

UNIVERSIDAD DEL VALLE
INSTITUTO DE EDUCACIÓN Y PEDAGOGÍA
PROGRAMA ACADÉMICO LICENCIATURA EN MATEMÁTICAS Y FÍSICA
SANTIAGO DE CALI
2016

ADRIAN MUÑOZ OROZCO

CODIGO: 201125957

DE LAS MATEMÁTICAS CLÁSICAS A LAS MATEMÁTICAS MODERNAS Y
CONTEMPORÁNEAS: EL CASO DE LA TEORÍA DE GALOIS COMO UNA
ADJUNCIÓN.

DE LAS MATEMÁTICAS CLÁSICAS A LAS MATEMÁTICAS MODERNAS Y
CONTEMPORÁNEAS: EL CASO DE LA TEORÍA DE GALOIS COMO UNA
ADJUNCIÓN.

ADRIAN MUÑOZ OROZCO

Trabajo de grado presentado al Programa Académico Licenciatura en Matemáticas y Física
como requisito para optar al título de Licenciado en Matemáticas y Física.

DIRECTOR.

GUILLERMO ORTIZ RICO.

PROFESOR DEL DEPARTAMENTO DE MATEMÁTICAS



UNIVERSIDAD DEL VALLE

INSTITUTO DE EDUCACIÓN Y PEDAGOGÍA

PROGRAMA ACADÉMICO LICENCIATURA EN MATEMÁTICAS Y FÍSICA

SANTIAGO DE CALI

2016



Programa Académico Licenciatura Matemáticas Física

Fecha

Código del programa: 3487

Resolución del programa: _____

Día	Mes	Año
17	03	2016

Título del Trabajo o Proyecto de Grado

De las Matemáticas clásicas a las modernas y contemporáneas: El caso de la teoría de Galois

Se trata de:

Proyecto

Informe Final

Director

Guillermo Ortiz

Nombre del Primer Evaluador

Ligia Amparo Torres R.

Nombre del Segundo Evaluador

Jaime Andrés Castaño

Estudiantes

Nombres y Apellidos	Código	Plan	E-mail	Télefonos de contacto
<u>Adrian Muñoz Orozco</u>	<u>1125957</u>	<u>3487</u>		

Evaluación

Aprobado

Meritorio

Laureado

Aprobado con recomendaciones

No Aprobado

Incompleto

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

Director del Trabajo o Proyecto de Grado

Primer Evaluador

Segundo Evaluador

En el caso de que el Informe Final se considere **Incompleto** (diligenciar la página siguiente), se da un plazo máximo de _____ semestre (s) para realizar una nueva reunión de Evaluación el _____

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

Guillermo Ortiz

Ligia Amparo Torres R.

Jaime Andrés Castaño

Director del Trabajo o Proyecto de Grado

Primer Evaluador

Segundo Evaluador

Si se considera necesario, usar hojas adicionales.

* Se reconoce la importancia del trabajo desde la perspectiva matemática e histórica, con relación a lo primero el contenido de la teoría de Galois y desde lo histórico permite comprender un paso entre el álgebra clásica y Moderna desde una perspectiva diferente a lo trabajado tradicionalmente.

• Se recomienda en la evaluación, la valoración de Aprobado Meritorio. Esto porque.

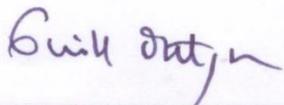
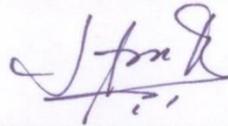
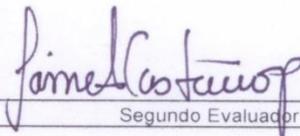
* Aborda una temática que trayendo los contenidos programáticos de su formación lo que implicó una dedicación y trabajo individual sobresaliente.

* El Trabajo, por su forma de presentación de los contenidos permite que otros estudiantes de la licenciatura y de matemáticas y público en general puedan comprender esta temática.

* En el campo de la Educación matemática aporta a la formación de profesores en formación inicial en el pas

so del álgebra clásica a la Moderna

Firmas

		
Director del Trabajo o Proyecto de Grado	Primer Evaluador	Segundo Evaluador

Dedico este trabajo a mi madre, Alcira Orozco, por su sacrificio y esfuerzo durante mi proceso de formación. A mi tía, María Deysi Orozco por sus palabras y compañía.

AGRADECIMIENTOS

Agradezco en primer lugar a mi madre, Alcira Orozco que me ha brindado todo su amor para que yo culmine esta etapa de mi vida y por su constante apoyo en cada momento.

En segundo lugar, agradezco a mi tía, Deysi Orozco que me brindo un apoyo incondicional durante mi proceso de formación profesional, y con sus palabras de aliento no me dejaba decaer para que siguiera adelante.

Agradezco a cada uno de los profesores que me guiaron por este sendero durante mi proceso de formación.

Al profesor Guillermo Ortiz por asumir cordialmente la dirección de este trabajo, por leer cada uno de los borradores que le presentaba y cuyos comentarios fueron de gran aporte para el desarrollo de éste. Además, le agradezco por brindarme bibliografía fundamental que me sirvió como base para la ampliación de mi conocimiento, y por su constante motivación para que continué con mis estudios.

A la profesora Ligia Amparo Torres y al profesor Jaime Castaño por sus aportes y consejos que fueron esenciales para concluir la escritura de este trabajo.

Finalmente agradezco a Diana Pineda por su comprensión y apoyo durante el tiempo que estuve escribiendo este trabajo.

RESUMEN.....	9
0. INTRODUCCIÓN	10
1. ALGUNOS ASPECTOS HISTÓRICOS DE LA SOLUCIÓN DE ECUACIONES POR EL MÉTODO DE SOLUCIÓN POR RADICALES.....	15
1.1 La tradición subcientífica.....	16
1.2 El álgebra árabe.....	17
1.3 El álgebra renacentista.....	19
1.4 La obra de Lagrange.....	20
2. UN ACERCAMIENTO A LAS CONEXIONES DE GALOIS DESDE UNA PERSPECTIVA HISTÓRICA Y MATEMÁTICA.....	22
2.1 Aspectos históricos de las conexiones de Galois.....	23
2.2 Aspectos matemáticos modernos de las conexiones de Galois.....	26
2.2.1 Elementos de conjuntos parcialmente ordenados.....	27
2.2.2 Elementos matemáticos de las Conexiones de Galois.....	36
3. UN ACERCAMIENTO A LA TEORÍA DE GALOIS DESDE UNA PERSPECTIVA MODERNA.....	40
3.1 Teoría de cuerpos.....	41
3.1.1 Nociones básicas de la teoría de extensiones.....	41
3.1.2 Extensiones algebraicas.....	49
3.1.3 Cuerpos de descomposición.....	54
3.1.4 Extensiones separables.....	57
3.2 Teoría de Galois.....	58
3.2.1 Definiciones básicas.....	58
3.2.2 Teorema moderno de la teoría de Galois.....	66
4. TEORÍA DE GALOIS, ALGUNOS ASPECTOS HISTÓRICOS Y MATEMÁTICOS.....	72
4.1 La vida de Galois.....	72
4.2 Aspectos históricos de la teoría de Galois.....	75
4.2.1 El papel de Abel en la teoría de Galois.....	76
4.2.2 El papel de Galois.....	78
4.3 Aspectos matemáticos históricos de la teoría de Galois.....	80
4.3.1 Grupo de Galois de una ecuación.....	81

4.3.2 El grupo de Galois bajo una extensión de cuerpo.....	94
4.3.3 Solubilidad por radicales.....	99
5. LA TEORÍA DE GALOIS COMO UNA ADJUNCIÓN. UNA REFLEXIÓN DIDÁCTICA EN LA ENSEÑANZA DE LAS MATEMÁTICAS EN LA FORMACIÓN INICIAL DE PROFESORES.	106
5.1 La Teoría de Galois como una adjunción.	107
5.1.1 Algunos comentarios de la teoría de Galois como una adjunción.	107
5.2. Una reflexión sobre el papel de la obra de Galois en la formación inicial de profesores en el campo de las matemáticas.	110
5.2.1. Un ejemplo histórico en la educación actual. El papel de las conexiones de Galois. ...	110
5.2.2. El papel de la teoría de Galois.....	112
5.3. Conclusiones.	113
5.3.1. Síntesis histórica.	113
5.3.2. La teoría de Galois como un ejemplo paradigmático en el desarrollo de las matemáticas clásicas a las modernas y contemporáneas	114
BIBLIOGRAFÍA	118

RESUMEN

En este trabajo de grado se presentan algunos elementos a considerar en el estudio de la transición de las matemáticas clásicas a las matemáticas modernas y contemporáneas, a través de un estudio histórico – epistemológico y matemático de la obra de Galois. Así, nos concentraremos en la indagación de la teoría de Galois como una adjunción, lo cual será analizado desde dos perspectivas: una matemática que nos muestra el presente teórico de la teoría de Galois y las adjunciones, lo que nos permite comentar como la teoría de Galois es un caso particular de una adjunción; y otra histórica que muestra la evolución de la teoría de Galois desde 1830 hasta la actualidad. Todo esto, porque consideramos la teoría de Galois como un ejemplo paradigmático en la transición de las matemáticas clásicas a las matemáticas modernas y contemporáneas. Al final presentaremos una reflexión didáctica y epistemológica vinculada directamente a la formación inicial de profesores en el cuerpo de las matemáticas.

Palabras claves: Teoría de Galois, Adjunción, Estudio histórico – epistemológico, Estudio matemático, Matemáticas clásicas, Matemáticas modernas y contemporáneas.

0. INTRODUCCIÓN

Las Matemáticas son una ciencia en continua evolución, y como toda ciencia, se consideran un constructo social y cultural. Las matemáticas del siglo XX se caracterizan por ser esencialmente estructurales. Más aún, las Matemáticas aparecen como una ciencia axiomatizada, es decir, “cada concepto matemático se define a partir de un conjunto de axiomas. Este cambio es muy significativo; se pasa de las matemáticas (clásicas) de contar, medir y ordenar a unas matemáticas de estructuras formales (modernas); caracterizadas por propiedades estructurales y cualitativas que llegan hoy a sofisticados grados de interrelación, de transferencia y pegamientos (contemporáneas)” Lautman (2006).

Estudiar aspectos fundamentales que describen este cambio es obviamente de interés para los profesores en formación inicial en matemáticas. Esperemos que este trabajo apunte en la búsqueda de una visión más amplia de la evolución de las matemáticas; comprendiendo que la matemática axiomatizada y estructural continua siendo el producto social y cultural más importante de nuestra especie.

Aunque, este tipo de transiciones no son fáciles de abordar, en este trabajo se intenta realizar un acercamiento a la transición de tres etapas que son consideradas esenciales en la Historia de las Matemáticas, las cuales son definidas por Lautman (2006) como: **matemáticas clásicas** (mediados del siglo *XVII* - mediados del siglo *XVIII*), en el cual se profundiza en la noción de infinito por parte de Pascal, Leibniz, Carl Friedrich Gauss y Euler; **matemáticas modernas** (mediados del siglo *XIX* – mediados del siglo *XX*), que introduce el uso sofisticado de propiedades estructurales y cualitativas, abordado por matemáticos como Galois, Riemann, Hilbert; y **matemática contemporánea** (mediados del siglo *XX* –

hasta hoy), se implementa el uso sofisticado de propiedades de transferencia, reflexión y pegamiento por parte de Grothendieck, Serre, Shelah.

En este sentido, el paso de un periodo a otro está definido por una compleja jerarquización de las diversas teorías matemáticas irreducibles entre si relativamente, en donde se entrelazan los conceptos matemáticos y surgen muchas de sus grandes teorías Zalameda (2009). De esta manera, se observa que el paso de las matemáticas clásicas a las matemáticas modernas, da lugar a escalas constructivas, correspondencias inversas y gradaciones de todo tipo, que son particularmente visibles en la teoría de Galois y en teorías generalizadas de dualidad.

Además, es importante destacar que la transición de los dos periodos anteriores es de gran influencia en el estudio de la matemática contemporánea, puesto que “la teoría de Galois es uno de los grandes momentos del desarrollo de las matemáticas, con notables transferencias conceptuales, hacia los más variados dominios de la matemática” [Zalamea (2009)] y afecta directamente los procesos de abstracción y demostración matemática de los últimos años.

En esta dirección, referirse a la teoría de Galois históricamente es intervenir en uno de los grandes aspectos relacionados con la historia del álgebra, más concretamente en la solución de ecuaciones por el método de radicales. Tema que abarca desde los trabajos egipcios en el siglo XVII a. n. e. (antes de nuestra era) hasta la demostración de la no solubilidad de la ecuación general de grado mayor o igual a cinco por el método de radicales por parte de Abel, quien dejó abierto el interrogante de: ¿Qué ecuaciones de grado mayor a cuatro eran solubles por el método de radicales? posteriormente resuelto por Galois.

Por otra parte, la teoría de Galois soluciona uno de los grandes problemas del siglo XIX relacionado con las condiciones que debe cumplir una ecuación de grado mayor o igual a cinco para ser soluble por el método de radicales; y como señala Denecke (2004), ésta teoría es la puerta de entrada a las adjunciones (también conocidas por conexiones de Galois), que como se mencionó anteriormente, es otro de los aspectos que inciden en el recorrido de las matemáticas clásicas a las matemáticas modernas.

De este modo, en este trabajo se analizan dos conceptos matemáticos que están ligados histórica y matemáticamente, los cuales influyen en el paso de dos periodos de la historia y generan repercusiones sobre un tercero. Se trata, de identificar algunos de los aspectos más relevantes que caracterizan la transición de las matemáticas clásicas a las matemáticas modernas y contemporáneas, a través del estudio histórico – epistemológico y matemático de la teoría de Galois como una adjunción. Se espera explorar, la relación de elementos históricos de la teoría de Galois y de la evolución de las matemáticas con aspectos actuales de nuestra educación matemática.

Para desarrollar lo planteado anteriormente, se esbozan los siguientes objetivos específicos:

1. Caracterizar algunos aspectos históricos de la solución de ecuaciones por el método de solución por radicales.
2. Describir desde un punto de vista histórico las adjunciones a través de una síntesis de algunos elementos de la obra *Galois Connections and Applications* escrita por Denecke (2004) y desde un punto de vista matemático a través de estudio algunos

elementos de la obra de Smith (2010) *The Galois Connection between Syntax and Semantics*.

3. Estudiar la teoría de Galois desde dos perspectivas una histórica y otra matemática. En dos momentos, el primero; en la actualidad desde un lenguaje matemático moderno y el segundo; a través del estudio del capítulo 14 del libro *Galois Theory of Algebraic Equations* de Jean-Pierre Tignol, en el cual se realiza una reescritura de la memoria de Galois.
4. Mostrar que el trabajo de Galois, sobre la solubilidad de ecuaciones de grado mayor igual a cinco es una adjunción, a partir del estudio del ejemplo 3.14 de la página 59 de la obra de Steven Roman "*Lattices and ordered sets*".
5. Explorar una reflexión didáctica y epistemológica acerca de la influencia de ésta investigación en la formación inicial de profesores en el campo de las matemáticas.

Los cuales se desarrollan en los siguientes capítulos:

En el primer capítulo se realiza una síntesis de algunos aspectos que desde nuestro punto de vista son relevantes en el desarrollo histórico de la solución de ecuaciones por el método de radicales, tomando como punto de referencia los trabajos de grado de Chavarría (2014) y Murcia (2009) considerados además como antecedentes del presente trabajo. De los aspectos que se destacan consideramos los siguientes: la tradición subcientífica, el desarrollo de la teoría de ecuaciones en los árabes, el desarrollo del álgebra renacentista y la obra de Lagrange.

En el capítulo dos, en primer lugar se realiza un acercamiento histórico a las conexiones de Galois, a través del estudio de un material bibliográfico que reseña los distintos aspectos

matemáticos que dan origen a la teoría de adjunciones y además se presentan un par de ejemplos que muestran las primeras huellas de las conexiones de Galois. En segundo lugar, se realiza una descripción matemática de la teoría de adjunciones, tomando en consideración la definición establecida en conjuntos parcialmente ordenados.

En el capítulo tres se expone la teoría de Galois desde una perspectiva moderna, a través, de la presentación de los elementos matemáticos modernos necesarios para comprender el teorema fundamental de la teoría moderna de Galois, el cual es enunciando y ejemplificado a lo largo de todo el capítulo a través de los ejemplos de cada uno de los conceptos necesarios para enunciar este teorema. Entre estos elementos, se destacan las nociones básicas de la teoría de extensiones, extensiones algebraicas, cuerpos de descomposición y extensiones separables.

En el cuarto capítulo, inicialmente se presenta una síntesis de la vida memorable de Évariste Galois; luego se muestra una breve recapitulación de los últimos aspectos que dieron origen a la teoría de Galois, resaltando el papel de Abel y de Évariste; y por último se expone nuevamente la teoría de Galois vista en el capítulo tres pero esta vez, desde una perspectiva histórica abordando, el apartado 14 de la obra de Tinol (2011) *Galois' Theory of Algebraic Equations*, en la cual se realiza una reescritura de la memoria original escrita por Galois.

En el quinto capítulo; primero se presentan la teoría de Galois como una adjunción relacionando los conceptos abordados en los capítulos anteriores; y segundo se presenta una reflexión didáctica en la formación inicial de profesores en el campo de las matemáticas, utilizando, la presentación e interpretación de un ejemplo que muestra los cambios de las matemáticas a lo largo del tiempo, y se reflejan en la actualidad de la enseñanza de las matemáticas.

1. ALGUNOS ASPECTOS HISTÓRICOS DE LA SOLUCIÓN DE ECUACIONES POR EL MÉTODO DE SOLUCIÓN POR RADICALES.

“Los encantos de esta ciencia sublime, las matemáticas, solo se revelan a aquellos que tienen el valor de profundizar en ella”

Carl Friedrich Gauss.

En este capítulo se realiza un acercamiento a algunos aspectos históricos que incidieron en el desarrollo de la teoría de ecuaciones, a través del estudio de elementos de la solución de ecuaciones por el método de radicales, los cuales influyen directamente (como lo podremos ver más adelante) en la constitución histórica de la Teoría de Galois y las adjunciones, temas centrales de este documento. En esta dirección, se presentan algunos elementos de la tradición subcientífica, el álgebra árabe, el álgebra renacentista y la obra de Lagrange. Sin embargo, es importante aclararle al lector que en esta sección no se va a profundizar en ninguno de los aspectos anteriores, solo se realizará un recorrido muy global, debido a que este no es el interés central de este documento; y si el lector desea profundizar en estas temáticas se recomienda el estudio del trabajo de Chavarría (2014) *“De las ecuaciones a la teoría de grupos, algunos obstáculos epistemológicos”* y el trabajo de Murcia (2009) *“La Transición del Álgebra Clásica al Álgebra Moderna: Algunos aspectos históricos-epistemológicos en el desarrollo de la noción de estructura a través de la teoría de ecuaciones”*.

1.1 La tradición subcientífica

La “tradición subcientífica” señala Torres (2010) surge en la Edad de Bronce Babilonia dentro de un medio de Geómetras prácticos (como agrimensores, arquitectos o constructores) y se entiende, como técnicas para resolver problemas que no son de uso práctico, si no de tipo recreativo, probablemente destinados a la formación de personas en estos oficios. Dentro de estas técnicas se solucionaban acertijos, enigmas y problemas de la vida cotidiana generados por las necesidades básicas de una cultura como por ejemplo calcular áreas de terrenos, repartir cerveza entre otros.

De la “tradición subcientífica” se resalta que se dieron los primeros pasos en la solución de ecuaciones por el método de radicales, debido a, que en este periodo se presentaron los procesos de solución de ecuaciones de primer y segundo grado, a través de inventivas como la técnica de cortar y pegar y otras no propiamente de la tradición subcientífica como el método de falsa posición para solucionar la ecuación de grado uno.

El método de falsa posición, básicamente consiste en asignar un valor de un número natural cualquiera a la incógnita y empleando nociones de proporcionalidad (regla de tres simple) entre la ecuación original y el resultado después de la sustitución permitía determinar el valor de dicha incógnita. Referente a la técnica de cortar y pegar se puede describir desde una perspectiva moderna como el método de completar cuadrados y desde una perspectiva histórica mediante una serie de ejemplos presentados en Torres (2010) *“Fenomenología histórica del concepto de ecuación y potencialidades de su uso en la escuela”* y en la cual se desarrolla esta técnica a profundidad. Además todos sus procesos se realizaban sobre segmentos de líneas conmensurables y con superficies, no con números; lo que evidencia que

las ecuaciones como objetos algebraicos propiamente no existían y hasta el momento solo eran las relaciones entre objetos geométricos más concretamente entre magnitudes conmensurables o cantidades. También se menciona, que en esta técnica se consideran tanto líneas como rectángulos en la solución de problemas, lo que da inicio a un proceso de homogenización bastante significativo, ya que es necesario operar con objetos de la misma naturaleza.

1.2 El álgebra árabe.

La historia del Álgebra se distingue según Puig (1998) por el descubrimiento de técnicas y fórmulas en la solución de ecuaciones y en el descubrimiento del lenguaje en el cual se representan estas técnicas. Este desarrollo histórico se caracteriza por los periodos de “álgebra retórica”, “álgebra sincopada” y “álgebra simbólica” los cuales reciben una gran influencia en la obra de Al-Khwarizmi y culminan con los trabajos de Vieta y Descartes en los siglos XVI y XVII.

Ahora bien, hay que resaltar que el álgebra que actualmente conocemos está directamente influenciada por el desarrollo del álgebra árabe a través del trabajo de Al-Khwarizmi en su obra “*El libro conciso del cálculo de al-jabr y de al-muqabala*”, debido a, que esta obra fue pensada como un manual de referencia para la solución de problemas de cálculo, relativas a distintas problemáticas en contextos algebraicos y se integraron los primeros elementos en la transición del “álgebra retórica” al “álgebra sincopada”.

Además, la obra de Al-Khwarizmi se destaca porque se realizan las primeras caracterizaciones de los tres términos de una ecuación cuadrática. Retornando a la referencia Torres (2010) se tenía que:

- i. Una raíz es cualquier cosa que será multiplicada por sí misma, consiste en la unidad de números, hacia arriba, o fracciones hacia abajo
- ii. Un tesoro es el valor de una raíz multiplicada por sí misma
- iii. Un simple número cualquiera que puede expresarse sin atribuirlo a raíz ni a tesoro

Donde la expresión tesoro se puede relacionar con el término cuadrático, la raíz al término lineal y un simple número con el término constante. Aunque es importante tener en consideración que la expresión tesoro no necesariamente traduce el término cuadrático, es decir, estas caracterizaciones en lenguaje moderno pueden aludir a dos contextos; el primero $x^2 + ax + c = 0$ o el segundo $x + a\sqrt{x} + c = 0$.

Caracterizaciones que permitieron desarrollar los primeros aspectos de generalización, debido a que los métodos que solucionan ecuaciones de segundo grado presentados en la obra Al-Khwarizmi se clasificaban en seis casos;

- i. Tesoros igual a raíces,
- ii. Tesoros igual a números,
- iii. Raíces igual a números,
- iv. Tesoros y raíces igual a números,
- v. Tesoros y números igual a raíces, y
- vi. Raíces y números igual a tesoros.

Donde, en los seis casos solo se consideraban coeficientes positivos.

En esta misma referencia se resalta, del trabajo de los árabes el avance en los procesos de generalización y el desarrollo de la escritura de los procesos algebraicos; además que en los

árabes, y más concretamente en la teoría de Al-Khwarizmi se desarrolla, el concepto de objeto matemático, el concepto de ecuación y la teoría de ecuaciones.

1.3 El álgebra renacentista.

El álgebra renacentista se presenta a principios XIV y se caracteriza en gran medida porque en este periodo se logran solucionar de forma general las ecuaciones de tercer y cuarto grado por el método de radicales y se validan las mismas. Siguiendo a Murcia (2009) se tiene que en este periodo se da un impulso significativo en la forma de representar cantidades y de realizar operaciones, todo esto gracias a los aportes realizados por los matemáticos italianos Leonardo de Pissa, Scipio del Ferro, Rafael Bombelli, Antonio María Fior, Girolamo Cardano y Luigi Ferrari.

Una de las obras que más influyeron en el periodo renacentista fue la realizada en el año de 1545 por Cardano llamado el “*Ars Magna*”, que presenta las soluciones de las ecuaciones de tercer y cuarto grado. En esta obra se rompe con ataduras matemáticas anteriores, respecto al concepto número y las relaciones dimensionales de las cantidades con lo geométrico, es decir, se logra un proceso de homogenización (ver Torres (2010)).

Otro de los resultados importantes logrados en el álgebra renacentista, se centra en la naturaleza de las raíces de una ecuación cuadrática, debido a que en este periodo se aceptan soluciones negativas de una ecuación. También se empiezan a generar interrogantes sobre el número de raíces de una ecuación cuadrática, es decir, se plantea la posibilidad de que existan raíces de multiplicidad dos.

En relación, con la multiplicidad de la raíces de una ecuación cuadrática Cardano en 1545 amplía este concepto a las ecuaciones de cualquier grado, lo cual le permite plantear dos

aspectos muy importantes. El primero, enunciar por primera vez el teorema fundamental del álgebra a pesar de que no lo demuestra; y el segundo, se plantea la existencia de los números complejos que son posteriormente dados a conocer en la comunidad matemática de la época por Gauss.

Por último, podemos aludir que el álgebra renacentista dejó muchos aportes a la matemática actual entre estos es importante destacar, el planteamiento de Cardano que hace visible la relación entre las raíces de una ecuación y los coeficientes, es decir, la solución de una ecuación se puede expresar en términos de sus coeficientes; los polinomios que cumplen la relación anterior se conocen como polinomios simétricos los cuales son fundamentales en el desarrollo de la obra de Lagrange y la Teoría de Galois.

1.4 La obra de Lagrange.

La solución de ecuaciones por el método de radicales se convirtió en uno de los grandes problemas matemáticos del siglo XIV, en especial la solución general de la ecuación de quinto grado, el cual fue abordado por distintos matemáticos de la época entre ellos el italiano Joseph Louis Lagrange, quién centro su interés en esta problemática, debido a que las ecuaciones de grado 2, 3 y 4 ya habían sido resueltas con éxito en el álgebra árabe y renacentista lo que hacía pensar en la comunidad de matemáticos de la época que todas las ecuaciones eran completamente solubles por el método de radicales.

Lagrange, en su interés por solucionar la ecuación quintica implementa un nuevo método conocido como la resolvente de Lagrange, el cual se aplicaba a polinomios simétricos y consiste básicamente en relacionar los coeficientes de una ecuación con sus raíces mediante una serie de permutaciones. El procedimiento de la resolvente se encuentra documentado en

la memoria de Lagrange “*Réflexions sur la Résolution Algébrique des Equations*” publicada en 1771.

En relación con lo anterior, la resolvente de Lagrange fue aplicada a las ecuaciones de tercer y cuarto grado, de lo cual se obtuvieron resultados similares de los logrados por los matemáticos renacentistas, babilonios y árabes. Es decir, se solucionaron las ecuaciones de grado tres y cuatro, y se persistió con el problema de la no solución de la ecuación de grado cinco. Sin embargo, en este nuevo fracaso paso algo diferente, por primera vez se plantea la imposibilidad de solucionar la ecuación general de grado cinco por el método de radicales.

Por último, del trabajo de Lagrange es importante mencionar dos aspectos que influyeron en la matemática actual. El primero, referente a los trabajos realizados sobre permutaciones, los cuales fueron uno de los elementos que dieron origen al álgebra moderna a través del desarrollo del concepto de grupo; y el segundo, se relaciona con las distintas repercusiones en el desarrollo de la historia de las matemáticas en el planteamiento de la imposibilidad de solucionar la ecuación de quinto grado, que fue abordado posteriormente por los matemáticos Niels Abel y Évariste Galois.

2. UN ACERCAMIENTO A LAS CONEXIONES DE GALOIS DESDE UNA PERSPECTIVA HISTÓRICA Y MATEMÁTICA.

“los encantos de esta ciencia sublime, las matemáticas, solo se revelan a aquellos que tienen el valor de profundizar en ella”

Carl Friedrich Gauss

En este capítulo se realiza un acercamiento a algunos aspectos históricos y matemáticos de las adjunciones (conexiones de Galois), a través del estudio de referencias bibliográficas que abordan estos aspectos. Así, este capítulo se divide en dos apartados: en el primero, se expresan los diferentes conceptos matemáticos los cuales son la puerta de entrada a las conexiones de Galois, resaltando que el desarrollo del concepto de adjunción no es lineal y el cual debe su origen a muchos conceptos matemáticos, también se contemplan dos ejemplos que muestran las raíces de las adjunciones siglos atrás, uno de ellos, en la solución de ecuaciones de segundo grado y el otro en los procesos matemáticos relacionados con las clases residuales modulo primo; el segundo, relaciona aspectos matemáticos modernos de las adjunciones, en la cual se realiza un estudio de conceptos matemáticos como conjuntos parcialmente ordenados, tipos de funciones entre conjuntos parcialmente ordenados, entre otros conceptos que inciden en una definición de conexión de Galois, lo cual le permite al lector una mejor comprensión de lo que es una conexión, además en el segundo apartado se presentan ejemplos de conexiones, que evidencian como las adjunciones están inmersas en diferentes conceptos matemáticos.

2.1 Aspectos históricos de las conexiones de Galois.

En esta sección se realiza un acercamiento histórico a las conexiones de Galois, a través del estudio de dos ejemplos de la teoría de ecuaciones en la cual se evidencian, las primeras nociones de adjunción. Sin embargo, es importante mencionar que desde un punto de vista histórico la teoría de ecuaciones, no es la única puerta de entrada a las adjunciones pues existen otros elementos como: la teoría moderna de Galois, los orígenes de teoría reticular, las polaridades, el cálculo lógico y la teoría residual; además de las apariciones esporádicas de las adjunciones en importantes teoremas matemáticos. Se recomienda al lector si desea profundizar en los aspectos históricos de las conexiones de Galois, el estudio del libro de M. Érne, K. Denecke y S. L. Wismath (2014) “*Galois Connections and Applications*” en el cual se aborda de forma amplia las diferentes teorías que dieron origen a las conexiones de Galois.

En un sentido más amplio, una conexión de Galois permite relacionar dos “mundos” (objetos matemáticos) con el objetivo de reunir información de un mundo al pasar al otro quizás mejor conocido. Precisamente el paso de un mundo a otro debe hacerse de forma que ciertas estructuras de orden sean preservadas o invertidas. En pocas palabras, dos típicos “mundos” podrían ser la mano derecha y la mano izquierda, la igualdad y la desigualdad. Así el proceso habitual de simplificar o evaluar, como por ejemplo en una desigualdad es cambiar un poco de “basura” de un lado a otro con la intención de encontrar una información desconocida.

Un ejemplo tomado de Érne (2014) que ilustra lo mencionado anteriormente, lo encontramos en un problema del libro de Abu Kamil’s Álgebra (cerca de 880 a.c):

¿En qué condiciones es posible solucionar la ecuación?

$$-x^2 + 2bx + c = \blacksquare$$

(donde \blacksquare representa un cuadrado). La respuesta dada por Abu Kamil's es: si $c < 0$ entonces $-c$ debe ser menor que b^2 ; y $b^2 + c$ es la suma de dos cuadrados. Es poco probable que Abu Kamil's ya fuese consciente de la siguiente sutil diferencia; mientras que la segunda condición es necesaria y suficiente para la existencia de una solución dentro de los racionales, la primera es necesaria y suficiente para la existencia de al menos una solución en los reales. El argumento aquí, es un caso típico de las piezas removibles entre dos lados de una desigualdad, que adoptan el hecho de que en los reales, los cuadrados son sólo números positivos:

$$-x^2 + 2bx + c > 0 \quad \leftrightarrow \quad c > x^2 - 2bx$$

$$c + b^2 > x^2 - 2bx + b^2 \quad \leftrightarrow \quad c + b^2 > (x - b)^2$$

$$\rightarrow c + b^2 > 0 \quad \leftrightarrow \quad b^2 > -c.$$

Observe que la flecha implicación puede invertirse si x está lo suficientemente cerca a b , y si esto sucede se puede considerar la igualdad

$$x - b = 0 \rightarrow (x - b)^2 = 0$$

lo que nos permitiría si lo deseáramos, reconstruir la ecuación dada a partir de la condición de que $b^2 > -c$. El tratamiento de las desigualdades equivalentes, requiere de adición o sustracción de los valores en ambos lados, o de multiplicar simultáneamente por números positivos, etc.

No es difícil precisar, los aspectos necesarios para cambiar una pieza de un lado a otro en una desigualdad, la adecuada presentación de cada una de estas situaciones es por medio de dos adjuntos

$$\begin{array}{ccc} & \delta & \\ P & \xrightarrow{\quad} & Q \\ & \xleftarrow{\quad} & \\ & \varphi & \end{array}$$

entre conjuntos parcialmente ordenados, sujetos a una condición de orden.

$$p \leq \delta(q) \leftrightarrow \varphi(p) \leq q.$$

Que resulta ser equivalente a la restricción, si δ y φ son monótonas (es decir, preservan el orden) se cumplen las desigualdades

$$p \leq \delta(\varphi(p)) \text{ y } \varphi(\delta(q)) \leq q.$$

Regresando al ejemplo de Abu Kamil's; notemos que δ puede significar la adición de una constante, mientras que φ es la sustracción de la misma constante. De forma más general, cualquier grupo parcialmente ordenado con traslaciones isomorfas.

$$\tau_a: x \rightarrow x + a.$$

Y la sustracción

$$\sigma_a: x \rightarrow x - a.$$

Donde τ_a y σ_a son a la vez los adjuntos¹ izquierdo y derecho, y el uno es el inverso del otro.

Ahora consideremos un ejemplo similar, tal vez un tanto inesperado de adjunción, el cual surge cuando el primer adjunto es una relación de equivalencia y el segundo en una relación

¹ Un adjunto es una función entre dos conjuntos parcialmente ordenados que conserva relaciones de orden.

de identidad; representado por el mundo de congruencias modulo p , donde p es un primo. Considerando las clases de las clases de residuos modulo p dado por $F_p = Z/Z_p$; el adjunto derecho

$$\gamma: Z \rightarrow Z/Z_p$$

$$n \rightarrow n + pZ$$

Y el adjunto inverso $\delta: n + Z_p \rightarrow Z$, donde δ toma una clase residual y lo envía en su representante. Lo cual satisface la relación

$$\gamma(n) = q \text{ si y solo si } n \equiv \delta(q) \text{ mod } p.$$

que es una adjunción.

A modo de conclusión, en los dos ejemplos anteriores se abordó el concepto de adjunción o conexión de Galois desde una perspectiva poco formal y aludiendo a un contexto histórico en el cual se evidencian las primeras huellas de adjunción, mucho tiempo atrás y se introduce que las conexiones están inmersas en muchos aspectos matemáticos, tanto históricos como modernos.

2.2 Aspectos matemáticos modernos de las conexiones de Galois.

En esta sección se realiza una descripción de aspectos matemáticos modernos de las conexiones de Galois (adjunciones) a través de la interpretación de conjuntos parcialmente ordenados, conjuntos con orden total y tipos de funciones entre conjuntos parcialmente ordenados lo que le permite al lector una mejor apropiación de lo que es una conexión de Galois; además de la presentación de ejemplos de cada uno de estos conceptos, incluyendo ejemplos de conexiones de Galois. Si el lector desea profundizar acerca del estudio de las

conexiones, se recomienda el estudio de la referencia de esta sección, que es la obra de Smith (2010) “*The Galois Connection between Syntax and Semantics*”, que desde nuestra perspectiva describe los aspectos básicos de las adjunciones.

2.2.1 Elementos de conjuntos parcialmente ordenados.

2.2.1.1. Conjunto parcialmente ordenado.

Definición 2.1. Un conjunto parcialmente ordenado es una dupla $\mathcal{p} = \langle P, \leq \rangle$, donde P es un conjunto junto a una relación de orden \leq , es decir \leq , satisface para todo $x, y, z \in P$:

- i. $x \leq x$ (reflexiva)
- ii. Si $x \leq y$ y $y \leq x$ entonces $y = x$ (antisimétrica)
- iii. Si $x \leq y$ y $y \leq z$ entonces $x \leq z$ (transitiva)

Para comprender mejor la definición 2.1 consideremos los siguientes ejemplos.

Ejemplo 2.2 El conjunto de los números naturales con divisibilidad; es decir, si $m \leq n$ si y solo m divide a n .

Sea $m, n, r \in N$ entonces se cumple que

- i. $n \leq n$

Si $n \leq n$ entonces n divide a n , por definición de divisibilidad se debe cumplir que $n = tn$ con $t \in N$ lo cual es verdadero para $t = 1$.

- ii. Si $n \leq m$ y $m \leq n$ entonces $n = m$

Si $n \leq m$ y $m \leq n$ entonces n divide a m y m divide a n ; por definición de divisibilidad se tiene que $m = tn$ y $n = sm$ con $t, s \in N$; así para $t = s = 1$ se concluye que $m = n$.

iii. Si $n \leq m$ y $m \leq r$ entonces $n \leq r$

Si $n \leq m$ y $m \leq r$ se cumple que n divide a m y m divide a r ; así por definición de divisibilidad $m = tn$ (1) y $r = sm$ (2) con $t, s \in \mathbb{N}$; sustituyendo (1) en (2) se tiene que $r = s(tn)$; por propiedad asociativa y clausurativa de la multiplicación de números naturales se concluye que n divide a r por lo tanto $n \leq r$.

Ejemplo 2.3. Considere un lenguaje formal interpretado L . Sea $|\alpha|$ un conjunto de clases de equivalencia que contiene a todos los elementos de L que son lógicamente equivalentes de α , y sea E el conjunto de todas las clases de equivalencia. Sea \rightarrow la relación entre las clases de equivalencia $|\alpha|$ y $|\beta| \in E$ si $\alpha \vDash \beta$, es decir, $|\alpha|$ y $|\beta|$ son dos tautologías entonces $\langle E, \rightarrow \rangle$ es un conjunto parcialmente ordenado.

Sea $|\alpha|, |\beta|, |\gamma| \in E$ entonces se cumple que

i. $|\alpha| \rightarrow |\alpha|$

Si $|\alpha| \rightarrow |\alpha|$, entonces $\alpha \vDash \alpha$ es trivial ya que α se deduce α .

ii. Si $|\alpha| \rightarrow |\beta|$ y $|\beta| \rightarrow |\alpha|$ entonces $|\alpha| = |\beta|$

Si $|\alpha| \rightarrow |\beta|$ y $|\beta| \rightarrow |\alpha|$ entonces $\alpha \vDash \beta$ y $\beta \vDash \alpha$; así por definición de deducción se obtiene $|\alpha| = |\beta|$.

iii. Si $|\alpha| \rightarrow |\beta|$ y $|\beta| \rightarrow |\gamma|$ entonces $|\alpha| \rightarrow |\gamma|$

Si $|\alpha| \rightarrow |\beta|$ y $|\beta| \rightarrow |\gamma|$ entonces $\alpha \vDash \beta$ y $\beta \vDash \gamma$; por transitividad de \vDash se obtiene que $\alpha \vDash \gamma$.

Ejemplo 2.4. Los números reales con la relación mayor o igual.

Para la demostración de que la dependencia mayor o igual, es una relación de orden parcial consideremos tres aspectos, primero definamos el conjunto de los reales positivos unidos con el $\{0\}$ expresado como R^+_0 ; segundo el axioma de tricotomía: existe un subconjunto tal que $R^+ \subset R$, tal que $\forall x \in R$ se cumple que $x \in R^+$ ó $x = 0$ ó $-x \in R^+$; y el tercero, la definición de la relación de orden \leq, N si $x \leq y$ si y solo si $y - x \in R^+_0$. Ahora si $x, y, z \in R$ demostremos que

i. $x \geq x$

Si $x \in R$ entonces por el axioma de tricotomía $x \in R^+$ ó $x = 0$ ó $-x \in R^+$, y por cerradura de la suma para R^+ , $x + (-x) \in R^+$ que es equivalente a $x + (-x) > 0$; por otra parte, por axioma de opuesto aditivo $x + (-x) = 0$, así por definición de mayor o igual se obtiene que $x + (-x) \geq 0$ que es equivalente a $x \geq x$.

ii. Si $x \leq y$ y $y \leq x$ entonces $y = x$

Sea $x \leq y$ y $y \leq x$, entonces $y - x \in R^+_0$ y $x - y \in R^+_0$, y por propiedad clausurativa de R^+_0 $[(x < y) \vee (x = y)] \wedge [(x > y) \vee (x = y)]$; por propiedad distributiva $[(x = y)] \vee [(x > y) \wedge (x < y)]$; por el principio de contradicción es cumple $[(x = y)] \vee F$ y por principio de tercer excluido se concluye que $(x = y)$.

iii. Si $x \leq y$ y $y \leq z$ entonces $x \leq z$.

Sea $x \leq y$ y $y \leq z$; entonces se cumple que $y - x \in R^+_0$ y $z - y \in R^+_0$; que por cerradura de la suma para R^+_0 , permite concluir que $y - x + z - y \in R^+_0$, por propiedad asociativa, conmutativa e inverso aditivo se obtiene $-x + z \in R^+_0$, se concluye que $x \leq z$.

Ejemplo 2.5. Sea $\mathcal{P}(A)$ el conjunto de partes del conjunto A . Entonces partes de A es parcialmente ordenado bajo la relación inclusión “ \subseteq ”; es decir $\langle \mathcal{P}(A), \subseteq \rangle$ es un conjunto parcialmente ordenado.

Ejemplo 2.6. Los números naturales con la relación “menor o igual” $\langle \mathbb{N}, \leq \rangle$.

Después de los ejemplos ilustrados anteriormente de conjuntos parcialmente ordenados es conveniente enunciar dos teoremas de conjuntos parcialmente ordenados.

Teorema 2.7. Si $\mathcal{p} = \langle P, \leq \rangle$ es conjunto parcialmente ordenado y $Q \subseteq P$; entonces también lo es $q = \langle Q, \leq \rangle$ para algún $Q \subseteq P$, donde \leq está restringido a \leq ; es decir que q es un subconjunto parcialmente ordenado de \mathcal{p} .

Teorema 2.8. (Relación orden dual) Si $\mathcal{p} = \langle P, \leq \rangle$ es conjunto parcialmente ordenado entonces también lo es $\mathcal{p}^{op} = \langle P, \leq^{op} \rangle$, donde \leq^{op} es la relación opuesta de \leq ; es decir, si $x \leq^{op} y$ entonces $y \leq x$.

La relación orden dual es importante en el estudio de funciones entre conjuntos parcialmente ordenados, es por ello que se hace necesario, la interpretación del teorema 2.8 a través de los ejemplos 2.9 y 2.10.

Ejemplo 2.9. Como se demostró en el ejemplo 2.4, los números reales son un conjunto parcialmente ordenado con la relación de orden mayor o igual. Se define la relación orden dual de $\langle \mathbb{R}, \geq \rangle$ como los números reales con la relación de orden menor o igual $\langle \mathbb{R}, \leq \rangle$.

Ejemplo 2.10. Como se mencionó en el ejemplo 2.5, el conjunto de partes de A con la relación de orden con la inclusión. Se define la relación orden dual de $\langle \mathcal{P}(A), \subseteq \rangle$ como el conjunto parcialmente ordenado $\langle \mathcal{P}(A), \supseteq \rangle$.

2.2.1.2 Conjunto estrictamente ordenado.

Definición 2.11. Un conjunto estrictamente ordenado es un par $\mathcal{L} = \langle Q, < \rangle$, donde Q es un conjunto, con la relación $<$. Es decir $<$ satisface, para todo $x, y, z \in Q$:

- i. $x \not< x$ (antireflexiva)
- ii. Si $x < y$ entonces $y \not< x$ (asimétrica)
- iii. Si $x < y$ y $y < z$ entonces $x < z$ (transitiva)

Para una apropiación más completa por parte del lector de la definición 2.11, se citan los ejemplos 2.12 y 2.13 de conjuntos estrictamente ordenados.

Ejemplo 2.12. Los números Reales con la relación “mayor que”

Sea $x, y, z \in R$ entonces se cumple que

- i. $x \not< x$

Si $x \in R$ por axioma de tricotomía $\exists R^+ \subset R$, tal que $\forall x \in R$ se cumple que $x \in R^+ \text{ ó } x = 0$ ó $-x \in R^+$ o lo que es equivalente a $0 < x$ ó $x < 0$ ó $x = 0$. Ahora supongamos que $x < x$, por lo tanto $x - x < 0$, así $0 < 0$; por otra parte, por reflexividad de la igualdad, $0 = 0$ lo que contradice el axioma de tricotomía, por lo tanto $x \not< x$.

- ii. Si $x < y$ entonces $y \not< x$

Supongamos que $y < x$ y por hipótesis tenemos $x < y$; así por propiedad transitiva $y < y$ lo que contradice el inciso i, por lo tanto $y \not< x$.

- iii. Si $x < y$ y $y < z$ entonces $x < z$

Si $x < y$ y $y < z$ entonces $-x + y \in R^+$ y $-y + z \in R^+$ por propiedad clausurativa de R se obtiene que $-x + z \in R^+$, por lo tanto $x < z$.

Ejemplo 2.13. Sea el par $\langle N, < \rangle$; y relación de orden $<$ definida por: si $m, n \in N$ entonces $m < n$ si y solo si $m \neq n$ y m divide a n .

Sea $m, n \in N$ entonces se cumple que

i. $n \nless n$

Supongamos que $n < n$ entonces n divide a n y $n \neq n$; por definición de divisibilidad se cumple que $n = tn$ para algún $t \in N$; si consideramos $t = 1$, concluimos que $n = n$ lo que contradice nuestro supuesto, por lo tanto $n \nless n$.

ii. Si $n < m$ entonces $m \nless n$.

Supongamos que $m < n$ y $n < m$ entonces n divide a m , m divide a n y $m \neq n$; por definición de divisibilidad se tiene que $m = tn$ y $n = sm$ con $t, s \in N$; así para $t = s = 1$ se concluye que $m = n$ lo que contradice nuestro supuesto por lo tanto $m \nless n$.

iii. Si $n < m$ y $m < r$ entonces $n < r$.

Si $m < n$ y $m < r$ se cumple que n divide a m , m divide a r , $m \neq n$ y $m \neq r$; así por definición de divisibilidad $m = tn$ (1) y $r = sm$ (2) con $t, s \in N$; sustituyendo (1) en (2) se tiene que $r = s(tn)$; por propiedad asociativa y clausurativa de la multiplicación de números naturales se concluye que n divide a r y $n \neq r$, lo tanto $n \leq r$.

Las definiciones 2.1 y 2.11 se pueden expresar una en términos de la otra, a través del uso de nociones de lógica, como se expresa en el teorema 2.14.

Teorema 2.14.

- i. Supongamos que $\mathcal{p} = \langle P, \leq \rangle$ es un conjunto parcialmente ordenado, para todo $x, y, \in P$, se define $x < y$ como $x \leq y \wedge x \neq y$. Entonces $\mathcal{p}^- = \langle P, < \rangle$ es un conjunto parcialmente ordenado
- ii. Supongamos lo contrario, sea $\mathcal{L} = \langle Q, < \rangle$ un conjunto estrictamente ordenado y todo $x, y, \in Q$ se define $x \leq y = x < y \vee x = y$. Entonces $\mathcal{L}^+ = \langle Q, \leq \rangle$ es un conjunto parcialmente ordenado.
- iii. El resultado de pasar de un conjunto parcialmente ordenado, a un conjunto estrictamente ordenado tiene un retorno a la estructura original. Es decir $(\mathcal{p}^-)^+ = \mathcal{p}$. De forma similar $(\mathcal{L}^+)^- = \mathcal{L}$.

En relación con el teorema 2.14 se hace necesario aclarar un aspecto de notación que será muy importante de aquí en adelante; como por ejemplo $x < y$ es una abreviación de $x \leq y \wedge x \neq y$, $x \sqsubset y$ es una abreviación de $x \sqsubseteq y \wedge x \neq y$.

2.2.1.3 Funciones entre conjuntos parcialmente ordenados.

En el estudio de las funciones entre conjuntos parcialmente ordenados se destacan cuatro tipos de funciones: función monótona, función antimonótona, función inmersión de orden y función isomorfismo de orden.

Definición 2.15. Supongamos que $\mathcal{p} = \langle P, \leq \rangle$ y $\mathcal{L} = \langle Q, \sqsubseteq \rangle$ son conjuntos parcialmente ordenados. Sea $f: P \rightarrow Q$ una función entre conjuntos y sus relaciones de orden. Entonces

- i) f es monótona si y solo si, para todo $x, y \in P$, si $x \leq y$ entonces $f(x) \sqsubseteq f(y)$;
- ii) f es antimonótona si y solo si, para todo $x, y \in P$ si $x \leq y$ entonces $f(x) \sqsupseteq f(y)$.

Es importante resaltar, que si f es una función monótona preserva relaciones de orden entre imágenes y pre imágenes; mientras si f es una función antimonótona invierte las relaciones de orden de las imágenes respecto a preimágenes.

Observación 2.16. Si una función f es monótona e inyectiva, se considera una **inmersión** de orden; es decir, para todo $x, y \in P$, $x \leq y$ si y solo si $f(x) \sqsubseteq f(y)$.

Definición 2.17. Sea $\mathcal{P} = \langle P, \leq \rangle$ y $\mathcal{L} = \langle Q, \sqsubseteq \rangle$ dos conjuntos parcialmente ordenados; si $f: P \rightarrow Q$ es una función biyectiva y además f, f^{-1} son monótonas entonces f es un isomorfismo de orden.

A continuación se presentan algunos ejemplos de funciones, entre conjuntos parcialmente ordenados.

Ejemplo 2.18. Considere los conjuntos parcialmente ordenados $\langle R^+, \leq \rangle$ y $\langle N, \leq \rangle$, R^+ es el conjunto de los números reales positivos y las relaciones de orden son las usuales. Sea $f: R^+ \rightarrow N$ una función que asigna la parte entera de un real $r \in R^+$ a un número natural $n \in N$. Entonces f es monótona pero no una **inmersión** de orden.

Ejemplo 2.19. Sea $\langle R, \leq \rangle$ y su dual $\langle R, \geq \rangle$, entonces $h: R \rightarrow R$ definida como $h: x \rightarrow -x$ para $x \in R$ es un isomorfismo de orden.

Ejemplo 2.20. Tomando los conjuntos $\langle R^+, \leq \rangle$, $\langle N, \leq \rangle$ y la función $g: N \rightarrow R^+$, donde g asigna un número natural a su correspondiente parte entera en R^+ , note que g es una inmersión de orden pero no un isomorfismo de orden. Debido a que g incrusta una copia de los números naturales en los números reales; pero g no es sobreyectiva.

2.2.1.4 Composición de funciones.

Una operación importante en torno a la teoría de funciones es la composición de funciones, y que centra nuestra atención en algunos teoremas sobre composición de funciones entre conjuntos parcialmente ordenados.

Teorema 2.21. Si $f: P \rightarrow Q$ es una función monótona entre $\mathcal{P} = \langle P, \leq \rangle$ y $\mathcal{L} = \langle Q, \sqsubseteq \rangle$; y $g: Q \rightarrow R$ es una función monótona entre $\mathcal{L} = \langle Q, \sqsubseteq \rangle$ y $\mathcal{R} = \langle R, \leq \rangle$, entonces la función compuesta $g \circ f = P \rightarrow R$ es una función monótona de \mathcal{P} a \mathcal{R} .

Una característica de las funciones compuestas es que cumplen la propiedad asociativa como lo ilustra el siguiente teorema.

Teorema 3.22. La composición de funciones monótonas es asociativa: es decir, si las funciones $f: P \rightarrow Q$, $g: Q \rightarrow R$, y $h: R \rightarrow S$ son monótonas entonces $(f \circ g) \circ h$ y $f \circ (g \circ h)$ son funciones monótonas y además $(f \circ g) \circ h = f \circ (g \circ h)$.

Note que el teorema 2.21 de composición de funciones solo hace referencia a la composición entre funciones monótonas; dejando de lado la función inmersión de orden y la función isomorfismo de orden que también cuentan con la propiedad de composición de funciones.

Teorema 2.23. Si $f: P \rightarrow Q$ es una función inmersión de orden (isomorfismo de orden) entre los conjuntos $\mathcal{P} = \langle P, \leq \rangle$ y $\mathcal{L} = \langle Q, \sqsubseteq \rangle$; y $g: Q \rightarrow R$ es una inmersión de orden (isomorfismo de orden) entre $\mathcal{L} = \langle Q, \sqsubseteq \rangle$ y $\mathcal{R} = \langle R, \leq \rangle$, entonces la función compuesta $g \circ f = P \rightarrow R$ es una función inmersión de orden (isomorfismo de orden) de \mathcal{P} a \mathcal{R} .

2.2.1.5 Similaridad.

Recordemos que una inmersión de orden es una función inyectiva que refleja una correspondencia uno a uno de un conjunto a otro, al igual que las relaciones de orden (observación 2.16), que conservan ordenamientos entre los elementos de cada conjunto. Es por ello que designamos una forma de clasificar funciones equivalentes entre conjuntos parcialmente ordenados mediante la siguiente definición.

Definición 2.24. Los conjuntos parcialmente ordenados \mathcal{P} y \mathcal{L} son de orden similar, en símbolos $\mathcal{P} \cong \mathcal{L}$ si y solo si existe un isomorfismo de orden entre \mathcal{P} y \mathcal{L} .

Ahora consideremos dos aspectos; el primero, es un teorema que relaciona las funciones similares como una relación de equivalencia; el segundo, refleja un ejemplo de conjuntos similares.

Teorema 2.25. Similaridad es una relación de equivalencia.

Ejemplo 2.26. Consideremos los conjuntos parcialmente ordenados $\mathcal{P} = \langle N, \leq \rangle$ y $\mathcal{L} = \langle N, \geq \rangle$ y consideremos la función $h: R \rightarrow R$ definida como $h: x \rightarrow -x$ para $x \in N$; h es isomorfismo de orden entre \mathcal{P} y \mathcal{L} , por lo tanto $\langle N, \leq \rangle$ y $\langle N, \geq \rangle$ son de órdenes similares.

2.2.2 Elementos matemáticos de las Conexiones de Galois.

A partir del estudio de conjuntos parcialmente ordenados y de funciones entre estos conjuntos, se sientan las bases para el estudio de las conexiones de Galois, que es uno de los objetivos a desarrollar en este trabajo. En este sentido, el estudio de las conexiones de Galois, nos permite comprender su significado a través de la inclusión de su definición formal y de algunas proposiciones, que involucran ejemplos de adjunciones; además el estudio de las

conexiones nos permite mostrar como la teoría de Galois (sección 5.1) es un caso particular de una adjunción. Para el estudio de los elementos teóricos de esta sección continuaremos con la referencia de Smith (2010) de la sección anterior.

2.2.2.1 Conexiones de Galois.

Definición 3.27. Sea $\mathcal{P} = \langle P, \leq \rangle$ y $\mathcal{L} = \langle Q, \sqsubseteq \rangle$ conjuntos parcialmente ordenados y supongamos que $f_*: P \rightarrow Q$ y $f^*: Q \rightarrow P$ son un par de funciones tales que para todo $x \in P$ y todo $y \in Q$ se cumple que

$$f_*(x) \sqsubseteq y \text{ si y solo si } x \leq f^*(y).$$

Entonces el par $\langle f_*, f^* \rangle$ forman una conexión de Galois, donde f_* se conoce como adjunto izquierdo o inferior y f^* se conoce como adjunto derecho o superior.

Para comprender de forma amplia la definición anterior se hace necesario explorar algunos ejemplos.

Proposición 2.28. Suponga que f es un isomorfismo de orden entre $\mathcal{P} = \langle P, \leq \rangle$ y $\mathcal{L} = \langle Q, \sqsubseteq \rangle$, si se tiene una función inversa f^{-1} que también es un isomorfismo de orden, entonces $\langle f, f^{-1} \rangle$ forman una conexión de Galois.

Demostración: Sea $x \in P$ y $y \in Q$, por definición de imagen directa se tiene la relación $f(x) \in Q$ y $f^{-1}(y) \in P$. Supongamos que $y \sqsubseteq f(x)$ como f^{-1} es un orden isomorfismo, por la definición 2.14 es una orden inmersión entonces $f^{-1}(y) \leq f^{-1}(f(x))$ que es equivalente $f^{-1}(y) \leq x$. Análogamente, sea $f^{-1}(y) \leq x$ como f es un orden isomorfismo,

por la definición 2.17 es una inmersión de entonces $f(f^{-1}(y)) \sqsubseteq f(x)$ que es equivalente $y \sqsubseteq f(x)$. Por lo tanto $\langle f, f^{-1} \rangle$ es una conexión de Galois ■

Proposición 2.29. Sea $\mathcal{P} = \langle N, \leq \rangle$ y $\mathcal{L} = \langle Q^+, \leq \rangle$, en cada caso el orden usual, considere la función $f_*: N \rightarrow Q^+$ una inmersión estándar de un número natural a un número racional positivo y la función $f^*: Q^+ \rightarrow N$ que asigna un $q \in Q^+$ su correspondiente parte entera en N . Entonces el par adjunto $\langle f_*, f^* \rangle$ es una conexión de Galois entre los números racionales positivos y los números naturales.

Demostración: Sea $n \in N$, $q \in Q^+$ y $f_*(n) = \frac{n}{1} = n$; tal que $f_*(n) \in Q^+$ y que $f^*(p) \in N$. Supongamos que $f_*(n) \leq p$, por lo tanto $f^*(p) = n + k$ con $k \in N$; entonces $n \leq f^*(p)$. Ahora, sea $n \leq f^*(p)$ con $f_*(n) = n$ y notemos que $f^*(p) \leq p$ por lo tanto se concluye que $f_*(n) \leq p$ ■

Proposición 2.30. Considere el conjunto arbitrario $\mathcal{P} = \langle P, \leq \rangle$ y el conjunto $\mathcal{L} = \langle \{0\}, = \rangle$. Sea $f_*: P \rightarrow \{0\}$, tal que $f_*(p) = 0$, $p \in P$ y $f^*: \{0\} \rightarrow P$ es tal que $f^*(0) = p$, para algún $p \in P$. Entonces el par adjunto $\langle f_*, f^* \rangle$ es una conexión de Galois entre \mathcal{P} y \mathcal{L} si y solo si para cada $p \in P$; $f_*(p) = 0$ si y solo si $p \leq f^*(0)$, si y solo si $f^*(0)$ es el máximo en P .

Demostración: Sea $p \in P$ entonces $f_*(p) = 0$; por otra parte se tiene que $f^*(0) = q$ para $q \in P$. Supongamos que $p \leq f^*(0)$ entonces $f_*(p) = 0$ lo cual siempre es cierto porque el consecuente es verdadero por la definición de f_* . Por otra parte, sea $p, q \in P$ y por hipótesis $q = f^*(0)$ es el máximo, entonces $p \leq q$ lo que significa que $p \leq f^*(0)$; por lo tanto si $f_*(p) = 0$ entonces $p \leq f^*(0)$ porque análogamente el consecuente es verdadero. En conclusión $\langle f_*, f^* \rangle$ es una conexión de Galois entre \mathcal{P} y \mathcal{L} ■

2.2.2.2 Definición alternativa.

Es conveniente enunciar una definición alternativa de conexión de Galois, precisando que la definición anterior y esta son equivalentes, y su diferencia básicamente se hace notoria en la notación empleada. Para esto se toma como referencia el libro de Roman (2008). Además en esta sección se enuncian dos teoremas respecto a las adjunciones, para complementar el estudio del concepto de adjunción, lo cual le permite al lector tener una visión amplia, de los diferentes aspectos matemáticos y de notación que involucra una conexión.

Definición 2.31. Sea $\mathcal{P} = \langle P, \leq \rangle$ y $\mathcal{L} = \langle Q, \sqsubseteq \rangle$ conjuntos parcialmente ordenados. Una conexión de Galois entre \mathcal{P} y \mathcal{L} , con las funciones $f: P \rightarrow Q$ y $g: Q \rightarrow P$ es tal que $f(x) = x^*$ y $g(y) = y'$, con las siguientes propiedades:

- i) f y g son antimonótonas.
- ii) Para todo $x \in P$, $y \in Q$, $x \leq x^*$ y $y^* \sqsubseteq y$

Teorema 2.32. Si $\langle f_*, f^* \rangle$ son una conexión de Galois entre $\mathcal{P} = \langle P, \leq \rangle$ y $\mathcal{L} = \langle Q, \sqsubseteq \rangle$ entonces

- i) $f^*(y) = \max \{x \in P / f^*(x) \sqsubseteq y \}$
- ii) $f_*(x) = \min \{y \in Q / x \leq f^*(y)\}$

3. UN ACERCAMIENTO A LA TEORÍA DE GALOIS DESDE UNA PERSPECTIVA MODERNA.

“Las leyes de la matemática no son meramente invenciones o creaciones humanas. Simplemente “son”: existen independientemente del intelecto humano. Lo más que puede hacer un hombre de inteligencia aguda es descubrir que esas leyes están allí y llegar a conocerlas.”

Mauritis Cornelis Escher

Después de estudiar la teoría de adjunciones (conexiones de Galois) desde una perspectiva histórica y moderna en el capítulo anterior, este capítulo se centra en realizar un acercamiento a la teoría de Galois desde una perspectiva moderna tomando como referencia el libro de David S. Dummit y Richard M. Foote (2003) *“Abstract Algebra”* lo cual le permitirá al lector realizar un acercamiento a esta teoría. Además los aspectos abordados en este capítulo nos brindaran las bases teóricas para abordar dos elementos. El primero, permitirá nuevamente el estudio de la teoría de Galois en el siguiente capítulo, pero esta vez desde una representación histórica a través del estudio del capítulo 14 del texto *“Galois’ Theory of Algebraic Equations”* escrita por Jean-Pierre Tinol (2011) en la cual se realiza una reescritura de la memoria de Galois; y el segundo, nos permitirá mostrar la teoría de Galois como un caso particular de una adjunción en el capítulo final, tomando como referencia el ejemplo 3.14 de la página 59 del libro de Steven Román (2008) *“Lattices and ordered sets”*, el cual enuncia la teoría de Galois como una adjunción.

3.1 Teoría de cuerpos.

La teoría de cuerpos juega un papel esencial en la teoría de Galois y por este motivo, hemos dedicado esta sección a estudiar algunos elementos de esta teoría, de los cuales se destacan: las nociones básicas de la teoría de extensiones, extensiones algebraicas, cuerpos de descomposición y extensiones separables. Además, estas temáticas nos permitirán realizar un recorrido de los distintos elementos que componen la teoría de Galois, a través de la ejemplificación de algunos elementos que se distinguen como ejemplos del teorema fundamental de la teoría de Galois. Por otra parte, para una mejor comprensión de los elementos abordados en esta sección y en la siguiente se le recomienda al lector un estudio previo de nociones de teoría de grupos y teoría de anillos; las cuales no serán abordadas en este documento.

3.1.1 Nociones básicas de la teoría de extensiones.

En esta sección abordaremos las nociones básicas de la teoría de extensiones, más un breve repaso de las definiciones de grupo, subgrupo y anillos; con la intención de conocer paso a paso cada uno de los elementos del teorema fundamental de la teoría de Galois, lo que le permitirá al lector una mejor comprensión de este teorema y de sus ejemplos. Para exponer las nociones básicas teoría de extensiones tomaremos como referencia el trabajo de Dummit y Richard M. Foote (2003), en el cual además se puede profundizar si el lector lo desea, en el estudio de la teoría de grupos y anillos.

Definición 3.1. Un grupo es par ordenado $(G, *)$, donde G es un conjunto y $*$ es una operación binaria en G que cumple los siguientes axiomas:

- i.* Es asociativa

- ii. Existe el elemento neutro e en G , que cumple $a * e = a$ para todo $a \in G$.
- iii. Existe el elemento inverso en G , que cumple $a * a^{-1} = e$ para todo $a \in G$.

Definición 3.2. Un grupo $(G,*)$ es llamado abeliano si es un grupo que satisface la propiedad asociativa para $*$.

Ejemplo 3.3. El conjunto de los números enteros con la suma es un grupo y se denota $(\mathbb{Z}, +)$.

Ejemplo 3.4. El grupo $(\mathbb{Z}, +)$ es un grupo abeliano, debido a que la operación $+$ satisface la propiedad conmutativa.

Ejemplo 3.5. El conjunto de los racionales menos el cero es un grupo abeliano con la multiplicación.

Definición 3.6. Sea G un grupo. El subconjunto H de G es un subgrupo de G si es no vacío y H es cerrado para el producto de dos elementos de H y sus inversos. Es decir, si $x, y \in H$ implica que $x^{-1} \in H$ y $xy \in H$. Si H es un subgrupo de G se denota $H \leq G$.

Definición 3.7. Un anillo es un conjunto R con dos operaciones binarias $+$ y \cdot (llamadas adición y multiplicación) que satisfacen los siguientes axiomas:

- i. $(R, +)$ es un grupo abeliano
- ii. La operación \cdot es asociativa
- iii. la operación \cdot es distributiva respecto a $+$, es decir, $\forall a, b, c \in R$, se cumple

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

Definición 3.8. Un anillo R es conmutativo si \cdot es conmutativo.

Definición 3.9 Un anillo R es llamado unitario si la operación \cdot tiene elemento neutro. Es decir, $1 \in R$ y se satisface

$$1 \cdot a = a \cdot 1 = a$$

para todo $a \in R$.

Ejemplo 3.10. El conjunto de los números racionales con las operaciones de suma y multiplicación es un anillo.

Definición 3.11. Un anillo polinomial $R[x]$ en la variable x con coeficientes en R es el conjunto formado por la suma $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ con $n \geq 0$ y $a_i \in R$.

Ejemplo 3.12. El conjunto de los números complejos con las operaciones de suma y multiplicación es un anillo.

Definición 3.13. Un **cuerpo** es un anillo conmutativo, unitario no trivial.

Ejemplo 3.14. El conjunto de los números reales es un cuerpo.

Ejemplo 3.15. El conjunto de los números racionales es un cuerpo.

Ejemplo 3.16. El conjunto de la clase residual de los números primos, denotados Z_p es un cuerpo.

Definición 3.17. Sea K un cuerpo. Un subcuerpo F de K es un subconjunto de K con las operaciones de K y estructura de cuerpo no trivial.

Definición 3.18. La característica de un cuerpo F , denotada $ch(F)$, es definida como el entero positivo p más pequeño tal que $p \cdot 1_F = 0$, si existe p y en caso contrario el cuerpo es de característica cero.

Definición 3.19. El subcuerpo primo de un cuerpo F , es un subcuerpo de F generado por la identidad multiplicativa 1_F de F . Esto es (isomorfo a) o bien Q (es $ch(F) = 0$) o F_p (es $ch(F) = p$).

Ejemplo 3.20. La característica del cuerpo de los números reales es $ch(R) = 0$, debido a, que se puede establecer un isomorfismo entre R y Q .

Ejemplo 3.21. La característica del conjunto de la clase residual de los números primos $ch(Z_p) = p$.

Definición 3.22. Si K es un cuerpo que contiene al subcuerpo F , entonces K es conocido como una extensión del cuerpo (o simplemente extensión) de F , denotado K/F que se representan en el diagrama

$$\begin{array}{c} K \\ \uparrow \\ F \end{array}$$

En particular, el cuerpo K es una extensión de su subcuerpo primo. El cuerpo K es a veces llamado el cuerpo base de la extensión.

Observación 3.23. La notación K/F para una extensión de cuerpo, es una abreviatura de “ K sobre F ”.

Si K/F es una extensión de cuerpos, entonces la multiplicación en K , hace en K un espacio vectorial sobre F . En particular cada cuerpo K_F se puede considerar un espacio vectorial sobre su subcuerpo primo.

Definición 3.24. El grado (o grado relativo o índice) de la extensión K/F , denotado $[K:F]$, es la dimensión de K como un espacio vectorial sobre F (es decir $[K:F] = \dim(K_F)$). La extensión es llamada finita si $[K:F]$ es finito y en caso contrario es infinita.

Una clase importante de extensiones de cuerpo, son las obtenidas al tratar de resolver una ecuación en más de un cuerpo F . Para ilustrar lo anterior consideremos el siguiente ejemplo

Ejemplo 3.25. Sea $F = \mathbb{R}$ el cuerpo de los números reales, entonces la ecuación $x^2 + 1 = 0$ no tiene solución en F . Entonces surge el interrogante si existe un cuerpo que contiene a \mathbb{R} tal que la ecuación tiene solución, este interrogante se resuelve al introducir el cuerpo de los números complejos $\mathbb{C} = \mathbb{R} + Ri$, donde i es la solución de la ecuación representada por la relación $i^2 + 1 = 0$.

Ampliando el concepto reflejado en el ejemplo 3.25 consideremos un cuerpo F y un polinomio $p(x) \in F[x]$, donde $p(x) = 0$ no tiene solución en el cuerpo F , entonces planteemos el siguiente interrogante ¿existe la extensión K de F tal que $p(x) = 0$ tiene solución en K ? (es decir las raíces de $p(x)$ están en K y no en F). Como $p(x)$ no tiene solución en $F[x]$ entonces $p(x)$ es irreducible² en $F[x]$, en consecuencia este polinomio no se puede expresar como el producto de factores lineales en $F[x]$, pero sí en un cuerpo que contiene F . Por lo tanto, la respuesta a este interrogante es si. Lo que nos permite explorar los siguientes resultados referentes a homomorfismos entre cuerpos.

² Un polinomio $p(x)$ es irreducible en un cuerpo $F[x]$, si las raíces de $P(x)$ no están en F .

Proposición 3.26. Sea $\varphi: F \rightarrow F$ un homomorfismo entre cuerpos. Entonces φ es idénticamente 0 o es inyectiva. Así se tiene, que la imagen de φ es cero o un isomorfismo de F .

Teorema 3.27. Sea F un cuerpo y sea $p(x) \in F[x]$ un polinomio irreducible en F . Entonces existe un cuerpo K que contiene un isomorfismo que copia el cuerpo F a través de las raíces de $p(x)$. Este isomorfismo muestra que existe una extensión K de F que contiene una raíz de $p(x)$.

Teorema 3.28. Sea F un cuerpo y sea $p(x) \in F[x]$ un polinomio irreducible de grado n sobre el cuerpo F y sea el cuerpo $K = F[x]/(p(x))$. Sea $\theta = x \text{ mod}(p(x)) \in K$. Entonces los elementos

$$1, \theta, \theta^2 \dots \theta^{n-1}$$

son la base para el espacio vectorial K sobre el cuerpo F , entonces el grado de la extensión $[K:F] = n$. Donde

$$K = \{a_0, a_1\theta, a_2\theta^2, \dots, a_{n-1}\theta^{n-1} : a_0, a_1, \dots, a_{n-1} \in F\}$$

se compone de polinomios de grado $< n$.

Otro importante resultado que se desprende del teorema anterior es el siguiente

Teorema 3.29. Sea K el cuerpo del teorema anterior y sea $a(\theta), b(\theta) \in K[x]$ polinomios de grado menor a n en θ . Entonces se define la adición en K como la adición usual de polinomios y la multiplicación en K se define como

$$a(\theta).b(\theta) = r(\theta).$$

Para comprender un poco mejor los conceptos anteriores consideremos los siguientes ejemplos.

Ejemplo 3.30. Consideremos el cuerpo $F = R$ y el polinomio $p(x) = x^2 + 1$ entonces se obtiene la extensión

$$R[x]/(p(x))$$

que es una extensión de grado 2, debido a que $p(x)$ es irreducible en R y $p(x)$ es un polinomio de grado 2. Los elementos de este cuerpo son de la forma $a + b\theta$ con $a, b \in R$, y se define la adición como

$$(a + b\theta) + (c + d\theta) = (a + c) + (b + d)\theta.$$

Y la multiplicación, teniendo en cuenta que $\theta^2 + 1 = 0$, $\theta^2 = -1$ como

$$(a + b\theta)(c + d\theta) = (ac - bd) + (ad + bc)\theta.$$

Note que al cambiar $\theta = i$ las operaciones de multiplicación y suma de la extensión son equivalentes a las operaciones del cuerpo de los números complejos \mathbb{C} . Descrito de otra forma, considere la función

$$\begin{aligned} \varphi: R[x]/(x^2 + 1) &\rightarrow \mathbb{C} \\ a + bx &\rightarrow a + bi \end{aligned}$$

como φ es isomorfismo entonces como consecuencia del teorema anterior se puede considerar la extensión $R[x]/(x^2 + 1) \cong \mathbb{C}$.

Ejemplo 3.31. Sea $F = Q$ y $P(x) = x^2 - 2$ que es irreducible en Q por el criterio de Eisenstein³. Entonces se obtiene la extensión de Q de grado 2 que contiene la raíz θ de P , denotado $Q(\theta)$. Donde la base está dada por

$$B = \{a + b\theta\} \quad a, b \in Q.$$

Note que $\theta = \sqrt{2}$, y se define la suma como

$$(a + b\sqrt{2}) + (c + d)\sqrt{2} = (a + c) + (b + d)\sqrt{2}$$

y la multiplicación

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Es importante continuar con este estudio, por lo tanto es conveniente revisar las siguientes definiciones

Definición 3.32. Sea K una extensión del cuerpo F y sea $\alpha, \beta, \dots \in K$ una colección de elementos sobre K . Entonces el subcuerpo más pequeño de K que contiene a F y los elementos α, β, \dots , es llamado el cuerpo generado por α, β, \dots sobre F y se denota $F(\alpha, \beta, \dots)$.

Definición 3.33. Si el cuerpo K es generado por un único elemento α sobre F , es decir, se representa como $K = F(\alpha)$, entonces K es llamado una extensión simple de F y el elemento α es llamado el elemento primitivo de la extensión.

Es importante tener en consideración que una extensión simple de un cuerpo F , es una extensión de característica cero.

³ Sea $P \in Z[x]$, $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, con $a_n \neq 0$. Supongamos que existe un número primo p tal que p/a_j para todo $0 \leq j \leq n-1$, $p \nmid a_n$ y $p^2 \nmid a_0$. Entonces p es irreducible en $Q[x]$.

La conexión entre la extensión simple $F(\alpha)$ generado por α sobre F , donde α es la raíz de un polinomio irreducible $p(x)$ sobre F y la construcción del cuerpo del teorema 3 es proporcionado por el siguiente teorema

Teorema 3.34. Sea F un cuerpo y sea $p(x) \in F[x]$ un polinomio irreducible en F . Suponga que K es un extensión de cuerpo de F que contiene la raíz α de $p(x): p(\alpha) = 0$. Sea $F(\alpha)$ un subcuerpo de K generado por α sobre F , entonces

$$F(\alpha) \cong F[x]/p(x)$$

Corolario 3.35. Supongamos que el polinomio del teorema 3.34 es de grado n . Entonces

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, \dots, a_{n-1}\} \subseteq K$$

Ejemplo 3.36. Consideremos el ejemplo 3.31, que determina el cuerpo $Q[\sqrt{2}]$ sobre Q por el elemento $\sqrt{2} \in R$, que es determinado por la solución del polinomio $x^2 - 2 = 0$.

Ejemplo 3.37. Sea la ecuación $x^2 + 2 = 0$ con una solución en R , llamada $-\sqrt{2}$. Entonces el cuerpo generado por $-\sqrt{2}$ sobre Q tiene elementos de la forma $\{a + b(-\sqrt{2})/a, b \in Q\}$ y es isomorfo al cuerpo generado por $\sqrt{2}$. Este isomorfismo se representa mediante la función

$$a + b(\sqrt{2}) \rightarrow a - b(\sqrt{2}).$$

3.1.2 Extensiones algebraicas.

Las extensiones algebraicas juegan un papel importante en el teorema fundamental de la teoría de Galois, debido a que para determinar la solución de una ecuación empleamos una extensión generada por una o unas raíces de este polinomio. En consecuencia, esta sección está dedicada a conocer teoremas y definiciones que le permite al lector la comprensión de qué es una extensión algebraica y

posteriormente su papel en la teoría de Galois. Para el desarrollo de esta sección seguiremos con la referencia de Dummit y Richard M. Foote (2003).

Sea F un cuerpo y K una extensión de F .

Definición 3.38. Sea $\alpha \in K$; α es un elemento algebraico sobre F , si α es la raíz de un polinomio no nulo $f(x) \in F[x]$. Si α no es algebraico sobre F se dice que α es trascendente sobre F . La extensión K/F es llamada algebraica si todo elemento de K es algebraico sobre F .

Observación 3.39. Si α es algebraico sobre el cuerpo F entonces es algebraico para alguna extensión L sobre F . (Si $P(x)$ tienes raíces, con coeficientes en F también los tiene en L).

Proposición 3.40. Sea α un elemento algebraico sobre F . Entonces existe un único polinomio mónico irreducible $m_{\alpha,F}(x) \in F[x]$ tal que el elemento α es una raíz. Un polinomio $f(x) \in F(x)$ tiene como raíz α si y solo si el polinomio $m_{\alpha,F}(x)$ divide a $f(x)$ en $F(x)$.

Corolario 3.41. Si L/F es una extensión de cuerpo y α es algebraico sobre F y L entonces $m_{\alpha,L}(x)$ divide a $m_{\alpha,F}(x)$ en el cuerpo $L[x]$.

Definición 3.42. El polinomio $m_{\alpha,F}(x)$ es llamado el polinomio mínimo de α sobre F . El grado de $m_{\alpha,F}(x)$ es llamado el grado de α .

Observación 3.43. La definición anterior hace parte esencial de una extensión algebraica puesto que toda extensión es generada a partir de las raíces de un polinomio mínimo.

Proposición 3.44. Sea α un elemento algebraico sobre el cuerpo F y sea $F(\alpha)$ el cuerpo generado por α sobre F . Entonces

$$F(\alpha) \cong F[x]/(m_\alpha(x))$$

de modo que

$$[F(\alpha):F] = \text{grado } m_\alpha(x) = \text{grado } \alpha,$$

es decir el grado de α sobre F es igual al grado de la extensión generada sobre F .

Ejemplo 3.45. El polinomio mínimo de la extensión $\sqrt{2}$ sobre Q es $x^2 - 2$ el cual es un polinomio de grado 2 sobre Q , entonces el grado de la extensión $[Q[\sqrt{2}]:Q] = 2$.

Ejemplo 3.46. De forma similar al ejemplo 3.45, consideremos el polinomio $x^n - 2$ que es irreducible sobre el cuerpo Q por el criterio de Eisenstein. Denotando una de sus raíces como $\sqrt[n]{2}$ entonces el grado de la extensión $Q[\sqrt[n]{2}]$ sobre Q es igual a n .

Los dos ejemplos anteriores y en especial el primero, nos sirven de referencia para definir el cuerpo de descomposición de una ecuación, que una de las dos grandes partes del teorema fundamental de la teoría de Galois.

Teorema 3.47. Sea $F \subseteq K \subseteq L$ extensiones finitas de cuerpos. Entonces

$$[L:F] = [L:K][K:F],$$

es decir, el grado de la extensión es multiplicativo.

Teorema 3.48. Suponga L/F es una extensión finita de cuerpo y sea K un sub cuerpo de L que contiene a F , y $F \subseteq K \subseteq L$. Entonces $[K:F]$ divide a $[L:F]$.

Ejemplo 3.49. Determinemos el grado de la extensión $Q[\sqrt[6]{2}]/Q[\sqrt{2}]$. Para ello consideremos la extensión $Q[\sqrt[6]{2}]$ sobre Q , donde $[Q[\sqrt[6]{2}]:Q] = 6$ y la extensión $Q[\sqrt{2}]/Q$

donde $[Q[\sqrt{2}]:Q] = 2$. Por otro lado, note que $(\sqrt[6]{2})^3 = \sqrt{2}$ en consecuencia se cumple que $Q[\sqrt{2}] \subset Q[\sqrt[6]{2}]$ y al aplicar el teorema 3.28

$$[Q[\sqrt[6]{2}]:Q] = [Q[\sqrt{2}]:Q][Q[\sqrt[6]{2}]:Q[\sqrt{2}]]$$

se concluye que

$$[Q[\sqrt[6]{2}]:Q[\sqrt{2}]] = 3.$$

En particular el polinomio mínimo de $\sqrt[6]{2}$ sobre $Q[\sqrt{2}]$ es de grado tres. El cual está dado por $x^3 - \sqrt{2}$ debido a que este es un polinomio irreducible sobre $Q[\sqrt{2}]$.

El ejemplo anterior hace evidente que se pueden relacionar dos raíces de un polinomio para generar una extensión de cuerpo que contenga a ambas. También nos presenta el modo de determinar el grado de una extensión que es generada por más de un elemento algebraico.

Definición 3.50. Una extensión K/F es finitamente generada por los elementos $\alpha_1, \alpha_2, \dots, \alpha_k$ en K de tal manera que $K = F(\alpha_1, \alpha_2, \dots, \alpha_k)$.

Observación 3.51. El cuerpo $F(\alpha_1, \alpha_2, \dots, \alpha_k)$ es el cuerpo más pequeño que contiene a F y todos los elementos $\alpha_1, \alpha_2, \dots, \alpha_k$. Además es generado por un encadenamiento de sucesiones simples correspondientes a los elementos $\alpha_1, \alpha_2, \dots, \alpha_k$.

Lema 3.52. La extensión $F(\alpha, \beta) = (F(\alpha))(\beta)$, es decir es el cuerpo generado sobre F por α y β , se construye a partir del cuerpo generado por β sobre $F(\alpha)$ generado por α .

Teorema 3.53. La extensión K/F es finita si y solo si K es generado por un número finito de elementos algebraicos sobre F . Más concretamente, un cuerpo generado sobre F por un

número finito de elementos algebraicos de grados n_1, n_2, \dots, n_k es algebraico y de grado es p tal que se cumple la condición $p \leq n_1, n_2, \dots, n_k$.

Teorema 3.54. Supongamos α y β son algebraicos sobre F . Entonces $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ ($\beta \neq 0$) son algebraicos sobre F .

Teorema 3.55. Sea L/F una extensión arbitraria. Entonces la colección de elementos de L son algebraicos sobre F y forman un subcuerpo K de L .

Ejemplo 3.56. Consideremos el cuerpo $Q(\sqrt{2}, \sqrt{3})$ generado sobre Q por $\sqrt{2}$ y $\sqrt{3}$. Note que la extensión generada por $\sqrt{3}$ sobre Q es de grado 2, entonces el grado de la extensión $Q(\sqrt{2}, \sqrt{3})/Q(\sqrt{2})$ es como máximo 2 y es precisamente 2 si y solo si el polinomio mínimo de $\sqrt{3}$ sobre Q $x^2 - 3$ es irreducible sobre $Q(\sqrt{2})$. Probaremos ahora que $x^2 - 3$ es irreducible sobre $Q(\sqrt{2})$ para ello es suficiente con demostrar que $\sqrt{3} \notin Q(\sqrt{2})$. Utilizando el método de contradicción supongamos que $\sqrt{3} \in Q(\sqrt{2})$ por lo tanto $\sqrt{3}$ se puede expresar como $\sqrt{3} = a + b\sqrt{2}$ con $a, b \in Q$. Al elevar a ambos lados al cuadrado se obtiene la relación $3 = (a^2 + 2b^2) + 2ab\sqrt{2}$. Ahora si $ab \neq 0$ entonces $\sqrt{2}$ es un racional lo cual es una contradicción. Si $b = 0$ entonces $3 = a^2$ por lo tanto $a = \sqrt{3}$ lo cual contradice que $a \in Q$. Finalmente si $a = 0$ entonces $\sqrt{3} = b\sqrt{2}$ donde b es un múltiplo de $\sqrt{6}$ (racionalizando la solución de la ecuación $\sqrt{3} = b\sqrt{2}$) por lo tanto es un irracional lo que contradice que $b \in Q$. En consecuencia, $x^2 - 3$ es irreducible sobre $Q(\sqrt{2})$; $[Q(\sqrt{2}, \sqrt{3})/Q(\sqrt{2})/Q: Q] = 4$ y la base para la extensión $Q(\sqrt{2}, \sqrt{3})/Q(\sqrt{2})$ sobre Q es

$$\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} / a, b, c, d \in Q\}.$$

3.1.3 Cuerpos de descomposición⁴.

En esta sección se articulan lo visto en las dos secciones anteriores, puesto que en esta sección se busca determinar el cuerpo más pequeño que contiene las raíces de un polinomio irreducible sobre un cuerpo dado. Además en esta sección se presentan una serie de ejemplos que hacen parte de las representaciones del teorema de la teoría de Galois.

Sea F un cuerpo. Si $f(x)$ es un polinomio en $F[x]$ entonces por lo abordado en la sección 3.1.2 existe un cuerpo K , que es considerado una extensión de F que contiene una raíz α de $f(x)$. Esto es equivalente a que existe un factor lineal $x - \alpha$ de $f(x)$ tal que, este pertenece a $K[x]$.

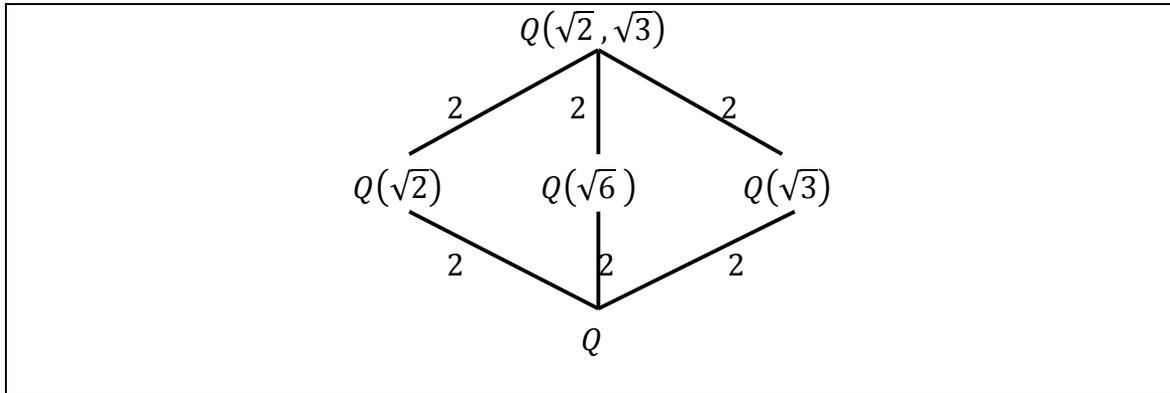
Definición 3.57. La extensión K de F es llamada un cuerpo de descomposición para el polinomio $f(x) \in F[x]$, si $f(x)$ se puede descomponer completamente como el producto de factores lineales en $K[x]$. Si $f(x)$ no se puede descomponer completamente como el producto de factores sobre $K[x]$ entonces K es un subcuerpo propio del cuerpo de descomposición de F tal que K contiene a F .

Teorema 3.58. Para todo cuerpo F , si $f(x) \in F[x]$ entonces existe una extensión K de F que es un cuerpo de descomposición para $f(x)$.

Definición 3.59. Si K es una extensión algebraica de F , el cual es cuerpo de descomposición sobre F para una colección de polinomios $f(x) \in F[x]$ es llamado una extensión normal sobre F .

⁴ Este término se conocido en inglés como Splitting field

Ejemplo 3.60. El cuerpo de descomposición para el polinomio $(x^2 - 2)(x^2 - 3)$ es la extensión $Q(\sqrt{2}, \sqrt{3})$ generado sobre Q por $\sqrt{2}$ y $\sqrt{3}$, donde las raíces del polinomio son $\pm\sqrt{2}$ y $\pm\sqrt{3}$. Note que el grado de esta extensión es cuatro y se puede representar mediante el siguiente diagrama



Ejemplo 3.61. Calculemos el cuerpo de descomposición para el polinomio $x^3 - 2$ que no es $Q(\sqrt[3]{2})$ como se podría pensar previamente. Debido a, que las raíces del polinomio están dadas por

$$\sqrt[3]{2}, \quad \sqrt[3]{2} \left(\frac{-1 + i\sqrt{3}}{2} \right), \quad \sqrt[3]{2} \left(\frac{-1 - i\sqrt{3}}{2} \right)$$

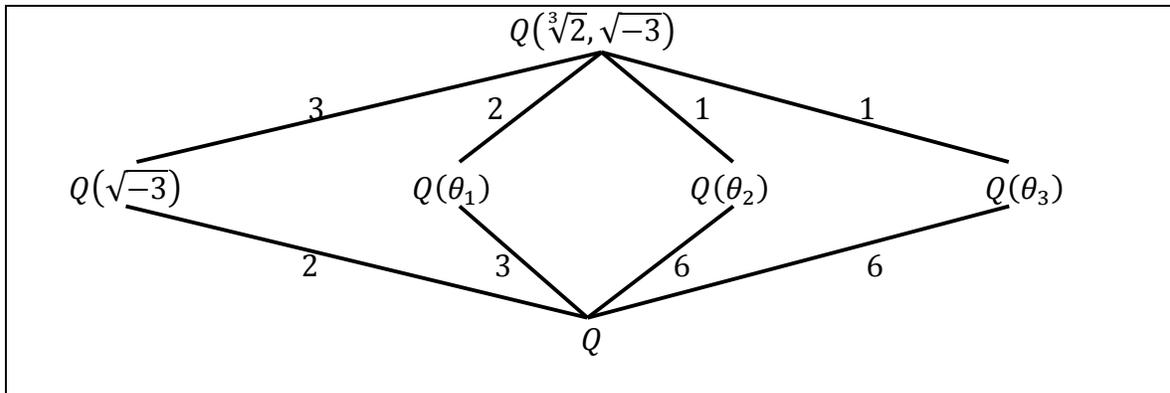
y no son elementos de $Q(\sqrt[3]{2})$, puesto que no se pueden expresar como una combinación lineal de $a, b\sqrt[3]{2}, c\sqrt[3]{4}$, con $a, b, c \in Q$.

Por otra parte, el cuerpo de descomposición K se obtiene a través de la adjunción de todas las raíces del polinomio sobre Q , en este sentido, note que, las raíces del polinomio contiene los elementos $\sqrt{-3}$ y $\sqrt[3]{2}$ por lo tanto el cuerpo de descomposición del polinomio $x^3 - 2$ sobre Q está dado por

$$K = Q(\sqrt[3]{2}, \sqrt{-3}).$$

Nos interesa calcular el grado de la extensión $(\sqrt[3]{2}, \sqrt{-3})$ sobre Q . Para ello, consideremos el polinomio $x^2 + 3$ que es irreducible en Q , y $\sqrt{-3}$ es una de sus raíces, por lo tanto se obtiene la extensión $Q(\sqrt{-3})/Q$ de grado 2 que divide a $[K: Q]$. Además, si consideremos la extensión $Q(\sqrt[3]{2})$ sobre Q con $[Q(\sqrt[3]{2}): Q] = 3$ concluimos que $[Q(\sqrt[3]{2}, \sqrt{-3}): Q] = 6$.

En consecuencia, el cuerpo de descomposición está dado por



Donde

$$\theta_1 = \sqrt[3]{2}, \quad \theta_2 = \sqrt[3]{2} \left(\frac{-1 + i\sqrt{3}}{2} \right), \quad \theta_3 = \sqrt[3]{2} \left(\frac{-1 - i\sqrt{3}}{2} \right).$$

Proposición 3.42. Si K es un cuerpo de descomposición de un polinomio de grado n sobre el cuerpo F entonces $[K: F] = n!$.

Los dos ejemplos anteriores nos muestran la forma en que se articulan extensiones simples para generar un campo de descomposición. Además estos dos ejemplos son claves en la explicación del teorema de Galois como una adjunción, puesto que hacen parte de los elementos que ejemplifican este teorema.

3.1.4 Extensiones separables.

Sea F un cuerpo y sea $f(x) \in F(x)$ un polinomio, sobre un cuerpo de descomposición para el cual se tiene la factorización

$$f(x) = (x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \dots (x - \alpha_k)^{n_k}$$

donde $\alpha_1, \alpha_2, \dots, \alpha_k$ son elementos distintos y $n_i \geq 1$ para todo i . Recordemos que α_i es llamada raíz múltiple si $n_i > 1$ y es llamada raíz simple si $n_i = 1$. Y n_i es llamado multiplicidad de α_i .

Definición 3.62. Un polinomio sobre F es llamado separable si todas las raíces del polinomio son diferentes, es decir, de multiplicidad uno.

Ejemplo 3.63. El polinomio $x^2 - 2$ es separable sobre Q , debido a, que las raíces $\sqrt{2}$ y $-\sqrt{2}$ son diferentes.

Es necesario mencionar cuando un polinomio es separable y los criterios para determinar si un polinomio posee esta característica, debido a que el teorema de Galois se aplica solo a polinomios separables, dejando de lado a polinomios que tienen raíces multiplicidad mayor a uno.

Definición 3.64. La derivada de un polinomio

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

es definida como

$$D_x f(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1$$

Proposición 3.65. Un polinomio $f(x)$ tiene una raíz múltiple α si y solo si α también es una raíz del polinomio $D_x f(x)$, es decir, $f(x)$ y $D_x f(x)$ son divisibles por el polinomio mínimo de α . En particular, $f(x)$ es separable si y solo si $(f(x), D_x f(x)) = 1$ son primos relativos.

3.2 Teoría de Galois.

En esta sección se dará a conocer el teorema fundamental de la teoría de Galois y dos ejemplos que representan la aplicabilidad de este teorema. Además se presentan algunas definiciones necesarias para definir este teorema.

3.2.1 Definiciones básicas.

Con el desarrollo de esta sección se busca definir otros elementos que hacen parte de la teoría de Galois. Lo que le permite al lector un acercamiento más concreto a este teorema y de paso su interpretación como una adjunción.

Definición 3.66. Un isomorfismo σ de el cuerpo K con si mismo es llamado un automorfismo de K . La colección de automorfismos de K es denotado como $Aut(K)$. Si $\alpha \in K$ escribiremos $\alpha\sigma$ o $\sigma(\alpha)$.

Definición 3.67. Un automorfismo $\sigma \in Aut(K)$ se dice que fija un elemento $\alpha \in K$ si se cumple que $\sigma(\alpha) = \alpha$. Si F es un subconjunto de K (por ejemplo un subcuerpo), entonces un automorfismo σ se dice que fija a F si para todo elemento de F , $\sigma(a) = a$.

Definición 3.68. Sea K/F una extensión de cuerpo. Sea $Aut(K/F)$ la colección de automorfismos de K que fija F .

Proposición 3.69. El conjunto $Aut(K)$ es un grupo bajo la composición y $Aut(K/F)$ es un subgrupo de $Aut(K)$.

Proposición 3.70. Sea K/F una extensión de cuerpo y sea $\alpha \in K$ un elemento algebraico sobre F . Entonces para todo $\sigma \in \text{Aut}(K/F)$, $\sigma(\alpha)$ es una raíz del polinomio mínimo de α sobre F , es decir, las permutaciones de $\text{Aut}(K/F)$ se realizan con las raíces de un polinomio irreducible sobre el cuerpo F . Y de forma equivalente si un polinomio con coeficientes en F tiene una raíz α también tiene a $\sigma(\alpha)$ como una raíz, para cada elemento $\sigma \in \text{Aut}(K/F)$.

Ejemplo 3.71. Sea $K = Q(\sqrt{2})$. Si $\tau \in \text{Aut}(Q(\sqrt{2})) = \text{Aut}(Q(\sqrt{2})/Q)$, entonces se tiene que $\tau(\sqrt{2}) = \pm\sqrt{2}$ ya que estas son las raíces del polinomio mínimo para $\sqrt{2}$ sobre Q . En consecuencia, si $\tau \in \text{Aut}(Q\sqrt{2})$ entonces

$$\tau(a + b\sqrt{2}) = a \pm b\sqrt{2}.$$

Por lo tanto, si consideramos la permutación $\sqrt{2} \rightarrow \sqrt{2}$ que es justamente la identidad o isomorfismo 1 de $Q(\sqrt{2})$; y la permutación $\sigma: \sqrt{2} \rightarrow -\sqrt{2}$, se obtiene la relación $\text{Aut } Q(\sqrt{2}) \cong \{1, \sigma\}$ que es precisamente un grupo cíclico de orden 2 generado por σ . Es decir, $\text{Aut } Q(\sqrt{2}) \cong Z_2$.

Ejemplo 3.72. Sea $K = Q(\sqrt[3]{2})$. Como antes, si $\tau \in \text{Aut}(K/Q)$, entonces τ es completamente determinado por la acción de $\sqrt[3]{2}$ ya que

$$\tau\left(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2\right) = a + b\tau\sqrt[3]{2} + c\tau(\sqrt[3]{2})^2$$

y $\sqrt[3]{2}$ es la raíz del polinomio $x^3 - 2$ que es el polinomio mínimo de la extensión $Q(\sqrt[3]{2})$ sobre Q . Por lo tanto solo existe una posibilidad y es la permutación identidad $\tau\sqrt[3]{2} = \sqrt[3]{2}$, así $\text{Aut}(K/Q) = \{1\}$.

En general, si K es generado sobre el cuerpo F por una colección de elementos, entonces un automorfismo $\sigma \in \text{Aut}(K/Q)$, es completamente determinado por los elementos generadores. Si K/F es una extensión finita entonces K es generado sobre F por un número finito de elementos algebraicos, por lo tanto el $\text{Aut}(K/Q)$ es un grupo finito.

Proposición 3.73. Sea $H \leq \text{Aut}(K)$ un subgrupo del grupo de automorfismos de K . Entonces la colección F de elementos de K fija para todos los elementos de H es un subcuerpo de K .

Definición 3.74. Si H un subgrupo de un grupo de automorfismos de K , el subcuerpo de K que es fijado por todos los elementos de H es llamado el cuerpo fijo de H y se denota $\text{fix}\{H\}$.

El estudio de las permutaciones que dejan invariantes a las raíces de un polinomio, permiten esclarecer relaciones entre un campo y sus extensiones, lo cual brinda herramientas para determinar la solubilidad de esta ecuación.

Proposición 3.75. La asociación de grupos con cuerpos y de cuerpos con grupos, se definen a través de una inclusión inversa, es decir

- i. Si $F_1 \subseteq F_2 \subseteq K$ son dos subcuerpos de K entonces $\text{Aut}(K/F_2) \leq \text{Aut}(K/F_1)$.
- ii. Si $H_1 \leq H_2 \leq \text{Aut}(K)$ son dos subgrupos de automorfismos asociados a los cuerpos fijos F_1 y F_2 respectivamente, entonces $F_2 \subseteq F_1$.

Ejemplo 3.76. Consideremos el cuerpo $K = Q(\sqrt{2})$, entonces $\text{Aut}(Q(\sqrt{2})) = \{1, \sigma\}$, por lo tanto los elementos del conjunto de $Q(\sqrt{2})$ están dados por

$$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$$

bajo el automorfismo identidad. De lo contrario, bajo σ se obtiene la ecuación

$$a + b\sqrt{2} = a - b\sqrt{2}$$

que es equivalente para $b = 0$, por lo tanto el cuerpo fijo para $\text{Aut}(Q(\sqrt{2})/Q)$ es justamente el cuerpo Q .

Ejemplo 3.77. Consideremos el cuerpo $K = Q(\sqrt[3]{2})$, que en este caso $\text{Aut}(K) = 1$ de modo que cada elemento de K es fijo, es decir el cuerpo fijo del $\text{Aut}(Q(\sqrt[3]{2})/Q)$ es $Q(\sqrt[3]{2})$.

Los dos ejemplos anteriores nos permiten observar las relaciones de equivalencia entre las extensiones de un cuerpo base y los grupos de automorfismos de las permutaciones que dejan invariantes las raíces de un polinomio irreducible sobre este campo base.

Proposición 3.78. Sea E el cuerpo de descomposición sobre el cuerpo F del polinomio $f(x) \in F[x]$. Entonces

$$|\text{Aut}(E/F)| \leq [E:F]$$

con la igualdad si $f(x)$ es separable sobre F .

A lo largo de este capítulo hemos abordado cada una de las definiciones y conceptos que hacen parte del teorema fundamental de la teoría de Galois, sin embargo, de los conceptos que más se destaca **grupo de Galois** porque vincula directamente el grupo de permutaciones que dejan invariante una ecuación con el campo de descomposición de esta.

Definición 3.79. Sea K/F una extensión finita. Entonces K se dice que es el **grupo de Galois** sobre F y K/F es una extensión de Galois si $|\text{Aut}(K/F)| = [K:F]$. Si K/F es Galois, el grupo de automorfismos $\text{Aut}(K/F)$ es llamado el grupo de Galois y se denota como $\text{Gal}(K/F)$.

Observación 3.80. El grupo de Galois de una extensión K/F es a veces definida como el grupo de automorfismos $Aut(K/F)$ para todo K/F . Pero en este caso se ha elegido la notación anterior debido a que se hará hincapié que la extensión K/F tiene el máximo número de automorfismos.

Proposición 3.81. Si K es el cuerpo de descomposición sobre F de un polinomio separable $f(x)$ entonces K/F es de Galois.

Definición 3.82. Si $f(x)$ es un polinomio separable sobre F , entonces el grupo de Galois de $f(x)$ sobre F es el grupo de Galois del cuerpo de descomposición de $f(x)$ sobre F .

Ejemplo 3.83. La extensión $Q(\sqrt{2})/Q$ es Galois, con el grupo de Galois definido como $Gal(Q(\sqrt{2})/Q) = \{1, \sigma\}$ donde σ es el automorfismo

$$\begin{aligned}\sigma: Q(\sqrt{2}) &\rightarrow Q(\sqrt{2}) \\ a + b\sqrt{2} &\rightarrow a - b\sqrt{2}\end{aligned}$$

Ejemplo 3.84. La extensión $Q(\sqrt[3]{2})/Q$ no es de Galois, porque el grupo de automorfismos es de solo orden 1.

Ejemplo 3.85. La extensión $Q(\sqrt{2}, \sqrt{3})$ es de Galois sobre Q , ya que es el cuerpo de descomposición del polinomio $(x^2 - 3)(x^2 - 2)$. Y los automorfismo σ estan completamente determinados por la adjunción de los elementos generadores $\sqrt{2}$ y $\sqrt{3}$, que deben ser asignadas a $\pm\sqrt{2}$ y $\pm\sqrt{3}$ respectivamente. De ahí que las únicas posibilidades de automorfismos son las permutaciones

$$\begin{array}{cccc}\left\{ \begin{array}{l} \sqrt{2} \rightarrow \sqrt{2} \\ \sqrt{3} \rightarrow \sqrt{3} \end{array} \right. & \left\{ \begin{array}{l} \sqrt{2} \rightarrow -\sqrt{2} \\ \sqrt{3} \rightarrow \sqrt{3} \end{array} \right. & \left\{ \begin{array}{l} \sqrt{2} \rightarrow \sqrt{2} \\ \sqrt{3} \rightarrow -\sqrt{3} \end{array} \right. & \left\{ \begin{array}{l} \sqrt{2} \rightarrow -\sqrt{2} \\ \sqrt{3} \rightarrow -\sqrt{3} \end{array} \right.\end{array}$$

Ya que el grupo de Galois es de orden 4, ya que todos los elementos son de hecho automorfismos de $Q(\sqrt{2}, \sqrt{3})$ sobre Q .

Definiendo los automorfismos σ y τ como

$$\sigma = \begin{cases} \sqrt{2} \rightarrow -\sqrt{2} \\ \sqrt{3} \rightarrow \sqrt{3} \end{cases} \quad \tau = \begin{cases} \sqrt{2} \rightarrow \sqrt{2} \\ \sqrt{3} \rightarrow -\sqrt{3} \end{cases}$$

O, más explícitamente,

$$\sigma: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \rightarrow a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$\tau: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \rightarrow a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

(ya que, por ejemplo

$$\sigma(\sqrt{6}) = \sigma(\sqrt{2}\sqrt{3}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = (-\sqrt{2})(\sqrt{3}) = -\sqrt{6}).$$

Entonces, $\sigma^2(\sqrt{2}) = \sigma\sigma(\sqrt{2}) = \sigma(-\sqrt{2}) = \sqrt{2}$ y claramente $\sigma^2(\sqrt{3}) = \sqrt{3}$. Por lo tanto $\sigma^2 = 1$ es la identidad de automorfismos. De forma similar $\tau^2 = 1$. El automorfismo $\sigma\tau$ puede ser fácilmente calculable

$$\sigma\tau(\sqrt{2}) = \sigma(\tau(\sqrt{2})) = \sigma(\sqrt{2}) = \sqrt{2}$$

y

$$\sigma\tau(\sqrt{3}) = \sigma(\tau(\sqrt{3})) = \sigma(-\sqrt{3}) = -\sqrt{3}$$

de manera que $\sigma\tau$ es el restante no trivial de automorfismos que componen el grupo de Galois. Dado que este automorfismo también es de orden 2 en el grupo de Galois, así se obtiene que

$$\text{Gal}(Q(\sqrt{2}, \sqrt{3})/Q) = \{1, \sigma, \tau, \sigma\tau\}.$$

Es decir $\text{Gal}(Q(\sqrt{2}, \sqrt{3})/Q) \cong \text{grupo Klein}$, donde *grupo Klein* es un grupo de orden 4.

Asociando a cada subgrupo del $\text{Gal}(Q(\sqrt{2}, \sqrt{3})/Q)$ con el correspondiente subcuerpo fijo de $Q(\sqrt{2}, \sqrt{3})$. Por ejemplo, el subcuerpo fijado por $\{1, \sigma\tau\}$, es decir, fijado por

$$\sigma\tau: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \rightarrow a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$

está dado por elementos de la forma $a + d\sqrt{6}$, es decir, $Q(\sqrt{6})$. De forma similar se puede determinar los cuerpos fijos correspondientes a los subgrupos de $\text{Gal}(Q(\sqrt{2}, \sqrt{3})/Q)$ están dados por

Subgrupo	Subcuerpo fijo
$\{1\}$	$Q(\sqrt{2}, \sqrt{3})$
$\{1, \sigma\}$	$Q(\sqrt{3})$
$\{1, \sigma\tau\}$	$Q(\sqrt{6})$
$\{1, \tau\}$	$Q(\sqrt{2})$
$\{1, \sigma, \tau, \sigma\tau\}$	Q

Ejemplo 3.86. El cuerpo de descomposición del polinomio $x^3 - 2$ sobre Q es Galois y de índice 6, puesto que $x^3 - 2$ se puede factorizar como $(x^3 - 2 = (x - \sqrt[3]{2})(x^2 + x + 1))$ el producto de dos polinomios irreducibles en Q de grado 3 y 2 respectivamente; y así las raíces de la ecuación son $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$ donde $\rho = \frac{-1+\sqrt{-3}}{2}$ es la raíz cubica primitiva de la unidad

y $\rho^2 = \frac{-1-\sqrt{-3}}{2}$. Por lo tanto el cuerpo de descomposición puede escribirse como $Q(\sqrt[3]{2}, \rho\sqrt[3]{2})$.

Para determinar el grupo de Galois, usamos de forma conveniente el conjunto de generadores $\sqrt[3]{2}$ y ρ . Entonces algún automorfismo σ asigna a $\sqrt[3]{2}$ a un elemento $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$ y asigna el elemento ρ a ρ o a ρ^2 . Por lo tanto σ es completamente determinado bajo la acción de estos dos elementos con 6 posibles automorfismos. Para calcular estos automorfismos de forma explícita, sea σ y τ automorfismos definidos como

$$\sigma: \begin{cases} \sqrt[3]{2} \rightarrow \rho\sqrt[3]{2} \\ \rho \rightarrow \rho \end{cases} \quad \tau: \begin{cases} \sqrt[3]{2} \rightarrow \sqrt[3]{2} \\ \rho \rightarrow \rho^2 = 1 - \rho \end{cases} .$$

Note que, al igual que antes se puede calcular de forma explícita los elementos de $Q(\sqrt[3]{2}, \rho)$ a través de la combinación lineal de los elementos bases $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \rho, \rho\sqrt[3]{2}, \rho(\sqrt[3]{2})^2\}$.

Por ejemplo

$$\sigma(\rho\sqrt[3]{2}) = \rho\rho\sqrt[3]{2} = \rho^2\sqrt[3]{2} = (1 - \rho)\sqrt[3]{2} = -\sqrt[3]{2} - \rho\sqrt[3]{2}.$$

De igual modo, se pueden determinar los otros elementos bajo la acción de σ sobre el conjunto base.

Así, los elementos del grupo de Galois son

$$\begin{aligned} 1: & \begin{cases} \sqrt[3]{2} \rightarrow \sqrt[3]{2} \\ \rho \rightarrow \rho \end{cases} & \sigma^2: & \begin{cases} \sqrt[3]{2} \rightarrow \rho^2\sqrt[3]{2} \\ \rho \rightarrow \rho \end{cases} \\ \tau\sigma: & \begin{cases} \sqrt[3]{2} \rightarrow \rho^2\sqrt[3]{2} \\ \rho \rightarrow \rho^2 \end{cases} & \tau\sigma^2: & \begin{cases} \sqrt[3]{2} \rightarrow \rho\sqrt[3]{2} \\ \rho \rightarrow \rho^2 \end{cases} . \end{aligned}$$

$$\sigma\tau: \begin{cases} \sqrt[3]{2} \rightarrow \rho\sqrt[3]{2} \\ \rho \rightarrow \rho^2 \end{cases}$$

así $\sigma\tau = \tau\sigma^2$, y al realizar cálculos similares se obtiene que $\sigma^3 = \tau^2 = 1$. Por lo tanto el

$$\text{Gal}(\sqrt[3]{2}, \rho)/Q = \langle \sigma, \tau \rangle \cong S_3$$

que es el grupo simétrico de grado 3. De otro lado $\text{Gal}(\sqrt[3]{2}, \rho)/Q$ es el subgrupo alternante de S_3 , generado por las permutaciones de las 3 raíces del polinomio $x^3 - 2$. La relación entre los elementos del grupo de Galois y los campos fijos está dada por

Subgrupo	Subcuerpo fijo
$\{1\}$	$Q(\sqrt[3]{2}, \rho)$
$\{\sigma\}$	$Q(\rho)$
$\{\tau\}$	$Q(\sqrt[3]{2})$
$\{\sigma\tau\}$	$Q(\rho\sqrt[3]{2})$
$\{\sigma\tau^2\}$	$Q(\rho^2\sqrt[3]{2})$
$\{\sigma, \tau\}$	Q

3.2.2 Teorema moderno de la teoría de Galois.

Antes de abordar el teorema moderno de la teoría de Galois, es conveniente revisar algunos teoremas preliminares.

Teorema 3.87. Sea $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ un subgrupo de automorfismos de un cuerpo K y sea un cuerpo fijo F . Entonces

$$[F: K] = n = |G|$$

Teorema 3.88. Sea K/F una extensión finita. Entonces

$$|Aut(K/F)| \leq [K: F]$$

con la equivalencia si y solo si F es un cuerpo fijo de $Aut(K/F)$. De otro forma, K/F es de Galois si y solo si F es un cuerpo fijo de $Aut(K/F)$.

Teorema 3.89. Sea G un subgrupo finito de automorfismos de un cuerpo K y sea F el cuerpo fijo. Entonces para cada automorfismo K sobre el cuerpo fijo F está contenido en G , es decir $Aut(K/F) = G$, de modo que K/F es de Galois, con G un grupo de Galois.

A lo largo de este capítulo, se ha realizado un acercamiento a las distintas temáticas que inciden en el teorema moderno de la teoría de Galois, como las extensiones de campo, la noción de extensiones algebraicas, extensiones separables, cuerpos de descomposición, automorfismos, grupo de Galois todo esto para abordar de la forma más amena posible este teorema lo cual facilite al lector su interpretación. De las temáticas mencionadas es importante resaltar el papel de dos especialmente. La primera, el campo de descomposición; y el segundo el grupo de Galois de una ecuación debido a que son las dos temáticas principales expresadas en el teorema como se puede observar a continuación.

Teorema 3.90. (Teorema moderno de la teoría de Galois). Sea K/F una extensión de cuerpo y sea $G = Gal(K/F)$. Entonces hay una biyección

$$\left\{ \begin{array}{l} \text{Subcampos } E \\ \text{de } K \\ \text{contenidos en } F \end{array} \begin{array}{l} \uparrow \\ E \\ \uparrow \\ F \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{Subgrupos} \\ H \text{ de } \\ G \end{array} \begin{array}{l} \downarrow \\ H \\ \downarrow \\ G \end{array} \right\}$$

Dadas las correspondencias

$$E \rightarrow \left\{ \begin{array}{l} \text{Los elementos de } G \\ \text{fijados con } E \end{array} \right\}$$

$$\left\{ \begin{array}{l} \text{El campo} \\ \text{fijo de } H \end{array} \right\} \leftarrow H$$

Que son inversas a cada uno. Bajo esta correspondencia

- 1) (inclusión inversa). Si E_1, E_2 corresponden a los grupos H_1, H_2 respectivamente entonces $E_1 \subseteq E_2$ si y solo si $H_2 \leq H_1$.
- 2) $[K : E] = H$ y $[E : F] = [G : H]$, el índice de H en F .

$$\begin{array}{l} K \\ \uparrow \} \quad |H| \\ E \\ \uparrow \} \quad |G:H| \\ F \end{array}$$

- 3) Si K/E es siempre una extensión de Galois, con el grupo de Galois se cumple la igualdad $G = \text{Gal}(K/E) = H$.

$$\begin{array}{l} K \\ \downarrow \quad H \\ E \end{array}$$

- 4) E es Galois sobre F si y solo si H es normal a un subgrupo de G . Si este es el caso, entonces el grupo de Galois es homorfismo al grupo cociente

$$\text{Gal}(E/F) \cong G/H$$

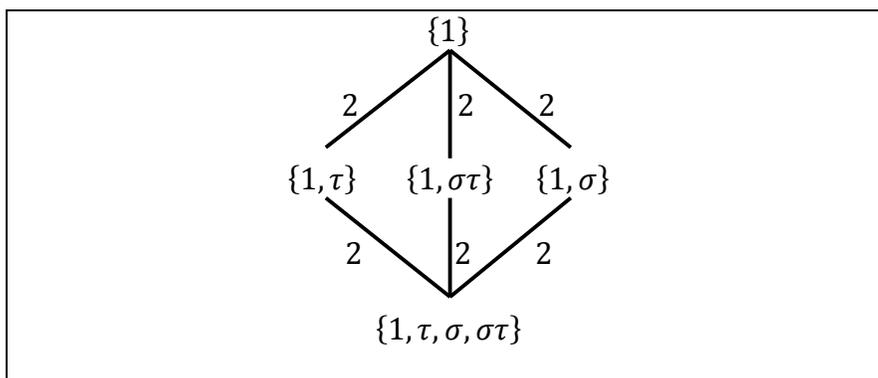
Mas en general, incluso si H no es normal en G , entonces el isomorfismo de E (en una clausura algebraica de F que contiene a K) con $\text{fix } \{F\}$ están en una correspondencia uno a uno con las clases $\{\sigma H\}$ de H en G .

- 5) Si E_1, E_2 corresponden a los grupos H_1, H_2 , respectivamente, entonces la intersección $E_1 \cap E_2$ corresponde al grupo $\langle H_1, H_2 \rangle$ generado por H_1 y H_2 y el cuerpo compuesto entre E_1, E_2 correspondiente a la intersección $H_1 \cap H_2$. De ahí la secuencia de K que contiene a F y la secuencia de subgrupos de G que tienen un orden dual. (El diagrama de secuencia para uno, es el diagrama para el otro pero al revés).

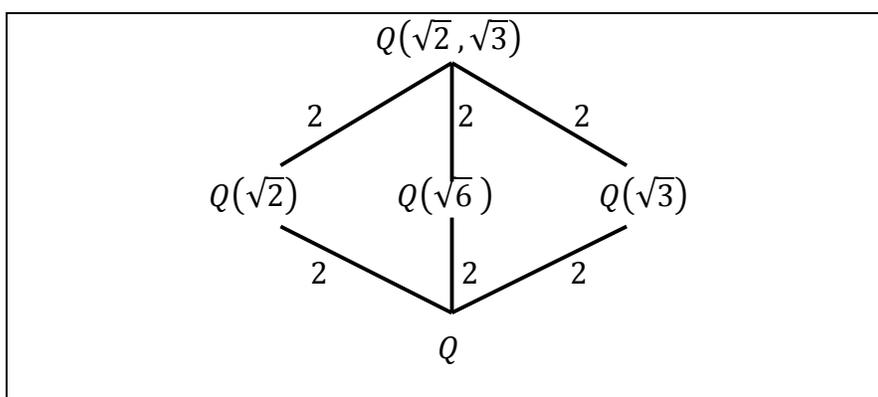
Ejemplo 3.91. Representemos mediante un diagrama la secuencia de subgrupos de grupo de Galois del polinomio $P(X) = (X^2 - 3)(X^2 - 2)$ y la secuencia de las extensiones del cuerpo Q que están contenidos en el cuerpo de división de $(X^2 - 3)(X^2 - 2)$.

Este ejemplo ha sido abordado con anterioridad (o al menos en su gran mayoría), a través de los ejemplos de los teoremas presentados a lo largo de este capítulo, debido a que con anterioridad ya se calculó el grupo de Galois (ejemplo 3.85) y las extensiones de cuerpo. A continuación solo presentaremos la secuencia de subgrupos normales y de extensiones del cuerpo base.

Secuencia de subgrupos normales



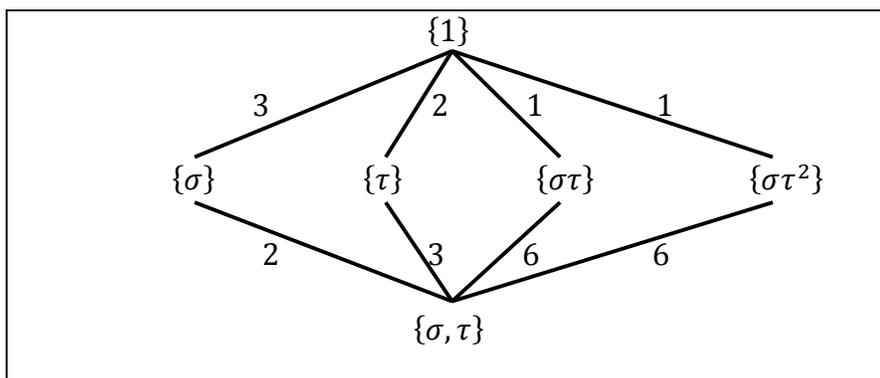
Secuencia de extensiones



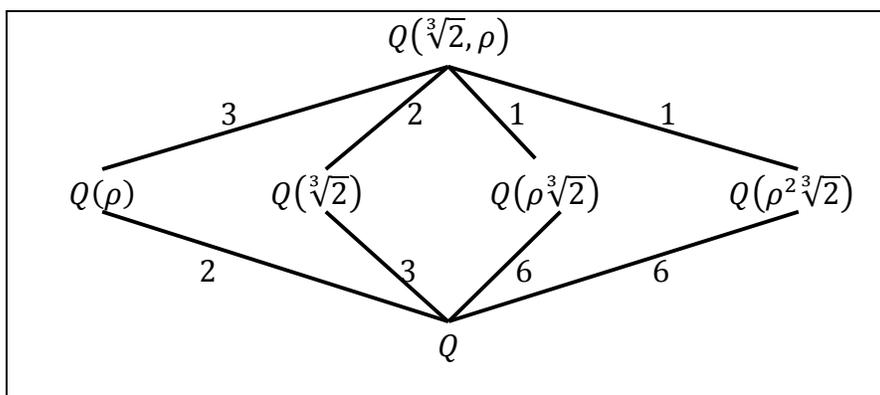
Ejemplo 3.92. Determine la secuencia de subgrupos del grupo de Galois y la secuencia de extensiones cuerpo del polinomio $x^3 - 2$ sobre el cuerpo Q .

Al igual que en el ejemplo anterior, este ejemplo ya ha sido abordado a lo largo de este capítulo a través de los teoremas presentados. Por lo tanto, en esta parte simplemente nos dedicaremos a presentar el diagrama de secuencias de subgrupos (ejemplo 3.86) y la secuencia de extensiones de Galois (variación ejemplo 3.59).

Secuencia de subgrupos



Secuencia de extensiones



4. TEORÍA DE GALOIS, ALGUNOS ASPECTOS HISTÓRICOS Y MATEMÁTICOS.

“algunos misterios siempre se escapan de la mente humana, para convencernos de ello, solo hay que echar un vistazo a las tablas de números primos, y ver que no reina, ni orden, ni reglas”

Évariste Galois.

Este capítulo se divide en tres partes: en la primera parte, se realiza una presentación de unos períodos de la vida de Évariste Galois, en el cual se hace referencia a algunos aspectos familiares, académicos y biográficos; en la segunda parte, se plasma un acercamiento de algunos aspectos históricos de la teoría de Galois, en la cual se presenta un breve repaso histórico de las primeras investigaciones de Abel sobre las condiciones bajo las cuales una ecuación de grado mayor a cuatro es soluble por el método de radicales y se alude a las fechas y resultados de las presentaciones de las memorias de Galois a la comunidad de matemáticos de la época, en las cuales presenta las condiciones necesarias y suficientes para que una ecuación de grado mayor o igual a cinco sea soluble por radicales; en la tercera parte, se presentan algunos aspectos matemáticos desde un punto de vista histórico de la teoría de Galois, tomando como referencia dos elementos teóricos: el primero, el capítulo 14 del libro *“Galois' Theory of Algebraic Equations”* escrita por Jean-Pierre Tinoi (2011) que presenta una reescritura de la teoría de Galois de la memoria escrita por Galois; y el segundo, los aspectos teóricos abordados en el capítulo anterior.

4.1 La vida de Galois.

En este apartado se presentan algunos aspectos referentes a la vida de Galois, en el cual se enfatiza en aspectos de su vida académica, se realiza una breve introducción de la relación con su familia y de los hechos que desencadenaron su muerte. Para conocer un poco más acerca de la vida de Galois, se recomienda un artículo referencia de este apartado, escrito por Santiago Gutiérrez (2011) “*Évariste Galois: un genio en la base del álgebra moderna*”.

En el año de 1811 nace en Bourg-la-Reine cerca de Paris el matemático Évariste Galois, quien es considerado uno de los fundadores de la teoría de grupos y uno de sus principales trabajos se centró en estudiar las condiciones bajo las cuales una ecuación de grado mayor a cuatro era soluble por medio de radicales. Teniendo en cuenta que Galois no se había interesado por las matemáticas hasta los 15 años y falleció a los 21 años es considerado un genio de las matemáticas.

Évariste era hijo de Nicolás Gabriel Galois alcalde de la población de Bourg-la-Reine y Adélaïde-Marie Demante una mujer culta, quien se ocupó intensamente de la educación de su hijo proporcionándole una sólida formación en latín y griego. Sin embargo se cree que Galois no tenía nociones de aritmética debido a que para la época las matemáticas no se consideraban importantes.

En 1823 Galois ingresa *College Royal de Louis-le-Grand* un prestigioso colegio de Paris, donde rápidamente y gracias a la motivación del profesor Hippolyte Jean Vernier, Évariste a la edad de 15 años descubre su interés por las matemáticas, estudiando las principales obras en el cuerpo de las matemáticas de la época. Aunque esta motivación por las matemáticas le trajo consecuencias negativas por su bajo rendimiento en otras áreas como las humanidades. Por este motivo Évariste decide presentarse al centro de estudios científicos más prestigioso

de Francia el *École Polytechnique* un año antes de lo debido sin la adecuada preparación, por lo cual como era de esperarse fue rechazado.

Después de fallar en su intento de ingresar al *École Polytechnique*, Galois dedica su tiempo a la investigación y publica su primer trabajo llamado *Annales de mathématiques pures et appliqués* en marzo de 1829, obra que trata acerca de la demostración de un teorema de fracciones continuas. Para esta misma época Évariste ya se encuentra investigando acerca de las condiciones bajo las cuales una ecuación es soluble por radicales.

Los resultados en las investigaciones acerca de la solución de ecuaciones se evidenciaron a finales de mayo de 1829, cuando presenta a la academia de ciencias de Paris su primera memoria, la cual fue entregada a Cauchy para su evaluación. Sin embargo, se dice que Cauchy no comprendió la memoria, y recomendó a Galois que escribiera una memoria más comprensible para ser presentada al Gran premio de matemáticas de la academia de ciencias.

A pesar de este un nuevo revés, Évariste decide continuar con sus investigaciones acerca de la solución de ecuaciones y en el año de 1831 llega a reflexiones importantes pero nuevamente no son comprendidas, esta vez por Siméon D. Poisson, quién nuevamente le recomienda mejorar sus demostraciones y en la forma en que desarrolla sus ideas.

Al año siguiente de la presentación de su segunda memoria a Siméon, un nuevo hecho desafortunado sacude la de Galois. Después de unos periodos en la cárcel debido a sus ideales políticos, Évariste es retado a un duelo a finales de Mayo de 1832 por unos presuntos conocidos, aunque no es claro el motivo por lo cual fue retado, se especula que fue por motivos de honor o ideales políticos.

Por motivo del duelo, Galois debió apresurarse a entregar sus resultados acerca de las investigaciones sobre las condiciones bajo las cuales una ecuación de grado mayor o igual a cinco es soluble por el método de radicales. Así la noche anterior al duelo se especula que Évariste escribió su última memoria donde logra determinar las condiciones para la solubilidad de una ecuación de grado mayor a cuatro, todo esto expresado en una carta enviada a un amigo, además en esta carta Galois aludía en múltiples ocasiones que le hacía falta tiempo.

A pesar de que Galois trato de conciliar con sus retadores, estos no cambiaron de parecer y el 30 de agosto de 1832 Galois se presenta a este duelo, donde recibe un impacto de bala en su vientre y es abandonado por sus contradictores. Galois fue recogido por una persona que pasaba por el lugar y es llevado a un hospital, sin embargo falleció al día siguiente.

4.2 Aspectos históricos de la teoría de Galois.

Como se mencionó en la sección anterior, Évariste Galois empleo gran parte de su corta vida al estudio de las condiciones necesarias bajo las cuales una ecuación de grado mayor a cuatro es soluble por el método de radicales. La búsqueda de estas condiciones es conocida desde una perspectiva moderna como teoría de Galois, que presento sus primeras huellas a través de los trabajos de Gauss sobre la solución de ecuaciones ciclotómicas. Sin embargo, se podría pensar que la teoría de Galois tiene sus primeras huellas en los trabajos de los egipcios en el siglo XVII antes de nuestra era, quienes fueron los primeros en solucionar ecuaciones, para el caso particular de grado dos, por el método de radicales.

En relación con los dos aspectos mencionados anteriormente, con la intención de realizar un acercamiento a los elementos que dieron origen a la teoría de Galois, en el capítulo uno

se caracterizaron algunos aspectos referentes a la teoría de ecuaciones y la solución por el método de radicales y en esta sección se busca describir algunos sucesos puntuales que dieron origen a la teoría de Galois.

Dentro de los sucesos puntuales que dieron origen a la teoría de Galois, consideramos como relevantes dos aspectos: el primero, las investigaciones realizadas por Abel, quién a través del estudio de las soluciones de las ecuaciones ciclotómicas dado por Gauss llega a resultados importantes; y la segunda, las investigaciones realizadas por Évariste, quién a través de fracasos y hechos desafortunados logra dar con las condiciones necesarias para que una ecuación sea soluble por radicales. Para la documentación de estos dos aspectos se considera como referencia la introducción del capítulo 14 del texto de Tinol (2011), para profundizar acerca del trabajo de Abel se recomienda la lectura del trabajo de grado de Chavarría (2014) en la cual se realiza la demostración del teorema de Abel que será mencionado en la sección siguiente.

4.2.1 El papel de Abel en la teoría de Galois.

Después de las obras de Gauss, Ruffini y Abel las dos principales clases de ecuaciones habían sido tratadas a fondo con resultados divergentes; las ecuaciones ciclotómicas⁵ de cualquier grado eran solubles por el método de radicales, mientras que las ecuaciones generales de grado mayor a cuatro no lo eran. Por lo tanto, se plantea el siguiente interrogante ¿Cuáles ecuaciones de grado mayor o igual a cinco son solubles por radicales?

⁵ Una ecuación de la forma $\phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$

Abel abordó esta cuestión y regresó al estudio de la teoría de ecuaciones, considerando que era uno de sus temas favoritos, en busca de una pista dejada por Gauss. Así, él descubrió una clase de ecuaciones que tiene solución por radicales en particular las ecuaciones ciclotómicas. Al seguir esta pista Abel se dio cuenta que el método empleado por Gauss para la solución de ecuaciones ciclotómicas, también se podía aplicar a las ecuaciones que surgen de la división infinita de un arco. En analogía con los resultados de Gauss en la construcción de polígonos regulares con regla y compas, Abel logró probar que el arco se puede dividir en $2^n + 1$ partes utilizando regla y compas, siempre que $2^n + 1$ sea un número primo.

En este sentido Abel continuó con sus investigaciones y finalmente logró llegar a la siguiente generalización:

Teorema 4.1: (Teorema de Abel) Sea P un polinomio con raíces r_1, \dots, r_n . Si las raíces r_1, \dots, r_n se pueden expresar en forma racional en términos de r_1 , es decir si existe una fracción racional $\theta_2, \dots, \theta_n$ tal que

$$r_i = \theta_i(r_1) \text{ para } i = 2, \dots, n$$

y si además

$$\theta_i \theta_j(r_1) = \theta_j \theta_i(r_1)$$

entonces la ecuación $P(X) = 0$ es soluble por radicales.

El teorema 4.1 se aplica en particular en las ecuaciones ciclotómicas que se representan de la forma

$$\phi_p(x) = X^{p-1} + X^{p-2} + \dots + X + 1 = 0$$

para p primo. De hecho las raíces de ϕ_p son las raíces primitivas p -ésimas de la unidad y se denotan como ζ , las otras son potencias de ζ . Las fracciones racionales $\theta_2, \dots, \theta_{p-1}$ se pueden expresar como

$$\theta_i(X) = X^i \text{ para } i = 2, \dots, p$$

por la condición se tiene que

$$\theta_i \theta_j(\zeta) = \zeta^{ij} = \theta_j \theta_i.$$

Al profundizar más en estos resultados, Abel se acerca más a la condición necesaria y suficiente para que una ecuación sea soluble por radicales, sin embargo no alcanzó a desarrollar su trabajo por completo porque falleció prematuramente por una tuberculosis en el año 1829.

4.2.2 El papel de Galois.

Quien logró dar solución al problema de las condiciones necesarias para que una ecuación sea soluble por radicales, fue el joven Évariste Galois, en el año de 1829 con tan solo 18 años, cuando presentó en la Academia de Ciencias de París una memoria sobre la teoría de ecuaciones. En esta memoria, describió lo que ahora se conoce como el grupo de Galois de una ecuación, y como se aplica esta nueva herramienta para encontrar las condiciones bajo las cuales una ecuación sea soluble por radicales.

El evaluador de esta memoria fue Augustin Louis Cauchy (1789-1857), quien argumentó que la memoria era poco comprensible y con ideas difusas, lo que causó que la memoria presentada por Galois se perdiera entre los papeles de Cauchy. Después de un año Galois vuelve a escribir una segunda memoria la cual es presentada a la real Academia de Ciencias

pero nuevamente es rechazada por Siméon D. Poisson debido a que no era lo suficientemente clara.

A pesar del esfuerzo hecho por Galois, él no logra completar y expresar de forma más clara sus ideas en su memoria titulada “*Memoire sur les conditions de resolubilité des equations par Radicaux*”, debido a, que en el año de 1832 muere en un duelo. Pese a esto Josep Luis Liouville (1809 – 1882) generosamente decidió estudiar la memoria de Galois y la publicó con algunas de sus propias interpretaciones en el año de 1846, rescatando así la teoría de Galois del completo olvido.

Por otra parte, se resalta, que la idea básica de la teoría de Galois es asociar a cualquier ecuación un grupo de permutaciones a sus raíces, este grupo está formado por todas las permutaciones que conservan las relaciones entre sus raíces, lo cual muestra en qué medida las raíces son intercambiables. La brillante idea de Galois se fundamenta, al considerar este grupo como una herramienta para determinar la solubilidad de una ecuación por el método de radicales. Así, en particular la solubilidad de una ecuación por radicales puede ser traducida en términos de un grupo asociado, esto se consigue gracias al comportamiento del grupo bajo la extensión de un cuerpo base (es el cuerpo más pequeño que contiene las raíces de la ecuación). De estas nuevas ideas, Galois ofrece una única aplicación que demuestra que las ecuaciones irreducibles de grado primo son solubles por radicales si y solo si ninguna de las raíces puede expresarse de forma racional en términos de otras dos.

Lo interesante del estudio realizado por Galois señala Tinol (2001), se representa en que no es claro como caracterizar las permutaciones que preservan las relaciones entre las raíces, no obstante esta dificultad disminuye si se evita la utilización de noción de cuerpo, que es la

idea central de la teoría de Galois. Pese a esto Galois soluciona este problema mediante el uso de la irreductibilidad de polinomios de forma brillante.

El concepto de cuerpo y de extensiones de cuerpos, empiezan a ser claros en las primeras líneas de su memoria, donde se profundiza en la noción de irreductibilidad y se destaca que el cuerpo base puede estar dado de forma arbitraria. (Tenga en cuenta que al momento de hablar de irreductibilidad se alude a una ecuación que se dice, es reducible si admite divisores racionales, de lo contrario es irreducible).

Por otra parte, al continuar con la discusión de la memoria de Galois se puede observar que estas siguen su propio orden. Iniciando con la definición de grupo de Galois de una ecuación, pasando por el estudio del comportamiento de un grupo de Galois bajo una extensión del cuerpo base, y por último deduciendo una condición necesaria y suficiente para que una ecuación sea soluble por radicales en términos de un grupo de Galois.

4.3 Aspectos matemáticos históricos de la teoría de Galois.

En el capítulo tres se abordó la teoría de Galois desde una perspectiva moderna, lo cual nos permite tener las bases teóricas para abordar esta teoría nuevamente, pero esta vez desde una perspectiva histórica a través del estudio de algunos apartados del capítulo 14 del texto de Tinol (2011) que consideremos realiza una buena interpretación de la memoria de Galois. En este sentido, es importante mencionar que al tratarse de una obra histórica la notación empleada en esta sección tendrá algunas diferencias respecto al capítulo anterior, al igual encontraremos sutiles diferencias en los contenidos que si bien son los mismos tienen una interpretación diferente; debido a que Galois aún no conocía algunos objetos matemáticos como extensiones de cuerpo y no era claro el concepto de grupo Tinol (2011). Por otra parte,

el estudio de esta nueva perspectiva de la Teoría de Galois nos permite tener más herramientas teoricas para el conocimiento de la obra de Galois, desde diferentes miradas (historica y moderna) lo cual le permite al lector una visión más amplia de esta teoría y nos permite desarrollar la tesis de este trabajo la cual se fundamenta en comprender como un paso historico en el estudio de la teoría de Galois como una adjuncion brinda elementos teoricos para explorar los procesos de enseñanza de las matematicas.

En esta sección en primer lugar se expone el grupo de Galois de ecuación en el cual se expresan algunos resultados o pasos a seguir para determinar el grupo de Galois y se citan algunos ejemplos de ecuaciones, a las cuales se les determina el grupo de Galois; en un segundo momento, se presenta los elementos a considerar al definir el grupo de Galois bajo una extensión de un cuerpo base, además de introducir algunos ejemplos para comprender un poco mejor esta noción; finalizando con la presentación moderna del teorema de Galois

4.3.1 Grupo de Galois de una ecuación.

En esta sección se estudian los aspectos que componen el grupo de Galois, los cuales se representan mediante una serie de resultados, que son fundamentales para comprender el significado de este grupo. Estos resultados se presentan como herramientas para determinar el grupo de Galois de una ecuación, como se exhiben por medio de algunos ejemplos en los que se determina el grupo de Galois de algunas ecuaciones polinómicas en casos generales y particulares.

A lo largo de esta sección y de las siguientes es necesario considerar algunos aspectos, que son importantes por precisar. El primero, consideraremos cuerpos de característica cero (definición 4.2) lo cual nos permite dividir por números enteros distintos de cero

tranquilamente; segundo, en muchas ocasiones emplearemos la noción de función racional $f \in F(x_1, \dots, x_n)$ tal que f se representa de la forma $f = \frac{P}{Q}$ donde P y Q son polinomios en $F[x_1, \dots, x_n]$ tal que $Q \neq 0$; tercero, el grupo de Galois solo se determinara para polinomios con raíces simples (raíces de multiplicidad uno), es decir para polinomios separables (definición 3.43); por último, en el resto de esta sección se considerara el polinomio $P(X)$ de grado n sobre un cuerpo $F[x]$, que tiene n raíces distintas en algún cuerpo que contiene a F . El polinomio $P(X)$ se representa como

$$P(X) = X^n - a_1X^{n-1} + a_2X^{n-2} - \dots + (-1)^n a_n = (X - r_1) \dots (X - r_n)$$

con a_1, \dots, a_n en F y r_1, \dots, r_n en algún cuerpo que contiene a F .

El cuerpo $F(r_1, \dots, r_n)$ se conoce como el cuerpo de fracciones racionales ($F[r]$ es una extensión de $F[x]$ definición 3.4) con elementos que se expresan como la combinación lineal de funciones racionales de $F[x]$ generado por r_1, \dots, r_n y con coeficientes en $F(x_1, \dots, x_n)$.

Así

$$F(r_1, \dots, r_n) = \{f(r_1, \dots, r_n) / f \in F(x_1, \dots, x_n)\}.$$

Vale la pena subrayar que, r_1, \dots, r_n no son independientes e indeterminadas sobre $F[r]$ (es decir, una raíz se puede expresar en términos de otra) por lo tanto un elemento de $F(r_1, \dots, r_n)$ se puede escribir de la forma $f(r_1, \dots, r_n)$ y en otras formas de representación, como por ejemplo $0 \in F[r]$ y se puede simbolizar como $P(r_i)$ para cualquier $i = 1, \dots, n$. Esto es muy importante, debido a la forma en que se consideran las permutaciones σ de r_1, \dots, r_n . Sin embargo, al considerar la función racional $f(\sigma(r_1), \dots, \sigma(r_n))$, note que está bien definida

para cualquier fracción racional $f \in F(x_1, \dots, x_n)$ y además el denominador no se anula para $x_i = \sigma(r_i)$ por lo tanto al definir la permutación $\sigma(f(r_1, \dots, r_n))$ se satisface la ecuación

$$\sigma(f(r_1, \dots, r_n)) = f(\sigma(r_1), \dots, \sigma(r_n)) \quad (4.1).$$

Note que, se requiere precaución de la ecuación 4.1, debido a que no es claro que el lado derecho depende solamente del valor de $f(r_1, \dots, r_n)$, y no de la fracción racional $f(x_1, \dots, x_n)$. Más concretamente se debe probar que si g es otra fracción racional de tal manera que

$$g(r_1, \dots, r_n) = f(r_1, \dots, r_n)$$

se cumple la ecuación

$$g(\sigma(r_1), \dots, \sigma(r_n)) = f(\sigma(r_1), \dots, \sigma(r_n))$$

y si este no es el caso entonces la ecuación 4.1 no tiene sentido.

Después de revisar algunos elementos, los cuales deben ser tenidos en consideración en la definición del grupo de Galois de la ecuación $P(X) = 0$ y caracterizar algunos elementos del cuerpo que contiene a $F[x]$. Se hace necesario revisar algunos resultados preliminares que también juegan un papel importante en la interpretación de un grupo de Galois.

Resultado 4.2. Hay un elemento $V \in F(r_1, \dots, r_n)$, tal que

$$r_i \in F(V) \text{ para } i = 1, \dots, n$$

Tenga en cuenta que los elementos V que satisfacen esta condición son llamados *resolventes de una ecuación* $P(X) = 0$ sobre el cuerpo $F[r]$. Este resultado es importante

puesto que para resolver la ecuación $P(X) = 0$ es suficiente con determinar V , ya que las raíces r_1, \dots, r_n de $P(X)$ son fracciones racionales en V .

Resultado 4.3. Para cada elemento $u \in F(r_1, \dots, r_n)$, hay un único polinomio mónico irreducible $\pi \in F(X)$, tal que $\pi(u) = 0$. Este polinomio se puede expresar como el producto de factores lineales sobre el cuerpo $F(r_1, \dots, r_n)$.

El polinomio π es llamado el polinomio mínimo de u sobre $F[X]$. El grupo de Galois sobre una ecuación $P(x) = 0$ sobre $F[X]$ se puede describir en términos de V un resolvente de Galois, de modo que para $i = 1, \dots, n$ se cumple para alguna fracción racional $f_i(X) \in F(X)$ la igualdad

$$r_i = f_i(V)$$

y $V_1, \dots, V_m \in F(r_1, \dots, r_n)$ son las raíces del polinomio mínimo de V sobre $F[r]$.

Resultado 4.4. Para cualquier $j = 1, \dots, m$, los elementos $f_1(V_j), f_2(V_j), \dots, f_n(V_j)$ son las raíces r_1, \dots, r_n de $P(X)$ en algún orden.

A partir de este resultado, se deduce que, para $j = 1, \dots, m$, la función

$$\sigma_j: r_i \rightarrow f_i(V_j) \text{ para } i = 1, \dots, n$$

es una permutación de r_1, \dots, r_n . El conjunto $\{\sigma_1, \dots, \sigma_m\}$ es llamado el grupo de Galois de la ecuación $P(X) = 0$ sobre $F[X]$, y se denota $Gal(P/F)$.

Resultado 4.5. El grupo $Gal(P/F)$ es un subgrupo de un grupo de permutaciones de r_1, \dots, r_n que no depende de la elección de la resolvente de Galois V y que preserva las relaciones entre las raíces.

Resultado 4.6. El orden del grupo de Galois, es igual al grado del polinomio mínimo π de la resolvente de Galois.

Resultado 4.7. Sea $f(x_1, \dots, x_n)$ una fracción racional con n indeterminados x_1, \dots, x_n con coeficientes en F . Entonces

$$f(r_1, \dots, r_n) \in F[X]$$

si y solo si para todo $\sigma \in Gal(P/F)$, es equivalente a

$$f(r_1, \dots, r_n) = f(\sigma(r_1), \dots, \sigma(r_n)).$$

Este resultado que ilustra nuevamente la ecuación 4.1

$$\sigma(f(r_1, \dots, r_n)) = f(\sigma(r_1), \dots, \sigma(r_n))$$

lo que tiene sentido para $\sigma \in Gal(P/F)$ y definida una extensión de σ como un automorfismo de $F(r_1, \dots, r_n)$ que deja cada elemento en F invariante.

Para ilustrar los aspectos que conducen a la construcción de un grupo de Galois para una ecuación reflejados en los resultados 4.2 hasta 4.7 consideraremos el siguiente ejemplo que refleja cada uno de los resultados anteriores. Además este ejemplo juega un papel especial porque ya ha sido abordado desde una perspectiva moderna en el capítulo anterior.

Es importante mencionar la forma en la cual Galois abordaba y utilizaba múltiples conceptos que para la época aún no estaban establecidos. Si el lector analiza a profundidad los aspectos abordados en esta sección y los compara con lo abordado en el capítulo tres se puede evidenciar que son equivalentes, pero con una diferencia en organización y

axiomatización amplia lo que evidencia el impacto en el paso de las matemáticas clásicas a las modernas y contemporáneas.

Ejemplo 4.8. Sea $P(X) = (X - 1)(X^2 - 2)(X^2 - 3)$

Aplicando diferencia de cuadrados, se descompone en factores lineales como

$$P(X) = (X - 1)(x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$$

por lo tanto, las raíces de P son:

$$r_1 = 1, r_2 = \sqrt{2}, r_3 = -\sqrt{2}, r_4 = \sqrt{3}, r_5 = -\sqrt{3}.$$

Para determinar el grupo de Galois de $P(X) = 0$ sobre el cuerpo Q de los números racionales, primero se elige un resolvente de Galois.

Sea

$$V = \sqrt{2} + \sqrt{3} = r_2 + r_4$$

despejando $\sqrt{3}$ y elevando al cuadrado a ambos lados obtiene

$$(V - \sqrt{2})^2 = (\sqrt{3})^2$$

$$V^2 - 2\sqrt{2}V + 2 = 3$$

como $r_2 = \sqrt{2}$ al sustituir

$$V^2 - 2r_2V + 2 = 3$$

despejando r_2 en función de la resolvente de Galois

$$r_2 = \frac{V^2 - 1}{2V}$$

luego

$$r_2(V) = \frac{V^2 - 1}{2V}.$$

Recordemos que $r_3 = -\sqrt{2}$ y $r_2 = \sqrt{2}$, así $r_3 = -r_2$; por lo tanto

$$r_3 = -\left(\frac{V^2 - 1}{2V}\right) = \frac{1 - V^2}{2V}$$

$$r_3(V) = \frac{1 - V^2}{2V}.$$

Por otra parte, se despeja $\sqrt{2}$ de nuestra escogencia de la resolvente y se obtiene

$$V - \sqrt{3} = \sqrt{2}$$

y de forma análoga, como se obtuvo $r_2(V)$ y $r_3(V)$ se obtiene

$$r_4(V) = \frac{V^2 + 1}{2V}$$

$$r_5(V) = -\frac{V^2 + 1}{2V}.$$

Por ultimo para $1 = r_1(V) = \frac{V}{V}$.

Así, desde $r_1 = 1$ hasta $r_5 = -\sqrt{3}$ son expresiones racionales en V . Por lo tanto V es un resolvente de Galois de la ecuación $P(X) = 0$ sobre el cuerpo Q como se mencionó anteriormente.

Continuando con este proceso, nuestro próximo objetivo es encontrar el polinomio mínimo π de V sobre Q . Para ello empleamos la ecuación utilizada anteriormente

$$V^2 - 2\sqrt{2}V + 2 = 3$$

que reescribiendo se obtiene

$$V^2 - 1 = 2\sqrt{2}V$$

$$(V^2 - 1)^2 = (2\sqrt{2}V)^2$$

$$V^4 - 2V^2 + 1 = 8V^2.$$

Donde el posible polinomio mínimo es

$$V^4 - 10V^2 + 1 = 0.$$

Debido a que V es la raíz del polinomio $X^4 - 10X^2 + 1 \in Q[X]$ y una condición necesaria para determinar el polinomio mínimo, es que este tenga raíces en el cuerpo que contiene a Q lo cual queda garantizado cuando V es una de sus raíces.

La otra condición necesaria para que $X^4 - 10X^2 + 1$ sea el polinomio mínimo sobre el cuerpo Q , es que esté sea irreducible sobre Q . Así para determinar si $X^4 - 10X^2 + 1$ es el polinomio mínimo, es suficiente con mostrar que es irreducible en Q . Para ello, descompongamos este polinomio como el producto de factores lineales.

Utilizando el método de completar cuadrados

$$\begin{aligned} X^4 - 10X^2 + 1 &= X^4 - 10X^2 + 25 - 25 + 1 \\ &= (X^2 - 5)^2 - 24 \end{aligned}$$

luego, aplicando diferencia de cuadrados

$$\left((X^2 - 5) - \sqrt{24} \right) \left((X^2 - 5) + \sqrt{24} \right) = \left(X^2 - (5 + 2\sqrt{2}\sqrt{3}) \right) \left(X^2 - (2\sqrt{2}\sqrt{3} - 5) \right)$$

considerando la relación $(\sqrt{2} \pm \sqrt{3})^2 = 5 \pm 2\sqrt{2}\sqrt{3}$ se obtiene

$$\begin{aligned} X^4 - 10X^2 + 1 &= (X^2 - (\sqrt{2} + \sqrt{3})^2)(X^2 - (\sqrt{2} - \sqrt{3})^2) \\ &= (X - (\sqrt{2} + \sqrt{3}))(X + (\sqrt{2} + \sqrt{3}))(X - (\sqrt{2} - \sqrt{3}))(X + (\sqrt{2} - \sqrt{3})) \end{aligned}$$

Los factores anteriores no se pueden combinar para producir un divisor no trivial del polinomio $X^4 - 10X^2 + 1$ con coeficientes racionales. Así el polinomio $X^4 - 10X^2 + 1$ es irreducible, en consecuencia es el polinomio mínimo de V sobre Q .

Al descomponer en factores lineales hemos encontrado las raíces del polinomio mínimo que están dadas por

$$V_1 = \sqrt{2} + \sqrt{3}, \quad V_2 = \sqrt{2} - \sqrt{3}, \quad V_3 = -\sqrt{2} + \sqrt{3}, \quad V_4 = -\sqrt{2} - \sqrt{3}.$$

Ahora la determinación del grupo de Galois de $P(x) = 0$ depende de los siguientes cálculos, debido a que las fracciones racionales $f_i(X)$ que son tales que $r_i = f_i(V)$ para $i = 1, \dots, 5$, donde

$$f_1(X) = 1, \quad f_2(X) = \frac{X^2-1}{2X}, \quad f_3(X) = \frac{1-X^2}{2V}, \quad f_4(X) = \frac{X^2+1}{2X}, \quad f_5(X) = -\frac{X^2-1}{2X}$$

que equivale a

$$f_1(X) = 1, \quad f_2(X) = \frac{X^2-1}{2X}, \quad f_3(X) = -f_2(X), \quad f_4(X) = \frac{X^2+1}{2X}, \quad f_5(X) = -f_4(X)$$

sustituimos sucesivamente V_1, V_2, V_3, V_4 para X y obtenemos los elementos para el $Gal(P/F)$ como

$$\sigma_i = r_i \rightarrow f_i(V_j) \text{ para } j = 1, \dots, 4$$

De forma explícita

$$\sigma_1 = \text{identidad}$$

$$\sigma_2 = \begin{cases} r_1 \rightarrow r_1 \\ r_2 \rightarrow r_2 \\ r_3 \rightarrow r_3 \\ r_4 \rightarrow r_5 \\ r_5 \rightarrow r_4 \end{cases} \quad \sigma_3 = \begin{cases} r_1 \rightarrow r_1 \\ r_2 \rightarrow r_3 \\ r_3 \rightarrow r_2 \\ r_4 \rightarrow r_4 \\ r_5 \rightarrow r_5 \end{cases} \quad \sigma_4 = \begin{cases} r_1 \rightarrow r_1 \\ r_2 \rightarrow r_3 \\ r_3 \rightarrow r_2 \\ r_4 \rightarrow r_5 \\ r_5 \rightarrow r_4 \end{cases}$$

Por lo tanto, el grupo de Galois para la ecuación $P(X) = 0$ sobre Q consta de permutaciones de r_1, \dots, r_5 que dejan invariante a r_1 , o bien se deja invariante o de intercambio r_2 y r_3 en un lado y r_4 y r_5 en el otro.

Como se mencionó en el resultado 4.5 las permutaciones de un grupo de Galois, son permutaciones que dejan invariantes las raíces. De hecho las raíces $\sqrt{2}$ y $-\sqrt{2}$ tienen exactamente el mismo papel respecto a los números racionales, debido a que no hay forma de distinguir la una de la otra, con la ayuda de los números racionales. En consecuencia pueden ser intercambiados en un grupo de Galois. Lo mismo sucede con $\sqrt{3}$ y $-\sqrt{3}$, pero las raíces de los diversos factores $X - 1, X^2 - 2$ y $X^2 - 3$ de P no se pueden intercambiar, por ejemplo r_2 satisface $r_2^2 - 2 = 0$ mientras que r_4 no lo hace. Las permutaciones $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ son las únicas permutaciones que conservan las relaciones entre las raíces.

Observación 2.9. Los elementos a tener en consideración para determinar un grupo de Galois de una ecuación son:

- a. Encontrar las raíces de una ecuación dada.
- b. Encontrar la resolvente de Galois.
- c. Determinar el polinomio mínimo.
- d. Encontrar las raíces del polinomio mínimo.

Para ampliar la observación 4.9, se hace necesario la presentación de ejemplos que modelan los elementos presentados en esta observación y completan lo expresado en los resultados anteriores. Es importante mencionar que hemos considerado como ejemplos ecuaciones generales y no particulares como en el ejemplo 4.8, esto para facilitar al lector una nueva mirada partiendo desde lo particular y lograr un acercamiento a lo general (en vista de que este documento es de tipo expositivo y no demostrativo estos ejemplos son presentados con efectos motivadores hacia el lector en caso de que este interesado en conocer más sobre esta teoría, en contrario el lector puede pasar directamente a la sección 4.3.2.).

Ejemplo 4.10. Determine el grupo de Galois de una ecuación de grado n .

Sea

$$P(X) = X^n - x_1X^{n-1} + \dots + (-1)^n x_n = (X - r_1) \dots (X - r_n) = 0$$

Una ecuación $P(X) = 0$ sobre un cuerpo F con fracciones racionales r_1, \dots, r_n sobre algún cuerpo de constantes K que contiene a F . El grupo de todas las permutaciones de r_1, \dots, r_n , se puede identificar con el grupo simétrico completo de S_n .

En efecto, si utilizamos el método contradicción y suponemos que $Gal(P/F)$ no es un grupo de permutaciones de r_1, \dots, r_n entonces por la proposición 10.5 Tinol (2001, pág 146) que indica *que para cualquier subgrupo G en S_n existe una fracción racional f en n indeterminados tal que $I(f)^6 = G$* podemos encontrar una fracción racional tal que $f(r_1, \dots, r_n) \in K(r_1, \dots, r_n) = F(r_1, \dots, r_n)$, que es no simétrico, de tal manera que

⁶ La notación $I(f)$ hace referencia a las permutaciones que quedan invariantes bajo la acción de f

$$f(\sigma(r_1), \dots, \sigma(r_n)) = f(r_1, \dots, r_n) \text{ para todo } \sigma \in \text{Gal}(P/F)$$

Lo que contradice el *resultado 4.7*

Ejemplo 4.11. Determine el grupo de Galois para las ecuaciones ciclotómicas de grado primo.

Sea

$$\phi_p(x) = X^{p-1} + X^{p-2} + \dots + X + 1 = 0$$

con p primo entonces el grupo de Galois es el grupo cíclico de orden $p - 1$.

Para probar esto, regresamos a los pasos en la determinación de un grupo de Galois. Sea ζ alguna raíz primitiva de la unidad de orden p , es decir, cualquier raíz de $\phi_p(x)$ son potencias de ζ , podemos elegir ζ como resolvente de Galois de $\phi_p(x)$. Ya que $\phi_p(x)$ es irreducible, el polinomio mínimo de ζ es $\phi_p(x)$.

La elección de la raíz primitiva g de $\phi_p(x)$, la denotamos

$$\zeta_i = \zeta^{g^i} \text{ para } i = 0, \dots, p - 2$$

por lo tanto las raíces de $\phi_p(x)$ son $\zeta_0, \dots, \zeta_{p-2}$, y las fracciones racionales de f_i son

$$f_i(X) = X^{g^i}.$$

Acorde a la definición de grupo de Galois, los elementos de $\text{Gal}(\phi_p/Q)$ son

$$\sigma_j: \zeta_i \rightarrow f_i(\zeta_j)$$

ya que

$$f_i(\zeta_j) = (\zeta^{g^j})^{g^i} = \zeta^{g^{i+j}}$$

y por el teorema de Fermat, se cumple que $g^{p-1} \equiv g^0 \pmod{p}$, que se deduce de la descripción anterior de σ_j , se puede simplificar a

$$\sigma_j: \zeta_i \rightarrow \zeta_{i+j}$$

Donde el subíndice $i + j$ es tomado del modulo $p - 1$ (es decir, reemplazando por el número entero entre 0 y $p - 2$ es congruente con $i + j$, si $i + j \geq p - 1$).

Por lo tanto

$$\sigma_j = \sigma_1^j \text{ para } j = 0, \dots, p - 2$$

así el $Gal(\phi_p/Q)$ es generado por el elemento σ_1 , en conclusión es un grupo cíclico de orden $p - 1$

Ejemplo 4.12. Sea P un polinomio con raíces simples r_1, \dots, r_n que cumplen la condición de Abel, es decir no son fracciones racionales $\theta_i(X) = F(X)$ tal que

$$r_i = \theta_i(r_1) \text{ para } i = 2, \dots, n$$

$$\text{y } \theta_i \theta_j(r_1) = \theta_j \theta_i(r_1) \text{ para todo } i, j.$$

A continuación se muestra, que el grupo de Galois de la ecuación $P(X) = 0$ es conmutativo⁷.

De hecho, en este caso se puede elegir r_1 como la resolvente de Galois. Ya que r_1 es una raíz de P , y el polinomio mínimo generado por r_1 divide a P por el lema 14.2 del texto de

⁷ Es por esto que los grupos conmutativos son conocidos como grupos abelianos.

Tinol (2001, pág 178) de ahí las raíces del polinomio mínimo son r_1 se encuentra en r_1, \dots, r_n .

El cambio de numeración es necesaria, por lo cual podemos suponer que estas raíces son r_1, \dots, r_m (con $m \leq n$). De acuerdo con la definición del grupo de Galois los elementos de $Gal(P/F)$ son $\sigma_1, \dots, \sigma_m$ donde

$$\sigma_j: r_i \rightarrow \theta_i(r_j) \text{ para } i = 1, \dots, n \text{ y } j: 1, \dots, m.$$

De esto se deduce que, para todo j, k entre 1 y m .

$$\sigma_j \circ \sigma_k: r_i \rightarrow \theta_j \theta_k(r_i) = \theta_j \theta_k \theta_i(r_1)$$

y

$$\sigma_k \circ \sigma_j: r_i \rightarrow \theta_k \theta_j(r_i) = \theta_k \theta_j \theta_i(r_1)$$

por lo tanto, la conmutatividad de $Gal(P/F)$ sigue fácilmente la condición de Abel.

4.3.2 El grupo de Galois bajo una extensión de cuerpo.

En la definición del grupo de Galois de una ecuación, el cuerpo base F juega un papel poco visible, pero importante. Así el propósito de esta sección es ampliar el foco sobre el cuerpo base e investigar que ocurre con el grupo de Galois cuando el cuerpo base se amplía por la adjunción de raíces de polinomios auxiliares. En vista a las aplicaciones a la solubilidad por los radicales, el caso crucial es la adjunción de p -ésimas raíces de elementos, es decir, las raíces de ecuaciones auxiliares del tipo X^p donde p es un número primo.

Al igual que en la sección anterior, denotemos por $P(X)$ el polinomio monico de grado n sobre el cuerpo F . Que tiene n raíces distintas r_1, \dots, r_n sobre algún cuerpo S que contiene a F .

$$P(X) = X^n - a_1X^{n-1} + \dots + (-1)^n a_n = (X - r_1) \dots (X - r_n)$$

La existencia del cuerpo S se garantiza por el teorema de Girard's (para un polinomio no constante $P(X) \in F[X]$ existe un cuerpo K que contiene a F , tal que P se puede descomponer como el producto de factores lineales sobre K). De hecho el cuerpo S puede ser elegido arbitrariamente grande, debido a, que solo el subcuerpo $F(r_1, \dots, r_n)$ es suficiente para la determinación del grupo de Galois para $P(X) = 0$ sobre F . Por lo tanto si algún cuerpo K que contiene a F podemos asumir que S contiene a K . De hecho, es suficiente aplicar el teorema de Girard's con el cuerpo base K en lugar de F . Esto nos permite combinar los elementos de K con elementos de $F(r_1, \dots, r_n)$ en los cálculos, y en particular, considerar el cuerpo $K(r_1, \dots, r_n)$ de fracciones racionales en r_1, \dots, r_n con coeficientes en K . Podemos entonces determinar el grupo de Galois $P(X) = 0$ sobre K así como sobre F , por el método mencionado en la sección anterior. La equivalencia de este enunciado se hace evidente en la siguiente proposición.

Proposición 2.13. Si K es un cuerpo que contiene a F , entonces $Gal(P/K)$ es un subgrupo de $Gal(P/F)$.

El objetivo de esta sección es obtener información adicional de las relaciones entre $Gal(P/K)$ y $Gal(P/F)$, considerando ciertas suposiciones sobre K . Más concretamente vamos a ilustrar, que si de K se obtiene de un adjunto (es decir, un par de funciones isomorfas que preservan relaciones de orden) de una raíz de un polinomio auxiliar irreducible $T(X) = 0$, entonces el cociente

$$\frac{|Gal(P/F)|}{|Gal(P/K)|}$$

es un número entero, es decir, el índice de $Gal(P/K)$ en $Gal(P/F)$ divide el grado de T . Por otra parte el cuerpo K se obtiene por un adjunto de todas las raíces de la ecuación $T(X) = 0$, entonces se cumple la siguiente propiedad.

$$\sigma \circ \tau \circ \sigma^{-1} \in Gal(P/K) \text{ para } \sigma \in Gal(P/F) \text{ y } \tau \in Gal(P/K)$$

La propiedad anterior se expresa diciendo que $Gal(P/K)$ es un subgrupo normal⁸ de $Gal(P/F)$.

En relación con los elementos abordados en esta sección es conveniente ilustrar estos aspectos en la solución de la ecuación de general de grado cuatro, que se ve afectada por la adjunción de una o todas sus raíces de un resolvente cubico.

Ejemplo 4.13. Sea $P(X) = (X - r_1)(X - r_2)(X - r_3)(X - r_4) = 0$ que es equivalente a $P(X) = X^4 - s_1X^3 + s_2X^2 - s_3X + s_4 = 0$, donde $P(X) = 0$ es la ecuación general de grado cuatro, con el cuerpo base de fracciones racionales en s_1, s_2, s_3, s_4

$$F = K(s_1, s_2, s_3, s_4)$$

Para algún cuerpo de constantes K (Observe que el cuerpo $K(s_1, s_2, s_3, s_4) = K(r_1, r_2, r_3, r_4)$ debido a que los coeficientes se pueden expresar como la combinación lineal de las raíces del polinomio). En el ejemplo 2.10 se encontró que el grupo de Galois $Gal(P/F)$ es el grupo de permutaciones de r_1, r_2, r_3, r_4 , el cual puede ser identificado como el grupo simétrico de S_4 ,

$$Gal(P/F) = S_4.$$

⁸ Definido $gAg^{-1} = \{gag^{-1} : a \in A\}$. Se define el grupo normal A en G como el conjunto que satisface $N_G(A) = \{g \in G : gAg^{-1} = A\}$

A partir, de los aportes hechos por Lagrange en la solución de las ecuaciones de grado 3 y 4, en el cual Lagrange plantea una forma de relacionar las raíces del polinomio en un grupo de permutaciones que brindan una herramienta para determinar la solución de las ecuaciones de grado 3 y 4 (si el lector desea conocer acerca de los aportes de Lagrange se recomienda estudiar la sección 10.2 Tinol (2001) o el trabajo de Chavarria (2014) en la sección 3.3.). A partir de este trabajo se deduce ecuación cúbica del resolvente realizado por Ferrari es

$$u_1 = -\frac{1}{2}(r_1 + r_2)(r_3 + r_4)$$

$$u_2 = -\frac{1}{2}(r_1 + r_3)(r_2 + r_4)$$

$$u_3 = -\frac{1}{2}(r_1 + r_4)(r_2 + r_3)$$

Dado que ninguna de estas raíces está en el cuerpo F (debido a que u_1, u_2, u_3 son números complejos), la resolvente cúbica es irreducible sobre F . Entonces se puede concluir $Gal(P/F(u_1))$ es un subgrupo de subíndice tres del grupo $Gal(P/F)$, así que el grupo $Gal(P/F(u_1, u_2, u_3))$ es un subgrupo normal en $Gal(P/F)$, de índice a lo sumo de seis.

De hecho, no es difícil determinar estos grupos de forma explícita, para ello consideremos lo siguiente. Note que las permutaciones en $Gal(P/F(u_1))$ dejan a u_1 invariante por el teorema 14.11 Tinol (2001, pág 250). Al denotar $I(u_1)$ como el subgrupo de s_4 que consiste en todas las permutaciones que dejan a u_1 invariante, se obtiene la relación

$$Gal(P/F(u_1)) \subset I(u_1).$$

Dado que, por el teorema de Lagrange, el índice de $I(u_1)$ en S_4 es 3 (es decir, el número de permutaciones de u_1 bajo las permutaciones en s_4), se deduce que

$$|I(u_1)| = |Gal(P/F(u_1))|$$

por lo tanto

$$I(u_1) = Gal(P/F(u_1)).$$

El razonamiento anterior, acerca de las permutaciones en $I(u_1)$ se pueden expresar de forma más explícita como los vértices de un cuadrado

$$\begin{array}{ccc} 1 & \rightarrow & 3 \\ \uparrow & & \downarrow \\ 4 & \leftarrow & 2 \end{array}$$

por la isometría que deja un cuadrado usualmente invariante. Este grupo es llamado usualmente grupo diedrico de orden 8. Los subgrupos $I(u_1)$, $I(u_2)$ y $I(u_3)$ de s_4 corresponden a las tres numeraciones no equivalentes de los vértices de un cuadrado.

Note que, el grupo $I(u_1)$ no es normal en s_4 . En efecto, si $\sigma \in s_4$ es una permutación que transforma u_1 en u_2 , entonces

$$\sigma \circ I(u_1) \circ \sigma^{-1} = I(u_2) \quad (\neq I(u_1)).$$

Sin embargo, el subgrupo $Gal(P/F(u_1, u_2, u_3))$ si es normal en s_4 , donde u_1 , u_2 y u_3 son invariantes bajo las permutaciones de este grupo. Por lo tanto se cumple la inclusión

$$Gal(P/F(u_1, u_2, u_3)) \subset I(u_1) \cap I(u_2) \cap I(u_3).$$

Las permutaciones del grupo $I(u_1) \cap I(u_2) \cap I(u_3)$ se definen como:

$$Id: \begin{cases} 1 \leftrightarrow 1 \\ 2 \leftrightarrow 2 \end{cases} \quad \sigma_1: \begin{cases} 1 \leftrightarrow 2 \\ 3 \leftrightarrow 4 \end{cases} \quad \sigma_2: \begin{cases} 1 \leftrightarrow 3 \\ 2 \leftrightarrow 4 \end{cases} \quad \sigma_3: \begin{cases} 1 \leftrightarrow 4 \\ 2 \leftrightarrow 3 \end{cases}$$

Por lo tanto se cumple la relación

$$|Gal(P/F(u_1, u_2, u_3))| \leq |I(u_1) \cap I(u_2) \cap I(u_3)| = 4$$

Por otro lado, el subíndice de $Gal(P/F(u_1, u_2, u_3))$ en S_4 es a lo sumo 6, por lo tanto se obtiene que

$$|Gal(P/F(u_1, u_2, u_3))| \geq 4.$$

Así

$$Gal(P/F(u_1, u_2, u_3)) = \{Id, \sigma_1, \sigma_2, \sigma_3\}.$$

4.3.3 Solubilidad por radicales.

Después de estudiar los elementos que componen el grupo de Galois de una ecuación y la importancia del cuerpo base, es momento de presentar la utilidad de estos dos aspectos en la solubilidad de una ecuación por el método de radicales. En consecuencia, una ecuación es soluble por radicales sobre un cuerpo F , si dado el polinomio $P(X)$ irreducible sobre F , la ecuación $P(X) = 0$ es soluble por radicales si y sólo si existe una extensión del cuerpo de F que contiene a todas las raíces de la ecuación.

Así, el resultado central de esta sección se representa en el teorema 4.14 que tiene como eje principal relacionar el grupo de Galois de una ecuación y las extensiones de cuerpo de cada una de sus raíces, determinando dos secuencias. La primera, es una secuencia que decrece a través de subgrupos normales al grupo de Galois; y la segunda, una secuencia creciente (implícita en el teorema) de cada uno de los cuerpos que contiene a las raíces del polinomio. Lo importante de este teorema es que es una antelación al teorema moderno de la

teoría de Galois (capítulo 4) el cual nos permite mostrar de forma más clara como la teoría de Galois es un caso particular de una conexión de Galois.

Teorema 4.14. Sea P un polinomio sobre un cuerpo F , y asuma que P solo tiene raíces simples en cualquier cuerpo que contiene a F . La ecuación $P(X) = 0$ es completamente soluble sobre F si y solo si el grupo de Galois $Gal(P/F)$ contiene la secuencia de subgrupos

$$Gal(P/F) = G_0 \supset G_1 \supset G_2 \dots \supset G_t = \{Id\}$$

de tal manera que, para $i = 1, \dots, t$, el subgrupo G_i es normal al índice anterior G_{i-1} . (Posiblemente, $t = 0$, es decir $Gal(P/F) = \{Id\}$)

De acuerdo con lo anterior, un grupo finito G se dice que es soluble si se satisface la condición del teorema, es decir, si contiene una secuencia de subgrupos empezando por G y terminando con $\{Id\}$, de manera que cada subgrupo es normal al subgrupo del índice anterior. En consecuencia, si el grupo G es soluble podemos asegurar que la ecuación es soluble por el método de radicales.

Observación 4.15. Al asumir que todas las raíces de la unidad se encuentran en el cuerpo base F entonces se cumple que el grupo de Galois $Gal(P/F)$ es soluble, es decir, existe una secuencia de subgrupos

$$Gal(P/F) = G_0 \supset G_1 \supset G_2 \dots \supset G_t = \{Id\}$$

Con G_i es normal al índice anterior G_{i-1} para $i = 1, \dots, t$, entonces una extensión racional de F que contiene todas las raíces de P se puede obtener por t extracciones de raíces. Primero la extracción de la raíz i -ésima de $(G_0:G_1)$, reduce al grupo de Galois a G_1 y la extracción de la raíz i -ésima de $(G_1:G_2)$, reduce el grupo de Galois a G_2 y así sucesivamente hasta t .

Para ilustrar el teorema 4.14 y la observación 4.15 se presenta el siguiente ejemplo

Ejemplo 4.16. Consideremos la solución de las ecuaciones de grado 3 y 4 empleando el método de solución por radicales. En primer lugar, se define para cualquier entero $n > 2$ un subgrupo A_n (un grupo alternante) de un grupo simétrico S_n , el cual es el conjunto de todas las permutaciones que deja invariante al polinomio (Discriminante) $\Delta(r_1, \dots, r_n)$ que se define como

$$\Delta(r_1, \dots, r_n) = \prod_{1 \leq i < j \leq n} (r_i - r_j).$$

Denotaremos el grupo A_n como el grupo de permutaciones que dejan invariante a Δ al discriminante como

$$A_n = I(\Delta)$$

donde el grupo A_n se llama alternante para $\{1, \dots, n\}$.

Note que cualquier permutación en $I(\Delta)$ deja invariante a Δ o la transforma en su contrario $-\Delta$ entonces A_n tiene índice 2 en S_n . Ahora, si empleamos el teorema de Lagrange se cumple la igualdad

$$|A_n| = \frac{n!}{2}$$

por lo tanto A_n es normal a S_n . Entonces, si $\sigma \in S_n$ y para todo $\tau \in A_n$, se cumple que $\sigma \circ \tau \circ \sigma^{-1} \in A_n$ por lo tanto $\sigma \in A_n$, ya que A_n es estable en los productos, si por el contrario $\sigma \notin A_n$, entonces $\sigma^{-1} \notin A_n$, donde

$$\sigma(\Delta) = \sigma^{-1}(\Delta) = -\Delta.$$

Por consiguiente, se cumple

$$\sigma \circ \tau \circ \sigma^{-1}(\Delta) = \sigma \circ \tau(\Delta) = \sigma(\Delta) = \Delta$$

lo que demuestra que $\sigma \circ \tau \circ \sigma^{-1} \in A_n$, como se requiere.

Consideremos, la ecuación general de grado n

$$P(X) = X^n - s_1X^{n-1} + \dots + (-1)^n s_n = (X - x_1) \dots (X - x_n) = 0$$

para $F = C(s_1, \dots, s_n)$ (El cuerpo de constantes se elige C de modo que todas las raíces de la ecuación están en F) y el grupo de Galois $Gal(P/F)$ puede identificarse con S_n (ejemplo 4.10). Dado que Δ^2 es el discriminante,

$$\Delta^2 = D(s_1, \dots, s_n) \in F,$$

donde Δ es la raíz del polinomio

$$X^2 - D(s_1, \dots, s_n) \in F[X].$$

Luego por el teorema 14.17 Tinol (2001, pág 256) el grupo $Gal(P/F(\Delta))$ es un subgrupo de índice 2 en $Gal(P/F) = S_n$. Dado que los elementos en $Gal(P/F(\Delta))$ dejan Δ invariante se da la contención

$$Gal(P/F(\Delta)) \subseteq A_n$$

por lo cual se concluye

$$Gal(P/F(\Delta)) = A_n$$

ya que estos grupos tienen índice 2 en S_n y tienen, por tanto, el mismo número de elementos.

Veamos ahora el caso de $n = 3$. Entonces se da secuencia de los subgrupos

$$S_3 \supset A_3 \supset \{Id\}$$

que muestra que s_3 es soluble, ya que el índice de A_3 en S_3 es 2 y el índice de $\{Id\}$ en A_3 es $|A_3| = 3$. Por lo tanto la ecuación de grado tres es totalmente soluble por el método de radicales. Por otra parte la extensión racional de F que contiene todas las raíces puede ser obtenida por dos extracciones de raíces: en primer lugar, la extracción de una raíz cuadrada, que reduce el grupo de Galois de S_3 a A_3 , y luego la extracción de una raíz cúbica, lo que reduce el grupo de Galois a $\{Id\}$. Más precisamente, la discusión anterior muestra que la raíz cuadrada tiene que ser extraída primero, debe ser la del discriminante $D(s_1, s_2, s_3)$, ya que de hecho $Gal(P/F(\Delta)) = A_3$.

Ahora consideremos el caso para $n = 4$, recordemos que en el ejemplo 4.13, hemos visto que la adjunción sobre el cuerpo F de todas las raíces del resolvente cubico de Ferrari reduce el grupo de Galois a

$$V = \{Id, \sigma_1, \sigma_2, \sigma_3\},$$

donde σ_1, σ_2 y σ_3 son conmutativos y satisfacen $(\sigma_1)^2 = (\sigma_2)^2 = (\sigma_3)^2 = Id$. Por lo tanto, $\{Id, \sigma_1\}$, $\{Id, \sigma_2\}$ y $\{Id, \sigma_3\}$ son subgrupos normales de índice 2 en V . Por otra parte, una verificación directa muestra que σ_1, σ_2 y σ_3 dejan invariante a Δ , en donde

$$V \subset A_4.$$

Al contar los elementos en A_4 , obtenemos

$$(A_4:V) = 3.$$

Puesto que V es normal en S_4 (en el ejemplo 2.13) entonces V es normal en A_4 . Así la secuencia

$$S_4 \supset A_4 \supset \{Id, \sigma_1\} \supset \{Id\}$$

muestra que S_4 es soluble. En consecuencia, la ecuación general de grado 4 es completamente soluble por radicales sobre F .

Además, la secuencia anterior de subgrupos, muestra que una extensión racional de F que contiene todas las raíces se obtiene por las siguientes operaciones:

- 1) La extracción de la raíz del discriminante $D(s_1, s_2, s_3, s_4)$ que reduce el grupo de Galois a A_4 .
- 2) La extracción de la raíz cúbica, que reduce el grupo de Galois a V .
- 3) La extracción sucesiva de raíces cuadradas que reduce el grupo de Galois a $\{Id, \sigma_1\}$.
- 4) La extracción sucesiva de raíces cuadradas que reduce el grupo de Galois a $\{Id\}$.

A modo de conclusión, se hace necesario mencionar que el trabajo de Galois a progresado en su representación axiomática tal como se quiere relacionar con la transición de las matemáticas clásicas a las modernas y contemporáneas; este progreso se ve representado en la forma en la cual se representan sus contenidos matemáticos del capítulo tres y el capítulo cuatro. Puesto que en el capítulo tres se realiza paso a paso la elaboración detallada de cada uno de los elementos que hacen parte del teorema fundamental de la teoría de Galois mientras que en el capítulo cuatro nuevamente se realiza este proceso pero con la diferencia de que no se es tan claro y organizado al momento de definir cada concepto, en parte porque aún no están claramente definidos y en otras porque la notación empleada en el cuarto capítulo es más compleja.

Por otro lado, es necesario mencionar la relación entre la teoría de Galois y la solución de ecuaciones por el método de radicales la cual se hace evidente en la sección 4.3.3. Puesto que, en esta sección se aborda nuevamente en relación con otros periodos históricos la solución general de las ecuaciones de grado tres y cuatro y nuevamente se logra demostrar que estas ecuaciones tienen soluciones generales como lo habían logrado los matemáticos Renacentistas y Lagrange. Y también continúa la dificultad para abordar las ecuaciones de grado mayor a cuatro en forma general, por lo cual Galois solo se limita a dar condiciones para la solución de ecuaciones particulares.

5. LA TEORÍA DE GALOIS COMO UNA ADJUNCIÓN. UNA REFLEXIÓN DIDÁCTICA EN LA ENSEÑANZA DE LAS MATEMÁTICAS EN LA FORMACIÓN INICIAL DE PROFESORES.

“Las matemáticas poseen no sólo la verdad, sino cierta belleza suprema. Una belleza fría y austera, como la de una escultura.”

Bertrand Russell

Este capítulo se divide en tres partes, en la primera, se presenta una explicación de un ejemplo tomado del libro de Román (2008), el cual hace evidente la relación entre la teoría de Galois como un caso particular de una adjunción, utilizando como referencia los elementos teóricos abordados en los capítulos dos, tres y cuatro y profundizando en los ejemplos 3.91 y 3.92; en la segunda, se expone una reflexión acerca del papel de la obra de Galois en la formación inicial de profesores, la cual se enfoca en destacar una de las ventajas de conocer la obra de Galois, en especial de la teoría de adjunciones por parte de un profesor en formación inicial de matemáticas; en la tercera se presentan las conclusiones de este documento a través de la visualización de un objeto matemático representado en los periodos de las matemáticas clásicas, modernas y contemporáneas, lo que permite vincular algunas problemáticas de la evolución del objeto matemático con algunas de las problemáticas de la transición de un estudiante de secundaria a los primeros años de la universidad.

5.1 La Teoría de Galois como una adjunción.

Uno de los objetivos a desarrollar en este trabajo se enfoca, en realizar un acercamiento a la teoría de Galois como una adjunción y para esto tomaremos como referente los elementos teóricos abordados en el capítulo dos hasta el capítulo cuatro, en los cuales se realizó un recorrido histórico y matemático de las adjunciones y la teoría de Galois y el ejemplo 3.14 de la página 59 de la obra de Steven Román “*Lattices and ordered sets*” el cual expresa la teoría de Galois como una adjunción.

5.1.1 Algunos comentarios de la teoría de Galois como una adjunción.

Para comentar acerca de la teoría de Galois como una adjunción se recomienda al lector revisar los ejemplos 3.91 y 3.92 los cuales serán referentes en unos comentarios. Además es importante mencionar el ejemplo de Steven Román a través de la proposición 5.1 como uno de los elementos referentes para este documento.

Proposición 5.1. Sea F y E dos cuerpos con $F \subseteq E$. Sea $G = G(E/F)$ el grupo de isomorfismos que fijan cada elemento de F . El grupo es llamado grupo de Galois de la extensión de cuerpo $F \leq E$. Existe una correspondencia de Galois entre los cuerpos intermedios $F \subseteq K \subseteq E$ y los subgrupos H del grupo de Galois G .

Esta correspondencia está dada por

$$K \rightarrow G(E/K) := \{\sigma \in G / \sigma x = x \text{ para todo } x \in K\}$$

Y

$$H \rightarrow \text{fix}(H) := \{x \in E / \sigma x = x \text{ para todo } \sigma \in H\}.$$

Recordemos que, una conexión de Galois se compone de dos funciones llamadas adjunto izquierdo y adjunto derecho, las cuales envían elementos entre conjuntos parcialmente ordenados. Por lo tanto si queremos interpretar la idea expresada en la proposición 5.1 lo primero que debemos identificar son estos dos conjuntos y cuáles son sus relaciones de orden.

En este sentido, el primer conjunto se puede definir como la colección de todos los cuerpos los cuales se relacionan bajo la inclusión y más concretamente un cuerpo es la extensión de otro a partir de un cuerpo base. El segundo conjunto es la colección de todos los subgrupos normales del grupo de Galois de una ecuación separable y su relación de orden nuevamente es la inclusión esta vez entre grupos.

Continuando con este proceso, observemos que en la proposición 5.1 se definen ya los dos adjuntos los cuales como se mencionó dependen de las extensiones de cuerpo y de los subgrupos del grupo de Galois, ahora nos interesa hablar de la relación inversa entre estos dos adjuntos los cuales se pueden ver reflejas en las secuencias estudiadas en los ejemplos 3.91 y 3.92.

Así, al analizar estos ejemplos podemos evidenciar que mientras la secuencia de extensiones de cuerpo va creciendo, partiendo del cuerpo en el cual se encuentra los coeficientes del polinomio hasta el cuerpo más pequeño que contiene las raíces de la ecuación $P(x) = 0$; la secuencia de subgrupos va decreciendo partiendo del grupo de Galois del polinomio y llegando hasta la permutación. Lo interesante de esta dualidad es que existe una correspondencia entre las extensiones y los elementos que componen el grupo de Galois

como se puede evidenciar en el ejemplo 3.66 que refleja como a cada extensión le corresponde una extensión.

Con base a lo expresado en la proposición 5.1 y los comentarios anteriores podemos afirmar que la teoría de Galois es un caso particular de una adjunción, lo cual nos permitirá llegar a algunas conclusiones en la sección siguiente, debido a, que “la teoría de Galois es uno de los grandes momentos del desarrollo de las matemáticas, con notables transferencias conceptuales, hacia los más variados dominios de la matemática” Zalamea (2009) e incide en el paso de las matemáticas clásicas a las matemáticas modernas y contemporáneas.

En relación con lo anterior, consideremos un ejemplo de las matemáticas contemporáneas que sea producto de la transición de las matemáticas clásicas a las modernas y contemporáneas, el cual nos permita observar los beneficios de realizar este estudio, para ello consideremos la teoría de categorías que relaciona dos morfismos (adjuntos) y se respeta la composición entre estos. En este sentido, como se mencionó anteriormente la teoría de adjunciones está vinculada con diversos aspectos de las matemáticas actuales lo que le permite al lector una visión más amplia de cada uno de estos.

Por otra parte, el estudio de la teoría de Galois como una adjunción contempla otros factores los cuales hacen parte de estas teorías, como por ejemplo la teoría de extensiones y la teoría de grupos las cuales se estudiaron a lo largo de este documento, a pesar de no estar dentro de los objetivos, debido a que de una forma u otra su desarrollo como objeto matemático estuvo influenciado por la teoría de adjunciones como se puede evidenciar si se realiza un análisis de los capítulos tres y cuatro de este documento.

5.2. Una reflexión sobre el papel de la obra de Galois en la formación inicial de profesores en el campo de las matemáticas.

A lo largo de este documento se abordó en su gran mayoría la obra de Galois en dos conceptos importantes: el primero, la teoría de Galois que logra resolver uno de los grandes problemas en la historia del álgebra, referente a qué tipo de ecuaciones de grado mayor o igual a cinco son solubles por el método de radicales; el segundo las conexiones de Galois que deben sus orígenes a las investigaciones en múltiples objetos matemáticos y actualmente muchos objetos matemáticos se pueden expresar como una conexión. Así el estudio de la obra de Galois nos permite realizar un acercamiento a aspectos históricos de las matemáticas, y conocer nuevos elementos o aspectos “ocultos” de los objetos matemáticos modernos.

En este sentido, en la parte final de este documento nos interesa relacionar el recorrido histórico de la teoría de Galois, las adjunciones y la teoría de Galois como una adjunción con las distintas interpretaciones que puede tener un profesor en formación inicial en matemáticas de un objeto matemático y en qué forma puede contribuir en los procesos de enseñanza de las matemáticas que un educador matemático conozca la obra de Galois.

5.2.1. Un ejemplo histórico en la educación actual. El papel de las conexiones de Galois.

Consideremos el ejemplo del libro de Abu Kamil's Álgebra abordado en el capítulo dos en los aspectos históricos de las conexiones de Galois, en el cual se argumenta como Abu Kamil's llegaba a conclusiones y resultados verídicos acerca de las condiciones bajo las cuales una ecuación tenía soluciones en los números racionales, de seguro, sin tener

conciencia de lo que realmente se desarrollaba detrás de sus resultados; como se expuso en ese mismo ejemplo tenía que ver directamente con el concepto de conexión de Galois.

Ahora consideremos el mismo argumento anterior, pero esta vez con dos procesos matemáticos tan vigentes en la vida cotidiana de una persona, como en la enseñanza de las matemáticas. Nos referimos a las operaciones de sumar y restar que ambas constituyen una conexión de Galois y que tal vez muchos profesores en formación inicial de matemáticas, al igual que Abu Kamil's no lo tienen en consideración. Es decir, que muchos años después seguimos llegando a resultados y pasando por alto la profundidad en argumentos de fondo en las matemáticas.

Argumentos como los anteriores, nos permiten reflexionar acerca de lo útil que puede ser conocer el concepto de una conexión de Galois. Puesto que, cuando un educador en matemáticas conoce lo que hay de fondo, tiene una visión más amplia de lo que desea enseñar, cuenta con una nueva herramienta didáctica que le permite anticiparse a las dificultades que puedan afrontar sus estudiantes.

Además, es importante mencionar que el estudio de las conexiones enriquece los conocimientos de un docente de matemáticas en procesos elementales como sumar y restar a procesos muchos más abstractos como la teoría de Categorías Román (2008). Así que al realizar un acercamiento a las conexiones no solo le brinda herramientas a un docente para enseñar un determinado concepto, sino que también para abrir acercamientos a conceptos más generales, lo cual nuevamente contribuye a la formación de profesores en matemáticas.

5.2.2. El papel de la teoría de Galois.

Hasta ahora, hemos dejado un poco de lado la teoría de Galois pero cabe resaltar que esta teoría es un ejemplo de una conexión de Galois y es uno de los factores históricos en el desarrollo de una conexión. Sin embargo, es importante darle el protagonismo a la teoría de Galois que se merece.

La teoría de Galois, como se mencionó anteriormente influyó en el desarrollo histórico de las matemáticas, siendo relevantes el paso por los periodos de contar, medir y ordenar hasta el periodo de estructuras. Ahora, nuestro interés se centra en relacionar, el desarrollo histórico de las matemáticas con el proceso educativo que afronta un estudiante cuando realiza el cambio de la educación secundaria (etapa de contar, medir y ordenar) a la educación superior (etapa de estructuras) el cual para muchos estudiantes causa grandes dificultades.

En este orden de ideas, si un profesor en formación inicial en matemáticas ha estudiado el impacto histórico de la teoría de Galois en el desarrollo de las matemáticas y conoce de la relación de la historia de esta ciencia con la educación, le permite conocer en que desarrollos aparentemente elementales, como por ejemplo la solución de ecuaciones en procesos de $+$ y $-$, se encierran características estructurales de las matemáticas actuales. Por lo tanto, estudiar este tipo de transiciones, las cuales generan procesos de decantamiento sobre las problemáticas de abordar un objeto matemático, le permiten al educador abordar dicho objeto desde perspectivas diferentes.

5.3. Conclusiones.

En esta sección se presentan dos elementos que nos permiten desarrollar las conclusiones de este documento. El primero, referente a una síntesis histórica que muestra la relación de momentos históricos de la matemática con el desarrollo de este trabajo; y el segundo, que expone un ejemplo paradigmático generado por la teoría de Galois que expone el desarrollo de un objeto matemático a través de las matemáticas clásicas, modernas y contemporáneas.

5.3.1. Síntesis histórica.

Hemos mostrado que la hoy denominada Teoría de Galois tiene sus inicios alrededor de 1830, al interior del estudio de la resolución de ecuaciones polinómicas. Específicamente se trataba de responder el interrogante ¿Por qué no existe una fórmula para la resolución de ecuaciones polinómicas de quinto grado por el método de radicales? Para ser más precisos la pregunta se extendía a ecuaciones de grado mayor o igual a cinco, y se entendía por fórmula una expresión en términos de los coeficientes del polinomio, usando sólo operaciones algebraicas y la extracción de raíces. Las operaciones algebraicas consideradas eran la suma y la multiplicación; que con los opuestos e inversos incluía la resta y la división.

Recordemos que ya se conocían fórmulas para las ecuaciones de segundo, tercer y cuarto grado. Realmente es el teorema de Abel-Ruffini el que inicia formalmente la Teoría de Galois dando una respuesta al interrogante planteado. Pero es justamente Galois quién proporciona una elegante respuesta a este interrogante, que además da cuenta en detalle por qué es posible resolver ecuaciones de grado inferior al cuarto, y por qué las soluciones son expresables mediante operaciones algebraicas y extracción de raíces.

De otro lado la Teoría de Galois dio respuesta a otros interrogantes clásicos, como el de la constructibilidad mediante regla y compás. Determina cuándo es posible construir una cierta longitud proporcional a una dada y así se responde a interrogantes como: ¿Qué polígonos regulares son construibles mediante regla y compás? ¿Por qué no es posible la trisección de un ángulo?

Hoy por hoy la teoría de Galois tiene aplicaciones en la teoría de códigos lineales detectores-correctores de errores, comunicaciones digitales, seguridad informática, cifrado de datos, geometría algebraica sobre campos de Galois, sucesiones sobre estructuras algebraicas finitas, funciones especiales, esquemas de compartición de secretos, esquemas de autenticación, polinomios de permutación, sumas exponenciales sobre campos y anillos de Galois, entre otras.

En su tiempo los aportes de Évariste Galois no alcanzaron la comprensión de sus contemporáneos, debido a que el lenguaje empleado por Galois no era lo suficientemente claro para sus lectores sino hasta finales del siglo XIX., que se tuvo una comprensión de la profundidad y alcance de los mismos dando lugar al surgimiento de Teoría de Grupos y Cuerpos de Galois.

Por demás esta teoría se convierte en el ejemplo de adjunción; al punto que este tipo de conexiones hoy llevan su nombre, debido a que históricamente la teoría de Galois genera el desarrollo de las conexiones.

5.3.2. La teoría de Galois como un ejemplo paradigmático en el desarrollo de las matemáticas clásicas a las modernas y contemporáneas

Consideremos un objeto matemático generado por la teoría de Galois como un ejemplo paradigmático el cual nos permita ilustrar su proceso de evolución en las matemáticas

clásicas, las matemáticas modernas hasta llegar a las matemáticas contemporáneas. En este sentido, hemos tomado en consideración la teoría de ecuaciones, el cual es absequible para nosotros debido a que ha sido abordada de forma explícita durante este documento.

En el primer objetivo se presentó un acercamiento a algunos elementos relacionados con la solución de ecuaciones por el método de radicales, lo cual influyo en el desarrollo histórico de la teoría de ecuaciones. Así este periodo lo podemos describir como la representación de la teoría de ecuaciones en las matemáticas clásicas, como se hizo referencia en el capítulo uno que se caracterizaban por realizar cálculos relacionados con problemas de la vida cotidiana y apenas se gestaba el concepto de ecuación, es decir era una teoría de ecuaciones en la cual se realizaban procesos aplicativos y se inducía a los procesos de generalización, por lo tanto podemos describir este periodo como una teoría de ecuaciones de contar, medir y ordenar.

En el tercer objetivo se abordó la teoría de Galois desde una perspectiva matemática e histórica respectivamente, donde se puede observar que se soluciona uno de los grandes problemas de la teoría de ecuaciones referente a las condiciones bajo las cuales una ecuación de grado mayor a cuatro era soluble por radicales. Durante la búsqueda de estas condiciones se empieza a establecer el concepto de grupo gestado principalmente por Lagrange quien sienta las bases del álgebra moderna. En este sentido el proceso de evolución de la teoría de ecuaciones al origen y desarrollo de los conceptos del álgebra moderna, como grupos, cuerpos, extensiones de cuerpo, se puede describir como la representación de la teoría de ecuaciones en las matemáticas modernas.

Dentro de los comentarios de este documento (objetivo cinco) y en el desarrollo del mismo (objetivo dos), se mencionaron dos aspectos, el primero, que a través del desarrollo de la

teoría de ecuaciones se dio origen a la teoría de adjunciones; y el segundo, que la teoría de categorías se puede representar por medio de las adjunciones. Por lo tanto, podemos aludir que la evolución de la teoría de ecuaciones es la teoría de categorías, la cual la podemos visualizar como la representación de la teoría de ecuaciones en las matemáticas contemporáneas.

En este orden de ideas, podemos concluir que es posible visualizar la evolución de un objeto matemático durante los tres periodos históricos mencionados, lo cual nos permite relacionar las problemáticas de la evolución de este objeto y las problemáticas que puede enfrentar un estudiante a medida que avanza en los distintos procesos educativos.

En relación con lo anterior, consideremos el proceso académico de un estudiante en el área de matemáticas en dos niveles educativos, el colegio y los primeros años de la universidad. En este sentido desde nuestro punto de vista y desde nuestra experiencia personal las matemáticas que se enseñan en el colegio son de tipo aplicativas, es decir, están relacionadas con las matemáticas clásicas, y las matemáticas que se enseñan al iniciar el proceso universitario están relacionadas con las matemáticas estructurales, es decir, con las matemáticas modernas.

Ahora bien, a lo largo de este documento estudiamos algunos procesos y algunas dificultades en la evolución de las matemáticas a través de la transición de las matemáticas clásicas a las modernas y contemporáneas, tal vez las mismas problemáticas que afronta un estudiante cuando pasa de la educación secundaria a la educación universitaria en sus primeros años, es por esto que si un educador matemático conoce este tipo de problemáticas históricas cuenta con herramientas didácticas como el conocer las adjunciones y los problemas históricos, las cuales les pueden contribuir en sus procesos de enseñanza.

Además, si un educador matemático, vincula herramientas didácticas relacionadas a conocer las problemáticas históricas como el abordado en este documento, enriquece sus procesos de enseñanza y de paso le facilita al estudiante la transición en sus procesos académicos, debido a, que el educador matemático es consciente del paso del colegio (matemáticas clásicas) a la universidad en sus primeros años (matemáticas modernas), permitiéndole anticiparse a esta problemática vinculando las matemáticas estructurales mucho antes de entrar a la universidad.

Finalmente se insiste que este sólo es un ejemplo con el que se intenta llamar la atención a la práctica de la educación matemática. Que colateralmente llama la atención de una mejor formación matemática en los profesores de esta área, que incluso sin tener formación plena en matemáticas se enfrentan a este tipo de teorías brindando una apertura al devenir académico de los estudiantes.

BIBLIOGRAFÍA

- Chavarria, S. (2014). *De las ecuaciones a la teoría de grupos, algunos obstáculos epistemológicos*. Santiago de Cali: Universidad del valle.
- David S. Dummit, Richard M. Foote . (2003). *Abstract Algebra*. John Wiley & Sons Inc.
- Gutiérrez, S. (2011). Évariste Galois: un genio en la base del álgebra moderna. *Suma*, 101-106.
- K. Denecke, M. E. (2004). *Galois Connections and Applications*. University of Lethbridge, Lethbridge: Springer Science+Business Media, B.V.
- Lautman, A. (2006). *Ensayos sobre la dialéctica, estructura y unidad de las matemáticas modernas*. Bogotá: Universidad Nacional de Colombia. Facultad de Ciencias Humanas.
- Murcia, F. (2009). *La Transición del Álgebra Clásica al Álgebra Moderna: Algunos aspectos históricos- epistemológicos en el desarrollo de la noción de estructura a través de la teoría de ecuaciones*. Santiago de Cali: Universidad del Valle.
- Puig, L. (1998). Componentes de una historia del álgebra. El texto de Al-Khwarizmi restaurado. *Investigaciones en Matemática Educativa II*, 109-131.
- Roman, S. (2008). *Lattices and Ordered Sets*. New York: Spring Street.
- Smith, P. (2010). *The Galois Connection Between Syntax and Semantics*. Cambridge : University of Cambridge .
- Tinol, J.-P. (2001). *Galois' Theory of Algebraic Equations* . Universite Catholique de Louvain, Belgium: World Scientific.
- Torres, L. A. (2010). *Fenomenología histórica del concepto de ecuación y potencialidades de su uso en la escuela*. Santiago de Cali: Universidad del Valle.
- Zalamea, F. (2009). *Filosofía sintética de las matemáticas contemporáneas*. Bogotá: Universidad Nacional de Colombia.