ANÁLISIS DE ESTRUCTURAS DEL GRUPO DE MONODROMÍA Y EL GRUPO DE GALOIS PARA POLINOMIOS POR MEDIO DEL TEOREMA DE ABEL RUFFINI

Autor: Mónica Julieth Barón Aya

Universidad El Bosque

Facultad de Ciencias

Matemáticas

Bogotá D.C.
2021

ANÁLISIS DE ESTRUCTURAS DEL GRUPO DE MONODROMÍA Y EL GRUPO DE GALOIS PARA POLINOMIOS POR MEDIO DEL TEOREMA DE ABEL RUFFINI

Autor: Mónica Julieth Barón Aya

Directores de Tesis: Andrei Alain González Galeano
Esteban Herrera Carvajal

Universidad El Bosque

Facultad de Ciencias

Matemáticas

Bogotá D.C.
2021

El presente trabajo de grado recibió aprobación por parte de los jurados asignados.

Calificación: 4.3

Resumen

El teorema fundamental del álgebra garantiza que la ecuación general de grado n tiene al menos una solución en los complejos, pero no es posible encontrar una solución general por radicales para tal ecuación cuando $n \geq 5$, esta afirmación es conocida como el teorema de Abel-Ruffini.

Son varias las demostraciones para este teorema, siendo una de estas la planteada por el mismísimo Niels Henrick Abel. Sin embargo, en este trabajo las demostraciones de interés son aquellas desarrolladas por Évariste Galois y Vladimir Igorevich Arnold, quienes abordan el teorema desde distintos campos de la matématica; por un lado la primera demostración usa el grupo de Galois, por su parte, la segunda usa el grupo de monodromía.

El objetivo principal del presente trabajo consiste en analizar el grupo de Galois desde la Teoría de Galois y el grupo de monodromía desde la topología Algebraica con el fin de encontrar las herramientas que permitan la creación de un isomorfismo entre ambos grupos. Para ello se realiza una revisión de todos los conceptos previos que permiten comprender a cada uno de los grupos con su respectiva demostración del teorema de Abel-Ruffini.

Tras el análisis se encuentra que los grupos de Galois de un polinomio $f(x)$ y monodromía de una función multivaluada $w(z)$ son grupos de permutaciones, en el primer caso se permutan las raíces del polinomio, mientras que en el segundo hay una permutación de los posibles valores que toma la función w al ser evaluada en un punto z_0. Además, si se toma la función multivaluada $w(z)$ tal que $f(w(z)) = 0$ las permutaciones del grupo de Galois permutan la misma cantidad de elementos que las del grupo de monodromía.

Palabras claves – Grupo Galois, grupo monodromía, polinomio general.

Abstract

The fundamental theorem of algebra guarantees that the general equation of degree n has at least one solution in the complexes, but it is not possible to find a general solution by radicals for such an equation when $n \geq 5$, this statement is known as the Abel-Ruffini theorem.

There are several proofs of this theorem, one of them being the one proposed by Niels Henrick Abel himself. However, in this work the proofs of interest are those developed by Évariste Galois and Vladimir Igorevich Arnold, who approach the theorem from different fields of mathematics; first proof uses the Galois group while the second uses the Monodromy group.

The main objective of of the present work is the analysis of the Galois group from the Galois Theory and the monodromy group from the algebraic topology in order to find those tools that allow the creation of an isomorphism between both groups. For this we will first review all the previous concepts that that hat allow understanding each of the groups with their respective proof of the Abel-Ruffini.

After the analysis it is found that the Galois group of a polynomial $f(x)$ and the monodromy group of a multivalued function $w(z)$ are groups of permutations, in the first case the roots of the polynomial are permuted, while in the second there is a permutation of the possible values that the function w takes when it is evaluated at a point z_0. Moreover, if one takes the multivalued function $w(z)$ such that $f(w(z)) = 0$ the permutations of the Galois group permute the same number of elements as those of the monodromy group.

Keywords – Galois group, monodromy group, general polynomial.

Índice general

Índice de figuras

Introducción

Históricamente las ecuaciones han tenido gran impacto en el desarrollo de la matemática y facilitando la vida humana, naciendo como la forma de resolver problemas cotidianos de distribución, pagos, entre otros (El papiro de Rhind evidencia ello, así como otros tantos papiros antiguos). Por otro lado, a través del tiempo, las ecuaciones, también han sido la motivación para formular nuevos debates y problemas matemáticos, como fue en su momento la aceptación de los números negativos, irracionales e imaginarios como números.

Aunque las definiciones de polinomio y ecuación de la antigüedad no estaban tan formalizadas como las actuales, Ruiz (sf) explica que para la época de los babilonios ya se resolven problemas que implícitamente dan solución para algunos polinomios de grado 2, pues resuelven ecuaciones del tipo $x^2 + bx = c$ y $x^2 - bx = c$ siempre y cuando b y c fuesen números positivos. En lo que respecta a las ecuaciones lineales de la forma $ax + b = 0$ en el papiro de Rhind (Egipto) se evidencian varios problemas que dan solución a esta ecuación.

Previo al siglo XVI se presentan soluciones particulares a los polinomios de grado 3, pero es en el siglo XVI cuando los italianos Scipione dal Ferro, Niccolò Tartaglia y Gerolamo Cardano dan una solución general para las ecuaciones cúbicas.

En el caso de los polinomios de grado 4, Rzedowski Calderón (2016) cuenta como Ludovico Ferrari, alumno y secretario de Cardano descubre que estas ecuaciones pueden ser reducidas a ecuaciones cúbicas y, por lo tanto, ser resuelta por medio de las fórmulas generales para las ecuaciones cúbicas y cuadráticas, los resultados para estas dos últimas no salieron a la luz hasta que Cardano las publica en 1545 en su libro "Ars Magna", dando crédito a Ferro, Tartaglia y Ferrari.

Por más de un siglo la incógnita sobre una fórmula general para las ecuaciones de grado 5 se mantiene viva, hasta que en 1799 Paolo Ruffini en la búsqueda de ésta descubre que no es posible encontrar una solución general por radicales, presentando una demostración basada en argumentos de teoría de grupos y en específico los métodos de Lagrange que asociaban los grupos simétricos de permutaciones S_n con los polinomios. Tal demostración se encuentra en sus textos *"Teoria generale della equazione"*(1799) y *Reflessioni intorno alla soluzione della equazioni algebriche generali"*(1813). Aunque esta demostración iba por buen

camino, no es aceptada en su tiempo, pues cuenta con la ausencia de detalles importantes para que se considere completa, como lo es justificar que los radicales pudiesen expresarse como funciones racionales de las raíces de la ecuación.

Por su parte, a finales del año 1823 el matemático escandinavo Niels Henrick Abel logra dar una demostración concreta para el que ahora es conocido como el Teorema de Abel-Ruffini "*Para $n \geq 5$ la ecuación general algebraica de grado n, no es soluble por radicales.*" En el año 1824 publica su primera demostración en una memoría, que debido al coste de la impresión no fue tan detallada como esperaba, siendo en algunos casos hasta ilegible. No obstante, en 1826 realiza una demostración más elaborada que publica en el primer volumen del *"Journal de Crelle"*.

Para su demostración, Sánchez Muñoz (2011) explica que Abel parte considerando el coeficiente $a_n = 1$ y al resto de coeficientes a_i como sumas y productos de sus raíces. De manera que a_{n-1} es la suma de todas las raíces, a_{n-2} es la suma del producto de las raíces tomadas dos a dos, en general a_{n-i} es la suma del producto de las raíces tomadas i en i, siendo estas las llamadas identidades de Girard.

Años después, en 1843 Joseph Liouville publica las contribuciones matemáticas del francés Évariste Galois, quien había fallecido en 1832. Finalmente en 1846 el manuscrito de Galois fue publicado en el *"Journal des mathématiques pures et appliquées"*, donde , inspirado por Abel crea su propia demostración del teorema usando el concepto de grupo de Galois para polinomios, que consiste en un subconjunto de permutaciones de las soluciones del polinomio. Un desarrollo muy importante en esta demostración es el teorema que garantiza que un polinomio es soluble por radicales si y solo si su grupo de Galois es soluble.

Para el año 1963 se presenta una nueva demostración del teorema de Abel-Ruffini, pero esta vez con el uso de superficies de Riemann. Esta es presentada por el profesor ruso Vladimir Igorevich Arnold en una de sus conferencias en una escuela secundaria de Moscú, y la cual es publicada en el 2004 por uno de sus alumnos del momento B.V. Aleskeseev en un libro donde se encuentra información de lo propuesto en todas esas clases.

En términos generales esta demostración consiste en considerar la función algebraica $w(z)$ que expresa las raíces de la ecuacione polinomial de grado 5 $3w^5 - 25w^3 + 60w - z = 0$ y calcular el grupo monodromía para esta función, de

forma que finalmente se obtenga que este es el grupo simétrico de permutaciones S_5. Para concluir de igual forma a como se hizo con la prueba de Galois, se usa el argumento de que S_n no es soluble para $n \geq 5$.

Justificación

La humanidad ha estudiado los polinomios y sus soluciones durante siglos, desde la época de los babilonios-1800 a.C- ya era conocida la solución para polinomios de grado 2. Esta busqueda de soluciones generales para polinomios continua avanzando en la historia de las matemáticas hasta llegar al conocido teorema de Abel- Ruffini, el cuál plantea la imposibilidad de encontrar una fórmula general por radicales para la solución de los polinomios de grado mayores o igual que 5. Demostraciones sobre este teorema ha habido varias, entre ellas las realizadas por Abel y Ruffini.

En este trabajo se estudian las demostraciones realizadas por Évariste Galois desde la teoría que lleva su nombre, y por el ruso Vladimir Igorevich Arnold desde la topología algebraica, pues es de gran interés la similitud de estas dos demostraciones.

La principal razón e interés para el desarrollo de este proyecto yace de la ampliación del conocimiento respecto al teorema de Abel-Ruffini que da respuesta a la pregunta de si es posible resolver por radicales los polinomios generales de grado mayor o igual que 5.

El enfoque principal consiste en encontrar similitudes entre ambas demostraciones y así proponer una relación entre el grupo de Galois de un polinomio $f(x)$ con el grupo monodromía de una función multivaluada $w(z)$.

Objetivos

Objetivo General

Encontrar las condiciones necesarias para construir un isomorfismo entre el grupo monodromía de funciones multivaluadas y el grupo de Galois para polinomios, por medio de la demostración del Teorema de Abel-Ruffini.

Objetivos específicos

- Comparar la demostración del teorema de Abel-Ruffini usando grupo de Galois y grupo de monodromía.
- Analizar y describir las caracteristicas principales de los grupo de monodromía de una función multivaluada $w(z)$ y Galois de un polinomio $f(x)$.

Metodología

Por la naturaleza de este trabajo, se inicia con la revisión y análisis del marco teórico, lo que permite la comprensión de conceptos básicos necesarios para realizar la demostración del teorema de Abel-Ruffini "*Para $n \geq 5$ la ecuación general algebraica de grado n, no es soluble por radicales.*" desde la teoría de Galois y la topología algebraica con principal enfoque en las superficies de Riemann.

Posteriormente, se realiza la respectiva demostración usando cada concepto para registrar las ideas principales en un cuadro comparativo.

Por último, por medio de ambas demostraciones se analiza como se pueden relacionar los grupos Galois de un polinomio $f(x)$ y monodromía de una función $w(z)$ de manera que se encuentran las condiciones necesarias para la construcción de un isomorfismo entre estos dos.

Estado del arte

El teorema fundamental del algebra afirma que la ecuación de la forma $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$, con a_i un número complejo para todo $i = 0, \ldots, n, n \in \mathbb{N}$ y $a_0 \neq 0$ tiene al menos una solución compleja. Pero, aunque esté garantizada la existencia de tal solución, no para todo n se cumple que sea posible hallar una solución general por radicales. A partir de esto nace el Teorema de Abel-Ruffini, *"La ecuación general algebraica de grado n, no es soluble por radicales cuando* $n \geq 5$*."* Que garantiza la imposibilidad de encontrar una solución general por radicales para todo polinomio de grado mayor o igual que 5.

A continuación se hará la revisión de aquellos textos que hacen explicación de estas demostraciones, teniendo un principal enfoque en aquellos que brindan aporte en la demostración por grupo de Galois y grupo de monodromía, las cuales son de vital interés para la realización de este trabajo.

Documentación sobre la demostración usando grupo de Galois

Son varios los textos que recolectan y realizan la demostración del teorema de Abel-Ruffini siguiendo las construcciones de Galois, dentro de las cuales podemos encontrar los siguientes:

- ***Texto:*** *"Las ecuaciones polinomiales como el origen de la teoría de Galois"* por Villa Salvador (2011)

  Contenido: En este trabajo Villa Salvador (2011) presenta inicialmente una revisión histórica sobre la vida de Galois para continuar con un desarrollo de los conceptos necesarios para intuir la demostración del teorema de Abel-Ruffini que Galois realizó. Villa Salvador (2011) resalta que Galois da una solución sobre cuáles polinomios son solubles por radicales. Posterior muestra algunos otros resultados de la teoría de Galois.

  Relevancia en el trabajo: Aunque este texto presenta un análisis general de como Galois realiza la demostración de el teorema de Abel-Ruffini basado en lo que trabajaron Lagrange, Ruffini y Abel, permite entender la

idea principal para la demostración: El grupo simétrico S_n y su relación con el grupo de Galois de un polinomio.

- ***Texto:*** *"¡Qué bonita es la Teoría de Galois"* por Chamizo Lorente (2005)

  Contenido: Chamizo Lorente (2005) muestra en este texto un amplio desarrollo de la teoría de Galois, partiendo de la teoría de Anillos para terminar en el tema de la resolubilidad por radicales. En lo que respecta al texto muestra de manera didáctica todos los conceptos referentes a esta rama de la matemática, dándose la oportunidad de plantearse y resolverse preguntas sobre su origen y relevancia en la actualidad.

  Relevancia en el trabajo: A diferencia del texto anterior mencionado Chamizo Lorente (2005) hace una muestra detallada de todos los conceptos de teoría de Galois necesarios para la demostración del teorema de Abel-Ruffini. Aunque en el texto se muestren otras construcciones interesantes como la fórmula general para resolver ecuaciones de tercer grado, en el trabajo que se está realizando es de vital importancia solo lo primero mencionado.

Documentación sobre la demostración usando el grupo de monodromía

En esta sección no solo se encuentran los trabajos con enfoque en la superficie de Riemann, sino que también se muestran otros desarrollos que implican trabajar otros tópicos de topología algebraica.

- ***Texto:*** *"Abel's theorem in problems and solutions* por Alekseev (2004)

  Contenido: Este es el primer texto que contiene la demostración de V. I. Arnold. Alekseev (2004) alumno de Arnold escribe en este texto tal demostración, usando conceptos de superficies de Riemann y el grupo monodromía de una función multivaluada solución de un polinomio $P_z(x)$. En este libro el autor presenta la propiedad de monodromía y el grupo de monodromía de una función multivaluada $w(z)$, el cual Alekseev (2004) define como el grupo de permutaciones de hojas de un esquema de la

superficie de Riemann para $w(z)$ o el grupo de permutaciones de los valores de $w(z_0)$ para algún punto no especial z_0.

Relevancia en el trabajo: Este texto presenta de manera completa una de las demostraciones de vital interés en el trabajo que se realiza, además de dar un desarrollo extenso en temas de teoría de Grupos y números complejos, dándole principal relevancia a las superficies de Riemann.

- ***Texto:*** *"Configuraciones, trenzas y el teorema de Abel-Ruffini"* por Jiménez Rolland and Valdespino (sf)

Contenido: En este artículo Jiménez Rolland and Valdespino (sf) analizan la prueba de V.I. Arnold, para hacer énfasis en su relación con los espacios de configuraciones y grupos de trenzas. Trabajando también el concepto de monodromía de funciones algebraicas y los conmutadores de elementos. Así Jiménez Rolland and Valdespino (sf) muestran como los grupos de trenzas inducen permutaciones de las raíces de un polinomio y la manera en que esto da información sobre la solubilidad por radicales de una ecuación polinomial.

Relevancia en el trabajo: Aunque trabaje la misma demostración de Arnold, realiza un análisis desde los grupos de trenzas, agregando también información sobre la monodromía de una función algebraica teniendo en cuenta conceptos de topología algebraica y definiendo también la monodromía de un espacio cubriente.

- ***Texto:*** *"Demostración topológica del teorema de Abel-Ruffini"* por Cabria Zambrano (2017)

Contenido: En este trabajo Cabria Zambrano (2017) además de hacer una introducción útil como curso para la comprensión de topología algebraica, realiza la demostración del teorema de Abel-Ruffini usando lo trabajado por Arnold y conceptos de topología algebraica de distintos textos como el Munkres. Cabria Zambrano (2017) define el grupo monodromía de un espacio cubriente de n-hojas como la imagen del homomorfismo $\phi_\pi : \pi_1(X, x_0) \to Aut(F)$, donde $\pi : X \to Y$ y Y es el espacio cubriente

de n-hojas, $x_0 \in X$ y su fibra F es $F := \{a \in Y | a = \pi^{-1}(x_0)\}$. Con esto posteriormente define que "El grupo monodromía de la función algebraica f es el grupo monodromía del espacio cubriente de n-hojas $\pi : S \to \hat{C} - \{puntos \quad singulares \quad de \quad f\}$" (Cabria Zambrano, 2017) con S una superficie de Riemann. Asociando esta definición de grupo de monodromía de una función algebraica con la presentada en el texto de Alekseev 13 años antes.

Relevancia en el trabajo: En el texto Cabria Zambrano (2017) da un interesante paso en la conexión entre la topología algebraica y la demostración de Arnold, presentando una gran variedad de ejemplos y desarrollos que llevan como objetivo final una de las demostraciones de interés en este trabajo.

Capítulo 1

Marco teórico

Inicialmente es importante enunciar los conceptos básicos que tienen en común la demostración usando grupo de Galois y grupo de monodromía. Uno de los conceptos más relevantes que se enuncian en la siguiente sección es el de grupo simétrico S_n y su solubilidad dependiendo del valor de n.
En las dos últimas secciones se describen los conceptos de teoría de Galois, topología algebraica y superficies de Riemann necesarios para la realización de las demostraciones objetivo del trabajo.

1.1. Conceptos básicos

Las conceptos descritos a continuación están basados en en los textos Charris Castañeda et al. (2013), Judson et al. (2020) , Herstein (1996), Fraleigh (1988), Ottina (2018) y Rotman (1995).

1.1.1. Grupos

Definición 1. Un ***Grupo*** $(G, \cdot)$ es un sistema formado por un conjunto G y una ley de composición interna $(\cdot)$ sobre G, tal que satisface:

i. La ley de composición interna es ***asociativa***, es decir,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)\,, \ \ \forall a, b, c \ \in G$$

ii. Existe un elemento $e \in G$ llamado ***identidad***, tal que para todo $a \in G$:

$$e \cdot a = a \cdot e = a$$

iii. Para todo $a \in G$ existe $a^{-1} \in G$ llamado el elemento ***inverso*** tal que:

$$a \cdot a^{-1} = a^{-1} \cdot a = e$$

Para la construcción de ambas demostraciones también es necesario tener en cuenta los siguientes conceptos.

Definición 2. Un grupo es ***conmutativo*** o ***abeliano*** si para todo $a, b \in (G, \cdot)$, $a \cdot b = b \cdot a$.

Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ de los números enteros, racionales, reales y complejos, respectivamente, junto con la ley de composición de la suma son grupos abelianos.

Ejemplo 1. Sea $K = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, entonces $M_{m\times n}(K)$ el conjunto de todas las matrices de tamaño $m \times n$ sobre K con la suma usual de matrices es un grupo, donde el elemento identidad es la matriz de ceros. Sea $A \in M_{m\times n}(K)$ una matriz cualquiera, entonces $B \in M_{m\times n}(K)$ es su elemento inverso.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \quad B = \begin{bmatrix} -a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & -a_{22} & \cdots & -a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{m1} & -a_{m2} & \cdots & -a_{mn} \end{bmatrix}$$

Además como la suma de matrices es elemento a elemento, y cada uno de estos pertenece a grupos abelianos con la suma, entonces el grupo $M_{m\times n}(K)$ es abeliano.

Por otro lado el conjunto $M_{n\times n}(K)$ de matrices cuadradas con determinante no nulo junto con la multiplicación de matrices es un grupo pero no es abeliano, pues la multiplicación de matrices no es conmutativa.

Teorema 1.1.1. Sea $a \in G$ con G un grupo, entonces

$$H = \{a^n | n \in \mathbb{Z}\}$$

es un subgrupo de G.

Definición 3. Un subgrupo de G es un subgrupo ***cíclico de*** G ***generado por*** a si se define como en el teorema anterior, a este se le denota por $\langle a \rangle$.

Definición 4. Si el grupo $\langle a \rangle = G$, se dice que a ***genera*** a G. Un grupo G es ***cíclico*** si existe algún elemento $a \in G$ que lo genere.

Un ejemplo de grupo cíclico es el grupo de los enteros $(\mathbb{Z}, +)$ el cual está generado por 1.

Definición 5. Sea G un grupo y $H \leq G$ un subgrupo de G. Una ***clase lateral*** con representante $g \in G$, es el conjunto:

$$gH = \{g \cdot h : h \in H\} \quad (\textbf{Clase lateral izquierda})$$

$$Hg = \{h \cdot g : h \in H\} \quad (\textbf{Clase lateral derecha})$$

Definición 6. Sea $(G, \cdot)$ un grupo. Se dice que un subgrupo N de G es un ***subgrupo normal*** de G si para todo $a \in G$ se cumple $a^{-1}Na \leq N$ y se denota entonces como $N \trianglelefteq G$. Además como se cumple para todo $a \in G$ esto es equivalente a que $a^{-1}Na = N$ lo que implica que el subgrupo N es normal si sus clases laterales izquierdas son iguales a las derechas, pues $aN = Na$.

Definición 7. Sea $(G, \cdot)$ un grupo y $N \trianglelefteq G$. Se define el ***grupo factor*** como:

$$G/H = \{Ha : a \in G\} \text{ o bien } G/H = \{aH : a \in G\}$$

Donde G/H es un grupo relativo a la operación $(aH)(bH) = (a \cdot b)H$

Ejemplo 2. Como el grupo $(\mathbb{Z}, +)$ es abeliano, entonces el subgrupo $(3\mathbb{Z}, +)$ es un grupo normal, de manera que $\mathbb{Z}/3\mathbb{Z}$ es el grupo factor

$$\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$$

Observación 1. *En general los subgrupos* $(n\mathbb{Z}, +)$ *con* $n \in \mathbb{Z}$ *son subgrupos normales de* $\mathbb{Z}$.

Definición 8. Una serie subnormal de un grupo $(G, \cdot)$ es una sucesión finita de subgrupos

$$e = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

Como se puede ver H_{i-1} es subgrupo normal de H_i. Si cada H_i es además también subgrupo normal de G a esta serie se le llama una ***serie normal***.

Ejemplo 3. Sea $(\mathbb{Z}, +)$ entonces por la observación 1 las siguientes son series normales:

$$\{0\} \trianglelefteq 8\mathbb{Z} \trianglelefteq 4\mathbb{Z} \trianglelefteq \mathbb{Z}$$

$$\{0\} \trianglelefteq 9\mathbb{Z} \trianglelefteq \mathbb{Z}$$

Definición 9. Sea $\phi : (G, \cdot) \to (G', *)$ donde G, G' son grupos, ϕ es un ***isomorfirmos*** si y solo si para todo $a, b \in G$ se cumple:

i. ϕ es un ***homomorfismo***, es decir, $\phi(a \cdot b) = \phi(a) * \phi(b)$.

ii. ϕ es ***epimorfismo***, es decir, para todo $m \in G'$, existe $a \in G$ tal que $\phi(a) = m$.

iii. ϕ es ***monomorfismo***, es decir, si $\phi(a) = \phi(b)$, implica $a = b$.

Además se dice que G y G' son isomorfos y se denota $G \cong G'$.

Lema 1.1.1. Sea φ un homomorfismo de G en G', entonces

i. $\varphi(e) = e'$ el elemento neutro de G'.

ii. $\varphi(a^{-1}) = (\varphi(a))^{-1}$, $\forall a \in G$.

Definición 10. Si φ es un homomorfismo de G en G', se define el ***Kernel*** de φ

$$Ker(\varphi) = \{a \in G \mid \varphi(a) = e'\}$$

Ejemplo 4. Los grupos $\mathbb{Z}/3\mathbb{Z}$ y $\mathbb{Z}_3$ son isomorfos con el isomorfismo definido como:

$$\begin{aligned} \phi : \mathbb{Z}/3\mathbb{Z} &\longrightarrow \mathbb{Z}_3 \\ a + 3\mathbb{Z} &\longrightarrow a \bmod(3) \end{aligned}$$

Teorema 1.1.2 (Primer teorema de homomorfismos)**.**
Sea φ un homomorfismo de G en G', que es sobreyectivo, con kernel K, entonces $G' \cong G/K$.

Definición 11. Una ***acción*** (izquierda) de un grupo G en un conjunto X es una función $\varphi : G \times X \to X$ tal que para cada $x \in X$ y $g, h \in G$ se cumple:

i. $\varphi(e, x) = x$.

ii. $x \in X$, $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$.

Ejemplo 5. Sea H un subgrupo de G entonces:

$$\begin{aligned} \varphi : H \times G &\longrightarrow G \\ (h, g) &\longrightarrow hgh^{-1} \end{aligned}$$

Es una acción de H en G.

1.1.2. Grupo simétrico S_n

A partir de las definiciones del apartado anterior, se da paso los concepto de grupo simétrico S_n, solubilidad de grupos y en específico la solubilidad del grupo simétrico S_n. En esta sección se toman conceptos del Herstein (1996), Fraleigh (1988) y Rotman (1995).

Definición 12. El ***grupo simétrico*** $A(S)$, es aquel conformado por el conjunto de funciones inyectivas de un conjunto S en sí mismo, bajo la composición de funciones ($\circ$). Cuando $S = \{1, 2, \ldots, n\}$ es un conjunto finito de n elementos, $A(S)$ recibe el nombre de ***grupo simétrico de grado*** n denotado por S_n. Cada elemento de S_n será llamado ***permutación***.

Cada permutación $\sigma \in S_n$ se representa como:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

tal que $\sigma(1) = i_i$, $\sigma(2) = i_2$, ..., $\sigma(n) = i_n$.

Observación 2. *En general los elementos identidad $e \in S_n$ e inverso $\sigma^{-1} \in S_n$*

se representan como:

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & & n \end{pmatrix}$$

Si $\sigma, \tau \in S_n$ entonces la composición $\sigma\tau$ se construye aplicando primero la permutación τ y a ese resultado se le aplica la permutación σ.

Ejemplo 6. Sean $\sigma, \tau \in S_4$, tal que:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

entonces las composiciones $\sigma\tau$ y $\tau\sigma$ son:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

de lo cual es notorio que $\sigma\tau \neq \tau\sigma$.

Observación 3. *Por como se vio en el ejemplo anterior, el grupo simétrico S_n no es un grupo abeliano.*

Definición 13. Sea $i_1, i_2, \ldots, i_k$ con k distintos enteros en $S = \{1, 2, \ldots, n\}$, el simbolo $(i_1\ i_2\ \cdots\ i_k)$ representa la permutación $\sigma \in S_n$ donde $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \ldots, \sigma(i_j) = i_{j+1}$ para $j < k$ y $\sigma(i_k) = i_1$. Para $s \neq i_1, i_2, \ \ldots\ i_k \in S$ se cumple $\sigma(s) = s$. A esto se le llama un ***k-ciclo.***

Ejemplo 7. Sea $\sigma \in S_7$, de manera que $\sigma = (1\ 3\ 5\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 1 & 4 & 6 & 7 \end{pmatrix}$

Definición 14. Cuando $k = 2$, los $k-$ciclos de la forma $(i_1\ i_2)$ se denominan ***transposiciones.***

Definición 15. Un $k-$ciclo y un $m - ciclo$ son ***ciclos disjuntos*** si no tienen elementos i_j enteros en común.

Ejemplo 8. (1 3 5) y (4 6 7 2) son ciclos disjuntos de S_7.

Teorema 1.1.3. Cada permutación de S_n es producto de ciclos.

Teorema 1.1.4. Toda permutación $\sigma \in S_n$ es el producto de transposiciones.

Ejemplo 9. Sea $\sigma \in S_4$ como en el ejemplo 6, es sencillo notar que $\sigma = (1\ 3)(1\ 4)$.

Definición 16. Una permutación $\sigma \in S_n$ es una ***permutación impar*** si σ es el producto de un número impar de transposiciones. Se dirá que σ es una ***permutación par*** en el caso que sea el producto de un número par de transposiciones. Al subgrupo $A_n < S_n$ de todas las permutaciones pares se le denomina ***el grupo alternante de grado*** n.

Definición 17. Un grupo $(G, \cdot)$ es ***soluble*** si tiene una serie subnormal, tal que todos los grupos factor H_{i+1}/H_i son abelianos.

Ejemplo 10. El grupo de los enteros $\mathbb{Z}$ es soluble ya que los grupos factot $9\mathbb{Z}$ y $\mathbb{Z}/9\mathbb{Z}$ de la segunda serie normal del ejemplo 3 son grupos abelianos.

Teorema 1.1.5. Sea G un grupo soluble,entonces:

i. Cualquier subgrupo $H \leq G$ es soluble.

ii. Para cualquier $H \triangleleft G$, el grupo cociente G/N es soluble.

Teorema 1.1.6. Sea $H \triangleleft G$, si H y G/H son solubles, luego G es soluble.

Teorema 1.1.7. Si H y G son grupos solubles, luego $H \times G$ es soluble.

Ejemplo 11. El grupo S_4 es soluble, ya que al tomarse la serie subnormal:

$$\{e\} < \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} < A_4 < S_4$$

los grupos factores son grupos abelianos.

Por otro lado cuando $n \geq 5$ la única serie subnormal de S_n es $\{e\} < A_n < S_n$ pues A_n no tiene subgrupos normales.

Teorema 1.1.8. Para $n \geq 5$ el grupo S_n no es soluble.

Demostración. La prueba resulta directa teniendo en cuenta el ejemplo 11 y que A_n no es un grupo abeliano. □

1.1.3. Anillos

Definición 18. Un ***anillo*** $(R, +, \cdot)$ es un conjunto R junto a dos leyes de composición internas $+, \cdot$ que se denotan como suma y multiplicación definidas en R tales que:

i. $(R, +)$ es un grupo abeliano.

ii. La operación $(\cdot)$ es asociativa.

iii. Para todas $a, b, c \in R$ se cumple:

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

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

Definición 19.

i. Un anillo donde la multiplicación es conmutativa es un ***anillo conmutativo o abeliano***.

ii. Un anillo R con identidad 1 (es decir $1 \cdot x = x \cdot 1 = x, \forall x \in R$) es un ***anillo con unitario***.

iii. Una identidad multiplicativa en un anillo es un ***elemento unitario***.

Ejemplo 12.

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son grupos abelianos.
- $(M_n(K), +, \cdot)$ donde $K = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ es un anillo pero no es abeliano.

Definición 20. Sea R un anillo con unitario. Un elemento u de R es una ***unidad*** de R si tiene un inverso multiplicativo en R. Si todo elemento no-nulo en R es unidad entonces R se dice es un ***anillo con división*** o ***semicampo***.

Definición 21. Un ***Campo*** o ***Cuerpo*** es un anillo conmutativo con división.

Ejemplo 13. Como todo $a \in \mathbb{Z}$ tal que $a \neq 1$ no es una unidad en $(\mathbb{Z}, +, \cdot)$ este no es un campo. Por otro lado $\mathbb{Q}$, $\mathbb{R}$ y C sí son campos.

1.1.4. Polinomios

Los conceptos que se enuncian a continuación hacen referencia al objetivo de estudio principal del teorema de Abel-Ruffini: Los polinomios.

Definición 22. Se define como ***polinomio de grado*** n sobre F a:

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

Con $a_0, a_1, \ldots, a_{n-1}, a_n \in F$. Cada a_i recibe el nombre de coeficiente, además $a_n \neq 0$. El coeficiente a_n se le llama ***coeficiente principal*** del polinomio, mientras que a_0 es el ***coeficiente independiente***. Al grado del polinomio se denotara como $grad(f(x))$.

Definición 23. La ***raíz*** del polinomio $f(x)$ es un elemento $a \in F$ tal que $f(a) = 0$.

Ejemplo 14.

$$f(x) = 2x^2 + 4x - 6$$

Es un polinomio de grado 2 cuyas raíces son $x_1 = -3$ y $x_2 = 1$.

Definición 24. Sean $p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$ y $q(x) = b_0 + b_1x + \cdots + b_{m-1}x^{m-1} + b_mx^m$ dos polinomios sobre un campo F, entonces se define:

i. **Suma**$(+)$**:** $p(x) + q(x) = r(x)$. Donde el grad$(r) \leq$ máx$\{grad(p), grad(q)\}$, además los coeficientes de x^k son de la forma $a_k + b_k$.

ii. **Multiplicación**$(\cdot)$**:** $p(x) \cdot q(x) = r(x)$. Donde para calcularlo se multiplica cada a_kx^k de $p(x)$ por cada b_lx^l del polinomio $q(x)$. Además $r(x)$ el coeficiente principal es a_nb_m, con $grad(r) = n + m$ y es de la forma.

$$r(x) = a_0b_0 + \cdots + (a_nb_{m-1} + a_{n-1}b_m)x^{n+m-1} + a_nb_m$$

Teorema 1.1.9. El conjunto de polinomios con coeficientes en un campo F, y las leyes de composición interna suma $(+)$ y multiplicación $(\cdot)$ como definidos anteriormente, es un anillo.

Definición 25. Al anillo del teorema anterior se le denota $F[x]$ y es llamado ***anillo de polinomios*** con coeficientes en F.

Ejemplo 15. $\mathbb{R}[x]$ es el anillo de los polinomios con coeficiente en los reales.

Definición 26. La ***derivada*** del polinomio:

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in F[x]$$

Se define como el polinomio:

$$D_xf(x) = a_1 + 2a_2x \cdots +(n-1)a_{n-1}x^{n-1} + na_nx^{n-1} \in F[x]$$

Teorema 1.1.10. Sean $f(x)$ y $g(x)$ polinomios sobre un campo F, entonces se cumplen las siguientes reglas de sumas y multiplicación de derivadas

$$D_x(f(x) + g(x)) = D_x(f(x)) + D_x(g(x))$$

$$D_x(f(x)g(x)) = D_x(f(x))g(x) + f(x)D_x(g(x))$$

Ejemplo 16. Sean $f(x) = x^2 + 2x - 5$ y $g(x) = 3x^4 - 2x^2$ entonces:

- Las derivadas de $f(x)$ y $g(x)$ son:

$$D_x(f(x)) = 2x + 2 \text{ y } D_x(g(x)) = 12x^3 - 4x$$

- La derivada de $f(x) + g(x)$ es:

$$D_x(f(x) + g(x)) = D_x(f(x)) + D_x(g(x)) = 12x^3 - 2x + 2$$

- La derivada de $f(x)g(x)$ es:

$$\begin{aligned} D_x(f(x)g(x)) &= D_x(f(x))g(x) + f(x)D_x(g(x)) \\ &= 18x^5 + 30^4 - 68x^3 - 12x^2 + 20x \end{aligned}$$

Definición 27. Sea $f(x) \in F[x]$ un polinomio. Sobre un campo de descomposición para f(x)(El cual se define en la sección 2.3) se tiene la factorización

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

con $\alpha_1, \alpha_2, \ldots, \alpha_k$ elementos distintos del campo de descomposición y n_i un entero ≥ 1 para todo i. Entonces α_i es una ***raíz multiple*** si $n_i > 1$ y es una ***raíz simple***

cuando $n_i = 1$. Además n_i recibe es la ***multiplicidad de la raíz*** α_i.

Definición 28. Un polinomio sobre F es ***separable*** si no tiene raíces multiples. Si un polinomio no es separable se denomina ***inseparable***.

Teorema 1.1.11. Un polinomio $f(x)$ tiene una raíz multiple α si y solo si α es raíz también de $D_x(f(x))$. En particular $f(x)$ es separable si y solo si es primo relativo con su derivada, es decir, $(f(x), D_x(f(x))) = 1$.

Ejemplo 17. El polinomio $x^2 - 2$ es separable sobre $\mathbb{Q}$ pues sus raíces $\pm\sqrt{2}$ son distintas. Mientras que el polinomio $(x^2 - 2)^n$ para cualquier $n \geq 2$ es inseparable, pues tiene raíces multiples $\pm\sqrt{2}$, donde cada una es de multiplicidad 2.

1.2. Conceptos de teoría de Galois

A continuación se hace referencia a los conceptos necesarios de la teoría de Galois para comprender y realizar en el siguiente capítulo la demostración del teorema de Abel-Ruffini por medio de grupo de Galois. Los conceptos fueron tomados de Dummit and Foote (2004) y Aceff and Lluis-Puebla (2016).

1.2.1. Extensiones

Definición 29. Un campo K es una ***extensión*** K/F de un campo F si este es un subcampo de K. El campo F recibe el nombre de ***campo base*** donde $[K : F]$ denota el grado de la extensión K/F.

Si K es una extensión de F es posible ver a K como un espacio vectorial sobre F, donde $[K : F]$ es la dimensión de tal espacio vectorial.

Definición 30. Una extensión es ***finita*** si el valor de $[K : F]$ es finito, y es ***infinita*** en el caso de que $[K : F]$ fuese infinito.

Definición 31. Sea K una extensión de F y $\alpha \in K$. El menor subcampo de K que contiene a α y a F es llamado el ***generado por*** α ***y*** F denotado por $F(\alpha)$. Además si $K = F(\alpha)$ recibe el nombre de ***extensión simple*** y α el de ***elemento primitivo***.

Como ejemplo se ve que el campo de los complejos $\mathbb{C}$ es una extensión simple de $\mathbb{R}$, pues $\mathbb{C} = \mathbb{R}(i)$.

Teorema 1.2.1. Sea $p(x) \in F(x)$ un polinomio irreducible y K una extensión de F que contiene una raíz α de $p(x)$, entonces:

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

Además, sea $K = F[x]/\langle p(x)\rangle$ y $grad(p(x)) = n$, entonces $[K : F] = n$.

Demostración. Se considera el homomorfismo

$$\varphi : F[x] \longrightarrow F(\alpha)$$

definido por $\varphi(f(x)) = f(\alpha)$.

Se demostrará a continuación que $Ker\varphi = \langle p(x)\rangle$.

- $\subseteq$ $\langle p(x)\rangle \subseteq Ker\varphi$ ya que al cumplirse $\varphi(p(x)) = p(\alpha) = 0$, $p(x) \in Ker\varphi$.
- $\supseteq$ Sea $f(x) \in Ker\varphi$, luego $\varphi(f(x)) = f(\alpha) = 0$. Entonces, como α es raíz de $f(x)$ y $p(x)$ irreducible, $p(x)|f(x)$, lo que implica que $f(x) = p(x)g(x)$ y así $f(x) \in \langle p(x)\rangle$. Finalmente se tiene que $\langle p(x)\rangle \supseteq Ker\varphi$

Notese que

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

y

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

con $a_i \in F$ para $i = 0, 1, \ldots, n$. Entonces se verá que $\varphi(F) = F$ y $\varphi(x) = \alpha$.

Ahora se prueba que $Im\varphi = F(\alpha)$.

- $\subseteq$ Esta primera contenencia se obtiene por definición de φ.
- $\supseteq$ Previamente se vió que $\varphi(F) = F \subseteq Im\varphi$ y $\varphi(x) = \alpha \subseteq Im\varphi$, por lo tanto, $Im\varphi \supseteq F(\alpha)$.

Por primer teorema de homomorfismos se tiene finalmente que

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

Para la segunda parte de la demostración se tiene que en general

$$F(\alpha) = \{a_n\alpha^n + a_{n-1}\alpha^{n-1}\cdots + a_1\alpha + a_0 | a_0, \ldots, a_{n-1} \in F\}.$$

Se considera $\mathcal{B} = \{1, \alpha, \ldots, \alpha^{n-1}\}$. Sea $\beta \in K$, tal que $\beta = a_n\alpha^n + a_{n-1}\alpha^{n-1}\cdots + a_1\alpha + a_0$ con $a_0, \ldots, a_{n-1} \in F$. $\mathcal{B}$ es linealmente independiente, pues al considerarse $b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} = 0$ con $b_i \in K$ y $g(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$, entonces $g(\alpha) = 0$ y como α también es raíz de $p(x)$ irreducible $p(x)|g(x)$. Además, ya que $grad(g(x)) < grad(p(x))$ entonces $g(x) = 0$, lo que implica que $b_i = 0$ para $i = 1, \ldots, n-1$, demostrando así que $\mathcal{B}$ es una base para K y como $\mathcal{B}$ tiene n elementos $[K : F] = n$. □

Definición 32. Sea $\alpha \in K$, entonces α es ***algebraico*** sobre F si es una raíz de algún polinomio $f(x) \in F[x]$ diferente de cero. Si α no es algebraico sobre

F se dice que es ***trascendente*** sobre F. La extensión K/F es una ***extensión algebraica*** si todo elemento de K es algebraico sobre F.

Ejemplo 18.

- Sea $K = \mathbb{C}$ y $F = \mathbb{Q}$, donde claramente K es extensión de F. Entonces π y e son números trascendentes. Por otro lado si $F = \mathbb{R}$ estos dos número sí serían algebraicos al ser solución de los polinomios $p(x) = x - \pi$ y $p(x) = x - e$.
- $\sqrt{2}$ es un número algebraico sobre $\mathbb{Q}$ pues es raíz del polinomio $x^2 - 2$.

Proposición 1.2.1. Sea α algebraico sobre F. Existe un único polinomio mónico irreducible $m_{\alpha,F}(x) \in F[x]$ el cuál tiene a α como una raíz.

Demostración. Sea $g(x) \in F[x]$ un polinomio de grado mínimo para el cual α es una raíz. Multiplicando $g(x)$ convenientemente puede suponersele mónico. Supongase $g(x)$ reducible en $F[x]$, luego existen $a(x), b(x) \in F[x]$, con grados menores que el de $g(x)$, tales que $g(x) = a(x)b(x)$. Como $0 = g(\alpha) = a(\alpha)b(\alpha)$, entonces $a(\alpha) = 0$ o $b(\alpha) = 0$, lo cual es una contradicción pues se supuso que $g(x)$ era el polinomio de grado minimo para el cual α es raíz. De manera que $g(x)$ debe ser irreducible.
Para demostrar la unicidad se supondrá que existe $f(x) \in F[x]$ que tiene a α como raíz. Usando el algoritmo de la división de Euclides se ve que existen $q(x), r(x) \in F[x]$ tales que

$$f(x) = g(x)q(x) + r(x) \text{ con } grad(r(x)) < grad(g(x))$$

Al evaluar $f(x)$ en α se llega a $r(\alpha) = 0$, y como $g(x)$ es de grado mínimo, $r(x) = 0$, de manera que $g(x)|f(x)$ implicando que $m_{\alpha,F}(x) = g(x)$. □

Definición 33. El polinomio $m_{\alpha,F}(x)$ es llamado el ***polinomio mínimo*** para α sobre F. El grado de $m_{\alpha,F}(x)$ recibe el nombre del grado de α.

En el caso de que no haya confusión sobre el campo en el cual se encuentra el polinomio $m_{\alpha,F}(x)$, se puede denotar simplemente como $m_\alpha(x)$.

Proposición 1.2.2. Sea α algebraico sobre F, entonces

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

En particular, $[F(\alpha) : F] = grad(m_\alpha(x)) = grad(\alpha)$.

Ejemplo 19. El polinomio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$ es $x^2 - 2$ y por lo tanto $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. De manera similar se tiene que el polinomio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ es $x^3 - 2$, dando que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Definición 34. Una extensión K/F es generada de manera finita si hay elementos $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$ tales que $K = F(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Definición 35. Sean K_1 y K_2 dos subcampos de K, luego el ***campo compuesto*** de K_1 y K_2, denotado por K_1K_2, es el subcampo de K más pequeño que contiene a K_1 y a K_2.

1.2.2. Campos de descomposición y extensiones separables

Definición 36. Si K es una extensión de F, se dice que K es el ***campo de descomposición para un polinomio*** $f(x) \in F[x]$ si este se descompone completamente en factores lineales $(x - \alpha)$ sobre $K[x]$ pero no en los subcampos de K que contienen a F.

Teorema 1.2.2. Sea F un campo cualquiera, si $f(x) \in F[x]$ entonces existe una extensión K de F que es un campo de descomposición para $f(x)$.

Ejemplo 20. El campo de descomposición de $x^2 - 2$ sobre $\mathbb{Q}$ es el campo $\mathbb{Q}(\sqrt{2})$, pues las dos raíces son $\pm\sqrt{2}$ y $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Proposición 1.2.3. El grado de un campo de descomposición de un polinomio de grado n sobre F es a lo más de $n!$.

Demostración. Sea $f(x) \in F[x]$ un polinomio de grado n, al adherir una raíz de $f(x)$ a F se genera una extensión F_1 de grado a lo más n (se cumple la igualdad si y solo si $f(x)$ es irreducible). Ahora se tiene que sobre F_1 el polinomio $f(x)$ tiene al menos un factor lineal, así que alguna otra raíz de $f(x)$ satisface una ecuación de grado que como máximo $n - 1$ sobre F_1. Adhiriendo esta raíz a la extensión F_1 se obtendrá una extensión F_2 de grado a lo más $n - 1$.

Así, si se continúa con este proceso se obtiene la siguiente cadena de extensiones

$$F \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{n-1}$$

Y por multiplicidad de grados

$$[F_{n-1} : F] = [F_{n-1} : F_{n-2}][F_{n-2} : F_{n-3}] \cdots [F_2 : F_1][F_1 : F] = n!$$

Donde claramente F_{n-1} termina siendo el campo de descomposición para $f(x)$.

□

Definición 37. Se considera el campo de descomposición del polinomio $x^n - 1$ sobre $\mathbb{Q}$, las raices para este polinomio son denominadas las ***n-ésimas raíces de la unidad.***

Definición 38. Un generador del grupo ciclico de todas las n-ésimas raíces de la unidad es llamada una ***n-ésima raíz primitiva de la unidad*** a la cual se le denota como ζ_n.

Notese que si ζ_n es una n-ésima raíz primitiva de la unidad, las otras n-ésimas raíces primitivas de la unidad vendrían siendo los elementos ζ_n^a, donde $1 \leq a < n$ y es un entero primo relativo con n, es decir, el máximo común divisor $(a, n) = 1$. Por otro lado, sobre el campo de los complejos $\mathbb{C}$, tomando

$$\zeta_n = e^{2\pi i/n} = cos(\frac{2\pi}{n}) + isen(\frac{2\pi}{n})$$

se puede ver las n-esimas raíces de la unidad como

$$\zeta_n^k = e^{2k\pi i/n} = cos(\frac{2k\pi}{n}) + isen(\frac{2k\pi}{n})$$

.

Definición 39. Sea ζ_n una n-ésima raíz primitiva de la unidad. Entonces el campo $\mathbb{Q}(\zeta_n)$ recibe el nombre del ***campo ciclotomico de las n-ésimas raíces de la unidad***.

Teorema 1.2.3. Sea $\varphi : F \longrightarrow F_1$ un isomorfismo de campos. Además sea $f(x) \in F[x]$ un polinomio y $f_1(x) \in F_1[x]$ el polinomio que se obtiene de aplicar φ a los coeficientes de $f(x)$. Si E es el campo de descomposición de $f(x)$ sobre F

y E_1 el campo de descomposición para $f_1(x)$ sobre F_1, entonces el isomorfismo φ se extiende a un isomorfismo $\sigma : E \longrightarrow E_1$, es decir, σ restringido al campo E es el isomorfismo φ:

$$\begin{array}{ccc} \sigma: & E & \longrightarrow & E_1 \\ & | & & | \\ \varphi: & F & \longrightarrow & F_1 \end{array}$$

Definición 40. Un campo K es ***algebraicamente cerrado*** si todo polinomio con coeficientes en K tiene una raíz en K.

Teorema 1.2.4 (Teorema fundamental del Algebra)**.**
El campo de los complejos $\mathbb{C}$ es algebraicamente cerrado.

Recordando los conceptos de polinomios separables que se trabajaron previamente en la sección 1.1.4, se definirá qué es un campo separable.

Definición 41. Un campo K es ***separable*** sobre F si todo elemento de K es una raíz de un polinomio separable sobre F. Y cuando un campo no es separable se llama ***inseparable***.

1.2.3. Extensiones y grupos de Galois

Los conceptos de isomorfismo, homomorfismo, monomorfismo, epimorfismo y endomorfismo se mantienen igual para anillos, teniendo en cuenta que estos cuentan con dos operaciones. En especial el homomorfismo debe cumplirse con ambas operaciones.

Definición 42. Un isomorfismo σ de un campo K en si mismo, recibe el nombre de ***automorfismo de*** K. Se denota como $Aut(K)$ al conjunto de los automorfismos de K.

Definición 43. Sea K/F una extensión de campos. Al conjunto de todos los automorfismos $\sigma \in Aut(K)$ que fijan al campo F, es decir, $\sigma(\alpha) = \alpha \ \forall \alpha \in F$ se denota como $Aut(K/F)$.

Teorema 1.2.5. El conjunto de todos los automorfismos $Aut(K)$ de un campo K es un grupo bajo la composición de funciones. Además el conjunto de automorfismos $Aut(K/F)$ es un subgrupo.

Si se tiene $\alpha \in K$ algebraico sobre el campo base F. Entonces α satisface

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

con coeficientes en F. Aplicando $\sigma \in Aut(K/F)$ a la ecuación se obtiene

$$\sigma(\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \cdots + \sigma(a_1\alpha) + \sigma(a_0) = \sigma(0) = 0$$

Por como está definido σ se llega finalmente a la ecuación:

$$\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 = 0$$

entonces es claro que $\sigma(\alpha)$ es raíz del mismo polinomio sobre F para el cual α es raíz. Esto permite demostrar la siguiente proposición.

Proposición 1.2.4. Sea K/F una extensión de campos y $\alpha \in K$ algebraico sobre F. Luego para cualquier $\sigma \in Aut(K/F)$, $\sigma(\alpha)$ es una raíz del polinomio mínimo para α sobre F, es decir, $Aut(K/F)$ permuta las raíces de los polinomios irreducibles. Equivalentemente, cualquier polinomio con coeficientes en F que tiene a α como una ráiz, tiene a $\sigma(\alpha)$ como raíz.

Ejemplo 21. Sea $K = \mathbb{Q}(\sqrt{2})$. Sea $\tau \in Aut(\mathbb{Q}(\sqrt{2})) = Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, luego $\tau(\sqrt{2}) = \pm\sqrt{2}$, las cuales son dos raíces del polinomio mínimo de $\sqrt{2}$. Por otro lado como τ fija a $\mathbb{Q}$, se puede determinar τ por lo siguiente

$$\tau(a + b\sqrt{2}) = a \pm b\sqrt{2}, \quad \text{con } a, b \in \mathbb{Q}$$

Así $Aut(\mathbb{Q}(\sqrt{2})) = \{1, \sigma\}$, donde 1 es la función identidad, es decir manda a $\sqrt{2}$ en ella mísma, mientras que $\sigma : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ es el automorfismo que se determina por:

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

Teorema 1.2.6. Sea H un subgrupo del grupo de automorfismos sobre K. Luego la colección F de elementos de K fijados por todos los elementos de H es un subcampo de K.

Definición 44. Si H es subgrupo del grupo de automorfismos de K, el subcampo

de K fijado por todos los elementos de H es llamado el ***campo fijado por*** H.

Ejemplo 22. Se supone $K = \mathbb{Q}(\sqrt{2})$, del ejemplo 21 se sabe que $Aut(\mathbb{Q}(\sqrt{2})) = \{1, \sigma\}$. Entonces el campo fijado por este grupo es aquel que fije los elementos de $\mathbb{Q}$ con

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

pues todos son fijados por la identidad 1. Entonces como

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

es necesario que $b = 0$, implicando que el campo fijado por $Aut(\mathbb{Q}(\sqrt{2}))$ es $\mathbb{Q}$.

Proposición 1.2.5.

i. Si $F_1 \subseteq F_2 \subseteq K$ son dos subcampos de K entonces $Aut(K/F_2) < Aut(K/F_1)$.

ii. Si $H_1 \leq H_2 \leq Aut(K)$ son dos subgrupos de automorfismos con campos fijados F_1 y F_2 respectivamente, luego $F_2 \subseteq F_1$.

Teorema 1.2.7. Sea E un campo de descomposisción sobre F para el polinomio $f(x) \in F[x]$, luego

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

y la igualdad se cumple si $f(x)$ es separable sobre F.

Demostración. Sea E el campo de descomposición sobre un campo F para un polinomio $f(x) \in F[x]$. Por teorema 1.2.3, cualquier isomorfismo $\varphi : F \longrightarrow F_1$, puede ser extendido a un isomorfismo $\sigma : E \longrightarrow E_1$, con E_1 el campo de descomposición para $\varphi(f(x)) = f_1(x) \in F_1[x]$.

Entonces se demuestra por inducción sobre $[E : F]$ el grado de la extensión E que el número de extensiones definidas por los isomorfismos dichos anteriormente es a lo más $[E : F]$, donde la igualdad se tendra cuando $f(x)$ sea separable sobre F.

Para el caso de $[E : F] = 1$ se cumple directamente pues $E = F$, lo que implica $E_1 = F_1$ y $\varphi = \sigma$ y por lo tanto el número de extensiones es 1. Supongase como hipotesis de inducción, que el número de esas extensiones es menor a n, para todo $n < [E : F]$. De manera que si $[E : F] > 1$ se ve que $f(x)$ tiene al menos un factor irreducible $p(x)$ de grado mayor que uno, con un correspondiente factor

irreducible $p_1(x)$ de $f_1(x)$.

Sea α una raiz fija de $p(x)$, si σ es una extensión cualquiera de φ para E, entonces σ restringida al campo $F(\alpha)$ de E es un isomorfismo τ de $F(\alpha)$ en algún subcampo de E_1. Es decir, si

$$\sigma : E \longrightarrow E_1$$

$$\varphi : F \longrightarrow F_1$$

el isomorfismo τ sería

$$\tau = \sigma_{|F(\alpha)} : F(\alpha) \longrightarrow \text{Subcampo de } E_1$$

y por lo tanto estaría determinado por sus acciones sobre α al ser este elemento el que genera $F(\alpha)$ sobre F. Además como $\tau(\alpha) = \beta$ es alguna raíz de $p_1(x)$ se tendría el siguiente diagrama

$$\begin{array}{rcl} \sigma : & E & \longrightarrow & E_1 \\ & | & & | \\ \tau : & F(\alpha) & \longrightarrow & F_1(\beta) \\ & | & & | \\ \varphi : & F & \longrightarrow & F_1 \end{array} \tag{1.2.1}$$

Por otro lado para cada β raíz de $p_1(x)$ existen extensiones τ y σ dando este diagrama. De manera que para saber el número de extensiones σ lo único necesario es contar el número de diagramas como 1.2.1. Además el número de extensiones de φ a un isomorfismo τ será igual al número de las distintas raíces β de $p_1(x)$ y como el grado de $p_1(x)$ es el mismo $grad(p1(x)) = [F(\alpha) : F]$, se verá que el número de extensiones de φ a τ es a lo más $[F(\alpha) : F]$, donde la igualdad se cumple si las raíces de $p(x)$ son distintas.

Como E también es un campo de descomposición para $f(x)$ sobre $F(\alpha)$, E_1 será el campo de descomposición para $f_1(x)$ sobre $F_1(\beta)$ y así $[E : F(\alpha)] < [E : F]$. Aplicando la hipotesis de inducción se tiene que el número de extensiones de τ a σ es $\leq [E : F(\alpha)]$ donde se cumple la igualdad si $f(x)$ tiene distintas raíces.

Ahora, como $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, el número de extensiones de φ a σ es $\leq [E : F]$, con igualdad cuando $f(x)$ y $p(x)$ tienen distintas raíces.

Por último en el caso particular que se tenga $F = F_1$ y φ como el isomorfismo identidad, $f(x) = f_1(x)$ y $E = E_1$, así los isomorfismos que restringen a φ en F terminan perteneciendo a $Aut(E/F)$ al ser automorfismos de E que fijan a F. □

Definición 45. Sea K/F una extensión finita. Luego K es ***Galois*** sobre F y K/F es una ***extensión Galois*** si $|Aut(K/F)| = [K : F]$. Si K/F es Galois, el grupo de automorfismos $Aut(K/F)$ recibe el nombre de ***Grupo de Galois de K/F*** que se denota como $Gal(K/F)$.

Corolario 1.2.8. Si K es el campo de descomposición sobre F de un polinomio separable $f(x)$, luego K/F es Galois.

Demostración. Se obtiene directamente del teorema 1.2.7. □

Ejemplo 23.

- La extensión $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ es Galois, con grupo de Galois $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$ donde el automorfismo σ es el mismo del ejemplo 21.
- La extensión de grado tres $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es Galois, pues su grupo de automorfismos es de orden uno.

1.2.4. Teorema fundamental de la teoría de Galois

Definición 46. Sea σ un homomorfismo inyectivo de un campo K en uno L, este será llamado un ***incrustamiento*** de K en L. En particular σ es un homomorfismo del grupo multiplicativo $K^\times$ en el grupo multiplicativo $L^\times$.

Teorema 1.2.9. Si $\sigma_1, \sigma_2, \ldots, \sigma_n$ son incrustamientos distintos de un campo K sobre L, luego hay independencia lineal como funciones en K. En particular distintos automorfismos de un campo K son linealmente independientes como funciones en K.

Teorema 1.2.10. Sea $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ un subgrupo de automorfismos de un campo K y sea F un campo fijado, entonces:

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

Corolario 1.2.11. Sea K/F una extensión finita, luego

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

Donde la igualdad se cumple si y solo si F es el campo fijado de $Aut(K/F)$. En otras palabras K/F es Galois si y solo si F es el campo fijado del $Aut(K/F)$.

Corolario 1.2.12. Sea G un subgrupo finito de automorfismos de un campo K, y sea F el campo fijado. Todo automorfismo de K fijando a F está contenido en G, es decir, $Aut(K/F) = G$ así que K/F es Galois con grupo de Galois G.

Corolario 1.2.13. Si $G_1 \neq G_2$ son distintos grupos finitos de automorfismos de un campo K, luego sus campos fijados son también distintos.

Teorema 1.2.14. La extensión K/F es Galois si y solo si K es el campo de descomposición de algún polinomio separable sobre F. Además si este es el caso entonces todo polinomio irreducible con coeficientes en F el cual tiene una raíz en K es separable y tiene todas sus raíces en K. En particular se ve que K/F es una extensión separable.

Definición 47. Sea K/F una extensión Galois. Si $\alpha \in K$, entonces a los elementos $\sigma(\alpha)$, para algún $\sigma \in Gal(K/F)$ reciben el nombre de ***conjugados Galois*** de α sobre F. Por otro lado si E es un subcampo de K que contiene a F, el campo $\sigma(E)$ es llamado el ***campo conjugado*** de E sobre F.

De las distintas definiciones y teoremas desarrollados previamente, se pueden caracterizar las extensiones de Galois K/F con las siguientes cuatro definiciones:

- Son campos de descomposición de polinomios separables sobre F.
- Campos donde F es precisamente el conjunto de elementos fijados por $Aut(K/F)$.
- Campos en los cuales se cumple $|Aut(K/F)| = [K : F]$.
- Extensiones finitas, nomales y separables.

Teorema 1.2.15 (Teorema fundamental de la Teoría de Galois)**.**
Sea K/F una extensión de Galois, $G = Gal(K/F)$ y E un subcampo de K que contiene a F, entonces.

i. Existe una biyección $\varphi : E \longrightarrow G$, como se ve en este diagrama:

$$\left\{\begin{array}{cc} & K \\ \text{Subcampo } E & | \\ \text{de } K & E \\ \text{conteniendo a } F & | \\ & F \end{array}\right\} \longleftrightarrow \left\{\begin{array}{cc} & 1 \\ & | \\ \text{Subgrupos } H \text{ de } G & H \\ & | \\ & G \end{array}\right\}$$

dada por la correspondencia

$$\begin{array}{ccc} E & \longrightarrow & \{\text{Elementos de } G \text{ fijando } E\} \\ \{\text{El campo fijado por } H\} & \longleftarrow & H \end{array}$$

que son inversos el uno al otro.

ii. Si E_1, E_2 corresponden a H_1, H_2 respectivamente, entonces $E_1 \subseteq E_2$ si y solo si $H_1 \leq H_2$.

iii. $[K : E] = |H|$ y $[E : F] = |G : H|$ el indice de H en G:

$$\begin{array}{ll} K & \\ \quad | & \} \ |H| \\ E & \\ \quad | & \} \ |G : H| \\ F & \end{array}$$

iv. K/E es siempre Galois, con grupo de Galois $Gal(K/E) = H$:

$$\begin{array}{ll} K & \\ \quad | & \} \ H \\ E & \end{array}$$

v. E es Galois sobre F si y solo si H es un subgrupo normal en G. Si este es el caso, entonces el grupo de Galois es isomorfo al grupo cociente

$$Gal(E/K) \cong G/H$$

más generalmente, aunque H no es necesariamente normal en G los isomorfismos de E (dentro de una clausura algebraica fija de F que contiene a K) que fijan a F son uno a uno, correspondiente con las clases σH de H en G.

vi. Si E_1, E_2 corresponden a 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. La composición de campos $E_1 E_2$ corresponde a la intersección $H_1 \cap H_2$.

Demostración.

i. Dado cualquier subgrupo H de G, por el corolario 1.2.13 se obtiene un único campo fijado $E = K_H$, lo cual demuestra que φ es inyectivo de derecha a izquierda. Ahora, si K es el campo de descomposición para un polinomio separable $f(x) \in F[x]$, se verá a $f(x)$ como un elemento de $E[x]$ para algún E como se definió en la hipotesis. De manera que K es también el campo de descomposición para $f(x)$ sobre E, y por lo tanto K/E es una extensión Galois. Por el corolario 1.2.11 E es el campo fijado de $Aut(K/E) \leq G$, demostrando que todo subcampo de K que contiene a F surge como el campo fijado por algún subgrupo de G. De esta forma se concluye que φ es sobreyectiva de derecha a izquierda y por lo tanto una biyección.

   Por último, se demuestra que estas correspondencias son inversas unas con otras, pues los automorfismos que fijan a E son precisamente aquellos que están en $Aut(K/E)$ por el corolario 1.2.11.

ii. Esta parte se demuestra directamente por la proposición 1.2.5.

iii. Se sigue tomando $E = K_H$ como el campo fijado por H, entonces por el teorema 1.2.10 $[K : E] = |H|$ y $[K : F] = |G|$. Haciendo el cociente se tiene que $[E : F] = |G : H|$.

iv. Acá la demostración sale directamenre del corolario 1.2.12.

v. Supongase $E = K_H$, campo fijado por el subgrupo H. Todo $\sigma \in G$ restringido a E es un incristamiento $\sigma_{|E}$ de E con el subcampo $\sigma(E)$ de K. Sea $\tau : E \longrightarrow \tau(E) \subseteq \overline{F}$ un incrustamiento cualquiera de E que fija a F. Luego $\tau(E) \subseteq K$. Si $\alpha \in E$ tiene un polinomio mínimo $m_\alpha(x)$ sobre F, luego $\tau(\alpha)$ es otra raíz de $m_\alpha(x)$ y K contiene todas estas raíces por el teorema 1.2.14.

K es el campo de descomposición para $f(x)$ sobre E y por lo tanto es también el campo de descomposición para $\tau(f(x))$ sobre $\tau(E)$. Por teorema 1.2.3 en extensión de isomorfismos, demuestra que se puede extender τ a un isomorfismo σ:

$$\begin{array}{ccccc} \sigma: & K & \longrightarrow & K \\ & | & & | \\ \varphi: & E & \longrightarrow & \tau(E) \end{array}$$

Como σ fija a F, todo incrustamiento de E es de la forma $\sigma_{|E}$ para algún $\sigma \in G$.

Dos automorfismos $\sigma, \sigma' \in G$ restringen al mismo incrustamiento de E si y solo si $\sigma^{-1}\sigma'$ es el mapeo identidad en E. Luego como $\sigma^{-1}\sigma' \in H$ por el numeral (iv) los automorfismos de K que fijan a E son los elementos en H. Por lo tanto los distintos incrustamientos de E están en biyección con las clases σH de H en G. Dando en particular

$$|Emb(E/F)| = |G : H| = [E : F]$$

Donde $Emb(E/F)$ denota los inscrustamientos de E que fijan a F. Por lo tanto, $Aut(E/F) \subseteq Emb(E/F)$. Entonces la extensión E/F será Galois si y solo si $|Aut(E/F)| = [E : F]$, lo que se cumple si y solo si cada uno de los incrustamientos de E es un automorfismo de E, es decir, si y solo si $\sigma(E) = E$ para todo $\sigma \in G$.

Si $\sigma \in G$, luego el subgrupo de G que fija al campo $\sigma(E)$ es el grupo $\sigma H \sigma^{-1}$, es decir, $\sigma(E) = K_{\sigma H \sigma^{-1}}$.

Por la naturaleza biyectiva de la correspondencia Galois demostrada en (i), se sabe que dos subcampos de K que contienen a F son iguales si y solo si sus grupos que fijan son iguales en G. Por lo tanto E es Galois sobre F si y solo si H es un subgrupo normal de G.

Ya se han identificado los incrustamientos de E como el conjunto de clases de H en G. Cuando H es normal en G se verán los incrustamientos como automorfismos. En este caso el grupo de clases G/H se identifica como el grupo de automorfismos de la extensión de Galois E/F. Por lo tanto $G/H \cong Gal(E/F)$ cuando H es normal en G.

vi Supongase H_1, H_2 los subgrupos de elementos de G que fijan a los subcampos E_1 y E_2, respectivamente. Cualquier elemento en $H_1 \cap H_2$ fija a E_1 y a E_2, por lo tanto, fija a cada elemento de la compuesta E_1E_2, pues los elementos en este campo son combinacioens lineales de elementos de E_1 y E_2. Por otro lado si un automorfismo σ fija a la compuesta E_1E_2. Luego en particular σ fija a E_1 y a E_2, es decir $\sigma \in H_1, H_2$, de manera que $\sigma \in H_1 \cap H_2$. Esto demuestra que el campo compuesto E_1E_2 corresponde a la intersección $H_1 \cap H_2$, de manera similar la intersección $E_1 \cap E_2$ corresponde al grupo $\langle H_1, H_2 \rangle$ generado por H_1 y H_2.

□

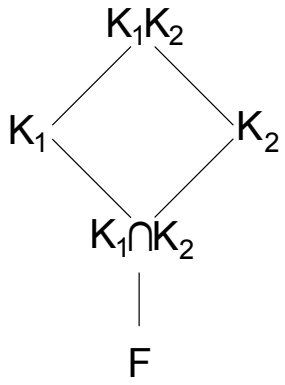
Teorema 1.2.16. Sea K_1 y K_2 extensiones de Galois de un campo F. Luego

i. La intersencción $K_1 \cap K_2$ es Galois sobre F.

ii. La composición K_1K_2 es Galois sobre F. El grupo Galois es isomorfo al subgrupo

$$H = \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

Del producto directo $Gal(K_1/F) \times Gal(K_2/F)$, que consiste de los elementos para los cuales sus restricciones de la intersencción $K_1 \cap K_2$ son iguales.



Teorema 1.2.17. Sea E/K una extensión finita separable cualquiera. Entonces E está contenida en una extensión K, la cual es Galois sobre F y es minimal en el sentido de que en una clausura algebraica fija de F cualquier otra extensión Galois de F que contiene a E, contiene a K.

Definición 48. La extensión Galois K de F que contiene a E como en el teorema previo, es llamada la ***clausura de Galois*** de E sobre F.

1.2.5. Grupo de Galois de polinomios

Definición 49. Si $f(x)$ es un polinomio separable sobre F, luego el ***grupo de Galois de*** $f(x)$ ***sobre*** F es el grupo de Galois del campo de descomposición para $f(x)$ sobre F.

Sea K una extensión Galois de F, luego K es el campo de descomposición para algún polinomio separable $f(x)$ sobre F. Sea $\sigma \in Gal(K/F)$, ya se ha visto que σ grafica una raíz de un factor irreducible de $f(x)$ en una raíz de otro factor irreducible, de manera que σ esta determinado por su acción sobre estas raíces. Etiquetando cada una de las raíces del polinomio $f(x)$ como $\alpha_1, \alpha_2, \ldots, \alpha_n$, entonces cualquier automorfismo $\sigma \in Gal(K/F)$ define una permutación única en los subíndices de las ráices. De manera que se obtiene la inyección $\varphi : Gal(K/F) \longrightarrow S_n$. Así que valdrá la pena analizar los grupos de Galois como subgrupos de grupos simétricos S_n.

Ahora como se ha evidenciado el grado del campo de descomposición es el mismo grado que el orden del grupo de Galois, implicando así que el campo de descomposición para cualquier polinomio de grado n sobre F es a lo más $n!$.

Si la factorización de $f(x)$ en factores irreducibles es $f(x) = f_1(x)\cdots f_k(x)$ donde cada f_i tiene grado n_i, con $i = 1, 2, \ldots, k$, entonces el grupo de Galois permuta las raíces de los factores irreduccibles entre ellos mismos, dando como resultado que $Gal(K/F) \leq S_{n_1} \times \cdots \times S_{n_k}$.

Definición 50. Sean $x_1, x_2, \ldots, x_n$ indeterminantes. Se define como ***funciones simétricas elementales*** $s_1, s_2, \ldots, s_n$ a las funciones

$$
\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n \\
&\vdots \\
s_n &= x_1x_2\cdots x_n
\end{aligned}
$$

es decir, la i-ésima función simétrica s_i de $x_1, x_2, \ldots, x_n$ es la suma de todos los productos de los $x_j's$ tomando i en un momento.

Definición 51. El ***polinomio general de grado*** n es el polinomio

$$(x - x_1)(x - x_2)\cdots(x - x_n)$$

Del cual sus raíces son los indeterminantes $x_1, x_2, \ldots, x_n$.

Teorema 1.2.18. El campo fijado del grupo simétrico S_n, actuando en el campo de las funciones racionales en n variables $F(x_1, x_2, \ldots, x_n)$ es el campo de las funciones racionales en las funciones simétricas elementales $F(s_1, s_2, \ldots, s_n)$.

Demostración. Es facil notar que los coeficientes del polinomio de grado n son las funciones simétricas elementales

$$(x - x_1)(x - x_2)\cdots(x - x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n \quad (1.2.2)$$

Luego para cualquier campo F la extensión $F(x_1, x_2, \ldots, x_n)$ es una extensión de Galois del campo $F(s_1, s_2, \ldots, s_n)$ pues es el campo de descomposición del polinomio general de grado n.

Ahora si $\sigma \in S_n$ es una permutación de $\{1, 2, \ldots, n\}$. Entonces σ actua en las funciones racionales en $F(x_1, x_2, \ldots, x_n)$, permutando los indices de las variables x_i. $S_n \subseteq Aut(F(x_1, x_2, \ldots, x_n))$, pues $\sigma \in S_n$ da un automorfismo de $F(x_1, x_2, \ldots, x_n)$. Además como las funciones simétricas elementales $s_1, s_2, \ldots, s_n$ se mantienen fijas por cualquier permutación de sus subíndices, el subcampo $F(s_1, s_2, \ldots, s_n)$ está contenido en el campo fijado de S_n. Luego por el teorema fundamental de la teoría de Galois (1.2.15), el campo fijado de S_n tiene grado $n!$ en $F(x_1, x_2, \ldots, x_n)$. Pero como $F(x_1, x_2, \ldots, x_n)$ es el campo de descomposición para el polinomio de grado n en la ecuación 1.2.2 sobre $F(s_1, s_2, \ldots, s_n)$, se tiene que

$$[F(x_1, x_2, \ldots, x_n) : F(s_1, s_2, \ldots, s_n)] \leq n$$

De manera que $F(s_1, s_2, \ldots, s_n)$ es el campo fijado de S_n. □

Definición 52. Una función racional $f(x_1, x_2, \ldots, x_n)$ es ***simétrica*** si no es cambiada por alguna permutación de las variables $x_1, x_2, \ldots, x_n$.

Teorema 1.2.19 (Teorema fundamental en funciones simétricas)**.**
Cualquier función simétrica en las variables $x_1, x_2, \ldots, x_n$ es una función racional en las funciones simétricas elementales $s_1, s_2, \ldots, s_n$.

Ejemplo 24.

- El polinomio $(x_1 - x_2)^2$ es simétrico en x_1, x_2, pues

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = s_1^2 - 4s_2$$

un polinomio en las funciones elementales simétricas.

- Como el polinomio $x_1^2 + x_2^2 + x_3^2$ cumple

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 =& (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_1x_3) \\ =& s_1^2 - 2s_2 \end{aligned}$$

es simétrico en x_1, x_2, x_3.

1.2.6. Polinomios solubles por radicales

Definición 53. Una extensión K se dice una ***extensión radical simple*** si se obtiene adhiriendo a un campo F las $n-$ésimas raíces de un elemento $a \in F$. Además $\sqrt[n]{a}$ con $a \in F$ denotará cualquier raíz del polinomio $x^n - a \in F[x]$.

Definición 54. La extensión K/F es ***cíclica*** si es Galois con un grupo de Galois cíclico.

Teorema 1.2.20. Sea F un campo de característica que no divide a n, el cual contiene las n-ésimas raíces de la unidad, luego la extensión $F(\sqrt[n]{a})$ para $a \in F$ es cíclica sobre F de grado que no divide a n.

Teorema 1.2.21. Cualquier extensión cíclica de grado n sobre F de característica que no divida a n, la cual contiene la n-ésima raíz de la unidad, es de la forma $F(\sqrt[n]{a})$ para algún $a \in F$.

Definición 55.

i. Un elemento α el cual es algebraico sobre F puede ser ***expresado por radicales***, o ***soluble en términos de radicales***, si α es un elemento de un campo K el cual puede ser obtenido por una sucesión de extensiónes radicales simples

$$F = K_0 \subset K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_s = K \tag{1.2.3}$$

donde $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ para algún $a_i \in K_i$, $i = 0, 1, \ldots, s$. Donde $\sqrt[n_i]{a_i}$ denota alguna raíz del polinomio $x^{n_i} - a_i$. Tal campo K puede ser llamado una ***extensión de raíces*** de F.

ii. Un polinomio $f(x) \in F[x]$ es ***soluble por radicales*** si todas sus raíces pueden ser solubles en términos de radicales.

Si K y K' son dos extensiones de raíces de un campo F, con subcampos K_i y K'_i, $i = 0, 1, ..., s$ respectivamente. Primero se toma la compuesta de K'_1 con los subcampos K_i, se continúa con la compuesta de estos subcampos con K'_2, y así con los demás K'_i. Luego cada extensión individual sacada de este proceso es una extensión simple de radicales, y por lo tanto la compuesta de los campos KK' es una extensión de raíces.

1.3. Conceptos de topología algebraica y superficies de Riemann

En esta sección se detallan temas de topología algebraica para la comprensión del grupo monodromía y para la posterior demostración del teorema de Abel-Ruffini usando el grupo de monodromía. Los textos en los que se basan los desarrollos y conceptos que se muestran a continuación son Lipschutz (sf), Cabria Zambrano (2017), Munkres (2002) y Alekseev (2004).

1.3.1. Conceptos topológicos

La definición de los conceptos que se muestran a continuación vienen del texto Lipschutz (sf).

Al conjunto X al cual se le define la topología τ recibe el nombre de ***espacio topologico***, y tendra como notación (X, τ) o simplemente X.

Definición 56. La biyección $f : X \longrightarrow Y$ entre dos espacios topologicos X y Y, donde f y f^{-1} son continuas, recibe el nombre de ***homeomorfismo***. A los espacios X y Y se les llama espacios ***homeomorfos***.

Definición 57. Se dice que un espacio topológico X es ***segundo contable*** si existe una base contable para este.

Definición 58. Un espacio topológico X es un ***espacio de Hausdorff***, si dados dos puntos distintos cualesquiera $a, b \in X$, cada uno pertenece a un conjunto abierto, tales que estos conjuntos sean disjuntos, es decir existen G, H conjuntos abiertos tales que:

$$a \in G,\ b\ \in H \quad y \quad G \cap H = \emptyset$$

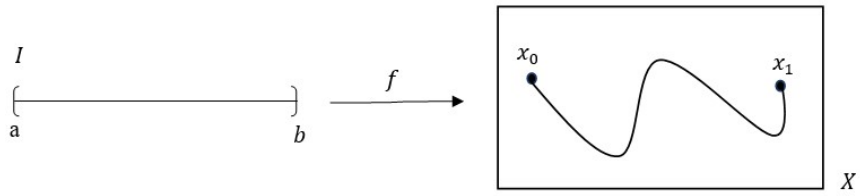
Definición 59. Una ***superficie*** es un espacio de hausdorff, segundo contable en el cual todo punto tiene una vecindad homeomorfa a una bola en $\mathbb{R}^2$.

Definición 60. Sea f una aplicación del conjunto A en el conjunto B, se llama ***función multivaluada*** si a cada $a \in A$ lo manda en más de un elemento del conjunto B.

1.3.2. Monodromía del espacio de recubrimiento

Definición 61. Sea $I = [a, b]$ un intervalo cerrado y x_0, x_1 puntos de un espacio topológico X, un camino es una función continua en $f : I \to X$ con punto inicial $f(a) = x_0$ y punto final $f(b) = x_1$.

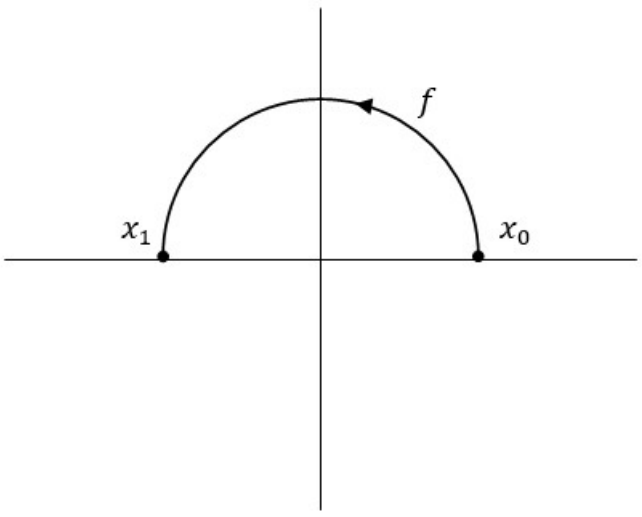
Figura 1.1:
Camino



Ejemplo 25. Sea $I = [0, 1]$ y el espacio topológico $\mathbb{R}^2$, un camino $f : I \to \mathbb{R}^2$ sería

$$f(s) = (cos\pi s, sen\pi s)$$

Figura 1.2:
Camino $f(s) = (cos\pi s, sen\pi s)$



Por conveniencia, de ahora en adelante el intervalo que se usará es $I = [0, 1]$.

Definición 62. Sean f y f_1 aplicaciones continuas del espacio X en el espacio Y, se dice f es ***homotópica*** a f_1 si existe una aplicación continua $F : X \times I \to Y$ tal que $F(x, 0) = f(x)$ y $F(x, 1) = f_1(x)$ Para todo $x \in X$. A F se le llama ***homotopía*** entre f y f_1. Si f es una aplicación constante, se dice que f es ***homotópica nula***.

Definición 63. Sean f y f_1 dos caminos que aplican el intervalo I en X, se denominan ***homotópicos por caminos*** si comparten el mismo punto inicial x_0 y final x_1 y además existe una aplicación continua $F : I \times I \to X$ tal que

$$F(s, 0) = f(s) \;\; y \;\; F(s, 1) = f_1(s)$$

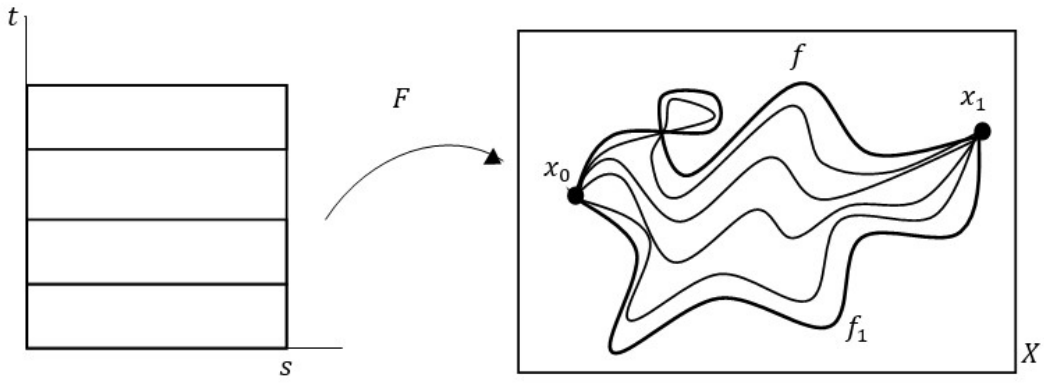
$$F(0, t) = x_0 \;\; y \;\; F(1, t) = x_1$$

Para todo $s, t \in X$. F recibe el nombre ***homotopía de caminos*** entre f y f_1.

En otras palabras, una homotopía entre los caminos f y f_1 puede ser explicada como una función que permite pasar de f a f_1 por medio de caminos que por su definición son funciones continuas.

Ejemplo 26. La figura 1.3 muestra una homotopía F entre los caminos f y f_1.

Figura 1.3:
Homotopía entre caminos

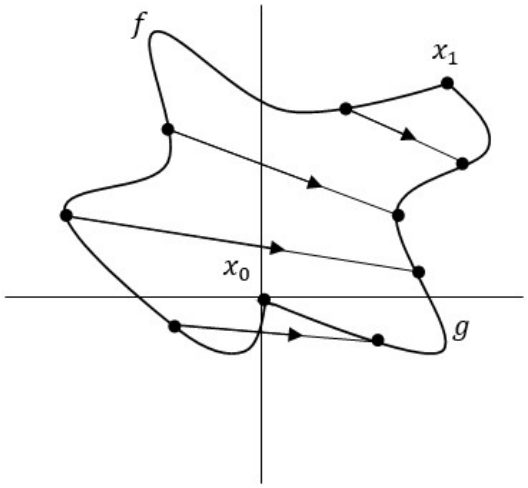


Nota: Adaptado de Topología (2.ªedición, p.368), por J.R. Munkres, 2002.

Ejemplo 27. Tomese f y g dos caminos de I en $\mathbb{R}^2$, que van de x_0 en x_1 como se ve en la figura 1.4, notese como f y g son homotópicos mediante la aplicación:

$$F(s, t) = (1 - t)f(s) + tg(s)$$

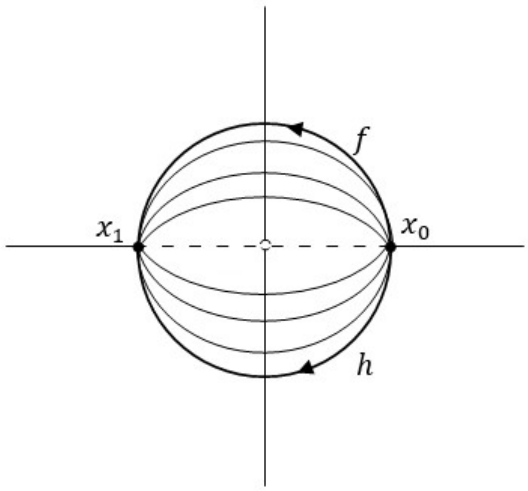
Figura 1.4:
Homotopía $F(s,t) = (1-t)f(s) + tg(s)$



Nota: Adaptado de Topología (2.ªedición, p.369), por J.R. Munkres, 2002.

Ejemplo 28. Sea f como en el ejemplo 25 y $h(s) = (cos\pi s, -sen\pi s)$ dos caminos en el espacio topológico $X = \mathbb{R}^2 - \{0\}$, f y h no son homotópicos por caminos, como se puede notar en la figura 1.5 no hay manera de pasar de una a la otra por medio de caminos.

Figura 1.5:
Caminos no homotópicos



Definición 64. Sea $f : Y \to X$ una aplicación continua y sobreyectiva entre espacios topológicos. Se dice que es una ***aplicación cubriente*** si todo $x \in X$ tiene una vecindad abierta U_x tal que $f^{-1}(U_x)$ cumple ser unión de abiertos disjuntos donde cada uno es homeomorfo a U_x, a este último conjunto se denomina

vecindad regular de X. El espacio topológico Y se le llama un espacio cubriente de X si existe f.

Ejemplo 29. Sea el circulo $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$. La función exponencial $\varphi : \mathbb{R} \to \mathbb{S}^1$ definida por $\varphi(t) = e^{2\pi it}$ es una aplicación cubriente.

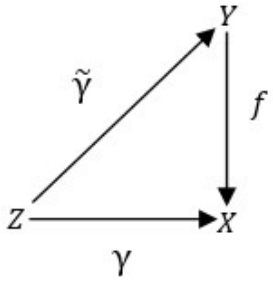
Lema 1.3.1. La función exponencial $\varphi : \mathbb{R} \to \mathbb{S}^1$ definida en el ejemplo anterior es una función abierta.

Demostración. Sea $U \subset \mathbb{R}$ un abierto y $F = \mathbb{S}^1 - \varphi(U)$. Observese que $\varphi^{-1}(\varphi(U)) = \bigcup_{n\in\mathbb{Z}}(U + \{n\})$ es abierto, por lo tanto $\varphi^{-1}(F)$ es cerrado. Ahora para cada $t \in \mathbb{R}$ existe $t' \in I$ tal que $\varphi(t) = \varphi(t')$. Luego $F = \varphi(\varphi^{-1}(F) \cap I)$ es la imagen continua de un compacto, por lo tanto es cerrado, de manera que U es abierto. □

Observación 4. Con el resultado anterior se deduce que la restricción de la función exponencial φ a cualquier intervalo $(t, t + 1)$, es un homeomorfismo sobre $\mathbb{S}^1 - \{\varphi(t)\}$.

Definición 65. Sea $f : Y \to X$ una aplicación cubriente. Si $\gamma : Z \to X$ es una aplicación continua, un ***levantamiento*** de γ es una aplicación continua $\widetilde{\gamma} : Z \to Y$ tal que $f \circ \widetilde{\gamma} = \gamma$. Es decir, el siguiente diagrama conmuta:

Figura 1.6:
Diagrama levantamiento



Nota: Adaptado de "Demostración topológica del teorema de Abel-Ruffini", por M. L. Cabria Zambrano, 2017.

Lema 1.3.2. Sea $\varphi : \mathbb{R} \to \mathbb{S}^1$ la función exponencial. Para todo camino $\gamma : I \to \mathbb{S}^1$, con $\gamma(0) = \varphi(0) = 1$, existe un único levantamiento de γ tal que $\widetilde{\gamma}(0) = 0$.

Lema 1.3.3 (*Lema de levantamiento de homotopías*)**.**
Sean $\gamma_1, \gamma_2 : I \to \mathbb{S}^1$ dos caminos homotópicos vía $F : I \times I \to \mathbb{S}^1$ tales que

$\gamma_1(0) = \gamma_2(0) = 1$, entonces existe un único levantamiento $\widetilde{F}$ de F tal que los levantamientos $\widetilde{\gamma_1}$ y $\widetilde{\gamma_2}$ de γ_1 y γ_2 respectivamente son homotópicos vía $\widetilde{F}$.

Corolario 1.3.1. Si $\gamma_1, \gamma_2 : I \to \mathbb{S}^1$ son homotópicos por caminos, entonces sus respectivos levantamientos $\widetilde{\gamma_1}$ y $\widetilde{\gamma_2}$ son homotópicos por caminos. En particular $\widetilde{\gamma_1}(1) = \widetilde{\gamma_2}(1)$.

Definición 66. Sean f y g dos caminos en X, tales que f va de x_0 a x_1 y g va de x_1 a x_2, la operación $(\cdot)$ que define el producto $f \cdot g$ es el camino h dado por las ecuaciones

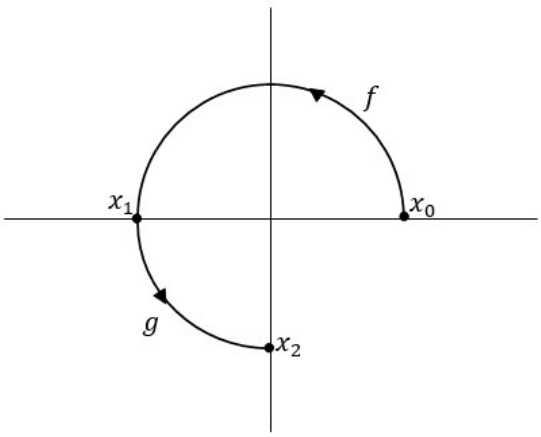
$$h(s) = \begin{cases} f(2s) & s \in [0, \frac{1}{2}] \\ g(2s-1) & s \in [\frac{1}{2}, 1] \end{cases}$$

Ejemplo 30. Tomese $f(s) = (cos\pi s, sen\pi s)$ y $g(s) = (-cos\frac{\pi}{2}s, -sen\frac{\pi}{2}s)$ dos caminos en $\mathbb{R}^2$, de donde $h = f \cdot g$ se define por las ecuaciones

$$h(s) = \begin{cases} (cos2\pi s, sen2\pi s) & s \in [0, \frac{1}{2}] \\ (-cos\frac{\pi}{2}(2s-1), -sen\frac{\pi}{2}(2s-1)) & s \in \left[\frac{1}{2}, 1\right] \end{cases}$$

y gráficamente tiene la forma como se muestra en la figura 1.7.

Figura 1.7:
Producto de los caminos $f(s) = (cos\pi s, sen\pi s)$ y $g(s) = (-cos\frac{\pi}{2}s, -sen\frac{\pi}{2}s)$



Definición 67. Sea X un espacio topológico y $x_0 \in X$. Un camino en X que comienza y termina en el punto x_0 se llama ***lazo basado en*** x_0. Al conjunto de las clases de homotopía de caminos asociadas a los lazos basados en x_0 con la operación $(\cdot)$ se denomina ***grupo fundamental*** de X relativo al punto base x_0. Se denota como $\pi_1(X, x_0)$.

Definición 68. Si $f : Y \to X$ es una aplicación cubriente, entonces al conjunto $f^{-1}(x)$ se le llama ***fibra***, siendo su cardinalidad denominada como ***número de hojas*** del espacio cubriente.

Si $\pi : Y \to X$ es una aplicación cubriente con Y un espacio cubriente de n-hojas, un punto $x_0 \in X$ y su fibra que consta de n elementos, $F := \{a \in Y | a = \pi^{-1}(x_0)\}$. Se toma el grupo fundamental de X y se define una acción de π en la fibra F de x_0. Sea $\gamma : I \to X$ un lazo basado en x_0,se toma $a \in F$. Por el lema 1.3.3 f se levanta a un único camino $\widetilde{\gamma}_a : I \to Y$ que inicia en $\widetilde{\gamma}_a(0) = a$. Como Y es un recubrimiento de n-hojas y $\pi(\widetilde{\gamma}_a(1)) = \gamma(1)$, la preimagen $\pi^{-1}(\gamma(1))$. Aunque no necesariamente coinciden con a. Significa que cada lazo en x induce una permutación de los elementos de F y habrá una cantidad finita de las mismas, pues la cantidad de hojas del espacio de recubrimiento es finita.

Definición 69. Al homomorfismo $\varphi_\pi : \pi_1(X, x_0) \to Aut(F)$ correspondiente a la acción anteriormente mencionada, se llamará ***monodromia del espacio de recubrimiento*** y la imagen de este homomorfismo es el ***grupo de monodromia*** de π.

1.3.3. Superficies de Riemann

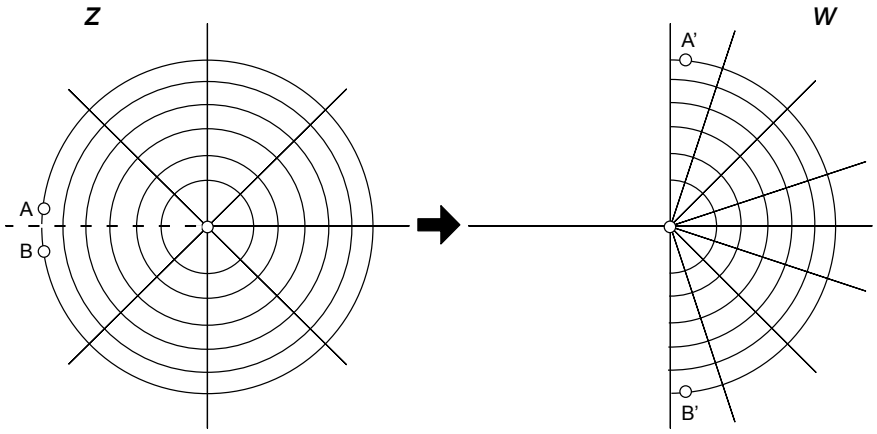
En esta parte iniciará haciendo un desarrollo para la superficie de Riemann de la función multivaluada $w = \sqrt{z}$, ya que permite desarrollar con mas claridad el tema.

La función multivaluada $w = \sqrt{z}$ toma un único valor $w = 0$ cuando $z = 0$, pero cuando $z \neq 0$ la función w toma dos valores distintos, siendo w_0 uno de los valores para $\sqrt{z_0}$ y el otro valor viene dado por $w_1 = -w_0$.

Cortando el plano Z por el lado negativo del eje real, desde el 0 hasta $-\infty$. Para cada z que no este en el corte hecho se toma el valor $w = \sqrt{z}$ que esté en la mitad derecha del plano W. De esta manera se obtiene una función continua univaluada (es decir, cada valor del dominio lo manda en un único valor en el rango) de todo el plano Z menos el corte, en la mitad derecha del plano W. A esta función se denotará como ${}_1\sqrt{z}$.

En la figura 1.8 se logra ver gráficamente el procedimiento descrito para la función ${}_1\sqrt{z}$, donde $A' = \sqrt{A}$ y $B' = \sqrt{B}$.

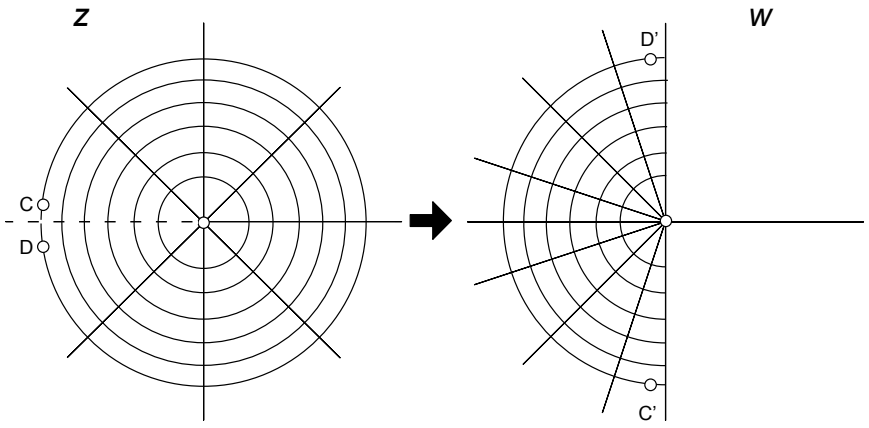
Figura 1.8:
Función univaluada ${}_1\sqrt{z}$



Nota: Adaptado de Abel's Theorem in Problems and Solutions (p.76), V. B. Alekseev, 2004.

Ahora, se nota como ${}_2\sqrt{z}$ es la función que manda a todos los z fuera del corte en el valor $w = -\sqrt{z}$ que están en la mitad izquierda del plano W. En este caso resulta una función univaluada sobre todo el plano Z menos el corte en la mitad izquierda del plano W, donde ${}_2\sqrt{z} = -{}_1\sqrt{z}$, como se muestra la figura 1.9. De esta manera se ve que $C' = -\sqrt{C}$ y $D' = -\sqrt{D}$.

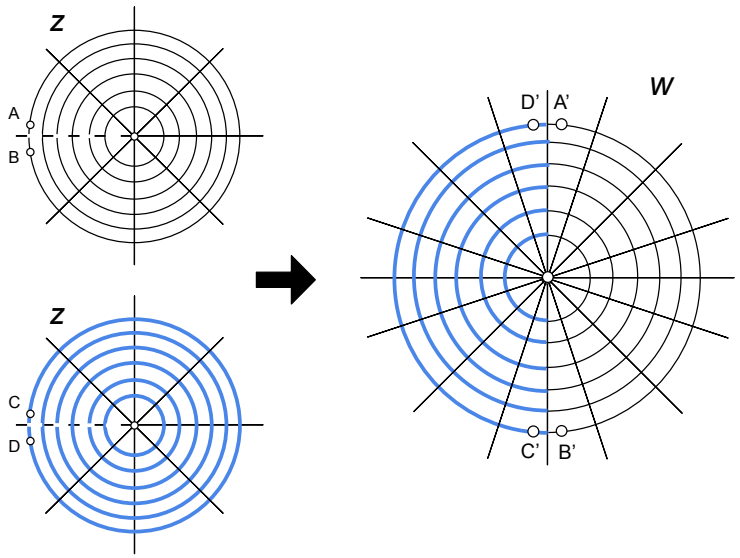
Figura 1.9:
Función univaluada ${}_2\sqrt{z}$



Nota: Adaptado de Abel's Theorem in Problems and Solutions (p.76), V. B. Alekseev, 2004.

A las funciones ${}_1\sqrt{z}$ y ${}_2\sqrt{z}$ definidas como en el ejemplo anterior serán llamadas ***las ramas continuas univaluadas*** de la función $w = \sqrt{z}$.

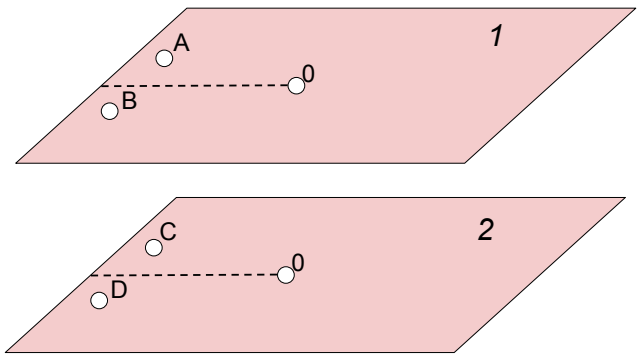
Figura 1.10:
Ramas continuas univaluadas de la función $w = \sqrt{z}$



Nota: Adaptado de "Demostración topológica del teorema de Abel-Ruffini", por M. L. Cabria Zambrano, 2017.

Tómese dos copias del plano Z, a las cuales se les llamar ***hojas*** y se corta cada una alrededor del lado negativo del eje real, es decir de 0 a $-\infty$, como se muestra en la figura 1.11.

Figura 1.11:
Hojas de las ramas continuas univaluadas de la función $w = \sqrt{z}$



Nota: Adaptado de Abel's Theorem in Problems and Solutions (p.77), V. B. Alekseev, 2004.

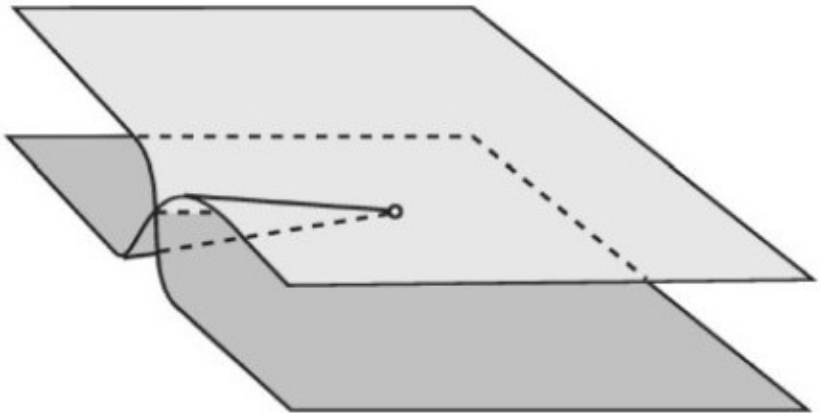
Ahora se asigna cada función ${}_1\sqrt{z}$ y ${}_2\sqrt{z}$ en una hoja cada una. De manera que estas funciones se verán como una única función univaluada, definida en una superficie compleja que consiste de dos hojas. Lo que sigue es encontrar el modo

para que esa única función univaluada sea continua.

Si un punto z se mueve continuamente dentro de la hoja para ${}_1\sqrt{z}$ o la hoja para ${}_2\sqrt{z}$ sin cruzar el corte, la función univaluada definida anteriormente varia continuamente. El problema surge cuando el punto z que se mueve, por ejemplo, en la hoja de ${}_1\sqrt{z}$, cruza el corte, pues en ese caso se perdería la continuidad.

Para resolver este problema la idea es conectar las hojas por medio de la unión entre la parte superior del corte de la primera hoja con la parte inferior del corte de la segunda hoja, y así mismo unir la parte inferior del corte de la primera hoja con la parte superior del corte de la segunda hoja. Además se añade entre ellas el eje real negativo que se corta desde el punto 0 hasta $-\infty$. Haciendo que en la primera unión para los puntos z que están en esta mitad del eje se eligen los valores de $w = \sqrt{z}$ que están en el eje positivo de los imaginarios. Mientras que en la segunda unión se escogen los valores de $w = \sqrt{z}$ que están en el eje negativo de los imaginarios.

Figura 1.12:
Superficie de Riemann para la función $w(z) = \sqrt{z}$.



Nota: Tomado de Abel's Theorem in Problems and Solutions (p.78), V. B. Alekseev, 2004.

Finalmente se logra transformar la función 2-valuada $w = \sqrt{z}$ en otra función que es univaluada y continua en una nueva superficie, que es la descrita por la unión anterior. A esta superficie se le llamará ***Superficie de Riemann de la función*** $w = \sqrt{z}$ y es como la que se muestra en la figura 1.12.

De lo construido anteriormente se definen distintos conceptos de manera general para cualquier función multivaluada $w(z)$.

Definición 70. Los distintos valores que puede tomar una función multivaluada, recibirán el nombre de ***ramas***. Estas ramas son funciones continuas univaluadas en sus respectivas copias de $\mathbb{C}$, las cuales reciben por nombre ***hojas***.

Luego para la construcción de una superficie de Riemann de una función $w(z)$ cualquiera, se separarán las ramas continuas univaluadas de la función $w(z)$ sin incluir los puntos de z que pertenezcan al corte que se haya hecho. Después se deben unir las ramas obtenidas, escogiendo los valores en los cortes de tal manera que se obtenga una función continua univaluada en toda la superficie. Siendo esta superficie la ***superficie de Riemann de una función*** $w(z)$.

Definición 71. Los puntos en los cuales una función multivaluada $w(z)$ toma un único valor se llaman ***puntos singulares***.

Definición 72. Sea S una superficie definida por la unión de las hojas de una función multivaluada $w(z)$ y $s \in S$ un punto en esta superficie. Si es posible cambiar de hoja al dar una vuelta alrededor de s entonces se dice que s es un ***punto de ramificación de la función multivaluada***.

Las definiciones de la curva inversa y la multiplicación entre curvas son similares aquellas trabajadas en la sección de caminos.

Definición 73. Sea C una curva continua con una parametrización $z(t)$. A la curva geométricamente identica a C pero con una orientación en dirección contraria se le asignara como C^{-1}, que está parametrizada por $z_1(t) = z(1-t)$.

Definición 74. Sea C_1 una curva continua que inicia en z_0 y termina en z_1. Si C_2 es una curva continua que inica en z_1 y termina en z_2. C_1C_2 es la curva obtenida de unir la curva C_1 con la curva C_2 a partir del punto en comun z_1, de manera que la curva continua C_1C_2 inica en el punto z_0 y termina en el punto z_2.

Sea z_0 un punto central, el cual tiene como una de sus imagenes $w_0 = w(z_0)$. Supongase una curva continua C que inicia en el punto z_0 y termina en un punto central z_1. Moviéndose a través de la curva C se tomará para cada z en la curva el valor $w(z)$, de manera que estos varíen continuamente mientras se hace un desplazamiento a través de C iniciando con el valor w_0. Así al llegar al punto final z_1 el valor $w_1 = w(z_1)$ va a estar definido completamente. Se dirá entonces que w_1 es el valor de $w(z_1)$ ***definido de manera continua sobre la curva*** C bajo la condición de $w_0 = w(z_0)$. Si los valores de la función $w(z)$ definidos en todos los

puntos z escogidos sobre la curva, están representados en plano W, entonces se tendrá una curva continua que inicia en w_0 y termina en w_1. Esta curva se define como una de las ***imagenes continuas*** de la curva C bajo la función $w = w(z)$.

Definición 75. Aquellos puntos donde se pierde la unicidad de las imagenes continuas de la curva, pero que no son puntos de ramificación, reciben el nombre de ***puntos de no unicidad***.

Definición 76. Los ***puntos especiales*** de la superficie de Riemann, corresponden a la unión de los puntos de no unicidad y puntos de ramificación.

Ejemplo 31. Se encuentran los puntos especiales de la función multivaluada $w(z)$ que expresa las raíces de la ecuación

$$3w^5 - 25w^3 + 60w - z = 0 \tag{1.3.1}$$

Primero, ver que si w_0 es una raíz multiple de la ecuación $P_z(w) = 0$, entonces w_0 sera raíz de la derivada $P'_z(w) = 0$ del polinomio $P_z(w)$ con respecto a w. Con esto se encontrará que

$$D_w P_z(w) = 15w^4 - 74^2 + 60 = 15(w^4 - 5w^2 + 4) = 15(w-2)(w-1)(w+1)(w+2)$$

Y como $D_w P_z(w) = 0$ tiene cuatro raíces de multiplicidad uno, $w_0 = -2, 2, -1, 1$ los cuáles van a ser los únicos valores con múltiples raíces de la ecuación $P_z = 0$ de multiplicidad dos. Al reemplazar estos valores en la ecuación 1.3.1, se obtiene que estos valores son las raíces de multiplicidad dos cuando z toma los valores de $-16, 16, -38, 38$, respectivamente. Por lo tanto para estos valores de z se tienen cuatro raices distintas, pues una es de multiplicidad dos y cualquier z diferente de $\pm 16, \pm 38$ tiene cinco raíces distintas.

A continuación se observa como los valores anteriores de z son puntos de ramificación.

Sea z_0 un punto arbitrario diferente a $z = \pm 16, \pm 38$.

- Por como se definió z_0 y por lo visto anteriormente z_0, tiene cinco imagenes distintas, se llamaran w_1, w_2, w_3, w_4, w_5.
- z_0 ***no es un punto de no unicidad***. Pues si una curva continua C inicia

en el punto z_0, para cada w_i, con $i = 1, 2, 3, 4, 5$, al menos una imagen continua de la curva C inicia en w_i. Pero si dos imagenes continuas de la curva C iniciaran en algún w_i, por ejemplo w_1, la curva C que inicia en z_0 tendría seis imagenes continuas distintas y en el punto z_0 se tendrían seis raices distintas, lo cual no puede ser pues una ecuación de grado cinco no puede tener más de cinco raíces.

- z_0 ***no es un punto de ramificación.*** Sean D_i con $i = 1, 2, 3, 4, 5$, en el plano W con centros w_i respectivamente y radio r lo suficientemente pequeño para que los discos sean disjuntos. Entonces existe D_0 en el plano Z con centro z_0, tal que para cada z_0' su imagen cae en un único disco D_i. Sea C una curva continua que está completamente dentro del disco D_0, por como esta definido D_0, cada punto en la curva C tiene una imagen en alguno de los discos D_i, pero al ser estos disjuntos, no hay posibilidad de que la imagen de C sea una curva continua que salte de un disco a otro. De manera que la imagen de C debe ser una curva que esté completamente dentro de algún disco D_i.

  Por otro lado si C es una curva cerrada con punto inical z_0', su imagen C' bajo la función $w(z)$ debe ser una curva cerrada que inicia y termina en un único punto imagen del punto z_0'. Por lo tanto no hay forma de pasar de una hoja a otra dando giros al rededor del punto z_0.

Ahora se toma el punto $z_0 = 16$ (esto sucederá de igual forma con alguno de los otros z encontrados inicialmente) es importante recordar que z_0 tiene una raíz w_1 de multiplicidad dos, y otras tres raices w_2, w_3, w_4 que son simples. Supongase un punto z_0' cercano a z_0, entonces cerca al punto w_1 hay dos imagenes del punto z_0' bajo la función $w(z)$, y cerca a los puntos w_i con $i = 2, 3, 4$ hay una sola imagen de z_0'. Sea C una curva circular, con centro en z_0 y que inicia en el punto z_0'. De manera similar al desarrollo para demostrar cuales no son puntos de ramificación, se vera que si la imagen continua de C inicia en los puntos w_i con $i = 2, 3, 4$ esta será un lazo basado en w_1, w_2 o w_3 respectivamente. Pero si la imagen de C inicia en un punto cercano a w_1, esta será una curva C_1 que inicia en una imagen de z_0' y termina en la otra imagen. Esto permite ver como sería el paso entre las distintas hojas de la superficie, donde en el punto z_0 solo dos hojas pueden conectarse, y no hay paso entre las otras tres hojas.

Por las especificaciones anteriores, como cada punto distinto a $z = \pm 16, \pm 38$ no es un punto especial, y además en los puntos $z = \pm 16, \pm 38$ es posible unir unicamente dos hojas, se concluye que los puntos z terminan siendo los únicos puntos de ramificación de la función $w(z)$.

Definición 77. Supongase dos curvas continuas C_1 y C_2, que unen un punto z_0 con un punto diferente z_1 y no pasan por puntos especiales de la función $w(z)$. Además supongase que la curva C_1 puede transformarse variando continuamente en la curva C_2, de tal manera que ninguna de las curvas durante la deformación pase a través de puntos de ramificación y que los puntos extremos de las curvas están fijos. Por lo tanto el valor $w(z_1)$ esta definido de manera única por la continuidad a lo largo de la curva C_1 y C_2.

Esta posibilidad de deformar una curva en otra cumpliendo las condiciones anteriormente descritas se define como ***propiedad de monodromía***.

Teorema 1.3.2. Si una función multivaluada posee la propiedad de monodromía, entonces es posible la construcción de su superficie de Riemann.

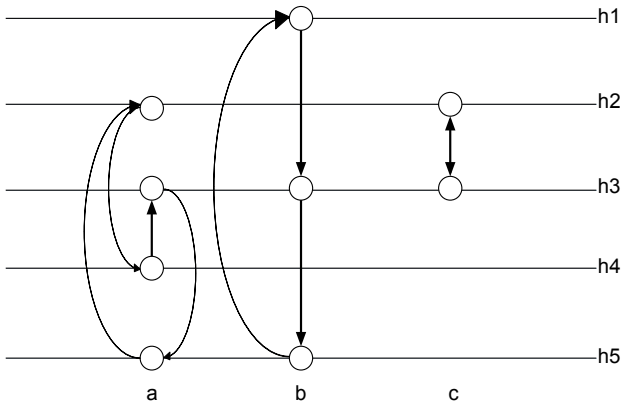
Ejemplo 32. La función multivaluada $w(z)$ que expresa las raíces de la ecuación 1.3.1 en términos del parámetro z cumple la propiedad de monodromía.

Sea z_0 un número complejo arbitrario y w_0 una de las raíces de la ecuación 1.3.1 para $z = z_0$. Considerese un disco de radio r arbitrariamente pequeño, con su centro en w_0, así que existe un número real $\rho > 0$ tal que si $|z_0' - z_0| < \rho$ entonces en el disco considerado existe al menos una raíz de la ecuación para $z = z_0'$ también.

Supongase que la función $w(z)$ expresa las raíces de la ecuación 1.3.1 en el parámetro z y w_0 uno de los valores de $w(z_0)$. De lo dicho anteriormente se sigue que si z cambia de manera continua alrededor de una curva, iniciando en el punto z_0, entonces se puede elegir uno de los valores de $w(z)$ de tal manera que el punto w también se mueva continuamente al rededor de la curva, iniciando en el punto w_0. En otras palabras la función $w(z)$ puede ser definidad por continuidad alrededor de una curva arbitraria C. Así, si la curva C evade los puntos especiales de la función $w(z)$, la función esta definida únicamente por la continuidad de la curva C. Por lo tanto la función $w(z)$ siendo una función algebraica, cumple con la propiedad de monodromía, y es posible construir la superficie de Riemann de la función $w(z)$, la cual cuenta con cinco hojas.

Para las superficies de Riemann es posible la creación de esquemas que teniendo en cuenta los conceptos definidos en esta sección, permiten dar una descripción de la superficie. Estos esquemas son de gran importancia para la definición del grupo monodromía de funciones multivaluadas que se verá en la siguiente sección.

Figura 1.13:
Esquema general de la superficie de Riemann



En la figura 1.13 se puede ver como sería un esquema de la superficie de Riemann para una función multivaluada $w(z)$, donde $h1, h2, h3, h4, h5$ son las distintas hojas respectivas a cada rama univaluada que tiene la función multivaluada y a, b, c son los puntos de ramificación de la función, con las respectivas flechas señalando como se puede pasar de una hoja a otra a través de curvas alrededor de estos puntos.

Teorema 1.3.3. Sean f(z) y g(z) dos funciones multivaluadas, la construcción de los esquemas de las superficies de Riemann de las funciones $h(z) = f(z) \pm g(z)$, $h(z) = f(z) \cdot g(z)$, $h(z) = f(z)/g(z)$ a partir de los esquemas de las superficies de Riemann de $f(z)$ y $g(z)$, con los mismos cortes, tiene los siguientes pasos:

I. Hacer corresponder cada pareja de ramas univaluadas, $f_i(z)$ y $g_j(z)$ en una hoja en la cual la rama $h_{i,j}(z)$ igual a $h_{i,j}(z) = f_i(z) \pm g_j(z)$, $h_{i,j}(z) = f_i(z) \cdot g_j(z)$ o $h_{i,j}(z) = f_i(z)/g_j(z)$ respectivamente, este definida.

II. Si girar al rededor de un punto z_0 hace que se mueva de una hoja $f_{i1}(z)$ a una hoja $f_{i2}(z)$, y de la hoja $g_{j1}(z)$ a la hoja $g_{j2}(z)$, entonces haciendo el mismo giro en la función $h(z)$ es posible moverse de la hoja $h_{i_1,j_1}(z)$ a la hoja $h_{i_2,j_2}(z)$.

III. Identidicar en las hojas en las cuales las ramas $h_{i,j}(z)$ coincidan.

Teorema 1.3.4. Para la construcción del esquema de la superficie de Riemann para la función $h(z) = [f(z)]^n$ a partir del esquema de la superficie de Riemann de la función multivaluada $f(z)$ definido en los mismos cortes, basta con hacer los siguientes pasos:

I. En el esquema para la superficie de Riemann de la función $f(z)$, en lugar de considerar las ramas $f_i(z)$, se considerarán las ramas $h_i(z) = [f_i(z)]^n$.

II. Identificar las hojas en las cuales las ramas $h_i(z)$ coincidan.

Teorema 1.3.5. Para construir el esquema de la superficie de Riemann para la función $h(z) = \sqrt[n]{f(z)}$ a partir del esquema de la superficie de Riemann de la función multivaluada $f(z)$ definido en los mismos cortes, es suficiente seguir los siguientes pasos:

I. Se reemplaza cada hoja del esquema de la superfice de Riemann de la función $f(z)$ por un paquete de n hojas.

II. Cuando se gira al rededor de un punto de ramificación, se pasa de todas las hojas de un paquete a todas las hojas de otro paquete distinto.

III. Este paso de un paquete de hojas a otro, corresponde al pasar entre las hojas del esquema de la superficie de Riemann para la función $f(z)$.

IV. Se definirá ϵ_n^k como:

$$\epsilon_n^k = [\cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})]^k = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$$

Si las ramas en las agrupaciones estan enumeradas de tal manera que $f_{i,k}(z) = f_{i,0}(z) \cdot \epsilon_n^k$, entonces al moverse de una agrupación a otra, las hojas de los paquetes correspondientes no están mezcladas, si no que permutan de manera cíclica.

1.3.4. Funciones representables por radicales

Definición 78. Sean $f(z)$ y $g(z)$ dos funciones multivaluadas, se denota la función multivaluada $h(z) = f(z) + g(z)$ como aquella en la cual los valores en el punto z_0 se consiguen al hacer $f(z_0) + g(z_0)$. De manera similar se construyen las funciones multivaluadas $h(z) = f(z) - g(z)$, $h(z) = f(z) \cdot g(z)$ y $h(z) = f(z)/g(z)$. En el caso de $h(z) = [f(z_0)]^n$ con n un entero diferente de cero, los valores en el punto z_0,

serán los valores de la potencia n-ésima de $f(z_0)$. Por último para $h(z) = \sqrt[n]{f(z)}$, con n un entero distinto de cero, los valores para el punto z_0 se consiguen al extraer todas las raíces de orden n de cada $f(z_0)$.

Definición 79. Sea $h(z)$ una función multivaluada, donde $h(z)$ es ***representable por radicales*** si puede ser escrita como funciones $f(z) = z$ y funciones constantes $g(z) = a$, con a un complejo, en términos de las operaciones definidas anteriormente.

Teorema 1.3.6. Las funciones representables por radicales poseen la propiedad de monodromía y por lo tanto para cada una de estas es posible la construcción de sus respectivas superficies de Riemann.

1.3.5. Grupo monodromía de funciones multivaluadas

Definición 80. Sean $g_1, g_2, \cdots, g_s$ las permutaciones de las hojas del esquema de la superficie de Riemann que corresponden a los giros en sentido horario alrededor de los puntos de ramificación. Al grupo generado por estas permutaciones $g_1, g_2, \cdots, g_s$ se le da el nombre de ***grupo de permutación del esquema dado***.

Sea z_0 un punto que no es un punto especial de la función multivaluada $w(z)$, y sean $w_1, w_2, \cdots, w_n$ los valores de la función $w(z)$ en este punto. Ahora se considera C un lazo basado en z_0 que no pasa a través de algún punto especial de la función $w(z)$. Se toma un valor $w_i = w(z_0)$ y por continuidad a lo largo de C se define un nuevo punto $w_j = w(z_0)$. Se observa que al iniciar con distintos valores para w_i se obtienen distintos valores para w_j. De manera que al lazo C le corresponde una permutación de los valores $w_1, w_2, \cdots, w_n$. Entonces si a C le corresponde una permutación g, al lazo C^{-1} le corresponderá la permutación g^{-1}. Por otro lado, si se toma C_1 y C_2 ambos lazos basados en z_0 a los cuales les corresponden las permutaciones g_1 y g_2, entonces a C_1C_2 le corresponde la permutación g_1g_2.

Definición 81. El conjunto de las permutaciones correspondientes a los lazos basados en z_0, junto la operación composición forman un grupo llamado ***el grupo de permutaciones de los valores*** $w(z_0)$.

Teorema 1.3.7. Sea G_1 el grupo de permutaciones de los valores $w(z_0)$ y G_2 el grupo de permutación para algún esquema de la función $w(z)$. Entonces G_1 y G_2

son isomorfos.

Definición 82. Por el teorema anterior se tiene que tanto el grupo de los valores $w(z_0)$ para todos los puntos z_0 y el grupo de permutación de todos los esquemas de la superficie de Riemann de la función $w(z)$ representan un único grupo. A este grupo se le llamara el ***grupo de monodromía de la función multivaluada*** $w(z)$.

Vale la pena recalcar que el grupo de monodromía de una función algebraica $w(z)$ puede ser también definido como el grupo de monodromía del espacio cubriente de n-hojas

$$\pi : S \longrightarrow (\mathbb{C}\, U\{\infty\}) - \{ \text{ puntos singulares de } w(z)\}$$

donde S denota la superficie de Riemann de la función algebraica. Es sencillo notar que está definición viene siendo la misma que se da en la definición 81.

En general, se denota al grupo de monodromia para una función multivaluada $w(z)$ como $Mon[w(z)]$.

Teorema 1.3.8. Sea $h(z) = f(z) \pm g(z)$, $h(z) = f(z) \cdot g(z)$ o $h(z) = f(z)/g(z)$, supongase que se construye el esquema de la superficie de Riemann de la función $h(z)$ a partir de los esquemas de las superficies de Riemann de las funciones $f(z)$ y $g(z)$, usando el metodo formal del teorema 1.3.3. Si F y G son los grupos de permutaciones de los esquemas para $f(z)$ y $g(z)$ respectivamente, entonces el grupo de permutaciones del esquema construido para $h(z)$ es isomorfo a un subgrupo del producto directo $F \times G$.

Demostración. Sea z_0 un punto de ramificación de la función $h(z)$ y supongase que dar un giro alrededor de este punto le corresponde las permutacione d_1 y d_2 de los esquemas de las funciones $f(z)$ y $g(z)$ respectivamente. Notese que si z_0 no fuese un punto de ramificación de $f(z)$ o de $g(z)$, entonces la permutación correspondiente a d_1 o a d_2 sería la identidad. Si las ramas $h_{i,j}(z)$ de la función $h(z)$ están enumeradas en dos subíndices como en el teorema 1.3.3, entonces, luego del giro alrededor de z_0 los primeros y segundos subíndices estarán permutados independientemente. Además, la permutación de los primeros subíndices es igual a d_1 y la de los segundos es igual a d_2. Así que hacer un giro alrededor de un punto de ramificación corresponde a la permutación de las hojas del esquema de

la superficie de Riemann de la función $h(z)$, el cual puede ser considerado como una pareja de permutaciones (d_1, d_2). Ya que d_1 y d_2 son elementos de F y G (los grupos de monodromia de las funciones $f(z)$ y $g(z)$), luego la pareja (d_1, d_2) es un elemento del producto directo $F \times G$. Esta pareja, correspondiente a todos los puntos de ramificación de $h(z)$ genera un subgrupo del grupo $F \times G$. □

Teorema 1.3.9. Sea H_1 el grupo de permutaciones del esquema construido bajo el método de la hipótesis del teorema anterior, y sea H_2 el grupo de permutaciones del esquema real de la superficie de Riemann de la función $h(z)$. Entonces existe un homomorfismo sobreyectivo del grupo H_1 sobre el grupo H_2.

Teorema 1.3.10. Sea H el grupo de permutaciones del esquema de la función $h(z) = \sqrt[n]{f(z)}$ y F el grupo de permutaciones del esquema de la función $f(z)$, hecho con los mismos cortes. $\varphi : H \longrightarrow F$ que manda las permutaciones de los paquetes de n-hojas del esquema de la función $h(z) = \sqrt[n]{f(z)}$ en las permutaciones de hojas del esquema de la función $f(z)$, es un homomorfismo sobreyectivo del grupo H sobre el grupo F. Además $Ker\varphi$ es conmutativo.

Capítulo 2

Demostración teorema de Abel-Ruffini

2.1. Demostración por grupo de Galois

Retomando los conceptos explicados en el marco teórico se enunciarán dos teoremas fundamentales para poder demostrar el teorema de Abel-Ruffini y posteriormente se realizará tal demostración. Este desarrollo fue basado en el de Dummit and Foote (2004).

Teorema 2.1.1. El polinomio general

$$x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n$$

sobre el campo $F(s_1, s_2, \ldots, s_n)$ es separable y su grupo de Galois es S_n.

Lema 2.1.1. Si α está contenida en una extensión de raíces de K como en la ecuación 1.2.3 de la sección 1.2.6, luego α está contenida en una extensión de raíces la cual es Galois sobre F y donde cada extensión K_{i+1}/K_i es cíclica.

Demostración. Se toma L como la clausura Galois de K sobre F. Para cualquier $\sigma \in Gal(L/F)$ se tiene entonces que la siguiente cadena de subcampos

$$F = \sigma(K_0) \subset \sigma(K_1) \subset \cdots \subset \sigma(K_i) \subset \sigma(K_{i+1}) \subset \cdots \subset \sigma(K_s) = \sigma(K)$$

donde $\sigma(K_{i+1})/\sigma(K_i)$ es una extensión radical simple al ser generada por el

elemento $\sigma(\sqrt[n_i]{a_i})$ raíz de la ecuación $x^{n_i} - \sigma(a_i)$ sobre $\sigma(K_i)$. Como la compuesta de extensiones de raíces es una extensión de raíces, la compuesta de todos los campos conjugados $\sigma(K)$ para $\sigma \in Gal(L/F)$ es una extensión de raíces. Además, ya que este campo es precisamente L se concluye que α está contenido en una extensión de raices Galois.
Ahora, adhiriendo a F las n_i-ésimas raíces de la unidad para todas las raíces $\sqrt[n_i]{a_i}$ de la extensión radical simple en la extensión de raíces Galois sobre K/F, obteniendo el campo F' y luego forma la compuesta de K con las extensiones de raíces.

$$F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \cdots \subseteq F'K_i \subseteq F'K_{i+1} \subseteq \cdots \subseteq F'K_s = F'K$$

El campo $F'K$ es una extensión Galois de F, pues es la compuesta de dos extensiones Galois. Las extensiones de F a $F' = F'K_0$ pueden ser obtenida como una cadena de subcampos, donde cada una de las extensiones en esta es una extensión cíclica. Así cada extensión $F'K_{i+1}/F'K_i$ es una extensión radical simple y tomando las raíces de la unidad apropiadas en los campos base, cada una de estas extensiones individuales de F' a $F'K$ es una extensión cíclica por el teorema 1.2.20. Por lo tanto $F'K/F$ es una extensión de raíces que es Galois sobre F, con extensiones cíclicas intermedias. □

Teorema 2.1.2. El polinomio $f(x)$ es soluble por radicales si y solo si su grupo de Galois es un grupo soluble.

Demostración. $\longrightarrow$ Supongase que $f(x)$ es soluble por radicales, luego cada raíz de $f(x)$ está contenida en una extensión como en el lema anterior. La extensión compuesta L de tales extensiones es del mismo tipo. Ahora se toma G_i los subgrupos de Galois correspondientes a los subcampos K_i con $i = 0, 1, \ldots, s-1$. Por teorema fundamental de Galois(Teorema 1.2.15)

$$Gal(K_{i+1}/K_i) = G_i/G_{i+1}, \quad i = 0, 1, \ldots, s-1$$

Así con los G_i se forma una cadena de subgrupos, con G_i/G_{i+1} cíclico, y por lo tanto el grupo de Galois $Gal(L/F)$ es un grupo soluble. Además como se tiene que el campo L contiene el campo de descomposición para $f(x)$, de manera que el grupo de Galois de $f(x)$ es el grupo cociente de un grupo soluble G y por lo tanto

es soluble.

$\longleftarrow$ Ahora se supondrá que el grupo de Galois G de $f(x)$ es un grupo soluble. Sea K el campo de descomposición para $f(x)$. Al ser G soluble,se tiene una cadena de subgrupos

$$1 = G_s \leq G_{s-1} \leq \cdots \leq G_{i+1} \leq G_i \leq \cdots \leq G_0 = G$$

Con G_i/G_{i+1} cíclico para $i = 0, 1, \ldots, s-1$. Entonces si se toman los campos fijados por los subgrupos de G de esta cadena, se obtiene la siguiente cadena.

$$F = K_0 \subset K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_s = K$$

de donde K_{i+1}/K_i es una extensión cíclica de grado n_i para $i = 0, 1, \ldots, s-1$. Sea F' el campo ciclotomico sobre F de todas las raíces de la unidad de orden n_i, con $i = 0, 1, \ldots, s-1$ que forma la compuesta de campos $K_i' = F'K_i$, se obtiene la siguiente cadena de extensiones

$$F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \cdots \subseteq F'K_i \subseteq F'K_{i+1} \subseteq \cdots \subseteq F'K_s = F'K$$

Luego la extensión $F'K_{i+1}/F'K_i$ es cíclica de grado que divide a n_i con $i = 0, 1, \ldots, s-1$. Como ahora se tienen las raíces de la unidad apropiadas en los campos bases, cada una de estas extensiones cíclicas es una extensión radical simple por el teorema 1.2.21. Cada una de estas raíces de $f(x)$ está por lo tanto contenida en la extensión de raíz $F'K$, de manera que $f(x)$ puede ser soluble por radicales.

□

Teorema 2.1.3 (Teorema de Abel-Ruffini)**.** La ecuación general de grado n no es soluble por radicales para $n \geq 5$.

Demostración. Del teorema 2.1.1 se tiene que el grupo de Galois para el polinomio general de grado n es el grupo simétrico S_n. Luego por el teorema 2.1.2 el polinomio de grado n es soluble por radicales si y solo si S_n es soluble. Pero este no lo es con $n \geq 5$, siendo entonces que el polinomio no es soluble por radicales. □

2.2. Demostración por grupo monodromía

Retomando los conceptos y construcciones de la sección 1.3, en el presente apartado se enuncia y demuestra el teorema fundamental y así probar el teorema de Abel-Ruffini. Este desarrollo se basa en la demostración mostrada en Alekseev (2004).

Teorema 2.2.1. Si la función multivaluada $h(z)$ es representable por radicales, entonces su grupo de monodromía es soluble.

Demostración. Sean $f(z)$ y $g(z)$ dos funciones multivaluadas, para las cuales sus grupos de monodromia son solubles, entonces:

i. Como por hipotesis los grupos F y G (grupos de permutaciones de los esquemas para $f(z)$ y $g(z)$) son solubles, luego el grupo $F \times G$ es soluble también. Ya que el grupo H_1 (como se describió en el teorema 1.3.9) puede ser considerado un subgrupo del grupo $F \times G$ esto por el teorema 1.3.8, el grupo H_1 es soluble. Por último, por el teorema 1.3.9 se sabe que existe un homomorfismo sobreyectivo de H_1 sobre el grupo H_2 de las permutaciones del correcto esquema de la función $h(z)$, por propiedades de los grupos solubles, H_2 es también soluble, y por lo tanto los grupos de monodromia de las funciones $h(z) = f(z) \pm g(z)$, $h(z) = f(z) \cdot g(z)$ y $h(z) = f(z)/g(z)$ son solubles.

ii. Sean F y H los grupos de monodromia para las funciones $f(z)$ y $h(z) = [f(z)]^n$ respectivamente, con H se contruido con el método del teorema 1.3.4.

   Por el segundo paso de la construcción en el teorema 1.3.4, se ve que el esquema contendrá algunos conjuntos de hojas en los cuales las ramas coinciden. Entonces por unicidad al hacer un giro alrededor de un punto de ramificación cualquiera, se realizan movimientos de las hojas de un conjunto a las de un conjunto distinto del esquema construido.

   De manera que una permutación d de las hojas del esquema construido por el metodo del teorema, correspondiente a un giro alrededor de un punto de ramificación, permuta los conjunto de las hojas en el que las ramas coinciden, sin romperlos.

Sea $\varphi : F \longrightarrow H$, definida como $\varphi(d) = d'$, donde d permuta las hojas $f_i(z)$ y d' permuta las hojas $h_i(z) = [f_i(z)]^n$, pero como se vio d' vendria siendo la permutación entre los conjuntos de hojas en los cuales las ramas coinciden. Haciendo así una correspondencia entre las permutaciones entre hojas y la permutación de los conjuntos.

Sea d_i y d_j dos permutaciones de hojas, es claro que:

$$\varphi(d_i d_j) = (d_i d_j)' = d_i' d_j' = \varphi(d_i)\varphi(d_j)$$

De manera que φ es un homomorfismo. Por último, se observa que es sobreyectivo, ya que a cada conjunto de hojas le corresponde una sola hoja del esquema de la superficie de Riemann para la función $h(z)$ luego de escoger las hojas con las ramas que coinciden. Además, como los pasajes entre las hojas del esquema original se transforman exactamente en los pasajes entre los conjuntos de hojas, φ es sobreyectiva.

Por propiedad de los grupos solubles, como F es soluble, y φ es un homomorfismo sobreyectivo de F sobre H, entonces H, el grupo de monodromia dela función multivaliada $h(z)$ es soluble.

iii. Sea $\varphi : H \longrightarrow F$ un homomorfismo del grupo de permutaciones del esquema de la función $h(z) = \sqrt[n]{f(z)}$ en el gupo de permutaciones del esquema de la función $f(z)$, definido como en el teorema 1.3.10 y $Ker\varphi$ su kernel, entonces el grupo cociente $H/ker\varphi$ es isomorfo al grupo F. Ya que el grupo $Ker\varphi$ es conmutativo y el grupo F es soluble por hipotesis, el grupo H es soluble.

iv. Las funciones $h(z) = a$ y $h(z) = z$ son continuas y univaluadas en todo el plano Z. Sus superficies de Riemann consisten de una única hoja, y por lo tanto su correspondiente grupo de monodromía consiste en un solo elemento e y por lo tanto es soluble.

Por la definición de funciones representables por radicales y teniendo en cuentan i,ii,iii y iv en cada uno de esos casos se encuentra que sus respectivos grupos de monodromía son solubles, entones $h(z)$ es soluble. □

Para demostrar el teorema de Abel-Ruffini es de utilidad continuar analizando la

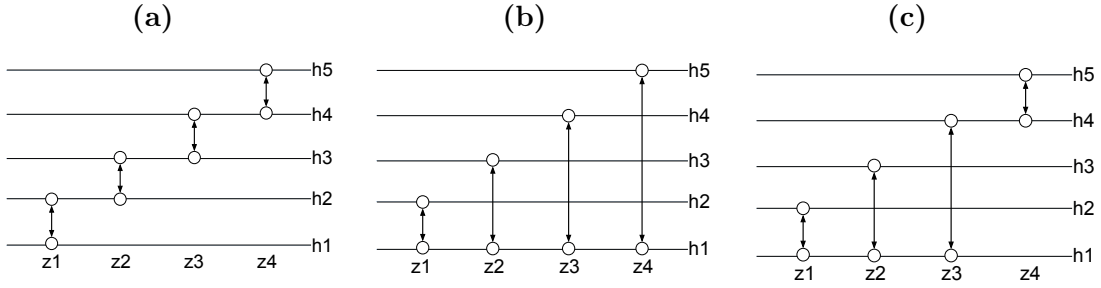
función multivaluada $w(z)$ que expresa las raíces de la ecuación

$$3w^5 - 25w^3 + 60w - z = 0$$

que se ha visto en los ejemplos 31 y 32.

Ya que es posible pasar de una hoja cualquiera a otra de la superficie de Riemann al moverse alrededor de una curva continua que no pase por los puntos $z = \pm 16, \pm 38$ de ramificación y teniendo en cuenta el ejemplo 31, el esquema de Riemann para esta función $w(z)$ terminará coincidiendo con alguno de los esquemas de la figura 4.2, por medio de permutación entre las hojas y puntos de ramificación.

Figura 2.1:
Esquemas de Riemann de la función $w(z)$ raíz de $3w^5 - 25w^3 + 60w - z = 0$



Nota: Adaptado de Abel's Theorem in Problems and Solutions (p.207), V. B. Alekseev, 2004.

De donde $h1, h2, h3, h4, h5$ son las cinco hojas de la superficie y $z1, z2, z3, z4$ son los valores de $z = \pm 16, \pm 38$, es decir, los puntos de ramificación.

Asociando a cada hoja $h1, h2, h3, h4, h5$ los números respectivos $1, 2, 3, 4, 5$ se puede notar como en el grupo de permutaciones de cada uno de los tres esquemas contienen todas las transposiciones elementales (1 2),(2 3),(3 4),(4 5). En el caso del esquema 2.1a, es facil notarlo, pues las transposiciones en cada punto de ramificación, están descritas por (1 2),(2 3),(3 4),(4 5), respectivamente. En el caso de los esquemas 2.1b y 2.1c, en el en punto de ramificación $z1$ ya se tiene una de las transposiciones elementales (1 2), pero además las otras transposiciones elementales pueden ser obtenidas de productos de las transposiciones de estos esquemas:

$$(2\ 3) = (1\ 2) \cdot (1\ 3) \cdot (1\ 2)$$

$$(3\ 4) = (1\ 3) \cdot (1\ 4) \cdot (1\ 5)$$

En el caso de la transposición (4 5) puede ser obtenida en el esquema 2.1b del producto $(4\ 5) = (1\ 4) \cdot (1\ 5) \cdot (1\ 4)$, y en el esquema 2.1c se obtiene directamente como transpocisión del punto $z4$.

Como grupo de monodromía contiene todas sus transposiciones elementales $((1\ 2), (2\ 3), (3\ 4)$ y $(4\ 5))$, entonces el grupo de monodromía coincide con S_5, el cual en la parte de conceptos básicos se dijo que no es soluble, por lo tanto $w(z)$ no es representable por radicales y finalmente $P_z(w)$ no es soluble por radicales.

Teorema 2.2.2 (Teorema de Abel-Ruffini)**.**
Para $n \geq 5$ la ecuación algebraica general

$$a_0 w^n + a_1 w^{n-1} + \ldots + a_{n-1} w + a_n = 0 \tag{2.2.1}$$

con $a_i \in \mathbb{C}$ para $i = 0, 1, \ldots, n$ y $a_0 \neq 0$. No es soluble por radicales.

Demostración.
Primero se demuestra para el caso $n = 5$. Notando que si la ecuación

$$a_0 w^5 + a_1 w^4 + a_2 w^3 + a_3 w^2 + a_4 w + a_5 = 0$$

Fuese soluble por radicales, entonces al tomar los parámetros $a_0 = 3,\ a_1 = 0,\ a_2 = -25,\ a_3 = 0,\ a_4 = 60,$ y $a_5 = z$ esta sería soluble por radicales, pero anteriormente se demostró que esto no es así. Por lo tanto la ecuación 2.2.1 para $n = 5$ no es soluble por radicales.

Para demostrar el caso $n > 5$, se toma en cuenta la ecuación

$$(3w^5 - 25w^3 + 60w - z)w^{n-5} = 0 \tag{2.2.2}$$

Para la función $w(z)$ que expresa las raíces de la ecuación 2.2.2 en términos del parámetro z, la superficie de Riemann consta de algunas hojas separadas que cumplen $w(z) = 0$ y de cinco hojas separadas que representan el esquema de la función $w_1(z)$ que representa las raíces de la ecuación:

$$3w^5 - 25w^3 + 60w - z = 0$$

Entonces el grupo de $Mon[w(z)]$ coincide con $Mon[w_1(z)]$, el cual al ser el grupo

de permutaciones S_5 no es soluble por radicales.

□

Capítulo 3

Comparación entre demostraciones

Luego de demostrar el teorema de Abel-Ruffini usando los grupos de Galois y monodromía, es posible ver las similitudes y diferencias entre estas dos. En el cuadro comparativo que se muestra a continuación se mostrará el desarrollo general para ambas.

Demostración por Grupo de Galois	**Demostración por Grupo Monodromia**
Campo de la matemática usado	
Teoría de Galois.	Topología Algebraica, con principal enfoque en las superficies de Riemann.
Conceptos previos generales	
Extensión: Simple, algebraica, finita.	Caminos y homotopía de caminos.
Campo: base, compuesto, de descomposición, separable, ciclotomico de las n-ésimas races de la unidad.	Aplicación y espacio cubriente.
Elemento: primitivo, algebraico.	Fibras y levantamientos.
Polinomio mínimo, n-esimas raices de la unidad.	Grupo fundamental.

<table>
<tr><th>Demostración por Grupo de Galois</th><th>Demostración por Grupo Monodromia</th></tr>
<tr><td colspan="2">Conceptos previos Fundamentales</td></tr>
<tr><td rowspan="3">Automorfismo de Anillos.</td><td>Función multivaluada $w(z)$.</td></tr>
<tr><td>Superficie de Riemann, ramas continuas univaluadas y hojas de la función multivaluada $w(z)$.</td></tr>
<tr><td>Puntos: Singulares, de ramificación y de no unicidad.</td></tr>
<tr><td rowspan="2">$Aut(K/F)$: Sea K/F una extensión de campos. Al conjunto de automorfismos σ de K que cumplen $\sigma(\alpha) = \alpha$, $\forall \alpha \in F$, con la composición, es un grupo el cual se denotará $Aut(K/F)$.</td><td>Curvas e imagenes continuas de una curva.</td></tr>
<tr><td>Propiedad de Monodromía.</td></tr>
<tr><td>De cumplir una función multivaluada $w(z)$ la propiedad de monodromía es posible construir superficie de Riemann.</td></tr>
<tr><td colspan="2">Los grupos fundamentales para la demostración</td></tr>
<tr><td>Grupo de Galois [$Gal(K/F)$]: Grupo de los automorfismos de $Aut(K/F)$ de una extensión finita K/F, para la cual se cumple que $|Aut(K/F)| = [K : F]$, es decir, el orden del grupo de automorfismos es el mismo que el grado de la extensión.</td><td>Grupo Monodromía del espacio cubriente π: Es la imagen del homomorfismo φ_π del grupo fundamental de X relativo a x_0 $(\pi_1(X, x_0))$ en el grupo de automorfismos de la fibra F de la apliación cubriente $\pi : Y \to X$ de n-hojas.</td></tr>
</table>

Demostración por Grupo de Galois	**Demostración por Grupo Monodromia**
Grupo de Galois de $f(x)$ ***sobre*** F***:*** Es el grupo de Galois del campo de descomposición de $f(X)$ sobre F, donde $f(x)$ es separable en F.	***Grupo Monodromia*** $Mon[w(z)]$***:*** Grupo de permutaciones de las hojas del esquema de la superficie de Riemann de la función multivaluada $w(z)$. El cual es el mismo grupo de las permutaciones correspondientes de los lazos basados en z_0, con z_0 que no es un punto especial, y donde $w_1, w_2, \ldots, w_n$ son los valores de la función $w(z)$ evaluados en z_0.
Otros conceptos previos	
Clausura Galois, Funciones simétricas elementales y polinomio general de grado n.	
Extensión de radicales simples, y extensión cilcica	
Definición de Soluble por Radicales	
Un polinomio $f(x) \in F[x]$ se dice soluble por radicales si todas sus raices pueden ser determinadas en términos de radicales, es decir, si todo elemento α algebraico sobre F cumple ser un elemento del campo K que puede ser obtenido por una suseción de extensiones de radicales simples con $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ para algun $a_i \in K_i$, $i = 0, 1, \ldots, s-1$.	Un polinomio $P(w)$ con w una función multivaluada, es soluble por radicales si la solución $w(z)$ del polinomio es una función multivaluada representable por radicales, es decir, puede ser escrita en términos de funciones $f(z) = z$, funciones constantes $g(z) = a$ y funciones que representen la suma, resta, multiplicación, división, potenciación y n-ésimas raíces de funciones multivaluadas.

Demostración por Grupo de Galois	**Demostración por Grupo Monodromia**
Teoremas más importantes para la demostración	
Teorema G1: El polinomio general $x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$ sobre el campo $F(s_1, s_2, ..., s_n)$ es separable y su grupo de Galois es el grupo simétrico S_n.	
Teorema G2: El polinomio $f(x)$ puede ser resuelto por radicales si y solo si su grupo de Galois es un grupo soluble.	***Teorema M1:*** Si la función multivaluada $h(z)$ es representable por radicales, entonces su grupo de monodromía es soluble.
La demostración del teorema de Abel Ruffini.	
Por el teorema G1 se ve que el polinomio general $f(x)$ tiene como grupo de Galois al grupo S_n, pero este grupo no es soluble para $n \geq 5$, y por lo tanto por el teorema G2 $f(x)$ no es soluble por radicales.	Sea $P(w)$ un polinomio de grado n. Se demuestra primero con $n = 5$, viendo que el grupo de monodromía de la función multivaluada que expresa las raices de $P(w) = 3w^5 - 25w^3 + 60w - z$ termina siendo S_5, el cual no es soluble, y por teorema M1 $P(w)$ no es soluble por radicales, luego el polinomio general de grado 5 no lo es. De manera similar para $n > 5$, tomandose el polinomio $P(w) = (w^5 - 25w^3 + 60w - z)w^{n-5}$, y analogamente se demuestra que no es soluble por radicales.
Otras aplicaciones de los grupos estudiados	
Códigos lineales detectores-correctores de errores de longitud n sobre campos de Galois $\mathbb{F}_{p^k}$ enteros modulo p^k con p un primo. (Código Reed-Solomon)	Investigar en futuros trabajos

Demostración por Grupo de Galois	**Demostración por Grupo Monodromia**
(Cifrado de datos) ▪ Cifrado DES, basadas en el campo de Galois $\mathbb{F}_2$ Enteros modulo 2 (en el espacio vectorial $\mathbb{F}_{2^6}$). ▪ Cifrado AES, basadas en el campo binario de Galois $\mathbb{F}_2$ (en el espacio vectorial $\mathbb{F}_{2^8}$). ▪ Cifrado Twofish, que usa el campo de Galois con 2^8 elementos y el espacio vectorial $\mathbb{F}_{2^8}$. ▪ Cifrado SAFER, que usa el campo de Galois $\mathbb{F}_{257}$. ▪ Cifrado basado en curvas elipticas, tiene gran relevancia el campo de Galois $\mathbb{F}_{p^k}$ de los enteros modulo p^k con p un primo.	Investigar en futuros trabajos
Geométria Algebraica sobre campos de Galois	Investigar en futuros trabajos

Las aplicaciones del Grupo de Galois fueron extraidas del texto (Tapia-recillas, 2011).

Capítulo 4

Análisis de los grupos

4.1. Consideraciones previas

Del ejemplo usado para demostrar el teorema de Abel-Ruffini se puede notar como el grupo de monodromía $Mon[w(z)]$ está completamente definido por las permutaciones asociadas a cada uno de sus puntos de ramificación, permitiendo concluir el siguiente teorema.

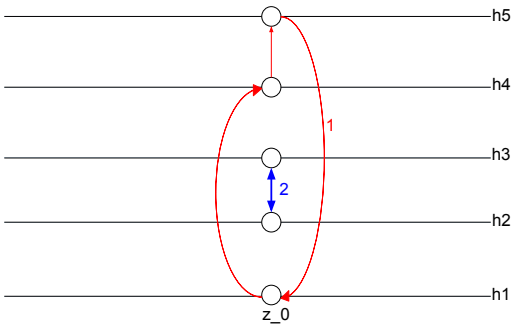
Teorema 4.1.1. Sea $w(z)$ una función multivaluada con n hojas en el esquema de su superficie de Riemann, donde $z_1, z_2, \ldots, z_k$ son puntos de ramificación de la función, entonces $Mon[w(z)] = \langle \tau_{z_1}, \ldots, \tau_{z_k} \rangle$, siendo $\tau_{z_i} \in Mon[w(z)]$ las permutaciones asociadas a cada punto de ramificación.

Demostración. Como $Mon[w(z)]$ es el grupo de permutaciones de las hojas del esquema de la superficie de Riemann de $w(z)$ al dar giros en sentido horario alrededor de sus puntos de ramificación z_i si a cada uno de estos se le asigna una permutación τ_{z_i} entonces todo $\tau \in Mon[w(z)]$ estará definido por un producto de permutaciones τ_{z_i}. □

Observación 5. *Aunque podría haber más de $n!$ puntos de ramificación, bastará con tener en cuenta las $k \leq n!$ permutaciones distintas asignadas a cada punto, pues al ser $Mon[w(z)]$ un grupo de permutaciones de un conjunto de n elementos a lo más puede tener $n!$ permutaciones.*

Definición 83. Sea z_0 un punto de ramificación de una función $w(z)$, se define como ***unión de hojas*** en el esquema de la superficie de Riemann de $w(z)$ a los caminos entre hojas dando giros en sentido horario alrededor del punto z_0 de manera que después de una cantidad finita de giros alrededor del mismo punto de ramificación es posible volver a la hoja inicial. Cada unión de hojas representa un k-ciclo de $Mon[w(z)]$ con k el número de hojas que se unen.

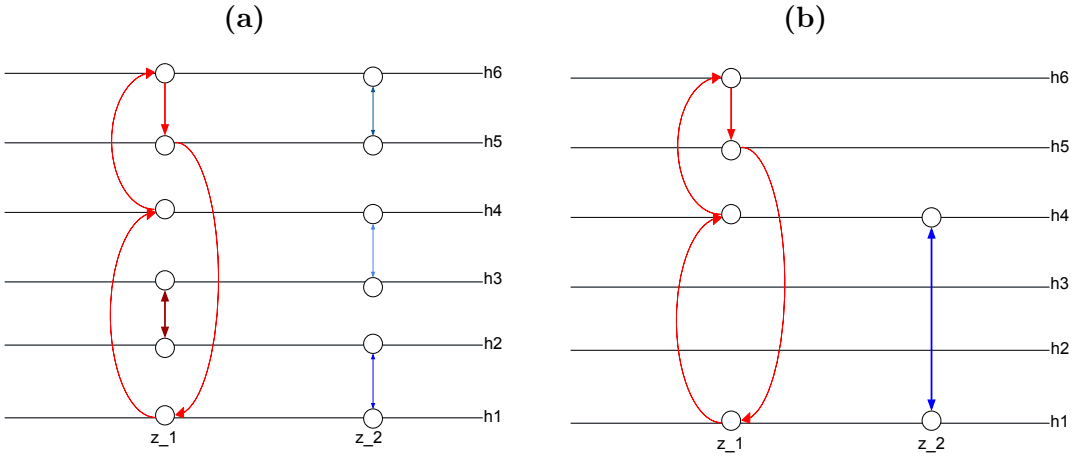
Figura 4.1:
Uniones en un punto de ramificación z_0



En la figura 4.1 se pueden observar dos uniones distintas en el punto z_0. Siendo la unión 1 representada por el 3-ciclo (1 4 5) y la unión 2 por la transposición (2 3), de manera que $\tau_{z_0} = (1\ 4\ 5)(2\ 3)$.

Definición 84. Dos uniones se dicen ***disjuntas*** si sus respectivos k-ciclos son disjuntos.

Figura 4.2:
Tipos de uniones



v

En el punto z_1 de la figura 4.2a hay dos uniones disjuntas, pues sus respectivos k-ciclos son (1 4 6 5) y (2 3) que son disjuntos, de forma análoga en el punto z_2 hay tres uniones disjuntas. Por otro lado, en la figura 4.2b se cuenta con una única unión en cada punto.

4.2. Relación entre el grupo de Galois y el grupo monodromía

Como el grupo de Galois $Gal[f(x)]$ de un polinomio $f(x)$ y el grupo monodromía $Mon[w(z)]$ de una función multivaluada $w(z)$ están definidos por $f(x)$ y $w(z)$ respectivamente, para relacionar estos dos grupos en necesario definir $f(x)$ y $w(z)$ de manera que cumplan ciertas características especificas, a continuación se ve tal construcción.

Sea $f_z(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + z$ un polinomio de grado n con coeficientes $a_i \in \mathbb{C}$ para $i = 1, 2, \ldots, n$, $a_n \neq 0$ y que además es separable. Si se construye la función n-valuada $w(z)$ en los complejos, tal que $f_z(w(z)) = 0$, entonces:

- El polinomio $f_z(x)$ tiene n raíces $\alpha_i(z)$, las cuales son funciones univaluadas en los complejos.
- Por su construcción $w(z)$ tiene n ramas, que son funciones univaluadas, por lo tanto n hojas en su esquema de la superficie de Riemann.

De esta forma $Gal[f_z(x)]$ y $Mon[w(z)]$ van a estar relacionados, tal que se cumplirá lo siguiente.

- Como $\sigma \in Gal[f_z(x)]$ permuta los subíndices de las raíces $\alpha_1(z), \alpha_2(z), \ldots \alpha_n(z)$ de los factores irreducibles de $f_z(x)$, entonces $\sigma(i) = j$, con i, j subíndices de las raíces de $f_z(x)$.
- Como $\tau \in Mon[w(z)]$ permuta los valores de $w(z)$ evaluado en un punto z_0, si $w_1, w_2, \ldots, w_n$ son los respectivos valores de $w(z_0)$ entonces τ permuta los subíndices de estos valores, de manera que $\tau(l) = r$ con l, r subíndices de los valores de $w(z_0)$.

Por la manera en que se construyeron $f_z(x)$ y $w(z)$ se puede llegar a las conclusiones especificadas en los siguientes teoremas.

Teorema 4.2.1. Sea z_0 un punto de ramificación de $w(z)$ que tiene m uniones disjuntas que unen k_i (para $i = 1, 2, ..m$) hojas del esquema de la superficie de Riemann, respectivamente, entonces $f_{z_0}(x)$ tendrá m raíces múltiples cada una con su multiplicidad k_i respectiva.

Demostración. Sea z_0 un punto de ramificación de $w(z)$ talque z_0 tiene m uniones disjuntas de k_i hojas del esquema de la superficie de Riemann, entonces $w(z_0)$ contará con $N = (n + m) - (k_1 + k_2 + \cdots + k_m)$ valores distintos, donde cada uno es raíz del polinomio $f_{z_0}(x)$. Por el teorema fundamental del álgebra $f_{z_0}(x)$ cuenta con n raíces en los complejos, y como $w(z_0)$ tiene N valores distintos que son raíz, y k_i valores iguales a su respectivo $i = 1, 2, \ldots, m$ que también son raíz, $f_{z_0}(x)$ tiene m valores $w(z_0)$ con multiplicidad k_i, respectivamente. □

Corolario 4.2.2. Si z_0 es un punto de ramificación de $w(z)$ tiene una única unión de $k \leq n$ hojas del esquema de la superficie de Riemann, entonces $f_{z_0}(x)$ tendrá una raíz múltiple de multiplicidad k.

Demostración. Se obtiene directamente del teorema anterior tomando $m = 1$. □

4.3. Descripción de los elementos de cada grupo

De la sección anterior se obtiene que ambos grupos están generados por permutaciones de n elementos, en la presente sección se continúa describiendo como son estos elementos en cada grupo.

Definición 85.

i. La ***identidad*** $e_G \in Gal[f_z(x)]$ es la permutación que cumple $e_G(i) = i$ para todo i subíndice de las raíces de $f_z(x)$, es decir, es la permutación que mantiene fijas todas las raíces de $f_z(x)$.

ii. La ***identidad*** $e_M \in Mon[w(z)]$ es la permutación que mantiene fijo el subíndice de los valores de $w(z_0)$, es decir, $e_M(l) = l$ para todo l subíndice de los valores de $w(z_0)$. Esto implica que al girar al rededor de algún punto de ramificación no se cambia de hoja.

Mientras $f_z(x)$ tenga un número finito de raíces la función $w(z)$ tendrá un número finito de valores, de manera que cada permutación de los respectivos grupos de Galois y monodromía va a ser de orden finito k_σ y k_τ respectivamente, es decir, si $\sigma \in Gal[f_z(x)]$ y $\tau \in Mon[w(z)]$ entonces

$$\sigma^{k_\sigma} = \overbrace{\sigma \cdot \sigma \cdot \sigma \cdots \sigma \cdot \sigma}^{k_\sigma - veces} = e_G$$

y

$$\tau^{k_\tau} = \overbrace{\tau \cdot \tau \cdot \tau \cdots \tau \cdot \tau}^{k_\tau - veces} = e_M$$

Teorema 4.3.1.

i. Para todo $\sigma \in Gal[f_z(x)]$, el inverso de σ es $\sigma^{-1} = \sigma^{k_\sigma - 1}$, donde k_σ es su respectivo orden.

ii. Para todo $\tau \in Mon[w(z)]$, el inverso de τ es $\tau^{-1} = \tau^{k_\tau - 1}$, siempre y cuando k_τ sea su respectivo orden.

Demostración.

i. Sea $\sigma \in Gal[f_z(x)]$ de orden k_σ una permutación cualquiera, entonces

$$\sigma^{k_\sigma - 1} \cdot \sigma = \sigma^{k_\sigma} = e_G$$

y

$$\sigma \cdot \sigma^{k_\sigma - 1} = \sigma^{k_\sigma} = e_G$$

por lo tanto $\sigma^{k_\sigma - 1}$ es el elemento inverso de σ.

ii. Está demostración se obtiene de manera análoga a la anterior

□

Sea φ una aplicación que va del grupo $Gal[f_z(x)]$ al grupo $Mon[w(z)]$, tal que:

$$\begin{array}{ccc} \varphi : Gal[f_z(x)] & \longrightarrow & Mon[w(z)] \\ \sigma & \longrightarrow & \tau_\varphi \end{array} \tag{4.3.1}$$

Para poder concluir que φ es un isomorfismo es necesario considerar τ_φ de tal manera que se cumpla que:

- $\varphi(e_G) = e_M$.
- Si $\sigma \in Gal[f_z(x)]$ y $\tau_\varphi \in Mon[w(z)]$ entonces $\varphi(\sigma^{-1}) = \tau_\varphi^{-1}$.
- $\varphi(Gal[f_z(x)]) = Mon[w(z)]$.
- φ es inyectiva.

Capítulo 5

Conclusiones

- Mientras en el grupo de Galois lo que se permutan son las raíces de un polinomio general $f(x) \in F[x]$, el grupo de monodromía permuta las hojas del esquema de Riemann de una función multivaluada $w(z)$ en los complejos, al igual que permuta los distintos valores que puede tomar un punto z_0 al ser evaluado en la función $w(z)$.
- Aunque en general la definición de que un polinomio sea soluble por radicales implica que sus raíces sean representadas en términos de radicales (sumas, restas, multiplicaciones, divisiones, n-potencias y raíces n-ésimas de funciones), para la demostración por teoría de Galois es más útil usar una definición equivalente que es la de la sucesión de extensiones radicales simples.
- El teorema fundamental para ambas demostraciones del teorema de Abel-Ruffini es aquel que implica que un polinomio (o función multivaluada) es soluble por radicales si su grupo ya sea de Galois (o monodromía) es soluble por radicales.
- La principal idea en ambas demostraciones es encontrar la relación entre el grupo simétrico de permutaciones y los grupos de Galois y monodromía.
- Para hallar la relación entre el grupo de Galois del polinomio $f_z(x)$ y el grupo de monodromía de la función multivaluada $w(z)$, es necesario tomar $w(z)$ que satisfaga $f_z(w(z)) = 0$. Por lo tanto las permutaciones del grupo de Galois permutan la misma cantidad de elementos que las permutaciones

del grupo monodromía.

- La relación entre los puntos de ramificación z_0 de la función $w(z)$ y las raíces de $f_{z_0}(x)$ va dada por los valores de la función $w(z)$ en cada punto de ramificación.

Capítulo 6

Limitaciones e investigaciones futuras

- A lo largo de este trabajo se enuncian algunas aplicaciones del grupo de Galois (en específico de los campos de Galois), valdría la pena ver aplicaciones del grupo monodromía y analizar si este es útil para las aplicaciones del grupo de Galois.
- Además se realiza el análisis teniendo en cuenta un polinomio $f_z(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + z$ de grado n con coeficientes $a_i \in \mathbb{C}$, en futuras investigaciones podría hacerse tal análisis tomando un polinomio $f_z(x)$ más general con coeficientes $a_i \in \mathbb{C}[z]$ polinomios en los complejos.
- Aunque no se demuestra el isomorfismo entre los dos grupos, se da una descripción lo suficientemente detallada para poder concluirlo, sentando las bases necesarias para un trabajo futuro donde se pueda realizar el isomorfismo explicito.

Referencias bibliográficas

Aceff, F. D. M. and Lluis-Puebla, E. (2016). Teoría de galois, un primer curso. *Publicaciones electronicas Sociedad Matemática Mexicana*, 14.

Alekseev, V. B. (2004). Abel's theorem in problems and solutions.

Cabria Zambrano, M. L. (2017). Demostración topológica del teorema de abel-ruffini.

Chamizo Lorente, F. (2005). ¡Qué bonita es la teoría de Galois!

Charris Castañeda, J. A., Aldana Gómez, B., and Acosta-Humánez, P. (2013). *Algebra Fundamentos, Grupos, Anillos, Cuerpos y Teoría de Galois*.

Dummit, D. S. and Foote, R. M. (2004). *Abstract Algebra*. Third edition.

Fraleigh, J. B. (1988). *Algebra Abstracta Primer Curso*.

Herstein, I. N. (1996). *Abstract algebra*. Prentice-Hall.

Jiménez Rolland, R. and Valdespino, M. (s.f). Configuraciones, trenzas y el teorema de abel-ruffini.

Judson, T. W., Austin, S. F., Beezer, R. A., and Behn, A. (2020). *Abstract Algebra Theory and Applications Traducción al español*.

Lipschutz, S. (s.f.). *Teoría y problemas de topología general*.

Munkres, J. R. (2002). *Topología*. Segunda edition.

Ottina, M. (2018). Estructuras algebraicas i.

Rotman, J. J. (1995). *An introduction to the theory of groups*. Fourth edition.

Ruiz, A. (s.f.). *Historia y Filosofía de las matemáticas*.

Rzedowski Calderón, M. (2016). La demostración de abel. *Miscelánea Matemática*, 63.

Sánchez Muñoz, J. M. (2011). Historias de matemáticas abel y la imposibilidad de resolver la "quíntica"por radicales. *Pensamiento Matemático*.

Tapia-recillas, H. (2011). Sobre algunas aplicaciones de los campos de Galois. *Miscelánea Matemática*, 53(53):81–100.

Villa Salvador, G. (2011). Las ecuaciones polinomiales como el origen de la teoría de Galois. *Miscelanea Matemática*, 53:1–22.