DE LOS GRUPOS Y CUERPOS COMO "HERRAMIENTAS" A "OBJETOS" MATEMÁTICOS

LUZ MARINA GAVIRIA LONDOÑO

UNIVERSIDAD DEL VALLE
INSTITUTO DE EDUCACIÓN Y PEDAGOGÍA
ÁREA DE EDUCACIÓN MATEMÁTICAS
SANTIAGO DE CALI, AGOSTODE 2014

DE LOS GRUPOS Y CUERPOS COMO “HERRAMIENTAS” A “OBJETOS” MATEMÁTICOS.

Luz Marina Gaviria Londoño

Código 0639734

Trabajo de Grado presentado para optar al título de

Licenciada en Matemáticas y Física

Tutora:

Maribel Anacona

Profesora Área de Educación Matemática

Instituto de Educación y Pedagogía

Universidad del Valle

Instituto de Educación y Pedagogía

Área de Educación Matemática

Santiago de Cali, Agosto de 2014

UNIVERSIDAD DEL VALLE
INSTITUTO DE EDUCACIÓN Y PEDAGOGÍA
ÁREA DE EDUCACIÓN MATEMÁTICA

Acta de Evaluación de Trabajo de Grado

Tenga en cuenta: **1.** *Marque con una* **X** *la opción escogida.*
2. *diligencie el formato con una letra legible.*

Título del Trabajo:	*De los grupos y cuerpos como "herramientas" a "objetos" matemáticos.*							
Se trata de:	*Proyecto*		*Informe Final*	X				
Director:	*Maribel Anacona*							
1er Evaluador:	*Guillermo Ortiz Rico*							
2do Evaluador:	*Celimo Alexander Peña*							
Fecha y Hora	*Año:*	*2014*	*Mes:*	*10*	*Día:*	*10*	*Hora:*	*8:00 AM*

Estudiantes

Nombres y Apellidos completos	*Código*	*Programa Académico*
LUZ MARÍNA GAVIRIA LONDOÑO	*200639734*	*3487*

Evaluación

Aprobado	X	*Meritorio*		*Laureado*	X
Aprobado con recomendaciones		*No Aprobado*		*Incompleto*	

En el caso de ser ***Aprobado con recomendaciones*** *(diligenciar la página siguiente), éstas deben presentarse en un plazo de* _____ *(máximo un mes)* ***ante****:*

Director del Trabajo		*1er Evaluador*		*2do Evaluador*	

En el caso que el Informe Final se considere ***Incompleto****, se da un plazo de máximo de* _____ *semestre(s) para realizar una nueva reunión de evaluación el:*

Año:		*Mes:*		*Día:*		*Hora:*	

En el caso que no se pueda emitir una evaluación por falta de conciliación de argumentos entre Director, Evaluadores y Estudiantes; expresar la ***razón del desacuerdo*** *y las* ***alternativas*** *de solución que proponen (diligenciar la página siguiente).*

Firmas:

Director del Trabajo de Grado	*1er Evaluador*	*2do Evaluador*

1

PARTE 1. Términos de la licencia general para publicación digital de obras en el repositorio institucional de Acuerdo a la Política de Propiedad Intelectual de la Universidad del Valle

Actuando en nombre propio los AUTORES o TITULARES del derecho de autor confieren a la UNIVERSIDAD DEL VALLE una Licencia no exclusiva, limitada y gratuita sobre la obra que se integra en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha en que se incluye en el Repositorio, por un plazo de cinco (5) años, que serán prorrogables indefinidamente por el tiempo que dure el derecho patrimonial del AUTOR o AUTORES. El AUTOR o AUTORES podrán dar por terminada la licencia solicitando por escrito a la UNIVERSIDAD DEL VALLE con una antelación de dos (2) meses antes de la correspondiente prórroga.

b) El AUTOR o AUTORES autorizan a la UNIVERSIDAD DEL VALLE para que en los términos establecidos en el Acuerdo 023 de 2003 emanado del Consejo Superior de la Universidad del Valle, la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993 y demás normas generales sobre la materia, publique la obra en el formato que el Repositorio lo requiera (impreso, digital, electrónico, óptico, usos en red o cualquier otro conocido o por conocer) y conocen que dado que se publica en Internet por este hecho circula con un alcance mundial.

c) El AUTOR o AUTORES aceptan que la autorización se hace a título gratuito, por lo tanto renuncian a recibir emolumento alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente Licencia y de la ***Licencia Creative Commons*** con que se publica.

d) El AUTOR o AUTORES manifiestan que se trata de una obra original y la realizó o realizaron sin violar o usurpar derechos de autor de terceros, obra sobre la que tiene (n) los derechos que autoriza (n) y que es él o ellos quienes asumen total responsabilidad por el contenido de su obra ante la UNIVERSIDAD DEL VALLE y ante terceros. En todo caso la UNIVERSIDAD DEL VALLE se compromete a indicar siempre la autoría incluyendo el nombre del AUTOR o AUTORES y la fecha de publicación. Para todos los efectos la UNIVERSIDAD DEL VALLE actúa como un tercero de buena fé.

e) El AUTOR o AUTORES autorizan a la UNIVERSIDAD DEL VALLE para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión. El AUTOR o AUTORES aceptan que la UNIVERSIDAD DEL VALLE pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

SI EL DOCUMENTO SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA O UNA ORGANIZACIÓN, CON EXCEPCIÓN DE LA UNIVERSIDAD DEL VALLE, LOS AUTORES GARANTIZAN QUE SE HA CUMPLIDO CON LOS DERECHOS Y OBLIGACIONES REQUERIDOS POR EL RESPECTIVO CONTRATO O ACUERDO.

VICERRECTORIA ACADÉMICA
División de Bibliotecas

Universidad del Valle

AUTORIZACIÓN PARA PUBLICACIÓN DIGITAL DE OBRAS

PARTE 2. Autorización para publicar y permitir la consulta y uso de obras en el Repositorio Institucional.

Con base en este documento, Usted autoriza la publicación electrónica, consulta y uso de su obra por la UNIVERSIDAD DEL VALLE y sus usuarios de la siguiente manera;

a. Usted otorga **una (1) licencia especial para publicación de obras en el repositorio institucional de la UNIVERSIDAD DEL VALLE** (Parte 1) que forma parte integral del presente documento y de la que ha recibido una (1) copia.

Si autorizo ☒ No autorizo ☐

b. Usted autoriza para que la obra sea puesta a disposición del público en los términos autorizados por Usted en los literales a), y b), con la ***Licencia Creative Commons Reconocimiento - No comercial - Sin obras derivadas 2.5 Colombia*** cuyo texto completo se puede consultar en http://creativecommons.org/licenses/by-nc-nd/2.5/co/ y que admite conocer.

Si autorizo ☒ No autorizo ☐

Si Usted no autoriza para que la obra sea licenciada en los términos del literal b) y opta por una opción legal diferente descríbala[1]:

En constancia de lo anterior,

Título de la obra: De los grupos y cuerpos como "herramientas" o "objetos" matemáticos.

Autores:

Nombre: Luz Marina Gaviria Londoño Firma: _____
C.C. 43.798.269 Bello

Nombre: _____ Firma: _____
C.C.

Nombre: _____ Firma: _____
C.C.

Fecha: _____

[1] Los detalles serán expuestos de ser necesario en documento adjunto

Agradecimientos

A Dios por permitirme cumplir con este propósito, por darme salud y todo cuanto necesite en este camino.

A mis hijos Alejandro y José David por su paciencia, buen comportamiento y ternura.

A mi esposo Carlos Arturo por su ayuda en la consecución de momentos de calma y soledad necesarios para concentrarme en la realización de este trabajo.

A la profesora Maribel Anacona por su maravillosa manera de decir las cosas, las cuales se convirtieron siempre en motivación e ideas.

A mis hermanos y hermanas por demostrarme todo su amor y comprensión en los momentos en que no pude acompañarlos en las reuniones familiares y por ayudarme con las tareas del hogar en tantos instantes.

A todos mis profesores de Univalle, por contribuir en mi formación.

A mis compañeros de la Institución José A. Galán por su compresión en momentos de cansancio y dificultad.

A los profesores Guillermo Ortiz y Celimo Peña, por las observaciones y recomendaciones.

A los profesores Jaime Arango Cabarcas, Jairo Duque Robles, Manuel Villegas y Liliana Camargo del departamento de matemáticas por su ayuda en las traducciones del alemán al español y por dar respuesta a mis múltiples dudas.

Tabla de Contenido

Resumen

El presente trabajo contiene un estudio histórico sobre la constitución como objetos del Álgebra Moderna de las nociones de *Grupo y Cuerpo*. Los momentos centrales de esta historia, se hallaron en la exposición de los sucesos relacionados con la emergencia y evolución histórica de dichos objetos; los aportes de Dedekind y Emmy Noether en la consolidación de una teoría coherente; y el análisis de los contenidos, los prólogos y algunas definiciones encontradas en los libros de textos: Lehrbuch der Algebra de Heinrich Weber y Modern Álgebra de B. Van der Waerden.

Palabras Clave: Historia de las matemáticas, Álgebra Moderna, teoría de Grupos, teoría de Cuerpos, Emmy Noether, Richard Dedekind, Heinrich Weber, Van der Waerden, Lehrbuch der Algebra y Modern Álgebra, Herramienta y objeto matemático.

0. INTRODUCCIÓN

El presente trabajo se inscribe en la línea de formación en Historia y Epistemología de las Matemáticas del programa de Licenciatura en Matemáticas y Física de la Universidad del Valle. Se pretende identificar los aspectos centrales que permiten explicar históricamente el paso epistemológico de las nociones de *Grupo* y *Cuerpo* como "herramientas" a "objetos" matemáticos en el periodo de 1870 a 1930. Para ello se parte del estudio de la trayectoria y acontecimientos vinculados a las distintas etapas de los objetos matemáticos en cuestión, con el fin de conocer su evolución y desarrollo.

Abordar el estudio epistemológico de las nociones de *Grupo* y *Cuerpo* implicó revelar aspectos de la prehistoria de dichos conceptos y las etapas principales de su evolución. También la búsqueda de conexiones históricas fundamentales entre los aportes de varios matemáticos y de documentos que surgieron en la época. En la tarea de recrear el paso epistemológico de las nociones de Grupo y Cuerpo como "herramientas" a "objetos matemáticos" se toma la siguiente definición citada por D' Amore & Godino (2007): "El *objeto matemático* designa todo lo que es indicado, señalado o nombrado cuando se construye, comunica o aprende matemáticas".

En la definición anterior, el autor expresa que intervienen varios tipos de entidades: lenguaje, situaciones, procedimientos, conceptos, argumentos y propiedades o atributos de los objetos. Todos estos en conjunto se organizan en sistemas conceptuales o teorías, su emergencia por separado los sitúa en la categoría de herramienta debido a su vinculación directa con la necesidad histórica de resolver algún problema concreto.

El periodo de 1870 a 1930 se toma como base de la investigación debido a que durante este se desarrolla el enfoque estructural del álgebra. Según Corry (1991) el surgimiento de éste enfoque tuvo como consecuencia un cambio sustancial en la concepción misma del alcance y de los fines de la investigación algebraica. Tras la clasificación de diversos Grupos y Cuerpos, vino la separación de la naturaleza de estos de cualquier problema concreto.

Alrededor de esto, Morris Klein (1972) afirma que "el hecho básico de que el álgebra puede tratar sistemas de objetos que no sean necesariamente números reales o complejos, quedó definitivamente demostrado en una buena docena de creaciones del siglo XIX" (p. 1499).

Creaciones que sugieren una nueva manera de hacer matemáticas. Así como la definición de nuevos objetos, operaciones, propiedades, relaciones y métodos que constituyen las pistas para armar el entramado histórico en el que se puede vislumbrar el surgimiento de las diferentes ideas que configuran luego los conceptos abstractos de *Grupos* y *Cuerpos* en una teoría unificadora del Álgebra Moderna.

Precisamente en este periodo surgió el Álgebra Moderna o Álgebra Abstracta, así como el cambio de status de las nociones de Grupo y Cuerpo, usados inicialmente como *herramientas* que permitían solucionar problemas concretos de diferentes teorías matemáticas y luego como unos conceptos en sí mismos independientes de la naturaleza de los objetos. Los libros de texto de Weber (1895, 1896,1908) y el de van der Waerden (1930)[1], en particular, muestran ese cambio. Las contribuciones de Richard Dedekind y Emmy Noether, por su parte, desempeñan un papel principal en esta historia.

Historiadores como Morris Klein (1972), Leo Corry (1996) e Israel Klein (2007), reconocen que los libros de Weber (1895) y van der Waerden (1930) de Álgebra Moderna presentan diferencias cruciales en su contenido debido al periodo histórico en el que fueron escritos. Weber da cuenta en su libro sólo de los avances del álgebra hasta finales del siglo XIX y de los primeros usos de los conceptos emergentes de Grupo y Cuerpo. Estos aparecen dotados de un programa intelectual que corresponde con el enfoque estructural que se mantiene hasta nuestros días. En el Álgebra de van de Waerden los conceptos de Grupo y Cuerpo alcanzaron gran parte de la madurez con la que se les reconoce en la actualidad.

Para cumplir con los objetivos que se plantean en este trabajo fue necesario contrastar diferencias y similitudes en los contenidos de estas obras y en las definiciones de los conceptos objeto de estudio.

Tal contraste es de gran importancia en los procesos curriculares de la enseñanza del Álgebra Moderna. Analizarlos permite encontrar posibles respuestas a rupturas de tipo epistemológico presentes en los métodos empleados, los significados particulares y

[1] La obra de van der Waerden fue publicada en 1930, en este trabajo el análisis de texto se hace de la edición en inglés publicada en 1953.

generales que se dan a conocer en cada periodo histórico y las pretensiones que se evidencian en la metodología que esconde el libro de texto. En forma general, la siguiente cita muestra la importancia que revierten los libros de textos universitarios en la planeación curricular y en la organización de contenidos académicos:

> Los libros de texto universitarios desempeñan un papel muy importante en la planeación curricular y en la organización de contenidos académicos, tienen una marcada influencia en las decisiones de profesores y estudiantes en la forma en que un curso es impartido, siendo no solo fuente de contenido curricular sino también una exposición organizada en una estructura de un Cuerpo de conocimientos. (Acero, 2008, p. 4)

También es importante explicitar las imágenes de álgebra que dichos textos contienen, ya que éstas develan una forma de hacer matemáticas y se convierten en la posibilidad de encontrar las rupturas epistemológicas que impiden en muchos casos el acceso al conocimiento, además de observar el potencial que poseen los estudios históricos en los procesos de enseñanza de las matemáticas.

Así, si se logran identificar los aspectos centrales que permiten explicar histórica y epistemológicamente el paso de la nociones de *Grupo* y *Cuerpo* como "herramientas" a "objetos" matemáticos" es muy probable que se alcance a mostrar algunos de los procesos y métodos que aclaren el panorama de la enseñanza de estas nociones fundamentales del Álgebra Abstracta. Se sabe que dificultades en la comprensión de la estructura de objetos matemáticos formales, generales y abstractos son una de las causas de la deserción y repitencia del curso de Álgebra Moderna en los programas de Matemáticas y Licenciaturas en Matemáticas.

Es por ello, que el estudio de la historia del álgebra desde principios del siglo XIX hasta las primeras décadas del siglo XX en torno a la noción de *Grupo* y de *Cuerpo*, junto con la marcada influencia de los aportes de Richard Dedekind, Emmy Noether y el análisis de los textos *Lehrbuch de Álgebra* y *Modern Algebra*, puede significar un aporte para esclarecer el panorama histórico que dio surgimiento a una nueva Álgebra, tan extraña y complicada como la ven muchos, tan encantadora y llena de promesas como la ven otros.

Todo lo anterior, confluye necesariamente en una reflexión de orden epistemológico en torno al status de las nociones de Grupo y de Cuerpo en ambos momentos históricos, de tal manera que se aprovechen las ventajas heurísticas del proceso de evolución de éstos y en la transformación de algunas ideas que han permanecido en el tiempo y se juzgue el por qué se establece un Cuerpo de conocimientos en los textos de matemáticas de una forma y no de otra.

Sin embargo, para dicha reflexión fue necesario adoptar una postura metamatemática frente al trabajo investigativo, esto debido a que las posibilidades de comprensión de un texto de matemáticas se encuentran envueltas en un sistema de "*imágenes de conocimiento*"[2], que hacen parte de la ideología de su autor. Estas imágenes son de alguna forma concretadas por el escritor de un libro en el *Cuerpo de conocimientos*[3]. "Las ideologías suelen constar de dos componentes: una representación del sistema, y un programa de acción. La primera proporciona un punto de vista propio y particular sobre la realidad, las creencias, preconceptos o bases intelectuales, a partir del cual se analiza y enjuicia, habitualmente comparándolo con un sistema alternativo, real o ideal. El segundo tiene como objetivo acercar en lo posible el *sistema real* existente al *sistema ideal* pretendido" (Nocera, 2009).

Dichas imágenes de conocimiento según Corry (1996) dan origen a cierto "*Cuerpo de conocimientos*" y el reconocimiento de la interacción entre el Cuerpo y las imágenes de conocimiento en un periodo histórico determinado, son un factor importante en el desarrollo de la disciplina en tanto abre posibilidades para la investigación histórica de las matemáticas y permite el estudio de los cambios particulares que afectan por separado a los contenidos del texto y los principios selectores que el autor tuvo en cuenta al escribir su obra.

De lo anterior surge que todos los libros de Álgebra Moderna no son iguales. Revelan imágenes de conocimiento diferentes, conceptos matemáticos introducidos de diversas maneras y esto implica procesos disímiles para aprender lo mismo. Al respecto y con

2 Para el historiador Leo Corry las imágenes de conocimiento son principios de selección que rigen el programa intelectual del matemático que escribe un libro, para escribirlo debe realizar cierto tipo de metapreguntas que configuran los fines, las teorías, métodos, conceptos, hechos, metodologías entre otras cosas que se encuentran implícitos en el Cuerpo de conocimientos que se expone en dicho texto.

33El Cuerpo de conocimientos no es más que los contenidos que un autor decide incorporar en su obra.

relación al texto de Álgebra Moderna de van der Waerden y al papel de las estructuras en Bourbaki, Corry (1996) expresa que:

> "La formulación abstracta de los conceptos algebraicos era una condición necesaria para la aparición del enfoque estructural representado por el Álgebra Moderna, pero si intentamos enumerar las diferencias entre ese libro y un texto como el de Weber encontraremos que hay mucho más. El enfoque estructural del álgebra de van der Waerden es reflejo de una imagen del álgebra: allí se establece tácitamente qué cuestiones son importantes en álgebra, cuales son las respuestas adecuadas a esas preguntas, cuales son los métodos adecuados para obtenerlas. Esta imagen del conocimiento fue pronto la aceptada por los algebristas, aún cuando no se hubiera articulado ni sugerido ningún concepto formal de estructura algebraica en el libro de van der Waerden o en otro lugar previamente. La búsqueda de este concepto formal fue una consecuencia a posteriori del surgimiento de la concepción originada por la imagen informal, y Bourbaki fue uno de los participantes en esa búsqueda" (p.6).

La anterior cita de Corry, deja abierto el problema de encontrar diferencias en los libros que son objeto de análisis en este trabajo, en particular se hace alrededor de las nociones de Grupo y Cuerpo. Esto es importante, en tanto éstas permitan mostrar el avance o retroceso que implican dichas diferencias en las imágenes del conocimiento en el proceso de comprensión de los conceptos *Grupo* y *Cuerpo.* También, que puedan dilucidarla necesidad o no de dicho enfoque estructural como ventaja heurística en la enseñanza del Álgebra Moderna. La potencialidad o desventaja que se tienen a partir de la *imagen de conocimiento* inmersa en el libro de Weber, en el cual los conceptos de *Grupo y Cuerpo* prefiguran como una "herramienta" para solucionar problemas concretos, en lugar de la imagen de las estructuras algebraicas presentes en el libro de van der Waerden.

Sin perder el objetivo de este trabajo es importante una mirada a las discusiones sobre este cambio de estatus del álgebra. En particular, las que hacen algunos autores como Kline (1976) en torno a una preocupación suscitada por el fracaso de un programa instaurado a mediados del siglo XX en los Estados Unidos. Dicho programa hace referencia a las matemáticas modernas como parte del currículo de la educación formal. El autor citado realiza la siguiente pregunta al respecto: *¿Es posible entender una teoría si desde el primer momento se le da la forma definitiva que impone la lógica rigorosa, sin mencionar para nada el camino por la que ha llegado a adoptar esta forma?* Su respuesta fue: "*No, realmente no es posible entenderla; incluso resulta imposible retenerla sino es de memoria"* (p. 58).

La anterior respuesta muestra de alguna manera la importancia que reviste el estudio histórico de los conceptos que hacen parte de las matemáticas modernas, entre estos, las nociones de Grupo y Cuerpo; y reflexionar sobre la metodología instaurada por la escuela formal.

También es importante resaltar que las imágenes de conocimiento de los autores de textos universitarios de matemáticas son imperceptibles, a menos que se realicen este tipo de análisis en los textos académicos, ya que esto permite vislumbrar las formas del quehacer matemático que permean el currículo de las universidades por años.

En el currículo de las universidades colombianas el proceso de enseñanza del Álgebra Abstracta corresponde al Grupo de matemáticas avanzadas o cursos de formación profesional de los planes de Matemáticas y de Licenciatura en Matemáticas que se introducen en los últimos semestres de la carrera. No obstante, se presentan las mismas dificultades de compresión y quizás mayores que las que se tenían en los primeros semestres en los cursos de Álgebra Lineal y Cálculo I donde el índice de repitencia y deserción es ampliamente conocido.

Al mismo tiempo, las investigaciones revelan que los estudios centrados en textos académicos universitarios de matemáticas avanzadas son escasos (Acero, F. 2008), reduciéndose aún más cuando el estudio se refiere a un área del saber determinado como es el Álgebra Moderna. Esto sugiere una problemática adicional que tiene que ver con el desarrollo de los procesos didácticos alrededor de estos cursos, sobre todo aquellos que tienen que ver con la evolución histórica de los conceptos.

En la investigación de Acero (2008) también se afirma que la cantidad de libros de texto dedicados a la enseñanza de Álgebra Moderna es escasa y muchos de ellos corresponden a traducciones o se encuentran escritos en otros idiomas. Esto pone al descubierto que la problemática de acceso al conocimiento se vincula de alguna manera a la dependencia con el contexto sociocultural del autor de textos académicos (sus imágenes de conocimiento). Situación que además puede convertirse en determinado momento en una dificultad para la comprensión de los significados expuestos en estos.

Es importante resaltar que un concepto central del Álgebra Moderna es el de estructura de *Grupo* y este conduce al estudio de las estructuras denominadas *Anillos* y *Cuerpos*, es decir, para comenzar el estudio de conceptos tan complejos como el de "Cuerpo" es necesario arrancar en la constitución de la noción de "Grupo". Sin embargo, la tarea no es fácil debido a que la constitución de la noción de estructura de *Grupo* ha sido un proceso largo que incluye la construcción de diversos conceptos que fueron prerrequisito para su establecimiento. El problema radica en que la emergencia de dichos conceptos no ha sido lineal y mucho menos parte del plan de un solo matemático o de una sola disciplina, lo cual advierte sobre maniobras intelectuales importantes en el devenir de éstos.

Algunos autores como Kleiner (2007) muestran implícitamente la necesidad de observar las imágenes de álgebra en la evolución de la teoría de *Grupos*, puesto que el enfoque para la producción de las nuevas matemáticas que surgieron en el periodo que se desea analizar estaba cambiando, al respecto este investigador afirma que:

> Nuestra historia sobre la evolución de la teoría de Grupos se inicia en 1770 y se extiende hasta el siglo XX, pero los mayores avances se produjeron en el siglo XIX. Algunas de las funciones matemáticas generales de ese siglo que tenían relación con la evolución de la teoría de Grupos son: (a) un aumento de la preocupación por el rigor; (b) la aparición de la abstracción; (c) el nacimiento del método axiomático; (d) el punto de vista de las matemáticas como una actividad humana es posible sin referencia a, o la motivación de las situaciones físicas. (p.15)

Para abordarlas problemáticas que se describen en los párrafos anteriores en el primer capítulo se aborda la emergencia y evolución de los conceptos de Grupo y Cuerpo, en el segundo se describen las contribuciones de Richard Dedekind y Emmy Noether a la consolidación de dichos conceptos. El tercer capítulo se considera, describe y contrasta algunos de los contenidos de los libros *Lehrbuch de Álgebra* (1895) de Heinrich Weber y *Modern Álgebra* (1930) de B.L. van der Waerden con el fin de reconocer las *imágenes de conocimiento* para cada autor.

Capítulo 1.

EMERGENCIA Y EVOLUCIÓN DE LOS GRUPOS Y CUERPOS

> *¿Es posible entender una teoría si desde el primer momento se le da la forma definitiva que impone la lógica rigorosa, sin mencionar para nada el camino por la que ha llegado a adoptar esta forma? (Kline, 1972.)*

Las clases de objetos que configuran la teoría de Grupos, es decir, esas estructuras algebraicas llamadas Grupos, fueron emergiendo en diferentes momentos de forma aislada y sin conexión alguna (Kline, 1972). A finales del siglo XIX la formulación de los axiomas de *Grupo* sobre un conjunto cualquiera y una operación binaria posibilita una separación de la naturaleza concreta de los *Grupos* y de su funcionamiento. La clave en la búsqueda de dichos objetos parece estar en la clasificación de propiedades que permanecen invariantes bajo un determinado tratamiento y no simplemente de la adopción de la terminología usual en el álgebra abstracta.

Kleiner (2007) indica por dónde empezar esta búsqueda. Dice que la génesis de la noción de Grupo tiene lugar desde cuatro fuentes principales: La primera proviene del álgebra clásica, dado que de esta emerge la teoría de *Grupos de permutaciones*. La segunda se origina de la teoría números, en la cual se desarrolla la teoría de *Grupos abelianos*. La tercera y cuarta surgen de la geometría y análisis, en las que en conjunto nace la teoría de los *Grupos de transformación*. Sin embargo, la gran tarea aquí es encontrar las conexiones entre cada parte sin dejar por fuera el paso decisivo que dio Richard Dedekind para esclarecer la emergencia y consolidación del concepto de Grupo.

1.1 Emergencia y Evolución del Concepto de Grupo

A principios del siglo XIX la necesidad de la noción de *Grupo* se comenzaba a perfilar, es decir, se consideraba necesario cierto andamiaje sobre todo por la tradición de la matemática de ser demostrativa. Esto permitió que los Grupos se establecieran como herramienta que permitía solucionar algunos problemas concretos de la época.

Hasta finales del siglo XVIII el álgebra consistía, en gran parte, en el estudio de las soluciones de las ecuaciones polinómicas. En el siglo XX, el álgebra se convirtió en el estudio de los sistemas axiomáticos abstractos. La transición de la llamada álgebra clásica de ecuaciones polinómicas al álgebra moderna de los sistemas axiomáticos se produjo en las últimas décadas del siglo XIX. Razón por la cual en el presente trabajo se realiza una lectura juiciosa pero global de algunos acontecimientos que posibilitaron tal transición.

Antes que todo es conveniente partir de una definición moderna del concepto de Grupo y tenerla presente durante los acontecimientos que perfilaron la emergencia de esos primeros ejemplos (Grupos de permutaciones, Grupos abelianos y Grupos de transformaciones):

> Se dice que un conjunto no vacío G es un Grupo si en él hay definida una operación * tal que:
> $a, b \in G$ implica $a * b \in G$.
> (Esto se describe diciendo que G es cerrado respecto a $*$.)
> Dados $a, b, c \in G$, se tiene que $a * (b * c) = (a * b) * c$
> (Esto se describe diciendo que es válida la ley asociativa en G.)
> Existe un elemento especial $e \in G$ tal que $a * e = e * a = a$; y para todo $a \in G$ (e se llama elemento identidad o unidad de G.)
> Para todo $\boldsymbol{a} \in \boldsymbol{G}$ existe un elemento $b \in G$ tal que $a * b = b * a = e$.
> (Este elemento b se escribe como a^{-1} y se llama inverso de a en G bajo la operación *.)
> (Heirstein, 1986, p. 40).

La anterior definición fue tomada debido a que el libro de Heirstein (en distintas ediciones) se ha utilizado de manera recurrente en los curso de álgebra abstracta en diferentes universidades de Colombia, sin embargo, esta definición desconoce dos propiedades importantes, a saber, la propiedad uniforme y la unicidad de la inversa. Cuando se tiene un conjunto y una operación, existe una doble implicación, tal que:

Si $*$ es una operación en $A \leftrightarrow *$:

$$A \times A \to A, \text{ esto equivale,}$$

$$\{i) Para\ todo\ (a, b) \in A \times A\}$$

$$ii)\ Existe\ un\ único * (a, b) \equiv a * b$$

$$\text{En } i) \left\{ \begin{array}{c} si\ a,b \in A \rightarrow a * b \in A \ \leftrightarrow \\ para\ todo\ a,b,c,d\ \in A\ (clausurativa) \\ (a,b) = (a,d) \rightarrow a * b = c * d\ (uniforme) \\ a = c \rightarrow a * b = c * b\ (uniforme\ por\ izquierda) \\ b * a = b * c (uniforme\ por\ derecha) \end{array} \right\}$$

En otras palabras debería decirse lo siguiente:

$$* \ es\ una\ operación\ en\ A \leftrightarrow * \ es\ clausurativa\ y$$

$$* \ es\ uniforme\ (por\ izquierda\ y\ por\ derecha).$$

1.1.1Grupos de Permutaciones

Los Grupos de permutaciones son el ejemplo de Grupo finito que más se utiliza, esto obedece a dos cuestiones fundamentales, una de éstas es que todo Grupo es isomorfo a un Grupo de permutaciones (teorema de representación de Cayley) y la otra es que el Grupo de las raíces de las ecuaciones de un polinomio permite determinar la solubilidad de una ecuación algebraica asociada a él.

Para comenzar, se puede esbozar a groso modo algunos antecedentes históricos que desarrolla Kleiner (2007) y enriquecerlos para mejorar la visualización del panorama que se establece alrededor de la problemática que se busca resolver en el momento en que emerge los Grupos de permutaciones, también llamados Grupos simétricos.

Alrededor del año 1600 antes de Cristo los babilonios ya sabían cómo resolver ecuaciones de segundo grado esencialmente por el método de completar cuadrados; con los métodos de Diofanto de Alejandría (siglo III d.c.) se podían resolver casi todas las ecuaciones cuadráticas; la resolución de las ecuaciones cúbica y cuartica se dio en torno a 1540 en el Renacimiento italiano. Se dice que Scipio del Ferro (1465-1526) resolvió las ecuaciones cúbicas (con notación algebraica) y en 1535, en una competición pública, Tartaglia (1500-1557) frente a Fior (discípulo de Ferro) presentó un método general para la resolución de las ecuaciones cúbicas, pero se negó a contar los detalles. Se los contó bajo secreto de juramento a Cardano (1501-1576), el cual publicó en su Ars Magna. El Ars Magna contenía también un método, debido a Ferrari (1522-1565), para resolver la ecuación de cuarto grado, con el artificio de reducir la cuartica a una cúbica mediante una ecuación auxiliar.

Es importante resaltar que en el mismo periodo histórico, Vieta (1540-1603) y luego Harriot (1560-1621) introdujeron un nuevo simbolismo algebraico que permitió, entre otras cosas, que las operaciones en la resolución de ecuaciones se hicieran más visibles y de esa forma se diera un paso decisivo en los procesos de generalización. De hecho Vieta utiliza expresiones generales y no particulares como lo hacen sus antecesores. Posteriormente con los aportes de René Descartes (1596-1650) se formaliza la teoría de ecuaciones, se introduce muchos de los símbolos y terminología del álgebra actual. Su método contribuyó a que las curvas pudieran ser estudiadas por ecuaciones y las ecuaciones por curvas. Además, realiza la primera aproximación al teorema fundamental del álgebra mediante la sentencia: "toda ecuación puede tener tantas raíces distintas como el número de dimensiones de la incógnita de la ecuación."La solución de ecuaciones de mayor grado de la cuartica, tardó más de doscientos años en hallarse, pese a que D' Alembert en 1749 (de forma poco rigurosa), y más adelante Gauss (1799) con todo el rigor que le caracterizaba, habían demostrado el *Teorema Fundamental del Álgebra*[4], refinando su demostración en publicaciones posteriores, hasta obtener una completamente satisfactoria en 1849.

Desde ese entonces, muchos matemáticos intentaron resolver las ecuaciones de quinto grado. Euler (1707-1783) fracasó en el intento de resolver estas ecuaciones, pero encontró nuevos métodos para resolución de las cuarticas. Lagrange (1736-1813) en 1770 mostró que el método de resolución de las cúbicas y cuarticas dependía de encontrar funciones en las raíces que fueran invariantes por efecto de ciertas permutaciones; y mostró que dicho método fallaba con las quinticas. Inspirado en los trabajos de Lagrange, en 1799 Ruffini (1765-1822) publicó un trabajo titulado *Teoria generale delle equazioni*que contenía una demostración, poco rigurosa, aunque básicamente correcta, que conducía a establecer que la ecuación de quinto grado no es resoluble por radicales[5]. Según Villa (2011) el primero en introducir las nociones de orden de un elemento, conjugación, descomposición cíclica de elementos de los Grupos de permutaciones y las nociones de primitividad e imprimitividad fue Ruffini. Él probó, entre otras cosas, agrega Villa, que el orden de una permutación es el

[4] El Teorema Fundamental del Algebra afirma que toda ecuación polinomial de grado n con coeficientes complejos tiene n raíces complejas.

[5] Una ecuación resoluble por radicales es aquella que solo usa operaciones de suma, resta, multiplicación, división, exponenciación y radicación de sus coeficientes.

mínimo común múltiplo de las longitudes de la descomposición en ciclos disjuntos y que S_5 no tiene subgrupos de orden 3,4 u 8.

Lagrange (1736-1813) por su parte, en su obra *Reflexión sur la resolution algebrique des equations* (1770), observó que la solución de Ferrari de la ecuación de cuarto grado consistía en encontrar otra de grado tres, cuyas soluciones se conectaban con las soluciones de la ecuación de grado cuarto original. Es decir, la ecuación de grado cuatro también tiene una resolvente[6] de grado tres. Logró así, encontrar la característica subyacente en otros métodos: el hecho de que funcionen se debe a que es posible reducir cualquier ecuación cúbica o bicuadrática a una auxiliar cuyo grado es menor, en uno, que el de las ecuaciones originales; éstas, por lo tanto, admiten una solución por medio de radicales. Dávila (2003) expone de la siguiente manera el método de Lagrange:

> Supongamos que x, y, z son las raíces de la cúbica general, las cuales no conocemos a priori. Consideremos ahora la cantidad t dada por
>
> $$t = x = ay + a^2z \qquad (1)$$
>
> Donde a es una raíz cúbica primitiva de la unidad. Si permutamos las raíces en (1), entonces obtenemos seis valores posibles para t pues el total de permutaciones de tres objetos es $3! = 6$.
>
> Sean $t_1, t_2, \dots, t_6$ los distintos valores que se obtienen de (1) al permutar las raíces de la cúbica. Estos seis valores satisfacen la ecuación
>
> $$f(x) = (x - t_1)(x - t_2)(x - t_3)(x - t_4)(x - t_5)(x - t_6) \qquad (2),$$
>
> Los coeficientes de esta ecuación cómo es posible observar son polinomios simétricos en las t_i, por la manera en que fueron definidas las t_i, también son simétricos en x, y, z; luego se pueden conocer en términos de los coeficientes de la cúbica que se pretende resolver. La ecuación (2) es la ecuación que hoy se llama resolvente de Lagrange para el caso de la cúbica.
>
> Nótese que (2) es una ecuación de sexto grado, considerablemente mayor que el de la que el de la cúbica que se quiere resolver por radicales. Sin embargo, en este caso las cantidades t_i satisfacen las relaciones $t_2 = at_1$, $t_3 = a^2t_1$, $t_5 = at_4$, $t_6 = a^2t_4$. Este se cumple para cierto orden de las permutaciones de las raíces en (1); si se permutan las raíces en otro orden, se obtienen relaciones similares a las anteriores. De esta manera, (2) es una ecuación cuadrática en x^3 pues
>
> $$f(x) = (x^3 - t_1^3)(x^3 - t_4^3) = (x^3)^2 - (t_1^3 + t_4^3)x^3 + (t_1^3 + t_4^3)x^3.$$

[6] Expresión del latín que quiere decir "ecuación que resuelve"

> Si hacemos $u = t_1^3$ y $v = t_4^3$, entonces los coeficientes de esta ecuación son precisamente $u + v$ y uv, para los cuales es posible una expresión en términos de la cúbica original y se obtiene a través de ellos la solución. De esta manera, se obtienen los seis valores para t; por consiguiente, las soluciones de la cúbica están dadas por
>
> $$x = \frac{1}{3}[(x - y + z) + t_1 + t_4],$$
>
> $$y = \frac{1}{3}[(x - y + z) + a^2 t_1 + a t_4],$$
>
> $$z = \frac{1}{3}[(x - y + z) + a t_1 + a^2 t_4],$$
>
> por lo que solo se necesita identificar bien a t_1 y a $t_4$de entre las seis posibles soluciones de la ecuación resolvente (2). Recuerdese que la expresión $x + y + z$ es un polinomio simetrico elemental de estas tres raíces y, por lo tanto, conocemos su valor pues es el coeficiente del termino cuadratico en la cubica de la forma $x^3 + ax^2 + bx + c = 0$. En este caso, Lagrange va más alla y da una nueva manera explícita para calcular esos valores. (pp. 53-54)

Lagrange aplicó el mismo método a la ecuación general de quinto grado y a pesar de que no logró resolver el problema de la solución algebraica de la ecuación de quinto grado, ésta fue la primera vez, según Kleiner (2007), que alguien realizara una asociación entre las soluciones de una ecuación polinómica y las permutaciones [7]de sus raíces. Villa (2011) asegura que Lagrange no realizó composición de permutaciones, por lo cual no es posible decir que la teoría utilizada por él pueda considerarse totalmente como una teoría de Grupos. Sin embargo, Las permutaciones corresponden actualmente al Grupo finito que más se utiliza dentro de la teoría de Grupos.

En las fórmulas empleadas por Lagrange el orden en que se escriben las raíces no afecta al polinomio, lo cual refleja la simetría existente en las expresiones de los coeficientes en términos de los coeficientes de los polinomios, es decir, el resultado no se ve afectado por permutar el orden en que se escriben los coeficientes.

De hecho, el estudio de las permutaciones de las raíces de una ecuación es una piedra angular de la teoría general de ecuaciones. Aunque Lagrange habló de permutaciones sin tener en cuenta un "cálculo " de permutaciones (por ejemplo, no hay ninguna consideración

7 En matemáticas, una permutación es la variación del orden o de la disposición de los elementos de un conjunto. Por ejemplo, en el conjunto {1,2,3}, cada ordenación posible de sus elementos, sin repetirlos, es una permutación.

de su composición o de cerradura), Kleiner afirma que el germen del concepto de Grupo -como un Grupo de permutaciones- está presente en su obra. Así mismo, por su parte, Kline (1972) asevera que lo que inició Lagrange significó luego una manera de estudiar subgrupos de un Grupo de sustituciones.

En términos modernos los teoremas sobre funciones no simétricas, son el fundamento del método de Lagrange, que si bien no conduce a la resolución general para $n \gg 5$, como él perseguía, preparó la forma para obtener la estructura algebraica que debía adoptar dicho proceso. Este método según Rey Pastor (1957) tiene tres etapas a saber:

> Formulación de una función lineal $\zeta = c_1 x_1 + \cdots + c_n x_n$, cuya potencia p-ésima $z = \zeta^p$ tenga solamente un número $v < n$ de valores;
> 2. Formación de la ecuación $(z-\varphi)(z-\varphi_1)\ldots(z-\varphi_{v-1}) = z^v + A_1 z^{v-1} + A_2 z^{v-2} + \cdots + A_n = 0$, llamada "la resolvente de Lagrange", que reduce la solución de $f(x) = 0$ ala de esta resolvente, cuyo grado es el número v de valores de la función z elegida;
> La expresión racional de las raíces x_1 mediante los valores $\zeta = \sqrt[p]{z}$. (p.209)

Cauchy (1789-1857) generaliza el teorema de Ruffini sobre el orden de una permutación en 1815. El prueba que si mediante las permutaciones de sus n variables un polinomio toma más de dos valores, entonces toma al menos p valores, donde p es el mayor primo en n; en otras palabras, no hay subgrupos del Grupo simétrico de n permutaciones con un índice i tal que $2 < i < p$. Según Grandjot [8](1940), Cauchy creó la noción de Grupo de permutaciones al estudiar las permutaciones de las raíces de ecuaciones.

Abel (1802-1829) en 1824 probó que la ecuación general de quinto grado no es resoluble por radicales. En sus memorias sobre ecuaciones algebraicas, demuestra por el método de reducción al absurdo la imposibilidad de resolver la ecuación general de grado quinto y de grado superior a cinco en la cual utiliza los resultados obtenidos por Cauchy. En Sánchez (2011) se encuentra la siguiente versión de la demostración realizada por Abel en 1824:

Sea $y^5 - ay^2 + by^3 - cy^2 + dy - e = 0$ (1)

[8] Carlos Grandjot (1930-1960), fue alumno de Landau y de Hilbert, uno de los fundadores del Instituto de Ciencias de Chile en 1929. Procedente de Alemania, contratado para introducir el álgebra abstracta en las universidades de Chile. Prolonga su estadía en Chile debido a la II guerra mundial.

La ecuación general de quinto grado; y supongamos que es resoluble algebraicamente, es decir, y puede ser expresada por una función formada por radicales de las cantidades a, b, c, d, e.

Claramente en este caso podemos expresar y de la forma:

$$y = p + p_1 R^{\frac{1}{m}} + p_2 R^{\frac{2}{m}} + \cdots + p_{m-1} R^{\frac{m-1}{m}}, \qquad (2)$$

Siendo m un número primo y $R, p, p_1, p_{2,}, \ldots$, funciones similares a y, y así hasta que obtenemos funciones racionales expresadas en función de los términos a, b, c, d, e.

Podemos también asumir que es imposible expresar $R^{\frac{1}{m}}$ mediante una función racional en términos de $a, b, \ldots, p, p_1, p_{2,}, \ldots$, y considerando $p_1 R^{\frac{1}{m}}$ en lugar de R, está claro que podemos hacer que $p_1 = 1$.

Entonces

$$y = p + R^{\frac{1}{m}} + p_2 R^{\frac{2}{m}} + \cdots + p_{m-1} R^{\frac{m-1}{m}} \qquad (3)$$

Sustituyendo este valor de y en la ecuación (1) y reduciendo, obtenemos un resultado de la forma:

$$P = q + q_1 R^{\frac{1}{m}} + q_2 R^{\frac{2}{m}} + \cdots + q_{m-1} R^{\frac{m-1}{m}} \qquad (4)$$

siendo $q, q_1, q_2, \ldots$, racionales de funciones enteras (por ejemplo: polinomiales) de los términos, $a, b, c, d, e, p, p_1, p_{2,}, \ldots, R$. (5)

Si los términos $q, q_1, q_2, \ldots$, no son igual a cero, las ecuaciones expresadas en (5) tienen necesariamente una o más raíces en común. Si K es el número de esas raíces mencionadas y en la cual todos los coeficientes sean funciones racionales de $R, q, q_1,$ y q_{m-1}.

Sea $r + r_1 z + r_2 z^2 + \cdots + r_k z^k = 0$ (6), dicha ecuación. Esta tiene raíces en común con la ecuación $z^m - R = 0$; así, todas las raíces de esta ecuación tienen la forma $a\mu z$, donde $a\mu$ designa una de las raíces de la ecuación $a_\mu^m - 1 = 0$.

Entonces sustituyendo en (6) $z \to a\mu z,$ tenemos las siguientes ecuaciones,

$$r + r_1 z + r_2 z^2 + \cdots + r_k z^k = 0 \qquad (7.1)$$

$$r + a r_1 z + a^2 r_2 z^2 + \cdots + a^k r_k z^k = 0 \qquad (7.2)$$

$$\ldots r + a_{k-2} r_1 z + a_{k-2}^2 r_2 z^2 + \cdots + a_{k-2}^k r_k z^k = 0 \qquad (7.k)$$

En estas k ecuaciones, uno puede siempre encontrar el valor de z expresado mediante una función racional de los términos $r, r_1, r_2, \ldots, r_k$, y, como los términos son en sí mismos funciones racionales de $a, b, c, d, e, R, p, p_1, p_2, \ldots$, se deduce que z es también una función racional de estos mismos términos, lo cual es contrario a la hipótesis. Por lo tanto, tiene que cumplirse necesariamente que

$$q = 0, q_1 = 0, \ldots, q_{m-1} = 0. \qquad (8)$$

Si ahora estas ecuaciones son válidas, está claro que la ecuación propuesta en (1) es se satisface con todos los valores que se obtienen para y dándole a $R^{\frac{1}{m}}$todos los valores.

$$R^{\frac{1}{m}}, aR^{\frac{1}{m}}, a^2R^{\frac{1}{m}}, \dots, a^{m-1}R^{\frac{1}{m}}, \quad (9)$$

Siendo a una raíz de la ecuación

$$a^{m-1} + a^{m-2} + \cdots + a + 1 = 0 \quad (10)$$

Tenemos entonces que todos los valores de y son diferentes, por el contrario en el caso de que tuviéramos una ecuación de la misma forma que la ecuación $P = 0$, ésta nos llevaría, como hemos visto, a un resultado que no puede ser válido. El número m por lo tanto no puede exceder de 5. Por lo tanto designando y_1, y_2, y_3, y_4, y_5 como las raíces de la ecuación (1), tendremos

$$y_1 = p + R^{\frac{1}{m}} + p_2R^{\frac{2}{m}} + \cdots + p_{m-1}R^{\frac{m-1}{m}} \quad (11.1)$$

$$y_2 = p + aR^{\frac{1}{m}} + a^2p_2R^{\frac{2}{m}} + \cdots + a^{m-1}p_{m-1}R^{\frac{m-1}{m}}, \quad (11.2)$$

$$y_m = p + a^{m-1}R^{\frac{1}{m}} + a^{m-2}p_2R^{\frac{2}{m}} + \cdots + ap_{m-1}R^{\frac{m-1}{m}} \quad (11.3)$$

De estas ecuaciones, deducimos fácilmente que:

$$p = \frac{1}{m}(y_1 + y_2 + \cdots + y_m), \quad (12.1)$$

$$R^{\frac{1}{m}} = \frac{1}{m}(y_1 + a^{m-1}y_2 + \cdots + ay_m), \quad (12.2)$$

$$p_2R^{\frac{2}{m}} = \frac{1}{m}(y_1 + a^{m-2}y_2 + a^2y_m), \quad (12.3)$$

……..

$$p_{m-1}R^{\frac{m-1}{m}} = \frac{1}{m}(y_1 + ay_2 + \cdots + a^{m-1}y_m) \quad (12.m)$$

Veamos de esto que $p, p_1, \dots, p_{m-1}, RyR^{\frac{1}{m}}$ son funciones racionales de las raíces de la ecuación (1).

Consideremos ahora uno de estos términos, por ejemplo R. Sea

$$R = S + v^{\frac{1}{n}} + S_2v^{\frac{2}{n}} + \cdots + S_{n-1}v^{\frac{n-1}{n}}, \quad (13)$$

Tratando este término del mismo modo que y, obtenemos un resultado similar, mostrando que los términos $v^{\frac{1}{n}}, v, S, S_2$, ...son funciones racionales de los diferentes valores de la función R, y como estos valores son funciones racionales de designando y_1, y_2, y_3, y_4, y_5 entonces también lo son lasfunciones $v^{\frac{1}{n}}, v, S, S_2, \dots$

Siguiendo este razonamiento, concluimos que todas las funciones irracionales contenidas en la expresión de y son funciones racionales de las raíces de la ecuación.

Establecido este resultado, no es difícil completar la demostración. Consideremos primero las funciones irracionales de la forma $R^{\frac{1}{m}}$, donde R es una función racional de a, b, c, d, e. Sea $R^{\frac{1}{m}} = r$, donde r es una función racional de las raíces y_1, y_2, y_3, y_4, y_5y R una función simetrica de estos términos. Ahora como el caso en cuestión es la solución general de la ecuación de quinto grado, está claro que uno puede considerar y_1, y_2, y_3, y_4, y_5como variables independientes; En consecuencia, podemos intercambiar los términos y_1, y_2, y_3, y_4, y_5entre ellos en la ecuación $R^{\frac{1}{m}} = r$, ya que por el intercambio, $R^{\frac{1}{m}}$ necesariamente toma valores m diferentes ya que R es una función simétrica.

La función r debe tomar también los m valores diferentes de la permutación de las cinco variables que contiene todas las formas posibles. Para mostrar esto, es necesario que $m = 5\ o\ m = 2$, ya que m es un número primo (ver la memoria del Sr. Cauchy en el *Journal del'Êêcole Polytechnique*, vol.17.)

Primeramente, sea $m = 5$. La función r por lo tanto tiene cinco valores diferentes y consecuentemente puede ser expresada de la forma

$$R^{\frac{1}{5}} = r = p + p_1 y_1 + p_2 y_1^2 + p_3 y_1^3 + p_4 y_1^4, \tag{14}$$

Siendo $p, p_1, p_2, \ldots$funciones simétricas de $y_1, y_2, \ldots$ intercambiando y_1 e y_2, la ecuación nos da,

$$p + p_1 y_1 + p_2 y_1^2 + p_3 y_1^3 + p_4 y_1^4 \tag{15}$$

Donde $$a^4 + a^3 + a^2 + a + 1 = 0 \tag{16}$$

Pero esta ecuación resulta imposible, por lo que consecuentemente m debe ser igual a dos.

Entonces sea $R^{\frac{1}{2}} = r$ (17)

Donde r debe tomar dos valores diferentes de distinto signo. Entonces tenemos (ver la memoria del Sr. Cauchy)

$$R^{\frac{1}{2}} = r = v(y_1 - y_2) * (y_1 - y_3) \ldots (y_2 - y_3) \ldots (y_4 - y_5) = vS^{\frac{1}{2}} \tag{18}$$

Siendo v una función simétrica. Consideremos ahora las funciones irracionales de la forma

$$(p + p_1 R^{\frac{1}{v}} + p_2 {R_1}^{\frac{1}{\mu}} + \cdots)^{\frac{1}{m}}, \tag{19}$$

Siendo $p, p_1, p_2, \ldots, R, R_1, \ldots$ funciones racionales de a, b, c, d, e y consecuentemente funciones simétricas de y_1, y_2, y_3, y_4, y_5, como hemos visto, debemos tomar $v = \mu = etc. = 2$, $R = v^2 S, R_1 = v_1^2 S, etc.$ La función procedente de (19) puede por lo tanto ser expresada de la forma

$$\left(p + p_1 S^{\frac{1}{2}}\right)^{\frac{1}{m}}, \tag{20}$$

Sean$r = \left(p + p_1 S^{\frac{1}{2}}\right)^{\frac{1}{m}}$, (21)

$$r_1 = \left(p - p_1 S^{\frac{1}{2}}\right)^{\frac{1}{m}}, \quad (22)$$

Multiplicándolas obtenemos

$$rr_1 = \left(p^2 + {p_1}^2 S^{\frac{1}{2}}\right)^{\frac{1}{m}}, \quad (23)$$

Ahora si (23) no es una función simétrica, m debe ser igual a 2, pero en este caso r tendría cuatro valores diferentes, lo cual es imposible; por lo tanto rr_1debe ser una función simétrica.

Sea v esta función simétrica ($v = rr_1$), entonces

$$r + r_1 = \left(p + p_1 S^{\frac{1}{2}}\right)^{\frac{1}{m}} + v\left(p + p_1 S^{\frac{1}{2}}\right)^{-\frac{1}{m}} = z\,, \quad (24)$$

Esta función tiene m diferentes calores, entonces m debe ser igual a 5, ya que m es un número primo. Por lo tanto, tenemos

$$z = q + q_1 y + q_2 y^2 + q_3 y^3 + q_4 y^4 = \left(p + p_1 S^{\frac{1}{2}}\right)^{\frac{1}{m}} + v\left(p + p_1 S^{\frac{1}{2}}\right)^{-\frac{1}{m}} \quad (25)$$

Siendo $q, q_1, q_2, \ldots$, funciones simétricas de $y_1, y_2, y_3, \ldots$y por lo tanto funciones racionales de a, b, c, d, e.

Combinando esta ecuación con la propuesta, podemos expresar y en términos de una función racional de z, a, b, c, d, e. Ahora tales funciones son siempre reducibles a la forma

$$y = P + R^{\frac{1}{5}} + P_2 R^{\frac{2}{5}} + P_3 R^{\frac{3}{5}} + P_4 R^{\frac{4}{5}}, \quad (26)$$

Donde P, R, P_2, P_3 y P_4 son funciones de la forma $p + p_1 S^{\frac{1}{2}}$, siendo p, p_1y S

Funciones racionales de a, b, c, d, e

De esta expresión para y obtenemos que

$$R^{\frac{1}{5}} = \frac{1}{5}(y_1 + a^4 1\, y_2, + a^3 y_3 + a^2 y_4 + a y_5 = (p + p_1 S^{\frac{1}{2}})^{\frac{1}{5}}, \quad (27)$$

Donde

$$a^4 + a^3 + a^2 + a + 1 = 0 \quad (28).$$

Ahora el lado izquierdo de la igualdad (27) tiene 120 valores diferentes y el lado derecho sólo 10; consecuentemente, y no puede tener la forma que hemos considerado, pero hemos demostrado que y debe ser necesariamente de esta forma la ecuación propuesta es resoluble. Por lo tanto concluimos que es imposible resolver por radicales la ecuación general de quinto grado.

> De este teorema se deduce inmediatamente que resulta también imposible resolver por radicales ecuaciones de grado superior a cinco (pp. 22-30).

La anterior demostración parece cerrar definitivamente el problema de buscar una fórmula para resolver ecuaciones polinómicas por radicales de grado cinco. Sin embargo, no fue así, ya que hay algunas ecuaciones de quinto grado o superior a estas, que si son resolubles por radicales. Un ejemplo de esto es la ecuación de la forma $X^n = a$ cuyas soluciones son las raíces *n-ésimas* de a, que se pueden expresar por los radicales de la forma$X = \sqrt[n]{a}$. Otros ejemplos son las ecuaciones abelianas y las ecuaciones de la forma $x^{p-1} + x^{p-2} + \cdots + x + 1 = 0$, con $p$primo. Estas últimas ecuaciones, llamadas ciclotómicas, fueron consideradas por Gauss en conexión con el problema de la construcción con regla y compás de polígonos regulares.

El avance esencial de Abel sobre Ruffini no estriba en el mayor alcance dado al teorema que cierra la vía de los algebristas italianos desde del Ferro a Lagrange, para la resolución algebraica general; sino en el análisis de ciertos tipos de problemas que expresan relaciones no simétricas entre las raíces y los coeficientes que para clases importantes conduce a la resolución. El problema entonces, era determinar el método para decidir cuales ecuaciones eran resolubles por radicales y cuáles no.

Lo antepuesto le permitió a Lagrange desarrollar un importante trabajo sobre polinomios simétricos, que junto con los trabajos de Ruffini[9] y de Abel permitieron a Galois obtener las bases para lo que luego se convertiría en la teoría que lleva su nombre. Con esta teoría se resolvió con éxito el problema de determinar cuándo las raíces de una ecuación polinómica pueden resolverse por radicales.

El objeto fundamental de las investigaciones de Evaristo Galois (1811-1832) fue el determinar cuando son resolubles mediante radicales las ecuaciones polinómicas. Inicialmente y mediante un proceso bastante engorroso, Galois pudo establecer que "Si en

[9] Paolo Ruffini es conocido por descubrir un método que permite hallar los coeficientes del polinomio que resulta de la división de un polinomio cualquiera por el binomio $x - a$. Hacia 1805 elaboró una demostración de la imposibilidad de la solución general de las ecuaciones algebraicas de grado quinto y superior, aunque cometió ciertas inexactitudes que serían corregidas por Abel.

una ecuación polinómica la potencia más alta es un número primo y si, supuesto conocidos dos valores de la x, los demás se pueden obtener a partir de estos usando únicamente la suma, la resta, la multiplicación y la división, entonces la ecuación puede ser resuelta mediante radicales."

En 1831 Galois comprobó que para todos los polinomios $f(x)$, una fórmula como la buscada existe. Así logró obtener una forma más general y menos difícil para identificar las ecuaciones de grado mayor o iguala cinco, resolubles por radicales. Para ello, Galois examinó ciertas permutaciones de la ecuación $f(x)$ y observó que ellas obedecían a un sistema algebraico que denominó Grupo. Luego observó que existe una fórmula para las raíces $f(x)$ si y solo si este Grupo (Grupo de Galois) satisface que:

> El producto de dos permutaciones es otra permutación. El orden al combinar dos permutaciones adyacentes es indiferente. Si llamamos a, b y c a tres permutaciones y $*$ a la operación, esta propiedad se puede representar como $(a * b) * c = a * (b * c)$. Existe una permutación, que notaremos por e, tal que dada cualquier permutación a, se verifica que $a * e = a$. Dada cualquier permutación a, existe otra, que notaremos por a^{-1} tal que $a * a^{-1} = e$.

Estas condiciones corresponden a los axiomas de Grupo. Éstos fueron definidos por Galois en su trabajo concerniente a la resolución de ecuaciones polinómicas. Es decir que, para conseguir un objetivo concreto fue necesario crear toda una estructura algebraica: la estructura axiomática de Grupo.

Rey Pastor (1957) afirma que Galois logró esquematizar la estructura de cada ecuación en un Grupo, donde se refleja la trama de relaciones entre las raíces, y cuya extensión mide en cierto modo la distancia que nos separa de la resolución. A continuación se presenta la definición de Grupo de Galois de una ecuación algebraica $f(x) = 0$ que aparece en la obra de Rey Pastor:

> Def. El Grupo de Galois de una ecuación algebraica $f(x) = 0$, en un Cuerpo Q al cual pertenecen los coeficientes a_i (o simplemente el Grupo G de la ecuación en Q), es el Grupo de sustituciones entre las raíces x_i admitidas por el sistema de ligaduras de ecuación, esto es, por el sistema de igualdades racionales con coeficientes de Q existentes entre las raíces. De otro modo: G es un Grupo de sustituciones que transforman igualdades ciertas en igualdades ciertas con coeficientes de Q. (p. 216)

Este autor dice que la teoría general de Galois puede ser desarrollada sin ejemplos, ni desarrollos de cálculo. Sin embargo, la resolución efectiva de tipos importantes de ecuaciones exige conocer su estructura, reflejada en el Grupo G de cada una. Muestra además varios Grupos en los que se forma el Grupo de Galois con facilidad, entre estos el siguiente:

> La ecuación ciclotómica ($p = 5$):
>
> $$x^4 + x^3 + x^2 + x + 1 = 0.$$
>
> Sus cuatro raíces están ligadas por las relaciones de Gauss:
>
> $x_1^2 = x_2,\ x_2^2 = x_3,\ x_3^2 = x_4,\ \ x_1^2 = x_1.$ [1]
>
> Si efectuamos entre los índices la sustitución circular (1234), cada una de esas relaciones [1] se transforman en la siguiente; admiten, pues, la sustitución (1234); también admiten, por tanto, su cuadrado y su cubo. En suma: las relaciones [1] admiten las sustituciones circulares:
>
> $$1, (1234), (13)(24), (1432),$$
>
> Que forman Grupo. (p. 218)

Seguidamente Rey pastor muestra la manera en que forman Grupo la ecuación ciclotómica de orden primo […], la ecuación binómica de grado primo p […], el Grupo de la ecuación recíproca […], y el Grupo de la ecuación bicuadrada […]. Otro de los aportes de Galois fue encontrado en la carta que envía a su amigo Chevalier poco antes de su muerte. La carta define, en términos modernos el teorema de normalidad (H es normal en G) de la siguiente manera:

> *… cuando un Grupo G contiene otro Grupo H, el Grupo G puede ser dividido entre Grupos cada uno de ellos obtenido operando una misma sustitución sobre las permutaciones de H, de tal forma que*
> *$G = H + HS + HS' + \cdots$y puede ser descompuesto entre Grupos teniendo la misma sustitución de tal forma que $G = H + T\,H + T'H + \cdots$*
>
> *En la mayoría de los casos estas descomposiciones no coinciden. Cuando ellas si coinciden, la descomposición se llama propia*. (Villa, 2011, pp.16-17)

Para llegar a la conclusión de Abel sobre la ecuación general de grado $n > 4$, bastó con demostrar la inexistencia de un subgrupo invariante en el Grupo alternado; sin embargo, para llegar al punto culminante de la teoría de Galois, es necesario dar respuesta a la

siguiente pregunta: ¿cuáles son las condiciones necesarias y suficientes del Grupo G de una ecuación, para que dicha ecuación sea resoluble por radicales?[10]

La teoría de Galois clásica, en términos modernos, demuestra que el Grupo (de Galois) de los automorfismos del Cuerpo de descomposición de $p(x)$ es resoluble si y sólo si las raíces de $p(x)$ se pueden obtener mediante radicales. En este caso, el procedimiento para obtenerlas raíces es el siguiente:

Se dice que un Grupo G es resoluble si y sólo si existe una cadena de subgrupos $\{1\} = G_0 \subset G_1 \subset \ldots \subset G_{s-1} \subset G_s = G$, de modo que G_{i-1} es normal en G_i y el orden de G_i/G_{i-1} es primo, para todo i. También, que las raíces de $p(x)$ se obtienen por radicales, si pueden expresarse mediante las cuatro operaciones fundamentales (suma, resta, producto y división) y la toma de radicales ($\sqrt[*]{\ }$), de números racionales. Esto prueba que las raíces de $p(x)$ pueden obtenerse por radicales si y sólo si el Grupo G, de la ecuación $p(x) = 0$ es resoluble; y si es conocida la cadena de subgrupos, se obtiene el procedimiento para calcular las raíces de $p(x)$.

En general, los polinomios de grado n tienen como Grupo, el Grupo de permutaciones S_n. Estos Grupos, sólo son resolubles para $n = 2, 3, 4$. De esto se deduce que las raíces de las ecuaciones de grado $2, 3$ y 4 pueden obtenerse por radicales.

Actualmente, el teorema de Galois se enuncia de la siguiente forma:

> Sea $f(x) \in K[x]$ un polinomio separable e irreductible de grado n, K un campo cualquiera y L el campo de descomposición de f sobre K. Sea $G = Gal\left(\frac{L}{K}\right)$. Entonces f es soluble por radicales si y sólo si G es un Grupo soluble. (Villa, 2011, p.15).

Según Kline (1972), Camile Jordán (1838-1922) fue el primero en añadir conceptos significativos a la teoría de Galois; en 1869 demostró que:

> Sea G_1 un subgrupo maximal autoconjugado (normal) de G_0, G_2 un subgrupo maximal autoconjugado de G_1, y así en adelante hasta que la serie termine en el elemento identidad. Esta serie de subgrupos es llamada una serie de composición de G_0. Si G_{i+1} es cualquier subgrupo autoconjugado de orden r en G_i cuyo orden es p, entonces G_i puede ser descompuesto $\lambda = p/r$ clases. Dos elementos están en

[10]Tales ecuaciones suelen llamarse metacíclicas; pero es más claro y sencillo llamarlas *resolubles*.

> la misma clase si uno es el producto real del otro y un elemento de G_{i+1}. Si a es cualquier elemento en una clase y b cualquier elemento en otra, el producto estará en la misma tercera clase. Estas clases forman un Grupo para el cual G_{i+1} es el elemento identidad y el Grupo es llamado Grupo cociente o Grupo factor de G_i por G_{i+1}. Se denota por G_i/G_{i+1}, notación introducida por Jordan en 1872. Los Grupos cociente $\frac{G_o}{G_1}, \frac{G_1}{G_2}$, ... (Kline, 1972, p. 1011).

Estos Grupos cociente son los llamados los Grupos factores de composición de G_0 y sus órdenes se conocen como los factores de composición o índices de composición. Puede haber más de una serie de composición en G_0. Jordan demostró que el conjunto de factores de composición es invariante excepto por el orden en que pueden aparecer.

Luego, Arthur Cayley (1821-1895), influenciado por el trabajo de Cauchy (1789-1857), reconoció que la noción de Grupo de sustituciones podía ser generalizada. Para presentar la noción de Grupo abstracto, Cayley supone un conjunto de operadores 1, $\alpha, \rho,$ ..., todos ellos diferentes y tales que el producto de cualquiera de ellos en cualquier orden, o el producto de cualquiera por sí mismo, pertenece al conjunto. Usó el símbolo de operador general θ aplicado a un sistema de elementos $x, y, z,$ ... de $x', y', z',$ ... Señaló que en particular el producto $\theta * \phi$, es un producto compuesto de dos operaciones y el compuesto es asociativo pero no necesariamente conmutativo. En 1849 y 1854, Cayley había propuesto la idea de Grupo abstracto; sin embargo, en esta época no se reconoció su importancia. Posteriormente, en 1878 Cayley escribió cuatro artículos sobre Grupos finitos abstractos, en estos, así como en los anteriores, Cayley subraya que un Grupo puede ser considerado como un concepto general y no necesita limitarse a los Grupos de sustituciones; aunque todo Grupo (finito) pueda ser representado como un Grupo de sustituciones.

Kline (1972) asevera que la teoría de sustituciones o Grupos de permutaciones fue la primera gran investigación que en última instancia promovió el surgimiento de la teoría abstracta de Grupos. En el siguiente párrafo se sintetizan las investigaciones de Kline (1972, pp.1009-1015), acerca de los teoremas se surgieron durante el siglo XIX, alrededor del concepto de Grupo.

El orden de un subgrupo divide el orden del Grupo [Lagrange][11].Un Grupo de permutaciones es transitivo si cada letra del Grupo es reemplazada por cada una de las letras bajo las varias permutaciones del Grupo y no existe un Grupo de orden K, para todo K en un Grupo de orden n [Ruffini (1799)]. Cauchy demuestra que no existe un Grupo de n letras (grado n) cuyo índice relativo a la totalidad del Grupo simétrico en n letras sea menor que el máximo número primo que no excede n, a menos que el índice sea 2 ó 1[12]. También probó que el número de valores diferentes de una función simétrica de n letras no puede ser menor que el máximo primo p menor que n, a menos que sea 2. Demuestra además la aserción de Galois de que todo Grupo finito (de sustituciones) cuyo orden es divisible por un primo p contiene al menos un subgrupo de orden p. Si existe una correspondencia uno a uno entre los elementos de dos Grupos tal que si $a.b = c$ en el primero, entonces para los elementos correspondientes en el segundo $a'.b' = c'$ (el isomorfismo entre dos Grupos), introduce el concepto de subgrupo normal: invariante o auto-conjugado. Un Grupo que carece de subgrupo invariante es simple, sino es compuesto (la noción de Grupo simple y compuesto) [Galois].

La obra de Galois no fue comprendida en la época en que surgió, y debió esperar hasta 1870 cuando Camille Jordán (1838-1921) aplicó la teoría de Grupos a las ecuaciones algebraicas. Grandjot (1940) asevera que el primer libro dedicado enteramente a Grupos fue el tratado de Jordán (1870*): traite des substituciones et des équetions algébriques* y este únicamente abarcó Grupos de permutaciones y sustituciones. Rey Pastor (1957) afirma que tras la codificación de la teoría de Galois en dicho tratado, realmente se da inicio a una nueva álgebra que junto con toda el álgebra de Weber en los tres tomos de Lehrbuch hace que el interés se desvíe de las ecuaciones para elaborar la teoría de Cuerpos y números irracionales; siguiendo la traza que Dedekind había marcado en 1871, hasta que Steinitz formuló 1910 una síntesis de los Cuerpos abstractos.

A mediados del siglo XIX, se escribieron libros de texto de álgebra como consecuencia de los abundantes resultados que fueron apareciendo después de las investigaciones obtenidas

[11] Kline (1972, p. 1009): Prieto Abbati (1768-1842), en una carta del 30de septiembre de 1802, en la que comunicó a Ruffini la demostración de este teorema.
[12] Ibidem. Serret (1866) muestra una versión mejorada que la de Cauchy: si una función de n letras toma menos de p valores, donde p es el mayor primo menor que n, entonces la función no admite más de dos valores.

por Lagrange. Español (1998) referencia los tratados de álgebra de Serret (1849) y Salmon (1859); los cuales, aunque presentan algunos temas en común, persiguen objetivos diferentes.

Español (1998) afirma que estas dos obras tuvieron una amplia difusión hasta los primeros años del siglo XX y aunque el primer libro fue más utilizado que el segundo, sus últimas ediciones no fueron actualizadas. Por tanto, se puede afirmar que se prolongó en el tiempo el uso de un texto que ya estaba desfasado. Dicho desfase consiste en gran parte en que no incorporó las novedades producidas en el tratado de Jordán (1870), donde los Grupos ocupan un papel central. Rescata, sin embargo, que en la tercera edición publicada en 1866 se encuentra por primera vez la teoría de Galois. El contenido de dichas obras es comentado por Español (1998) de la siguiente manera:

> La primera edición del *Cours* de Serret apareció tres años después de que Liouville publicará los escritos inéditos de Galois y en la tercera, de 1866, aparece por primera vez en libro de texto la teoría de Galois. El contenido de esta tercera edición es el siguiente: (i) La primera sección contiene fracciones continuas, funciones complejas necesarias para demostrar el teorema fundamental del álgebra, la teoría de la eliminación clásica (sin determinantes ni funciones simétricas), el estudio gaussiano de las raíces de la unidad y la resolución numérica de ecuaciones, incluyendo el teorema de Sturm de 1829 y su uso para calcular el número de raíces complejas contenidas en el interior de un entorno dado. (ii) En la segunda sección se introducen las funciones simétricas y los determinantes, que se aplican al obtener nuevos métodos de eliminación y al análisis de las soluciones reales de una ecuación, incluyendo una forma todavía poco elaborada de la ley de inercia de Sylvester, tema en el que se incorporan algunas contribuciones de Hermite. (iii) La sección tercera es un fragmento de aritmética, que abarca las congruencias y las acotaciones de Tchebichef del teorema del número primo. La cuarta se dedica a los Grupos de sustituciones, con un capítulo especial sobre las sustituciones dadas por funciones racionales lineales y su aplicación a cuestiones de la teoría de números. (iv) La última es la sección dedicada a la resolución algebraica de ecuaciones, que empieza por las ecuaciones de grados tres y cuatro, sigue con la demostración del teorema de Abel sobre la quintica, reproduciendo una demostración de Wantzel, y un estudio particular de las ecuaciones abelianas

> y de una ecuación de grado nueve asociada a los puntos de inflexión de una cúbica; el último capítulo lo forman cincuenta página dedicadas a las investigaciones de Galois, Hermite y Kronecker, añadidas en sucesivas ediciones, pero que no llegan a formar un Cuerpo de doctrina elaborado de la teoría de Galois. (pp. 66-67).

Hasta aquí lo fundamental es reconocer que la obra de Serret fue la primera en ofrecer posibilidades amplias de difusión de la teoría de Galois. A continuación el mismo autor se refiere a los contenidos de la obra de Salmon:

> La obra de G. Salmon (1819-1904) se dirige hacia la teoría de invariantes, aspecto del álgebra superior muy vinculado a la geometría. Comienza tratando también, pero con un estilo distinto al de Serret, sobre determinantes, funciones simétricas y eliminación, lo que ocupa la tercera parte de la obra. El resto se dedica a los invariantes y covariantes de las formas algebraicas asociados a las transformaciones lineales, completado con las formas canónicas y haciendo aplicaciones de los de los métodos simbólicos. Con este contenido, Salmon recoge resultados de Cayley, Sylvester, Aronhold, Clebsh y Hermite que expone con métodos largos y pesados cálculos, propio de los primeros estadios de esta disciplina. (pp. 66-67).

La importancia de estos textos presenta además un interés intrínseco, en tanto permiten una visualización de los cambios expuestos en lo que luego se convertiría en el texto, cuyo reconocimiento ha sido estándar en la producción intelectual alemana: *Lehrbuch der Álgebra* de H. Weber. El mismo Weber reconoce la importancia del texto de Serret, sin embargo, considera que es necesario introducir otros contenidos de vital importancia para los nuevos desarrollos del álgebra, a saber, los avances obtenidos especialmente por Dedekind para una mejor comprensión de la teoría de Galois. Klein en sus memorias del programa de Erlangen cita el libro de álgebra superior escrito por Serret y la definición de Grupos finitos derivada de los Grupos de permutaciones, dada por Dedekind en 1858.

Es importante reconocer en este punto, como lo explica Corry (2004), muchos de los escritos de Heinrich Weber (1842-1913) anteriores a Lehrbuch der Álgebra permitieron que se desarrollara el concepto de Grupo presente en la teoría de Galois, En 1893, durante su período de Gôttingen, Weber publicó un importante artículo titulado *"Die allgemeinen*

Grundlagen der Galois'schen Gleichungstheorie". Este artículo contiene una exposición de la teoría de Galois en los términos más generales conocidos hasta esa fecha, con lo cual realiza un aporte muy significativo e innovador a uno de los dominios activos de investigación más importante de la época: la teoría de polinomios.

Corry (2004) también nos dice que mediante el uso de los resultados obtenidos por Dedekind sobre la relación entre Grupos y Cuerpos, Weber vio la teoría no sólo como un análisis de su problema con la resolvente de sus raíces sino más bien como un examen más general de la interacción entre el Grupo específico y la definición de ciertos Cuerpos. Bajo este punto de vista, Corry (2004) asevera que:

> El estudio de resolvente era una aplicación particular de la teoría más general. En muchos aspectos, el artículo de Weber representa la primera presentación verdaderamente moderna publicada de la teoría de Galois. En particular, se introdujo todos los elementos necesarios para establecer el isomorfismo entre el Grupo de permutaciones de las raíces de la ecuación y el Grupo de Automorfismos del Cuerpo de descomposición que dejan los elementos del campo de base invariantes (p. 34).

Como es posible observar en todo lo referido anteriormente, el término Grupo empieza a conocerse explícitamente sólo hasta las obras de Galois, Cayley, Jordán y Dedekind. En la modernidad, la teoría de Galois, se ha convertido en una disciplina matemática compleja y ramificada, que incluye un amplio material sobre las relaciones entre las propiedades de las ecuaciones, los números algebraicos y los Grupos.

Para Zalamea (2009), la teoría de Galois es uno de los grandes puntales de desarrollo de las matemáticas, con notables transferencias conceptuales hacia los más variados dominios de la matemática. Por ejemplo, si se tiene un objeto X relacionado con un cierto campo L de tal forma que el Grupo de Galois $G = Gal\,(L/K)$ de una extensión L/K actúa en X, se dice que la acción de G en X es de Galois o galosiana. También si la acción de G en X da lugar a Grupos de cohomología, se habla de cohomología de Galois.

Sin embargo, en Villa (2011) se encuentra que el problema abierto en general se considera como el más difícil, es decir, el llamado problema inverso de la teoría de Galois. Este problema fue inicialmente establecido por Emmy Noether en los años treinta y consiste en dar respuesta a la siguiente pregunta: *Dado un Grupo finito G, ¿Existe un campo numérico*

K que sea una extensión de Galois sobre $\mathbb{Q}$ *y tal que* $G \cong Gal\left(\frac{K}{\mathbb{Q}}\right)$*?* Este problema se generaliza por ejemplo a campos de diversas funciones con diversos campos de constantes, a la exacta realización de un campo de un Grupo finito como el Grupo completo de automorfismos de un campo de funciones $Aut_k(K)$.

Zalamea (2009) por su parte afirma que la teoría de Galois permitió abordar problemáticas de gran complejidad, como posibilitar el establecimiento de redes de nociones asociadas a resoluciones algebraicas e invarianzas geométricas e hizo que las matemáticas modernas se vean obligadas a combinar múltiples perspectivas, herramientas y conocimientos. Como se verá más adelante después del surgimiento de los Grupos de transformaciones.

1.1.2 Grupos Abelianos Finitos

El concepto de *operación binaria*[13] o ley de composición interna aparece por vez primera en la obra *Disquisitiones Arithmeticae* del matemático alemán C. F. Gauss (1801), se sabe que este concepto es fundamental en la definición abstracta de Grupo. Tal definición es usada en la sección V de las *Disquisiciones* la cual trata sobre la composición de formas cuadráticas del tipo: $f(x,y) = ax^2 + bxy + cy^2$ con coeficientes enteros. Con estas formas buscaba conocer la manera como un número dado m puede ser representado por formas binarias $ax^2 + 2bxy + cy^2$ y terciarias $ax^2 + 2bxy + cy^2 + 2dxz + 2eyz + f$. Define también, la equivalencia de formas cuadráticas y una operación de multiplicación de formas, que posteriormente utiliza para demostrar que esta multiplicación es compatible con la relación de equivalencia.

Antes de Gauss, la aritmética modular fue estudiada por Euler en su obra de 1761. En ésta analizó los restos módulo n de potencias de un número y aunque no estableció los resultados de dicho estudio en términos de la teoría de Grupos, una lectura moderna de estos permite concluir que Euler fue el primero en dar un ejemplo de descomposición de un Grupo abeliano finito en clases adjuntas y probar que el orden de un subgrupo divide al orden del Grupo (teorema de Lagrange). Si bien fue necesario esperar que Galois, Cauchy y

[13]Una operación n-aria sobre A es una aplicación de A^n en A. Si n = 2 se tiene una operación binaria, si n = 3 una operación terciaria. $*$ es una operación en $A \leftrightarrow *$ es clausurativa y uniforme $\leftrightarrow *: A \times A \to A$ $(función)$.

otros matemáticos introdujera la noción "Grupo", el mérito de Gauss alrededor de este asunto reside en que describe los conjuntos de congruencia de enteros módulo m como clases de una relación de equivalencia, esto de alguna manera permite generalizar los métodos de aritmética modular que se aplican en la teoría de Grupos.

Kline (1972) afirma que "hasta el siglo XIX la teoría de números era una serie de resultados aislados, aunque muchas veces brillantes". Por su parte Kleiner (2007), considera que la obra de Gauss (1801) *Disquisitiones Arithmeticae* resume y unifica gran parte de la teoría de los números que le precedió. Kline (1972) además dice que en ese libro "Gauss estableció la notación, sistematizó y extendió la teoría existente; clasificó los problemas e introdujo los métodos conocidos y nuevos que debían ser estudiados".

A continuación se describe a grandes rasgos el contenido de las *Disquisiciones Aritmética*s de Gauss. Las tres primeras secciones están dedicadas a una recopilación introductoria de los principales resultados de la teoría de números de la época. En estas se expresan ideas de gran importancia, tales como: La noción de congruencia entre dos enteros racionales módulo p, resultados como la prueba de la unicidad de la factorización de enteros en primos y las definiciones de máximo común divisor y de mínimo común múltiplo; la investigación de los residuos de una potencia de un número dado módulo primo; esto es, partiendo del "pequeño" teorema de Fermat $a^{p-1} \equiv 1\ (mod. p)$, donde p es un número primo que no divide a.

Finalmente, en la sección IV y V de la obra se aborda la ley de reciprocidad cuadrática e investiga la teoría de las formas binarias cuadráticas. Aunque ese teorema había sido formulado por Euler, así como discutido por Legendre, Gauss es quien realiza una prueba completa y correcta del teorema.

Kleiner (2007) afirma también que *Disquisitiones* dio inicio a la teoría de Grupos abelianos finitos. La base para hacer tal afirmación es que Gauss estableció las propiedades importantes de estos Grupos (propiedades de suma y multiplicación de los enteros módulo p, con p primo), aun cuando para ello no haya utilizado la terminología de la teoría de Grupos actual. El investigador dice también que los Grupos aparecieron en la obra de Gauss en cuatro formas diferentes: el Grupo aditivo de los enteros módulo m, el Grupo

multiplicativo de enteros primos relativos a m, módulo m, el Grupo de clases de equivalencia de formas cuadráticas binarias, y el Grupo de $n - raíces$ de la unidad.

A continuación se presentan algunos teoremas de la obra de Gauss (1801) en la que aparece el uso de la estructura de Grupo abeliano:

> Dados m números enteros sucesivos $a, a-1, a+2, \ldots a+m-1$, y dado otro entero A, uno y sólo uno de estos enteros será congruente a A según el módulo m. (Gauss 1801, p. 8)

Es teorema corresponde en términos modernos al Grupo aditivo de los enteros módulo n (conjunto de las clases residuales módulo n), es decir, las clases de equivalencia de la relación de congruencia módulo n. Esta relación se expresa actualmente como $\mathbb{Z}/\mathbb{Z}_n$, de la siguiente manera: dos enteros a y b son congruentes módulo n si existe un entero q tal que $b - a \equiv qn$, lo cual se escribe $b \equiv a\ (mod\ n)$. donde, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

El siguiente teorema hace referencia al Grupo que en la actualidad corresponde al Grupo multiplicativo $U\ (p)$ de enteros relativamente primos al módulo p: todo elemento es de orden finito menor que p y subgrupo generado por un elemento $a \in U\ (p)$. En palabras de Gauss:

> Teorema. En toda progresión geométrica $1, a, a^2, a^3, etc.$, aparte del primer término, se da además otro término a^t, congruente a la unidad, según el módulo p, que es primo a a, cuyo exponente es $t < p$. (p.38).

En cuanto al Grupo de las n -Raíces de la unidad, en la actualidad se prueba que es un Grupo mediante el uso del teorema De Moivre. Gauss en este caso procede de la siguiente manera:

> Iniciaremos con el caso más sencillo, donde $A = 1$, es decir, donde se buscan las raíces de la congruencia $x^n \equiv 1\ (mód. p)$. Aquí, por lo tanto, tomando cualquier raíz primitiva como base, debe resultar $n\ Ind. x \equiv 0\ (mód. p-1)$ En este caso $\sqrt[n]{1}\ (mód\ p)$ tendrá un único valor, o sea $\equiv 1$. Sin embargo, cuando los números n y $p-1$ tengan máximo común divisor δ, la solución completa de la congruencia $n\ Ind. x \equiv 0\ (mód. p-1)$ será $Ind. x \equiv 0\left(mod. \frac{p-1}{\delta}\right)(ver\ art. 29)$: $i. e, Ind. x$, según el módulo $p-1$, deberá ser congruente a alguno de estos números.
>
> $$0, \frac{p-1}{\delta}, \frac{2(p-1)}{\delta}, \frac{3(p-1)}{\delta}, \ldots, \frac{(\delta-1)(p-1)}{\delta}$$

> o tendrá δ valores incongruentes según el módulo $p-1$, por lo tanto, también es este caso, x tendrá δ valores diferentes (incongruentes según el módulo p). De donde se percibe que la expresión $\sqrt[\delta]{1}$ también tiene δ valores diferentes, cuyos índices coinciden completamente con los anteriores. Por eso, la expresión $\sqrt[\delta]{1}\,(mód.p)$ equivale totalmente a $\sqrt[n]{1}\,(mód.p)$; i.e., la congruencia $x^{\delta} \equiv 1\,(mód.p)$ tiene las mismas raíces que ésta, $x^{n} \equiv 1\,(mód.p)$. La anterior, sin embargo, será de grado inferior, si δ y n no son iguales. (p. 50)

De igual manera Gauss presenta las siguientes clases de formas con la estructura de un Grupo abeliano:

> De las ecuaciones
>
> $$\beta' a + \beta'' a' + \beta'' (b + b') = \mu \qquad B = \frac{1}{\mu}(\beta a a' + \beta' a b' + \beta'' a' b + \beta''' (b b' + D))$$
>
> Deducimos
>
> $$B = b + \frac{a}{\mu}(\beta a' + \beta' (b' - b) - \beta''' c) = b' + \frac{a'}{\mu}(\beta a + \beta\beta'' (b - b') - \beta''' c')$$
>
> Por lo tanto
>
> $B \equiv b\ (mód.\frac{a}{\mu})$ y $B \equiv b'\ (mód.\frac{a'}{\mu})$
>
> Ahora, cuando $\frac{a}{\mu}$ y $\frac{a'}{\mu}$ son primos relativos, existirá entre 0 y $A-1$ (o entre 0 y $A-1$ cuando A es negativo) sólo un número que será $\equiv b\ (mód.\frac{a}{\mu}\ )$ y $\equiv b'\,(mód.\frac{a'}{\mu})$. Si dejamos que sea $= B$ y $\frac{B^2 - D}{A} = C$ es claro que (A, B, C) está compuesta de las formas (a, b, c) y $a', b', c')$. Entonces en este caso no es necesario considerar los números β, β', β'' y $\beta'')$ para encontrar la forma compuesta *). Pero la condición de que $\frac{a}{\mu}$ y $\frac{a'}{\mu}$ sean primos relativos es equivalente a pedir que los dos números a y a' no tengan divisor común mayor que los tres números $a, a', b + b'$ o lo que es lo mismo, que el máximo común divisor de a y a' también sea divisor del número $b + b'$. (p. 268)

A pesar de que estos ejemplos aparecieron en contextos de la teoría de números, Gauss los trató como *Grupos abelianos* en forma general y cada uno de estos por separado del otro. De cierta manera, los dotó de una estructura de Grupo sin el empleo una terminología que fue posterior a ese momento histórico. En este mismo sentido Kleiner (2007) afirma que los métodos utilizados en *Disquisiciones* carecían de una teoría unificadora de Grupo que se aplicara a todos los casos de forma general.

Aquí es necesario tener presente que Gauss dedicó una gran parte de las *Disquisitiones* a un exhaustivo estudio de las formas cuadráticas binarias y la representación de los números enteros por tales formas. Estudió el problema de encontrar las raíces de las ecuaciones

ciclotómicas, las cuales son de la forma $x_n - 1 = 0$ con n primo impar, en donde todas las soluciones son complejas excepto $x = 1$.

Una forma cuadrática binaria es una expresión de la forma $ax^2 + bxy + cy^2$ con a, b, c enteros (nótese que en estás además de las dos variables hacen referencia al grado dos). Gauss (1801) definió una composición en tales formas, y comentó que si K_1 y K_2 son dos de tales formas, uno puede denotar su composición por $K_1 + K_2$. Luego mostró que esta composición es asociativa y conmutativa, que existe una identidad, y que cada forma tiene una inversa, verificando de este modo todas las propiedades de un *Grupo abeliano.*

1.1.3 Grupos de Transformaciones

El matemático alemán Felix Klein (1849-1925)[14] publica en 1872 un programa de investigación con el título *Vergleichende Betrachtungen über neuere geometrische Forschungen*, conocido comúnmente como el **Programa de Erlangen**. Dicho programa constituye un proyecto de unificación en el dominio de las matemáticas que podía alcanzarse considerando cada rama de la geometría como la teoría de los invariantes de un Grupo de transformaciones particular. Para ello, Klein introduce en la Geometría un nuevo concepto de carácter algebraico: el Grupo de transformaciones. A continuación se presenta la definición de Grupo de transformaciones dada por Klein, que se encuentra en Bauza (S.F.)[15]:

> De las nociones necesarias para las consideraciones que van a seguir, la más esencial es la de *Grupo* de transformaciones del espacio. La composición de un número cualquiera de transformaciones del espacio[16] produce siempre otra transformación. Supongamos ahora que un conjunto dado de transformaciones tenga la propiedad de que toda transformación resultante de la composición de un

[14] *El trabajo de investigación* de Christian Felix Klein (1849-1925) profesor de la universidad de Erlangen, está asociado a tres cuestiones fundamentales: 1) la fundación de geometría moderna al unificar, con la noción de Grupo de transformaciones y de invariantes geométricos, las geometrías euclídeas y no euclídeas, a partir del llamado Programa de Erlangen ("Consideraciones comparativas sobre las investigaciones geométricas modernas") (1872); 2) la botella de Klein, 3) el llamado Grupo de Klein, que constituirá una condición fundamental de estructura de Grupo.

[15] El documento de Bauza no presenta fecha de traducción y pese a que su trabajo no corresponde propiamente a las matemáticas sino al gremio del sicoanálisis, traduce la obra de Klein para dar soporte a sus investigaciones donde los Grupos de transformación cobran una vital importancia.

[16] Las transformaciones están siempre aplicadas a la totalidad de los elementos del espacio. Las transformaciones, como, por ejemplo, las realizadas por dualidad, pueden introducir, en lugar de puntos, nuevos elementos. En el texto este caso no se distingue de los otros.

> número cualquiera de ellas que pertenezca también al conjunto[17], constituye lo que se llama un *Grupo de transformaciones*[18]. *(p.15)*

Las propiedades que se conservan en tales Grupos permiten definir la geometría correspondiente para el Grupo de transformaciones que la caracteriza. Klein observa que estas propiedades están en relación íntima con el tipo de algoritmo que hay que utilizar para la representación de las nociones, al respecto dice lo siguiente:

> Las expresiones analíticas que pueden presentarse en el estudio de una multiplicidad en el sentido de un Grupo deben ser, en razón de su significación, independientes del sistema de coordenadas, en tanto que este sigue siendo arbitrario; y se trata simplemente de poner también en evidencia esta independencia *en las fórmulas (*...) tiene una ley de formación general y perfecta de las expresiones invariantes y se restringe a no operar más que con estas. Es necesario que el algoritmo se adapte a lo que se desea, que se lo utilice como una expresión clara y precisa de la concepción, o que se lo quiera utilizar para penetrar fácilmente en campos todavía no explorados. (Bauza, S.F., p.36)

También expone algunos problemas que considera importante y fecundo tratar según los puntos de vista desarrollados en la investigación del programa de Erlangen:

> En la teoría de ecuaciones de Galois tal como se expone, por ejemplo, en el *Traité d'Algèbre supérieur* de *Serret*[19] o en el *Traité des substitutions* de *C. Jordan*[20], lo que constituye propiamente el objeto de las investigaciones, es la teoría misma de los Grupos o de las sustituciones; la teoría de las ecuaciones se deduce de ello como aplicación. Por analogía, quisiéramos una *teoría de las transformaciones*, una teoría de los Grupos que pueden engendrarse mediante transformaciones de una naturaleza dada. Las nociones de conmutatividad, de semejanza, etc., encontrarían empleo como en la teoría de las sustituciones. El tratamiento de una multiplicidad sacado de la consideración de un Grupo fundamental de transformaciones aparecería como una aplicación de la teoría de las transformaciones [...] En la teoría de las ecuaciones son primeramente las funciones simétricas de los coeficientes las que ofrecen un interés, pero a continuación son las expresiones que permanecen inalteradas, sino para todas las permutaciones de las raíces, al menos para un gran número de ellas. En el

[17][NT] Esta propiedad es lo que se conoce como *operación interna* y es sólo una de las condiciones para que en un conjunto sobre el que se aplica una operación que induce ciertas propiedades en él tenga lo que se conoce como una estructura de Grupo. Es necesario además que se cumpla la *propiedad asociativa, existencia de elemento neutro, existencia para cada elemento del conjunto de un elemento inverso.*

[18]Está implícitamente supuesto, en los Grupos del texto que, cualquier operación que figura en ellos se acompaña de la operación inversa; pero, en el caso en que haya una infinidad de operaciones, esto no es en absoluto una consecuencia de la noción misma de Grupo; es pues una hipótesis que se debe agregar explícitamente a la definición de Grupo, tal como viene dada en el texto.] La noción y la denominación están tomadas de la teoría de las *sustituciones* donde se trata, no de las *transformaciones* de un campo continuo, sino de las permutaciones de un número finito de magnitudes discretas.

[19]Cf. Joseph-Alfred SERRET, *Cours d'Algèbre supérieure,* 4ª ed., 1877-1879, reed. por Ed. Jacques Gabay.

[20]Cf. Camille JORDAN, *Traité des substitutions et des équations algébriques*, 1870, reed. por Ed. Jacques Gabay.

> tratamiento de una multiplicidad con un Grupo tomado como fundamental, quisiéramos en primer lugar, por analogía, determinar los Cuerpos, las figuras que permanecen inalteradas por todas las transformaciones del Grupo; pero hay figuras que no admiten todas las transformaciones del Grupo, sino solamente algunas de ellas, y estas figuras, en el sentido del tratamiento basado sobre el Grupo, son particularmente interesantes, gozan de propiedades notables. Así, por ejemplo, en el sentido de la Geometría ordinaria, se distinguen Cuerpos simétricos irregulares, superficies de revolución y helicoidales. (Bauza, S.F., pp.37-38)

Como es posible observar en las notas anteriores, Klein en el programa Erlangen realiza una importante clasificación de la geometría como el estudio de los invariantes bajo varios Grupos de transformaciones[21] y a partir de esto, surgieron diversos ejemplos de Grupos, como el proyectivo, el de movimientos rígidos, el de las similitudes, el hiperbólico, los de las elípticas, así como las geometrías asociadas con ellos (El Grupo afín no fue mencionado por Klein.) Según Kleiner (2007) el siglo XIX fue testigo gracias a Klein de un crecimiento explosivo en la geometría, nuevas geometrías surgieron: la proyectiva, las no euclidianas, la diferencial, la algebraica, la n-dimensional, y la de Grassmann.

La obra de Klein recoge el trabajo de muchos de matemáticos y físicos tanto de época en que vivió Klein como de otros que le antecedieron. Desde 1830 Évariste Galois (1811-1832) junto con Neils H. Abel (1802-1829) ya habían enunciado propiedades de Grupo tal como se hace en la teoría de Grupos moderna, sólo que referida a Grupos de permutaciones y Grupos abelianos. No obstante fueron los hallazgos que se comentan en el siguiente parrafo, según Bauza (S.F.), los que perfilaron el nacimiento de los Grupos de transformaciones.

En 1832 János Bolyai (1802-1860) en su obra *La ciencia absoluta del espacio* formula un sistema de geometría absoluta no euclidiana basado en la hipótesis de que pueden pasar infinitas paralelas por un punto exterior a una recta dada. Sin embargo, es de notar que desconoce desarrollos de ideas equivalentes (la llamada geometría hiperbólica) ya desarrolladas por Gauss (1777-1855) y posteriormente por Lobatchevski (1793-1856).

[21]Un Grupo de transformaciones puede definirse grosso modo como sigue: Dado un Grupo de sustituciones*, G_S , que actúa sobre un conjunto X, (G_S ,X), si en este definimos una estructura y los elementos de G_S que la conservan, se suele decir que G_T es el Grupo de transformaciones de dicha estructura. *Grupo de sustituciones, G_S consiste en la totalidad de sustituciones en un conjunto X, tales que forman Grupo respecto a una operación. Es decir dado un conjunto X y un Grupo G, tal que a todo $\gamma \in G$ le corresponde una sustitución $x \rightarrow \gamma$ (x) del conjunto X, que responde a la estructura de Grupo. El Grupo G se dice que ejerce una acción de representación sobre el conjunto X, efectivamente el Grupo de sustituciones permite la representancia mutua de los elementos del conjunto

Cinco años después Michel Chasles (1793-1880) en su *Ojeada histórica sobre el origen y el desarrollo de los métodos en geometría* expresa dos puntos de vista básicos de la geometría pura y general: la distinción entre propiedades métricas y propiedades descriptivas a las que se había referido Poncelet (1788-1867), así como el papel de las transformaciones. Chasles se interesa esencialmente en las transformaciones proyectivas pero no llega a elucidar la naturaleza exacta y las relaciones entre estos dos tipos de propiedades, de tal manera que sus puntos de vista al respecto permanecen bastante vagos.

En 1841 George Boole (1815-1864) desarrolla un trabajo sobre invariantes algebraicos, aunque su presentación era bastante limitada, atrajo la atención de Cayley quien empezó a publicar artículos matemáticos sobre el aspecto algebraico de la geometría proyectiva. El artículo de Boole, según Kline (1972), sugirió a Cayley el cálculo de los invariantes de las funciones homogéneas de grado n a las cuales llamó los invariantes derivados y después hiperdeterminantes.

Luego de tres años Grassmann (1809-1877) expone en su obra *Ausdehnungslehre (Teoría ampliada de las dimensiones)* las nociones básicas del cálculo vectorial extendidas a espacios de varias dimensiones. En 1847 Christian von Staudt (1798-1867) se había propuesto desarrollar como Poncelet y Chasles la geometría sin apelar a los métodos analíticos y logra efectivamente a diferencia de aquellos, introducir las nociones proyectivas sin hacer intervenir consideraciones métricas apuntando a una presentación de los fundamentos de la geometría más sistemática y rigurosa. Su *Geometrie der Lage (Geometría de posición)* (1847), otra forma de llamar a la geometría proyectiva, presenta esta geometría de manera axiomática y abstracta independientemente de toda noción métrica con la sola ayuda de axiomas referidos a la posición o al orden de los elementos fundamentales. Pero, no más que sus predecesores, Staudt no se preocupa de mostrar que esta geometría es independiente del axioma de las paralelas.

Por su parte, Riemann (1826-1866) en su conferencia *Acerca de las hipótesis que subyacen a la geometría*, publicada en 1854 amplía el trabajo de Gauss (1827) sobre las geometrías no euclídeas, relacionado esencialmente con geometrías donde el espacio es finito. Arthur Cayley (1821-1895) desarrolla la geometría $n - dimensional$ y de la teoría general de los

invariantes algebraicos[22] al que corresponde el mérito de la primera definición proyectiva explícita y completa de la distancia de dos puntos y por ahí de las propiedades métricas[23]. Sin embargo, Cayley todavía está lejos de las perspectivas mucho más generales en las que se desenvolvería Klein.

También de 1868 el trabajo de Helmholtz (1821-1894) *Ueber die Tatsache welche der Geometrie zu Grunde legen,* el *Tratado de las sustituciones* de Jordan (1838-1922) y los primeros trabajos sobre los *Grupos de transformaciones* de Lie (1842-1899) en 1870, aportan elementos a lo que Klein materializa en su obra en el programa de Erlangen.

Efectivamente, los trabajos de los matemáticos anteriores desarrollaron puntos muy importantes en el proceso de investigación realizado por Klein en el programa Erlangen, de los cuales se destacan principalmente los aportes de Cayley:

> Klein fue el primero que puso en evidencia la naturaleza proyectiva de las geometrías no euclidianas al aplicarles los puntos de vista de Cayley. Además estableció claramente que los tres tipos de geometrías de Euclides, de Bolyai-Lobatchevski y de Riemann eran casos particulares de la métrica general de Cayley. Planteando el problema general de la determinación de las geometrías proyectivas con curvatura constante, mostró que sólo podían existir tres tipos que corresponden precisamente a estas tres geometrías (cf. *Mathematische Annalen,* 1871, p. 623-625).

Después de todo lo anterior es importante resaltar que Klein fue el primero en mostrar que la geometría proyectiva es independiente de la teoría de las paralelas. Sus antecesores no habían dilucidado este punto y ni siquiera se habían planteado verdaderamente la cuestión. Klein amplía la naturaleza y el objeto de la Geometría. Realiza por así decirlo una Geometría generalizada que le permite incluir todas las geometrías en ella como casos particulares y restringidos de la misma, constituyendo uno de los factores mayores del advenimiento de la matemática moderna.

[22]Esta teoría proporciona un procedimiento sistemático (el *"método simbólico"*) que permite determinar todos los invariantes algebraicos de un sistema de objetos geométricos y todas las relaciones algebraicas que verifican.

[23]Efectivamente Cayley caracteriza con precisión el lugar de las propiedades "métricas" en Geometría proyectiva, mostrando que son las que dejan invariantes las transformaciones proyectivas particulares caracterizadas por la condición de dejar invariantes ciertos elementos fijos de una vez por todas, por ejemplo, los puntos cíclicos, en el plano proyectivo complejo.

Es importante resaltar que el espacio que aparece en la obra de Klein es ahora el objeto de la geometría. Se refiere al espacio en un sentido geométrico, un espacio que determinará las propiedades geométricas de los objetos contenidos en él; es decir, un espacio que aparece como condición de estructura. Las transformaciones que podamos operar sobre un elemento en el espacio dependerán de la estructura de ese espacio determinada geométricamente.

Por su parte, Sophus Lie en 1873 estudiando propiedades de las soluciones de sistemas de ecuaciones diferenciales fundó la teoría de Grupos de transformaciones continuas (ahora llamados Grupos de Lie). Introdujo la noción de invariantes al análisis y a la geometría diferencial (Galina, 2003, p. 1).

Galina (2003) afirma que una de las observaciones que hizo Lie, fue que los métodos clásicos de resolución de ecuaciones diferenciales "por cuadraturas" se basaban todos en el hecho que la ecuación es invariante por una familia "continua" de transformaciones, obteniendo que este conjunto de transformaciones continuas era un Grupo cerrado para la composición. El hecho importante en todo esto, es que a cada Grupo de transformaciones le podía asociar una familia de transformaciones infinitesimales" que contenía la información que ahora viene asociada al álgebra de Lie.

1.2 Emergencia y Evolución del Concepto de Cuerpo

La evolución de la teoría de Cuerpos estuvo estrechamente relacionada con la preocupación de algunos matemáticos del siglo XVIII y XIX por el rigor, la generalización y la abstracción. Kleiner (2007) afirma que su génesis fue posible a partir la teoría algebraica de números, la teoría de *Galois* y la geometría algebraica.

Con respecto a la teoría algebraica de números el asunto se relaciona con el teorema de "reciprocidad cuadrática". Este teorema fue inicialmente propuesto por Leonard Euler como una conjetura en 1742, en una carta enviada a Golbach y en el *Opuscula Analytica* de 1783. Legendre intentó demostrarlo en 1875, sin embargo, utilizó argumentos no probados que desvirtuaron su intención.

En 1801, Gauss trata en la sección IV de *Disquisitiones Arithmeticae* el asunto de los residuos cuadráticos y demuestra el teorema en general para números enteros; y en 1825 introdujo una clase de números complejos conocidos hoy en día como "enteros complejos gaussianos[24]" (es decir, de la forma $a + bi$, *con* $a,\ b$ enteros racionales).

El problema continúo en 1828 cuando Gauss probó dicha ley para los enteros complejos. Aunque las propiedades subyacentes a los números complejos ya habían sido introducidas por Fermat, Euler y Lagrange. Gauss demostró, en particular, que la descomposición única en factores primos se cumplía para cada entero de la siguiente manera:

> Si p es un número primo y b un no residuo cuadrático dado de p, el valor de la expresión
>
> $$(A)\ \ldots \frac{(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}}{\sqrt{b}}$$
>
> (Se observa con facilidad que el desarrollo de ésta carece de irracionales) siempre será divisible por p, cualquiera que sea el número que se tome para x. De hecho, es claro de la inspección de los coeficientes que se obtienen del desarrollo de A, que todos los términos desde el segundo al penúltimo (inclusive) son divisibles por p y que $A \equiv 2(p+1)\left(x^p + xb^{\frac{p-1}{2}}\right)(mód.p)$. Pero ya que b es un no residuo de p, será $b^{\frac{p-1}{2}} \equiv -1\ (mód.p)(art.106)$; pero x^p siempre es $\equiv x(sección\ anterior)$, de donde $A \equiv 0.\ \ Q.E.D.$
>
> En la congruencia $A \equiv 0\ (mód.p)$ la indeterminada x tiene exponente p y todos los números $0, 1, 2, \ldots, p-1$ serán raíces de ella. Ahora, tómese a e como un divisor de $p+1$. La expresión
>
> $$\frac{(x+\sqrt{b})^e - (x-\sqrt{b})^e}{\sqrt{b}}$$
>
> (la cual denotamos por B), si se desarrolla, no tendrá irracionales, la indeterminada x tendrá exponente $e-1$, y resulta de los primeros elementos del análisis que A es divisible (algebraicamente) por B. Ahora digo que existen $e-1$ valores de x, que sustituidos en B, hacen B divisible por p. En efecto, si $A \equiv BC$, x tendrá exponente $p-e-1$ en C, y la congruencia $C \equiv 0\ (mód\ p)$ tendrá no más que $p-e+1$ raíces.
>
> De donde resulta evidente que todos los $e-1$ números restantes entre $0, 1, 2, 3, \ldots, p-1$, serán raíces de la congruencia $B \equiv 0$.

[24]Los puntos expuestos sobre la obra de Gauss, son de gran trascendencia en el álgebra abstracta, ya que junto con la demostración del Teorema fundamental de la Aritmética publicada en 1801 por Gauss en los Disquisiciones Arithmeticae, todos los desarrollos de Gauss convergieron en el surgimiento de una serie de teoremas y lemas: los enteros son un dominio Gaussiano, y por lo tanto todo entero irreducible es primo. Los enteros Gaussianos forman un dominio de ideales principales y cualquier dominio de ideales principales forma un dominio de factorización única. Todo Cuerpo es un dominio de ideales principales. Todo dominio de ideales principales, tiene unidad. Todo dominio de ideales principales es gaussiano.

> Ahora supóngase que p es de la forma $5n+4, e=5, b$ es un no residuo de p, y el número a se determina tal que
>
> $$\frac{(a+\sqrt{b})^5-(a-\sqrt{b})^5}{\sqrt{b}}$$
>
> es divisible por p. Pero esa expresión es $= 10a^4+20a^2b+2b^2 = 2(b+5a^2)^2-20a^4)$
> Por lo tanto, también $(b+5a^2)^2-20a^4)$ será divisible por p, de igual forma, $20a^4$ es un residuo de p; pero ya que $4a^4$ es un residuo no divisible por p (de hecho, se comprueba fácilmente que a puede dividirse por p), también 5 será un residuo de p. *Q. E. D. (*p. 92)

Dicho tratamiento de los enteros complejos abrió el camino para el desarrollo de los números algebraicos, además de ser el punto de partida de los desarrollos de otros matemáticos. Por ejemplo, Kummer [25](1810-1893), discípulo de Gauss y de Dirichlet, intentó en 1840 generalizar la ley de reciprocidad cuadrática de Gauss con la finalidad de demostrar el último teorema de Fermat. Kummer, sigue una sugerencia de Gauss en su célebre memoria sobre los residuos bicuadráticos de 1831, en la que detallaba la divisibilidad en el conjunto Z_i. En ésta, Gauss expone la importancia que tendría para los problemas clásicos de la teoría de los números la extensión de la noción de divisibilidad más allá de los enteros, colocando como ejemplo la resolución de ecuaciones diofánticas. Para lo cual debía extender la aritmética de los enteros a los complejos. Kummer mediante esta tarea logró la introducción de una nueva clase de números complejos.

Por su parte, Dirichlet se dio cuenta que en los resultados que consigue Kummer, no todas las propiedades aritméticas de los números enteros se verifican en general en los números complejos. Esto llevó a Kummer a replantear sus escritos y a la búsqueda de una forma de factorización única. Para ello introduce los *números ideales y los números algebraicos.* De esa forma logra comprobar para algunos casos particulares la conjetura de Fermat[26]

Kleiner (2007) asevera que "El principal resultado de Kummer fue que cada elemento en el dominio de los números enteros ciclotómicos es un producto único de ideales primos" (p. 51). Aunque los conceptos fundamentales de número *ideal y de ideal primario* no fueron

[25]Los dominios de enteros ciclotómicos, fueron centrales en el estudio del Último Teorema de Fermat. También demostraron ser importante en la investigación de leyes de reciprocidad. Ambos problemas fueron de gran interés para Kummer y esenciales para establecer la factorización única.

[26] Kummer (1857) demuestra el teorema de Fermat para una serie de números primos, todos los menores que 100 salvo el 37, 59 y el 67.

definidos por Kummer en forma general, marcaron puntos de partida muy importantes para Dedekind (1831- 1916), otro de los discípulos de Gauss.

El reto de Dedekind fue entonces, encontrar una teoría de descomposición que se aplicaría a dominios más generales que enteros algebraicos. El estudio de la factorización única se volvió para Dedekind el mecanismo teórico para la definición de nuevos números y entidades. Dedekind en 1871, en lugar de trabajar con las raíces de la unidad, formuló una definición más amplia de los números algebraicos[27] e introdujo el concepto de Cuerpo numérico.

Con el establecimiento de un *Cuerpo numérico* mostró que los números algebraicos forman un *Cuerpo*; introdujo entonces la noción de anillo[28], y probó que los enteros algebraicos formaban precisamente un anillo. Con las nuevas definiciones de números ya podía Dedekind buscar una solución al problema de la factorización única, pero ahora en el Cuerpo de los números algebraicos, con un esquema bastante diferente al de Kummer. Dedekind necesita introducir la idea de Cuerpo en el campo de números algebraicos $Q(a) = \{q_0 + q_1 a + q_2 a^2 + \cdots + q_N a^N : q_i \in Q\}$, donde a es una raíz de un polinomio con coeficientes enteros; en los cuales los elementos de $Q\ (a)$, son las raíces de los polinomios monicos con coeficientes enteros. Kleiner (2007) manifiesta que Dedekind mostró que

[27]Sea r una raíz de la ecuación$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$ con los a_i enteros racionales negativos o positivos, y tal que $r$no es raíz de ninguna ecuación del mismo tipo y de grado menor a_n, se llama a $r$un número algebraico de grado n. Si el coeficiente a_n es $1, r$ se llama un entero algebraico de grado n.

[28] La teoría de anillos se divide en dos grandes categorías: la teoría de anillos conmutativos y la teoría de anillos no-conmutativos, su génesis se remonta a principios del siglo XIX, mediante el surgimiento de diversos ejemplos, tales como los anillos de enteros, los de polinomios, las matrices y los cuaterniones. Kleiner (2007) afirma que mientras la teoría de anillos conmutativos se originó dentro de la teoría algebraica de números, la geometría algebraica y la teoría de invariantes. El punto de partida para el desarrollo de estos temas fueron los anillos de enteros en Cuerpos de números algebraicos y Cuerpos de funciones algebraicas, y los anillos de polinomios en dos o más variables. La teoría de anillos no conmutativos surgió con los intentos de extender los números complejos a diversos sistemas numéricos hipercomplejos. Kleiner (2007, p. 28) indica que esta teoría se originó a partir de un solo ejemplo, los *cuaterniones*, descubiertos por Hamilton en 1843. Estos son "números " de la forma $a + bi + cj + dk\ (a, b, c, d$ números reales) que se suman componente a componente y en el que la multiplicación está sujeto a las relaciones $i\,2 = j2 = k2 = ijk = -1$. Este fue el primer ejemplo de un sistema de numeración no conmutativa, que obedece todas las leyes algebraicas de los números reales y complejos, excepto para conmutatividad de la multiplicación. Este sistema se llama ahora un *Cuerpo de inclinación o un anillo de división*. La motivación de Hamilton en la introducción de los cuaterniones era extender el álgebra de vectores en el plano de un álgebra de vectores en el espacio de tres dimensiones.

forman un anillo conmutativo con la identidad cuyo Cuerpo de cocientes es $Q\,(a)$. Sin embargo, para esto le faltaba un nuevo concepto que era precisamente el de *ideal*, en el sentido moderno.

Como se había mencionado antes los ideales introducidos por Kummer sólo eran casos particulares. Dedekind introduce las clases de números algebraicos y con esto logra una generalización de los enteros ordinarios a los que llama *ideales* y los define de la siguiente manera:

> Sea *K* un Cuerpo de números algebraicos específico. Un conjunto de enteros A de K se dice que forma un ideal si cuando α y β son dos enteros cualesquiera en el conjunto, los enteros $\mu\alpha + v\beta$, donde μ y v son otros dos enteros cualesquiera en *K*, también pertenecen al conjunto. Alternativamente $\alpha_{1,}a_2, \dots, a_v$ *de* K si a consiste en todas las sumas $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n$, donde los λ_i son enteros cualesquiera de un Cuerpo K. Este ideal es denotado mediante $(\alpha_{1,}a_2, \dots, a_v)$. El ideal cero consiste en el número 0 únicamente y por consiguiente es denotado por (0). El ideal unidad es generado por el número 1, esto es, (1). Un ideal A es llamado principal si es generado por un entero únicoα, de tal forma que (α) consta de todos los enteros algebraicos divisibles porα. En el anillo de los enteros algebraicos todo ideal es un ideal principal. (Kline, 2004, pp.1088-1089)

Para establecer los dominios con la factorización única[29], Dedekind considera primero el producto de dos ideales. El producto del ideal $A = (\alpha_{1,}a_2, \dots, a_s)$ y el ideal $B = (\beta_{1,}\beta_2, \dots, \beta_t)$ de K está definido como el ideal $AB = (\boldsymbol{\alpha_1}\,\beta_1, a_2\beta_2, \dots, a_s\beta_t)$. Este producto es conmutativo y asociativo. A divide a B si existe un ideal C tal que $B = AC$. Se escribe A/B y A es llamado un factor de B, los elementos de B están incluidos en los elementos de A. El ideal P se define como aquel que solo tiene como factores el mismo (p) y el ideal (1), de tal forma que p no está contenido en ningún otro ideal de K. El ideal primo es también llamado maximal. Encuentra también, que cualquier ideal es divisible únicamente por un número finito de ideales y si un ideal primo divide el producto AB de dos ideales (de la misma clase de números) divide a A ó a B. Concluyendo que la factorización de los enteros de un Cuerpos K de números algebraicos en primos es única si y solo si todos los ideales de K son principales.

[29] Para hacer frente a los problemas centrales de la teoría de números en aquel entonces, es decir, a el último teorema de Fermat, las leyes de reciprocidad, y las formas cuadráticas binarias, se encontró importante formular problemas en dominios de enteros algebraicos, lo cual dio origen a un nuevo problema: el estudio de la factorización única en este tipo de dominios.

Todas estas definiciones y teoremas condujeron a los teoremas básicos para ideales de un Cuerpo de números algebraicos K; con esto puso su teoría en un contexto más amplio, dando definiciones axiomáticas de los anillos, los Cuerpos y los ideales.

La definición de un *Cuerpo* dada por Dedekind es la siguiente:

> "Por un *Cuerpo* tendremos que entender todo sistema infinito de números reales o complejos de modo cerrado en sí mismo y al realizar una operación de suma, resta, multiplicación y división de dos de estos sistemas de números de nuevo se obtiene un número real o complejo". (Kleiner, 2007, p. 55)

Para Dedekind entonces, las propiedades de los Cuerpos se representaban muy bien en los conjuntos de los números complejos o reales, lo cual es por supuesto, todo lo que necesitaba para su teoría de números algebraicos. Sin embargo, Kleiner (2007) dice:

> Una definición axiomática de la teoría de números algebraicos incluso en este sentido restringido es notable para la época. También son notables el uso que Dedekind le da a los conjuntos infinitos ("sistemas"), que es anterior a Cantor, y su definición "descriptiva" en lugar de "constructiva" de un objeto matemático como un conjunto de todos los elementos de un cierto tipo que satisface una serie de propiedades. (p. 66)

La definición de *Cuerpo* expuesta por Dedekind fue la base de desarrollos posteriores. Klein mediante ésta, por ejemplo, define la idea de un conjunto engendrado por un Grupo generador como *Cuerpo*. Él manifiesta en las notas de pie de página que "el nombre de Cuerpo es elegido por Dedekind para identificar un conjunto de números que resulta por medio de operaciones y elementos dados (última edición de las *Lecciones* de Dedekind)" (p. 25); tal como se muestra a continuación:

> Dado para el espacio un Grupo cualquiera por ejemplo el Grupo principal. Elijamos una figura particular como un punto o una recta, o aún un elipsoide, etc., y efectuemos sobre ella todas las transformaciones del Grupo fundamental. Obtenemos así un conjunto varias veces infinito en un número de dimensiones en general igual al número de los parámetros arbitrarios contenidos en el Grupo. En ciertos casos particulares este número es más pequeño, a saber, cuando la figura escogida en primer lugar tiene la propiedad de ser reproducida por un número infinito de transformaciones del Grupo. Cada conjunto así engendrado se llama, relativamente al Grupo generador, un Cuerpo. Si ahora, por una parte, queremos estudiar el espacio en el sentido del Grupo, y, con esta finalidad, especificar como elemento del espacio algunas figuras determinadas; si, por otra parte, no queremos que algunas cosas equivalentes sean representadas de desigual manera, deberemos evidentemente escoger los elementos del espacio de tal manera que su conjunto

> forme un solo Cuerpo o pueda descomponerse en Cuerpos[30], haremos más tarde (Cap. IX) una aplicación de esta observación evidente. La noción misma de Cuerpo se representará una vez más, en el último parágrafo, asociada a nociones de la misma naturaleza. (Klein, 1872, p. 25)

Otro de los caminos en los que Dedekind dejó su importante huella con la definición de la noción de Cuerpo fue la teoría de Galois. En 1799 una prueba de Ruffini sobre la irresolubilidad de las ecuaciones polinómicas de quinto grado, presentaba una distancia importante frente a los trabajos de Dedekind, porque carecía de elementos suficientes para el desarrollo de las ideas teóricas de *Cuerpo*. No obstante, esas ideas fueron puntos de partida para la reformulación en términos más generales de teoría la Galois y así establecer las condiciones de resolución de las ecuaciones polinómicas por radicales. Esto y lo ya expuesto anteriormente sobre teoría de números, configuran un punto de intersección en la emergencia de las teorías de anillos, Grupos y Cuerpos.

El aparato algebraico introducido por Galois para establecer cuándo una ecuación polinómica es resoluble por radicales tuvo un impacto mayor que el perseguido por mismo Galois. Ferreirós (1998) resalta que Dedekind en su obra de 1872 se dio cuenta de la necesidad de la noción de Cuerpo para la teoría de Galois; ya que esto le permitía obtener avances en la teoría de números algebraicos y realizar una presentación general del teorema de factorización única. De esa manera Dedekind logró concebir y definir el anillo de enteros de un Cuerpo de números algebraicos y demostrar que la manera en que Kummer, Dirichlet, Einstein, entre otros definían el concepto de anillo era errónea y esto hacía imposible una teoría general de factorización.

La idea del estudio de la estructura de los Cuerpos algebraicos y la comparación con ellos de la estructura de los Grupos de un número finito de sustituciones que presentó Dedekind fue la base fructífera del Álgebra Moderna.

[30][En el texto no está suficientemente subrayado que el Grupo propuesto puede contener lo que se llaman subGrupos *excepcionales*. Si una figura geométrica permanece inalterada por las operaciones de un subGrupo excepcional, sucede lo mismo con todas aquellas que se deducen de ella por las operaciones del Grupo total, por consiguiente, de todos los elementos del Cuerpo que resulta de ella. Ahora un Cuerpo así formado es totalmente impropio para la representación de las operaciones del Grupo. Sólo se deben tener en cuenta, pues, en el texto, Cuerpos que resulten de elementos del espacio que no se conservan inalterados por ningún subGrupo excepcional del Grupo propuesto.]

A continuación se señala la emergencia de definiciones de Cuerpo más generales que las de Dedekind y aparición en diferentes contextos de ciertos Cuerpos particulares. Kronecker (1881), llama a los conjuntos cerrados respecto a las cuatro operaciones aritméticas dominios de racionalidad, sobre estos introduce la noción de indeterminada adjunta a un Cuerpo siendo la indeterminada una nueva cantidad abstracta. Para Kline (2004) el concepto de Cuerpo de Kronecker era mucho más general que el de Dedekind, ya que consideró campos de funciones racionales en cualquier número de variables (indeterminadas). En particular, observó que si x es trascendente sobre un Cuerpo K entonces el campo $k(x)$ obtenido al añadir la indeterminada x a k, es isomorfo al Cuerpo Kx de funciones racionales de una variable con coeficientes en K.

Kurt Hensel (1861-1941) en su artículo de 1908 *Theorie der Álgebraichen Zahlen* define un nuevo ejemplo de Cuerpo, los Cuerpos $p-$á$dicos$. para ello introduce los números $p-$á$dicos$, En principio los números $p-$á$dicos\,(p\ primo)$ son una notación conveniente para hablar simultáneamente de las soluciones de una ecuación módulo p, p^2, p^3 ,... Hensel en su trabajo de 1910 *Álgebraische Theorie der Körper* estudia de manera axiomática las propiedades de los Cuerpos y define importantes conceptos como el de Cuerpo primo, Cuerpo perfecto, Cuerpo perfecto y de grado de trascendencia de una extensión. Además de la formulación y demostración de que todo Cuerpo conmutativo tiene una extensión algebraicamente cerrada.

Siguiendo la misma dirección de Dedekind, Weber en 1893 publicó el artículo titulado *"Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie"*.[31]Corry (2004) afirma que dicho artículo contiene una exposición de la teoría de Galois en los términos generales e introdujo todos los elementos necesarios para establecer el isomorfismo entre el Grupo de permutaciones de las raíces de la ecuación y el Grupo de automorfismos del Cuerpo de descomposición que dejan los elementos del campo de base invariantes.

El artículo de Weber (1893) presenta la teoría de Galois desde el punto de vista más general que era posible para la época. Según Corry (2004) Weber no la exhibe como una teoría que se ocupa de ecuaciones sino más bien como una teoría que se ocupa de Grupos y Cuerpos.

[31] Weber (1893) *"Fundamentación general de la teoría de las ecuaciones de Galois"*.

En su artículo Weber define y examina las propiedades básicas de Grupo de una manera abstracta, considera Grupos finitos e infinitos como sujetos de una sola teoría, así como las propiedades de los Grupos de permutación en conjunto. Dicho artículo se inicia con la siguiente declaración:

> La teoría se presenta aquí como una consecuencia inmediata del concepto de Cuerpo, que no es sino una extensión del concepto de Grupo, visto como una ley formal, independiente del significado numérico de los elementos relacionados (…) Así, la teoría aparece como un formalismo absoluto, el cual cobra vida y contenido, sólo al otorgársele a los elementos valores numéricos. (Corry, 2004, p. 35)

Corry aclara que en la obra de Weber se define por primera vez la noción de Cuerpo como una extensión del concepto de Grupo (es decir, mediante la adición de una segunda operación). Al acercarse al concepto de esta manera se puede percibir en toda su generalidad, lo que permite un tratamiento análogo de Cuerpos finitos e infinitos. Los Grupos, Cuerpos finitos e infinitos fueron subsumidos aquí por primera vez bajo una definición única y general.

Kline (2004) dice que la teoría de Cuerpos la inició Heinrich Weber, cuando definió Cuerpo como "una colección de elementos sometida a dos operaciones llamadas suma y multiplicación que satisfacen la condición de clausura, las propiedades asociativa y conmutativa, y la distributiva; además, cada elemento debe tener un inverso único para cada operación, excepto la división por cero" No obstante, dice que es importante resaltar que Weber en el artículo de 1893 (o en otro lugar) no consideró el problema de la *característica del Cuerpo*[32].

Dicho problema fue considerado por Ernst Steinitz (1871-1928) al emprender un estudio sistemático de los Cuerpos abstractos en su publicación de 1910 *Álgebraischen Theorie der Kôrper*. Según él, todos los Cuerpos pueden dividirse en dos tipos principales, los de característica cero y los de característica p. Al demostrar esto obtiene su teorema fundamental "todo Cuerpo se puede obtener a partir de su Cuerpo primo haciendo primero una serie de adjunciones trascendentes (posiblemente infinitas), y a continuación una serie

[32] Definición: Diremos que un Cuerpo K (o un anillo) tiene característica n si n es el menor número natural tal que *1+1+ n veces...+1 = 0.* Si esta suma fuera siempre distinta de cero se dice que el Cuerpo tiene característica cero. La notación habitual es *char(K) = n*.

de adjunciones algebraicas al Cuerpo trascendente". Estudió además el problema de determinar en que Cuerpos se verifica la teoría de Galois. El resultado de Steinitz dice esencialmente que la teoría de Galois se verifica en los Cuerpos de rango finito que pueden obtenerse de un Cuerpo; dada por una serie de adjunciones de raíces de polinomios irreducibles $f(x)$ que no tengan raíces iguales, a estos los llamó completos (volkommen).

A continuación se muestra la demostración de Steinitz, encontrada en Kline (1972):

> Sea K un Cuerpo y consideremos todos los subcuerpos de K. Los elementos comunes a todos estos constituyen el subcuerpo primo P de K.
>
> Hay dos tipos posibles de Cuerpos primos; el elemento identidad e está contenido en P y, por tanto, lo están
>
> $$e, 2e, \dots, ne, \dots$$
>
> Estos elementos, o bien son todos distintos o existe un entero p tal que $pe = 0$. En primer caso P tiene que contener todas las fracciones ne/me y, dado que estos elementos forman un Cuerpo$P$ ha de ser isomorfo al Cuerpo de los números racionales, y se dice que K tiene característica 0. Si en cambio se tiene que $pe = 0$, es fácil demostrar que el más pequeño p que cumple esta condición tiene que ser primo, y el Cuerpo es isomorfo al de los restos de los enteros $módulo\ p$, es decir $0,1,2,\dots,p-1$. Entonces se dice que K es un Cuerpo de característica p y cualquier subcuerpo suyo tiene la misma característica. En este caso $pa = pe = 0$, es decir, todas las expresiones en K pueden reducirse $módulo\ p$.
>
> A partir del Cuerpo primo P, en cualquiera de los dos casos anteriores, se puede obtener el Cuerpo original K por un proceso de adjunción de elementos. (p.p. 1514-1515)

Sin embargo, Kline (1972) objeta este resultado diciendo:

> No todo Cuerpo se puede extender por adjunciones algebraicas, por ejemplo, en el caso de los complejos es imposible porque todo polinomio $f(x)$ es reducible sobre este Cuerpo; un Cuerpo con esta propiedad se llama algebraicamente cerrado. Steinitz demostró al respecto que para todo Cuerpo K existe un único Cuerpo algebraicamente cerrado K' que es algebraico sobre K en el sentido de que cualquier otro Cuerpo algebraicamente cerrado K (que contenga a K) contiene un subcuerpo isomorfo a K'. (p.1516)

El trabajo de Steinitz pone de manifiesto que tras la extensión de los enteros a los racionales, subyace una construcción algebraica que permite imbuir cualquier dominio de integridad en un Cuerpo, mediante la construcción de fracciones (Corrales, 2011).

Según Rey Pastor (1957) mientras que Galois perseguía la resolvente, Weber se fijo más en el Cuerpo; y en esa dirección elaboró Steinitz su teoría general de Cuerpos algebraicos, despreocupándose de su aplicación a problemas; que por derecho propio de Galois, tenían su nombre. Después de la famosa monografía de Steinitz (1910) sobre los Cuerpos algebraicos, el gran impulso para la consolidación del concepto de Cuerpo fue dada por Artin en Hamburgo y Emmy Noether en Gôttingen, cuyas creaciones fueron sistematizadas por van der Waerden en su libro de 1930.

También en Rey Pastor se encuentra la siguiente diferenciación entre campos y Cuerpos.

Campos: conjunto de entes (llamados elementos), entre los cuales son realizables la adición, sustracción, multiplicación y división por divisor no nulo. Los campos más interesantes son los de multiplicación conmutativa, que llamaremos Cuerpos; los otros (Schiefkôrper), se llamaran seudocuerpos.

En Cuanto al origen de los Cuerpos a partir de la geometría algebraica, Kline (2004) afirma que después de que el método algebraico fuera ampliamente usado en la geometría proyectiva, el problema era reconocer qué propiedades [33]métricas de las figuras geométricas eran independientes de la representación en coordenadas lo que motivó el estudio de los invariantes algebraicos[34]. Escenario en el que se llevó a un primer plano la teoría abstracta de los módulos, anillos y Cuerpos. La unión de geometría y el álgebra en la teoría de invariantes fue principalmente promovida por Klein y Cayley.

Es importante resaltar aquí que los problemas concernientes a la teoría de números, la teoría de ecuaciones y a las transformaciones convergían ahora en la teoría de invariantes. El primer problema importante que afrontaron los fundadores de la teoría de invariantes, según Kline (1972), fue el descubrimiento de invariantes particulares; esto debido a que algunos invariantes tomados junto con la forma original dan un nuevo sistema de formas

[33]Las propiedades proyectivas de las figuras geométricas son aquellas que quedan invariantes bajo transformaciones lineales de las figuras. Las clases de transformaciones, que pronto reemplazaron a las transformaciones lineales como interés preferido, es llamada birracional de las coordenadas y transformaciones inversas también son funciones racionales de sus coordenadas.

[34]El término invariante algebraico se usa para distinguir aquellos que surgen bajo las transformaciones lineales más generales de los invariantes modulares de la teoría de números y, de los invariantes diferenciales de la geometría riemanniana.

que tiene invariantes simultáneos. La continuación del cálculo de invariantes trajo consigo la necesidad de encontrar un sistema completo de invariantes. Cayley demostró que los invariantes y covariantes encontrados por Ferdinand Eisenstein (1823-1852) para la forma cúbica binaria y los que obtuvo para la forma cuartica binaria son un sistema completo para los casos respectivos. Esto dejó abierto el problema de un sistema completo para otras formas.

Al respecto conviene decir que la existencia de un sistema completo finito o base para las formas binarias de indistinto grado y la demostración de que cualquier sistema finito de formas binarias que tiene un sistema completo de invariantes y covariantes fueron establecida por Paul Gordan (1837-1912). Las pruebas de Gordan mostraron cómo calcular los sistemas completos lo cual permitió que se obtuvieran varias extensiones de este resultado. Sin embargo, pasó mucho tiempo antes que estas tuvieran un efecto realmente innovador. En 1886, Franz Martens (1840-1927) volvió a demostrar el teorema de Gordan obteniendo como resultado una prueba de existencia del conjunto finito de invariantes y covariantes independiente para los sistemas binarios.

El problema ahora era descubrir un proceso para encontrar el sistema completo. Hilbert volvió a demostrar en 1888 el teorema de Gordan obteniendo desde un enfoque diferente del problema una demostración de existencia de la colección finita de invariantes y covariantes, esto es, el sistema completo de invariantes. Es decir, encontró que para cualquier forma o sistema de formas existe un número finito de invariantes y covariantes enteros racionales por medio de los cuales se pueden expresar todos los demás invariantes o covariantes enteros racionales como combinación lineal del conjunto finito.

Sin embargo, el teorema de Hilbert no mostraba cómo calcular los invariantes para cualquier forma o sistema de formas dados. Luego de que Hilbert hubiese abandonado el tema de los invariantes, Emmy Noether (1882-1935), escribió su tesis doctoral en 1907 “Sobre sistemas completos de invariantes para formas bicuadráticas ternarias”. También dio un sistema completo de 331 formas covariantes para una cuartica ternaria. En este sistema, reformula el teorema de la base de Hilbert de la manera siguiente: Un anillo de polinomios en un número cualquiera de indeterminadas sobre un anillo de coeficientes con unidad y una base finita, tiene él mismo una base finita.

Luego de esto, Kleiner (1972) afirma que Hilbert demostró en el lenguaje de Grupos que todo sistema modular (un ideal en la clase de los polinomios en n variables) tiene una base que consiste en un número finito de polinomios, o que todo ideal en un dominio polinomial de n variables posee una base finita siempre que el dominio de los coeficientes de los polinomios de todo ideal tenga una base finita. En 1910 Emmy Noether, extendió el resultado de Gordan a n variables; y de 1911 a 1919, escribió muchos artículos sobre bases finitas para casos distintos.

La importancia de la metodología instaurada por Hilbert y enriquecida por Emmy Noether en la teoría de invariantes reside en que llevó a un primer plano la necesidad de utilizar la teoría abstracta de los módulos, anillos y Cuerpos. Kline (1972) se refiere al estudio de geometría algebraica en la actualidad en los siguientes términos:

> En la actualidad el estudio de la geometría algebraica abarca el estudio de mayores dimensiones ("manifolds" o variedades) definidas por una o más ecuaciones algebraicas. Más allá de la generalización en esta dirección, otra extensión, a saber, el uso de los coeficientes más generales en las ecuaciones que las definen, también ha sido llevada a cabo. Estos coeficientes pueden ser elementos de un anillo o Cuerpo abstracto y se aplican a los métodos de álgebra abstracta (p. 1248).

Capítulo 2.

LOS APORTES A LA CONSOLIDACIÓN DE LA NOCIÓN DE GRUPO Y CUERPODE RICHARD DEDEKIND Y EMMY NOETHER

En el panorama histórico de la emergencia de Grupos y Cuerpos en varios momentos han aparecido tanto Richard Dedekind como Emmy Noether cerrando las brechas de producción intelectual de muchos de sus antecesores con su maravilloso ingenio, cargado de un refinamiento exquisito donde el rigor de los objetos bien definidos siempre está presente. Ambos vivieron en la sombra y enigmáticamente su labor salió a la vista de todos pues era imposible dejar de reconocer lo que habían hecho. Una labor, que se puede decir estuvo provista de una única ambición; la de asegurar una investigación sistemática, exhaustiva, rigurosa y sin lagunas ni contradicciones.

2.1 Los Aportes de Richard Dedekind

Richard Dedekind (1831- 1916) es reconocido principalmente por sus aportes en la construcción del continuo numérico y al estructuralismo como fundamento conceptual de las matemáticas. Por presentar en 1888 el artículo *Was sind und was sollen die Zahlen*, basado en los trabajos de Grassmann y Frege, que consistía en una "caracterización algebraica" de los números naturales a partir de dos conceptos primitivos, el 1 y sucesor. También por proporcionar una base sólida para el sistema de los números reales. Según Corry (2004), varios matemáticos como Weierstrass, Cantor y Charles Meray estaban intentando una tarea similar casi al mismo tiempo. Sin embargo, el trabajo de Dedekind se destaca claramente por su abstracción, exhaustividad y claridad conceptual. Esto sin duda alguna permitió el avance en las consideraciones numéricas que presentó en sus investigaciones en el campo del álgebra y la teoría de *números algebraicos*.

Corry (2004) menciona que la obra intelectual de Dedekind refleja una unidad metodológica notable de las cuales se pueden mencionar: una clara inclinación a abordar problemas matemáticos, reformulando radicalmente todo el entorno conceptual de los objetos de estudio; y la introducción sistemática de nuevos conceptos. Esto tuvo un papel central en la solución de diferentes problemas, ya que esta metodología le permitía la clarificación del conocimiento matemático existente.

En dichas investigaciones se estableció el escenario necesario para la consolidación de diferentes conceptos del Álgebra Moderna. Dedekind generalizó y unificó los razonamientos de matemáticos como Gauss, Kummer, Dirichlet, Galois, entre otros. Según Ferreirós (1998), propuso un tratamiento conjuntista-estructural de la teoría de números algebraicos. A pesar de que muchos de los conceptos de carácter abstracto introducidos en el desarrollo de la teoría, surgieron de forma natural desde el contexto técnico específico del problema investigado.

Según Corry (2004), Dedekind sometía a un largo período de maduración sus trabajos antes de publicarlos. Por esta razón varios de los trabajos que se conocen ahora corresponden a la lectura de las obras póstumas tomadas de los manuscritos (*Nachlass*) de los cursos que Dedekind dictaba en la universidad de Gôttingen sobre la teoría de Galois.

Uno de estos manuscritos *Eine vorlesung über Álgebra* (Una Lección de Álgebra) fue dividido en cuatro secciones; de las cuales se hará referencia a las secciones I y III, puesto que estas tienen mayor relación con los propósitos de este trabajo. En la primera sección *"Elemente der Lehre von den Substitutionen"*, desarrolla la teoría de Grupos de permutaciones o de sustituciones; y en la sección III "Uber die Algebraische Verwandtschaft der Zahlen" utiliza las nociones de Grupo teórico con el fin de presentar los principios introducidos por Galois en el estudio de "álgebra superior". Corry (2007) al respecto afirma que de todo el manuscrito es el en capítulo tercero, donde Dedekind se acerca más a la identificación de cualquier cosa como un Cuerpo.

Corry exhibe cómo Dedekind define los Grupos de sustitución en el capítulo I, a través de la siguiente cita:

> Las siguientes investigaciones se basan sólo en los dos principales resultados que fueron probados anteriormente, la asociatividad cancelable por derecha e izquierda y en el supuesto de que el número de sustituciones es finito: Con estas dos hipótesis encontró que los resultados son válidos para cualquier dominio finito, tanto de elementos, cosas, conceptos $\theta, \theta', \theta'', \ldots$ Para luego admitir la composición $\theta\theta'$ en cualquier par de elementos θ, θ' dados. Después de esto hizo producto $\theta\theta'$, probando que este es en sí mismo un miembro del dominio y que dicha composición satisface las leyes expresadas inicialmente. Finalmente dice que en muchas partes de las matemáticas, y especialmente en la teoría de los números y el álgebra, a menudo se encuentran ejemplos de esta teoría dado que los mismos métodos de prueba son válidos en estos (Corry, 2004, p. 78).

Como es posible advertir, Dedekind definió un cambio en un conjunto finito (complejo) y explicó cómo multiplicar dos sustituciones del mismo conjunto. Mostró como resultado que el Cuerpo de sustituciones es asociativo –cancelable por izquierda y por derecha- con respecto a su producto. También que cualquier conjunto finito de sustituciones se llama un Grupo siempre que el producto de cualquiera de los dos elementos de estos pertenezca al conjunto. Corry (2004) menciona que Dedekind deriva todos los resultados sobre Grupos de esas dos hipótesis. En todo el artículo continuó refiriéndose a las sustituciones y las sustituciones de productos, con lo cual dejó muy claro que él tenía en mente una teoría de Cuerpos más general con aplicaciones en muchos campos de las matemáticas.

Para aclarar lo anterior Corry (2004) dice:

> Los Grupos, por una parte, y las colecciones específicas de números complejos, por el otro, aparecen aquí como entidades matemáticas que pertenecen a diferentes ámbitos conceptuales. El sistema de números complejos y las interrelaciones entre los "dominios racionales" contenidos en el mismo constituyen para Dedekind la materia de álgebra superior; Grupos, por otro lado, ofrecen una herramienta muy eficaz que se puede aplicar para hacer frente a un problema relacionado con ecuaciones polinómicas con raíces en esos dominios. (p. 80)

Por consiguiente, Dedekind tomó los Grupos como entidades matemáticas autónomas, en lugar de sus elementos de Grupos, sin embargo resalta su categoría de herramienta en la resolución de un problema particular. Ferreirós en Dedekind (1888) resalta además de la visión anticipada de Dedekind para definir los Grupos abstractos (de por lo menos treinta años), el hecho de que él se haya dado cuenta de la necesidad esencial de la noción de Cuerpo para la teoría de Galois; ya que esto le permitió obtener los avances presentados en teoría de números algebraicos, en tanto que desde esta noción logra concebir y definir el anillo de enteros de un Cuerpo de números algebraicos. También demostrar que la manera formal en que Kummer, Dirichlet, Steinitz, entre otros, definían el concepto de anillo era errónea, y eso hacia imposible una teoría general de factorización.

Dedekind publica entre 1847 y 1894, cuatro versiones sucesivas de la teoría de ideales, las cuales presentan un tratamiento integral del problema de factorización única [35]en el campo

[35]El teorema de factorización única, también llamado el teorema fundamental de la aritmética, afirma que todo número natural se puede escribir de una manera única (excepto tal vez por la orden) como producto de sus factores primos.

de los números algebraicos. Corry (2004) afirma que las diversas versiones de su teoría de los ideales ayudan a la comprensión de la forma real en que Dedekind concibió, desarrolló y aplicó los conceptos que introdujo de la teoría de ideales y los homomorfismos.

Dedekind, partió de las nociones introducidas por Kummer alrededor de los números enteros. Generalizó la noción de número algebraico y con esto, restauró la factorización única en los Cuerpos de números algebraicos. Mientras Kummer, llamaba ideales a números ordinarios, Dedekind lo hacia con clases de números algebraicos. Dedekind usa la noción de número ideal de Kummer y crea la noción de ideal en un anillo. Se interesa principalmente por los anillos de los enteros algebraicos, es decir, anillos conmutativos unitarios e íntegros. La importancia de la estructura de anillo conmutativo radica en que, al disponer de los conceptos de suma y producto con las propiedades más usuales, también tenemos muchos de las nociones básicas de la aritmética: múltiplos y divisores, máximo común divisor y mínimo común múltiplo, primos, elementos primos entre sí, congruencias, etc. En cada anillo podemos desarrollar una teoría de la divisibilidad, usando las ideas y los métodos propios de la aritmética elemental. Cada anillo conmutativo es una aritmética generalizada, y la aritmética tradicional se obtiene cuando se considera el anillo $\mathbb{Z}$ de los números enteros. Para explicar esto Kline (1972) expresa lo siguiente:

> En lugar del entero 2, Dedekind toma la clase de los enteros $2m$, donde m es cualquier entero. Esta clase consiste de todos los enteros divisibles por 2. De la misma manera, el 3 es reemplazado por la clase de todos los enteros $3n$ divisible por 3. El producto 6 se convierte en la colección de todos los números $6p$, donde p es cualquier entero. Entonces el producto $2 * 3 = 6$ es reemplazado por la afirmación de que la clase $2m$ multiplicada por la clase $3n$ es igual a la clase $6p$, a pesar del hecho de que ésta última contiene a las anteriores. Estas clases son ejemplos en el anillo de los enteros ordinarios, de lo que Dedekind llama ideales. (p. 1088)

En primer lugar, Dedekind observó que el término "números primos ideales" en las investigaciones de Kummer sugerían propiedades injustificadas de los números enteros y que hablaba de "números complejos ideales" sin definirlos. Corry dice que, estos

escrúpulos metodológicos de Dedekind con respecto al trabajo Kummer eran no sólo una cuestión de gusto personal; sino también reacciones a las lagunas que había encontrado en las pruebas Kummer. Estas lagunas fueron en opinión de Dedekind una consecuencia de la analogía defectuosa entre los números ideales primos y los números enteros primos, y en consecuencia, cada caso particular expuesto lo llevó a buscar una formulación más general y por lo tanto una solución del problema general.

En segundo lugar, simplificó y generalizó los ideales de Kummer. Tomó la teoría de divisores ideales y sustituyó la construcción formal axiomática por una construcción algebraica, en la que cada divisor ideal era identificado con el conjunto de todos los múltiplos "reales". A su vez, estos conjuntos de múltiplos podían ser determinados mediante las propiedades que definen los ideales en el sentido moderno de la palabra. Kummer buscaba una caracterización práctica de los primos irregulares lo que supone ser capaz de decidir si un numero primo p divide o no al número de clases del Cuerpo ciclotómicos de orden p. Dedekind al abordar el problema se dio cuenta que podía aprovechar el trabajo de Dirichlet sobre los primos en progresiones aritméticas, que a su vez se basaban en su propia teoría de factorización ideal en los Cuerpos ciclotómicos.

El surgimiento de los *enteros algebraicos*[36] permitieron desarrollar una teoría general que recoge como casos particulares los resultados clásicos sobre enteros cuadráticos (enteros de Gauss) o enteros ciclotómicos. La importancia de trabajar con enteros algebraicos es que éstos permiten simplificar los cálculos usando aproximaciones racionales sin más pretensiones que vigilar que los errores de redondeo no lleguen a la media unidad. Ferreiros afirma lo siguiente al respecto:

> La teoría de números algebraicos se enfrentó al problema de que los enteros algebraicos no responden a ley de factorización única en factores primos, que es típica de los números naturales o enteros y constituye el fundamento de la teoría de números, conocido ya por los griegos. Para restablecer esa Ley se recurrió a la introducción de factores ideales, siguiendo una idea de Kummer. Dedekind y Kronecker fueron los primeros en obtener una teoría satisfactoria de la factorización en cualquier conjunto de enteros algebraicos. En ciclotomía, o teoría de la "división del circulo", se estudian las soluciones complejas de ecuaciones de la forma $x^n = 1; si\ n = 3$, esas soluciones nos dan los puntos del plano complejo

36 Se llama entero algebraico a todo número que es raíz de un polinomio p(x) con coeficientes a_i enteros.

> que dividen al circulo de radio unidad en tres partes, y así sucesivamente, de donde viene el nombre. Semejantes números complejos engendran los llamados Cuerpos ciclomáticos (Dedekind, 1888, p. 22)

Dedekind considera el concepto de entero algebraico en el campo de todos los números algebraicos; a saber, todas las raíces, real y compleja, de polinomios con coeficientes racionales. La teoría de Dedekind pensada como una generalización del resultado de Kummer, es también una respuesta al problema principal que se generó en ese entonces, a saber un intento por dar una definición adecuada de los dominios implicados. La primera versión de la teoría de la factorización de Dedekind abre las puertas a la definición de sus conceptos básicos. Estos conceptos incluyen Cuerpos, módulos, congruencia en relación con un determinado módulo, y los ideales. En Corry (2007) se presenta las siguientes definiciones dadas por Dedekind:

> Un Cuerpo de los números es un sistema de números cerrados bajo las cuatro operaciones: adición, sustracción, multiplicación y división (excepto por cero). El Cuerpo "más pequeño" es el de todos los números racionales, mientras que el mayor posible es el de los números complejos. Un Cuerpo A se llama un divisor de otro M (M y se dice que es un múltiplo de A) siempre que todos los números contenidos en A también están contenidos en M. Los Cuerpos "simples" son aquellos que poseen sólo un número finito de "divisores "(es decir subcampos), y estos son llamados por Dedekind" finitos". (pp. 94).

En la sección III, según Corry (2007) se discuten las propiedades de las raíces, centrándose en un Grupo de permutaciones. Dedekind se refirió al dominio S con el término "Dominio racional" aunque sólo de paso, porque lo importante para él es que dicho subdominio del sistema de números complejos, tiene la propiedad específica de ser cerrado bajo las cuatro operaciones aritméticas; tal cómo se muestra en la siguiente cita:

> Dado un polinomio $f\ (x)$ de grado m, cuyos coeficientes se puede expresar como combinaciones racionales de números pertenecientes a un dominio S de números complejos dado, Si s, s', s'' son las tres raíces de esta ecuación, entonces se puede establecer $s' = \theta'(s), s'' = \theta''(s)$; donde los coeficientes de las funciones racionales θ y θ' pertenecen al dominio racional S. (pp.79)

En la introducción de la traducción de la obra de Dedekind (1888), Ferreirós menciona algunos aspectos sobre la importancia y la influencia de los aportes de Dedekind a la teoría de Grupos y Cuerpos. Por ejemplo, afirma que dicho autor entre 1856 y 1858 imparte cursos de invierno sobre álgebra superior y ciclotomía, en los cuales la parte central estaba dedicada a la teoría de Galois. Por primera vez esta teoría era objeto de un curso

universitario. Lo más notable, como lo señala Ferreirós, era que Dedekind analizaba independientemente los fundamentos de teoría de Grupos (de manera abstracta) necesarios para la teoría de Galois; además veía con certeza la importancia de tener en cuenta, en cada momento de referencia, a un Cuerpo de base y la interrelación entre Cuerpos y Grupos, que constituye el núcleo de la teoría de Galois desde el punto de vista moderno.

En 1853 Kronecker publicó un estudio en el que se aplica a la teoría de las ecuaciones polinómicas el tipo de ideas introducidas por Galois, siendo así uno de los primeros matemáticos en Alemania en mostrar cierto interés en esta teoría. Esa fue de alguna manera la dirección subrayada por el propio Galois, que se centró en la posibilidad de aplicar la teoría de Grupos de permutaciones para estudiar la resolvente de ecuaciones particulares. Dedekind, por el contrario desarrolló la idea que finalmente se convirtió en la forma estándar del tratamiento de la teoría de Galois en el siglo XX: un enfoque directo en la interacción entre los Grupos de permutaciones de las raíces y los automorfismos definidos en los subcampos del Cuerpo de los números complejos. Este punto de vista, fue el que desarrolló inicialmente Weber y más tarde Artin alumno de Emmy Noether.

Según Corry (2007), Dedekind estudió la teoría de Galois a fondo consiguiendo de alguna manera comprender el alcance de la teoría en una perspectiva más amplia que cualquier otra persona en las primeras etapas de su desarrollo. Corry (2007) afirma que en su versión de 1894, de la teoría de ideales, Dedekind dedica una sección entera a la presentación de las ideas centrales de la teoría de Galois. Pero ya en sus primeras conferencias se hace evidente cómo Dedekind con el fin de superar las deficiencias y carencias inherentes al tratamiento original de dicha teoría, se acercó a ésta centrándose en una reformulación original de los conceptos básicos involucrados, generalizarlos mediante la construcción argumentos rigurosos y formales.

2.2 Los Aportes de Emmy Noether

Emmy Noether (1882-1935) a pesar de ser reconocida por sus contribuciones en el campo de la física teórica y el álgebra abstracta, muchos de sus aportes fueron absorbidos por la cultura matemática general, razón por la cual no es fácil ver la influencia directa que tuvo

en las investigaciones de otras personas. Por fortuna sus colegas y estudiantes se encargaron de darle el debido crédito a sus aportes.

Kleiner (2007) manifiesta que Noether contribuyó a las siguientes grandes áreas de álgebra: teoría invariante (1907-1919), el álgebra conmutativa (1920-1929), el álgebra no conmutativa y teoría de la representación (1927-1933), y las aplicaciones del álgebra no conmutativa a problemas en álgebra conmutativa (1932-1935). "Ella sentó las bases de casi todas las ramas emergentes de la tradición algebraica de los siglos XIX y XX (con la posible excepción de la teoría de Grupos adecuada)" (pp.59).

Es posible que algunas de las puertas que se abrieron inicialmente a Emmy Noether, se debieran a su padre Max Noether, sucesor de Felix Klein en la Universidad de Erlangen; debido a que en ese entonces había muchas restricciones para que una mujer fuera a la universidad como estudiante y mucho más en calidad de docente. Max Noether es reconocido por sus aportes en el álgebra geométrica y cuyo principal trabajo se conoce como el teorema del residuo o teorema fundamental de Noether. Emmy trabajó inicialmente en Erlangen, bajo la tutela de Paul Jordán gran amigo de Max Noether, en donde realizó uno de sus primeros escritos (1907) titulado "*Sobre sistemas completos de invariantes para formas ternarias bicuadráticas*", el cual contenía 331 invariantes de las formas bicuadráticas ternarias. Pese a ser principalmente fórmulas, dicho trabajo le permitió a Emmy Noether familiarizarse con la teoría de invariantes y con el tratado sobre grupos escrito por él 1870.

Paul Jordán al retirase de sus labores académicas es reemplazado por Ernst Fischer, él era también un especialista en la teoría de invariantes pero a diferencia de Jordán su estilo era en la línea conceptual de Hilbert, su influencia permitió que Noether dejará el estilo computacional y algorítmico de Jordán. Poco después Noether comenzó a desempeñarse como asistente de David Hilbert en el seminario de matemática física, en Gôttingen.

Por sugerencia de Hilbert —para ayudarle Klein y a él— comienza su trabajo en los invariantes diferenciales de Albert Einstein y problemas variacionales, que la mantuvo ocupada durante los años 1917 y 1918. Los resultados de estas investigaciones son presentados en seminarios. Al finalizar la primera guerra mundial, las mujeres adquieren

algunos derechos; lo cual hace que pueda presentar su tesis de habilitación (1919) titulada "*Invariante Variationsprobleme*". Un tratado sobre Grupos continuos finitos e infinitos, de gran importancia en la física teórica porque presenta los teoremas de primeras integrales según se conocen en mecánica; los teoremas de conservación y las relaciones entre las ecuaciones de campo en la teoría de la relatividad. (Montero, 2005, p. 7)

Luego de estos trabajos, centró su atención en el estudio de los ideales, anillos, módulos y otras estructuras. En el periodo 1920-1926, las investigaciones de Emmy Noether giran en torno a la teoría de anillos conmutativos. El trabajo más importante de este periodo, publicado en 1921, "*Idealtheorie in Ringbereichen*", es dedicado a la teoría general de ideales. En éste, aparecen por primera vez los conceptos modernos de anillo, ideal y módulo sobre un anillo; con la particularidad de extender la definición de ideal en un anillo de enteros o en un anillo de polinomios, a *anillos conmutativos*[37] en general. Además, el concepto de la condición de cadena ascendente (CCA)[38] para ideales, usado de manera reiterativa en investigaciones posteriores para la demostración de diversos teoremas.

La condición de cadena ascendente fue previamente estudiada por Dedekind en 1894 y Lasker en 1905 en casos particulares. Noether moviéndose de lo concreto, anillos de polinomios, a lo abstracto, un anillo conmutativo noetheriano, obtiene cuatro teoremas de descomposición de ideales, de los cuales el segundo es el de descomposición primaria, conocido como el teorema de Lasker-Noether. Con la descomposición primaria de ideales, Noether introduce el concepto de *ideal primario*[39], que generaliza el concepto de ideal primo, lo cual facilita la obtención de ideales primarios no primos. En Carrasco (2004), se encuentra que:

> Históricamente el desarrollo de la teoría de ideales tiene dos puntos de partida: La teoría de ideales de anillos de enteros algebraicos de R. Dedekind, y la teoría de ideales en anillos de polinomios iniciada por Hilbert, Lasker y Macaulay y completamente diferentes. En el primer caso el problema central era el de factorización, esto es, la formulación del teorema fundamental de la aritmética para

[37]Un ideal de un anillo conmutativo $R = (R,+,\cdot)$ es subgrupo aditivo α, que contiene a todos los productos ra para cualesquiera $r \in R$ y a $\in \alpha$.

[38]Explícitamente, un anillo conmutativo R satisface esta condición si toda cadena ascendente de ideales de R: $\alpha 1 \subseteq \alpha 2 \subseteq \cdots \subseteq \alpha n \subseteq \cdots$es estacionaria, esto es, existe $k \geq 1$ tal que $\alpha k = \alpha k+1 = \alpha k+2 = \cdots$.

[39] Un ideal Q de un anillo conmutativo R se dice primario si $Q \subset R$, y siempre que $ab \in Q$, $ab \in R$, ó bien $a \in Q$ ó bien $b^n \in Q$, para algún $n \geq 1$.

> otros números además de los enteros. Mientras que en el caso de ideales de anillos de polinomios, las cuestiones que se planteaban eran la determinación de los ceros de un ideal (esto es, de las soluciones de ecuaciones polinómicas), y el establecimiento de las condiciones necesarias y suficientes para que un polinomio pertenezca a un ideal (pp.336).

Según Corry (2004) el trabajo de Emmy Noether en la teoría de los ideales constituye un punto decisivo que conduce a la nueva imagen estructural del álgebra. Por un lado, sus ideas conjugan las elaboradas por Dedekind en el marco de la teoría algebraica de números, la investigación de Hilbert sobre invariantes y teoría algebraica de números, y el trabajo de Lasker y Macaulay sobre polinomios. Por lo tanto, permiten una identificación directa de sus raíces inmediatas y motivaciones. Por otro lado, su trabajo muestra todos los rasgos que caracterizan el álgebra abstracta moderna como una disciplina de las estructuras.

Noether adoptó plenamente los lineamientos metodológicos establecidos por Dedekind junto con sus logros, especialmente los específicos de la teoría algebraica de números, buscó combinar éste con resultados similares que se habían alcanzado en la teoría de polinomios. Al igual que Dedekind, ella se esforzó por formular conceptos precisos como base legítima para explicar la similitud y la proximidad de teorías aparentemente distantes.

En 1926 presenta el articulo *Abstrakter Aufbau del Idealtheorie in Álgebraischen Zahlund Funktionsk¨orpen*, cuyo interés se encuentra en la teoría de ideales en anillos de enteros algebraicos desarrollada por Dedekind. En el artículo se proporciona una caracterización abstracta de aquellos anillos cuya teoría de ideales coincida con la de un anillo de enteros de un Cuerpo de números algebraicos. Noether da cinco axiomas para caracterizar este tipo de anillos denominados hoy: *Dominios de Dedekind*[40], esto es, dominios de integridad (es decir sin divisores de cero no nulos) donde todo ideal propio no nulo es un producto finito de ideales primos y cuya factorización es única.

[40](Kleiner 2007, pp. 96) Ella mostró que R es un dominio de Dedekind si y sólo si:
1) R es noetheriano, es decir, R satisface la Condición de cadena ascendente (a.c.c),
2) R/α es un anillo artiniano, para cada ideal no nulo α de R. (R/α respeta la condición de cadena descendente (d.c.c.) para todos los que ideales no nulo de R),
(3) R tiene elemento unidad.
(4) R es un dominio de integridad, y
5) R es íntegramente cerrado en su Cuerpo de cocientes.

Con lo anterior, demuestra que en todo dominio donde hay factorización única de ideales primos es posible. Introduce luego el conjunto de ideales fraccionarios no nulos de un anillo, los cuales constituyen un Grupo con el producto de ideales. Según Carrasco (2004) esta última propiedad es la más utilizada actualmente para definir a los dominios de Dedekind; de la cual se desprende que el Grupo de clases de anillo sea posible si y solo si todo ideal es principal, lo que ocurre si y solo si el Grupo de clase tiene un solo elemento.

También en 1926 Noether, publica *Der Endlichkeitssatz der Invarianten endlicher Linearer Gruppen der Charakteristik,* en el cual se resalta el lema de normalización, importante entre otras, por sus aplicaciones en el estudio de variedades algebraicas, en tanto proporciona la existencia de proyecciones lineales con ciertas propiedades. Esto lleva al estudio de la ramificación para tales proyecciones y permite definir el grado y dimensión de una variedad algebraica o normalización de una variedad algebraica afín (Montero, 2005).

Después de 1927, Emmy Noether se comenzó a interesar por el álgebra no conmutativa y sus aplicaciones a representaciones de Grupos finitos. Uno de los trabajos que giran en este sentido es *Hyperkomplexe Grôssen und Darstellungstheorie* (1929):

> En este trabajo, dividido en cuatro capítulos Noether desarrolla una teoría de ideales en anillos no conmutativos verificando ciertas condiciones de finitud, con el objeto de tratar de forma unificada la teoría de estructuras del álgebra y la teoría de representaciones de Grupos finitos (Corrales, 2004, pp.344)

Kleiner (2007) afirma que el trabajo de Noether en esta área estableció un marco conceptual muy eficaz en el estudio de la teoría de la representación. Por ejemplo, mientras que el enfoque clásico (computacional) para teoría de la representación es válido sólo en el campo de los números complejos; o en el mejor de los casos sobre un campo algebraicamente cerrado de característica 0, en el enfoque de Noether sigue siendo significativo para cualquier campo de cualquier característica. El uso de campos arbitrarios en teoría de la representación se volvió importante en la década de 1930 cuando Brauer comenzó sus estudios pioneros de representaciones modulares, es decir, aquellos en los que la característica del Cuerpo divide el orden del Grupo.

Noether fue la primera en utilizar la noción de módulo de manera abstracta y de reconocer su potencial, con un anillo de Dominio de operadores. En efecto, es a través de su trabajo

que el concepto de módulo se convirtió en un concepto central del álgebra Moderna. De hecho, los módulos son importantes no sólo por su carácter unificador, sino también debido a su poder de linealización. Son, después de todo, las generalizaciones de los espacios vectoriales, y de muchas de las construcciones de vectores en el espacio estándar, como subespacio, espacio cociente, suma directa y el producto tensorial (Kleiner, 2007, pp. 98).

Noether observó que sus desarrollos teóricos con módulos, tenían aplicaciones en la topología combinatoria, concretamente comprendió que los números de Betty y los coeficientes de Torsión, invariantes numéricos de un espacio compacto triangulado podían ser sustituidos por módulos de homología.

> En 1932, publica *Uber minimale Zerf¨ allungsk¨ orperirreduziblerDarstellungen* artículo que realiza en colaboración con R. Brauer donde por primera vez se define de forma clara la noción de Cuerpos de descomposición para representaciones de álgebras (es decir, en los que una representación dada se descompone en representaciones completamente irreducibles), Observa su relación con Cuerpos de descomposición de álgebras simples y álgebras de división. Lo cual le permite en 1933 escribir el artículo *Nichtkommutative Algebren*, en el cual se realiza un estudio detallado de Cuerpos de descomposición de álgebras simples, así establece nuevamente la base para futuros desarrollos en este campo. (Carrasco, 2004, pp. 344).

Es posible que muchas contribuciones de Emmy Noether se escapen en este estudio debido a que fue una mujer con una dedicación y claridad conceptual inigualables y es factible conocerlas en gran medida en el álgebra moderna de van der Waerden. En Arenzana (1995) se dice que van Waerden reconoce que para escribir su álgebra moderna, estudió las obras de: A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung*, publicada en Berlín en 1927; H. Hasse, *Hôhere Algebrá I, II and Aufgabensammlung zur Hôlerem* álgebra publicada entre 1926-27; O. Perron, *Álgebra I, II* de 1927 y el álgebra de Dickson, L.E. Modern Algebraic Theories, publicada en Chicago en 1926. Sin embargo, la mayor inspiración de van der Waerden para la escritura del libro surgió de las lecciones de álgebra recibidas por Emil Artin, alumno de Emmy Noether, en el verano de 1926 en Hamburgo; y de las notas de clase de Emmy Noether sobre teoría de Grupos y números hipercomplejos, en Gotinga, en los inviernos de 1924-25 y 1927-28.

CAPÍTULO 3.

EL ÁLGEBRA MODERNA DE WEBER Y VAN DER WAERDEN

A lo largo de la investigación que en el presente trabajo se expone, se observan las finas líneas que unen a una gran cantidad de matemáticos desde incluso antes de Cristo; profundizando sobre todo en lo que aconteció a partir del siglo XIX hasta 1930. En la obra de Weber es posible observar su preocupación por dar este recorrido histórico detallado mediante la exposición de los diferentes métodos y definiciones; lo cuales perfilaron la compresión de la teoría de Galois (tomo I) y el surgimiento de una gran cantidad de Grupos y sus aplicaciones en diversos campos de las matemáticas en especial a la geometría y el análisis. Weber mismo reconoce que su fuente de inspiración fueron las clases de Richard Dedekind del invierno de 1872 y que recibió de él permanentes consejos en la labor de editor de los tres volúmenes que conforman su obra. Mientras que el reconocimiento para Emmy Noether está en la obra de B.L: van der Waerden quien menciona en el prologo de su libro Modern Algebra que fueron las clases del invierno de 1924-25 y 1927-28 de Noether la fuente de mayor inspiración para el desarrollo de su libro.

3.1 El *Álgebra Moderna*de Weber (Lehrbuch der Algebra)

El Álgebra Moderna de Weber está compuesta por tres volúmenes[41]. En el primer volumen se exponen según el autor las partes elementales del álgebra designadas con el calificativo de "aritmética generalizada" o "cálculo de letras" (*Buchstabenrechnung*), las disposiciones relativas al cálculo numérico de las raíces de la ecuación y los comienzos de la teoría de Galois. La intención de Weber era presentar un resumen que vinculará los diversos aspectos teóricos y múltiples aplicaciones del álgebra de las últimas décadas del siglo XIX, además de introducir al lector en un álgebra sin muchos prerrequisitos pero que a la vez fuera llevándolo a un estado creciente de dificultad sin la necesidad de remitirse a otros libros de texto. El segundo volumen presenta un tratamiento de la teoría general de los Grupos finitos, la teoría de los Grupos de sustitución lineales y las aplicaciones a distintos

[41] Algunos contenidos de Lehrbuch der Algebra (índice de contenidos, prólogos y las definiciones de Grupo y Cuerpo) importantes para los propósitos del presente trabajo, fueron traducido directamente del alemán al español por los profesores: Jaime Arango, Manuel Villegas, Jairo Duque y Liliana Camargo del departamento de Matemáticas de la Universidad del Valle.

problemas particulares, concluyendo en la teoría de números algebraicos. Su propósito en este era unificar los distintos puntos de vista bajo los cuales estas teorías habían sido observadas hasta ese momento, esto incluye un lenguaje uniforme y sin ambigüedades. El tercer volumen de *Lehrbuch* apareció en 1908, presenta un tratado sobre funciones elípticas y números algebraicos en el marco de la naciente teoría de ideales. Señala que dicho volumen es una segunda edición del libro que el mismo había publicado en 1891 y que por dificultades editoriales se divulgó al mismo tiempo que la primera edición.

3.1.1 Primer volumen

El primer volumen inicia con una introducción en el cual se abordan las propiedades de los diferentes sistemas numéricos. En este se hace evidente la influencia de las ideas desarrolladas por Dedekind (1872), Weber reconoce también su participación como editor de su álgebra y aunque su participación en el desarrollo de las ideas no fue directa, Dedekind fue su motor de inspiración desde el invierno de 1857-58 en el cual impartía un curso pionero sobre la teoría de Galois y del cual conservaba sus notas de clase. Después de la introducción aparece un breve recuento de las propiedades de los enteros y luego se introduce el concepto de conjunto. Se definen conjunto densos (*dicht*), ordenados, discretos y continuos, y sus propiedades; también define las cortaduras al estilo de Dedekind. Los números racionales constituyen un conjunto denso no-continuo mientras que los reales forman un sistema denso y continuo. Weber trabaja aquí con formulaciones que pueden clasificarse de abstractas, sin ser propiamente axiomáticas, más bien versan de objetos particulares, cuyas propiedades deben especificarse de antemano.

En este volumen (Volumen I) el autor muestra que el problema central que desea abordares el de la resolución de ecuaciones polinómicas. Este problema es considerado desde varios puntos de vista, pero en todo caso se trata de ecuaciones polinómicas cuyas raíces son números reales o complejos, y cuyas propiedades dependen directamente de las propiedades de los diferentes sistemas numéricos considerados en la introducción.

A continuación se presentan los títulos y subtitulaciones que hacen parte del índice de contenidos de cada uno de los volúmenes del álgebra de Weber:

"**Los Fundamentos**" está dedicado a desarrollar cuestiones relacionadas con las funciones racionales, los determinantes, las raíces de las ecuaciones algebraicas, las funciones simétricas, las transformaciones lineales alrededor de la invarianza y la transformación de Tschirnhausen[42]. **"Las Raíces"** por su parte desarrolla los capítulos con las siguientes titulaciones: existencia de las raíces, El teorema de Sturm, evaluación de las raíces, el cálculo aproximado de las raíces, las fracciones continuas y la teoría de las raíces de la unidad. Finalmente el libro de **Álgebra superior** presenta: La teoría de Galois, aplicación de los Grupos de permutaciones en ecuaciones, ecuaciones cíclicas, división del círculo, solución algebraica de ecuaciones y las raíces de las ecuaciones metacíclicas.

El capítulo uno "Las Funciones Racionales" está dedicado a: las funciones enteras, el teorema de Gauss, división, división por una función lineal, divisibilidad de funciones a trozos, máximo común divisor, factores lineales del producto, teorema del binomio, interpolación del teorema del binomio, solución de problemas de interpolación usando diferencias, serie aritmética del orden superior, teorema generalizado del binomio aplicado a polinomios, derivadas de funciones (aproximación por Taylor), derivadas del producto, parametrización para obtener funciones homogéneas y el teorema del binomio generalizado, derivada de funciones de varias variables, y el teorema de Euler sobre funciones homogéneas.

El capítulo dos es sobre determinantes, los temas que trata son los siguientes: Permutaciones de n elementos, permutaciones de primera y segunda clase, determinantes, principales teoremas sobre determinantes, cofactores de los determinantes, ecuaciones lineales homogéneas, método de eliminación, Ecuaciones lineales no homogéneas, multiplicación de los determinantes, determinante de los cofactores y la interpolación.

El capítulo tres es sobre las raíces de las ecuaciones algebraicas, comprende los siguientes temas: El concepto de raíz, la multiplicidad de las raíces, continuidad de las funciones, cambios de signo de $f(x)$, raíces de las ecuaciones de grado pares y de las raíces impares, soluciones de ecuaciones pares usando funciones trigonométricas, solución de una ecuación

42 Una transformación de Tschirnhause, es un tipo de mapeo de polinomios desarrollados por Ehrenfried Walther von Tschirnhaus en 1683. Puede definirse como la transformación más general de un polinomio irreductible que tiene una raíz en cierta función racional aplicado a esa raíz.

de segundo orden, ecuaciones cúbicas, el método de Cardano, la resolución de Cayley del método de Cardano, las ecuaciones bicuadráticas, demostración del Teorema Fundamental del Álgebra, algoritmos para calcular las raíces de una ecuación y continuidad de las raíces.

El capítulo Cuatro estudia las funciones simétricas: concepto de las funciones simétricas, funciones simétricas fundamentales, series de potencias, demostración de los teoremas fundamentales de sistemas de dos variables, generalidades de los teoremas fundamentales, segunda demostración funciones simétricas, el discriminante, discriminante de tercer y cuarto orden, la resultante, teorema de eliminación de Bezout, método de eliminación para la mayoría de ecuaciones, funciones divisibles y no divisibles, transformación de Tschirnhausen, aplicaciones de las ecuaciones cúbicas y bicuadráticas, la transformación de Tschirnhausen de la ecuación de quinto grado.

El capítulo quinto trata sobre transformaciones lineales e invariantes. Comprende: la transformación lineal, las formas cuadráticas, la transformación de la forma cuadrática en una suma de cuadrados, ley de inercia de las formas cuadráticas, transformación de formas de n grado, invariantes y covariantes, transformación lineal de las formas binarias, formas cubicas binarias, la forma completa del sistema cubico binario, formas bicuadráticas, covariante, sistema completo de invariantes de la forma binaria bicuadrática.

En el capítulo sexto "Transformación de Tschirnhausen" se encuentra los siguientes subtemas: Forma de Hermite de la transformada de Tschirnhausen, Los invariantes de la transformada de Tschirnhausen, desarrollo del teorema delas formas Hermitianas, transformación de la ecuación cúbica, desarrollo general de la transformación, la Bezoutiana, transformación de la ecuación de quinto grado, y la forma normal de la ecuación de quinto grado.

A partir de aquí y hasta el capítulo XII se desarrolla el **libro II**. En el **capítulo séptimo** "la existencia de las raíces" incluye: Generalidades sobre la existencia de las raíces de la ecuación y de su discriminante, discusión sobre la ecuación cuadrática y cubica, discusión sobre las ecuaciones bicuadráticas, la Bezoutiana y su significado para existencia de las raíces, ley de la inercia de las formas cuadráticas, formas cuadráticas con determinante nulo

y distinto de cero, número de cuadrados positivos y negativos y la aplicación de la Bezoutiana.

En el capítulo VIII, El teorema de Sturm, trabaja los temas: el problema de Sturm, las cadenas de Sturm, primer y segundo ejemplo de la función de Kugel, las funciones de Sturm, la solución de Hermite del problema de Sturm, análisis de las formas Hermitianas, el determinante de la forma de Hermite, fundamento de la teoría de características, característica de un sistema de tres funciones, relación de las características con los puntos de corte, aplicación de las características para la determinación de las raíces, análisis de las características y primera demostración del teorema fundamental del álgebra.

En el capítulo IX, "evaluación de las raíces" está dedicado a: El teorema de Budan Fourier, la regla de Newton, valoración de las raíces positivas, criterio de Jacobi, comparación geométrica de Klein delos distintos criterios, análisis de una cota superior para las raíces, evaluación de las raíces imaginarias, teorema de Rolle y los conjuntos de Laguerre para las ecuaciones que tienen sólo raíces reales.

Para el desarrollo del **capítulo X** incluye: Interpolación. Regula falsi, el método de aproximación de Newton, el método de aproximación de Daniel Bernoulli y métodos aplicados, método de aproximación de Graffe, solución trigonométrica de la ecuación cúbica, resolución de trinomios por el método de Gauss, y la regla de las raíces imaginarias para los trinomios.

Capítulo XI Fracciones Continuas: transformaciones de fracciones racionales en fracciones continuas, desarrollo de fracciones continuas de números irracionales, aproximaciones racionales, solución de ecuaciones indeterminadas de dos variables, convergencia de la aproximaciones racionales, números equivalentes, desarrollo de números equivalentes en las fracciones continuas, forma de las ecuaciones irracionales de una ecuación cuadrática, raíces irracionales de ecuaciones de segundo grado, números reducibles de discriminante negativo, números reducibles de discriminante positivo, desarrollo de ecuaciones cuadráticas en términos de fracciones continuas, ejemplos, la ecuación de Pell, forma de obtener todas las soluciones de las ecuaciones de Pell desde el menor positivo, observación

de la teoría Gaussiana de las formas cuadráticas, raíces, racionales de ecuaciones que se pueden descomponer completamente y ecuaciones reducibles.

Capitulo XII, Teoría de las raíces de la unidad, comprende: las raíces de la unidad, raíces primitiva de la unidad, ecuaciones de las raíces primitivas de la unidad de n-ésimo grado, irreductibilidad, el discriminante de la ecuación ciclotómica, raíces primitivas congruentes, multiplicación y división de las funciones trigonométricas, análisis del signo y los restos cuadráticos.

En el libro de álgebra superior se encuentra en el **capítulo XIII** la teoría de Galois con las siguientes subtitulaciones: El concepto de Cuerpo, adjunción, funciones en un Cuerpo, Cuerpo algebraico, adjunción simultanea de varias magnitudes algebraicas, Cuerpo primitivo y no primitivo, Cuerpo normal, resolvente de Galois, las sustituciones de un Cuerpo normal, composición delas sustituciones, Grupos de permutaciones, Grupo de Galois, Grupos transitivos y no transitivos, Grupos primitivos y no primitivos.

Capitulo XIV "Aplicación de los Grupos de permutaciones en ecuaciones" aquí se desarrolla: el efecto de los Grupos de permutaciones sobre funciones de $n$variables independientes, la descomposición de las permutaciones en la transposición y el ciclo, divisores de los Grupos, Grupos segundarios y Grupos conjugados, resolución del resolvente de Galois mediante la adjunción, división normal de un Grupo, el Grupo de los resolventes, reducción del Grupo de Galois mediante cualquier adjunción irracional, Grupos no primitivos.

Capitulo XV "ecuaciones cíclicas" contiene: ecuaciones cúbicas, Grupos de permutación con cuatro elementos, solución de las ecuaciones, ecuaciones de Abel, reducción de la ecuación de Abel a cíclica, resolventes de Lagrange, solución de las ecuaciones cíclicas, división de ángulos.

Capítulo XVI "División del Circulo" aquí aparece: periodo del circulo y las ecuaciones periódicas, método gaussiano para el cálculo del resolvente, reducción de la ecuación ciclotómicas a partir de ecuaciones puras. División décimo séptima, caracterización de los

números ψ, la suma gaussiana, las particiones de los periodos de $\frac{1}{3}(n-1)$ y $\frac{1}{4}(n-1)$, los números complejos de Gauss, el Cuerpo de las terceras raíces de la unidad.

Capítulo XVII "Solución algebraica de ecuaciones" desenvuelto en los siguientes desarrollos: reducción de Grupos mediante ecuaciones, ecuaciones metacíclicas, disposiciones de los Grupos alternados, ecuaciones que no son metacíclicas en Cuerpos de números racionales, solución por medio de radicales reales, ecuaciones metacíclicas de grado primo, aplicación de las ecuaciones metacíclicas de quinto grado, el Grupo del resolvente, postulación de problemas, proposiciones sobre los resolventes, raíces de las ecuaciones metacíclicas, independencia de las condiciones reducidas, condiciones de existencia y ecuaciones metacíclicas de quinto grado.

3.1.2 Segundo volumen

Está dividido en cuatro libros. Weber afirma haberse esforzado en escoger las aplicaciones que en áreas como la geometría y la teoría de funciones por si mismas son interesantes y al mismo tiempo mostrar los principales puntos de la teoría algebraica. La aplicación de la teoría de números algebraicos se desarrolla hasta la teoría de números ciclotómicos. Para la escritura y edición de este tomo cuenta de nuevo los consejos y visión de Dedekind y Klein. El primer libro titulado "Grupos" contiene las siguientes Secciones: teoría general de Grupos, Grupos abelianos, el Grupo de Cuerpos ciclotómicos, Cuerpo Abeliano de tercer y cuarto grado y la naturaleza de los Grupos generales; el segundo libro "Grupos lineales" comprende: Grupos de sustituciones lineales, Grupos de sustituciones lineales binarios y Grupos de congruencias; y el Tercero, "Aplicaciones de la teoría de Grupos" presenta: teoría general de ecuaciones metacíclicas, los "puntos de inflexión de una curva de tercer orden, las dobles tangentes de una curva de cuarto orden, teoría general de las ecuaciones de quinto grado, Grupos de sustituciones ternarias lineales, el problema de la forma del GrupoG_{168} y la teoría ecuaciones de séptimo grado, Finalmente el cuarto libro "Números algebraicos" abarca los temas Números y funciones de un Cuerpo algebraico, teoría algebraica de Cuerpos, los discriminantes, los ideales primos en Cuerpo relativamente normal, Cuerpo cuadrado, Cuerpos ciclotómicos y abelianos, número de clases y figuras trascendentes.

A continuación se detallan los contenidos de cada sección del tomo II:

Primer libro: Grupos. Sección. I -Teoría General Grupos: definición Grupo, los divisores de Grupos finitos, subgrupo normal de un Grupo, Composición de las partes, isomorfismo multinivel, la serie de composición y el teorema de C. Jordán, más teoremas sobre la serie de composición, Grupos metacíclicos.

Sección II -Grupos abelianos: representación Grupos abelianos por una base, los invariantes de Grupos abelianos, caracteres de Grupo, divisores de un Grupo abeliano, Grupos recíprocos, los generadores en un Grupo abeliano, índices por una potencia prima impar como módulo, índices para una potencia de 2 como módulo, los Grupos en el número clases por un módulo compuesto.

Sección III -El Grupo de campos ciclotómicos: los resolventes de la teoría ciclotómica, campos ciclotómicos, factor primario y no primario del Grupo $\mathfrak{R}$, los períodos ciclotómicos, campos ciclotómicos con un Grupo determinado, la determinación del Grupo $\mathfrak{A}$.

Sección IV –Cuerpo abeliano de tercer y cuarto grado: campos ciclotómicos cúbicos, campos ciclotómicos bi-cuadráticos, ecuaciones cúbicas abelianas, ecuaciones de cuarto grado abelianas.

Sección V -Constitución de los Grupos generales: La formación de Grupos de acuerdo a Cayley, relación de los Grupos de permutaciones generales, la primera proposición Sylow, la segunda proposición de Sylow, Grupos de grado p^a, teorema Frobenius, Grupos de grado $p^a q$, Grupos simples, Grupos de grado $p\,q$, límites del índice de un divisor del Grupo de permutación simétrica.

Segundo libro: Grupos lineales * Sección VI -Grupos de sustituciones lineales: sustituciones lineales y su composición, la sustitución de las proporciones, las permutaciones como sustituciones lineales, los invariantes de Grupos finitos de sustituciones lineales, el conjunto de Hilbert, la finitud de sistemas lineales finitos Invariantes, Grupo de sustitución, el problema de moho, extensión de Klein del problema fundamental del álgebra, influencia de los invariantes relativos, el término invariante extendido, formas normales .

Sección VII -Grupos de sustituciones lineales binarios: sustituciones ortogonales ternarias, sustituciones fraccionales lineales, condiciones, Grupos finitos de sustituciones fraccionales lineales, polos de los Grupos, los diversos tipos de posibles Grupos, transformación de las sustituciones de la G a formas simples, las formas básicas, sección de popa, el Grupo de poliedros, los Grupos cíclicos y Grupos diedros, el Grupo tetraédrico, el Grupo octaédrico, el icosaédrico, el divisor de la icosaédrica, las formas básicas de la icosaédrica, las invariantes del icosaedro, Grupo de poliedros del segundo tipo, Grupos cristalográficos

Artículo IX -Grupos de Congruencias: Funciones –congruencias, Cuerpos congruentes, Grupo de congruencias en el Cuerpo $\mathfrak{C}$, simplicidad Grupo E, Cuerpo de congruencias de segundo grado, Grupo lineal congruente L_p, forma imaginaria de GrupoL_p, divisores del GrupoL_p cuyo grado es divisible por p, divisores del GrupoL_p, cuyo grado no es divisible por p, constitución del Grupo L_7 de grado 168.

Libro Tercero: Aplicaciones de la teoría de Grupos. Sección X -Teoría general de ecuaciones metacíclicas: los resolventes de la serie de composición, ecuaciones metacíclicas, ecuaciones metacíclicas cuyo grado es una potencia principal, representación de Abel ver Grupo Q, representación analítica de permutaciones, representación del Grupo P metacíclicas, congruencias Grupo lineal ternario para el módulo 2, ecuación resolutivo octavo grado, el sistema triple de los resolventes, aplicación a las ecuaciones octavo grado, ecuaciones metacíclicas octavo grado, ecuaciones bicuadráticas.

Sección XI -Los "puntos de inflexión de una curva de la tercera orden": formas ternarias y curvas algebraicas, los puntos singulares, puntos de inflexión, tangentes dobles, covariantes fundamentales forman un ternario, la curva de Hesse, los puntos de inflexión de una curva de la tercera orden, transformación de la forma cúbica en la forma canónica, los invariantes de la curva de la tercera orden y la ecuación bicuadrática, ecuaciones triples, el Grupo de ecuaciones triples, índices reales para de ecuaciones triples.

Sección XII -Las dobles tangentes de una curva de cuarto orden: Número de dobles tangentes de una curva de cuarto orden, los complejos de Steiner, pares complejos y complejos triples, los sistemas de sietes de Aronhold, el algoritmo de Hesse-Cayley para designar las tangentes dobles, determinación racional de la curva de una completa, sistemas

de sietes, el Grupo de Galois del problema doble tangente, representación del Grupo, simplicidad del Grupo del problema doble tangente, la realidad de los dobles tangentes, prueba de la existencia de los cuatro casos

Sección XIII -Teoría general de las ecuaciones de quinto grado: la pregunta (relativa a la cuestión de la Grupo de sustitución lineal del menor número posible de dimensiones), teorema de Lüroth, resolventes con un parámetro, Grupo de resolventes con un parámetro, el icosaedro, los resolventes de la icosaédrica, el resolutivo canónica del quinto grado, resolventes del sexto grado, la solución de la ecuación icosaédrica por funciones trascendentales.

Sección XIV Grupos de sustituciones ternarias lineales: Grupos de sustituciones lineales ternarias de 168 grados, polos y ejes de los Grupos ternarios, aplicación en el GrupoG_{168}, siete veces Polo, los ejes principales, los tres-y seis veces polos, la configuración del GrupoG_{168}, curva invariante del GrupoG_{168}, la primera invariante del GrupoG_{168} y la curva de base, los invariantes mayores, el sistema completo de invariantes.

Sección XV -El problema de la forma del GrupoG_{168} y la teoría ecuaciones de séptimo grado: los resolventes del problema de forma, reducción del séptimo grado resolutivo general sobre la especial, Grupo de la permutación de siete dígitos de grado 168, ecuaciones séptimo grado con un Grupo 168 grado, Grupos contra gradiente, solución de la ecuación de séptimo grado con el Grupo$P_{168,}$ Pj a través del problema de moho del GrupoG_{168}, posibilidad de determinar las funciones de X_1, X_2, X_3.

Cuarto libro: Números algebraicos. Sección XVI -Números y Funciones de un Cuerpo algebraico: definición de los números algebraicos, todos los números algebraicos, Cuerpo algebraico, funciones integradas en un Cuerpo algebraico, el funciones de un Cuerpo algebraico Ω y la extendida, Cuerpo $\overline{\Omega}$, función entera, la divisibilidad, asociación funcional, unidades, máximo común divisor, función prima en el Cuerpo Ω, la separación de conjunto y funciones en factores primos, funciones integradas en el Cuerpo Ω, los factores primos de los números del Cuerpo Ω.

Sección XVII -Teoría algebraica de Cuerpos: bases de un campo de números algebraicos, discriminante, la base mínima y el Cuerpo discriminante, las bases de la funciones, la norma absoluta de funciones, sistema Eest completo de cualquier módulo, congruencias, el teorema de Fermat, los ideales de Dedekind, equivalencia, el número de clase del Cuerpo Ω,el Grupo de clases de ideales.

Sección XVIII Discriminantes: mínimo de una forma cuadrática, aplicación a campos algebraicos, factores primos de los números primos naturales, el teorema de Dedekind en el Cuerpo discriminante.

Sección XIX -Relación de un Cuerpo sobre su divisor: normas relativas, ideales primos en Cuerpo relativamente normal, raíces primitivas de ideales primos, el ideal base parcial, los ideales de la teoría de los divisores primarios del Cuerpo Ω.

Sección XX -Cuerpo cuadrado: bases de un Cuerpo cuadrático, los ideales primos enΩ, funciones en el Cuerpo cuadrado y de irracionales cuadráticos, los números irracionales, equivalentes funcionales y números equivalentes, composición de los irracionales cuadráticos.

Sección XXI -Campos ciclotómicos: la descomposición de q en primer ciclotómico campos Ωq^x, base mínima del Cuerpo Ω_m, los ideales primos en el Cuerpo Ω_m, los ideales primos conjugados, presentación de los factores primos de p, el teorema Kummer, las raíces de la unidad en el Cuerpo Ω_m, el contenido en Ω_m Cuerpo real Hm, los ideales primos del Hm Cuerpo, las unidades del Cuerpo Hm.

Sección XXII Cuerpo abeliano y Campos ciclotómicos: Cuerpo abeliano simple, los resolventes, preparación para pruebas, la prueba de las primeras mitades para m impar, prueba de las segundas mitades de la serie para m impar, preliminar en el caso de un m.

Sección XXIII Número de clases: el teorema de las unidades de Dirichlet, Sistemas de unidades y exponentes de sistemas independientes, Sistemas fundamentales de unidades, números reducibles, límite de un número de enteros divisibles por un ideal de Cuerpo Ω, determinar el volumen, los registros de la teoría de las series, aplicación a la determinación del número de clases.

Sección XXIV Número de Clases de Cuerpos ciclotómicos: representación de número de clases en Cuerpos ciclotómicos Ω_m, determinación de la suma X, sobre el número de clases en el Cuerpo real contenida en Ω_m, número de clases en el Cuerpo de la octava raíces de la unidad, cálculo recurrente del número de clases en Cuerpos Ω_m, si,m es una potencia de 2, el número de clase factor A, el número de clase de factor B, unidades normales en Hm, sistema fundamental de las unidades del Cuerpo Hm, unidades positivas.

Sección XXV Figuras trascendentes: conjuntos numerables, conjuntos no numerables, la trascendencia del número e, trascendencia del número π, la regla general de Lindemann en la función exponencial, los suplementos, irreductibilidad de la ecuación ciclotómica II, la irreductibilidad de la ecuación ciclotómica y el teorema de los números primos contenida en una forma lineal.

3.1.3 Tercer volumen

El tercer volumen está compuesto por veintisiete secciones contenidas en cinco libros. El primer libro: **Parte analítica** se compone de las secciones: las integrales elípticas, las Theta – funciones, la transformación de la theta –funciones, las funciones elípticas, las funciones del módulo, la multiplicación y la división de las funciones elípticas y la teoría de las ecuaciones de transformación. El segundo libro **Cuerpo cuadrado** estudia: los discriminantes, números y formas algebraicas, Ideales en campos cuadráticos, las órdenes en campos cuadráticos, equivalencia según Grupos de números, composición de formas e ideales y las familias de formas cuadráticas. El tercer libro L**a multiplicación compleja** trabaja las funciones elípticas y formas cuadráticas, Grupo de Galois de la ecuación clase, cálculo de los invariantes de clase, la ecuación multiplicador en la multiplicación compleja, las normas de las clases invariantes $f(w)$ y el desarrollo de funciones modulares de Cayley; el cuarto denominado **Cuerpo de la clase** desarrolla la división del Cuerpo ω y el último libro **funciones algebraicas.** Se ocupa de las funciones algebraicas de una variable, funciones, los valores numéricos de funciones algebraicas y las diferencias algebraicas de Abel.

Primer libro. Parte analítica. Primera sección. Las integrales elípticas: definición de las integrales elípticas, relaciones dobles transformación lineal de la diferencia elíptica, la forma normal de Legendre, la forma normal de Weierstrass, curvas elípticas, curvas

elípticas espacio de la cuarta orden, el principio de transformación de Jacobi, la transformación de segundo grado, la transformación de tercer grado, los tres tipos de integrales elípticas, representación de las integrales elípticas por las integrales más básicos, el teorema de adición y origen de las funciones elípticas.

Segunda Sección. Theta –funciones: Requisitos de la teoría de funciones, periodicidad, las funciones T, las relaciones entre las T-funciones, T-funciones de primer orden, ∂-función, la theta -funciones de diferentes características, características principales, el teorema de adición, ∂-derivado las funciones y representación de ∂-funciones por productos infinitos, representación de las cinco funciones de series infinitas y desarrollo de ∂-cociente

Sección Tercera. Transformación de las theta –funciones, el principio de transformación, composición de transformaciones, composición de transformaciones desde simples las transformaciones fundamentales lineales, as transformaciones lineales de las ∂ - funciones fundamentales, el segundo orden de las cinco funciones principales transformaciones, las principales transformaciones de orden impar, las funciones $\eta(w).f(w),\ f_1(w), f_2(w)$ ... , σ-función de Weierstrass , las funciones $\sigma_{00}, \sigma_{01}, \sigma_{10}$, representación de las funciones de σ por $.\partial$ −Funciones, transformaciones lineales de la función $\eta(w)$, transformación lineal de.∂ −Funciones, transformación lineal de las funciones $f(w),\ f_1(w), f_2(w)$ ...

Sección Cuarta. Las funciones elípticas: contexto de las ∂- funciones con las integrales elípticas, funciones elípticas de Jacobi, función de Jacobi $\theta(v),\ H(v)$, otros teoremas de las funciones elípticas, la transformación lineal de la función elíptica, la $\mathfrak{H}$ −función de Weierstrass, la segunda clase trascendente elíptica, la elíptica de tercer género trascendente, las segundas y terceras clases trascendentes de Weierstrass, evoluciones de las funciones elípticas.

Sección Cinco. Las funciones del módulo: las ecuaciones diferenciales elípticas, la variable independiente z^2, ecuación diferencial lineal de K , las soluciones de la ecuación j $(w) = j\ (w')$, las funciones del módulo, representación de funciones elípticas v y z^2, series de potencias para el $\mathfrak{Y}(u), o(u)$- funciones de Weierstrass.

Sección Sexta. La multiplicación y la división de las funciones elípticas, la multiplicación de las funciones elípticas, multiplicación de la función $\mathfrak{P}(u)$, la división por dos, la división por un número impar, la división de los períodos, las relaciones abelianos, el Grupo de Galois de la ecuación ciclotómica, los factores de la ecuación división irreducible, revertir potencias de las ecuaciones por división de ecuaciones de transformación.

Sección VII. Teoría de las ecuaciones de transformación: formación de ecuaciones de transformación, ecuaciones especiales de transformación, segunda presentación de las raíces de las ecuaciones de transformación, las ecuaciones invariantes, ecuaciones de transformación -primera etapa, la ecuación de transformación para γ_2 e γ_3, ecuaciones multiplicadores de la primera etapa, las ecuaciones modulares Schlaefi, la forma de las ecuaciones modulares de Schlaefi, las formas irracionales de ecuaciones modulares, composición del grado de transformación, interpretación geométrica de las ecuaciones modulares irracionales como correspondencias, Sección de la parte posterior, el conjunto de ecuaciones de transformación y la ecuación de quinto grado, el Grupo de Galois de las ecuaciones de transformación para un primer grado, investigación del Grupo T, Subgrupo normal del Grupo ß sin divisores normales de 2, divisor del índice de p para $p = 5, 7, 11$, varios resolventes quinto grado para la transformación de 5º grado,

Segundo libro. Cuerpo cuadrado. Sección Novena. Discriminante: definición de la discriminante, el símbolo Legendre-Jacobi extendida, las sumas de Gauss.

Décima sección. Números y formas algebraicas: los ideales y las formas en Cuerpos algebraicos, clases y clases de ideales, composición de formas y la multiplicación de los ideales.

Sección XI. Ideales en campos cuadráticos, discriminante del campo cuadrática, los ideales y las formas en campos cuadráticas, ideales primos en los campos cuadráticos, representación de números como normas ideales, la reciprocidad cuadrática, formas equivalentes e ideales en campos cuadráticas,

Sección XII. Las disposiciones en campos cuadráticos: disposición de discriminantes, disposición de ideales.

Sección XIII. Equivalencia según Grupos de números: número de Grupos en los ordenados, equivalencia en las órdenes, clases ideal de acuerdo a las órdenes.

Sección XIV. Composición de formas e ideales: composición de los ordenados, composición de las órdenes.

Sección XV. Las familias de formas cuadráticas: representación de números por formas cuadráticas, caracteres y familias de formas cuadráticas, aplicación de símbolo Set umbral, las familias de las clases ideales, composición del Grupo normal, restos estándar de potencias principales, el género de los ideales

Sección XVI. Número de clases en campos cuadráticas: unidades fundamentales en las órdenes, la fórmula límite de Dirichlet, número de Clase de la ecuación modular Schlaefli para el grado 23 de la transformación, los resolventes séptimo y undécimo grado para el séptimo y undécimo grado de transformación

Libro Tercero. La multiplicación compleja. Sección XVII. Funciones elípticas y formas cuadráticas: períodos singulares de funciones doblemente periódicas, los valores singulares de la invariante$j(w)$, relaciones de clases numéricas, naturaleza aritmética de la función de la clase $Hm\,(u)$, composición de formas cuadráticas, el discriminante de la ecuación invariante.

Sección XVIII. Grupo de Galois de la ecuación clase, relaciones entre los invariantes de la clase de igual discriminante, separación de clases opuestas, Irreductibilidad, relaciones entre los invariantes de clase en los distintos órdenes, Cuerpo de la clase y el Cuerpo ordenado.

Sección XIX. Cálculo de los invariantes de clase: la clase γ_2, Los invariantes de clase $f(w)^{24}$, las potencias de $f(w)$ como clase invariante, los primeros casos de cálculo de $f(\overline{l-m})$, aplicación de la transformación de segundo orden para calcular clases invariantes, cálculo de invariantes de clase de la Schläefli, ecuaciones modulares, cálculo de invariantes de clase de las formas irracionales, las ecuaciones modulares, la ecuación modular Schlaefli para el grado 23 de la transformación, los resolventes de séptimo y undécimo grado para el séptimo y undécimo grado de transformación.

Sección XX. La ecuación multiplicador en la multiplicación compleja: la clase invariante $\gamma_3(w)$, los invariantes de clase x^2 y x, grado de la transformación cuadrática, revertir la dirección de discriminantes impares, técnicas que parten de la ecuación de clase para los generadores, ejemplos.

Sección XXI. Las normas de las clases invariantes $f(w)$: la convergencia de una serie infinita, la fórmula límite de Kronecker, las normas de los invariantes de clase $f(w)$, Normas parciales de $f(w)$, cálculo de algunos otros invariantes de clase.

Sección XXII. Desarrollo de funciones modulares de Cayley: límites para $s = 1$, un teorema de la convergencia de la serie, desarrollo de f, f_1, f_2, derivación elemental de los desarrollos, desarrollos de la función $log\ \eta\ (w)$.

Cuarto libro. Cuerpo de la clase: Sección XXIII. La división del Cuerpo: las funciones homogéneas de Weierstrass ver la multiplicación compleja de la función $\wp(u)$, los polos de la función $p\ (uu)$, la función de $t\ (u)$, la división del Cuerpo, la multiplicación de las funciones elípticas para un multiplicador impar, multiplicadores complejos, transición a los módulos singulares, multiplicadores complejos, la descomposición de la función $A\ (x)$, ideales primos, ideales primos de primer grado en ζ_m, número de Grupos y Grupos Ideales, la divisible por un ideal de ideales de las clases principales, las sumas de Dirichlet, el Cuerpo de la clase • , ideales primos en clases, ideales primos en las clases de ideales, Primos en formas lineales, reducción de la ecuación de clase en las partes ciclotómicas, relación de división al Cuerpo de la clase Cuerpo, el número de clase.

Libro Quinto. Funciones algebraicas. Sección XXIV. Funciones algebraicas de una variable: Introductoria, definición de funciones algebraicas, normas y trazas, discriminantes, las cantidades de energía, funciones enteras de z, base mínima y Cuerpo discriminante.

Sección XXV. Funciones: funciones racionales, funciones del Cuerpo $\overline{\Omega}$, funciones enteras del Cuerpo $\overline{\Omega}$, la divisibilidad de funcionales, unidades, máximo común divisor, funciones primas en $\overline{\Omega}$, bases y formas de bases de las funciones, forma de base y la

ramificación funcional, las funciones discontinuas en Ω y el desarrollo de Taylor, transformación birracional.

Sección XXVI. Libro Quinto. Funciones algebraicas. Funciones algebraicas de una variable Funciones Los valores numéricos de las funciones algebraicas: el punto, números atómicos, los polígonos, puntos de ramificación y los números de sucursales, clases de polígonos y clase cociente, Grupos de polígonos, bases normales, diferencial cociente, representación del cociente diferencial por polígono cociente. Generador CuerpoΩ.

Sección XXVII. Diferencias algebraicas de Abel: los diferenciales enΩ, la multitud de polígonos de la primera clase, el teorema Riemann-Roch, diferenciales segundo y tercer tipo, los residuos.

3.1.4 Definición de Grupo y Cuerpo en *Lehrbuch der Algebra*.

Weber antes de definir Grupo de una forma general dice que en su primer volumen muestra la idea de Grupo en torno a las permutaciones y genera a partir de éstas, importantes aplicaciones algebraicas. En este volumen su tarea fue generalizar esas ideas para lo cual establece la siguiente definición de Grupo (ver anexo 1):

> Un sistema P de Objetos (elementos) de alguna clase, forma un Grupo cuando se cumplen las siguientes condiciones:
>
> 1. Hallo una regla de un elemento y de otro elemento del Grupo para determinar un tercer elemento.
>
> Cuando a es el primer elemento, b el segundo elemento y c es el tercer elemento que se determina, simbólicamente se escribe de la forma:
>
> $ab = c$ ó $c = ab,$
>
> y uno llama c como el compuesto de a y de b.
>
> En esa composición no se supone la conmutatividad, es decir, ab y ba pueden ser diferentes.
>
> 2. Se supone la ley asociativa, es decir, cuando a, b y c son tres elementos arbitrarios de P, entonces se tiene
>
> $$(ab)c = a(bc),$$
>
> y por supuesto de aquí se sigue por inducción que eso vale para cualquier número de elementos. Por ejemplo:

$$abcd = (ab)cd = [(ab)c]d = (ab)\{c\ d)$$

$$= a(bc)d = [a(bc)]d = a[(bc)d]$$

$$= ab(cd) = (ab)\ (cd)\ a[b(cd)]^{1}).$$

3. Se supondrá que cuando $ab = ab'$ o $ab = a'b$, entonces necesariamente se tiene en el primer caso que $b = b'$ y en el segundo caso que $a = a'$.

Cuando P tiene un número finito de elementos, el grado del Grupo se dice finito. Se deduce de 1., 2., 3. lo siguiente:

4. Cuando hay tres elementos a, b, c de P entonces se puede determinar un elemento de forma única de tal forma

$$ab = c,$$

Esto es,

Si se dan los elementos a y b entonces las afirmaciones 1. y 4., son la misma cosa. Por el contrario si a y c son dadas, entonces de la composición ab se deja correr todo el sistema P cuyo $grado = n$, entonces uno obtiene de 1. y de 3. en la expresión ab cantidades distintas, elementos diferentes de P, así por esa razón todos los elementos de P deben aparecer, inclusive c. Algo análogo se concluye, si uno permite que a corra en el sistema P o que a tome todos los valores posibles en el sistema P.

Para Grupos infinitos no se puede seguir la misma argumentación. En los Grupos infinitos la propiedad 4. es una exigencia junto con la determinación de los elementos. (Dirichlet y Dedekind –Lecciones sobre teoría de números).

En los Grupos de permutaciones del primer tomo se pueden reconocer fácilmente las ideas generales de los Grupos.

De la definición de Grupos sacamos una conclusión general.

Según 4. para cada elemento b existe un elemento e en P tal que

$$eb = b$$

ese elemento e es independiente de b; de (1) se sigue que para cualquier c,

$$ebc = bc,$$

y bc representan cualquier elemento de P. De la misma manera existe un elemento e' para cada b que satisface la condición

$$be' = b$$

ese elemento e' es diferente de e pues si escribimos $b = e'$ en (1) y $b = e$ en (2) entonces se tiene $ee' = e'\ y\ ee' = e$ en consecuencia $e = e'$.

En otras palabras el elemento e no cambia nada cuando se compone con otro elemento del Grupo y se llamará la unidad. En muchos casos sin que haya peligro de mala interpretación simplemente escribamos "1".

Para cada elemento a hay un elemento, según (4), muy bien determinado que se llama a^{-1}, que satisface la siguiente condición

$a^{-1}a = e$

De la ecuación (3), (1) y (2) se sigue

$$a^{-1}aa^{-1} = ea^{-1} = a^{-1} = a^{-1}e,$$

Y por consiguiente de (3) se tiene que

(4) $$aa^{-1} = e$$

Los elementos a y a^{-1} se dice que el uno es reciproco del otro.

En algunos casos particulares vale la ley de la conmutatividad para los elementos del Grupo P, eso quiere decir que para dos elementos cualesquiera del Grupo se tiene que

$ab = ba.$

5. Los Grupos que tienen esa propiedad se llaman conmutativos, también se les llama Grupos Abelianos.

Cuando los elementos de dos Grupos

$a, b, c, d...$

Y $$a', b', c', d'...$$

están relacionados de forma univoca de manera que siempre que se tiene $ab = c$, debe tenerse que $a'b' = c'$ entonces, los dos Grupos se llaman isomorfos, y por supuesto es evidente el teorema que dice que si dos Grupos isomorfos son isomorfos a un tercer Grupo entonces todos son isomorfos entre si. Uno puede tener todos los Grupos isomorfos en una sola clase que otra ves es un Grupo. Los elementos de ese Grupo son clases de equivalencia. Los elementos de los Grupos que son isomorfos simplemente se ven como representantes de las clases de equivalencia. (pp. 3-6, §.1, tomo II)

Weber define un Grupo como un sistema finito o infinito de elementos dotados de una regla de composición (una operación) que se supone cerrada, sin suponer para ésta que sea también uniforme, que es asociativa, por derecha e izquierda cancelables, pero, en general, no conmutativa. La existencia de una unidad para el sistema y de un elemento inverso para cada elemento del sistema se ha demostrado como consecuencias de los axiomas. Sin embargo no es clara la idea de "muy bien determinado" cuando habla del elemento inverso,

en tanto no se sabe si hace referencia al carácter de unicidad de la inversa. Weber también define la noción de isomorfismo y declara que dos Grupos isomorfos pueden ser considerados como representación de un concepto genérico (*Gattungsbegriff*).

Por lo tanto, no importa si se tiene en cuenta uno u otro representante específico, mientras que se mantengan las propiedades del Grupo.

La parte del libro de Weber dedicado a la teoría de Galois incluye la definición de Cuerpo dada por Dedekind en lecciones sobre teoría de números de 1871: Definición: (Ver anexo 2) Un sistema de números se llama un Cuerpo de números, cuando es cerrado y completo en el sentido en que las cuatro operaciones fundamentales suma, sustracción, multiplicación y división; se puedan hacer con cualquier elemento del sistema, con la única excepción de la división por cero, y el resultado este dentro del sistema. (p. 449)

Weber dice después de expresar la definición de Cuerpo que efectivamente esa idea fue introducida por Dedekind en sus lecciones sobre teoría de números. Argumenta también que los Cuerpos son el álgebra de mayor importancia y que el significado de Cuerpo de números se construye a partir de numerosas analogías hechas por Dedekind sobre el Cuerpo (corpus, corps) en un sentido análogo al de completes o unión de de distintas cosas. Luego expresa que:

> La idea de número se puede generalizar a cosas más grandes donde simplemente se dan las reglas de las operaciones, ya mencionadas, en especial las funciones racionales de alguna variable. (p.449)

Al respecto añade que se va referir luego al Cuerpo de funciones como un sistema de funciones de una o más variables que tienen la propiedad que las operaciones fundamentales pueden ser cerradas y como siempre se exceptúa la división por cero. Define a continuación Cuerpo de funciones de la siguiente manera:

> Una función de un Cuerpo de funciones es la función nula cuando se vuelve cero para todos los posibles valores de la variable. Entonces dado que nosotros no queremos limitar los conceptos vamos a referirnos a Cuerpos y a sus objetos bien sean números o funciones y a sus elementos como elementos del Cuerpo. Un Cuerpo es entonces, un sistema de cantidades con la propiedad de la completitud en el sentido que se puede sumar, restar, multiplicar y dividir entre estas cantidades. Cuando todas las cantidades de un Cuerpo están incluidas en otro Cuerpo, entonces se dice que el primer Cuerpo es parte del segundo Cuerpo.
>
> Si Ω es un subcuerpo (theiler) de Ω', también diremos que Ω' es un Cuerpo sobre Ω. hablando estrictamente de la cantidad cero en si es un Cuerpo (Cuerpo trivial) pero

nosotros no nos vamos a ocupar de esto. El ejemplo típico y natural de un Cuerpo son precisamente los números racionales. Este Cuerpo (los números racionales) es un subcuerpo de cualquier otro Cuerpo. Cada Cuerpo contiene por lo menos un elemento no cero $\frac{\Omega}{\Omega} = 1,$ es decir, el número 1 así como todos los demás números enteros y todas las fracciones están en ese Cuerpo. Otro ejemplo de Cuerpo es la idea de los números en donde $i = \sqrt{-1}$, x, y sean números racionales e irracionales llamados los reales. Como ejemplo de un Cuerpo de funciones uno puede mencionar las funciones racionales de una variable incluidas las constantes. (pp. 450-451)

3.1.4*Álgebra Moderna* de van der Waerden (Modern algebra)

Van der Waerden reconoce que la escuela formalista[43], permitió el surgimiento de una serie de nuevos conceptos e interrelaciones de gran alcance especialmente en las teorías de Cuerpos, ideales, Grupos y números hipercomplejos que hasta ese momento permanecían ocultas a gran parte de la comunidad matemática. El propósito de Van der Waerden al escribir su obra era introducir al lector en todo este mundo de los nuevos conceptos en donde los resultados y métodos clásicos encontraban su debido lugar bajo el enfoque de la escuela formal, abstracta o axiomática que propuso de alguna manera Hilbert.

Buscó entonces presentar y desarrollar con suficiente claridad y actualidad los puntos de vista generales que dominan la concepción "abstracta" del álgebra, mediante los nuevos fundamentos de la teoría de Grupos del álgebra elemental, el álgebra clásica, y la teoría de Cuerpos principalmente extraídos de los cursos y publicaciones de Emil Artin y Emmy Noether. Además proporcionar al lector una obra en lo posible autocontenida, por ejemplo para familiarizarse con la teoría general de los ideales o con la teoría de los números hipercomplejos se puede según el autor, prescindir del estudio de la teoría de Galois, y viceversa; y para consultar en el libro sobre la eliminación o el álgebra lineal no se necesita ser disuadidos por términos complicados de la teoría de ideales.

43La escuela formalista presenta sus resultados matemáticos dentro de un "sistema formal", compuesto por un conjunto de proposiciones llamadas axiomas que se asumen como verdades y que no necesitan demostración y una serie de reglas para unirlas, que dan origen a otras proposiciones llamadas teoremas, los cuales son demostrados a partir de los axiomas.

Por esta razón, los temas fueron distribuidos de tal manera que los tres primeros capítulos mostraran una exposición concisa de lo que es requisito previo para todos los capítulos siguientes. Dicha distribución es la siguiente: Los fundamentos de la teoría de conjuntos, los Grupos, los anillos e ideales y la teoría de Cuerpos. Los restantes capítulos del primer volumen son en su mayoría dedicados a la teoría de los Cuerpos conmutativos y se basan principalmente en el tratado fundamental de Steinitz en Crelles Journal, vol. 137 (1910). La teoría de módulos anillos, e ideales con aplicaciones a las eliminaciones son tratados en el segundo volumen en varios capítulos, en su mayoría independientes.

La teoría de las funciones algebraicas y la teoría de Grupos continuos tuvieron que ser omitidos en la segunda edición, ya que un tratamiento adecuado de ambos, según van der Waerden, implicaba conceptos y métodos trascendentales. Debido a su extensión, la teoría de invariantes no se incluyó en esta edición, tampoco los determinantes puesto que se suponen conocidos.

La obra de van der Waerden está formado por dos tomos cuya tabla de contenidos es la siguiente:

3.2.1 Tomo I:

Capítulo I: Números y Conjuntos: Conjuntos, aplicaciones, Cardinalidad, el número natural, conjuntos finitos y numerables y particiones.

Capítulo II: Grupos: El concepto de Grupo, Subgrupos, complejos, clases, isomorfismos, y automorfismos, homomorfismos, subgrupos normales y Grupo cociente.

Capítulo III: Anillos y Cuerpos: Anillos, homomorfismos e isomorfismos, el concepto de Cuerpo de cocientes, espacio vectorial y sistemas hipercomplejos, Anillo de polinomios, ideales, el anillo de clases de residuos, divisibilidad, ideales primos, anillos euclidianos, anillos ideales principales, factorización.

Capítulo IV: Polinomios: diferenciación, los ceros de un polinomio, fórmulas de interpolación, factorización, criterios de irreductibilidad, factorización en un número finito de pasos, funciones simétricas, resultante de dos polinomios, la resultante como función simétrica de las raíces y descomposición en fracciones simples.

Capítulo V: Teoría de Campos: subcuerpos, Cuerpos primos, adjunción, extensión simple de un Cuerpo, extensión finita de un Cuerpo, dependencia lineal de Cuerpos asimétricos, ecuación lineal sobre Cuerpos asimétricos, extensiones algebraicas de un Cuerpo, raíces de la unidad, campos de Galois (Cuerpos finitos conmutativos), extensiones separables y no separables, Cuerpos perfectos e imperfectos, simplicidad de extensiones algebraicas, teorema del elemento primitivo, operaciones de la teoría de Cuerpos en un número finito de conjuntos.

Capítulo VI: Continuación de la teoría de Grupos: Grupos con operadores, el operador isomorfismo y el operador homomorfismo, las dos leyes de isomorfismo, series normales y series composición, Grupos de orden P^n, producto directo, carácter de G, simplicidad del Grupo alternado, transitividad y primitividad.

Capítulo VII: Teoría de Galois: el Grupo de Galois, el teorema fundamental de la teoría de Galois, Grupos conjugados, Cuerpos conjugados y elementos, Cuerpos ciclotómicos, el periodo de una ecuación ciclotómica, Cuerpos cíclicos, y ecuaciones puras, solución de ecuaciones mediante radicales, ecuación general de grado n, ecuaciones de segundo, tercer y cuarto grado, construcciones con regla y compás, cálculo del Grupo de Galois, ecuaciones de un Grupo simétrico.

Capítulo VIII: Extensiones infinitas de Cuerpos: Cuerpos algebraicamente cerrados, extensiones simples trascendentes, el grado de trascendencia, diferenciación de funciones Algebraicas.

Capítulo IX: Cuerpos Reales: Cuerpos ordenados, definición de números Real, ceros de funciones reales, el Cuerpo de los números complejos, teoría algebraica de los Cuerpos reales, teorema de existencia para campos reales formales, sumas de cuadrados.

Capitulo X: Cuerpos con valoraciones: valoraciones, extensión de Cuerpos completos, valoración de Cuerpos de números racionales, valoración de la extensión de Cuerpos algebraicos, valoración del número de Cuerpos algebraicos.

3.2.2 Tomo II.

Capítulo XII: Álgebra Lineal: módulos sobre un anillo, módulos sobre anillo euclidianos, divisores elementales, teorema fundamental de los Grupos abelianos, representaciones y representaciones modulares, formas normales de una matriz en un Cuerpo conmutativo, divisores elementales y funciones características, formas cuadráticas y hermitianas, formas bilineales anti simétricas.

Capítulo XIII: Álgebras: sumas directas e intersecciones, ejemplos de álgebras, productos y productos cruzados, las álgebras como Grupos con operadores, módulos y representaciones, radicales, producto Star ($a * b = a + b - ab$), anillos con condición minimal, descomposiciones laterales y centrales, anillos simples y primitivos, el anillo de endomorfismos de una suma directa, teorema de estructura para anillos semisimples y simples, el comportamiento de las álgebras bajo la extensión del Cuerpo base.

Capítulo XIV: Teoría de la representación de Grupos y álgebras: exposición del problema, representación de álgebras, representación del centro, trazas y caracteres, representaciones de Grupos finitos, carácter de un Grupo, la representación de los Grupos simétricos, carácter de un Grupo, la representación de los Grupos simétricos, semigrupos de transformaciones lineales, dobles módulos y productos de álgebras, campo de descomposición de un álgebra simple, el Grupo de Bauer, sistemas multiplicativos.

Capítulo XV: Teoría general de ideales y anillos conmutativos: anillos conmutativos: anillos noetherianos, producto y cociente de ideales, ideales primos y primarios, el teorema general de descomposición, el primer teorema de unicidad, componentes aisladas y potencias simbólicas, teoría de ideales relativamente primos, ideales simples-primos, anillos cociente, intersección de todas las potencias de un ideal, la longitud de un ideal primario, cadenas de ideales en un anillo noetheriano.

Capítulo XVI: Teoría de ideales de polinomios: variedades algebraicas, el campo universal, ceros de un ideal primo, la dimensión, el teorema de los ceros de Hilbert, sistemas resultantes para ecuaciones homogéneas, ideales primarios, teorema de Noether, reducción de ideales multidimensionales a ideales cero dimensionales.

Capítulo XVII. Elementos algebraicos enteros: R-módulos finitos, elementos enteros sobre un anillo, los elementos enteros de un Cuerpo, fundamentos axiomáticos de la teoría clásica de ideales, inversión y extensión de los resultados, ideales fraccionarios, teoría de ideales de un dominio entero arbitrario integradamente cerrado.

Capítulo XVIII: Funciones Algebraicas de una Variable: desarrollo en serie en la variable uniformizada, divisores y múltiplos, la clase G, vectores y covectores, diferenciales, el teorema de los índices espaciales, el teorema de Riemann –Roch, generación separable de campos de funciones, diferenciales o integrales en el caso clásico, prueba del teorema de los residuos.

Capítulo XIX: Álgebra topológica: el concepto de espacio topológico, clase de entornos, continuidad, limites, axioma de separación y numerabilidad, Grupos topológicos, entornos de la unidad, subgrupos y Grupo cociente-anillos, T-Cuerpos, compleción de un Grupo mediante filtros de Cauchy, espacios vectoriales topológicos, compleción de Cuerpos.

3.2.3 Definición de Grupo y Cuerpo en *Modern Algebra*:

El concepto de Grupo en van der Waerden no depende del nombre de la operación del Grupo que bien puede ser la adición de números en lugar de la multiplicación, siempre y cuando los postulados de 1 a 4 se cumplan como en la definición de Weber donde recae sobre las operaciones de suma, sustracción, multiplicación y división un especial interés, como se observa en la siguiente definición:

> Definición: un conjunto no vacío $\mathfrak{G}$ con cualquier tipo de elementos (como números, mapeos, transformaciones) se dice que es un Grupo si se cumplen los cuatro postulados siguientes:
>
> Una regla de composición dada que asocia a cada par de elementos a, b of $\mathfrak{G}$ un tercer elemento del mismo conjunto, que frecuentemente se llama un producto de a y b y se denota por ab o $a.b$ (el producto puede depender del orden en que están dispuestos los factores; ab puede o no puede ser igual a ba).
>
> La ley asociativa: Si a, b, c son los elementos de $\mathfrak{G}$, entonces
>
> $$ab.c = a.bc.$$
>
> Existe (al menos) un elemento e en $\mathfrak{G}$, llamado la identidad (por izquierda), de manera que

$ea = a$ para cada elemento de $\mathfrak{G}$.

Si a es un elemento de $\mathfrak{G}$, existe (al menos) un elemento a^{-1}en $\mathfrak{G}$, (por izquierda) llamado la inversa de a, de tal manera que

$$a^{-1}a = e.$$

Un Grupo se llama abeliano

si ab es siempre igual a ba (ley conmutativa) (p.11).

Esta definición es expresada por van der Waerden en términos sintéticos, se observa en ésta una total independencia de los objetos de estudio pues los elementos son de cualquier tipo. La importancia recae en este caso en las propiedades de Grupo y una regla de composición, la cual en términos modernos sugiere la calidad de operación, sin embargo es posible observar que no incluye como condición de Grupo, la propiedad de uniforme y además desconoce la unicidad de la inversa. Luego de dar esta definición van der Waerden como se acostumbra define en el mismo capítulo subgrupo, isomorfismo y automorfismos, homomorfismo, divisor normal y Grupo factor. El concepto de *Cuerpo* lo define a partir del concepto de *anillo* de la siguiente manera:

Se entenderá por *sistema de doble composición* un conjunto de elementos en los que para cualquier par de elementos $a, b, \ldots$, una suma $a + b$ y un producto $a.b$ pertenecen al conjunto, en el cual están definidos de forma exclusiva.

Un sistema de doble composición se llama anillo si se satisfacen para todos los elementos del sistema las siguientes reglas de formación:

I. Leyes de adición
   a) Ley asociativa: $a + (b + c) = (a + b) + c$.
   b) Ley conmutativa: $a + b = b + a$.
   c) Solubilidad de la ecuación $a + x = b$ para toda a, b.

II. Leyes de la multiplicación.
   a) Ley asociativa: $a.bc = ab.c$.

III. Leyes distributivas.
   a) $a.(b + c) = ab + ac$.
   b) $(b + c).a = ba + ca$.

Además. Un anillo es llamado conmutativo si la ley conmutativa se cumple para la multiplicación.

II. b)$a.b = b.a$.

[...]

Cuerpos. Un anillo se llama campo ($skew\ field$[44]) si:

a) contiene al menos un elemento distinto de cero,

b) siempre hay una solución para las ecuaciones

$$ax = b,$$

$$ya = b.$$

Para $a \neq 0$.

Si para la adición estos anillos son conmutativos, estos simplemente son llamados Cuerpos de un dominio de racionalidad, en ocasiones Cuerpos conmutativos.

Para a) y b) probamos, justamente como para Grupos:

c) La existencia de la identidad por izquierda; para solucionar la ecuación $xa = a$ para $a \neq 0$, y llamar a la solución e. para un b arbitrario, de la solución $ax = b$; se deduce que:

$$eb = eax = ax = b.$$

Similarmente la existencia por derecha de un anillo de identidad puede ser probada, y así se ha demostrado la existencia de la identidad.

d) La existencia por izquierda de la inversa a^{-1} para toda $a \neq 0$. Como en el caso de los Grupos, se puede demostrar que la inversa por la izquierda es al mismo tiempo una inversa por derecha. Como en el caso de Grupos, podemos mostrar que, a la inversa, b) se sigue de c) y d). (pp. 32-37).

Van der Waerden define como se puede ver el concepto de Cuerpo a partir de los anillos como se hace actualmente. Esto es posible a que en ese entonces los desarrollos encontrados en las investigaciones de Hilbert, Artin y Noether se encontraban en un estado bastante avanzado. La proeza de este autor fue precisamente dotar su obra de la mayor actualidad posible en estos temas. Para van der Waerden las propiedades de Grupo, anillo y Cuerpo son las que tienen importancia puesto que basta con tener una regla de composición

[44] Literalmente las palabras s*kew field* traduce campos de inclinación pero de acuerdo a los elementos de la definición esta se refiere a los anillos de división. Los anillos de división solían ser llamados "campos" como un término genérico. En muchos idiomas, una palabra que significa "Cuerpo" se utiliza para los anillos de división, en otros designan anillos de división a todos los "skew fields" y hacen una distinción entre los campos conmutativos y no conmutativos. También designan campos específicamente a los anillos de división conmutativos (a los que ahora se les denomina campos en inglés). Modernamente se dice que un Cuerpo es un anillo de división conmutativo y unitario en el que todo elemento distinto de cero es invertible respecto del producto.

para los Grupos y una de doble composición para los anillos y campos. Estas reglas de composición se llaman suma y producto. Cada una de las propiedades es explicada por este de la siguiente manera:

RESPECTO A LAS LEYES DE ADICIÓN. Las tres leyes a, b, c se limitan a afirmar que los elementos del anillo forman un Grupo abeliano bajo la adición. En consecuencia, podemos aplicar a todos los anillos los teoremas probados para el Grupo abeliano. Existe un (y sólo uno) elemento cero 0, tal que:

$a + 0 = a$ para toda a.

Además, para cada elemento de a, existe una -a negativa tal que

$$-a + a = 0.$$

Además, la ecuación $a + x = b$ no sólo es soluble, pero la solución es única; su única solución es

$$x = -a + b;$$

Que denotamos también por $b - a$. En virtud de

$$a - b = a + (-b)$$

Cualquier diferencia puede escribirse como una suma. En este sentido, para hacer la suma las diferencias obedecen a las mismas reglas para permutar términos; $(a - b) - c = (a - c) - b$, Etcétera.

Finalmente – $a(-a) = a$ y $a - a = 0$.

RESPECTO A LAS LEYES DE ASOCIATIVIDAD. Es posible, sobre la base de la ley asociativa para la multiplicación, definir

$$\prod_{1}^{n} a_v = a_1 a_2 \dots a_n$$

Y para demostrar su propiedad característica

$$\prod_{1}^{m} a_\mu \cdot \prod_{v=1}^{n} a_{m+v} = \prod_{1}^{m+n} a_v$$

Del mismo modo, definimos las sumas

$$\sum_{1}^{n} a_v = a_1 + a_2 + \cdots + a_n$$

Y demostrar su propiedad característica

$$\sum_{1}^{m} a_\mu + \sum_{v=1}^{n} a_{m+v} = \sum_{1}^{m+n} a_v$$

En virtud de Ib, los términos de una suma se pueden intercambiar a voluntad, y en los anillos conmutativos lo mismo se puede hacer para los productos.

RESPECTO A LAS LEYES DE DISTRIBUTIVIDAD. Siempre que la ley conmutativa de la multiplicación se cumpla. IIIb es por supuesto, una consecuencia de IIIa.

Por inducción sobre n se sigue inmediatamente de IIIa que

$$a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n,$$

Y para IIIb que

$$(a_1 + a_2 + \cdots + a_n)b = a_1 b + a_2 b + \cdots + a_n b.$$

De la combinación de estas dos relaciones, obtenemos la conocida regla de la multiplicación de las sumas:

$$(a_1 + \cdots + a_n)(b_1 + \cdots + b_m)$$

$$= a_1 b_1 + \cdots + a_1 b_m$$

$$+ \cdots + a_n b_1 + \cdots + a_n b_m$$

$$= \sum_{i=1}^{n} \sum_{k=1}^{m} a_i b_k$$

Las leyes distributivas se cumplen para la resta y,

$$a(b - c) = ab - ac,$$

Como puede verse a partir

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

En particular

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

En otras palabras: Un producto es cero siempre que uno de los factores sea cero.

La inversa de este teorema no es necesariamente cierta, como se verá a partir de ejemplos que se muestran a continuación. Puede suceder que

$a.b = 0,$ donde $a \neq 0,\ b \neq 0.$

En tal caso a y b se llaman divisores cero o divisores de cero, a se encuentra a la izquierda y b a la derecha del cero divisor. (En los anillos conmutativos estas dos definiciones coinciden).

Por conveniencia propia se considera un divisor de cero. Por lo tanto esto implica $a = 0 \quad ó \; b = 0$, el anillo se llama un anillo sin divisor de cero. Si, por otra parte, el anillo es conmutativo, también se conoce como un dominio de integridad.

LA IDENTIDAD. Si un anillo tiene una identidad e por izquierda,

$ex = x$ para toda x,

Y simultáneamente e' es la identidad por derecha,

$xe' = x$ para toda x,

Las dos identidades resultan ser iguales, entonces

$$e = ee' = e'.$$

Luego toda identidad por derecha es igual a e, y así es toda identidad por izquierda. Entonces e se llama simplemente la identidad, y un anillo que contiene un elemento de este tipo se llama un anillo con el elemento unidad. Con frecuencia, la identidad se denota por 1, aunque tiene que ser distinguido del número 1.

Los enteros forman un anillo C con la identidad; los números pares, un anillo sin identidad. Hay también anillos con uno o más identidades adecuadas, pero sin una identidad izquierda, o viceversa.

EL ELEMENTO INVERSA. Si a es un elemento arbitrario de un anillo con identidad e, entonces, por la inversa por izquierda de a comprenderemos un elemento a_i^{-1} de tal manera que

$$a_i^{-1}a = e,$$

Y por la inversa por derecha de $a$un elemento a_r^{-1} tal que:

$$a_i^{-1}a_r^{-1} = e.$$

Si en el elemento a tiene tanto a la izquierda y la derecha inversa, entonces ambos son iguales, ya que

$$a_{(i)}^{-1} = a_{(i)}^{-1}\left(aa_{(r)}^{-1}\right) = (a_{(i)}^{-1}a)a_{(r)}^{-1} = a_{(r)}^{-1}$$

Y por lo tanto, cada inversa derecha, así como cada una izquierda de a es igual a éste. En este caso se dice: a posee un elemento inverso, y se denota la inversa a^{-1}.

POTENCIAS Y MÚLTIPLOS. En virtud de la ley asociativa, los potencias a^n (n es un entero positivo) puede ser definida para cada elemento del anillo de a, cumplen siguientes reglas:

$$a^n.a^m = a^{n+m},$$

$$(a^n)^m = a^{n.m},$$

$$(ab)^n = a^n b^m,$$

La última igualdad se cumple por los anillos conmutativos.

Si el anillo tiene a la identidad, y si a tiene inversa, se introduce el grado cero y potencias negativas (artículo 6); las normas (1) siguen siendo válidas.

Dado que cualquier anillo está en el Grupo aditivo múltiple

$n.a$ ($= a + a + \cdots a$, con n términos) se puede definir, y tendremos:

$$na + ma = (n + m)a,$$

$$n.ma = nm.a,$$

$$n(a + b) = na + nb,$$

$$n.ab = na.b = a.nb.$$

Si definimos

$$(-n).a = -an.$$

Así como para los potencias, las reglas (2) se mantienen durante todo n y m integral (positivos, negativos o cero).

La expresión na no debe ser considerada como un producto real de dos elementos en el anillo; por lo general, n no es un elemento del anillo, pero sí se introduce desde el exterior: un entero. Sin embargo, si el anillo tiene la identidad e, na se puede escribir como un producto real, a saber $na = n.ea = ne.a$. (pp. 33-35).

Capítulo 4.

REFLEXIONES y CONCLUSIONES

La historia nos revela en este trabajo momentos muy importantes, en los cuales las nuevas ideas surgen como piezas que entran a asociarse con un objetivo común. Sin saber si son parte de un proyecto de mayor envergadura que pueda dilucidar el matemático cuando intenta solucionar un problema particular. Al estudiar la trayectoria y los acontecimientos vinculados a las distintas etapas de las nociones de *Grupo* y *Cuerpo* como "herramientas" fue posible observar este camino. Por ejemplo la introducción de un nuevo simbolismo algebraico permitió, entre otras cosas, que las operaciones en la resolución de ecuaciones se hicieran más visibles y de esa forma se diera un paso decisivo en los procesos de generalización.

Las ecuaciones generales de tercer y cuarto grado al lado de la primera aproximación al teorema fundamental del álgebra por Descartes, hizo que varios matemáticos intentaran resolver las ecuaciones de quinto grado. Y aún con el fracaso en el intento de resolver estas ecuaciones, se encontraron aportes al edificio de las matemáticas que conocemos hoy; nuevos métodos para resolución de ecuaciones cúbicas y cuarticas, en una dependencia totalmente diferente, encontrar funciones cuyas raíces que fueran invariantes por efecto de ciertas permutaciones.

Por primera vez alguien realizaba una asociación entre las soluciones de una ecuación polinómica y las permutaciones de sus raíces y con esto colocaba una piedra angular de la teoría general de ecuaciones. Así mismo, se dio inicio a una manera de estudiar subgrupos de un Grupo de sustituciones. En términos modernos los teoremas sobre funciones no simétricas, son el fundamento del método de Lagrange, que si bien no conduce a la resolución general para $n \gg 5$, como se perseguía en ese momento, preparó la forma para obtener la estructura algebraica que debía adoptar dicho proceso.

Una demostración hizo creer que se cerraba definitivamente el problema de buscar una fórmula para resolver ecuaciones polinómicas por radicales de grado cinco. Sin embargo, no fue así, ya que surgieron nuevos problemas, métodos y demostraciones para abordar la

existencia de ecuaciones de quinto grado o superior a estas, que sí fueran resolubles por radicales. Así se logró obtener una forma más general y menos difícil para identificar las ecuaciones de grado mayor o igual a cinco, resolubles por radicales. Galois examinó ciertas permutaciones de la ecuación $f(x)$ y observó que ellas obedecían a un sistema algebraico que denominó Grupo. Logró a su vez, esquematizar la estructura de cada ecuación en un Grupo, donde se refleja la trama de relaciones entre las raíces.

Quizá muchos entiendan el uso de la palabra Grupo en la teoría de Evariste Galois como la única fuente en que esta noción surgió. Sin embargo, es posible evidenciar en este trabajo que aún sin el empleo del nombre "Grupo" su estructura era una necesidad en los desarrollos que Gauss estaba obteniendo en la teoría de números.

La teoría de números era una serie de resultados aislados, antes de Gauss. Él estableció la notación, sistematizó y extendió la teoría existente; clasificó los problemas e introdujo los métodos conocidos y nuevos que debían ser estudiados. Gauss dedicó gran parte de las *Disquisitiones* a un exhaustivo estudio de las formas cuadráticas binarias y a la representación de los números enteros por tales formas. Estudió el problema de encontrar las raíces de las ecuaciones ciclotómicas, definió una composición en tales formas, y comentó que si K_1 y K_2 son dos de tales formas, uno puede denotar su composición por $K_1 + K_2$. Luego mostró que esta composición es asociativa y conmutativa, que existe una identidad, y que cada forma tiene una inversa, verificando de este modo todas las propiedades de un *Grupo abeliano.*

Los Grupos estaban al servicio de la resolución de esos problemas. No obstante, necesitaban ciertos elementos para atraer la mirada de otros matemáticos. Estos elementos fueron detectados por Dedekind. Su tesón para hilar cosas era extraordinario, pudo trabajar tanto en la teoría de ecuaciones como en la teoría de números, esgrimiendo grandes resultados para ambos ámbitos. Por una parte, encontró una teoría de descomposición que se aplicaría a dominios más generales que enteros algebraicos. Estudió la factorización única y la convirtió en el mecanismo teórico para la definición de nuevos números y entidades. En lugar de trabajar con las raíces de la unidad, formuló una definición más amplia de los números algebraicos e introdujo el concepto de Cuerpo numérico. Por otra parte, analizó de forma independiente los fundamentos de teoría de Grupos (de manera

abstracta) necesarios para la teoría de Galois; además vio la importancia de tener en cuenta, en cada momento de referencia, a un Cuerpo de base y la interrelación entre Cuerpos y Grupos, que constituye el núcleo de la teoría de Galois desde el punto de vista moderno.

Con el establecimiento de un *Cuerpo numérico* mostró que los números algebraicos forman un *Cuerpo*; introdujo entonces la noción de anillo, y probó que los enteros algebraicos formaban precisamente un anillo. Con Dedekind la teoría de Galois se presentó como una consecuencia inmediata del concepto de Cuerpo, que no es sino una extensión del concepto de Grupo, visto como una ley formal, independiente del significado numérico de los elementos relacionados.

Dedekind refleja una unidad metodológica notable de las cuales se pueden mencionar: una clara inclinación a abordar problemas matemáticos, reformulando radicalmente todo el entorno conceptual de los objetos de estudio; y la introducción sistemática de nuevos conceptos. Esto tuvo un papel central en la solución de diferentes problemas, ya que la metodología que Dedekind estableció permitía la clarificación del conocimiento matemático existente. Tomó los Grupos como entidades matemáticas autónomas, en lugar de sus propiedades de Grupo. Nuevos y significativos conceptos se incorporaron a la teoría de Galois; De ese modo, Arthur Cayley reconoció que la noción de Grupo de sustituciones dada por Dedekind podía ser generalizada.

Klein en un contexto totalmente diferente fue el primero en mostrar que la geometría proyectiva es independiente de la teoría de las paralelas, con lo cual surgieron los Grupos de transformaciones. Sus antecesores no habían dilucidado este punto y ni siquiera se habían planteado verdaderamente la cuestión. Klein amplía la naturaleza y el objeto de la Geometría. Realiza por así decirlo una Geometría generalizada que le permite incluir todas las geometrías en ella como casos particulares y restringidos de la misma, constituyendo uno de los factores mayores del advenimiento de la matemática moderna.

Es importante resaltar que el espacio que aparece en la obra de Klein es ahora el objeto de la geometría. Un espacio que determina las propiedades geométricas de los objetos contenidos en él; es decir, un espacio que aparece como condición de estructura. Sin embargo, Klein tiene la ventaja de que ya había surgido para ese entonces los Grupos de

permutaciones y tomó la definición de Grupos finitos derivada de los Grupos de permutaciones dada por Dedekind en 1858 y de Cayley en 1870.

La historia también conduce a mostrar que existen momento en los cuales ideas novedosas no se entienden, la obra de Galois por ejemplo, no fue comprendida en la época en que surgió, y debió esperar hasta 1870 cuando Camille Jordán (1838-1921) aplicó la teoría de Grupos a las ecuaciones algebraicas. Por su parte, el trabajo sistemático de Dedekind, Cayley, Steinitz y Weber sirvieron, en grado sumo para que la comprensión de dicha obra se extendiera a otros campos del saber.

Mediante el uso de los resultados obtenidos por Dedekind sobre la relación entre Grupos y Cuerpos, Weber vio la teoría de Galois no sólo como un análisis de su problema con la solución de sus raíces sino más bien como un examen más general de la interacción entre el Grupo específico y la definición de ciertos Cuerpos. Inició un proceso de sistematización de los métodos, definiciones y teorías necesarias según su propio criterio para la comprensión de la teoría de Galois. Define por primera vez la noción de Cuerpo como una extensión del concepto de Grupo (es decir, mediante la adición de una segunda operación). Al acercarse al concepto de esta manera se puede percibir en toda su generalidad, lo que permite un tratamiento análogo de Cuerpos finitos e infinitos. Los Grupos, Cuerpos finitos e infinitos fueron subsumidos aquí por primera vez bajo una definición única y general (Tomo II).

Mientras que Galois perseguía la resolvente, Weber se fijó más en el Cuerpo; y en esa dirección elaboró Steinitz (1910) su teoría general de Cuerpos algebraicos, despreocupándose de su aplicación a problemas particulares. Lo cual constituye los primeros pasos para el cambio de estatus de las nociones de Grupo y Cuerpo de herramientas a objetos matemáticos independientes de su naturaleza. Este proceso de sistematización de los Cuerpos existentes hasta el momento, posibilitó posteriormente el estudio de los cuerpos por el interés que tenían en si mismos.

La intención de Weber era presentar un resumen que vinculará los diversos aspectos teóricos y múltiples aplicaciones del álgebra de las últimas décadas del siglo XIX. Es posible por tanto, observar su preocupación por dar este recorrido histórico detallado mediante la exposición de los diferentes métodos y definiciones; los cuales perfilaron la

compresión de la teoría de Galois (tomo I) y el surgimiento de una gran cantidad de Grupos y sus aplicaciones en diversos campos de las matemáticas en especial a la geometría y el análisis. También su intención era llevar la teoría de Grupos a un estadio más general, sin embargo, lo que se había avanzado hasta ahora en teoría de ideales y anillos no permitía tal empresa.

Como es posible observar hasta aquí la influencia de Dedekind en esta historia fue fundamental, Weber reconoce que como fuente de inspiración para escribir su obra las lecciones de álgebra y sobre la teoría de Galois de Richard Dedekind.

Después de la famosa monografía de Steinitz (1910) sobre los Cuerpos algebraicos, el gran impulso para la consolidación del concepto de Cuerpo fue dada por Artin en Hamburgo y Emmy Noether en Gôttingen, cuyas creaciones fueron sistematizadas por van der Waerden en su libro de 1930.

Los problemas concernientes a la teoría de números, la teoría de ecuaciones y de las transformaciones convergieron de manera especial en la teoría de invariantes y se preparó el escenario para los Grupos y Cuerpos en el cual su status debían necesariamente cambiar porque la matemática también había cambiado su enfoque, estaba en manos de hombres y mujeres de una nueva escuela, la escuela formalista. La metodología instaurada por Hilbert y Emmy Noether en la teoría de invariantes llevó a un primer plano la necesidad de utilizar la teoría abstracta de los módulos, anillos y Cuerpos. Los problemas de factorización condujo al concepto de ideal y con este se desarrolló la teoría de anillos.

Cuando Emmy Noether centró su atención en el estudio de los ideales, anillos, módulos y otras estructuras aparecen por primera vez los conceptos modernos de anillo, ideal y módulo sobre un anillo; con la particularidad de extender la definición de ideal en un anillo de enteros o en un anillo de polinomios, a *anillos conmutativos* en general. Además, el concepto de la condición de cadena ascendente (CCA) para ideales, usado de manera reiterativa en investigaciones posteriores para la demostración de diversos teoremas.

Según Corry (2004) el trabajo de Emmy Noether en la teoría de los ideales constituye un punto decisivo que conduce a la nueva imagen estructural del álgebra. Y eso es cierto, Noether fue la primera en utilizar la noción de módulo de manera abstracta y de reconocer

su potencial, con un anillo de dominio de operadores. En efecto, es a través de su trabajo que el concepto de módulo se convirtió en un concepto central del álgebra Moderna. De hecho, los módulos son importantes no sólo por su carácter unificador, sino también debido a su poder de linealización. Son, después de todo, las generalizaciones de los espacios vectoriales.

Noether se movió de lo concreto, anillos de polinomios, a lo abstracto, un anillo conmutativo noetheriano; con lo cual obtiene cuatro teoremas de descomposición de ideales, de los cuales el segundo es el de descomposición primaria, conocido como el teorema de Lasker-Noether. Con la descomposición primaria de ideales, Noether introduce el concepto de *ideal primario,* generaliza con este último el concepto de ideal primo, lo cual facilita la obtención de ideales primarios no primos.

La noción de anillo se convirtió después de todo el eje articulador de la teoría de Grupos y Cuerpos, al ser un anillo un Grupo en todos los casos y ser un Cuerpo cuando es un anillo de división. Cuando Emmy Noether se fijo en los ideales de anillos consiguió que estos tuvieran un alcance mucho más amplio que el de ayudar a la factorización única. En la actualidad son los únicos con los que se pueden hacer cocientes de anillos, es decir, reducirlos. Si se toma cociente entre los ideales más grandes, los maximales, quedan trozos de anillo más pequeños. Por ejemplo, en geometría algebraica se arreglan las cosas para que una curva algebraica sea un anillo, y en esta correspondencia los puntos son los ideales maximales. En general se puede asignar un anillo a una variedad algebraica (curvas, superficies, etc. definidas por polinomios) y sus ideales primos corresponden a las subvariedades algebraicas. Las definiciones de epimorfismo, monomorfismo e isomorfismo se pueden aplicar igualmente a Cuerpos, porque un Cuerpo es en particular un anillo con unidad.

En las definiciones de Grupo y Cuerpo de Weber y van der Waerden se presentan algunas diferencias que corresponden específicamente a los objetivos que cada autor perseguía y a los desarrollos a los que la comunidad matemática había tenido. La obra de Weber escrita en un alemán muy culto, muestra una definición de Cuerpo centrada en el uso que inicialmente le dio, la teoría de Galois, en la que los Cuerpos numéricos bastaban para ese propósito. Weber a pesar de esto extiende el concepto de Cuerpo al de funciones y dice que

esto funciona con sistemas más generales, desarrolla en el tercer volumen en el campo de las funciones y la geometría algebraica; y aunque se puede considerar una definición clásica de Cuerpo carece de los desarrollos que permitieron que este concepto tuviera el estatus de objeto matemático. Weber habla de las cuatro operaciones fundamentales (suma, sustracción, multiplicación y división) forma que tuvo su momento histórico y ahora está en desuso.

En la obra de van der Waerden el acento se hace en los axiomas algebraicos y basta con disponer con una regla de composición para Grupos y una de doble composición para Cuerpos. En términos modernos dichas reglas de composición se pueden leer como operaciones n-arias. Para que van der Waerden tuviera esa unidad teórica de las estructuras era necesario desarrollos como los que se encuentran en el tratado de Steinitz sobre Cuerpos. También la generalidad que Emmy Noether encontró a partir de los anillos e ideales pues es desde estos que van der Waerden define los Cuerpos, que en este caso pueden ser de cualquier naturaleza (mapeos, transformaciones) y no sólo números.

En el álgebra de Weber no se habían decantado las ideas sobre Grupos y éste debe de dar demasiados rodeos para convencer al lector que funcionan como tal. Weber no tiene el lenguaje, la terminología ni la notación actual y sin embargo presenta una definición de Grupo que comparada con la de van der Waerden y Heirstein la diferencia estriba básicamente en su carácter sintético.

No obstante, hay que admitir en este punto que las definiciones de grupo en los tres (Weber, van der Waerden y Heirstein) desconocen la propiedad uniforme. Hacen referencia a una operación que solo debe ser clausurativa. Además la inversa no se establece como única, por derecha y por izquierda. Para obedecer a la doble implicación que surge de considerar una operación es necesario lo siguiente:

$$A \times A \to A \qquad i)\ para\ todo\ (a,b) \in A \times A.$$
$$ii)\ existe\ un\ unico * (a,b) \equiv a * b$$

Queda la tarea de revisar otras álgebras y establecer si es un error que se ha reproducido históricamente. En van der Waerden la unicidad de la inversa, se contempla únicamente en la explicación dada para anillos.

Las ideas de Weber revolucionaron al mundo aún sin tener lo que se mencionó anteriormente. La obra de Weber constituye una pieza muy importante en la construcción del conocimiento matemático ya que presenta esos ejemplos que permiten rescatar la estructura de los Cuerpos y Grupos que este autor utilizó, aunque atente contra la intuición como muchos matemáticos contemporáneos consideran cuando esconden estas herramientas a sus estudiantes.

Bajo los nuevos desarrollos del álgebra, que incluyen muchos de los logros de Weber, Van der Waerden en su obra buscó presentar y desarrollar con suficiente claridad y actualidad los puntos de vista generales que dominaron esa nueva concepción "abstracta" del álgebra; mediante los nuevos fundamentos de la teoría de Grupos del álgebra elemental, el álgebra clásica, y la teoría de Cuerpos principalmente extraídos de los cursos y publicaciones de Emil Artin y Emmy Noether. La historia continúo después de esto y es importante seguirla contando, pero por ahora rebaza los objetivos que se plantearon en este trabajo.

Como es posible ver en toda esta historia, el álgebra cambio sustancialmente con el advenimiento de la escuela formalista y con ella cambio la forma de hacer y conocer las matemáticas. Para conocer desde las estructuras es importante decodificar el conocimiento encerrado en ella, sus múltiples ejemplos y eso ha traído como consecuencia nuevas matemáticas. Esta historia es un fiel resultado de procesos deductivos, no de procesos inductivos como tal vez lo ve Morris Kline en *el fracaso de las matemáticas modernas ¿Por qué Juanito no aprende matemáticas?* Esta forma de hacer matemáticos produjo y sigue produciendo mucha matemática.

Para terminar, es preciso decir que si bien no es una conclusión de este trabajo es importante reflexionar sobre la metodología que permitió el logro de los propósitos del mismo. Este trabajo necesitaba de la experiencia y conocimientos tanto de matemáticos como de los que supieran leer textos en alemán en los cuales se encontraban las primeras fuentes. Dio resultado acudir a la comunidad científica, representada por los profesores Jaime Arango, Jorge Duque, Manuel Villegas y Liliana Camargo, quienes además de ayudar a romper las barreras del idioma, mediante una metodología de la indagación respondieron a las dudas epistemológica que en muchos momentos permitían establecer las conexiones y las partes finas en las cuales la discusión era por si misma interesante.

5. REFERENCIAS:

Acero, F. (2008). *Estructura del libro de texto universitario: Un análisis de textos de Álgebra lineal*. Tesis de maestría no publicada. Universidad de San Andrés, Buenos Aires, Argentina. Recuperado el 03 de Octubre de 2013, de http://www.udesa.edu.ar/files/MaeEducacion/Microsoft%20Word%20-%20Resumen%20Acero.pdf

Arenzana, V. (1995). Un libro de Álgebra Moderna que ha hecho historia. [Versión Electrónica], *Revista SUMMA*, (20), 99-104. Recuperado el 30 de septiembre del 2013, de: http://revistasuma.es/IMG/pdf/20/099-104.pdf.

Bauzá, J. (S. F.). *Felix Klein (1849-1925): Su interés para el psicoanálisis lacaniano. I. Presentación del* "Programa de Erlangen". Recuperado el 18 de abril de 2014, *de: http://www.alaletra.com/archivos/erlangen-t.bauza.pdf*

Carrasco, P. (2004). Emmy Noether y el inicio del Álgebra Abstracta. *La Gaceta de la RSME*. Universidad de Granada 7(2), 331–346. Recuperado el 03 de Octubre de 2013, de http://dmle.cindoc.csic.es/pdf/GACETARSME_2004_07_2_01.pdf.

Corrales, C. (2001). *Matemáticas y matemáticas: vida y obra de Emmy Noether*. Universidad de Sevilla. España

_____ (2011). *Número*. Universidad de Complutense. Madrid. Recuperado el marzo 15 de 2014, de:http://www.mat.ucm.es/catedramdeguzman/ideas/documentos/capi.pdf

Corry, L. (1991). *Estructuras algebraicas y textos algebraicos del siglo XIX*. Recuperado el 30 de septiembre del 2013, dehttp://Www.Tau.Ac.Il/~Corry/Publications/Articles/Pdf/Llull.Pdf.

_____ (1996).*Modern Algebra and theeise of mathematical structurs*. Basilea, Birkhaûser.

Dávila, G. (2003). El Desarrollo del Álgebra Moderna. Parte III: el surgimiento del álgebra abstracta. *Apuntes de Historia de las Matemáticas*. 2 (2, mayo 2003). Recuperado el 27 de abril de 2014, de: http://www.mat.uson.mx/depto/publicaciones/apuntes/pdf/2-2-4-algebra3.pdf.

Dedekind, R. (1888*) ¿Que son y para qué sirven los números?* (J. Ferreiros, Trad. 1998). Alianza Editores. Madrid.

De Ríos, M. *(c.f.). Ecuaciones Algebraicas.* Recuperado el 26 de abril de 2014, de*: www.um.es/adelrio/Docencia/**Ecuaciones**/EcuAlg.pdf.*

Español, L. (1998). *Julio Rey Pastor ante los cambios en el álgebra de su tiempo.* Matemática y Región: La Rioja. Universidad de la Rioja. España. Recuperado el 11 de mayo de 2014, de: http://documat.unirioja.es/servlet/autor?codigo=107630

Galina, E. (2003) *Conceptos básicos de Álgebra de Lie*. Universidad Nacional de Córdoba. Recuperado el 22 de febrero del 2014, de http://www2.famaf.unc.edu.ar/publicaciones/documents/serie_b/BMat45-2.pdf.

Gauss, C. (1801). *Disquisitiones Arithmeticae.* (A. Ruiz, Trad.1995) Asociación Costarricense de Historia y Filosofía de la Ciencia. Ciudad Universitaria "Rodrigo Facio". San José de Costa

Rica. Recuperado el 17 de abril de 2014, de: http://epsaleph.tripod.com/sitebuildercontent/sitebuilderfiles/disquisitionesarithmeticae.pdf.

Grandjot, C. (1940). Álgebra Abstracta. *Apartado de la revista universitaria. Año XXV*. Universidad Católica de Chile. (1), 21-58

Gutiérrez, C. & Gutiérrez, F. (2004). *Carlos Grandjot, tres décadas de matemáticas en Chile 1930-1960*. Boletín de la Asociación Matemática Venezolana. XI (1). Recuperado el 4 de Octubre de 2014, de: http://users.dcc.uchile.cl/~cgutierr/hcyt/grandjot.pdf.

Herstein. (1986) I. *Abstract Algebra.* (E. Ojeda, Trad. 1988). Universidad autónoma de Guadalajara. Grupo Editorial Iberoamérica. México.

Kleiner, *I. (*2007*). A history of abstract Algebra.* Birkhâuser Boston York University. Toronto, Canadá.

Kline, Morris. (1976). *El fracaso de la matemáticas moderna ¿por qué Juanito no sabe sumar?* Siglo Veintiuno Editores. España.

_____ (1972a). *El pensamiento Matemático de la antigüedad a nuestros días, II.* Alianza Editorial. Madrid.

_____ (1972b). *El pensamiento Matemático de la Antigüedad a nuestros días, III.* Alianza Editorial. Madrid.

Nocera, P. (2009*).* Discurso, Escritura e Historia en L'idéologie de Destutt de Tracy. Nómadas. *Revista Crítica de Ciencias Sociales y Jurídicas.* 21 (1, 2009). Universidad de Buenos Aires. Recuperado el 11 de mayo de 2014, de: http://pendientedemigracion.ucm.es/info/nomadas/21/pablonocera.pdf

Sánchez, J.M. (2011*) Historia de Matemáticas Abel y la imposibilidad de resolver la "quintica" por radicales.* Revista de investigación Pensamiento matemático. Recuperado 27 de abril de 2014, de: http://www.caminos.upm.es/matematicas/revistapm/.../abel_y_la_quintica.pdf.

van der Waerden, B (1953). *Modern Álgebra*. (F.Ungar, Trad.). New York, USA.

_____(1985). History of Álgebra- Fromal-Khwārizmīto Emmy Noether.*Springer*. Verlag Berlin Heidelberg. Recuperado el 14 de octubre de 2013, de: https://mail.google.com/mail/?shva=1#inbox/141b8c8e4d834ff2?projector=1

Várilly, J. (2006) *M. A. 660- Teorías de Galois*. Escuela de matemáticas. Universidad de Costa Rica. Encontrado el 11 de mayo de 2014, de: http://www.miscelaneamatematica.org/Misc53/5301.pdfhttp://163.178.101.243/claroline/claroline/backends/download.php?url=L0dhbG9pcy5wZGY%3D&cidReset=true&cidReq=MA0660.

Villa, G. (2011). *Las ecuaciones polinomiales como el origen de la teoría de Galois.* Recuperado el 16 de abril de 2014, de: http://www.miscelaneamatematica.org/Misc53/5301.pdf.

Weber, H. (1895). *Lehrbuch der Álgebra.* Volumen I. Beaunschweig. Alemania. Recuperado el 17 de noviembre de 2013, de: https://ia600201.us.archive.org/3/items/lehrbuchderalgeb01weberich/lehrbuchderalgeb01weberich.pdf.

_____ (1896). *Lehrbuch der Álgebra.* Volumen II. Beaunschweig. Alemania. Recuperado el 17 de noviembre de 2013, de: https://ia600201.us.archive.org/3/items/lehrbuchderalgeb01weberich/lehrbuchderalgeb01weberich.pdf.

_____ (1908) *Lehrbuch der Álgebra*. Volumen III. Beaunschweig. Alemania. Recuperado el 17 de noviembre de 2013, de: https://ia600201.us.archive.org/3/items/lehrbuchderalgeb01weberich/lehrbuchderalgeb01weberich.pdf.

Zalamea, F. (2009). *Filosofía sintética de las matemáticas contemporáneas*. Universidad Nacional de Colombia. Editorial Universidad Nacional de Colombia. Recuperado el 11 de mayo de 2014, de: http://acervopeirceano.org/wp-content/uploads/2011/09/Zalamea-Fil-Sint-Mat-Cont.pdf.

6. Anexos

Anexo 1: Definition der Gruppen.

(Weber, 1896, pp.3-6, §.1).

Erster Abschnitt.
Allgemeine Gruppentheorie.
§. 1.
Definition der Gruppen.

Wir haben im ersten Bande bei den Permutationen den Begriff einer Gruppe kennen gelernt und wichtige algebraische Anwendungen von ihm gemacht. Es muss nun unsere nächste Aufgabe sein, diesen in der ganzen neueren Mathematik so überaus wichtigen Begriff allgemeiner zu fassen und die dabei herrschenden Gesetze kennen zu lernen. Wir stellen folgende Definition an die Spitze:
Ein System P von Dingen (Elementen) irgend welcher Art wird zur Gruppe, wenn folgende Voraussetzungen erfüllt sind:

1. Es ist eine Vorschrift gegeben, nach der aus einem ersten und einem zweiten Elemente des Systems ein ganz bestimmtes drittes Element desselben Systems abgeleitet wird.
   Man schreibt symbolisch, wenn a das erste, b das zweite, c das dritte Element ist:
   $$ab = c, \qquad c = ab,$$
   und nennt c aus a und b componirt und a und b die Componenten von c.
   Bei dieser Composition wird im Allgemeinen nicht das
   commutative Gesetz vorausgesetzt, d. h. es kann ab von ba verschieden sein, dagegen wird.

2. das associative Gesetz vorausgesetzt, d. h. wenn a, b, c irgend drei Elemente aus P sind, so ist
   $$(ab)c = a(bc),$$

   und hieraus folgt durch die Schlussweise der vollständigen Induction, dass man immer zu demselben Resultate kommt, wenn man in einer beliebigen Reihe von Elementen aus P in endlicher Anzahl, $a, b, c, d \ldots$ zuerst zwei benachbarte Elemente componirt, dann wieder zwei benachbarte u. s. w., bis die ganze Reihe auf ein Element reducirt ist, das mit $abcd$ ... bezeichnet wird. So ist z. B.:
   $$\begin{aligned} abcd &= (ab)cd = [(ab)c]d = (ab)\{c\ d) \\ &= a(bc)d = [a(bc)]d = a[(bc)d] \\ &= ab(cd) = (ab)\,(cd)\,a[b(cd)]^1). \end{aligned}$$
3. Es wird vorausgesetzt, dass, wenn $ab = ab'$ oder $ab = a'b$ ist, nothwendig im ersten Falle $b = b'$, im zweiten $a = a'$ sein muss.
   Wenn P eine endliche Anzahl von Elementen umfasst, so heisst die Gruppe eine endliche und die Anzahl ihrer Elemente ihr Grad.
   Für endliche Gruppen ergiebt sich aus 1., 2., 3. die Folgerung:
4. Wenn von den drei Elementen a, b, c aus P zwei beliebig gegeben sind, so kann man das dritte immer und nur auf eine Weise so bestimmen, dass
   $$ab = c$$
   ist.
   Sind nämlich a, b die gegebenen Elemente, so fällt die Behauptung 4. mit 1. zusammen. Ist aber a und c gegeben, so lasse man in dem Compositum ab die zweite Componente b das ganze System P durchlaufen, dessen $Grad = n$ sei. Dann erhält man nach 1. und 3. in ab lauter verschiedene Elemente von P, und da ihre $Anzahl = n$ ist, so müssen alle Elemente von P, also auch c, darunter vorkommen. Ebenso schliesst man, wenn b und c gegeben sind, indem man a das ganze System P durchlaufen lässt.

Für unendliche Gruppen kann nicht mehr so geschlossen werden. Für unendliche Gruppen wird also noch die Eigenschaft 4. als Forderung in die Begriffsbestimmung mit aufgenommen. (Vgl. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, §. 2).

Bei den im ersten Bande betrachteten Permutationsgruppen wird man leicht die Merkmale des allgemeinen Gruppenbegriffes erkennen.
Wir ziehen nun aus dieser Definition zunächst einige ganz allgemeine Folgerungen.
Nach 4. giebt es für jedes gegebene b ein Element e in P, das der Bedingung

(1) $$eb = b$$

genügt, und dies e ist von b unabhängig; denn aus (1) folgt für jedes c

$$ebe = bc,$$

und bc kann nach 4. jedes Element in P bedeuten. Ebenso giebt es ein Element e' das für jedes b der Bedingung

(2) $$be' = b$$

genügt. Dies Element e' ist aber von e nicht verschieden; denn setzen wir $b = e'$ in (1) und $b = e$ in (2), so folgt

$$ee' = e', . ee' = e,$$

also $$e = e'.$$

Das Element e ändert nichts, wenn es mit irgend welchen Elementen aus P componirt wird, und wird die Einheit der Gruppe genannt.
In vielen Fällen kann es ohne Missverständniss geradezu mit „1" bezeichnet werden.
Zu jedem Element a giebt es nach 4. ein bestimmtes Element a^{-1}, das der Bedingung

(3) $$a^{-1}a = e$$

genügt. Aus (3), (1) und (2) folgt

$$a^{-1}aa^{-1} = ea^{-1} = a^{-1} = a^{-1}e,$$

und folglich nach 3.

(4) $$aa^{-1} = e$$

Die beiden Elemente a, a^{-1} heissen zu einander entgegengesetzt oder reciprok. In besonderen Fällen kann bei der Composition der Elemente einer Gruppe P auch das commutative Gesetz gelten, d. h. es kann für je zwei Elemente a, b der Gruppe

$$ab = ba$$

sein.

5. Gruppen, die diese Eigenschaft haben, heissen commutative Gruppen oder auch Abel'sche Gruppen.
Wenn sich die Elemente zweier Gruppen

$$a, b, c, d \ldots$$

Und $$a', b', c', d', \ldots$$

in der Weise gegenseitig eindeutig entsprechen, dass immer, wenn $ab = c$ ist , auch $a' b' = c'$ wird , so heissen die Gruppen isomorph, und es gilt der evidente Satz, dass zwei mit einer dritten isomorphe Gruppen unter einander isomorph sind. Man kann hiernach alle unter einander isomorphe Gruppen zu einer Classe von Gruppen zusammenfassen, die selbst wieder eine Gruppe ist, deren Elemente die Gattungsbegriffe sind, die man erhält, wenn man die entsprechenden Elemente der einzelnen isomorphen Gruppen zu einem Allgemeinbegriff zusammenfasst.
Die einzelnen unter einander isomorphen Gruppen sind dann als verschiedene Repräsentanten eines Gattungsbegriffes aufzufassen.
Die Eigenschaften der Gruppen, die in Betracht kommen können, sind von verschiedener Art. Sie können nämlich entweder den besonderen Gruppen anhaften und aus der Natur der Elemente abgeleitet sein, aus denen die Gruppe besteht, oder auch aus der Natur des Compositionsgesetzes. Oder sie können
den Gruppen als solchen anhaften und müssen sich dann lediglich aus der Definition des Gruppenbegriffes ableiten lassen. Die letzteren Eigenschaften kommen allen isomorphen Gruppen gemeinsam zu und können als invariante Eigenschaften der Gruppe bezeichnet werden. Wenn ein Vergleich gestattet ist, so
könnte man an den Unterschied zwischen den metrischen und projectiven Eigenschaften in der Geometrie erinnern.

Zu der ersten Art der Eigenschaften, die aus der besonderen Natur der Elemente abgeleitet werden, gehören z. B. bei den Permutationsgruppen die Eigenschaften der Transitivität und Intransitivität , der Primitivität und Imprimitivität ; zu den invarianten Eigenschaften gehören die Vertauschbarkeit oder Nichtvertauschbarkeit, der Grad, die Divisoren und ihr Index, die Normaltheiler. Mit diesen invarianten Eigenschaften, bei denen es gleichgültig ist, aus welchem Repräsentanten einer Classe isomorpher Gruppen sie abgeleitet sind, haben wir uns zunächst zu beschäftigen.

Anexo 2: Der Körperbegriff.

(Weber 1895, pp. 149-151, §.139.)

Dreizehnter Abschnitt.
Die Galois'sche Theorie.
§. 139.
Der Körperbegriff.

Ein System von Zahlen wird ein Zahlkörper genannt, wenn es so in sich vollendet und abgeschlossen ist, dass die vier fundamentalen Rechenoperationen (die vier Species), die Addition, die Subtraction, die Multiplication und die Division, ausgeführt mit irgend welchen Zahlen des Systems, ausgenommen die Division durch Null, immer auf Zahlen führen, die demselben System angehören. Dieser Begriff, der eine Eintheilung der Zahlenarten nach einem natürlichen Gesichtspunkte giebt, ist von Dedekind eingeführt (Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 2. Aufl. 1871, §. 159).

Er ist für die Algebra von der grossten Bedeutung, und es ist nicht gleichgültig, dafür einen bezeichnenden und ausdrucksvollen Namen zu haben. Das Wort Zahlkörper ist von Dedekind nach zahlreichen Analogien gebildet, in denen das Wort Körper (corpus, corps) in ähnlicher Weise eine Vereinigung von zusammengehörigen Dingen, der eine gewisse Vollständigkeit zukommt, bedeutet.

Der Begriff des Zahlkörpers kann erweitert und auf alle Grössen übertragen werden, mit denen nach den Regeln der vier Species gerechnet werden kann; insbesondere also auf rationale Functionen irgend welcher Veränderlichen.

Wir nennen also einen Functionenkörper ein System von Functionen von einer oder mehreren Veränderlichen von der Beschaffenheit, dass in diesem System die Rechnungen mit den vier Species unbegrenzt ausgeführt werden können und immer auf eine bestimmte Function desselben Systems führen (immer mit Ausnahme der Division durch Null). Die Veränderlichen Weber, Algebra. I. 99 können ganz von einander unabhängig sein; es ist aber auch der Fall nicht ausgeschlossen, dass gewisse Beziehungen zwischen ihnen festgesetzt sind, die beim Rechnen zu berücksichtigen sind.

Eine Function eines Functionenkörpers gilt nur dann als Null, wenn sie identisch, d. h. für alle in Betracht kommenden Werthe der Veränderlichen, verschwindet.

Da wir vorläufig unsere Betrachtungen nicht einschränken wollen, so werden wir jetzt von Körpern schlechtweg sprechen, und die Objecte, mit denen die Rechnungen auszuführen sind, die sowohl Zahlen als Functionen sein können, als Grössen oder auch als die Elemente des Körpers bezeichnen [1]).

Ein Körper ist dann also ein System von Grössen von der Vollständigkeit, dass in ihm die Grössen addirt, subtrahirt, multiplicirt und dividirt werden können.

Wenn alle Grössen eines Körpers in einem zweiten Körper enthalten sind, so heisst der erste Körper ein T heiler des zweiten.

Ist Ω ein Theiler von Ω', so werden wir auch sagen, Ω' ist ein Körper über Ω.

Streng genommen, bildet die einzige Zahl „Null" für sich einen Körper. Diesen wollen wir aber der Kürze wegen ein- für allemal- ausnehmen.

Dann ist das nächstliegende Beispiel eines Körpers der Inbegriff aller rationalen Zahlen.
Dieser Körper ist ein Theiler von jedem anderen Körper; denn jeder Körper enthält wenigstens eine von Null verschiedene Grösse ω, also auch den Qaotienten $\omega : \omega = 1$, d. h. die Zahl 1, also auch, da, alle ganzen Zahlen durch Addition und Subtraction von Einern entstehen, alle ganzen Zahlen; und aus den ganzen Zahlen kann man wieder durch Division alle Brüche ableiten.
Andere Beispiele von Zahlkörpern sind: der Inbegriff aller complexen Zahlen von der Form $x + yi$, worin $i = \sqrt{-1}$, x und y alle rationalen Zahlen bedeuten ; ferner der Inbegriff' aller (rationalen und irrationalen) reellen Zahlen, oder der Inbegriff aller überhaupt existirenden complexen Zahlen $x + yi$.
Als Beispiel eines Functionenkörpers mag der Inbegriff' aller ganzen und gebrochenen rationalen Functionen einer Veränder-liehen (mit Einschluss der Constanten) dienen, wobei man die Constanten Coefficienten auf einen beliebigen Zahlkörper, etwa auf den der rationalen Zahlen beschränken oder auch ganz unbeschränkt annehmen kann. Wir wollen hier nicht weiter die Beispiele häufen, da die genaue Untersuchung von Körpern besonderer Art eine der Hauptaufgaben unserer späteren Ausführungen sein wird.

Anexo 3: Group

(Van der Waerden, 1953, p. 11)

Definition: A non –empty set $\mathfrak{G}$ of any sort of elements (such as numbers, mappings, transformations) is said to be a group if the following four postulates are fulfilled:
A rule of combination is given which associates with every pair of elements a, b of $\mathfrak{G}$ a third element of the same set, which most frequently is called a product of a and b which is denoted by ab or $a.b$ (the product may depend on the order in which the factors are arranged; ab may or may not be equal to ba).
The associative law: If a, b, c are any elements of $\mathfrak{G}$, then

$$ab.c = a.bc.$$

There exists (at least) one element e in $\mathfrak{G}$, called the (left) identity, such that
$ea = a$ for every element a of $\mathfrak{G}$.
If a is an element of $\mathfrak{G}$, there exists (at least) one element a^{-1} in $\mathfrak{G}$, called the (left) inverse of a, such that

$$a^{-1}a = e.$$

A group is called abelian if ab is always equal to ba (commutative law).