PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
ESCUELA DE POSGRADO

Aspectos geométricos de la irresolubilidad de una ecuación algebraica de grado cinco

Tesis para optar el grado de
Magíster en Matemáticas.

Autor:
Sandro Wilfredo Sosaya Salazar.

Asesor
Dr. Rudy Rosas Bazan.
Jurado
Dr. Christian Valqui Haase.
Dr. Jonathan Farfán Vargas.

LIMA-PERÚ
2015

ASPECTOS GEOMÉTRICoS DE LA IRRESOLUBILIDAD DE UNA ECUACIÓN DE GRADO CINCO

Sandro Wilfredo Sosaya Salazar

Tesis presentada a consideración del cuerpo docente de la Escuela de Posgrado, de la PUCP, como parte de los requisitos para obtener el grado académico de Magíster en Matemática.

Miembros del jurado:

Dr. Christian Valqui Haase (presidente)

Dr. Jonathan Farfán Vargas (miembro)

Dr. Rudy Rosas Bazan (asesor)

LIMA - PERÚ

2015

ESCUELA DE POSGRADO

RESUMEN DE LA TESIS

Sandro Wilfredo Sosaya Salazar
Matemática

ASPECTOS GEOMÉTRICOS DE LA IRRESOLUBILIDAD DE UNA ECUACIÓN DE GRADO CINCO

En el presente trabajo estudiaremos que es imposible obtener una fórmula a base de operaciones fundamentales (adición, sustracción, división, multiplicación, potenciación y radicación) que nos dé las soluciones de una ecuación algebraica general de grado $n \geq 5$. Este problema fue resuelto por el matemático Niels Henrik y por Évariste Galois. Daremos una demostración algo "más geométrica" que la clásica demostración vía la teoría de Galois. La idea central será el estudio de las "deformaciones" que sufren las raíces de un polinomio como consecuencia de una "deformación" del polinomio.

a mis hijos Matías y Fabián.

Agradecimientos

Al Dr. Rudy Rosas por su orientación y apoyo en el desarrollo de la tesis. A mi familia, por su constante apoyo para la obtención de mi grado. En especial a mi esposa Jakelí por estar siempre a mi lado apoyándome en los buenos y malos momentos de mi vida.

Índice general

Introducción

En el presente trabajo tratamos uno de los más grandes problemas que tuvo la matemática, encontrar una "fórmula" que dé las soluciones (resolver) de la ecuación algebraica general $a_n x^n + ... + a_1 x + a_0 = 0$ de grado $n \in \mathbb{N}$. Antes de iniciar con nuestro trabajo daremos una breve historia de los intentos por encontrar las soluciones (dar una fórmula que las provee) de las ecuaciones algebraicas, para más información ver [12],[8], [10]. Una de la fórmulas más conocidas en las Matemáticas es la que provee las soluciones de una ecuación algebraica de segundo grado ($n = 2$). Los babilonios fueron los primeros que resolvieron estas ecuaciones (llamadas ecuaciones cuadráticas) empleando el método conocido actualmente como "completar el cuadrado". También encontraron las soluciones para algunas ecuaciones de grado 4, tratándolas como ecuaciones cuadráticas "disfrazadas" y resolverlas como tales. Por ejemplo, si deseamos obtener las soluciones de $x^4+5x^2+4 = 0$, podemos considerar $y = x^2$, obteniendo la ecuación $y^2 + 5y + 4 = 0$. Posteriormente, los griegos y los árabes consiguieron resolver ecuaciones de segundo grado utilizando, también, el método de completar el cuadrado con la aplicación del concepto de área; se valieron de representaciones geométricas para mostrar hechos algebraicos, como se evidencia en el libro II de los Elementos de Euclides.[11]

La fórmula que permite encontrar las soluciones de cualquier ecuación para $n = 3$ (ecuación cúbica) no se encontró sino hasta el siglo XVI, en Italia. Una ecuación cúbica es de la forma $a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ donde a_0, a_1, a_2 y a_3 son números cualesquiera, con $a_3 \neq 0$. Spicione Del Ferro(1465 - 1526) encontró un método para encontrar las soluciones de $x^3+a_1x+ = a_0$. De hecho todas la ecuaciones cúbicas pueden ser reducidas a esta forma (ver capítulo 2) si permitimos a a_1 y a_0 ser negativos, pero los números negativos no eran conocidos por aquel entonces. En 1530 Niccolo Fontana (1500-1557) conocido como *Tartaglia* recibió dos problemas en ecuaciones cúbicas y anunció que podía resolverlos (uno de estos era $x^3+a_1x+ = a_0$). Más adelante Gerolano Cardano(1501-1576) convenció a Tartaglia de que revelara su secreto para resolver ecuaciones cúbicas. La fórmula que permite conocer las soluciones de una ecuación cúbica es conocida con el nombre de “Fórmula de Cardano”, por que Cardano estudió a detalle las soluciones de Tartaglia y Del Ferro, luego fue quien publicó la fórmula por primera vez en un gran tratado sobre resolución de ecuaciones titulado *“Ars Magna”*. Cardano había notado que el método de Tartaglia requería de raíces cuadradas de números negativos; por consiguiente, incluyó estos cálculos en Ars Magna. Rafael Bombelli (1526-1572) estudió este problema en detalle y por esto es considerado como el descubridor de los números complejos. El método para encontrar las soluciones de una ecuación algebraica de grado cuatro fue dada por Lodovico Ferrari (1522-1565) y fue publicado en Ars Magna en 1545.

A lo largo de la historia fueron muchos los matemáticos que intentaron conseguir una fórmula que diera las soluciones de una ecuación algebraica de grado 5 y superior (desconociendo que esto era imposible lograrlo). Paolo Ruffini(1765-1822), haciendo uso de los trabajos sobre “permutaciones” de Joseph Louis Lagrange (1736-1813), fue el primero en acertar con la estrategia utilizada para demostrar la “irresolubilidad por radicales” de una ecuación algebraica de grado 5 a más, problema que sería finalmente resuelto por Niels Henrick Abel (1802-1829) en 1823. Abel publicó una prueba detallada en 1826 en el *Journal de Crelle(Journal für die reine und angewandte Mathematick)*. Este trabajo fue conocido por Évariste Galois (1811-1832). A diferencia del trabajo de Abel, Galois da una solución completa sobre exactamente qué ecuaciones son resolubles por radicales. La demostración de Galois es la ahora clásica demostración hecha cuando se estudia “La teoría de Galois”. El objetivo de este trabajo es demostrar, de una forma algo más geométrica, la irresolubilidad de la ecuación general de grado 5, veremos más adelante que demostrar esto es suficiente para decir que una ecuación general algebraica de grado n no es resoluble por radicales para $n > 5$.

En el primer capítulo iniciamos con algunos conceptos básicos que se deben tomar en cuenta para una mejor comprensión de nuestro trabajo. En el capítulo 2 daremos una definición de qué es ser “resoluble por radicales”. En el capítulo 3 estudiaremos el comportamiento de las raíces de un polinomio a medida que hacemos variar sus coeficientes. En el capítulo 4 estudiaremos el comportamiento de las de los “radicales intermedios” usando resultados del capítulo 3; por último, demostraremos por razonamiento por del absurdo la **irresolubilidad de una ecuación algebraica de grado 5** de una forma simple basándonos en resultados obtenidos a lo largo de este trabajo.

Capítulo 1

Preliminares

En este capítulo, discutiremos algunos tópicos que serán útiles para la continuación de los demás capítulos. Para más detalles pueden revisar [3],[5] y [4].

1.1. Grupos Simétricos y Alternados

Daremos inicio con el siguiente concepto simple que junto a otras ideas será de mucha utilidad para el desarrollo de nuestro trabajo .
Sea $n \in \mathbb{N}$. Definimos S_n como el conjunto de las biyecciones

$$\sigma : \{1, 2, ..., n\} \to \{1, 2, ..., n\}.$$

Este conjunto S_n junto con la operación usual de composición de funciones forman una estructura de grupo $(S_n, \cdot)$, llamado **Grupo Simétrico de grado** n. A una biyección $\sigma \in S_n$ le llamaremos permutación y a los elementos del dominio le llamaremos índices de la permutación. Por motivos de simplicidad en la definición de σ, denotaremos a σ por

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$$

que resume toda la información de la permutación σ.
Sea σ, $\tau \in S_n$. Definimos $\sigma \cdot \tau$ por

$$\begin{aligned} \sigma \cdot \tau &= \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & ... & n \\ \tau(1) & \tau(2) & ... & \tau(n) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & ... & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & ... & \tau(\sigma(n)) \end{pmatrix} \end{aligned}$$

Observación 1.1. *Debemos hacer notar que $(\sigma \cdot \tau)(i) = \tau(\sigma(i))$. Denotaremos a la permutación identidad mediante id. Esta permutación es el elemento neutro del grupo S_n.*

Ejemplo 1. *Sea $n = 3$. Los siguientes elementos de S_3:*

$$\sigma : \{1,2,3\} \to \{1,2,3\} \text{ tal que } \sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$$
$$\tau : \{1,2,3\} \to \{1,2,3\} \text{ tal que } \tau(1) = 3, \tau(2) = 1, \tau(3) = 2$$

se pueden denotar por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad y \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

y su producto es

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id$$

1.1.1. La Simplicidad de los Grupos A_n, $n \geq 5$

Recordemos que en la teoría de grupos, un grupo es llamado simple si no tiene subgrupos normales propios [5]. En esta sección probaremos la simplicidad de A_n, $n \geq 5$, que será el principal motivo por la cual una Ecuación algebraica general de grado $n \geq 5$ no puede ser resoluble por radicales.

Antes de definir el grupo A_n y probar su simplicidad para $n \geq 5$, precisamos desarrollar algunas definiciones y proposiciones sobre permutaciones.

Definición 1.1. *Decimos que una permutación $\sigma \in S_n$ es un ciclo de longitud $r > 1$ si existen $i_1, i_2, ..., i_r$ elementos distintos de $\{1, 2, ..., n\}$ tales que:*

1. $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$,...,$\sigma(i_{r-1}) = i_r$, $\sigma(i_r) = i_1$

2. $\sigma(j) = j$ *para todo* $j \in \{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_r\}$.

En este caso usaremos la siguiente notación simplificada:

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_r \end{pmatrix} \in S_n$$

Observación 1.2. *De acuerdo a la definición anterior también podemos expresar un ciclo de la siguiente forma*

$$\sigma = \begin{pmatrix} k & \sigma(k) & \dots & \sigma^{r-1}(k) \end{pmatrix},$$

donde $k = \text{mín}\,\{i /\, \sigma(i) \neq i,\ \text{siendo } i \text{ un índice de } \sigma\}$.

Observemos que cada vez que expresamos una permutación como un ciclo debemos hacer notar a que grupo simétrico pertenece, ya que esto podría causar confusión.

Ejemplo 2. *Sea* $\sigma = \begin{pmatrix} 2 & 4 & 5 \end{pmatrix}$ *un ciclo. Observar que no indicamos a que grupo simétrico pertenece, con lo cual se puede suponer que:*

1. *si* $\sigma \in S_5$, *entonces* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$,

2. *si* $\sigma \in S_6$, *entonces* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 5 & 2 & 6 \end{pmatrix}$.

Definición 1.2. *Sean* $\sigma, \tau \in S_n$ *ciclos de longitud* $r > 1$, *decimos que:*

1. *el conjunto* $Sop(\sigma) = \{i/\sigma(i) \neq i, \text{ siendo } i \text{ un índice de } \sigma\}$ *es el soporte de* σ.

2. σ *es una transposición si es un ciclo de longitud* 2*; y es dicha* **transposición simple** *si es una transposición tal que su soporte es* $\{i,\ i{+}1\}$ *para algún índice* $i < n$.

3. σ *y* τ *son ciclos disjuntos si sus soportes son disjuntos.*

Ejemplo 3. *En* S_4 *tenemos lo siguiente:*

1. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 4 \end{pmatrix}$ *es una transposición.*

2. $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ *no es un ciclo pero se puede escribir como producto de transposiciones, observemos que*

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

3. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix}$ *es una transposición simple.*

Proposición 1.3. *Si* σ *es un ciclo de longitud* $r > 1$, *entonces* $\sigma^r = id$.

Demostración. Por la observación 1.2, tenemos que $\sigma = \begin{pmatrix} k & \sigma(k) & \ldots & \sigma^{r-1}(k) \end{pmatrix}$, siendo $k = \text{mín } \text{Sop}(\sigma)$. Sea h un índice de σ, demostraremos para cada caso:

Si $h \notin \mathrm{Sop}(\sigma)$, entonces es claro que $\sigma^r(h) = h$. Si $h \in \mathrm{Sop}(\sigma)$, entonces $h = \sigma^s(k)$ para algún $s < r$ y, por lo tanto se tiene que

$$\sigma^r(h) = \sigma^r(\sigma^s(k)) = \sigma^s(\sigma^r(k)) = \sigma^s(k) = h.$$

Lo que prueba la proposición. □

Proposición 1.4. *Si dos ciclos son disjuntos, entonces conmutan.*

Demostración. Sean σ_A y σ_B dos ciclos de soporte disjuntos A y B. Si h es un índice fuera de ambos soportes, entonces queda fijo por ambos ciclos y

$$\sigma_A \cdot \sigma_B(h) = h = \sigma_B \cdot \sigma_A(h).$$

Por otro lado, si $h \in A$, entonces ni $\sigma_A(h)$ ni h son elementos de B y quedan fijos por σ_B. Así,

$$\sigma_A \cdot \sigma_B(h) = \sigma_A(h) = \sigma_B \cdot \sigma_A(h).$$

El mismo razonamiento se aplica a los índices $h \in B$. □

Visto el ítem 2 del ejemplo anterior, demostraremos un teorema relativo a esta idea de representar una permutación como producto de ciclos disjuntos.

Teorema 1.5. *Toda permutación $\sigma \in S_n$ diferente de id puede ser escrita de manera única (salvo el orden) como producto de ciclos disjuntos.*

Demostración. Demostraremos este teorema por inducción sobre n.

- Para $n = 2$ tenemos $S_2 = \left\{ id, \begin{pmatrix} 1 & 2 \end{pmatrix} \right\}$. Observemos que la única permutación de S_2 (distinta de la identidad) ya es una transposición.
- Supongamos que se cumple hasta cierto $n \geq 2$, entonces debemos probar que se cumple para $n + 1$.

Como $\sigma \neq id$, entonces $h \neq \sigma(h)$ para algún $h \in \{1, \ldots, n + 1\}$. Podemos suponer que dicho indice h es igual a 1. Con esto podemos formar el conjunto

$$\{1, \sigma(1), \sigma^2(1), \ldots, \sigma^k(1), \ldots\}$$

que tiene por lo menos 2 elementos distintos y a lo mas $n + 1$ elementos distintos. Entonces existe un k mínimo tal que

$$\sigma^k(1) \in \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)\}.$$

Afirmación: $\sigma^k(1) = 1$. En efecto: Sabemos que $\sigma^k(1) = \sigma^j(1)$ para algún $0 \leq j \leq k-1$.
Si $j \geq 1 \Rightarrow \sigma^{k-1}(1) = \sigma^{j-1}(1) \Rightarrow \ldots \Rightarrow \sigma^{k-j}(1) = \sigma^0(1) = 1$ ($\Rightarrow\Leftarrow$). Por lo tanto $j = 0$. Con esto tenemos la siguiente información con respecto de la permutación σ tal como se muestra en la figura 1.1

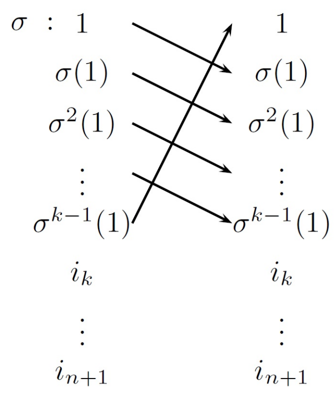

Figura 1.1: Definición de σ- Una parte.

Además, σ se puede expresar como producto de σ_1 y σ_2, donde

- $\sigma_1(i) = \begin{cases} \sigma(i) & \text{para } i \in \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)\} \\ i & \text{para } i \in \{i_k, \ldots, i_{n+1}\} \end{cases}$ y

- $\sigma_2(i) = \begin{cases} i & \text{para } i \in \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)\} \\ \sigma(i) & \text{para } \in \{i_k, \ldots, i_{n+1}\} \end{cases}$.

Observemos que σ_1 es un ciclo de longitud k cuyo soporte es $\{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1)\}$. Hasta ahora hemos demostrado que

$$\sigma = \begin{pmatrix} 1 & \sigma(1) & \sigma^2(1) & \ldots & \sigma^{k-1}(1) \end{pmatrix} \cdot \sigma_2$$

Solo nos faltaría demostrar que σ_2 se puede expresar como producto de ciclos disjuntos. Definamos

$$i_k := 1, \quad i_{k+1} := 2, \quad i_n + 1 := n - k + 1.$$

Estos índices son los únicos que cambian por la permutación σ_2, y podemos verlo como una permutación de S_{n-k+1}. Como $2 \leq n - k + 1 < n + 1$, entonces (por hipótesis) podemos expresarlo como producto de ciclos disjuntos. $\square$

Proposición 1.6. *Sea $\sigma \in S_n$ una permutación distinta de id, entonces σ se puede escribir como producto de transposiciones.*

Demostración. Por el teorema 1.5, será suficiente probar que un ciclo de longitud $r > 2$, $\begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_r \end{pmatrix}$, es producto de transposiciones y esto se sigue inmediatamente de la igualdad:

$$\begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_r \end{pmatrix} = \begin{pmatrix} i_1 & i_r \end{pmatrix} \begin{pmatrix} i_2 & i_r \end{pmatrix} \dots \begin{pmatrix} i_{r-1} & i_r \end{pmatrix}.$$

□

Ahora introduciremos el subgrupo $A_n \subset S_n$.[5]
Sea $P = p(x_1, ..., x_n)$ el siguiente polinomio en las variables $x_1, ..., x_n$

$$P = (x_1 - x_2)(x_1 - x_3)...(x_1 - x_n)(x_2 - x_3)...(x_2 - x_n)...(x_{n-1} - x_n)$$

el cual denotaremos por

$$P = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Si $\sigma \in S_n$, denotaremos por P^σ al siguiente polinomio:

$$P^\sigma = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Si $P^\sigma = P$ decimos que la permutación σ es una permutación par y si $P^\sigma = -P$ decimos que σ es una permutación impar. Es fácil verificar que si σ, $\tau \in S_n$ entonces $(P^\sigma)^\tau = P^{\sigma \cdot \tau}$ y de aquí se sigue inmediatamente que el conjunto de las permutaciones pares A_n es un subgrupo de S_n. Este subgrupo es llamado **grupo alternante de grado n**.

Observación 1.7. *Notar que* $|S_n/A_n| = 2$*; es decir, se trata de un subgrupo de índice* 2 *(de aquí se tiene por ejemplo que* $|A_5| = 60$*). El grupo alternante adquiere relieve por no poseer subgrupos normales propios, para* $n \geq 5$*; entre otras consecuencias, este hecho dará conclusiones al intento de resolver la ecuación algebraica general de grado* n *(*$n \geq 5$*).*

Por el momento sabemos que se puede descomponer una permutación cualquiera como producto de transposiciones. Tenemos muchas formas de descomponer una permutación en transposiciones, supongamos que se descompone en k transposiciones, ¿será cierto que la descomposición en producto de transposiciones mantiene la paridad de k?. Observemos lo siguiente:

Supongamos que $\sigma = \tau_1 \cdot \tau_2 \cdot \ldots \cdot \tau_{2k}$ se puede escribir como producto de una cantidad par de transposiciones. Tenemos que si

$$P = P(x_1, ..., x_n) = \prod_{1\leq i<j\leq n} (x_i - x_j)$$

entonces $P^\sigma = (-1)^{2k} \cdot P = P$ y por lo tanto $\sigma \in A_n$.

Nuestro interés es escribir toda permutación como producto de **transposiciones simples**, lo cual demostraremos en el siguiente corolario.

Corolario 1.8. *Toda permutación diferente de la identidad es producto de un número finito de transposiciones simples.*

Demostración. Sea $\sigma \in S_n$. Por la proposición 1.6 se tiene que σ se puede escribir como producto de transposiciones. Ahora, sólo demostraremos que cada transposición se puede escribir como producto de transposiciones simples. Observemos lo siguiente:

1. $\begin{pmatrix}1 & 2\end{pmatrix}$ ya es una transposición simple,
2. $\begin{pmatrix}1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}$,
3. $\begin{pmatrix}1 & 4\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}$,
4. y así se puede observar que

$$\begin{pmatrix}1 & k\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}...\begin{pmatrix}k-1 & k\end{pmatrix}\begin{pmatrix}1 & k-1\end{pmatrix}\begin{pmatrix}2 & k-1\end{pmatrix}\ldots\begin{pmatrix}k-2 & k-1\end{pmatrix}.$$

Análogamente podemos generar factores de transposiciones simples para otras transposiciones. En efecto:

1. $\begin{pmatrix}2 & 3\end{pmatrix}$ ya es una transposición simple,
2. $\begin{pmatrix}2 & 4\end{pmatrix} = \begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}$,
3. $\begin{pmatrix}2 & 5\end{pmatrix} = \begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}4 & 5\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}$,
4. y así se puede observar nuevamente que

$$\begin{pmatrix}2 & k\end{pmatrix} = \begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}...\begin{pmatrix}k-1 & k\end{pmatrix}\begin{pmatrix}2 & k-1\end{pmatrix}\begin{pmatrix}3 & k-1\end{pmatrix}\begin{pmatrix}k-2 & k-1\end{pmatrix}.$$

De manera análoga podemos descomponer las demás transposiciones. □

Tenemos que las transposiciones simples de S_5 son $\begin{pmatrix}1 & 2\end{pmatrix}$, $\begin{pmatrix}2 & 3\end{pmatrix}$, $\begin{pmatrix}3 & 4\end{pmatrix}$ y $\begin{pmatrix}4 & 5\end{pmatrix}$.
Definamos las siguientes permutaciones de S_5:

$$\psi_1 = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 2 & 3 & 4 & 1\end{pmatrix}, \qquad \psi_2 = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 5 & 3 & 4 & 2\end{pmatrix}$$
$$\psi_3 = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 5 & 4 & 3\end{pmatrix}, \qquad \psi_4 = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 3 & 5 & 4\end{pmatrix}$$

Con esto podemos mostrar el siguiente teorema que será muy útil para la demostración del objetivo principal de la tesis.

Teorema 1.9. *Cualquier permutación de S_5 puede ser representada como producto de los ψ_i definidos anteriormente.*

Demostración. Tenemos que

$$\begin{aligned}
\psi_2 \cdot \psi_1 \cdot \psi_2 &= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 1 & 3 & 4 & 5\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix}\\
\psi_3 \cdot \psi_2 \cdot \psi_3 &= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 2 & 4 & 5\end{pmatrix} = \begin{pmatrix}2 & 3\end{pmatrix}\\
\psi_4 \cdot \psi_3 \cdot \psi_4 &= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 4 & 3 & 5\end{pmatrix} = \begin{pmatrix}3 & 4\end{pmatrix}\\
\psi_4 &= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 3 & 5 & 4\end{pmatrix} = \begin{pmatrix}4 & 5\end{pmatrix}
\end{aligned}$$

son las transposiciones simples de S_5. Por el corolario 1.8 toda permutación de S_5 puede expresarse como producto de los ψ_i. □

Lema 1.10. *A_n $(n \geq 3)$ está generado por los ciclos de longitud* 3.

Demostración. Puesto que A_3 es cíclico de orden 3, se puede suponer $n > 3$. Ahora toda permutación par es producto de un número par de transposiciones. Agrupando de 2 en 2, cada pareja mueve cuatro indices o tres. Ahora bien

$$\begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}c & d\end{pmatrix} = \begin{pmatrix}a & c & b\end{pmatrix}\begin{pmatrix}a & c & b\end{pmatrix}\begin{pmatrix}a & c & d\end{pmatrix}\begin{pmatrix}a & c & d\end{pmatrix}$$

$$y \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} a & c \end{pmatrix} = \begin{pmatrix} a & c & b \end{pmatrix} \begin{pmatrix} a & c & b \end{pmatrix}$$

son productos de ciclos de longitud 3. □

Suponemos al lector familiarizado con lo que es un subgrupo normal (para más información ver [2]) para dar paso al siguiente lema.

Lema 1.11. *Si $A_n, (n \geq 5)$ posee un subgrupo normal N con un 3-ciclo, $N = A_n$.*

Demostración. Se verá que N contiene cualquier 3-ciclo.
En efecto, sean $\begin{pmatrix} a & b & c \end{pmatrix} \in N$ y $\begin{pmatrix} i & j & k \end{pmatrix}$ otro 3-ciclo. Sea $\sigma \in S_n$ tal que $\sigma(a) = i$, $\sigma(b) = j$, $\sigma(c) = k, \ldots$. Entonces, $\sigma \begin{pmatrix} a & b & c \end{pmatrix} \sigma^{-1} = \begin{pmatrix} i & j & k \end{pmatrix}$. Si σ es par, $\begin{pmatrix} i & j & k \end{pmatrix} \in N$; en caso contrario sea $\alpha = \begin{pmatrix} l & m \end{pmatrix}$, $l, m \notin \{i, j, k\}$; entonces $\alpha\sigma$ es par y $\alpha\sigma \begin{pmatrix} a & b & c \end{pmatrix} \sigma^{-1}\alpha^{-1} = \begin{pmatrix} i & j & k \end{pmatrix}$. □

Recordemos algo sobre el conmutador de dos elementos de un grupo

Definición 1.3. *Sean $\sigma\tau \in A_n$. Llamaremos conmutador de σ y τ a*

$$[\sigma, \tau] = \sigma \cdot \tau \cdot \sigma^{-1} \cdot \tau^{-1}$$

.

Observación 1.12. *Si $C = \{[\sigma, \tau]/\sigma, \tau \in A_n\}$, entonces el conjunto*

$$\langle C \rangle = [A_n, A_n]$$

generado por C es un subgrupo normal de A_n. La prueba de esta afirmación la podemos encontrar en [5].

Teorema 1.13. *A_n $(n \geq 5)$ es simple, y en consecuencia $A_n = [A_n, A_n]$.*

Demostración. Sea $\{id\} \neq N \triangleleft A_n$. Probaremos que $N = A_n$. Consideraremos dos casos:
Caso 1: Si N contiene un ciclo de longitud 3 entonces $N = A_n$ por lema 1.11.
Caso 2: Si N no contiene un ciclo de longitud 3, entonces vamos a producir un ciclo de longitud 3 para N. Como $N \neq id$ podemos escoger $\tau \in N$, $\tau \neq id$, fijando el máximo número posible de símbolos. Vamos a demostrar que τ es un ciclo de longitud 3.
Supongamos (por el absurdo) que τ no es un ciclo de longitud 3. Así; por lo menos 4 símbolos aparecerán en la representación de τ como producto de ciclos.
Por lo tanto tenemos dos posibilidades

1. $\tau = \begin{pmatrix} a & b & c & d & f & \dots \end{pmatrix} \dots$ (ya que $\begin{pmatrix} a & b & c & d \end{pmatrix} \notin A_n$) ó

2. $\tau = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c & d \end{pmatrix} \dots$

Ahora sea $\sigma = \begin{pmatrix} c & d & e \end{pmatrix} \in A_n$. Entonces tenemos,

1.
$$\begin{aligned} \tau_1 = \sigma \cdot \tau \cdot \sigma^{-1} &= \begin{pmatrix} c & d & f \end{pmatrix} \begin{pmatrix} a & b & c & d & f & \dots \end{pmatrix} \dots \begin{pmatrix} c & e & d \end{pmatrix} \\ &= \begin{pmatrix} a & b & d & f & c & \dots \end{pmatrix} \dots \in N \end{aligned}$$

2. $\tau_1 = \sigma \cdot \tau \cdot \sigma^{-1} = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} d & f \end{pmatrix} \dots \in N$

En ambos casos $\tau \neq \tau_1$. Ahora consideraremos $\gamma = \tau^{-1} \cdot \tau_1 \in N$. Tenemos que γ fija más elementos que τ lo que es una contradicción. por lo tanto τ es un ciclo de longitud tres y por el caso 1 se prueba la primera parte del teorema. Es fácil observar que $[A_n, A_n]$ es un subgrupo normal de A_n. Por lo tanto $[A_n, A_n] = A_n$. □

1.2. Funciones Holomorfas de Varias Variables Complejas

En esta sección estudiaremos algunos conceptos del análisis en varias variables complejas. Nuestro objetivo será dar forma y demostrar el teorema de la función implícita para el caso de los complejos. Para lograr el objetivo usaremos el **Teorema de la función implícita en $\mathbb{R}^n$**, el cual sólo enunciaremos. Su demostración se puede encontrar en libros del curso de análisis en varias variables reales [4]. Suponemos al lector familiarizado con algunos conceptos fundamentales del análisis en $\mathbb{R}^n$, en todo caso puede revisar los libros citados en la descripción bibliográfica.

Teorema 1.14 (**Teorema de la Función Implícita en $\mathbb{R}^n$**). *Sean $f : U \subset \mathbb{R}^m \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$ de clase C^k, para $k \geq 1$ y $(a, b) \in U$ tal que $D_2 f(a, b) : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ es isomorfismo. Entonces, existen: Un abierto $\Omega_1 \subset \mathbb{R}^m$, $a \in \Omega_1$; un abierto $\Omega_2 \subset \mathbb{R}^n$, $b \in \Omega_2$ y una función $g : \Omega_1 \longrightarrow \Omega_2$ de clase C^k tales que:*

- *$g(a) = b$.*
- *Para cada $x \in \Omega_1$: $g(x)$ es el único punto en Ω_2 tal que $f(x, g(x)) = f(a, b)$.*
- *$D_2 f(x, y)$ es isomorfismo, para todo $(x, y) \in \Omega_1 \times \Omega_2$.*

Ahora daremos algunas definiciones básicas que serán útiles para lograr el objetivo de esta sección.

Definición 1.4. Derivada Compleja en un Punto y Función Holomorfa. *Sea* $f : \Omega \subset \mathbb{C} \to \mathbb{C}$ *una función de variable compleja. Decimos que* $f(z)$ *es derivable en* z_0 *si existe el límite siguiente, llamado* **derivada de f en** z_0*:*

$$\lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0} = f'(z_0)$$

También decimos que f *es holomorfa en* Ω *si es derivable en* z_0 *para todo* $z_0 \in \Omega$*.*

Ahora, daremos una condición necesaria y suficiente para que una función compleja de variable compleja sea holomorfa en un subconjunto abierto de $\mathbb{C}$.

Teorema 1.15. Ecuaciones de Cauchy-Riemann. *Sea* $f : \Omega \subset \mathbb{C} \to \mathbb{C}$ *tal que* $f(x, y) = u(x, y) + iv(x, y)$ *para algunas funciones* $u, v : \mathbb{R}^2 \to \mathbb{R}$*. Entonces,* f *es holomorfa en* Ω *si y solo si* u *y* v *son diferenciables en todo punto de* Ω *y cumplen las ecuaciones siguientes:*

$$\frac{\partial}{\partial x}u = \frac{\partial}{\partial y}v, \quad y \quad \frac{\partial}{\partial y}u = -\frac{\partial}{\partial x}v \text{ para todo } z = x + iy \approx (x, y) \in \Omega,$$

llamadas ecuaciones de Cauchy-Riemann.

Sea $U \subset \mathbb{C}^n$ un abierto y sea $f : U \longrightarrow \mathbb{C}$ una función compleja. Decimos que f es de clase C^∞ si f es de clase C^∞ cuando se interpreta como una función de $U \subset \mathbb{R}^{2n}$ en $\mathbb{R}^2$

Observación 1.16. *El isomorfismo* $\mathbb{C} \approx \mathbb{R}^2$ *se hace vía la identificación* $x + iy \approx (x, y)$*. Lo que se quiere decir es que un elemento* $z = x + iy$ *de* $\mathbb{C}$ *se puede ver o tomar como un elemento de* $\mathbb{R}^2$*.*

Es fácil verificar que todo polinomio en las variables $z_1, ..., z_n \in \mathbb{C}$ define una función de clase C^∞ de $\mathbb{R}^{2n}$ en $\mathbb{R}^2$.

Ejemplo 4. *Sea* $P : \mathbb{C}^2 \longrightarrow \mathbb{C}$ *tal que* $P(z_1, z_2) = {z_1}^2 + {z_2}^2$*. Se tiene que* $z_1 = x_1 + iy_1$ *y* $z_2 = x_2 + iy_2$*, de donde se tiene que*

$$\begin{aligned} P(x_1, y_1, x_2, y_2) &= (x_1 + iy_1)^2 + (x_2 + iy_2)^2 \\ &= (x_1^2 - y_1^2 + x_2^2 - y_2^2) + (2x_1y_1 + 2x_2y_2)i \\ &\approx (x_1^2 - y_1^2 + x_2^2 - y_2^2,\ 2x_1y_1 + 2x_2y_2) \in \mathbb{R}^2 \end{aligned}$$

Con esto se puede expresar P *como una función de* $\mathbb{R}^4$ *en* $\mathbb{R}^2$*, definida por la ecuación anterior.*

Definición 1.5. *Sea $f : U \subset \mathbb{C}^n \longrightarrow \mathbb{C}$ de clase C^∞. Decimos que f es holomorfa respecto de la variable z_1 si, fijados $a_2, a_3, ..., a_n \in \mathbb{C}$, la función*

$$\begin{array}{rll} \tilde{f}: & \{z_1 \in \mathbb{C}; (z_1, a_2, ..., a_n) \in U\} & \longrightarrow \mathbb{C} \\ & z_1 & \longmapsto \tilde{f}(z_1) = f(z_1, a_2, ..., a_n) \end{array}$$

es holomorfa. Análogamente definimos que f es holomorfa respecto de la variable z_j para $j = 2, ..., n$.

Definición 1.6. *Sea $f : U \subset \mathbb{C}^n \longrightarrow \mathbb{C}$ de clase C^∞. Decimos que f es holomorfa si f es holomorfa respecto de la variable z_j, para todo $j = 1, ..., n$.*

Definición 1.7. Derivadas Parciales Complejas.
Sea $f : U \subset \mathbb{C}^m \rightarrow \mathbb{C}$ una función holomorfa. Definimos $\frac{\partial f}{\partial z_i} : U \rightarrow \mathbb{C}$, llamada derivada parcial de f con respecto de la variable z_i, como el siguiente límite

$$\frac{\partial}{\partial z_i} f(a_1, ..., a_n) = \lim_{h \to 0} \frac{f(a_1, ..., a_i + h, ..., a_n) - f(a_1, ..., a_n)}{h}$$

Observación 1.17. *Para calcular $\frac{\partial}{\partial z_i} f(a_1, ..., a_n)$ se puede hacer constantes las variables $z_1, ..., z_{i-1}, z_{i+1}, ..., z_n$ e iguales a $a_1, ..., a_{i-1}, a_{i+1}, ..., a_n$ y derivar la función $f(a_1, ..., a_{i-1}, z_i, a_{i+1}, ..., a_n)$ que es función de una variable compleja. Finalmente se evalúa en a_i.*

Observación 1.18. *Sea $f : U \subset \mathbb{R}^m \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ diferenciable. Entonces se tiene que $df(a, b) : \mathbb{R}^m \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ es lineal, y define la aplicación $d_2 f(a, b) : \mathbb{R}^n \rightarrow \mathbb{R}^n$ tal que $d_2 f(a, b).v = df(a, b).(0, v)$ donde $0 \in \mathbb{R}^m$. De acá se concluye que $d_2 f(a, b)$ es un isomorfismo si el conjunto de vectores $\{d_2 f(a, b).e_1, ..., d_2 f(a, b).e_n\}$ es linealmente independiente, o mejor dicho, cuando el conjunto de vectores $\left\{\frac{\partial}{\partial y_1} f(a, b), \frac{\partial}{\partial y_2} f(a, b), ..., \frac{\partial}{\partial y_n} f(a, b)\right\}$ es linealmente independiente.*

Observación 1.19. (Derivada Compleja y Derivada Real).
Sea $f : \Omega \subset \mathbb{C} \rightarrow \mathbb{C}$ holomorfa. Considere $a \in \Omega$ y suponga que $f'(a) = \alpha + i\beta \in \mathbb{C}$. Esta derivada compleja se relaciona con la derivada real de la manera siguiente. Si pensamos que f es una función real $f : U \subset \mathbb{R}^2 \rightarrow \mathbb{R}^2$, la derivada de f en $a \in U$ es una transformación

$$df(a) : \mathbb{C} \rightarrow \mathbb{C}$$

que es $\mathbb{R}$-lineal. Entonces $df(a)$ es la multiplicación por el complejo $f'(a)$, o sea:

$$df(a).(h) = f'(a).h$$

para todo $h \in \mathbb{C}$. En particular tenemos

$$\frac{\partial f}{\partial x}(a) = df(a)(e_1) \cong df(a)(1) = f'(a) \cdot 1 = f'(a) \ \ y$$

$$\frac{\partial f}{\partial y}(a) = df(a)(e_2) \cong df(a)(i) = f'(a).i\,.$$

A partir de lo anterior, para el caso de una función $f : U \subset \mathbb{C}^n \to \mathbb{C}$ holomorfa tenemos lo siguiente:

$$df(a).(h_1, ..., h_n) = \frac{\partial f}{\partial z_1}(a)h_1 + ... + \frac{\partial f}{\partial z_n}(a)h_n,\ \forall (h_1, ..., h_n) \in \mathbb{C}^n.$$

Teorema 1.20. Función Implícita en Complejos.
Sea $f : U \subset \mathbb{C}^n \times \mathbb{C} \to \mathbb{C}$ holomorfa. Denote los puntos de U por $(x, y) \in \mathbb{C}^n \times \mathbb{C}$ y suponga que $\frac{\partial f}{\partial y}(a, b) \neq 0$. Entonces, existen abiertos $V_1 \subset \mathbb{C}^n$, $V_2 \subset \mathbb{C}$, $a \in V_1$, $b \in V_2$ y existe una función $g : V_1 \to V_2$ holomorfa tales que:

- $g(a) = b$
- *Para todo $x \in V_1$: $g(x)$ es el único punto en V_2 tal que $f(x, g(x)) = f(a, b)$.*

Demostración. Tenemos $f : U \subset \mathbb{C}^n \times \mathbb{C} \to \mathbb{C}$, si pensamos $\mathbb{C}^n \approx \mathbb{R}^{2n}$, $\mathbb{C} \approx \mathbb{R}^2$, entonces $D_2f(a, b) : \mathbb{R}^2 \to \mathbb{R}^2$ es un isomorfismo si $\left\{\frac{\partial}{\partial y_1}f(a, b), \frac{\partial}{\partial y_2}f(a, b)\right\}$ es linealmente independiente (aquí $(x, y) \in \mathbb{C}^n \times \mathbb{C}$, $y = y_1 + iy_2$).
Se tiene

$$\begin{aligned}\left\{\frac{\partial}{\partial y_1}f, \frac{\partial}{\partial y_2}f\right\} &= \left\{\frac{\partial}{\partial y}f(a, b), i\frac{\partial}{\partial y}f(a, b)\right\} \\ &= \frac{\partial}{\partial y_1}f(a, b)\,\{1, i\}\end{aligned}$$

linealmente independiente ya que $\frac{\partial}{\partial y_1}f(a, b) \neq 0$.
Por la observación 1.18 y por teorema 1.14, existen $V_1 \subset \mathbb{C}^n$, $V_2 \subset \mathbb{C}$, $a \in V_1$, $b \in V_2$ y existe $g : V_1 \to V_2$ tal que

- $g \in \mathbb{C}^\infty$, $g(a) = b$
- Para todo $x \in V_1$: $g(x)$ es el único punto en V_2 tal que $f(x, g(x)) = f(a, b) = c$.
- $\frac{\partial f}{\partial y}(x, g(x)) \neq 0\ \forall x \in V_1$.

Ahora solo nos queda demostrar que g es holomorfa, en efecto:
Como $f(x, g(x)) = c$ para todo $x \in V_1$ siendo $x = (x_1, ..., x_n)$ con $x_1 = s + it$; derivando f, por la regla de la cadena se tiene que

$$df(x, g(x)) \cdot dh(x) = 0 \tag{1.1}$$

donde $h(x) = (x, g(x))$ y

$$\begin{aligned} dh(x) \cdot v &= \frac{\partial}{\partial v} h(x) \\ &= (\frac{\partial}{\partial v} x, \frac{\partial}{\partial v} g(x)) \end{aligned}$$

con lo cual

$$\begin{aligned} dh(x) \cdot e_1 &= \frac{\partial}{\partial s} h(x) \\ &= (\frac{\partial}{\partial s} x, \frac{\partial}{\partial s} g(x)) \\ &= (1, 0, ..., 0, \frac{\partial}{\partial s} g(x)). \end{aligned}$$

y reemplazando en (1.1) se tiene

$$df(x, g(x)) \cdot (1, 0, ..., 0, \frac{\partial}{\partial s} g(x)) = \frac{\partial}{\partial x_1} f(x, g(x)) \cdot 1 + \frac{\partial}{\partial y} f(x, g(x)) \cdot \frac{\partial}{\partial s} g(x) = 0$$

Por lo tanto

$$\frac{\partial}{\partial s} g(x) = -\frac{\frac{\partial}{\partial x_1} f(x, g(x))}{\frac{\partial}{\partial y} f(x, g(x))}.$$

Análogamente, de $df(x, g(x)) \cdot dh(x) \cdot e_2 = 0$ se obtiene que

$$\frac{\partial}{\partial t} g(x) = -i \frac{\frac{\partial}{\partial x_1} f(x, g(x))}{\frac{\partial}{\partial y} f(x, g(x))}.$$

Entonces,

$$\frac{\partial}{\partial t} g(x) = i \frac{\partial}{\partial s} g(x),$$

que son las ecuaciones de Cauchy Riemann, por lo tanto g es holomorfa respecto de $x_1 = s + it$.
Análogamente se puede probar para $x_2, ..., x_n$, con lo cual queda demostrado que g es holomorfa. □

1.3. Caminos Continuos y el Índice de un Camino Respecto de $0 \in \mathbb{C}$.

En esta sección consideraremos funciones continuas $\gamma : [a, b] \to A \subset \mathbb{C}$ y diremos que γ es un camino en A definido en el intervalo $[a, b]$. Diremos que el camino γ es cerrado si $\gamma(a) = \gamma(b)$ (en este trabajo consideraremos un "lazo" como un camino cerrado). Sea γ un camino en $\mathbb{C}^*$ definido en algún intervalo $[a, b]$. Entonces existen funciones continuas $\rho : [a, b] \to (0, +\infty)$ y $\theta : [a, b] \to \mathbb{R}$, tales que:

$$\gamma(t) = \rho(t)e^{\theta(t)i} \tag{1.2}$$

Observación 1.21. *ρ es único; pues, $\rho(t) = |\gamma(t)|$. Pero, θ no es único, ya que $\tilde{\theta} = \theta + 2\,k\,\pi$, para algún $k \in \mathbb{Z}$, también satisface la igualdad (1.2). Cada vez que nos referimos a un camino en A, daremos por sobrentendido que esta definido en el intervalo $[a, b]$, a menos que indiquemos lo contrario.*

Observemos que si γ es un camino cerrado en $\mathbb{C}^*$ y lo expresamos como en la igualdad (1.2) (para algunos ρ y θ), se tiene

$$\rho(a) = \rho(b) \ \text{ y } \ \theta(b) - \theta(a) = 2k\,\pi \text{ para algun } k \in \mathbb{Z}.$$

Definición 1.8. *El numero $k \in \mathbb{Z}$ es llamado índice de γ respecto de 0 y será denotado por $k = Ind(\gamma, 0)$.*

Observación 1.22. *Obviamente*

$$Ind(\gamma, 0) = \frac{\theta(b) - \theta(a)}{2\pi}.$$

Teorema 1.23. *Sea $\gamma : [a, b] \to \mathbb{C}^*$ un camino de clase C^1 por partes. Entonces,*

$$Ind(\gamma, 0) = \frac{1}{2\pi}\int_\gamma \frac{\mathrm{d}z}{z}.$$

Demostración. Tal como vimos al inicio de la sección, podemos escribir $\gamma(t) = \rho(t)e^{\theta(t)i}$, para algunas funciones continuas ρ y θ. Como γ es C^1 por partes, es fácil verificar que ρ y θ son también de clase $\mathbb{C}^1$ por partes.

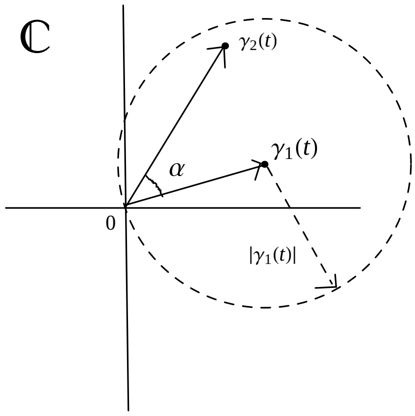

Figura 1.2: Ángulo α

Con esto tenemos

$$\begin{aligned}
\frac{1}{2\pi i}\int_\gamma \frac{\mathrm{d}z}{z} &= \frac{1}{2\pi i}\int_a^b \frac{\gamma'(t)\mathrm{d}t}{\gamma(t)}\\
&= \frac{1}{2\pi i}\int_a^b \frac{(\rho(t)e^{\theta(t)i})'\mathrm{d}t}{\rho(t)e^{\theta(t)i}}\\
&= \frac{1}{2\pi i}\left[\int_a^b \frac{\rho'(t)\mathrm{d}t}{\rho(t)} + \int_a^b i\theta'(t)\mathrm{d}t\right]\\
&= \frac{1}{2\pi i}\left[\ln(\rho(t))|_a^b + i\theta(t)|_a^b\right]\\
&= Ind(\gamma, 0)
\end{aligned}$$

□

Teorema 1.24. *Sean γ_1 y γ_2 caminos cerrados en $\mathbb{C}^*$ tales que $|\gamma_1(t) - \gamma_2(t)| < |\gamma_1(t)|$ para todo $t \in [a,b]$. Entonces, $Ind(\gamma_1, 0) = Ind(\gamma_2, 0)$.*

Demostración. Podemos escribir

$$\begin{aligned}
\gamma_1(t) &= \rho_1(t)e^{\theta_1(t)i}\\
\gamma_2(t) &= \rho_2(t)e^{\theta_2(t)i}
\end{aligned}$$

para ciertas funciones reales ρ_1, ρ_2, θ_1 y θ_2, C^1 por partes. Fijemos $t \in [a,b]$ por hipótesis tenemos que

$$\gamma_2(t) \in B_{|\gamma_1(t)|}(\gamma_1(t)).$$

De la figura 1.2, observemos que el angulo α(en valor absoluto) formado por los vectores $\gamma_1(t)$ y $\gamma_2(t)$ es menor que $\frac{\pi}{2}$.

Afirmación: Dado $\theta \in \mathbb{R}$, existe un único $k \in \mathbb{Z}$ y un único $\alpha \in (-\pi, \pi]$ tal que $\theta = 2k\pi + \alpha$.

Con esta afirmación podemos escribir

$$\theta_1(t) - \theta_2(t) = 2k_t\pi + \alpha(t)$$

con $k_t \in \mathbb{Z}$ y $\alpha(t) \in \mathbb{R}$ tal que $-\pi < \alpha(t) \leq \pi$. Por la observación anterior obtenida de la figura 1.2, deducimos que $|\alpha(t)| < \frac{\pi}{2}$ para todo $t \in [a, b]$.

Afirmación: α es continua. En efecto: Como $|\alpha(t)| < \frac{\pi}{2}$, según cual sea el valor de K_t, tenemos las siguientes posibilidades:

$$\begin{array}{lll}
\vdots & \vdots & \vdots \\
\text{Si} & k_t = 0 & \rightarrow \theta_1(t) - \theta_2(t) \in (-\dfrac{\pi}{2}, \dfrac{\pi}{2}) \\
\text{Si} & k_t = 1 & \rightarrow \theta_1(t) - \theta_2(t) \in (2\pi - \dfrac{\pi}{2}, 2\pi + \dfrac{\pi}{2}) \\
\vdots & \vdots & \vdots
\end{array}$$

O sea, se tiene que $\theta_1(t) - \theta_2(t)$ pertenece a

$$... \cup (-\frac{\pi}{2}, \frac{\pi}{2}) \cup (2\pi - \frac{\pi}{2}, 2\pi + \frac{\pi}{2}) \cup ...,$$

siendo todos los intervalos abiertos disjuntos dos a dos.

Ahora; como $(\theta_1 - \theta_2)([a, b])$ es conexo, entonces $\theta_1(t) - \theta_2(t) \in (2k\pi - \frac{\pi}{2}, 2k\pi + \frac{\pi}{2})$ para un único $k \in \mathbb{Z}$ y para todo $t \in [a, b]$. De aquí se obtiene $\alpha(t) = \theta_1(t) - \theta_2(t) - 2k\pi$ función continua.

Volviendo a la prueba del teorema, tenemos que

$$\begin{aligned}
|Ind(\gamma_1, 0) - Ind(\gamma_2, 0)| &= \left| \frac{\theta_1(b) - \theta_1(a)}{2\pi} - \frac{\theta_2(b) - \theta_2(a)}{2\pi} \right| \\
&= \left| \frac{(\theta_1(b) - \theta_2(b)) - (\theta_1(a) - \theta_2(a))}{2\pi} \right| \\
&= \left| \frac{(2k\pi + \alpha(b)) - (2k\pi + \alpha(a))}{2\pi} \right| \\
&= \left| \frac{\alpha(b) - \alpha(a)}{2\pi} \right| < \frac{1}{2}
\end{aligned}$$

Como los índices son números enteros, entonces deducimos que

$$Ind(\gamma_1, 0) = Ind(\gamma_2, 0).$$

□

La demostración del siguiente teorema la pueden encontrar en [6].

Teorema 1.25. *Sea V un conjunto abierto de $\mathbb{C}$ cuya frontera ∂V es una curva de Jordan C^1 por partes. Sea $f : U \to \mathbb{C}$ función holomorfa tal que $\bar{V} \subset U$. Sean $a_1, ..., a_n \in V$ los ceros de f en V y suponga que f no tiene ceros en ∂V. Sean $m_1, ..., m_n$ las multiplicidades de los ceros $a_1, ..., a_n$ respectivamente. Entonces,*

$$m_1 + m_2 + ... + m_n = \frac{1}{2\pi i} \int_{\partial V} \frac{f'(z)\mathrm{d}z}{f(z)}.$$

Observación 1.26. *Si ∂V es parametrizada por $\gamma(t)$, $t \in [a, b]$, entonces*

$$\begin{aligned}
\frac{1}{2\pi i} \int_{\partial V} \frac{f'(z)\mathrm{d}z}{f(z)} &= \frac{1}{2\pi i} \int_a^b \frac{f'(\gamma(t))\gamma'(t)\mathrm{d}t}{f(\gamma(t))} \\
&= \frac{1}{2\pi i} \int_a^b \frac{(f \circ \gamma)'(t)\mathrm{d}t}{(f \circ \gamma)(t)} \\
&= \frac{1}{2\pi i} \int_{f \circ \gamma} \frac{\mathrm{d}z}{z} \\
&= Ind(f \circ \gamma, 0)
\end{aligned}$$

O sea; el numero de ceros (contado con sus multiplicidades) es igual al índice de $f \circ \gamma$ respecto de $0 \in \mathbb{C}$.

Teorema 1.27. Teorema de Rouché. *Sea V un abierto en $\mathbb{C}$ tal que ∂V es una curva de Jordan C^1 por partes. Sean f y g dos funciones holomorfas en un dominio que incluye a $\bar{V}$. Si $|g(\zeta) - f(\zeta)| < |f(\zeta)|$ para todo $\zeta \in \partial V$, entonces f y g tienen el mismo número de ceros contados tantas veces como indica sus multiplicidades en la región interior a la curva ∂V.*

Demostración. Por el teorema 1.25, tenemos

$$\begin{aligned}
\#\text{ceros}(f|_V) &= Ind(f \circ \partial V, 0) \\
\#\text{ceros}(g|_V) &= Ind(g \circ \partial V, 0).
\end{aligned}$$

Sea $\theta(t)$, $t \in [0, 1]$, una parametrización de ∂V. Entonces,

$$\gamma_1 = f \circ \theta \text{ y } \gamma_2 = g \circ \theta$$

son las parametrizaciones de $f(\partial V)$ y $g(\partial V)$ respectivamente.
Como $|f(\zeta) - g(\zeta)| < |f(\zeta)|$ para todo $\zeta \in \partial V$, entonces

$$|f(\theta(t)) - g(\theta(t))| < |f(\theta(t))|$$

para todo $t \in [0,1]$. Luego,

$$|\gamma_1(t) - \gamma_2(t)| < |\gamma_1(t)| \text{ para todo } t \in [0,1].$$

Y por el teorema 1.24 tendremos

$$\begin{aligned} & Ind(\gamma_1, 0) && = Ind(\gamma_2, 0) \\ \rightarrow \quad & Ind(f(\partial V), 0) && = Ind(g(\partial V), 0) \\ \rightarrow \quad & \#\text{ceros}(f|_V) && = \#\text{ceros}(g|_V) \end{aligned}$$

$\square$

Capítulo 2

Fórmulas Radicales.

2.1. Resolución de Algunas Ecuaciones Generales.

En esta parte recordaremos las fórmulas para la obtención de las soluciones de ecuaciones algebraicas generales de grado 2, 3 y 4.

Ecuación general de grado 2:

Conocida también como ecuación cuadrática, esta ecuación es de la forma $ax^2 + bx + c = 0$. Una forma de encontrar una fórmula general para calcular las soluciones es mediante el método de completar cuadrados, lo que conlleva a despejar x de la siguiente manera:

$$\begin{aligned}
ax^2 + bx + c &= 0 \\
x^2 + \frac{b}{a}x + \frac{c}{a} &= 0 \\
x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} + \frac{c}{a} &= \frac{b^2}{4a^2} \\
\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\
x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.
\end{aligned}$$

Este resultado es la fórmula general de una ecuación cuadrática.

Ecuación general de grado 3:

Conocido también como ecuación cúbica, esta ecuación es de la forma $x^3+ax^2+bx+c=0$. El primer paso para resolver esta ecuación cúbica es haciendo la siguiente sustitución que permite simplificarla o reducirla: $x = y - \frac{a}{3}$ reemplazando en la ecuación cúbica tenemos:

$$0 = \left(y - \frac{a}{3}\right)^3 + a\left(y - \frac{a}{3}\right)^2 + b\left(y - \frac{a}{3}\right) + c$$
$$0 = y^3 + \left(b - \frac{a^2}{3}\right)y + \left(\frac{2a^2}{27} - \frac{ab}{3} + c\right). \tag{2.1}$$

Si definimos $p = b - \frac{a^2}{3}$ y $q = (\frac{2a^2}{27} - \frac{ab}{3} + c)$, entonces podemos escribir la ecuación 2.1 de la forma:

$$y^3 + py = q.$$

Ahora consideraremos la siguiente identidad (algebraica) conocida

$$(r-s)^3 + 3rs(r-s) = r^3 - s^3.$$

Si se eligen r y s de modo que $3rs = p$ y $r^3 - s^3 = q$, entonces la identidad algebraica se puede reescribir como

$$(r-s)^3 + p(r-s) = q.$$

De este modo, $x = r - s$ sera una solución de la ecuación cúbica reducida. El problema de resolver la ecuación cúbica reducida se transforma en el problema de resolver el sistema de ecuaciones simultáneas:

$$r^3 - s^3 = q \tag{2.2}$$

$$rs = \frac{p}{3}. \tag{2.3}$$

Para lograrlo, se eleva al cuadrado la ecuación (2.2) y la ecuación (2.3) se eleva al cubo y se multiplica por 4. Luego se suman ambas para obtener

$$(r^3+s^3)^2 = r^6 + 2r^3s^3 + s^6 = q^2 + \frac{4p^3}{27}$$

o bien

$$r^3 + s^3 = \sqrt{q^2 + \frac{4p^3}{27}}.$$

Ahora, si resolvemos las ecuaciones

$$r^3 - s^3 = q \ \text{ y } r^3 + s^3 = \sqrt{q^2 + \frac{4p^3}{27}}$$

en forma simultánea, se pueden obtener los valores de r^3 y s^3, y por lo tanto de r y s:

$$r = \sqrt[3]{\frac{1}{2}(q + \sqrt{q^2 + \frac{4p^3}{27}})} = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$
$$s = \sqrt[3]{\frac{1}{2}(-q + \sqrt{q^2 + \frac{4p^3}{27}})} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Por consiguiente, como $x = r - s$

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Esta es la fórmula conocida como "Fórmula de Cardano".

Ecuación general de grado 4: La solución de esta ecuación se resolverá en el siguiente teorema.[13]

Teorema 2.1. (Ferrari) *Las raíces de la ecuación*

$$x^4 + a\,x^3 + b\,x^2 + c\,x + d = 0. \tag{2.4}$$

vienen dadas por

$$x = \frac{Q \pm \sqrt{Q^2 - 4(P - R)}}{2} - \frac{a}{4}, \quad x = \frac{-Q \pm \sqrt{Q^2 - 4(P + R)}}{2} - \frac{a}{4},$$

donde, llamando

$$p = \frac{8b - 3a^2}{8}, \; q = \frac{8c - 4ab + a^3}{8}, \; r = \frac{256d - 64ac + 16a^2b - 3a^4}{256}, \tag{2.5}$$

P es una raíz de la ecuación

$$P^3 - \frac{p}{2}P^2 - rP + \frac{4pr - q^2}{8} = 0, \tag{2.6}$$

y Q, R se determinan mediante las ecuaciones

$$p = 2P - Q^2, \; q = -2QR, \; r = P^2 - R^2. \tag{2.7}$$

En la prueba veremos, de forma más concreta , que, si $q \neq 0$, la primera ecuación de (2.7) es redundante, de modo que, a partir de una solución P de (2.6), la tercera ecuación de (2.7) nos da un valor para R, necesariamente no nulo, y la segunda ecuación nos da un valor para Q que necesariamente cumplirá la primera ecuación.

Si $q = 0$ el sistema (2.7) tiene también una solución fácil de calcular, pero enseguida veremos que en este caso hay un procedimiento más rápido para encontrar las raíces de la ecuación. En efecto, el cambio de variable

$$x = t - \frac{a}{4}$$

nos lleva a la ecuación incompleta

$$t^4 + pt^2 + qt + r = 0, \tag{2.8}$$

donde p, q, r son dados por (2.5). Así, si $q = 0$, tenemos lo que se conoce como una ecuación bicuadrada, cuyas raíces cumplen:

$$t^2 = \frac{-p \pm \sqrt{p^2 - r}}{2};$$

luego las 4 raíces de (2.4) son

$$x = \pm\sqrt{-p \pm \sqrt{p^2 - r}} - \frac{a}{4}.$$

Demostración. Ya hemos visto que basta resolver la ecuación incompleta (2.8). Para ello observamos que

$$(t^2 + P)^2 - (Qt + R)^2 = t^4 + (2P - q^2)t^2 - 2QRt + P^2 - R^2$$

Por lo tanto, si encontramos valores P, Q, R que cumplan (2.5), las soluciones de (2.8) serán las mismas que las de la ecuación

$$(t^2 + P)^2 = (Qt + R)^2.$$

Ésta puede descomponerse en dos ecuaciones cuadráticas:

$$t^2 + P = \pm(Qt + R).$$

Equivalentemente,

$$t^2 - Qt + P - R = 0, \;\; t^2 + Qt + P + R = 0,$$

y las raíces de estas ecuaciones son las indicadas en el enunciado.
Así pues, sólo hemos de encontrar una solución de (2.5). Para ello despejamos

$$Q = -\frac{q}{2R}, \;\; Q^2 = \frac{q^2}{4R^2} = \frac{q^2}{4(P^2 - r)},$$

con lo que la primera ecuación se convierte en

$$p = 2P - \frac{q^2}{4(P^2 - r)}$$

o, equivalentemente, en la cúbica

$$4(P^2 - r)(2P - p) = q^2 \tag{2.9}$$

que se simplifica hasta (2.6).
De este modo, podemos tomar una raíz cualquiera P de (2.6), luego una raíz cualquiera R de $r = P^2 - R^2$ y, por último, si $R \neq 0$, hacemos $Q = -\frac{q}{2R}$. Así, las dos últimas ecuaciones de (2.5) se cumplen por las elecciones de Q y R, mientras que la primera se cumplen porque es equivalente a (2.6).
Si nos encontramos con $R = 0$ es porque $P^2 - r = 0$ y, a la vista de (2.9), para que esto pueda suceder ha de ser $q = 0$. Más aún, en tal caso, esta misma ecuación muestra que las raíces de (2.6) son $P = \sqrt{r}$ o bien $P = p/2$ y, tomando $R = 0$ en el primer caso o $Q = 0$ en el segundo, encontramos igualmente una solución de (2.5).
En cualquier caso veremos que cualquier raíz P de (2.6) se puede completar (fácilmente) hasta una solución (P, Q, R) del sistema (2.5). $\square$

2.2. Ecuaciones Resolubles por Radicales.

Sea $n \in \mathbb{N}$, entendemos por ecuación algebraica general de grado n a una ecuación de la siguiente forma

$$x^n + a_{n-1}\, x^{n-1} + \ldots + a_1\, x + a_0 = 0.$$

En este capítulo daremos una definición precisa de lo que significa que una ecuación sea "resoluble por radicales". Empezaremos con ecuaciones conocidas para darnos una idea de lo que se quiere hacer. Empezaremos con la ecuación cuadrática

$$x^2 + bx + c = 0. \tag{2.10}$$

Vimos en la sección anterior que las soluciones de la ecuación cuadrática (2.10) son halladas por la fórmula $x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$; pero, también se puede encontrar las raíces por medio de una sucesión de fórmulas que contienen las operaciones de suma, resta, multiplicación, división y potenciación; donde evitamos colocar el símbolo "$\sqrt{}$", de la siguiente manera:

$$\begin{aligned} x_1^2 &= b^2 - 4c \\ x_2 &= -\frac{b}{2} + \frac{x_1}{2} \end{aligned}$$

En este sistema de ecuaciones b y c son conocidos. Con estos valores se puede encontrar números complejos x_1 usando fórmula de la raíz cuadrada de números complejos. Ahora teniendo x_1(2 valores) conocidos, se tiene dos valores para x_2. Estos últimos valores son las soluciones de la ecuación (2.10).

Ahora podemos hacer lo mismo con la ecuación general de grado 3 (ecuación cúbica)

$$x^3 + ax^2 + bx + c = 0. \tag{2.11}$$

Como vimos en la sección anterior la solución esta dada por la fórmula

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} - \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

De la misma forma que la ecuación anterior se puede obtener las raíces por medio una sucesión de ecuaciones, de la siguiente manera:

$$\begin{aligned} x_1^2 &= \frac{p^3}{27} + \frac{q^2}{4} \\ x_2^3 &= \frac{q}{2} + x_1 \\ x_3^3 &= -\frac{q}{2} + x_1 \\ x_4 &= x_2 - x_3. \end{aligned}$$

Los valores de p y q están en términos de a, b y c tal como vimos en el capítulo anterior. Con p y q conocidos tenemos como máximo 2 valores para x_1. Ahora conocido el valor de x_1 tenemos como máximo 3 valores para x_2 y x_3. Por ultimo 36 valores como máximo para x_4. De estos últimos valores solo 3 de ellos podrían ser las soluciones de la ecuación (2.11).
Formar tales sistemas de ecuaciones será la idea que usaremos para definir cuando una ecuación general de grado n es resoluble por radicales. Con esto podemos definir lo siguiente

Definición 2.1. *Sea $n \in \mathbb{N}$. Decimos que la ecuación general de grado n es resoluble por radicales si existen polinomios $p_1, \ldots, p_N$ de coeficientes complejos (en n, $n+1, \ldots,$ $n+N-1$ variables respectivamente) y enteros positivos $k_1, \ldots,$ k_N, tales que: para cualquier polinomio fijado*

$$P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \tag{2.12}$$

con $a_1, ..., a_{n-1} \in \mathbb{C}$ y para cada raíz r de P , existen $x_1, ..., x_N \in \mathbb{C}$ tales que satisfacen el siguiente sistema de ecuaciones

$$\begin{aligned}
x_1^{k_1} &= p_1(a_0, a_1, \ldots, a_{n-1}) \\
x_2^{k_2} &= p_2(a_0, a_1, \ldots, a_{n-1}, x_1) \\
\vdots \quad & \quad \vdots \\
x_N^{k_N} &= p_N(a_0, a_1, \ldots, a_{n-1}, x_1, \ldots, x_{N-1}),
\end{aligned}$$

siendo $x_N = r$. Llamaremos a los valores x_1, x_2, ..., x_N radicales intermedios.

Ejemplo 5. *Como vimos al inicio de la sección, los polinomios generales de grado 2 y 3 son resolubles por radicales. También lo son los de grado 1 y 4.*

Observación 2.2. *Podemos formar "clases" de ecuaciones algebraicas considerando que las constantes a_0, a_1, ..., a_{n-1} por lo menos uno sea variable.*

Definición 2.2. *Sea $\iota : \mathbb{C}^n \to \mathbb{C}^n$ definida por*

$$\iota(z) = (\iota_1(z),\ \iota_2(z),\ ...,\ ,\ \iota_n(z))$$

de tal forma que o $\iota_i(z) =$ constante o $\iota_i(z) = z_i$, donde $z = (z_1, ..., z_n) \in \mathbb{C}^n$. Definimos

$$P^\iota = \{P(\iota(z)) := x^n + \iota_n(z)x^{n-1} + \ldots + \iota_2(z)x + \iota_1(z) = 0 / z \in \mathbb{C}^n\}$$

*y decimos que P^ι es una **clase** de ecuaciones algebraicas y $P(\iota(z))$ es una clase de polinomios.*

Ejemplo 6. *Sea $\iota : \mathbb{C}^5 \to \mathbb{C}^5$ definida por*

$$\iota(a, z_2, z_3, z_4, z_5) = (a,\ 1,\ 0,\ 0\,1).$$

Entonces P^ι es una clase ecuaciones algebraicas cuya clase de polinomios son de la forma

$$P(a,\ 1,\ 0,\ 0\ 0) = x^5 + x + a$$

donde $a \in \mathbb{C}$.

Observación 2.3. *Sea* $\iota : \mathbb{C}^6 \to \mathbb{C}^6$ *definida por*

$$\iota(c, z_2, z_3, b, z_5, z_6) = (c,\ 0,\ 0,\ b,\ 0,\ 0)$$

Tenemos que las raíces de la clase de polinomios $P(\iota(z)) = x^6 + bx^3 + c = 0$ *con* $z = (c, z_2, z_3, b, z_5, z_6) \in \mathbb{C}^6$ *se pueden obtener por el siguiente sistema de ecuaciones*

$$\begin{aligned} x_1^2 &= b^2 - 4c \\ x_2^3 &= -\frac{b}{2} + \frac{x_1}{2} \end{aligned}$$

siendo x_2 *(no todas en algunos casos, tal como se observa en el problema de la ecuación cúbica) las raices para* $x^6 + bx^3 + c = 0$.

Definición 2.3. *Sea* ι *como en la definición 2.2. Sea* P^ι *una clase de ecuaciones algebraicas. Decimos que* P^ι *es resoluble por radicales si existen polinomios* $p_1, \ldots, p_N$ *de coeficientes complejos (en* n, $n+1, \ldots, n+N-1$ *variables respectivamente) y enteros positivos* $k_1, \ldots, k_N$, *tales que: para cualquier* $z \in \mathbb{C}^n$ *fijado y para cada raíz* r *de* $P(\iota(z))$, *existen* $x_1, ..., x_N \in \mathbb{C}$ *tales que satisfacen el siguiente sistema de ecuaciones*

$$\begin{aligned} x_1^{k_1} &= p_1(\iota_1(z), \iota_2(z), \ldots, \iota_n(z)) \\ x_2^{k_2} &= p_2(\iota_1(z), \iota_2(z), \ldots, \iota_n(z),\ x_1) \\ \vdots\ \ & \quad \vdots \\ x_N^{k_N} &= p_N(\iota_1(z), \iota_2(z), \ldots, \iota_n(z),\ x_1, \ldots,\ x_{N-1}), \end{aligned}$$

siendo $x_N = r$.

Observación 2.4. *La definición 2.3 será igual a la definición 2.1 en caso de que las funciones componentes de* ι *no sean todas constantes. O sea, si* $\iota(z_1, z_2, ..., z_n) = (z_1, z_2, ..., z_n)$, *entonces tenemos que* $P(\iota(z)) = 0$ *representa a la ecuación algebraica general de grado* n, *donde* $z = (z_1, z_2, ..., z_n) \in \mathbb{C}$.

Proposición 2.5. *Sea* $n \in \mathbb{N}$. *Si la ecuación algebraica general de grado* n *es resoluble por radicales, entonces* P^ι *es resoluble por radicales para cualquier* $\iota : \mathbb{C}^n \to \mathbb{C}^n$ *como en la definición 2.2.*

Demostración. Directamente de la definición 2.1. □

Nuestro objetivo principal es demostrar que la ecuación algebraica general de grado 5 no es resoluble por radicales. Para conseguir nuestro objetivo principal, bastará encontrar una clase de ecuaciones algebraicas P^{ι} que no sea resoluble por radicales para luego aplicar la proposición 2.5.

Teorema 2.6 (**Teorema principal**). *La clase de ecuaciones $x^5 - x + a = 0$ no es resoluble por radicales, donde $a \in \mathbb{C}$.*

La prueba de este teorema se dará en el capítulo 4. Necesitaremos mas herramientas para tal objetivo, lo cual estudiaremos en los siguientes capítulos.

Corolario 2.7. *La ecuación algebraica general de grado $n > 5$ no es resoluble por radicales.*

Demostración. Sea $n \in \mathbb{N}$ arbitrario mayor que 5. Podemos expresar $n = n_0 + 5$ para algún $n_0 \in \mathbb{N}$. Supongamos que la ecuación algebraica general de grado n es resoluble por radicales. Por proposición 2.5, la clase de ecuaciones P^{ι} , con $\iota : \mathbb{C}^{n_0+5} \to \mathbb{C}^{n_0+5}$ definida por

$$\iota(z_1, z_2, z_3, ..., a, z_{n_0+2}, z_{n_0+3}, z_{n_0+4}, z_{n_0+5}) = (0, 0, 0, ..., a, -1, 0, 0, 0),$$

debe ser resoluble por radicales. Observemos que

$$P(\iota(z)) = x^{n_0+5} - x^{n_0+1} + ax^{n_0} = x^{n_0}(x^5 - x + a),$$

con lo que las raíces de esta clase de polinomios se encontraría por medio de un sistemas de ecuaciones según la definición 2.1, el cual debe incluir las raíces del polinomio $x^5 - x + a$ contradiciendo al teorema 2.6. □

Capítulo 3

Deformaciones de un Polinomio

Sean $n \in \mathbb{N}$ y $P(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ un polinomio en $\mathbb{C}[x]$. ¿Que ocurre con las raíces de P cuando varían los coeficientes $a_0, ..., a_{n-1}$ de forma continua? ¿Varían las raíces de manera continua con respecto a la variación de los coeficientes?. En esta sección daremos respuesta a estas preguntas para la "mayoría" de los polinomios.

3.1. Variación Continua de las Raíces de un Polinomio

Sea $\iota : \mathbb{C}^n \to \mathbb{C}^n$ definida por $\iota(z_1, z_2, ..., z_n) = (z_1, z_2, ..., z_n)$. Recordemos por observación 2.4, P^ι representa a una ecuación algebraica de grado n. Sea $\mathcal{P}_n$ el conjunto de los polinomios $P(\iota(z))$. Este conjunto se puede identificar con el espacio $\mathbb{C}^n$ de la siguiente manera: a cada
$z = (z_1, z_2, ..., z_n) = \in \mathbb{C}^n$ se le puede asociar el polinomio

$$P(z) = z_1 + z_2\,x + ... + z_nx^{n-1} + x^n \ \text{ en } \mathcal{P}_n.$$

Es claro que la función

$$\begin{aligned} \mathbb{C}^n &\to \mathcal{P}_n \\ a &\to P(a) \end{aligned}$$

es una biyección.
Daremos una definición muy conocida acerca de las raíces de polinomios

Definición 3.1. *Sea $P \in \mathcal{P}_n$ y r raíz de P. Se dice que:*

1. *r es raíz simple de P si y sólo si $(x-r)^2 \nmid P$, o sea $P=(x-r)Q$ con $Q(r)\neq 0$. A nivel de factorización de P, esto significa que el factor irreductible $x-r$ aparece en la factorización de P con potencia exactamente 1.*

2. *r es raíz múltiple de P si y sólo si $(x-r)^2 \mid P$, o sea $P=(x-r)^2Q$ A nivel de factorización de P, esto significa que el factor irreductible $x-r$ aparece en al factorización de P con potencia estrictamente mayor que 1.*

3. *r es raíz de multiplicidad exactamente k de P si y sólo si $(x-r)^k \mid P$ pero $(x-r)^{k+1} \nmid P$. A nivel de factorización de P, esto significa que el factor irreductible $x-r$ aparece en la factorización de P con potencia exactamente k.*

Ejemplo 7. -2 *es raíz de multiplicidad exactamente* 3 *de*

$$P(x)=(x+2)^3(x^2+1).$$

Ahora, definimos $\mathcal{G}_n$, el conjunto de los polinomios en $\mathcal{P}_n$ que tienen todas sus raíces simples. A los elementos de $\mathcal{G}_n$ le llamaremos **polinomios genéricos de grado** n.

Proposición 3.1. *Sea $P\in\mathcal{P}_n$. Entonces,*

1. *r es raíz múltiple de P si y sólo si r es simultáneamente raíz de P y P'. Equivalentemente, r es raíz simple de P si y sólo si $P(r)=0$ y $P'(r)\neq 0$.*

2. *r es raíz de multiplicidad exactamente k de P ($k\geq 1$) si y sólo si r es raíz de P y además es raíz de multiplicidad exactamente $k-1$ de P'.*

Demostración. En esta prueba denotaremos $P(x), Q(x)$ y $H(x)$ simplemente como P, Q Y H.

1. ($\Rightarrow$) $P=(x-r)^2Q$, luego $P'=2(x-r)Q+(x-r)Q'=(x-r)(2Q+(x-r)Q')$ y se verifica $P(r)=P'(r)=0$.
   ($\Leftarrow$) Como r es raíz de P, se puede escribir $P=(x-r)Q$, y se quiere mostrar entonces que $Q(r)=0$, o sea $x-r\mid Q$, para así probar que $(x-r)^2\mid P$: Se tiene $P'=Q+(x-r)Q'$ y la condición $P'(r)=0$ implica inmediatamente que $Q(r)=0$.

2. $(\Rightarrow)$ $P = (x-r)^k Q$ con $Q(r) \neq 0$, luego $P' = k(x-r)^{k-1}Q + (x-r)^k Q' = (x-r)^{k-1}(kQ + (x-r)Q')$ y, tomando $H := kQ + (x-r)Q'$, se verifica que $P' = (x-r)^{k-1}H$ con $H(r) \neq 0$ (pues $Q(r) \neq 0$, $k \neq 0$).

   $(\Leftarrow)$ Como r es raíz de P, tiene una cierta multiplicidad $k_1 \geq 1$ como raíz. Se pretende probar que $k_1 = k$:

   Sea $P = (x-r)^{k_1}Q$ con $Q(r) \neq 0$. Luego $P' = (x-r)^{k_1-1}(k_1Q + (x-r)Q')$. Si definimos $H := k_1Q + (x-r)Q'$, resulta que $P' = (x-r)^{k_1-1}H$ con $H(r) \neq 0$, por consiguiente r es raíz de multiplicidad exactamente $k_1 - 1$ de P', pero por hipótesis esa multiplicidad es $k-1$, por lo tanto $k_1 - 1 = k - 1$, es decir $k_1 = k$.

$\square$

Definición 3.2. *Sea $n \in \mathbb{N}$. Definimos $\mathcal{S}_n = \{a \in \mathbb{C}^n \;/\; P(a) \in \mathcal{G}_n\}$.*

$\mathcal{S}_n$ puede presentarse también de la manera siguiente.

Proposición 3.2. *Sea $n \in \mathbb{N}$. Entonces,*

$$\mathcal{S}_n = \{a \in \mathbb{C}^n / (P(a))'(r) \neq 0 \text{ para toda raiz } r \text{ de } P(a)\}.$$

Demostración. La prueba es consecuencia directa del punto 1 de la proposición 3.1 aplicado a $P(a) \in \mathcal{G}_n$. $\square$

Proposición 3.3. *Sean $\mathcal{S}_n$ abierto en $\mathbb{C}^n$ y $\bar{a} \in \mathcal{S}_n$. Sean $r_1, ..., r_n \in \mathbb{C}$ raíces de $P(\bar{a}) \in \mathcal{G}_n$. Entonces, existen:*

1. *una bola $B \subset \mathbb{C}^n$ centrada en $\bar{a}$,*
2. *discos $D_1, ..., D_n \subset \mathbb{C}$ centrados en $r_1, ..., r_n$ respectivamente y disjuntos dos a dos,*
3. *funciones holomorfas $f_i : B \to D_i$ con $i = 1, ..., n$,*

de manera que para todo $a \in B$, el punto $f_i(a)$ es la **única** *raíz de $P(a)$ en D_i $(i = 1, ..., n)$.*

Demostración. Definamos $F : \mathbb{C}^n \times \mathbb{C} \to \mathbb{C}$ tal que $F(a, x) = P(a)(x)$. Tenemos que F es holomorfa, $F(\bar{a}, r_i) = 0$ para $i = 1, ..., n$ y además

$$\frac{\partial F}{\partial x}(\bar{a}, r) = (P(\bar{a}))'(r_i) \neq 0 (i = 1, ..., n)$$

por la proposición 3.2. Aplicando el teorema de la función implícita 1.14, se tiene que existen:

1. una bola $B \subset \mathbb{C}^n$ centrada en $\bar{a}$,
2. discos $D_1, ..., D_n \subset \mathbb{C}$ centrados en $r_1, ..., r_n$ respectivamente,
3. funciones holomorfas $f_i : B \to D_i$ para $i = 1, ..., n$,

de manera que para todo $a \in B$, el punto $f_i(a)$ es la única raíz de $P(a)$ en $D_i (i = 1, ..., n)$. Como los discos D_i están centrados en puntos diferentes dos a dos y las funciones f_i son continuas, podemos, reduciendo B si es necesario, suponer que los discos D_i son dos a dos disjuntos. □

Si $B \subset \mathbb{C}^n$ es como en la proposición anterior 3.3, tenemos que, dado $a \in B$, los puntos $f_1(a), ..., f_n(a)$ son las n raíces del polinomio $P(a)$. Como estas raíces pertenecen a los discos disjuntos $D_1, ..., D_n$, concluimos que $P(a)$ tiene n raíces diferentes y por lo tanto $P(a)$ tiene todas sus raíces simples. Esto muestra que $a \in \mathcal{S}_n$ y entonces tenemos el siguiente corolario.

Corolario 3.4. *$\mathcal{S}_n$ es abierto.*

Veremos ahora como es la "variación" de la raíces cuando el parámetro a describe un camino en $\mathcal{S}_n$.

Teorema 3.5. (Dependencia Continua) *Sean $\gamma : [0, 1] \to \mathcal{S}_n$ un camino continuo y $x_1, ..., x_n$ las raíces de $P(\gamma(0))$. Entonces, existen caminos continuos $\alpha_1, ..., \alpha_n : [0, 1] \to \mathbb{C}$ con $\alpha_1(0) = x_1$, ..., $\alpha_n(0) = x_n$ y tales que los puntos $\alpha_1(t), ..., \alpha_n(t)$ son las raíces diferentes de $P(\gamma(t))$ para todo $t \in [0, 1]$. Además, estos caminos son únicos salvo permutación.*

Demostración. Sea $a = \gamma(0)$. Por el corolario 3.3 existen:

1. una bola $B \subset \mathcal{S}^n$ centrada en a,
2. discos $D_1, ..., D_n \subset \mathbb{C}$ centrados en $x_1, ..., x_n$ respectivamente,
3. funciones holomorfas $f_i : B \to D_i$ tales que $f_i(a) = x_i$ $(i = 1, ..., n)$,

de manera que para todo $\gamma(t) \in B$, el punto $f_i(\gamma(t))$ es la **única** raíz de $P(\gamma(t))$ en D_i $(i = 1, ..., n)$.
Por la continuidad de γ, para la bola B existe $\epsilon_0 > 0$ tal que $\gamma(t) \in B$ para todo $t \in [0, \epsilon_0]$. Con esto definimos $\alpha_i(t) = f_i(\gamma(t))$ para todo $t \in [0, \epsilon_0]$. Es claro que $\alpha_1(t), ..., \alpha_n(t)$ son las raíces de $P(\gamma(t))$ para todo $t \in [0, \epsilon_0]$. Ahora sea $\mathbf{E}$ el

conjunto de todos los $\epsilon \in [\epsilon_0, 1]$ tal que α_i se extiende continuamente a $[0, \epsilon]$ y $P(\gamma(t))(\alpha_i(t)) = 0$ para todo $t \in [0, \epsilon]$. Obviamente $\mathbf{E} \neq \emptyset$ ($\epsilon_0 \in \mathbf{E}$) y es acotado superiormente por 1. Sea $\tau = \sup \mathbf{E}$. Afirmamos que $\tau = 1$. Supongamos que $\tau < 1$ y tomemos $s < \tau$. Por la definición de supremo existe $\epsilon \in \mathbf{E}$ tal que $s < \epsilon < \tau$. Por la definición de $\mathbf{E}$ se tiene que $\alpha_1, \ldots, \alpha_n$ se extienden continuamente a $[0, \epsilon]$ de manera que $\alpha_1(t), \ldots, \alpha_n(t)$ son las raíces de $P(\gamma(t))$ para todo $t \in [0, \epsilon]$. De esto, como ϵ es arbitrariamente próximo a τ, se puede deducir que $\alpha_1, \ldots, \alpha_n$ se extienden continuamente a $[0, \tau)$. Sea $a' = \gamma(\tau)$ y sean $r_1, ..., r_n$ las raíces de $P(a)$. Por la proposición 3.3 existen:

1. una bola B' centrado en a',
2. discos D'_i centrados en r_i respectivamente ($i = 1, ..., n$) disjuntos dos a dos,
3. funciones $g_1, \ldots, g_n : B' \to D'_i$ holomorfas tal que $g_i(a') = r_i$,

de manera que para todo $\gamma(t) \in B'$ el punto $g_i(\gamma(t))$ es la única raíz de $P(\gamma(t))$ en D_i. Nuevamente por la continuidad de γ existe $\delta > 0$ tal que $\gamma(t) \in B'$ para todo $t \in [\tau - \delta, \tau + \delta]$. En particular para $t \in [\tau, \tau + \delta\rangle$ se tiene que $\gamma(t) \in B'$. Por consiguiente $g_1(\gamma(t)), \ldots, g_n(\gamma(t))$ son la raíces de $P(\gamma(t))$ para todo $t \in [\tau, \tau + \delta)$. Considere α_1 y fije $t \in [\tau - \delta, \tau\rangle$.Tenemos que $\alpha_1(t)$ es raíz de $P(\gamma(t))$, luego $\alpha_1(t) \in \{g_1(\gamma(t)), \ldots, g_n(\gamma(t))\}$ y por ultimo $\alpha_1(t) \in D_1 \cup D_2 \cup \ldots \cup D_n$ para todo $t \in [\tau - \delta, \tau\rangle$. Como $\alpha_1([\tau - \delta, \tau\rangle)$ es conexo y esta contenido en $D_1 \cup D_2 \cup \ldots \cup D_n$, entonces $\alpha_1([\tau - \delta, \tau\rangle) \subset B_j$ para algún $j = 1, ..., n$. Supongamos que $\alpha_1([\tau - \delta', \tau\rangle) \subset B_1$. Si $t \in [\tau - \delta, \tau\rangle$, entonces $\alpha_1(t)$ es raíz de $P(\gamma(t))$ y por lo tanto $\alpha_1(t) \in \{g_1(\gamma(t), \ldots, g_n(\gamma(t)\}$. Pero $\alpha_1(t) \in B_1$, lo que implica que $\alpha_1(t) = g_1(\gamma(t))$ $\forall t \in [\tau - \delta, \tau\rangle$. Si definimos

$$\bar{\alpha_1} = \begin{cases} \alpha_1(t) & \text{si} \quad t \in [0, \tau\rangle \\ \\ g_1(\gamma(t)) & \text{si} \quad \tau \leq t \leq \tau + \delta \end{cases}$$

se ve claramente que $\bar{\alpha_1}$ es una extensión continua de α_1. Repitiendo el argumento podemos extender $\alpha_2, \ldots, \alpha_n$ al intervalo $[0, \tau + \delta\rangle$ y esto contradice la definición de τ. Por lo tanto $\tau = 1$ y $\alpha_1, \ldots, \alpha_n$ se extienden continuamente a $[0, 1\rangle$. Sea $a'' = \gamma(1)$ y suponga que $r_1, ..., r_n$ denotan ahora las raíces de $P(a'')$. Nuevamente por la proposición 3.3 existen:

1. una bola abierta B'' centrada en a'',

2. discos D_1'', ..., D_n'' centrados en $r_1, ..., r_n$ respectivamente y dos a dos disjuntos,

3. funciones holomorfas $h_1, \ldots, h_n : B'' \to D_i''$ tales que $h_i(a'') = r_i$ respectivamente,

de manera que para todo $\gamma(t) \in B''$, el punto $h_i(\gamma(t))$ es la única raíz de $P(\gamma(t))$ en D_i''. Si tomamos $\delta'' > 0$ adecuado tal que $\gamma(1-\delta'', 1] \subset B''$, entonces $h_1(\gamma(t)), \ldots, h_n(\gamma(t))$ son la raíces de $P(\gamma(t))$ $\forall t \in \langle 1-\delta'', 1]$. Por lo tanto siguiendo los mismos pasos de antes y reordenando los h_j si es necesario podemos concluir que

$$\alpha_j(t) = h_j(\gamma(t)) \; \forall t \in \langle 1-\delta'', 1] \, .$$

Por último, si definimos

$$\bar{\alpha_j}(t) = \begin{cases} \alpha_j(t) & \text{si} \quad t \in [0, 1\rangle \\ \\ h_1(\gamma(t)) & \text{si} \quad t = 1 \end{cases}$$

Se concluye que $\alpha_1, \ldots, \alpha_n$ se extienden a $[0, 1]$.

Unicidad:

Suponga que $\theta_1, \ldots, \theta_n : [0, 1] \to \mathbb{C}$ son otros caminos continuos de las raíces de $P(\gamma(t))$. Como $\theta_1(0)$ es raíz de $P(\gamma(0))$, entonces $\theta_1(0) = \alpha_j(0)$ para algún $j \in \{1, ..., n\}$. Reordenando los θ_i podemos suponer que $\theta_1(0) = \alpha_1(0)$. Probemos que $\theta_1(t) = \alpha_1(t)$ para todo $t \in [0, 1]$. Por conexidad, será suficiente demostrar que el conjunto no vacío

$$A = \{t \in [0, 1] \, : \, \theta_(t) = \alpha_1(t)\}$$

es abierto y cerrado en $[0, 1]$. Claramente A es cerrado ya que θ_1 y α_1 son continuas. Probemos que A es abierto en $[0, 1]$. Sea $t_0 \in A$. Por proposición 3.3 existen:

1. una bola B centrada en $a_0 = \theta_1(0) = \alpha_1(0)$,

2. discos $D_1, ..., D_n$ disjuntos dos a dos y centrados en las raíces $r_1, ..., r_n$ de $P(a)$,

3. funciones holomorfas $h_i : B \to D_i$ tales que $h_i(a_0) = r_i$,

de manera que, para todo $a \in B$, el punto $h_i(a)$ es la única raíz de $P(a)$ en D_i. Como θ_1 y α_1 son continuas en t_0, existe una vecindad conexa J de t_0 en $[0, 1]$ tal que $\gamma(t) \in B$ para todo $t \in J$. Entonces, para todo $t \in J$, los puntos $h_i(\gamma(t))$ son las raíces de $P(\gamma(t))$ y estas raíces están contenidas en $D_1, ..., D_n$.

Reordenando los h_i podemos suponer que $\theta_1(t_0) = \alpha_1(t_0) = h_1(\gamma(t_0))$. Entonces, repitiendo el argumento de la conexidad hecho anteriormente podemos concluir que $\theta_1(t) = h_1(\gamma(t))$ para todo $t \in J$. De la misma forma tendremos $\alpha_1(t) = h_1(\gamma(t))$ para todo $t \in J$ y por lo tanto $J \subset A$, lo que muestra que A es abierto en $[0, 1]$. Repitiendo los argumentos anteriores para $\theta_2, ..., \theta_n$ podemos concluir que, salvo reordenación, $\theta_j = \alpha_j$ para todo $j = 1, ..., n$. $\square$

3.2. Lazos y Permutaciones

Por el teorema 3.5, si γ es un camino continuo en $\mathcal{S}_n$, entonces existen $\alpha_1, ..., \alpha_n$ caminos continuos de las raíces de $P(\gamma(t))$ para todo $t \in [0, 1]$. En este caso diremos que γ produce los caminos continuos $\alpha_1, ..., \alpha_n$ de las raíces de $P(\gamma(t))$ o también podemos decir que $\alpha_1, ..., \alpha_n$ son caminos de las raíces de $P(\gamma(t))$ (teniendo en cuenta que los α_i fueron producidos por γ). Podemos pensar que los caminos $\alpha_1, ..., \alpha_n$ representan movimientos para las raíces de $P(\gamma(t))$: Sea r_1 una de las raíces de $P(\gamma(0))$, digamos $r_1 = \alpha_1(0)$.Cuando t varia de 0 a 1, la raíz r_1 "se mueve" siguiendo el camino $\alpha_1(t)$. Al final del movimiento, podemos pensar que la raíz r_1 de $P(\gamma(0))$ "se transforma" en la raíz $\alpha_1(1)$ de $P(\gamma(1))$. En este caso podemos decir también que el camino γ "transforma" la raíz r_1 de $P(\gamma(0))$ en la raíz $\alpha_1(\gamma(1))$ de $P(\gamma(1))$. Denotemos $\alpha_1(\gamma(1)) = r_1$. Considere ahora dos caminos $\gamma_1, \gamma_2 : [0, 1] \to \mathcal{S}_2$ con los mismos extremos, o sea, $\gamma_1(1) = \gamma_2(1) = b$, Dada r_1 raíz de $P(a)$, entonces γ_1 transforma r_1 en la raíz ${r_1}^{\gamma_1}$ de $P(b)$. De la misma manera, γ_2 transforma la raíz r_1 de $P(a)$ en la raíz ${r_1}^{\gamma_2}$ de $P(b)$. Más aún, si $r_1, ..., r_n$ son las raíces de $P(a)$, tendremos que γ_1 transforma estas raíces en

$$ {r_1}^{\gamma_1}, ..., {r_n}^{\gamma_1} $$

respectivamente. Por otro lado, γ_2 transforma $r_1, ..., r_n$ en ${r_1}^{\gamma_2}, ..., {r_n}^{\gamma_2}$. Claramente

$$ \{{r_1}^{\gamma_1}, ..., {r_n}^{\gamma_1}\} = \{{r_1}^{\gamma_2}, ..., {r_n}^{\gamma_2}\} $$

ya que ambos son el conjunto de raíces de $P(b)$. ¿Pero el orden de las raíces se respeta? O sea, ¿Es cierto que ${r_i}^{\gamma_1} = {r_i}^{\gamma_2}$?. Pues ¡esto no es cierto en general!. Veamos un ejemplo. Considere los polinomios $P(a) = x^2 + a$ para todo $a \in \mathbb{C}^*$. Es fácil ver que $P(a) \in \mathcal{S}_2$ para todo $a \in \mathbb{C}^*$. Considere los caminos $\gamma_1(t) = e^{i\pi t}$, $\gamma_2(t) = e^{-i\pi t}$, $t \in [0, 1]$. Claramente $\gamma_1(0) = \gamma_2(0) = 1$ y las raíces de $P(1)$ son i y $-i$. $\gamma_1(t)$ "produce" el camino $ie^{\frac{i\pi t}{2}}$ para la raíz i y el camino $-ie^{\frac{i\pi t}{2}}$ para la raíz $-i$. Entonces, γ_1 transforma las raíces i y $-i$ en las raíces -1 y 1 de

$P(-1) = x^2 - 1$. Por otro lado, γ_2 produce los caminos $ie^{\frac{-i\pi t}{2}}$ y $-ie^{\frac{-i\pi t}{2}}$ para i y $-i$ respectivamente. Luego estas raíces se transforman en la raíces 1 y -1 respectivamente.

Denotemos por $R(P(a))$ al conjunto de las raíces de $P(a)$.

Definición 3.3. *Sea γ un camino en $\mathcal{S}_n$ tal que $\gamma(0) = a$ y $\gamma(1) = b$. Sean $\alpha_1, ..., \alpha_n$ caminos de las raíces de $P(\gamma(t))$. Entonces definimos una biyección $\phi_{a,b}(\gamma) : R(P(a)) \to R(P(b))$ por*

$$\phi_{a,b}(\alpha_i(0)) = \alpha_i(1).$$

con $i = 1, ..., n$. En este caso decimos que γ induce la biyección $\phi_{a,b}$. Cuando $a = b$, γ induce una permutación de las raíces de $P(a)$.

Definición 3.4. *Sean γ_1 y γ_2 caminos continuos en $\mathcal{S}_n$ tales que: $\gamma_1(0) = a$, $\gamma_1(1) = \gamma_2(0) = b$ y $\gamma_2(1) = c$. Definimos*

$$(\gamma_1 * \gamma_2)(t) = \begin{cases} \gamma_1(2t) & si \quad t \in [0, \frac{1}{2}] \\ \gamma_2(2t-1) & si \quad t \in \langle \frac{1}{2}, 1] \end{cases}$$

Observar que solo se trata de la yuxtaposición de caminos en $\mathcal{S}_n$.

Proposición 3.6. *Sea γ_1 y γ_2 caminos continuos en $\mathcal{S}_n$ tales que $\gamma_1(0) = a$, $\gamma_1(1) = \gamma_2(0) = b$ y $\gamma_2(1) = c$. Entonces*

$$\phi_{a,c}(\gamma_1 * \gamma_2) = \phi_{b,c}(\gamma_2) \circ \phi_{a,b}(\gamma_1).$$

Demostración. Sean $\alpha_1, \ldots, \alpha_n : [0,1] \to \mathbb{C}$ y $\beta_1, \ldots, \beta_n : [0,1] \to \mathbb{C}$ caminos de las raíces de $P(\gamma_1(t))$ y $P(\gamma_2(t))$ respectivamente. Entonces tenemos que :

$$\phi_{a,b}(\gamma_1)(\alpha_i(0)) = \alpha_i(1)$$
$$\phi_{b,c}(\gamma_2)(\beta_i(0)) = \beta_i(1).$$

Además por la definición 3.4 se tiene que:

$$(\gamma_1 * \gamma_2)(t) = \begin{cases} \gamma_1(2t) & \text{si} \quad t \in [0, \frac{1}{2}] \\ \gamma_2(2t-1) & \text{si} \quad t \in \langle \frac{1}{2}, 1] \end{cases}$$

Por el teorema 3.5 aplicado a $\gamma_1 * \gamma_2$ existen caminos $\omega_1, \ldots, \omega_n : [0,1] \to \mathbb{C}$ tales que $\omega_1(t), \ldots, \omega_n(t)$ son las raíces de $P((\gamma_1 * \gamma_2)(t))$. Pero observemos que:

$$c_i(t) = \begin{cases} \alpha_i(2t) & \text{si} \quad t \in [0, \frac{1}{2}] \\ \beta_j(2t-1) & \text{si} \quad t \in \langle \frac{1}{2}, 1] \end{cases}$$

con j escogido adecuadamente tal que $\alpha_i(1) = \beta_j(0)$ y para que c_i sea continuo en $[0,1]$. Por lo tanto se tiene que:

$$\phi_{a,c}(\gamma_1 * \gamma_2)(\alpha_i(0)) = \beta_j(1).$$

□

Dados $a, b \in \mathcal{S}_n$, definimos:

$$\mathcal{L}_{a,b} := \{\gamma : [0,1] \to \mathcal{S}_n \text{ continuo } / \gamma(0) = a \text{ y } \gamma(1) = b\}.$$

Definición 3.5. *Sean γ_1, $\gamma_2 \in \mathcal{L}_{a,b}$. Decimos que γ_1 y γ_2 son homotópicos en $\mathcal{S}_n$ si existen una familia $\{\eta_s\}_{s\in[0,1]} \in \mathcal{L}_{a,b}$ de caminos continuos, tales que:*

1. *$\eta_0 = \gamma_1$ y $\eta_1 = \gamma_2$*
2. *La función $F : [0,1] \times [0,1] \to \mathcal{S}_n$ definida por $F(s,t) = \eta_s(t)$ es continua.*

Cuando se cumple la condición 2, diremos que $\{\eta_s\}_{s\in[0,1]}$ es una familia continua de caminos de $\mathcal{L}_{a,b}$.

Observación 3.7. *Rigurosamente, esta es la definición de caminos homotópicos con extremos fijos*

Sean γ_1, $\gamma_2 \in \mathcal{L}_{a,b}$. ¿Que relación deben cumplir ambos caminos para que con seguridad induzcan la misma biyección?. Daremos respuesta a esta pregunta con el siguiente teorema importante.

Teorema 3.8. *Si γ_1, γ_2 son homotópicos en $\mathcal{S}_n$, entonces $\phi_{a,b}(\gamma_1) = \phi_{a,b}(\gamma_2)$. En particular, si $a = b$, dos caminos homotópicos en $\mathcal{S}_n$ inducen la misma permutación en $R(p(a))$.*

Demostración. Como γ_1 es homotópico a γ_2, existe una familia $\{\eta_s\}_{s\in[0,1]}$ tal que:

1. $\eta_0 = \gamma_1$, $\eta_1 = \gamma_2$
2. La función $F(s,t) = \eta_s(t)$, $s, t \in [0,1]$ es continua.

Fije $r \in R(P(a))$. Para cada $s \in [0,1]$, por el teorema 3.5, existe un único camino $\zeta_s : [0,1] \to \mathbb{C}$ tal que

$$\zeta_s(0) = r \text{ y } \zeta_s(t) \in R(P(\eta_s(t))) \text{ para todo } t \in [0,1].$$

Afirmación:

La función $H(s,t) = \zeta_s(t)$; $s,t \in [0,1]$, es continua. En otras palabras $\{\zeta_s\}_{s\in[0,1]}$ es una familia continua de caminos de $\mathcal{L}_{a,b}$.

En efecto: Fije $s_0 \in [0,1]$. Sea

$$A = \{t \in [0,1]/\, \exists U \supset \{s_0\} \times [0,t] \text{ abierto en } [0,1]^2 \text{ tal que } H|_U \text{ es continua}\}.$$

Por el teorema 3.3, existen:

1. una vecindad D de $\eta_s(0) = a$,

2. vecindades D_1, D_2, ..., D_n de las raíces de $P(a)$ disjuntas dos a dos,

3. funciones $f_1 : D \to D_1$, ..., $f_n : D \to D_n$ holomorfas tales que $\{f_1(z), ..., f_n(z)\} = R(P(z))$ para todo $z \in D$.

Como $\{f_1(a), ..., f_n(a)\} = R(P(a))$, podemos suponer que $f_1(a) = r$.

Por continuidad de F en $(s_0, 0)$, existe U abierto en $[0,1]^2$ tal que $\eta_s(t) \in D$ para todo $(s,t) \in U$. Podemos suponer que $U = (s_0 - \epsilon,\, s_0 + \epsilon) \times [0,\, \epsilon)$ para cierto $\epsilon > 0$.

Sea $(\bar{s},\, \bar{t}) \in U$ un punto arbitrario. Considere $\alpha : [0, \bar{t}] \to \mathbb{C}$ definido por

$$\alpha(t) = f_1(\eta_{\bar{s}}(t)) = f_1(F(\bar{s},\, t)).$$

Tenemos que α es continua; además, $\alpha(t) \in D_1$ para todo $t \in [0, \bar{t}]$.

Como $\alpha(0) = f_1(\eta_{\bar{s}}(0)) = f_1(a) = r$ y $\alpha(t) \in R(P(\eta_{\bar{s}}(t)))$, por la unicidad del teorema 3.5 deducimos que $\alpha = \zeta_{\bar{s}}|_{[0,\bar{t}]}$. Luego

$$\zeta_{\bar{s}}(\bar{t}) = \alpha(\bar{t}) = f_1(\eta_{\bar{s}}(\bar{t})).$$

En otras palabras: $H(\bar{s}, \bar{t}) = f_1(F(\bar{s}, \bar{t}))$ para todo $(\bar{s}, \bar{t}) \in U$. Pero $g = f_1 \circ F|_U$ es continua, por lo tanto $H|_U$ es continua. Luego, como U es vecindad de $\{s_0\} \times [0, \frac{\epsilon}{2}]$, vemos que $\frac{\epsilon}{2} \in A$ (en realidad es obvio que $[0,\, \frac{\epsilon}{2}] \subset A$]). Por lo tanto $A \neq \emptyset$.

Como A es acotado y no vacío, existe $\tau = \sup$ A. Supongamos que $\tau < 1$. Sea $c = \eta_{s_0}(\tau)$. Ahora aunque no se trata de los mismos objetos usados antes, usaremos la misma notación para una mejor comprensión de los argumentos.

De nuevo, por la proposición 3.3 aplicado a c, existen:

1. una vecindad D de $\eta_{s_0}(\tau) = c$,

2. vecindades D_1, D_2, ..., D_n de las raíces de $P(c)$ disjuntas dos a dos,

3. funciones $f_1 : D \to D_1$, ..., $f_n : D \to D_n$ holomorfas tales que $\{f_1(z), ..., f_n(z)\} = R(P(z))$ para todo $z \in D$.

Definamos (existe) ahora $\tilde{K} = [s_0 - \epsilon,\, s_0 + \epsilon] \times [\tau - \delta, \tau + \delta]$ tal que $F(s,t) \in D$ para todo $(s,t) \in \tilde{K}$.

Como $\tau - \delta \in A$, existe una vecindad U de $\{s_0\} \times [0, \tau - \delta]$ tal que $H|_U$ es continua, en particular $(s_0, \tau - \delta) \in U$. Como U es abierto, reduciendo ϵ si es necesario, podemos suponer que $[s_0 - \epsilon,\, s_0 + \epsilon] \times \{\tau - \delta\} \subset U$. Consideremos $J = H([s_0 - \epsilon,\, s_0 + \epsilon] \times \{\tau - \delta\})$ y observemos que J es conexo. Si $z \in J$, entonces $z = H(\bar{s}, \tau - \delta)$, donde $\bar{s} \in [s_0 - \epsilon,\, s_0 + \epsilon]$. Con esto tenemos que $z = \zeta_{\bar{s}}(\tau - \delta) \in R(P(\eta_{\bar{s}}(\tau - \delta)))$; pero, recuerde que $\eta_{\bar{s}}(\tau - \delta) = F(\bar{s}, \tau - \delta) \in D$. Por lo tanto $z \in \{f_j(F(\bar{s}\tau - \delta))\}_{j=1,\dots,n} \subset D_1 \cup \dots \cup D_n$; así, $J \subset D_1 \cup \dots \cup D_n$. Como J es conexo, entonces podemos suponer que $J \subset D_1$; luego,

$$H(\bar{s}, \tau - \delta) = f_1(F(\bar{s}, \tau - \delta)) \text{ para todo } \bar{s} \in [s_0 - \epsilon,\, s_0 + \epsilon].$$

Fije $\bar{s} \in (s_0 - \epsilon,\, s_0 + \epsilon)$. Sea $\alpha : [\tau - \delta,\, \tau + \delta] \to \mathbb{C}$ definido como

$$\alpha(t) = f_1(F(\bar{s}, t)).$$

Observemos que α es continua,

$$\alpha(\tau - \delta) = f_1(F(\bar{s},\, \tau - \delta)) = H(\bar{s}, \tau - \delta) = \zeta_{\bar{s}}(\tau - \delta)$$

y $\alpha(t) \in R(P(\eta_{\bar{s}}(t)))$ para todo $t \in [\tau - \delta,\, \tau + \delta]$. Luego, por el teorema 3.5 (unicidad):

$$\alpha(t) = \zeta_{\bar{s}}|_{[\tau - \delta,\, \tau + \delta]}$$

entonces $H(\bar{s}, t) = \alpha(t) = f_1(F(\bar{s}, t))$ para todo $t \in [\tau - \delta,\, \tau + \delta]$. Como $\bar{s} \in [s_0 - \epsilon, s_0 + \epsilon]$ es arbitrario, entonces

$$H(s,t) = f_1(F(s,t)) \text{ para todo } (s,t) \in [s_0 - \epsilon,\, s_0 + \epsilon] \times [\tau - \delta,\, \tau + \delta].$$

Luego, si denotamos $V = (s_0 - \epsilon,\, s_0 + \epsilon) \times (\tau - \delta,\, \tau + \delta)$ tenemos que $H|_V$ es continua. Si definimos $\tilde{U} = U \cup V$, vemos que $\{s_0\} \times (0, \tau + \frac{\delta}{2}] \subset \tilde{U}$ y $H|\tilde{U}$ es continua. Por lo tanto $\tau + \frac{\delta}{2} \in A$(contradicción). Luego $\tau = 1$.

Probemos ahora que $1 \in A$. Para evitar abuso de notación y para mejor comprensión del trabajo emplearemos nuevamente las mismas notaciones de los objetos usados anteriormente, teniendo en cuenta que no se tratan de los mismos. Nuevamente, por la proposición 3.3 aplicado a b, existen:

1. una vecindad D de $\eta_{s_0}(\tau) = c$,

2. vecindades D_1, D_2, ..., D_n de las raíces de $P(c)$ disjuntas dos a dos,

3. funciones $f_1 : D \to D_1$, ..., $f_n : D \to D_n$ holomorfas tales que $\{f_1(z), ..., f_n(z)\} = R(P(z))$ para todo $z \in D$,

definimos (existe) $\tilde{K} = [s_0 - \epsilon,\, s_0 + \epsilon] \times [1 - \delta,\, 1]$ tal que $F(s,t) \in D$ para todo $(s,t) \in K$. Como $1 - \delta \in A$, existe una vecindad U de $\{s_0\} \times [0, 1 - \delta]$ tal que $H|_U$ es continua, en particular $(s_0, 1 - \delta) \in U$. Como U es abierto, reduciendo ϵ si es necesario, podemos suponer que $[s_0 - \epsilon,\, s_0 + \epsilon] \times \{1 - \delta\} \subset U$. Consideremos $J = H([s_0 - \epsilon,\, s_0 + \epsilon] \times \{1 - \delta\})$ y observemos que J es conexo. Si $z \in J$, entonces $z = H(\bar{s}, 1 - \delta)$, donde $\bar{s} \in [s_0 - \epsilon,\, s_0 + \epsilon]$. Con esto tenemos que $z = \zeta_{\bar{s}}(1 - \delta) \in R(P(\eta_{\bar{s}}(1 - \delta)))$; pero, recuerde que
$\eta_{\bar{s}}(1-\delta) = F(\bar{s}, 1-\delta) \in D$. Por lo tanto $z \in \{f_j(F(\bar{s}1-\delta))\}_{j=1,\ldots,n} \subset D_1 \cup \ldots \cup D_n$. Así, $J \subset D_1 \cup \ldots \cup D_n$. Como J es conexo, entonces podemos suponer que $J \subset D_1$; luego, $H(\bar{s}, 1-\delta) = f_1(F(\bar{s}, 1-\delta))$ para todo $\bar{s} \in [s_0-\epsilon,\, s_0+\epsilon]$. Fije $\bar{s} \in (s_0-\epsilon,\, s_0+\epsilon)$. Sea $\alpha : [1 - \delta,\, 1] \to \mathbb{C}$ definido como $\alpha(t) = f_1(F(\bar{s}, t))$. Observemos que α es continua,

$$\alpha(1 - \delta)) = f_1(F(\bar{s},\, 1 - \delta)) = H(\bar{s}, 1 - \delta) = \zeta_{\bar{s}}(1 - \delta)$$

y $\alpha(t) \in R(P(\eta_{\bar{s}}(t)))$ para todo $t \in [1 - \delta,\, 1]$. Luego, por teorema 3.5 (unicidad):

$$\alpha(t) = \zeta_{\bar{s}}|_{[1-\delta,\, 1]}$$

entonces $H(\bar{s}, t) = \alpha(t) = f_1(F(\bar{s}, t))$ para todo $t \in [1 - \delta,\, 1]$. Como $\bar{s} \in [s_0 - \epsilon, s_0 + \epsilon]$ es arbitrario, entonces

$$H(s, t) = f_1(F(s, t)) \text{ para todo } (s, t) \in [s_0 - \epsilon,\, s_0 + \epsilon] \times [1 - \delta,\, 1].$$

Luego, si denotamos $V = (s_0 - \epsilon,\, s_0 + \epsilon) \times (1 - \delta,\, 1]$ tenemos que $H|_V$ es continua. Si definimos $\tilde{U} = U \cup V$, vemos que $\{s_0\} \times [0, 1] \subset \tilde{U}$ y $H|\tilde{U}$ es continua. Por lo tanto $1 \in A$.

Hasta el momento tenemos que existe una vecindad $\tilde{U}$ de $\{s_0\} \times [0, 1]$ tal que $H|_{\tilde{U}}$ es continua. En particular: $H|_{\tilde{U}}$ es continua en (s_0, t_0) cualquiera que sea $t_0 \in [0, 1]$. Como $\tilde{U}$ es un abierto en $[0, 1]^2$, concluimos que H es continua en s_0, t_0. Como s_0, $t_0 \in [0, 1]$ son arbitrarios, hemos demostrado que H es continua.

Ahora, si definimos la función $f : [0,1] \to \mathbb{C}$ tal que $f(s) = \zeta_s(1)$ para todo $s \in [0,1]$ tendremos que f es continua. Como f toma valores en el conjunto finito $R(P(b))$, concluimos que $f = cte$. Por lo tanto γ_1 y γ_2 producen la misma biyección.

$\square$

3.3. El Grupo $\pi_1(\mathcal{S}_n, a)$ y las Permutaciones Inducidas en las Raíces de $P(a)$.

Sea $\gamma_1, \gamma_2 \in \mathcal{L}_{a,b}$. Decimos que

$$\gamma_1 \equiv \gamma_2 \text{ si y sólo si } \gamma_1 \text{ y } \gamma_2 \text{ son homotópicos en } \mathcal{S}_n.$$

Proposición 3.9. *La relación "$\equiv$" es de equivalencia.*

Demostración. Probaremos las siguientes condiciones:

1. Definamos $F : [0,1] \times [0,1] \to \mathcal{S}_n$ tal que $F(s,t) = \gamma(t)$ para todo $s, t \in [0,1]$. Tenemos que esta función es continua. Por lo tanto $\gamma \equiv \gamma$. Lo cual prueba que la relación es reflexiva.

2. Si $\gamma_1 \equiv \gamma_2$, entonces existe una familia $\{\eta_s\}_{s\in[0,1]}$ y una función $F : [0,1] \times [0,1] \to \mathcal{S}_n$ continua, talque: $\eta_0 = \gamma_1$ y $\eta_1 = \gamma_2$. Definamos $G : [0,1] \times [0,1] \to \mathcal{S}_n$ tal que $G(s,t) = F(1-s,t)$. Observemos que esta función es continua y además $G(0,t) = \gamma_2$ y $G(1,t) = \gamma_1$. Por lo tanto $\gamma_2 \equiv \gamma_1$.

3. si $\gamma_1 \equiv \gamma_2$ y $\gamma_2 \equiv \gamma_3$, entonces existen familias de caminos continuos $\{\eta_s\}_{s\in[0,1]}$, $\{\mu_s\}_{s\in[0,1]}$ en $\mathcal{S}_n$ y funciones $F(s,t) = \eta_s(t)$, $G(s,t) = \mu_s(t)$ tales que: $\eta_0 = \gamma_1$, $\eta_1 = \gamma_2$, $\mu_0 = \gamma_2$ y $\mu_1 = \gamma_3$. Definamos

$$h_s(t) = \begin{cases} \eta_s(2t) & \text{si} \quad t, s \in [0, \frac{1}{2}] \\ \mu_s(2t-1) & \text{si} \quad t, s \in [\frac{1}{2}, 1] \end{cases}$$

Entonces es fácil ver que $\{h_s\}_{s\in[0,1]}$ es una homotopía entre γ_1 y γ_3.

$\square$

Como $\equiv$ es una relación de equivalencia podemos definir el conjunto

$$\pi_1(\mathcal{S}_{n,a,b}) = \mathcal{L}_{a,b}/\equiv$$

formado por las clases de equivalencia obtenidas por la relación $\equiv$.

Definición 3.6. *Sean* $[\gamma_1] \in \pi_1(\mathcal{S}_n, a, b)$ *y* $[\gamma_2] \in \pi_1(\mathcal{S}_n, b, c)$*. Definimos*

$$\gamma_1] \cdot [\gamma_2] = [\gamma_1 * \gamma_2].$$

Proposición 3.10. *Sean* $[\gamma_1] \in \pi_1(\mathcal{S}_n, a, b)$ *y* $[\gamma_2] \in \pi_1(\mathcal{S}_n, b, c)$*. El producto "* $\cdot$ *" esta bien definido.*

Demostración. Si $\gamma_1' \equiv \gamma_1$ y $\gamma_2' \equiv \gamma_2$, entonces existe una familia continua $\{\eta_s\}_{s\in[0,1]}$ y $\{\mu_s\}_{s\in[0,1]}$ que pertenecen a $\mathcal{L}_{a,b}$ y $\mathcal{L}_{b,c}$ tales que

$$\eta_0 = \gamma_1',\ \eta_1 = \gamma_1,\ \mu_0 = \gamma_2' \text{ y } \mu_1 = \gamma_2.$$

Definamos la familia de caminos continuos $\{\eta_s * \mu_s\}_{s\in[0,1]} \in \mathcal{L}_{a,c}$. Como se trata de solo la yuxtaposición de caminos continuos, se tiene que:

1. $(\eta_s * \mu_s)(0) = a$,
2. $(\eta_s * \mu_s)(1) = c$,
3. $(\eta_0 * \mu_0)(t) = (\gamma_1' * \gamma_2')(t)$ y
4. $(\eta_1 * \mu_1)(t) = (\gamma_1 * \gamma_2)(t)$.

Por lo tanto $[\gamma_1 * \gamma_2] = [\gamma_1' * \gamma_2']$. □

3.3.1. El Grupo $\pi_1(\mathcal{S}_n, a)$.

De ahora en adelante denotaremos a $\mathcal{L}_{a,a}$ simplemente como $\mathcal{L}_a$(cuyos elementos serán llamados lazos basados en a) y a $\pi_1(\mathcal{S}_n, a, a)$ como $\pi_1(\mathcal{S}_n, a)$.

Proposición 3.11. *El producto "* $\cdot$ *" hace de* $\pi_1(\mathcal{S}_n, a)$ *un grupo, llamado grupo fundamental de* $\mathcal{S}_n$ *basado en* a*.*

Demostración. Se debe probar las siguientes condiciones:

1. **Cerradura:** Sea $[\gamma_1]$, $[\gamma_2] \in \pi_1(\mathcal{S}_n, a)$. Observemos que

$$\gamma_1 * \gamma_2 = \begin{cases} \gamma_1(2t) & \text{si} \quad t \in [0, \frac{1}{2}] \\ \gamma_2(2t-1) & \text{si} \quad t \in [\frac{1}{2}, 1] \end{cases}$$

Donde se obtiene que $(\gamma_1 * \gamma_2)(0) = (\gamma_1 * \gamma_2)(1) = a$. Por lo tanto $[\gamma_1] \cdot [\gamma_2] \in \pi_1(\mathcal{S}_n, a)$

2. **Asociativa:** En efecto:

$$([\gamma_1]\cdot[\gamma_2])\cdot[\gamma_3] = [(\gamma_1 * \gamma_2) * \gamma_3] = [\gamma_1 * (\gamma_2 * \gamma_3)] = [\gamma_1]\cdot([\gamma_2]\cdot[\gamma_3]).$$

3. **Existencia de elemento inverso:** Notar que la inversa de $[\gamma]$ es $[\gamma^{-1}]$ definido por

$$\gamma^{-1}(t) = \gamma(1-t)$$

para $t \in [0,1]$.

4. **Existencia del elemento neutro:** observemos que el camino constante $\theta(t) = a$ para todo $t \in [0,1]$ es el elemento neutro.

□

3.3.2. El Grupo $\pi_1(\mathcal{S}_n, a)$ y las Raíces de $P(a)$.

Hasta el momento tenemos lo siguiente: Sea $[\gamma] \in \pi_1(\mathcal{S}_n, a)$. Sean x_1, x_2, ..., x_n las raíces de $P(\gamma(0))$. Por el teorema 3.5, aplicado a $\gamma \in \mathcal{L}_a$, existen caminos continuos $\alpha_1, \alpha_2, ..., \alpha_n : [0,1] \to \mathbb{C}$, tales que

1. $\alpha_1(0) = x_1$, $\alpha_2(0) = x_2, ..., \alpha_n(0) = x_n$
2. $\alpha_1(t), \alpha_2(t), ..., \alpha_n(t)$ son las raíces de $P(\gamma(t))$ para todo $t \in [0,1]$.

Se definió

$$\begin{array}{rcl} R(P(a)) & \stackrel{\phi_a(\gamma)}{\to} & R(P(a)) \\ \alpha_j(0) & \mapsto & \alpha_j(1) \end{array}$$

y vimos que $\phi_a(\gamma)$ es biyección. En este caso, como γ es un lazo basado en a, vemos que $\phi_a(\gamma)$ se trata de una permutación de raíces. Con lo cual podemos relacionarlo con el grupo simétrico S_n de la siguiente manera: Sea $j \in \{1, 2, ..., n\}$ dado. Como $\alpha_j(1) \in R(P(a))$, entonces $\alpha_j(1) \in \{\alpha_1(0), ..., \alpha_n(0)\}$. Luego existe un único $i \in \{1, ..., n\}$ tal que $\alpha_j(1) = \alpha_i(0)$. Definimos $\tilde{\phi}_\gamma$ como sigue

$$i = \tilde{\phi}_\gamma(j).$$

Ahora por el teorema 3.8, $\tilde{\phi}_\gamma$ solo depende de $[\gamma]$ en $\pi_1(\mathcal{S}_n, a)$. Así, podemos definir una aplicación

$$\begin{array}{rcl} \pi_1(\mathcal{S}_n, a) & \stackrel{\Phi_a}{\to} & S_n \\ [\gamma] & \mapsto & \tilde{\phi}_\gamma \end{array}$$

donde S_n es el grupo simétrico de grado n.

Proposición 3.12. Φ_a *es un homomorfismo de grupos.*

Demostración. Para todo $[\gamma_1]$, $[\gamma_2] \in \pi_1(\mathcal{S}_n, a)$ se tiene que

$$\Phi_a([\gamma_1]) \cdot \phi_a([\gamma_2]) = \tilde{\phi}_{\gamma_1} \cdot \tilde{\phi}_{\gamma_2} = \tilde{\phi}_{\gamma_1 * \gamma_2} = \Phi_a([\gamma_1 * \gamma_2]) = \Phi_a([\gamma_1] \cdot [\gamma_2]),$$

usando la proposición 3.6. $\square$

Capítulo 4

Movimiento de la Raíces del Polinomio $X^5 - X + a$.

En este capítulo demostraremos el resultado principal de la tesis, o sea, la irresolubilidad por radicales de la ecuación general de grado 5. Para esto estudiaremos las deformaciones de una clase especial de polinomios de grado 5, que son polinomios de la forma

$$X^5 - X + a$$

con $a \in \mathbb{C}$, que es obtenido con ι tal como se define en el ejemplo 6. Por supuesto, para poder aplicar los teoremas que hemos visto sobre deformaciones de polinomios, consideraremos "movimientos" a lo largo de caminos $\gamma : [0, 1] \to \mathcal{S}$ donde

$$\mathcal{S} = \{a \in \mathbb{C}/(a, -1, 0, 0, 0) \in \mathcal{S}_5\}.$$

Observemos que cada $a \in \mathcal{S}$ define un polinomio

$$P(a) = P(a, -1, 0, 0, 0) = x^5 - x + a;$$

con esta notación trabajaremos de aquí en adelante.

4.1. Un Lazo Particular Basado en 0.

Estudiaremos la permutación que induce un lazo especifico que lo definiremos más adelante. Por ahora enunciamos las siguientes afirmaciones que serán útiles a lo largo de esta sección.

Lema 4.1. *Si b es una raíz múltiple de $P(a)(x) = x^5 - x + a$, entonces $5b^4 = 1$.*

Demostración. Tenemos que $(P(a))'(x) = 5x^4 - 1$. Ahora, como b es una raíz múltiple de $P(a)$, entonces se tiene que $(P(a))'(b) = 0$. Por lo tanto $5b^4 - 1 = 0$ □

Proposición 4.2. *Si el polinomio $P(a)$ tiene raíces múltiples, entonces $a^4 = \frac{4^4}{5^5}$; en otras palabras*

$$a = \pm\frac{4}{5\sqrt[4]{5}} \text{ o } \pm\frac{4i}{5\sqrt[4]{5}}.$$

Demostración. Sea b la raíz múltiple de $P(a)$, entonces por Lema 4.1 tenemos que $5b^4 = 1$. Pero $b^5 - b + a = 0 \Rightarrow a = b - b^5 \Rightarrow a^4 = (b - b^5)^4 \Rightarrow a^4 = b^4(1 - b^4)^4 = \frac{1}{5} \cdot \frac{4^4}{5^4} = \frac{4^4}{5^5}$. □

Corolario 4.3. $\mathcal{S} = \mathbb{C} - \left\{\pm\frac{4}{5\sqrt[4]{5}}, \pm\frac{4i}{5\sqrt[4]{5}}\right\}$.

Demostración. Directo de la definición de $\mathcal{S}$ y proposición 4.2. Es fácil verificar que $\mathcal{S}$ es abierto en $\mathbb{C}$. □

Proposición 4.4. *Si $a_0 = \frac{4}{5\sqrt[4]{5}}$, entonces el polinomio $P(a_0)$ tiene una raíz múltiple $b_0 \in \mathbb{R}^+$ de multiplicidad 2, dos raíces β_2, $\beta_4 \notin \mathbb{R}$ y una raíz $\beta_3 \in \mathbb{R}^-$.*

Demostración. Por la proposición 4.2, $P(a_0)$ tiene alguna raíz múltiple b_0. Entonces $b_0^5 - b_0 + a_0 = 0$ y por el lema 4.1 tendremos $5b_0^4 = 1$. De estas dos ecuaciones obtenemos $b_0 = \sqrt[4]{\frac{1}{5}}$ y entonces es fácil verificar que

$$P(a_0)(b_0) = P(a_0)'(b_0) = 0 \text{ y } P(a_0)''(b_0) \neq 0,$$

o sea, b_0 tiene multiplicidad dos.
Tenemos que $P(a_0)(0) = a_0 > 0$ y $P(a_0)(-5\sqrt[5]{a_0}) = -5^5 a_0 + 5\sqrt[5]{a_0} + a_0 < 0$. Entonces por el teorema del valor intermedio existe una raíz $\beta_3 \in (-5\sqrt[5]{a_0}, 0)$. Es claro que $\beta_3 \in \mathbb{R}^-$.
Tenemos hasta el momento 3 raíces reales únicas en todo $\mathbb{R}$. Por lo tanto las otras dos raíces β_2 y β_4 son complejas conjugadas. □

Es fácil verificar que β_0 es la única raíz en $\mathbb{R}^+$ y β_3 es la única raíz en $\mathbb{R}^-$ Sea $F : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$ tal que $F(x, y) = y^5 - y + x$. Aplicando **el teorema de la función implícita** 1.20 a F con los puntos (a_0, β_2), (a_0, β_3), (a_0, β_4), ya que $F(a_0, \beta_2) = 0$, $F(a_0, \beta_3) = 0$, $F(a_0, \beta_4) = 0$ y $\frac{\partial}{\partial y}F(a_0, \beta_j) \neq 0$ (j=2,3 y 4) se tiene que: existen un disco D centrado en a_0 y funciones holomorfas f_2, f_3, $f_4 : D \subset \mathbb{C} \to \mathbb{C}$ tales que

1. $f_2(a_0) = \beta_2$, $f_3(a_0) = \beta_3$ y $f_4(a_0) = \beta_4$.

2. Para todo $y \in \Omega$ tenemos que $f_2(y)$, $f_3(y)$, $f_4(y)$ son raíces de $y^5 - y + x = 0$.

Sean D_2, D_3, D_4 y $\bar{D}_1$ discos centrados en $\beta_2, \beta_3, \beta_4$ y b_0 respectivamente. Suponga que estos discos son pequeños de manera que sean disjuntos y tal que D_2 y D_4 no contengan números reales. Por continuidad, podemos suponer D pequeño suficiente de manera que $f_2(D) \subset D_2$, $f_3(D) \subset D_3$ y $f(D) \subset D_4$.

Denotemos por δ_1 y $\bar{r}$ los radios de D y $\bar{D}_1$ respectivamente.

Proposición 4.5. *Dado $\bar{D}$ un disco compacto en $\mathbb{C}$, existe $\eta > 0$ tal que: si $|a - a_0| < \eta$, entonces las funciones $f(z) = z^5 - z + a_0$ y $h(z) = z^5 - z + a$ son tales que*

$$|f(\zeta) - h(\zeta)| < |f(\zeta)| \quad \textit{para todo } \zeta \in \partial\bar{D}.$$

Demostración. $|f| : \partial\bar{D} \to \mathbb{R}$ tiene un máximo y un mínimo valor por tener como dominio un conjunto compacto en $\mathbb{C}$. Sea η este mínimo valor. Luego, si $|a - a_0| < \eta$, tenemos

$$|f(\zeta) - h(\zeta)| = |a - a_0| < \eta \leq |f(\zeta)| \text{ para todo } \zeta \in \partial\bar{D}.$$

□

Ahora, aplicando la proposición 4.5 al disco compacto $\bar{D}_1$, existe $\eta > 0$ tal que: si $|a - a_0| < \eta$, entonces la funciones $f(z) = z^5 - z + a_0$ y $h(z) = z^5 - z + a$ son tales que

$$|f(\zeta) - h(\zeta)| < |f(\zeta)| \text{ para todo } \zeta \in \partial\bar{D}_1.$$

Entonces, por el teorema 1.27 se concluye que f y g tienen la misma cantidad de raíces en la región interior de $\bar{D}_1$. Como $f(z) = z^5 - z + a_0$ tiene una raíz b de multiplicidad dos, entonces $g(z) = z^5 - z + a$ tiene 2 raíces en el interior de $\bar{D}_1$.

Lema 4.6. *Existe $\tilde{\epsilon} > 0$ tal que: si $|z| \leq \tilde{\epsilon}$, entonces*

$$|c_3 z^3 + c_4 z^4 + z^5| < |c_2 z^2|.$$

Demostración. Tenemos que

$$\lim_{z \to 0} \frac{c_3 z^3 + c_4 z^4 + z^5}{c_2 z^2} = 0;$$

entonces para $\epsilon = 1$, existe $\tilde{\epsilon} > 0$ tal que: si $|z| \leq \tilde{\epsilon}$, entonces

$$\left| \frac{c_3 z^3 + c_4 z^4 + z^5}{c_2 z^2} \right| < 1.$$

Obteniéndose la prueba del lema. □

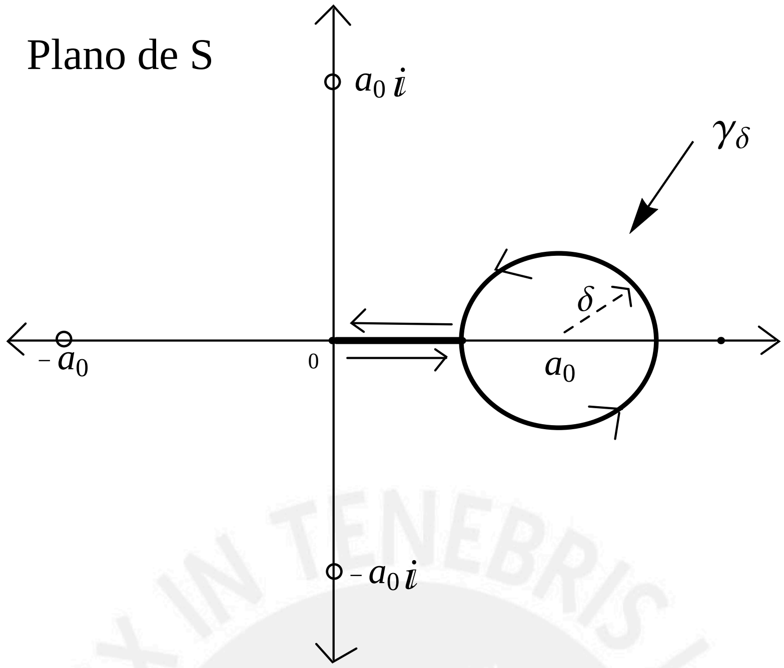

Figura 4.1: Gráfico de γ_δ

Sea $\delta = \text{mín}\{1, \delta_1, \eta, , \tilde{\epsilon}, |a_0|\}$, donde $\tilde{\epsilon}$ es dado en el lema 4.6. Definimos $\gamma_\delta : [0,1] \to \mathcal{S}$ Camino especial γ_δ tal que

$$\gamma_\delta(t) = \begin{cases} C_1(t) = 3t(a_0 - \delta) & \text{si} \quad 0 \leq t < \frac{1}{3} \\ a_0 + \delta e^{(-3\pi+6\pi t)i} & \text{si} \quad \frac{1}{3} \leq t < \frac{2}{3} \\ C_3(t) = (3-3t)(a_0 - \delta) & \text{si} \quad \frac{2}{3} \leq t \leq 1 \end{cases}$$

tal como se muestra en la figura 4.1.

Se estudiará la permutación que produce γ_δ en el conjunto de raíces de $x^5 - x$. Para esto será necesario analizar el comportamiento de las raíces de $P(\gamma_\delta(t))$ a medida que t varía en $[0,\,1]$.

Empezaremos analizando la cantidad de raíces reales que tiene $P(\gamma_\delta(t)) \in \mathbb{R}[x]$ para $t \in [0, \frac{1}{3}]$. Para este objetivo graficaremos $P(\gamma_\delta(t))$ mediante algunos conceptos y teoremas clásicos del cálculo diferencial. Sea $t \in [0, \frac{1}{3}]$ fijo, tenemos que $(P(\gamma_\delta(t)))'(x) = 5x^4 - 1$ e igualando a 0 tenemos que $x = \pm\frac{1}{\sqrt[4]{5}}$. Reemplazando x en la ecuación se tiene que

$$\left(\frac{1}{\sqrt[4]{5}}\right)^5 - \left(\frac{1}{\sqrt[4]{5}}\right) + 3t\left(\frac{1}{5\sqrt[4]{5}} - \delta\right) < 0$$

y

$$\left(-\frac{1}{\sqrt[4]{5}}\right)^5 - \left(-\frac{1}{\sqrt[4]{5}}\right) + 3t\left(\frac{1}{5\sqrt[4]{5}} - \delta\right) > 0$$

para todo $t \in \left[0, \frac{1}{3}\right]$. Es fácil verificar que $P(\gamma_\delta(t))$ tiene un máximo local en $-\frac{1}{\sqrt[4]{5}}$ y un mínimo local en $\frac{1}{\sqrt[4]{5}}$. Ahora analizaremos los intervalos de monotonía de $P(3t(a_0-\delta))$. Tenemos por calculo sencillo que
$(P(3t(a_0-\delta))'(0) < 0$, $(P(3t(a_0-\delta))'(1) > 0$ y $(P(3t(a_0-\delta))'(-1) > 0$, por lo tanto $P(\gamma_\delta(t))$:

1. En $\left(-\infty, -\frac{1}{\sqrt[4]{5}}\right)$ es estrictamente creciente,

2. En $\left(-\frac{1}{\sqrt[4]{5}}, \frac{1}{\sqrt[4]{5}}\right)$ es estrictamente decreciente,

3. En $\left(\frac{1}{\sqrt[4]{5}}, +\infty\right)$ es estrictamente creciente

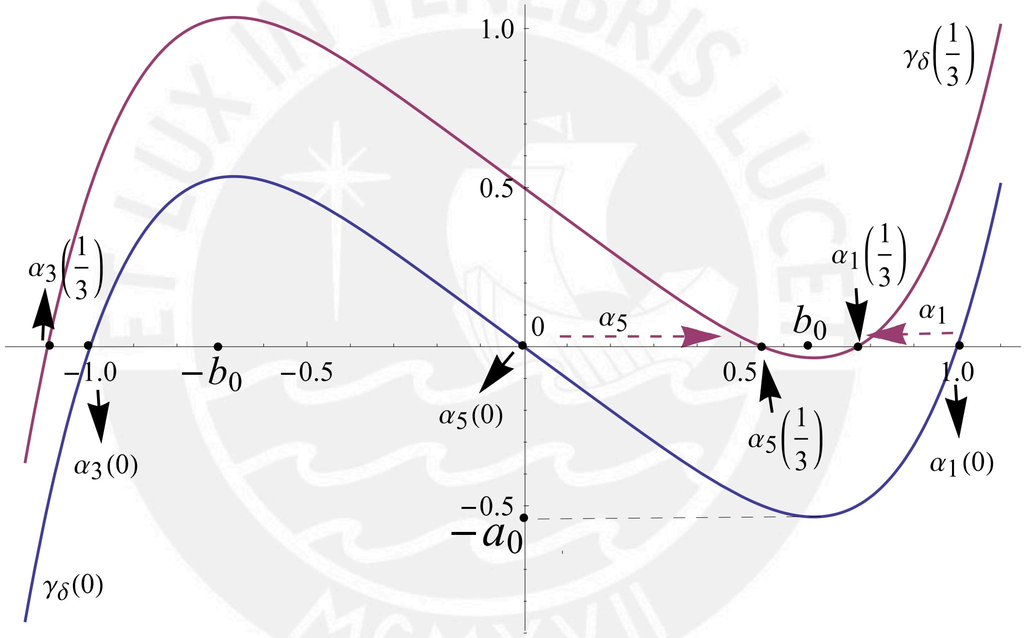

Figura 4.2: Gráfico de $P(\gamma_\delta)$, $t \in [0, \frac{1}{3}]$

para todo $t \in [0, \frac{1}{3}]$, tal como se muestra en la figura 4.2. Por lo tanto, cuando t varia en $\left[0, \frac{1}{3}\right]$ el polinomio $P(\gamma_\delta(t)) = x^5 - x + 3t(a_0-\delta)$ tiene exactamente 3 raíces reales.
Por el teorema 3.5 aplicado a γ_δ y $\{1, i, -1, -i, 0\}$ raíces de $P(\gamma_\delta(0))$, existen caminos continuos $\alpha_1, ..., \alpha_5 : [0,1] \to \mathbb{C}$ tales que:

1. $\alpha_1(0) = 1$, $\alpha_2(0) = i$, $\alpha_3(0) = -1$, $\alpha_4(0) = -i$ y $\alpha_5(0) = 0$

2. $\alpha_1(t), ..., \alpha_5(t)$ son las raíces diferentes de $P(\gamma_\delta(t))$ para todo $t \in [0,1]$.

Lema 4.7. $\alpha_1(t)$, $\alpha_3(t)$, *y* $\alpha_5(t) \in \mathbb{R}$ *para todo* $t \in [0, \frac{1}{3}]$.

Demostración. Sea

$$A = \left\{ s \in \left[0, \frac{1}{3}\right] \; / \, \alpha_1(t),\ \alpha_3(t) \text{ y } \ \alpha_5(t) \in \mathbb{R} \text{ para todo } t \in [0, s] \right\}.$$

Como $A \subset [0, \frac{1}{3}]$ y $A \neq \emptyset (0 \in A)$, entonces existe $\tau = sup\, A$. Probemos primero que $\tau \in A$. Por definición de supremo existe una sucesión $(s_n) \subset A$ tal que $s_n \to \tau$.
Si $i \in \{1, 3, 5\}$, por continuidad tenemos $\lim_{n\to\infty} \alpha_i(s_n)) = \alpha_i(\tau)$. Pero $\alpha_i(s_n) \in \mathbb{R}\ \forall n \in \mathbb{N}$, entonces, como $\mathbb{R}$ es un conjunto cerrado en $\mathbb{C}$, tendremos que $\alpha_i(\tau) \in A$. Por lo tanto $\tau \in A$. Ahora será suficiente demostrar que $\tau = \frac{1}{3}$. Suponga que $\tau < \frac{1}{3}$. Entonces, podemos aplicar el teorema de la función implícita real y concluir que existe $\epsilon > 0$ tal que $[\tau, \tau + \epsilon] \subset A$, lo que es una contradicción. □

Corolario 4.8. $\alpha_2(t), \alpha_4(t) \notin \mathbb{R}\ \forall t \in [0, \frac{1}{3}]$.

Lema 4.9. *Se cumplen las siguientes afirmaciones*

1. $\alpha_3 : [0, \frac{1}{3}] \to \mathbb{R}$ *es decreciente,*

2. $\alpha_5 : [0, \frac{1}{3}] \to \mathbb{R}$ *es creciente y*

3. $\alpha_1 : [0, \frac{1}{3}] \to \mathbb{R}$ *es decreciente.*

Demostración. Daremos la prueba para α_1, la prueba para los demás puntos será de forma análoga. Del gráfico 4.2 observamos que $\alpha_1(0) > \alpha_1(\frac{1}{3})$. Entonces basta demostrar que α_1 es inyectiva. Supongamos que no, entonces existen $t_0 \neq t_1$ tal que $\alpha_1(t_0) = \alpha_1(t_1)$, entonces

$$\begin{aligned} 0 &= P(\gamma_\delta(t_1))(\alpha_1(t_0)) = \alpha^5(t_0) - \alpha_1(t_0) + 3t_1(a_0 - \delta) \\ &= \alpha^5(t_0) - \alpha_1(t_0) + 3t_0(a_0 - \delta) + 3t_1(a_0 - \delta) - 3t_0(a_0 - \delta) \\ &= 3t_1(a_0 - \delta) - 3t_0(a_0 - \delta) \end{aligned}$$

obteniéndose $t_1 = t_0$(contradicción). □

Podemos ver claramente este hecho ya que solo se trata de trasladar el gráfico de $P(0)$ hacia arriba cuando t varía de 0 a $\frac{1}{3}$, tal como lo muestra la figura 4.2. Recordar que δ usado en la definición de γ_δ es menor que δ_1. Por lo tanto $\gamma_\delta(\frac{1}{3}) \in D$, con lo cual se tiene que

$$f_2\left(\gamma_\delta\left(\frac{1}{3}\right)\right) \in D_2,\ f_3\left(\gamma_\delta\left(\frac{1}{3}\right)\right) \in D_3,\ f_4\left(\gamma_\delta\left(\frac{1}{3}\right)\right) \in D_4.$$

Como $\{f_2\left(\gamma_\delta\left(\frac{1}{3}\right)\right), f_3\left(\gamma_\delta\left(\frac{1}{3}\right)\right), f_4\left(\gamma_\delta\left(\frac{1}{3}\right)\right)\}$ son raíces de $x^5 - x + \gamma_\delta\left(\frac{1}{3}\right) = 0$, entonces

$$\left\{f_2\left(\gamma_\delta\left(\frac{1}{3}\right)\right), f_3\left(\gamma_\delta\left(\frac{1}{3}\right)\right), f_4\left(\gamma_\delta\left(\frac{1}{3}\right)\right)\right\} \subset \left\{\alpha_1\left(\frac{1}{3}\right), \alpha_2\left(\frac{1}{3}\right), \alpha_3\left(\frac{1}{3}\right), \alpha_4\left(\frac{1}{3}\right), \alpha_5\left(\frac{1}{3}\right)\right\}.$$

Con todo lo dicho anteriormente se puede verificar fácilmente que:

- $f_2\left(\gamma_\delta\left(\frac{1}{3}\right)\right) \notin \mathbb{R}$ y tiene parte imaginaria positiva,
- $f_4\left(\gamma_\delta\left(\frac{1}{3}\right)\right) \notin \mathbb{R}$ y tiene parte imaginaria negativa,
- $f_3\left(\gamma_\delta\left(\frac{1}{3}\right)\right)$ no tiene parte real positiva,
- $\alpha_1\left(\frac{1}{3}\right)$ es real y positivo mayor que b_0,
- $\alpha_2\left(\frac{1}{3}\right) \notin \mathbb{R}$ y tiene parte imaginaria positiva,
- $\alpha_4\left(\frac{1}{3}\right) \notin \mathbb{R}$ y tiene parte imaginaria negativa,
- $\alpha_5\left(\frac{1}{3}\right) \in \mathbb{R}$ y es positivo menor que b_0,
- $\alpha_3(\frac{1}{3}) \in \mathbb{R}$ y es negativo.

Por lo tanto:

$$f_2\left(\gamma_\delta\left(\frac{1}{3}\right)\right) = \alpha_2\left(\frac{1}{3}\right), \; f_4\left(\gamma_\delta\left(\frac{1}{3}\right)\right) = \alpha_4\left(\frac{1}{3}\right) \text{ y } f_3\left(\gamma_\delta\left(\frac{1}{3}\right)\right) = \alpha_3\left(\frac{1}{3}\right).$$

Recuerde que $\gamma_\delta(t) \in D$ para todo $t \in [\frac{1}{3}, \frac{2}{3}]$. Luego $f_2(\gamma_\delta(t))$ es raíz de $P(\gamma_\delta(t))$ para todo $t \in [\frac{1}{3}, \frac{2}{3}]$. Como $f_2(\gamma_\delta(\frac{1}{3})) = \alpha_2(\frac{1}{3})$, por la unicidad del teorema 3.5 tendremos que $f_2(\gamma_\delta(t) = \alpha_2(t))$ para todo $t \in [\frac{1}{3}, \frac{2}{3}]$ y entonces $\alpha_2(t) \in D_2$ para todo $t \in [\frac{1}{3}, \frac{2}{3}]$. Análogamente tendremos $\alpha_3(t) \in D_3$ y $\alpha_4(t) \in D_4$ para todo $t \in [\frac{1}{3}, \frac{2}{3}]$. Si $t \in [\frac{1}{3}, \frac{2}{3}]$, entonces $\gamma_\delta(t)$. Luego $P(\gamma_\delta(t))$ tiene exactamente dos raíces en $\bar{D}_1$, justamente $\alpha_1(t)$ y $\alpha_5(t)$ ya que $\alpha_2(t)$, $\alpha_3(t)$ y $\alpha_4(t)$ están en los discos D_2, D_3 y D_4. Como $\gamma_\delta(\frac{1}{3}) = \gamma_\delta(\frac{2}{3})$, entonces $P(\gamma_\delta(\frac{1}{3}))$ y $P(\gamma_\delta(\frac{2}{3}))$ son el mismo polinomio, así que tienen las mismas raíces en $\bar{D}_1$. Entonces

$$\left\{\alpha_1\left(\frac{1}{3}\right), \alpha_5\left(\frac{1}{3}\right)\right\} = \left\{\alpha_1\left(\frac{2}{3}\right), \alpha_5\left(\frac{2}{3}\right)\right\}.$$

Afirmación $\alpha_1(\frac{1}{3}) = \alpha_5(\frac{2}{3})$ y $\alpha_5(\frac{1}{3}) = \alpha_1(\frac{2}{3})$

Demostración. Definamos

$$F(z) = 10b_0^3 z^2 + 10b_0^2 z^3 + b_0 z^4 + z^5$$

y $h_1(t) = \alpha_1(t) - b_0$, camino en $\mathbb{C}^*$ definido en $[\frac{1}{3}, \frac{2}{3}]$. Como $\alpha_1(t) = b_0 + h_1(t)$ es raíz de $P(\gamma_\delta(t))$, entonces $(b_0 + h_1)^5 - (b_0 + h_1) + a_0 - \delta e^{6\pi it} = 0$. Luego,

$$(F \circ h_1)(t) = 10b_0^3 h_1^2(t) + 10b_0^2 h_1^3(t) + 5b_0 h_1^4(t) + h_1^5(t) = \delta e^{6\pi it},$$

obteniéndose por último que $F(h_1(t)) = \delta e^{6\pi it}$. Observemos que $1 = Ind(F \circ h_1, 0)$. Supongamos que $\alpha_1\left(\frac{1}{3}\right) = \alpha_1\left(\frac{2}{3}\right)$. Entonces

$$h_1\left(\frac{1}{3}\right) = h_1\left(\frac{2}{3}\right) \text{ y } (F \circ h_1)\left(\frac{1}{3}\right) = (F \circ h_1)\left(\frac{2}{3}\right),$$

concluyéndose así que h_1 y $F \circ h_1$ son caminos cerrados en $\mathbb{C}^*$. Como $\delta \leq \tilde{\epsilon}$ (obtenido del lema 4.6), entonces

$$|F(h_1(t)) - 10b_0^3(h_1)^2(t)| = |10b_0^2(h_1)^3(t) + b_0(h_1)^4(t) + (h_1)^5(t)| < |10b_0^3(h_1)^2(t)|.$$

Luego, por el teorema 1.24, se tiene

$$\begin{aligned} 1 = Ind(F \circ h_1, 0) &= Ind(10b_0^3(h_1)^2, 0) \\ &= \frac{1}{2\pi i}\int_{\frac{1}{3}}^{\frac{2}{3}} \frac{(10b_0^3(h_1)^2(t))' \mathrm{d}t}{10b_0^3(h_1)^2(t)} \\ &= \frac{1}{2\pi i}\int_{\frac{1}{3}}^{\frac{2}{3}} \frac{10(2)b_0^3(h_1)(t)(h_1'(t))\mathrm{d}t}{10b_0^3(h_1)^2(t)} \\ &= 2\, Ind(h_1, 0), \end{aligned}$$

entonces $Ind(h_1, 0) = \frac{1}{2}$ (contradicción), ya que el indice de h_1 con respecto de 0 es entero. Por lo tanto, $\alpha_1(\frac{2}{3}) = \alpha_5(\frac{1}{3})$ y $\alpha_5(\frac{2}{3}) = \alpha_1(\frac{1}{3})$. □

Hasta el momento se tiene la siguiente figura 4.3 (mirando dentro de $\bar{D}_1$), que nos da una visualización de los caminos de las raíces a medida que t varia en $[0, \frac{2}{3}]$.

Para finalizar todo sobre el comportamiento de las raíces de $P(\gamma_\delta(t))$ a medida que t varía de 0 hasta 1, usaremos la siguiente observación

Observación 4.10. *Sean γ, $\eta : [0,1] \to \mathcal{S}$ dos caminos continuos tales que $\eta(t) = \gamma(1-t)$. Sean $\alpha_i : [0,1] \to \mathbb{C}$,con $i = 1, \ldots, 5$, caminos continuos de las raíces de $P(\gamma(t))$. Entonces $\beta_1, \beta_2, \ldots, \beta_5 : [0,1] \to \mathbb{C}$ definidos como $\beta_i(t) = \alpha_i(1-t)$, son los caminos continuos de las raíces que produce $P(\eta(t))$.*

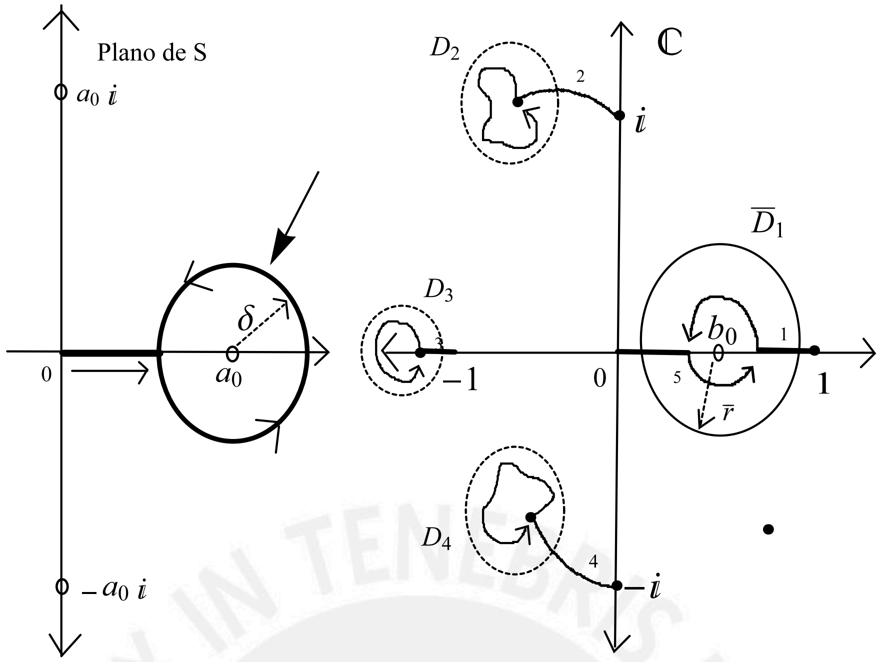

Figura 4.3: Movimiento de las raíces a medida que t varia en γ_δ en $[0, \frac{2}{3}]$

Con esta observación tenemos la siguiente información que buscábamos:

$$\begin{array}{ccccc}
\alpha_1(0) = 1 & \alpha_2(0) = i & \alpha_3(0) = -1 & \alpha_4(0) = -i & \alpha_5(0) = 0 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\alpha_1(\frac{1}{3}) = \theta_1 & \theta_2 & \theta_3 & \theta_4 & \alpha_5(\frac{1}{3}) = \theta_5 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\alpha_1(\frac{2}{3}) = \theta_5 & \theta_2 & \theta_3 & \theta_4 & \alpha_5(\frac{2}{3}) = \theta_1 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\alpha_1(1) = 0 & \alpha_2(1) = i & \alpha_3(1) = -1 & \alpha_4(1) = -i & \alpha_5(1) = 1
\end{array}$$

Lográndose demostrar que

Teorema 4.11. $\Phi_0([\gamma_\delta]) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}.$

4.1.1. Permutaciones de las Raíces de $x^5 - x + a$ Inducidas por $\pi_1(\mathcal{S}, a)$

Proposición 4.12. *Las raíces del polinomio $P(ia)(x) = x^5 - x + ia$ son obtenidas de las raíces del polinomio $P(a)(x) = x^5 - x + a$ por multiplicación por i.*

Demostración. Si r una raíz de $P(a)$, entonces $r^5 - r + a = 0$. Luego se tiene que:

$$\begin{aligned}(ri)^5 - (ri) + ia &= i^5 r^5 - ri + ia \\ &= i(r^5 - r + a) \\ &= 0\end{aligned}$$

Lo que demuestra la proposición. $\square$

Corolario 4.13. *Se cumplen las siguientes afirmaciones:*

1. $\Phi_0([i\gamma_\delta]) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$

2. $\Phi_0([i^2\gamma_\delta]) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}$

3. $\Phi_0([i^3\gamma_\delta]) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$.

Demostración. Por el teorema 4.11, se se tiene que

$$\begin{aligned}\phi(\gamma_\delta): \quad & R(P(0)) && \to R(P(0)) \\ & \alpha_1(0) = 1 && \mapsto \alpha_1(1) = 0 \\ & \alpha_2(0) = i && \mapsto \alpha_2(1) = i \\ & \alpha_3(0) = -1 && \mapsto \alpha_3(1) = -1 \\ & \alpha_4(0) = -i && \mapsto \alpha_4(1) = -i \\ & \alpha_5(0) = 0 && \mapsto \alpha_5(1) = 1\end{aligned}$$

Luego aplicando el teorema 3.5 a $i\gamma_\delta$ junto a las raíces de $P(i\gamma_\delta(0))$ existen caminos continuos $\beta_1, ..., \beta_5$ de las raíces de $P(i\gamma_\delta(0))$. Luego aplicando la proposición 4.12 y reordenando si es necesario se tiene que

1. $\beta_1(0) = i\alpha_4(0) = 1$, $\beta_2(0) = i\alpha_1(0) = i$,
   $\beta_3(0) = i\alpha_2(0) = -1$, $\beta_4(0) = i\alpha_3(0) = -i$ y $\beta_5(0) = i\alpha_5(0) = 0$

2. $\beta_i(t) = i\alpha_j(t)$ son las raíces diferentes de $P(i\gamma_\delta)$, eligiendo i y j adecuadamente tal que se cumpla el punto número 1.

Observemos que

$$\beta_1(1) = \beta_1(0),\ \beta_2(1) = \beta_5(0),\ \beta_3(1) = \beta_3(0),\ \beta_4(1) = \beta_4(0) \text{ y } \beta_5(1) = \beta_2(0).$$

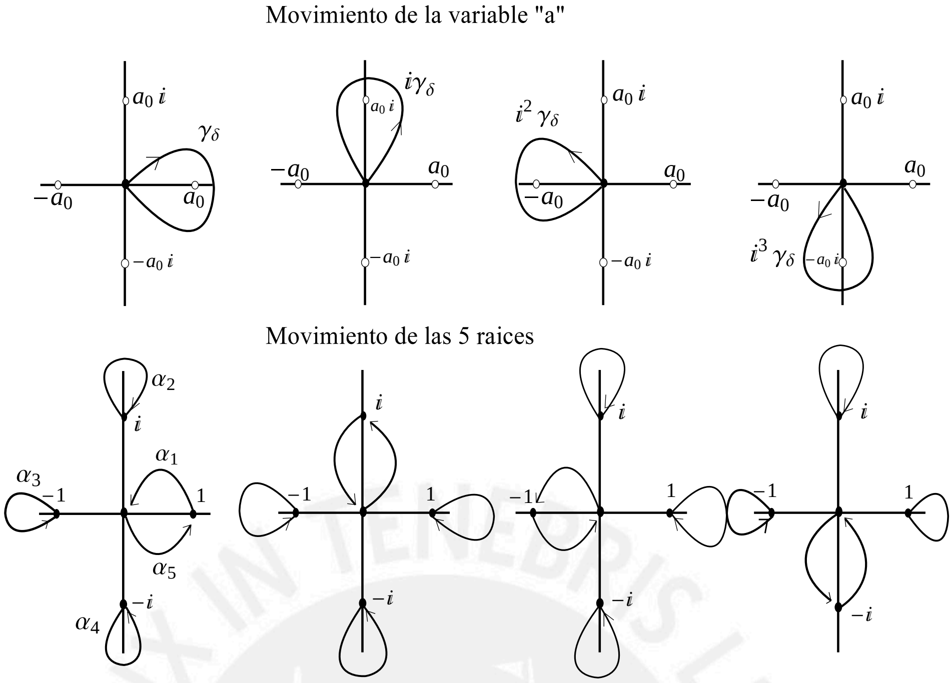

Figura 4.4: Todos los movimiento de a y variación de raíces

Con esto podemos decir que

$$\Phi_0([i\gamma_\delta]) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}.$$

Análogamente se pueden probar las afirmaciones restantes. $\square$

Corolario 4.14. $\Phi_0 : \pi_1(\mathcal{S}, 0) \to S_5$ *es sobreyectiva.*

Demostración. Sea $\sigma \in S_5$. Por teorema 1.9 σ se puede escribir como producto de $\psi_1 = \Phi_0([\gamma_\delta])$, $\psi_2 = \Phi_0([i\gamma_\delta])$, $\psi_3 = \Phi_0([i^2\gamma_\delta])$ y $\psi_4 = \Phi_0(i^3\gamma_\delta)$. Lo que prueba el corolario. $\square$

Hasta ahora solo se ha logrado demostrar la sobreyectividad de Φ_0. Si consideramos lazos basados en $a \neq 0$ ¿Φ_a será también sobreyectiva?.
Observemos que la definición de Φ_a depende de la elección del orden de las raíces. En el caso de Φ_0, las raíces de $P(0)$ son $\{1, i, -1, -i, 0\}$, de tal forma que al denotar $1 := 1$, $i := 2$, $-1 := 3$, $-i := 4$ y $0 := 5$ y al definir un camino $\gamma \in \mathcal{L}_0$, tenemos que $\Phi_0([\gamma]) \in S_5$. Es lógico pensar que si hubiéramos dado otro orden o denotado

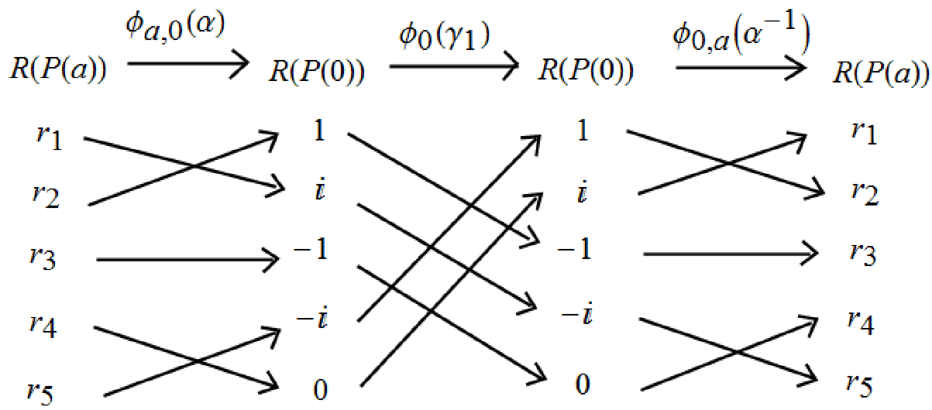

Figura 4.5: Diagrama de $\phi_{a,0}(\alpha)$, $\phi_0(\gamma_1)$ y $\phi_{0,a}(\alpha^{-1})$

de otra forma a las raíces de $P(0)$, $\Phi_0([\gamma])$ sería otra permutación de S_5.
Por tanto; debemos dar un orden fijo a las raíces de $P(a)$. Sean $\{r_1, r_2, r_3, r_4, r_5\}$ sus raíces (ya definidos en orden). Sea $\alpha \in \mathcal{L}_{a,0}$ y supongamos que $\phi_{a,0}(\alpha)$ está definido tal como se muestra en la figura 4.5, también podemos observar la definición de $\phi_{0,a}(\alpha^{-1})$. Sea $\gamma_1 \in \mathcal{L}_0$ tal que

$$\Phi_0([\gamma_1]) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix},$$

esto quiere decir que $\phi_0(\gamma_1)$ está definida tal como se muestra en la figura 4.5. Observemos que si $\gamma_2 = \alpha * \gamma_1 * \alpha^{-1}$, entonces por el diagrama de la figura 4.5 se tiene que

$$\Phi_a([\gamma_2]) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}.$$

Sería ideal encontrar caminos que pertenecen a $\mathcal{L}_a$ de tal forma que induzcan cualquier permutación. Debemos de notar un problema: no sabemos como está definido $\phi_{a,0}(\alpha)$ al ser elegido $\alpha \in \mathcal{L}_{a,0}$, ¿y si supiéramos como esta definido $\phi_{a,0}$, es posible encontrar $\gamma_1 \in \mathcal{L}_0$ adecuado de tal forma que $\gamma_2 = \alpha * \gamma_1 * \alpha$ induzca la permutación deseada?. ¡Eso es posible!, en efecto:
Sea $\gamma_2 = \alpha * \gamma_1 * \alpha \in \mathcal{L}_a$, el objetivo es encontrar una definición para γ_1 de tal forma que γ_2 induzca una permutación σ cualquiera. En otras palabras debemos obtener

$$\Phi_a([\gamma_2]) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) \end{pmatrix}$$

Esto quiere decir encontrar γ_1 de tal manera que $\phi_a(\gamma_2)$ esté definida por $\phi_a(\gamma_2)(r_1) = r_{\sigma(1)}$, $\phi_a(\gamma_2)(r_2) = r_{\sigma(2)}$, $\phi_a(\gamma_2)(r_3) = r_{\sigma(3)}$, $\phi_a(\gamma_2)(r_4) = r_{\sigma(4)}$ y

$\phi_a(\gamma_2)(r_5) = r_{\sigma(5)}$.
Es fácil verificar que $\vartheta : R(P(0)) \to R(P(0))$ definido por

$$\begin{array}{ll} \vartheta(\phi_{a,0}(\alpha_1)(r_1)) = \phi_{0,a}(\alpha^{-1})(r_{\sigma(1)}) & \vartheta(\phi_{a,0}(\alpha_1)(r_2)) = \phi_{0,a}(\alpha^{-1})(r_{\sigma(2)}) \\ \vartheta(\phi_{a,0}(\alpha_1)(r_3)) = \phi_{0,a}(\alpha^{-1})(r_{\sigma(3)}) & \vartheta(\phi_{a,0}(\alpha_1)(r_4)) = \phi_{0,a}(\alpha^{-1})(r_{\sigma(4)}) \\ \vartheta(\phi_{a,0}(\alpha_1)(r_5)) = \phi_{0,a}(\alpha^{-1})(r_{\sigma(5)}) & \end{array}$$

cumple con nuestro objetivo. Observemos que es posible encontrar un camino γ_1 tal que $\phi_0(\gamma_1) = \vartheta$ por la sobreyectividad de Φ_0. Con esto podemos afirmar lo siguiente,

Proposición 4.15. *Sea $a \neq 0 \in \mathcal{S}$. Entonces,*

$$\Phi_a : \pi_1(\mathcal{S}, a) \to S_5 \text{ es sobreyectiva.}$$

4.2. Variación de a y Permutación de Radicales Intermedios

Supongamos que la ecuación algebraica general de grado 5

$$a_0 + a_1 x + ... + a_4 x^4 + x^5 = 0$$

puede resolverse por radicales. Como vimos en el capítulo 2 se puede encontrar:

- polinomios de coeficientes complejos $\tilde{p}_1, ..., \tilde{p}_N$,
- naturales $k_1, ..., k_N$,

tales que, dado un polinomio $a_0 + a_1 x + ... + a_4 x^4 + x^5 = 0$ y dado una raíz r de este, existen complejos $x_1, ..., x_N = r$ tales que

$$\begin{aligned} x_1^{k_1} &= \tilde{p}_1(a_0, ..., a_4) \\ x_2^{k_2} &= \tilde{p}_2(a_0, ..., a_4, x_1) \\ \vdots &= \vdots \\ x_N^{k_N} &= \tilde{p}_N(a_0, ..., a_4, x_1, ..., x_N). \end{aligned}$$

En el caso particular de la familia $x^5 - x + a$, esta supuesta resolución por radicales nos dice los siguiente: Dada una raíz r de $x^5 - x + a$, existen

$x_1, ..., x_N = r$ tales que

$$\begin{aligned} x_1^{k_1} &= \tilde{p}_1(a, -1, 0, 0) \\ x_2^{k_2} &= \tilde{p}_2(a, -1, 0, 0, x_1) \\ \vdots &= \vdots \\ x_N^{k_N} &= \tilde{p}_N(a, -1, 0, 0, x_1, ..., x_N). \end{aligned}$$

Denotemos

$$\begin{aligned} p_1(a) &= \tilde{p}_1(a, -1, 0, 0) \\ p_2(a, x_1) &= \tilde{p}_2(a, -1, 0, 0, x_1) \\ \vdots &= \vdots \\ p_N(a, x_1, ..., x_{N-1}) &= \tilde{p}_N(a, -1, 0, 0, x_1, ..., x_{N-1}) \end{aligned}$$

Entonces, para la familia de polinomios $x^5 - x + a$ la resolubilidad por radicales viene expresada por el sistema:

$$\begin{aligned} x_1^{k_1} &= p_1(a) \\ x_2^{k_2} &= p_1(a, x_1) \\ \vdots &= \vdots \\ x_N^{k_N} &= p_N(a, x_1, ..., x_N). \end{aligned} \tag{4.1}$$

A continuación discutiremos algunas hipótesis que pueden ser asumidas en relación al sistema 4.1.

Hipótesis 1. En el sistema (4.1) podemos asumir que los números $k_1, ..., k_N$ son primos: Supongamos que $k_j = ab$ con $a, b > 1$, $a, b \in \mathbb{N}$. En este caso podemos retirar la línea

$$x_j^{k_j} = (x_j^a)^b = p_j(a, x_1, ..., x_{j-1})$$

del sistema (4.1) y colocar en su lugar el par de líneas siguiente:

$$\begin{aligned} \bar{x}_j^b &= p_j(a, ..., x_{j-1}) \\ x_j^a &= \bar{x}_j. \end{aligned}$$

Es fácil ver que el sistema (4.1) modificado de esta forma satisface los requerimientos de una "resolución por radicales". De manera sencilla: Si $k = ab$, "una raíz

$k-\acute{e}sima$" es equivalente a "una raíz $a-\acute{e}sima$" seguida de "una raíz $b-\acute{e}sima$". La aplicación sucesiva del argumento anterior nos lleva a un sistema como (4.1) pero con todos los k_j primos.

Hipótesis 2. Para cada línea

$$(*)...x_j^{k_j} = p_j(a, x_1, x_1, ..., x_{j-1})$$

del sistema(4.1) es posible encontrar valores $a, x_1, ..., x_{j-1}$ que cumplen todas las líneas anteriores a $(*)$ y tales que

$$p_j(a, x_1, ..., x_{j-1}) \neq 0.$$

La justificación de esta hipótesis es la siguiente: Caso contrario, en la línea $j-\acute{e}sima$ obtendríamos siempre $x_j = 0$. En este caso podemos simplemente "borrar" la linea $j-\acute{e}sima$ y reemplazar $x_j = 0$ en los polinomios $p_j + 1, ..., p_N$.

hipótesis 3. Para cada línea

$$x_j^{k_j} = p_j(a, x_1, ..., x_{j-1})$$

se tiene una de las siguientes posibilidades:

1. o bien p_j es constante e igual a 1,
2. o bien $x_j^{k_j} - p_j$ es irreductible.

Justificación: Suponga que $x_j^{k_j} - p_j$ es reductible. Como k_j es primo (hipótesis 1), entonces se sabe que existe $d = d(a, x_1, ..., x_N)$ tal que
$p_j = d^{k_j}$([2]). Entonces tendremos $x_j = \zeta d$, donde ζ es alguna raíz $k_j - \acute{e}sima$ de 1. En este caso podemos modificar el sistema (4.1) sustituyendo la linea $x_j^{k_j} = p_j$ por $\zeta^{k_j} = 1$ y sustituyendo $x_j = \zeta d$ en todas las líneas siguientes; así obtendremos:

$$\begin{aligned}
x_1^{k_1} &= p_1(a)\\
\vdots &= \vdots\\
x_{j-1}^{k_{j-1}} &= p_{j-1}(a, x_1, ..., x_{j-2})\\
\zeta^{k_j} &= 1\\
x_{j+1}^{k_{j+1}} &= p_{j+1}(a, x_1, ..., x_{j-1}, \zeta d)\\
x_{j+2}^{k_{j+2}} &= p_{j+2}(a, x_1, ..., x_{j-1}, \zeta d, x_{j+1})\\
\vdots &= \vdots\\
x_N^{k_N} &= p_N(a, x_1, ..., x_{j-1}, \zeta d, X_{j+1}, ..., x_{N-1})
\end{aligned}$$

Naturalmente acá podemos cambiar la letra "ζ" y volver a colocar "x_j". Así tendremos un nuevo sistema que define una resolución por radicales.
Comenzaremos ahora con la idea que finalmente nos permitirá demostrar la irresolubilidad de la ecuación de grado 5. Lo que haremos será "variar" el complejo a a lo largo de un camino cerrado en $\mathcal{S}$. Sabemos que, fijada una raíz r de $x^5 - x + \gamma(0)$, entonces γ induce un "movimiento" continuo de la raíz r. Pero ¿Qué ocurre con los valores intermedios $x_1, ..., x_{N-1}$ cuando a varia sobre γ? ¿Será cierto que estos puntos describen movimientos continuos? Veamos primero que ocurre con x_1. Si $p_1(\gamma(t))$ no se anula, entonces el teorema 3.5 garantiza que x_1 varia continuamente describiendo un camino $\alpha_1(t)$. ¿Qué ocurre en caso contrario?. Tenemos dos casos:

1. $p_1(\gamma(t))$ se anula $\forall t \in [0,1]$. A pesar de tratarse de una situación súper degenerada, en este caso el punto x_1 describe un camino continuo: el camino constante es igual a cero.

2. $p_1(\gamma(t))$ no es idénticamente nulo, pero se anula para ciertos valores de t. En este caso γ pasa por algunas de las finitas raíces de p_1. Entonces, como lo que nos va a interesar es la permutación de raíces que induce γ, nos permitiremos "cambiar" γ por otro camino γ_1, próximo suficiente a γ de manera que ambos sean homotópicos, pero que γ_1 no pase por ninguna raíz de p_1. Con esta modificación tendremos que x_1 describe un camino continuo α_1. veamos que pasa con x_2. Esta vez tenemos
$x_2^{k_2} = p_2(\gamma_1(t), \alpha_1(t))$. Si $p_2(\gamma_1(t), \alpha_1(t))$ nunca se anula entonces, de nuevo por el teorema 3.5, x_2 describe un camino continuo α_2. Supongamos que $p_2(\gamma_1, \alpha_1)$ se anula para algunos valores de t. Analizaremos los 2 casos siguientes:

   a) p_1 es constante igual a 1. Entonces $p_1(\gamma(t)) \equiv 1$ y el camino α_1 será constante igual a una raíz $k - \acute{e}sima$ de la unidad, digamos $\alpha_1 = \zeta$; luego $p_2(\gamma_1(t), \alpha_1(t)) = p_2(\gamma_1(t), \zeta)$. Si $p_2(\gamma_1(t), \zeta) \equiv 0$, entonces tendremos $\alpha_2 \equiv 0$. Caso contrario, tendremos que γ_1 pasa por algunas de las finitas raíces de $p_2(z, \zeta)$. Luego,como antes, podemos deformar γ_1 "un poquito"de manera que $p_2(\gamma_1, \zeta)$ nunca se anule y aplicamos el teorema 3.5 para obtener $\alpha_2(t)$ continua.

   b) p_1 no es constante igual a 1. Entonces, según la hipótesis 3 tendremos que $x_1^{k_1} - p_1$ es irreductible. Si $p_2(\gamma_1(t), \alpha_1(t))$ se anula para $t = t_0$, tendremos que $b = \gamma_1(t_0)$ pertenece al siguiente conjunto

$$\begin{aligned} B \;&= \{b \in \mathcal{S} \,/\, p_1(b) \neq 0 \text{ y existe } x_1 \in \mathbb{C} \text{ con } x_1^{k_1} = p_1(b) \\ &\qquad\qquad \text{y tal que } p_2(b, x_1) = 0\}. \end{aligned}$$

O sea: $p_2(\gamma_1, \alpha_1)$ se anula cuando γ_1 pasa por algún punto de b. Ahora será suficiente demostrar que B es discreto, ya que entonces podremos deformar γ_1 "un poquito" de manera que ahora $p_2(\gamma_1, \alpha_1)$ nunca se anula y entonces tendremos que x_2 varia continuamente por el teorema 3.5. Suponga, por contradicción, que existen $b_n (n \in \mathbb{N})$ puntos en B tal que $b_n \to b \in B$. De aquí, existen $x_n \in \mathbb{C}$ tal que

$$x_n^{k_1} = p_1(b_n) \text{ y } p_2(b_n, x_n) = 0 \text{ para todo } n \in \mathbb{N}.$$

Como $p_1(\gamma_1) \neq 0$, entonces $p_1(b) \neq 0$ y aplicando teorema 1.20 existen:

1) Un disco $D = D_\epsilon(b)$

2) Funciones holomorfas $g_1,\, g_2,\, \ldots,\, g_{k_1} : D \to \mathbb{C}$ tales que $g_1(z),\, \ldots,\, g_{k_1}(z)$ son las soluciones de

$$x_1^{k_1} = p_1(z) \text{ para todo } z \in D.$$

Pasando a subsucesiones, podemos suponer que $b_n \in D$ para todo $n \in \mathbb{N}$, entonces

$$x_n \in \{g_1(b_n),\, \ldots,\, g_{k_1}(b_n)\} \text{ para todo } n \in \mathbb{N}.$$

Nuevamente, pasando a subsucesiones y reordenando si es necesario podemos suponer que $x_n = g_1(b_n)$ para todo $n \in \mathbb{N}$, entonces $p_1(b_n, g_1(b_n)) = 0$ y por el Principio de Identidad se tiene

$$p_1(z, g_1(z)) = 0 \text{ para todo } z \in D.$$

Definamos los siguientes conjuntos

$$\begin{aligned} \mathcal{C} &= \{(z, x_1) \in \mathbb{C}^2 / \, x_1^{k_1} = p_1(z)\} \\ \mathcal{C}_1 &= \{(z, x_1) \in \mathbb{C}^2 / \, p_2(z, x_1) = 0\} \\ \Delta &= \{(z, g_(z)) / \, z \in D\}. \end{aligned}$$

Observe que Δ es un abierto de la curva algebraica irreductible $\mathcal{C}$. Además $\Delta \subset \mathcal{C}$. Luego, por el teorema de **Ceros de Hilbert** tendremos que $x_1^{k_1} - p_1(z)$ es un factor de $p_2(z, x_1)$.

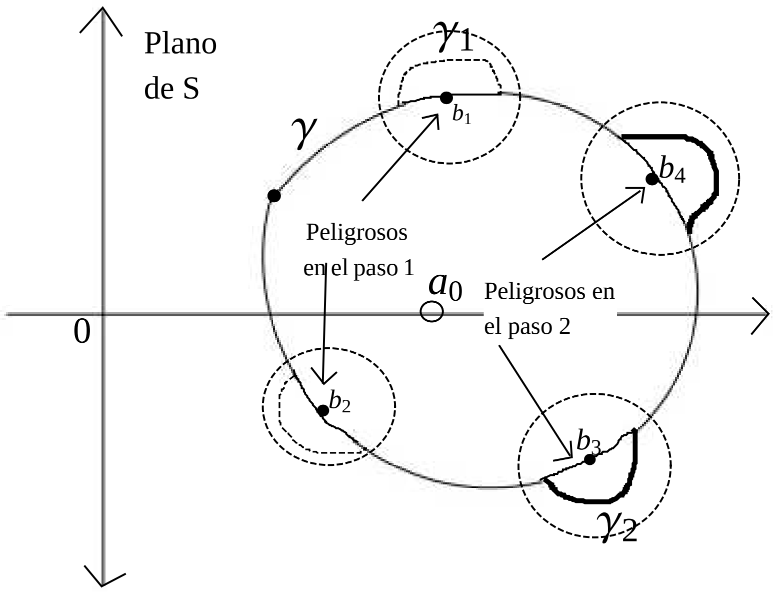

Figura 4.6: Eleccion de γ_1 y γ_2 en base de γ

En otras palabras: si (a, x_1) son soluciones de $x_1^{k_1} = p_1(a)$, tendremos automáticamente que en la siguiente ecuación $x_2^{k_2} = p_2(a, x_1)$ necesariamente $x_2 = 0$, ya que

$$p_2(a, x_1) = (x_1^{k_1} - p_1(a))Q(x_1, a) = 0.$$

Esto contradice la hipótesis 2. Este argumento a requerido el uso de la teoría de conjuntos algebraicos y teoremas especializados como el **Teorema de los Ceros de Hilbert**[17]. Como el propósito de este trabajo es mostrar las ideas geométricas que están detrás de la resolución por radicales. Simplemente asumiremos como hipótesis

Proposición 4.16. *Dado $\gamma : [0, 2] \to \mathcal{S}$, existe $\tilde{\gamma}$ arbitrariamente próximo a γ en $\mathcal{S}$ tal que, si r es una raíz de $x^5 - x + \tilde{\gamma}(0)$ y $x_1, ..., x_N = r$ son los valores intermedios dados por la resolución por radicales (Sistema (4.1)), entonces existen caminos $\alpha_1, ..., \alpha_N : [0, 1] \to \mathcal{S}$ continuos tales que*

$$\begin{aligned}
(\alpha_1(t))^{k_1} &= p_1(\tilde{\gamma}(t)),\\
(\alpha_1(t))^{k_2} &= p_2(\tilde{\gamma}(t), \alpha_1(t)),\\
\vdots &= \vdots\\
(\alpha_N(t))^{k_N} &= p_N(\tilde{\gamma}(t), \alpha_1(t), ..., \alpha_{N-1}).
\end{aligned}$$

Además, para cada $j = 1, ..., N$ *se tiene que* $p_j(t) = p_j(\tilde{\gamma}(t), \alpha_1(t), ..., \alpha_{j-1})$ *es no nulo para todo* $t \in [0,1]$ *o entonces nulo para todo* $t \in [0,1]$*. O sea: O* α_j *es no nulo* $\forall\, t \in [0,1]$*, o* $\alpha_j \equiv 0$*.*

Observación 4.17. *Esta observación dice que, a medida que a describe el camino* $\tilde{\gamma}$*, cada valor intermedio* $x_1, ..., x_N$ *(de una raíz* r *dada) describe un camino continuo. A estos caminos los llamaremos caminos intermedios producidos por* $\tilde{\gamma}$*.*

Observación 4.18. *Si* γ *es cerrado y basado en* $0 \in \mathbb{C}$*, es posible que* $\tilde{\gamma}$ *no sea más basado en* $0 \in \mathbb{C}$ *estamos interesados en aplicar esta proposición a varios caminos "simultáneamente"; entonces, dados* $\gamma_1, ..., \gamma_k$ *encontraremos caminos* $\tilde{\gamma}_1, ..., \tilde{\gamma}_k$*. Si los* α_j *son cerrados y basados en* $0 \in \mathbb{C}$*, entonces se puede conseguir que* $\tilde{\gamma}_j$ *están basadas en un mismo punto* $a \in \mathbb{C}$ *próximo de* $0 \in \mathbb{C}$*.*

Para facilitar la exposición definamos lo siguiente.

Definición 4.1. *Sea* G *un grupo. Diremos que* $\alpha \in G$ *es un 1-conmutador si existen* $\alpha_1, \alpha_2 \in G$ *tal es que*

$$\alpha = \alpha_1\alpha_2\alpha_1^{-1}\alpha_2^{-1}.$$

Si $n \in \mathbb{N}$*, diremos que* α *es un* $n-$*conmutador si existen* $(n-1)-$*conmutadores* α_1 *y* α_2 *en* G *tal es que*

$$\alpha = \alpha_1\alpha_2\alpha_1^{-1}\alpha_2^{-1}.$$

Claramente, si α es un $n-$conmutador, entonces α es un $m-$conmutador para todo $m \leq n$.

Lema 4.19. *Sea* $k \in \mathbb{N}$ *y sean* γ_1 *y* γ_2 *caminos cerrados en* $\mathbb{C}^*$ *basados en un mismo punto* $a_0 \in \mathbb{C}^*$*. Suponga que el parámetro* a *en la ecuación*

$$x^k - a = 0$$

se mueve a lo largo del camino

$$\gamma = \gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}.$$

Entonces γ *induce la permutación identidad en el conjunto de raíces de* $x^5 - a_0 = 0$*.*

Demostración. Definamos $\theta_1, \theta_2 : [0,1] \to \mathbb{C}^{*k}$ por $\theta_i(t) = (-\gamma_i(t), 0, ..., 0, 1)$. Observemos que $P(\theta_i(t))(x) = x^k - \gamma_i(t)$, por el teorema 3.5 existen $\alpha_1^i, ..., \alpha_k^i : [0,1] \to \mathbb{C}$ caminos continuos de las raíces de $P(\theta_i(t))$. Definamos

$\beta_j^i(t) = \alpha_1^i(t)e^{\frac{2\pi i(j-1)}{k}}$, es fácil verificar que $\beta_j^i(t)$ es raíz de $P(\theta_i(t))$. Ahora por la unicidad del teorema 3.5 se tiene que, reordenando si es necesario,
$\alpha_j^m(t) = \alpha_1^m(t)e^{\frac{2\pi i(j-1)}{k}}$ para todo $t \in [0,1]$.
Tenemos lo siguiente, si $\alpha_1^1(1) = \alpha_r^1(0)$, entonces

$$\begin{aligned}
\alpha_n^1(1) &= \alpha_1^1(1)e^{\frac{2\pi i(n-1)}{k}} \\
&= \alpha_r^1(0)e^{\frac{2\pi i(n-1)}{k}} \\
&= \alpha_1^1(0)e^{\frac{2\pi i(r-1)}{k}}e^{\frac{2\pi i(n-1)}{k}} \\
&= \alpha_1^1(0)e^{\frac{2\pi i(n+r-1)}{k}} \\
&= \alpha_{r+n-1}^1(0)
\end{aligned}$$

de la misma forma se puede probar que si $\alpha_1^2(1) = \alpha_s^1(0)$, entonces
$\alpha_n^2(1) = \alpha_{s+n-1}^1(0)$. Con lo cual tenemos que

$$\begin{aligned}
&\alpha_n^1(0) \to \alpha_{r+n-1}^1(0) \to \alpha_{r+n+s-2}^2(0) \\
\to \alpha_{r+n+s-s+1-2}^2(0) \to \alpha_{r-r-1+n+s-s+1-2}^1(0) = \alpha_n^1(0)
\end{aligned}$$

De aquí, $\theta_1\theta_2\theta_1^{-1}\theta_2^{-1}$ induce la permutación identidad, pero como θ_i solo depende de γ_i, podemos decir que γ induce la permutación id. □

Proposición 4.20. *Si $[\gamma] \in \pi_1(\mathcal{S}, 0)$ es un $N-$conmutador, entonces*

$$\Phi_0([\gamma]) = id.$$

Demostración. **Paso 1.** Como $[\gamma]$ es $N-$conmutador, entonces $[\gamma]$ es un $1-$conmutador, así que $[\gamma] = [\gamma_1][\gamma_2][\gamma_1]^{-1}[\gamma_2]^{-1}$. Teniendo en cuenta la proposición 4.16 podemos suponer que γ_1, γ_2 están basados en $a \in \mathbb{C}$ próximo de $0 \in \mathbb{C}$. Además, fijada una raíz r, tendremos que γ_1, γ_2 producen los caminos intermedios

$$\alpha_1^1, \alpha_2^1, ..., \alpha_N^1 \text{ y}$$

$$\alpha_1^2, \alpha_2^2, ..., \alpha_N^2$$

respectivamente. Se vé fácilmente que α_1 es un camino cerrado. Si $N = 1$, ya que $\alpha_1 = \alpha_N$ describe el movimiento de la raíz r, tener α_1 cerrado significa que r vuelve a su lugar, o sea, $\Phi_a([\gamma])(r) = r$. Esto implica que $\Phi_a([\gamma]) = id$ y esto demuestra la proposición para el caso $N = 1$.
Paso 2. $N \geq 2$. Como $[\gamma]$ es $N-$conmutador, entonces $[\gamma]$ es $2-$conmutador. Podemos repetir el paso 1, pero esta vez asumir que γ_1 y γ_2 son $1-$conmutadores.

Repitiendo los argumentos del paso 1 para α_j $(j = 1, 2)$ en lugar de γ tendremos que α_1^j $(j = 1, 2)$ es cerrado.
Observe que

$$\begin{aligned} p_2(\gamma, \alpha_1) &= p_2(\gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}, \alpha_1^1\alpha_2^2(\alpha_1^1)^{-1}(\alpha_1^2)^{-1}) \\ &= p_2(\gamma_1, \alpha_1^1)p_2(\gamma,\alpha_1^2)p_2(\gamma_1^{-1}, (\alpha_1^1)^{-1})p_2(\gamma_2^{-1}, (\alpha_1^2)^{-1}) \\ &= p_2(\gamma_1, \alpha_1^1)p_2(\gamma,\alpha_1^2)[p_2(\gamma_1, \alpha_1^1)]^{-1}[p_2(\gamma_2, \alpha_1^2)]^{-1} \end{aligned}$$

y en esta expresión los caminos $p_2(\gamma_1, \alpha_1^1)$ y $p_2(\gamma,\alpha_1^2)$ son cerrados. Entonces el camino $p_2(\gamma, \alpha_1)$ es $1-$conmutador y de nuevo por el lema 4.19, ya que $\alpha_2^{k_2} = p_2(\gamma, \alpha_1)$ tendremos que α_2 es camino cerrado. Si $N = 2$, entonces $\alpha_N = \alpha_2$ sería cerrado y la proposición estaría demostrada. Si $N \geq 3$ seguimos con el paso 3.
Paso 3. $N \geq 3$. $[\gamma]$ es $3-$conmutador. Esta vez tendremos que γ_1, γ_2 son $2-$conmutadores. repitiendo el paso 2 con γ_1 y γ_2 en lugar de γ obtenemos que α_2^1 y α_2^2 son cerrados. Luego

$$p_3(\gamma, \alpha_1, \alpha_2) = p_3(\gamma_1, \alpha_1^1, \alpha_2^1)p_3(\gamma_2, \alpha_1^2, \alpha_2^2)[p_3(\gamma_1, \alpha_1^1, \alpha_2^1)]^{-1}[p_3(\gamma_2, \alpha_1^2, \alpha_2^2)]^{-1}$$

es $1-$conmutador y por lo tanto α_3 es cerrado. Si $N = 3$, acabó. Caso contrario, podemos proseguir un número finito de pasos hasta demostrar que α_N es cerrado. $\square$

Observación 4.21. *El lema 4.19 requiere que el camino $\gamma = \gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}$ este en $\mathbb{C}^*$. Sin embargo, nosotros lo hemos aplicado sin ninguna preocupación. Como lo que queríamos demostrar es que cada α_j es un camino cerrado, cuando no se puede aplicar el lema 4.19 es porque α_j es constante igual a cero y por lo tanto también es cerrado.*

Considere $\alpha \in A_5$. Por aplicaciones sucesivas del teorema 1.13 tenemos que α es $n-$conmutador $\forall\, n \in \mathbb{N}$.

Proposición 4.22. *Para todo $n \in \mathbb{N}$, existe un $n-$conmutador $[\gamma] \in \pi_1(\mathcal{S}, 0)$ tal que $\Phi_0([\gamma]) = \alpha$.*

Demostración. Como α es $1-$conmutador, entonces

$$\alpha = \alpha_1\alpha_2\alpha_1^{-1}\alpha_2^{-1},\ \alpha_1,\ \alpha_2 \in A_5$$

. Por el teorema 4.15 Φ_0 es sobreyectiva, entonces existen $[\gamma_1], [\gamma_2] \in \pi_1(\mathcal{S}, 0)$ tal que $\Phi_0([\gamma_j]) = \alpha_j\,(j = 1, 2)$. Luego $\gamma = \gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}$ es

$1-$conmutador y es tal que $\Phi_0([\gamma]) = \alpha$. Por lo tanto la proposición vale para $n = 1$. Suponga que la proposición vale para $n = k$. Como α es $(k+1)-$conmutador,existen $\alpha_1, \alpha_2 \in A$, $k-$conmutadores tal que $\alpha = \alpha_1\alpha_2\alpha_1^{-1}\alpha_2^{-1}$. Por la hipótesis inductiva existen $k-$conmutadores $\gamma_1, \gamma_2 \in \pi_1(\mathcal{S}, 0)$ tal que
$\Phi_0([\gamma_j]) = \alpha_j\,(j = 1, 2)$. Luego, $\gamma = \gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}$ es un $(k+1)-$conmutador tal que $\Phi_0([\gamma]) = \alpha$. □

4.3. Demostración del Teorema Principal

Ver teorema 2.6. Fije $\alpha \in A_5$ tal que $\alpha \neq id$. Por la proposición 4.22 existe $[\gamma] \in \pi_1(\mathcal{S}, 0)$ tal que $[\gamma]$ es $N-$conmutador y $\Phi_0([\gamma]) = \alpha$. Luego, por la proposición 4.20 tendremos que $\Phi_0([\gamma]) = id$, lo que es una contradicción.

Bibliografía

[1] Dmitry Fuchs Serge Tabachnikov *Mathematical Omnibus: Thirty Lectures on Classic Mathematics* Departament of mathematics University of California, Davis, CA 95616.
Departament of mathematics, Penn State University, University Park, PA 16802.

[2] Serge Lang *ALGEBRA* Departament of mathematics Yale University New Haven, CT, 96520.

[3] John B. Fraleig *Algebra Abstracta.* Departament of mathematics University of Rhode Island, 1982.

[4] Elon Lages Lima. *Curso de Análise Volumen 2.* Instituto de Matemática Pura y Aplicada, 1981.

[5] I. N. Herstein. *Algebra Moderna.* Editorial Trillas- Traducido al Español Federico Velasco Coba, 1988.

[6] Serge Lang. *Complex Analysis.* Fourth Edition, Springer.

[7] Jean-Pierre Tignol. *Galois'Theory of Algebraic Equations.* Université Catholique de Louvain, Belgium, 2001.

[8] José Mnuel Sanchez Muñoz. *Historias de matemáticas Abel y la imposibilidad de resolver la "quíntica" por radicales.* Revista de Investigación Pensamiento Matemático, 2011.

[9] Réal Gélinas/ Marcel Lambert. *ÉLÉMENTS D'ANALYSE COMPLEXE.* Presses de I'Université du Québec, 1994.

[10] Ministerio de Educación Pública. *Ecuaciones de segundo grado en la antigüedad.* Reforma de la Educación Matemática en Costa Rica. www.reformamatematica.net

[11] THE GREEK TEXT OF J.L. HEIBERG (1883-1885) *EUCLID´S ELEMENTS OF GEOMETRY.* from Euclidis Elementa, editit et Latine Interpretatus est I.L. Heiberg, in aedibus B.G. Teubneri, 1883-1885 edited, and provided whit a modern English translation, by Richard Fitzpatrick.

[12] GABRIEL VILLA SALVADOR. *Las ecuaciones polinomiales como el origen de la teoría de Galois.* Departamento de control automático, 2011.

[13] CARLOS IVORRA. *Las fórmulas de Cardano-Ferrari.* http://www.uv.es/ivorra

[14] TAMURA I. *Topology of Foliations: An Introduction.* American Mathematical Society, 1992.

[15] WALSH J. *The Dynamics of Circle Homeomorphism: A Hands-on Introduction.* Mathematics Magazine, Vol.72, Nº 1, pp.3-13, 1999.

[16] YOCCOZ J. *Conjugaison différentiable des difféomorphismes du cercle dont le nombre de rotation vérifie une condition diophantienne.* Annales scientifiques de l'É.N.S 4ª Serie, tome 17, nº3, p.333-359, 1984.

[17] ALINA OSTAFE *Hilbert's Nullstellensatz* Seminar Computational Algebra 15.04.2008

Índice alfabético