



FACULTAD DE EDUCACIÓN Y PEDAGOGÍA
Escuela de Educación en Ciencias, Tecnologías y Culturas

La Teoría de Galois en las prácticas matemáticas del estructuralismo categórico

Trabajo de Grado realizado por Miguel Ángel Moreno Ramírez para optar al título
de Licenciado en Matemáticas

SANTIAGO DE CALI
2022

UNIVERSIDAD DEL VALLE
FACULTAD DE EDUCACIÓN Y PEDAGOGÍA
ESCUELA DE EDUCACIÓN EN CIENCIAS, TECNOLOGÍAS Y CULTURAS

**La Teoría de Galois en las prácticas matemáticas del
estructuralismo categórico**

Trabajo de Grado realizado por Miguel Ángel Moreno Ramírez para optar al título
de Licenciado en Matemáticas

Directora:
Maribel Anacona
Profesora de la Escuela de Educación en Ciencias, Tecnologías y Culturas
Facultad de Educación y Pedagogía

SANTIAGO DE CALI
2022

RESUMEN

Este trabajo de grado muestra la relación que existe entre la teoría de Galois y la teoría de categorías, además identifica ciertas prácticas matemáticas como promotoras del proceso de generalización a lo largo de más de un siglo. El estudio inicia con la presentación de algunos antecedentes algebraicos que dieron origen al teorema fundamental de la teoría de Galois, fundamentalmente, los de Lagrange y Abel. Luego se exhibe una generalización de este teorema en el marco del álgebra moderna, a través de las denominadas conexiones de Galois propuestas por Ore. Finalmente, en el contexto contemporáneo y en el marco de la teoría de categorías, se interpretan los funtores adjuntos como la expresión más abstracta y general del teorema. El análisis de estos tres momentos revela que las ideas, actividades, métodos y técnicas empleadas por Galois en la construcción de su teoría, permiten identificarlo –filosófica y retrospectivamente– como practicante del estructuralismo categórico.

Palabras clave: Teoría de Galois; Conexiones de Galois; Teoría de Categorías; Funtores adjuntos; Práctica matemática.

ABSTRACT

This degree work shows the relationship between Galois theory and category theory, also identifies certain mathematical practices as promoters of the generalization process over more than a century. The study begins with the presentation of some algebraic background that gave rise to the fundamental theorem of the Galois theory, fundamentally, those of Lagrange and Abel. Then a generalization of this theorem is exhibited within the framework of modern algebra, through the so-called Galois connections proposed by Ore. Finally, in the contemporary context and within the framework of category theory, the adjoint functors are interpreted as the most abstract and general expression of the theorem. The analysis of these three moments reveals that the ideas, activities, methods and techniques used by Galois in the construction of his theory allow him to be identified –philosophically and retrospectively– as a practitioner of categorical structuralism.

Keywords: Galois theory; Galois connections; Adjoint functors; Category theory; Mathematical practice.

TABLA DE CONTENIDOS

RESUMEN.....	3
ABSTRACT.....	4
TABLA DE FIGURAS	6
0. INTRODUCCIÓN	7
CAPÍTULO 1 El surgimiento de la teoría de Galois	11
1.1 La primera puesta en duda de Lagrange.....	12
1.2 La contundente respuesta de Abel.....	15
1.3 Galois y una visión distinta	19
1.4 Preliminares algebraicos a la solución de Galois	20
1.5 La resolubilidad de Galois y su teorema fundamental	40
CAPITULO 2 Los funtores adjuntos y las conexiones de Galois	48
2.1 Las estructuras más generales: las categorías	50
2.2 Los funtores adjuntos	55
2.3 Teorema fundamental de la teoría de Galois.....	60
2.4 Las conexiones de Galois.....	65
2.5 La categoría de los posets y sus funtores adjuntos.....	69
CAPÍTULO 3 Algunas reflexiones desde la práctica matemática	72
3.1 La práctica matemática.....	73
3.2 Las consideraciones de Mancosu	79
3.3 Lo que logra el estructuralismo	83
3.4 La emergencia abismal de la matemática moderna y la adjunción en Deleuze	88
4. CONCLUSIONES.....	94
4.1 La previa y punto de partida de la Teoría de Galois	95
4.2 Las estructuras cruciales.....	96
4.3 Funtore adjuntos y conexiones de Galois	97
4.4 La práctica estructuralista de Galois	98
5. REFERENCIAS.....	100

TABLA DE FIGURAS

Figura 1.1 Simetría r del cuadrado	25
Figura 1.2 Retículo de subgrupos de D_4	26
Figura 1.3 Extensión de $\mathbb{Q}$	32
Figura 1.4 $\mathbb{C}$ como extensión de $\mathbb{R}$	33
Figura 1.5 Puntos construibles de rectas dados los puntos iniciales.....	36
Figura 1.6 Puntos construibles a partir de rectas y circunferencias.....	37
Figura 1.7 Puntos construibles de intersecciones entre circunferencias	38
Figura 1.8 Operatividad del grupo $\text{Gal}(\mathbb{Q}(3,5)/\mathbb{Q})$	43
Figura 2.1 Morfismos entre dos categorías.....	54
Figura 2.2 Morfismos identidad.....	54
Figura 2.3 Composición de morfismos.....	55
Figura 2.4 funtor F de la categoría C a D	57
Figura 2.5 representación gráfica de funtores adjuntos	59
Figura 2.6 Retículo de campos de la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{5})$	64
Figura 2.7 Retículo invertido de los subgrupos de G	64
Figura 2.8 Correspondencia reticular del teorema de Galois.....	64
Figura 2.9 Comportamiento esquemático de las conexiones de Galois	68
Figura 2.10 Asociatividad entre morfismos de una categoría	69
Figura 3.1 Sustituciones del grupo de Galois	90
Figura 3.2 Método de Galois desde Novalis.....	92

0. INTRODUCCIÓN

Durante el siglo XIX y principios del siglo XX las matemáticas vivieron un incesante proceso de abstracción y generalización que conllevó a la unificación de las distintas disciplinas en torno a la noción de estructura. El estructuralismo conjuntista se constituyó en el entramado conceptual sobre el cual se erigieron -esencialmente- las matemáticas de las primeras décadas del siglo XX, conocidas como matemáticas modernas. Sin embargo, desde hace un poco más de medio siglo son otros estructuralismos, entre ellos el categórico, los que fundamentan de manera primordial las matemáticas contemporáneas. Esta transformación epistemológica que experimentaron diversas disciplinas merece ser estudiada con detalle para comprender de manera auténtica y profunda el devenir histórico de las matemáticas en el último siglo y medio. Este conocimiento provee un panorama conceptual más claro de la reciente actividad matemática y a su vez ofrece elementos de orden epistemológico claves en toda reflexión educativa.

Por tanto, en este trabajo de grado se propone analizar dicho proceso de transformación en un caso muy particular: la teoría de Galois.

En primera instancia, la intención es hacer un análisis histórico-epistemológico que nos muestre cómo esta teoría algebraica, que en sus comienzos giraba en torno a la resolución de polinomios de grado mayor o igual a cinco, se transformó poco a poco en una teoría abstracta muy potente que vincula la teoría de cuerpos con la teoría de grupos. Un estudio de esta naturaleza

ofrece luces para esclarecer el paso del álgebra clásica de principios del siglo XIX al álgebra moderna de principios del siglo XX. Sin embargo, una expresión de esta teoría, las conexiones de Galois específicamente, se puede identificar en el marco del estructuralismo categórico, propio de finales del siglo XX. De ahí, que resulte de mucho interés para este trabajo, analizar en un segundo momento, algunas relaciones epistemológicas que existen entre las conexiones de Galois y los funtores adjuntos en la teoría de categorías. Posterior a esto y como tercer momento, resulta relevante establecer algunos vínculos directos con la práctica en las matemáticas a la luz de la filosofía de las matemáticas, esto podría aportar elementos que también justifiquen la relevancia de un trabajo como este en la educación matemática.

De esta manera, en un recorrido de casi dos siglos se trata de identificar, como propósito fundamental del presente trabajo, los elementos de orden histórico, epistemológico y filosófico que subyacen en el proceso de transformación de la teoría de Galois: de una teoría del álgebra clásica a una teoría del álgebra moderna con componentes de matemáticas contemporáneas.

Con base en este propósito, se reconocen algunos antecedentes como los de Chavarría (2014), Gaviria (2014) y Muñoz (2016). El primero de estos hace énfasis en la génesis de las ecuaciones hasta llegar a las nociones de grupo y cuerpo del álgebra moderna. El segundo antecedente centra su atención en relacionar los grupos y cuerpos con desarrollos del estructuralismo conjuntista. Y el tercer antecedente destaca la teoría de Galois como centro de estudio, también establece algunas relaciones con la noción de adjunción.

La distancia que pretende tomar este trabajo respecto a estos antecedentes se caracteriza, en primer lugar, por acotar el surgimiento de la teoría de Galois sin desconocer la génesis del álgebra clásica; en segundo lugar, por presentar de manera más profunda la teoría de categorías e intentar establecer relaciones más estrechas respecto a los funtores adjuntos y los resultados de

Galois; en tercer lugar, por hacer una reflexión desde la filosofía de las matemáticas acerca de las prácticas matemáticas que se movilizan en el pensamiento de Galois.

En el esquema global de indagación que guía y articula este trabajo se priorizan cuatro problemas fundamentales: i) identificar el contexto en el cual emerge la teoría de Galois, a partir de los aportes de Lagrange y Abel al problema de la resolución general de ecuaciones, ii) reconocer el papel unificador de las estructuras algebraicas de grupo y cuerpo en el proceso de generalización de la teoría de Galois; iii) esclarecer la relación que existe entre las conexiones de Galois y los funtores adjuntos en el marco de la teoría de categorías; y iv) reflexionar sobre algunos de los elementos inmersos en la práctica matemática, ligados al estructuralismo categórico, claves para el desarrollo de competencias en la apropiación del álgebra y sus aplicaciones a nivel de la educación universitaria.

Con estos objetivos como telón de fondo, el trabajo se articula de la siguiente manera. En el primer capítulo se presentan tres momentos referentes al contexto en el cual emerge la teoría de Galois. En el primero, se estudian los aportes de Lagrange y Abel al problema de la resolución general de ecuaciones, en el segundo, se miran algunos preliminares matemáticos, que ayuden a entender el resultado principal de Galois que se presenta en el tercer momento.

En el segundo capítulo se estudian algunos conceptos elementales de la teoría de categorías, en particular, las definiciones de categoría y funtor, esto con el fin de hacer énfasis al concepto de funtor adjunto; luego se estudian las conexiones de Galois desde el teorema fundamental de la teoría de Galois. Por último, se analiza la relación entre los funtores adjuntos y las conexiones de Galois.

En el tercer y último capítulo se plantea una reflexión respecto a la práctica matemática, se estudia lo que se conoce por práctica; luego las prácticas que se podrían considerar para el desarrollo de las matemáticas y su relación con las actividades de las matemáticas contemporáneas, en particular, las prácticas del estructuralismo categórico. Por último, se hace énfasis en las prácticas de Galois que apoyaron la necesidad del cambio a las matemáticas modernas.

A manera de conclusión se presentan al final del documento una serie de reflexiones acerca de las diversas problemáticas abordadas en el trabajo, así como las distintas posibilidades de investigación que surgen a partir del mismo y que se esperan desarrollar en el corto y mediano plazo.

CAPÍTULO 1

El surgimiento de la teoría de Galois

La ciencia es obra del ingenio humano, que está destinado a estudiar más que a conocer, a buscar más que a encontrar la verdad¹.

Evariste Galois

La historia de las matemáticas es la herramienta crucial para identificar lo importante que fueron los escritos de una noche en vela de aquel joven francés con no más de cinco años de vida académica, sobre el problema de la resolución general de ecuaciones, asunto que tuvo relación desde las matemáticas antiguas. La génesis de este problema se puede ubicar hacia el año 2000 A.C en sociedades como la egipcia y la babilónica, en las cuales surgió la necesidad de resolver ecuaciones lineales en el marco de sus prácticas agrícolas. Para tal efecto, emplearon técnicas como la “regla de la falsa posición” que consiste en asignarle un valor cualquiera a la incógnita, calcular el resultado y hacer una regla de tres simple; así como la “regla de la doble falsa posición” que se basa en un procedimiento similar, pero asignándole dos valores distintos a la incógnita, para crear un sistema de ecuaciones dos por dos simple. Estas técnicas se fueron mejorando gracias a los posteriores aportes de los árabes y su simbología más algebraica y simplificada.

¹ Citado por (Macho, 2014)

Esta génesis es relevante de analizar y profundizar debido a que puede justificar la naturaleza algebraica del problema y el contexto previo de la pregunta ¿cuál es la fórmula general para resolver ecuaciones polinómicas? La intención es empezar a analizar el tratamiento de esta pregunta desde el primer registro del cuestionamiento de la existencia de aquella fórmula. Esto llevará a estudiar los aportes de Lagrange, y posteriormente los de Abel para finalizar con Evariste Galois y su adelanto en ciertas ideas que se volverían fuertes solo cien años después junto con el surgimiento de su teoría.

Si el lector desea profundizar más en la génesis de la teoría de ecuaciones se sugieren trabajos como el de Chavarría (2014), el de Gaviria (2014) o el de Muñoz (2016), los cuales son antecedentes y referencias importantes para el desarrollo de este trabajo.

1.1 La primera puesta en duda de Lagrange

Joseph Louis Lagrange (1736-1813) fue un físico, matemático y astrónomo italiano que por sus contribuciones científicas se le puede considerar como uno de los matemáticos y físicos más grandes de la historia con aportes muy relevantes en ambos campos de conocimiento. En matemáticas, en álgebra particularmente, publicó artículos como *Réflexions sur la Résolution Algébrique des equations* en 1771, en el cual propuso fórmulas generales para ciertas ecuaciones polinómicas.

Dado que para la época de Lagrange se contaba con aportes importantes por parte de Scipione del Ferro (1465-1526), Tartaglia (1499-1557), Cardano (1501-1576) y Ferrari (1522-1565) para la construcción de fórmulas generales en ecuaciones de grado tres y cuatro, Lagrange pudo desarrollar bajo técnicas conocidas su *resolvente* para llegar a estas resoluciones y tenerlas como base para obtener lo que hasta ese momento parecía muy difícil, pero en algún momento

posible. Resultaba tentador pensar que se podría encontrar la fórmula general para resolver ecuaciones de grado cinco o más. Encontrar este resultado parecía más fascinante incluso después de Lagrange, pues se tenían resultados importantes como el *Teorema fundamental del álgebra* propuesto por Gauss en su tesis doctoral *Una nueva demostración del teorema de que toda función algebraica racional integral de una variable puede resolverse en factores reales de primer o segundo grado* publicada en 1799. Es así como el intento de Lagrange de tratar de ir más allá y dominar después de tanto tiempo el grado cinco, adquirió todo su sentido.

1.1.1 Lagrange y su resolvente

Inicialmente Lagrange tuvo en cuenta sus resoluciones para los casos de grado tres y cuatro, en particular su metodología la basaba en un polinomio resolvente de grado inferior que principalmente se construía a partir de ciertas permutaciones de las raíces de los polinomios. Este razonamiento aparentemente se inspiró en el hecho de que las soluciones ofrecidas por los matemáticos del Renacimiento se basaban en encontrar una ecuación asociada a la original cuyas raíces tuviesen relación entre sí. Esta técnica se emplea para las ecuaciones de grado tres y cuatro, por lo que parece tentador hacer el intento para las de grado cinco. En particular, Dávila (2003, p. 53-54) muestra la resolución de ecuaciones de grado tres ofrecida por Lagrange, en los siguientes términos:

Supongamos que x, y, z son las raíces de la cúbica general, las cuales no conocemos a priori. Consideremos ahora la cantidad t dada por

$$t = x + ay + a^2 z \quad (1)$$

Donde a es una raíz cúbica primitiva de la unidad. Si permutamos las raíces en (1), entonces obtenemos seis valores posibles para t pues el total de permutaciones de tres objetos es $3! = 6$.

Sean $t_1, t_2, \dots, t_6$ los distintos valores que se obtienen de (1) al permutar las raíces de la cúbica. Estos seis valores satisfacen la ecuación

$$f(x) = (x - t_1)(x - t_2)(x - t_3)(x - t_4)(x - t_5)(x - t_6) \quad (2),$$

Los coeficientes de esta ecuación cómo es posible observar son polinomios simétricos² en las t_i , por la manera en que fueron definidas las t_i , también son simétricos en x, y, z ; luego se pueden conocer en términos de los coeficientes de la cúbica que se pretende resolver. La ecuación (2) es la ecuación que hoy se llama resolvente de Lagrange para el caso de la cúbica. Nótese que (2) es una ecuación de sexto grado, considerablemente mayor que el de la que el de la cúbica que se quiere resolver por radicales. Sin embargo, en este caso las cantidades t_i satisfacen las relaciones $t_2 = at_1, t_3 = a^2t_1, t_5 = at_4, t_6 = a^2t_4$. Este se cumple para cierto orden de las permutaciones de las raíces en (1); si se permutan las raíces en otro orden, se obtienen relaciones similares a las anteriores. De esta manera, (2) es una ecuación cuadrática en x_3 pues $f(x) = (x^3 - t_1^3)(x^3 - t_4^3) = (x^3)^2 - (t_1^3 + t_4^3)x^3 + (t_1^3 + t_4^3)x^3$.

Si hacemos $u = t_1^3$ y $v = t_4^3$, entonces los coeficientes de esta ecuación son precisamente $u+v$ y uv , para los cuales es posible una expresión en términos de la cúbica original y se obtiene a través de ellos la solución. De esta manera, se obtienen los seis valores para t ; por consiguiente, las soluciones de la cúbica están dadas por

$$\begin{aligned}x &= \frac{1}{3}[(x - y + z) + t_1 + t_4], \\y &= \frac{1}{3}[(x - y + z) + a^2t_1 + at_4], \\z &= \frac{1}{3}[(x - y + z) + at_1 + a^2t_4],\end{aligned}$$

Por lo que solo se necesita identificar bien a t_1 y a t_4 de entre las seis posibles soluciones de la ecuación resolvente (2). Recuérdese que la expresión $x + y + z$ es un polinomio simétrico elemental de estas tres raíces y, por lo tanto, conocemos su valor pues es el coeficiente del término cuadrático en la cúbica de la forma $x^3 + ax^2 + bx + c = 0$. En este caso, Lagrange va más allá y da una nueva manera explícita para calcular esos valores.

Veremos más adelante cómo esta metodología empleada por parte de Lagrange sirvió como base para la construcción que establece Galois en su resolución. Inicialmente se puede pensar que el trabajo de Lagrange sugiere una temprana idea de estructura para su tratamiento, en particular la que se conoce como grupo de permutación³.

Esta misma metodología continuó siendo empleada por Lagrange para las ecuaciones de grado cinco, y a pesar de que llega a una fórmula general, es el primer matemático en cuestionar

² Un polinomio simétrico es un polinomio con n variables, tal que si se intercambian las variables el polinomio se mantiene invariante, es decir, sigue siendo el mismo.

³ A Lagrange también se le atribuyen aportes como el de su teorema en la misma teoría de grupos: Si G es un grupo finito y H un subgrupo de G , entonces el orden de H divide al orden de G (es decir, $(|H| \mid |G|)$) y el índice de H en G equivale a $\frac{|H|}{|G|}$ (Dummit & Foote 2003).

la existencia de esta fórmula junto con la efectividad de su método para encontrarla: “De nuestro razonamiento vemos que es muy dudoso que los métodos que hemos considerado pudieran dar una completa solución a las ecuaciones de quinto grado” (Lagrange 1869, p. 305).

1.2 La contundente respuesta de Abel

Niels Henrik Abel (1802-1829) fue un matemático noruego principalmente conocido por sus aportes en el desarrollo de las funciones elípticas y por ser el primer matemático que demostró la imposibilidad de obtener una fórmula general para los polinomios de grado mayor o igual a cinco en un artículo que publicó en 1824 llamado *Mémoire sur les équations algébriques où on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré* (que en 1826 amplió). Con este trabajo se dio un paso importante en la línea del álgebra que matemáticos como los mencionados anteriormente habían tratado de dar. Para comprender los aspectos generales de la demostración, se toma como referencia la exposición de Almira y Cid (2017) presentada en un lenguaje cómodo y simplificado.

En primer lugar, es importante tener en cuenta que la prueba de Abel procede por reducción al absurdo, esto lo hace con la suposición de que existe una fórmula algebraica que proporciona las soluciones de un polinomio de grado cinco simplemente manipulando sus coeficientes con las operaciones elementales de suma, resta, multiplicación, división, potenciación y radicación. Este polinomio tiene la siguiente forma:

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

A partir de esto, se supone una fórmula que combina los coeficientes $a_0, a_1, \dots, a_4$ mediante un número finito de sumas, restas, multiplicaciones, divisiones y extracción de raíces

capaz de proporcionar las soluciones de la ecuación. El primer paso que Abel explicó en su artículo de 1826 consistió en probar que toda solución por radicales podía escribirse como

$$x = g_0 + \sqrt[m]{R} + g_2 \sqrt[m]{R^2} + g_3 \sqrt[m]{R^3} + \cdots + g_{m-1} \sqrt[m]{R^{m-1}}$$

Siendo m un número primo y $R, g_0, g_2, \dots, g_{m-1}$ números reales. Con esto, en la solución aparecen raíces anidadas, es decir, raíces dentro de raíces, esto con el fin de llegar en el nivel más interior a las funciones racionales sin raíces.

Un ejemplo de esto se puede ver en la solución de la ecuación cúbica reducida $y^3 + py + q = 0$ la cual es

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

Según la fórmula Del Ferro-Tartaglia-Cardano-Ferrari, esta expresión admite la expresión equivalente y descrita por Abel $y = \sqrt[3]{R} + g_2 \sqrt[3]{R^2}$ considerando a

$$R = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad y \quad g_2 = \frac{9 \left(-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right)}{p^2}$$

En este sentido, Abel logró deducir que $g_0, g_1, \dots, g_{m-1}$ y $\sqrt[m]{R}$ son funciones racionales construidas a partir de las raíces de la ecuación de grado cinco. Así, $\sqrt[m]{R}$, que necesariamente es una función irracional de los coeficientes de la ecuación, es a la vez una función racional de las raíces; esta última propiedad, fundamental para la prueba de Abel, había sido usada por Ruffini (1765-1822) en su memoria *Teoria Generale delle Equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto* publicada en 1799 pero sin haberla demostrado. La comprobación de

esta propiedad justifica la reputación que tiene Abel como el primero en resolver el misterio sobre la ecuación de grado cinco.

Como ejemplo se puede considerar la ecuación cuadrática $x^2 + bx + c = 0$, la cual tiene las raíces

$$x_1 = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad y \quad x_2 = \frac{-b - \sqrt{b^2 - 4c}}{2}$$

Con esto, se comprueba que $\sqrt{b^2 - 4c} = x_1 - x_2$ y por tanto la función $\sqrt{b^2 - 4c}$, que es irracional con los coeficientes b y c , es por contrario una función racional en las raíces x_1 y x_2 , que tiene sentido con el resultado general de Abel.

Análogamente, Abel concluyó que todo radical que apareciese en la solución x debía ser una función racional de las raíces. A partir de esto, Abel usó el teorema de Cauchy sobre el número de valores que toma una función racional cuando se permutan sus valores, esto con el fin de llegar a una contradicción y demostrar así que la solución por radicales no podía existir.

Con este fin, Abel prestó atención a los radicales del nivel más inferior, es decir, aquellos de la forma $\sqrt[n]{R}$ donde R es una función racional de los coeficientes $a_0, a_1, \dots, a_4$ de la ecuación de quinto grado, esto implica que R está libre de raíces, además nótese que n es un número primo. Como los coeficientes son las funciones simétricas elementales de las raíces, se cumple que R es también una función simétrica de las raíces y, además, Abel había probado que $\sqrt[n]{R} = r(x_1, x_2, \dots, x_5)$ era una función racional construida a partir de las raíces de la quintica $x_1, x_2, \dots, x_5$. Al hacer las permutaciones de las cinco variables de r se obtiene un único valor de R , esto se cumple porque R es simétrica, y por lo tanto $\sqrt[n]{R}$ toma los n valores distintos de la raíz n -ésima.

A partir de lo anterior, Abel utilizó el teorema de Lagrange para garantizar que $n = 2, 3$ o 5 -debido a que n divide a $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ y n es primo- y el teorema de Cauchy para establecer entonces que $n = 5$ o $n = 2$, puesto que no es posible el caso $n = 3$. En particular, esto quiere decir que la raíz situada en el nivel más inferior de la expresión debe de ser una raíz quinta o una raíz cuadrada. Con esto, es suficiente con mirar cada caso y descartarlo si existe alguna contradicción.

Para el caso $n = 5$ se considera la ecuación probada previamente por Abel

$$\sqrt[5]{R} = \frac{1}{5}(x_1 + \alpha^4 x_2 + \cdots + \alpha x_5)$$

En la que $x_1, x_2, \dots, x_5$ son las raíces de la ecuación de grado cinco y α es una raíz quinta de la unidad distinta de uno; de aquí, el miembro izquierdo de la ecuación toma cinco valores distintos al permutar las raíces, mientras que el miembro de la derecha cambia su valor con cada permutación y toma $5! = 120$ valores. Por lo tanto, no es posible que ambas expresiones sean iguales, y solo queda el caso $n = 2$.

Para descartar el caso $n = 2$ Abel prueba que para este caso se cumplía la ecuación

$$\frac{1}{5}(x_1 + \alpha^4 x_2 + \cdots + \alpha x_5) = \sqrt[5]{h_0 + h_1 \sqrt{S}}$$

En el cual h_0, h_1 y S eran funciones simétricas de las raíces. Con esto, al permutar las cinco raíces de todas las posibles formas, el miembro de la izquierda tomó $5! = 120$ valores, pero el miembro de la derecha solo 10, al tener la raíz cuadrada dos valores posibles y multiplicarlos por cinco admisibles de cada raíz quinta. Abel llegó de esta forma a una contradicción que implicaba que la primera premisa era falsa; no existía solución por radicales para la ecuación general de grado cinco.

Con esta demostración como base, se pudo deducir que multiplicando por x^{n-5} las ecuaciones de grado cinco o más, tampoco puede existir una fórmula general que proporcione las raíces de una ecuación de cualquier grado.

Es fácil de ver que esta prueba que construye Abel y los pensamientos sobre la resolución de ecuaciones que propone Lagrange, se basan principalmente en la idea de permutación de las raíces en una expresión, que puede ser difícil de abstraer en una primera mirada; pero en esencia, trata de identificar qué expresiones se encuentran invariantes al aplicar esos cambios, es decir, que su valor no cambia.

Para que se entienda esta idea -que será también crucial dentro del pensamiento de Galois- nótese los siguientes casos:

$$1) 2^3 \rightarrow 3^2$$

$$2) 2 + 3 \rightarrow 3 + 2$$

Evidentemente en el primer caso donde se permuta el 2 con el 3 hay un cambio en el resultado de la expresión; sin embargo, en el segundo caso (con la suma que normalmente conocemos en $\mathbb{R}$) la expresión se mantiene invariante.

1.3 Galois y una visión distinta

El matemático francés Evariste Galois (1811-1832), claro protagonista de este trabajo y de la reciente historia de las matemáticas, aportó de manera sustancial en la construcción de los cimientos del álgebra moderna. Dentro de su convulsa y romántica historia, el joven revolucionario no se quedó con los grandes resultados planteados por Abel -o por el mismo Lagrange- acerca de la irresolubilidad por radicales de los polinomios de grado cinco o más. El trabajo de Galois consistió en ofrecer las condiciones necesarias y suficientes para que puedan existir fórmulas que

resuelvan ciertos polinomios de *cualquier grado* mediante las operaciones básicas $+$, $-$, $\times$, $\div$, radicación y potenciación.

Aunque Abel había demostrado la imposibilidad de encontrar una fórmula general para resolver cualquier polinomio, ya existían trabajos que trataban algunas ecuaciones de grado cinco o más que se podían resolver por radicales, entre estos vale la pena mencionar el trabajo de Vandermonde (1735-1796) publicado en 1770 y titulado *Mémoire sur la Résolution des Equations* que posteriormente fue completado por Gauss de forma general y que asegura la resolución por medio de radicales de la ecuación $x^p - 1 = 0$ donde p es primo. El trabajo de Galois consistió entonces en generalizar este tipo de reflexiones a polinomios de grado cualquiera.

Para comprender ampliamente la propuesta de Galois, es necesario recordar ciertos conceptos básicos de la teoría de grupos, de anillos y de cuerpos, los cuales se presentan en el siguiente apartado, con el propósito de que el presente trabajo sea auto-contenido.

1.4 Preliminares algebraicos a la solución de Galois

El estudio de las estructuras es la principal herramienta para el resultado de Galois, por lo que naturalmente surge la pregunta acerca de su definición ¿qué son las estructuras matemáticas?

Para abordar esta pregunta y los preliminares necesarios de esta sección, vale la pena considerar la visión moderna del álgebra, presente en literatura como la de Jacobson (1974), Herstein (1988), Judson (2017), Dummit & Foote (2003) que destacan esta perspectiva desarrollada en la escuela de Göttingen a cargo de Emmy Noether (1882-1935)⁴ y sus estudiantes;

⁴ En cuanto a la figura de Emmy Noether, las palabras se quedan cortas para describir su papel en la perspectiva de las matemáticas modernas. Muchas de sus contribuciones en los campos de la física teórica y del álgebra abstracta quedaron implícitos en la cultura matemática general; el hecho de ser mujer con origen judío en una época convulsa y con fuertes subestimaciones hacia la figura femenina provocó que no se le diera igual relevancia y respeto en la academia. A pesar de esto, el legado de Noether se mantiene por la influencia que tuvo en sus estudiantes y sus

estos últimos, matemáticos muy destacados e influenciados por Noether, entre estos Bartel van der Waerden (1903-1996), reconocido por su libro *Moderne Algebra*, editado por primera vez en 1931 y citado hasta el día hoy en múltiples trabajos sobre álgebra.

Ahora bien, respecto a esta perspectiva moderna del álgebra, se podría definir a una estructura como una o varias colecciones de elementos y un conjunto de operaciones o relaciones definidas en esas colecciones; principalmente cuando se estudian las estructuras, se analizan las propiedades y regularidades que cumplen sus elementos respecto a sus operaciones. La intención de esta visión es hacer énfasis en cómo se comportan las relaciones de un sistema sin necesidad de enfatizar en la naturaleza de los elementos que se movilizan en ese sistema.

En particular, Galois se centra en el estudio de las estructuras de *grupo* y *cuerpo*; sin embargo, existen más estructuras como el *magma* o el *monoide*, la primera cumple la propiedad de ser cerrada con su operación, mientras que la segunda, además de cumplir esta cerradura, cumple con ser asociativa y tener un elemento neutro. Si el lector quisiera mirar más particularidades epistemológicas —e incluso históricas y filosóficas— de estas y otras estructuras, se recomienda el libro de Panza (2019).

1.4.1 La estructura de grupo

El *grupo* es la primera estructura que hay que considerar en el desarrollo de este trabajo, esta estructura nació a partir de los estudios de Galois en la teoría de ecuaciones con una incógnita; sin embargo, la noción que se utiliza actualmente se debe a desarrollos futuros a su muerte. Los matemáticos contemporáneos a Galois no entendían sus resultados. Solo veinte años después de su muerte Enrico Betti (1823-1892) presenta de forma detallada sus resultados, los cuales fueron

trabajos. Si el lector le interesa conocer con más detalle la figura de Noether en el desarrollo del álgebra abstracta, y en especial sus aportes en conceptos como los *ideales*, se recomienda el trabajo de Gaviria (2014).

publicados por primera vez por Joseph Liouville (1809-1882) en 1846. Posteriormente, en 1870, Marie Camille Jordan (1838-1922) publica un tratado que destaca la importancia de la teoría de grupos -al igual que la teoría de Galois- para investigaciones matemáticas; así, esta teoría se constituyó como uno de los ejes fundamentales en el álgebra moderna (Chavarria, 2014).

La estructura de grupo se define a partir de un conjunto G y una operación binaria $*$, esta estructura se puede simbolizar como $\langle G, * \rangle$. Recordando que una *operación binaria* $*$ en un conjunto G es una función $*$: $G \times G \rightarrow G$; y para cualquier $a, b \in G$ se escribe $a * b$ para $*(a, b)$.

Además, una operación binaria $*$ en un conjunto G es *asociativa* si para todo $a, b, c \in G$ se tiene $a * (b * c) = (a * b) * c$. Finalmente, si los elementos a y b de G son conmutables, se dice que $*$ es *conmutativa* si para todo $a, b \in G$, $a * b = b * a$.⁵

Con estos elementos se puede definir de manera adecuada lo que es un Grupo y algunos tipos de estas estructuras:

Definición 1.1 Un *grupo* es una pareja ordenada $\langle G, * \rangle$ donde G es un conjunto y $*$ es una operación binaria en G que satisface los siguientes axiomas:

- i. $(a * b) * c = a * (b * c)$, para todo $a, b, c \in G$, es decir, $*$ es asociativa,
- ii. Hay un elemento e en G , llamado una *identidad* de G , tal que para todo $a \in G$ tenemos que $a * e = e * a = a$,
- iii. Para cada $a \in G$ hay un elemento a^{-1} de G , llamado un *inverso* de a , tal que $a * a^{-1} = a^{-1} * a = e$.

Observación: El grupo $\langle G, * \rangle$ es llamado *abeliano*⁶ (o conmutativo) si $a * b = b * a$ para todo $a, b \in G$.

⁵ Estas definiciones se pueden encontrar en diversos libros de álgebra, tales como Algebra Abstracta de Herstein o Abstract Algebra de Dummit & Foote, este último se ha tomado en cuenta para la elaboración de este apartado.

⁶ El nombre de abeliano se le da en honor al matemático noruego Niels Henrik Abel que fue el primero en estudiar esta clase de estructuras.

Ejemplo: los números enteros con la suma tienen estructura de grupo; es decir $\langle \mathbb{Z}, + \rangle$ es un grupo. Esta estructura inicialmente cumple que la suma es cerrada, pues si operamos dos elementos $a, b \in \mathbb{Z}$, tenemos que $(a + b) \in \mathbb{Z}$, también tenemos que la suma es asociativa, posee un neutro que en este caso sería el cero $e = 0$ y por último cada elemento n posee un inverso que es justamente $-n$ y que satisface que $n + (-n) = 0 = e$ ⁷.

Sin embargo, este mismo conjunto con la operación producto no tiene estructura de grupo. Es decir, $\langle \mathbb{Z}, \cdot \rangle$ no es un grupo, puesto que no existe el elemento inverso $(1/n)$ de todo entero $n \in \mathbb{Z}$. Esto muestra el rol tan importante que tiene la operación en la definición. Así mismo, si en el ejemplo inicial dejamos la operación de suma, pero cambiamos el conjunto $\mathbb{Z}$ por $\mathbb{N}$, tenemos que no se conforma una estructura de grupo. Es decir, $\langle \mathbb{N}, + \rangle$ no es un grupo, puesto que no existe el elemento inverso de la suma $(-n)$ para todo $n \in \mathbb{N}$. Esto muestra la dependencia del conjunto en la definición.

Por otro lado, hay dos definiciones, que surgen a partir de la definición de grupo, las cuales vale la pena señalar y que justifican que esta definición no tiene una existencia arbitraria; a partir de estas estructuras se ha desarrollado parte de la teoría de grupos y se han alcanzado resultados tan importantes como al que llegó Galois. De manera particular, es relevante mirar los subgrupos haciendo énfasis en los subgrupos normales, y en los grupos de simetrías. Para tal efecto, se presenta en primera instancia la definición de subgrupo. En palabras de Dummit & Foote (2003):

⁷ Esto se puede probar dejando claro dos cosas, inicialmente la definición de los enteros que se pueden ver como la unión de los naturales con sus opuestos y el cero, es decir, $\mathbb{Z} = \mathbb{N} \cup Op(\mathbb{N})$ donde $Op(\mathbb{N}) = \{-n: n \in \mathbb{N}\} \cup \{0\}$ y la definición de su suma que se puede ver en tres casos apoyándonos en el orden: cuando $a, b \in \mathbb{N}$, cuando $a, b \in Op(\mathbb{N})$ o cuando $a \in \mathbb{N}$ y $b \in Op(\mathbb{N})$.

Definición 1.2 Dado un grupo G , el subconjunto H de G es un *subgrupo* de G si H es no vacío y H es cerrado bajo productos (de G) e inversos (es decir, $x, y \in H$ implica que $x^{-1} \in H$ y $xy \in H$). Si H es subgrupo de G escribimos $H \leq G$.

En esencia, lo que se puede rescatar en la definición de subgrupo es que puede haber estructuras más grandes que otras bajo las mismas operaciones, o lo que es lo mismo, se puede establecer un orden entre algunos grupos manteniendo la característica de su operación; de alguna forma este orden se podría asemejar con el de contenencia dentro de la teoría de conjuntos ($\subseteq$).

Ahora bien, teniendo estas consideraciones se pueden mirar los siguientes casos que son relevantes para ilustrar de manera clara el resultado de Galois.

Grupos de simetrías. Los grupos de simetrías constituyen un clásico ejemplo de la teoría de grupos, los cuales se basan en el concepto de permutación dentro de los conjuntos finitos; las permutaciones (que son los elementos del conjunto dentro de esta estructura) se definen como una función biyectiva θ cuyo dominio y rango son el mismo conjunto finito $X = \{x_1, x_2, \dots, x_n\}$ y funciona con la operación composición ($\circ$), así por ejemplo, si se tiene $\alpha \circ \beta$ entonces primero se opera la permutación β y luego α ; nótese también que en este caso la identidad del grupo es la permutación que no altera la relación de los elementos.

Entre los ejemplos más conocidos están las simetrías de un cuadrado. Para su intuición, se puede aprovechar algunos recursos digitales de la plataforma GeoGebraTube, como el de Jaimes (2016) “Grupos de simetrías del cuadrado” que ilustra gráficamente las transformaciones. El lector podría acceder a este recurso mediante el enlace: <https://www.geogebra.org/m/d8Dy3CwY>.

En particular, el grupo de simetrías del cuadrado -y en general de cualquier polígono regular- consiste en aplicarle transformaciones geométricas a la figura de tal manera que no se altere visualmente y que mantenga su posición inicial.

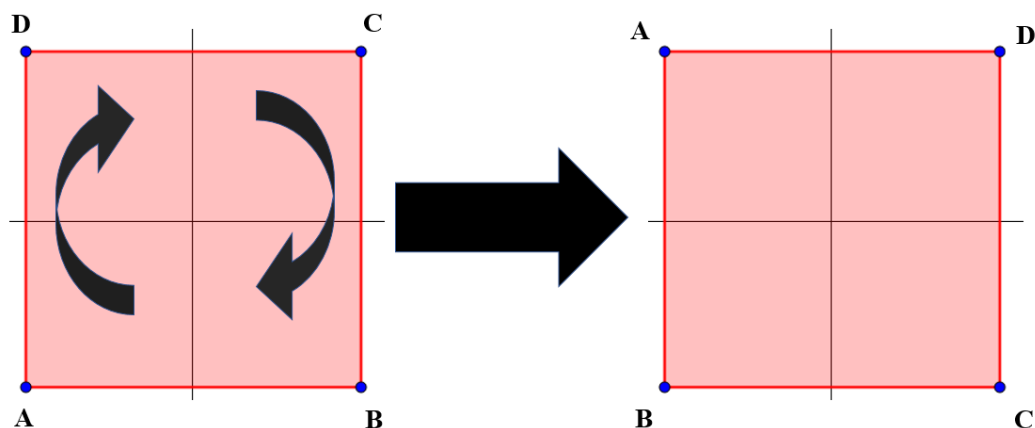


Figura 1.1 Simetría r del cuadrado

Con apoyo del recurso de Jaimes (2016), el lector podrá notar que serían en total ocho simetrías del cuadrado, usualmente estas simetrías son denotadas de la siguiente manera:

- Id : Identidad, no hacerle nada a la figura inicial.
- r : Rotar 90° al cuadrado.
- r^2 : Rotar 180° al cuadrado.
- r^3 : Rotar 270° al cuadrado.
- S_v : Reflejar respecto al eje vertical al cuadrado.
- S_h : Reflejar respecto al eje horizontal al cuadrado.
- S_p : Reflejar respecto a una diagonal al cuadrado, también es denotada como S_d .
- S_i : Reflejar respecto a la otra diagonal del cuadrado -contradiagonal-, también es denotada como S_c .

En este caso del cuadrado, se tiene en cuenta que se deben realizar las rotaciones con múltiplos del ángulo de 90° , esto para no alterar visualmente el cuadrado; por otro lado, la operatividad de la composición efectivamente es cerrada y por tanto bien definida, así por ejemplo $S_v \circ r = S_d$, aplicando primero r y posteriormente S_v . Queda para el lector comprobar las otras posibles operaciones.

En términos generales, cuando se habla de grupos de simetrías en polígonos regulares se refiere a los *grupos diédricos* que son simbolizados por D_n donde n es la cantidad de lados del polígono, el grupo diédrico del cuadrado sería D_4 .

Con la anterior consideración y la definición de subgrupo, se podrían establecer relaciones de contención de subgrupos en el grupo D_4 ; en concreto, una manera de representar las relaciones y órdenes entre estos subgrupos es mediante la *representación reticular*⁸. A continuación, se muestra el caso del grupo diédrico D_4 con la notación más común en la literatura:

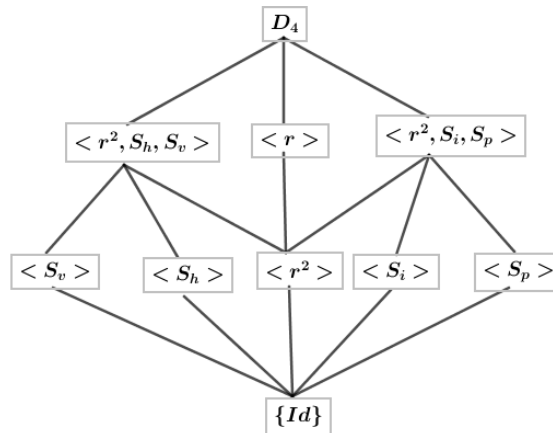


Figura 1.2 Retículo de subgrupos de D_4 ⁹

⁸ Esta representación es comúnmente usada en la teoría de retículos, y se basa en las siguientes dos propiedades: dados dos elementos de un conjunto siempre se puede encontrar un elemento mayor o igual a ambos elementos; por otro lado, con esta pareja de elementos se puede encontrar un elemento menor o igual a ambos elementos.

⁹ Elaboración basada de Calero (2019). Muestra todos los grupos que se pueden formar con D_4 ordenados, $\{Id\}$ es el menor y D_4 el mayor. Además, la notación $\langle r \rangle$ en la figura simboliza el grupo que es generado a partir de la rotación r .

Esta representación resulta bastante útil para analizar propiedades y la naturaleza que tiene una familia de subgrupos. Las permutaciones que están en este conjunto también pueden ser representadas de forma compuesta y cíclica para más comodidad. Así, la permutación r de D_4 (ver figura 1.1) se puede ver como (a, b, c, d) donde cada letra representa una esquina del cuadrado y la que está a su derecha a la que debe de ir, con esto a debe ir a b , b va a c , c debe ir a d y por último d va a a .

Los grupos diédricos son un caso particular en el que se analizan las simetrías de un polígono regular; sin embargo, en términos más generales se habla de los grupos de simetrías, los cuales son denotados por S_n donde n representa la cantidad de elementos del conjunto inicial¹⁰.

Subgrupos normales. Otros subgrupos que hay que considerar dentro de la teoría de Grupos son los subgrupos normales, que se definen y se ejemplifican en Judson (2017, p. 178):

Definición 1.3 Un subgrupo H de un grupo G es *normal* en G si $gH = Hg$ para todo $g \in G$. Es decir, un subgrupo normal de un grupo G es un subgrupo para el que las clases laterales derechas e izquierdas¹¹ coinciden.

En consideración, se tiene que si H es subgrupo normal de G lo denotamos por $H \triangleleft G$. Uno de los ejemplos más triviales es el siguiente:

Ejemplo. Sea G un grupo abeliano. Todo subgrupo H de G es un subgrupo normal. Como $gh = hg$ para todo $g \in G$ y $h \in H$, siempre se cumple que $gH = Hg$.

¹⁰ Como dato interesante y que representa la importancia que tienen los grupos de permutaciones en la teoría de grupos, existe el teorema de Cayley que permite asociar cualquier grupo con un grupo de permutaciones isomórficamente. Herstein (1988) lo enuncia como: todo grupo G es isomorfo a algún subgrupo de $A(S)$, para un S apropiado.

¹¹ Las clases laterales se construyen a partir de hacer el producto de un elemento $g \in G$ por izquierda o derecha con todo los elementos que pertenezcan a H . Esto se simboliza como gH si es por izquierda o Hg si es por derecha.

Hay que recalcar que esta propiedad de los grupos normales no asegura que un grupo o subgrupo sea abeliano, esta propiedad $gH = Hg$ asegura una igualdad entre grupos, no una igualdad entre elementos; en pocas palabras, un subgrupo de un grupo abeliano G es normal y abeliano, pero un subgrupo normal de G no necesariamente es abeliano.

1.4.2 Los homomorfismos

Una idea que resulta muy relevante dentro de la teoría de grupos es la de *homomorfismo*, este concepto tiene su importancia debido a que permite resolver problemas de un grupo a otro que podría tener una naturaleza más conocida y cómoda.

En palabra de Dummit & Foote (2003)¹² tenemos que:

Definición 1.4 Dado $(G, \star)$ y $(H, \diamond)$ grupos. Un mapeo $\varphi: G \rightarrow H$ tal que para todo $x, y \in G$, se tiene que $\varphi(x \star y) = \varphi(x) \diamond \varphi(y)$, es llamado un *homomorfismo*.

Esta definición implica inicialmente que estos “movimientos” están pensados para estructuras que tengan naturalezas parecidas (en este caso, de grupos a grupos). Sin embargo, como veremos en el mismo resultado de Galois o en el capítulo siguiente con los funtores adjuntos y las conexiones de Galois, los “movimientos” pueden darse entre estructuras que no necesariamente tienen igual naturaleza.

Para dar un ejemplo de homomorfismo considérense los grupos $G = (\mathbb{Z}, +)$ y $H = (\mathbb{R} - \{0\}, *)$ y el mapeo $\varphi: G \rightarrow H$ definido como $\varphi(n) = e^n$. Resulta que φ es un homomorfismo por lo siguiente:

$$\varphi(a + b) = e^{a+b} = e^a * e^b = \varphi(a) * \varphi(b)$$

¹² Las definiciones y citas de Dummit & Foote (2003) son traducciones libres.

$$\varphi(a + b) = \varphi(a) * \varphi(b)$$

Estos movimientos entre estructuras, se utilizan para trabajar problemas dentro de otra teoría o en otro contexto en el que se puedan tener más elementos para llegar a ciertos resultados. Como veremos más adelante, el problema de la resolución de polinomios que naturalmente se puede encontrar directamente en la teoría de anillos y cuerpos, es un problema que se puede trabajar en de la teoría de grupos.

Por ahora, es necesario entender esta definición de homomorfismo y algunas otras definiciones que surgen a partir de esta. En particular, interesan las definiciones de isomorfismo y auto-morfismo. Siguiendo a Dummit & Foote (2003), se tiene la siguiente definición:

Definición 1.5 Un mapeo $\varphi: G \rightarrow H$ es llamado un *isomorfismo* y G y H son llamados *isómorfos* o del mismo *tipo de isomorfismo*, denotado $G \cong H$, si

1. φ es un homomorfismo, y
2. φ es una biyección

Por último y continuando con la idea, un *automorfismo* se puede definir como un isomorfismo entre dos grupos que coinciden. Es decir, φ es un automorfismo si φ es un isomorfismo de G en G . Al seguir la idea que presenta Muñoz (2016, p. 58) se puede mostrar una definición formal de los automorfismos:

Definición 1.6 Un isomorfismo $\sigma: K \rightarrow K$ es llamado un automorfismo de K . La colección de automorfismos de K es denotado por $Aut(K)$.

Se mostrará más adelante que esta clase de grupos y conceptos como los automorfismos va a ser relevante para la metodología que emplea Galois. Pero antes es necesario revisar un tipo

de estructura más compleja en términos de sus operaciones y propiedades a comparación de la estructura de grupo, esta estructura es la de cuerpo.

1.4.3 La estructura de cuerpo

El desarrollo de la teoría de anillos y cuerpos surge como necesidad luego de hacer un análisis referente a la divisibilidad entre los números enteros, entre los polinomios y entre otros conjuntos de números. Inicialmente estos temas se vinculaban esencialmente a la teoría de números o a la geometría algebraica, pero sirvió de base para definir conceptos como anillo, cuerpo e ideal; dichos conceptos tuvieron una relevancia esencial para las matemáticas futuras a Galois, fueron la base para definir axiomáticamente y de forma contundente a los números reales, principalmente con los aportes de Dedekind (1831-1916), Cantor (1845-1918) y David Hilbert (1862-1943).

Ahora bien, la estructura inicial que hay que tener en cuenta es la de *anillo* puesto que sirve como base para definir a la estructura de cuerpo. Para el estudio de esta estructura se considera la presentación de Herstein (1988, p. 125-127):

Definición 1.7 Se dice que un conjunto no vacío R es un *anillo* si tiene dos operaciones $(+)$ y $(\cdot)$ tales que:

- a) $a, b \in R$ implica que $a + b \in R$.
- b) $a + b = b + a$ para $a, b \in R$.
- c) $(a + b) + c = a + (b + c)$ para $a, b, c \in R$.
- d) Existe un elemento $0 \in R$ tal que $a + 0 = a$ para todo $a \in R$.
- e) Dado $a \in R$, existe un $b \in R$ tal que $a + b = 0$. (b se expresará como $-a$).

Estas primeras propiedades muestran que R es un grupo abeliano con la operación $+$, sin embargo, aparecen dos propiedades más que relaciona a la segunda operación de la estructura:

- f) $a, b \in R$ implica que $a \cdot b \in R$.

$$g) \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{ para } a, b, c \in R.^{13}$$

Por último, y que convierte a la estructura de anillo sustancialmente diferente a la de grupo, es que se puede entrelazar sus operaciones mediante las dos siguientes *leyes distributivas*:

$$h) \quad a \cdot (b + c) = a \cdot b + a \cdot c \quad y \quad (b + c) \cdot a = b \cdot a + c \cdot a, \text{ para } a, b, c \in R.$$

Como se puede ver, esta definición no exige la existencia de un neutro para la multiplicación, sin embargo, cuando esto ocurre se denomina a la estructura como un *anillo con unidad*.

Definición 1.8 Se dice que un anillo con unidad R , es un *anillo con división* si para $a \neq 0$ en R existe un elemento $b \in R$ (que normalmente se expresa como a^{-1}) tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Teniendo estas definiciones en cuenta se puede definir adecuadamente la estructura de *cuerpo*. En este caso, Herstein (1988, p. 127) lo denomina como *campo* que es otra forma de nombrarlo¹⁴.

Definición 1.9 Se dice que un anillo R es un *campo* si R es un anillo con *división conmutativo*.

Esta estructura sugiere que se puede dividir sin ningún problema entre los elementos que sean distintos de cero, el ejemplo más cercano que podemos mirar de esta estructura son los números racionales con la suma y el producto.

¹³ Como dato relevante y que Herstein (1988) destaca, los anillos que cumplen este axioma (g) se denominan como *anillos asociativos*; sin embargo, es importante mencionar que en las matemáticas tienen mucha relevancia los *anillos no asociativos*. Carlos Vasco en su tesis doctoral *Homogeneous identities on algebraic loops* (1969) destaca la importancia de los desarrollos algebraicos no asociativos.

¹⁴ La denominación de campo es mucho más común en inglés con el término *field*.

Como nota adicional, la estructura de anillo y la de cuerpo normalmente se puede denotar como $(R, +, \cdot)$ donde R simboliza un conjunto de elementos; esto es distinto a denotarlo por $(R, \cdot, +)$. Respecto a esto, Panza (2019, p. 322) muestra un ejemplo con la suma y producto usual “se tiene evidentemente el anillo conmutativo unitario $(\mathbb{Z}, +, \cdot)$. Sin embargo, se puede ver que la terna $(\mathbb{Z}, \cdot, +)$ no es un anillo porque en $\mathbb{Z}$ la adición no es distributiva sobre la multiplicación”. Se sugeriría tener claridad respecto a la operación que prioriza respecto a las propiedades que deben de cumplir estas estructuras.

1.4.4 La extensión de un cuerpo

Al entrar más en los preliminares de la teoría de anillos y cuerpos hay que señalar la importancia de un concepto fundamental dentro de la teoría de Galois, este es la extensión de un cuerpo. En términos generales lo que se trata de encontrar, cuando se resuelven ecuaciones de un grado cualquiera, son los conjuntos en los cuales viven esas mismas soluciones.

Por ejemplo, no es necesario considerar el conjunto de los números irracionales o de los reales para resolver la ecuación $x^2 - 2 = 0$. No se requiere de conjuntos tan grandes para encontrar la solución, basta con hacer una extensión algebraica de los racionales que se puede simbolizar como $\mathbb{Q}(\sqrt{2})$ o también como $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ y que representa el conjunto de números de la forma $p + q\sqrt{2}$ con $p, q \in \mathbb{Q}$. Reticularmente esta extensión se puede representar como:



Figura 1.3 Extensión de $\mathbb{Q}$

Ahora bien, para generalizar más esta idea, se puede mirar la definición planteada por Dummit & Foote (2003) y el comentario que hace en su sección sobre la teoría básica de extensiones de campo:

Definición 1.10 Si K es un campo que contiene el subcampo F , entonces K se considera una *extensión del campo* (o simplemente una *extensión*) de F , denotado K/F o por el diagrama

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

En particular, todo campo K es una extensión de su subcampo principal F . El campo F es llamado algunas veces el *campo base* de la extensión.

Usualmente, la extensión de un campo se puede escribir como una *combinación lineal*¹⁵ de elementos del campo base junto con un elemento de la extensión que no está en el campo base; como ejemplo se puede ver la definición de los números complejos; estos se definen como una combinación $x + yi$ cuando $x, y \in \mathbb{R}$, en concreto, los números complejos son una extensión del campo de los reales.

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \end{array}$$

Figura 1.4 $\mathbb{C}$ como extensión de $\mathbb{R}$

¹⁵ Una combinación lineal es una expresión matemática que consiste en la suma entre pares de elementos, de determinados conjuntos y que son multiplicados entre sí. Por ejemplo, $7 = 2(2) + 3(1)$, lo cual implica que el 7 es combinación lineal de 2 y 3.

A partir de esta noción cabe preguntarse qué otras estructuras se pueden construir a partir de esta noción de extensión, en particular, ¿una estructura como la de los reales podría verse como una extensión de cuerpo? ¿Se podrían establecer combinaciones lineales que expresen los reales a partir de un campo base?

Por último, hay que considerar dos definiciones que serán relevantes más adelante, estas están relacionadas con los polinomios que se movilizan en una extensión de campo.

Definición 1.11 Un polinomio es separable dentro de una extensión K si sus raíces son distintas, esto quiere decir que el polinomio se puede expresar como producto de funciones lineales distintas.

Definición 1.12 La extensión K es normal respecto al polinomio $P(x)$ cuando contiene todas las raíces de $P(x)$.

Así, si se tiene $P(x) = x^2 - 2$, este polinomio es separable en la extensión $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, puesto que se puede expresar como $P(x) = (x - \sqrt{2})(x + \sqrt{2})$; y claramente la extensión es normal puesto que contiene todas las raíces del polinomio.

Estas definiciones –y en particular la de extensión de cuerpo- resultan interesantes para la resolución de nuevos problemas en matemáticas. En particular, un conjunto de problemas relevantes y atendidos desde esta visión algebraica son los problemas clásicos de la Antigüedad griega, los cuales deben ser resueltos con regla y compás: el primer problema consiste en construir un cuadrado con igual área que un círculo dado, el segundo consiste en dividir un ángulo en tres partes iguales y el tercero en construir un cubo con el doble de volumen que un cubo dado. En la siguiente subsección se ampliará esta idea dando algunos elementos respecto al problema de la trisección del ángulo, esto con el fin de destacar la noción de extensión de cuerpo.

1.4.5 La extensión de estructuras en la resolución de los clásicos problemas de la antigüedad griega

Una de las aplicaciones que se le pueden dar a la teoría de anillos y cuerpos, pero en especial a las extensiones, está en los problemas geométricos euclidianos, los cuales se pueden resolver modernamente utilizando solamente lenguaje algebraico, lo cual hace que el procedimiento operativo y demostrativo se vea hoy más limpio.

Algunos de los elementos de la geometría euclidiana se pueden interpretar en una versión moderna como una extensión de un cuerpo, dados unos puntos iniciales. En esto se basa la idea de los *objetos construibles* (o simplemente construibles), una estructura generada con unos puntos base, tal como lo expone Jacobson (1985) en su libro *Basic Algebra I*.

Jacobson parte de un conjunto finito de puntos $S = \{p_1, p_2, \dots, p_k\}$ en un plano w , estos puntos corresponden a puntos iniciales que requiere la construcción, con este conjunto define un subconjunto S_m , $m = 1, 2, \dots$, de puntos de w que se caracteriza por la interacción $S_{r+1} = \cup \{S_r\}$, esto significa que los puntos contruidos en S_{r+1} surgen a partir de la unión de los puntos de S_r . En este sentido, nótese que el conjunto S es la base de la interacción, esto es $S = S_1$.

Ahora, en cuanto a los detalles que definen la interacción y la construcción de nuevos puntos dados unos puntos base; se pueden diferenciar tres tipos de construcción de puntos. A continuación, se muestran esos tres tipos de construcciones.

En primer lugar, se construyen puntos de intersección de un par de líneas que conectan los puntos iniciales. En la siguiente figura se puede observar que a partir de la intersección de las rectas AC y BD , uno de los puntos construibles que se genera es el punto E :

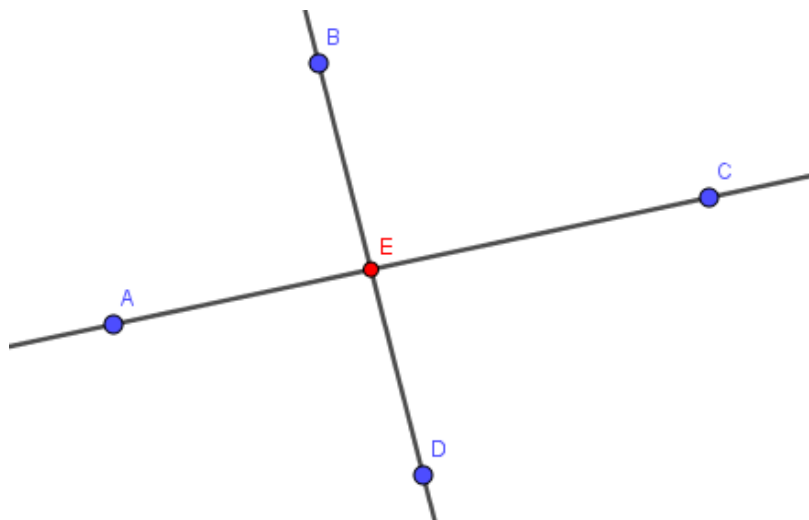


Figura 1.5 Puntos construibles de rectas dados los puntos iniciales

En cuanto a la notación conjuntista que propone Jacobson, este ejemplo gráfico se puede escribir de la siguiente forma: el conjunto inicial de puntos $S_1 = \{A, B, C, D\}$ que genera $S_2 = \{A, B, C, D, E, \dots\}$, el cual es otro conjunto con los puntos iniciales, el nuevo punto E y otros puntos contruidos a partir de las otras construcciones.

Además, se puede observar que los subíndices del conjunto S_m de construibles están dados de acuerdo con la relación inmediata que tengan con los puntos iniciales. Es decir, como E es construido a partir de los puntos iniciales entonces este estaría en los S_2 , pero si generamos un punto F a partir de la construcción de segmentos utilizando a E entonces este entraría en S_3 .

En segundo lugar, el siguiente tipo de construcción se basa en el conjunto de puntos de intersección entre, las rectas de la construcción anterior y todos los círculos con centros en un punto dado inicialmente y los radios iguales a los segmentos que generan esos puntos iniciales. Nótese la siguiente figura para favorecer la intuición:

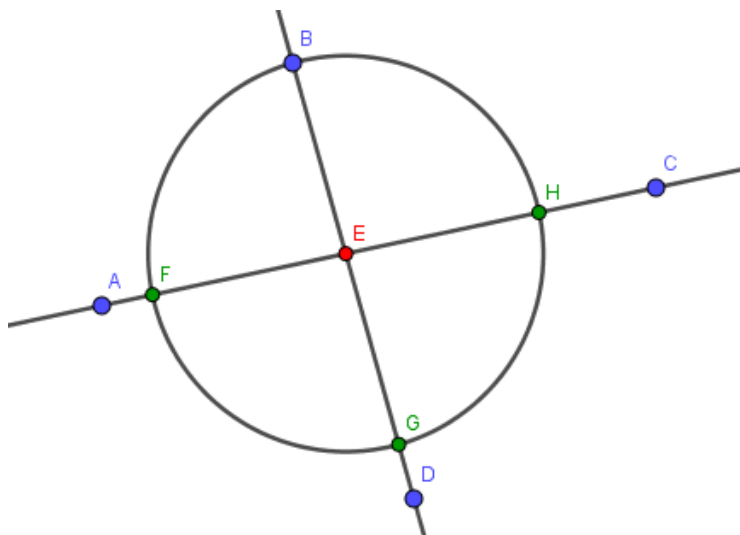


Figura 1.6 Puntos construibles a partir de rectas y circunferencias

Los puntos F, G y H corresponden a los mencionados anteriormente, esto debido a que son contruidos a partir de las intersecciones entre los segmentos de puntos iniciales BD y AC junto con la circunferencia con centro en E y radio EB . Estos puntos se pueden generar con los puntos iniciales -es decir $S_1 = \{A, B, C, D\}$ - y los generados a partir de las intersecciones de rectas entre estos -como ejemplo está el punto E - utilizándolo como centro y el radio igual al segmento entre el centro y uno de los puntos iniciales -es decir, EB -.

En este segundo ejemplo, la notación de Jacobson mostraría a $S_3 = \{A, B, C, D, E, F, G, H, \dots\}$, los puntos F, G y H no pertenecerían a S_2 puesto que son contruidos a partir del punto E que pertenece a S_2 .

Por tercer lugar, el último tipo de construcción se define a partir del conjunto de puntos de intersección de pares de círculos definidos a partir de los puntos iniciales o los contruidos con las dos anteriores construcciones. Nótese la siguiente figura para favorecer la intuición:

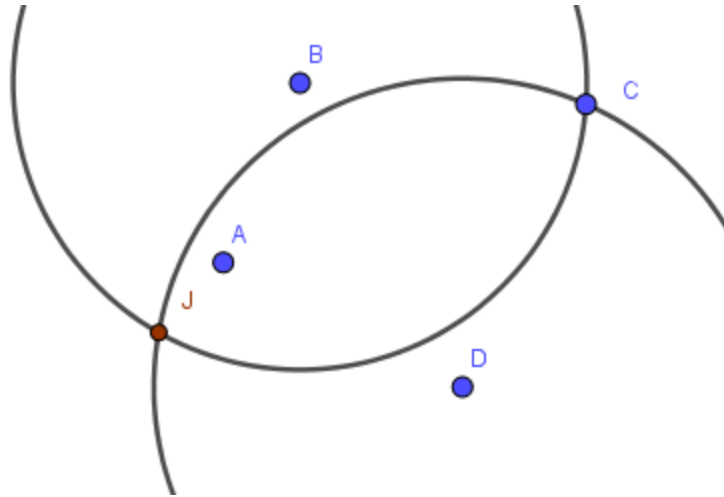


Figura 1.7 Puntos construibles de intersecciones entre circunferencias

El punto J corresponde a uno de los puntos especificados en el párrafo anterior. Esto debido a que es la intersección entre las circunferencias construidas a partir de los puntos iniciales, la primera circunferencia tiene centro en B y radio BC , mientras que la segunda tiene centro en D y radio DC .

Usando la notación de Jacobson para el anterior ejemplo, se tiene que $S_1 = \{A, B, C, D\}$ que genera $S_2 = \{A, B, C, D, J, \dots\}$, el punto J pertenece a S_2 debido a que es construido a partir de los puntos iniciales.

Con los anteriores tipos construcciones, la noción de los construibles se puede definir por $\mathcal{C}(p_1, p_2, \dots, p_k) = \bigcup_1^\infty S_i$; es decir, los construibles es la unión de todas las interacciones dados los puntos iniciales $p_1, p_2, \dots, p_k$.

Los construibles se pueden poner en correspondencia con un subconjunto de los números complejos, teniendo en cuenta que a cada punto le va a corresponder una coordenada (x, y) . Además, se prueba que es un cuerpo bajo las operaciones de suma y multiplicación, contando que cumple con la radicación y la existencia del conjugado para todo punto.

Lo anterior evidencia que, para demostrar la existencia de un punto en los construibles, se puede probar la existencia del número complejo en un campo generado a partir de los puntos base.

No sobra decir que esta definición de los construibles satisface los conceptos de la geometría euclidiana, tales como puntos, líneas, círculos y ángulos. En esta visión algebraica una línea es determinada por dos puntos, un círculo por su centro y por un punto en el círculo, y, por último, el ángulo por su vértice y dos puntos distintos equidistantes respecto al vértice (Jacobson, 1985).

Respecto al problema de la trisección del ángulo, Jacobson muestra que, en el caso particular del ángulo de 60° , este no puede ser trisecado mediante el uso de regla y compás exclusivamente. Para tal efecto, habría que mirar si el ángulo de 20° puede ser construido a partir del ángulo de 60° , lo cual requiere garantizar la existencia del punto $P = (\cos 20^\circ, \sin 20^\circ)$ a partir de los puntos $P_1 = (0,0)$, $P_2 = (1,0)$ y $P_3 = (\cos 60^\circ, \sin 60^\circ) = (\frac{1}{2}, \frac{1}{2}\sqrt{3})$. De esta forma, Jacobson asocia los puntos P_1, P_2 y P_3 con los números complejos $z_1 = 0$, $z_2 = 1$ y $z_3 = \frac{1}{2} + \frac{1}{2}\sqrt{3}i$, los cuales definen el campo $F = \mathbb{Q}(z_1, z_2, z_3, \bar{z}_1, \bar{z}_2, \bar{z}_3) = \mathbb{Q}(\sqrt{-3})$. A partir de aquí, el autor realiza varias deducciones que fueron construidas con base en algunos resultados explicitados en su libro, pero en concreto llega al análisis del polinomio $x^3 - 3x - 1$, en el cual el autor demuestra que tiene la propiedad de que cualquiera de sus raíces racionales es un entero y por lo tanto tiene como divisor al 1; pero esto último genera una contradicción debido a que ni 1 ni -1 son raíces, por lo que el polinomio $x^3 - 3x - 1$ es irreducible. Por lo tanto, no es posible la trisección del ángulo de 60° por regla y compás.

La potencia del álgebra y de *los construibles* en particular, está en que se puede dar respuesta a problemas como el de la trisección de un ángulo con regla y compás, además ofrece la

posibilidad de emplear construcciones mucho más generalizadas, puesto que esta idea no solo se limita a dos dimensiones. Si el lector desea profundizar en los tecnicismos que utiliza Jacobson (1985) para trabajar este y otros problemas como el de la duplicación del cubo, toda esta descripción detallada se encuentra en el capítulo 4 *Galois Theory of Equations* en la sección 4.2.

1.5 La resolubilidad de Galois y su teorema fundamental

Ahora bien, teniendo estudiados los elementos preliminares importantes dentro de la teoría de grupos, y la teoría de anillos y cuerpos, se puede profundizar en el resultado que garantiza la resolubilidad o no por medio de radicales a los polinomios independientemente de su grado.

Para esto, inicialmente hay que tener en cuenta la definición de *K-automorfismo*, la cual es derivada de las definiciones de automorfismo y las extensiones de cuerpo vistas en la anterior sección. Esta noción es clave para la unión de ambas teorías, por lo que mirando la definición de Calero (2019, p. 121) tenemos que:

Definición 1.13 Dado una extensión de cuerpos F/K donde $K \subset F$, decimos que $f: F \rightarrow F$ es un *K-automorfismo* si:

- f es un isomorfismo.
- f deja fijos los elementos de K , es decir, $f(\alpha) = \alpha$ si $\alpha \in K$.

También, con base en lo que se mencionó en la sección de los preliminares, y en particular acerca de los automorfismos; el conjunto de *K-automorfismos* de una extensión es un grupo con la composición de funciones y se denota $Aut(F/K)$; este grupo resulta ser un subgrupo del grupo $Aut(K)$.

Para ofrecer claridad, un ejemplo de estos K -automorfismos puede ser la conjugación compleja $\sigma: (a + bi) \rightarrow (a - bi)$ respecto al cuerpo base de los números reales ($\mathbb{R} \subset \mathbb{C}$), esto debido a que:

$$\sigma(a) = \sigma(a + 0i) = a - 0i = a$$

Por lo que $\sigma \in \text{Aut}(\mathbb{C}/\mathbb{R})$. En concreto, los reales se mantienen invariantes respecto al automorfismo que conjuga los números complejos. Esto mismo ocurre con el automorfismo identidad definido en la extensión compleja.

Ahora bien, el paso a seguir para determinar la resolubilidad o no de un polinomio, será particularizar los subgrupos de $\text{Aut}(F/K)$ cuando el polinomio asociado en la extensión cumple con la condición de ser separable y normal, en este caso se hablará del *grupo de Galois* y será denotado como $\text{Gal}(F/K)$.

Para dar un ejemplo, se puede retomar el que se miró en la sección de extensiones donde $\mathbb{Q}(\sqrt{2})$ es una extensión de $\mathbb{Q}$ y es generada a partir de mirar el conjunto solución de la ecuación $x^2 - 2 = 0$. Nótese que $P(x) = x^2 - 2$ es separable y normal en la extensión $\mathbb{Q}(\sqrt{2})$ puesto que se puede expresar como producto de factores lineales $P(x) = (x + \sqrt{2})(x - \sqrt{2})$ y la extensión contiene todas sus raíces.

Por tanto, el grupo de Galois $\text{Gal}(\mathbb{Q}(\sqrt{2}))$ o también $\text{Gal}(x^2 - 2)$ tiene todos los $\mathbb{Q}$ -automorfismos de $\mathbb{Q}(\sqrt{2})$ que dejan fijo a $\mathbb{Q}$.

Ahora, para mirar dentro de este caso cuáles son los automorfismos, la clave está en recordar cómo son los elementos dentro de la extensión, estos son de la forma $a + b\sqrt{2}$ con

$a, b \in \mathbb{Q}$ y a partir de esta forma, hay que alterar el signo que acompaña a la raíz, esto nos haría encontrar dos automorfismos que dejan invariante a $\mathbb{Q}$:

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$$

$$\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$$

Por lo que $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$, que si se estudia más a profundidad dentro de la teoría de grupos revela que es isomorfo al grupo cíclico C_2 ¹⁶; o en el caso que habíamos estudiado en los preliminares a S_2 , reconocer estos isomorfismos resulta muy útil debido a que se puede trabajar con estos grupos elementales reconociendo que sus propiedades funcionan de igual manera en el grupo inicial.

Otro ejemplo relevante respecto a la articulación entre los grupos de Galois y las extensiones de cuerpo se puede extraer de Judson (2017, p. 417) que considera los cuerpos $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Para esto, nótese que para $a, b \in \mathbb{Q}(\sqrt{5})$

$$\sigma(a + b\sqrt{3}) = a - b\sqrt{3}$$

Es un automorfismo de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ que deja fijo a $\mathbb{Q}(\sqrt{5})$, esto ocurre sustancialmente porque el automorfismo no se moviliza en $\mathbb{Q}(\sqrt{5})$. Por esta misma razón, obsérvese que

$$\tau(a + b\sqrt{5}) = a - b\sqrt{5}$$

¹⁶ Los grupos cíclicos son una clase de grupos que son generados por un elemento y sus potencias, C_2 en particular tiene la naturaleza de que al elevar al cuadrado su elemento se llega a la identidad, es decir: $x^2 = 1$ con $x \in C_2$.

Es un automorfismo de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ que deja fijo a $\mathbb{Q}(\sqrt{3})$. De aquí, el automorfismo $\mu = \sigma\tau$ mueve tanto a $\sqrt{3}$ como a $\sqrt{5}$. Con esto se destaca que $\{Id, \sigma, \tau, \mu\}$ es el grupo de Galois de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ sobre $\mathbb{Q}$. Este grupo tiene el siguiente comportamiento:

	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

Figura 1.8 Operatividad del grupo $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{5}/\mathbb{Q})$ ¹⁷

Y se puede establecer un isomorfismo con el grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ ¹⁸, el cual es un caso conocido en la teoría de grupos.

Esta forma de actuar revela un profundo resultado y que termina siendo uno de los grandes pasos para las matemáticas contemporáneas. En esencia, Galois hace una correspondencia entre dos estructuras diferentes, las extensiones de cuerpo asociadas a una ecuación y los subgrupos del grupo de Galois de la misma ecuación, dentro de su teoría esto se explicita como *Teorema Fundamental de la Teoría de Galois*; esta correspondencia no tiene para nada una naturaleza trivial, y más si se analiza desde el lente de las matemáticas contemporáneas con la teoría de categorías.

¹⁷ Tomada de Judson (2017, p. 417)

¹⁸ El grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ corresponde al producto directo de dos copias del grupo $\mathbb{Z}_2$, el cual es compuesto por dos elementos $\{0,1\}$. Estos dos elementos corresponden a los representantes de los posibles residuos que pueden tener los números enteros al dividirlos entre 2.

Para mirar un poco más el potencial del Teorema fundamental de la teoría de Galois se presentarán, en el capítulo siguiente, las conexiones de Galois como un caso particular de los funtores adjuntos. Para tal efecto, se tomará como referencia la sección 4.5 del libro de Jacobson (1985).

Sin embargo, por ahora hace falta analizar el resultado final que compete a resolver la pregunta: ¿qué tipos de ecuaciones se pueden resolver por radicales? Para esto es necesario mirar cuándo un grupo es *resoluble*.

En este sentido, una noción que se debe de tomar en cuenta es la de *serie subnormal*. Judson (2017, p. 225), la presenta de la siguiente manera:

Definición 1.14 Una *serie subnormal* de un grupo G es una sucesión finita de subgrupos

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

Donde H_i es un subgrupo normal de H_{i+1} . Si cada subgrupo H_i es normal en G , entonces la serie se llama *serie normal*. La *longitud* de una serie subnormal o normal es el número de inclusiones propias.

El ejemplo trivial de la anterior definición está relacionado con los grupos abelianos, y es que, toda serie de subgrupos de un grupo abeliano es una serie normal, el mismo Judson destaca algunos de estos casos:

$$\mathbb{Z} > 9\mathbb{Z} > 45\mathbb{Z} > 180\mathbb{Z} > \{0\}$$

$$\mathbb{Z}_{24} > \langle 2 \rangle > \langle 6 \rangle > \langle 12 \rangle > \{0\}$$

Sin embargo, Judson además destaca que una serie subnormal no necesariamente es una serie normal. Para esto, se destaca el caso del grupo D_4 :

$$D_4 > \{(1), (12)(34), (13)(24), (14)(23)\} > \{(1), (12)(34)\} > \{(1)\}$$

Aquí, el subgrupo $\{(1), (12)(34)\}$ no es normal en D_4 ; en consecuencia, esta no es una serie normal.

Con esto como base, se puede hablar respecto a la resolubilidad de un grupo, en concreto, Calero (2019, p. 124) lo define como sigue:

Definición 1.15 el grupo G es *resoluble* si existe una cadena de subgrupos normales:

$$\{e\} \triangleleft N_k \triangleleft N_{k-1} \triangleleft \cdots \triangleleft N_1 \triangleleft N_0 = G$$

De modo que los cocientes¹⁹ entre los grupos N_i/N_{i+1} son grupos abelianos.

La clave de esto, es que, si un grupo resulta ser resoluble, entonces el polinomio asociado a este grupo podrá ser resuelto por radicales.

Para hacer la aplicación de este resultado, se retoma el ejemplo del $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$, haciendo explícito que la permutación σ_1 se puede ver como la identidad del grupo Id_g .

Ahora bien, los subgrupos normales que se pueden establecer de este grupo son solo dos $N_1 = \{Id_g\}$ y $N_0 = \{Id_g, \sigma_2\}$, los cuales son normales porque inicialmente son subgrupos abelianos, y esto es una condición suficiente para asegurar la normalidad. De aquí se establece la cadena simple:

$$N_1 \triangleleft N_0$$

¹⁹ Judson (2017) define el grupo cociente como: Si N es un subgrupo normal de un grupo G , entonces las clases laterales de N en G forman un grupo G/N con la operación $(aN)(bN) = abN$. Este grupo se llama **cociente** de G por N . o sea el conjunto con todas las clases laterales de G sobre N .

A continuación se analiza el grupo cociente N_0/N_1 que termina siendo isomorfo al mismo N_0 pues al operar por izquierda la identidad Id_g que es el único elemento de N_1 con los elementos de N_0 obtenemos un grupo isomorfo a N_0 , además como se sabe que N_0 es abeliano, entonces el grupo de Galois es resoluble y la ecuación $x^2 - 2 = 0$ puede ser resuelta por radicales.

Otro ejemplo de grupo resoluble es el que presenta Judson (2017, p. 228), en el cual asegura que S_4 es soluble debido a que:

$$S_4 > A_4 > \{(1), (12)(34), (13)(24), (14)(23)\} > \{(1)\}$$

Tiene grupos cociente abelianos.

Los anteriores ejemplos recogen los elementos más elementales y profundos del resultado de Galois; sin embargo, si el lector quisiera ahondar un poco más en estos resultados, se puede sugerir la lectura de Jacobson (1985) a partir de la sección 4.7 que se titula como *Galois criterion for solvability by radicals*.

Por otro lado, surge la siguiente pregunta: ¿qué es lo que ocurre cuando miramos las ecuaciones de grado cinco o más? ¿El resultado de Galois es coherente con el resultado al que llegó Abel? Claramente la respuesta es afirmativa. Calero (2019, p. 124) lo muestra de la siguiente forma para el grado cinco:

... el grupo de Galois de algunas de ellas pueden ser A_5^{20} o S_5 ; pero A_5 es simple, es decir, la única cadena que puede formarse es $\{e\} \triangleleft A_5$. Este resultado es el que probaron Abel y Ruffini, y se conoce como “teorema de Abel”, o “de Abel-Ruffini”, la prueba de que A_n es simple para $n \geq 5$.

Entonces, A_5 no puede ser resoluble, pues $A_5/\{e\} \cong A_5$, que no es abeliano, y así se incumple la definición de resoluble. Por su parte, S_5 tampoco será resoluble, ya que las únicas cadenas que se pueden formar son $\{e\} \triangleleft S_5$ o $\{e\} \triangleleft A_5 \triangleleft S_5$. Pero ambos casos incumplen la

²⁰ A_5 es el grupo formado a partir de elevar al cuadrado los elementos de S_5 ; esto es, aplicar dos veces las permutaciones que se encuentran en S_5 .

condición de resolubilidad, pues $S_5/\{e\} \cong S_5$ y $A_5/\{e\} \cong A_5$, que no son abelianos, y se incumple la condición del teorema.

Es por esta razón que se puede considerar que Galois fue un paso más allá comparado al resultado de Abel, Lagrange y Ruffini respecto a la resolubilidad de ecuaciones por medio de radicales, Galois construyó un algoritmo que determina si una ecuación puede ser resuelta por radicales o no.

Este resultado de Galois tiene amplias implicaciones que no hay que pasar por alto; en este sentido, en los siguientes capítulos se profundizará respecto a las relaciones de estudios contemporáneos que se pueden establecer y algunas reflexiones que genera esta nueva forma de hacer matemáticas. El cambio del álgebra clásica al álgebra moderna se generó a partir de esta forma de pensar, y esto no es un hecho trivial.

CAPITULO 2

Los funtores adjuntos y el caso particular de las conexiones de Galois

*Los matemáticos no estudian los objetos, sino las relaciones entre los objetos; por tanto, les es indiferente reemplazar estos objetos por otros, con tal que no cambien las relaciones. La sustancia no les importa, sólo les interesa la forma*²¹

Henri Poincaré

Para la segunda parte del trabajo se tiene en cuenta el estudio realizado por Valencia (2021) en su tesis doctoral *Le concept d'adjunction dans la théorie des catégories: son développement et son importance*. De igual manera se considera la primera parte del trabajo de Armstrong (2016) sobre conexiones de Galois y funtores adjuntos, titulado *Fancy Algebra*, entre otras referencias bibliográficas principalmente centradas en la teoría de categorías.

Ya se ha hablado del resultado de Galois y en algún momento se ha hecho énfasis en lo relevante que pudo haber sido para las matemáticas; sin embargo, vale la pena preguntarse sobre la forma en la que pudo influir en las matemáticas posteriores a este resultado ¿tiene esta metodología e ideas de Galois influencia en las matemáticas contemporáneas? ¿Cuál pudo ser el cambio sustancial de las matemáticas respecto al resultado de Galois? Un posible enfoque para responder

²¹ Citado por Dávila (2003).

estas preguntas se puede guiar estudiando los resultados que se obtuvieron en las matemáticas contemporáneas y que siguen siendo objeto de estudio hoy en día.

Para tal efecto, es necesario mirar algunos elementos preliminares referentes a las matemáticas contemporáneas, y en particular a la teoría de categorías que es una teoría consolidada actualmente. De igual forma, vale la pena analizar la naturaleza de la relación que establece Galois entre las estructuras de cuerpo y de grupo. Como se presentó anteriormente este parece ser el primer caso importante en el que se pueden establecer comparaciones entre estructuras que *a priori* no tienen naturalezas similares y esto es razón suficiente como para no tomarlo a la ligera.

Con el fin de abordar las anteriores temáticas, este segundo capítulo, en primera instancia, pretende ambientar al lector a la teoría de categorías, destacando la noción de funtor adjunto; posteriormente tiene la intención de retomar los resultados del primer capítulo al dedicar una sección al teorema fundamental de la teoría de Galois. Este teorema dará paso a las conexiones de Galois, para finalmente relacionar los funtores adjuntos con las conexiones de Galois. Esta estructura se escoge con el ánimo de establecer un paralelismo entre las matemáticas contemporáneas y las matemáticas modernas, las cuales se articularían al final del capítulo.

En este sentido, este capítulo lleva a entender lo que se conoce por teoría de categorías y parte de su génesis que puede explicar su esencia. En primer lugar, se destacan los trabajos Eilenberg (1913-1998) y Mac Lane (1909-2005) que pueden ser considerados como los fundadores de la teoría de categorías con las definiciones básicas en el artículo *General Theory of Natural Equivalences* publicado en 1945; sin embargo, como lo destaca Valencia (2021) conceptos relevantes como el de funtor o equivalencia natural son definidos desde antes en el artículo *Natural Isomorphism in Group Theory* publicado en 1942.

Estas nociones que inicialmente surgen como necesidad dentro del estudio de la topología algebraica tuvieron especial importancia debido al lenguaje más simplificado que lo caracterizaba, o como lo expresa Español (1999, p. 1) esta teoría tiene “...la finalidad de obtener un lenguaje que permitiera expresar de modo concreto y simple construcciones matemáticas cuya complejidad en detalle era muy aparatosa”. A pesar de esto, la teoría de categorías empezó a ser mucho más explotada a finales de los años 50 cuando, entre otras cosas, se empieza a estudiar a fondo la noción de *functor adjunto*. Esta noción será importante tenerla presente para determinar la relación con el resultado principal de la teoría de Galois.

2.1 Las estructuras más generales: las categorías

Anteriormente se habían visto dos estructuras elementales, y que precisamente reciben su importancia dentro de las teorías que llevan sus nombres, el protagonista de esta sección no será la excepción. Su relevancia radica en que es mucho más general que las estructuras de grupo y de cuerpo, de hecho, es capaz de trabajar estructuras como los grupos y los cuerpos como si fueran simples “elementos” de su composición; este es el concepto de *Categoría*, que surge a partir de la generalización de las estructuras y la previa definición de los funtores. Eilenberg & MacLane (1945) fueron los encargados de introducir esta idea; en concreto, su primera definición se apoyó de ejemplos como los grupos junto con homomorfismos o los espacios junto con asignaciones continuas.

Definición 2.1a Una categoría $\mathfrak{A} = \{A, \alpha\}$ es un agregado de elementos abstractos A (por ejemplo, grupos), llamados **objetos** de la categoría, y unos elementos abstractos α (por ejemplo, homomorfismos), llamados **morfismos**²² de la categoría. Cierta par de morfismos $\alpha_1, \alpha_2 \in \mathfrak{A}$ determinan únicamente un morfismo producto $\alpha = \alpha_1 \alpha_2 \in \mathfrak{A}$, y sujetos a los

²² O mapeos, acorde a la traducción exacta del documento original.

axiomas C_1 , C_2 y C_3 . Correspondiente a cada objeto $A \in \mathfrak{A}$ hay un único morfismo, denotado e_A o también $e(A)$, y sujeto a los axiomas C_4 y C_5 .

C₁. El triple producto $\alpha_3(\alpha_1\alpha_2)$ está definido si y solo si $(\alpha_3\alpha_1)\alpha_2$ está definido. Cuando cualquiera se define, la ley asociativa

$$\alpha_3(\alpha_2\alpha_1) = (\alpha_3\alpha_2)\alpha_1$$

Se mantiene. Este triple producto se escribe $\alpha_3\alpha_2\alpha_1$.

C₂. El triple producto $\alpha_3\alpha_2\alpha_1$ es definido siempre que $\alpha_3\alpha_2$ y $\alpha_2\alpha_1$ estén definidos.

C₃. Para cada morfismo $\alpha \in \mathfrak{A}$ hay al menos una identidad $e_1 \in \mathfrak{A}$ tal que αe_1 está definida, y al menos una identidad $e_2 \in \mathfrak{A}$ tal que αe_2 está definida.

C₄. El morfismo e_A corresponde a todos los morfismos identidad del objeto A .

C₅. Para cada identidad $e \in \mathfrak{A}$ hay un único objeto A de $\mathfrak{A}$ tal que $e_A = e$.

No obstante, una definición más cercana al desarrollo de la teoría de categorías actual puede favorecer su comprensión, a continuación, se presenta la definición que plantea Roman (2017), la cual respeta la génesis de Eilenberg & MacLane (1945); queda para el lector considerar una de las dos definiciones para la comprensión de las presentaciones futuras, además -como tarea- encontrar diferencias a rescatar entre ambas definiciones:

Definición 2.1b Una categoría consiste de lo siguiente:

1. **(Objetos)** Una clase **Obj**(C) cuyos miembros son llamados **objetos**. Regularmente se escribe $A \in C$ en lugar de $A \in \mathbf{Obj}(C)$.
2. **(Morfismos)** Para cada (no necesariamente distintos) par de objetos $A, B \in C$, un conjunto $\text{hom}_C(A, B)$ es llamado el conjunto hom (o **hom-set**) para el par (A, B) . Los elementos de $\text{hom}_C(A, B)$ son llamados **morfismos**, **mapeos** o **flechas** de A a B . Si $f \in \text{hom}_C(A, B)$, también se escribe

$$f: A \rightarrow B \text{ o por } f_{AB}$$

El objeto $A = \text{dom}(f)$ es llamado el **dominio** de f y el objeto $B = \text{codom}(f)$ es llamado el **codominio** de f .

3. Distintos hom-set son disyuntos, esto es, $\text{hom}_C(A, B)$ y $\text{hom}_C(C, D)$ son disyuntos a no ser que $A = C$ y $B = D$.

4. **(Composición)** para $f \in \text{hom}_C(A, B)$ y $g \in \text{hom}_C(B, C)$ hay un morfismo $g \circ f \in \text{hom}_C(A, C)$, llamada **composición** de g con f . Además, la composición es asociativa:

$$f \circ (g \circ h) = (f \circ g) \circ h$$

Siempre que la composición sea definida.

5. **(Morfismo identidad)** para cada objeto $A \in C$ hay un morfismo $1_A \in \text{hom}_C(A, A)$, llamado **morfismo identidad** para A , con la propiedad de que si $f_{AB} \in \text{hom}_C(A, B)$ entonces

$$1_B \circ f_{AB} = f_{AB} \quad \text{y} \quad f_{AB} \circ 1_A = f_{AB}$$

La clase de todos los morfismos de C es denotado por **Mor**(C).

La definición de categoría -cualquiera de las dos presentadas-, muestra sustanciales diferencias con las definiciones de grupo, anillo y cuerpo presentadas anteriormente, principalmente porque no es suficiente con definir un conjunto de elementos, o que en este caso se determinan como objetos, sino que también es necesario establecer una clase de relaciones entre estos objetos para mirar la operatividad²³. Otra diferencia consiste de la única propiedad que se establece entre morfismos -la asociatividad- no es necesario que una categoría cumpla más propiedades cuando se toman morfismos diferentes. Por último, en las categorías no existe un

²³ Como dato relevante, y que además muestra un desprendimiento de la intuición que se tiene de la teoría de conjuntos, la definición de categoría por lo general se presenta como: *una categoría consta... o una categoría se compone...* estos verbos se ponen para no definir a una categoría en términos de conjuntos.

morfismo identidad para todos los objetos, sino que, para cada objeto, existe un morfismo identidad.

2.1.1 Un ejemplo de categoría: La categoría de los conjuntos finitos

Esta forma de definir las categorías si bien logra simplificar mucho más el lenguaje y generalizar mucho más las ideas estructurales de las matemáticas, puede ser una definición aislada a los lectores que tengan un primer contacto con la teoría de categorías y la naturaleza de los conceptos que la definen, es por eso que habría que mirar estos detalles con algo más de familiaridad. Para empezar, se pueden mirar los **objetos** debido a que no aparentan definirse explícitamente como el concepto de elementos en un conjunto (que es la naturaleza que normalmente se le asocia a los que actúan dentro de una estructura algebraica).

Véase entonces a Lawvere y Schanuel (2002, p. 11-12) para estudiar este concepto con un lenguaje más familiar. Así, se puede definir la categoría de los conjuntos finitos:

Un **objeto** en esta categoría es un conjunto finito (o una colección finita), He aquí algunos ejemplos: (El conjunto de todos los estudiantes en la clase) es un objeto, (El conjunto de todos los escritorios en la clase) es otro objeto.

Por otro lado, está el concepto de morfismo dentro de categoría, que ejemplificado en la categoría de los conjuntos finitos puede verse de la siguiente forma:

Un **morfismo** f en esta categoría consiste de tres cosas:

1. Un conjunto A , llamado el *dominio* del morfismo,
2. Un conjunto B , llamado el *codominio* del morfismo,
3. Una regla que le asigna a cada elemento a en el dominio, un elemento b en el codominio.

Esta b se denota por $f \circ a$ (o en algunas ocasiones " $f(a)$ "), y se lee " f de a ".

(En otras palabras, para el término morfismo son: "función", "transformación", "operador", "flecha" y "mapeo").

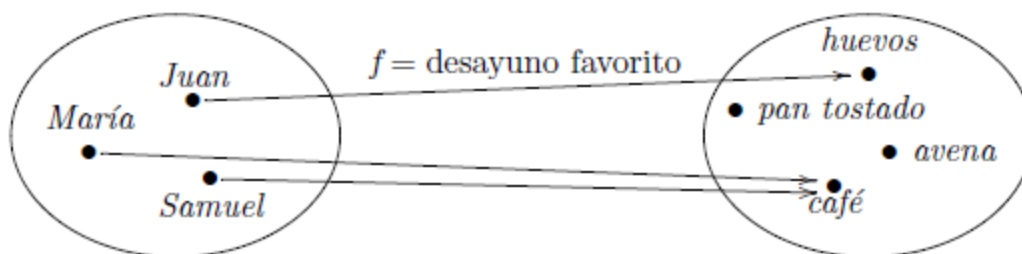


Figura 2.1 Morfismos entre dos objetos²⁴

Si bien mirar los objetos y los morfismos con relación a su categoría podría llevar a interpretaciones referentes a su analogía con los conjuntos y los elementos, que incluso puede ayudar a entender más el concepto de categoría (principalmente por el hecho de que a pesar de que la categoría se compone de objetos, los que actúan y se relacionan son los morfismos bajo la operación de composición) no se conecta sustancialmente con la intención de estudio aquí, sin embargo podría ser interesante analizarlo en futuros trabajos, desde incluso una visión didáctica.

En el caso del **morfismo identidad** que hace parte de lo que compone una categoría se refiere al morfismo en el cual para cada objeto se va a dejar exactamente igual, es decir, “en el que el dominio y el codominio son el mismo conjunto A , y para cada a en A , $f(a) = a$ ” (Lawvere y Schanuel, 2002, p. 14).

Gráficamente como lo siguiente:

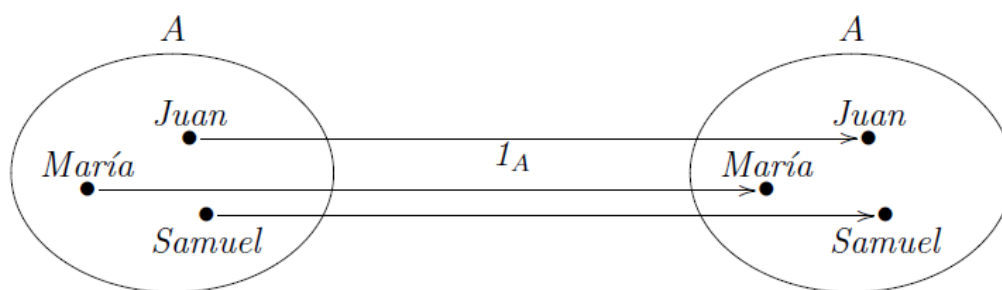


Figura 2.2 Morfismos identidad²⁵

²⁴ Tomada de Lawvere y Schanuel (2002, p. 12).

²⁵ Tomada de Lawvere y Schanuel (2002, p. 13)

En esencia este es un caso particular de morfismo pero que tiene que cumplirse para definir a la categoría correctamente.

Por último, está la **composición de morfismos** “a través de la cual dos morfismos se combinan para dar lugar a un tercero” (p. 14).

Se puede dar un ejemplo:

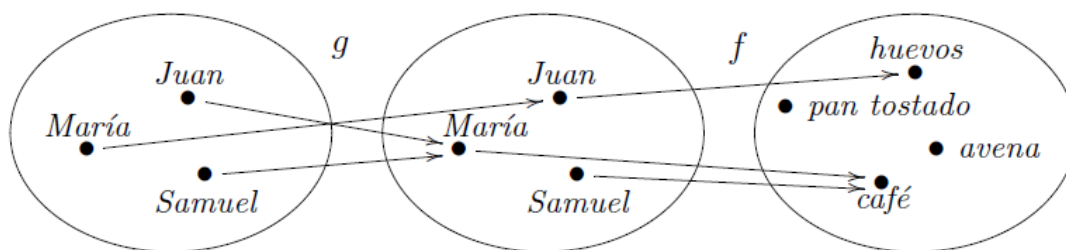


Figura 2.3 Composición de morfismos

Y podrían generarse preguntas como: ¿qué le da de desayunar Juan a la persona que le gusta? Con respuestas tipo: Juan le daría café a María.

2.2 Los funtores adjuntos

Si bien ya se ha visto lo que define una categoría y un ejemplo concreto que puede ser mucho más cómodo para un primer acercamiento a la teoría, habría que conocer sustancialmente el potencial que tiene este lenguaje para justificar su consolidación actual; y es que como se mencionó anteriormente la misma teoría de categorías empieza a hacerse fuerte cuando en los años 50 se estudian los funtores adjuntos y otros conceptos referentes a su teoría.

Valencia (2021) destaca dos publicaciones que cautivan el interés en esta teoría donde solo parecía tener progreso por parte de sus fundadores; en concreto, el libro *Foundations of Algebraic Topology* de Eilenberg y Steenrod de 1952, y el artículo *Acyclic Models* de Eilenberg y MacLane de 1953. La incidencia de estos textos -particularmente la del libro- ha sido tal que los matemáticos

se han interesado en estas nuevas herramientas conceptuales. Antes de la aparición de estos artículos, los conceptos categoriales habían sido solamente utilizados por sus creadores.

Pero antes de mirar ese concepto trascendental de funtor adjunto naturalmente surge la pregunta: ¿qué es un funtor? Para responder a esta pregunta cabe mencionar que existen dos tipos de funtores, estos son los covariantes y los contravariantes; en particular, este estudio se centra en los funtores covariantes; sin embargo, los contravariantes no son un tipo de funtores aislados y distintos, su única característica diferente consiste en que, al aplicarse, cambian el sentido de los morfismos.

En este sentido, Eilenberg y MacLane (1945) definen estos funtores de la siguiente forma:

Definición 2.2a La función entre objetos $T(A, B)$ y la función entre morfismos $T(\alpha, \beta)$ forman un funtor T , covariante en $\mathfrak{A}$ y contravariante en $\mathfrak{B}$, con valores en $\mathfrak{C}$, si

$$(i) \quad T(e_A, e_B) = e_{T(A, B)},$$

Si se cumple que $\alpha: A_1 \rightarrow A_2$ en $\mathfrak{A}$ y $\beta: B_1 \rightarrow B_2$ en $\mathfrak{B}$, entonces

$$(ii) \quad T(\alpha, \beta): T(A_1, B_2) \rightarrow T(A_2, B_1),$$

Y si, siempre que $\alpha_2 \alpha_1 \in \mathfrak{A}$ y $\beta_2 \beta_1 \in \mathfrak{B}$, entonces

$$(iii) \quad T(\alpha_2 \alpha_1, \beta_2 \beta_1) = T(\alpha_2, \beta_1) T(\alpha_1, \beta_2)$$

En una notación más cómoda y familiar Roman (2017) también presenta los funtores:

Definición 2.2b Sean C y D categorías, un funtor $F: C \Rightarrow D$ es un par de funciones²⁶:

(i) La **parte objeto** del funtor

$$F: \mathbf{Obj}(C) \rightarrow \mathbf{Obj}(D)$$

Asigna objetos en C a objetos en D .

(j) La **parte flecha** del funtor

²⁶ El término “función” está relacionado con la teoría de conjuntos, por lo que un término más apropiado en este caso sería el de aplicación o transformación.

$$F: \mathbf{Mor}(C) \rightarrow \mathbf{Mor}(D)$$

Asigna morfismos en C a morfismos en D de la siguiente forma:

- a. Para un **funtor covariante**,

$$F: \text{hom}_C(A, B) \rightarrow \text{hom}_D(FA, FB)$$

Para todo $A, B \in C$, esto es, F mapea un morfismo $f: A \rightarrow B$ en C a un morfismo $Ff: FA \rightarrow FB$ en D .

- b. Para un **funtor contravariante**,

$$F: \text{hom}_C(A, B) \rightarrow \text{hom}_D(FB, FA)$$

Para todo $A, B \in C$, esto es, F mapea un morfismo $f: A \rightarrow B$ en C a un morfismo $Ff: FB \rightarrow FA$ en D . (Nótese la dirección inversa)

- (k) Identidad y composición son preservadas, esto es,

$$F1_A = 1_{FA}$$

Y para un funtor covariante,

$$F(g \circ f) = Fg \circ Ff$$

Y para un funtor contravariante,

$$F(g \circ f) = Ff \circ Fg$$

Siempre que todas las composiciones estén definidas.

Esta definición de Roman no se aleja de la que se construye en su génesis y en desarrollos posteriores como los de Cartan y Eilenberg en su libro *Homological Algebra*, publicado en 1956 y que mejora su comprensión con la versión que plantea Grothendieck (Valencia, 2021).

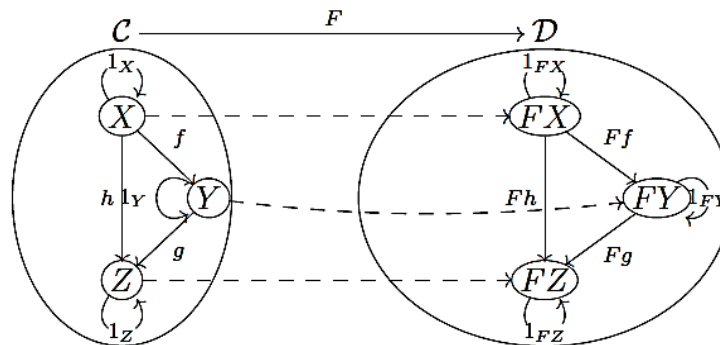


Figura 2.4 funtor F de la categoría C a D ²⁷

²⁷ Tomado de Valencia (2021, p. 49)

Naturalmente puede interpretarse a un funtor como una función (como intuitivamente siempre se ha trabajado) entre categorías, y si bien esta intuición didácticamente puede favorecer la construcción de la noción, hay que afirmar que el funtor es una idea mucho más general; esta idea se hace explícita cuando se abstrae que las categorías no necesariamente son conjuntos con elementos, que son con los que sustancialmente se trabaja en funciones.

Además, existe el análisis respecto a la forma de “devolverse” de una categoría a otra, aquí se podría intuir la existencia de lo que es un “funtor inverso”; sin embargo, esto no es tan simple como lo puede mostrar la idea de función y su función inversa. Para empezar a estudiar “las idas y vueltas” de una categoría a otra habría que mirar la noción de *funtor adjunto*.

La idea de funtor adjunto se formaliza por primera vez en 1958 en el artículo *Adjoint Functors* escrito por Daniel Kan (1927-2013) y tiene el plan fundamental de establecer relaciones de ida y vuelta entre dos categorías, esto implica definirlo como una pareja de funtores. Respecto a su surgimiento, este se presenta con el desarrollo del *álgebra homológica*²⁸ y la necesidad por generalizarse y sistematizarse en la categoría de los grupos abelianos.

Anaconda (2017, p. 244) en su tesis doctoral presenta sustancialmente la misma definición de Kan, esto lo hace dejando claro que existen otras definiciones equivalentes a la que presenta Kan, a continuación, se muestra su presentación:

Definición 2.3 Sean $\mathcal{X}$ y $\mathcal{A}$ dos categorías y sean $F: \mathcal{X} \rightarrow \mathcal{A}$ y $G: \mathcal{A} \rightarrow \mathcal{X}$ funtores entre ellas. Entonces, F y G son funtores adjuntos, si para todo x en $\mathcal{X}$ y a en $\mathcal{A}$, existe un isomorfismo ϕ natural²⁹ en x y en a :

²⁸ El álgebra homológica se encarga de estudiar la noción de homología, el cual es un procedimiento que establece correspondencias entre objetos y sucesiones de grupos abelianos; un libro clásico de esta teoría es el mencionado anteriormente *Homological Algebra* de Eilenberg y Cartan de 1956.

²⁹ La noción de naturalidad en teoría de categorías está asociado a las relaciones que se pueden establecer entre funtores, principalmente se estudia la transformación natural que es un funtor entre funtores (o también entre

$$\varphi_{x,a}: \text{hom}_{\mathcal{A}}(Fx, a) \cong \text{hom}_{\mathcal{X}}(x, Ga)$$

Notación: $\text{hom}_{\mathcal{A}}(Fx, a)$ es el conjunto de todos los morfismos de Fx en a , en la categoría $\mathcal{A}$.

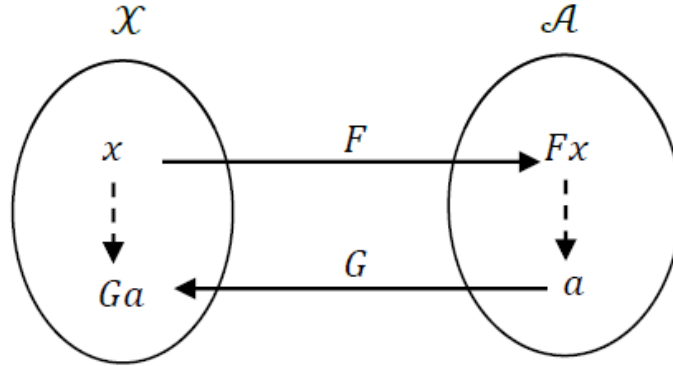


Figura 2.5 representación gráfica de funtores adjuntos³⁰

Una ampliación que puede hacerse es que, en este caso, a F se le denomina como adjunto izquierdo de G y a G como adjunto derecho de F .

De esta presentación podría hacerse una interpretación con apoyo de la gráfica: del objeto x en la categoría $\mathcal{X}$ pasamos a la categoría $\mathcal{A}$ mediante el funtor F dando la imagen Fx , de aquí ocurre que no necesariamente el funtor F tiene un funtor directamente “inverso”, por lo que para volver a la categoría inicial $\mathcal{X}$ habría que construir un camino relacionando a Fx con un objeto dentro de su categoría que se denomina a , esta relación (o flecha) no necesariamente puede ser única, por esto existe la notación $\text{hom}_{\mathcal{A}}(Fx, a)$ que simboliza todas esas relaciones que se pueden establecer entre estos dos objetos; ahora bien, resulta que a posee una imagen en $\mathcal{X}$ mediante el funtor G que se simboliza por Ga y x (que es el objeto inicial) resulta estar relacionado con Ga , esto explicita a $\text{hom}_{\mathcal{X}}(x, Ga)$.

flechas); en este caso el isomorfismo natural indica una equivalencia entre dos familias flechas, véase a (Armstrong, 2016, p. 30-31).

³⁰ Tomada de Anaconda (2017, p. 245)

A partir de aquí, lo que se empieza a analizar es si las colecciones de flechas $\text{hom}_{\mathcal{X}}(x, Ga)$ y $\text{hom}_{\mathcal{A}}(Fx, a)$ se comportan de manera similar -hablando naturalmente-.

Nótese que en el caso en el que $\text{hom}_{\mathcal{X}}(Ga, x)$ exista, es decir, en el esquema la flecha de la categoría $\mathcal{X}$ vaya hacia arriba, estamos hablando del caso particular en el que los funtores son inversos como normalmente se intuye este concepto, es por esto que la idea de funtor adjunto puede ser considerada como más general a la de una función junto con su inversa. Esta última interpretación se recoge de la idea de Marquis (2006), quien destaca que los funtores adjuntos no son, estrictamente hablando, inversos entre sí. Los inversos estrictos son isomorfismos de categorías. Pero los funtores adjuntos son inversos de alguna forma y eso es lo que los hace tan importantes. Es tentador y ciertamente atractivo decir que los funtores adjuntos son inversos conceptuales entre sí.

2.3 Teorema fundamental de la teoría de Galois

En este punto de la presentación, se presenta un contexto contemporáneo de las matemáticas desarrolladas a partir de la segunda mitad del siglo XX. Parece que la teoría de categorías tiene algunas relaciones con el planteamiento de Galois, principalmente la relación se ve desde la necesidad de las estructuras; sin embargo, las relaciones entre estructuras no son tan explícitas en la presentación del primer capítulo respecto al problema de la resolución de ecuaciones por radicales.

Es por esto que, desde este capítulo, que tiene una perspectiva más estructural de las matemáticas, parece conveniente exponer el resultado más importante de la teoría de Galois, este es el Teorema fundamental de la teoría de Galois; este resultado expresa mejor la relación que se

establece entre las extensiones de cuerpo y los subgrupos del grupo de Galois asociados a las extensiones.

Esta correspondencia entre los subgrupos y los subcuerpos se estudia incluso desde una visión más general con el concepto de *conexión de Galois* propuesto por el matemático noruego Ore (1899-1968), y como se verá en la siguiente sección, este concepto será el esencial para establecer la relación con el funtor adjunto.

Para la presentación del teorema se considera a Jacobson (1985) en su sección 4.5. Sin embargo, hay dos apartados importantes previos al teorema, el primero corresponde a la definición de *invariantes* en un campo y el segundo, a un teorema base para el teorema fundamental.

Definición 2.4 Sea G cualquier grupo de automorfismos en un campo E (que es, un subgrupo del grupo de automorfismos de E), y sea:

$$\text{Inv } G = \{a \in E \mid \eta(a) = a, \eta \in G\}$$

En otras palabras, $\text{Inv } G$ es el conjunto de elementos de E que no son movidos -o que son invariantes- para cualquier $\eta \in G$.

Note que como mínimo este conjunto contiene al campo base, debido a que los automorfismos del grupo de automorfismos cumplen la propiedad de dejar invariante a este campo.

Por otro lado, esto también asegura unos movimientos que se pueden establecer entre las estructuras, es decir, si se tiene el subgrupo G , se obtiene $\text{Inv } G$; y si se tiene el subcampo F , se obtendría el grupo de Galois $\text{Gal}(E/F)$ para la extensión E de F .

$$G \rightarrow \text{Inv } G$$

$$F \rightarrow \text{Gal}(E/F)$$

Este mapeo incluso cumple cuatro propiedades con las que vale la pena familiarizarse dentro de la teoría de Galois:

1. $G_1 \supset G_2 \Rightarrow \text{Inv } G_1 \subset \text{Inv } G_2$.
2. $F_1 \supset F_2 \Rightarrow \text{Gal } (E/F_1) \subset \text{Gal } (E/F_2)$.
3. $\text{Inv } (\text{Gal } E/F) \supset F$.
4. $\text{Gal } (E/\text{Inv } G) \supset G$.

Teniendo clara esta definición, junto con las propiedades de los mapeos a la hora de “ir y volver” entre los subgrupos y subcampos, se puede presentar un teorema previo al teorema fundamental:

Teorema 2.1 Sea E una extensión del campo F . Entonces las siguientes condiciones en E/F son equivalentes:

1. E es un campo con división sobre F de un polinomio separable $f(x)$.
2. $F = \text{Inv } G$ para algún grupo finito de automorfismos de E .
3. E es normal de dimensión finita y separable sobre F .

Además, si E y F son como en 1) y $G = \text{Gal } (E/F)$ entonces $F = \text{Inv } G$, y si G y F son como en 2), entonces $G = \text{Gal}(E/F)$.

La clave de este teorema está en que, para que se pueda utilizar el teorema fundamental, el campo a trabajar tiene que cumplir una de estas condiciones, esto justifica la necesidad de que haya una equivalencia entre las proposiciones. Teniendo en consideración esto, se muestra a continuación el Teorema fundamental de la teoría de Galois:

Teorema 2.2 (Teorema fundamental de la teoría de Galois). Sea E una extensión del campo F satisfaciendo una (por lo tanto, todas) de las condiciones equivalentes del Teorema 2.1. Sea G el grupo de Galois de E bajo F . Además, definamos $\Gamma = \{H\}$, como el conjunto de subgrupos de G , y Σ , el conjunto de campos intermedios entre E y F (los subcampos de E/F). Los mapeos $H \rightarrow \text{Inv } H$, $K \rightarrow \text{Gal } (E/K)$, $H \in \Gamma$, $K \in \Sigma$, son

inversos y entonces son biyecciones de Γ en Σ y de Σ en Γ . Además, se tienen las siguientes propiedades:

- a. $H_1 \supset H_2 \Leftrightarrow \text{Inv } H_1 \subset \text{Inv } H_2$.
- b. $|H| = [E: \text{Inv } H]$, $[G: H] = [\text{Inv } H: F]$.
- c. H es normal en $G \Leftrightarrow \text{Inv } H$ es normal sobre F . En este caso $\text{Gal } \text{Inv } (H/F) \cong G/H$.

Como se puede ver, la primera propiedad establece una relación inversa entre los subgrupos del grupo de Galois junto con los invariantes; la segunda propiedad tiene dos partes, en la primera establece la igualdad entre la cantidad de elementos del subgrupo y la dimensión de su invariante respecto a la extensión, en la segunda parte se establece la igualdad en las dimensiones del grupo respecto al subgrupo y con la del invariante con el cuerpo base. La última parte del teorema establece una relación respecto a la normalidad de un subgrupo respecto al grupo y la normalidad de los invariantes sobre el cuerpo base.

Con el ánimo de ilustrar el potencial del teorema de manera clara, considérese el caso de la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ del campo $\mathbb{Q}$, note que esta extensión también es extensión de los campos $\mathbb{Q}(\sqrt{2})$ (esta extensión se trabajó en el primer capítulo), $\mathbb{Q}(\sqrt{5})$ además del campo $\mathbb{Q}(\sqrt{10})$. Como estas extensiones no se contienen a sí mismas, pero contienen al campo base, se puede establecer el siguiente retículo:

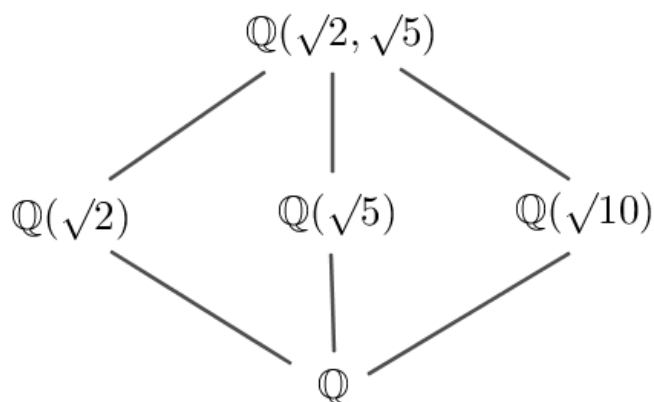


Figura 2.6 Retículo de campos de la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{5})$

Y a esta composición le corresponde un retículo con los subgrupos del grupo de Galois, pero ordenado de forma inversa:

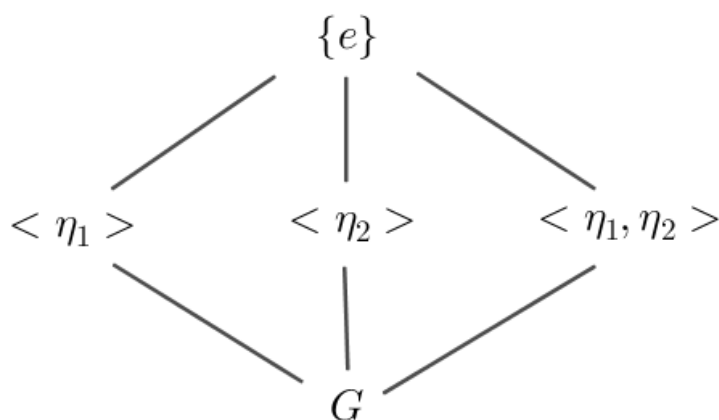


Figura 2.7 Retículo invertido de los subgrupos de G

La ilustración de esta correspondencia se muestra a continuación:

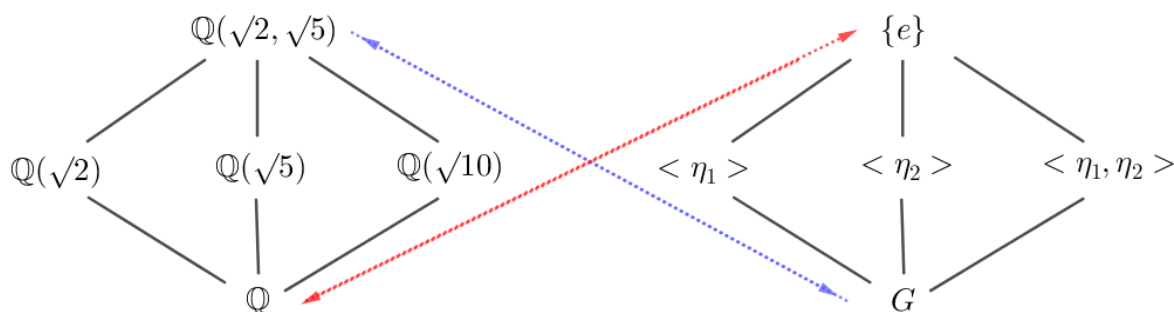


Figura 2.8 Correspondencia reticular del teorema de Galois

Esto evidencia la primera parte del teorema en un caso concreto. Esta primera parte resulta especialmente relevante por las correspondencias que se pretenden aclarar con los resultados de las siguientes secciones; no obstante, el lector no se sorprenderá al revisar que se cumplen las otras condiciones del teorema fundamental para el caso presentado anteriormente.

2.4 Las conexiones de Galois

Como se vio en el primer capítulo, la genialidad de Galois está en que pudo ver estas relaciones, que además de resolver el problema de las fórmulas generales por radicales, amplió el panorama respecto a una nueva forma de hacer matemáticas.

El matemático noruego Oystein Ore (1899-1968), destacado por sus trabajos en teoría de anillos, teoría de grafos y en historia de las matemáticas; adicionando la influencia de la Universidad de Göttingen y su nuevo enfoque en álgebra abstracta de Emmy Noether, fue el encargado de generalizar más estas relaciones que establece Galois.

Ore, logró fundamentar el concepto de conexiones de Galois, que reduce el caso de las relaciones entre los subgrupos y las extensiones a un caso particular; para esto, es necesario presentar la noción de conjunto parcialmente ordenado o simplemente *poset* por sus siglas en inglés, dicha noción es clave para establecer las conexiones.

En este sentido, Lezama (1996, p. 2) presenta los conjuntos parcialmente ordenados de la siguiente forma:

Definición 2.5 (Poset). Un par $(X, \preceq)$ es una clase preordenada si X es una clase no vacía y $\preceq$ es una relación reflexiva y transitiva³¹ en X .

Dando ejemplos de un poset, se tiene a los racionales junto con la desigualdad $(\mathbb{Q}, \leq)$, así como los naturales con la igualdad $(\mathbb{N}, =)$.

Sin embargo, los subconjuntos de un conjunto X diferentes de vacío con la contención estricta, es decir $(P(X) - \{\emptyset\}, \subset)$, no son un poset puesto que no cumple con la propiedad reflexiva. De igual manera, los reales junto con la desigualdad estricta tampoco son un poset porque falla la propiedad reflexiva.

Quedaría como actividad para el lector pensar si la relación: x es amigo de y en el conjunto de personas en el mundo es un poset. Así como generar otros ejemplos.

Teniendo como base la anterior definición, la presentación de Ore (1944, p. 495) de conexión de Galois se muestra a continuación:

Definición 2.6 (Conexión de Galois)³². Sean P y Q dos conjuntos parcialmente ordenados. Y se asume que existe una correspondencia de P a Q ,

$$p \rightarrow \mathfrak{Q}(p),$$

Y también una correspondencia de Q a P ,

$$q \rightarrow \mathfrak{P}(q),$$

Estas dos correspondencias juntas son llamadas una *correspondencia de Galois* entre P y Q si cumplen completamente las dos siguientes condiciones:

³¹ Recordando estas definiciones, una relación es reflexiva si dado un elemento x en el conjunto X , él está relacionado con él mismo, generalmente tiene la notación $R(x, x)$. Por otro lado, una relación es transitiva si dados $x, y, z \in X$, se tiene que $R(x, y) \wedge R(y, z) \rightarrow R(x, z)$.

³² Esta presentación es una traducción libre; además, a diferencia de la versión original, se denotan las relaciones de forma distinta entre ambos posets para evitar ambigüedades.

- a. Cuando $p_1 \succcurlyeq p_2$ con dos elementos en P o $q_1 \sqsupseteq q_2$ con dos elementos en Q , entonces

$$\mathfrak{Q}(p_1) \sqsubseteq \mathfrak{Q}(p_2), \quad \mathfrak{P}(q_1) \preceq \mathfrak{P}(q_2)$$

- b. Para un elemento p en P o q en Q

$$\mathfrak{P}\mathfrak{Q}(p) \succcurlyeq p \quad \mathfrak{Q}\mathfrak{P}(q) \sqsupseteq q$$

Note la diferencia que hay entre ambas relaciones, $\succcurlyeq$ está actuando en P , mientras que $\sqsupseteq$ es la relación del poset Q . Esta definición, además de presentar dos propiedades fundamentales, también cumple las siguientes mostradas por Lezama (1996) pero manteniendo la notación de Ore (1944):

1. $\mathfrak{Q}\mathfrak{P}\mathfrak{Q}(p) = \mathfrak{Q}(p)$
2. $\mathfrak{P}\mathfrak{Q}\mathfrak{P}(p) = \mathfrak{P}(p)$
3. Para todo $a \in P$, $(\mathfrak{P}\mathfrak{Q}(p), \mathfrak{Q}(p))$ es un par fijo de Galois.
4. Para todo $b \in Q$, $(\mathfrak{P}(q), \mathfrak{Q}\mathfrak{P}(q))$ es un par fijo de Galois.
5. $p \preceq \mathfrak{P}(q) \Leftrightarrow \mathfrak{Q}(p) \sqsubseteq q$ para cualquier p en P y q en Q .

Con la última propiedad (5) es suficiente para asegurar una conexión de Galois, de ahí viene la relevancia en su presentación.

Un caso particular de conexión de Galois, y que el lector podría comprobar utilizando esta última propiedad es considerando las funciones $f: \mathbb{Z} \rightarrow \mathbb{R}$, $g: \mathbb{R} \rightarrow \mathbb{Z}$ definidas como $f(x) = 3x$ y $g(x) = \lceil x/3 \rceil$, considerando la notación $\lceil a \rceil$ como el entero igual o mayor a a .

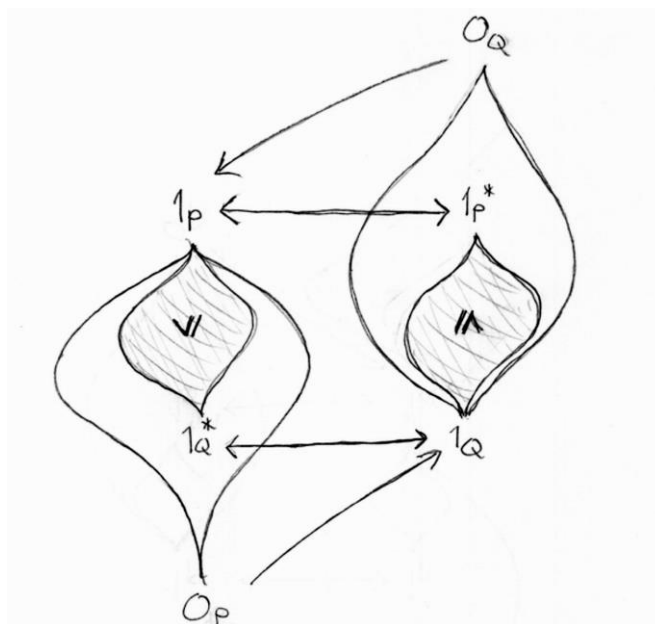


Figura 2.9 Comportamiento esquemático de las conexiones de Galois³³

Armstrong (2016) propone que la conexión de Galois es como una “biyección suelta”, pues no es necesariamente una biyección, pero se puede convertir en una; esta idea se puede asemejar a la que se mostró de Marquis (2006) respecto a los funtores adjuntos y su interpretación como inversos conceptuales entre sí.

Es aquí donde se ve la particularidad del teorema fundamental de la teoría Galois. Nótese que en ese caso los poset que se relacionan son la colección generada por la extensión de cuerpo Σ , y la colección de los subgrupos del grupo de Galois $\Gamma = \{H\}$, teniendo como relaciones transitivas y reflexivas la contención de campos y la de grupos.

$$\begin{array}{ccc}
 & \leftarrow & \\
 (\Sigma, \subseteq) & \Rightarrow & (\Gamma, \leq) \\
 & \rightarrow &
 \end{array}$$

³³ Interpretación de Armstrong (2016, p. 20)

2.5 La categoría de los posets y sus funtores adjuntos

Hasta este punto se ha sugerido una relación estrecha entre los funtores adjuntos y las conexiones de Galois, sin embargo, no es tan evidente la particularidad de las conexiones en términos de los funtores adjuntos, de aquí la necesidad de hablar sobre la categoría de los *posets* y las tres consideraciones que la definen.

Como primera consideración, los objetos de esta categoría son los elementos de los conjuntos, estos pueden ser subconjuntos de un conjunto o números, depende de cuál sea la naturaleza de los conjuntos con los que se trabaja.

Como segunda consideración, los morfismos o flechas establecidas para estas categorías son las relaciones de orden que se pueden hacer entre los elementos del conjunto; por ejemplo, si se tiene la relación $a \leq b$ esta se puede expresar como $a \rightarrow b$. Nótese que el morfismo identidad está en estas relaciones para cualquier objeto de la categoría, esto se asegura por la reflexividad de la relación.

Como tercera y última consideración, obsérvese que la composición entre los morfismos se cumple y además es asociativa; es decir, si $x \xrightarrow{\alpha} y$ y $y \xrightarrow{\beta} z$, se obtiene $x \xrightarrow{\beta \circ \alpha} z$, considerando que $\alpha: x \leq y$ y $\beta: y \leq z$, en esencia esto se cumple porque las relaciones son transitivas. Además, $(\gamma \circ \beta) \circ \alpha = \gamma \circ (\beta \circ \alpha)$, pues se cumple el siguiente esquema:

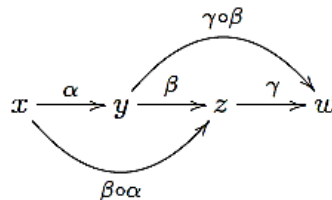


Figura 2.10 Asociatividad entre morfismos de una categoría³⁴

³⁴ Tomada de Armstrong (2016, p. 10)

Por otro lado, note que los funtores están definidos a partir de las relaciones que se establecen en los posets, por ejemplo, si la categoría A es el poset de los subconjuntos de un conjunto X con la relación de contención y la categoría B es el poset de los números naturales con la desigualdad usual, entonces el funtor F va estar definido como:

$$A \subseteq B \xrightarrow{F} F(A) \leq F(B)$$

Esto es lo que se considera como una aplicación monótona, debido a que preserva el orden, en contraposición con una antitona que invierte el orden. Con base en esto, la adjunción en el caso de los *posets* se puede definir de la forma que muestra Armstrong (2016):

Definición 2.7 (Adjunción de posets). Sean $(P, \leq_P)$ y $(Q, \leq_Q)$ dos posets. Un par de funciones $L: P \rightleftarrows Q : R$ es llamado una adjunción si para todo $p \in P$ y $q \in Q$ se tiene:

$$p \leq_P R(q) \Leftrightarrow L(p) \leq_Q q$$

En este caso se escribe $L \dashv R$ y se llama a esto un par adjunto de funciones. La función L es el adjunto izquierdo, y la función R el adjunto derecho.

Respecto a esta definición se tienen tres consideraciones para relacionarlo con la definición de funtores adjuntos presentada en anteriores secciones. La primera es que la notación $hom_{\mathcal{A}}(x, a)$ no es necesario usarla puesto que la relación -flecha- entre dos objetos dentro de un poset es única, a diferencia de las posibles infinitas relaciones que se pueden establecer entre los objetos de una categoría. La segunda consideración es que la equivalencia ($\Leftrightarrow$), se puede interpretar, en el lenguaje de la teoría de categorías, como un caso particular de la equivalencia isomórfica ($\cong$). Y en la tercera consideración, se nota que, a diferencia de la definición presentada de la conexión de Galois, esta definición no invierte el orden del poset Q . En resumen, esta adjunción de poset es un caso particular de los funtores adjuntos, pero no es tan particular como una conexión de Galois.

Armstrong (2016), para precisar la definición de conexión de Galois en términos de funtores adjuntos, propone el *poset opuesto* Q^{op} del poset Q , tal que para todo $q_1, q_2 \in Q$:

$$q_1 \leq_{Q^{op}} q_2 \Leftrightarrow q_2 \leq_Q q_1$$

Por lo tanto, la adjunción de los poset $P \rightleftarrows Q$ es como la conexión de Galois $P \rightleftarrows Q^{op}$.

En conclusión, a partir de este resultado se puede entender a las conexiones de Galois como un caso particular de la adjunción de poset, y en consecuencia, un caso particular de los funtores adjuntos. Lo anterior evidencia que, para definir las conexiones de Galois en términos de la teoría de categorías, hay que recurrir a la categoría de los poset -un caso particular de categoría-; añadiendo la condición del poset opuesto en la segunda categoría.

Esta presentación no solo muestra un cambio de perspectiva respecto a la forma de hacer matemáticas desde mediados del siglo XX, sino también una posible génesis en Galois respecto a las prácticas estructuralistas y que sirvieron para dar respuesta a la pregunta sobre la ecuación general por radicales.

CAPÍTULO 3

Algunas reflexiones desde la práctica matemática

¿Qué es entonces una filosofía de la matemática real? La intención de este término es la de trazar una línea entre el trabajo documentado con las preocupaciones de los matemáticos pasados y presentes y aquél hecho sobre la base de, en el mejor de los casos, un contacto nominal con su historia o prácticas³⁵

David Corfield

Si bien la naturaleza de este trabajo es esencialmente histórico-epistemológica, es importante mencionar que dicho análisis se realiza a la luz del nuevo concepto histórico-filosófico de “práctica matemática”, el cual nos ofrece un amplio panorama de reflexión en el cual se puede ver el fuerte vínculo que existe entre la historia de las matemáticas y la educación matemática.

Desde esta perspectiva, se reconoce la importancia que tiene el análisis histórico de la evolución de un concepto o teoría, dado que aporta elementos de orden epistemológico claves para ahondar en la comprensión del mismo concepto y conocer sus relaciones con otras disciplinas matemáticas. De igual forma aporta luces de orden didáctico para abordar de una mejor manera su tratamiento en el aula. Sin embargo, se considera de manera complementaria que resulta muy

³⁵ De (Corfield, 2003)

importante estudiar las prácticas que puede desarrollar un ser humano a partir de la comprensión y apropiación de un objeto en matemáticas.

Por la anterior razón, en este capítulo, se reflexionará sobre la *práctica matemática* y los elementos que la definen. Con estos elementos teóricos, se trata de identificar prácticas matemáticas en el pensamiento de Galois que hayan sido determinantes en el desarrollo de su teoría que puedan ser vinculadas a la génesis del estructuralismo matemático.

En este sentido, se presentan a continuación algunos lineamientos generales sobre esta línea de la filosofía de las matemáticas.

3.1 La práctica matemática

La investigación en el tema de la *práctica matemática* ha tenido especial importancia en los últimos años debido a que compone una de las recientes líneas de estudio en filosofía de las matemáticas. Esta línea tiene varios enfoques dentro de las reflexiones en la educación matemática, algunos protagonistas contemporáneos de estos planteamientos son filósofos como Paolo Mancosu, José Ferreirós, Philip Kitcher, Jessica Carter, entre otros.

3.1.1 Enfoques de estudio en la práctica matemática

En primera instancia, antes de presentar las discusiones sobre lo que se podría considerar práctica matemática, habría que tener un panorama general acerca de los diversos enfoques en los que se han venido desarrollando. Carter (2019) destaca tres:

En primer lugar, está la *filosofía de la práctica matemática* -que a partir de ahora se puede abreviar por FPM- basada en agentes, en esta postura se sostiene que es imposible tratar de hacer filosofía de las matemáticas sin tener en cuenta a los seres humanos que hacen matemáticas. El énfasis está en los practicantes, sus actividades en desarrollo, en cómo hacen uso y aprenden las

matemáticas. En este enfoque, se pueden diferenciar dos perspectivas de estudio, la primera tiene fuertes relaciones con la sociología, y parte de la consideración de las matemáticas como una actividad social; mientras que la segunda centra su atención en el funcionamiento cognitivo de la mente del individuo que transmite la capacidad de formar conceptos matemáticos. En este sentido, la FPM basada en agentes aporta elementos relevantes para el campo de la educación matemática; puesto que trata de una construcción social que va en contra de la idea platónica de “deshumanizar” las matemáticas.

Como segundo enfoque, está la FPM histórica. Desde este enfoque, a diferencia del anterior, la atención se centra en los resultados de las actividades que realizan los practicantes de las matemáticas. Aquí se generan preguntas relacionadas con cómo estos resultados matemáticos se han formado a lo largo del tiempo; esta perspectiva parte de la suposición de que las matemáticas son producto de ciertas actividades y no de una teoría estática, aquí se enfatiza en los factores culturales y sociales que ayudan a la construcción de las matemáticas. La FPM histórica adquiere importancia con cuestionamientos respecto a la influencia mutua entre la filosofía y la historia de las matemáticas; sobre cómo el desarrollo de las matemáticas ha influido en el pensamiento filosófico y viceversa.

Como tercer y último enfoque se destaca la FPM epistemológica, la cual destaca algunos aspectos de la filosofía tradicional, como tratar de evitar suposiciones dependientes de los agentes humanos (aunque este agente no necesariamente está excluido), así como tratar de responder a preguntas como cuál es la naturaleza de los objetos matemáticos y qué constituye el conocimiento humano sobre ellos. A pesar de que se tiene de referencia la filosofía tradicional, esto no implica

el uso de la epistemología tradicional en el sentido de “una visión desde ninguna parte”³⁶ y la posibilidad de obtener un conocimiento absoluto. La importancia de esta línea para un campo como la Educación Matemática puede estar en la intención de dar sentido a la naturaleza de los objetos que se emplean en la disciplina matemática.

3.1.2 Definición de práctica matemática

Con la anterior sección como telón de fondo, se pueden considerar varias discusiones respecto a la definición de práctica matemática, en particular, una discusión relevante surge a partir de la propuesta hecha por Kitcher (1984, p. 163-164) en la cual destaca el desarrollo de la práctica matemática con base en la relación entre cinco componentes:

Como una notación conveniente, uso la expresión $\langle L, M, Q, R, S \rangle$ como un símbolo para una práctica matemática arbitraria (donde L es el lenguaje de la práctica, M el conjunto de visiones metamatemáticas, Q el conjunto de cuestiones aceptadas, R el conjunto de razonamientos aceptados y S el conjunto de proposiciones aceptadas).

Lo interesante de esta definición es que muestra elementos que al relacionarse componen una práctica, además, sugiere unas condiciones para que haya crecimiento en el conocimiento matemático a partir de un cambio en la práctica; por ejemplo, si hay un cambio en el componente de lenguaje de la práctica, la práctica matemática cambiará respecto a la establecida inicialmente, así como se muestra a continuación:

$$\langle L, M, Q, R, S \rangle \Rightarrow \langle L', M', Q', R', S' \rangle$$

³⁶ Esta “visión desde ninguna parte” tiene la intención de ver los objetos aislados totalmente de cualquier contexto en particular, se podría entender desde una visión platónica como el tratar de ver a los objetos que están en el mundo de las ideas, fuera del mundo sensible.

Esta idea manifiesta profundamente la importancia de la historia de las matemáticas, debido a que es uno de los factores para generar cambios en los componentes que definen a la práctica; con esto en consideración, se puede inferir que la historia es un elemento relevante para el profesor de matemáticas, debido a que muestra las particularidades, las prácticas y los contextos que permiten justificar la naturaleza de un objeto.

Bello (2017, p. 5) sostiene la importancia de este elemento, en el cual “se reconoce una historia de las matemáticas para el profesor de matemáticas, la que permite conocimiento matemático a partir de la comprensión de las prácticas que permitieron la constitución de los objetos matemáticos”.

Además, muestra la existencia de una relación de estos componentes de la práctica -según la definición de Kitcher (1984)- con los dominios de conocimiento del profesor de matemáticas³⁷, en el cual se pueden destacar algunas consideraciones respecto a los cambios en las componentes.

Al especificar una consideración por cada componente se puede mirar, en primer lugar, al lenguaje, el cual puede cambiar en la sintaxis y la semántica dentro de la enseñanza, producto de que surge a partir de la resolución de un problema en un momento determinado. En segundo lugar, las visiones históricas metamatemáticas, las cuales pueden permitir ver las diferentes fases de un mismo conocimiento matemático con las diferentes creencias que no permitieron en su momento desarrollar un objeto matemático. En tercer lugar, están las cuestiones aceptadas, las cuales permiten mirar las limitaciones de las teorías matemáticas, que en educación develaría la importancia del desarrollo de aquellas teorías. En cuarto lugar, el cambio de modelos de razonamientos y heurísticas permite al profesor convertirse en experto en la comprensión de estos

³⁷ Estos dominios vienen del modelo *Mathematical Knowledge Teacher* (MKT), si el lector quisiera empezar a familiarizarse con esto, se sugiere hacer una lectura al marco teórico de Bello (2017).

modelos para mejorar la enseñanza en términos de la resolución de problemas. Por último, está el cambio en el conocimiento de proposiciones aceptadas, la cual permite el establecimiento de una verdad en matemáticas, sus consecuencias y estatus en una teoría.

Volviendo a la definición de práctica matemática planteada por Kitcher (1984), esta podría manifestar un enfoque más histórico acorde a los presentados en la sección anterior; sin embargo, como lo plantea Carter (2019) esta definición parte de unas suposiciones que la hacen inapropiada para una definición general; en primer lugar, esta definición de práctica carece de practicantes, Kitcher se refiere a unas prácticas con “agentes idealizados”, es decir, los agentes reales quedan excluidos; además, esta propuesta defiende una visión antirrealista, por lo que también excluye los objetos matemáticos.

En este sentido, Ferreirós (2016) también discrepa respecto a esta definición, en concreto sostiene que la práctica debe tomarse en el sentido de las actividades de los agentes humanos y que el conocimiento no tiene sentido sin los conocedores. De aquí, considerando el par marco de referencia-agente, o simplemente marco-agente propone la cuádrupla de Kitcher $\langle L, S, Q, R \rangle$ excluyendo las visiones meta-matemáticas, puesto que las incluye dentro del agente. Ferreirós también sostiene que las prácticas no son universales y únicas en un momento dado³⁸, sino que coexisten varios niveles de prácticas y conocimientos.

Respecto a esta última idea, la teoría de Galois podría servir como ejemplo considerando el desarrollo del álgebra clásica al álgebra moderna. Las ideas de Galois, si bien son brillantes, surgen a partir de unas prácticas y conocimientos anteriores como los planteados por Lagrange, es

³⁸ Esta idea adquiere relevancia con ejemplos como la demostración en los *Elementos* en comparación con la de las otras matemáticas, la primera si bien muestra unas pruebas que son aceptadas por la comunidad, esto no implica que sean las únicas pruebas válidas para el resto de matemáticas.

decir, las prácticas de Galois -que hoy en día se podrían asociar a un pensamiento estructuralista- se construyen a partir de unos antecedentes académicos y contextuales que permitieron el estímulo de unas nuevas prácticas.

Siguiendo con la discusión sobre cómo definir a una práctica, Carter (2019) considera los trabajos de Ferreirós y de Epple³⁹. Este último lo destaca por considerar los agentes humanos que desarrollan matemáticas y que piensan en los objetos matemáticos y epistemológicos; ambos trabajos junto con el de Kitcher, si bien Carter los considera valiosos cuando se investigan cuestiones relacionadas con las actividades al hacer matemáticas, ella interpreta que son insuficientes por no cubrir todos los enfoques de la FPM para definir lo que es una práctica.

En consecuencia, Carter (2019) propone una definición de práctica que recoge los elementos importantes de Kitcher, Ferreirós y Epple; en general, una práctica es capturada por una dupla que consiste de “agentes” y “matemáticas”, la cual puede ser escrita como $\langle A, M \rangle$. La componente A consiste de agentes, ya sean reales o idealizados, junto con sus actividades y creencias; mientras que M se refiere a los contenidos de las matemáticas, ya sean teorías, teoremas, pruebas, modelos matemáticos, entre otros. En general, una práctica consiste en diversas relaciones entre los agentes y lo que constituyen las matemáticas.

Para justificar que la anterior propuesta considera todos los enfoques de FPM, Carter (2019) afirma en primer lugar que, la FPM basada en agentes empieza por los agentes -la componente A - y considera a las matemáticas solo en relación con esos agentes; en segundo lugar, la FPM histórica empieza en el nivel de las matemáticas -la componente M - y considera el

³⁹ Moritz Epple es un matemático alemán e historiador de la ciencia nacido en 1960 en Stuttgart, es reconocido por investigaciones en historia del análisis matemático, así como por haber sido profesor en importantes instituciones académicas como Dübner Institute for the History of Science and Technology del Massachusetts Institute of Technology (MIT). Desde 2013 es co-editor de la revista *Science in Context*.

desarrollo de una parte particular de las matemáticas a través de una interrelación entre agentes y las matemáticas; y por último, la FPM epistemológica empieza en algún lugar del espacio establecido entre los dos - las componentes *A* y *M*-, con mayor énfasis en los estudios de casos matemáticos, con la intención de transcender los ejemplos a generalizaciones, o incluso a idealizaciones basadas en las consideraciones de la práctica real. Es así como esta perspectiva da cuenta de los tres enfoques presentados.

Teniendo en cuenta la anterior discusión que permite tener un acercamiento a eso que se denomina como práctica, vale la pena considerar algunas de estas prácticas estudiadas en la FPM para entender la necesidad de esta línea en la filosofía de las matemáticas, es por esto que la siguiente sección se centra en presentar a grandes rasgos diferentes estudios sobre algunas prácticas matemáticas.

3.2 Las consideraciones de Mancosu

El hecho de considerar una definición de práctica matemática -como se presenta en la sección anterior- parte del hecho de aceptar que existe una práctica matemática; sin embargo, este subcampo de la filosofía de las matemáticas no en todos los casos ha sido aceptado como relevante. Según Mancosu (2016), una de las razones es que dos de los artículos clásicos del filósofo contemporáneo Paul Benacerraf⁴⁰, tuvieron mucha influencia por pensar sobre el acceso a los objetos abstractos. Sin embargo, dichos artículos también tuvieron la consecuencia indeseada de dejar otros temas relevantes por fuera, entre estos la práctica matemática.

⁴⁰ Paul Benacerraf es un reconocido filósofo venezolano-francés, el cual trabaja en la filosofía de las matemáticas y se le reconoce por importantes artículos como *What Numbers Could Not Be* publicado en 1965 y *Mathematical Truth* publicado en 1973.

Teniendo en cuenta lo anterior, Mancosu (2016) identifica dos tradiciones respecto a la filosofía de las matemáticas. Por un lado, se podría catalogar una tradición “fundacionista”⁴¹, la cual está centrada en los fundamentos de las matemáticas y cómo a partir de su lógica se puede hacer filosofía de las matemáticas; es decir, existen unas bases proporcionadas a partir de la lógica matemática. Por otro lado, está la tradición “inconformista”, la cual, en contraparte de la primera, considera tres aspectos divergentes: (i) no existe cimiento cierto para la matemática, la matemática es una actividad falible (ii) la lógica es insuficiente para analizar adecuadamente la matemática y su desarrollo y (iii) presta atención a la práctica matemática.

Más allá de tomar partido por una de estas tradiciones, Mancosu (2016) propone, sin desconocer el trabajo de los “fundacionistas”, extender la visión actual de la filosofía de las matemáticas, a partir del enriquecimiento de los planteamientos abordados de la tradición “inconformista”. Desde esta visión, la práctica matemática resulta más relevante:

...considero que la teoría del conocimiento matemático necesita ser extendida más allá de sus confines actuales para abordar temas gnoseológicos que tienen que ver con fecundidad conceptual, evidencia, visualización, razonamiento diagramático, comprensión, explicación, y otros aspectos de la teoría del conocimiento matemático que son ortogonales respecto del problema del acceso a «objetos abstractos» (Mancosu, 2016, 132)

En este sentido, Mancosu (2016) resume en ocho temas las contribuciones hechas en el libro *The Philosophy of Mathematical Practice* publicado en 2008 y del cual, el mismo Mancosu es editor, estos ocho temas recogen algunas posturas filosóficas respecto a la práctica matemática.

Los temas destacados son: la visualización, razonamiento diagramático, explicación, pureza de los métodos, conceptos y definiciones, aspectos filosóficos de los usos de la ciencia de la computación en matemática, teoría de categorías y física matemática. También, el autor hace

⁴¹ Este término es propuesto por el autor de este trabajo.

una explicación general de la importancia de estos temas, así como la presentación de algunos ejemplos que presenta el libro.

Siguiendo esta idea, vale la pena hacer una mirada general de estas temáticas; sin embargo, dentro del objetivo de este trabajo, el énfasis estará en la teoría de categorías -sin dejar de lado elementos de las otras temáticas- debido a que presenta relaciones más estrechas respecto al pensamiento de Galois.

En el primer tema, se sostiene que los procesos de *visualización* han conseguido un rol importante por la influencia de las imágenes generadas por computadoras para estudios como el de la geometría diferencial o la teoría del caos, además se destaca que la visualización no solo es una heurística, sino que puede tener un rol epistémico.

El segundo tema es el *razonamiento diagramático*, el cual se destaca por su potencial en el desarrollo de la inteligencia artificial y la introducción de algunos temas filosóficos centrales en geometría.

Por su lado, el autor destaca la *explicación* como tercer tema, en la que sostiene como virtud para los matemáticos porque muestra alternativas que justifican por qué un resultado es verdadero. A menudo, un resultado convence que es verdadero, pero no dice por qué ese resultado es verdadero.

El cuarto tema es la *pureza de los métodos*, el cual es valorado en la comunidad matemática por el hecho de liberar las matemáticas de los *ideales*⁴², se considera como ejemplo para este caso, la eliminación de la intuición geométrica para el desarrollo del análisis en el siglo XIX⁴³.

⁴² La noción de ideal viene de la presentación de (Mancosu, The philosophy of mathematical practice, 2008), la cual hace referencia a ideas dentro de una teoría que se introducen en otra teoría para construir sus pruebas.

⁴³ En concreto, este tema centra su atención en el intento de construir métodos autosuficientes dentro de una teoría; es decir, que estos métodos no dependan de otra teoría distinta a la teoría donde se moviliza para poder construirse adecuadamente. Como ejemplo, nótese el caso del teorema de Pitágoras en los *Elementos*, dicha prueba

Como quinto tema, el autor se refiere a los *conceptos y definiciones* en una teoría matemática, principalmente desde la perspectiva de su productividad y naturalidad en la teoría donde se movilizan.

En cuanto al sexto tema, Mancosu (2016) destaca *la ciencia de la computación en matemática*, principalmente se nota en la matemática contemporánea y en conexión con el tema de visualización; se destaca la computación porque proporciona una confirmación experimental, nótese el caso del teorema de los cuatro colores.

Como séptimo tema está la *teoría de categorías*, objeto de estudio en el segundo capítulo y que para el autor recibe su importancia por ser un marco alternativo fundacional para toda la matemática, también por su poder de unificación y productividad en campos como el de la geometría algebraica, topología algebraica y el álgebra homológica.

Finalmente está la *física matemática*, que el autor considera importante debido a los aportes de las matemáticas puras para el desarrollo de la física y viceversa, el ejemplo expuesto es la topología de las dimensiones bajas; sin embargo, se destaca que los estándares en ambas disciplinas son diferentes, por lo que la rigurosidad en cada disciplina es un problema al que hay que prestarle atención.

Todas las anteriores temáticas resultan relevantes dentro del estudio de las prácticas matemáticas, sin embargo, parece notable considerar el estructuralismo -y en particular el estructuralismo categórico- como explícito en la forma contemporánea de practicar matemáticas.

no necesita el uso de aritmética u otros campos para demostrarse en los términos que plantea Euclides; en consecuencia, la prueba del teorema de Pitágoras en los *Elementos* es pura.

Por tal razón se dedica la siguiente sección a una reflexión sobre el potencial que tiene el estructuralismo matemático.

3.3 Lo que logra el estructuralismo

Existe la idea contemporánea de que los matemáticos no piensan en la naturaleza de los objetos sino en las estructuras, McLarty (2008) sostiene esta idea trayendo el caso de los *Elementos de Euclides*, las diferentes líneas y los vértices en los diagramas euclidianos tienen relaciones específicas entre sí, pero por fuera de estos diagramas no tienen ningún significado. Las definiciones de puntos y líneas son irrelevantes para las demostraciones, así como el lugar en el espacio en el cual se encuentran los vértices y lados de estos diagramas. En las matemáticas modernas lo anterior ocurre de forma más extensa, para definir los elementos de un sistema, en términos generales se recurre a definir las relaciones que existen entre estos mismos elementos.

A pesar de esta visión matemática, para la filosofía existen varias preocupaciones que los matemáticos resolvieron hace mucho tiempo respecto a las siguientes preguntas: ¿Cómo pueden relacionarse entre sí estructuras separadas? ¿Existe una forma coherente de definir las estructuras como lugares en sí mismas dentro de estructuras más grandes? Desde Emmy Noether, los matemáticos describen rutinariamente las estructuras enteramente por las relaciones estructurales entre ellas, esto debido a que, en la práctica, las matemáticas estructurales logran el descubrimiento y demostración de grandes teoremas (McLarty, 2008).

La expresión más evidente del potencial estructuralista se presenta en la formulación de enunciados para pruebas importantes en matemáticas. No hay cuestionamientos para McLarty (2008) respecto a que las definiciones y teoremas de la literatura que circula en los posgrados es insuficiente para generar resultados importantes en matemáticas. Hace falta una visión más amplia

de la teoría, es por esto que existen tres criterios aceptados por la comunidad para dar generalidad a un problema en matemáticas:

- Cada teorema debe ser conciso y explícito, de tal forma que sea fácil y rigurosamente separable de su contexto original. La razón de este primer ítem es porque las demostraciones usualmente son largas, es por esto que cada enunciado debe de ser breve y rigurosamente autosuficiente.
- Los teoremas deben enunciarse estructuralmente, es decir, cada definición o resultado necesario debe de estar probado previamente, tampoco se pueden dejar implícitos.
- Los métodos deben manejar estructuras en todos los niveles, desde los números naturales hasta los funtores, esto mediante medios que sean comparables y que relacionen fácilmente todos los niveles.

Nótese que, si bien el primer ítem tiene la intención de aislar los problemas en matemáticas de su contexto con el fin de simplificar su lenguaje. Esta forma de pensar no está aislada de la propuesta de Carter (2019) que involucra los agentes humanos; se podría considerar la práctica de “generalizar” como una actividad estructuralista pero que involucra las prácticas de los agentes, generalizar una idea es distinto a la visión deshumanizada de Platón respecto a los objetos matemáticos.

Con estos criterios podrían surgir perspectivas como la de Resnik (1997), el cual entiende a los objetos matemáticos como posiciones en patrones, los cuales no tiene propiedades por sí solos excepto relaciones con los otros objetos en el mismo patrón.

En este sentido, si se estableciera una intuición respecto a esta forma de entender las matemáticas, se podría pensar en una visión desde arriba de un mapa, la cual ve la composición, aspectos relacionales y características entre las diferentes subregiones. Esta visión no partiría de mirar unos axiomas atómicos y la construcción que surge a partir de estos como usualmente se trabaja en los cursos de matemáticas.

Sin embargo, McLarty (2008) ejemplifica una problemática a partir de esta visión, y es que esta visión podría sugerir una ausencia de convenciones que se hacen en las prácticas matemáticas; para esto, muestra el siguiente caso:

Si los números reales solo tienen relaciones entre sí ¿cómo obtienen relaciones los números complejos? La respuesta más apropiada a esto es que los complejos necesitan una construcción, pero ¿cuál construcción?

Normalmente se conoce la definición de los números complejos por $x_0 + y_0i$ con x_0, y_0 reales y operados:

$$(x_0 + y_0i) + (x_1 + y_1i) = (x_0 + x_1) + (y_0 + y_1)i$$

$$(x_0 + y_0i)(x_1 + y_1i) = (x_0y_0 - x_1y_1) + (x_0y_1 + x_1y_0)i$$

No obstante, existen infinitos cuaterniones para definir estos números, como $x_0 + 0i + x_1j + 0k$ o $x_0 + 0i + 0j + x_1k$, es una cuestión de convención, por lo que las exigencias de la práctica deciden la naturaleza de estos objetos, no la teoría de conjuntos ni la visión general que plantea Resnik.

A pesar de esto, la visión de Resnik (1997) resulta interesante en el sentido de que da importancia a las relaciones entre una estructura y otra, esto lo hace considerando que los propios patrones se posicionan al ser identificados con posiciones de otro patrón, lo cual permite obtener

resultados sobre otros patrones que antes no eran identificados; significativamente esto ha cambiado las prácticas matemáticas.

Un ejemplo de la anterior idea es la de las estructuras algebraicas trabajadas en el primer capítulo. La teoría de grupos que empleó Galois, si bien es una generalización -o patrón- surgido a partir de las propiedades invariantes de unos elementos en un sistema; componen un objeto particular en un patrón mucho mayor -como se vio en el segundo capítulo-, en el de la teoría de categorías. La clave de esta idea está en que nunca es necesario particularizar los objetos, siempre son objetos globales, solo son patrones ubicados en otro patrón.

Esta intención, según McLarty (2008), destaca un espíritu unificador en las prácticas estructurales, para sostener esta idea él propone el ejemplo de la topología de la década de 1920, la cual se basó en la noción de homología⁴⁴, que era una noción en auge y a la vez en caos, esto debido a que había muchas versiones; en algún momento, los topólogos asumieron que los resultados probados para una versión serían válidos para todas, pero no podían decir exactamente qué era invariante y general ahí. Más adelante se demostró que algunas versiones de la noción de homología eran equivalentes entre sí, pero no había ninguna caracterización estructural.

Esta caracterización de homología -incluso el isomorfismo- fue encontrada por Eilenberg y Steenrod (1945), y fue definida a partir de un patrón de funtores de una cierta categoría de espacios topológicos y mapas continuos a la categoría de grupos abelianos. Dicha caracterización permitió un significativo progreso en homología; así como en otras teorías.

⁴⁴ Recordando la noción de homología, este es un procedimiento general en el que se asocia un objeto matemático con una sucesión de grupos abelianos, se podría pensar como una acción funtorial, esta noción es usualmente trabajada en topología algebraica y en álgebra homológica.

Esta forma de pensar respecto al comportamiento de las estructuras, no solo permitió avances y demostraciones en el sentido del ejemplo sobre la homología, sino que también ayuda a entender prácticas como las que considera Mancosu (2016). En particular, la pureza de los métodos se puede evidenciar en las intuiciones generales de los expertos, los cuales desarrollan una visión -intuición- global dentro de una teoría con el fin de volver autosuficientes sus métodos; sin embargo, esta visión es difícil de desarrollar debido a que la introducción de objetos “intuitivos” de otras teorías puede favorecer la comprensión de algunas personas respecto a un objeto, es decir, un inexperto necesita las perspectivas de otra teoría para comprender e intuir un objeto, un experto no. La intuición de una persona -en este caso el experto- puede ser la pesadilla de otro -el no experto- (McLarty, 2008).

Respecto a la anterior idea, un ejemplo puede ser el uso de los números para las demostraciones a regla y compás de los dos primeros libros de los *Elementos* de Euclides; si bien para algunas personas podría ser más intuitiva la introducción de los números para algunas pruebas, una visión más general respecto a los objetivos planteados por ambos libros muestra que los números pensados de forma aritmética no son necesarios; el pensar las pruebas y las teorías de forma “pura” puede ser una manifestación estructuralista porque evidencia las relaciones y la composición de los objetos tomados en conjunto.

Por otro lado, existen prácticas mucho más primitivas beneficiadas desde esta visión estructuralista, y es que el estudio que hizo Galois -el cual permitió el desarrollo de sus conexiones- evidencia prácticas como la de *comparar*, necesaria para cada ser humano debido a que es de las principales actividades en matemáticas (Lezama, 1996, p. 1). Galois encontró una forma de comparar estructuras que en primera instancia no tenían una naturaleza similar. Sería fascinante pensar en que esta comparación fue fácil para Galois al tener una perspectiva más general de las

estructuras, en esencia, viendo a los grupos y los cuerpos como pequeños patrones relacionables en un gran patrón.

Como cierre respecto a las anteriores ideas, no deja de ser deslumbrante pensar que Galois haya tenido esta visión, una perspectiva como la de Resnik (1997), la cual para la época y para el desarrollo de las matemáticas hasta ese punto hubieran justificado el rechazo que tuvieron sus resultados; pensar en que el álgebra clásica se podía analizar y ver de forma particular -patrón dentro de otro patrón- desde estructuras que en apariencia no tenían ninguna relación con los polinomios clásicos pudo haber sido un choque fuerte, aun habiendo tenido los resultados y las dudas que puso Lagrange y Abel; ese cambio de visión es el que puede justificar la genialidad del joven francés, esa nueva forma de ver las matemáticas, la cual tiene relación con la necesidad del pensamiento estructuralista que se desarrolló un siglo después de su muerte.

3.4 La emergencia abismal de la matemática moderna y la adjunción en la ontología de Deleuze

En otro orden de ideas, si bien este capítulo tiene el énfasis de centrarse en las fundamentaciones actuales respecto al concepto y estudio de lo que es la práctica matemática, y orientarlo hacia ese pensamiento estructuralista contemporáneo; también vale la pena considerar unas últimas reflexiones que podrían ser pertinentes dentro de las temáticas y actividades que definían el pensamiento del matemático francés protagonista de este trabajo. En este sentido, resulta interesante entender la visión romántica de Novalis (1772-1801) que ilustra Zalamea (2017) respecto a las ideas de Galois enmarcadas en las matemáticas modernas; así como la relación que existe entre la adjunción -que, en este caso, es un término que refiere al procedimiento de resolubilidad de Galois- con la ontología de Deleuze, la cual es presentada por Santaya (2014).

En primer lugar, una de las ideas de Galois que caracterizó ese cambio de las prácticas matemáticas clásicas a las modernas es la de explorar los *abismos contradictorios*, esta práctica es una de las identidades del romanticismo de Georg von Hardenberg, más conocido por su pseudónimo de Novalis, el cual fue un joven filósofo y escritor alemán representante del romanticismo alemán temprano.

El explorar los abismos contradictorios implica una oposición al principio de contradicción: todo puede ser al mismo tiempo; una ecuación es irresoluble sin ignorar que hay soluciones, todas las ecuaciones de grado cinco o más no pueden ser resueltas por radicales, pero ¿y qué tal que alguna sí se pueda? De aquí la intención de las condiciones necesarias y suficientes para la resolubilidad; la ecuación $x^2 - 2 = 0$ no tiene solución en $\mathbb{Q}$, pero ¿y qué tal que lo hubiera? ¿cómo podría existir esa solución? Con la experiencia de los preliminares del primer capítulo, una respuesta sería con la extensión $\mathbb{Q}(\sqrt{2})$, pero en este caso, el hecho de agregar un elemento que genere combinaciones lineales con el fin de enriquecer esa estructura no es algo trivial, salirse de la teoría mediante la creatividad que exige la contradicción requiere ir en contra de unas tradiciones que tal vez justificaron la no aceptación a Galois.

Esta última idea refleja el caso de la adjunción que es entendida en la perspectiva de Galois. Adjuntar un elemento con el fin de solucionar un problema que requiere entender cómo funcionan las relaciones de la estructura, no el elemento adjuntado; esta adjunción es la que sustancialmente permite la construcción de los resultados de Galois, y que desde los lentes de Novalis que plantea Zalamea (2017) permite ver una metodología que identifica las condiciones de solubilidad para una ecuación.

A continuación, se muestra este “algoritmo metodológico” desde la visión de Santaya (2014, p. 40-44), esto con el ánimo de extender y favorecer la comprensión al lector; en concreto,

Galois parte de la intuición de que la resolubilidad parte del campo en donde se movilice el polinomio, esto quiere decir que no es necesario con particularizar polinomios, es suficiente con modificar este campo con el fin de resolver la ecuación en términos de ese campo. En particular, el conjunto comúnmente utilizado es el de los números racionales junto con las operaciones elementales $\pm, \times, \div$ que forman un *cuerpo base* que se puede simbolizar por R , la cuestión con este cuerpo base es que existirán ecuaciones que requieran el uso de elementos que no están ahí para determinar una expresión que muestre sus soluciones, como $\sqrt{2}, \sqrt{-4}, p, q$.

Como ejemplo se puede tomar $x^4 + px^2 + q = 0$ cuando p y q son indeterminadas en R , sin embargo, desde esta perspectiva estas magnitudes se suponen como conocidas, la adjunción consiste precisamente en esto: considerar como conocidas cantidades que en principio son indeterminadas, a partir de esto, la intención es encontrar a partir de progresos el conjunto de las raíces de la ecuación $\{x_1, x_2, x_3, x_4\}$. Este proceso se simboliza como $R(p, q) = R^I$ *cuerpo de adjunción* (Santaya, 2014, 41).

A partir de lo anterior, el siguiente paso se resume en la construcción del grupo de Galois de la ecuación -que es una temática vista en el primer capítulo-, este grupo tiene las siguientes permutaciones:

$$\begin{aligned} E, & \quad \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}, \quad \begin{pmatrix} x_3 & x_4 \\ x_4 & x_3 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_4 & x_3 \end{pmatrix}, \\ & \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_4 & x_1 & x_2 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_4 & x_3 & x_1 & x_2 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_4 & x_2 & x_1 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_4 & x_3 & x_2 & x_1 \end{pmatrix}. \end{aligned}$$

Figura 3.1 Sustituciones del grupo de Galois⁴⁵

⁴⁵ Tomada de Santaya (2014, p. 42)

Siendo “ E ” la sustitución identidad y asignando la correspondencia de este grupo con el cuerpo base -en esencia, correspondencia de Galois, como se vio en el segundo capítulo-. Con esto, el resultado de Galois consistió en un avance progresivo que tenía como fin la búsqueda de subgrupos dentro del grupo de la ecuación, además de la construcción de ecuaciones parciales y correspondientes que reduzcan gradualmente el número de los subgrupos; esto es, buscar expresiones dentro de la extensión que dejen invariantes al campo base.

Al seguir con el ejemplo, se supone que se da con la relación $x_1^2 - x_3^2 = t$. Con esto, la intención es buscar el valor de esta relación ignorando los valores de las raíces. Esto se realiza a través de un método que permite construir una nueva ecuación para la cual el valor de esa relación entre las raíces es una raíz. Esta ecuación se llama *resolvente parcial*, y en este caso es: $t^2 - (p^2 - 4q) = 0$. El resultado de esta ecuación $\sqrt{p^2 - 4q}$ se adjunta a R^I , obteniendo así el cuerpo $R^{II} = R^I(\sqrt{p^2 - 4q})$. Luego, R^{II} no le corresponde el grupo de Galois de la ecuación, sino el subgrupo H más grande de ese grupo de Galois.

A continuación, se presentan a H y R^{II} como antes se veía a G y R^I . El método a aplicar es el mismo, del cual resulta el grupo K , subgrupo máximo de H y referido al cuerpo R^{III} (que adjunta a R^{II} el resultado de la segunda resolvente parcial). Por último, se alcanza el grupo E , la sustitución idéntica, referida al cuerpo R^{IV} (que adjunta a R^{III} el resultado de la tercera resolvente parcial). Al llegar a este punto, las relaciones entre las raíces no permiten sustitución alguna, y cada una de ellas es expresable en R^{IV} . En esencia, este método de Galois se basa en la reducción de grupos encajonados (G, H, K, E) , cuyo orden depende de la adjunción progresiva de magnitudes $(R^I, R^{II}, R^{III}, R^{IV})$.

La analogía que plantea Zalamea (2017, p. 12-13) respecto a este algoritmo metodológico resulta interesante en el sentido de que establece unas relaciones entre dos mundos aparentemente aislados, entre un mundo simple y preciso con otro mundo lleno de complejidades y variantes.

‘El llevar una cosa a través de otra’, recomendación del poeta romántico, encarna a la perfección en Galois. De hecho, el ascenso y el descenso entre el *eidos* (idealización, abstracción) y el *quidditas* (realización, concreción) da lugar a una notable espiral metodológica (1) *adjunción*: ascensos al *eidos*, raíces de irreducibles, imaginarios de Galois; (2) *variación*: tránsitos en el *eidos*, ecuación auxiliar, grupo de Galois; (3) *descomposición*: descensos al *quidditas*, normalidad, primitividad; (4) *invarianza*: tránsitos en el *quidditas*, funciones racionales, representaciones lineales. Nos encontramos así ante una plena realización matemática (en los linderos de lo abstracto y lo concreto, lo ideal y lo real, lo negativo y lo positivo) del ‘oscilar entre opuestos’ y de la ‘facultad de ser libre’ según Novalis.

Esta correspondencia se puede interpretar gráficamente considerando a (1) extensiones de campos, (2) grupos de automorfismos, (3) subgrupos normales y (4) subcampos fijos:

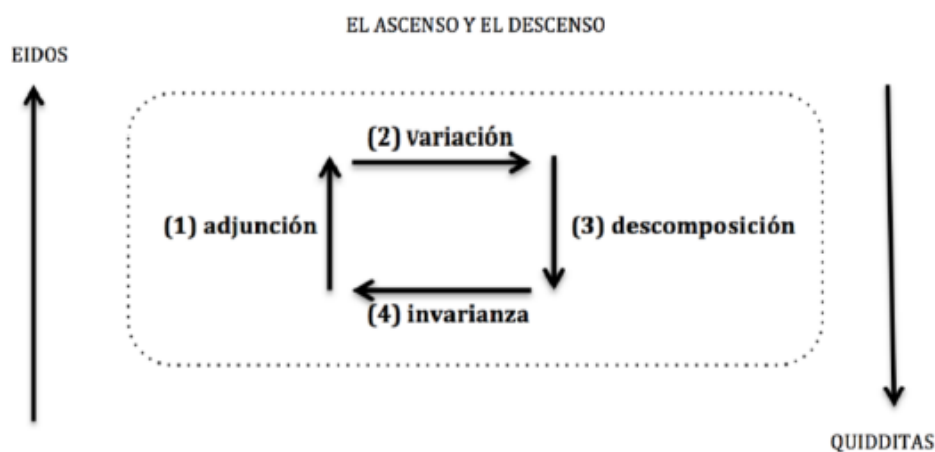


Figura 3.2 Método de Galois desde Novalis⁴⁶

Por otro lado, la perspectiva de la ontología de Deleuze que plantea Santaya (2014) muestra más particularidades respecto a esta metodología del pensamiento de Galois, no solo el análisis de los abismos contradictorios resulta interesante, sino el énfasis que se hace en *determinar* un

⁴⁶ Tomada de Zalamea (2017, p. 13)

resultado a partir de lo *indeterminable*; en concreto, el núcleo de la ontología deleuziana está centrada en la noción de Idea y su desarrollo problemático como principio genético de la realidad.

En esencia, la estructura de esta noción de Idea se basa en tres principios presentados desde la notación del cálculo diferencial: en primer lugar, está el dx que corresponde al momento totalmente indeterminado, no se podría decir mucho respecto a este objeto por sí solo, el ejemplo de esto son las adjunciones p, q que Galois hace en su algoritmo metodológico; en segundo lugar, está la relación dy/dx , lo cual es determinable, tiene sentido la relación que se establece entre los objetos indeterminables, el ejemplo concreto son las relaciones y expresiones que se establecen entre los coeficientes desconocidos de las ecuaciones, la ecuación tiene sentido independiente de lo indeterminable de sus coeficientes; por último están los valores determinados que equivalen a la relación (x, y) , estos se podrían interpretar como los valores determinables, en el resultado de Galois se puede ver como la respuesta respecto a la resolubilidad o no del polinomio.

4. CONCLUSIONES

Lamentablemente lo que se reconoce poco es que los libros científicos más valiosos son aquellos en los que el autor indica claramente lo que no sabe; porque un autor daña más a sus lectores al ocultar las dificultades⁴⁷

Evariste Galois

El recorrido de este trabajo plantea unas relaciones significativas referentes a la construcción de los resultados de Galois, sin embargo, el análisis histórico-epistemológico, las relaciones entre las matemáticas contemporáneas y las implicaciones filosóficas centradas en las prácticas que se pueden ver de las ideas del matemático francés se quedan cortas para dimensionar el choque que generó en el cambio de las matemáticas clásicas a las modernas.

Lo que sustenta la anterior idea es lo mucho que queda por estudiar y particularizar de la teoría de Galois y sus interpretaciones con las filosofías y matemáticas contemporáneas; este trabajo significa un punto de partida respecto a los principios e implicaciones que muestran los resultados y prácticas de Galois; en este sentido, las conclusiones a las que se llega -en los términos de los objetivos planteados para el presente trabajo- tienen la característica de, además de mostrar

⁴⁷ Citada en (Bowen & Giannini, 2015)

lo que se aclara, evidenciar las limitaciones y lo que queda por estudiar desde los lentes históricos, epistemológicos y filosóficos.

4.1 La previa y punto de partida de la Teoría de Galois

La historia de las matemáticas ofrece la perspectiva de mirar las condiciones y naturaleza de los resultados previos para el desarrollo de un resultado, en concreto, en este trabajo se logró exponer algunos resultados previos que fueron claves para el surgimiento de la teoría de Galois; estos resultados previos, si bien estuvieron cerca -cronológicamente-, tuvieron la particularidad de poner por primera vez en duda la resolubilidad de las ecuaciones de grado cinco o más, además, de pensar en las permutaciones que resultarían importantes en Galois. En particular, se destacan los resultados de Lagrange y Abel, el primero planteó la pregunta que pondría en duda la resolubilidad, mientras que el segundo demostraría finalmente la irresolubilidad. Por tanto, estos dos se pueden presentar como dos de los grandes partidarios del cambio a las matemáticas modernas.

No obstante, quedaría como tarea entender con mayor profundidad la génesis del álgebra clásica, unos antecedentes como los de Muñoz (2016), Chavarria (2014) y Gaviria (2014) evidencian un desarrollo previo y robusto de la teoría de ecuaciones clásica, la cual justifica el surgimiento de una teoría como la de Galois -esto al entender a las matemáticas como una construcción histórica y humana-. En este sentido, una presentación o lectura más completa de un trabajo como este, que se centra en el punto de partida de la teoría de Galois y sus implicaciones posteriores, se complementaría adecuadamente con una revisión cuidadosa de los antecedentes presentados anteriormente.

Por ejemplo, si se quisiera profundizar en los resultados previos a la teoría de Galois, llama especial atención el analizar las ideas de Ruffini, que contribuyeron sustancialmente en el resultado de Abel visto en el primer capítulo; así como las implicaciones matemáticas -distintas de Galois- de la primera puesta en duda que planteó Lagrange respecto a la ecuación general de grado cinco o más. Estudiar a Ruffini y sus antecedentes es una de las intenciones para futuros trabajos.

4.2 Las estructuras cruciales

El surgimiento y desarrollo de las estructuras resultaron claves para Galois, en particular, las estructuras protagonistas fueron la de grupo y cuerpo, ambas estructuras tienen en común el establecimiento de relaciones invariantes entre los conjuntos con los que son definidas; en concreto, este trabajo no solo presentó las características que definen estas estructuras, sino que también hizo énfasis en que, lograr comparar dos estructuras que en principio son diferentes es una práctica posible. Galois encontró una forma de comparar un grupo en particular -grupo de Galois- y las extensiones de un cuerpo centrándose en las relaciones que definían las estructuras.

Resultaría apresurado y pretencioso pensar en que no queda más por analizar en esta unificación de la teoría de grupos y la de cuerpos, estudiar las particularidades y resultados posteriores al resultado de Galois es una tarea que siempre estará latente; sin embargo, como caso particular, el estudio computacional de esta teoría es algo que llama especialmente la atención, ¿las computadoras de hoy en día consideran prácticas similares a las que planteó Galois? ¿Cómo funciona la resolución de polinomios en la computación? ¿Existe algún algoritmo que determine la resolubilidad o no de una ecuación? Y en caso de que lo haga ¿podría este algoritmo mostrar la fórmula general para este polinomio? ¿Qué otros problemas de la teoría de Galois podrían apoyarse con la implementación de la computación?

4.3 Funtores adjuntos y conexiones de Galois

La teoría de categorías fue clara protagonista de las ideas planteadas para este trabajo, pero en particular, la noción de funtor adjunto -covariante- recibió especial atención, no solo por extender la visión de otras nociones como la de función junto con su inversa, sino también por poderse interpretar como la generalización de las conexiones de Galois.

Esta generalización es la que concluye la relación entre estas dos nociones, en concreto, las conexiones de Galois surgen como una generalización del teorema fundamental de la teoría de Galois, este último es el que relaciona los elementos que están involucrados en la teoría de Galois, es decir, las ecuaciones, las extensiones asociadas a esas ecuaciones, los grupos, etc. Pero las conexiones de Galois resultan ser más generales al definirse a partir de los *posets* (conjuntos parcialmente ordenados), esto quiere decir que no es necesario que haya correspondencias entre familias de extensiones y subgrupos de un grupo, es suficiente con dos *posets*. Los funtores adjuntos resultan ser más generales, no es necesario que establezcan correspondencias entre *posets*, sino entre dos categorías, las cuales no son tan particulares como dos *posets*.

A pesar de la claridad respecto a esta generalización, el presente trabajo pretende dejar otros elementos importantes que podrían ser estudiados en futuros estudios, en particular, el estudio respecto a los objetos iniciales y terminales resulta relevante para analizar en profundidad las relaciones entre las conexiones de Galois y los funtores adjuntos; asimismo como las particularidades que tiene analizar los funtores adjuntos contravariantes y más generalidades como la de transformación natural.

4.4 La práctica estructuralista de Galois

Como cierre de conclusiones, y que muestra la reflexión central del autor de este trabajo, se consideran las prácticas matemáticas, pero en particular las prácticas matemáticas inmersas en el estructuralismo categórico.

En este sentido, el presente trabajo expuso las consideraciones respecto a la definición de práctica matemática, así como las prácticas estructuralistas que se movilizan en el pensamiento de Galois; en concreto, las ideas del joven francés se podrían interpretar desde la generalización de invarianzas entre relaciones -patrón dentro de otro patrón-, así como la práctica de comparar, encontrar una forma de comparar; estas ideas se pueden ver desde la exploración de abismos contradictorios.

Estas prácticas interpretadas desde la visión de Galois -si bien son tratadas desde una visión filosófica durante el transcurso del presente trabajo- son importantes para el desarrollo de competencias que un docente de matemáticas debe de propiciar, y no solo para él, sino también para sus estudiantes, ¿cómo no va a ser importante para un docente de matemáticas entender cómo cambian las prácticas matemáticas con sujetos activos en el tiempo? ¿Cómo no va a ser importante desarrollar prácticas como las de generalizar o comparar? ¿Por qué no se podría explorar la contradicción? ¿Por qué no sería relevante ver a los fundamentos desde una visión estructuralista?

Entender lo que significan las prácticas es lo que puede justificar la razón por la cual un trabajo como estos es relevante para la educación matemática, la intención no es solo conocer las anécdotas o datos interesantes sobre la vida de Galois -que en algunos casos pueden ser atractivos para los estudiantes-. El fin es también entender cuáles fueron las problemáticas contextuales que propiciaron un resultado como al que llegó el joven francés, qué fue lo que escribió, qué

antecedentes tuvo, qué ideas se desarrollaron con el resultado de Galois. Todos estos son elementos que debe de tener presente un docente de matemáticas.

Por otro lado, con la intención de generar más tópicos para futuros trabajos, respecto a la visión filosófica de la práctica matemática, y en particular desde las definiciones que se plantean, las cuales muestran un cambio de prácticas en el tiempo, podrían surgir estudios respecto a los cambios entre las prácticas de las obras originales de Galois y las prácticas que se podrían sugerir en libros como *Moderne Algebra* de van der Waerden o en libros más contemporáneos.

Habiendo presentado los anteriores elementos como cierre, la moraleja con la cual vale la pena cerrar este trabajo consiste en generar al lector un punto de partida para futuros estudios, a no suponer que los resultados de Galois están acabados; al contrario, el desarrollo de sus ideas se mantiene, y un estudio especialmente relevante como este tiene coherencia con la intención de mejorar día a día las competencias de los docentes en matemáticas. Es por esto que una frase como la de Chevalier (1832), amigo cercano de Galois, cobra todo su sentido:

Piedad, ¡nunca! Odio, eso es todo. Quien no resiente profundamente ese odio del presente, no posee realmente el amor del porvenir

5. REFERENCIAS

- Abel, N. H. (1824). Mémoire sur les equations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré.
- Almira, J. M., & Cid, J. Á. (2017). En busca de la solución perdida. En J. M. Almira, & J. Á. Cid, *Abel: El desarrollo de las funciones elípticas* (págs. 57-87). España: RBA.
- Anaconda, M. (2017). Una mirada a los funtores adjuntos. En M. Anaconda, *Los números reales en el estructuralismo bourbakista: un análisis histórico-epistemológico con fines educativos* (págs. 244-245). Cádiz, España: Universidad de Cádiz.
- Armstrong, D. (2016). Adjoint Functors. En D. Armstrong, *Fancy Algebra* (págs. 1-65).
- Bello, J. (2017). La perspectiva de la práctica matemática en la formación del conocimiento matemático del profesor de matemáticas. *Redumate*.
- Bowen, J. P., & Giannini, T. (2015). Galois connections: Mathematics, Art, and Archives. *Electronic Visualisation and the Arts (EVA)*, (págs. 176-183). London.
- Calero Sanz, J. (2019). *La revolución algebraica: El nacimiento de la teoría de grupos*. España: Emse Edapp.
- Carter, J. (2019). Philosophy of mathematical practice. *Philosophia Mathematica*, 27(1), 1-32.
- Chavarria, S. (2014). *De las ecuaciones a la teoría de grupos, algunos obstáculos epistemológicos*. Cali: Universidad del Valle.
- Chevalier, A. (1832). Nécrologie. Evariste Galois. *Revue Encyclopédique*(55), 744-754.
- Corfield, D. (2003). *Towards a Philosophy of Real Mathematics*. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511487576

- Dávila Rascón, G. (Mayo de 2003). El Desarrollo del Álgebra Moderna. *Apuntes de Historia de las Matemáticas*, II(II), 38-78. Obtenido de https://issuu.com/abelgalois/docs/apuntes_de_la_historia_de_las_matematicas_vol_ii
- Dummit, D., & Foote, R. (2004). *Abstract Algebra* (Third ed.). John Wiley and Sons.
- Eilenberg, S., & MacLane, S. (1945). General Theory of Natural Equivalences. *Transactions of the American Mathematical Society*, 58(2), 231-294.
- Español, L. (1999). Matemática conceptual: la propuesta didáctica de F.W Lawvere y S.H Schanuel. *Suma*, 11-16.
- Ferreirós, J. (2016). *Mathematical Knowledge and the Interplay of Practices*. Princeton University Press.
- Gaviria, L. M. (2014). *De los grupos y cuerpos como "herramientas" a "objetos" matemáticos*. Cali: Universidad del Valle.
- Herstein, I. N. (1988). *Algebra Abstracta*. (E. Ojeda, Trad.) Iberoamérica.
- Jacobson, N. (1974). *Basic Algebra I* (Second ed.). Yale University.
- Jaimes, L. (13 de Julio de 2016). *Grupo de simetrías del cuadrado*. Obtenido de GeoGebraTube: <https://www.geogebra.org/m/d8Dy3CwY>
- Judson, T. (2017). *Algebra Abstracta: Teoría y Aplicaciones*. (A. Behn, Trad.) Universidad del Chile. Obtenido de <http://abstract.ups.edu/aata-es/aata.html>
- Kitcher, P. (1985). *The Nature of Mathematical Knowledge*. New York: Oxford University Press.
- Lagrange, J. L. (1869). Réflexions sur la Résolution des Équations. En J. L. Lagrange, *Oeuvres de Lagrange* (Vol. III, págs. 200-420). París: CNRS.
- Lawvere, W., & Schanuel, S. (2002). *Matemáticas conceptuales: Una primera introducción a categorías* (Segunda ed.). (F. Marmolejo, Trad.) Madrid: Siglo veintiuno Editores.

- Lezama, C. (1996). Conexiones de Galois. *Integración*, XIV(1), 1-8.
- Macho, M. (16 de Abril de 2014). *Estudiar más que conocer, buscar más que encontrar la verdad*.
Obtenido de Cultura científica: <https://culturacientifica.com/2014/04/16/estudiar-mas-que-conocer-buscar-mas-que-encontrar-la-verdad/>
- Mancosu, P. (Ed.). (2008). *The philosophy of mathematical practice*. Oxford: Clarendon Press.
- Mancosu, P. (2016). Algunas observaciones sobre la filosofía de la práctica matemática. *Disputatio Philosophical Research Bulletin*, V(6), 131-156.
- Marquis, J. P. (2006). What is category theory? *Polimetrica International Scientific Publisher Monza/Italy*, 221-255.
- McLarty, C. (2008). What Structuralism Achieves. En P. Mancosu (Ed.), *The philosophy and Mathematical Practice* (págs. 354-369). Oxford: Clarendon Press.
- Muñoz, A. (2016). *De las matemáticas clásicas a las matemáticas modernas y contemporáneas*. Cali: Universidad del Valle.
- Ore, O. (1944). Galois Connexions. *Transactions of the American Mathematical Society* 55, 493-513.
- Panza, M. (2019). Algunas estructuras algebraicas elementales. En M. Panza, *Números: elementos de matemáticas para filósofos* (F. Galvez, L. C. Arboleda, & M. Anaconda, Trads., págs. 281-329). Cali, Colombia: Universidad del Valle.
- Resnik, M. (1997). *Mathematics as a Science of Patterns*. Oxford: Oxford University Press.
- Roman, S. (2017). *An Introduction to the Language of Category Theory*. Springer.
- Santaya, G. (2014). El procedimiento de adjunción de Évariste Galois y su presencia en la ontología Deleuziana. En J. Ferreyra, & M. Soich (Edits.), *Deleuze y las fuentes de su filosofía* (págs. 37-47). Buenos Aires.

Valencia, S. (2021). *Le concept d'adjunction dans la théorie des catégories: son développement et son importance*. Paris: Université de Paris.

Zalamea, F. (2017). La emergencia abismal de la matemática moderna. *Mathesis*, 1-23.