Miscelánea Matemática **67** (2018) 23-41 SMM

Configuraciones, trenzas y el teorema de Abel-Ruffini

Rita Jiménez Rolland
Instituto de Matemáticas, Universidad Nacional Autónoma de México, Oaxaca de Juárez, Oaxaca, México 68000
rita@im.unam.mx y
Manuel Valdespino
Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México, Morelia, Michoacán, México 58089
mavb256@gmail.com

Resumen

El teorema de Abel–Ruffini afirma que no existe una combinación finita de sumas, restas, productos, cocientes y radicales que solucionen la ecuación algebraica general de grado mayor o igual a 5. Entre 1963 y 1964, V. I. Arnold presentó, en un curso para estudiantes de preparatoria en Moscú, una prueba de este resultado usando métodos topológicos. En este artículo panorámico revisamos la prueba de Arnold haciendo énfasis en su relación con los espacios de configuraciones y grupos de trenzas. Estudiamos cómo las trenzas inducen permutaciones de las raíces de un polinomio y qué información nos dan sobre la solubilidad por radicales de una ecuación polinomial.

Introducción

Desde hace más de 4000 años los babilonios ya conocían la solución a la ecuación general de grado 2. No fue sino hasta el siglo XVI que del

Palabras clave: polinomios, solución de ecuaciones algebraicas, teorema de Abel–Ruffini, grupo fundamental, monodromía, superficies de Riemann, espacios cubrientes, espacios de configuraciones, grupo de trenzas.

Ferro, Tartaglia, Cardano y Ferrari[1] dieron las soluciones de las ecuaciones generales de grado 3 y 4. Por muchos años se buscó una solución general por radicales para el polinomio de grado 5. En 1799 Paolo Ruffini presentó una prueba de la no existencia de dicha solución, pero su prueba no fue aceptada por la comunidad matemática de la época. Finalmente en 1824 Niels Henrik Abel demostró[2] que tales soluciones no existen para las ecuaciones generales de grado mayor que 4, resultado que ahora se conoce como el *teorema de Abel–Ruffini*. Como escribe Vladimir Igorevich Arnold en el prefacio de [2]:

> El teorema de Abel, que afirma que no existe una combinación finita de radicales y funciones racionales que solucionen la ecuación algebraica genérica de grado 5 (o mayor que 5), es uno de los primeros y más importantes resultados de imposibilidad en matemáticas.

Las nociones de grupo abeliano y grupo soluble se originaron a partir de este contexto. Más tarde, Évariste Galois dio las bases de una nueva teoría la cual generalizó el teorema de Abel–Ruffini, dando condiciones necesarias y suficientes para que un polinomio tuviera una solución por radicales. Este enfoque es el que tradicionalmente se sigue en un primer curso de teoría de Galois, detalles del mismo pueden encontrarse, por ejemplo, en [16, 3.66].

Entre 1963 y 1964 Arnold presentó una prueba del teorema de Abel–Ruffini (para el caso complejo), en un curso para estudiantes de preparatoria en Moscú, usando métodos topológicos. V.B. Alekseev fue uno de los alumnos que asistió a este y publicó sus notas del curso en [2], una referencia autocontenida que nos lleva de la mano mediante una serie de problemas y soluciones.

La idea fundamental de Arnold es el estudio de la *monodromía* de funciones algebraicas: entender cómo se comportan las soluciones de ecuaciones polinomiales cuando circundan una singularidad. En este artículo repasamos la prueba de Arnold haciendo énfasis en su relación con espacios de configuraciones y grupos de trenzas. En nuestra exposición aprovechamos para introducir las nociones de grupo fundamental, espacio cubriente, superficie de Riemann y grupo de monodromía.

Al considerar el espacio de polinomios de un grado dado, los polinomios que llamaremos *singulares* corresponden a aquellos polinomios que tienen raíces repetidas. Para circundar estos puntos singulares tomamos lazos de polinomios sin raíces repetidas basados en un polinomio

[1]La historia alrededor de estas fórmulas esta llena de intrigas. Recomendamos el artículo *Las ecuaciones polinomiales como el origen de la teoría de Galois* [17] para más detalles sobre la historia sobre la solución de la ecuación cúbica y el teorema de Abel–Ruffini.

[2]Véase el artículo *La demostración de Abel* [14] para un bosquejo de la prueba de Abel y una descripción de su contexto histórico.

fijo. Estos lazos corresponden a elementos del grupo fundamental de un *espacio de configuraciones*, concretamente, a *trenzas*. Estudiando cómo esas trenzas permutan las raíces de un polinomio base, podemos obtener información sobre la solubilidad por radicales de una ecuación polinomial.

Al final de la prueba de Arnold se concluye que la razón por la que no existe una solución por radicales para la ecuación general de grado mayor o igual a 5, es la misma que se obtiene después de un curso de teoría de Galois: el grupo simétrico S_n no es *soluble* cuando $n \geq 5$. Es decir, podemos tomar conmutadores anidados no triviales de longitud arbitrariamente grande.

Esperamos que el enfoque presentado aquí ilustre el porqué de este resultado y motive al lector a estudiar con más profundidad los temas discutidos.

1. Solución de ecuaciones polinomiales

Nos interesa estudiar la solución de una ecuación algebraica general de grado n con coeficientes complejos

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

Puesto que estamos buscando soluciones de ecuaciones, podemos suponer que el coeficiente principal de los polinomios es $a_n = 1$, tales polinomios se denominan mónicos.

El teorema fundamental del álgebra nos dice que todo polinomio con coeficientes en $\mathbb{C}$ de grado n tiene exáctamente n raíces, contando multiplicidades. En consecuencia la ecuación algebraica (1) no define una sola función solución, sino lo que se llama una *función multivaluada*. Usaremos la notación $f : A \twoheadrightarrow B$ para denotar una función multivaluada f que a cada elemento del dominio A puede asignar uno o más elementos del contradominio B.

Una *función algebraica en n-variables* se define como una función multivaluada $z = f(a_0, \ldots, a_{n-1})$ con contradominio $\mathbb{C}$, que satisface una ecuación polinomial de $n+1$-variables

$$P(z, a_0, \ldots, a_{n-1}) = 0.$$

La solución de la ecuación algebraica general (1) es un ejemplo de lo que se conoce como función algebraica. En nuestro caso,

$$P(z, a_0, \ldots, a_{n-1}) = z^n + a_{n-1} z^{n-1} + \ldots a_1 z + a_0 = 0.$$

Por ejemplo, para la ecuación general de grado 2

$$P(z, a_0, a_1) = z^2 + a_1 z + a_0 = 0$$

la solución viene dada por la fórmula general que aprendemos en secundaria

$$z = f(a_0, a_1) = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2}. \tag{2}$$

En la fórmula (2), $\sqrt{\cdot} : \mathbb{C} \twoheadrightarrow \mathbb{C}$ es la función multivaluada[3] que asigna a cada $x = re^{i\theta} \neq 0$ sus dos raíces cuadradas $r^{1/2}e^{\frac{\theta}{2}i}$ y $r^{1/2}e^{\frac{\theta+2\pi}{2}i}$ y tal que $\sqrt{x} = 0$ cuando $x = 0$. Notemos que la función algebraica $z = f(a_0, a_1)$ toma exactamente dos valores cuando el *discriminante* $\Delta(a_0, a_1) = a_1^2 - 4a_0 \neq 0$. Los polinomios mónicos de grado 2 sin raíces repetidas están parametrizados por los coeficientes (a_0, a_1) en $\mathbb{C}^2 \backslash V(\Delta)$, donde

$$V(\Delta) = \{\, (a_0, a_1) \in \mathbb{C}^2 \mid \Delta(a_0, a_1) = 0 \,\}.$$

Los polinomios parametrizados por $V(\Delta)$ son los polinomios que tienen raíces repetidas.

Para un grado n fijo, la solución $z = f(a_0, a_2, \ldots, a_{n-1})$ de la ecuación general (1) toma exactamente n valores distintos cuando el polinomio

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

no tiene raíces repetidas.

El *discriminante*[4] de un polinomio $p(z)$ es un polinomio $\Delta(a_0, a_1, \ldots, a_{n-1})$ no constante en los coeficientes de $p(z)$, que es igual a cero si y solo si el polinomio tiene raíces múltiples en el plano complejo. Así pues, los polinomios mónicos de grado n con raíces repetidas están parametrizados por los coeficientes $(a_0, \ldots, a_{n-1})$ en

$$V(\Delta) = \{(a_0, \ldots, a_{n-1}) \in \mathbb{C}^n \mid \Delta(a_0, \ldots, a_{n-1}) = 0\}$$

y la solución general $z = f(a_0, a_2, \ldots, a_{n-1})$ es una función multivaluada que en $\mathbb{C}^n \setminus V(\Delta)$ toma exactamente n valores. Escribimos

$$f : \mathbb{C}^n \setminus V(\Delta) \twoheadrightarrow \mathbb{C}.$$

Observemos que en grado 2, la solución $z = f(a_0, a_1)$ se expresa con una fórmula, en términos de los coeficientes del polinomio, con un número finito de operaciones algebraicas como la suma, resta, multiplicación, división y radicales. Las fórmulas de Ferrari, Tartaglia y Cardano para grado 3 y 4 también son de esta forma[5]. Se dice que la ecuación (1) es *soluble por radicales* para $n \leq 4$. Por muchos años se buscó una solución por radicales para el polinomio general de grado $n \geq 5$. El teorema de Abel–Ruffini dice que una solución por radicales no puede existir cuando $n \geq 5$:

[3] Observe que $y = \sqrt{x}$ es la función algebraica en una variable que satisface la ecuación algebraica $P(y, x) = y^2 - x = 0$.

[4] Para obtener el discriminante Δ de $p(z)$ calculamos el *resultante* de p y p_z (la derivada de p con respecto a z). Para la definición del resultante de dos polinomios, así como propiedades de este puede consultarse [16, p. 82].

[5] Las cuales se pueden encontrar, por ejemplo, en [16, p. 139].

Teorema 1.1 (**Abel–Ruffini**). *La ecuación general de grado $n \geq 5$ no es soluble por radicales. Es decir, no existe una fórmula para expresar las raíces de dicha ecuación, en términos de los coeficientes, por medio de la combinación finita de sumas, restas, multiplicaciones, divisiones y radicales.*

2. Entra la topología: espacios cubrientes

A una función algebraica le podemos asociar lo que se llama un *espacio cubriente*. Esto nos permite estudiar, como lo hizo Arnold, la solubilidad de ecuaciones algebraicas desde una perspectiva topológica. Primero veamos qué sucede en el caso de funciones algebraicas de una variable.

Consideremos una función algebraica $z = f(w)$ en una variable definida por una ecuación polinomial

$$P(z, w) = z^n + a_{n-1}(w)z^{n-1} \cdots + a_0(w) = 0, \tag{3}$$

donde los coeficientes $a_i(w)$ son polinomios en w con coeficientes complejos. Veamos cómo asociarle a esta función algebraica un espacio topológico $\widetilde{X}$.

Empezamos por remover los puntos $w \in \mathbb{C}$ tales que el polinomio $P(z, w)$ en z tiene raíces repetidas, es decir, quitamos los puntos w tales que el discriminante $\Delta(w) := \Delta(a_0(w), a_1(w), \ldots a_{n-1}(w)) = 0$. Para ser consistentes con la notación anterior consideramos el conjunto finito $V(\Delta) = \{w \in \mathbb{C} \mid \Delta(w) = 0\}$. Así, un punto a en el conjunto abierto

$$X := \mathbb{C} \setminus V(\Delta)$$

corresponde a un polinomio $P(z, a)$ en z que tiene exactamente n raíces distintas $\{z_1, \ldots, z_n\}$. Para estas raíces tenemos que $P(z_k, a) = 0$, y la derivada con respecto a z satisface $P_z(z_k, a) \neq 0$ (¿por qué?). Por el teorema de la función implícita[6], la ecuación $P(z, w) = 0$ determina no solo una función solución, sino n funciones $f_{a,1}(w), f_{a,2}(w), \ldots, f_{a,n}(w)$ definidas en un disco abierto U_a centrado en a: las *ramas locales de la función f*.

A la función algebraica f definida por la ecuación (3) le asociamos el subespacio topológico[7] de $\mathbb{C}^2$ definido como sigue:

$$\widetilde{X} = \{(z, w) \in \mathbb{C}^2 : P(z, w) = 0, w \in X\}.$$

El espacio $\widetilde{X}$ tiene asociadas dos proyecciones continuas:

$$\tilde{f} : \widetilde{X} \to \mathbb{C}, \text{ dada por } (z, w) \mapsto z,$$

[6] Ver por ejemplo [18, p. 86] para el caso de polinomios en dos variables, y [8, p. 11] para el caso en varias variables.

[7] Se considera $\mathbb{C}^2$ como $\mathbb{R}^4$ con la topología que induce la métrica euclidiana.

$$\pi : \widetilde{X} \to X \text{ dada por } (z, w) \mapsto w.$$

La proyección $\pi : \widetilde{X} \to X$ es sobreyectiva. Más aún, como vimos antes, para cada $a \in X$ la preimagen $\pi^{-1}(a)$, llamada *la fibra de* π *sobre* a, consiste de n puntos distintos

$$\{(z_1, a), (z_2, a), \ldots, (z_n, a)\},$$

donde $\{z_1, z_2, \ldots, z_n\}$ son las n raíces distintas de $P(z, a) = 0$. La función $\tilde{f}$ manda a cada punto $(z_k, a) \in \pi^{-1}(a)$ en z_k, donde z_k es el valor de la rama local $f_{a,k}$ de la función f evaluada en a. Podemos pensar en $\tilde{X}$ como un nuevo dominio «más grande» para el que la función $\tilde{f}$ es univaluada. La relación entre las funciones está dada por el diagrama:

$$\begin{array}{ccc} \widetilde{X} & \xrightarrow{\tilde{f}} & \mathbb{C} \\ \downarrow{\scriptstyle \pi} & \nearrow_{f} & \\ X & & \end{array} \tag{4}$$

Para cada $a \in X$, podemos escoger un disco abierto $U_a \subset X$ dominio común de las ramas locales $f_{a,1}, \ldots, f_{a,n}$ de f y definir

$$\widetilde{U}_{a,k} = \{(z, w) \in \mathbb{C}^2 : z = f_{a,k}(w), w \in U_a\} \text{ para } k = 1, 2, \ldots, n.$$

Cada $\widetilde{U}_{a,k}$ es homeomorfo al disco U_a bajo π y es posible escoger U_a de manera que $\widetilde{U}_{a,k} \cap \widetilde{U}_{a,h} = \varnothing$ si $k \neq h$ (¿por qué?). De este modo, tenemos que

$$\pi^{-1}(U_a) = \bigsqcup_{k=1}^{n} \widetilde{U}_{a,k}.$$

Intuitivamente, podemos pensar en los conjuntos abiertos $\widetilde{U}_{a,k}$ como n «rebanadas» disjuntas, homeomorfas a U_a, que la función π proyecta en el conjunto abierto U_a.

A un espacio topológico $\widetilde{X}$ junto con una función continua $\pi : \widetilde{X} \to X$ que cumple las propiedades antes descritas se le llama un *espacio cubriente* de X. En nuestro caso $|\pi^{-1}(a)| = n$ es finito y decimos que $\pi : \widetilde{X} \to X$ es una *función cubriente de n-hojas*. [7] y [12] son referencias estándares para el estudio de espacios cubrientes y sus propiedades, así como las nociones de grupo fundamental y monodromía a tratar en la siguiente sección.

Resulta que la construcción anterior es válida para funciones algebraicas de n-variables y podemos asociar a la función algebraica definida por (1) un espacio cubriente de n-hojas

$$\pi : \tilde{X} \to \mathbb{C}^n \setminus V(\Delta).$$

En este caso, la fibra sobre $\bar{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{C}^n \setminus V(\Delta)$ corresponde a las n raíces distintas del polinomio $P(z, \bar{a}) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$.

El espacio topológico $\widetilde{X}$ asociado a una función algebraica f en una variable definida por una ecuación polinomial $P(z,w)=0$ es localmente homeomorfo al plano. Cuando el polinomio $P(z,w)$ es irreducible, $\widetilde{X}$ es conexo y una compactación apropiada nos da lo que se conoce como la *superficie de Riemann* asociada a la función algebraica f. Para una introducción a superficies de Riemann, recomendamos al lector el artículo panorámico [11]. Para ver los detalles de esta construcción y los prerrequisitos véase [13] y [18]. Terminamos esta sección con el siguiente ejemplo:

El espacio cubriente asociado a la raíz n-ésima. Consideremos el caso de la función algebraica en una variable $z=f(w)$ determinada por la ecuación polinomial $P(z,w)=z^n-w=0$.

El único punto $a\in\mathbb{C}$ para el cual $P(z,a)=z^n-a$ tiene raíces repetidas es $a=0$, por lo que $X=\mathbb{C}\setminus V(\Delta)=\mathbb{C}\setminus\{0\}$. La función algebraica f es una función multivaluada, la raíz n-ésima

$$\sqrt[n]{\cdot}:\mathbb{C}\setminus\{0\}\twoheadrightarrow\mathbb{C}$$

que a cada $a\in\mathbb{C}\setminus\{0\}$ le asigna sus n raíces n-ésimas distintas:

$$z_k=|a|^{1/n}e^{\left(\frac{\mathrm{Arg}(a)+2k\pi}{n}i\right)}\quad\text{para}\quad k=1,2,\ldots,n.^{8}$$

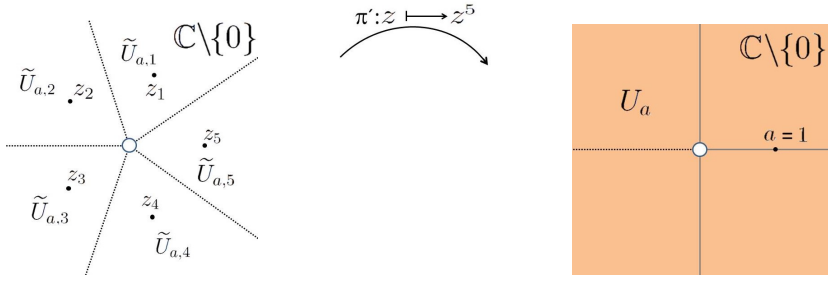


Figura 1. El espacio cubriente asociada a la raíz quíntica. La fibra sobre $a=1$ es el conjunto $\pi^{-1}(a)=\{z_1,z_2,z_3,z_4,z_5\}$ de raíces quínticas de la unidad. La imagen inversa bajo π del abierto $U_a=\mathbb{C}\setminus\{z\in\mathbb{C}:\mathrm{Re}(z)\leq 0,\mathrm{Im}(z)=0\}$ es la unión disjunta de las «rebanadas» $\widetilde{U}_{a,1},\widetilde{U}_{a,2},\widetilde{U}_{a,3},\widetilde{U}_{a,4}$ y $\widetilde{U}_{a,5}$.

Como antes, sea $\widetilde{X}=\{(z,w)\in\mathbb{C}^2:z^n-w=0,w\in X\}$ con las proyecciones $\tilde{f}$ y π. El espacio cubriente $\pi:\widetilde{X}\to X$ tiene n hojas, pues la fibra de π sobre $a\in X$ es $\pi^{-1}(a)=\{(a,z_1),\ldots,(a,z_n)\}$, que corresponde precisamente al conjunto de raíces n-ésimas de $a\neq 0$.

[8]Donde $\mathrm{Arg}:\mathbb{C}\setminus\{0\}\to(-\pi,\pi]$ es la rama principal del argumento.

$$\begin{array}{ccc} \widetilde{X} & \overset{\tilde{f}}{\underset{h}{\rightleftarrows}} & \mathbb{C}\setminus\{0\} \\ \downarrow{\scriptstyle \pi} & \swarrow{\scriptstyle \pi'} & \\ \mathbb{C}\setminus\{0\} & & \end{array} \tag{5}$$

Resulta que la función $\tilde{f}$ es un homeomorfismo en su imagen $\mathbb{C}\setminus\{0\}$, cuya función inversa $h : \mathbb{C}\setminus\{0\} \to \widetilde{X}$ está dada por $z \mapsto (z, z^n)$. Así pues, podemos pensar en $\mathbb{C}\setminus\{0\}$ como el espacio cubriente $\widetilde{X}$ asociado a la raíz n-ésima con función cubriente la composición $\pi' := \pi \circ h : \mathbb{C}\setminus\{0\} \to \mathbb{C}\setminus\{0\}$ que está dada por $z \mapsto z^n$ y que «enrolla» n veces el plano complejo sin el origen (véase figura (1)).

3. Monodromía: circundando singularidades

La idea fundamental de Arnold en su prueba del teorema de Abel–Ruffini es el estudio de la *monodromía* de funciones algebraicas: entender cómo se comportan las soluciones de ecuaciones polinomiales cuando circundan una singularidad.

Para rodear singularidades de los espacios topológicos de interés tomaremos caminos que inician y terminan en el mismo punto. Si X es un espacio topológico, un *camino en* X es una función continua del intervalo $[0, 1]$ en X. Un *lazo basado en el punto* $\mathbf{x_0}$ *en* X es un camino en X que inicia y termina en el punto $\mathbf{x_0}$.

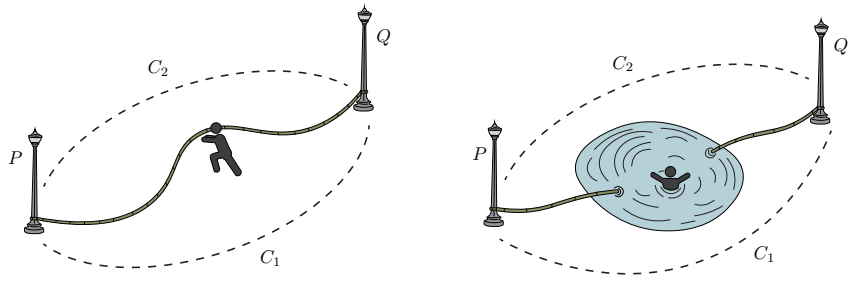


Figura 2. En (a) los caminos C_1 y C_2 son homotópicos. En (b), el camino C_1 no se puede deformar continuamente en el camino C_2. Fuente: Imagen elaborada por Raymundo Iván González Ballesteros (basada en [10, p. 39]).

Dos lazos se consideran *homotópicos* si se pueden deformar continuamente el uno en el otro sin mover el punto base, es decir si existe lo que

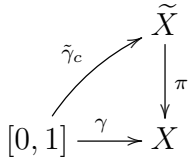
se llama una *homotopía de caminos*[9] entre ellos. La clase de homotopía de un lazo γ se denota como $[\gamma]$. Más aún, dos lazos basados τ y μ se pueden multiplicar para obtener un nuevo lazo basado $\tau * \mu$ vía concatenación: se recorre el primer lazo y luego el segundo, duplicando la velocidad de recorrido. Puede demostrarse que este producto está bien definido en clases de homotopía, es asociativo, toda clase de equivalencia tiene un inverso (verifica que $[\gamma]^{-1} = [\bar{\gamma}]$, donde $\bar{\gamma}(t) = \gamma(1-t)$ para $t \in [0,1]$) y existe un elemento neutro que corresponde a la clase de homotopía del lazo constante $e(t) = \mathbf{x_0}$ para todo $t \in [0,1]$.

Al conjunto de clases de homotopía de lazos basados con el producto anterior se le llama el *grupo fundamental de X basado en $\mathbf{x_0}$* y se denota por $\pi_1(X, \mathbf{x_0})$. Este grupo determina si dos lazos basados pueden o no deformarse uno en otro y proporciona información básica sobre la forma del espacio topológico X. Es un *invariante topológico*: dos espacios topológicos homeomorfos tienen el mismo grupo fundamental.

Sea $\mathbf{x_0} = 1 \in \mathbb{C}$. No es difícil ver que $\pi_1(\mathbb{C}, \mathbf{x_0})$ es el grupo trivial, pues todos los lazos en $\mathbb{C}$ pueden deformarse continuamente al lazo trivial. Menos evidente es el hecho de que $\pi_1(\mathbb{C} \setminus \{0\}, \mathbf{x_0}) \cong \mathbb{Z}$ y está generado por el lazo que da una vuelta al origen $\gamma : [0,1] \to \mathbb{C}\setminus\{0\}$ dado por $\gamma(t) = e^{-2\pi i t}$, $t \in [0,1]$ (véase figura 3). En estos ejemplos, el grupo fundamental refleja que el espacio $\mathbb{C}$ no tiene «agujeros», mientras que $\mathbb{C} \setminus \{0\}$ tiene un «agujero», el punto $\{0\}$.

Consideremos ahora un espacio cubriente $\pi : \widetilde{X} \to X$ de n-hojas, con X un espacio conexo por trayectorias, y $\mathbf{x_0} \in X$. La *fibra* de π sobre $\mathbf{x_0}$ es el conjunto $F = \pi^{-1}(\mathbf{x_0})$ que consiste de n puntos en $\tilde{X}$ que se proyectan a $\mathbf{x_0}$ bajo π. Existe una acción del grupo $\pi_1(X, \mathbf{x_0})$ en la fibra F sobre $\mathbf{x_0}$ que a continuación describimos.

Sea $\gamma : I \to X$ un lazo basado en $\mathbf{x_0}$ y tomemos $c \in F$. Una de las propiedades fundamentales de los espacios cubrientes es que «levantan» caminos a $\widetilde{X}$ de manera única salvo por el punto inicial, es decir, existe un único camino $\tilde{\gamma}_c : [0,1] \to \tilde{X}$ con punto inicial $\tilde{\gamma}_c(0) = c$ tal que el siguiente diagrama conmuta:



Puesto que $\pi(\tilde{\gamma}_c(1)) = \gamma(1)$, el punto final del camino $\tilde{\gamma}_c$ no es necesariamente c, pero debe pertenecer a la fibra F de $\mathbf{x_0}$. Es decir, cada lazo γ induce una permutación de los elementos de la fibra F dada por

[9] Una *homotopía de caminos* entre dos caminos $\alpha, \beta : [0,1] \to X$ en X que van del punto p al punto q es una función continua $H : [0,1] \times [0,1] \to X$ tal que $H(0,t) = \alpha(t)$ y $H(1,t) = \beta(t)$ para todo $t \in [0,1]$, $H(s,0) = p$ y $H(s,1) = q$ para todo $s \in [0,1]$.

$\sigma_\gamma : c \mapsto \tilde{\gamma}_c(1)$. Resulta que este punto final solo depende de la clase de γ en $\pi_1(X, \mathbf{x_0})$ y se obtiene una acción derecha $c \cdot [\gamma] = \tilde{\gamma}_c(1)$ (y en consecuencia una acción izquierda[10]) bien definida de $\pi_1(X, \mathbf{x_0})$ en la fibra F.

Al homomorfismo $\phi_\pi : \pi_1(X, \mathbf{x_0}) \to \mathrm{Aut}(F)$ correspondiente a la acción izquierda anterior se le llama la *monodromía del espacio cubriente* y la imagen de este homomorfismo es el *grupo de monodromía de* π. Observemos que como la fibra F tiene n elementos, el grupo de monodromía es un subgrupo del grupo simétrico $S_n \cong \mathrm{Aut}(F)$.

En el caso del espacio cubriente asociado a una función algebraica de una variable, el levantamiento de un camino corresponde a lo que se llama la *continuación analítica* de la función a largo del camino. Para profundizar sobre el tema se recomienda [13] y [20].

Monodromía de funciones racionales. Consideremos una función algebraica de una variable $z = f(w)$ determinada por la ecuación $h(w)z - g(w) = 0$, con g, h polinomios. Luego

$$z = f(w) = \frac{g(w)}{h(w)}$$

es una función racional (¡no es multivaluada!) y la función cubriente asociada $\pi : \tilde{X} \to X$ es inyectiva. El grupo de monodromía es trivial: no hay permutaciones no triviales de un conjunto de un punto.

Monodromía de la raíz n-ésima. En la sección anterior vimos que la función multivaluada $\sqrt[n]{\cdot} : \mathbb{C} \setminus \{0\} \twoheadrightarrow \mathbb{C}$ tiene asociado un espacio cubriente de n-hojas $\pi' : \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$ dado por $z \mapsto z^n$. Los puntos en la fibra F de π' sobre $\mathbf{x_0} = 1$ son a las raíces n-ésimas de la unidad $\{z_1, z_2 \ldots, , z_n\}$, donde $z_k = e^{2k\pi i/n}$ para $k = 1, 2, \ldots, n$. Identificando a la fibra F con $\{1, \ldots, n\}$ vía $z_k \mapsto k$, es claro que el grupo de automorfismos de la fibra $\mathrm{Aut}(F)$ es isomorfo a S_n.

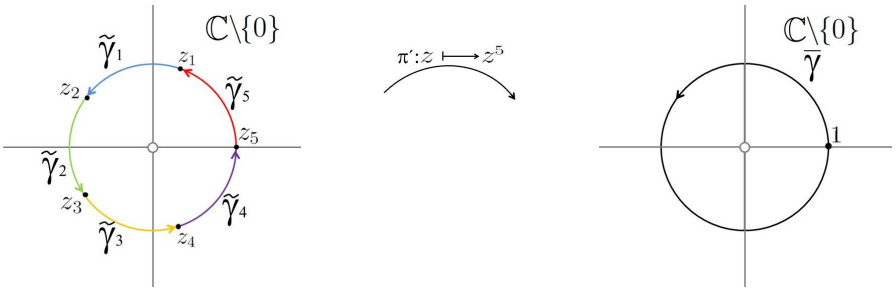


Figura 3. Levantamientos $\tilde{\gamma}_1, \tilde{\gamma}_2, \tilde{\gamma}_3, \tilde{\gamma}_4$ y $\tilde{\gamma}_5$ del lazo $\bar{\gamma}$ basado en $\mathbf{x_0} = 1$ en el espacio cubriente $\pi' : \tilde{X} \to X$ asociado a la raíz quíntica.

[10] Recordemos que dada una acción derecha de un grupo G en un conjunto F, podemos definir una acción izquierda de G en F: $g \cdot a = a \cdot g^{-1}$, $g \in G$, $a \in F$.

Para obtener el grupo de monodromía de este espacio cubriente consideremos el lazo γ basado en $\mathbf{x_0} = 1$ dado por $\gamma(t) = e^{-2\pi it}$ con $t \in [0,1]$. Este lazo le da una vuelta al 'agujero' $V(\Delta) = \{0\}$. Para enteder cómo actúa $[\gamma]$ en la fibra F (por la izquierda), consideramos $[\gamma]^{-1} = [\bar{\gamma}]$, donde $\bar{\gamma}(t) = e^{2\pi it}$ con $t \in [0,1]$. Para $k = 1, 2, \ldots, n$, el levantamiento de $\bar{\gamma}$ que inicia en z_k está dado por $\tilde{\gamma}_k(t) = z_k\bar{\gamma}(\frac{t}{n})$, con $t \in [0,1]$ (véase figura (3)). Observemos que $\bar{\gamma}(\frac{1}{n}) = z_1$ y que $z_k z_1 = z_{k+1}$, así que $\tilde{\gamma}_k(1) = z_k z_1 = z_{k+1}$. Luego, el lazo γ induce la permutación en las n-raíces de la unidad dada por: $z_1 \mapsto z_2 \mapsto \ldots \mapsto z_n \mapsto z_1$. Es decir, la monodromía $\phi_\pi : \pi_1(\mathbb{C} \setminus \{0\}, \mathbf{x_0}) \to S_n$ manda la clase de homotopía $[\gamma]$ en el n-ciclo $(1\ 2\ \ldots\ n) \in S_n$. Puesto que $[\gamma]$ genera a $\pi_1(\mathbb{C} \setminus \{0\}, \mathbf{x_0})$, el grupo de monodromía de la raíz n-ésima es $Im(\phi_\pi) = \langle (1\ 2\ \ldots\ n) \rangle \cong \mathbb{Z}_n$.

Notemos que en este ejemplo para que un lazo induzca permutaciones no triviales de las raíces es necesario, mas no suficiente, que el número total de vueltas alrededor de una singularidad sea distinto de cero. Si el número total de vueltas es cero, entonces el lazo es homotópico al lazo trivial (¿por qué?) y por ende induce la permutación trivial de los elementos de la fibra.

4. Configuraciones, trenzas y polinomios

Regresemos a la ecuación algebraica general de grado n. Queremos movernos en el espacio de polinomios circundando los polinomios singulares, aquellos con raíces repetidas parametrizados por sus coeficientes en $V(\Delta)$, y entender cómo se permutan las soluciones.

En concreto, nos interesa entender el grupo de monodromía del espacio cubriente $\pi : \tilde{X} \to \mathbb{C}^n \setminus V(\Delta)$ de n hojas asociado a la función algebraica definida por (1). Como lo hicimos en la sección anterior, nos interesa primero obtener el grupo fundamental del espacio

$$\mathbb{C}^n \setminus V(\Delta) = \{p(z) \in \mathbb{C} : p(z) \text{ es mónico de grado } n \text{ sin raíces repetidas}\},$$

pues los lazos de polinomios en este espacio circundan los polinomios singulares de $V(\Delta)$. Resulta que es más fácil entender y visualizar estos lazos si pensamos en el espacio $\mathbb{C}^n \setminus V(\Delta)$ como un espacio de configuraciones.

El *espacio de configuraciones no ordenadas de n puntos en el plano* es

$$\mathrm{Conf}_n(\mathbb{C}) = \big\{\{z_1, z_2, \ldots, z_n\} : z_i \in \mathbb{C}, z_i \neq z_j\big\}.^{11}$$

[11] El *espacio de configuraciones ordenadas de n puntos en el plano*

$$\mathrm{PConf}_n(\mathbb{C}) = \big\{(z_1, z_2, \ldots, z_n) : z_i \in \mathbb{C}, z_i \neq z_j\big\}$$

Al igual que $\mathbb{C}^n \setminus V(\Delta)$, el espacio $\mathrm{Conf}_n(\mathbb{C})$ parametriza al espacio de polinomios mónicos de grado n sin raíces repetidas vía

$$\{z_1, z_2, \ldots, z_n\} \leftrightsquigarrow p(z) = (z - z_1) \cdot (z - z_2) \cdot \ldots \cdot (z - z_n).^{12}$$

Una configuración base $\mathbf{x_0} = \{z_1, z_2, \ldots, z_n\} \in \mathrm{Conf}_n(\mathbb{C})$ corresponde al polinomio base $\mathbf{p_0}(\mathbf{z}) = (z - z_1) \cdot (z - z_2) \cdot \ldots \cdot (z - z_n)$ y

$$\pi_1\big(\mathbb{C}^n \setminus V(\Delta), \mathbf{p_0}(\mathbf{z})\big) = \pi_1\big(\mathrm{Conf}_n(\mathbb{C}), \mathbf{x_0}\big).$$

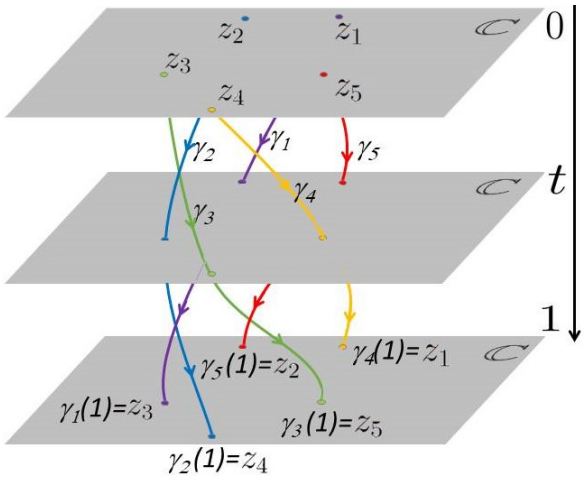


Figura 4. Un lazo de polinomios γ basado en $\mathbf{x_0} = (z_1, z_2, z_3, z_4, z_5)$ corresponde a una trenza.

Consideremos un lazo de configuraciones $\gamma : [0, 1] \to \mathrm{Conf}_n(\mathbb{C})$ basado en $\mathbf{x_0}$ (véase figura (4)). Si pensamos a $t \in [0, 1]$ como una variable de tiempo, el lazo γ puede pensarse como las trayectorias $\gamma_i : I \to \mathbb{C}$ de n partículas que no colisionan moviéndose en el plano $\mathbb{C}$, empezando y terminando en la configuración base:

$$\gamma(t) = \{\gamma_1(t), \gamma_2(t), \ldots, \gamma_n(t)\},$$

donde $\{\gamma_1(0), \ldots, \gamma_n(0)\} = \{z_1, \ldots, z_n\}$, $\gamma_i(t) \neq \gamma_j(t)$ si $i \neq j$ y es un lazo si $\{\gamma_1(1), \ldots, \gamma_n(1)\} = \{z_1, \ldots, z_n\}$, es decir, las partículas regresan a la configuración base $\mathbf{x_0}$, pero posiblemente permutadas. Así podemos visualizar al lazo de configuraciones $\gamma : [0, 1] \to \mathrm{Conf}_n(\mathbb{C})$ como una *trenza* de n hebras de $\mathbb{C}$ que empiezan en los puntos $\{z_1, z_2, \ldots, z_n\}$ en la «tapa superior» de $\mathbb{C} \times I$ y terminan en el mismo conjunto de puntos en la «tapa inferior», con los puntos posiblemente permutados. ¿A qué lazo de polinomios corresponde el lazo γ?

---

es un subespacio de $\mathbb{C}^n$ y el grupo simétrico S_n actúa libremente en $\mathrm{PConf}_n(\mathbb{C})$ permutando estas coordenadas. El espacio $\mathrm{Conf}_n(\mathbb{C})$ es $\mathrm{PConf}_n(\mathbb{C})/S_n$ con la topología cociente.

[12] De hecho, los *polinomios simétricos elementales* nos permiten recuperar los coeficientes del polinomio $p(z)$ en términos de sus raíces $\{z_1, z_2, \ldots, z_n\}$.

El grupo fundamental $\pi_1\big(\mathrm{Conf}_n(\mathbb{C}), \mathbf{x_0}\big)$ es el *grupo de trenzas de Artin* y usualmente se denota por B_n. Este grupo fue definido por E. Artin a principios del siglo pasado y se aplica en varias áreas de matemáticas. Para una introducción al fascinante tema de las trenzas y las diversas maneras en que pueden estudiarse, recomendamos al lector *Tutorial on the braid groups* por Dale Rolfsen incluido en el volumen [3] así como las referencias que dicho artículo cita. Para más información sobre espacios de configuraciones y grupos de trenzas sugerimos el artículo [4].

Como observamos anteriormente, cada trenza γ define una permutación de los puntos en la configuración base $\mathbf{x_0}$, un elemento bien definido del grupo simétrico S_n

$$\sigma_\gamma : \{z_1, z_2, \ldots, z_n\} \to \{z_1, z_2, \ldots, z_n\} \text{ dada por } \quad \gamma_k(0) \mapsto \gamma_k(1)$$

y se tiene un homomorfismo natural $\phi : B_n \to S_n$ que a cada trenza le asigna la permutación de los n puntos $\{z_1, z_2, \ldots, z_n\}$. Por ejemplo, la trenza de la figura (4) induce la permutación $(1\ 2\ 3\ 4\ 5) \in S_5$.

Resulta que este homomorfismo de grupos es sobreyectivo (¿por qué?) y su núcleo es un subgrupo normal que corresponde a las trenzas que no permutan los puntos en $\{z_1, z_2, \ldots, z_n\}$: el *grupo de trenzas puras* P_n.[13]

Más aún, el homomorfismo

$$\phi : B_n = \pi_1\big(\mathbb{C}^n \setminus V(\Delta), \mathbf{p_0}(\mathbf{z})\big) \twoheadrightarrow S_n$$

es la monodromía del espacio cubriente $\pi : \tilde{X} \to \mathbb{C}^n \setminus V(\Delta)$ de n hojas. En efecto, para el espacio cubriente $\pi : \tilde{X} \to \mathbb{C}^n \setminus V(\Delta)$, la fibra sobre el polinomio base $\mathbf{p_0}(\mathbf{z})$ corresponde a las n raíces distintas $\{z_1, z_2, \ldots, z_n\}$ de $\mathbf{p_0}(\mathbf{z}) = 0$. Para un punto z_k en la fibra, el levantamiento de un lazo basado γ de polinomios en $\mathbb{C}^n \setminus V(\Delta)$, con punto inicial en z_k, corresponde precisamente a la hebra de la trenza asociada a γ que empieza en el punto z_k. Por ende, el grupo de monodromía de la solución general de la ecuación algebraica (1) es el grupo simétrico S_n.

5. Conmutadores y la fórmula general

Para entender mejor la idea la prueba de Arnold veremos primero qué pasa para polinomios de grados 2 y 3, y posteriormente el caso general. Esperamos, con estos argumentos, mostrar al lector qué propiedades del grupo de monodromía dan la obstrucción para la existencia de una fórmula general cuando $n \geq 5$.

[13] El grupo de trenzas puras P_n es el grupo fundamental del espacio de configuraciones ordenadas $\mathrm{PConf}_n(\mathbb{C})$.

Ecuaciones polinomiales de grado 2. Consideremos nuevamente la ecuación general de grado 2

$$P(z, a_0, a_1) = z^2 + a_1 z + a_0 = 0. \tag{6}$$

Olvidemos por un momento la fórmula general que aprendemos en secundaria y supongamos que la solución $z = f(a_0, a_1)$ es una función racional. Es decir, f es una expresión en términos de los coeficientes del polinomio, que involucra sumas, restas, productos y divisiones de los mismos (pero no radicales), en particular f no es multivaluada[14]. Así al recorrer cualquier lazo de polinomios γ basado en $\mathbf{p_0}(\mathbf{z}) = (z - z_1)(z - z_2)$, el valor de la solución $z(t) = f \circ \gamma(t)$ empezará y terminará en el mismo punto y no intercambiará las raíces $\{z_1, z_2\}$.

Sin embargo, como vimos en la sección anterior, siempre podemos tomar lazos de polinomios γ que intercambien las raíces $\{z_1, z_2\}$ del polinomio base $\mathbf{p_0}(\mathbf{z})$. Por ejemplo, podemos tomar el lazo que corresponde al generador del grupo de trenzas $B_2 = \mathbb{Z}$. La monodromía $\phi : \pi_1\big(\mathbb{C}^2 \setminus V(\Delta), \mathbf{p_0}(\mathbf{z})\big) \twoheadrightarrow S_2$ de la función algebraica definida por (6) manda la clase de γ en la transposición $(12) \in S_2$. Por ende una expresión racional no puede ser la solución de la ecuación general de grado 2.

La fórmula general (2) que conocemos

$$z = f(a_0, a_1) = \frac{-a_1 + \sqrt{a_1^2 - 4a_0}}{2}.$$

no presenta una contradicción de este tipo. El grupo de monodromía de esta función algebraica coincide con S_2 y en particular el lazo γ induce la permutación (12) (¿por qué?).

Ecuaciones polinomiales de grado 3 y 4. Consideremos ahora la ecuación general de grado 3

$$P(z, a_0, a_1, a_2) = z^3 + a_2 z^2 + a_1 z + a_0 = 0. \tag{7}$$

Supongamos que una expresión de la forma

$$z = \sqrt[k]{r(a_0, a_1, a_2)},$$

con $r(a_0, a_1, a_2)$ una función racional, es una solución de la ecuación (7). Como antes, consideremos un polinomio base $\mathbf{p_0}(\mathbf{z}) = (z - z_1)(z - z_2)(z - z_3)$ en el espacio de polinomios $\mathbb{C}^3 \setminus V(\Delta)$ sin raíces repetidas y tomemos un lazo de polinomios γ en este espacio que induzca la permutación (123) como sigue. Notemos primero que en el grupo S_3

$$(123) = (12)(13)(12)(13) = (12)(13)(12)^{-1}(13)^{-1} = [(12), (13)].$$

[14] De hecho, como vimos en el caso de funciones racionales de una variable, la función cubriente asociada a una función racional es inyectiva y el grupo de monodromía es trivial.

Decimos que el 3-ciclo (123) es un *conmutador* de elementos de S_3. En general, para un grupo G y elementos $g, h \in G$, el elemento $[g,h] := ghg^{-1}h^{-1}$ se llama el *conmutador de g y h*.

Puesto que la monodromía de la función algebraica (7) es un homomorfismo $\phi : \pi_1\big(\mathbb{C}^3 \setminus V(\Delta), \mathbf{p_0}(\mathbf{z})\big) \twoheadrightarrow S_3$ sobreyectivo, podemos considerar lazos de polinomios τ y μ en $\mathbb{C}^3 \setminus V(\Delta)$ basados en $\mathbf{p_0}(\mathbf{z})$ tales que $\phi([\tau]) = (12)$ y $\phi([\mu]) = (13)$ (¿puedes pensar en lazos explícitos?). Entonces el lazo de polinomios $\gamma := \tau * \mu * \bar{\tau} * \bar{\mu}$ es tal que $[\gamma] = \big[[\tau],[\mu]\big]$ e induce la permutación no trivial (123) de las raíces de $\mathbf{p_0}(\mathbf{z})$.

Al recorrer el lazo $\bar{\gamma} = \mu * \tau * \bar{\mu} * \bar{\tau}$, la *variación del argumento*[15] de la expresión $r(a_0, a_1, a_2)$, es decir, el número total de vueltas que el lazo $r \circ \bar{\gamma} : [0,1] \to \mathbb{C} \setminus \{0\}$ le da al origen, es cero. En efecto, el número de vueltas que se obtenga al recorrer el lazo τ se cancela con el número de vueltas que resulta de recorrer $\bar{\tau}$ y lo mismo para μ y $\bar{\mu}$. En consecuencia, como vimos al final de la sección 3, al recorrer $r \circ \bar{\gamma}$, la función algebraica $z = \sqrt[k]{w}$ no permuta las raíces $\{z_1, z_2, z_3\}$ del polinomio $\mathbf{p_0}(\mathbf{z})$, contradiciendo nuestro párrafo anterior. Lo que estas ideas muestran es que una función algebraica $z = f(a_0, a_1, a_2)$ sin radicales anidados tiene monodromía que manda conmutadores de lazos en la permutación trivial, y en consecuencia no puede ser la solución de la ecuación general de grado 3.

Notemos que en nuestra discusión anterior fue crucial el hecho de que S_3 tiene elementos no triviales que son conmutadores. El lazo γ puede tomarse porque $(12)(13) \neq (13)(12)$, es decir de que el grupo S_3 es no conmutativo. Puede probarse que el grupo de monodromía de una función algebraica que puede expresarse como función racional con radicales simples (sin anidar) debe ser un grupo conmutativo. Los grupos S_3 y S_4 no son conmutativos, por lo cual las fórmulas generales si son solubles por radicales, deben tener radicales anidados. Si observamos las fórmulas de del Ferro, Tartaglia, Cardano y Ferrari vemos que efectivamente son expresiones con radicales anidados.

¿Qué más nos dice este tipo de argumento con respecto a la forma que debe tener la solución de la ecuación de grado 4?

Ecuaciones polinomiales de grado mayor o igual a 5. A continuación esbozamos las ideas de la prueba de Arnold para mostrar la imposibilidad de una fórmula soluble por radicales para ecuaciones polinomiales de grado mayor o igual a 5.

---

[15] La variación del argumento es un homomorfismo de grupos

$$var : \pi_1(\mathbb{C} \setminus \{0\}, \mathbf{x_0}) \to \mathbb{Z}$$

que se define como $var([\delta]) = \tilde{\delta}(1) - \tilde{\delta}(0)$, donde $\tilde{\delta}$ es cualquier levantamiento del lazo $\delta'(t) = \frac{\delta(t)}{||\delta(t)||}$ en $\mathbb{S}^1$, al espacio cubriente $\pi : \mathbb{R} \to \mathbb{S}^1$ dado por $\theta \mapsto e^{2\pi i\theta}$. Luego el homomorfismo

$$\pi_1(\mathbb{C}^3 \setminus V(\Delta), \mathbf{p_0}(\mathbf{z})) \xrightarrow{r_*} \pi_1(\mathbb{C} \setminus \{0\}, \mathbf{x_0}) \xrightarrow{var} \mathbb{Z}$$

manda los conmutadores a cero.

Diremos que una función algebraica $z = f(a_0, a_1, \ldots, a_{n-1})$ tiene *nivel* 0 *de anidamiento de radicales* si es una función racional, *nivel* 1 si tiene radicales no anidadas y *nivel* d *de anidamiento* si el número máximo de radicales anidados es d. Procediendo como antes podemos ver que la ecuación polinomial general de grado $n \geq 5$ no puede tener por solución una función con nivel d de anidamiento de radicales, es decir, no es soluble por radicales.

Consideremos la ecuación general de grado n

$$P(z, a_0, a_1, \ldots, a_{n-1}) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 = 0. \quad (8)$$

Supongamos que una expresión de la forma

$$z = \sqrt[k]{r(a_0, a_1, \ldots, a_{n-1})}, \quad (9)$$

con $r(a_0, a_1, \ldots, a_{n-1})$ una función con nivel $d-1$ de anidamiento de radicales, es una solución de la ecuación (8). Si $d = 0$ suponemos que la función (9) es racional. Nuevamente tomemos un polinomio base $\mathbf{p_0}(\mathbf{z}) = (z - z_1) \cdot \ldots \cdot (z - z_n)$ sin raíces repetidas. Como antes, podemos producir un lazo γ basado de polinomios en $\mathbb{C}^n \setminus V(\Delta)$ que induzca una permutación no trivial de las raíces $\{z_1, z_2, \ldots, z_n\}$ del polinomio $\mathbf{p_0}(\mathbf{z})$ (digamos por ejemplo la permutación (123)), pero tal que, al recorrer γ, la expresión $z = \sqrt[k]{r(a_0, a_1, \ldots, a_{n-1})}$ no permute las raíces $\{z_1, \ldots, z_n\}$. En consecuencia, una función algebraica de la forma (9) no puede ser solución de la ecuación (8).

¿Cómo podemos producir un lazo γ con tales características? El primer paso es escribir el elemento (123) de S_n como un conmutador de conmutadores de conmutadores... anidando los conmutadores d veces. Si $d \geq 3$ esto puede hacerse para $n \geq 5$, pero no para $n = 4$ (¿por qué?, ¿puedes escribirlo para $n = 5$?). Por otro lado tenemos que la monodromía de la función algebraica (8) es un homomorfismo $\phi : \pi_1\big(\mathbb{C}^n \setminus V(\Delta), \mathbf{p_0}(\mathbf{z})\big) \twoheadrightarrow S_n$ sobreyectivo, entonces podemos escoger un lazo de polinomios γ que induzca la permutación (123) y que se escriba como conmutadores anidados d veces, de lazos de polinomios. Resulta que al recorrer este lazo γ, en la expresión (9) no se permutan las raíces del polinomio base.

Para ilustrar esto supongamos que la ecuación (8) tiene por solución una expresión con nivel de anidamiento $d = 2$, por ejemplo

$$z = \sqrt[k]{g(a_0, a_1, \ldots, a_{n-1}) + \sqrt[s]{f(a_0, a_1, \ldots, a_{n-1})}}, \quad (10)$$

donde f y g son funciones racionales. Consideremos un lazo de polinomios γ que induzca la permutación (123) y tal que $[\gamma] := \big[[[\tau_1], [\mu_1]], [[\tau_2], [\mu_2]]\big]$. Como vimos antes, al recorrer el lazo $\gamma_1 := \tau_1 * \mu_1 * \bar{\tau_1} * \bar{\mu_1}$ (y el lazo $\gamma_2 := \tau_2 * \mu_2 * \bar{\tau_2} * \bar{\mu_2}$) la expresión $z = \sqrt[s]{f(a_0, a_1, \ldots, a_{n-1})}$ no permuta las raíces del polinomio base,

y tampoco lo hace la función racional $z = g(a_0, a_1, \ldots, a_{n-1})$. Más aún, la variación del argumento de la expresión

$$z = g(a_0, a_1, \ldots, a_{n-1}) + \sqrt[s]{f(a_0, a_1, \ldots, a_{n-1})},$$

al recorrer el lazo $\gamma := \gamma_1 * \gamma_2 * \bar{\gamma}_1 * \bar{\gamma}_2$ es cero. En consecuencia, al recorrer γ la expresión (10) no permuta la raíces del polinomio base (también es cierto para $\bar{\gamma}$, ¿por qué?). Es decir, para una función algebraica con nivel de anidamiento $d = 2$, la monodromía manda a un conmutador de conmutadores de lazos en la permutación trivial y, por ende, no puede ser solución general de la ecuación (8).

En general, la obstrucción a la existencia de una fórmula con nivel d de anidamiento de radicales corresponde a la posibilidad de anidar conmutadores en S_n hasta d veces y seguir obteniendo permutaciones no triviales (véase la tabla 5).

Cuadro 1. ¿Qué tanto podemos anidar conmutadores en S_n?

n	$\lvert S_n\rvert = n!$	Conmutadores $\lvert(S_n)^{(1)}\rvert = n!/2$	"Conm. de conm." $\lvert(S_n)^{(2)}\rvert$	"Conm. de conm. de conm." $\lvert(S_n)^{(3)}\rvert$	$\ldots$ $\lvert(S_n)^{(k)}\rvert$
2	2	1	1	1	1
3	6	3	1	1	1
4	24	12	4	1	1
5	120	60	60	60	60
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	$n!$	$n!/2$	$n!/2$	$n!/2$	$n!/2$

Dado un grupo G, el subgrupo de G generado por conmutadores se llama el *subgrupo conmutador* y se denota con frecuencia por $[G, G]$, G' o $G^{(1)}$. Esta última notación resulta útil si queremos iterar el proceso. Denotamos por $G^{(2)}$ al subgrupo $[G^{(1)}, G^{(1)}]$, el subgrupo conmutador de $G^{(1)}$, y en general por $G^{(d)}$ al subgrupo $[G^{(d-1)}, G^{(d-1)}]$. Resulta que

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \ldots \trianglerighteq G^{(d-1)} \trianglerighteq G^{(d)} \ldots$$

lo que se conoce como *serie normal descendente*. Los subgrupos $G^{(d)}$ no triviales dan una «medida» de qué tanto podemos anidar conmutadores sin obtener elementos triviales del grupo. Si todos los conmutadores son triviales, es decir $G^{(1)} = \{1\}$, entonces el grupo G es abeliano.

El subgrupo conmutador del grupo simétrico S_n coincide con el grupo alternante A_n, el subgrupo de S_n de permutaciones de orden par y es generado por 3-ciclos de la forma $(i\ i{+}1\ i{+}2)$. El argumento de Arnold muestra que los subgrupos $(S_n)^{(d)}$ no triviales nos dan una obstrucción para la existencia de una fórmula con nivel d de radicales anidados. Así, vimos que en grado 2 no puede haber una fórmula general racional y

en grado 3 no existe una fórmula general sin radicales anidados pues $(S_3)^{(1)} \neq \{1\}$. Puesto que $(S_4)^{(2)} \neq \{1\}$ se tiene una obstrucción para la existencia de una fórmula general con nivel 2 de radicales anidados para grado 4 (¿por qué?).

Para $n \geq 5$ se demuestra en un primer curso de teoría de grupos que $(S_5)^{(d)} \neq \{1\}$ para todo d (véase por ejemplo [5]). Es decir, se pueden tener conmutadores anidados no triviales arbitrariamente largos. Entonces, no puede existir una fórmula general $z = f(a_0, a_1, \ldots, a_{n-1})$ con nivel d de radicales anidados y esto es cierto para todo d. Concluimos que no puede haber una fórmula general soluble por radicales, lo que demuestra el teorema de Abel–Ruffini.

A los grupos G tales que $G^{(d)} = \{1\}$ para algún d se les llama *solubles*. Los grupos S_2, S_3 y S_4 son solubles. La prueba de Arnold consiste en probar que:

(a) La solución de la ecuación algebraica general de grado n tiene grupo de monodromía S_n.

(b) Si una ecuación algebraica es soluble por radicales, entonces su grupo de monodromía es soluble.

El teorema de Abel–Ruffini se sigue entonces del hecho que S_n es no soluble para $n \geq 5$.

Esta demostración comparte muchos elementos en común con la dada en un curso de teoría de Galois. Esto se debe a que el grupo de monodromía de una función algebraica $z = f(a, \ldots, a_{n-1})$ que satisface la ecuación polinomial $P(z, a_0, \ldots, a_{n-1}) = 0$ coincide con el grupo de Galois del polinomio P visto como un elemento de $\mathbb{C}(a_0, \ldots, a_{n-1})[z]$ (véase por ejemplo [6, p. 689]).

Finalmente queremos mencionar varias de las referencias existentes sobre el tema. Además del libro de problemas y soluciones de Alekseev [2] antes mencionado, una prueba rigurosa siguiendo las ideas de Arnold es presentada por Henryk Zoladek en [19] y [20]. Basado en estas ideas Boaz Katz publicó el video *Short proof of Abel's theorem that 5th degree polynomial equations cannot be solved* ([9]) y Fred Akalin escribió la entrada de blog *Why is the Quintic Unsolvable?* ([1]). En estas presentaciones se da una explicación elemental de esta prueba con fundamentos de teoría de grupos y variable compleja, además de ilustrar las ideas principales con animaciones interactivas. Esta prueba topológica también se expone en el artículo panorámico [15], en el que se enfatiza la importancia de la noción de monodromía.

Agradecimientos

Agradecemos al Centro de Ciencias Matemáticas de la UNAM por brindar las condiciones favorables para el desarrollo de este proyecto. La

primera autora agradece a Benson Farb por introducirla a estas ideas y el apoyo del proyecto PAPIIT-UNAM IA100816. El segundo autor agradece el financiamiento de la EMALCA 2015 y del Centro de Ciencias Matemáticas de la UNAM. Agradecemos a Mónica Cabria por varias conversaciones sobre el tema, y a Omar Antolín y a los dos árbitros por sus cuidadosas sugerencias para mejorar la presentación de este escrito.

Bibliografía

[1] F. Akalin, «Why is the Quintic Unsolvable? Entrada del blog "Notes on math, tech, and everything in between"», 2016, disponible en: `https://www.akalin.com/quintic-unsolvability`.

[2] V. B. Alekseev, *Abel's Theorem in Problems and Solutions*, Springer Netherlands, 2004, Based on the lectures of Professor V.I. Arnold.

[3] Berrick, A. J. et al., *Braids : introductory lectures on braids, configurations and their applications*, Lecture notes series, vol. 19, World Scientific, 2010.

[4] F. Cohen y J. Pakianathan, «Configuration spaces and braid groups», 1999, Disponible en: `http://web.math.rochester.edu/people/faculty/jonpak/newbraid.pdf`.

[5] D. Dummit y R. Foote, *Abstract Algebra*, 3.ª ed., John Wiley and Sons, 2004.

[6] J. Harris, «Galois groups of enumerative problems», *Duke Mathematical Journal*, vol. 46, núm. 4, 1979, 685–724.

[7] H. Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002.

[8] D. Huybrechts, *Complex Geometry: An Introduction*, Springer Science and Business Media, New York, 2006.

[9] B. Katz, «Short proof of Abel's theorem that 5th degree polynomial equations cannot be solved», Video (2013): `https://www.youtube.com/watch?v=RhpVSV6iCko`.

[10] M. Kuga, *Galois' dream: group theory and differential equations*, Birkhäuser Boston, Inc., Boston, MA, 1993, Translated from the 1968 Japanese original by Susan Addington and Motohico Mulase.

[11] J. Muciño, «Superficies de Riemann y uniformización», 1985, Disponible en: `http://www.matmor.unam.mx/~muciray/articulos/Superficies_de_Riemann.pdf`.

[12] J. Munkres, *Topología*, 2.ª ed., Pearson Educación, Prentice-Hall, 2002.

[13] M. Porter, *Superficies de Riemann - 3er coloquio del departamento de matemáticas*, Centro de Investigación y de Estudios Avanzados del IPN, Tlaxcala, 1983.

[14] M. Rzedowski Calderón, «La demostración de Abel», *Miscelánea Matemática*, núm. 63, 2016, 1–28.

[15] H. Santa Cruz, «A survey on the monodromy groups of algebraic functions. Research Experience for Undergraduates Summer Program», 2016, Disponible en: `http://math.uchicago.edu/~may/REU2016/REUPapers/SantaCruz.pdf`.

[16] J. Vargas, *Álgebra clásica*, Serie: Textos, vol. 7, SMM, 2006, Disponible en: `http://www.pesmm.org.mx/Serie%20Textos_archivos/T7.pdf`.

[17] G. Villa Salvador, «Las ecuaciones polinomiales como el origen de la teoría de Galois», *Miscelánea Matemática*, núm. 53, 2011, 1–22.

[18] F. Zaldívar, *Funciones algebraicas de una variable compleja*, Universidad Autónoma Metropolitana, México D.F., 1995.

[19] H. Zoladek, «The topological proof of Abel–Ruffini Theorem», *Topological Methods in Nonlinear Analysis Journal of the Juliusz Schauder Center*, vol. 16, 2000, 253–265.

[20] ———, *The monodromy group*, vol. 67, Mathematics Institute of the Polish Academy of Sciences. Mathematical Monographs (New Series) Birkhäuser Verlag, Basel, 2006.