, promueve la inclusión de temas históricos en la enseñanza de la matemática y vinculan a quienes aprenden con algunos de los diferentes procesos que dieron origen a los conocimientos matemáticos, así como las problemáticas que motivaron tales aspiraciones. (Rodriguez, Pochulu, & Espinoza, 2022, p. 50)

Dedekind era un estructuralista. En una interpretación propia, afirmamos que Dedekind marca una brecha estructuralista en la teoría de conjuntos⁸⁵ al proporcionar una identidad y noción de abstracción al sistema implicado, cuya naturaleza de la estructura, no considera, ni depende de las características de los elementos contenidos en dicho sistema. Debemos interpretar la noción de abstracción planteada por Dedekind como un procedimiento lógico,

⁸⁵ Gran parte de sus ideas acerca de la teoría de conjuntos fueron compartidas y complementadas por Cantor en sus famosas cartas.

donde primero se especifica el lenguaje y la lógica que se utilizan, luego se construye un infinito simple particular; tercero, este infinito simple se usa para determinar los valores de verdad de todas las oraciones aritméticas y por último este resultado se justifica mostrando que todos los infinitos simples son isomorfos.

Por otro lado, en el capítulo 3 dedicado a los retículos, es pertinente detenernos y hacer mención de la equivalencia entre un retículo de orden y un retículo algebraico, estas dos grandes estructuras estudiadas por Bourbaki son consolidadas por Dedekind en un solo concepto y se da gracias a que este plantea que se puede encontrar dos operaciones representadas por el $\vee$ y el $\wedge$ para el caso de un retículo ordenado y de la misma forma, se puede consolidar una relación de orden para el caso de un retículo algebraico. Teniendo en cuenta el periodo en el que se gesta esta idea, resulta ser este un desarrollo bastante adelantado a la época.

En resumen y tomando como referencia a Schlimm, se identifican tres maneras distintas en la que la axiomática puede contribuir a la introducción de nuevas nociones. (Schlimm, 2011)

Por analogía: las propiedades que diferentes dominios análogos tienen en común son expresados por un conjunto de axiomas, que, a su vez, se toman como la definición de una noción nueva y más abstracta. En otras palabras, se comienza con una concepción previa de que ciertos dominios son similares y se captura esta similitud en términos de un sistema común de axiomas. Se entiende entonces que estos axiomas caracterizan una noción abstracta instanciada por dominios análogos.

Por abstracción: se axiomatizan propiedades específicas de un dominio determinado y se identifican otros dominios que también satisfacen estos axiomas. En otras palabras, aquí se comienza con un dominio matemático particular y se describe axiomáticamente, abstrayéndose así de todos los aspectos que se consideran irrelevantes. Esta caracterización axiomática luego

guía al descubrimiento de otros dominios que satisfacen los axiomas y que, sobre esta base, se consideran análogos.

Por modificación: se modifica un sistema axiomático determinado, añadiendo, eliminando o cambiando uno o más axiomas, y el sistema resultante se utiliza como definición de un nuevo tipo de dominio. Podemos entonces afirmar que los axiomas característicos de una nueva noción garantizan una conexión con el cuerpo matemático original, dado que estas nuevas nociones no se conciben de un conjunto de axiomas arbitrarios. Episodios históricos han revelado que el método axiomático más allá de ser una fórmula para sistematizar el conocimiento matemático es una poderosa herramienta para descubrir e introducir nuevas nociones matemáticas.

Si Por ejemplo pensamos en el proceso de germinación de la teoría de ideales de Richard Dedekind se puede reconocer principalmente una necesidad⁸⁶ que da un origen al problema de la factorización única para números de la forma $\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} | x, y \in \mathbb{Z}\}$ de lo cual se desencadena un proceso de formación de nuevos dominios⁸⁷ numéricos que permiten dar solución a esta problemática, esos números son precisamente los llamados *números ideales*, analizando más profundamente este desarrollo, se concluye que se puede conocer la constitución esencial de un número, sin llevar a cabo su descomposición en factores primos, observando solamente la manera de la que se comporta como divisor (Dedekind, 1872) Entonces diremos que el eje principal de esta investigación gira en torno al problema de la divisibilidad.

Hasta este punto, es válido detenernos a pensar, ¿de qué manera este proceso de investigación a la formación de un concepto matemático puede afectar o beneficiar el desarrollo

⁸⁶ Encontrar la representación única de primos para ecuaciones de la forma cuadrática $x^2 + 5y^2$.

⁸⁷ Ver nota al pie, número 13.

del aprendizaje? Juan Nápoles, investigador argentino, da respuestas a este interrogante: entre ellas, que el conocimiento de la evolución de las ideas matemáticas da al docente elementos para reconocer y atender a los obstáculos epistemológicos en la formación de ciertas nociones y también que favorece la reflexión sobre la enseñanza y el aprendizaje de las dificultades inherentes a las nociones usadas (Rodríguez, Pochulu, & Espinoza, 2022, p. 50).

Para este trabajo en particular, tratar de reinterpretar los aportes matemáticos de Dedekind, resultó una actividad retadora y enriquecedora en el sentido en que no solo se estudiaron los conceptos matemáticos, sino que se avistaron los cambios que la historia ha hecho a los mismos, es decir, nos enfrentamos a nociones que actualmente son conocidas con términos distintos y cuya simbología no se encuentra registrada de la misma manera que en la actualidad, podemos decir entonces que este trabajo de grado constituyó un proceso de descubrimientos del pasado al presente⁸⁸.

Desde luego que el uso de la historia en el proceso de enseñanza ha marcado una etapa importante en el desarrollo de la misma, veamos más a fondo de que se trata esto, como lo menciona (Rodríguez, Pochulu, & Espinoza, 2022) se resaltan dos principales usos de la historia en la enseñanza de la matemática, en primera instancia encontramos *los usos ilustrativos*, que son aquellos en los que la historia complementa el desarrollo del tema y pretende, principalmente, funcionar como motivante para quien se adentra en este mundo abstracto. Podría suprimirse sin que la actividad se viera modificada sustantivamente en cuanto a lo matemático.

Un ejemplo de esto se evidencia cuando precedemos el desarrollo de un tema haciendo una introducción histórica de esto; o cuando en el desarrollo de un tema mencionamos corrientes

⁸⁸ Algunos de estas nociones se han mencionado a lo largo del trabajo, tales como el termino estable para referirnos a la clausuratividad, la aplicación similar que hace referencia a la función inyectiva, los enteros racionales que hacen referencia a los enteros actuales etc).

o matemáticas relacionadas a la nueva noción; al tomar un problema y resolverlo tal como lo hicieron en un momento histórico correspondiente. Su uso hace más atractiva la actividad y aporta información nueva que vincula al contenido con elementos de su historia. “Pero estos usos reciben críticas: entre ellas, riesgo de reducir la historia de la matemática a anécdotas y favorecer la idea de que los conocimientos matemáticos son una especie de milagro o están asociados a personajes endiosados” (Nápoles Valdez, 2009).

En una segunda instancia, se identifican también los *usos significativos*, son aquellos en los que su inclusión transforma el tratamiento del contenido y, en alguna medida, es medular y constitutiva del contenido, un ejemplo de esto puede percibirse cuando se espera que el estudiante replique a grandes rasgos el proceso histórico que se ha desarrollado hasta la formulación actual del concepto o cuando se incluyen situaciones extra-matemáticas que sirvieron de emergentes de nuevos conocimientos matemáticos.

Para Nápoles Valdés, este tipo de usos tiene como ventajas favorecer el flujo entre la ciencia y la cultura, apreciar el arte de los procesos de creación matemática, mostrar la interdependencia de las diferentes partes de la matemática, humanizar la enseñanza de la matemática, etcétera (2009).

Referencias bibliográficas

- Anaconda, M. (2017). Los números reales en el estructuralismo bourbakista: Un análisis histórico-epistemológico con fines educativos. (*Tesis Doctoral*). Universidad de cadiz, Cadiz.
- Arbelaez, G., & Galvez, F. (2011). el conjunto de los numeros reales como objeto matematico: la construccion de Dedekind. En L. Recalde, & G. Arbelaez, *Los numeros reales como objeto matematico una perspectiva Historico-Epistemologica*. Cali, Colombia: Universidad del valle.
- Barnett, J. H. (2016). *Digital Commons @ Ursinus College*. Obtenido de Richard Dedekind and the Creation of an Ideal: Early developments in ring theory: https://digitalcommons.ursinus.edu/triumphs_abstract/1
- Birkhoff, G. (1940). Lattice Theory. *American Mathematical*, 25, 1-498.
- Burris, S., & Sankappanavar, H. (1981). *A course in universal algebra*. (T. m. Edition, Ed.)
- Carrasco, P. (2004). Emmy Noether y el inicio del Álgebra Abstracta. *La Gaceta de la Real Sociedad Matemática Española*, 337.
- Conjuntos ordenados, redes y algebras de Boole. (Abril de 2020). Matematica Discreta. Unidad 5 [video]. Youtube. Obtenido de <https://youtube.com/@maticamaravillosa?si=SYW85RKHCRfdafMY>
- Corry, L. (1991). Estructuras algebraicas y textos algebraicos del siglo XIX. *Llull: Revista de la Sociedad Española de Historia de las Ciencias y de las Técnicas*, 7-30.
- Corry, L. (2004). *Modern Algebra and the Rise of Mathematical Structures*. Springer Basel.
- De la Peña, J. A. (2000). El álgebra en el siglo XX. *Miscelánea matemática de la sociedad matemática mexicana*, 54-55.

- Dedekind, R. (1872). Teoremas auxiliares de la teoria de los modulos. En R. Dedekind, *Sobre la teoría de los números enteros algebraicos* (J. Bares, & J. Climent, Trads., págs. 32-116).
- Dedekind, R. (1872/1927). Continuidad del dominio de los numeros reales. En R. Dedekind, *Continuidad y numeros irracionales* (J. Bares, & J. Climent, Trads., Quinta Edicion ed., págs. 1-15). Brunswick.
- Dedekind, R. (1872/1927). Creacion de los numeros irracionales. En R. Dedekind, *Continuidad y numeros irracionales* (J. Bares, & J. Climent, Trads., Quinta Edicion ed., págs. 1-15). Brunswick.
- Dedekind, R. (1872/1927). El germen de la teoria de los ideales. En R. Dedekind, *Continuidad y numeros iracionales* (J. Bares, & J. Climent, Trads., Quinta edicion ed., págs. (1-15)).
- Dedekind, R. (1888/1930). Aplicacion de un sistema en si mismo. En R. Dedekind, *Que son y para que sirven los numeros* (J. Bares, & J. Climent, Trads., págs. 120-184).
- Dedekind, R. (1888/1930). Sistemas simplemente infinitos. La sucesion de los numeros naturales. En R. Dedekind, *Que son y para que sirven los numeros?* (J. Bares, & J. Climent, Trads., págs. 120-184).
- Dedekind, R. (1897). *Über zerlegungen von zahlen durch ihre grobten gemeinsamen teiler*. Brunswick.
- Dedekind, R. (1900). *Ueber die von drei moduln erzeugte dualgruppe*. Leipzig.
- Lezama, O. (2017). *Cuadernos de algebra Numero 2: anillos*. Universidad Nacional de Colombia, Bogota.
- Mehrtens, H. (1979). Die entstehung der verbandstheorie. *Chicago Journals*, 72.
- Nápoles Valdez, J. (2009). *Elementos para una historia de las matemáticas griegas*. Argentina.

- Ortiz, G., & Valencia, S. (2010). La categoria de los reales en Hilbert. *Revista Brasileira de Historia da Matematica*, Vol. 10(19), 39-65.
- Panza, M. (2007/2019). *Elements de mathematiques pour philosophes* (Primera ed.). (M. Anacona, F. Galvez, & L. C. Arboleda, Trads.) Lyon. Recuperado el 2019
- Reck, E. H. (2003). Dedekind's structuralism: an interpretation and partial defense. *Synthese*, 137, 369-419.
- Rodriguez, M., Pochulu, M., & Espinoza, F. (2022). Educacion matemática aportes a la formacion docente desde distintos enfoques teóricos Vol 2. En G. Carnelli, *Distintas formas de inclusion de la historia de la matemática en la enseñanza* (págs. 49-66). Buenos Aires.
- Schlimm, D. (2011). On the creative role of axiomatics: The discovery of lattices by Schroder, Dedekind, Birkhoff, and others. *Synthese*, 183, 47-68.
- Stillwell, John. (1877). Theory of Algebraic Integers.
- Valenzuela Requena, B. (2018). Mi clásico favorito. Emmy Noether. *Revista española de física*, 56-63.
- Vélez, C. (2013). La matemática como teoria de estructuras. *Revista Colombiana de Filosofía de la Ciencia*, 12.