Universidad de San Carlos de Guatemala
Escuela de Ciencias Físicas y Matemáticas
Departamento de Matemática

DEMOSTRACIÓN TOPOLÓGICA DEL TEOREMA DE ABEL-RUFFINI

Monica Lucía Cabria Zambrano
Asesorado por Dra. Rita Jiménez Rolland

Guatemala, marzo de 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

ESCUELA DE CIENCIAS FÍSICAS Y MATEMÁTICAS

DEMOSTRACIÓN TOPOLÓGICA DEL TEOREMA DE ABEL-RUFFINI

TRABAJO DE GRADUACIÓN
PRESENTADO A LA JEFATURA DEL
DEPARTAMENTO DE MATEMÁTICA
POR

MONICA LUCÍA CABRIA ZAMBRANO
ASESORADO POR DRA. RITA JIMÉNEZ ROLLAND

AL CONFERÍRSELE EL TÍTULO DE
LICENCIADA EN MATEMÁTICA APLICADA

GUATEMALA, MARZO DE 2017

UNIVERSIDAD DE SAN CAROLOS DE GUATEMALA
ESCUELA DE CIENCIAS FÍSICAS Y MATEMÁTICAS

CONSEJO DIRECTIVO

DIRECTOR	M.Sc. Edgar Anibal Cifuentes Anléu
SECRETARIO ACADÉMICO	Ing. José Rodolfo Samayoa Dardón

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

EXAMINADOR	Lic. William Roberto Gutiérrez Herrera
EXAMINADOR	Lic. Hugo Allan García Monterrosa
EXAMINADOR	Lic. Rubén Darío Narciso Cruz

Universidad de San Carlos de Guatemala
Escuela de Ciencias Físicas y Matemáticas

Ref. D.DTG. 002-2017
Guatemala 23 de marzo de 2017

El Director de la Escuela de Ciencias Físicas y Matemáticas de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Coordinador de la Licenciatura en Matemática Aplicada, al trabajo de graduación Titulado: **Demostración Topológica del Teorema de Abel-Ruffini** presentado por la estudiante universitaria **Monica Lucía Cabria Zambrano,** autoriza la impresión del mismo.

IMPRIMASE.

MsC. Edgar Aníbal Cifuentes Anleu
Director
Escuela de Ciencias Físicas y Matemáticas

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA ESCUELA DE CIENCIAS FISICAS Y MATEMÁTICAS DIRECCIÓN

EC/pec

AGRADECIMIENTOS

A mis padres	Por haberme apoyado en cada paso de mi vida académica y en los altibajos de la misma.
A mis hermanas	Por ser ejemplos en distintas áreas y motivarme siempre.
A mis amigos	Por creer en mí y por los momentos y conocimientos compartidos.
A mi asesora	Rita, por haber aceptado el trabajo a distancia y ser paciente con el desarrollo de este trabajo.
Al CCM e IRyA, UNAM	Por abrirme las puertas para trabajar en sus instalaciones.
A Manuel y Hannah	Por el apoyo, sugerencias de edición y material extra brindado.
A mis profesores	Por compartir el conocimiento y gusto por las matemáticas a lo largo de la carrera.

DEDICATORIA

A mis papás y a quien lea este trabajo.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
$\cdot(a,b) = a \cdot b$	$\cdot$ es una operación binaria
$\phi : A \to B$	Función del conjunto A al conjunto B
$\phi(a) = b$	Imagen del elemento a de un conjunto, bajo la fucnión ϕ
$\phi^{-1}(b)$	Pre-imagen del elemento b, bajo la función ϕ
G	Grupo arbitrario
$g \in G$	Elemento del grupo G
g^{-1}	Inverso del elemento g de un grupo G
e	Elemento neutro de un grupo
a^n	Elemento a operado n veces
$\circ(G)$	Orden del grupo G
$\circ(g)$	Orden del elemento $g \in G$
$\langle a \rangle$	Grupo cíclico generado por el elemento a
$\mathbb{Z}_n$	Grupo de los enteros bajo adición módulo n
$G_1 \cong G_2$	Grupo G_1 isomorfo al grupo G_2
$H < G$	H es subgrupo de G
$H \lhd G$	H subgrupo normal de G
aH	clase lateral izquiera del subgrupo H
Ha	clase lateral derecha del subgrupo H
$\mathrm{Aut}(G)$	Automorfismo
$\mathrm{Inn}(G)$	Automorfismo Interno
$H \triangleleft G$	H subgrupo normal de G
G/N	Grupo cociente
$K(G)$	Conmutador del grupo G
S_n	Grupo simétrico de grado n
A_n	Grupo Alternante de grado n
$\mathrm{mcd}(a,b)$	Máximo común divisor de a y b
$G \backsimeq F$	Grupo G homomorfo al grupo F

Símbolo	Significado
$\ker(\phi)$	Núcleo de la función ϕ
$\mathbb{R}$	Conjunto de los números Reales
$\mathbb{Z}$	Conjunto de los números Enteros
$\mathbb{C}$	Conjunto de los números Complejos
$z = a + bi$	Representación algebraica de un número complejo
$\mathrm{Re}(z)$	Parte real de un número complejo
$\mathrm{Im}(z)$	Parte imaginaria de un número complejo
$\overline{z}$	Conjugado de un número complejo
$P(z)$	Polinomio con variables complejas
$gr(P)$	Grado de un polinomio P
$\lvert z\rvert$	Módulo de un número complejo
$arg(z)$	Ángulo del origen a un vector complejo
$z = r(\cos\varphi + i\mathrm{sen}\varphi)$	Representación trigonométrica de un número complejo
ϵ_n	El número complejo $\cos\left(\frac{2\pi}{n}\right) + i\mathrm{sen}\left(\frac{2\pi}{n}\right)$
$\{A_i\}_{i\in I}$	Familia de conjuntos
(X, τ)	Espacio topológico
$\{x_n\}$	Sucesión de elementos en un conjunto X
$x_n \to x$	La sucesión $\{x_n\}$ converge al elemento x
$f\colon A \twoheadrightarrow B$	función multivaluada
$\mathbb{C}*$	Plano complejo sin el cero
$\hat{\mathbb{C}}$	Plano complejo extendido
$X \approx Y$	Espacios X y Y homeomorfos
$X \sqcup Y$	Unión disjunta de X y Y
I	Intervalo $[0, 1]$
γ	Caminos
id	Función identidad
(f_i, U_i)	Elementos analíticos de una función f multivaluada
$f_0 \simeq f_1$	Caminos homotópicos
ϵ_x	Camino constante x.
$\pi_1(X, x_0)$	Grupo fundamental de X basado en x_0
$\mathrm{Mon}(f)$	Grupo de monodromía de la función f

OBJETIVOS

General

Presentar los detalles de la demostración topológica del teorema de Abel-Ruffini.

Específicos

1. Establecer las nociones de teoría de grupos necesarias para introducir al grupo simétrico e identificar grupos solubles.

2. Introducir las propiedades en el campo de los números complejos, así como de las funciones continuas en el mismo.

3. Definir las nociones de función algebraica y explicar cómo se le puede asociar una superficie de Riemann y las propiedades de un espacio cubriente de n-hojas.

4. Estudiar el grupo de monodromía de un espacio cubriente para determinar la imposibilidad de una solución por radicales para ecuaciones polinomiales de grado mayor o igual a cinco siguiendo el enfoque de Arnold.

INTRODUCCIÓN

En los cursos escolares de álgebra se enseña a resolver ecuaciones lineales, de la forma $ax + b = 0$, donde la solución es de la forma $x = -b/a$. También se nos enseña a resolver ecuaciones de grado dos, de la forma

$$ax^2 + bx + c = 0$$

con la fórmula que brinda de manera general las soluciones a cualquier ecuación de este tipo

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

La fórmula general para encontrar raíces de polinomios cuadráticos fue planteada por los babilonios aproximadamente en el año 2000 a.C. este tipo de soluciones fueron motivo de estudio en álgebra. Esta fórmula también ayudó al desarrollo de los números complejos. En algunas ocasiones el discriminante, $b^2 - 4ac$, es un número negativo. De esto, surge la idea de un elemento que sea $\sqrt{-1}$ y más adelante se comprueba que la fórmula cuadrática también funciona cuando los coeficientes del polinomio son complejos, esto es por las propiedades de campo, que estudiaremos a partir del capítulo 2.

Sabemos que estas fórmulas que dependen de los coeficientes de un polinomio y operaciones como suma, resta, multiplicación, división, potencias y radicales existen para las ecuaciones de grado 1 y 2, pero también existen fórmulas generales de este tipo para grado 3 y 4, que fueron desarrolladas por italianos en la época del Renacimiento.

A principios del siglo XVI, Scipione del Ferro (1465-1526) encontró un método para resolver las ecuaciones de la forma $x^3 + ax = b$, que mantuvo en secreto hasta justo antes de su muerte y lo comunicó a su estudiante Antonio Fiore. Actualmente, sabemos que todas las ecuaciones cúbicas se pueden reducir a esta forma cuando se permite a a, b ser negativos, pero en aquella época no eran conocidos estos números. En 1530 Niccolo Fontana, conocido como *Tartaglia* (1500-1557) anunció que podía

resolver dos problemas con ecuaciones cúbicas y fue retado por Fiore. Tartaglia resolvió los de la forma $x^3 + ax = b$ y Fiore no pudo resolver los de la forma $x^3 + ax^2 = b$, resultando ganador Tartaglia.

Más adelante, Gerolamo Cardano (1501-1576) persuadió a Tartaglia de revelar su secreto para resolver las ecuaciones cúbicas y él accedió bajo la condición de que no se revelara y en caso de que Cardano publicara un libro, le diera crédito al trabajo de Tartaglia. Años más tarde, Cardano descubrió el trabajo de del Ferro y lo publicó en un libro en 1545. Luego de eso, el primero sirviente de Cardano y luego colaborador, Ludovico Ferrari (1522-1565) aceptó las condiciones de Tartaglia y terminó por ganarle en competencia y prestigio.

Cardano notó que el método de Tartaglia requería eventualmente raíces de números negativos y probablemente lo publicó sin comprender, fue Rafael Bombelli (1526-1572) quien estudió a detalle este problema y a quien se le adjudica el *descubrimiento* de los números complejos.

La fórmula general para resolver una ecuación de la forma

$$ax^3 + bx^2 + cx + d = 0$$

necesita primero calcular

$$S = b^2 - 3ac$$
$$T = 2b^3 - 9abc + 27a^2d$$

Con esto, obtenemos

$$C = \sqrt[3]{\frac{S \pm \sqrt{T^2 - 4S}}{2}}$$

y finalmente las raíces son de la forma

$$x_k = -\frac{1}{3a}\left(b + \epsilon^k C + \frac{S}{\epsilon^k C}\right),\ k \in \{0, 1, 2\},$$

donde ϵ es una raíz de la unidad (en complejos).

Por último, fue Ferrari, en 1540, quien resolvió la ecuación general de grado cuatro, que fue publicado en 1545. El desarrollo de este método es bastante extenso, pero daremos la fórmula general para este caso a continuación. Dada una ecuación de la forma

$$ax^4 + bx^3 + cx^2 + dx + e = 0,$$

sus soluciones son de la forma:

$$x_{1,2} = -\frac{b}{4a} - S \pm \frac{1}{2}\sqrt{-4S^2 - 2p + \frac{q}{S}}$$

$$x_{3,4} = -\frac{b}{4a} + S \pm \frac{1}{2}\sqrt{-4S^2 - 2p + \frac{q}{S}},$$

donde p y q son las expresiones

$$p = \frac{8ac - 3b^2}{8a^2}$$

$$q = \frac{b^3 - 4abc + 8a^2d}{8a^3}$$

y P, Q están dadas por

$$S = \frac{1}{2}\sqrt{-\frac{2}{3}p + \frac{1}{3a}\left(Q + \frac{r}{Q}\right)}$$

$$Q = \sqrt[3]{\frac{t + \sqrt{t^2 - 4r^3}}{2}},$$

con

$$r = c^2 - 3bd + 12ae$$

$$t = 2c^3 - 9bcd + 27b^2e + 27ad^2 - 72ace.$$

En el estudio de las soluciones de ecuaciones polinomiales, no se logró encontrarlas para grado 5. Paolo Ruffini (1765-1822) a su vez estaba trabajando en la resolución de este tipo de ecuaciones, unificando la teoría de ecuaciones con teoría de grupos, introduciendo la noción de orden de un elemento y un grupo, también demostró que el grupo de permutaciones S_5 no era soluble, basado en las ideas de Lagrange, quien en 1770 asoció los polinomios con los grupos de permutación (Villa Salvador, 2011). Ruffini, en 1799, realizó un primer bosquejo de la prueba de la imposibilidad de grado cinco, pero no fue aceptada por la comunidad matemática de la época.

En 1820, el matemático noruego Niels Henrik Abel (1802-1829) propuso una solución general a la ecuación de grado cinco que dependía de los coeficientes, sin embargo esta falló cuando le pidieron ejemplos, así que continuó estudiando estas soluciones. En 1824 Abel demostró, con las ideas de Paolo Ruffini y Lagrange, que no existe una solución general radical para polinomios de grado cinco o mayor,

conocido ahora como el teorema de imposibilidad de Abel o teorema de Abel-Ruffini. La prueba era muy corta y con contenido muy avanzado para los matemáticos contemporáneos, por lo que Abel publicó una nueva versión más extensa de la misma en 1826. Puede leerse más detalles en (Schwartz, 2015).

Esto fue importante porque aparte de resolver la pregunta sobre la solubilidad de polinomios, brindó un enfoque abstracto, completamente nuevo al álgebra, utilizando los avances más recientes hasta esa época sobre grupos de simetrías y permutaciones, inspirando a jóvenes matemáticos como Galois, Cayley, Hamilton, Jordan, Kronecker y Sylvester a desarrollar y aplicar teoría de grupos, anillos, campos y otras estructuras algebraicas. En otras palabras, condujo al desarrollo del álgebra moderna. Abel trabajó también en análisis, en ecuaciones integrales y desarrolló gran parte de la geometría algebraica.

En 1828, Évariste Galois (1811-1832) presenta una prueba de la imposibilidad de resolver las ecuaciones de grado 5 por radicales, su trabajo fue independiente al de Abel y se basaba en estructuras matemáticas más abstractas, como extensiones de campos y descomposiciones de grupos. Esta prueba de Galois fue una de las aplicaciones de la rama que surgió con su trabajo, ahora llamada *Teoría de Galois*.

La prueba de Galois fue rechazada por Cauchy por tener puntos en común con el trabajo de Abel años antes. Galois siguió trabajando en este y otros temas, en 1830 envía una nueva versión a Cauchy, quien esta vez remitió el artículo a Joseph Fourier (1768–1830), pero Fourier falleció poco después de recibir el trabajo de Galois y éste se traspapeló.

Al morir Galois a temprana edad, su hermano Alfred y su amigo Auguste Chevalier se encargaron de recopilar el trabajo de Évariste y darlo a conocer a la academia, llamando la atención de Liouville. Las obras fueron publicadas en 1846 después de la revisión de Liouville, quien declaró que, en efecto, Galois había resuelto el problema de Abel.

En 1885, los matemáticos John Stuart Glasham, George Paxton Yung y Carl Runge presentan una nueva prueba utilizando el enfoque de teoría de Galois, relacionando las propiedades de una ecuación con sus propiedades algebraicas, como su grupo de Galois, permitiendo hacer la transición del análisis al álgebra. Para mayor detalle, leer (Villa Salvador, 2011).

Hacia el año 1963, el matemático Vladimir Igorevich Arnold (1937-2010) presenta una prueba nueva para el teorema de Abel-Ruffini con un enfoque topológico, que asocia superficies de Riemann a ecuaciones algebraicas, variando sus coeficientes (complejos) y calcular su grupo de monodromía. Arnold presentó esta prueba

a alumnos de bachillerato en Moscú. Uno de los participantes de este taller, V. B. Alekseev plasmó por escrito el contenido de las conferencias en su libro *Abel's theorem in problems and solutions* (Alekseev, 2004). Esta referencia autocontenida introduce fundamentos de teoría de grupos, análisis complejo, superficies de Riemann y grupos de monodromía través de una serie de problemas que se proponen al lector. Este trabajo de graduación se basa en gran medida en desarrollar los detalles de la presentación de (Alekseev, 2004). Se complementa la exposición con el trabajo de Hannah Santa Cruz (Santa Cruz, 2016), donde se enfatiza la noción de monodromía y el artículo de Henryk Zołądek (Zoł, 2000), que da un tratamiento más formal a la demostración propuesta por Arnold.

Otras referencias al tema son (Akalin, 2016) en su entrada *Why is the Quintic Unsolvable?* en el blog "Notes on math, tech, and everything in between", así como (Schwartz, 2015) en su artículo *Abel and the Insolubility of the Quintic*.

El propósito de este trabajo de graduación es presentar, basado en las referencias anteriores, los detalles de la prueba del teorema de Abel-Ruffini de manera que se introduzcan las nociones necesarias para que alumnos, tanto a nivel de licenciatura como de bachillerato, comprendan cada paso de la demostración.

Para ello, se introduce primero, en el Capítulo 1, las nociones y propiedades de grupos finitos, particularmente los grupos de permutaciones y su *solubilidad*. En el Capítulo 2 se presentan las bases de análisis complejo para poder entender el comportamiento de funciones de variable compleja y soluciones de polinomios con coeficientes complejos como ejemplo de funciones algebraicas. Esto permite, en el Capítulo 3, la construcción de *superficies de Riemann* asociadas a estas funciones y su estudio como *espacios de recubrimiento* del pano complejo perforado. Las perforaciones corresponden a los puntos singulares de la función algebraica. Siguiendo la idea central de Arnold, se estudia en el Capítulo 4 qué sucede con las hojas del espacio de recubrimiento cuando rodeamos las singularidades. De esta manera se asocia a la función algebraica un grupo, el *grupo de monodromía*, cuya solubilidad está relacionada con la *solubilidad por radicales* de la ecuación que define la función algebraica.

1. GRUPOS

Una noción esencial en matemática es la de un grupo, esto es un conjunto con una operación asociada que cumple con ciertas propiedades que le dan una estructura. Los grupos son importantes en la prueba del Teorema de Abel-Ruffini, específicamente la solubilidad de los mismos. En este capítulo se estudiará la noción de grupo y sus propiedades, así como operaciones y funciones entre ellos para comprender su solubilidad, con el fin de asociarla con la solubilidad algebraica de un polinomio de grado n.

1.1. Conceptos preliminares

Un conjunto G es una colección de elementos bien definidos. Si consideramos los elementos a_i de un conjunto A y le asignamos elementos b_i de un conjunto B, podemos formar pares (a_i, b_i). Al conjunto de todos los pares de elementos se le llama **producto** de los conjuntos A y B y se denota por $A \times B$. Estos pares pueden escogerse arbitrariamente o relacionarse a través de funciones, como se verá a continuación.

Definición 1.1. Una **función** $f\colon A \to B$ es un conjunto de pares ordenados donde para cada $a \in A$ existe un $b \in B$ tales que $(a, b) \in f$ y si $(a, b') \in f$, entonces $b = b'$.

Al conjunto de elementos de A en la primer coordenada se le llama **dominio** y al conjunto formado por los elementos de la segunda coordenada, se llama **contradominio** o rango. Denotaremos por $f(a)$ al elemento $b \in B$ y lo llamaremos imagen de a bajo f.

Una función $f\colon X \to Y$ puede ser:

- **Inyectiva**: Si dos elementos distintos tienen imágenes distintas, esto es:

$$x_1 \neq x_2 \text{ entonces } y_1 = f(x_1) \neq f(x_2) = y_2.$$

- **Sobreyectiva**: Si para cada $y \in Y$ existe una preimagen $x \in X$ tal que $f(x) = y$.

Definición 1.2. Una función f es **biyectiva** si es inyectiva y sobreyectiva, es decir que cada elemento $y \in Y$ tiene una preimagen $x \in X$ y ésta es única, denotada por $f^{-1}(y)$.

Ejemplo 1.1. Consideremos la función $f\colon \mathbb{Z} \to \mathbb{Z}^+ \cup \{0\}$

$$f(n) = \begin{cases} 2n, & si\ n \geqslant 0 \\ -2n-1, & si\ n < 0. \end{cases}$$

Esta función manda los números no negativos a los enteros pares y los negativos a los impares.

Tomemos $a, b \in \mathbb{Z}$:

a) Si $a \neq b$ con $a \geqslant 0$ y $b \geqslant 0$, entonces

$$f(a) = 2a \neq 2b = f(b).$$

b) Si $a < 0$ y $b < 0$ y $a \neq b$ entonces

$$f(a) = -2a - 1 \neq -2b - 1 = f(b).$$

c) Si $a < 0$ y $b \geqslant 0$ tendrán imágenes $-2a - 1$ y $2b$ respectivamente.

Por los casos anteriores, f es inyectiva.

Consideremos ahora un elemento $c \in \mathbb{Z}^+ \cup \{0\}$.

a) Si c es par, existe un número no negativo $n = c/2$ tal que

$$f(c/2) = 2(c/2) = c.$$

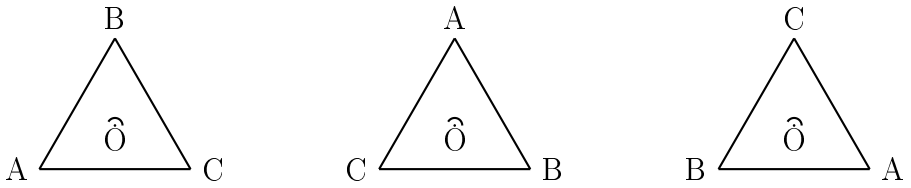
b) Si c es impar, existe un número negativo $n = -\frac{c+1}{2}$ tal que

$$f(-\frac{c+1}{2}) = -2(-\frac{c+1}{2}) - 1 = c.$$

Cualquier elemento en el contradominio tiene una preimagen, afirmando la sobreyectividad. Por lo tanto, f es una función biyectiva.

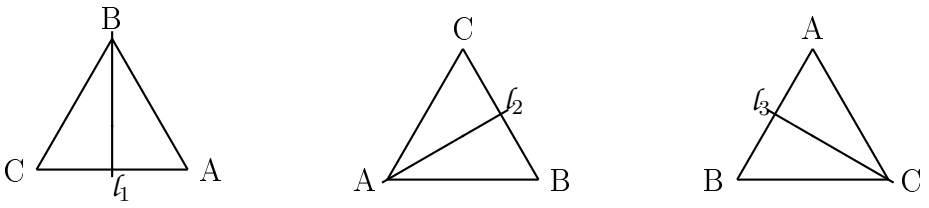
Ejemplo 1.2. Consideremos un triángulo equilátero y las rotaciones o reflexiones de manera que siga siendo el mismo triángulo. Es decir, rotando 120°, 240° y reflejando

con respecto a las alturas del mismo. A cada uno de estos movimientos le llamaremos **simetrías** del triángulo equilátero.



(a) Triángulo **(b)** Rotación 120°. **(c)** Rotación 240°.

Figura 1.1. Rotaciones del triángulo equilátero.



(a) Reflexión con respecto a altura ℓ_1. **(b)** Reflexión con respecto a altura ℓ_2. **(c)** Reflexión con respecto a altura ℓ_3.

Figura 1.2. Reflexiones del triángulo equilátero.

Todas estas simetrías son biyecciones del triángulo en él mismo, ya que se conserva la cantidad de vértices y la figura en el plano.

Definición 1.3. Una función biyectiva de un conjunto X en sí mismo es también llamada **permutación**. Definimos al conjunto de permutaciones como $S_X := \{f\colon X \to X \mid f \text{ es biyección}\}$, es decir, todas las biyecciones de un conjunto en sí mismo.

Ejemplo 1.3. Consideremos $S = \{A, B, C\}$ como el conjunto de vértices de un triángulo equilátero. Las formas de reordenar un arreglo de 3 elementos son biyecciones, por lo que las llamaremos permutaciones. Resulta ser que las simetrías del triángulo equilátero coinciden con todas las permutaciones de sus vértices.

- Rotaciones:

$$a = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, b = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}, e = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

- Reflexiones:

$$c = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}, d = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}, f = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

Llamaremos al conjunto de permutaciones de los vértices del triángulo S_3, las cuales pueden aplicarse una después de otra y siguen siendo una simetría. La operación $\cdot : S_3 \times S_3 \to S_3$ es llamada composición de permutaciones. Esta aplica una transformación luego de otra, así la composición

$$a \cdot f = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} = d$$

y se puede construir una *Tabla de Cayley* de S_3, de la siguiente forma:

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

Tabla 1.1. Composición de simetrías del triángulo equilátero o tabla de Cayley de S_3. Fuente: tomada de (Alekseev, 2004).

Entre las permutaciones existe una única que no modifica al triángulo, la simetría e, que corresponde a la función identidad. En la tabla 1.1 puede observarse que bajo la composición, siempre es posible obtener e al componer dos simetrías.

Ejemplo 1.4. La composición $ab = e$ rotando 120° y luego 240° se obtiene de nuevo la forma inicial del triángulo. Análogamante $ba = e$. Al elemento b le llamaremos **inverso** de a. A continuación estudiaremos estos elementos.

Definición 1.4. sea G un conjunto y $g \in G$, al elemento h tal que $gh = hg = e$ se le llama **inverso** de g y se denota por g^{-1}.

1.2. Grupos

Ya hemos estudiado las permutaciones y algunas de sus propiedades, así, podemos estudiar también las propiedades para un conjunto arbitrario con una operación

definida.

Una operación es una función que toma dos elementos y les asigna un tercer elemento. Cuando al operar dos elementos de un conjunto, siempre el resultado está en el mismo conjunto, se dice que la operación es cerrada.

Ejemplo 1.5. Consideramos la operación resta y el conjunto de números naturales, $\mathbb{N}$. Tomando los pares de elementos en $\mathbb{N} \times \mathbb{N}$, $(8, 5)$ y $(5, 8)$ obtenemos las restas

$$8 - 5 = 3 \text{ y } 5 - 8 = -3,$$

de donde notamos que en los números naturales, la suma es cerrada, mientras la resta es cerrada en los enteros, mas no en los naturales.

Definición 1.5. Sea G un conjunto con una operación $\cdot$ que satisface:

1. *Cerradura o clausura*: Para cualesquiera elementos $x, y \in G$, la operación $xy \in G$.

2. *Asociatividad*: Para cualesquiera elementos $x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

3. *Elemento neutro*: Existe un elemento $e \in G$ tal que $e \cdot a = a \cdot e = a$ para cada $a \in G$.

4. *Existencia de inversos*: Para cada $a \in G$ existe un elemento $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Entonces se dice que este conjunto forma un **grupo** bajo la operación $\cdot$ y es denotado por (G,$\cdot$) o simplemente *el grupo* G.

Si la operación es conmutativa, el grupo se llama **grupo abeliano**.

Ejemplo 1.6.

1. El grupo trivial es el conjunto $\{e\}$ formado por el elemento neutro con cualquier operación.

2. $(\mathbb{Z}, +)$ los números enteros con la operación adición forman un grupo abeliano.

3. S_2 el grupo de permutaciones de dos elementos con la composición.

Ejemplo 1.7. En el ejemplo 1.2, vimos que la composición de permutaciones (simetrías del triángulo equilátero) es cerrada y que todos sus elementos tienen un

inverso. Su elemento neutro es

$$e = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

y es único. Y falta considerar la asociatividad, de la tabla 1.1, tenemos

$$a(db) = ac = f \text{ y}$$

$$(ad)b = cb = f \text{ por lo que}$$

$$a(db) = (ad)b$$

y esto se puede verificar para cualesquiera tres elementos en S_3, la operación es asociativa.

Por lo tanto S_3 con la composición es un grupo, llamado **grupo simétrico** de 3 elementos.

Definición 1.6. En general para un conjunto X, S_X con la composición, forman un grupo, llamado **grupo de simetrías** de X. Particularmente, para arreglos de n elementos $(1, 2, 3, \ldots, n)$ pueden considerarse todas las permutaciones posibles de este arreglo. Al grupo formado con el conjunto de todas estas permutaciones con la operación composición, se le llama **grupo simétrico** de n elementos, denotado por S_n y tienen $n!$ elementos. Estos grupos no son abelianos cuando $n > 2$, como se mostrará en el lema 1.4.1.

Al considerar cada elemento del arreglo como un vértice de un n-gono regular. Se obtiene que dentro del conjunto de permutaciones, las que conservan la figura corresponden a rotaciones del mismo y reflexiones respecto a sus alturas. Estas simetrías también forman un grupo, llamado **grupo diédrico** y se denotará por D_n.

En el caso $n = 3$ se cumple que $S_3 = D_3$. En la sección 1.6 estudiaremos los grupos simétricos finitos.

Definición 1.7. A la cantidad de elementos de un se le llama **orden del grupo** y se denota por $\circ(G)$. Existen tanto grupos finitos como infinitos.

Ejemplo 1.8. Consideremos ahora a $(\mathbb{Z}, \cdot)$. Este no forma un grupo, ya que dado un entero a, su inverso multiplicativo a^{-1} no es un entero. Por otro lado, si consideramos a todos los reales menos el cero $(\mathbb{R} \setminus \{0\}, \cdot)$, esta propiedad se cumple y por lo tanto es un grupo abeliano de orden infinito.

Existen ciertas propiedades que caracterizan a un grupo, estas son:

1. El elemento neutro es único En efecto, si existen dos neutros, digamos e y $\hat{e}$, se tiene que:

$$ea = ae = a = \hat{e}a = a\hat{e}, \text{ de donde:}$$

$$ea = \hat{e}a = a, \text{ entonces } e = \hat{e}.^{1}$$

2. El inverso de un elemento es único. Sean a^{-1} y b inversos del elemento a, se tiene $aa^{-1} = a^{-1}a = e = ab = ba$, entonces

$$a^{-1}a = ba, \text{ lo que implica que } a^{-1} = b.$$

3. $(ab)^{-1} = b^{-1}a^{-1}$ y, en general,

$$(a_1a_2...a_n)^{-1} = a_n^{-1}...a_2^{-1}a_1^{-1}.$$

Un elemento en un grupo G puede operarse cualquier cantidad de veces, en este caso, $a \in G$ operado n veces se escribe a^n. Y dados los elementos de un grupo, operados con ellos mismos, se tienen las siguientes propiedades (puede verse la prueba en (Dummit y Foote, 2004), capítulo 1):

- $(a^{-1})^{-1} = a$.
- $(a^m)^{-1} = (a^{-1})^m$.
- $a^m \cdot a^n = a^{m+n}$.
- $(a^m)^n = a^{mn}$.
- Si $m < 0$, $a^m = (a^{-m})^{-1}$.

De la última propiedad, podemos afirmar que las anteriores valen para cada $m, n \in \mathbb{Z}$.

Definición 1.8. En algunos grupos puede suceder que existe un k, tal que $a^k = e$, al mínimo entero k (distinto de cero) que cumple esto, se le llama **orden del elemento** a en un grupo, denotado por $\circ(a)$.

[1] Por la ley de cancelación:

$$\text{Si } ab = ac \text{ entonces } b = c,$$

esto es fácil de comprobar, multiplicando por el inverso de a en ambos lados de la ecuación.

Definición 1.9. Si el orden de un elemento a es n, entonces todos los elementos $e, a, a^2, \ldots, a^{n-1}$ son distintos. Y si estos son todos los elementos que conforman al grupo, se dice que es un **grupo cíclico** de orden n, generado por a. Al elemento a se le llama **generador** del grupo y denotaremos a $G = \{e, a, a^2, \ldots, a^{n-1}\}$ por $G = \langle a \rangle$.

Si el orden de un grupo cíclico generado por a es infinito, lo escribiremos de la forma $\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$.

Ejemplo 1.9. El grupo $(\mathbb{Z}, +) = \langle 1 \rangle$ es un grupo cíclico infinito, cuyo generador es 1.

Ejemplo 1.10. Las rotaciones de un n-gono regular, con la composición, forman un grupo cíclico de orden n cuyo generador es la rotación de $360°/n$ (otros generadores pueden ser aquellos con rotaciones de $m * 360°/n$ donde m es primo relativo con n).

Los grupos cíclicos (de orden n) cumplen con las siguientes propiedades:

1. $a^m = e$ si y sólo si $m = nd$.

   Supongamos que, por el algoritmo de la división[2], $m = nd + r$, entonces:

   $$e = a^m = a^{nd+r} = a^{nd}a^r = (a^n)^d a^r = (e)^d a^r = a^r.$$

   Pero r no excede a n, lo cual contradice que n es el orden de a, $a^r = e$ si y sólo si $r = 0$, así $m = nd$.

2. Si $\text{mcd}(m, n) = d$ y el orden de a es n, el orden de a^m es n/d.

   Dado que $d|m$ y $d|n$, se puede escribir $m = \alpha d$ y $n = \beta d$ y se tiene que:

   $$(a^m)^{n/d} = a^{mn/d} = (a^n)^{m/d} = (a^n)^\alpha = e^\alpha = e.$$

   Si se toma un entero arbitrario p tal que $(a^m)^p = a^{mp} = e$, esto se cumple si y sólo si $n \mid mp$, entonces $n/d \mid mp/d$, y como $\alpha = m/d$ y $\beta = n/d$ son primos relativos, entonces $n/d|p$, por lo tanto n/d es el mínimo p tal que $(a^m)^p = e$, es decir, n/d es el orden de a^m.

Ejemplo 1.11. Al dividir un entero m entre n, este número genera residuos r tales que $0 \leqslant r < n$ de manera que el número m se escribe como $m = nd + r$ donde r es el

[2]El algoritmo de la división asegura que al dividir un natural m entre uno n se obtendrá una única representación de m, a decir, $m = nd + r$ donde r es un residuo que no excede a n.

residuo. Estos residuos bajo adición forman un grupo cíclico, que puede observarse con mayor claridad en la siguiente tabla:

·	0	1	2	3	...	n-1
0	0	1	2	3	...	n-1
1	1	2	3	4	...	0
2	2	3	4	5	...	1
3	3	4	5	6	...	2
⋮	⋮	⋮	⋮	⋮	⋱	⋮
n-1	n-1	n	0	1	...	n-2

Tabla 1.2. Tabla de Cayley de los residuos módulo n.

A partir de dos grupos puede obtenerse un tercer definido por los grupos, G y H.

Definición 1.10. El **producto directo** de los grupos G y H, denotado por $G \times H$ es el conjunto de pares ordenados (g, h) donde $g \in G$ y $h \in H$ y tiene un producto definido por:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2),$$

donde el producto $g_1 g_2$ es un elemento del grupo G y $h_1 h_2$, del grupo H.

Es fácil observar que $G \times H$ es un grupo con elemento neutro (e_G, e_H) y para cada $(g, h) \in G \times H$, su inverso $(g, h)^{-1}$ es (g^{-1}, h^{-1}). Si G y H son grupos finitos, se cumple $\circ(G \times H) = \circ(G) \circ (H)$.

1.2.1. Homomorfismos e isomorfismos de grupos

Ahora estudiaremos las funciones y tipos de relaciones entre grupos y qué propiedades de grupos se conservan de acuerdo a la función entre ellos.

Definición 1.11. Si consideramos un función entre dos grupos, ϕ: $G \to F$ tal que $\phi(ab) = \phi(a)\phi(b)$ se dice que ϕ es un **homomorfismo** de los grupos G y F. Llamaremos **imagen** de G bajo ϕ al conjunto de elementos en F de la forma $\phi(g)$.

En un homomorfismo, $\phi : G_1 \to G_2$ se preservan propiedades de grupos como:

1. **Elemento neutro**: es decir que la imagen bajo isomorfismo de e_1 es el elemento e_2 ya que por ser isomorfismo, se tiene

$$\phi(a) = \phi(ae_1) = \phi(a)\phi(e_1).$$

Y esto se cumple sólo si y sólo si la imagen $\phi(e_1) = e_2$.

2. **Elementos inversos**: La imagen del inverso de un elemento es el inverso de la imagen de ese elemento.

   Sabemos que $\phi(aa^{-1}) = \phi(a)\phi(a^{-1})$ y $\phi(e_1) = e_2$, entonces

   $$\phi(e_1) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = e_2 = \phi(a)\left[\phi(a)\right]^{-1}.$$

3. **Orden de un elemento**: $\phi(a)$ y a tienen el mismo orden. Supongamos que $\circ(a) = n$ y $\circ(\phi(a)) = m$, entonces:

   Sabemos que $a^n = e_1$ y $\phi(e_1) = e_2$, entonces

   $$\phi(a)^n = \phi(a) \cdot \phi(a) \cdot ... \cdot \phi(a) = \phi(a^n) = \phi(e_1) = e_2 \text{ de donde } m \leqslant n.$$

   De forma similar,

   $$\phi(e_1) = e_2 = \phi(a)^m = \phi(a^m), \text{ esto implica que } x^m = e_1,$$

   $$\text{entonces } n \leqslant m \text{ por definición de } \circ(a).$$

Proposición 1.1. *La composición de homomorfismos es también un homomorfismo.*

Demostración. Sean $\phi\colon G \to F$ y $\psi\colon F \to H$ homomorfismos de grupos. Tomando elementos $a, b \in G$, y la composición $(\psi\phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b))$, donde $\phi(a), \phi(b) \in F$, entonces $\psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b))$, de donde vale que la afirmación. □

Definición 1.12. Si el homomorfismo $\phi : G_1 \to G_2$, aparte de cumplir para cada a, $b \in G_1$

$$\phi(ab) = \phi(a) \cdot \phi(b),$$

también es biyectivo, se dice que es un **isomorfismo**.

Los elementos $\phi(a)$ y $\phi(b)$ pertenecen al grupo G_2. El inverso de un isomorfismo, $\phi^{-1}\colon G_2 \to G_1$ es también un isomorfismo, como consecuencia de la biyectividad. Se escribirá $G_1 \cong G_2$ cuando el grupo G_1 sea isomorfo al grupo G_2.

Ejemplo 1.12. Todo grupo cíclico de orden n es *isomorfo* al grupo de residuos módulo n bajo adición, bajo el la función $\varphi\colon \mathbb{Z} \to \langle a \rangle$ tal que $m \mapsto a^m$. Estos grupos se denotarán por $\mathbb{Z}_n$

En los ejemplos 1.11 y 1.12 trabajamos con los grupos $\mathbb{Z}_n$, a continuación veremos una afirmación importante con estos grupos.

Proposición 1.1. $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ si y sólo si m y n son primos relativos.

Demostración.

($\Leftarrow$) Si m, n son primos relativos, $\text{mcm}(m,n) = mn$. Consideremos el elemento $(1,1)$, donde $k(1,1) = (0,0)$ sólo si k es múltiplo de m y n, de donde $\circ((1,1)) = mn$. Por lo tanto el grupo $\langle(1,1)\rangle$ es el grupo cíclico $\mathbb{Z}_m \times \mathbb{Z}_n$ de orden mn.

($\Rightarrow$) Si $\text{mcd}(m,n) = d > 1$ podemos considerar un elemento $(r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ y sea $k = {}^{mn}/_{d}$, se tiene que

$$k(r,s) = (0,0)$$

para cualesquiera r, s. De donde cualquier elemento tendría orden menor a mn. Entonces $\text{mcd}(m,n)$ debe ser 1. □

Proposición 1.2. Todo grupo cíclico de orden infinito es isomorfo a $(\mathbb{Z}, +)$.

Demostración. Consideremos un grupo cíclico infinito $G = \langle g \rangle$ y la función $\varphi\mathbb{Z} \to G$ tal que $n \mapsto g^n$, es decir, $\varphi(n) = g^n$.

Probaremos que φ es biyectivo.

Sean $m, n \in \mathbb{Z}$, tales que $\varphi(m) = \varphi(n)$, entonces

$$g^m = g^n,$$

de donde

$$g^{m-n} = e,$$

dado que $\circ(g) = \infty$, el único valor posible para $m - n$ es cero, lo que implica que $m = n$. Entonces φ es inyectiva.

Por otro lado, $G = \{g^n \mid n \in \mathbb{Z}\}$, es decir que cada elemento de G es la imagen de al menos un número entero. Esto significa que φ es sobreyectiva.

Por lo tanto, φ es una biyección y $G \cong (\mathbb{Z}, +)$. Dada la arbitrariedad de G, esto se cumple para todo grupo cíclico infinito. □

Ejemplo 1.13. El grupo de rotaciones del triángulo equilátero es isomorfo a $\mathbb{Z}_3$, asignando $\phi(k) = a^k$, con $k = 0, 1, 2$.

Un isomorfismo es una relación de equivalencia, es decir, cumple:

- Es reflexiva ($G \cong G$).

- Es simétrica (si $G_1 \cong G_2$ entonces $G_2 \cong G_1$).
- Es transitiva (si $G_1 \cong G_2$ y $G_2 \cong G_3$ entonces $G_1 \cong G_3$). Esta última propiedad es consecuencia de que la composición de isomorfismos es isomorfismo.

1.3. Subgrupos

Un grupo es diferente de un conjunto ordinario porque está dotado de una operación binaria sobre todo el conjunto, por lo que es natural preguntarse qué sucede con los subconjuntos del mismo. Para responder esto, estudiaremos qué propiedades cumplen los subconjuntos bajo la operación del conjunto original.

Definición 1.13. Sea $(G, \cdot)$ un grupo y $H \subseteq G$. Si $(H, \cdot)$ es en sí mismo un grupo, se dice que H es un **subgrupo** de G y se denota por $H \leqslant G$. Cuando $H \subset G$, es decir, es un subconjunto propio de G, el subgrupo se denota como $H < G$.

Todo grupo G tiene dos subgrupos triviales, estos son todo G y el conjunto unitario que contiene al elemento neutro, $\{e\}$. También pueden generarse **subgrupos cíclicos**, dado $a \in G$, de la forma $\langle a \rangle = \{e, a, a^2, a^{n-1}\}$, con $0 \leqslant n < \circ(g)$.

Para mostrar que $H \leqslant G$, sólo es necesario comprobar la existencia del elemento neutro e inversos en H, ya que la operación definida en G es válida para todo el G.

Teorema 1.3.1 (Caracterización de subgrupos)**.** *$H < G$ si y sólo si:*

1. *Si $a, b \in H$, entonces $ab \in H$.*
2. *$e \in H$.*
3. *Si $a \in H$, entonces $a^{-1} \in H$.*

Tanto el elemento neutro como los inversos, coinciden en H y en G.

Demostración.

($\Rightarrow$) Si H es subgrupo entonces es un grupo y vale que la operación es cerrada en H, además tiene un elemento e tal que para cada $a \in H$, $ae = ea = a$, y ya que $e \in G$ es el único elemento que cumple estas propiedades, entonces e es el mismo en G y H. Como el elemento neutro coincide y H mismo es un grupo, los inversos $a^{-1} \in H$ para cada $a \in H$.

($\Leftarrow$) Dada $\cdot$ operación cerrada en H con un elemento neutro $e \in H$, para cada $a \in H$, $a \in G$ se sigue cumpliendo

$$ea = ae = a \quad \text{para cada } a \in H$$

Y si $a \in H$ y $a^{-1} \in H$ tenemos

$$aa_H^{-1} = e = aa_G^{-1},$$

de donde $a_G^{-1} = a_H^{-1} = a^{-1}$, por lo que H es un grupo y entonces $H < G$. □

Ejemplo 1.14. Las rotaciones de un n-gono son un subgrupo de todas las simetrías del mismo.

Ejemplo 1.15. Sean G_1 y G_2 dos grupos y $H_1 < G_1$, $H_2 < G_2$. El producto $H_1 \times H_2 < G_1 \times G_2$.

Como H_1 y H_2 son grupos, tienen elemento neutro $\{e_1\}$ y $\{e_2\}$ respectivamente, así como los inversos de cada elemento. De donde el elemento neutro de $H_1 \times H_2$ es (e_1, e_2) y los inversos, de la forma (a_1^{-1}, a_2^{-1}), entonces $H_1 \times H_2 < G_1 \times G_2$.

Para cada subgrupo $H < G$ existe una partición de G en subconjuntos. Una partición es inducida por una clase de equivalencia, es decir, que separa elementos o subconjuntos por clases. Cada clase es disjunta de la otra.

Definición 1.14. Sea G un grupo y $H < G$. Para cada elemento $g \in G$, consideremos los conjuntos de la forma $gH = \{gh \mid h \in H\}$. A este conjunto se le llama **clase lateral izquierda**[3] de H, generada por g. Y análogamente, llamamos **clase lateral derecha** al conjunto $Hg = \{hg \mid h \in H\}$.

Ejemplo 1.16. Consideremos al grupo de simetrías del triángulo equilátero y el subgrupo $\{e, c\}$ donde c es una reflexión, como en el ejemplo 1.3. Este es un subgrupo, ya que $c^2 = e$, y es un grupo de orden 2, por lo que es isomorfo a $\mathbb{Z}_2$. Entonces la clase lateral izquierda generada por el elemento a (rotación de 120^o) es:

$$aH = \{ae, ac\} = \{a, f\}$$

y la clase lateral derecha generada por el mismo elemento es:

$$Ha = \{ea, ca\} = \{a, d\}.$$

Algunas propiedades de las clases laterales son:

Lema 1.3.1. *Sea $H \leqslant G$.*

1. *Todo elemento de G pertenece a alguna clase lateral de H.*

[3] La función $f\colon H \to gH$ tal que $h \mapsto gh$ es biyectiva.

2. *Si* $y \in xH \Rightarrow yH = xH$.

3. *Si* xH *y* yH *tienen un elemento en común, entonces son iguales.*

Demostración.

1. Dado que $e \in H$ para cualquier $H < G$, cada $g \in G$ generará una clase gH donde $ge = g$, entonces $g \in gH$ y el resultado es análogo para las clases laterales derechas.

2. Sea $y \in xH$, entonces $y = xh$ para algún $h \in H$, de donde $yh^{-1} = x$, entonces $x \in yH$y, por lo tanto, $xH = yH$.

3. Basta tomar $x \neq y$ tal que $x \in yH$ y, por inciso anterior, $xH = yH$. □

De esto puede concluirse que:

- $G = \underset{a_i \in G}{\cup} a_i H$.
- $a_i H \cap a_j H = \emptyset$ para cada $i \neq j$.

Es decir, las clases (izquierdas) son disjuntas o iguales y forman una partición del conjunto G. Esto es cierto también para las clases derechas.

Proposición 1.3. Sea G un grupo y $H_i < G$ una familia de subgrupos. La intersección arbitraria de subgrupos H_i es un subgrupo de G.

Demostración. Sabemos que $\bigcap_i H_i$ es al menos $\{e\}$ por definición de subgrupo. Si $\bigcap_i H_i \neq \{e\}$ entonces existe al menos un $a \in \bigcap_i H_i$, es decir, $a \in H_i$ para cada H_i:

a) Si $a = a^{-1}$, entonces $\bigcap_i H_i \cong Z_2$, es un grupo.

b) Si $a \neq a^{-1}$, entonces existe un $b \in \bigcap_i H_i$, donde $ab \in \bigcap_i H_i$ y además $a^{-1} \in \bigcap_i H_i$ por definición de grupo en cada H_i.

Por lo tanto $\bigcap_i H_i \leqslant G$. □

Ejemplo 1.17. Regresando al ejemplo 1.16, con la notación del ejemplo 1.3. Se procederá a encontrar tanto las clases izquierdas como derechas del subgrupo $H = \{e, c\}$ del grupo de simetrías del triángulo. Recordando que el grupo $G = \{e, a, b, c, d, f\}$.

Izquierda	Derecha
$aH = \{a, f\}$	$Ha = \{a, d\}$
$bH = \{b, d\}$	$Hb = \{b, f\}$
$cH = \{c, e\}$	$Hc = \{c, e\}$

Por los resultados anteriores se sabe que $aH = fH$, $bH = dH$ y $cH = eH = H$; así mismo, $Ha = Hd$, $Hb = Hf$ y $Hc = He = H$.

Y resulta ser que todas las clases tienen el mismo orden que el subgrupo H y este número cumple con la siguiente afirmación:

Teorema 1.3.2 (Lagrange)**.** *Sea G un grupo finito y $H < G$. El orden de todo subgrupo H divide al orden del grupo G. Esto es $\circ(H) \mid \circ(G)$.*

Demostración. Sabemos que $G = \underset{a_i \in G}{\cup} a_i H$ donde cada clase es disjunta y $\circ(aH) = \circ(H)$ ya que son biyecciones, como se observó en la nota de la definición 1.14. Entonces $\circ(G) = \sum_{a_i \in G} \circ(a_i H)$ sobre los representantes (sin repeticiones). Dado que cada clase es de orden $\circ(H)$, se tiene que $o(G) = k \circ (H)$. Por lo tanto $\circ(H) \mid \circ(G)$. □

Al cociente $\frac{\circ(G)}{\circ(H)}$ se le llama **índice del subgrupo** H y se denota por $[G : H]$.

El teorema de Lagrange tiene como consecuencia:

Corolario 1.3.1. *Sea G un grupo finito y $a \in G$. El orden de todo elemento $a \in G$ divide al orden del grupo.*

Demostración. Supongamos que $\circ(a) = m$ para algún $g \in G$ entonces generará un subgrupo H de la forma $H = \{e, a, a^2, \ldots, a^{m-1}\}$ que es cíclico, y además, $\circ(H) = m$ y por el teorema 1.3.2, $\circ(H) | \circ(G)$ así, $\circ(g) | \circ(G)$. □

Proposición 1.2. *Un grupo G de orden primo es cíclico y cualquier elemento (distinto de e) puede ser su generador.*

Demostración. Si el grupo es de orden primo, digamos p, por el teorema 1.3.2 se tiene que cada subgrupo tendrá únicamente 1 elemento o p elementos. Por consiguiente, $H = \{e\}$ o $H = G$ y sabemos que al tomar un elemento $g \neq e \in G$ sus potencias generarán un subgrupo cíclico de la forma $H = \{e, a, a^2, \ldots, a^{p-1}\} = G$ entonces G cíclico. □

Proposición 1.3. *Todos los grupos de orden p donde p es un número primo son isomorfos.*

Demostración. Si se tienen dos grupos G_1 y G_2 de orden p, se tiene que son cíclicos del mismo orden, entonces se puede construir una biyección $\phi : G_1 \to G_2$ de manera que si $G_1 = \{e, a_1, a_1^2, \ldots, a_1^{p-1}\}$ y $G_2 = \{e, a_2, a_2^2, \ldots, a_2^{p-1}\}$, los asociamos de la siguiente manera:

$$\phi(a_1) = a_2,$$

entonces se cumple

$$\phi(a_1^m a_1^n) = \phi(a_1^{m+n}) = a_2^{m+n} = a_2^m a_2^n = \phi(a_1^m)\phi(a_1^n).$$

Y concluimos que $G_1 \cong G_2$. □

Todos los grupos están relacionados con subgrupos de un grupo de permutaciones, como afirma el siguiente teorema:

Teorema 1.3.3 (Cayley)**.** *Todo grupo es isomorfo a un subgrupo de un grupo de permutaciones.*

Demostración. Consideremos la función $\psi\colon G \to S_G$ dada por $\psi(a) = \varphi_a$, donde $\varphi_a\colon G \to G$ tal que $x \mapsto ax$.

Comenzaremos mostrando que ψ está bien definida, es decir, que φ_a es una biyección.

Si $\varphi_a(x) = \varphi_b(x)$, tenemos

$$ax = bx$$

y por la ley de cancelación,

$$a = b.$$

Por otro lado, dado $\varphi_a(x) = ax$ para cada $x \in G$, la imagen de esta función son $\circ(G)$ elementos distintos. Como G es un grupo, entonces cada elemento tiene una preimagen. Por lo tanto, ψ es una biyección.

Para concluir, basta mostrar que ψ es un homomorfismo inyectivo y que su imagen es un subgrupo de S_G.

Dado $\psi(a) = \varphi_a(x)$, se tiene

$$\psi(ab) = \varphi_{ab}(x) = abx = a(bx) = \varphi_a\varphi_b(x)$$

y es inyectivo ya que φ_a lo es.

Dada la definición de $\psi(a) = \varphi_a(x)$, entonces

$$Im(\psi) = \varphi_a(G) \subset S_G. \quad \square$$

Lema 1.3.2. *Los isomorfismos de un grupo con la composición forman un grupo.*

Demostración. En la proposición 1.1 se probó que la composición de homomorfismos es cerrada y de las propiedades de los isomorfismos, sabemos que conservan elementos neutros y por ser biyecciones, tienen inversos. La asociatividad puede probarse de manera similar a la composición de permutaciones. Entonces es un grupo. □

Definición 1.15. A los isomorfismos $\phi\colon G \to G$ los llamaremos **automorfismos** de G y se denotarán por $\mathrm{Aut}(G)$. Y a los automorfismos de la forma $\phi\colon G \to G$ de la forma $\phi_a = axa^{-1}$ se les llama **automorfismos internos**, denotados por $\mathrm{Inn}(G)$.

Nota 1.1. $\mathrm{Aut}(G)$ con la composición forman un grupo. Este es un caso particular del lema 1.3.2, donde se probó que todos los isomorfismos de grupos con la composición son un grupo. En este caso, estamos considerando los isomorfismos de un grupo en él mismo.

En el caso $\mathrm{Inn}(G)$, mostramos que de hecho son automorfismos:
Consideremos $\phi_{ab}\colon G \to G$ tal que $x \mapsto (ab)x(ab)^{-1}$, entonces

$$\phi_{ab} = abx(ab)^{-1} = abxb^{-1}a^{-1} = \phi_a(bxb^{-1}) = \phi_a(\phi_b(x)) = \phi_a\phi_b(x) \in \mathrm{Inn(G)}.$$

ϕ_{ab} es un automorfismo para cualquier par de elementos $a, b \in G$. Así, la composición es cerrada en $\mathrm{Inn}(G)$, de donde $\mathrm{Inn}(G) < \mathrm{Aut}(G)$.

Ejemplo 1.18. Consideremos el grupo de simetrías del triángulo equilátero, donde cada vértice tiene una etiqueta (A, B, C). Al multiplicar dos simetrías, se obtiene una nueva simetría, que es una permutación de las letras A, B y C. De esta forma, existe un isomorfismo entre las simetrías del triángulo equilátero y las permutaciones de las 3 letras. Pero el isomorfismo no está definido de manera única, ya que depende de cómo sean colocadas las letras A, B y C en cada vértice.

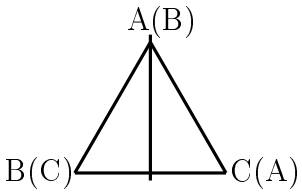


Figura 1.3. Cambio de notación en los vértices de un triángulo equilátero

Como se muestra en la figura, se cambió el orden de las etiquetas y esto fue a través de la permutación

$$g = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

a la cual llamaremos nueva notación. Sea h la permutación correspondiente a la altura trazada en la figura 1.3, obtenemos

$$\begin{array}{rccc} \text{original :} & (A,B,C) & \overset{h}{\mapsto} & (A,C,B) \\ \text{nueva notación :} & (B,C,A) & \overset{h}{\mapsto} & (C,B,A) \end{array}$$

Obteniendo de esta forma las permutaciones g y gh respectivamente. Se desea averiguar cómo se ve el cambio de notación g tras la permutación h. Para ello se necesita regresar a la notación original, esto es, aplicar g^{-1}, teniendo la notación original, realizamos la permutación h, obteniendo el producto hg^{-1} y por último, se cambia de notación. El producto final es ghg^{-1}, que es un automorfismo interno.

Cada subgrupo bajo un automorfismo interno es, en general, distinto del original, por ejemplo si tomamos un subgrupo que consta de la identidad y la reflexión con respecto a una altura del triángulo equilátero, un automorfismo interno lo enviará al subgrupo que contiene a la identidad y la reflexión con respecto a otra altura. Sin embargo, existen grupos que son invariantes bajo automorfismos internos, llamados subgrupos normales, como el subgrupo de rotaciones del triángulo.

Ejemplo 1.19. Para encontrar los automorfismos del grupo $H = \{e, c\} < S_3$. Calculamos únicamente los elementos generados con la reflexión c, ya que $aea^{-1} = e$ para cada $a \in G$:

$aca^{-1} = acb = d$

$bcb^{-1} = bca = f$

$ccc^{-1} = c^3 = c$

$dcd^{-1} = dcd = f$

$fcf^{-1} = fcf = d$

Donde f, d, c son las permutaciones que corresponden a las reflexiones con respecto a las 3 alturas del triángulo equilátero. Obteniendo así, los subgrupos: $aHa^{-1} = fHf^{-1} = \{e, d\} < G$, $bHb^{-1} = dHd^{-1} = \{e, f\} < G$ y $cHc^{-1} = H < G$.

Definición 1.16. Sea G un grupo y $H < G$ tal que la imagen de H bajo todos los automorfismos internos es él mismo, se dice que H es un **subgrupo normal** de G, es decir H es subgrupo normal de G si para todo $a \in H$ y para todo $g \in G$, el elemento $gag^{-1} \in H$. Si H es subgrupo normal de G, se escribe $H \lhd G$.

De esto se deriva el siguiente resultado:

Proposición 1.4. *H es un subgrupo normal de G si y sólo si sus clases laterales izquierdas coinciden con las derechas, es decir $gH = Hg$.*

Demostración.

($\Rightarrow$) Si $H \lhd G$, para cada $g \in G$ y para cada $h \in H$, como es invariante bajo $\mathrm{Inn}(H)$, cada $\phi_g(a) = gag^{-1} = b$ donde $a, b \in H$, entonces $ga = bg$, donde $ga \in gH$ y $bg \in Hg$, como es el mismo elemento, se cumple $gH = Hg$.

($\Leftarrow$) Sea $a \in N$ y $g \in G$ elementos arbitrarios, como $gH = Hg$, entonces $ga \in gN$ y $ga \in Ng$, es decir que existe $b \in N$ tal que $ga = bg$, de donde $gag^{-1} \in N$ y dada la arbitrariedad de los elementos escogidos, $N = gNg^{-1}$, es decir $N \lhd G$. □

Proposición 1.5. Inn(G) $\lhd$ Aut(G).

Demostración. Sabemos (ver nota 1.1) que $InnG < \mathrm{Aut}(G)$, falta mostrar que es normal. Sea $a \in G$ probaremos que $a\mathrm{Inn}(G)a^{-1} = \mathrm{Inn}(G)$.

Tomemos un elemento arbitrario $bgb^{-1} \in \mathrm{Inn}(G)$ y el producto

$$a(bgb^{-1})a^{-1} = ab(g)b^{-1}a^{-1} = (ab)g(ab)^{-1}$$

es un nuevo automorfismo interno, entonces es una biyección de $\mathrm{Inn}(G)$ es $\mathrm{Inn}(G)$. Por lo que $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$. □

Por el teorema 1.3.2 sabemos que el orden de todo subgrupo divide al de un grupo. Cuando el número que resulta al dividir el orden del grupo por el del subgrupo es 2, este subgrupo siempre es normal, en otras palabras:

Proposición 1.6. *Todo subgrupo de índice 2 es normal.*

Demostración. Sea $\circ(G) = m$ y $\circ(H) = m/2$, consideremos $H = \{a_1, a_2, \ldots, a_{n/2}\}$ entonces $H^c = \{a_{n/2+1}, a_{n/2+1}, \ldots, a_m\}$. Se tiene que la partición divide a los elementos que estén o no en H. Dado $g \in G$, $g \in H$ si y sólo si $gH = H = Hg$, mientras si $g \notin H$, implica que $g \in gH = G - H$ con las particiones izquierdas, y análogamente, $g \in Hg = G - H$, de donde $gH = Hg$, es decir $H \lhd G$. □

Todo subgrupo de un grupo G genera una partición, como se vio en 1.3.1 y cuando $H \lhd G$ esta es una relación de equivalencia.

Si definimos una operación $*$ entre estas clases, tal que si $x_1, x_2 \in x_1H$ y $y_1, y_2 \in y_1H$ donde x_1H, y_1H son clases de la partición generada por el subgrupo normal H, los productos x_1y_1 y x_2y_2 pertenecen a la misma clase.

Sabemos que $x_2 \in x_1H$ y $y_2 \in y_1H$, entonces existen $a, b \in H$ tales que $x_2 = ax_1$ y $y_2 = y_1b$, como $y_1H = Hy_1$, entonces existe $c \in H$ tal que $ay_1 = y_1c$.

así, el producto $x_2y_2 = x_1ay_1b = x_1y_1bc$, como $bc \in H$, entonces $x_2y_2, x_1y_1 \in x_1y_1H$.

De esta forma, multiplicando dos elementos en distintas clases de partición, se genera el producto: Sea $A = xH$, $B = yH$, $A * B = xyN$.

Definición 1.17. La partición generada por $H \lhd G$ con la operación definida anteriormente entre elementos de dicha partición, es denotada por G/H y se llama **grupo cociente** de G por H.

A continuación, se verificará que los elementos del grupo cociente bajo esta operación forman un grupo.

1. Sean T_1, T_2, T_3 clases laterales, y supongamos que $T_i = x_i N$ $(i \in [1,3])$, entonces
$$(T_1 * T_2) * T_3 = (x_1 H x_2 H)x_3 H = (x_1 x_2 H)x_3 H$$
$$= x_1 x_2 x_3 H = x_1 H(x_2 x_3 H) = T_1 * (T_2 * T_3).$$

2. Sea H un subgrupo normal y T una clase lateral tal que $T = bH = Hb$ para algún $b \in G$ entonces
$$HT = HbH = (eb)H = H(eb) = Hb = T = bH = (be)H = bHeH = TH,$$
por lo tanto, $HT = T = TH$.

3. Para toda clase lateral T existe T^{-1} tal que $TT^{-1} = T^{-1}T = H$ Sea $H = eH = He$ y $T = aH$, $a \in G$
$$\left.\begin{array}{l} eH = (aa^{-1})H = aHa^{-1}H = Ta^{-1}H \\ eH = (a^{-1}a)H = a^{-1}HaH = a^{-1}HT \end{array}\right\} \text{Donde } a^{-1}H \text{ es la clase } T^{-1}.$$

Ejemplo 1.20. Consideremos ahora al grupo de rotaciones del triángulo equilátero como subgrupo de las simetrías del mismo. Los grupos cocientes serán:

Dado $G = \{e, a, b, c, d, f\}$ y $H = \{e, a, b\}$, se tiene que $G/H = \{\{e, a, b\}, \{c, d, f\}\}$ o bien, las clases de equivalencia de los elementos $[a] = aH = H$ y $[c] = cH$ entonces $G/H = \{H, cH\} = \{H, H^c\}$, donde H^c es el complemento de H.

Los grupos cocientes cumplen las siguientes propiedades, ver demostración en (Dummit y Foote, 2004):

1. $G/\{e\} \cong G$.

2. $G/G \cong \{e\}$.

3. $(G_1 \times G_2)/(G_1 \times \{e\}) \cong G_2$ y $(G_1 \times G_2)/(\{e\} \times G_2) \cong G_1$.

4. Si $H_1 \lhd G_1$ y $H_2 \lhd G_2$, entonces $(G_1 \times G_2)/(H_1 \times H_2) \cong G_1/H_1 \times G_2/H_2$.

Definición 1.18. En un grupo G, dos elementos $a, b \in G$ conmutan si $ab = ba$. Cuando estos no conmutan, su grado de no conmutatividad puede medirse con el producto $aba^{-1}b^{-1}$. Este producto es llamado **conmutador** de los elementos a y b. Al grupo formado por los productos finitos de elementos conmutadores se le llama **grupo conmutador** o derivado de G, denotado por $[G, G] = G'$. Nótese que $G' = \{e\}$ si el grupo G es abeliano, ya que cualquier elemento de la forma $aba^{-1}b^{-1}$ es igual al elemento e.

Proposición 1.7. $G' \lhd G$.

Demostración. Sean $a, b \in G'$ entonces $ab \in G'$, con esto tenemos $G' = \{x_1 \cdot x_2 \cdot \ldots \cdot x_n \mid x_i = a_i b_i a_i^{-1} b_i^{-1}, a_i, b_i \in G\}$

1. $e \in G'$: en efecto, al expresar $e = eee^{-1}e^{-1}$ se obtiene un conmutador, entonces $e \in G'$

2. $x \in G'$ entonces $x^{-1} \in G'$:

   Sea $x = aba^{-1}b^{-1}$, entonces

   $$x^{-1} = (aba^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1}b^{-1}a^{-1} = bab^{-1}a^{-1}.$$

   x^{-1} también es un conmutador y en efecto

   $$xx^{-1} = aba^{-1}b^{-1}bab^{-1}a^{-1} = aba^{-1}ab^{-1}a^{-1} = abb^{-1}a^{-1} = aa^{-1} = e.$$

   Este principio también se cumple para productos, es decir:

   $$X = \prod_{i=1}^{n} x_i \Rightarrow X^{-1} = \left(\prod_{i=1}^{n} x_i\right)^{-1} = \prod_{i=n}^{1} x_i^{-1}$$

   de donde $G' < G$

3. $G' \lhd G$ si para cada $X \in G'$ y para cada $g \in G$, $gXg^{-1} \in G'$
   sea $X = \prod_{i=1}^{n} x_i$ y tomemos gXg^{-1} entonces,
   $\mathrm{g}\left(\prod_{i=n}^{1} x_i^{-1}\right) g^{-1} = gx_1x_2 \ldots x_n g^{-1} =$
   $gx_1(g^{-1}g)x_2(g^{-1}g) \ldots (g^{-1}g)x_n g^{-1} = \prod_{i=n}^{1}(gx_i^{-1}g^{-1})$.

Sustituyendo $x_i = a_i b_i a_i^{-1} b_i^{-1}$ en $g x_i g^{-1}$, se tiene

$$g x_i g^{-1} = g(a_i b_i a_i^{-1} b_i^{-1}) g^{-1} = (g a_i g^{-1})(g b_i g^{-1})(g a_i^{-1} g^{-1})(g b_i^{-1} g^{-1}),$$

donde los últimos dos factores son los inversos de los primeros dos factores

$$(g a_i g^{-1})^{-1} = (g^{-1})^{-1} a_i^{-1} g^{-1} = g a_i^{-1} g^{-1} \text{ y}$$

$$(g b_i g^{-1})^{-1} = (g^{-1})^{-1} b_i^{-1} g^{-1} = g b_i^{-1} g^{-1}.$$

Que también son conmutadores, por lo tanto, $G' \lhd G$. □

Ejemplo 1.21. En las simetrías del triángulo, los únicos subgrupos normales son los triviales G, $\{e\}$ y las rotaciones $H = \{e, a, b\}$. Si tomamos, por ejemplo las rotaciones y dos elementos a (una rotación) y f (una reflexión con respecto a una altura). Tenemos que los inversos de rotaciones son también rotaciones y el inverso de las reflexiones son ellas mismas, por ser de orden 2. Entonces independientemente del elemento a escoger, las rotaciones permanecen invariantes, es decir $afa^{-1}f^{-1}$ es una rotación y todos los productos volverán a generar a H, así $G' = H$.

Proposición 1.4. Sea G un grupo, G' es el subgrupo normal más grande de G tal que G/G' es conmutativo.

Demostración. Sea G/N con $N \lhd G$.

- Si G/G' es abeliano. Tomando las clases aG', bG' y su producto, tenemos

  $$abG' = (aG')(bG') = ab(a^{-1}b^{-1}ba)G' = ab(b^{-1}a^{-1}ba) = a(bb^{-1})a^{-1}baG' = baG'.$$

- Si G/N es conmutativo entonces $G' \subseteq N$. Como G/N es abeliano, $ab = ba \in G/N$, de donde $abG/N = baG/N$, así

  $$ab(G/N)a^{-1}b^{-1}(G/N) = aba^{-1}b^{-1}(G/N) = e(G/N) = G/N$$

  y todos los elementos de la forma $aba^{-1}b^{-1} \in N$ entonces $N \subseteq G'$. □

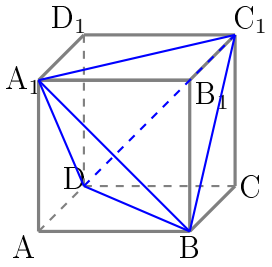


Figura 1.4. Tetraedro inscrito en un cubo

Ejemplo 1.22. Los vértices B, D, A_1, C_1 de la figura 1.4 forman un tetraedro inscrito en un cubo. Uniendo los otros vértices, $B1, D1, A, C$ se formará un segundo tetraedro. Las rotaciones del grupo forman un grupo, C [4], donde dada una rotación del cubo, se producirá una rotación que deje fijos ambos tetraedros o los intercambie entre sí.

Las rotaciones que dejan fijos a los tetraedros forman un subgrupo normal de las rotaciones del cubo. Las rotaciones de un tetraedro forman un grupo T dentro del grupo de rotaciones del cubo, por lo que $T < S$, más aún, $T \lhd C$, ya que una rotación g y su inversa g^{-1}, ambas intercambian o dejan fijos a los tetraedros, es decir $T = gTg^{-1}$ y puede mostrarse que $C' = T$ y además hay un homomorfismo de T en C.

Anteriormente, vimos que los homomorfismos $\phi\colon G \to F$ preservan el elemento neutro, inversos y el orden de un elemento, en el caso de la conmutatividad, tenemos que *Si G es conmutativo, F también.*

Si G es conmutativo, $ab = ba$, entonces $\phi(ab) = \phi(ba)$, y tenemos que

$$\phi(ab) = \phi(a)\phi(b)$$
$$\phi(ba) = \phi(b)\phi(a)$$

Por lo tanto

$$\phi(a)\phi(b) = \phi(b)\phi(a)$$

Entonces F es conmutativo, por otro lado, el recíproco no es cierto, ya que si tenemos F conmutativo,

$$\phi(a)\phi(b) = \phi(b)\phi(a),$$

pero ϕ es una función sobreyectiva, entonces $\phi(a)$ puede tener más de una preimagen,

[4] ver (Alekseev, 2004), Cap 1.12.

digamos $a' \neq a$, entonces

$$\phi^{-1}(b)\phi^{-1}(a) = ba'$$

$$\phi^{-1}(a)\phi^{-1}(b) = ab,$$

entonces $ba' = ab$, de donde $ba \neq ab$, por lo que G no es necesariamente conmutativo.

1.3.1. Homomorfismos y subgrupos

Estudiamos los homomorfismos de grupos y veremos ahora qué propiedades de los subgrupos se conservan bajo homomorfismos.

Dado un grupo G, $H \subset G$ y un homomorfismo de grupos $\phi : G \to F$. Al conjunto de elementos que tienen al menos una preimagen en H es llamado la **imagen** de H por el homomorfismo ϕ y se denota por $\phi(H)$. Asimismo, si se tiene $P \subset F$, al conjunto de elementos cuya imagen están en P es llamado la preimagen de P bajo el homomorfismo ϕ y se denota por $\phi^{-1}(P)$. En consecuencia $\phi^{-1}(P) \subset H$, pero no es necesariamente igual:[5]

1. Si $H < G$, entonces $\phi(H) < F$.

2. Si $N < F$, entonces $\phi^{-1}(N) < G$.

   Estas propiedades también son válidas para subgrupos normales, es decir:

3. Sea $H \lhd G$, entonces $\phi(H) \lhd F$.

4. Si $H \lhd F$, entonces $\phi^{-1}(H) \lhd G$.

   Para el grupo derivado, se cumple:

5. Considérese G' y F' entonces $\phi(G') \subseteq F'$ y $G' \subseteq \phi^{-1}(F')$.

6. $\phi(G') = F'$, sin embargo $G' \neq \phi^{-1}(F')$.

[5] Estas afirmaciones son necesarias para definir a un grupo soluble, la demostración de las mismas puede verse en el capítulo 1.14 de (Alekseev, 2004).

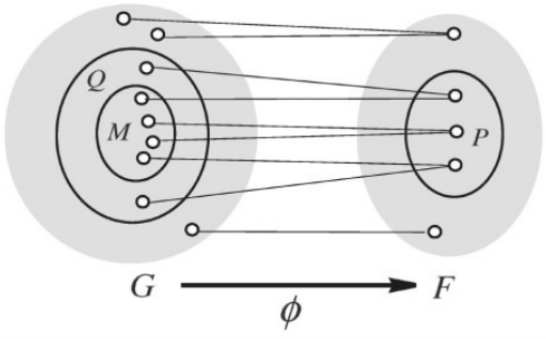


Figura 1.5. En este homomorfismo de grupos, puede notarse que la imagen del homomorfismo no es necesariamente igual a todo el conjunto F. Fuente: imagen tomada de(Alekseev, 2004).

Definición 1.19. Sea G un grupo y $N \lhd G$. El homomorfismo $\phi\colon G \to G/N$ se llama **homomorfismo natural** y es sobreyectivo. En el caso del subgrupo trivial $\{e\}$, ϕ es una biyección, por lo que $G \cong G/\{e\}$. A cada subgrupo normal corresponde un homomorfismo y cada homomorfismo sobreyectivo puede verse como un homomorfismo natural con un subgrupo normal adecuado.

Definición 1.20. Al conjunto de elementos en G tal que $\phi(g) = e_F$ se le llama **núcleo de** ϕ y se denota por $\ker(\phi)$.

En todo homomorfismo de grupos $\phi\colon G \to F$, el núcleo está bien definido. En el caso de que $\phi\colon G \to F$ sea sobreyectivo, entonces un elemento en el grupo F puede tener más de una preimagen, en particular, $\circ(\ker(\phi)) \geqslant 1$.

Proposición 1.8. $\ker(\phi) \lhd G$.

Demostración. $\ker(\phi) = \{g \in G \mid \phi(g) = e_F\}$.

Sea $\phi(a) = e_F$ y $\phi(b) = e_F$, entonces

$$\phi(ab) = \phi(a)\phi(b) = e_F e_F = e_F \text{ por lo que } \phi(ab) \in \ker(\phi).$$

Por otro lado, si $a \in \ker(\phi)$, entonces $a^{-1} \in \ker(\phi)$, y se cumple

$$\phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = \phi(a)\left[\phi(a)\right]^{-1} = e_F e_F^{-1} = e_F \text{ entonces } \left[\phi(a)\right]^{-1} \in \ker(\phi).$$

De esto, $\ker(\phi) < G$.

Considérese ahora $\phi(gag^{-1})$, entonces se tiene que

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)e_F\left[\phi(g)\right]^{-1} = \phi(g)\left[\phi(g)\right]^{-1} = e_F,$$

de donde $\phi(gag^{-1}) \in \ker(\phi)$ y por lo tanto $\ker(\phi) \lhd G$. □

Teorema 1.3.4 (Primer teorema de isomorfía)**.** *Sea $\phi : G \to F$ un homomorfismo de grupos. Entonces $G/\ker(\phi) \cong F$.*

Demostración. Para demostrar que $\psi : G/\ker(\phi) \to F$ es isomorfismo, se mostrará que:

a) ψ: $G/\ker(\phi) \to F$ está bien definido.

Sea $g \in G$ arbitrario, consideremos la correspondencia $g\ker(\phi) \mapsto \phi(g)$, esta está bien definida, ya que no depende de la clase $g\ker(\phi)$ que se escoja.

b) ψ es homomorfismo biyectivo.

Sean $g, g' \in G$, entonces $g\ker(\phi), g'\ker(\phi) \in G/\ker(\phi)$.

$$\psi(g\ker(\phi)g'\ker(\phi)) = \psi(gg') = \psi(g)\psi(g') = \psi(g\ker(\phi))\psi(g'\ker(\phi)),$$

entonces es homomorfismo y supóngase que $\psi(g\ker(\phi) = \psi(g'\ker(\phi))$, de donde

$$g\ker(\phi) = g'\ker(\phi),$$

dado que $g \in g\ker(\phi)$ y $g' \in g'\ker(\phi)$, entonces

$$\phi(g) = \psi(g\ker(\phi)) = \psi(g'\ker(\phi)) = \phi(g').$$

De donde $g\ker(\phi) = g'\ker(\phi)$ entonces ψ es inyectiva, ahora bien, dado que ϕ es sobreyectivo, para todo $f \in F$ existe algún $g \in G$ tal que $\phi(g) = f$ y sabemos que $g \in g\ker(\phi)$ entonces

$$\psi(g\ker(\phi)) = \phi(g) = f.$$

Entonces ψ es también sobreyectiva, por lo que ψ es biyectiva. □

Proposición 1.9. *Sea $N_1 \lhd G_1$ y $N_2 \lhd G_2$, entonces $N_1 \times N_2 \lhd G_1 \times G_2$ y $\frac{G_1 \times G_2}{N_1 \times N_2} \cong G_1/N_1 \times G_2/N_2$*

Demostración. Del ejemplo 1.15 se tiene este resultado para subgrupos, falta mostrar que conserva la condición de ser subgrupo normales. Dado que $\frac{G_1 \times G_2}{N_1 \times N_2} \cong G_1/N_1 \times G_2/N_2$, vemos que $\phi : G_1 \times G_2 \to G_1/N_1 \times G_2/N_2$ es el homomorfismo natural, entonces es sobreyectivo.

Si consideramos $\ker(\phi)$, es de la forma

$$\phi((g_1, g_2)) = (\phi(g_1), \phi(g_2)) \text{donde } \phi((g_1, g_2)) = (eG_1/N_1, eG_2/N_2),$$

que son las clases laterales que contienen a e en cada cociente G_1/N_1 y G_2/N_2 y esto si y sólo si

$$\phi(g_1) = G_1/N_1$$
$$\phi(g_2) = G_2/N_2$$

si y sólo si $\ker(\phi) = N_1 \times N_2$, por lo tanto, $N_1 \times N_2 \lhd G_1 \times G_2$. □

1.4. Grupos solubles

Otra clase de grupos tan importantes como los grupos abelianos son lo grupos solubles. Su nombre proviene de que la posibilidad de resolver ecuaciones algebraicas por radicales, que depende de la solubilidad de los grupos que asociaremos en el Capítulo 3 a este tipo de ecuaciones.

Si G es un grupo y G' su conmutador. Como G' es un grupo, puede considerarse también su conmutador de manera recursiva, generando así la **serie derivada**,

$$G,\, G',\, G'',\, G^{(3)},\, G^{(4)}, \ldots,\, G^{(n)} = \{G^{(j)}\}_{j\in\mathbb{N}},$$

donde $G^{(n)} = G^{(n-1)'}$ y por la proposición 1.7, se cumple que

$$G^{(n)} \lhd G^{(n-1)} \lhd \ldots \lhd G'' \lhd G' \lhd G.$$

Definición 1.21. Si la serie derivada, $\{G^{(j)}\}_{j\in\mathbb{N}}$ termina para algún número entero n, es decir $G^{(n)} = \{e\}$ se dice que el grupo G es **soluble**.

Ejemplo 1.23. Para todo grupo abeliano G, se cumple que $G' = \{e\}$, entonces la serie derivada termina para $n = 1$.

Si un grupo es soluble, se cumplirán las siguientes proposiciones:

Proposición 1.10. *Todo subgrupo de un grupo soluble es soluble.*

Demostración. Si $H < G$ entonces $H' \subseteq G'$ y cada $H^{(j)} \subseteq G^{(j)}$ dado que G soluble, $H^{(n)} \subseteq G^{(n)} = \{e\}$ para algún n entonces $H^{(m)} = \{e\}$ para algún $m \leqslant n$. □

Proposición 1.11. *Sea $\phi : G \to F$ un homomorfismo sobreyectivo, donde G es soluble, entonces F es soluble.*

Demostración. De las propiedades del subgrupo conmutador, se tiene que $\phi(G') = F'$ y dado que G es soluble, $G^{(n)} = \{e\}$ para algún n. Entonces

$$\phi(G^{(n)}) = \phi(e_G) = e_F, \tag{1.1}$$

$$\phi(G^{(n)}) = F^{(n)}. \tag{1.2}$$

De las ecuaciones 1.1 y 1.2 se tiene que $F^{(n)} = e_F$, entonces F es soluble. □

Proposición 1.12. *Sea G un grupo soluble y $N \lhd G$, entonces G/N es soluble.*

Demostración. Consideremos el homomorfismo natural $\phi : G \to G/N$ como ϕ es sobreyectivo, G/N es soluble (por resultado de la proposición 1.11). □

Proposición 1.13. *Sean G un grupo tal que $N < G$ y G/N son solubles, entonces G es soluble.*

Demostración. Considerando el homomorfismo natural $\phi : G \to G/N$ donde $\phi(G') = (G/N)'$, como G/N es soluble, existe algún n tal que $(G/N)^{(n)} = \{e\}$, entonces

$$(G/N)^{(n)} = \phi(G^{(n)}) = \{e\}.$$

Por otro lado, $G^{(n)} \subseteq N$ y dado que N es soluble, existe algún entero m tal que $N^{(m)} = \{e\}$, así:

$$G^{(n+m)} \subseteq N^{(m)} = \{e\},$$

donde $m + n$ es un entero finito y, por lo tanto, G es soluble. □

Proposición 1.14. *Sea G y F dos grupos solubles, su producto $G \times F$ es también soluble.*

Demostración. Por las propiedades del producto directo de grupos y grupos cocientes (propiedad 1), se tiene que:

$$\frac{G \times F}{G \times \{e_f\}} \cong F$$
$$\frac{G \times F}{\{e_g\} \times F} \cong G$$

Entonces consideremos los homomorfismos sobreyectivos

$$\phi_1 : G \times F \to \frac{G \times F}{G \times \{e_f\}} \cong F$$
$$\phi_2 : G \times F \to \frac{G \times F}{\{e_g\} \times F} \cong G$$

Como F y G son solubles, se cumplen las condiciones de la proposición 1.14, para que $G \times F$ sea soluble. □

Si un grupo no es conmutativo, se cumplirá lo siguiente:

Proposición 1.15. *Si un grupo G no es conmutativo y sus únicos subgrupos normales son los triviales, entonces G no es soluble.*

Demostración. Si G no es conmutativo, entonces $G' \neq \{e\}$, dado que sus únicos subgrupos son los triviales, $G' = G$, de donde $G^{(n)} = G$ para cualquier n, entonces no existe n tal que $G^{(n)} = \{e\}$ y por lo tanto G no es soluble. □

Otra forma equivalente para definir a los grupos solubles es:

Definición 1.22. G es un grupo soluble, si y sólo si existe una sucesión de subgrupos del mismo $G_0, G_1, \ldots, G_n$ tales que cada $G_i \lhd G_{i-1}$ y cada cociente G_{i-1}/G_i es conmutativo, donde $G_0 = G$ y $G_n = \{e\}$.

Proposición 1.16. *Las definiciones de grupos solubles 1.21 y 1.22 son equivalentes.*

Demostración.

($\Rightarrow$) Si G es soluble, podemos considerar la serie derivada, donde $G_0 = G^{(0)} = G$ y $G_n = G^{(n)} = \{e\}$ para algún n, por la Proposición 1.7, se tiene que $G^{(n)} \lhd \ldots \lhd G^{(2)} \lhd G^{(1)} \lhd G^{(0)} = G$, es decir que cada $G_i \lhd G_{i-1}$. Y de la propiedad 1.3 se tiene que cada G_{i-1}/G_i es conmutativo.

($\Leftarrow$) Si $G_i \lhd G_{i-1}$ y G_{i-1}/G_i es conmutativo, entonces $G^{(i-1)} \subseteq G_i$ (Propiedad 1.3), entonces

$$G'_{i-1} \subseteq G_i$$
$$G''_{i-1} \subseteq G'_{i-1}$$
$$\vdots$$
$$G^{(n+1)}_{i-1} \subseteq G^{(n)}_{i-1},$$

entonces $G_0^{(n)} \subseteq G_1^{(n-1)} \subseteq \ldots \subseteq G^{(n)} = \{e\}$, como G_n es conmutativo, se cumple $G_0^{(n+1)} = \{e\}$. Por lo tanto G es soluble. □

1.4.1. Grupos simétricos y su solubilidad

En esta sección se estudiarán aspectos importantes de los grupos simétricos S_n, una parte esencial en estos grupos es su solubilidad. Recordando que los grupos simétricos son el grupo formado por las permutaciones de un arreglo de n elementos, cada permutación del mismo puede ser representada de la forma

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix},$$

donde cada i_k es la imagen del elemento k bajo la permutación σ.

Estas permutaciones puede fijar algunos elementos e intercambiar el resto de forma cíclica.

Ejemplo 1.24. Considérese el arreglo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix}.$$

Esta permutación fija a los elementos 1 y 3, y envía los elementos $2 \to 4, 4 \to 6, 6 \to 5$ y $5 \to 2$. Es decir, que permuta cíclicamente a 2, 4, 6 y 5.

Definición 1.23. Llamaremos **ciclos** a las permutaciones cíclicas de los n elementos. En el ejemplo 1.24 el ciclo que permuta a los elementos 2, 4, 6, 5 se denotará (2 4 6 5). Algunas permutaciones no son cíclicas, por ejemplo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix},$$

sin embargo estas pueden ser representadas como un producto de ciclos, así,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 14 & 3 & 6 & 1 & 5 & 2 \end{pmatrix} = (14)(236).$$

A los ciclos que no tienen elementos en común, los llamamos **ciclos independientes**.

Así, puede mostrarse fácilmente el siguiente lema, que será importante en los siguientes capítulos:

Lema 1.4.1. *S_n no es conmutativo para $n \geqslant 3$*

Demostración. Considérense dos permutaciones en S_3

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Escritos en forma de ciclos, se tiene que $a = (12)$ y $b = (132)$ y los productos

$$ab = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13), \qquad ba = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23).$$

Entonces $ab \neq ba$ y, en general, para $n \geqslant 3$ pueden tomarse las permutaciones a y b, dejando fijos a los demás elementos y se cumplirá $ab \neq ba$ en todos los casos. □

Lema 1.4.2. *Toda permutación se puede representar de forma única como producto de ciclos independientes.*

Demostración. Consideremos una permutación en S_n tal que $i_{m-1} \mapsto i_m$ donde $2 \leqslant m \leqslant n$ donde que i_m es el primer elemento que cierra un ciclo. Luego se toma un elemento que no pertenezca al primer ciclo obtenido $(i_1 i_2 \dots i_m)$ y se construye un segundo ciclo (digamos de r elementos), obteniendo el producto

$$(i_1\, i_2\, \dots\, i_m)(i_{m+1}\, i_{m+2} \dots\, i_{m+r}) \dots$$

Se procede tomando un elemento que no pertenece a los elementos del producto anterior, este procedimiento es finito, ya que el arreglo tiene una cantidad finita de elementos, de manera que la permutación es de la forma:

$$(i_1\, i_2\, \dots\, i_m)(i_{m+1}\, i_{m+2} \dots\, i_{m+r}) \dots (i_k\, \dots\, i_n),$$

donde cada ciclo es independiente. Esta representación es única, ya que entre ciclos independientes el producto es abeliano. □

Definición 1.24. Cuando un ciclo tiene únicamente dos elementos, es llamado **transposición** y cuando las transposiciones son de la forma $(1\,2)$, $(2\,3)$, ..., $(n-1\,n)$ se llaman **transposiciones elementales**.

A partir de esto, se tienen las siguientes afirmaciones

Lema 1.4.3. *Todo ciclo se puede representar como producto de transposiciones.*

Demostración. Consideremos el grupo S_n y ciclos de m elementos. En efecto, si $m = 1$ un 1-ciclo (identidad) puede ser representado como $(1k)(k1)$, cuando $m = 2$ es ya una transposición. En general, si m es par, habrá $m/2$ transposiciones independientes y si es impar habrá $m - 1/2$ transposiciones independientes y cualesquiera 2 que sean la identidad, así la representación no será única, ya que se puede escoger un elemento arbitrario de las transposiciones anteriores para representar la identidad. Y, de forma general, se cumple que para todo ciclo de orden m

$$(i_1\, i_2\, \ldots\, i_m) = (i_1\, i_m)(i_1\, i_{m-1}) \ldots (i_1\, i_2). \qquad \square$$

Lema 1.4.4. *Toda transposición se puede representar de forma única como producto de transposiciones elementales*

Demostración. Sean $(i_1\, i_2)(i_2\, i_3) \ldots (i_{n-1}\, i_n)$ las transposiciones elementales y sea $1 \leqslant m \leqslant k \leqslant n$, consideremos la transposición $(i_m\, i_k)$.

Si $k = m + 1$, entonces $(i_m\, i_k) = (i_m\, i_{m+1})$.

Si $K = m + 2$, entonces $(i_m\, i_k) = (i_m\, i_{m+1})(i_{m+1}\, i_{m+2})(i_m\, i_{m+1})$.

$\vdots$

En general, para cualquier k se tiene

$$(i_m\, i_k) = (i_m\, i_{m+1})(i_{m+1}\, i_{m+2}) \ldots (i_{k-1}\, i_k)(i_{k-2}\, i_{k-1}) \ldots (i_{m+1}\, i_{m+2})(i_m\, i_{m+1}). \qquad \square$$

En consecuencia de los lemas 1.4.2, 1.4.3 y 1.4.4 se tiene el siguiente teorema:

Teorema 1.4.1. *Si un subgrupo de S_n contiene todas las transposiciones elementales, coincide con S_n.*

Demostración. Si tiene todas las transposiciones elementales, tendrá a todos los productos de las mismas. Por el Lema 1.4.4 esto genera a todas las transposiciones y, por el Lema 1.4.3, a todos los ciclos.

Entonces se tendrán todos los posibles ciclos disjuntos, que generarán a todas las permutaciones (Lema 1.4.2) de un arreglo de n elementos, esto es S_n. $\square$

Las permutaciones y transposiciones son intercambios de elementos en un arreglo, es decir, escribe a $(1\,2\,3 \ldots\, n)$ de forma arbitraria.

Definición 1.25. En una permutación, se dice que el par de elementos i, j son una **inversión** si en el arreglo ordenado arbitrariamente aparece j antes que i, siendo $i < j$.

Consideremos la función $\epsilon : S_n \to \{\pm 1\}$ tal que

$$\epsilon(\sigma) = \begin{cases} 1 & \text{si } (i,j) \text{ no es inversión} \\ -1 & \text{si } (i,j) \text{ es inversión} \end{cases}$$

El número de inversiones k define la paridad de una permutación. Consideremos $\varepsilon(\sigma) = (-1)^k$ el producto de los $\epsilon(\sigma)$. Cuando $\varepsilon(\sigma) = 1$, la permutación será una **permutación par**, si $\varepsilon(\sigma) = -1$, será una **permutación impar**.

Teorema 1.4.2. *Al intercambiar dos números, cambia la paridad de una permutación.*

Demostración. Supóngase que en una permutación se intercambian los elementos i_n e i_m y que existen $r = m - n - 1$ elementos en medio de ellos.

En el arreglo de i_n a i_m de la siguiente forma:

$$(\ldots\, i_n\, a_1\, a_2 \ldots a_r\, i_m \ldots),$$

al intercambiarlos se tendrá

$$(\ldots\, i_m\, a_1\, a_2 \ldots a_r\, i_n \ldots).$$

En el arreglo existen parejas de la forma (i_n, a_i), (a_i, i_m) y el par (i_n, i_m) haciendo un total de $2r+1$ parejas. Al intercambiarlos, se tendrán parejas de la forma (a_i, i_n), (i_m, a_i) y el par (i_m, i_n).

Supongamos que existen $k \leqslant 2r+1$ inversiones en esos pares y que el producto de $\epsilon(\sigma)$ de cada pareja es 1 (k es par). Al intercambiar, las $r - k$ que no eran inversiones, ahora lo son, obteniendo:

$$2r + 1 - k \text{ es par si } r \text{ es impar.}$$

$$2r + 1 - k \text{ es impar si } r \text{ es par.}$$

En consecuencia, luego del intercambio, cambiará la paridad del número de inversiones y por ende, la paridad de la permutación. □

Del Teorema 1.4.2, se tiene:

Corolario 1.4.1. *Al multiplicar una permutación por una transposición cambia su paridad.*

Demostración. Dado que una transposición es un intercambio de dos elementos, por el teorema anterior, se cumple la afirmación. □

Corolario 1.4.2. *Una permutación par puede ser representada únicamente por el producto de un número par de transposiciones y una impar, en un número impar de transposiciones.*

Demostración. Del Lema 1.4.3, se tiene que una permutación puede representarse como producto de transposiciones, consideremos una permutación par descompuesta en m transposiciones $\sigma = \prod_{i=1}^{m} a_i$ y sabemos que $\sigma = e\sigma$, donde e es el neutro (permutación par).

Dado que el producto de una permutación por una transposición cambia su paridad, tenemos

$$e(a_1) \text{ es impar.}$$

$$e(a_1)(a_2) \text{ es par.}$$

$$e(a_1)(a_2)(a_3) \text{ es impar.}$$

$$\vdots$$

$$e(a_m) \text{ es par sólo si m es par.}$$

y análogamente, $e(a_m)$ es impar sólo si m es impar. □

De esto se tiene que el producto de dos permutaciones de la misma paridad, darán como resultado una permutación par, así como permutaciones de paridades opuestas darán como resultado una permutación impar. Dado que S_n es un grupo cuya identidad e es una permutación par, se obtiene que el elemento inverso a^{-1} debe tener la misma paridad que a, para todo $a \in S_n$. De esto se tiene que las permutaciones pares de grado n forman un grupo. A este grupo se le llama **grupo alternante de grado** n y es denotado por A_n.

En consecuencia $A_n < S_n$ y más aún, $A_n \lhd S_n$ ya que $[S_n : A_n] = 2$, este generará una partición de los elementos de A_n, es decir permutaciones pares y A_n^c, que son las permutaciones impares.

Proposición 1.17. *El grupo A_n no es conmutativo para $n \geqslant 4$.*

Demostración. Considérense las dos permutaciones pares en S_4 escritas en forma de ciclos

(4 1 2) y (3 1 2) son permutaciones pares, de la forma

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (412), \qquad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (312).$$

Y sus productos son

$$ab = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24), \qquad ba = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23).$$

De donde se puede observar que $ab \neq ba$, utilizando estos ciclos y fjando el resto de elementos en permutaciones de orden $n \geqslant 4$, se obtiene que los grupos A_n no son conmutativos para $n \geqslant 4$. □

Proposición 1.18. *El grupo A_5 no es soluble.*

Demostración. Los grupos S_n tienen $n!$ elementos y A_n tiene entonces $n!/2$ elementos. Entonces $\circ(A_5) = 60$ del Teorema 1.3.2 sabemos que el orden de los subgrupos de A_5 debe dividir a 60. Entonces consideremos los distintos tipos de permutaciones en A_5

A_5 son las permutaciones de orden par en S_5, veremos a continuación las particiones de 5.

Caso	Partición	Forma
(a)	1, 1, 1, 1, 1	e
(b)	1, 1, 1, 2	$(i_1 i_2)$
(c)	1, 1, 3	$(i_1 i_2 i_3)$
(d)	1, 4	$(i_1 i_2 i_3 i_4)$
(e)	5	$(i_1 i_2 i_3 i_4 i_5)$
(f)	1, 2, 2	$(i_1 i_2)(i_3 i_4)$
(g)	2,3	$(i_1 i_2)(i_3 i_4 i_5)$

Tabla 1.3. Tipos de permutaciones en S_5.

- El caso (a) nos proporciona 5 formas equivalentes de escribir a la identidad como 1-ciclo, éste pertenece a todos los subgrupos de A_5.
- En el caso (b), los 2-ciclos del tienen una inversión por ser el intercambio de dos elementos (es impar), por lo que se necesitan dos, 2-ciclos para que sea un posible subgrupo (caso (f)) de A_5. Estos pueden representarse de 8 formas, entonces existen $120/8 = 15$ de este tipo.

- Los 3-ciclos o el caso (c), tienen un número par de inversiones, y existen $5!/3! = 5 * 4 = 20$ elementos de este tipo. Esto nos permite descartar el caso (g).
- Los 4-ciclos o caso (d) pueden tener 3 inversiones, que son impares, por lo que no pueden representar a una permutación de grado 5 como ciclo independiente de otro.
- Por último, el caso (e) o los 5-ciclos son permutaciones pares, cada 5-ciclo puede representarse de 5 formas equivalentes, entonces existen $120/5 = 24$ 5-ciclos

Consideremos ahora los casos posibles (c), (e), (f):

1. Si una permutación de la forma (c) pertenece a A_5, todas las demás también:

   Tomemos (sin pérdida de la generalidad) a la permutación de tres elementos $h = (123)$, con $(i_1 i_2 i_3)$ arbitrarios y a los elementos i_4, i_5 distintos en el arreglo $\{i_1, i_2, i_3, i_4, i_5\}$. Entonces sólo en una de las permutaciones

   $$g_1 = (i_1 i_2 i_3 i_4 i_5),\ g_2 = (i_1 i_2 i_3 i_5 i_4)$$

   hay un número par de inversiones. En cualquiera de los casos, se tiene

   $$g_i h g_i^{-1} = (i_1 i_2 i_3).$$

2. Si una permutación de la forma (e) pertenece a A_5, todas las demás también. Consideremos dos casos:

   - Si $g = (i_1 i_2 i_3 i_4 i_5)$ es par, entonces $ghg^{-1} = (i_1 i_2 i_3 i_4 i_5)$ para cualquier permutación g.
   - Si $g = (i_1 i_2 i_3 i_4 i_5)$ es impar, entonces podemos obtener una permutación par $g = (i_1 i_4 i_2 i_5 i_3)$ tal que $ghg^{-1} = (i_1 i_2 i_3 i_4 i_5)$ y $(ghg^{-1})^2 = (i_1 i_2 i_3 i_4 i_5)$.

3. Como en los casos (c) y (e), consideraremos para el caso (f) a la permutación $h = (12)(34)$.

   Sólo una de las permutaciones $g_1 = (i_1 i_2)(i_3 i_4), g_2 = (i_2 i_1)(i_3 i_4)$ es par, en ambos casos, el producto $g_i h g_i^{-1} = (i_1 i_2)(i_3 i_4)$.

Por lo tanto, si algún elementos de los tipos (c), (e), (f) pertenece a A_5, todos los del respectivo tipo pertenecen a A_5.

Cada clase de ciclos no cuenta a la identidad, por lo que el conjunto de los 5-ciclos más la identidad tiene 25 elementos y $25 \nmid 60$. Así mismo con los 3-ciclos, se tendrán 21 elementos y $21 \nmid 60$. En el caso de los pares de 2-ciclos, se tendrán 16 elementos. Dado que ninguno divide a 60, por el Teorema 1.3.2, los únicos subgrupos normales de A_5 son los triviales. Como A_5 no es conmutativo, por la Proposición 1.15, se sigue que no es soluble. □

Otra forma de ver la no solubilidad del grupo A_5 es inscribiendo en un dodecaedro los 5 tetraedros regulares, de manera que cada rotación del dodecaedro corresponda a una permutación par de los tetraedros y rotaciones diferentes, corresponden a permutaciones impares, así, se construye un isomorfismo entre las rotaciones del dodecaedro y el grupo de permutaciones pares de grado 5, A_5. Para encontrar los tetraedros, se inscriben cubos en el dodecaedro, cuyos vértices son los pares de vértices opuestos en el dodecaedro. Habiendo encontrado los 5 cubos, conocidos como cubos de Kepler, se inscribe en cada uno un tetraedro como en el ejemplo 1.22. Y dado que el grupo de simetrías del dodecaedro sólo tiene subgrupos normales triviales, es no soluble.

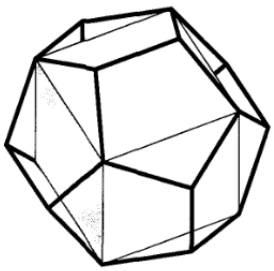


Figura 1.6. Cubo inscrito en un dodecaedro. Fuente: imagen tomada de(Artin, 1991).

Teorema 1.4.3. *S_n es soluble para $1 \leqslant n \leqslant 4$.*

Demostración. En el caso $n = 1$, es el grupo trivial, entonces es soluble.

Cuando $n = 2$, se obtienen dos permutaciones, la identidad y el intercambio de los dos elementos, generando un grupo isomorfo a $\mathbb{Z}_2$, que es abeliano y por consiguiente, soluble.

Sea $n = 3$, el grupo S_3 isomorfo a las simetrías del triángulo equilátero, no es abeliano, pero tiene un subgrupo normal formado por las rotaciones, nombremos H y $S_3' = S_3/H$, que es abeliano, entonces $S_3'' = (S_3/H)' = \{e\}$.

Si $n = 4$, encontraremos una cadena de subgrupos normales, así

$$S_4' = A_4$$

donde A_4 son las permutaciones:

$$A_4 = \{(234), (243), (12)(34), (123), (124), (132), (134), (13)(24), (142), (143), (14)(23)\}.$$

Nótese que los 3-ciclos (ijk) tienen inversas de la forma (ikj), mientras los 2-ciclos $A = (12)(34)$, $B = (13)(24)$, $C = (14)(23)$ con la identidad, forman un subgrupo normal de A_4 que es isomorfo a las rotaciones de un cuadrado, digamos V_4, y este es un grupo abeliano. De donde

$$S_4'' = A_4' = V_4$$

$$\text{y } V_4' = \{e\}.$$

Por lo tanto, es soluble. □

Nota 1.2. Otra prueba de esto, es dada la solubilidad de S_4, consideremos las permutaciones que dejan fijo un elemento y permutan los 3 elementos restantes, generando un subgrupo de S_4 isomorfo a S_3. De manera similar, $S_2 < S_3 < S_4$ y por la proposición 1.10, sabemos que todo subgrupo de un grupo soluble es soluble.

Teorema 1.4.4. *Para $n \geqslant 5$, el grupo S_5 no es soluble*

Demostración. Sabemos que $A_5 \lhd S_5$ y A_5 no es soluble, por la proposición 1.10, S_5 no es soluble.

Para el caso $n > 5$, consideraremos las permutaciones que dejen fijo al arreglo $\{6, 7, \ldots, n\}$ y permuten los primeros 5 elementos. Formando un subgrupo de S_n,isomorfo a A_5.

Entonces para $n \geqslant 5$, todo S_n tiene un subgrupo isomorfo a A_5, el cual no es soluble, por lo que S_n no es soluble para $n \geqslant 5$. □

2. NÚMEROS COMPLEJOS

En este capítulo estudiaremos las propiedades del campo de los números complejos $\mathbb{C}$, que son de gran importancia, ya que este $\mathbb{C}$ es la cerradura algebraica del campo $\mathbb{R}$. Por ser cerrado algebraicamente, se cumple el Teorema Fundamental del Álgebra, es decir que cualquier polinomio con coeficientes complejos tiene al menos una raíz compleja. En particular, nos interesa estudiar ecuaciones polinomiales con coeficientes complejos y sus soluciones, que es equivalente a encontrar las raíces de polinomios.

2.1. El campo de los números complejos

Definición 2.1. Sea F un conjunto, con dos operaciones binarias $(+, \cdot)$ de manera que cumple:

1. F forma un grupo conmutativo bajo adición $(+)$.
2. $F \setminus \{0\}$ forma un grupo bajo multiplicación $(\cdot)$.
3. Para cualesquiera a, b, c $\in F$, ambas operaciones se relacionan a través de la distributividad:
$$a(b+c) = ab + ac.$$

Se dice que F es un **campo**.

Para cualesquiera $a, b, c \in F$, donde F es un campo se cumplen las siguientes propiedades:

- $a0 = 0a = 0$.
- $(-a)b = a(-b) = -(ab)$.
- $ab = 0$ implica que $a = 0$ o $b = 0$.
- $(a-b)c = ac - bc$.

A continuación, analizaremos ejemplos de conjuntos que no son campos y conjuntos que sí lo son:

Ejemplo 2.1. Los enteros, forman un grupo abeliano con respecto a la adición, pero no forman un grupo bajo multiplicación, ya que no contiene a los inversos multiplicativos, que deberían ser de la forma $a^{-1} = \frac{1}{a} \notin \mathbb{Z}$. Por lo tanto $\mathbb{Z}$ no puede ser un campo.

Ejemplo 2.2. $\mathbb{Q}$ es un grupo abeliano con respecto a la adición y, a diferencia de los enteros, éste sí contiene a todos los inversos multiplicativos de la forma $a^{-1} = \frac{1}{a}$ cuando $a \neq 0$.

Otro ejemplo de campo son los números reales, $\mathbb{R}$.

Ejemplo 2.3. El conjunto de los números complejos $\mathbb{C}$, tiene elementos iguales a $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ con las operaciones definidas por:

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc),$$

también es un campo.

Notemos que todos elementos de $\mathbb{C}$ forman un grupo conmutativo con respecto a la adición, ya que $\mathbb{R}$ lo es y, por lo tanto el producto $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ también lo es.

Para el producto, vamos a tomar $z_1 = (a, b)$, $z_2 = (c, d)$ y $z_3 = (e, f)$ y nótese que es una operación asociativa, esto es:

$(z_1 \cdot z_2) \cdot z_3 = (ace - bde - adf - bcf, acf - bdf + ade + bce) =$
$(a, b)(ce - df, de + cf) = z_1 \cdot (z_2 \cdot z_3)$.

El elemento neutro es $e = (1, 0)$ ya que $(a, b) \cdot (1, 0) = (a, b)$ siempre se cumple. Falta mostrar que existe $(a, b)^{-1} = z^{-1}$ tal que $z \cdot z^{-1} = e$. Suponiendo que $z^{-1} = (c, d)$, se tiene

$$z \cdot z^{-1} = (ac - bd, ad + bc) = (1, 0).$$

Esto si y sólo si los inversos son de la forma:

$$z^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right).$$

Estos cocientes existen en $\mathbb{C}$ porque $z = (a, b) \neq (0, 0)$.

Puede comprobarse fácilmente la distributividad:

$$(z_1 + z_2)z_3 = z_1 z_3 + z_2 z_3.$$

Por lo tanto, $\mathbb{C}$ es un campo.

A cada número real a le corresponde el número complejo de la forma $(a, 0)$ a través de la inclusión $\mathbb{R} \hookrightarrow \mathbb{C}$ tal que $a \mapsto (a, 0)$, así mismo se incluirá el elemento i, al que se le asignará el número complejo $(0, 1)$. Así, el campo de números complejos contiene a todos los elementos de la forma bi y de la forma $a + bi$, a esta forma de representar a los números complejos se le llama **representación algebraica de los números complejos**.

El número complejo $z = a + bi$ tiene una parte real, $\mathrm{Re}(z) = a$ y una parte imaginaria, $\mathrm{Im}(z) = b$.

Con la representación algebraica, las operaciones definidas en $\mathbb{C}$ son:

$$(a + bi) + (c + di) = (a + b) + (c + d)i.$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i.$$

Las potencias de i cumplen:

$$i = i, i^2 = -1, i^3 = -i, i^4 = 1.$$

Siendo la *n-ésima* potencia determinada cíclicamente únicamente por r si escribimos $n = 4k + r$, es decir, su residuo módulo 4.

Definición 2.2. Llamaremos el **conjugado de un número complejo** $z = a + bi$ al número $a - bi$ denotado por $\overline{z}$ y se puede verificar que:

$$z + \overline{z} = 2a \quad y \quad z \cdot \overline{z} = a^2 + b^2$$

Otras propiedades que cumplen los conjugados son

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.
2. $\overline{z_1 - z_2} = \overline{z_1} - \overline{z_2}$.
3. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.
4. $\overline{z_1/z_2} = \overline{z_1}/\overline{z_2}$.
5. Si $z \in \mathbb{R}$, $\overline{z} = z$.

Definición 2.3. Una función $\varphi\colon F_1 \to F_2$ es un **isomorfismo** de los campos F_1 y F_2 si es biyectiva y para cada $a, b \in F$, se cumple:

$$\varphi(a+b) = \varphi(a) + \varphi(b) \text{ y}$$

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Se dice que F_1 y F_2 son *isomorfos* y escribimos $F_1 \cong F_2$.

Consideremos un campo F que contenga a todos los reales y a un elemento j tal que $j^2 = -1$, entonces contiene a todos los elementos de la forma $a + bj$ con $a, b \in \mathbb{R}$. A través del homomorfismo $\varphi\colon \mathbb{C} \to F$ tal que:

$$\varphi(a + bi) = a + bj$$

que es inyectivo, entonces podemos afirmar que $\mathbb{C} \subseteq F$ y por lo tanto, es el campo más pequeño (minimal) que contiene un elemento cuyo cuadrado es -1.

2.2. Representaciones de los complejos

El conjunto de los números complejos $\mathbb{C}$, es igual al conjunto $\mathbb{R}^2$, entonces pueden ser representados en un plano, como puntos y tienen otras representaciones que veremos a continuación.

2.2.1. Representación geométrica

Puesto que $\mathbb{C}$ corresponde a $\mathbb{R}^2$ como conjunto, podemos representar gráficamente a los números complejos como puntos en el plano cartesiano, de manera que ahora el eje x será considerado como la parte real y el eje y será la parte imaginaria para cualquier número complejo.

Ejemplo 2.4. Considerando el punto $z = 2 + i$ se ubicará en el plano $\mathbb{C}$ de la siguiente forma:

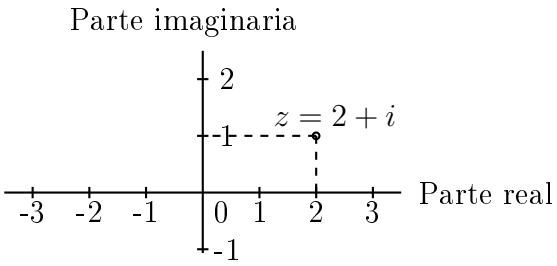


Figura 2.1. Representación geométrica de un punto en el plano complejo.

Definición 2.4. Tomando dos puntos en el plano complejo, $z_1 = a_1 + b_1 i$ y $z_2 = a_2 + b_2 i$, al segmento $z_1 z_2$ dirigido de z_1 a z_2 se llama **vector** y se denota por $\overrightarrow{z_1 z_2}$. Sus coordenadas se calculan de la siguiente forma:

$$a_{\overrightarrow{z_1 z_2}} = a_2 - a_1 \quad y \quad b_{\overrightarrow{z_1 z_2}} = b_2 - b_1.$$

Nota 2.1. Un número $z \in \mathbb{C}$, corresponde a las coordenadas de un vector con punto inicial en el origen de $\mathbb{C}$ y punto final en z, por lo que la notación de vector se omitirá.

Definición 2.5. Se dice que dos vectores son iguales si son paralelos y tienen la misma longitud. A la longitud de un vector $z \in \mathbb{C}$ se le llama **módulo** de z, denotado por $|z|$. El módulo de un número complejo $z = a + bi$ se calcula:

$$|z| = \sqrt{a^2 + b^2}.$$

De esta manera, es fácil mostrar que

$$|z|^2 = z \cdot \overline{z} = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2.$$

Los vectores pueden sumarse, restarse, multiplicarse y dividirse, el módulo de los vectores resultantes de la suma y resta de vectores cumple:

a) $|z_1 + z_2| \leqslant |z_1| + |z_2|$, llamada desigualdad del triángulo.

b) $|z_1 - z_2| \geqslant |z_1| - |z_2|$, esta es consecuencia de la anterior.

La desigualdad del triángulo afirma que ninguno de sus lados puede medir más que la suma de los otros dos, como puede verse en la siguiente figura.

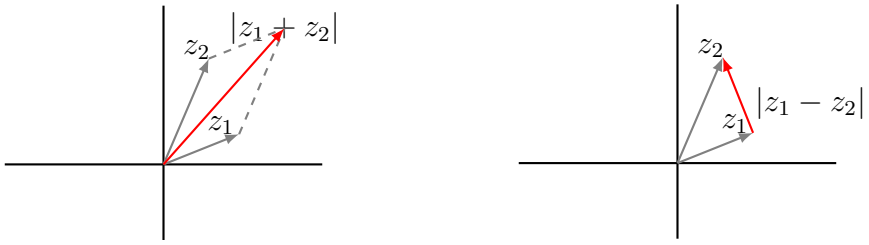


Figura 2.2. Desigualdad del triángulo.

Demostración. De la definición de módulo, se tiene que

$$|z|^2 = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2 \geqslant (\mathrm{Re}(z) + \mathrm{Im}(z))^2, \text{ de donde}$$

$$|z| \geqslant |\mathrm{Re}(z)| + |\mathrm{Im}(z)| \text{ entonces,}$$

Sabemos que

$$|z_1 + z_2|^2 = (z_1 + z_2)\overline{(z_1 + z_2)},$$

considerando el lado derecho de la igualdad, se tiene

$$z_1\overline{z_1} + z_1\overline{z_2} + \overline{z_1}z_2 + z_2\overline{z_2} = |z_1|^2 + 2Re(z_1\overline{z_2}) + |z_2|^2 \leqslant |z_1|^2 + 2|z_1||z_2| + |z_2|^2 = (|z_1| + |z_2|)^2$$

Por lo tanto,

$$|z_1 + z_2| \leqslant |z_1| + |z_2|. \qquad \square$$

Así como representación gráfica, existen funciones de z que tienen un significado geométrico, se tiene entonces que para todo $z \in \mathbb{C}$

- $-z$ rota al 180^o vector z.

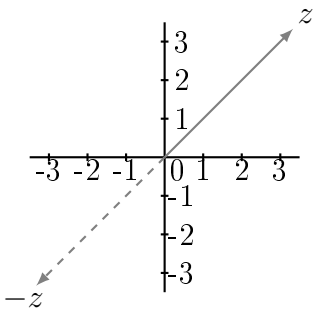


Figura 2.3. Significado Geométrico de $-z$.

- $\alpha z = \alpha z$ aumenta $(\alpha > 1)$ o disminuye $(0 < \alpha < 1)$ el tamaño del vector z.

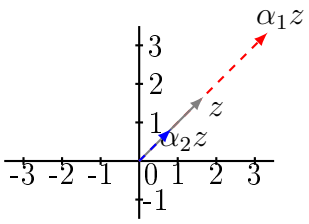


Figura 2.4. Significado Geométrico de αz.

- Conjugado de z, $\overline{z}$: Refleja z con respecto al eje x.

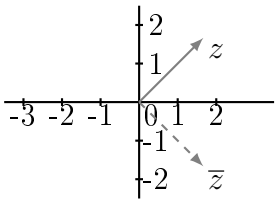


Figura 2.5. Significado Geométrico de $\overline{z}$.

2.2.2. Representación polar

Como vimos anteriormente, los números complejos pueden representarse como vectores en el plano complejo, es decir que tienen un tamaño y una dirección, así como un ángulo.

Definición 2.6. Sea $z \in \mathbb{C} - \{0\}$. Llamaremos al ángulo entre el eje real y el punto z **argumento de z**, que es la función $\arg(z)\colon \mathbb{C} - \{0\} \to \mathbb{R}$ dada por $z \mapsto \arg(z) = \theta + 2\pi n$. Obsérvese que esta no es una función, sino lo que se conoce como *función multivaluada*, es decir que no está definida de forma única, ya que representa infinitos valores cuya diferencia son múltiplos 2π entre cada valor. Para términos prácticos, se utilizará uno de los valores de los ángulos de z, siendo $\arg(z) = \theta$, donde $0 \leqslant \theta < 2\pi$.

De esta manera, es posible separar el vector por componentes, donde la componente x es la parte real y la componente y la parte imaginaria. Siendo entonces $a = |z|\cos(\theta)$ y $b = |z|\text{sen}(\theta)$ para un número $z = a + bi$, como se muestra en la figura 2.6.

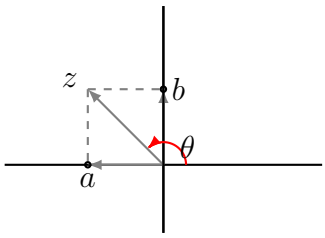


Figura 2.6. Argumento de un número complejo z.

De manera que si $|z|= r$,

$$z = a + bi = r \cdot \cos(\theta) + i \cdot r \cdot \text{sen}(\theta) = r(\cos\theta + i\,\text{sen}\theta).$$

Esta es la **representación polar** de un número complejo z. Gracias a la *fórmula de Euler*:

$$e^{i\theta} = \cos\theta + i\,\text{sen}\theta,$$

con esto podemos escribir a un número complejo $z \neq 0$ como $z = re^{i\theta}$, cuyo conjugado está dado por $\overline{z} = re^{-i\theta}$.

Ejemplo 2.5. Sea $z = -1 + \sqrt{3}i$, se tiene que

$$r = |z|= \sqrt{1+3} = \sqrt{4} = 2$$

y encontrando el ángulo,

$$\varphi = \tan^{-1}(b/a) = \tan^{-1}(\sqrt{3}/-1) = 2\pi/3,$$

entonces $z = 2e^{i2\pi/3}$.

Al multiplicar o dividir vectores, digamos $z_1 = r_1(\cos\varphi_1 + i\text{sen}\varphi_1) = r_1e^{i\theta_1}$ y $z_2 = r_2(\cos\varphi_2 + i\text{sen}\varphi_2) = r_2e^{i\theta_2}$, sucede lo siguiente:

$$z_1 \cdot z_2 = r_1r_2(e^{i(\theta_1+\theta_2)}).$$

Con la división, puede verse que:

$$1/z_2 = \frac{1}{r_2}(e^{-i\theta_2}),$$

entonces

$$z_1/z_2 = r_1/r_2(e^{i(\theta_1-\theta_2)}).$$

Es decir que al multiplicar dos vectores, sus argumentos se suman y el tamaño se multiplica, mientras con la división, el tamaño es el cociente y los argumentos se restan.

Como consecuencia, puede verificarse fácilmente para $z = re^{i\theta}$, la *fórmula de De Moivre*, que cumple:

$$z^n = r^n(\cos(n\theta) + i\text{sen}(n\theta)) \text{ para cada } n \in \mathbb{N}. \tag{2.1}$$

Sabiendo que el ángulo tiene infinitos valores, supóngase ahora que se desea encontrar todos los valores de z tales que

$$w^n = z$$

Entonces encontraremos los valores de w tales que $w = z^{1/n}$, para esto, se utilizarán todos los posibles valores del ángulo de z es decir $\theta + 2\pi m$ con $m \in \{0, \ldots, n-1\}$, así:

$$w = z^{1/n} = r^{1/n}\left(e^{i\left(\frac{\theta+2\pi m}{n}\right)}\right). \tag{2.2}$$

Nota 2.2. La expresión $\sqrt[n]{z}$ es una función multivaluada que pone en correspondencia a todos los números distintos de cero sus n raíces, cada una de ellas dada por un valor de m en la ecuación 2.2. En el caso de $z = 0$ la función $z^{1/n}$ toma un valor único.

A cada valor de la función, dado por un valor de m específico se le llama **rama de la función** multivaluada. En el capítulo 3 estudiaremos la importancia de las ramas de las funciones en la construcción de las superficies de Riemann.

Ejemplo 2.6. Consideremos la función $w(z) = \sqrt[n]{z}$ cuando $z = 1$. Los valores de las raíces están dados por $\epsilon_n = e^{i2\pi/n}$. El conjunto $\{1, \epsilon_n, \epsilon_n^2, \ldots, \epsilon_n^{n-1}\}$ forma un grupo cíclico bajo multiplicación, por lo que las raíces se distribuyen en el plano complejo como los vértices de un polígono regular de n lados inscrito en el círculo unitario.

Así, si z_1 es un valor de $\sqrt[n]{z}$, los otros valores están dados por:

$$z_1, z_1\epsilon_n, z_1\epsilon_n^2, \ldots, z_1\epsilon_n^{n-1}.$$

Ejemplo 2.7. Encontrando los valores de $\sqrt[3]{1+i}$, se tiene $z = 1 + i$, entonces

$$r = \sqrt{2} \text{ y } \varphi = \frac{\pi}{4},$$

$$\sqrt[3]{z} = r^{1/3}\left(e^{\left(i\frac{\pi/4+2\pi m}{3}\right)}\right) == 2^{1/6}\left(e^{\left(i\frac{\pi/4+2\pi m}{3}\right)}\right),$$

para $m = 0, 1, 2$, los valores son

$z_1 = 2^{1/6}\left(e^{\left(i\frac{\pi}{12}\right)}\right)$, $z_2 = 2^{1/6}\left(e^{\left(i\frac{\pi}{12}+\frac{2\pi}{3}\right)}\right) = 2^{1/6}\left(e^{\left(i\frac{9\pi}{12}\right)}\right)$ y $z_3 = 2^{1/6}\left(e^{\left(i\frac{\pi}{12}+\frac{4\pi}{3}\right)}\right) = 2^{1/6}\left(e^{\left(i\frac{17\pi}{12}\right)}\right)$, respectivamente.

Y gráficamente se ve:

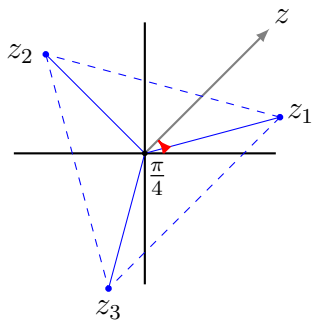


Figura 2.7. Representación geométrica de las raíces cúbicas del número complejo $z = 1+i$.

Aquí se encontraron los tres valores z_i que cumplen con la ecuación polinomial $1 + i - z^3 = 0$, que es equivalente a encontrar las raíces del polinomio $1 + i - z^3$, a continuación, estudiaremos los polinomios en un campo y sus propiedades.

2.3. Polinomios

Nuestros objetos de interés son expresiones de la forma

$$P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

donde los $a_0, a_1, \ldots, a_n$ son elementos del campo F, llamados coeficientes y $a_0 \neq 0$. A estas expresiones las llamaremos **polinomio de grado** n (sobre F), denotado por $P(x)$, al grado de $P(x)$ se le denotará por grad(P). A a_0 se le llama *coeficiente principal del polinomio*, a_n es el *coeficiente constante*.

El teorema de Abel-Ruffini trata sobre la imposibilidad de que exista una fórmula general para encontrar raíces de polinomios de grado mayor o igual a 5 y para entenderlos, estudiaremos las propiedades generales de los polinomios.

Definición 2.7. Se le llama **raíz del polinomio** $P(x)$ a un elemento $a \in F$ que cumple que $P(a) = 0$.

Todos los polinomios sobre cualquier campo pueden ser sumados, restados y multiplicados, obteniendo como resultado nuevos polinomios. A continuación se describirá lo que sucede con el grado y los coeficientes de los polinomios resultantes en cada operación.

Considerando dos polinomios $P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ y $Q(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$ sobre un campo F, entonces

- *Adición y resta*: $P(x) \pm Q(x) = R(x)$, donde el grado de $R(x)$ es a lo más el grado el de mayor grado entre $P(x)$ y $Q(x)$ y los coeficientes de x^k son de la forma $(a_k \pm b_k)$. Entonces $grad(R) \leqslant \text{máx}\{grad(P), grad(Q)\}$

- *Multiplicación*: $P(x) \cdot Q(x) = R(x)$, para calcular el producto, se multiplica cada monomio ax^k del polinomio $P(x)$ por cada monomio bx^l del polinomio $Q(x)$. Este polinomio tendrá como coeficiente principal a_0b_0, que tendrá grado $n + m$ y será de la forma:

$$P(x) \cdot Q(x) = a_0b_0x^{n+m} + (a_0b_1 + a_1b_0)x^{n+m-1} + \ldots + a_nb_m.$$

Al conjunto de polinomios con coeficientes en un campo F se le denota $F[x]$, llamado **anillo de polinomios** con coeficientes en F. Con la suma y multiplicación, puede verse que $F[x]$ es un anillo,[1] a partir de ahora, se utilizarán polinomios con coeficientes en $\mathbb{C}$ con variable z , es decir $\mathbb{C}[z]$.

Nos enfocaremos en polinomios $P(z)$ con coeficientes en $\mathbb{C}$. Para un $z \in \mathbb{C}$, tenemos que $P(z) \in \mathbb{C}[z]$, por lo que podemos considerar su conjugado, $\overline{P(z)}$. En particular, si $P(z) = a_0z^n + a_1z^{n-1} + \ldots + a_{n-1}z + a_n$ donde $z \in \mathbb{C}$ y cada $a_i \in \mathbb{R} \subset \mathbb{C}$, entonces

$$\overline{P(z)} = P(\overline{z}).$$

De donde se puede afirmar, entonces, que si z es una raíz del polinomio $P(z)$ con coeficientes reales, entonces $\overline{z}$, también es raíz de dicho polinomio.

Resulta ser que $\mathbb{C}[z]$ es un dominio euclidiano, [2] por lo que los polinomios en $\mathbb{C}[z]$ pueden ser sumados, restados y multiplicados en un campo F. Y también es posible dividirlos, pero habrán residuos. Es decir que al dividir un polinomio $P(z)$

[1] Se puede estudiar anillos en (Artin, 1991) y (Dummit y Foote, 2004).

[2] Los dominios euclideanos son dominios enteros en los cuales se puede realizar el algoritmo de Euclides, y todos los campos son dominios euclidianos. Más aún, $\mathbb{C}[z]$ es un dominio euclidiano, ver (Gopalakrishnan, 2004).

por un polinomio $Q(z)$, se obtendrá un polinomio $S(z)$ llamado *polinomio cociente* y uno $R(z)$ llamado *residuo*, tales que

$$P(z) = S(z) \cdot Q(z) + R(z)$$

Donde el grado de $R(z)$ será 0 o menor que el de $Q(z)$. Los polinimios cociente $S(z)$ y residuo $R(z)$ se pueden construir a través del **algoritmo de Euclides**[3] para polinomios, que es una serie de pasos finitos.

Descripción del algoritmo de Euclides:

Dados los polinomios

$$P(z) = a_0 z^n + a_1 z^{n-1} + \ldots + a_{n-1} z + a_n \text{ y } Q(z) = b_0 z^m + b_1 z^{m-1} + \ldots + b_{m-1} z + b_m.$$

Si $n < m$ se colocará $S(z) = 0$ y $R(z) = P(z)$, que son el cociente y residuo respectivos.

Sea $n \geqslant m$, entonces considérese el polinomio

$$P(z) \tfrac{a_0}{b_0} z^{n-m} Q(z) = R_1(z).$$

Donde $R_1(z)$ no tiene elementos con z^n, ya que si fuera así, su grado no sería menor que $n-1$ (el máximo valor para m). Entonces consideremos un k tal que $0 < k < n-1$, de manera que

$$R_1(z) = c_0 z^k + c_1 z^{k-1} + \ldots + c_k.$$

Dado que es de grado finito, el procedimiento también lo es, y en algún paso se obtendrá el polinomio

$$R_{s-1}(z) - \frac{d_0}{b_0} z^{l-m} \cdot Q(z) = R_s(z).$$

El algoritmo termina para un s tal que $R_s(z)$ es de grado menor que el de $Q(x)$ o es de grado cero. Escribiendo el algoritmo de forma completa, se tiene:

$$\begin{aligned} P(z) &= \tfrac{a_0}{b_0} z^{n-m} Q(z) + R_1(z) \\ &= \tfrac{a_0}{b_0} z^{n-m} Q(z) + \tfrac{c_0}{b_0} z^{k-m} Q(z) + R_2(z) \\ &\vdots \end{aligned}$$

[3] Análogo al algoritmo euclideano del capítulo 1, para números enteros.

$$= \frac{a_0}{b_0} z^{n-m} Q(z) + \frac{c_0}{b_0} z^{k-m} Q(z) \ldots + \frac{d_0}{b_0} z^{l-m} Q(z) + R_s(z)$$
$$= \left(\frac{a_0}{b_0} z^{n-m} + \frac{c_0}{b_0} z^{k-m} \ldots + \frac{d_0}{b_0} z^{l-m} \right) \cdot Q(z) + R_s(z).$$

Tabla 2.1. Algoritmo de Euclides.

Definición 2.8. Se dice que si un polinomio en un campo F puede expresarse como producto de dos polinomios de menor grado con coeficientes en el campo, es un **polinomio reducible** sobre F. En el caso contrario, se dice que es **irreducible**.[4]

Nota 2.3. Estamos trabajando en el campo $\mathbb{C}$, ya que es el campo más pequeño que contiene a los reales y un elemento cuyo cuadrado es -1, el elemento i. Otra forma de verificar la minimalidad de $\mathbb{C}$, es analizando los polinomios irreducibles en este campo. En $\mathbb{R}$ los polinomios irreducibles son de grado 1 o 2, en particular, los de grado 2 tienen raíces que siempre pertenecen a $\mathbb{R}$ o a $\mathbb{C}$. Por ello, a $\mathbb{C}$ se le conoce como **cerradura algebraica** de $\mathbb{R}$ o bien, $\mathbb{C}$ es la extensión de campos[5] más pequeña que contiene a las raíces de $\mathbb{R}[z]$.

Para encontrar las raíces de un polinomio, se debe resolver la ecuación polinomial $P(z) = 0$, es decir que dado un polinomio

$$P(z) = a_0 z^n + a_1 z^{n-1} + \ldots + a_{n-1} z + a_n$$

encontraremos sus raíces resolviendo la ecuación polinomial

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

Ejemplo 2.8. Un polinomio de grado dos, $az^2 + bz + c$ induce una ecuación cuadrática $az^2 + bz + c = 0$ la cual se resuelve a través de la conocida fórmula de Viète o fórmula cuadrática

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Así, también existen soluciones generales para encontrar las raíces de polinomios de grado 3 y 4. En particular, estudiaremos qué sucede con los polinomios a partir del grado 5. Estas soluciones son funciones multivaluadas, ya que tienen n valores para un polinomio de grado n.

[4] Un polinomio irreducible es el análogo a un número primo en los números enteros $\mathbb{Z}$.
[5] Puede leerse sobre extensiones de campos en (Roman, 2006).

2.4. Curvas continuas en el plano complejo

Las funciones continuas en el plano complejo y sus propiedades nos permitirán pasar a la noción de curvas continuas en el plano, para darnos un enfoque hacia una de las varias demostraciones al teorema fundamental del álgebra, que asegura la existencia de soluciones complejas para una ecuación polinomial con coeficientes complejos.

La noción de continuidad será útil también en el capítulo 3 para extender continuamente funciones analíticas y comprender así la construcción de las superficies de Riemann.

2.4.1. Funciones continuas

Definición 2.9. Sea $f\colon \mathbb{C} \to \mathbb{C}$ una función. Se dice que $f(z)$ es **continua** en z_0 si para cualquier número real $\epsilon > 0$, existe un $\delta > 0$ tal que para todos los z que satisfacen la condición $|z - z_0| < \delta$[6] se cumple la desigualdad:

$$|f(z) - f(z_0)| < \epsilon.$$

Es decir, que si tomamos puntos cercanos, las imágenes también serán cercanas. Existen varios tipos de funciones continuas, entre ellas:

1. Las funciones constantes $f(z) \equiv a$ para un $a \in \mathbb{C}$.

   En efecto, tomemos un z_0, un $\epsilon > 0$ y los elementos del disco $|z - z_0| < \delta$ donde $\delta > 0$, entonces,

   $$|f(z) - f(z_0)| = |a - a| = 0 < \epsilon,$$

   por lo que las funciones constantes son continuas.

2. La función identidad $f(z) = z$ para z complejo y $f(x) = x$ para x. reales.

   Tomando nuevamente $\delta = \epsilon > 0$ y $|z - z_0| < \delta$ como anteriormente, se tiene que

   $$|f(z) - f(z_0)| = |z - z_0| < \delta = \epsilon,$$

   por lo que la función identidad es continua.

Las operaciones entre funciones existen, ya que estas envían elementos $z \in \mathbb{C}$ a nuevos elementos $f(z) \in \mathbb{C}$. A continuación se mostrarán las propiedades de las

[6] La interpretación geométrica de $|z - z_0| < \delta$ es un disco de radio δ, centrado en z_0.

operaciones entre funciones, dadas $f(z)$ y $g(z)$ funciones continuas en z_0 reales o complejas.

1. $h(z) = f(z) \pm g(z)$ es continua en z_0.

   Supongamos $f(z_0) = f_0$ y $h(z_0) = h_0$. Considerando $|f(z) - f_0| < \epsilon/2$ y $|g(z) - g_0| < \epsilon/2$, entonces

   $$|h(z) - h_0| = |(f(z) + g(z)) - (f_0 + g_0)|$$

   $$\leqslant |f(z) - f_0| + |g(z) - g_0| < \epsilon/2 + \epsilon/2 = \epsilon.$$

2. $h(z) = f(z)g(z)$ es continua en z_0. Consideremos

   $$|h(z) - h_0| = |f(z)g(z) - f(z)g_0 + f(z)g_0 - f_0 g_0|$$

   $$\leqslant |f(z)(g(z) - g_0)| + |g(z_0)((f(z) - f_0)| = |f(z)||(g(z) - g_0)| + |g_0||((f(z) - f_0)|.$$

   Como f es continua, podemos escribir $|f(z_0)| > 0$ escogiendo un valor apropiado, digamos $|f(z_0)| = \epsilon_1$, existe un $\delta' < |z - z_0|$ tal que $|f(z) - f(z_0)| < \epsilon_1$, así

   $$|h(z)| = |f(z) - f(z_0) + f(z_0)| \leqslant |f(z) - f(z_0)| + |f(z_0)| < \epsilon_1 + \epsilon_1 = 2\epsilon_1.$$

   Considérese ahora $\epsilon_2 = \epsilon/(4|f(z_0)|)$, y por la continuidad de g, existe un $\delta'' > 0$ tal que si $|z - z_0| < \delta''$, $|g(z) - g(z_0)| < \frac{\epsilon}{4|f(z_0)|}$, entonces

   $$|f(z)||g(z) - g(z_0)| < \epsilon/2$$

   Y de forma similar, se obtiene

   $$|g(z_0)||f(z) - f(z_0)| < \epsilon/2$$

   De esto,

   $$|h(z) - h(z_0)| < \epsilon.$$

   Por lo tanto, $h(z)$ es continua en z_0. Teniendo como consecuencia principal, que la función $f(z) = z^n$ es una función continua, ya que es la multiplicación de$f(z) = z$ n veces.

3. Construyendo un ϵ adecuado, puede mostrarse también que la función $h(z) =$

$1/f(z)$ es continua, por lo que una función $\bar{h}(z) = f(z)/g(z)$ es continua, por ser producto de dos funciones continuas.

Definición 2.10. Sean $f\colon \mathbb{C} \to \mathbb{C}$ y $g\colon \mathbb{C} \to \mathbb{C}$ dos funciones. Se le llama **composición** de las funciones $f(z)$ y $g(z)$ a la función $h(z)$ que satisface, en cada punto z_0, la ecuación $h(z_0) = f(g(z_0))$. Si el valor de $g(z_0)$ no está definido o $f(z)$ no está definida en $g(z_0)$, el valor de $h(z_0)$ tampoco lo está.

4. Si $f(z)$ y $g(z)$ son funciones continuas, también lo es su composición.

   Tomando $z_1 = g(z_0)$ y asumiendo que f es continua en z_1, se tiene que existe $\delta_1 > 0$ tal que si $|z - z_1| < \delta_1$ implica que $|f(z)f(z_1)| > \epsilon_1$ y como g es continua en z_0, existe un $\delta_2 > 0$ tal que si $|z - z_0| < \delta_2$, se tiene que $|g(z) - g(z_0)| < \delta_1$, es decir,

   $$|g(z) - z_1| < \delta_1 \text{ entonces, } |z - z_0| < \delta_2,$$

   por lo que se cumple

   $$|h(z) - h(z_0)| = |f(g(z)) - f(g(z_0))| < \epsilon,$$

   podemos asegurar que todas las expresiones que involucren operaciones entre funciones continuas, son también continuas, en particular, los polinomios son funciones continuas. Para analizar las funciones que expresan las *raíces* de un polinomio, haremos un análisis de la continuidad de la función $f(z) = \sqrt[n]{z}$. Esta función encuentra raíces para polinomios de la forma $w^n = z$.

5. Consideremos la función multivaluada $f(z) = \sqrt[n]{z}$, p para $z \geqslant 0$. Tomaremos entonces una de las ramas de esta función.

   Sea $|z - z_0| < \delta$, debe cumplirse que $|\sqrt[n]{z} - \sqrt[n]{z_0}| < \epsilon$, esto se cumple si y sólo si

   $$-\epsilon < \sqrt[n]{z} - \sqrt[n]{z_0} < \epsilon,$$

   de donde

   $$(\sqrt[n]{z_0})^n - \epsilon < z < (\sqrt[n]{z_0} + \epsilon)^n.$$

   Esta función en particular es estrictamente creciente, lo que quiere decir que si $z < z_1$ entonces $f(z) < f(z_1)$. De la desigualdad anterior, tenemos

   $$(\sqrt[n]{z_0} - \epsilon)^n - z_0 < z - z_0 < (\sqrt[n]{z_0} + \epsilon)^n - z_0.$$

Y supóngase ahora que $\delta = \text{mín}\{x_0 - (\sqrt[n]{z_0} - \epsilon)^n, (\sqrt[n]{z_0} - \epsilon)^n - z_0\}$, que es un número positivo, entonces se cumple la condición de que $|z - z_0| < \delta$. Queda mostrado entonces que cada rama de la función (multivaluada) radical es continua.

Existen otras funciones que son continuas y no son combinaciones de la función constante e identidad o radicales. Un ejemplo de estas, son las funciones trigonométricas seno y coseno, que entran en una clasificación de funciones más amplia, llamada **funciones analíticas**, sobre las cuales se discutirá posteriormente.

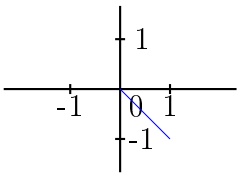
2.4.2. Imágenes de curvas continuas

Otras funciones continuas que son de gran importancia, son las funciones $\alpha\colon\ [0,1] \to \mathbb{C}$ que asignan a un valor $t \mapsto \alpha(t)$, un valor complejo.

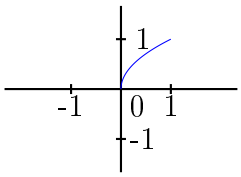
$$\alpha(t) = x(t) + iy(t)$$

Definición 2.11. Si las funciones $x(t)$ y $y(t)$ son continuas para todo valor de t, la imagen de $\alpha = z([0,1])$ es una **curva continua** o **camino** α en $\mathbb{C}$ con punto inicial, $\alpha_0 = \alpha(0)$ y un punto final $z_1 = z(1)$ (tiene orientación). La función $\alpha(t)$ es conocida como **ecuación paramétrica** de la curva.

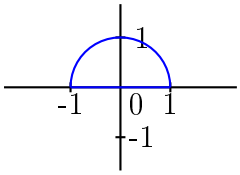
Ejemplo 2.9. A continuación, veremos 3 ejemplos de caminos, dada su ecuación paramétrica.



(a) $\alpha(t) = t - it$



(b) $\alpha(t) = t^2 + it$



(c) $\alpha(t) = \begin{cases} e^{i2\pi t}, & \text{si } 0 \leqslant t \leqslant 1/2 \\ 4t - 3, & \text{si } 1/2 \leqslant t \leqslant 1 \end{cases}$

Para construir ecuaciones que unen dos puntos dados, digamos $z_0 = a_0 + ib_0$ con $z_1 = a_1 + ib_1$. El parámetro t será entonces

$$t = \frac{(x - a_0)}{(a_1 - a_0)} = \frac{(y - b_0)}{(b_1 - b_0)} \text{ cuando } t \in [0,1]\,.$$

La curva que se mueve desde z_0 hacia z_1 está dada por:

$$x = a_0 + (a_1 - a_0)t$$
$$y = b_0 + (b_1 - b_0)t,$$

entonces $\alpha(t) = x(t) + iy(t)$ es de la forma:

$$\alpha(t) = a_0 + (a_1 - a_0)t + (b_0 + (b_1 - b_0)t)i = tz_1 + (1 - t)z_0$$

Sea α_1 la curva descrita por la función $\alpha_1(t)$. Podemos obtener una nueva curva α_2 con las siguientes funciones $\alpha_2(t)$:

1. $\alpha_2(t) = \alpha_1(t) + z_0$ con $z_0 \in \mathbb{C}$.

   La curva α_2 es la curva α_1 trasladada en cada eje por las coordenadas de z_0

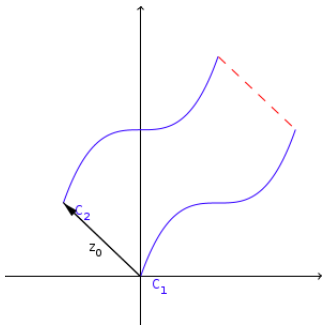


Figura 2.9. Traslación de la curva α_1.

2. $\alpha_2(t) = a \cdot \alpha_1(t)$, donde $a \in \mathbb{R}^+$.

   Sabiendo que $\arg(z_2) = \arg(z_1) + \arg < (z_0)$ y $|z_2| = |z_0| \cdot |z_1|$, dado que $a \in \mathbb{R}$, $\arg(a) = 0$ y la α_2 es la curva α_1 expandida a veces.

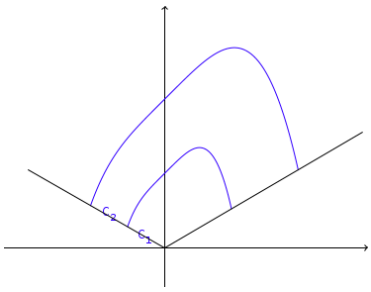


Figura 2.10. Expansión de la curva α_1.

3. $\alpha_2(t) = z_0 \cdot \alpha_1(t)$, donde $|z_0| = 1$.

   Únicamente rota la curva de acuerdo a $\arg(z_0)$ y conserva el tamaño.

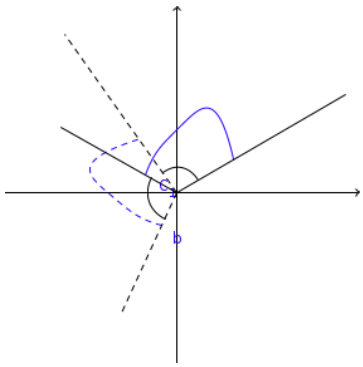


Figura 2.11. Rotación de la curva α_1.

4. $\alpha_2(t) = z_0 \cdot \alpha_1(t)$, donde $z_0 \in \mathbb{C}$.

   Rota la curva un ángulo $\theta = \arg(z_0)$ y la expande o retrae $|z_0|$ veces.

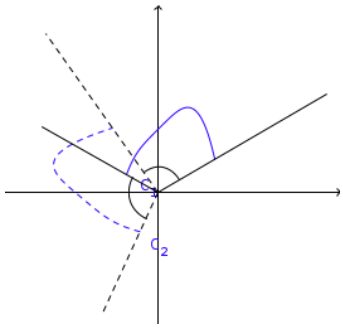


Figura 2.12. Rotación y expansión de la curva α_1 (Homotecia).

5. $\alpha_2(t) = \alpha_1(1-t)$ cuando $t \in [0,1]$, $1-t$ varía en dirección contraria, entonces $\alpha_2 = \alpha_1$ recorrida en dirección contraria.

6. $$\alpha_3(t) = \begin{cases} \alpha_1(2t), & \text{si } 0 \leqslant t \leqslant 1/2 \\ \alpha_2(2t-1), & \text{si } 1/2 \leqslant t \leqslant 1 \end{cases}$$

   La curva α_3 está recorriendo la mitad de su tiempo a toda la curva α_1 y la otra mitad a la curva α_2, donde $\alpha_1(1) = \alpha_2(0)$ para garantizar la continuidad de $\alpha_3(t)$, a esto se le llama **concatenación** de curvas.

Como se vio anteriormente, los vectores tienen un argumento, que es el ángulo entre el eje real positivo y el vector. Dada una ecuación paramétrica $\alpha = \alpha(t)$. La función $\varphi(t)\colon I = [0,1] \to \mathbb{R}$, tal que $t \mapsto \arg(\alpha(t))$, que estará bien definida si imponemos la condición inicial $\theta_0 = \arg(z_0)$.

Ejemplo 2.10. La ecuación paramétrica $\alpha(t) = \cos \pi t + i\text{sen}\pi t = e^{i\pi t}$ describe un semicírculo en el plano y la función $\arg(\alpha(t)) = \pi t$ describe de manera continua el argumento de cada vector $\alpha(t)$.

Uno de los valores del argumento de esta función es $\arg(\alpha(t)) = \pi t$ y considerando que $\arg(\alpha(t))$ es una función multivaluada, entonces los otros valores del argumentos están dados por $\arg(\alpha(t)) = \pi t + 2\pi k$. Definimos el argumento inicial $\arg(z_0) = 0$, entonces

$$0 = \arg(\alpha(0)) = 2\pi k,$$

esto se cumple sólo para $k = 0$, entonces $\arg(\alpha(t)) = \pi t$.

Si se define un nuevo valor para $\arg(\alpha(0)) = 2\pi$, entonces

$$2\pi = \arg(\alpha(0)) = 2\pi k$$

esto se cumple sólo para $k = 1$, entonces $\arg(\alpha(t)) = \pi t + 2\pi$ y puede construirse así cualquier condición inicial para $\arg(\alpha(0)) = 2\pi k$.

La función $\varphi(t) := \arg(\alpha(t))$ describe cómo varía $\arg(\alpha(t))$ a lo largo de una curva. Al cambio del argumento desde $\alpha(0)$ hasta $\alpha(1)$, se le llama **variación del argumento** a lo largo de la curva α con ecuación paramétrica $\alpha(t)$ denotada por $\text{var}(\alpha) = \varphi(1) - \varphi(0)$. Esta función cumple las siguientes proposiciones:

Proposición 2.1. *Si la curva α dada por $\alpha(t)$ no pasa por el origen de coordenadas y en su punto inicial, el argumento de la curva es φ_0. Es posible escoger un valor del argumento para todos los puntos de la curva α de manera que a lo largo de la curva,* $\arg(\alpha(t))$ *cambia continuamente, comenzando por φ_0. Es decir que para cada $t \in [0, 1]$ se puede escoger un valor de $\varphi(t)$ de manera que sea continua para cada t , con punto inicial φ_0.*[7]

Proposición 2.2. *Si dos funciones distintas $\varphi_1(t)$ y $\varphi_2(t)$ describen la variación continua de* $\arg(\alpha(t))$ *a lo largo de la curva α. La diferencia entre estas no depende de t, es decir: $\varphi_1(t) - \varphi_2(t) = 2\pi k$*

Demostración. Si k dependiera de t, se tendría:

$$k(t) = \frac{\varphi_1(t) - \varphi_2(t)}{2\pi}.$$

Donde $k(t)$ sería una función continua $\forall\, t \in [0, 1]$ y sabemos que esta diferencia es un número entero, esto si y sólo si $k(t) = 0$ o $k(t) = k$ donde k es constante. □

[7] La prueba de esta afirmación puede verse con detalle en (Chinn y Steenrod, 1966).

Proposición 2.3. *Al escoger $\varphi_0 = \varphi(0)$, la función $\varphi(t)$ queda definida de manera única. Y la diferencia $\varphi(t) - \varphi(0)$ está únicamente definida por la función $\alpha(t)$ y no depende de la elección de $\varphi(0)$.*

Demostración. Sean $\varphi_1(t)$ y $\varphi_2(t)$ dos funciones que describen la variación de $\arg(z(t))$ tales que $\varphi_1(0) = \varphi_2(0) = \varphi_0$, por la proposición anterior, se cumple

$$\varphi_1(t) - \varphi_2(t) = 2\pi k,$$

entonces $\varphi_1(t) - \varphi_2(t) = 0$ o $\varphi_1(t) - \varphi_2(t) = 2\pi k$.

Si $\varphi_1(0) - \varphi_2(0) = 0$, entonces $\varphi_1(t) = \varphi_2(t)$.

Si $\varphi_1(0) - \varphi_2(0) = 2\pi k$, entonces $\varphi_1(t) - \varphi_1(0) = \varphi_2(t) - \varphi_2(0) = 2\pi k = \varphi(t)$ está definido de manera única. □

Ejemplo 2.11. Calcularemos la variación de $\varphi(t)$ a lo largo de la curva $\alpha(t) = e^{i\pi t}$.

Anteriormente se encontró que para esta ecuación, uno de los valores de $\arg(\alpha(t)) = \pi t$, entonces calculando la diferencia, se tiene:

$$\varphi(t) - \varphi(0) = \pi t - 0 = \pi t.$$

Ejemplo 2.12. Al observar un camino en $\mathbb{C}$, puede calcularse la variación de su argumento fijándose en el punto inicial, final y su orientación.

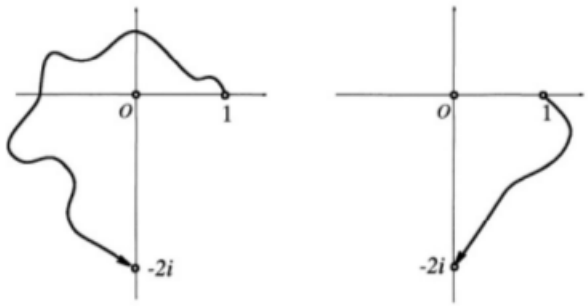


Figura 2.13. Calculando la variación del argumento a lo largo de una curva.

.

Puede observarse en la Figura 2.13, que las curvas coinciden en el punto inicial y en el punto final, sin embargo, la dirección en que se recorren hace que la variación del argumento a lo largo de ellas cambie. En la primera tenemos $\varphi(t) - \varphi(0) = 3\pi/2 - 0 = 3\pi/2$, mientras que para la segunda, la variación del argumento es $\varphi(t) - \varphi(0) = -\pi/2 - 0 = -\pi/2$.

Definición 2.12. Una curva o camino es **cerrado** o un **lazo** si la función que la describe cumple que $\alpha(0) = \alpha(1) = x$, con **punto base** x.

Sea α un lazo que no pasa por $z_0 \in \mathbb{C}$, $\text{var}(C) = 2\pi k$, donde k determina el número de vueltas que el camino da alrededor de z_0.

Pueden considerarse traslaciones de la forma $\alpha_2(t) = \alpha(t) - z_0$ y así, si el camino α da k vueltas alrededor de z_0, el nuevo camino α_2 da k vueltas alrededor del origen. Al número de vueltas que da una curva alrededor de un z_0 dado, se le llama **índice de la curva** (alrededor de z_0).

Ejemplo 2.13. Calcularemos el índice de la curva $\alpha(t) = \frac{1}{2}e^{4\pi t}$ alrededor de $z = 0$, de $z = 1$ y $z = 1/4$. Esta función describe un círculo de radio 1 centrado en el origen, donde $\text{var}(C) = 4\pi - 0 = 4\pi = 2(2\pi)$, entonces pasa 2 veces alrededor del origen.

En el caso de $z = 1/4$, sabemos que está dentro del círculo de radio $r = 1/2$, por lo tanto, la curva también lo rodea 2 veces, mientras $z = 1$ está fuera de la curva descrita, por lo que no es rodeada por esta.

Ejemplo 2.14. En la siguiente figura observaremos los índices respectivos a los puntos $z = 0$ y $z = 1$:

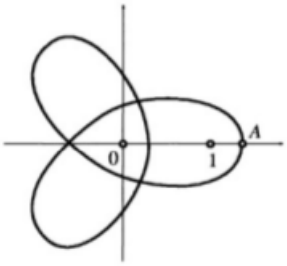


Figura 2.14. Análisis de la variación del argumento a lo largo de una curva desde distintos puntos. Fuente: tomada de (Alekseev, 2004, Cap. 2).

- $z = 0$. Al dividir la curva en dos, la variación de cada parte es 2π, entonces el total son 2 vueltas alrededor del origen.
- $z = 1$. En la primera parte, no rodea ninguna vez al uno, ya que la curva no "encierra" a este punto, sin embargo, añadiendo la segunda parte se obtiene que la variación de la curva total alrededor de $z = 1$ es 2π por lo que lo rodea 1 vez.

La variación del argumento también depende de las operaciones entre ecuaciones de curvas. Supóngase que se tienen dos caminos α_1 y α_2 dados por $\alpha_1(t)$ y

$\alpha_2(t)$ y variaciones de argumento a lo largo de la curva φ_1 y φ_2 respectivamente. Se calculará la variación del argumento a lo largo de la curva α si su ecuación es:

1. $\alpha(t) = \alpha_1(t) \cdot \alpha_2(t)$.

   Dado que $\alpha_1\alpha_2$ suma $\arg(\alpha_1) + \arg(\alpha_2)$, entonces $\varphi(t) = \varphi_1(t) + \varphi_2(t)$.

2. $\alpha(t) = \alpha_1(t)/\alpha_2(t)$.

   Análogamente, la división de α_1/α_2 resta $\arg(\alpha_1) - \arg(\alpha_2)$, por lo que $\varphi(t) = \varphi_1(t) - \varphi_2(t)$.

Consideremos un camino α descrito por la ecuación paramétrica $\alpha(t)$ y una función continua $f\colon \mathbb{C} \to \mathbb{C}$ tal que $\alpha(t) \mapsto w = f(\alpha(t))$. En el plano z se tendrá al camino α, mientras en el plano w tendremos un nuevo amino, al cual llamaremos **imagen continua del camino** α bajo f, denotado por $f(\alpha)$.

Ejemplo 2.15. Sea un camino α con ecuación $\alpha(t) = 0.7\left(e^{i\pi t/2}\right)$ y una función $w = f(z) = z^2$. La curva α describe un cuarto de círculo de radio 0.7 en el plano z, ya que su argumento varía $\pi/2$. Al considerar f, se tiene $f(z) = z^2 = (0.7)^2 e^{i\pi t}$, que describe un semicírculo de radio 0.7^2 en el plano w, la variación del argumento de $f(\alpha)$ es el doble de la de α.

(a) Plano z **(b)** Plano w

Figura 2.15. Imagen continua en el plano w de un camino en el plano z.

En general, si la variación del argumento a lo largo del camino α es φ, entonces cuando $f(z) = z^n$, la variación del argumento de $f(\alpha)$ es $n\varphi$. Y si la curva da k vueltas alrededor del origen en el plano z, entonces la función $f(\alpha)$ dará kn vueltas alrededor del origen en el plano w, esto se debe a la fórmula de De Moivre (2.1).

Ejemplo 2.16. Otras funciones que dependen de z pueden determinar la cantidad de vueltas que da una curva alrededor de un punto.

Sea α una curva en el plano, para la cual se conoce cuántas veces rodea a un conjuntos de puntos $\{z_i\}$ con $i = 1, 2, \ldots, n$. Consideraremos las siguientes funciones $f(z)$. Si los índices alrededor de $z = 0$, $z = 1$, $z = i$, $z = -i$ son k_1, k_2 :

a) $f(z) = z^2 - z$.

Se puede factorizar $z^2 - z = z(z-1)$ entonces igualando a cero, se tiene $z = 0$ o $z = 1$ ambas aparecen con potencia 1, de donde:

$$\text{var}(\alpha) = 2\pi k_1 + 2\pi k_2 = 2\pi(k_1 + k_2),$$

por lo que $f(z)$ da $k_1 + k_2$ vueltas alrededor de $w = 0$.

b) $f(z) = z^2 + 1$.

Factorizando, se obtiene $f(z) = (z - i)(z + i)$, por lo que var(C) está dada por

$$\text{var}(\alpha) = 2\pi(k_3 + k_4),$$

entonces la función rodea a $w = 0$ $k_3 + k_4$ veces.

c) $f(z) = (z^2 + iz)^4$.

Al factorizar esta función, tenemos $(z(z + i))^4$ en esta función, la variación del argumento alrededor de los puntos $z = 0$ y $z = -i$ se multiplica por 4, debido a la potencia. Por lo que

$$\text{var}(\alpha) = 4(2\pi k_1 + 2\pi k_4) = 2\pi(4(k_1 + k_4)),$$

así, la función rodea a $w = 0$, $4(k_1 + k_4)$ veces.

d) $f(z) = z^3 - z^2 + z - 1$.

Esta función es $z^2(z-1) + (z-1) = (z^2+1)(z-1) = (z+i)(z-i)(z-1)$.

Haciendo un cálculo similar a los anteriores, se obtiene que la curva pasará $k_2 + k_3 + k_4$ veces alrededor de $w = 0$.

2.5. Teorema fundamental del Álgebra

Para encontrar soluciones de ecuaciones polinomiales, es necesario saber que éstas existen y el teorema fundamental del Álgebra (FTA por sus siglas en inglés) asegura que todo polinomio $P(z) \in \mathbb{C}[z]$ tiene al menos una raíz en $\mathbb{C}$. Con las ideas anteriores, se presentará un esbozo de la demostración.

Teorema 2.5.1 (Teorema Fundamental del Álgebra)**.** *La ecuación*

$$a_0 z^n + a_1^{n-1} + \ldots + a_{n-1} z + a_n = 0,$$

donde todos los a_is son números complejos arbitrarios, $n \geqslant 1$, y $a_0 \neq 0$, tiene al menos una raíz compleja.[8]

Demostración. (Esbozo) Sea $w = f(z) = a_0 z^n + a_1^{n-1} + \ldots + a_{n-1}z + a_n = 0$, una función continua cuya imagen es una curva, denotaremos por A al máximo valor de las normas de los a_i, es decir $A = \text{máx}\{|a_0|, |a_1|, \ldots, |a_n|\}$ y números reales $c > 0$, $R_1 \leqslant 1$ y $R_2 > 1$ tales que cumplen:

$$R_1 > |a_n|/(cAn) \qquad R_2 > cAn/|a_0|$$

Y analizaremos qué sucede cuando $|z| = R_1$ y cuando $|z| = R_2$, donde $z(t) = Re^{i2\pi t}$ es una curva cerrada en el plano complejo z, cuya imagen también será una curva cerrada en el plano w

- Si $|z| = R_1$, entonces se cumple

$$|a_0 z^n + \ldots + a_{n-1}z| \leqslant |a_0 z^n| + \ldots + |a_{n-1}z|$$

$$= |a_0||z^n| + \ldots + |a_{n-1}||z| \leqslant A(R_1^n + \ldots + R_1)$$

$$\leqslant A(nR_1), \text{ ya que } R_1 \leqslant 1 < An\left(\frac{|a_n|}{Anc}\right) = \frac{|a_n|}{c},$$

  tenemos el polinomio inicial $|f(z) - a_n| = |a_0 z^n + \ldots + a_{n-1}z| < \frac{|a_n|}{c}$.

  Esto es un círculo en el plano w, centrado en a_n con radio suficientemente pequeño como para no cubrir a $w = 0$, ya que $\frac{|a_n|}{c}$ con $c > 0$, entonces la cantidad de vueltas alrededor de $w = 0$ es 0.

- Por otro lado, si $|z| = R_2$, se tiene que

$$|\frac{a_1}{z} + \ldots + \frac{a_n}{z^n}| \leqslant |\frac{a_1}{z}| \ldots + |\frac{a_n}{z^n}|$$

$$= \frac{|a_1|}{|z|} + \ldots + |\frac{|a_n|}{|z^n|} \leqslant \frac{|a_1| + \ldots + |a_n|}{R_2}, \text{ya que} R_2 > 1$$

$$< \frac{nA}{R_2} = \frac{nA|a_0|}{cAn} = \frac{|a_0|}{c},$$

  tenemos el polinomio inicial $|f(z)/z^n - a_0| = |\frac{a_1}{z} + \ldots + \frac{a_n}{z^n}| < \frac{|a_0|}{c}$ cuando z recorre la curva C con radio R_2 en el plano z, la variación del argumento de

[8] Puede verse una demostración más formal en (Ahlfors, 2004), (Dejon y Henrici, 1969) y (Fraleigh y Katz, 2003).

la función $f(z)/z^n$ se hace 0, ya que en $f(z)$, $\varphi = 2\pi n$ y para z^n, $\varphi = 2\pi n$, la resta de estos es cero. Pero, sabemos que$f(z) = f(z)/z^n \cdot z^n$ y utilizando las propiedades de la variación del argumento a lo largo de la curva, obtenemos la suma de las variaciones $0 + 2\pi n$, por lo que la curva, $f(C)$ da n vueltas alrededor de $w = 0$.

Si ahora aumentamos el radio R de R_1 a R_2, tomamos un radio R_* tal que $R_1 < R_* < R_2$ y entonces la imagen $f(C_R)$ puede ser continuamente deformada de $f(C_{R_1})$ a $f(C_{R_2})$. Si $f(C_{R_*})$ no pasa por el punto $w = 0$ se puede hacer pequeñas variaciones en el radio de manera que la cantidad de vueltas alrededor de $w = 0$ no varía, ya que la variación del argumento a lo largo de una curva es continuo y anteriormente se mostró que para ser continuo sólo puede ser una constante, sin embargo, también encontramos que para R_1 la cantidad de vueltas es 0 y para R_2 es n, lo cual contradice la continuidad. Esta contradicción viene a partir de asumir que la curva no pasa por $w = 0$, entonces debe existir $z \in \mathbb{C}$ tal que $f(z) = 0$. □

A continuación veremos algunas consecuencias del TFA y propiedades de las raíces de los polinomios en $\mathbb{C}[z]$.

Teorema 2.5.2. *Si z_0 es raíz de la ecuación $a_0z^n + a_1^{n-1} + \ldots + a_{n-1}z + a_n = 0$, entonces el polinomio $a_0z^n + a_1^{n-1} + \ldots + a_{n-1}z + a_n$ es divisible por el binomio $z - z_0$ sin residuo.*

Demostración. Suponiendo que existe un residuo, por el algoritmo de la división, tenemos que

$$P(z) = Q(z)(z - z_0) + r$$

y por ser z_0 raíz de $P(z)$, entonces $P(z_0) = 0$, entonces sustituyendo $z = z_0$, se obtiene

$$0 = P(z_0) = Q(z_0)(z_0 - z_0) + r$$

Por lo que $r = 0$ entonces no existe residuo y, por consiguiente, el binomio $(z - z_0)$ divide a $P(z)$. □

Corolario 2.5.1. *El polinomio $a_0z^n + a_1^{n-1} + \ldots + a_{n-1}z + a_n$, donde $a_0 \neq 0$, puede representarse en la forma*

$$a_0z^n + a_1^{n-1} + \ldots + a_{n-1}z + a_n = a_0(z - z_1)(z - z_2)\ldots(z - z_n).$$

El polinomio $P(z)$ descompuesto en factores es igual a cero solo si al menos uno de los factores es igual a cero, es decir z_i es una raíz de $P(z)$, para ciertos números complejos $z_1, z_2, \ldots, z_n$, entonces las raíces de $P(z)$ son precisamente $z_1, z_2, \ldots, z_n$.

Para encontrar los polinomios irreducibles en los números reales necesitamos saber en qué momento los polinomios con coeficientes reales dejan de tener raíces en $\mathbb{R}$, para esto, se encontrarán los polinomios irreducibles en $\mathbb{R}[z]$.

Supongamos entonces que el polinomio $P(x) = a_0z^n + a_1z^{n-1} + \ldots + a_{n-1}z + a_n \in \mathbb{R}[z]$ tiene una raíz $z_0 \in \mathbb{C}$, entonces también $\overline{z_0}$ es raíz y del Corolario 2.5.1, podemos expresar a $P(z)$ como:

$$P(z) = Q(z)(z - z_0)(z - \overline{z_0}),$$

donde

$$(z - z_0)(z - \overline{z_0}) = z^2 - zz_0 + z_0\overline{z_0} - z\overline{z_0} = z^2 - 2zRe(z_0) + |z_0|,$$

que es un polinomio de grado 2 con coeficientes reales. Lo que implica que un tipo de polinomios irreducibles en $\mathbb{R}$ son los cuadráticos que tienen raíces complejas.

Por otro lado, para factorizar un polinomio con coeficientes reales en polinomios irreducibles, podemos escribir

$$P(z) = Q(z)(z - z_0),$$

donde z_0 es una raíz para la cual se tienen dos casos

a) $z_0 \in \mathbb{R}$.

b) $z_0 \in \mathbb{C}$.

Si se da el caso a), este factor será de grado 1 y se procede a buscar la siguiente raíz, de manera que

$$P(z) = Q'(z)(z - z_0)(z_1),$$

para la cuela pueden darse, de nuevo los dos casos anteriores.

En el caso b), la siguiente raíz es el conjugado, por lo que $P(z)$ tiene como factor a un polinomio de grado 2 y se procede con las siguientes raíces. Este procedimiento es finito, ya que el polinomio inicial es de grado n.

Como resultado de esto, se tiene que en $\mathbb{R}$ los polinomios irreducibles son de grado 1 o 2, mientras en $\mathbb{C}$, todos son de grado 1.

Definición 2.13. Sea z_0 una raíz de la ecuación,

$$a_0 z^n + a_1^{n-1} + \ldots + a_{n-1} z + a_n = 0.$$

se dice que z_0 es una **raíz de multiplicidad k** si el polinomio $a_0 z^n + a_1^{n-1} + \ldots + a_{n-1} z + a_n$ es divisible por $(z - z_0)^k$ y no por $(z - z_0)^{k+1}$.

Una afirmación equivalente al teorema fundamental del álgebra es que todo polinomio de grado n tiene n raíces complejas, contando su multiplicidad.

Ejemplo 2.17. En la ecuación

$$z^5 - z^4 - 2z^3 + 2^2 + z - 1 = 0$$

tenemos,

$$z^5 - z^4 - 2z^3 + 2^2 + z - 1 = (z^4 - 2z^2 + 1)(z - 1) = (z^2 - 1)^2 (z - 1) = (z + 1)^2 (z - 1)^3 = 0$$

tiene dos raíces $z = 1$, de multiplicidad 3 y $z = -1$, de multiplicidad 2.

Definición 2.14. Sea $P(z) = a_0 z^n + a_1^{n-1} + \ldots + a_k z^{n-k} + \ldots + a_{n-1} z + a_n$ un polinomio, se le llama **derivada** de $P(z)$ al polinomio

$$P'(z) = a_0 n z^{n-1} + a_1 (n-1) z^{n-2} + \ldots + a_k (n-k) z^{n-k-1} + \ldots + a_{n-1}$$

A la derivada, la denotaremos por el símbolo $'$ (prima).

Las derivadas también son polinomios y tienen propiedades distintas, considerando los polinomios $P(z)$ $Q(z)$ y c una constante, se cumple:

1. $(P(z) + Q(z))' = P'(z) + Q'(z)$
2. $(c \cdot P(z))' = c \cdot P'(z)$
3. $(P(z)Q(z))' = P'(z)Q(z) + P(z)Q'(z)$
4. Si $P(z) = (z - z_0)^n$ entonces $P'(z) = n(z - z_0)^{n-1}$

Proposición 2.4. *Si la ecuación $P(z) = 0$ tiene una raíz z_0 de multiplicidad $k > 1$, entonces la ecuación $P'(z) = 0$ tiene raíz z_0 de multiplicidad $k - 1$ y si la ecuación $P(z) = 0$ tiene una raíz z_0 de multiplicidad 1, entonces $P'(z_0) \neq 0$.*

Demostración. Como z_0 es raíz de multiplicidad k, entonces podemos expresar $P(z)$ como

$$P(z) = (z - z_0)^k Q(z)$$

Entonces, por las propiedades anteriores, se tiene

$$P'(z) = ((z - z_0)^k)'Q(z) + (z - z_0)^k Q'(z) = k(z - z_0)^{k-1}Q(z) + (z - z_0)^k Q'(z),$$

donde $kQ(z) + (z - z_0)Q'(z)$ no es divisible por $(z - z_0)^k$, ya que $Q(z)$ no es divisible por $(z - z_0)$. Por lo tanto, $P'(z)$ es divisible por $(z - z_0)^{k-1}$ pero no por $(z - z_0)^k$, es decir, z_0 es raíz de multiplicidad $k - 1$. □

3. SUPERFICIES DE RIEMANN

El teorema de Abel-Ruffini habla sobre la imposibilidad de encontrar una fórmula general para calcular las raíces de polinomios de grado mayor o igual a cinco. Por el teorema fundamental del álgebra, todo polinomio de grado n tiene exactamente n soluciones hasta por su multiplicidad. Entonces las fórmulas que sirven para encontrar estas raíces deben tener más de un valor. Recordando que una función es una correspondencia entre los conjuntos A y B que asigna a $a \in A$ un único elemento $f(a) = b \in B$.

A las «funciones» que admiten más de un valor a estas les llamamos funciones *multivaluadas* y las denotaremos por $f\colon A \nrightarrow B$. Para convertir éstas en funciones genuinas necesitamos extender su dominio considerando sus ramas continuas y univaluadas. Al pegar estas ramas se construirá un nuevo dominio llamado *superficie de Riemann*, en honor al matemático alemán Bernhard Riemann. Estas superficies nos darán la intuición geométrica para analizar conceptos algebraicos como el grupo de monodromía de las funciones que hemos trabajado en el capítulo anterior. Se estudiarán también las propiedades de estas funciones, como subconjunto de las funciones analíticas, para construir las superficies de Riemann a través de la continuación analítica, en particular se construirán éstas para funciones solubles por radicales.

Para ello, estudiaremos primero los conceptos topológicos básicos que nos ayudarán a entender la construcción de superficies a través de uniones disjuntas o copias del plano complejo[1] $\mathbb{C}$. Posteriormente estudiaremos las funciones algebraicas, particularmente las solubles por radicales y su continuación analítica, así como la propiedad de monodromía para dar una construcción abstracta para las superficies de Riemann.

[1] A partir de ahora trabajaremos con $\mathbb{C}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ o $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ según convenga, como dominios y contradominios.

3.1. Conceptos topológicos

Para tener la noción de lo que es una superficie y saber específicamente qué son las superficies de Riemann, es necesario conocer algunos conceptos topológicos generales.

3.1.1. Topología general

Comenzaremos con la noción de topología y las relaciones entre espacios topológicos. Dado un conjunto X, una **topología** τ es una familia de subconjuntos de X que cumplen con tres propiedades:

1. $X \in \tau$ y $\emptyset \in \tau$.

2. Si $A_i \in \tau$, $\bigcup_{i \in I} A_i \in \tau$, con $i \in I$, un conjunto arbitrario de índices.

3. Si A_1 y $A_2 \in \tau$, entonces $A_1 \cap A_2 \in \tau$.

Al par (X, τ) se le llama espacio topológico y a los elementos de τ se les llama conjuntos **abiertos**.

Ejemplo 3.1.

1. $(\mathbb{R}, \tau)$ es un espacio topológico donde τ es la topología usual en $\mathbb{R}$ (generado por intervalos abiertos).

2. $(\mathbb{C}, \tau)$ donde τ es generada por discos abiertos centrados en un punto z (usaremos $z \in \mathbb{C}$), con radio $r > 0$.

En el capítulo anterior se dio una definición de función continua para $\mathbb{R}$ y $\mathbb{R}^2$, en general, una función $f\colon X \to Y$ es continua si dado un abierto V de Y, su preimagen $f^{-1}(V)$ es un abierto en X. Una forma de considerar equivalencias entre espacios topológicos es que existan *homeomorfismos* entre ellos. Escribimos $X \approx Y$ y decimos que X es homeomorfo a Y.

Definición 3.1. Un **homeomorfismo** entre dos espacios X y Y, es una biyección $f\colon X \to Y$ tal que f y f^{-1} son continuas.

3.1.2. Uniones disjuntas y espacios de identificación

En algunas ocasiones, necesitamos tomar dos valores donde hay uno único, para generar el segundo, usaremos las uniones disjuntas.

Definición 3.2. Dados dos conjuntos X, Y, su **unión disjunta** es

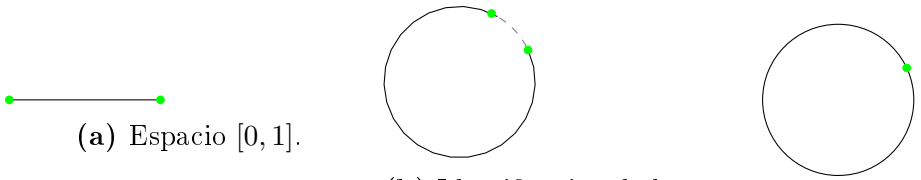
$$X \sqcup Y := X \times \{1\} \cup Y \times \{2\}.$$

El producto con 1 y 2 sirve cuando un punto x está en ambos conjuntos, es decir, $X \cup Y$. En este caso, la unión disjunta lo convierte en dos puntos: $(x, 1)$ y $(x, 2)$. Esta diferencia es aún más útil cuando hacemos una unión disjunta de dos o más copias de un solo conjunto. En general,

$$\bigsqcup_k U_k = \bigcup_k U_k \times \{k\}.$$

Este proceso nos ayuda a construir conjuntos o *espacios* más grandes. Para el propósito contrario, tenemos los espacios de identificación. En topología existe el concepto de *pegar* puntos o subespacios.

Ejemplo 3.2. Por ejemplo, tomaremos el segmento $[0, 1]$ y pegaremos o identificaremos el 0 con el 1, esto se verá como un círculo.



(a) Espacio $[0, 1]$.

(b) Identificación de los puntos 0 y 1.

(c) Espacio de identificación.

Figura 3.1. Círculo como espacio de identificación del segmento $[0, 1]$.

Así, obtenemos un nuevo espacio homeomorfo a un círculo, esto sucede cuando a este cociente le ponemos una topología particular, la *topología cociente*, tomaremos la idea de este ejemplo anterior para definir el *pegado* o identificación.

Definición 3.3. Sea X un espacio topológico y $\sim$ una relación de equivalencia que particiona a X en clases de equivalencia. Definimos a $Y := X/\sim$ como el conjunto de clases de equivalencia inducidas por la relación $\sim$, obteniendo una función sobreyectiva $\phi\colon X \to Y$. Dotaremos de una topología a Y, llamada **topología cociente** o **de identificación**. Esta topología cumple:

- Un subconjunto $V \subseteq Y$ es abierto si y sólo si $p^{-1}(V)$ es abierto en X.

Al espacio Y con la topología cociente, le llamamos **espacio cociente** o **espacio de identificación**.

En el ejemplo 3.2, había una clase de equivalencia con los elementos $\{0, 1\}$ y las demás clases eran los conjuntos singulares, cada uno con un punto del segmento $(0, 1)$, de esta forma estamos identificando a los puntos 0 y 1. Podemos probar que $[0, 1]/0 \sim 1 \approx S^1$, considerando la función

$$f\colon [0,1] \to S^1$$

$$t \mapsto e^{2\pi i t}.$$

Estas herramientas nos ayudarán a modificar los dominios para ciertas funciones que veremos en la siguiente sección. Es de particular interés el tratamiento de superficies, pues los dominios que formaremos son objetos de este tipo.

Definición 3.4. Una **superficie** es un espacio de *Hausdorff*,[2] *segundo numerable*,[3] donde todo punto tiene una vecindad homeomorfa a una bola en $\mathbb{R}^2$.

En particular, nos interesan las superficies conexas por caminos y compactas, ya que las superficies con las que trabajaremos son de este tipo. No incluimos la prueba de esto por lo que referimos al lector a (Ahlfors y Sario., 1960).

Definición 3.5. Decimos que un espacio es **conexo por caminos** si para cada par de puntos z_0 y z_1 existe un camino C en X que une a z_0 con z_1.

Definición 3.6. Una colección $\mathcal{A} = \{U_i\}_{i \in I}$ de abiertos en un espacio X tales que $\cup_i U_i = X$ se llama **cubierta abierta** de X. Una subcolección $\mathcal{B} \subset \mathcal{A}$ se llama **subcubierta** si la unión de sus elementos también es todo el espacio X. Decimos que X es **compacto** si cualquier cubierta abierta admite una subcubierta finita. Intuitivamente, quiere decir que al tomar dos puntos en el espacio, podemos acercarnos de uno al otro en una cantidad finita de pasos, sin escapar al infinito.

Nota 3.1. Hay espacios que no son compactos, como el plano. Estos espacios pueden ser compactificados agregando elementos. La razón por la que agregamos el punto ∞ al plano complejo $\mathbb{C}$, es que $\hat{\mathbb{C}}$ es homeomorfo a una esfera, como se vio en el capítulo anterior, y las esferas son objetos compactos.

[2] Un espacio de Hausdorff si para cada dos puntos distintos p y q existe una vecindad $U(p)$ y $V(q)$ tales que $U \cap V = \emptyset$. (Dugundji, 1978, cap VII).

[3] Un espacio es segundo numerable si tiene una base numerable (Dugundji, 1978, cap. VIII).

3.2. Funciones algebraicas

Los polinomios, las funciones racionales y las radicales son ejemplos de lo que se llaman funciones solubles por radicales.

Definición 3.7. En general, decimos que una función $h(z)\colon \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ es **soluble por radicales** si puede ser escrita en términos de la función $f(z) = z$ y de funciones constantes $g(z) = a$, con $a \in \mathbb{C}$, a través de operaciones como suma, resta, multiplicación, división, potencias y raíces enteras. Por ejemplo, la función $h(z) = (\sqrt[3]{\sqrt{z} + 5z^4} - 6/\sqrt{z})^4$ es soluble por radicales.

Las funciones solubles por radicales pertenecen a una clase de funciones llamadas algebraicas, estas funciones nos interesan, ya que para este tipo de funciones es posible construir una superficie de Riemann por continuación analítica, método que describiremos en la sección 3.3.

Definición 3.8. Una función en una variable $w(z)$ es una **función algebraica** si es solución de una ecuación algebraica cuyos coeficientes $P_k(z)$ son polinomios en la misma variable, de la forma:

$$F(z, w) = P_n(z)w^n + P_{n-1}(z)w^{n-1} + \ldots + P_o(z) = 0 \tag{3.1}$$

Asumiremos, sin perder la generalidad, que $P_n(z) \equiv 1$.

Nota 3.2. Las funciones algebraicas son un subconjunto de una clase más grande de funciones, llamadas **funciones analíticas**. Estas son las que pueden representarse como series de Taylor (ver (Ahlfors, 2004) y (Porter, 1983)). Algunos ejemplos de funciones analíticas son:

1. Trigonométricas
$$\operatorname{sen}(z) = z - \frac{1}{3!}z^3 + \frac{1}{5!z^5} - \frac{1}{7!} + \ldots$$
$$\cos(z) = 1 - \frac{1}{2!}z^2 + \frac{1}{4!}z^4 - \frac{1}{6!}z^6 + \ldots$$
2. Exponencial
$$e^z = 1 + z + \frac{1}{2!}z^2 + \frac{1}{3!}z^3 + \frac{1}{4!}z^4 + \ldots$$
3. El logaritmo en la bola unitaria, centrada en $z = 0$
$$\log(1 + z) = 1 - z + \frac{1}{2}z^2 - \frac{1}{3}z^3 + \frac{1}{4}z^4 - \ldots$$

4. Polinomios, centrados en $z = 0$, su radio de convergencia siempre es infinito, es decir, convergen en todo el plano $\mathbb{C}$.

De los ejemplos anteriores, sólo los polinomios son funciones algebraicas.

En otras palabras, una función algebraica es toda aquella que puede ser expresada como una ecuación con dos variables, donde una es un número complejo y la otra es un polinomio en esa variable. Estas ecuaciones se resuelven encontrando los ceros del polinomio.

Ejemplo 3.3. Algunas funciones algebraicas son:

1. Funciones lineales: $w = az + b$.

   Éstas cumplen con la ecuación $w - (az + b) = 0$.

2. Las cuadráticas: $w = az^2 + bz + c$.

   Éstas cumplen con la ecuación $w-(az^2+bz+c) = 0$. De esta forma, podemos verificar que cualquier polinomio de grado n es una función algebraica.

3. Las funciones racionales: $w = \frac{p(z)}{q(z)}$.

   Como solución a la ecuación $q(z)w - p(z)$, donde $q(z)$ y $p(z)$ son polinomios.

4. Las funciones solubles por radicales son algebraicas, pues dada $f(z)$ soluble por radicales, $f(z)$ es solución a la ecuación $w - f(z) = 0$, manipulando a w para eliminar las funciones de la forma $\sqrt[n]{z}$, consideremos $h(z) = \sqrt[3]{\sqrt{z} + 5z^4}$ como solución a $w - \sqrt[3]{\sqrt{z} + 5z^4} = 0$, eliminando las expresiones radicales, obtenemos la ecuación algebraica

$$64w^6 - 80w^2z^4 + 25z^8 - z = 0.$$

Ejemplo 3.4. Consideremos la «función» $\sqrt{z}\colon \hat{\mathbb{C}} \nrightarrow \hat{\mathbb{C}}$, que es solución a la ecuación:

$$w^2 - z = 0$$

entonces es algebraica y toma dos valores para cada $z \in \mathbb{C}^*$, en los puntos $z = 0$ y $z = \infty$, toma un valor único. A estos puntos les llamaremos *puntos singulares* de la función. Los valores de la función están dados por

$$_1\sqrt{z} = r^{1/2}e^{i\theta/2} \text{ y}$$

$$_2\sqrt{z} = r^{1/2}e^{i\theta/2+\pi} = -_1\sqrt{z}.$$

A los valores distintos que toma una función los llamamos **ramas** de la función.

En la sección 2.4.2 vimos que si tenemos un camino α definido por $z(t)$ y una función f continua, entonces $f(\alpha)$ es continua, llamada **imagen continua del camino**, por esto podemos considerar cómo varía el argumento de la imagen de una curva. Si $\text{var}(\alpha) = \theta$, entonces bajo la función $\sqrt{z(t)}$ es $\text{var}(\sqrt{\alpha}) = \theta/2$, probando así el siguiente lema.

Lema 3.2.1. *Sea α un camino cerrado dado por $z(t)$, entonces $\sqrt{(z(0))} = \sqrt{(z(1))}$ si y sólo si el camino α tiene un índice par alrededor de 0.*

Dado que hay dos imágenes, necesitamos construir un dominio mayor para que la función sea genuina. Para ello, haremos un corte el plano $\mathbb{C}$ a lo largo de $\mathbb{R}^-$, generando entonces al plano $\mathbb{C}$ como la unión disjunta de los semiplanos $\overline{P^+} = \{z \mid \text{Im}(z) > 0\} \cup \mathbb{R} \cup \{\infty\}$ y $\overline{P^-} = \{z \mid \text{Im}(z) < 0\} \cup \mathbb{R} \cup \{\infty\}$ a lo largo de $\mathbb{R}^+$, con dos ejes $\mathbb{R}^-$. Escribimos $\bar{\mathbb{C}} = \mathbb{C} \setminus \mathbb{R}^-$.

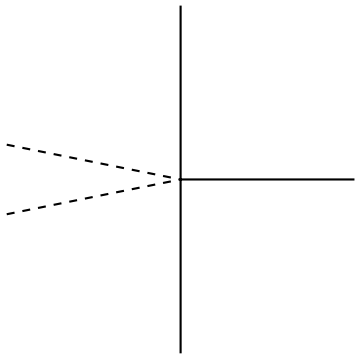


Figura 3.2. Corte en el plano complejo

Lema 3.2.2. *Dado un camino C:*

a) La imagen de C en $\bar{\mathbb{C}}$, $\sqrt{C}$ satisface $\sqrt{(z(t))} = {}_i\sqrt{z}$, para $t \in [0,1]$ con un $i = 1, 2$ fijo.

b) Si el camino C atraviesa el corte, su imagen cambia de rama.

Demostración.

a) Se sigue del lema anterior. Tomemos $t \in [0,1]$ tal que $\sqrt{z(0)} \neq \sqrt{z(t)}$, entonces puede ser $\sqrt{z(0)} = {}_1\sqrt{z(0)}$ y $f(z(t)) = {}_2\sqrt{z(t)}$ o $\sqrt{z(0)} = {}_2\sqrt{z(0)}$ y $\sqrt{z(t)} = {}_1\sqrt{z(t)}$. Y esto sólo sucede al rodear al menos una vez a 0. Entonces al tomar un camino cerrado C con ecuación $z(t)$, podemos fijar $\sqrt{z(0)} = {}_i\sqrt{z(0)}$ y obtener así $\sqrt{z(t)} = {}_1\sqrt{z(t)}$ para un i fijo.

b) Consideremos dos puntos $z_1, z_2 \in \mathbb{C}$ fuera del corte y dos caminos que los unen C_1 no atraviesa el corte y C_2 sí y sabemos que C_1 permanece en la misma rama. Si fijamos $\sqrt{z_1} = {}_1\sqrt{z_1}$, definimos por continuidad a lo largo de C_1 el valor ${}_1\sqrt{z_2}$ en la misma rama. Consideremos ahora el lazo $C_1^{-1}C_2$ con índice 1 alrededor de 0 como se muestra en la figura:

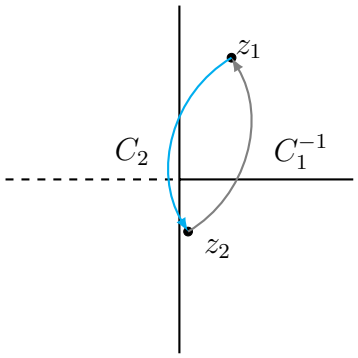


Figura 3.3. Composición de los caminos $C_1^{-1}C_2$ y cómo rodean el origen.

Sabemos que su imagen bajo $\sqrt{}$ no es cerrada, esto significa que el valor $\sqrt{z_2} \neq_1 \sqrt{z_2}$ que habíamos fijado y dado que ${}_1\sqrt{z_2}$ estaba en la misma rama que ${}_1\sqrt{z_1}$, entonces el valor $\sqrt{z_2}$ pertenece a otra rama. □

Tomemos dos copias de $\mathbb{C}$: $\mathbb{C} \times \{1\}$ y $\mathbb{C} \times \{2\}$, para cada $z \in \bar{\mathbb{C}}$, tenemos que $\pi < \arg(z) < -\pi$ y su imagen bajo$\sqrt{z}$, cumplirá $\pi/2 < \arg(z) < -\pi/2$, es decir que están en el lado derecho del plano, a esta rama la denotamos con ${}_1\sqrt{z}$. Al tomar la otra rama de la función, tendremos valores al lado izquierdo del plano, pues es la rotación de la otra con ángulo π y la llamaremos ${}_2\sqrt{z}$.

En la siguiente figura, la parte superior izquierda es una copia del plano $\mathbb{C}$ para el cual definimos a la rama ${}_1\sqrt{z}$, cuya imagen aparece en azul, mientras en una segunda copia del plano $\mathbb{C}$ en la parte inferior definimos a la rama ${}_2\sqrt{z}$, con imagen en color rojo.

Las ramas de la función $\sqrt{z}$, ${}_1\sqrt{z}$ y ${}_2\sqrt{z}$ son funciones continuas definidas en las correspondientes copias de $\mathbb{C}$, que llamaremos también *hojas*. A la primera la denotaremos por $\mathbb{C} \times \{1\}$ y la segunda será $\mathbb{C} \times \{2\}$, para indicar que es el mismo conjunto, pero el punto $(z, 1)$ pertenece a la copia 1, mientras $(z, 2)$ tiene las mismas coordenadas en la copia 2.

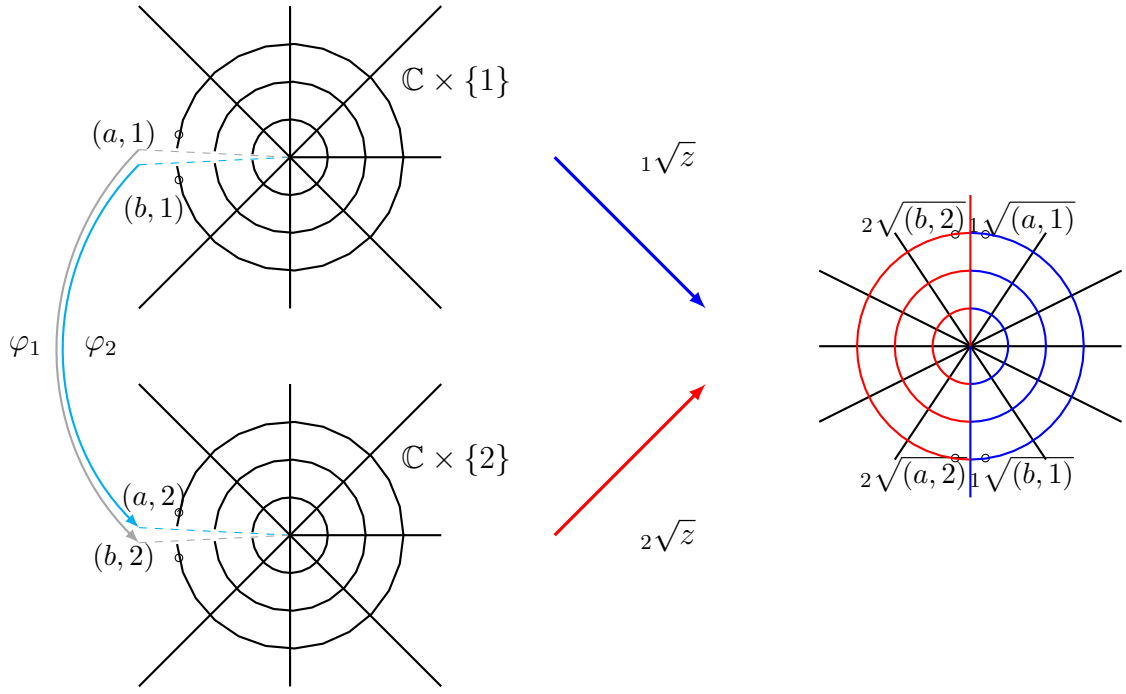


Figura 3.4. Ramas continuas de $\sqrt{z}$.

Para conservar la continuidad de la función, se necesita pasar de una hoja a otra en la superficie vía φ_1, mostrada en gris en la figura 3.4, que identifica la parte superior del corte de la hoja 1 con la parte inferior de la hoja 2, y φ_2, en celeste, que identifica la parte inferior del corte de la hoja 1 con la parte superior del corte en la hoja 2. Y así, definimos $w\colon S \to \hat{\mathbb{C}}$

$$w(z,i) = \begin{cases} {}_1\sqrt{(z,i)}, \text{ si } i = 1 \\ {}_2\sqrt{(z,i)}, \text{ si } i = 2 \end{cases}$$

Si $z = \infty$, $w(\infty, i) = \infty$ y si $z = 0$, entonces $w(z,i) = 0$.

Consideramos la superficie

$$S := \mathbb{C} \times \{1\} \sqcup \mathbb{C} \times \{2\} / \sim .$$

Los puntos $(z,1)$ y $(z,2)$ corresponden vía la **proyección** $\pi\colon S \to \hat{\mathbb{C}}$ al punto $z \in \hat{\mathbb{C}}$, como se muestra en la figura 3.6, donde $\sim$ es la relación correspondiente a φ_1 y φ_2.

De manera que si un punto z_0 fuera del corte y tomamos una vecindad $|z - z_0| < \delta$, donde $\delta > 0$, al dar una vuelta alrededor de él, es posible no tocar el corte con un radio muy pequeño. Para el punto $z_0 = 0$, la curva forzosamente atraviesa el corte, obligando a los puntos de esta a moverse de rama, haciendo que se pierda la

continuidad, en la figura 3.4 puede verse que los puntos $(a,1)$ y $(b,1)$ son cercanos, así como $(a,2)$ y $(b,2)$. Sin embargo, en sus imágenes bajo ${}_1\sqrt{}$ y ${}_2\sqrt{}$ están alejadas. ${}_1\sqrt{(a,1)}$ está cerca de ${}_2\sqrt{(b,2)}$ así como ${}_1\sqrt{(b,1)}$ es cercana a ${}_2\sqrt{(a,2)}$.

Definición 3.9. Los puntos en S, en los cuales es posible cambiar de hoja al dar una vuelta alrededor de ellos, se llaman **puntos de ramificación** de una función algebraica.

Conociendo los puntos de ramificación, puede construirse el *esquema de la superficie de Riemann* de dicha función. En la siguiente figura se muestra el esquema de la superficie de Riemann de la función $\sqrt{z}$, con punto de ramificación $z = 0$. Donde cada hoja es representada por una recta, las flechas indican las identificaciones entre cada hoja de la superficie a través de los círculos pequeños, que representan a los puntos de ramificación, indicando que al rodear una vez a ese punto, se puede mover de una hoja a otra, tanto al dar una vuelta alrededor de ellos, como al atravesar el corte entre 0 e infinito.

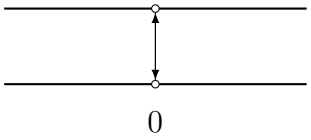


Figura 3.5. Esquema de la superficie de Riemann de $\sqrt{z}$.

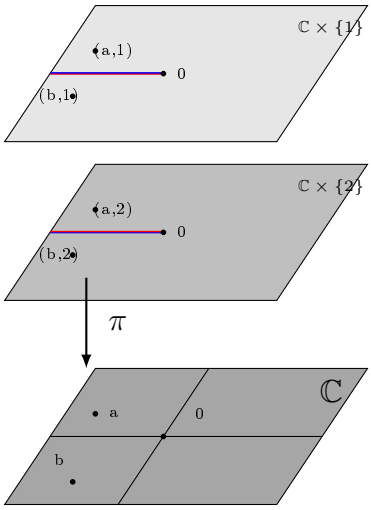


Figura 3.6. Hojas correspondientes a la función $\sqrt{z}$ y la proyección $\pi\colon S \to \hat{\mathbb{C}}$.

Al dominio resultante del pegado para la función $\sqrt{z}$ lo llamamos **superficie de Riemann**.

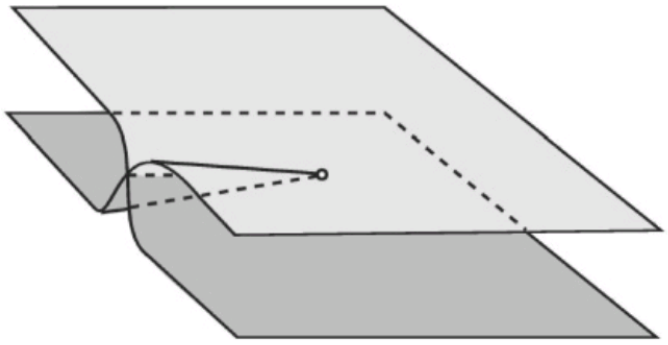


Figura 3.7. Superficie de Riemann de $\sqrt{z}$. Fuente: imagen tomada de(Alekseev, 2004).

Nota 3.3. En las figuras de las superficies de Riemann que utilizaremos a lo largo del capítulo, el punto al infinito corresponde al borde de las hojas.

Tenemos las funciones $w\colon S \to \hat{\mathbb{C}}$ y $\sqrt{z}\colon \hat{\mathbb{C}} \twoheadrightarrow \hat{\mathbb{C}}$, ambas están relacionadas por la proyección $\pi\colon S \to \hat{\mathbb{C}}$, $\pi(z,i) \mapsto z$. De manera que el siguiente diagrama conmuta y las funciones π y $w(z)$ están dadas explícitamente por continuación analítica, como veremos en las siguientes secciones.

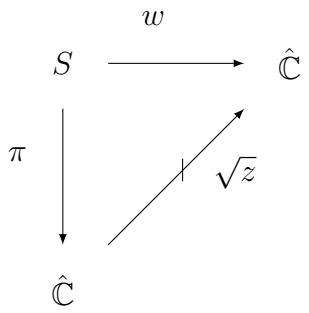


Figura 3.8. Diagrama de funciones y una superficie de Riemann como dominio de la nueva función continua.

Ejemplo 3.5. Si ahora consideramos la función $\sqrt{z^2}\colon \hat{\mathbb{C}} \to \hat{\mathbb{C}}$. Buscaremos, al igual que en $\sqrt{z}$, sus ramas univaluadas continuas. Se considera el plano z cuyos valores de las ramas de la función están dados por ${}_1\sqrt{z^2} = z$ y ${}_2\sqrt{z^2} = -z$. Al tomar una curva que rodea a 0, $\mathrm{var}(z^2)$ varía 4π mientras $\mathrm{var}(\sqrt{z^2})$ varía 2π, es decir que el valor de la función no cambia.

Por esto, $z = 0$ no es un punto de ramificación de la función $\sqrt{z^2}$ y las imágenes de las curvas que pasan por este punto no están definidas de manera única.

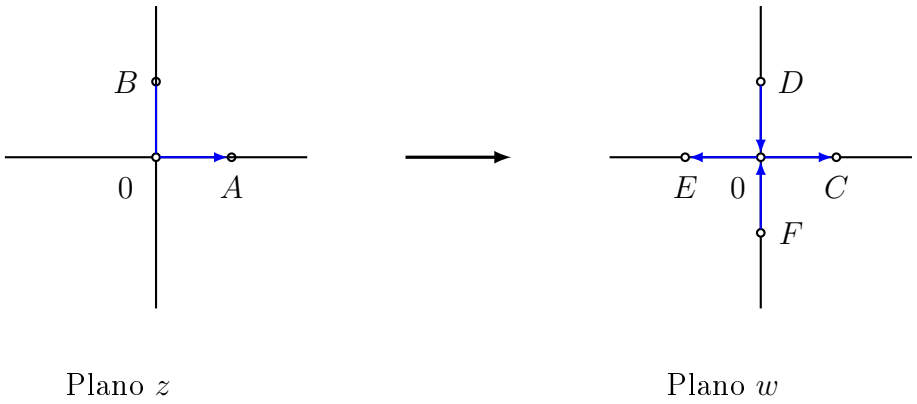
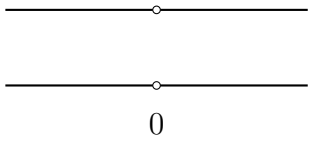
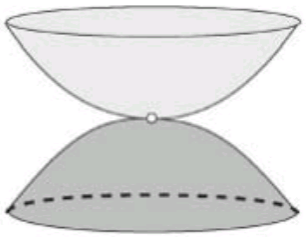


Figura 3.9. En el lado izquierdo tenemos a la curva BA que pasa por O. Al lado derecho, las imágenes de esta curva.

En la figura 3.9, las imágenes del segmento BA pueden ser DO o FO, independientemente de la elección, al pasar por $w = 0$ hay de nuevo dos imágenes para el segmento OA, estas son OE y OC, de esta forma podemos ver que los caminos que pasan por $z = 0$ no tienen una imagen bien definida y que la superficie consta de dos hojas disjuntas, representada en la siguiente figura, con su correspondiente esquema.



(a) Esquema de la superficie de Riemann de $\sqrt{z^2}$.



(b) Superficie de Riemann de $\sqrt{z^2}$.

Definición 3.10. Los puntos en los que se pierde la unicidad de las imágenes de las curvas continuas, pero no son puntos de ramificación, se llaman **puntos de no unicidad**. Al conjunto de puntos de ramificación y puntos de no unicidad le llamaremos **puntos especiales** de la superficie de Riemann.

Al construir superficies de Riemann, no se hacen cortes desde un punto de no unicidad, pero las curvas continuas deben evitar tocar estos puntos.

Con la idea de cómo construir la superficie de Riemann para la función $\sqrt{z}$. Podremos generalizar a cualquier función algebraica, para ello, usaremos las ideas principales y notación de (Porter, 1983).

Definición 3.11. Una **superficie de Riemann concreta** es un par (S, π) donde S es una superficie y $\pi\colon S \to \hat{\mathbb{C}}$ es una función continua con la propiedad de que para todo punto $s_0 \in S$ donde $\pi(s_0) \neq \infty$ existe un entero $n \leqslant 1$, una vecindad $V_0 \subset S$ de s_0 y un homeomorfismo $h\colon V_0 \to h(V_0) \subset \hat{\mathbb{C}}$ con $h(s_0) = 0$ tal que

$$\pi(s) = \pi(s_0) + h(s)^n$$

para todo $s \in V_0$. Para los puntos s_0 tales que $\pi(s_0) = \infty$, se necesita que

$$\pi(s) = h(s)^{-n}$$

para todo $s_0 \in V_0$.

Al número n se le llama **índice de ramificación** del punto s_0. Cuando $n \leqslant 2$, se dice que s_0 es un **punto de ramificación** de π. La proyección es n-a-1 en todos los puntos, excepto en estos puntos.

Nótese que la definición 3.9 no contradice la definición 3.11, pues al rodear a un punto de ramificación, estamos atravesando el corte al infinito y habíamos identificado las copias de $\mathbb{C}$ a lo largo de este corte. Es decir, al atravesar el corte desde la hoja k, paso a la hoja $k+1$ y por tanto, una función $w(z)$, pasaría de su k-ésima rama a la $k+1$.

Nota 3.4. Ahora, es conveniente mencionar a los espacios cubrientes, esta condición será importante para el estudio del grupo de monodromía.

Definición 3.12. Sea $f\colon Y \to X$ una aplicación entre espacios topológicos, decimos que es una **aplicación cubriente** si cada punto $x \in X$ tiene una vecindad abierta U_x tal que $f^{-1}(U_x)$ es una unión de abiertos disjuntos donde cada uno es homeomorfo a U_x, a la cual llamamos **vecindad regular** de x. Decimos que Y es un **espacio cubriente** de X s existe tal proyección. Al conjunto $f^{-1}(x)$ se le llama **fibra** y a su cardinalidad se le llama **número de hojas** del espacio cubriente.

En la definición de superficies de Riemann, la proyección

$$\pi\colon S \setminus \{\text{puntos de ramificación}\} \to \mathbb{C} \setminus \{\text{puntos singulares de } f(z)\}$$

es una aplicación cubriente de n hojas cuando el índice de ramificación es n. La prueba de esto puede verse en (Porter, 1983) y (Zoł, 2000).

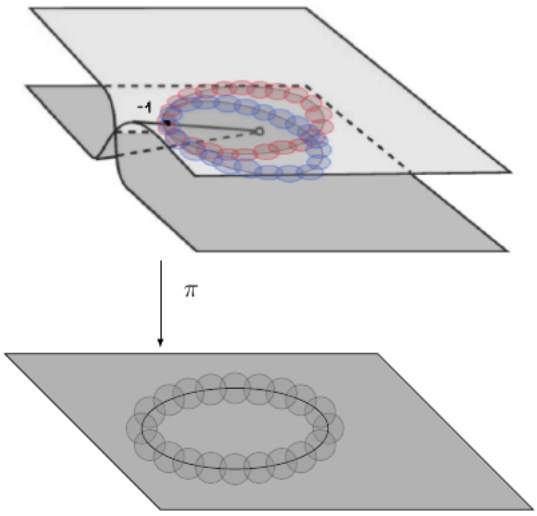


Figura 3.11. Superficie de Riemann asociada a $\sqrt{z}$ como espacio cubriente de $\mathbb{C}*$.

Por esta razón, los caminos en $\hat{\mathbb{C}}$ pueden ser *levantados* a las superficies de Riemann, propiedad que estudiaremos en el Capítulo 4.

Ejemplo 3.6. El ejemplo más simple es $(\hat{\mathbb{C}}, id)$, donde $\hat{\mathbb{C}}$ es la esfera de Riemann e id es la función identidad.

Consideremos a $h(s) = s - s_0$ para cada punto finito $s_0 \in \mathbb{C} \subset \hat{\mathbb{C}}$ cuya vecindad V_0 no contenga al infinito, de esta forma, $h(s_0) = 0$, entonces

$$\pi(s) = s = s_0 + h(s) = s_0 + (s - s_0) = \pi(s_0) + h(s),$$

donde el índice de ramificación es siempre $n = 1$. En el caso $s_0 = \infty$, tomaremos $h(s) = 1/s$ y en cualquier vecindad V_0 que no contenga al cero, se cumple $h(s_0) = 0$, de donde

$$\pi(s) = s = s_0 + 1/s = s_0 + h(s),$$

también con índice de ramificación 1. S es un espacio cubriente 1-a-1, es decir, de 1 hoja.

Ejemplo 3.7 (Ejemplo 3.4 revisitado)**.** Hemos construido una superficie de Riemann para la función multivaluada $\sqrt{z}$ a través uniones disjuntas e identificaciones, pero falta verificar que, en efecto, es una superficie de Riemann concreta.

Consideremos un punto $z \in \mathbb{C}^*$, es decir, puntos distintos de 0 e ∞. Entonces obtenemos un homeomorfismo de la forma

$$w(s) = \pi(s) - \pi(s_0),$$

es decir que tenemos índice de ramificación 1, confirmando así que no son puntos de ramificación.

Si tomamos un punto tal que $\pi(s_0) = 0$, tenemos que la proyección

$$\pi(s) = \pi(s_0) + [w(s)]^2,$$

donde el homeomorfismo w tiene índice de ramificación $n = 2$.

Para un punto tal que $\pi(s_0) = \infty$, tenemos que la proyección

$$\pi(s) = \pi(s_0) + [w(s)]^{-2},$$

donde el homeomorfismo w tendría índice de ramificación $n = 2$. Con esto, obtenemos un espacio de recubrimiento de 2 hojas.

Ejemplo 3.8. (S, π) donde S son n copias del plano $\mathbb{C}$ pegadas vía φ_k $1 \leqslant k \leqslant n$, que asignan la parte inferior de $\mathbb{R}^-$ de la $k-$ésima copia, con la superior de la copia $k+1$, módulo n.

Este es un espacio cubriente de n hojas, pues se construye de manera análoga a la superficie de $\sqrt{z}$. Sus puntos de ramificación son $z = 0, z = \infty$ y el índice de ramificación de cada uno es n. π es la proyección, donde hay un homeomorfismo $w : S \to \hat{\mathbb{C}}$ es la función $w(z, i) = {}_k\sqrt[n]{(z, k)}$, donde $i = k$.

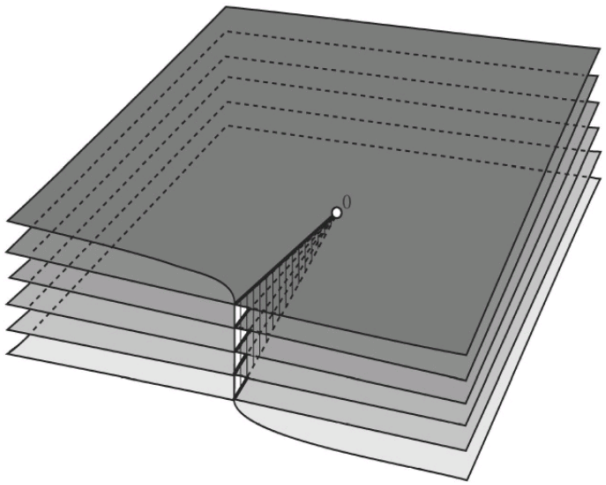


Figura 3.12. Superficie de Riemann de $\sqrt[6]{z}$. Fuente:imagen tomada de(Alekseev, 2004).

3.3. Continuación analítica

En las secciones anteriores se mencionó que las funciones solubles por radicales eran algebraicas y que éstas son parte de un conjunto más general de funciones, llamadas analíticas. Nos interesa hablar de estas funciones porque podemos extender su dominio por continuación analítica y obtener de esta manera un procedimiento más general para construir superficies de Riemann y asegurar así su existencia para las funciones algebraicas y a su vez, estudiar la monodromía de las mismas. Consideremos un punto $a \in \mathbb{C}$ tal que la función algebraica $F(a, w) = 0$ tiene n soluciones distintas$w = z_1, z_1, \ldots, z_n$. Entonces $F'(a, z_i) \neq 0$, por el *Teorema de la Función Implícita* (ver (Bartle, 1967)), si se toma un punto $x \neq a$ en una vecindad U_a de a, la ecuación $F(z, w) = 0$ también tiene n soluciones. Estas n soluciones definen funciones (univaluadas) $f_{a,1}(z), f_{a,2}(z), \ldots, f_{a,n}(z)$ con dominio U_a. donde las funciones $f_{a,i}(z)$ se expanden en series de Taylor[4] convergentes en a, entonces podemos tomar un disco U_a en la intersección de los discos de convergencia de estas series.

Llamamos **elemento de función analítica** a cada par ordenado $(f_{a,i}, U_a)$, donde $f_{a,i}$ es analítica en el disco U_a descrito anteriormente. Y llamaremos **función global analítica** de (f_0, D_0) a la función f, que es la colección de elementos tales que existe una cadena

$$(f_0, D_0), (f_1 D_1), \ldots, (f_n, D_n) = (f, D)$$

donde f_j es continuación analítica directa de f_{j-1} para $j = 1, 2, \ldots, n$.

Un elemento analítico puede ser extendido a un dominio más grande, en caso de que la ecuación 3.1 tenga soluciones univaluadas, el dominio es todo $\mathbb{C}$. Cada solución está definida en una copia de $\mathbb{C}$, que es conexo por caminos, en particular, podemos tomar puntos en $\mathbb{C} \setminus \{z_1, z_2, \ldots, z_n\}$, donde $\{z_1, z_2, \ldots, z_n\}$ es el conjunto de puntos donde la función f se hace cero, junto con el cero e infinito.

Para construir superficies de Riemann a partir de la continuación analítica, tomaremos puntos $a, b \in \mathbb{C} \setminus \{z_1, z_2, \ldots, z_n\}$ y al elemento analítico (f_a, U_a). Expandimos este elemento a través de caminos $C \subset \mathbb{C} \setminus \{z_1, z_2, \ldots, z_n\}$ hasta el punto b y cubrimos a los caminos con una cantidad finita de vecindades U_{a_i}, que son dominios de los elementos analíticos $(f_{a,i}, U_{a_i})$ y son compatibles cuando $f_{a_i} \equiv f_{a_{i-1}}$, esto es en las intersecciones de los discos $U_{a_i} \cap U_{a_{i-1}}$, como se muestra en la figura 3.13. El último elemento analítico (f_b, U_b) es una extensión del elemento (f_a, U_a) a lo largo del camino C.

[4] Ver(Porter, 1983).

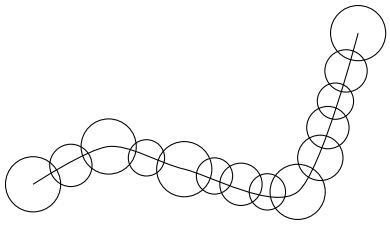


Figura 3.13. Continuación analítica por caminos.

Ejemplo 3.9. Sea $F(z,w) = (w-z)(w-z_0)$ entonces se tienen dos elementos analíticos, extendidos a las funciones $w = z$ y $w = z_0$ en todo el plano $\mathbb{C}$. Esta tiene un corte imaginario cuando $z = z_0$, pero es removible, ya que es univaluada. Sin embargo en el ejemplo 3.4 no puede removerse el punto de ramificación $z = 0$.

Pero, ¿es la continuación analítica única? En este punto afirmaremos que dos caminos C^1 y C^2, ambos uniendo a los puntos a y b, pueden ser deformados uno en el otro siempre que al concatenarlos no rodeen a un punto sinuglar de una función. A esta posibilidad de deformar caminos se le llama **propiedad de monodromía**, que será fundamental en el siguiente capítulo.

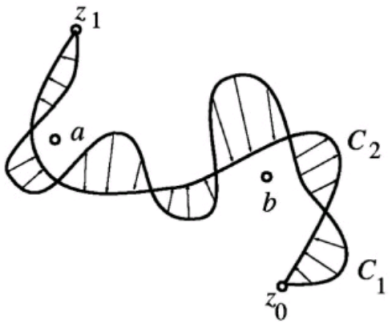


Figura 3.14. Propiedad de Monodromía

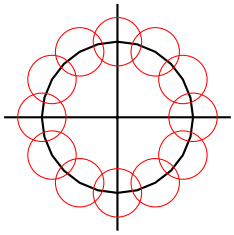
Definición 3.13. La unión de todos los elementos analíticos obtenidos de (f_a, U_a) a lo largo de todos los posibles caminos con la propiedad de monodromía, es decir, el *barrido* de las curvas, forma una superficie, que es precisamente la **superficie de Riemann** S, de una función sin contar los puntos de ramificación. Esta superficie cumple con:

$$\pi : S \to \hat{\mathbb{C}} \setminus \{z_1, z_2, \ldots, z_n\}$$

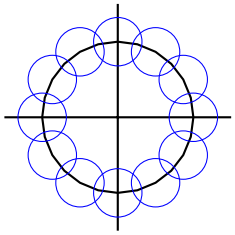
que asocia cada valor $w_i(z)$ con su argumento z. Sin embargo, falta unir a los puntos de ramificación para obtener una superficie de Riemann compacta con la topología inducida por los discos de los elementos analíticos.

Ejemplo 3.10 (Construcción equivalente para el ejemplo 3.4)**.** Estudiaremos la función $w(z) = \sqrt{z}$ tomando la curva $e^{2\pi it}$ con $t \in [0,1]$ (el círculo unitario en el plano $\mathbb{C}$). Al completar una vuelta al círculo a partir de $z = -1$ en una copia de $\mathbb{C}$, análogo al ejemplo **??**, el camino que se obtiene (imagen) es un semicírculo en la parte derecha del plano al utilizar la función ${}_1\sqrt{z}$, definida previamente.

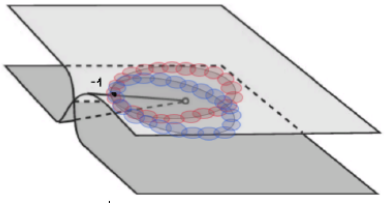
Haciendo continuación analítica, partiendo del mismo punto pero en la segunda copia de $\mathbb{C}$, como se estableció en el ejemplo 3.4, se da una vuelta en la segunda copia, generando, a través de la función ${}_2\sqrt{z}$ el semiplano derecho de $\mathbb{C}$. La superficie final es el barrido de los círculos de todos los radios $r > 0$, hasta infinito, que se muestra en todas las figuras como el borde de las hojas.



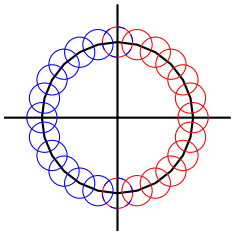
(a) Hoja 1 del plano $\mathbb{C}$.



(b) Hoja 2 del plano $\mathbb{C}$.



(c) Superficie de Riemann con los caminos circulares y las vecindades tomadas para la continuación analítica



(d) Imagen de la función $w(z)$.

3.4. Superficies de Riemann para funciones solubles por radicales

En general, podemos construir superficies de Riemann para todas las funciones algebraicas, pero para propósitos de esta tesis es de particular interés entender la construcción para funciones solubles por radicales. Si consideramos una función $h(z) = f(z)\square g(z)$, donde la casilla $\square$ puede ser cualquiera de las operaciones suma, resta, multiplicación, división, potencias y raíces, podemos construir sus superficies de Riemann a través de las siguientes construcciones:

Construcción 3.1. *Para construir el esquema de las superficies de Riemann de las funciones $h(z) = f(z)\square g(z)$, comenzando con los esquemas de las funciones $f(z)$*

$g(z)$, con los mismos cortes, basta con seguir el procedimiento descrito a continuación:

a) Poner en correspondencia cada par de ramas $f_i(z)$ y $g_i(z)$, una hoja con la cual rama $h_{i,j}(z) = f_i(z) \square g_j(z)$ está definida.

b) Si al girar una vez alrededor del punto z_0 se mueve de una rama $f_{i1}(z)$ a una nueva rama $f_{i2}(z)$ y de la rama $g_{j1}(z)$ a $g_{j2}(z)$, entonces para la función $h(z)$, con el mismo giro se moverá de la rama $h_{i1,j1}$ a la rama $h_{i2,j2}$.

c) Identificar las hojas en las que las ramas $h_{i,j}$ coinciden y reducirlas a una sola hoja.

A esto se le conoce como método formal.

Construcción 3.2. *Para construir el esquema de la superficie de Riemann de la función $h(z) = [f(z)]^n$, comenzando con el esquema de la superficie de Riemann de la función $f(z)$, definida con los mismos cortes, son suficientes los siguientes pasos:*

a) Considerar las ramas $h_i(z) = [f_i(z)]^n$, en vez de las ramas $f_i(z)$ en el esquema de $f(z)$

b) Identificar qué ramas de $h(z)$ coinciden.

Construcción 3.3. *Para construir el esquema de la superficie de Riemann de la función $h(z) = \sqrt[n]{f(z)}$ comenzando con el de la función $f(z)$, definidas en los mismos cortes, es suficiente hacer lo siguiente:*

a) Reemplazar cada hoja del esquema de la superficie de Riemann de la función $f(z)$ por un paquete de n hojas.

b) Al dar una vuelta alrededor de un punto de ramificación arbitrario de $h(z)$, se mueve de las hojas de un paquete a todas las hojas de un paquete distinto.

c) Cada movimiento de un paquete de hojas a otro paquete, corresponde a pasar de una hoja a otra en la $f(z)$.

d) Si las ramas dentro de los paquetes están enumeradas de manera que $f_{i,j}(z) = f_{i,0}(z)\epsilon_n^k$, entonces al moverse de un grupo de hojas a otro, las hojas del paquete correspondiente que las contiene no están mezcladas, sino que permutan cíclicamente.

Todos estos procedimientos se cumplen cuando la función compuesta $h(z)$, tiene los mismos cortes que las funciones de las que depende, a continuación, veremos cómo construir superficies de Riemann para funciones compuestas.

Ejemplo 3.11. Consideramos la función $h(z) = \sqrt{z} + \sqrt{z}$ se tiene que ambas funciones $f(z) = g(z)$ y el único punto de ramificación es $z = 0$. Si comenzamos en la rama $h_{0,0}$, al dar una vuelta alrededor de este punto, cambiará de f_0 a f_1 y de g_0 a g_1, pasando a la hoja $h_{1,1}$. Análogamente, si se comienza en $h_{0,1}$, se pasará a $h_{1,0}$, siendo su esquema:

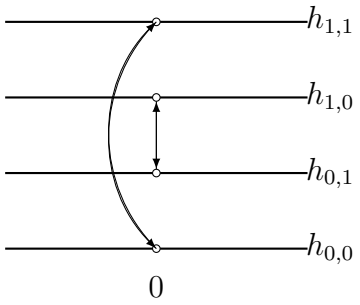


Figura 3.16. Esquema de la superficie de Riemann de $\sqrt{z} + \sqrt{z}$ con el método formal.

Sin embargo, al evaluar para algún $z \neq 0, z \neq \infty$ se tiene:

$$h_{0,0}(z) = f_0(z) + f_0(z) = 2f_0(z)$$

$$h_{0,1}(z) = f_0(z) + f_1(z) = 0$$

$$h_{1,0}(z) = f_1(z) + f_0(z) = 0$$

$$h_{1,1}(z) = f_1(z) + f_1(z) = f_1(z)$$

Puede notarse que dos hojas son idénticamente 0, entonces coinciden en el cambio de argumento y pasos de una hoja a otra, por lo que el esquema correcto de la superficie de Riemann para esta función se ve así:

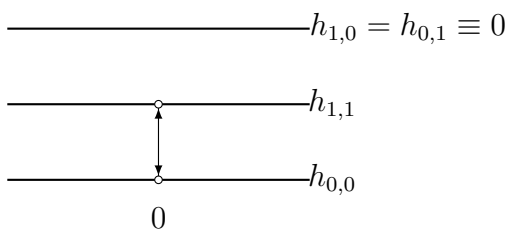


Figura 3.17. Esquema correcto de la superficie de Riemann de $\sqrt{z} + \sqrt{z}$.

Ejemplo 3.12. Al considerar la función $h(z) = (\sqrt{z} + \sqrt{z})/\sqrt[3]{z(z-1)}$, regresaremos a $f(z) = \sqrt{z} + \sqrt{z}$, función de la cual conocemos que tiene 3 ramas univaluadas continuas, $f_0(z) \equiv 0, f_1(z), f_2(z) = -f_1(z)$, con punto de ramificación $z = 0$ y la función $g(z) = \sqrt[3]{z(z-1)}$, que tiene 3 ramas univaluadas, con puntos de ramificación $z = 0$ y $z = 1$. Las ramas son $g_0(z), g_0(z)\epsilon_3, g_0(z)\epsilon_3^2$, entonces

$$h_{0,0}(z) = f_0(z)g_0(z) = 0$$

$$h_{0,1}(z) = f_0(z)g_1(z) = 0$$

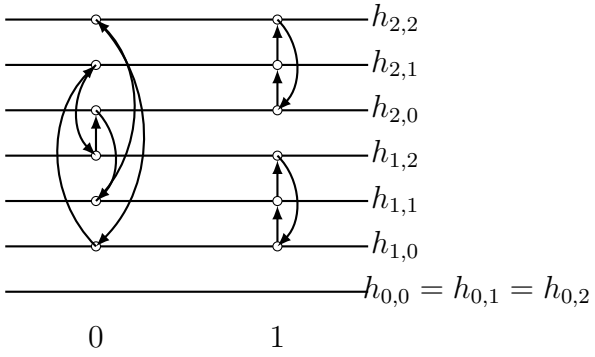
$$h_{0,2}(z) = f_0(z)g_2(z) = 0$$

$$h_{1,0}(z) = f_0(z)g_0(z)$$

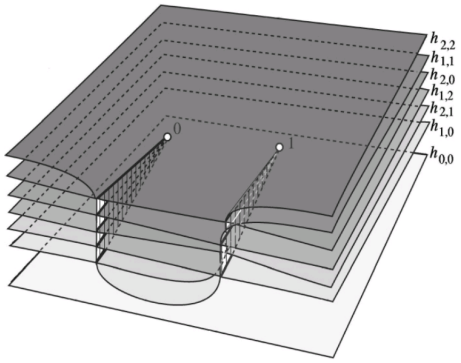
$$h_{1,1}(z) = f_0(z)g_1(z) = h_{1,0}\epsilon_3$$

$$h_{1,2}(z) = f_0(z)g_2(z) = h_{1,0}\epsilon_3^2$$

De donde puede observarse que tres hojas coinciden y son idénticamente 0. Se necesitan 3 vueltas alrededor del punto $z = 1$ para regresar a la rama inicial y el punto $z = 0$ por ser punto de ramificación de $f(z)$ y $g(z)$, permutará ambos índices en $h_{i,j}(z)$ cambiando cíclicamente $i \in \{1, 2\}$ y el índice $j \in \{0, 1, 2\}$. Dejando las hojas $i = 0$ fijas, ya que $h_{0,j} \equiv 0$.

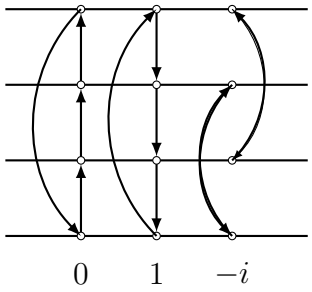


(a) Esquema de la superficie de Riemann de la función $(\sqrt{z} + \sqrt{z})/\sqrt[3]{z(z-1)}$.

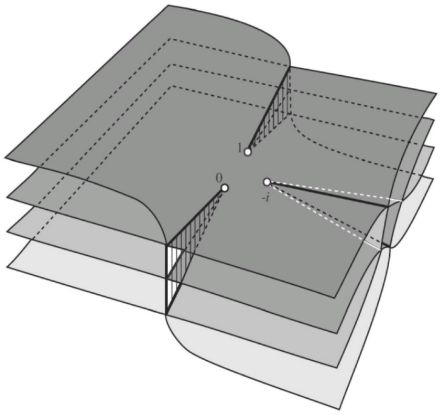


(b) Superficie de Riemann de la función $(\sqrt{z} + \sqrt{z})/\sqrt[3]{z(z-1)}$.

Ejemplo 3.13. Cuando un punto distinto de $z = 0$ aparece como denominador, la variación del argumento está en dirección contraria, a continuación, se analizará la función $\sqrt[4]{(z+i)^2/(z(z-1)^3)}$, donde los puntos de ramificación son $z = -i$ con multiplicidad dos, entonces asigna las hojas por parejas, $z = 0$ asigna las hojas cíclicamente, al igual que $z = 1$.



(a) Esquema de la superficie de Riemann de $\sqrt[4]{(z+i)^2/(z(z-1)^3)}$.



(b) Superficie de Riemann de $\sqrt[4]{(z+i)^2/(z(z-1)^3)}$.

4. GRUPO DE MONODROMÍA Y TEOREMA DE ABEL-RUFFINI

En este capítulo mostramos el teorema de Abel-Ruffini, siguiendo las ideas de la prueba de Arnold. En el capítulo anterior, vimos cómo asociar a una función algebraica una superficie y una aplicación cubriente. En este capítulo, estudiamos primero cómo capturar la información de los lazos que rodean los puntos singulares de la función algebraica a través de un grupo, *el grupo fundamental*. Posteriormente discutimos cómo estos lazos inducen permutaciones de las hojas del espacio de recubrimiento. El grupo generado por estas permutaciones es el llamado *grupo de monodromía* de una función algebraica. Veremos cómo se relaciona el hecho de que una función algebraica sea soluble por radicales con la solubilidad de dicho grupo y cómo se puede usar esto para concluir el teorema de Abel-Ruffini.

4.1. Lazos y grupo fundamental

Para rodear los puntos singulares de un espacio, consideraremos y estableceremos cuándo son equivalentes. Esta información estará capturada en lo que se llama grupo fundamental del espacio. Estudiaremos esta noción y propiedades relevantes en esta sección. Recordemos que un camino es una función continua en un espacio topológico $f\colon I \to X$ con punto inicial $f(0) = x_0$ y final $f(1) = x_1$. Podemos deformar caminos manteniendo sus extremos fijos, para ello, estudiaremos la homotopía de caminos.

Definición 4.1. Una **homotopía** de caminos $F\colon I \times I \to X$, definida por

$$F(s,t) = f_t(s)$$

es una función que deforma continuamente a los caminos $f_0(t)$ y $f_1(t)$, a través de la familia de camino $f_t\colon I \to X$ con punto inicial $f_t(0) = x_0$ y punto final $f_t(1) = x_1$.

Decimos que dos caminos $f_0, f_1\colon I \to X$ que están conectados de esta forma,

son **homotópicos** y escribimos $f_0 \simeq f_1$.

Si pensamos en t como una variable que parametriza el tiempo, tenemos un camino $f_0 \colon I \to X$ que varía continuamente desde $t = 0$ hasta el tiempo $t = 1$, al camino $f_1 \colon I \to X$. Por eso, decimos que una homotopía es una *deformación continua* de caminos.

Puede verse que la homotopía de caminos, define una relación de equivalencia: dos caminos se consideran equivalentes si pueden deformarse uno en otro dejando los extremos fijos[1]. A la clase de caminos equivalentes homotópicamente a f la denotaremos por $[f]$.

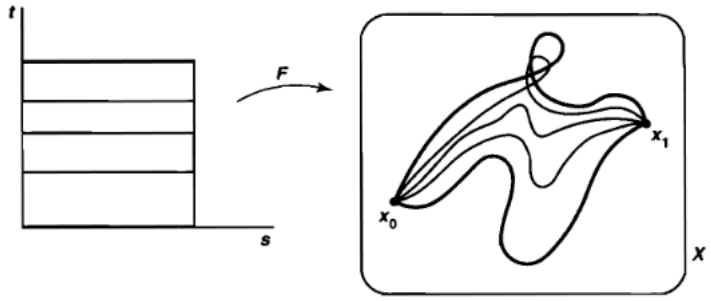


Figura 4.1. Caminos equivalentes homotópicos.Fuente: Imagen tomada de (Munkres, 2000).

En la siguiente figura mostramos dos caminos con extremos fijos que no son equivalentes homotópicamente, pues existe una singularidad entre ellos y al deformar continuamente siempre pasa por ese punto.

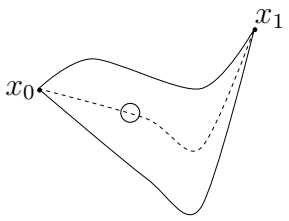


Figura 4.2. Caminos que no son homotópicos, pues no se puede deformar uno en el otro sin tocar el punto.

Con las clases de equivalencia, escribimos al producto entre ellas como

$$[f]\,[g] = [f * g]$$

[1] Ver (Hatcher, 2002).

donde el producto $*$ al lado derecho es la concatenación de caminos y está bien definido en clases de equivalencia siempre que $f(1) = g(0)$.

Dados f, g, h caminos en un espacio X, las principales propiedades de este producto son:

1. El producto entre clases de equivalencia es asociativo

$$([f]\,[g])\,[h] = [f]\,([g]\,[h]),$$

siempre que $f(1) = g(0)$ y $g(1) = h(0)$.

2. Si $x \in X$, la clase de equivalencia del camino constante $\epsilon_x \colon I \to X$, tal que $\epsilon_x(t) = x$ para cada $t \in I$, se comporta como elemento identidad, esto es,

$$[\epsilon_a]\,[f] = [f] = [f]\,[\epsilon_b]\,,$$

si $f \colon I \to X$ es un camino de a a b.

3. El camino en dirección contraria actúa como inverso, es decir si $f \colon I \to X$ es un camino de a a b y $f^{-1} \colon I \to X$ es tal que $f^{-1}(t) = f(t-1)$

$$[f]\left[f^{-1}\right] = [\epsilon_a] \text{ y } \left[f^{-1}\right][f] = [\epsilon_b]\,.$$

Para definir al grupo fundamental de un espacio X tomamos un punto $x_0 \in X$, restringiremos los caminos a caminos cerrados, tales que $f(0) = f(1) = x_0$, a los cuales llamaremos **lazos basados en** x_0.

Cuando consideramos lazos, la operación siempre está definida y el elemento neutro es único y corresponde al camino constante $\epsilon_x(t) = x_0$ para cada $t \in I$.

Definición 4.2. El conjunto de clases de equivalencia de lazos basados en x_0 forma un grupo con el producto descrito anteriormente. A este grupo lo llamamos **grupo fundamental** de X basado en x_0 y se denota por $\pi_1(X, x_0)$.

Nota 4.1. El grupo fundamental de un espacio X, $\pi_1(X, x_0)$ es invariante bajo homeomorfismos de espacios y más aún, de homotopía. Es decir, espacios topológicos homeomorfos (homotópicos) tienen grupos fundamentales isomorfos, como se muestra en (**?**) y puede probarse que $\pi_1(S^1, 1) \cong \mathbb{Z}$.

Otra propiedad importante del grupo fundamental es que al cambiar de punto base, es decir, tomando y_0, siempre que el espacio sea conexo por trayectorias, se cumple que $\pi_1(X, x_0) \cong \pi_1(X, y_0)$. Véase (Munkres, 2000).

Ejemplo 4.1 (El grupo fundamental del círculo)**.** Consideremos el círculo $S^1 \subset \mathbb{C}$ y el punto base $1 \in S^1$. Resulta que $\pi_1(S^1, 1) \cong \mathbb{Z}$ y está generado por el lazo $\gamma\colon I \to S^1$, $t \mapsto e^{2\pi it}$. Para probar esto, consideramos un espacio de recubrimiento de S^1 dado por $p\colon \mathbb{R} \to S^1$ $(t \mapsto (\cos(2\pi t), \operatorname{sen}(2\pi t))$.

Para visualizar este espacio de recubrimiento, consideramos un encaje de $\mathbb{R}$ a $\mathbb{R}^3$, donde se formará una hélice que asigna las coordenadas de la siguiente forma $t \mapsto (\cos 2\pi t, \operatorname{sen} 2\pi t, t)$ y p es la proyección al plano $\mathbb{C}$ desde $\mathbb{R}^3$, $(x, y, z) \mapsto x + iy$.

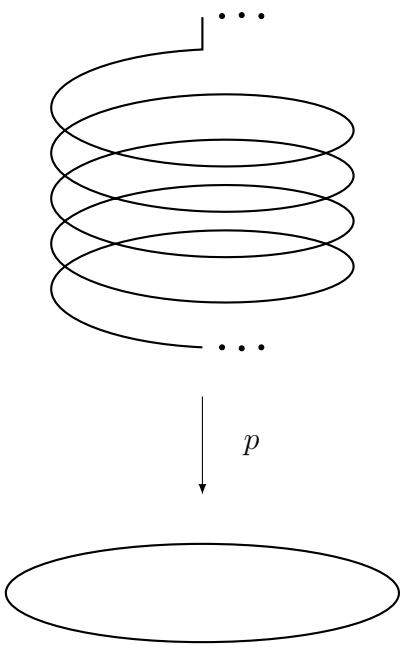


Figura 4.3. Aplicación cubriente p.

Sea $n \in \mathbb{Z}$, observemos que $[\gamma]^n = [\gamma_n]$, donde $\gamma_n\colon I \to S^1$, es el lazo dado por $t \mapsto e^{2\pi itn}$ para $n \in \mathbb{Z}$. Más aún, podemos considerar los caminos $\tilde{\gamma_n}\colon I \to \mathbb{R}$.

Dado un lazo $\alpha\colon I \to S^1$ basado en 1, veremos en la Sección 4.2 que existe un único levantamiento $\tilde{\alpha}\colon I \to \mathbb{R}$, que comienza en $\tilde{\alpha}(0) = 0$. Observemos que el punto final $\tilde{\alpha}(1)$ de este camino es un punto en $\mathbb{Z} = p^{-1}(1)$. De esta manera podemos considerar

$$\psi\colon \pi_1(S^1, 1) \to \mathbb{Z} \text{ dado por } [\alpha] \mapsto \tilde{\alpha}(1).$$

Resulta que ψ es un homomorfismo de grupos bien definido y más aún, es isomorfismo, puede verse los detalles en (Hatcher, 2002). En particular, observamos que $\psi([\gamma]) = 1$, lo que significa que el lazo γ genera el grupo fundamental $\pi_1(S^1, 1)$.

Ejemplo 4.2. Consideremos a los espacios que se muestra en la figura, un anillo A y un disco D.

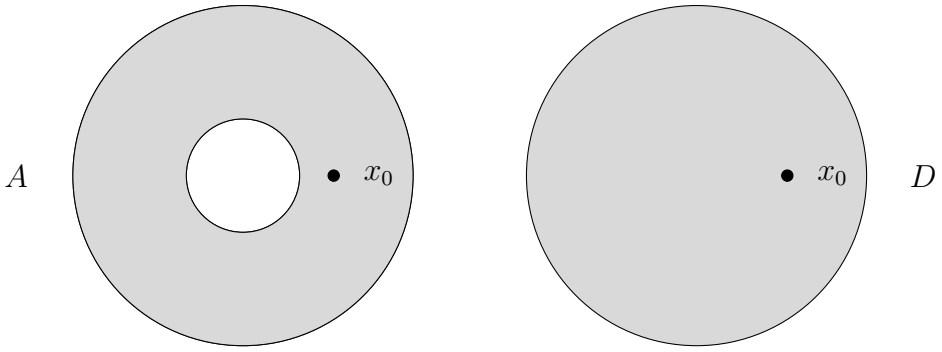


Figura 4.4. Puntos base en el espacio.

En este caso, $\pi_1(D, x_0) = \{e\}$ es el grupo trivial, ya que cualquier lazo en el disco D puede contraerse al punto x_0, pues es un espacio convexo[2] sin singularidades y estos lazos actúan como el elemento identidad. En (Hatcher, 2002) se muestra que el anillo A es homotópico al círculo S^1 y, como discutimos en el ejemplo 4.1, $\pi_1(S^1, 1) \cong \mathbb{Z}$. En consecuencia, $\pi_1(A, x_0) \cong \mathbb{Z}$.

En el contexto de funciones algebraicas, nos interesa estudiar el comportamiento de las soluciones alrededor de las singularidades y, como mencionamos antes, lo hacemos considerando lazos que rodean estas singularidades. Por ejemplo, la función algebraica $\sqrt{z}$ tiene a 0 como único punto singular. Para rodear a 0 consideramos el grupo fundamental $\pi_1(\mathbb{C}^*, 1)$.

Resulta, de la inclusión de S^1 en el plano perforado $\mathbb{C}^*$, que el grupo fundamental del plano perforado basado en 1, es el grupo libre generado por el lazo que rodea a 0, es decir $\pi_1(\mathbb{C}^*, 1) \cong \mathbb{Z}$.

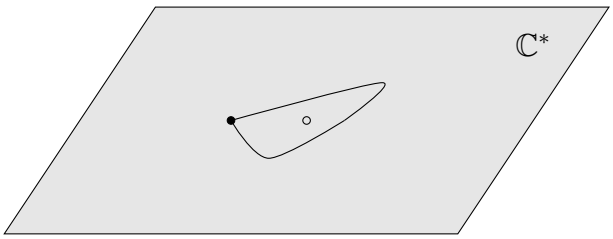


Figura 4.5. Lazo alrededor de 0 como generador del grupo fundamental del plano perforado.

En general, si la función algebraica f, tiene un número finito de puntos singulares $\{z_1, z_2, \ldots, z_m\}$, consideramos el grupo fundamental $\pi_1(\mathbb{C} \setminus \{z_1, z_2, \ldots, z_m\}, x_0)$. Puede probarse que este grupo fundamental es un grupo libre en generadores y cada

[2]Ver (Hatcher, 2002).

generador corresponde a un lazo $\gamma_i \colon I \to \mathbb{C} \setminus \{z_1, z_2, \ldots, z_m\}$ basado en x_0 que rodea a la singularidad z_i (Hatcher, 2002).A continuación describimos cómo podemos "levantar" estos lazos y cómo permutan las ramas de una función algebraica.

4.2. Espacios cubrientes, levantamientos y monodromía

En esta sección consideraremos espacios cubrientes de n-hojas con la aplicación cubriente $p \colon Y \to X$. Definiremos la noción de levantamientos y veremos cómo pueden utilizarse los levantamientos de lazos basados en el espacio X y explicaremos cómo estos levantamientos inducen permutaciones de las hojas del espacio de recubrimiento.

4.2.1. Espacios cubrientes y levantamiento

Ahora veremos cómo la noción de espacios cubrientes nos da las herramientas necesarias para afirmar la existencia de un levantamiento de caminos y por ende, del grupo fundamental. Este levantamiento conserva la estructura algebraica, es decir, también es un grupo, que está asociado a la función que correspondía a la superficie construida previamente.

Definición 4.3. Sea $p \colon Y \to X$ una aplicación cubriente. Si $\gamma \colon Z \to X$ es una aplicación continua, un **levantamiento** de γ es una aplicación continua $\tilde{\gamma} \colon Z \to Y$ ta que $p \circ \tilde{\gamma} = \gamma$, es decir, el siguiente diagrama conmuta.

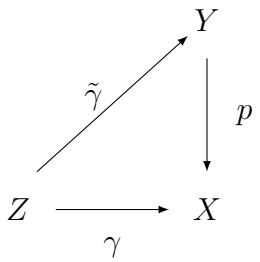


Figura 4.6. Diagrama que representa la propiedad de levantamiento.

Entre los resultados más importantes sobre levantamientos, tenemos los siguientes teoremas que aseguran la unicidad de levantamiento de caminos y más aún, de homotopías, las pruebas pueden ser revisadas en (Hatcher, 2002) y (Munkres, 2000).

Teorema 4.2.1 (Levantamiento de curvas)**.** *Sea $x_0 \in X$ y $p \colon Y \to X$ una función cubriente y supongamos que $p(y_0) = x_0$. Entonces cualquier camino $\gamma \colon I \to X$ que*

comienza en x_0 tiene un levantamiento único a un camino $\tilde{\gamma}$ en Y que comienza en y_0.

Así como podemos levantar caminos, podemos levantar también homotopías. Para ver esto, necesitamos el siguiente lema, cuya demostración se encuentra en (Munkres, 2000).

Lema 4.2.1. *Sea Z un espacio arbitrario y $\{U_j\}$ una cubierta abierta de $Z \times I$. Entonces para cada $z \in Z$ existe una vecindad N_z de z en Z y un entero positivo n tal que $N_z \times [t_{r-1}, t_r] \subset U_j$ para alguna j, para cada $1 \leqslant r \leqslant n$.*

Teorema 4.2.2 (Levantamiento de Homotopías)**.** *Sea $p\colon Y \to X$ una aplicación cubriente. Sea Z un espacio arbitrario y $\gamma\colon Z \to X$ una aplicación continua que tiene un levantamiento $\tilde{\gamma}\colon Z \to Y$. entonces toda homotopía $F\colon Z \times I \to X$ con $F(z,0) = \gamma(z)$ para cada $z \in Z$ puede ser levantada a una homotopía $\tilde{F}\colon Z \times I \to Y$ con $\tilde{F}(z,0) = \tilde{f}(z)$ para cada $z \in Z$. Además, si F es una homotopía relativa a un subconjunto Z' de Z, entonces $\tilde{F}$ también lo es.*

Sea $\varphi\colon X \to Y$ una aplicación continua, tenemos los siguientes hechos:

1. Si α, β son caminos en X, entonces $\varphi\alpha$ y $\varphi\beta$ son caminos en Y.
2. Si $\alpha \sim \beta$, entonces $\varphi\alpha \sim \varphi\beta$.
3. Si α es un lazo en X, basado en x, $\varphi\alpha$ es un lazo en Y, basado en $\varphi(x)$.

Así, si $[\alpha] \in \pi_1(X, x)$, $[\varphi\alpha]$ es un elemento bien definido de $\pi_1(Y, \varphi(x))$. Y definimos

$$\varphi_*\colon \pi_1(X, x) \to \varphi(Y, \varphi(x)),$$

donde

$$\varphi_*([\alpha]) = [\varphi\alpha]\,.$$

Y podemos probar que este es un homomorfismo de grupos, al cual llamamos **homomorfismo inducido** por φ, ver (Hatcher, 2002).

Corolario 4.2.1. *Sea $p\colon Y \to X$ una aplicación cubriente, $y_0 \in Y$ y $x_0 = p(y_0) \in X$. Entonces el homomorfismo inducido por los lazos basados en x_0, $p_*\colon \pi_1(Y, y_0) \to \pi_1(X, x_0)$ tal que $p_*[\gamma] = [p\gamma]$ es inyectivo.*

Demostración. Sean $[\tilde{\alpha}], [\tilde{\beta}] \in \pi_1(Y)$ tales que $[p \circ \tilde{\alpha}] = [p \circ \tilde{\beta}] \in \pi_1(X)$. Entonces los lazos $\tilde{\alpha}, \tilde{\beta}$ son levantamientos de los lazos $[\alpha] = [p \circ \tilde{\alpha}]$ y $\beta = [p \circ \tilde{\beta}]$. Como $[\alpha] = [\beta]$, es decir que α y β son equivalentes homotópicos, entonces $\tilde{\alpha}$ y $\tilde{\beta}$ también lo son. $\square$

4.2.2. Monodromía de un espacio cubriente de n-hojas

Consideremos entonces a la aplicación cubriente $\pi\colon Y \to X$, donde Y es un espacio cubriente de n hojas, un punto $x_0 \in X$ y su **fibra** que consta de n elementos, $F := \{a \in Y \mid a = \pi^{-1}(x_0)\}$. Tomamos el grupo fundamental de X y definimos una acción[3] de $\pi(X, x_0)$ en la fibra F de x_0.

Sea $\gamma\colon I \to X$ un lazo basado en x_0, tomaremos $a \in F$. El Teorema 4.2.1 nos asegura que f se levanta a un único camino $\tilde{\gamma_a}\colon I \to Y$ que inicia en $\tilde{\gamma_a}(0) = a$. Como Y es un recubrimiento de n hojas y $\pi(\tilde{\gamma_a}(1)) = \gamma(1)$, la preimagen $\pi^{-1}(\gamma(1)) \in F$ aunque no necesariamente coincide con a. Esto 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. Al homomorfismo $\varphi_\pi\colon \pi_1(X, x_0) \to \mathrm{Aut}(F)$ que corresponde a esta acción, lo llamamos **monodromía del espacio de recubrimiento** y la imagen de este homomorfismo es el **grupo de monodromía** de π. Nótese que F es un conjunto de n elementos, por lo que su grupo de monodromía es un subgrupo de $S_n = \mathrm{Aut}(F)$.

Ejemplo 4.3. En el Ejemplo 3.4.Tenemos un espacio de recubrimiento de 2 hojas y la aplicación cubriente ß: $S \to \mathbb{C}^*$, al dar una vuelta alrededor de cero en el plano $\mathbb{C}^*$, en la superficie pasamos de la hoja 1 a la hoja 2 y viceversa. Entonces el grupo de monodromía de este espacio es $\mathbb{Z}_2$.

En general, para las funciones de la forma $\sqrt[n]{z}$ se permutan cíclicamente las n hojas al dar vueltas alrededor de $z = 0$, por lo tanto, el grupo de monodromía correspondiente a estos espacios es $\mathbb{Z}_n$.

Ejemplo 4.4. La función $\sqrt{z^2}$ tiene como grupo de monodromía al grupo trivial $\{e\}$, pues las hojas no están conectadas entre sí.

4.3. Grupos de monodromía de funciones algebraicas

En esta sección consideraremos una función algebraica f. Como vimos en el capítulo anterior, a f podemos asociarle una superficie de Riemann S y una aplicación cubriente de n-hojas $\pi\colon S \to \hat{\mathbb{C}} \setminus \{\text{puntos singulares de } f\}$.

[3]Una acción (derecha) de un grupo G en un conjunto X es una función $\varphi\colon G \times X \to X$ tal que para cada $x \in X$ y para cada $g, h \in G$, se cumple

1. $x \cdot e = x$
2. $x \cdot (gh) = (x \cdot g) \cdot h$, (gh) es el elemento resultante de la operación en G.

Teniendo una función algebraica f n-valuada, consideraremos un punto base x_0 en el plano $\hat{\mathbb{C}} \setminus \{\text{puntos singulares de } f\}$. Tenemos una función con n elementos analíticos $(f_j, D_j), j = 1, \ldots, n$ y cuyos valores en ese punto son $f_j(x_0)$, es decir, la fibra.

Sea γ un lazo en $\hat{\mathbb{C}} \setminus \{\text{puntos singulares de } f\}$ un lazo dado por $x(t)$ tal que $x(0) = x(1) = x_0$ y fijamos un valor $f_j(x) = f_j$. Denotamos por $F_{x_0} = \{f_1, \ldots, f_n\}$ a la fibra sobre x_0. Y definimos el punto final de la imagen de la curva por continuidad a lo largo de γ, de manera que $f_j = f(x(1))$. Notemos que al iniciar en distintos valores, como vimos en el capítulo 2, terminamos en distintos valores de la función. Así, estamos definiendo entonces una acción del lazo $\gamma \in \pi_1(X, x_0)$ en la fibra F_{x_0}.

Nota 4.2. Podemos ver que el **grupo de monodromía** de la función algebraica f es el grupo de monodromía del espacio cubriente de n-hojas $\pi\colon S \to \hat{\mathbb{C}} \setminus \{\text{puntos singulares de } f\}$. Denotamos a este grupo por $\text{Mon}(f)$. Notemos que $\text{Mon}(f)$ está generado por las permutaciones de los valores de f aa lo largo de los lazos γ que rodean los puntos singulares de f.

Dado que la fibra de un punto en $\hat{\mathbb{C}} \setminus \{\text{puntos singulares de } f\}$ son los n valores de la función en ese punto, cada uno está definido en una hoja de la superficie de Riemann asociada a la función. Podemos considerar entonces una biyección entre las ramas de una función y las hojas de la superficie.

Sean $h_1, h_2, \ldots, h_n$ las hojas de la superficie de Riemann asociada a f, hacemos corresponder distintos valores con distintas hojas del esquema de la superficie a través de $\psi\colon F_x \to S$ tal que $f_i \mapsto h_i$.

Valores de $w(z)$ a lo largo de C, f_i	Hoja correspondiente $h_i = \psi(f_i)$
f_i	h_i
f_{i+1}	h_{i+1}
f_{i+2}	h_{i+2}
$\vdots$	$\vdots$
f_{i+k}	h_{i+k}
$\vdots$	$\vdots$
$f_{i+(n-1)}$	$h_{i+(n-1)}$

Tabla 4.1. Correspondencia entre valores de una función y hojas de una superficie de Riemann.

Ahora consideramos las acciones de $\pi_1(\hat{\mathbb{C}} \setminus \{\text{puntos singulares de } f\}, x_0)$ sobre estos elementos.

Definición 4.4. Al grupo libre generado por las permutaciones que corresponden al levantamiento de los lazos alrededor de todos los puntos de ramificación, le llamaremos **grupo de permutación del esquema** al subgrupo generado por las elementos $g_1, g_2, \ldots, g_k$.

Definición 4.5. Sean $g_1, g_2, \ldots, g_k$ las permutaciones de las hojas del esquema de la superficie de Riemann inducidas por los lazos en $\pi_1(\hat{\mathbb{C}}\backslash\{\text{puntos singulares de } f\}, x_0)$. Al subgrupo de S_n generado por estas permutaciones lo llamamos **grupo de monodromía** de la superficie de Riemann o asociado al esquema.

Así, cada permutación de los valores f_j corresponde a una única permutación de las hojas de la superficie, puede probarse que existe una biyección entre ellos y con esta biyección, probamos la siguiente propiedad importante:

Proposición 4.1. *El grupo de monodromía de una función algebraica f y el grupo de monodromía del esquema asociado a la misma, son isomorfos.*

A continuación veremos ejemplos de esquemas de algunas funciones específicas.

Ejemplo 4.5. Observemos el esquema de la superficie de Riemann para la función $\sqrt{z} + \sqrt{z-1}$ y enumeraremos las hojas de abajo hacia arriba.

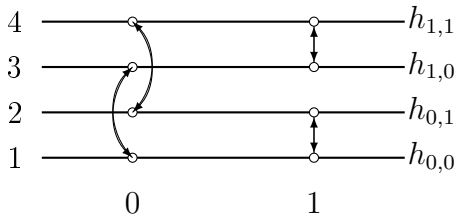


Figura 4.7. Esquema de la superficie de Riemann de la función $\sqrt{z} + \sqrt{z-1}$.

Ahora veremos sus permutaciones correspondientes, si se enumeran las hojas de 1 a n comenzando en la de abajo.

- Alrededor de $z = 0$

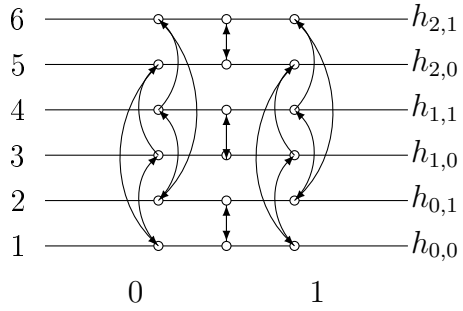
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24).$$

- Y alrededor de $z = 1$, tenemos:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34).$$

Su grupo de monodromía es el generado por las permutaciones anteriores, es decir $\langle (13)(24), (12)(34) \rangle$.

Ejemplo 4.6. De la misma manera, observamos el esquema de la función $\sqrt[3]{z^2-1}+\sqrt{1/z}$



Las permutaciones correspondientes a este esquema están dadas por

- Alrededor de $z = \pm 1$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (135)(246).$$
- Alrededor del punto $z = 0$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix} = (12)(34)(56).$$

El grupo de monodromía asociado a este esquema es $\langle (135)(246), (12)(34)(56) \rangle$.

Ejemplo 4.7. Consideremos el esquema de la función $\sqrt[3]{z^2-1}$.

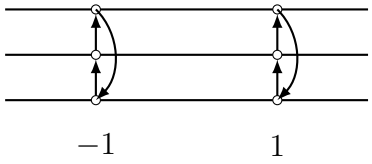


Figura 4.8. Esquema de la superficie de Riemann de la función $\sqrt[3]{z^2-1}$.

Ambos puntos de ramificación, $z = 1$ y $z = -1$, permutan las 3 hojas cíclicamente, por lo que el grupo correspondiente a este esquema es $\mathbb{Z}_3$.

Ejemplo 4.8. Del ejemplo 3.11, en la función $\sqrt{z}+\sqrt{z}$, el esquema construido por el método formal tiene 4 hojas que se permutan por pares, es decir $\mathrm{Mon}(\sqrt{z}+\sqrt{z}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Sin embargo, al observar el esquema real, que solamente tiene 3 hojas y únicamente dos están conectadas, alternándose de forma cíclica. Por lo tanto $\mathrm{Mon}(\sqrt{z}+\sqrt{z}) \cong \mathbb{Z}_2$.

Ejemplo 4.9. En el esquema de la función $\sqrt[3]{z^2-1}+\sqrt{1/z}$, analizado en el ejemplo 4.6, alrededor de los puntos $z=\pm 1$ fijamos el segundo índice 0 o 1 y permuta cíclicamente los primeros índices 0,1,2. Alrededor de $z=0$, se fija el primer índice 0, 1 o 2 y permutamos el segundo índice 0 y 1. Por lo tanto $\mathrm{Mon}(\sqrt[3]{z^2-1}+\sqrt{1/z}) \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

Recordando las propiedades de las funciones solubles por radicales cumplen con la propiedad de monodromía, describiremos ahora qué sucede con sus grupos de monodromía, estas propiedades son una parte crucial para la prueba de Arnold del teorema de Abel-Ruffini.

Proposición 4.2.

1. *Sea* $h(z)=f(z)\square g(z)$, *donde* $\square$ *puede ser cualquier operación aritmética,* $+,-,\cdot,/$. *Con* $\mathrm{Mon}(f)=F$ *y* $\mathrm{Mon}(g)=G$, *entonces el grupo de monodromía de* $\mathrm{Mon}(h) < F \times G$, *construida por el método formal.*

2. *Si* H_1 *es el grupo de monodromía del esquema obtenido por el método formal y* H_2 *el grupo del esquema real, existe un homomorfismo sobreyectivo de* H_1 *en* H_2.

Demostración.

1. Tomemos un punto de ramificación z_0 de $h(z)$ y que dar una vuelta alrededor de este punto corresponde a las permutaciones a_1 y a_2 del esquema de las funciones $f(z)$ y g_2 respectivamente. Nótese que si z_0 es punto de ramificación únicamente de $f(z)$, entonces $a_2=e$ y $g_1=e$ cuando z_0 es únicamente punto de ramificación de $g(z)$.

   Tomando las ramas $h_{i,j}(z)$ de $h(z)$ con subíndices i,j correspondientes a las ramas de $f(z)$ y $g(z)$ respectivamente, al rodear el punto z_0, las ramas i y j permutan de forma independiente, es decir, el índice i es permutado por g_1; y j, por g_2, siendo una permutación de $h(z)$ el par $(g_1,g_2)\in F\times G$. Al corresponder estas permutaciones a todos los puntos de ramificación de $h(z)$, estamos generando un subgrupo de $F\times G$.

2. Al construir un esquema por el método formal, resulta que algunas ramas coinciden. Sea z_i un punto de ramificación de $h(z)$, al dar una vuelta alrededor del mismo, nos movemos de un paquete de hojas a otro (en el método formal). Entonces obtenemos una permutación arbitraria $g_i\in H_1$ de los paquetes

de hojas, conservando los que coinciden. Entonces el producto de dos permutaciones $g_1 g_2$, que conservan los paquetes, también los conservará. Todas las permutaciones de H_1 conservan la cantidad de hojas.

Sea $\varphi : H_1 \to H_2$, $g_i \mapsto \tilde{g}_i$, dado que g_i conserva los paquetes repetidos y $\tilde{g}_i$ conserva únicamente un paquete que representa a los repetidos en el esquema real, entonces se seguirán conservando en el producto, es decir:

$$\varphi(g_1 g_2) = \tilde{g}_1 \tilde{g}_2$$

que es un homomorfismo que hace corresponder a cada conjunto de hojas en H_1 una única hoja en H_2. Es decir que cada hoja del esquema correcto tiene un conjunto de hoja en H_1 como preimagen, lo cual implica que el homomorfismo es sobreyectivo. □

4.4. Prueba de Arnold del teorema de Abel-Ruffini

En esta sección probaremos el teorema de Abel-Ruffini, basándonos en las ideas de Arnold, plasmadas en (Alekseev, 2004). Como detallamos a continuación, la prueba consiste en considerar una familia de ecuaciones polinomiales de grado 5 particular (ver ecuación 4.1) y estudiar la función algebraica que expresa sus raíces. Con lo desarrollado en este capítulo y los capítulos anteriores calculamos el grupo de monodromía de esta función y obtenemos que es el grupo simétrico S_5.

Como probaremos a continuación, en el Teorema 4.4.1, las funciones algebraicas solubles por radicales tienen grupo de monodromía soluble. En el capítulo 1 probamos que S_5 no es soluble, en consecuencia la función algebraica definida por la ecuación 4.1 no puede ser soluble por radicales, lo que implicará la imposibilidad de la existencia de una fórmula general para solucionar ecuaciones polinomiales de grado 5, como vemos a detalle en el Teorema 4.4.2.

Teorema 4.4.1. *Si la función multivaluada $h(z)$ es representable por radicales, su grupo de monodromía es soluble.*[4]

Demostración. Si F y G son solubles, también lo será el grupo de monodromía, H, de la función $h(z) = f(z) \square g(z)$, construidos por el método formal.

[4]Este teorema es válido en general para funciones analíticas. Utilizando combinaciones de la función identidad, operaciones aritméticas y funciones analíticas. En este caso, podemos obtener grupos de orden infinito. Ver (Porter, 1983).

Sabemos que $H \subseteq F \times G$, el cual es soluble, ya que F y G lo son. Y como existe un homomorfismo sobreyectivo $\varphi : H_1 \to H_2$, H_2, el grupo de monodromía del esquema real, es soluble, donde $\square$ es cualquiera de las operaciones $+, -, \cdot, /$.

Por otro lado, si F es soluble y $h(z) = [f(z)]^n$, entonces se hace corresponder $h_i(z) = [f_i(z)]^n$. Obteniendo entonces un homomorfismo sobreyectivo $\varphi F \to H$, por lo que H es soluble.

En el caso $h(z) = \sqrt[n]{f(z)}$, considerando el homomorfismo $\phi : H \to F$ tal que $\phi(g_i) = \tilde{g_i}$, cumplirá que $\phi(g_i g_j) = \tilde{g_i}\tilde{g_j}$, que es un homomorfismo sobreyectivo que hace corresponder cada hoja de F con un paquete en H. Entonces el cociente $H/ker(\phi) \cong F$ por el teorema 1.3.4. Como $ker(\phi)$ es conmutativo y F es soluble, entonces H es soluble.

Por lo tanto si una función es representable por radicales, tiene grupo de monodromía soluble. $\square$

Nos interesa probar que la fórmula general para las raíces de una ecuación de grado 5 o mayor no es soluble por radicales, entonces consideraremos la siguiente función y veremos paso a paso lo que sucede con sus raíces.

$$P_z(w) = 3w^5 - 25w^3 + 60w - z = 0. \tag{4.1}$$

Primero analizaremos sus puntos singulares. Para ello, usaremos la Proposición 2.4. Esta asegura que si w_0 es raíz de $P_z(w)$, entonces w_0 es raíz de $P'_z(w)$ con un grado menor de multiplicidad y tenemos que

$$P'_z(w) = 15w^4 - 75w^2 + 60 = 15(w^2 - 1)(w^2 - 4),$$

de donde encontramos las raíces $w_0 = \pm 2$ y $w_0 = \pm 1$, sustituyendo estos valores en 4.1 obtenemos que para los valores $z = \pm 16$ y $z = \pm 38$ respectivamente, éstas son raíces. Por lo que la ecuación 4.1 tiene 4 raíces distintas y para $z \in \mathbb{C} \setminus \{\pm 16, \pm 38\}$, tiene 5 raíces distintas.

Supongamos ahora que existe una función que representa las raíces de 4.1, $w(z)$, sabemos que es multivaluada y depende de z. Entonces tomamos un $z_0 \in \mathbb{C}$, fijando uno de sus valores $w(z_0) = w_0$ y consideremos un disco $D = |w - w_0| < r$ donde r es muy pequeño, delimitado por el círculo $\gamma = |w - w_0| = r$. Consideraremos la imagen de γ bajo $\tau = P_{z_0}(w)$ y la llamaremos C'.

Al descomponer $P_{z_0}(w)$ en polinomios de grado 1, obtenemos $P_{z_0} = 3(w - w_1)(w - w_2)(w - w_3)(w - w_4)(w - w_5)$, donde cada w_i es solución de $P_{z_0} = 0$.

Notamos que la variación del argumento de γ alrededor de cada w_i, depende de que w_i esté o no en D.

$$\varphi(\gamma) = \begin{cases} 2\pi, \text{ si } w_i \in D \\ 0, \text{ si } w_i \notin D \end{cases}$$

Por lo que $\varphi(\gamma') = 2\pi m$ donde m es la cantidad de raíces de $P_{z_0}(w) = 0$ con su multiplicidad, dentro de D, es decir, γ' tiene índice m alrededor de $\tau = 0$, como se muestra en la siguiente figura.

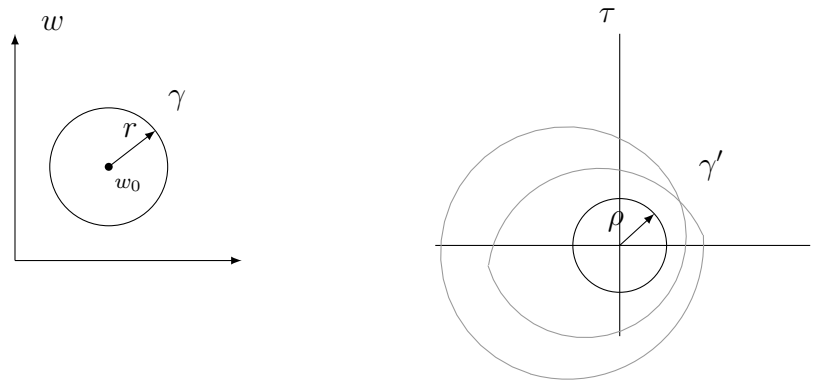


Figura 4.9. Comportamiento de los lazos γ y γ' alrededor de un punto dentro del disco D y $\tau = 0$ respectivamente.

Consideremos ahora el plano z y un punto z_0' cercano a z_0. Entonces tenemos un nuevo polinomio $\tau' = P_{z_0'}(w)$ y la imagen de γ bajo τ' se llamará γ''. Sabemos que

$$P_{z_0'}(w) = P_{z_0} + (z_0 - z_0'),$$

entonces la curva C'' es un desplazamiento de γ' dado por el vector $z_0 - z_0'$. Siempre que $|z_0 - z_0'| < \rho$, el índice de γ'' y γ' alrededor de $\tau = 0$ coinciden, entonces el disco contiene también a una raíz de la ecuación 4.1 cuando $z = z_0'$. Es decir, que variando continuamente z a lo largo de un camino comenzando en z_0, $w(z)$ queda definido por continuidad a lo largo de un camino que comienza en w_0.

Conociendo los puntos singulares de $P_z(w)$, que son $z = \pm 38$ y $z = \pm 16$, mostraremos que son los únicos puntos de ramificación que puede tener este polinomio.

Los puntos $z_0 \in \mathbb{C} \setminus \{\pm 16, \pm 38\}$ tienen 5 imágenes bajo $w(z)$, digamos w_i $i = 1, 2, 3, 4, 5$. Cada una de éstas define una imagen continua a lo largo de un camino γ bajo $w(z)$, que comienza en z_0 y está en definida en los discos D_i, con centro en w_i disjuntos entre sí. Si hubiesen dos imágenes de γ que comienzan en w_i, entonces habría al menos 6 imágenes y no es posible, pues el grado de $P_z(w)$ es 5.

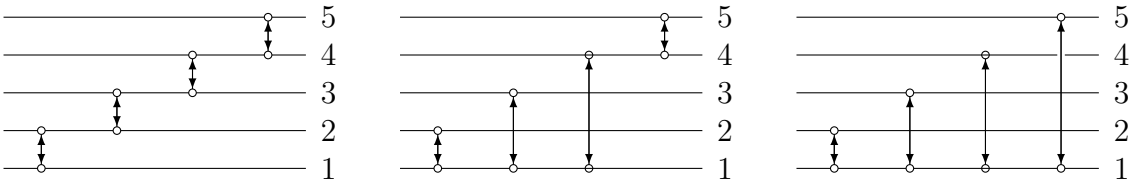
Sabemos que existe D_0 con centro en z_0 tal que para cada $z_0' \in D_0$ existe al menos una imagen en cada D_i en el plano w.

Cuando $\gamma \subset D_0$, todas sus imágenes están en los D_i, pero no existe ninguna función continua que permita pasar de un D_j a otro disco D_k, ya que son disjuntos, por lo tanto, todas las imágenes pertenecen a algún único D_j. Si γ comienza en z_0', sus puntos finales son las imágenes de z_0' bajo $w(z)$. Como $\gamma' \subseteq D_i$ y el disco contiene una única imagen de z_0', entonces γ' tiene sólo un punto final que coincide con el inicial cuando $\gamma \subset D_0$. En particular, esto sucede con todos los círculos con centro en z_0 y radio $\rho > 0$, lo que implica que z_0 no es punto de ramificación.

Ahora sabemos que para los valores distintos a $z = \pm 38$ y $z = \pm 16$, la ecuación 4.1 tiene raíces w_1, w_2, w_3, w_4 donde una tiene multiplicidad 2, digamos w_1. Tomando z_0' cerca de z_0 tenemos entonces que cerca de w_1 hay dos imágenes de z_0' bajo $w(z)$, mientras para las otras, tenemos una sola imagen. Entonces un lazo γ de radio pequeño con centro z_0 y basado en z_0', tiene imagen bajo $w(z)$ cerrada en w_2,w_3, w_4, mientras en w_1 puede tomar punto final distinto. Por lo que z_0' puede unir dos hojas.

Consideremos un camino que $\gamma\colon I \to \hat{C} \setminus \{\pm 38, \pm 16\}$ que une a $a, b \in \hat{C} \setminus \{\pm 38, \pm 16\}$ y γ' su imagen bajo $z(w) = 3w^5 - 25w^3 + 60w$, como $z(w)$ es continua, la imagen γ' es continua. Notemos que $z(w)$ y $w(z)$ representan la relación $3w^5 - 25w^3 + 60w - z = 0$, entonces γ es la imagen misma de γ' bajo $w(z)$ y no pasa por los puntos singulares. Por esto, $z = \pm 38$ y $z = \pm 16$ son los únicos puntos de ramificación y procedemos a construir el esquema de la superficie de Riemann.

Las formas posibles de obtener un esquema de 5 hojas con 4 puntos de ramificación donde cada uno une dos hojas son:



(a) Esquema 1 **(b)** Esquema 2 **(c)** Esquema 3

Notemos que el esquema 1 tiene todas las transposiciones elementales (12), (23),(34) y (45). Por el teorema 1.4.1, sabemos que S_5, el cual no es soluble.

En los esquemas 2 y 3, podemos expresar las transposiciones como (por el Lema 1.4.4) de la siguiente forma:

$$(23) = (12)(13)(12),$$

$$(34) = (13)(14)(13),$$

En el esquema 2,

$$(45) = (14)(15)(14),$$

mientras en el 3 corresponde únicamente a la permutación correspondiente a la cuarta raíz. Por lo tanto, $\mathrm{Mon}(f) = S_5$, que mostramos anteriormente (teorema 1.4.4) que no es soluble. Con esto, procedemos a probar el teorema de Abel-Ruffini.

Teorema 4.4.2 (Abel-Ruffini)**.** *Para $n \geqslant 5$, la ecuación general algebraica de grado n*

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

no es soluble por radicales.

Demostración. Consideremos el caso general, las ecuaciones de la forma

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

A la expresión para sus raíces $w(z)$ le correspondería una superficie de Riemann de 5-hojas, por lo que su grupo de monodromía sería un subgrupo de S_5.

En particular, para la ecuación 4.1 y siendo $w(z)$ la función que expresa sus raíces, vimos qu $\mathrm{Mon}(w) \cong S_5$, esto implica que w no es soluble por radicales, probando así, que el caso general no será soluble por radicales.

Para las ecuaciones polinomiales de grado $n > 5$, consideramos la ecuación

$$P_z(w) = (3w^5 - 25w^3 + 60w - z)w^{n-5} = 0 \tag{4.2}$$

Donde la expresión $w(z)$ para las raíces de ésta, es la misma que para la ecuación 4.1, entonces su grupo de monodromía es un subgrupo de S_n, isomorfo a S_5, es decir, es un grupo que no es soluble. Por lo tanto, las raíces de los polinomios de grado mayor o igual a 5, no son solubles por radicales.

Por lo tanto, la expresión general de las soluciones de ecuaciones polinomiales de grado mayor o igual a 5 no es soluble por radicales. □

CONCLUSIONES

1. Se identificó la solubilidad de un grupo estudiando sus subgrupos normales y se probó que los grupos S_n a partir de 5 no son solubles.

2. Se estudiaron las propiedades de curvas y funciones continuas en el plano complejo y sus imágenes bajo funciones continuas, específicamente polinomios. Se esbozó una prueba del teorema fundamental del Álgebra, que garantiza la existencia de las raíces de los polinomios en $\mathbb{C}$.

3. Se describió cómo asociar un espacio de recubrimiento a una función algebraica y se estudió cómo se permutan las hojas de este espacio al circundar los puntos singulares a través de caminos. Esta información se capturó al estudiar sus grupos de monodromía.

4. Se probó que si una función es soluble por radicales, su grupo de monodromía es soluble. Con esto, se prueba el teorema de Abel-Ruffini, mostrando que existe una familia de ecuaciones de grado 5 que definen una función algebraica con grupo de monodromía no soluble. Esto implica la imposibilidad de la existencia de una fórmula general para ecuaciones de grado mayor o igual a 5.

RECOMENDACIONES

1. Comparar la prueba topológica del teorema con la prueba clásica que se estudia en un curso de Teoría de Galois para establecer el isomorfismo entre el grupo de monodromía y el grupo de Galois de un polinomio.

2. Utilizar el material del capítulo 3 y 4 como introducción a la topología algebraica.

3. Tomar estas notas como material de apoyo en español para estudiantes a nivel de licenciatura para el estudio de superficies de Riemann y monodromía.

BIBLIOGRAFÍA

Ahlfors, L. V. (2004). *Complex Analysis.* Mc-Graw Hill,Inc., New Jersey, second edition.

Ahlfors, L. V. y Sario., L. (1960). *Riemann Surfaces.* Princeton University Press, New Jersey.

Akalin, F. (2016). Why is the quintic unsolvable.

Alekseev, V. B. (2004). *Abel's Theorem in Problems y Solutions.* Kluwer Academic Publishers, Dordrecht.

Artin, M. (1991). *Algebra.* Prentice Hall, New Jersey.

Bartle, R. G. (1967). *The Elements of real Analysis.* John Wiley & Sons, Inc., New York.

Chinn, W. y Steenrod, N. E. (1966). *First Concepts of Topology.* The Mathematical Association of America, Washington, D. C.

Conway, J. B. (1978). *Functions of One complex Variable.* Spinger-Verlag, New York, second edition.

Dejon, B. y Henrici, P. (1969). *Constructive Aspects of the Fundamental Theorem of Algebra.* John Wiley & Sons, Inc., New York.

Dörrie, H. (1965). *100 Great Problems of Elementary Mathematics.* Dover Publications, Inc, New York.

Dugundji, J. (1978). *Topology.* Allyn and Bacon, Inc, Boston.

Dummit, D. y Foote, R. (2004). *Abstract Algebra.* John Wiley & Sons, Inc, New Jersey, third edition.

Fraleigh, J. B. y Katz, V. J. (2003). *A First Course in Abstract Algebra.* Pearson Education, Inc, 7th edition. s.l.

Gallian, J. (2013). *Contemporary Abstract Algebra*. Cenage Learning, Boston, eighth edition.

Gopalakrishnan, N. S. (2004). *University Algebra*. New Age International Publishers, New Delhi, second edition.

Hatcher, A. (2002). *Algebraic Topology*. Cambridge University Press, Cambridge.

Herstein, I. N. (1988). *Álgebra Abstracta*. Grupo Editorial Iberoamérica, México.

Muciño, J. (1985). *Superficies de Riemann y uniformización*. México.

Munkres, J. (2000). *Topology*. Prentice Hall, New Jersey, second edition.

Porter, M. (1983). *Superficies de Riemann*. CINVESTAV I.P.N., México.

Roman, S. (2006). *Field Theory*. Springer, second edition, s.l.

Santa Cruz, H. (2016). *A survey on the monodromy groups of algebraic functions*. Chicago.

Schwartz, R. K. (2015). Abel and the insolubility of the quintic. Consultado en octubre de 2015 en `http://www.researchgate.net/publication/272181262`. s.l.

Teleman, C. (2003). Riemann surfaces: class notes. Cambridge. Consultado noviembre de 2016 en `http://www.jchl.co.uk/maths/Riemann.pdf`

Villa Salvador, G. (2011). Las ecuaciones polinomiales como el origen de la teoría de galois. México. *Miscelánea Matemática.SMM.*

Zoł, H.(2000). The topological proof of abel-ruffini theorem. *Journal of the Juliusz Schauder Center*.s.l.