La última noche de Galois

Bruno Giordano

FaMAF - UNC

La esencia de las matemáticas reside en su libertad.

Georg Cantor, 1845-1918

Concurso de monografías UMA - 2023

Agradecimientos

La primera vez que escuché la historia de Galois tenía 17 años. No tenía la suficiente matemática recorrida como para entender la mitad de lo que hoy escribo aquí. Jamas habría llegado a entender, mucho menos a escribir esta historia de no haber tenido la increíble oportunidad de estudiar en el universo paralelo en el que habita la Facultad de Matemática, Astronomía y Física de la Universidad Nacional de Córdoba. En ese mundo fantástico tuve el placer de conocer amigos, colegas, mentores e ídolos, todos impregnados no solo de un vasto conocimiento matemático, si no también de una abrumadora y contagiosa pasión por el arte de las ideas matemáticas. Estoy eternamente agradecido a la distribución probabilística del destino que me trajo hasta esas puertas de oro. Quiero agradecer particularmente a Diego Sulca y Lucas Villagra Torcomian, por ofrecerme una voz experta en esta hermosa Teoría de Galois. A Alejandro "ojo biónico" Tolcachier, por haber ayudado a mi faceta perfeccionista a encontrar hasta la más minúscula corrección. A mi futuro colega Augusto Vocos, por convidarme su preciso criterio en el arte de la pluma literaria. A Bauti Prioletta y Manu Fernandez, por haberse tomado el tiempo de descifrar y sugerir el texto críptico que fue este trabajo en su proceso de desarrollo.

Prólogo

Pienso mucho en la muerte. Como matemático, me sorprende su universalidad: todos corremos la misma suerte. Es curioso pensar que todo lo que soy, todo lo que aprecio y todo lo que veo, inevitablemente llegará a su fin. Todo lo que toco será reducido a átomos cuando la suficiente cantidad de agua pase por debajo del puente. Algún día alguien pronunciará mi nombre por última vez y luego todo será vacío. Por más empeño que yo dedique en vida a ser recordado, ese momento llegará tarde o temprano y todo habrá sido en vano. Hasta las insoslayables leyes de la física de nuestro universo se chocarán la una con la otra cuando todo se colapse sobre un punto. Cualquier sentido de propósito es derrumbado por la idea de esta singularidad. Todo corre la misma suerte.

Al momento de escribir esto tengo 21 años de edad. El día de su muerte, él había vivido solo 20. Hablo de Evariste Galois. Estoy seguro que Evariste pensó en la muerte el 29 de mayo de 1832. Al día siguiente estaba citado a un duelo a muerte con un capitán de la guardia. Nunca se supo el motivo. Lo que sabemos es que ese joven valoró más su honor que su propia vida, y al día siguiente murió a causa de las heridas contraídas en ese combate. Estoy seguro de que esa noche pensó mucho en la muerte. De tanto pensar en la muerte, su mente brillante encontró la solución. "No todo corre la misma suerte" habrá pensado. Pues recordó que él era matemático: "La suma del cuadrado de los catetos es igual al cuadrado de la hipotenusa" dijo Pitágoras hace milenios. "Pues claro... pero él también será olvidado" Le respondí yo a Galois. "Él sí... pero la suma del cuadrado de los catetos seguirá siendo igual al cuadrado de la hipotenusa" me dijo con un gesto cómplice. Incluso después de todas las muertes naturales del universo, allá donde dos catetos se abracen formando un ángulo recto el bendito teorema seguirá valiendo. Él pudo ver en mis ojos que yo entendí la idea, sonrió como no sonríen los condenados, me estrechó la mano y se fue diciéndome que tenía que escribir unas cartas. Leyendo los libros de historia hoy descubro que esa noche escribió varias cartas despidiéndose de sus familiares y amigos pero además escribió una para su amigo Auguste Chevallier. En ella plasmó todas las matemáticas que desbordaban de su mente.

Hoy yo tengo 21 años, me dedico a estudiar matemática y navego entre un hermoso y vasto mar de materias y asignaturas: álgebra, probabilidad, análisis, topología algebraica. Recuerdo muy bien la primera vez que leí un nombre propio en el título de un libro de matemática: Teoría de Galois. Ese nombre brillaba tanto como los ojos de Evariste. ¿Qué fue lo que escribió ese joven en la última noche de su vida, para que hoy existan libros con sus teorías? ¿Cuántas puertas abrió para que siglos después yo estudie una asignatura que porta su nombre? La intención de esta monografía es responder estas preguntas. Recorrer la increíble historia que dio origen al álgebra moderna y acompañar a Evariste Galois en sus últimas horas mientras se adentra solo en el eterno mundo de los teoremas matemáticos.

1. Una breve historia del Álgebra

1.1. El Tesoro Matemático de los Árabes: el origen del Álgebra

La historia de Galois es el capítulo final de una historia mucho más grande: la historia del álgebra. La historia "adulta" del álgebra comienza en el siglo IX con un hombre llamado Al-Juarismi. Al-Juarismi fue un matemático y astrónomo persa que vivió entre los años 780 y 850. De alguna manera, fue quien bautizó al álgebra, al publicar un tratado que llevaba de nombre *Al-jebr w'al-muqabala* que quiere decir "transposición y eliminación". Por transposición (*al-jebr*) se entiende a la operación de trasladar un término de una ecuación de un lado de la igualdad al otro y por eliminación (*al-muqabala*) la cancelación de términos iguales en ambos miembros de la misma.

La primera palabra del título de este texto, *al-jebr*, se transformó en *álgebra* cuando fue transcrita al latín. En sus orígenes, el álgebra trataba del estudio de las operaciones matemáticas de manera general y abstracta. Buscaba reglas y formas de operar con números independientemente del valor de los mismos, de ahí que se utilicen letras, en vez de números, para representar valores arbitrarios. Las técnicas desarrolladas por Al-Juarismi sirvieron para resolver ecuaciones del tipo $x^2 + px = q$ donde p y q son dos números positivos, pues estos eran los únicos números admitidos en aquella época. Esto significa que para Al-Juarismi, eran muy distintas las ecuaciones de la forma $x^2 = px+q$.

La siguiente persona en pasar al escenario es el famoso matemático indio Bhaskara. Una considerable parte de los lectores habrá tirado estas hojas al suelo luego de leer ese nombre y recordar las innumerables veces en las que lo maldijeron tras horas de luchar con la temible *fórmula resolvente*:

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

Pero no teman, queridos lectores, en esta ocasión no serán torturados con una lista de problemas para aplicarla. Muchos de ustedes quizás logren perdonarla luego de descubrir la increíble historia que hay detrás de ella y de su creador Bhaskara. Este injuriado matemático vivió entre los años 1114 y 1185. El principal registro que se tiene de sus contribuciones proviene de una obra suya titulada *Lilavati* ('la que posee diversión', la atractiva), un libro de aritmética escrito en versos que lleva el nombre de su hija y está dedicado a ella. A continuación pueden leerse la traducción de dos de ellos:

> Oh, mi querida chiquilla,
> si conoces el método de la transición,
> encuentra dos números que sumen ciento y uno
> y cuya diferencia sea veinticinco.
>
> Si un idiota presuntuoso
> te dice que hay un cuadrilátero
> de lados dos, seis, tres y doce,
> o un triángulo con lados tres, seis y nueve,
> explícale por qué no existen.
>
> Bhaskara (1114 – 1185)

En uno de estos relatos encontrado en una traducción persa del libro, Bhaskara dijo que había estudiado el horóscopo de su hija y predijo que si su primera relación sexual no sucedía en el momento astrológico que él prefijara, su marido pronto moriría. Para impedir esto, una hora antes del momento colocó una taza con un pequeño agujero en la parte inferior de una vasija rellena con agua, colocada de manera que la taza se hundiera a la hora propicia para el acto. Puso el mecanismo en la habitación nupcial y le avisó a Lilavati de no acercarse. Sin embargo, la curiosidad (una de las cualidades que los hinduistas consideran negativas de las mujeres) la llevó a mirar el mecanismo, y una perla de su aro de la nariz cayó accidentalmente dentro, tapando el orificio y afectando el conteo. El acto tuvo lugar más tarde del tiempo que se había predicho como correcto, y ella se quedó viuda pronto. La historia dice que, para consolarla en su dolor, ya que la mujer hinduista viuda no debe volver a casarse, Bhaskara le enseñó matemáticas y escribió este libro para ella.

La famosa fórmula resolvente no es más que la expresión general de las soluciones a la ecuación

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

Se puede obtener manipulando la misma de la siguiente manera:

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

1.2. Un Gran Duelo Matemático

El álgebra alcanzó su máximo desarrollo hacia el siglo XII y después se estancó. A partir de ese momento, ese conocimiento empezó a difundirse por Europa, sobre todo de la mano de comerciantes italianos que tenían relaciones comerciales con el mundo árabe. La evolución del álgebra en Europa fue lenta, principalmente debido a que los primeros algebristas describían la manipulación y la solución de ecuaciones usando el lenguaje cotidiano, lo que hoy denominamos como álgebra retórica. Con el tiempo, aparecieron algunas abreviaturas (álgebra sincopada) y progresivamente se comenzaron a usar letras

para representar tamaños y cantidades desconocidas y símbolos para representar operaciones (álgebra simbólica). Todo este paulatino proceso se extendió entre los siglos XV y XVII, y fue acortando considerablemente la descripción de los cálculos.

El siguiente gran avance en la disciplina sucedió en Italia en el siglo XVI. En 1494, Luca Pacioli, quien sería el profesor de matemática de Leonardo Da Vinci, publicó su libro *Summa de Aritmética*, un resumen de toda la matemática conocida en la Italia renacentista. Allí se puede encontrar una sección sobre una ecuación que para ese entonces parecía imposible resolver: la ecuación polinómica de grado 3 o cúbica. Desde los tiempos de Bhaskara ya sabíamos cómo resolver ecuaciones polinómicas de grado 2. Sin embargo, no se tenía una solución general para las de grado 3, es decir, de la forma $ax^3+bx^2+cx+d=0$, (ni para ningún otro grado mayor) a pesar de que los matemáticos habían intentado resolverla por siglos. Pacioli escribió explícitamente en su libro que era imposible resolver la ecuación cúbica general. Sin embargo, no mucho tiempo después de la publicación de este libro, una solución comenzó a tomar forma.

Scipione Del Ferro era un profesor de matemáticas en la Universidad de Bologna. En algún momento alrededor del año 1510, Del Ferro encontró un método general para resolver la *cúbica reducida*, ecuaciones de la forma $ax^3+px+q=0$. Es decir, cúbicas cuyo término cuadrático es nulo. ¿Qué fue lo que hizo Del Ferro tras descubrir un importante avance en un problema que había atormentado a los matemáticos por siglos e incluso había sido considerado imposible por el mismísimo profesor de Da Vinci? Nada. No se lo dijo a nadie.

En aquella época, ser matemático era muy distinto de lo que es hoy. Las posiciones docentes en las universidades se definían a través de *duelos matemáticos.* Si un matemático tenía un puesto, podía ser desafiado por otro que lo pretendiese. Luego, cada uno preparaba una lista de problemas para el otro y el que lograba resolver más problemas se quedaba con el trabajo, mientras que el perdedor sufría una profunda humillación pública. Del Ferro, que se creía la única persona en el mundo capaz de resolver estas ecuaciones, creía firmemente que mantener la confidencialidad de su método garantizaría su empleo. Del Ferro mantuvo su secreto durante casi dos décadas, hasta que, en su lecho de muerte, decide revelárselo a su alumno Antonio Fior.

Fior no era tan ingenioso para las matemáticas como su maestro, pero era joven y ambicioso. Luego de la muerte de Del Ferro, comenzó a jactarse de su destreza matemática y, específicamente, de su habilidad para resolver cúbicas reducidas. El 12 de febrero de 1535, Fior desafió al matemático Niccolo Fontana Tartaglia, quien recientemente se había trasladado a la ciudad natal de Fior, Venecia. A Tartaglia no le era para nada ajena la adversidad. De niño, un soldado francés le abrió la cara, dejándolo tartamudo de donde provino el nombre con el que sería recordado 'Tartaglia', que significa tartamudo en italiano. Habiendo crecido pobre, Tartaglia era principalmente autodidacta y, con mucho esfuerzo logró abrirse un camino en la sociedad italiana hasta convertirse en un matemático respetado. Tartaglia se jugaba toda su carrera en este duelo. Como de costumbre, Tartaglia le entregó a Fior una lista de 30 problemas matemáticos, mientras que Fior le entregó a Tartaglia 30 cúbicas reducidas. Cada duelista tuvo 40 días para resolver sus desafíos. Al terminar el plazo establecido, Fior no fue capaz de resolver ni un solo problema de los 30, mientras que Tartaglia resolvió las 30 cúbicas en apenas dos horas. La arrogancia de Fior le había cavado su propia tumba, pues Tartaglia había escuchado sobre su presunto descubrimiento de la solución general de la cúbica reducida y se mostró escéptico: "no lo creí capaz de encontrar tan importante regla por sí mismo"

escribió. El rumor decía que un prestigioso matemático le habría revelado el secreto a Fior. Así que, sabiendo que una solución para la cúbica era posible y con todo su prestigio sobre la mesa, Tartaglia se propuso resolver él mismo la ecuación general de la cúbica reducida antes del duelo. Así fue como, ante todo pronóstico, Tartaglia se convirtió en el segundo matemático en la historia en resolver la ecuación de una cúbica reducida. Para facilitar su resolución, Tartaglia diseñó un algoritmo que plasmó en un poema para recordarlo mejor. Escrito como fórmula, la solución a la ecuación $ax^3 + px + q = 0$ se obtiene, primero notando que podemos asumir que $a = 1$, pues de no ser ese el caso siempre podremos dividir toda la ecuación por a y obtener una ecuación de la forma $x^3 + px + q = 0$ cuya solución general es:

$$x = \sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{\frac{27q^2 + 4p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \frac{1}{2}\sqrt{\frac{27q^2 + 4p^3}{27}}}$$

Tras su victoria, Tartaglia se volvió una especie de celebridad. Todos los matemáticos estaban desesperados por saber cómo había logrado resolver la cúbica reducida, especialmente Girolamo Cardano, un erudito intelectual erradicado en Milán. Como es de esperarse, Tartaglia se niega a revelar ni el más mínimo indicio de su método a su competencia. Pero Cardano se muestra insistente y le escribe una serie de cartas que alternan entre halagos y ataques agresivos. Finalmente, bajo la promesa de presentarle a su pudiente mecenas, Cardano convence a Tartaglia de viajar a Milán. Y allí, el 25 de marzo de 1539, Tartaglia revela su método secreto, pero solo bajo la condición de que Cardano jurase no divulgar el más mínimo detalle del mismo y escribirlo solo en código de manera tal que, después de su muerte, nadie sea capaz de entenderlo.

Cardano empezó a experimentar con el algoritmo de Tartaglia con un objetivo claro en mente: encontrar un método para resolver la cúbica general, incluyendo el término al cuadrado. E inesperadamente, lo descubre. Su método consiste en transformar una cúbica general en una cúbica reducida, de la siguiente manera: si tenemos una cúbica general $ax^3 + bx^2 + cx + d = 0$ podemos reemplazar $x = y - \frac{b}{3a}$ y todos los términos al cuadrado desaparecen dejando como resultado una cúbica reducida, por lo que puede ser resuelta con el método de Tartaglia. Cardano, emocionado por haber resuelto el problema que había dejado perplejos a generaciones enteras de matemáticos, quiere publicar su solución. Contrario a sus colegas, Cardano no tenía un puesto en una universidad, sino que vivía de trabajar como médico y de su fama intelectual. No tenía la necesidad de mantener el secreto. Para él tiene más valor el crédito. Su única traba era el juramento que le había hecho a Tartaglia. Sin embargo, en 1542, en un viaje a Bologna, Cardano conoce a un matemático, que resultó ser el yerno de un tal Scipione Del Ferro, el hombre que en su lecho de muerte le había revelado el secreto de la cúbica reducida a Antonio Fior. Cardano encuentra en una antigua colección de notas de Del Ferro la solución a la cúbica reducida. Esta solución es décadas más antigua que la de Tartaglia, por lo que ahora, a los ojos de Cardano, él es libre de publicar la solución general de la cúbica sin que eso signifique romper su palabra con Tartaglia. Tres años más tarde, Cardano publica *Ars Magna*, o El Gran Arte, un compendio actualizado de las matemáticas de la época. Allí Cardano publica su método para resolver la cúbica general y a pesar de que reconoce el trabajo de Del Ferro, Fior y Tartaglia, este último está completamente disgustado con Cardano. Tartaglia le escribe insultantes cartas por lo que ha hecho. Hoy en día, la solución general de la cúbica es conocida como el método de Cardano.

Pero, este juego de tronos matemático no termina acá. Pues unos años antes, en 1536, Ludovico Ferrari, un niño de 14 años había llegado a Milán escapando de Bolonia, su ciudad natal, a causa de una guerra. Cuando llegó, comenzó a trabajar en la residencia de Cardano como su sirviente. Cardano pronto descubrió que Ludovico sabía leer y escribir y lo tomó como secretario para que le escribiera sus propios libros. Pronto se percató de que Ludovico aprendía con rapidez y empezó a enseñarle matemáticas. Cardano y Ferrari estudiaron la solución de las cúbicas que Tartaglia les había comunicado. En este proceso, Ferrari descubrió también la solución general de la cuártica en 1540, que con un bello argumento reducía el problema a resolver una cúbica por el método de Tartaglia. Como Cardano había jurado a Tartaglia que no publicaría la solución de las cúbicas, estos no podían publicar tampoco las cuárticas que dependían de la solución de aquellas. Sin embargo, tras descubrir los escritos de del Ferro, Cardano publicó la solución de las cuárticas en Ars Magna.

Cuando Tartaglia enfureció y comenzó a escribir a Cardano, Ferrari le escribió a Tartaglia, retándolo a un duelo. Tartaglia no quería disputar el reto con Ferrari, ya que lo consideraba un actor secundario. Luego de un año de cruzarse cartas e insultos con Ferrari sin recibir contestación del propio Cardano, se vio forzado a aceptar el reto de Ludovico. La situación económica de Tartaglia no era buena y había recibido una atractiva oferta de trabajo de su propia ciudad Brescia, bajo la condición de que aceptara el reto con Ferrari, que ya se había hecho famoso. El 10 de agosto de 1548, el esperado debate tuvo lugar en la iglesia y los jardines de Frati Zoccolanti en Milán. Una gran multitud se congregaba y todos los notables de la ciudad estaban pendientes de su resolución, incluido el mismísimo gobernador de Milán, que era el juez último. Aunque Tartaglia tenía experiencia y había ganado otros duelos, Ferrari tenía un mayor conocimiento de los problemas prácticos de cúbicas y sobre todo cuárticas que él mismo había resuelto para el libro de su patrón Cardano. Tartaglia, con menos carácter y más edad, pronto notó de que el público celebraba cada acción de su oponente y que él mismo no sabía resolver algunos de los problemas que implicaban cuárticas. Decidió abandonar Milán durante la noche antes de que concluyera el debate, en el que finalmente se declaró vencedor a Ferrari. Como consecuencia, Ferrari ganó fama y tuvo muchas ofertas de trabajo, incluida una del propio emperador, que deseaba un tutor para su hijo. Ferrari nunca volvió a trabajar en matemáticas.

1.3. El diamante en el barro: los números complejos

El libro *Ars Magna* fue sin duda un logro monumental. En ese entonces, la manera en la que los matemáticos razonaban seguía siendo mayoritariamente geométrica. Por ejemplo, interpretaban x^2 como el área de un cuadrado de lado x, o x^3 como el volumen de un cubo. Sin embargo, las ideas de Cardano llevaron este razonamiento a su límite. Un día, durante la escritura de *Ars Magna*, Cardano se encuentra con algunas cúbicas que no pueden ser resueltas fácilmente con el método de Tartaglia. Por ejemplo $x^3 = 15x+4$. Si se aplica el método de Tartaglia a esta ecuación, este requiere en un punto calcular $\sqrt{-121}$, lo que es imposible, pues cualquier número elevado al cuadrado es siempre positivo. Cardano le pregunta a Tartaglia respecto de este peculiar ejemplo, pero Tartaglia evade la pregunta diciendo que Cardano no es lo suficientemente inteligente como para usar su método de manera adecuada. En realidad, Tartaglia tampoco podía explicar lo que estaba ocurriendo. Cardano trata de observar cuidadosamente el fenómeno usando su

método geométrico y llega a la conclusión de que lo que necesita es permitir que cierto cuadrado tenga "área negativa". Esta ni siquiera es la primera vez que un matemático se topaba con el obstáculo que significaban las raíces cuadradas de números negativos. Desde los tiempos árabes existía la pregunta "Encuentre dos números que sumen 10 y que su producto sea 40", o equivalentemente, resolver la ecuación $x^2+40 = 10x$. Si aplicamos el método de Bhaskara veremos que el resultado es $5 \pm \sqrt{-15}$. Por esto mismo, siempre se llegó a la conclusión de que esta pregunta no tiene solución, y en cierto punto eso es correcto. No existen dos números reales que sumen 10 y que el producto de ambos sea 40. En los tiempos de Cardano, la aparición de una raíz cuadrada de un número negativo se interpreta como un signo de que el problema no tenía solución, pero si volvemos al caso de la cúbica $x^3 = 15x + 4$ podemos ver fácilmente que 4 es una solución posible. Entonces, ¿por qué el método que funciona perfectamente con cualquier otra cúbica falla para esta?

Sumido en frustración, Cardano no fue capaz de resolver el misterio por lo que decidió omitir este ejemplo en su obra. En ella escribió que la idea de tomar raíces de negativos era "tan sutil como inútil". Sin embargo, casi diez años más tarde, el ingeniero italiano Rafael Bombelli retoma la idea donde Cardano la dejó. El temerario ingeniero, sin miedo a estas extrañas raíces, se propuso encontrar el diamante enterrado en este barro "tan sutil como inútil". Es entonces cuando Bombelli hace una observación clave. Bombelli se convence de que la raíz cuadrada de un negativo no puede ser ni un número positivo, ni un número negativo. Con este indicio, Bombelli permite que estas raíces sean un nuevo "tipo" de número. Bombelli nota que los términos problemáticos en la solución de la cúbica de Cardano, pueden ser escritos como una combinación de un número usual más un término multiplicado por $\sqrt{-1}$. Cuando permite que este objeto imposible exista, resuelve la ecuación ignorando el elefante en la habitación que causa este término, y descubre que al final, los términos que involucran $\sqrt{-1}$ se cancelan, revelando que 4 es la solución. Este milagro matemático no fue una mera coincidencia. El método de Cardano funciona para cualquier cúbica, pero fue necesario abandonar la intuición geométrica que lo motivó en un principio para hacer manipulaciones con estas raíces cuadradas de negativos en los pasos intermedios.

Durante los siguientes 100 años comienza a surgir la matemática moderna. El álgebra simbólica se establece universalmente. La geometría deja de ser la única fuente de enunciados verdaderos. René Descartes hace un vasto uso de raíces cuadradas de negativos en toda su obra, popularizándolas como un resultado en sí mismo. A pesar de que Descartes reconoce su utilidad, llama a estos números "imaginarios" y el nombre quedó para toda la eternidad. Por esto mismo, después es Euler quien introduce el símbolo i para representar a $\sqrt{-1}$. Cuando estos números se combinan con los números usuales, se forman los denominados "números complejos". La solución de la cúbica llevó a descubrir esta estructura escondida detrás de una imposibilidad y a independizar por completo al álgebra de la intuición geométrica creando un nuevo paradigma en las matemáticas: el de la abstracción.

1.4. El Teorema Fundamental del Álgebra

Con el avance del estudio de las ecuaciones polinómicas comenzaron a surgir nuevas preguntas. Bhaskara nos convenció de que una ecuación cuadrática tiene que tener dos raíces y Tartaglia de que una cúbica tenía que tener tres raíces ¿Será que una ecuación

de grado n tiene siempre n soluciones? Pedro Rothe en su libro Arithmetica Philosophica (publicado en 1608), escribió que una ecuación polinómica de grado n (con coeficientes reales) *podría* tener n soluciones. Albert Girard, en su libro *L'invention nouvelle en l'Algebre* (publicado en 1629), mostró que una ecuación de grado n tiene n soluciones, pero no menciona que dichas soluciones deban ser números reales. Él además agrega que esto vale "salvo que la ecuación sea incompleta", que quiere decir que ninguno de los coeficientes del polinomio sea igual a cero. Sin embargo, parece que Girard sospechaba que esto era cierto para toda ecuación de grado n; en particular, muestra que

$$x^4 = 4x - 3,$$

a pesar de ser una ecuación incompleta, tiene cuatro soluciones (contadas con multiplicidades): 1 (dos veces), $-1 + i\sqrt{2}$ y $-1 - i\sqrt{2}$. Leibniz en 1702 y más tarde Nikolaus Bernoulli, conjeturaron lo contrario.

En 1637, Descartes publica *"La Géométrie"*, donde establece un resultado (que demostraremos más adelante) que resulta crucial en esta historia: si un polinomio $f(x)$ tiene una raíz en a, es decir $f(a) = x$, entonces el polinomio se puede escribir de la siguiente forma:

$$f(x) = q(x)(x - a)$$

donde $q(x)$ es otro polinomio de grado más chico. En la ecuación de antes, cuando decimos que 1 es una raíz *con multiplicidad* 2 nos referimos a que podemos escribir a $x^4 - 4x + 3$ como $q(x)(x - 1)^2$. Una vez establecido este hecho, bastaba probar que todo polinomio de grado mayor que cero tiene una raíz en $\mathbb{C}$, pues si esto valiese, podemos factorizar este polinomio como arriba, y volver a usar el resultado para $q(x)$ hasta llegar a que el polinomio original es un producto de n factores de grado 1, y por lo tanto n raíces.

El primero en intentar demostrar esto fue d'Alembert en 1746. Su demostración tenía un fallo, ya que asumía un cierto resultado que no había sido demostrado aún y que seguiría sin demostrarse hasta un siglo más tarde. Entre otros Euler (1749), de Foncenex (1759), Lagrange (1772) y Laplace (1795) intentaron demostrar este teorema, sin éxito.

Para finales del siglo XVIII, se presentaron dos valientes contendientes. James Wood y Gauss presentaron por separado dos pruebas distintas, pero ambas igualmente incorrectas. Finalmente, en 1806 Argand publicó una prueba correcta para el teorema, enunciando al que hoy conocemos como el *teorema fundamental del álgebra*: todo polinomio con coeficientes complejos tiene al menos una raíz compleja. Gauss no se quedó atrás y dio otro par de demostraciones en 1816 y 1849, siendo esta última otra versión corregida de su demostración original.

El primer libro de texto que contiene la demostración de este teorema fue escrito por un personaje que trataremos con más detalle en la siguiente sección, Augustin Louis Cauchy. Se trata de *Course d'analyse de l'École Royale Polytechnique* (1821). La prueba que se encuentra allí es la de Argand, sin embargo, en el texto no se le da crédito.

1.5. El Muro: la Fórmula Resolvente de la Quíntica

Perfecto, sabemos ya entonces que toda ecuación polinómica de grado n tiene n soluciones, pero nos topamos con un problema ¿Cómo las encontramos? Tenemos fórmulas resolventes para las de grado 2, 3 y 4, que son las que produjeron Bhaskara, Tartaglia y Ferrari respectivamente. Estos métodos utilizan la aritmética básica (sumas, restas,

productos y divisiones) además de la extracción de radicales como las raíces cuadradas o las raíces cúbicas; si una ecuación se puede resolver por un método que utilice estas operaciones se dice que es "soluble por radicales". El siguiente caso naturalmente sería el de las ecuaciones de grado 5 o mayor. Luego de siglos de un paulatino progreso los matemáticos y las matemáticas de la época se chocaron contra un muro, pues dar un método general de resolución la quíntica parecía imposible, aunque igual de imposible parecía demostrar que un método de tales características no existía. Verdaderos genios como Tschirnhaus, Euler, Bézout, Vandermonde, Waring y Lagrange trataron de atacar a este monstruo, pero no lograron resolverlo.

Pasaron 250 años sin que nadie fuera capaz de dar avances en resolver la quíntica, hasta que, siguiendo la tradición nacional, un matemático italiano llamado Paolo Ruffini tuvo un avance. Parece que antes de Ruffini, todo el mundo creía que la quíntica podría resolverse también por radicales. Incluso Lagrange en su célebre artículo "Reflexiones sobre la resolución de ecuaciones algebraicas" decía que volvería a trabajar en su resolución. En 1799, Ruffini publicó un libro sobre *Teoría de Ecuaciones* donde afirmaba que las quínticas no pueden ser resueltas por radicales. El trabajo era excelente, salvo por un salto lógico que invalida el resultado final. Ruffini escribió a Lagrange pero no recibió ninguna respuesta. El mundo matemático ignoró a Ruffini, que publicó una segunda demostración en 1803 y otras en 1808 y 1813.

Sin embargo, al mismo tiempo, un joven matemático noruego también estaba pensando en este gran problema, y también estaba por hacer un gran descubrimiento. Niels Henrik Abel nació en 5 de agosto de 1802, en la isla de Finnöy, en Noruega y bien pudo haber sido el protagonista de esta historia. Abel creció en un ambiente familiar de gran tensión, a causa de las tendencias alcohólicas de sus padres. Fue enviado junto con su hermano a una escuela de la capital, donde sus primeros destellos matemáticos fueron captados por uno de sus profesores, Holmboe. En el peor momento posible, el padre de Abel murió en 1820, dejando a su familia en situación trágica. En 1821 Abel logra ser matriculado en la Universidad de Oslo. Holmboe, muy convencido, había visto en los ojos de aquel frágil estudiante pálido y con atuendo descuidado, los ojos de uno de los más grandes matemáticos de todos los tiempos, por lo que decide ofrecerle alojamiento gratuito y algún dinero para pequeños gastos. Abel se graduó en 1822.

Ante toda adversidad, logra publicar sus primeros trabajos y comienza a hacerse de un considerable prestigio. En su último año de escuela, Abel se mostraría muy interesado en un importante problema del álgebra: la resolución por radicales de la quíntica. Debido a sus minuciosas lecturas, Abel estaba enterado no sólo de las fórmulas de Cardano y de Ferrari para las ecuaciones cúbicas y cuárticas, sino que conocía muy bien la problemática pendiente. A fines de 1823, Abel llegaría a la conclusión de que resultaba imposible la resolución por radicales de la quíntica, y da una demostración que resultó estar incompleta. El joven creyó en principio, haber resuelto el problema de la quíntica; pero como ni Holmboe ni ninguno de los mejores matemáticos de Noruega pudieron comprobar la veracidad de su conjetura, envió a través de Holmboe la presunta resolución al matemático F. Degen en Copenhague, para que la presentase a la Real Sociedad de Ciencias de Dinamarca. Degen le contestó requiriéndole algún ejemplo numérico, y sin comprometerse a dar su opinión. Al buscar ejemplos, hallaría el error. Tras algunas correcciones y después de los aportes que Ruffini haría sobre el trabajo de Abel en 1813, se logró demostrar que había una ecuación quíntica que no era resoluble por radicales. Nosotros demostraremos este resultado que hoy se conoce como Teorema de Abel-Ruffini.

Sin embargo y por desgracia, arruinado y aquejado de una brutal tuberculosis, Abel apenas pudo consolidar su prometedora carrera académica y murió a los veintisiete años. N.H. Abel, fue un genio incomprendido marcado por la fatalidad. Su vida es un triste ejemplo del drama que representa en muchos casos la pobreza y la tragedia. Tuvo que salir de su tierra, para contactar con los grandes matemáticos europeos que sumergidos en sus propia tareas, o tal vez porque encontraban a aquel mísero estudiante noruego un pobre diablo con vanas quimeras, no prestaron la debida atención. La Academia de Ciencias de Francia en 1830 concedió a Abel el Gran Premio de Matemáticas, pero Abel ya había fallecido. Hoy en día, Abel es uno de los iconos nacionales de Noruega.

Abel y Ruffini, en un esfuerzo monumental, lograron establecer que no todas las ecuaciones de grado 5 eran resolubles por radicales. Pero el tema estaba lejos de ser resuelto, pues después del 5 viene el 6 y luego el 7. El resto de las ecuaciones seguían siendo un misterio. Incluso la imposibilidad de resolver las ecuaciones de grado 5 deja una pregunta igual de grande en ese caso: ¿Bajo qué condiciones una ecuación es soluble por radicales? Se inaugura entonces un nuevo problema: dar condiciones necesarias y suficientes para que una ecuación sea soluble por radicales. Ahora bien, si tardamos 250 años en pasar del caso de grado 4 a la imposibilidad del grado 5 ¿Cuantos siglos íbamos a tardar en decir algo sobre el caso de grado 6? O mucho peor: ¡del caso de grado n para todo n natural! La respuesta es que no mucho y hay un joven matemático que está por anunciarse en medio de esta incógnita.

2. Evariste Galois

Francia, 1789. La toma de la Bastilla acaba de dar el pistoletazo de salida a la Revolución Francesa. Con ella, se produjo el mayor cambio social y político conocido hasta la fecha en Europa. Se pasó del absolutismo a la república, después se construyó el imperio napoleónico y se acabó en una monarquía constitucional. Se abolió el feudalismo y se proclamó la Declaración de los Derechos del Hombre y del Ciudadano. Ideas nuevas, como las del lema galo *liberté, égalité, fraternité*, inundaban las calles de París y de toda Francia. Fue una época de cambios convulsos y revoluciones. Es en este contexto alborotado, que comienza la historia de nuestro protagonista.

2.1. La infancia de Evariste Galois

Evariste Galois nació el 25 de octubre de 1811 al sur de París, en Bourg-la-Reine, un pueblo en los alrededores de la capital. Fue el segundo de tres hijos (su hermana mayor Nathalie-Theodore, y su hermano menor Alfred). Su padre, Nicolas-Gabriel Galois, era director de un colegio de ideas liberales, muy afines al régimen de Napoleón. Su madre Adelaide-Marie Demante, que era hija de juristas, se encargó de la educación de sus tres hijos durante su infancia, enseñándoles latín y griego.

A los doce años, Evariste salió de casa para comenzar sus estudios en el prestigioso liceo Louis-le-Grand. Allí han estudiado muchos intelectuales conocidos de la época, incluso matemáticos como Hermite, Borel o Lebesgue. Aquel liceo era uno muy exigente en el que se imperaba una férrea disciplina más propia de los cuarteles que de un colegio. Las instalaciones oscuras y las ventanas enrejadas le daban a este lugar una esencia tétrica. Gracias a la educación de su madre, Galois fue un muy buen estudiante durante

sus primeros años. Tenía 15 años cuando el nuevo director del liceo, presionó y consiguió que el muchacho repitiera un curso de retórica que ya había comenzado, alegando que era demasiado joven (ya había adelantado un curso) y por ende carecía de la madurez necesaria. Su padre y él no tuvieron más opción que aceptar. Al repetir el curso, Galois descubrió las matemáticas a través de Jean Hyppolite Vernier, su profesor de esa asignatura. Su maestro decidió usar el libro de texto *Éléments de Géométrie* de Adrien-Marie Legendre, que estaba pensado para un curso de dos años. Una supuesta anécdota relata que Evariste leyó todo el tomo en dos días. Comenzaba entonces una pasión que lo marcaría de por vida.

Enseguida Galois quedó fascinado por el mundo de las ideas matemáticas. Su obsesión lo llevó a descuidar por completo el resto de las asignaturas. Al menos eso pensaban sus profesores, que dijeron "El furor de las matemáticas lo domina". Recomendaron a sus padres que su hijo se centre en esta disciplina, aunque quizás solo Vernier podría llegar a vislumbrar que muy en el fondo ese niño tenía algo distinto. Para ese entonces Galois ya estaba leyendo libros más avanzados como algunos textos de Joseph-Louis Lagrange como *Lecciones sobre cálculo de funciones, Reflexiones sobre la resolución de ecuaciones algebraicas* o *La teoría de funciones analíticas.*

Llegamos entonces al verano de 1828, cuando por su propia voluntad, Galois decide presentarse a los exámenes de ingreso de la École Polytechnique. Lo hace con diecisiete años de edad, uno menos que la edad habitual de los alumnos que se presentaban a ese examen. Su don y su pasión por las matemáticas no resultaron ser suficientes y reprobó el examen. De todos modos, Evariste no se rindió. Decidió volver a Louis-le-Grand para terminar el curso de matemáticas y prepararse mejor.

A su vuelta conoce al profesor Louis Richard. Si con Vernier había descubierto que le gustaban bastante las matemáticas, con Richard empezó su carrera como matemático. Richard era un gran profesor; sabía motivar muy bien a sus alumnos y transmitir su pasión por las matemáticas. Cuando conoció a Galois, supo que estaba delante de una verdadera joya. De él dijo: "Este alumno tiene una marcada superioridad sobre sus compañeros de clase" y "solo trabaja en los rincones más elevados de la matemática". Por primera vez, Galois encontró alguien que compartía su pasión y lo entendía. Richard era un matemático, y como tal, se interesaba mucho por las novedades de la disciplina. Decidió entonces que era una buena idea llevar a Evariste un paso más lejos: la investigación matemática. A partir de esos momentos, Galois ya no solo lee matemáticas, sino que también empieza a sembrar ideas increíbles.

En la primavera de 1829, esas ideas ya llevaban un tiempo revoloteando por su cabeza, y empezaron a brotar. Su investigación se trataba de algunos aportes a la resolución de ecuaciones algebraicas. Galois publicó su primer artículo en la revista *Annales de mathématiques pures et appliquées.* Escribió sobre la resolución de una ecuación de segundo grado usando fracciones continuas, una idea matemática que estaba muy de moda en aquella época y que ahora ha caído un poco en desuso. Richard, convencido del potencial de su joven pupilo lo animó a escribir dos ensayos más *Recherches algebraiques* y *Recherches sur les équations algébriques de premier degré* (investigación sobre ecuaciones algebraicas de primer grado). Además, Richard fue a la Académie Royale des Sciences (Academia de ciencias de París), donde se podía encontrar a los matemáticos más conocidos del momento. Entre ellos, por ejemplo, Augustin Louis Cauchy, uno de los matemáticos más prestigiosos de dicha época. Richard le contó sobre este joven matemático que demostraba mucho potencial. El 25 de mayo, Cauchy presentó en la academia

uno de los artículos de Galois y la semana siguiente, el otro. El proceso era similar al que hoy en día siguen los investigadores que publican sus trabajos en revistas. Primero se enviaba el trabajo a La Academia, donde debía pasar por una agobiante burocracia, para luego ser enviada a varios referís que leían el trabajo y elaboraban un informe valorativo. Ese informe luego lo veían los encargados de la revista para decidir si publicaban o no el artículo. Como referís en este caso, quedaron finalmente el propio Cauchy, Claude-Louis Henri Navier y Joseph Fourier para el primer artículo; y para el segundo, de nuevo Cauchy con Simeon Denis Poisson. Menudo cuarteto. ¿Qué pasó entonces? La tragedia pegó primero, y un hecho inesperado que ocurrió antes de que se supiera el veredicto cambió de golpe la vida de Galois.

2.2. Que se rompa pero que no se doble

Recordemos el contexto histórico de la década: Cuando murió el rey Luis XVIII, en 1824, lo sucedió en el trono su hermano Carlos X, el último Rey Borbón francés. La Revolución Francesa había traído nuevas ideas progresistas y liberales, pero no todos comulgaban con esas ideas. Durante aquella época, la tensión entre monárquicos y liberales iba en aumento y el nuevo monarca era más afín a los sectores más conservadores y reaccionarios, lo que produjo que la iglesia y los conocidos como ultramonárquicos tuvieran mayor poder. Pero volvamos al pequeño pueblo de Bourg-la-Reine. Nicolás-Gabriel el padre de Galois, a pesar de suscribir a las ideas liberales, mantuvo su cargo durante la restauración borbónica. Sin embargo, en 1829 llegó al pueblo un nuevo sacerdote, que junto con los ultramonárquicos, se propuso acabar con la carrera del director; entonces recurrió a los métodos más antiguos de la política: la mentira y la difamación. Impulsó una campaña de desprestigio repartiendo textos haciéndose pasar por el padre de Galois en los que hablaba mal de los vecinos. Nicolás-Gabriel, incapaz de soportar el escándalo, se sumió en una gran depresión. Finalmente, se quitó la vida el 2 de julio de 1829.

Naturalmente, la noticia pesó mucho sobre la vida de Galois. Para colmo, el mismo sacerdote pretendió dirigir el funeral del injuriado después de conspirar en su contra. Es muy probable que Evariste haya heredado las ideas liberales de sus padres, pero sin duda este hecho despertó una nueva faceta en él, una rebelde y revolucionaria que rechazaba completamente a toda forma de autoridad. Además, desde ese momento, se implicó en causas liberales y revolucionarias que se organizaban en la zona. No había un peor contexto posible para que llegara el momento de volver a intentar entrar en la École Polytechnique. Este era su último cartucho, pues la institución sólo permitía dos intentos. Apenas un mes después del funeral de su padre, y como se podrá imaginar, Galois no aprobó. Se dice que terminó arrojando un borrador en la cabeza a uno de los examinadores por no ser capaz de entender sus razonamientos. Cerradas las puertas de la École Polytechnique, se conformó con la menos prestigiosa École Normale, que se encargaba de la formación de los profesores de secundaria. A principios de 1830 firmó un contrato con la institución, que le garantizó una beca con la que pudo sobrevivir y seguir estudiando matemáticas. A principios de ese mismo año, parecía que la Academia de Ciencias se iba a pronunciar respecto de los trabajos de Galois. Pero el 18 de enero, día pactado para que Cauchy diese sus impresiones, dijo que estaba enfermo y que no iba a poder asistir. Una semana después, Cauchy se presentó en la Academia, pero ignoró completamente el trabajo de Galois y se dedicó a hablar solo del suyo. La farándula matemática de la época rumoreaba que Cauchy, para decirlo en francés, era un ciprés en

el jardín, erguido y orgulloso, que se creía superior a las demás plantas. Parece que esta actitud egocéntrica privó a Galois de su reconocimiento.

Cuando parece que nada puede empeorar, el destino se ríe de nuestra inocencia. Resulta que Galois, impaciente e inconforme, reescribió el trabajo y se presentó a un premio muy prestigioso que otorgaba la Academia, que él creía merecer (para ser justos, Galois tampoco quería pasar muy desapercibido en el jardín de Cauchy). El título de la nueva obra era *Memorie sur les conditions de résolubilité des équations par radicaux* o Memorias sobre las condiciones de resolubilidad de ecuaciones por radicales (Memorias en este contexto quiere decir trabajo o artículo). En ese trabajo, se encontraba la pieza final que hacía falta para que este problema de milenios empezara a acabarse; solo era cuestión que alguien lo leyera para corroborar el enorme potencial que tenía esta teoría. Galois lo presentó a finales del mes de febrero del año 1830, y ahora el encargado de leerlo resultó ser Fourier, que se llevó la memoria a su casa; con el único problema de qué Fourier se murió días más tarde. La única copia quedó entre sus papeles, pero bien la pudieron haber enterrado junto a Fourier, pues nadie la iba a leer en el tiempo previsible. El trabajo ni siquiera fue considerado en el concurso, aunque (una buena para la academia) el premio fue entregado a título póstumo a N. H. Abel. De todos modos, la mala suerte se relamía con el atormentado Evariste.

Aunque parezca un poco forzado, no todo eran malas noticias para Galois. En aquellos años logró entablar una gran amistad con un compañero de la escuela, que años más tarde resultaría un actor crucial para que hoy sepamos de la existencia de Galois: se trata de Auguste Chevallier. Evariste, junto con su hermano Alfred, transmitieron sus ideas revolucionarias a Chevallier y juntos comenzaron a luchar por causas sociales que los interpelaban.

Y de revoluciones trata este texto. En julio de 1830, Francia era básicamente un barril de pólvora. El rey Carlos X tomó algunas decisiones ligeramente antipáticas como suspender por completo la libertad de prensa o disolver la Cámara de diputados, por lo que el barril explotó. Una revuelta social que se conocería como *Les Trois Glorieuses* o "las tres jornadas gloriosas" estalló en París y Carlos X se vió forzado a exiliarse (curiosamente, junto con Cauchy, que era totalmente leal a la causa borbónica) y la revolución culminó con la coronación de Luis Felipe I, de tendencia más liberal. Galois no pudo participar. El director de la escuela impidió a los alumnos que se unieran al resto de los manifestantes que se levantaron en armas. Durante su segundo año, sus ideas iban radicalizando cada vez más a la par que se involucraba en las luchas. Llegó a conocer a futuros líderes políticos como Auguste Blanqui y Francois Vincent Raspail. También se unió a la *Societé des Amis du Peuple* ("Sociedad de Amigos del Pueblo"), una organización popular clandestina que llegó a emplear métodos violentos para luchar contra los borbones.

Esta politización que transitó Galois, le hizo ganarse un adversario poco estratégico: el director de la École Normale. Su tensión fue aumentando hasta que se resolvió de la peor manera. Apareció una carta anónima en una gaceta estudiantil en la que se cargaba duramente contra el director. Pese a ser anónima, se le atribuyó a Galois, que no confirmó ni negó haberla escrito. Aunque nunca se pudo confirmar que fue él, el director no tuvo dudas y el 9 de diciembre de 1830 Galois fue expulsado de la École Normale. Incluso después de la expulsión, aparecieron algunos artículos en diversos periódicos pidiendo por la reincorporación del muchacho, como también apareció una del director, justificándose.

En medio de estos tiempos tan convulsos, Galois pensó que sería una buena idea

enlistarse en una sección de artillería. Pero poco le duró el puesto, pues menos de un mes más tarde, se reorganizó ese cuerpo por un decreto real y Galois quedó afuera. Para ganarse la vida, empezó a dar clases de álgebra en la librería de un amigo suyo. Para publicitarse incluso publicó un anuncio en el mismo diario en el que había arremetido en contra del director. Varios de sus amigos se anotaron para apoyarlo en un momento tan delicado para él. En sus clases enseñaba sus conocimientos sobre la materia que no eran pocos. Entre lo avanzadas que eran sus clases y que los alumnos iban por hacerle el favor, sus clases terminaron quedando desiertas. Perdido en el oscuro laberinto de la pobreza, al igual que Mozart, terminó dando clases particulares para sobrevivir, sin ningún interés matemático para él, pues eran clases muy elementales.

La Academia volvió a cruzarse en la vida de Evariste. En enero de 1831, le pidieron que entregara una nueva memoria de su trabajo. El día 17 se presentó *Memorie sur les conditions de résolubilité des équations par radicaux*, que cayó en manos de Poisson y Sylvestre Lacroix. Pasado un tiempo, harto de que no le dieran una respuesta, Galois terminó escribiendo un carta con sarcásticos reproches hacia la Academia:

> Señor presidente, le agradecería que expulsara mi inquietud invitando a declarar a los señores Poisson y Lacroix si han extraviado mi memoria (como ocurrió con la que se quedó Fourier) o si pretenden dar cuenta de ella en la Academia.

Siguió sin respuesta.

2.3. ¡A Luis Felipe!

Mientras que Galois esperaba una respuesta de la Academia, tenía mucho tiempo libre para dedicarse a la vida política. En abril de 1831, absolvieron a un grupo de la Guardia Nacional que se había negado a bajar las armas. Esto fue celebrado por la Sociedad de los Amigos del Pueblo con una gran comida de unos doscientos invitados, entre los que se encontraba nuestro pobre Evariste. En la sobremesa, los brindis y las consignas liberales eran proporcionales a la cantidad de alcohol que se servía, cuando de repente se oyó: "¡A Luis Felipe!". No era otro que el desafortunado de Galois, que justo resultaba llevar una copa en una mano y un cuchillo en la otra. Esto se interpretó como una amenaza al rey y al día siguiente lo detuvieron. Pasó un mes en la cárcel hasta que llegó el juicio, en el que se defendió argumentando que el cuchillo lo tenía porque estaba cortando carne, y que su consigna fue "A Luis Felipe, si nos traiciona", pero que por el bullicio no se escuchó la última parte. Por suerte, Galois fue absuelto de todos los cargos.

Menos de un mes le duró la libertad. En ese lapso, Chevallier y su hermano publicaron en un diario republicano llamado *Le Globe* un artículo narrando la vida de Galois. En esa defensa de su amigo, Chevallier contaba cómo las instituciones le habían negado las oportunidades que sus ideas merecían. Al poco tiempo, la Academia finalmente se pronunció, quizás apurada por las palabras de Chevallier. Pasados siete meses desde que fue presentado el trabajo este fue el veredicto de Poisson:

> Hemos hecho todos los esfuerzos por entender la demostración de Galois. Sus razonamientos no son lo suficientemente claros ni están bastante desarrollados para que podamos juzgar su exactitud y no estaríamos en disposición de dar una idea en este informe. El autor anuncia que la proposición que es el

> objeto principal de esta memoria es parte de una teoría general susceptible de otras aplicaciones. En ocasiones, resulta que diferentes partes de una teoría se clarifican mutuamente y son más fáciles de entender juntas que por separado. Esperamos que el autor haya publicado el trabajo entero para formarse una opinión definitiva; pero en el estado en el que está la parte que se ha presentado a la Academia no podemos recomendar la aprobación.

La vida le daba otro golpe. Otra vez, sus brillantes ideas no eran valoradas entre los matemáticos de elite de la época. Quizás simplemente no pudieron entenderlas y se excusaron para deshacerse de ellas.

Ese mismo verano, Galois volvió a caer preso. Su incontrolable desobediencia le jugó otra mala pasada. El 14 de julio, día de la Bastilla, se prohibieron las manifestaciones republicanas. Se hicieron detenciones preventivas la noche anterior, aunque Galois se salvó de esas. A la mañana siguiente, apareció en el famoso puente parisino Pont Neuf. Iba vestido de su traje de la Guardia Nacional (ilegalizado) y armado hasta el cuello. Esta actitud le constó una nueva detención y la posterior condena de nueve meses en prisión, hasta abril de 1832. En la cárcel de Sainte-Pélagie estuvo con su compañero revolucionario Raspail.

Parece que las pésimas condiciones de vida cambiaron algo en Galois. Raspail incluso cuenta un incidente en que Galois, estando borracho, trató de suicidarse. En la primavera de 1832 un brote de cólera atacó a toda Francia y en particular a la capital, donde las condiciones de higiene eran verdaderamente desagradables. Y si así estaba la ciudad, imagínese cómo deben haber estado las cárceles. Decidieron trasladar a los presos más vulnerables y jóvenes, entre ellos a Galois, a una casa de reposo, bajo la promesa de no fugarse.

Fue en ese momento cuando Galois conoció a Stephanie Poterin, que vivía en el mismo edificio. Esta es la primera vez, que sepamos, que Galois se enamoraba. Realmente se desconoce que fue lo que pasó entre Evariste y Stephanie, lo que si sabemos es que no terminó bien. Stephanie le escribió dos cartas a Galois, que este rompió en un ataque de rabia, aunque después trató de reconstruirlas. Esa reconstrucción incompleta es la que nos queda. En la primera se puede leer: “Pongamos punto final a esto, por favor. No tengo [...] para seguir una correspondencia de esta clase, pero trataré de tener el suficiente ánimo para conversar con usted”. La segunda carta, más contundente, le pide a Galois cortar cualquier tipo de relación. Lo que se puede intuir, es que Evariste se formó expectativas románticas que no fueron correspondidas. La amorosa era la última de las desdichas que le faltaba a Galois en su colección, y sin duda lo dejó muy deprimido.

El 29 de abril termina su condena, pero Galois, que solo tenía veinte años, no tenía hogar ni recursos, por lo que decidió quedarse a vivir provisionalmente en la casa de reposo. La muerte toca la puerta.

2.4. Tres Cartas, dos pistolas

La última parte de esta historia es por lo menos muy confusa. No sabemos que fue de Galois durante esos días, pero estamos citados a asistir al acontecimiento crucial el 29 de mayo. Sin pruebas fehacientes de los motivos, Galois está por su parte, citado a un duelo a pistola. Si en la sección anterior, mucho más iluminista, las diferencias se

dirimían con duelos matemáticos, las balas eran ahora mucho más comunes. Su rival y el origen de la disputa siguen siendo un misterio, lo que ha dado lugar a un montón de investigaciones históricas tratando de descubrir qué fue lo que pasó. Existen tres principales hipótesis: una disputa amorosa por Stephanie, un asesinato político o un suicidio pactado. La cantidad de testimonios contradictorios tornan muy difícil llegar a conclusiones: las cartas de Galois, la versión de su hermano Alfred, la reseña de una gaceta republicana, y más. Y como el pobre de Galois tuvo una vida tan revolucionada, ninguna se puede descartar del todo. La que más ha trascendido es la relacionada a Stephanie y a dos hombres de su entorno (serían familiares u otros pretendientes). Esta línea de investigación propone la teoría de que Galois le habría dicho algo (no se sabe si a Stephanie o a estos dos hombres) que resultó ofensivo para la mujer, por lo que los dos hombres sintieron la necesidad de defender el honor de Stephanie.

Convencido de que no tenía posibilidad de ganar, y como ya mencionamos, Galois pasó noche anterior al duelo escribiendo cartas. Una de ellas iba destinada a "todos los republicanos" y empieza pidiendo que no le reprochen no morir por su patria. En ellas deja algunas frases insinuando lo que ocurrió:

> Muero víctima de una infame coqueta y dos engañados por esta coqueta. Mi vida se apaga por un miserable chisme. El cielo da testimonio de que solo forzado he accedido a una provocación que he intentado evitar por todos los medios. Me arrepiento de haber contado una verdad fatal a hombres tan poco capaces de escucharla.

Y termina con una frase muy extraña: "Perdón por los que me mataron, son de buena fe". Resulta confuso que Galois esté tan convencido de su propia muerte. Al fin y al cabo, un duelo es impredecible, aunque no lo pueda ver un joven pesimista la noche anterior al mismo. Esto es lo que llevó a conjeturar también que pudo haber sido un suicidio pactado, bien para acabar con su desdichada vida o bien para involucrar a la policía y provocar un levantamiento que sirva a la causa revolucionaria. Eso explicaría su disculpa hacia sus asesinos pero deja un hueco en la parte de la "infame conqueta". Otra teoría dice que la quizás la coqueta no era Stephanie, y que en realidad todo fue un plan de la policía para acabar con Evariste, pero entonces ¿Por qué excusar a sus asesinos? Como se puede ver, nada cierra del todo.

Pero para confundir más todavía, la segunda carta estaba dirigida a sus amigos N. L. y V. D., que seguramente hayan sido Napoleón Lebon y Vincent Delaunay. En ella deja información aún más confusa sobre las circunstancias:

> He sido retado por dos patriotas [...]. Me ha sido imposible rehusar. Perdónenme no haberles advertido a ninguno de los dos. Pero mis adversarios me obligaron por mi honor no informar a ningún patriota.

La carta termina con una súplica:

> Recuérdenme, ya que la suerte no me ha concedido bastante vida para que la patria me recuerde.

Con respecto a la última carta, estaba dirigida a su amigo Auguste Chevallier, y esta es (con respeto a los amigos republicanos) la que verdaderamente importa. En ella Galois

deja escrito su testamento matemático, compuesto de las memorias perdidas, olvidadas e ignoradas por la Academia y de nuevas ideas que según sus propias palabras: "Han rondado mi cabeza por casi un año". La carta comienza así:

> Mi querido amigo: He hecho varias cosas nuevas en análisis. Unas conciernen a la teoría de ecuaciones, y otras a funciones integrales. En la teoría de ecuaciones, he investigado en qué casos las ecuaciones son solubles por radicales: esto me ha dado la ocasión de profundizar en esta teoría, y de descubrir todas las transformaciones posibles de una ecuación, incluso si no es soluble por radicales. Todo esto puede encontrarse en tres memorias.

En cuatro páginas, Galois hace una síntesis de la memoria que rechazó Poisson y agrega nuevos resultados que había ido desarrollando en esos meses. La carta termina diciéndole a su amigo Auguste que ha explorado más asuntos que no aparecen en los papeles y concluye con una frase que lamentaremos por siempre:

> No tengo tiempo y mis ideas no están todavía suficientemente desarrolladas en ese terreno, que es inmenso.

También le pide a su amigo que le lleve sus resultados a Jacobi o a Gauss, convencido que ellos sí sabrían valorarlo. Finaliza expresando su esperanza de que sus ideas sean estudiadas por alguien algún día:

> Después de eso, espero, habrá gente que encontrará provechoso descifrar todo este lío.

La hora ya es cumplida. Galois acude al amanecer a batirse a duelo, que se salda con un tiro en el abdomen que lo deja malherido. Alguien lo recoge y lo lleva al hospital más cercano, donde pasará las últimas horas entre esa delgada línea entre la vida y la muerte. Al hospital acude su hermano Alfred. Efectivamente, a las 10 de la mañana del 31 de mayo de 1832, Evariste Galois muere en la cama de un hospital. Lo acompañaba su hermano Alfred, al que le dedicó sus últimas palabras:

> No llores, necesito todo mi coraje para morir a los veinte años.

2.5. Legado

Tras su muerte, se celebró un funeral repleto de republicanos amigos que fueron a despedirse de Evariste. Sin embargo, a diferencia de la historia de Abel, el mundo matemático ni se inmutó por la gran pérdida que acababa de sufrir. Fueron su hermano Alfred y Chevallier, que recopilaron sus trabajos y cumplieron su cometido. Le entregaron todo lo que tenían a Joseph Liouville, que en 1843 lo hizo público, como no podía ser de otra manera, en la Academia de Ciencias. Tres años más tarde, Liouville que tenía su propia revista, publicó todos los resultados de Galois. Y, ahora sí, 14 años de muerto Galois, toda su teoría comenzó una revolución matemática. Jacobi, uno de los matemáticos que Galois pidió en las puertas del cielo que lo leyera, se interesó mucho por sus ideas a raíz de lo publicado por Liouville.

Galois había dado forma a una idea con la que Lagrange y Cauchy habían coqueteado, pero no habían podido ver el enorme potencial que yacía atrás de eso. Hablo de la

definición de Grupo. Galois fundó la Teoría de Grupos. Y lo hizo, como imaginarán, para establecer una condición necesaria y suficiente para que una ecuación sea soluble por radicales. Galois lo hizo. Vino a este mundo, puso fin a un problema de milenios y se fue. Fue tan efímero como impactante. Pero bueno, ¿cual es la respuesta?¿Qué fue lo que encontró? La respuesta a esta pregunta es la que se desarrolla en el resto de este trabajo.

3. La Teoría de Galois

Ha llegado el momento. Nos ponemos los guantes matemáticos y comenzamos a presentar a la estrella de esta historia: la Teoría de Galois. Por conveniencia pedagógica tendremos que abandonar el rigor histórico, pues la manera en la que se presentará esta teoría no es la que Galois empleó originalmente. Décadas después, Emmy Noether y Emil Artin reescribieron estas ideas en un lenguaje más moderno, compacto y mucho más conveniente para presentarlo en un trabajo como este. Tendremos que asumir también que el lector esta familiarizado con ideas generales del álgebra lineal y algunas ideas básicas de estructuras algebraicas como espacios vectoriales, grupos y anillos. De todos modos esta sección comienza con un breve repaso sobre teoría de anillos conmutativos. En caso de no estar muy familiarizado con la teoría de grupos, una amigable introducción a esta hermosa teoría se puede encontrar en [Wel].

3.1. Repaso de álgebra

Comenzaremos con un breve repaso sobre álgebra conmutativa. Pasaremos gran parte de este trabajo discutiendo sobre cuerpos y polinomios, y el sistema algebraico que abarca estos dos conceptos es el de los anillos conmutativos. Nos tomaremos el atrevimiento de dejar a lo largo de este capítulo algunos ejercicios instructivos que serán de utilidad más adelante. Si el lector ya está familiarizado con las ideas de este capítulo bastará un momentáneo pensamiento para convencerse de la validez de los mismos. En cambio, si este es su primer acercamiento a estas definiciones aconsejamos fuertemente detenerse a intentarlos.

Definición 1. Un **anillo conmutativo con 1** es un grupo abeliano R con una operación binaria $\cdot : R \times R \to R$ llamada producto o multiplicación que denotaremos como $(r, s) \mapsto rs$, tal que:

- El producto es conmutativo y asociativo.
- Existe un elemento $1 \in R$ tal que

$$1r = r, \ \forall\, r \in R.$$

- El producto es distributivo respecto de la suma:

$$r(s + t) = rs + rt, \ \forall\, r, s, t \in R.$$

De ahora en adelante todo anillo será considerado conmutativo y con 1.
Ejemplos:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos.
2. Dado un entero positivo n, el conjunto $\mathbb{Z}_n$ de enteros módulo n forman un anillo.
3. Si R es un anillo, definimos un **polinomio** $f(x)$ con **coeficientes** en R (o simplemente un **polinomio sobre** R) como una sucesión:

$$f(x) = (r_0, r_1, \dots, r_n, 0, 0, \dots)$$

con $r_i \in R$ para todo i y $r_i = 0$ para todo $i > n$ y para algún n. Si $g(x) = (s_0, s_1, \dots, s_m, 0, 0, \dots)$ es otro polinomio, decimos que $g(x) = f(x)$ solo si $s_i = r_i$ para todo i. Denotamos al conjunto de todos los polinomios sobre R como $R[x]$. Definiremos una suma y producto en $R[x]$ de la siguiente manera:

$$(r_0, r_1, \dots, r_i, \dots) + (s_0, s_1, \dots, s_i, \dots) = (r_0 + s_0, r_1 + s_1, \dots, r_i + s_i, \dots)$$

y

$$(r_0, r_1, \dots, r_i, \dots)(s_0, s_1, \dots, s_j, \dots) = (t_0, t_1, \dots, t_k, \dots)$$

donde $t_0 = r_0 s_0$, $t_1 = r_0 s_1 + r_1 s_0$, y, en general:

$$t_k = \sum_{i+j=k} r_i s_j.$$

Si definimos $1 = (1, 0, 0, \dots)$ podremos comprobar que $R[x]$ es un anillo con las operaciones definidas arriba. Llamaremos a este anillo, el **anillo de polinomios sobre** R. Es natural preguntarse cuál es el sentido de la letra x en la notación $f(x)$. Sea x el siguiente elemento de $R[x]$:

$$x = (0, 1, 0, 0, \dots)$$

Es fácil verificar que $x^2 = (0, 0, 1, 0, 0, \dots)$ y, por inducción, que x^n será la sucesión que tiene 0 en todas las entradas salvo en la n-ésima. El lector podrá verificar ahora, reencontrándose con la usual notación, que:

$$f(x) = (r_0, r_1, \dots, r_n, 0, 0, \dots) = r_0 + r_1 x + \cdots + r_n x^n = \sum_{i=0}^{n} r_i x^i.$$

También identificaremos al elemento $r_0 \in R$ con el polinomio $(r_0, 0, 0, \dots) \in R[x]$. Notar que en este contexto x es un polinomio en sí mismo y no una variable.

Recordamos también el vocabulario usual asociado a un polinomio $f(x) = r_0 + r_1 x + \cdots + r_n x^n$. El **coeficiente principal** de $f(x)$ es r_n, donde n es el mayor entero (si existiera) tal que $r_n \neq 0$; n se llama el **grado** de f y lo denotaremos por ∂f. Todo polinomio tiene un grado excepto el polinomio $0 = (0, 0, \dots)$. Un polinomio se dice **mónico** si su coeficiente principal es 1. El **término constante** de un $f(x)$ es r_0. Un **polinomio constante** es el polinomio 0 ó un polinomio de grado 0. Llamamos a un polinomio **lineal**, **cuadrático**, **cúbico**, **cuártico** y **quíntico** si es de grado 1, 2, 3, 4 o 5 respectivamente.

Teorema 1. Sea R un anillo.

(I) $0r = 0 \ \ \forall r \in R$

(II) $-r = (-1)r \ \ \forall r \in R$ (donde $-r$ es el inverso aditivo de r, es decir, $-r + r = 0$)

(III) $(-1)(-r) = r \ \ \forall r \in R$ (en particular, $(-1)(-1) = 1$)

Demostración. (I) Usamos la propiedad distributiva:

$$0r = (0 + 0)r = 0r + 0r$$

y restando $0r$ en ambos lados obtenemos que $0r = 0$

(II) $0 = 0r = (-1 + 1)r = (-1)r + r$; ahora sumando $-r$ a ambos lados obtenemos $-r = (-1)r$

(III)

$$\begin{aligned} 0 = 0(-1) &= (-r + r)(-1) \\ &= (-r)(-1) + r(-1) \\ &= (-r)(-1) - r \end{aligned}$$

sumando r a ambos lados se tiene $(-1)(-r) = r$.

□

Si R es un anillo en donde $1 = 0$ y tomamos $r \in R$, entonces:

$$r = 1r = 0r = 0$$

luego, en tal caso R tendrá solo un elemento, el 0. Vamos a permitir la existencia de este ejemplo peculiar, lo llamaremos **anillo nulo.** Este es un buen momento para recordar por qué es imposible definir la división por 0. Si $a, b \in R$, entonces a/b, de existir, debiera cumplir que $b(a/b) = a$. En particular, si $a/0$ existiese, sería un elemento de R tal que $0(a/0) = a$. Pero $0(a/0) = 0$, por el Teorema 1(I). Esto implica que un tal R debe ser el anillo nulo.

Hay dos tipos de anillos que resultarán de vital importancia: dominios íntegros y cuerpos.

Definición 2. Un anillo R es un **dominio íntegro** (o dominio) si no es el anillo nulo y el producto de dos elementos no nulos en R es no nulo.

Notar que $\mathbb{Z}_6$ no es un dominio porque $\overline{2} \neq 0$ y $\overline{3} \neq 0$ pero $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0} = 0$. Este ejemplo se extiende a cualquier $\mathbb{Z}_n$ donde n es un número compuesto. Si n es primo $\mathbb{Z}_n$ es un dominio.

Teorema 2. Un anillo no nulo R es un dominio si y solo si satisface la propiedad de cancelación: si $ra = rb$ y $r \neq 0$ entonces $a = b$.

Demostración. Supongamos que R es un dominio, $r \neq 0$ y $ra = rb$. Entonces $r(a-b) = 0$. Como R es un dominio y $r \neq 0$, $a - b = 0$ y por lo tanto $a = b$. Por otro lado, supongamos que vale la propiedad de cancelación. Si $a \neq 0$, $b \neq 0$ y $ab = 0$, entonces $ab = 0 = a0$ por lo tanto $b = 0$, un absurdo. □

Dejamos a continuación un par de ejercicios que nos serán de gran utilidad más adelante.

Ejercicio 1. Un elemento $u \in R$ se dice una **unidad** si existe otro elemento $v \in R$ tal que $uv = 1$. Mostrar que si R es un dominio y $f, g \in R$ son no nulos y satisfacen que

$$f = ug \text{ y } g = vf$$

donde $u, v \in R$ entonces u y v son unidades de R.

Observación 1. Si R es un anillo, vale la siguiente versión del **algoritmo de la división**: si $f(x)$, $g(x) \in R[x]$ y el coeficiente principal de $g(x)$ es una unidad, entonces existen polinomios $q(x)$ y $r(x)$ (llamados **cociente** y **resto**, respectivamente) tales que

$$f(x) = q(x)g(x) + r(x)$$

donde o bien $r(x) = 0$ o $\partial r < \partial g$

Ejercicio 2. Demostrar que el **teorema del binomio** vale en cualquier anillo R: Si $n \geq 1$,

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

donde $\binom{n}{i}$ denota el coeficiente binomial de Newton $\frac{n!}{i!(n-i)!}$. (Ayuda: probar primero que $\binom{n-1}{i-1} + \binom{n-1}{i} = \binom{n}{i}$)

Ejercicio 3. Si p es un primo, mostrar que p divide a $\binom{p}{i}$ para todo $i \neq 0, p$. (Notar que esto no es cierto si p no es primo estudiando el caso $p = 4$).

Definimos ahora uno de los objetos centrales de la Teoría de Galois que trataremos en profundidad más adelante: los cuerpos.

Definición 3. Un **cuerpo** es un anillo no nulo K tal que $K - \{0\}$ es un grupo con la multiplicación de K, es decir, todo elemento no nulo de K es una unidad.

Los ejemplos básicos de cuerpos son $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_p$ con p primo. Todo cuerpo es un dominio, pues el hecho de que $K - \{0\}$ sea un grupo implica que es cerrado por la multiplicación.

En el álgebra moderna cuando se estudia un objeto resulta de vital importancia tener una noción de morfismo entre dichos objetos. En el caso de los anillos, se tiene la siguiente definición.

Definición 4. Si S y R son dos anillos, una función $\psi : R \to S$ es un **morfismo de anillos** si:

$$\begin{aligned} \psi(r + r') &= \psi(r) + \psi(r') \\ \psi(rr') &= \psi(r)\psi(r') \\ \psi(1) &= 1 \end{aligned}$$

Un morfismo de anillos es un **isomorfismo de anillos** si ψ es biyectiva. En este caso decimos que R y S son isomorfos y escribimos $R \cong S$.

Ejercicio 4. Si $a \in R$ definimos $e_a : R[x] \to R$ mediante $e_a(f) = e_a(\sum r_i x^i) = \sum r_i a^i$ (llamamos a este elemento $f(a)$); mostrar que e_a es un morfismo de anillos (llamado **evaluación en** a). Si $f(a) = 0$ entonces a se dice una **raíz** de $f(x)$.

Definición 5. Un **ideal** en un anillo R es un conjunto I que contiene al 0 y tal que:

1. I es un subgrupo del grupo aditivo de R.
2. Si $a \in I$ y $r \in R$ entonces $ra \in I$

Ejemplos:

1. En todo anillo R y 0 son ideales.
2. Si $\psi : R \to S$ es un morfismo de anillos el **kernel** (o **núcleo**) es:

$$\ker \psi = \{r \in R : \ \psi(r) = 0\}.$$

   El kernel de un morfismo de anillos es siempre un ideal.

3. Si $r_0 \in R$ entonces $\{r \cdot r_0 : \ r \in R\}$ es un ideal. Llamamos a este ideal el **ideal principal generado por** r_0 y lo denotamos (r_0).
4. Si I y J son dos ideales, su suma $I + J = \{r + s : r \in I, s \in J\}$ es también un ideal.

Ejercicio 5. Sea u una unidad de un anillo R.

(I) Si un ideal I contiene a u entonces $I = R$

(II) Si $r \in R$ entonces $(ur) = (r)$.

(III) Si R es un dominio y r, $s \in R$, entonces $(s) = (r)$ si y solo si $s = ur$ para una unidad de R.

Ejercicio 6. (I) R es un cuerpo si y solo sí los únicos ideales son 0 y R

(II) Si F es un cuerpo, entonces las unidades de $F[x]$ son las constantes no nulas.

La definición de ideal puede parecer arbitraria a primera vista, particularmente la segunda condición. La siguiente definición esclarece un poco la razón por la cual esta condición es de crucial importancia.

Sea I un ideal de R. Ignorando momentáneamente la multiplicación de R, sabemos que I es un subgrupo del grupo aditivo R. Más aún, como este grupo es abeliano, I es un subgrupo normal. Por lo tanto, esta bien definido el grupo cociente R/I. Los elementos de este grupo son las co-clases $r + I$ con $r \in R$ y la suma viene dada por

$$(r + I) + (r' + I) = (r + r') + I.$$

En particular, la identidad aditiva es el elemento $0+I = I$. Recordemos que $r+I = r'+I$ si y solo si $r-r' \in I$. Finalmente, recordemos que existe un morfismo (de grupos) canónico $\pi : R \to R/I$ dado por $r \mapsto r + I$.

Teorema 3. Sea I un ideal de R. El grupo abeliano R/I puede ser equipado con una multiplicación que lo transforma en un anillo y que transforma al mapa $\pi : R \to R/I$ en un morfismo de anillos.

Demostración. Definimos una multiplicación en R/I dada por

$$(r+I)(r'+I) = (rr') + I.$$

Para ver que está bien definida, supongamos que $r+I = s+I$ y que $r'+I = s'+I$. Queremos ver que $rr'+I = ss'+I$, es decir $rr'-ss' \in I$. Pero

$$rr'-ss' = (rr'-rs') + (rs'-ss') = r(r'-s') + (r-s)s'$$

Luego, como $r'-s' \in I$ y $r-s \in I$, por hipótesis; tenemos que $r(r'-s') \in I$ y $(r-s)s' \in I$ porque I es un ideal. Como la suma de dos elementos de I es de nuevo un elemento de I tenemos que $rr'+I = ss'+I$. Es sencillo verificar que esta multiplicación cumple todas las propiedades de la definición de anillo. Tambien es fácil ver que con esta estructura π resulta un morfismo de anillos. Dejamos estos detalles como ejercicio para el lector. □

Definición 6. Si I es un ideal de R, entonces R/I se llama **anillo cociente** de R **módulo** I**.**

A continuación demostramos dos teoremas fundamentales relacionados con los anillos cociente.

Teorema 4 (Teorema de la Correspondencia)**.** Sea I un ideal de un anillo R. Existe una correspondencia biyectiva entre los ideales de J de R tales que $I \subset J$ y los ideales de R/I, dada por

$$J \mapsto \pi(J) = J/I = \{a+I \in R/I : a \in J\},$$

donde $\pi : R \to R/I$ es la proyección canónica. Más aún, si $J \subset J'$ entonces $\pi(J) \subset \pi(J')$.

Demostración. Sean $\mathscr{C}$ y $\mathscr{D}$ las familias de ideales de R que contienen a I y de ideales de R/I, respectivamente. Consideramos la proyección canónica $\pi : \mathscr{C} \to \mathscr{D}$ y definimos $f : \mathscr{D} \to \mathscr{C}$ mediante $f(J/I) = \{a \in R : a+I \in J/I\}$. Es sencillo verificar que $\pi(J)$ y $f(J/I)$ son ambos ideales.

Si $J \in \mathscr{D}$, entonces

$$(\pi \circ f)(J) = \{a+I : a \in f(J)\} = \{a+I : a+I \in J\} = J$$

Por otro lado, si $J \in \mathscr{C}$ entonces

$$\begin{aligned}(f \circ \pi)(J) = \{a \in R : a+I \in \pi(J)\} &= \{a \in R : a+I = b+I \text{ para algún } b \in J\} \\ &= \{a \in R : a \in b+I \text{ para algún } b \in J\}.\end{aligned}$$

Donde este último claramente contiene a J. Pero $a \in b+J$ implica que $(a-b) \in I \subset J$, luego, $a = b+J$ y por lo tanto $a \in J$. Es decir, $(f \circ \pi)(J) = J$. Concluimos así que π y f establecen una biyección. Dejamos como ejercicio completar la prueba mostrando que si $J \subset J'$ entonces $\pi(J) \subset \pi(J')$. □

Teorema 5 (Primer Teorema de Isomorfismo)**.** Si $\psi : R \to S$ es un morfismo de anillos y $\ker \psi = I$, existe un isomorfismo de anillos $R/I \to S$ dado por $r+I \mapsto \psi(r)$.

Demostración. Por la versión análoga a este teorema para grupos sabemos que existe un isomorfismo de grupos $R/I \to S$ dado por $r + I \mapsto \psi(r)$. Veamos que también es un morfismo de anillos. Si $r + I$, $s + I \in R/I$ tenemos que

$$(r + I)(s + I) = (rs + I) \mapsto \psi(rs) = \psi(r)\psi(s).$$

Luego, el morfismo $r + I \mapsto \psi(r)$ es efectivamente de anillos. □

Ejercicio 7. Sea I un ideal de un anillo R y J un ideal de otro anillo S. Si $\psi : R \to S$ es un morfismo de anillos con $\psi(I) = J$ entonces existe un isomorfismo de anillos $R/I \cong S/J$.

3.2. El anillo de polinomios sobre un cuerpo

Teorema 6. Si F es un cuerpo, entonces todo ideal de $F[x]$ es un ideal principal.

Demostración. Sea I un ideal de $F[x]$. Si $I = \{0\}$, entonces $I = (0)$ es principal con generador 0. Si $I \neq \{0\}$, consideremos un polinomio $m(x) \in I$ que tenga grado mínimo. Veamos que $I = (m(x))$. Claramente $(m(x)) \subset I$. Para la otra contención sea $f(x) \in I$. Por el algoritmo de la división existen polinomios $q(x)$ y $r(x)$ tal que

$$f(x) = q(x)m(x) + r(x)$$

donde o bien $r(x) = 0$ o bien $\partial r < \partial m$. Ahora, como $r(x) = f(x) - q(x)m(x) \in I$; si $r(x) \neq 0$ estaríamos contradiciendo la hipótesis de minimalidad del grado de $m(x)$ entre los elementos de I. Luego, $r(x) = 0$ y $f(x) = q(x)m(x) \in (m(x))$. □

Es fácil ver que uno siempre puede considerar que $m(x)$ es mónico, pues de no ser este el caso, dividimos toda la expresión por el coeficiente principal.

Definición 7. Un anillo R se dice **dominio de ideales principales** (DIP) si es un dominio en donde todo ideal es principal (Recordar el Ejemplo 3 después de la Definición 5).

El teorema anterior dice que $F[x]$ es un DIP cuando F es un cuerpo. Otro ejemplo de un DIP es $\mathbb{Z}$. Sin embargo, $\mathbb{Z}[x]$ no es un DIP.

Definición 8. Sea R un anillo; si $s, r \in R$, entonces decimos que r **divide** a s si existe un $r' \in R$ tal que $rr' = s$. En tal caso escribimos $r \mid s$.

Si $I = (r_0)$, entonces r_0 divide a todo $s \in I$. Notar que $r \mid 0\ \forall r \in R$, pero $0 \mid r \iff r = 0$. También tenemos que $r \mid r\ \forall r \in R$ y que r es una unidad si y solo si $r \mid 1$.

Definición 9. Sea F un cuerpo y sean $f(x)$, $g(x) \in F[x]$. El **máximo común divisor** (mcd) de $f(x)$ y $g(x)$ es un polinomio $d(x) \in F[x]$ tal que:

(I) $d(x)$ es un divisor común de $f(x)$ y $g(x)$; esto es, $d \mid f$ y $d \mid g$.

(II) Si $c(x)$ es un divisor común de $f(x)$ y $g(x)$ entonces $c \mid d$.

(III) $d(x)$ es mónico.

Denotaremos a $d(x)$ por $(f(x), g(x))$. Si $(f(x), g(x)) = 1$ entonces $f(x)$ y $g(x)$ se dicen **relativamente primos** o **coprimos**.

Notar que el mcd d de f y g, de existir, es único. Si d' es otro mcd, entonces usando (II) para ambos, tenemos que $d \mid d'$ y $d' \mid d$. Luego, por el Ejercicio 1, $d' = ud$ para alguna unidad $u \in F[x]$. Como las unidades de $F[x]$ son los polinomios contantes no nulos y además d y d' son mónicos, $u = 1$. Luego, $d = d'$.

Teorema 7. Sea F un cuerpo y sea $f(x)$, $g(x) \in F[x]$ con $g(x) \neq 0$. Entonces $(f(x), g(x)) = d(x)$ existe y es una combinación lineal de $f(x)$ y $g(x)$. Esto es, existen $a(x)$ y $b(x)$ tal que:

$$d(x) = a(x)f(x) + b(x)g(x).$$

Demostración. Sea

$$I = (f(x)) + (g(x)) = \{a(x)f(x) + b(x)g(x) : a(x),\, b(x) \in F[x]\}.$$

Tenemos que I es un ideal de $F[x]$ y como F es un cuerpo, $F[x]$ es un DIP, es decir, I es principal. Tomamos un generador mónico de grado mínimo $I = (d(x))$. Notar que $d(x)$ es una combinación lineal de f y g. Notar también que d es un divisor común de f y g, pues $f, g \in (d) = I$. Por último, si c es un divisor común de f y g tenemos que $f = ch$ y $g = cq$ con $h, q \in F[x]$. Luego, $d = af + bg = a(ch) + b(cq) = c(ah + bq)$ y por lo tanto $c \mid d$. □

Definición 10. Decimos que un polinomio $f(x) \in F[x]$ tiene una **raíz repetida** en $x = a$, si $(x - a)^2$ divide a $f(x)$

Ejercicio 8. Sea $f(x) = \prod(x - a_i) \in F[x]$, donde F es un cuerpo. Mostrar que $f(x)$ no tiene raíces repetidas si y solo si $(f(x), f'(x)) = 1$, donde $f'(x)$ es la derivada formal de $f(x)$.

Corolario 8 (Lema de Euclides)**.** Sea F un cuerpo. Si $(f(x), g(x)) = 1$ y $f(x)$ divide a $g(x)h(x)$, entonces $f(x)$ divide a $h(x)$ en $F[x]$.

Demostración. Por el teorema anterior, existen $a(x)$ y $b(x)$ tal que $1 = af + bg$. Por lo tanto, $h = afh + bgh$, pero $gh = fk$ para algún polinomio k. Luego, como $h = f(ah + bk)$, f divide a h. □

La prueba del Lema de Euclides es simplemente una adaptación de la prueba para $\mathbb{Z}$. De la misma manera, existe una adaptación del *algoritmo de Euclides* para calcular el mcd de dos polinomios y expresarlo como una combinación lineal. A continuación lo demostramos.

Teorema 9 (Algoritmo de Euclides)**.** Existe un algoritmo para calcular el mcd de dos polinomios y expresarlo como una combinación lineal.

Demostración. La idea del algoritmo es repetir el algoritmo de la división varias veces.

Consideremos la siguiente lista de ecuaciones:

$$\begin{aligned}
f &= q_1 g + r_1 & \partial r_1 &< \partial g \\
g &= q_2 r_1 + r_2 & \partial r_2 &< \partial r_1 \\
r_1 &= q_3 r_2 + r_3 & \partial r_3 &< \partial r_2 \\
r_2 &= q_4 r_3 + r_4 & \partial r_4 &< \partial r_3 \\
&\vdots & &\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n & \partial r_n &< \partial r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + r_{n+1} & \partial r_{n+1} &< \partial r_n \\
r_n &= q_{n+2} r_{n+1}. &&
\end{aligned}$$

Vamos a ver que $d = r_{n+1}$ es el mcd (después de volverlo mónico). Primero, notemos que el algoritmo siempre termina eventualmente porque los grados de los restos es estrictamente decreciente (de hecho, la cantidad de iteraciones necesarias es a lo sumo ∂g). Luego, d es un divisor común, pues $d = r_{n+1}$ divide a r_n y de la $(n+1)-$ésima ecuación se obtiene que $r_{n-1} = q_{n+1} r_n + r_{n+1}$ lo que muestra que d divide a r_{n-1}. Usando este argumento recursivamente, podemos llegamos a que r_n divide a ambos f y g. Por otro lado, si c es un divisor común, empezando por la primera ecuación, vemos que c divide a r_1 y siguiendo con el resto de las ecuaciones llegamos a que también divide a d. Por último, se pueden encontrar a y b con otro argumento recursivo empezando por la última ecuación y siguiendo hacia arriba. Efectivamente, si $d = r_{n+1} = r_{n-1} - q_{n+1} r_n$ es una combinación lineal de r_{n-1} y r_n. Combinando esto con $r_n = r_{n-2} - q_n r_{n-1}$ obtenemos

$$\begin{aligned}
d &= r_{n-1} - q_{n+1}(r_{n-2} - q_n r_{n-1}) \\
&= (1 + q_n q_{n+1}) r_{n-1} - q_{n+1} r_{n-2}
\end{aligned}$$

una combinación lineal de r_{n-1} y r_{n-2}. Este proceso termina con $d = af + bg$.

□

Corolario 10. Sean $F \subset E$ cuerpos, y sean $g(x)$, $f(x) \in F[x] \subset E[x]$. Entonces el mcd de f y g en $F[x]$ es el mismo que en $E[x]$.

Demostración. Si vemos a f y g como elementos en $E[x]$ y usamos el algoritmo de Euclides para calcular su mcd en $E[x]$ vamos a ver que, como estamos iterando el algoritmo de la división en $F[x]$, el resultado será el mismo que si consideramos a f y g en $F[x]$. □

Consideremos $R = F[x]/I$ donde F es un cuerpo e I es ideal principal generado por un polinomio $p(x)$. Si $(f(x), p(x)) = 1$ entonces existen polinomios $s(x)$, $t(x) \in F[x]$ tal que:

$$s(x)f(x) + p(x)t(x) = 1.$$

En R esta ecuación se vuelve:

$$s(x)f(x) + I = 1 + I.$$

Luego, $f(x) + I$ es una unidad en R con inverso $s(x) + I$.

Definición 11. Un polinomio no nulo $p(x) \in F[x]$ se dice **irreducible** si $\partial p \geq 1$ y no existe ninguna factorización $p(x) = f(x)g(x)$ en $F[x]$ con $\partial f < \partial p$ y $\partial g < \partial p$.

Notar que la irreducibilidad depende del cuerpo F. Por ejemplo, $x^2 + 1$ es irreducible sobre $\mathbb{R}$ pero se factoriza en $\mathbb{C}$. Los polinomios lineales (de grado 1) siempre son irreducibles sobre cualquier cuerpo.

Mencionamos a continuación a modo de observación algunos hechos sobre la irreducibilidad en anillos de polinomios. No daremos la demostración, pero su prueba es análoga a sus respectivas versiones en $\mathbb{Z}$, donde los números primos cumplen en rol de los polinomios irreducibles.

Observación 2.

1. Sea $p(x) \in F[x]$ irreducible. Si $g(x) \in F[x]$ no es constante, entonces o bien $(p(x), g(x)) = 1$ o bien $p(x)$ divide a $g(x)$
2. Si $p(x)$ es irreducible y divide a un producto $q_1(x)q_2(x)\cdots q_s(x)$, entonces $p(x)$ divide a algún $q_j(x)$.
3. Todo polinomio en $f(x) \in F[x]$ admite una factorización de la forma:

$$f(x) = ap_1(x)\cdots p_t(x),$$

donde a es una constante no nula y los $p_i(x)$ son todos polinomios irreducibles no necesariamente distintos. Más aún, estos factores y sus multiplicidades están unívocamente determinados por $f(x)$.

Hay una conexión muy importante entre la factorización de un polinomio y sus raíces.

Teorema 11. Sea $f(x) \in F[x]$ y sea $a \in F$. Existe un $q(x) \in F[x]$ tal que

$$f(x) = q(x)(x - a) + f(a).$$

Demostración. Usamos el algoritmo de la división. Dividiendo $f(x)$ por $x - a$ obtenemos un cociente y un resto que debe ser constante (ya que $x - a$ tiene grado 1):

$$f(x) = q(x)(x - a) + r.$$

Evaluando esta igualdad en $x = a$ vemos que $r = f(a)$. □

Corolario 12. Sea $f(x) \in F[x]$. Entonces $a \in F$ es una raíz de $f(x)$ si y solo sí $x - a$ divide a $f(x)$.

Demostración. Si a es una raíz de $f(x)$ entonces $f(a) = 0$ y el teorema anterior produce $f(x) = q(x)(x - a)$. En cambio, si $f(x) = q(x)(x - a)$, evaluando en $x = a$ vemos que $f(a) = 0$. □

3.3. Ideales Primos e Ideales Maximales

Definición 12. Un ideal I de un anillo R se dice **primo** si $I \neq R$ y

$$ab \in R \implies a \in I \text{ ó } b \in I.$$

Si $p(x) \in F[x]$ es irreducible entonces $I = (p(x))$ es un ideal primo, pues $a(x)b(x) \in I$ implica que $p(x)$ divide a $a(x)b(x)$. Luego, como $p(x)$ es irreducible, divide o bien a $a(x)$ o a $b(x)$, por lo tanto, $a(x) \in I$ o $b(x) \in I$. Como $I \neq R$ ya que $\partial p \geq 1$, se sigue que I es un ideal primo.

Teorema 13. Un ideal $I \subset R$ con $I \neq R$ es primo si y solo si R/I es un dominio.

Demostración. Sea I un ideal primo. Supongamos que $a+I \neq 0$ y que $b+I \neq 0$ en R/I, es decir, ni a ni b pertenecen a I. Si $(a+I)(b+I) = ab+I = 0$, entonces $ab \in I$, lo que contradice que I sea primo. La vuelta es similar. □

Definición 13. Un ideal I de un anillo R es maximal si $I \neq R$ y no hay ningún ideal J de R tal que $I \subsetneq J \subsetneq R$.

Teorema 14. Un ideal $I \subset R$ con $I \neq R$ es maximal si y solo si R/I es un cuerpo.

Demostración. El Teorema de la Correspondencia dice que I es maximal si y solo si R/I no tiene ideales además de $\{0\}$ y R/I; y el Ejercicio 6 nos muestra que esto pasa cuando R/I es un cuerpo. □

Corolario 15. Todo ideal maximal es primo.

Demostración. Todo cuerpo es un dominio. □

La vuelta del último corolario es falsa en general. Por ejemplo, el ideal (x) en $\mathbb{Z}[x]$ es primo, pero no maximal porque $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ que es un dominio pero no un cuerpo.

Teorema 16. Si R es un DIP, entonces todo ideal primo no nulo es maximal.

Demostración. Asumamos que existe un ideal $J \neq I$ con $I \subset J \subset R$. Como R es un DIP, $I = (a)$ y $J = (b)$ para algún $a, b \in R$. Ahora bien, $a \in J$ implica que existe un $r \in R$ tal que $a = rb$, por lo tanto, $rb \in I$. Como I es primo o bien $r \in I$ o $b \in I$. Si $b \in I$ entonces $J \subset I$ lo que implica un absurdo. Si $r \in R$ entonces $r = sa$ para algún $s \in R$, y por lo tanto $a = rb = sab$; luego $1 = sb$ y $J = (b) = R$, por el Ejercicio 5. Entonces, I es maximal.

□

Corolario 17. Si F es un cuerpo y $p(x) \in F[x]$ es irreducible, entonces $F[x]/(p(x))$ es un cuerpo que contiene a (una copia isomorfa a) F y a una raíz de $p(x)$.

Demostración. Como $p(x)$ es irreducible, el ideal $I = (p(x))$ es un ideal primo no nulo y por lo tanto, como $F[x]$ es un DIP, es maximal. Luego $E = F[x]/I$ es un cuerpo. Es fácil ver que $a \mapsto a + I$ es un isomorfismo de F a $\{a + I : a \in F\} \subset E$ (por lo general se identifica a F con este conjunto). Sea $\alpha = x + I \in E$; veamos que α es una raíz de $p(x)$. Supongamos que $p(x) = a_0 + a_1x + \cdots + a_nx^n$ donde $a_i \in F$, entonces, en E:

$$\begin{aligned} p(\alpha) &= (a_0 + I) + (a_1 + I)\alpha + \cdots + (a_n + I)\alpha^n \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_n + I)(x + I)^n \\ &= (a_0 + I) + (a_1x + I) + \cdots + (a_nx^n + I) \\ &= a_0 + a_1x + \cdots + a_nx^n + I \\ &= p(x) + I = I \end{aligned}$$

que es el 0 de $F[x]/I$, luego α es una raíz de $p(x)$. □

Definición 14. In polinomio $f(x) \in F[x]$ se **descompone sobre** F si es un producto de factores lineales.

Es claro que $f(x)$ se descompone sobre F si y solo si F contiene a todas las raíces de $f(x)$.

Teorema 18 (Kronecker)**.** Sea $f(x) \in F[x]$ donde F es un cuerpo. Entonces existe un cuerpo E que contiene a F en donde $f(x)$ se descompone.

Demostración. La prueba es por inducción en ∂f. Si $\partial f = 1$, entonces $f(x)$ es lineal y tomamos $F = E$. Si $\partial f > 1$ escribimos $f(x) = p(x)g(x)$ donde $p(x)$ es irreducible. Si $p(x)$ es lineal, entonces $f(x)$ se descompone sobre cualquier cuerpo E sobre el cual $g(x)$ se descomponga; un tal cuerpo existe por hipótesis inductiva. Si $\partial p > 1$, entonces el corolario anterior nos garantiza que existe un cuerpo B que contiene a F y a una raíz α de $p(x)$. Luego, $p(x) = (x-\alpha)h(x)$ en $B[x]$. De nuevo, por hipótesis inductiva, existe un cuerpo E que contiene a B sobre el cual $h(x)g(x)$ se descompone y por ende, también lo hace $f(x)$. □

Definición 15. Definimos un **subanillo** de un anillo R como un subgrupo S de R que contiene al 1 y que es cerrado por la multiplicación.

Se puede ver fácilmente que la intersección de una familia de subanillos es de nuevo un subanillo.

Definición 16. Un **subcuerpo** es un subanillo que también es un cuerpo.

Se puede ver fácilmente también, que un subconjunto de un anillo es un subcuerpo si es un subgrupo que contiene al 1 y es cerrado por multiplicación e inversos. También es claro que la intersección de dos subcuerpos es de nuevo un subcuerpo.

Ejercicio 9. Mostrar que si F es un subcuerpo de E entonces E es un F-espacio vectorial.

3.4. Cuerpos de Descomposición

Usando la idea del ejercicio anterior damos la siguiente definición.

Definición 17. Si F es un subcuerpo de E decimos que E es una **extensión de cuerpos** de F y escribimos "E/F es una extensión de cuerpos". Llamamos el **grado** de la extensión F/E a la dimensión de F como un E-espacio vectorial y lo denotamos por $[E : F]$. Decimos que E/F es **finita** si $[E : F]$ es finito.

Esta definición invierte nuestro punto de vista. En vez de estudiar subcuerpos F de un cuerpo E, estudiaremos cuerpos más grandes E que contienen a F como un subcuerpo.

Teorema 19. Sea $p(x) \in F[x]$ un polinomio irreducible de grado d. Entonces $E = F[x]/(p(x))$ es una extensión de F de grado d.

Demostración. Denotamos por $I = (p(x))$, y denotamos por $\alpha = x + I$ en E. Basta probar que $\{1, \alpha, \alpha^2, \ldots, \alpha^d\}$ es una base de E sobre F. Supongamos que existen, para $0 \leq i \leq d-1$, $a_i \in F$ tal que $\sum a_i \alpha^i = 0$. Esto quiere decir que $f(x) = \sum a_i x^i \in I =$

$(p(x))$. Por lo tanto $p(x)$ divide a $f(x)$, pero notemos que $\partial f < d = \partial p$, lo que constituye un absurdo. Luego, $\{1, \alpha, \alpha^2, \ldots, \alpha^d\}$ es independiente. Por otro lado, todo elemento de E es de la forma $f(x) + I$ para algún $f(x) \in F[x]$. Usando el algoritmo de la división obtenemos $f(x) = q(x)p(x) + r(x)$, donde $\partial r < \partial p = d$ y $f(x) + I = r(x) + I$. Entonces, $\{1, \alpha, \alpha^2, \ldots, \alpha^d\}$ genera todo E. □

Definición 18. Sea E/F una extensión de cuerpos y sean $\alpha_1, \ldots, \alpha_n \in E$. Entonces $F(\alpha_1, \ldots, \alpha_n)$ es el menor subcuerpo de E que contiene a F y a $\alpha_1, \ldots, \alpha_n$ y lo llamamos "F **adjuntando** $\alpha_1, \ldots, \alpha_n$". Una extensión E/F es **simple** si existe $\alpha \in F$ tal que $E = F(\alpha)$.

Se puede probar que

$$F(\alpha) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in F[x] \text{ y } g(\alpha) \neq 0\}.$$

Definición 19. Sea E/F una extensión de cuerpos y sea $\alpha \in E$. Entonces α se dice **algebraico** sobre F si α es la raíz de un polinomio en $F[x]$. En caso contrario α se dice **trascendente** sobre F. Una extensión E/F se dice **algebraica** si todo elemento de E es algebraico sobre F.

Cuando uno dice que π o e son trascendentes en el sentido usual, en realidad se refiere a que son trascendentes sobre $\mathbb{Q}$. Si F es un cuerpo, denotamos por $F(x)$ al cuerpo de **funciones racionales** sobre F; es el cuerpo de fracciones del anillo $F[x]$ y sus elementos son de la forma $f(x)/g(x)$ donde $f(x), g(x) \in F[x]$.

Lema 20. Toda extensión E/F finita es algebraica.

Demostración. Sea E/F una extensión finita con $[E : F] = n$. Sea $\alpha \in E$. Consideramos la lista de $n + 1$ elementos $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$. Como E es un F-espacio vectorial de dimensión n, este conjunto tiene que ser linealmente dependiente. Es decir, tienen que existir coeficientes $a_i \in F$ para $0 \leq i \leq n$ tal que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = \sum_{i=0}^{n} a_i\alpha^i = 0$$

Por lo tanto, α es la raíz del polinomio $f(x) = \sum a_i x^i \in F[x]$

□

Observación 3. Si $\sigma, \tau : F(\alpha_1, \cdots, \alpha_n) \to E$ fijan a F puntualmente y $\sigma(\alpha_i) = \tau(\alpha_i)$ para todo i, entonces $\sigma = \tau$.

Teorema 21. Sea E/F una extensión de cuerpos, y sea $\alpha \in E$ algebraico sobre F.

(I) Existe un polinomio mónico irreducible $m_\alpha(x) \in F[x]$ que tiene a α como raíz.

(II) $m_\alpha(x)$ es el polinomio mónico de grado mínimo en $F[x]$ que tiene a α como raíz, y por ende es único.

(III) Existe un isomorfismo $F(\alpha) \cong F[x]/(m_\alpha(x))$ que deja fijo a F puntualmente.

(IV) $[F(\alpha) : F] = \partial m_\alpha$

Demostración. Elegimos como $m_\alpha(x)$ al polinomio mónico de grado mínimo que tiene a α como raíz (que existe porque α es algebraico). El morfismo evaluación $F[x] \to F(\alpha)$ que lleva $f(x) \mapsto f(\alpha)$ es suryectivo y tiene kernel $(m_\alpha(x))$. Por lo que el primer teorema de isomorfismo produce un isomorfismo $F(\alpha) \cong F[x]/(m_\alpha(x))$ que deja a fijo puntualmente a F. Como $F(\alpha)$ es un cuerpo, $(m_\alpha(x))$ es un ideal maximal y por ende también es primo. Por lo tanto, $m_\alpha(x)$ es irreducible. Por último, (IV) vale por el Teorema 19. □

Definición 20. El polinomio $m_\alpha(x)$ en el Teorema 21 se llama **polinomio minimal de α sobre F.**

Si α es algebraico sobre F, la descripción de $F(\alpha)$ como funciones racionales en α se simplifica a solo polinomios en α. En particular, el inverso multiplicativo de $f(x)$ es $a(x)$ donde $a(x)f(x) + b(x)m_\alpha(x) = 1$ y $m_\alpha(x)$ es el polinomio minimal de α.

Definición 21. Un **cuerpo de descomposición** de un $f(x) \in F[x]$ es una extensión de cuerpos E/F en la cual $f(x)$ se descompone como producto de factores lineales, pero no lo hace en ningún subcuerpo propio de E.

Ejemplo: si ω es una raíz cúbica de la unidad, entonces $x^3 - 1 \in \mathbb{Q}[x]$ se descompone sobre $\mathbb{C}$ pero su cuerpo de descomposición es $\mathbb{Q}(\omega)$.

Teorema 22. Todo polinomio $f(x) \in F[x]$ tiene un cuerpo de descomposición.

Demostración. Por el Teorema de Kronecker (Teorema 18), existe una extensión de cuerpos K/F sobre la cual $f(x)$ se descompone. Definimos $E = F(\alpha_1, \cdots, \alpha_n)$, donde $\alpha_1, \cdots, \alpha_n$ son las raíces de $f(x)$ en K. Es claro que $f(x)$ se descompone en E, pero no puede hacerlo sobre cualquier subcuerpo propio de E, pues en tal caso omitiría necesariamente a algún α_i. □

Lema 23. Si $F \subset B \subset E$ son extensiones de cuerpos con $[E : B]$ y $[B : F]$ finitos, entonces E/F es finita y

$$[E : F] = [E : B][B : F].$$

Demostración. Sean $\{\alpha_1, \ldots, \alpha_m\}$ una base de E/B y $\{\beta_1, \ldots, \beta_n\}$ una base de B/F. Basta probar que $\{\alpha_i\beta_j : 1 \leq i \leq m, 1 \leq j \leq n, \}$ es una base de E/F. Este conjunto genera, pues si $\gamma \in E$ existen $b_i \in B$ tal que $\gamma = \sum b_i\alpha_i$. Pero a su vez, cada $b_i = \sum c_{ij}\beta_j$, con $c_{ij} \in F$. Por lo tanto $\gamma = \sum c_{ij}\beta_j\alpha_i$. Para ver que es independiente, asumimos que $\sum c_{ij}\beta_j\alpha_i = 0$ para algunos $c_{ij} \in F$. Ahora, definimos $b_i = \sum c_{ij}\beta_j \in B$. Por la independencia lineal de los α_i sobre B tenemos que $b_i = 0$ para todo i. Luego, $\sum c_{ij}\beta_j = 0$ para todo i, por lo que la independencia lineal de los β_j sobre F implica que $c_{ij} = 0$ para todo i, j.

□

Definición 22. Sea $f(x) \in F[x]$ un polinomio cuya factorización en irreducibles es:

$$f(x) = ap_1(x) \cdots p_t(x);$$

entonces $f(x)$ se dice **separable** si ningún $p_i(x)$ tiene raíces repetidas

Sea F un cuerpo y sea $q(x) \in F[x]$ un polinomio irreducible. Si su derivada $q'(x)$ no es el polinomio nulo, entonces su grado tiene que ser menor al de $q(x)$. Por lo tanto $(q', q) = 1$ (por la Observación 2) y $q(x)$ es separable (por el Ejercicio 8). Se sigue entonces que si F tiene característica 0 entonces todo polinomio es separable. Si F tuviese característica p podría pasar que $q' = 0$. Los cuerpos en los que todo polinomio no constante es separable se dicen **perfectos.** Si E/F es una extensión entonces $\alpha \in E$ se dice **separable** si su polinomio minimal es separable. Una extensión se dice **separable** si todos sus elementos son separables.

Teorema 24. Sea $\sigma : F \to F'$ un isomorfismo de cuerpos, sea $\sigma^* : F[x] \to F'[x]$ (definido por $\sum r_i x^i \mapsto \sum \sigma(r_i)x^i$) el correspondiente isomorfismo de anillos, sea E el cuerpo de descomposición de un $f(x)$ y E' el cuerpo de descomposición de $f^*(x) = \sigma^*(f(x))$.

$$\begin{array}{ccc} E & \xrightarrow{\tilde{\sigma}} & E' \\ \vdots & & \vdots \\ F & \xrightarrow[\sigma]{} & F' \end{array}$$

(I) Existe un isomorfismo $\tilde{\sigma} : E \to E'$ que extiende a σ.

(II) Si $f(x)$ es separable, entonces hay exactamente $[E : F]$ de estas extensiones $\tilde{\sigma}$ de σ

Esquema de prueba. (I) La prueba es por inducción en $[E : F]$. Si $[E : F] = 1$ entonces $E = F$ y $f(x)$ es un producto de factores lineales en $F[x]$, por lo que $f^*(x)$ también tiene que ser un producto de factores lineales y por ende $F' = E'$. Entonces, podemos definir $\tilde{\sigma} = \sigma$. Si $[E : F] > 1$, tomamos un factor irreducible $p(x)$ de $f(x)$ que tenga grado ≥ 2, y tomamos β una raíz de $p(x)$, que tendrá que ser también una raíz de $f(x)$ por lo que $\beta \in E$. Sea $p^*(x) \in F'[x]$ el polinomio correspondiente a $p(x)$, y sea $\beta' \in E'$ una raíz de $p^*(x)$. Se puede probar que para cada tal β' existe un único isomorfismo $\hat{\sigma} : F(\beta) \to F'(\beta')$ con $\hat{\sigma}(\beta) = \beta'$ que extiende σ. Notemos ahora que E un cuerpo de descomposición de $f(x)$ sobre $F(\beta)$ y que E' es un cuerpo de descomposición de $f^*(x)$ sobre $F'(\beta')$. Como $[E : F] = [E : F(\beta)][F(\beta) : F]$, y como $[F(\beta) : F] \geq 2$ se sigue que $[E : F(\beta)] < [E : F]$, por lo que, por hipótesis inductiva, existe un $\tilde{\sigma} : E \to E'$ que extiende a $\hat{\sigma}$ y por lo tanto, también extiende a σ.

(II) Modificamos ligeramente la prueba de (I), procediendo nuevamente por inducción en $[E : F]$. Si $[E : F] > 1$, sea $f(x) = p(x)g(x)$ donde $p(x)$ es irreducible de grado d. Podemos asumir que $d > 1$ pues si $d = 1$ podemos intercambiar $f(x)$ por $g(x)$ y replantear el problema. Ahora, elegimos β raíz de $p(x)$. Si $\tilde{\sigma}$ es una extensión de σ a E entonces $\sigma(\beta)$ es una raíz β' de $p^*(x)$; como $f^*(x)$ es separable, $p^*(x)$ tiene exactamente d raíces $\beta' \in E'$. De manera similar a (I), se puede probar que por cada una de estas raíces existe un único isomorfismo $\hat{\sigma} : F(\beta) \to F'(\beta')$. De nuevo, notemos que E es un cuerpo de descomposición de $f(x)$ sobre $F(\beta)$ y que E' es un cuerpo de descomposición de $f^*(x)$ sobre $F'(\beta')$. Como $[E : F(\beta)] = [E : F]/d$ la inducción arroja que cada uno de los d isomorfismos $\hat{\sigma}$ tiene exactamente $[E : F]/d$ extensiones a E. Concluimos así que σ tiene exactamente $[E : F]$ extensiones $\tilde{\sigma}$, porque cada τ que extiende a σ cumple que $\tau|_{F(\beta)} = \hat{\sigma}$ para algún $\hat{\sigma}$.

□

Corolario 25. Si $f(x) \in F[x]$, entonces dos cuerpos de descomposición de $f(x)$ son isomorfos.

Demostración. Elegimos $F = F'$ y σ la identidad de F. □

3.5. Solubilidad por Radicales y El Grupo de Galois

Comenzamos ahora a construir las definiciones que nos permitirán dar una respuesta a nuestro problema.

Definición 23. Una extensión de cuerpos B/F es una **extensión pura** si $B = F(\alpha)$ donde α es tal que $\alpha^m \in F$ para algún $m \in \mathbb{N}$.

Definición 24. Sea F un cuerpo y sea $f(x) \in F[x]$; entonces $f(x)$ es **soluble por radicales** sobre F si existe una torre de cuerpos[1]:

$$F = B_0 \subset B_1 \subset \cdots B_t,$$

donde cada B_{i+1}/B_i es una extensión pura y B_t contiene al cuerpo de descomposición E de $f(x)$ sobre F. La extensión B_t/F se llama **extensión radical.**

Hacemos un par de observaciones sin demostración. El lector entusiasta encontrará entretenidas sus demostraciones.

Observación 4. Esta torre de cuerpos siempre se puede refinar hasta llegar a una en donde $[B_{i+1} : B_i]$ sea un número primo para todo i.

Observación 5. Sea B/F una extensión finita. Se puede probar que existe una extensión E/B tal que E/F es el cuerpo de descomposición de un polinomio $f(x) \in F[x]$. La menor tal extensión se llama **clausura normal** de B/F.

Si E/F es una extensión y B y C son subcuerpos intermedios ($F \subset B \subset E$ y $F \subset C \subset E$) entonces el cuerpo $B \vee C$ es la intersección de todos los subcuerpos de E que contienen a B y a C. Se puede ver que si E/F es la clausura normal de B/F entonces $E = B_1 \vee B_2 \vee \cdots \vee B_t$, donde cada B_i es isomorfo a B mediante un isomorfismo que deja fijo a F puntualmente.

Usando esta idea, se puede probar que la clausura normal de una extensión radical es también una extensión radical. Por lo tanto, en la definición de solubilidad por radicales, podemos asumir que B_t es el cuerpo de descomposición de algún polinomio sobre F.

Esta idea es esencialmente el resultado teórico de la búsqueda de fórmulas resolventes. Después de los esfuerzos de Bhaskara, Tartaglia, Cardano, Ferrari y compañía. Se sospechaba que las cuatro operaciones permitidas en un cuerpo (suma, resta, producto y división) más la extracción de radicales serían operaciones suficientes para dar una fórmula para las raíces de un polinomio en términos de sus coeficientes. La extracción de radicales de un α en el contexto de un cuerpo E, refiere a la existencia de un $\beta \in E$ tal que, $\beta^n = \alpha$. Dicho esto, basta convencerse de que la existencia de una tal fórmula es equivalente a la existencia de una extensión radical.

[1]Este ha de ser el único contexto en el que la expresión *"torre de cuerpos"* puede pasar desapercibida sin levantar sospechas de asesinatos en serie. Recomendamos discreción al discutir estos temas en presencia de personas ajenas al ámbito matemático.

Una buena manera de ilustrar esta definición es corroborar que los polinomios cuadráticos son siempre solubles por radicales sobre $\mathbb{Q}$. Si $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$, definimos $d = \sqrt{b^2 - 4ac}$, así, $d \notin \mathbb{Q}$ pero $d^2 \in \mathbb{Q}$. Entonces si $B = \mathbb{Q}(d)$, $B/\mathbb{Q}$ es una extensión pura y claramente B es el cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$, pues ambas raíces de $f(x)$ se pueden escribir como sumas, restas, productos y divisiones en este cuerpo. Por lo tanto, $f(x)$ es soluble por radicales.

Sin embargo, aún no hemos resuelto nada. Solo reescribimos el problema en términos más sofisticados. Nuestro objetivo ahora es encontrar condiciones necesarias y suficientes bajo las cuales un polinomio es soluble por radicales.

Comenzamos por el siguiente lema que a pesar de tener una prueba simple es fundamental y tiene implicaciones muy profundas.

Lema 26. Sea $f(x) \in F[x]$ y sea E/F el cuerpo de descomposición de $f(x)$ sobre F. Si $\sigma : E \to E$ es un automorfismo (un isomorfismo de E en sí mismo) que deja fijo a F puntualmente, y si α es una raíz de $f(x)$ entonces $\sigma(\alpha)$ también es una raíz de $f(x)$.

Demostración. Sea $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. De esta manera, $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Aplicando σ tenemos que

$$\sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \cdots + \sigma(a_n)\sigma(\alpha)^n = a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha)^n = 0,$$

pues σ fija a F. Luego $\sigma(\alpha)$ también es una raíz de $f(x)$. □

Definición 25. Sea E/F una extensión de cuerpos. Su **Grupo de Galois**, al que denotaremos por $\mathrm{Gal}(E/F)$, es el conjunto de todos los automorfismos de E que dejan fijo a cada elemento de F. Este conjunto tiene una estructura de grupo bajo la operación de componer automorfismos.

Este objeto es el que esconde nuestro tesoro. Si bien esta definición así como fue presentada no es de Galois, es equivalente a su idea. Estudiemos un poco más las propiedades de este concepto.

Teorema 27. Si $f(x) \in F[x]$ tiene n raíces distintas en su cuerpo de descomposición E entonces $\mathrm{Gal}(E/F)$ es isomorfo a un subgrupo del grupo simétrico $\mathbb{S}_n$.

Demostración. Sea $X = \{\alpha_1, \ldots, \alpha_n\}$ el conjunto de raíces de $f(x)$ en E. Por el Lema 26 Si $\sigma \in \mathrm{Gal}(E/F)$, entonces $\sigma(X) = X$. El mapa $\mathrm{Gal}(E/F) \to \mathbb{S}_X$ definido por $\sigma \mapsto \sigma|_X$ es un morfismo de grupos y es inyectivo por la Observación 3. Por último, $\mathbb{S}_X \cong \mathbb{S}_n$. □

De esta manera, por ejemplo, el grupo de Galois de un polinomio de grado 4 es siempre un subgrupo de $\mathbb{S}_4$ y el de un polinomio de grado 5 es siempre un subgrupo de $\mathbb{S}_5$.

Teorema 28. Si $f(x) \in F[x]$ es un polinomio separable y E/F es su cuerpo de descomposición entonces $|\mathrm{Gal}(E/F)| = [E : F]$.

Demostración. Por el Teorema 24 (II) con $F = F'$ y $E = E'$, tomando σ la identidad en F, existen exactamente $[E : F]$ automorfismos de E que dejan fijo a F. □

Veamos un par de ejemplos:

1. El cuerpo de descomposición de x^2+1 sobre $\mathbb{R}$ es claramente $\mathbb{C}$ y $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| \leq 2$ por el Teorema 27. De hecho, $|\mathrm{Gal}(\mathbb{R}/\mathbb{C})| = 2$, pues este grupo contiene al automorfismo:
$$\sigma : z = a + bi \mapsto \overline{z} = a - bi.$$
Notar como $\sigma : i \mapsto -i$ y $-i \mapsto i$, está intercambiando las raíces. En cierta manera, los elementos del grupo de Galois generalizan la noción de conjugación compleja.

2. Sea $f(x) = x^3 - 1 \in \mathbb{Q}[x]$; $f(x)$ es separable, porque $\mathbb{Q}$ tiene característica 0. Ahora, $f(x) = (x-1)(x^2+x+1)$ es una factorización de $f(x)$ en irreducibles. Si E es el cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$, entonces $E = \mathbb{Q}(\omega)$ donde ω es una raíz cúbica primitiva de la unidad, es decir, una raíz de x^2+x+1. Como $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 2$, por el Teorema 28 por lo que de nuevo el grupo de Galois es cíclico de orden 2.

3. Sea $g(x) = x^3 - 2 \in \mathbb{Q}[x]$. El cuerpo de descomposición de $g(x)$ es $\mathbb{Q}(\alpha, \omega)$ donde α es la raíz cúbica real de 2 y ω es una raíz cúbica compleja de la unidad. Como $g(x)$ es irreducible sobre $\mathbb{Q}$, se tiene $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Pero como $\mathbb{Q}(\alpha)$ consiste solo de números reales no puede ser el cuerpo de descomposición E de $g(x)$. Por lo tanto:
$$|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 3[E : \mathbb{Q}(\alpha)] > 3;$$
y como el grupo de Galois debe ser un subgrupo de $\mathbb{S}_3$, la única posibilidad es que sea $\mathrm{Gal}(E/\mathbb{Q}) = \mathbb{S}_3$.

Lema 29. Sea $F \subset B \subset E$ una torre de cuerpos donde B/F es el cuerpo de descomposición de algún polinomio $f(x) \in F[x]$. Si $\sigma \in \mathrm{Gal}(E/F)$, entonces $\sigma|_B \in \mathrm{Gal}(B/F)$.

Demostración. Basta probar que $\sigma(B) = B$. Si $\alpha_1, \cdots, \alpha_n$ son las raíces de $f(x)$, entonces $B = F(\alpha_1, \cdots, \alpha_n)$. Tenemos que $\sigma(F) = F$, y que $\sigma(\alpha_i) \in B$ para todo i, por lo que se sigue de la Observación 3 que $\sigma(B) = B$. □

Teorema 30. Sea $F \subset B \subset E$ una torre de cuerpos donde B/F es el cuerpo de descomposición de algún polinomio $f(x) \in F[x]$ y E/F es el cuerpo de descomposición de algún polinomio $g(x) \in F[x]$. Entonces $\mathrm{Gal}(E/B)$ es un subgrupo normal de $\mathrm{Gal}(E/F)$ y:
$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/F)$$
.

Demostración. Definimos $\psi : \mathrm{Gal}(E/F) \to \mathrm{Gal}(F/B)$ mediante $\sigma \mapsto \sigma|_B$. Por el Lema 29, ψ efectivamente toma valores en $\mathrm{Gal}(F/B)$. Es fácil ver que ψ es un morfismo de grupos y que su kernel es $\mathrm{Gal}(E/B)$, lo que nos dice que este último es un subgrupo normal. Por último, si $\tau \in \mathrm{Gal}(B/F)$, entonces el Teorema 24 muestra que hay un automorfismo $\tilde{\tau}$ de E con $\psi(\tilde{\tau}) = \tilde{\tau}|_B = \tau$. Por lo que ψ es suryectiva. Entonces, el resultado se sigue por el primer Teorema de Isomorfismo para grupos. □

Un comentario importante es que la hipótesis de que E/F sea un cuerpo de descomposición se usó solo para probar que ψ es suryectiva. Sin esta hipótesis uno solo podría probar que el cociente es isomorfo a un subgrupo de $\mathrm{Gal}(B/F)$.

Teorema 31. Sea F un subcuerpo de $\mathbb{C}$ que contiene a una raíz n-ésima primitiva de la unidad y sea $f(x) = x^n - c \in F[x]$. Si E/F es un cuerpo de descomposición de $f(x)$, entonces hay una inyección

$$\phi : G = \mathrm{Gal}(E/F) \to \mathbb{Z}_n.$$

Más aún, $f(x)$ es irreducible si y solo si ϕ es suryectiva.

Demostración. Si ω es una raíz n-ésima primitiva de la unidad y si α es una raíz de $f(x)$, entonces $\alpha^n = c$ y la lista completa de las raíces de $f(x)$ es $\alpha, \alpha\omega, , \cdots, \alpha\omega^{n-1}$. Si $\sigma \in G$ entonces $\sigma(\alpha) = \alpha\omega^i$, y σ está completamente determinado por i. Así que definimos $\phi(\sigma) = [i]$ si $\sigma(\alpha) = \alpha\omega^i$. Veamos que $\phi : G \to \mathbb{Z}_n$ es un morfismo de grupos. Si $\tau \in G$ entonces $\tau(\omega) = \omega$ (porque $\omega \in F$) y $\tau(\alpha) = \alpha\omega^j$ para algún j. Luego:

$$\begin{aligned} \tau\sigma : \alpha \mapsto \alpha\omega^i &\mapsto \tau(\alpha\omega^i) \\ &= \tau(\alpha)\tau(\omega^i) \\ &= (\alpha\omega^j)\omega^i \\ &= \alpha\omega^{j+i}, \end{aligned}$$

de manera que $\phi(\tau\sigma) = [j+i] = \phi(\tau) + \phi(\sigma)$. Por lo tanto ϕ es morfismo de grupos, que resulta inyectivo por la Observación 3. Dejamos como ejercicio ver que ϕ es suryectiva. □

Lema 32. Sea p un primo y F un subcuerpo de $\mathbb{C}$ que contenga a una raíz p-ésima primitiva de la unidad. Sea E/F el cuerpo de descomposición de $f(x) = x^p - c \in F[x]$. Entonces $f(x)$ se descompone sobre F y $\mathrm{Gal}(E/F) = \{e\}$ o $f(x)$ es irreducible y $\mathrm{Gal}(E/F) \cong \mathbb{Z}_p$.

Demostración. Consideremos ϕ el mapa definido en el teorema anterior. Si $f(x)$ se descompone sobre F entonces $E = F$ y $\mathrm{Gal}(E/F) = \{e\}$ y por lo tanto su imagen es trivial. Si $f(x)$ no se descompone entonces su imagen es un subgrupo no trivial del $\mathbb{Z}_p$, pero $\mathbb{Z}_p$ no tiene subgrupos propios no triviales, por lo que el mapa tiene que ser suryectivo, $\mathrm{Gal}(E/F) \cong \mathbb{Z}_p$ y $f(x)$ irreducible. □

3.6. Grupos Solubles

Interrumpimos nuestra historia brevemente para presentar un concepto de la teoría de grupos: los grupos solubles. Usaremos la notación $H < G$ para referirnos a "H es un subgrupo de G".

Definición 26. Sea G un grupo. El subgrupo de G generado por el conjunto $\{aba^{-1}b^{-1} | a, b \in G\}$ se llama el **subgrupo conmutador** de G y se denota G' (algunos autores usan también $[G, G]$).

Los elementos $aba^{-1}b^{-1}$ con $a, b \in G$ se llaman conmutadores. Estos elementos simplemente *generan* a G'; es decir, G' bien podría contener elementos que no sean conmutadores.

Una observación simple sobre esta definición es que G es abeliano si y solo si $G' = \{e\}$. De alguna manera, G' mide qué tan lejos está G de ser abeliano.

Teorema 33. Si G es un grupo, entonces G' es un grupo normal de G y G/G' es abeliano. Además, si N es otro subgrupo normal de G, entonces G/N es abeliano si y solo si N contiene a G'.

Demostración. Sea $f : G \to G$ cualquier automorfismo. Entonces:

$$f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} \in G'.$$

Se sigue que $f(G') < G'$ ($<$ refiere a es un subgrupo de). En particular, si f es conjugar por un $a \in G$ entonces $aG'a = f(G') < G'$, luego G' es normal en G. Como $(ab)(ab)^{-1} = aba^{-1}b^{-1} \in G$, tenemos que $abG = baG$ por lo que G/G' es abeliano. Por último si G/N es abeliano, entonces $abN = baN$ para todo $a, b \in G$ por lo que $(ab)(ba)^{-1} = aba^{-1}b^{-1} \in N$. Por lo tanto $G' < N$. Por otro lado, si $G' < N$, se tiene que G/N es abeliano por un argumento análogo al usado para ver que G/G' es abeliano. □

Si G es un grupo entonces llamemos $G^{(1)}$ a G'. Luego para $i \geq 1$, definimos $G^{(i)}$ recursivamente, mediante $G^{(i)} := (G^{(i-1)})'$. $G^{(i)}$ se llama el **i-ésimo subgrupo derivado** de G. Esto produce una sucesión de subgrupos de G, cada uno normal en el anterior:

$$G > G^{(1)} > G^{(2)} > \cdots .$$

De hecho, cada $G^{(i)}$ es un subgrupo normal de G.

Definición 27. Un grupo G se dice **soluble** si $G^{(n)} = \{e\}$ para algún n.

Todo grupo abeliano es trivialmente soluble.

Teorema 34. (I) Todo subgrupo y toda imagen por un morfismo de un grupo soluble es soluble

(II) Si N es un subgrupo normal de un grupo G tal que N y G/N son solubles entonces G es soluble

Esquema de prueba. (I) Si $f : G \to H$ es un morfismo de grupos y supongamos que es suryectivo (pues siempre lo es sobre su imagen). Se verifica que $f(G^{(i)}) = H^{(i)}$ para todo i. Entonces, como G es soluble, para algún n, se tiene que

$$\{e\} = f(\{e\}) = f((G^{(n)}) = H^{(n)}.$$

Luego H es soluble. La prueba para un subgrupo es similar.

(II) Sea $f : G \to G/N$ la proyección canónica. Como G/N es soluble, para algún n, vale que $f((G^{(n)}) = (G/N)^{(n)} = \{e\}$. Luego, $G^{(n)} < \ker f = N$. Entonces, por (I), $G^{(n)}$ es soluble. Es decir, existe un k tal que $(G^{(n)})^{(k)} = G^{(n+k)} = \{e\}$. Por lo tanto, G es soluble.

□

Definición 28. Una **serie normal** de un grupo G es una cadena de subgrupos $G = G_0 > G_1 > \cdots > G_n$ tal que cada G_i es normal en G y además G_{i+1} es normal en G_i para cada i. Los **factores** de una serie son los grupos G_i/G_{i+1}.

Ejemplo: Dado un grupo finito G, la serie de los i-ésimos subgrupos derivados forman una serie normal.

Definición 29. Una serie normal se dice **serie soluble** si es $G = G_0 > G_1 > \cdots > G_n = \{e\}$ y además cada factor es abeliano.

Teorema 35. Un grupo G es soluble si y solo si tiene una serie soluble.

Demostración. Si G es soluble, entones la serie de los i-ésimos subgrupos derivados forman una serie soluble por el Teorema 33. Por otro lado, si $G = G_0 > G_1 > \cdots > G_n = \{e\}$ es una serie soluble de G entonces el hecho de que $G/G_1 = G_0/G_1$ sea abeliano implica que $G_1 > G^{(1)}$ por el Teorema 33. Como G_1/G_2 es abeliano, $G_2 > G_1' > G^{(2)}$. Procediendo por inducción se concluye que $G_i > G^{(i)}$, para todo i; en particular $\{e\} = G_n > G^{(n)}$ y por ende, G es soluble. □

Teorema 36. Si $n \geq 5$, entonces $\mathbb{S}_n$ no es soluble.

Demostración. Si $\mathbb{S}_n$ fuera soluble, entonces $\mathbb{A}_n$ (el subgrupo alternante en n letras) también sería soluble. Un resultado muy importante de la teoría de grupos es que $\mathbb{A}_n$, para $n \geq 5$, es un grupo simple (no tiene subgrupos normales propios). Por lo tanto, como $\mathbb{A}_n'$ es normal, debemos tener que $\mathbb{A}_n' = \mathbb{A}_n$. Por lo tanto, $\mathbb{A}_n^{(i)} = \mathbb{A}_n \neq \{e\}$ para todo $i \geq 1$. Por lo tanto, $\mathbb{A}_n$ no puede ser soluble y consiguientemente, $\mathbb{S}_n$ tampoco. □

3.7. Insolubilidad de la Quíntica

Contando ahora con la definición de grupo soluble, demostramos el siguiente teorema, que será el primer paso para atar los cabos sueltos. El lector podrá reclamar justificadamente que no se ha definido apropiadamente la noción de raíz primitiva de la unidad en un cuerpo arbitrario F. Por lo que, a fines prácticos, en la discusión que sigue, F es un subcuerpo del cuerpo de números complejos (por lo tanto tiene característica 0) y la noción de raíz primitiva de la unidad es la usual. Sin embargo, esta noción se puede generalizar a un contexto más general que no trataremos en este texto.

Teorema 37. Si F es un cuerpo y $E = F(\alpha)$, donde α es una raíz primitiva de la unidad, entonces $\mathrm{Gal}(E/F)$ es abeliano.

Demostración. Notemos que E es el cuerpo de descomposición de $x^n - 1$, pues α es una raíz primitiva de la unidad. Tenemos entonces que $\sigma(\alpha) = \alpha^i$ para todo $\sigma \in \mathrm{Gal}(E/F)$. Más aún, como $\sigma|_{\langle\alpha\rangle}$ es un automorfismo de $\langle\alpha\rangle$, $\sigma(\alpha) = \alpha^i$ tiene que ser un generador de $\langle\alpha\rangle$. Por lo tanto, se tiene que $(i, n) = 1$. Definimos $\psi : \mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ (el grupo de unidades de $\mathbb{Z}/n\mathbb{Z}$) mediante $\sigma \mapsto \bar{i}$, donde $\sigma(\alpha) = \alpha^i$. Es sencillo corroborar que ψ es un morfismo de grupos y que es inyectivo usando la Observación 3. Por lo tanto, $\mathrm{Gal}(E/F)$ es isomorfo a un subgrupo de un grupo abeliano y por lo tanto es abeliano. □

Hemos llegado a los enunciados fundamentales, de los que obtendremos una condición necesaria para que un polinomio sea soluble por radicales.

Lema 38. Sea F un subcuerpo de $\mathbb{C}$. Sea $f(x) \in F[x]$ un polinomio soluble por radicales y sea E el cuerpo de descomposición de $f(x)$ sobre F.

(I) Existe una torre de extensiones radicales

$$F = R_0 \subset R_1 \cdots \subset R_t$$

con $E \subset R_t$, donde R_t es el cuerpo de descomposición de algún polinomio sobre F y donde cada R_i/R_{i-1} es una extensión pura de grado p_i primo.

(II) Si R_t/F es una extensión radical como en (I) y F contiene todas las raíces p_i-ésimas de la unidad para todo i, entonces $\mathrm{Gal}(E/F)$ es un grupo soluble.

Demostración. (I) Como $f(x)$ es soluble por radicales existe una torre de cuerpos

$$F = B_0 \subset B_1 \cdots \subset B_l$$

con $E \subset B_l$. Por la Observación 5 existe una extensión K/B_l que es el cuerpo de descomposición de algún polinomio en $F[x]$ tal que K/F también es radical. Tenemos entonces que $E \subset B_l \subset K$. Por la Observación 4 podemos refinar esta torre hasta que cada extensión sea de grado primo.

(II) Sea

$$F = R_0 \subset R_1 \cdots \subset R_t$$

con $E \subset R_t$, como en (I). Definimos

$$G_i = \mathrm{Gal}(R_t/R_i).$$

Por hipótesis F contiene todas las raíces p_i-ésimas de la unidad, de manera que cada R_i es un cuerpo de descomposición sobre R_{i-1}. Luego, las hipótesis del Teorema 30 valen y

$$\mathrm{Gal}(R_t/F) = G_0 > G_1 > G_1 > \cdots > G_t = \{e\}$$

es una serie normal. Los factores $\mathrm{Gal}(R_t/R_{i-1})/\mathrm{Gal}(R_t/R_i)$ de esta serie son isomorfos a $\mathrm{Gal}(R_i/R_{i-1})$, por el Teorema 30 y estos grupos tienen que ser cíclicos de orden primo por el Lema 32. Luego, la serie de arriba es una serie soluble y, por el Teorema 35, $\mathrm{Gal}(R_t/F)$ es soluble. Finalmente, aplicando el Teorema 30 a $F \subset E \subset R_t$, se tiene que $\mathrm{Gal}(E/F)$ es un cociente del grupo soluble $\mathrm{Gal}(R_t/F)$ y por lo tanto es también soluble.

□

Ahora, removemos la hipótesis de que F contenga las mencionadas raíces de la unidad.

Teorema 39. Sea $f(x) \in F[x]$ un polinomio soluble por radicales sobre un subcuerpo F de $\mathbb{C}$ y sea E/F su cuerpo de descomposición. Entonces $\mathrm{Gal}(E/F)$ es un grupo soluble.

Demostración. Por hipótesis existe una torre radical

$$F = R_0 \subset R_1 \cdots \subset R_t,$$

con $E \subset R_t$. Por el Lema 38(I), podemos asumir que R_i/R_{i-1} es una extensión pura de grado p_i primo y que R_t es el cuerpo de descomposición de algún polinomio $h(x) \in F[x]$. Sea m el mínimo común múltiplo de todos los p_i's, y sea ω una raíz m-ésima primitiva de la unidad. Podemos estirar la torre agregando $R_t \subset R' = R_t(\omega)$, y luego refinarla

hasta que cada extensión sea pura de grado primo. Observemos que $(x^m-1)h(x) \in F[x]$. Construimos una nueva torre:

$$F = R_0 \subset F(\omega) \subset R_1(\omega) \subset \cdots \subset R_t(\omega) = R'.$$

Notemos que cada extensión en esta torre es pura y que $E \subset R'$. Como $F(\omega)/F$ es un cuerpo de descomposición, el Teorema 30 nos dice que $\mathrm{Gal}(R'/F(\omega)) \trianglelefteq \mathrm{Gal}(R'/F)$ y

$$\mathrm{Gal}(R'/F)/\mathrm{Gal}(R'/F(\omega)) \cong \mathrm{Gal}(F(\omega)/F).$$

Ahora, $\mathrm{Gal}(F(\omega)/F)$ es abeliano por el Teorema 37, y por lo tanto es soluble. Cada extensión en la torre truncada

$$F(\omega) \subset R_1(\omega) \subset \cdots \subset R_t(\omega) = R'$$

es pura de grado primo, por lo que el Lema 38(II), que vale porque $F(\omega)$ contiene todas las raíces de la unidad necesarias, nos dice que el subgrupo normal $\mathrm{Gal}(R'/F(\omega))$ de $\mathrm{Gal}(R'/F)$ es soluble. Por lo que $\mathrm{Gal}(R'/F)$ es soluble. Finalmente el Teorema 30 nos garantiza que $\mathrm{Gal}(E/F)$ es un cociente de $\mathrm{Gal}(R'/F)$ y por tanto, es también soluble. □

De hecho, este resultado es la razón por la que los *grupos solubles* llevan ese nombre, porque caracterizan a los polinomio solubles por radicales. Ahora que tenemos una condición necesaria nos preguntamos si podremos encontrar algún polinomio que no sea soluble por radicales. Lo mismo se preguntaron dos matemáticos que mencionamos al comienzo: Abel y Ruffini. Por eso lleva ese nombre el siguiente resultado.

Teorema 40 (Abel-Ruffini)**.** Existe un polinomio de grado 5 $f(x) \in \mathbb{Q}[x]$ que no es soluble por radicales.

Demostración. Si $f(x) = x^5 - 4x + 2$, entonces no es difícil ver que $f(x)$ es irreducible sobre $\mathbb{Q}$. Sea $E/\mathbb{Q}$ el cuerpo de descomposición de $f(x)$ contenido en $\mathbb{C}$, y sea $G = \mathrm{Gal}(E/\mathbb{Q})$. Si α es una raíz de $f(x)$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, y por lo tanto

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 5[E : \mathbb{Q}(\alpha)].$$

Por el Teorema 28, $|G| = [E : \mathbb{Q}]$ es divisible por 5. Usando un poco de análisis, vemos que $f(x)$ tiene exactamente dos puntos críticos en $\pm\sqrt[4]{4/5}$, con $f(\sqrt[4]{4/5}) < 0$ y $f(-\sqrt[4]{4/5}) > 0$. Se sigue fácilmente que $f(x)$ tiene tres raíces reales y dos raíces complejas que son conjugadas entre ellas. Si pensamos ahora a G como un grupo de permutaciones de las raíces de $f(x)$, sabemos que G tiene que ser un subgrupo de $\mathbb{S}_5$. Como 5 divide a $|G|$, por el teorema de Cauchy, existe un elemento de orden 5 y los únicos elementos en $\mathbb{S}_5$ de orden 5 son los 5-ciclos, por lo que sabemos que G contiene un 5-ciclo. Además, la restricción de la conjugación compleja, digámosle σ, es una transposición, pues σ intercambia las dos raíces complejas mientras que deja fijas las tres raíces reales. Es un resultado conocido de la teoría de grupos que una transposición y un 5-ciclo generan todo $\mathbb{S}_5$, por lo que debemos tener que

$$G = \mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{S}_5$$

que no es un grupo soluble por el Teorema 36.

□

Este teorema nos acaba de convencer, usando solo un polinomio, que no puede haber una fórmula general para resolver las ecuaciones polinómicas de grado 5 sobre $\mathbb{Q}$ como las que sí hay para grados menores que 5, pues, de haber una, debería funcionar para este polinomio. Pero este polinomio *no es soluble por radicales*, por lo que no se pueden escribir sus soluciones en términos de sus coeficientes usando las operaciones de cuerpos y la extracción de radicales.

Una pregunta natural que se puede plantear ahora es ¿qué hay de las ecuaciones polinómicas sobre $\mathbb{Q}$ de grado mayor a 5? Teniendo en cuenta lo que terminó sucediendo para las de grado 5 y el hecho de que el Teorema 36 nos dice que *todos* los grupos simétricos en n letras $\mathbb{S}_n$ para $n \geq 5$ no son solubles, tenemos razones para creer que no va haber una fórmula resolvente general para las ecuaciones de grado ≥ 5. Pues, basta que exista tan solo un polinomio en $\mathbb{Q}[x]$ de grado n cuyo grupo de Galois sea $\mathbb{S}_n$ para $n \geq 5$ (Como hicimos para $n = 5$) para que una tal fórmula no exista. Este es efectivamente el caso. Sin embargo, construir dichos polinomios, incluso permitiendo más libertades en el cuerpo de base requiere o teoría más sofisticada, o un arduo y tedioso trabajo que definitivamente escapa al objetivo de este texto. La construcción de estos polinomios se puede encontrar en [Lan, Ex. 4, p. 272]. Mucho más difícil aún resultó ser construir tales polinomios sobre $\mathbb{Q}$; pero en 1892, David Hilbert probó la existencia de polinomios sobre $\mathbb{Q}$ con grupo de Galois isomorfo a $\mathbb{S}_n$. El desarrollo de esta prueba y toda la teoría que yace detrás de ella se puede encontrar en [Mal].

3.8. El Teorema Fundamental de la Teoría de Galois

Si bien nuestra aventura pudo haber finalizado tranquilamente en la sección anterior, hay un par de resultados que vale la pena mencionar. Primero, una definición.

Definición 30. Sea $\mathrm{Aut}(E)$ el grupo de automorfismos de un cuerpo E. Si G es un subconjunto de $\mathrm{Aut}(E)$, entonces

$$E^G = \{\alpha \in E : \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

se conoce como el **cuerpo fijo** de G.

Es fácil ver que E^G es siempre un subcuerpo de E. La instancia más importante de esta definición es cuando G es un subgrupo de $\mathrm{Aut}(E)$. Una observación crucial es que

$$H \subset G \implies E^G \subset E^H.$$

Un ejemplo de suma importancia es cuando E/F es una extensión con grupo de Galois $G = \mathrm{Gal}(E/F)$. En ese caso:

$$F \subset E^G \subset E;$$

y nos va a interesar saber cuando E^G/F es una extensión propia.

Hacemos una última observación sin demostración.

Observación 6. Si G, H son dos subgrupos de $\mathrm{Aut}(E)$

(I) $[E : E^G] = |G|$

(II) Si $E^G = E^H$, entonces $G = H$.

Nuestra discusión sobre grupos de Galois empezó con una extensión finita E/F en donde a veces requeríamos que esta extensión satisficiera la peculiar condición de ser el cuerpo de descomposición de un polinomio sobre F. Por otro lado aparece la pregunta de, si $G = \mathrm{Gal}(E/F)$, cuando vale que $F = E^G$. Es decir, sabemos que los elementos de G dejan fijo a F, pero ¿cuando es F lo *único* que los elementos de G dejan fijo? Estas dos ideas tienen la siguiente conexión.

Teorema 41. Sea E/F una extensión finita con grupo de Galois $G = \mathrm{Gal}(E/F)$. Las siguientes condiciones son equivalentes:

(I) $F = E^G$

(II) Todo polinomio irreducible $p(x) \in F[x]$ con alguna raíz en E, es separable y tiene todas sus raíces en E, es decir, se descompone sobre E.

(III) E es el cuerpo de descomposición de un polinomio $f(x) \in F[x]$.

Demostración. (I) $\implies$ (II) Sea $p(x) \in F[x]$ un polinomio irreducible que tenga una raíz $\alpha \in E$. Sean los distintos elementos del conjunto $\{\sigma(\alpha) : \sigma \in G\} = \{\alpha_1, \ldots, \alpha_n\}$. Definimos $g(x) \in E[x]$ mediante

$$g(x) = \prod (x - \alpha_i).$$

Ahora, cada $\sigma \in G$ permuta a las α_i por lo que σ fija a los coeficientes de $g(x)$. Eso quiere decir que los coeficientes de $g(x)$ pertenecen a $E^G = F$. Es decir, $g(x)$ es un polinomio en $F[x]$. Como $p(x)$ y $g(x)$ tienen una raíz común en E su mcd en $E[x]$ es distinto de 1 y por el Corolario 10 tenemos que su mcd tampoco es 1 en $F[x]$. Como $p(x)$ es irreducible, tiene que dividir a $g(x)$. Por lo tanto, $p(x)$ no tiene raíces repetidas, es decir, es separable y se descompone sobre E.

(II) $\implies$ (III) Elegimos $\alpha_1 \in E$ con $\alpha_1 \notin F$. Como E/F es finita, α_1 debe ser algebraico sobre F. Sea $p_1(x) \in F[x]$ su polinomio minimal, que recordemos que es irreducible como polinomio de $F[x]$. Por hipótesis $p_1(x)$ es separable y se descompone en E; sea $K_1 \subset E$ su cuerpo de descomposición. Si $K_1 = E$, ya hemos terminado. En caso contrario, tomamos $\alpha_2 \in E$ con $\alpha_2 \notin K_1$. Por hipótesis, hay un polinomio separable irreducible $p_2(x) \in F[x]$ que tiene a α_2 como raíz. Sea $K_2 \subset E$ el cuerpo de descomposición del polinomio separable $p_1(x)p_2(x)$. Si $K_2 = E$ ya hemos terminado, de lo contrario seguimos iterando esta construcción. Este proceso acabará con $K_m = E$ para algún m porque E/F es finita.

(III) $\implies$ (I) Por el Teorema 28 $|G| = [E : F]$. Pero por la Observación 6 también tenemos $|G| = [E : E^G]$, por lo que $[E : F] = [E : E^G]$. Como $F \subset E^G$, se sigue que $F = E^G$. □

Definición 31. Una extensión de cuerpos se dice **Galois** si satisface alguna de las condiciones del teorema anterior.

Lema 42. Si E/F es una extensión de Galois y B es un cuerpo intermedio entonces E/B es Galois.

Demostración. Como E/F es el cuerpo de descomposición de algún polinomio $f(x) \in F[x]$ y $F[x] \subset B[x]$, podemos pensar a $f(x) \in B[x]$. Por lo que E/B es también el cuerpo de descomposición de un polinomio sobre B, es decir, E/B es Galois. □

Definición 32. Sea E/F una extensión de Galois. Dos cuerpos intermedios B y C se dicen **conjugados** si existe un isomorfismo $B \to C$ que deja fijo a F puntualmente.

Lema 43. Sea E/F una extensión de Galois y sea B un cuerpo intermedio. Entonces las siguiente condiciones son equivalentes:

(I) B no tiene conjugados (además de sí mismo).

(II) Si $\sigma \in \mathrm{Gal}(E/F)$, entonces $\sigma|_B \in \mathrm{Gal}(B/F)$.

(III) B/F es una extensión Galois.

Demostración. (I) $\implies$ (II) Es obvio, pues $\sigma(B)$ es claramente un conjugado de B y por ende $\sigma(B) = B$.

(II) $\implies$ (III) Sea $p(x) \in F[x]$ un polinomio irreducible con una raíz β en B. Como $B \subset E$ y E/F es Galois, todas las raíces de $p(x)$ pertenecen a E. Supongamos que existe una raíz $\beta' \in E$ con $\beta' \notin B$. Por el Teorema 24 existe un isomorfismo $\tau : F(\beta) \to F(\beta')$ que deja fijo a F y extiende a un $\sigma \in \mathrm{Gal}(E/F)$, porque E/F es Galois. Pero $\sigma(B) \cong B$ y $\sigma(B) \neq B$, porque $\beta' \in \sigma(B)$ y $\beta' \notin B$.

(III) $\implies$ (I) B/F es el cuerpo de descomposición de un polinomio $f(x)$ sobre F, de manera que $B = F(\alpha_1, \cdots, \alpha_n)$ donde los α_i son las raíces de $f(x)$. Como cada $\sigma \in \mathrm{Gal}(E/F)$ lleva una raíz de $f(x)$ en una raíz de $f(x)$, se sigue que σ debe mandar a B a sí mismo. □

Definición 33. Un **lattice** es un conjunto parcialmente ordenado $(L, \leq)$ en donde cada par de elementos a, b de L tiene una cota superior minimal $a \vee b$ y una cota inferior maximal $a \wedge b$.

Ejemplos:

1. Si X es un conjunto, sea L la familia de todos los subconjuntos de X y definimos que $A \leq B$ si $A \subset B$. Entonces L es un lattice con $A \vee B = A \cup B$ y $A \wedge B = A \cap B$.

2. Si G es un grupo, sea $\mathrm{Sub}(G)$ la familia de todos los subgrupos de G, y definimos $H \leq K$ si $h \subset K$. Entonces $\mathrm{Sub}(G)$ es un lattice con $H \vee K$ el subgrupo generado por H y K, y $H \wedge K = H \cap K$.

3. Sea E/F una extensión, sea $\mathrm{Lat}(E/F)$ la familia de todos los cuerpos intermedios. Definimos $B \leq C$ si $B \subset C$. Entonces $\mathrm{Lat}(E/F)$ resulta un lattices con $B \vee C = BC$ y $B \wedge C = B \cap C$.

Lema 44. Si L y L' son dos lattices y $\gamma : L \to L'$ es una biyección que invierte el orden ($a \leq b \implies \gamma(b) \leq \gamma(a)$), entonces:

$$\gamma(a \vee b) = \gamma(a) \wedge \gamma(b) \text{ y } \gamma(a \wedge b) = \gamma(a) \vee \gamma(b)$$

Demostración. Tenemos que $a, b \leq a \vee b$ implica que $\gamma(a), \gamma(b) \geq \gamma(a \vee b)$; es decir, $\gamma(a \vee b)$ es una cota inferior de $\gamma(a)$ y $\gamma(b)$. Se sigue entonces que $\gamma(a) \wedge \gamma(b) \geq \gamma(a \vee b)$. Como γ es suryectiva, existe un $c \in L$ tal que $\gamma(a) \wedge \gamma(b) = \gamma(c)$. Aplicando γ^{-1} (que fácilmente se puede corroborar que también es una biyección que revierte el orden) obtenemos $a, b \leq c \leq a \vee b$. Por lo tanto, c $= a \vee b$ y $\gamma(a \vee b) = \gamma(c) = \gamma(a) \wedge \gamma(b)$. La otra mitad del enunciado se demuestra de manera similar. □

Teorema 45. Sea E/F una extensión de Galois con grupo de Galois $G = \mathrm{Gal}(E/F)$.

(I) La función $\gamma : \mathrm{Sub}(G) \to \mathrm{Lat}(E/F)$, dada por $H \mapsto E^H$ es una biyección que invierte el orden, cuya inversa esta dada por $\delta : B \mapsto \mathrm{Gal}(E/B)$.

(II) $E^{\mathrm{Gal}(E/B)} = B$ y $\mathrm{Gal}(E/E^H) = H$.

(III)
$$E^{H\vee K} = E^H \cap E^K$$
$$E^{H\cap K} = E^H \vee E^K$$

(IV)
$$\mathrm{Gal}(E/B \vee C) = \mathrm{Gal}(E/B) \cap \mathrm{Gal}(E/C)$$
$$\mathrm{Gal}(E/B \cap C) = \mathrm{Gal}(E/B) \vee \mathrm{Gal}(E/C)$$

(V) $[B : F] = [G : \mathrm{Gal}(E/B)]$ y $[G : H] = [E^H : F]$

(VI) B/F es una extensión de Galois si y solo $\mathrm{Gal}(E/B)$ es un subgrupo normal de G.

Demostración. (I) Es fácil ver que γ invierte el orden: $K \leq H$ implica que $E^H \leq E^K$. El hecho de que γ sea inyectiva es precisamente el enunciado de la Observación 6(II). Para ver que es suryectiva considere la composición:

$$\mathrm{Lat}(E/F) \xrightarrow{\delta} \mathrm{Sub}(G) \xrightarrow{\gamma} \mathrm{Lat}(E/F),$$

donde δ es el mapa $B \mapsto \mathrm{Gal}(E/B)$. Entonces $\gamma\delta : B \mapsto \mathrm{Gal}(E/B) \mapsto E^{\mathrm{Gal}(E/B)}$. Por el Lema 42, E/F Galois implica que E/B es Galois para todo cuerpo intermedio B; por lo que el Teorema 41 nos da $B = E^{\mathrm{Gal}(E/B)}$; y por lo tanto $\gamma\delta$ es la identidad y esto implica que γ es suryectiva. Por lo tanto γ es una biyección.

(II) Esto es simplemente el enunciado de que $\gamma\delta$ y $\delta\gamma$ son las respectivas funciones identidad.

(III) Se sigue del Lema 44 porque γ es una biyección que invierte el orden.

(IV) De igual manera, se sigue del Lema 44 porque $\delta = \gamma^{-1}$ es una biyección que invierte el orden.

(V) $[B : F] = [E : F]/[E : B] = |G|/|\mathrm{Gal}(E/B)| = [G : \mathrm{Gal}(E/B)]$, de manera que el grado de B/F es el índice de $\mathrm{Gal}(E/B)$ en G. La segunda ecuación se sigue de tomar $B = E^H$, porque $\mathrm{Gal}(E/E^H) = H$.

(VI) Si B/F es Galois, entonces vimos en el Teorema 30 que $\mathrm{Gal}(E/B)$ es un subgrupo normal de G. Por otro lado, supongamos que H es un subgrupo normal de G ¿es E^H/F una extensión Galois? Si $\sigma \in G$, entonces $\tau\sigma(\alpha) = \sigma\tau'(\alpha)$ para algún $\tau' \in H$ por la normalidad de H en G, y $\sigma\tau'(\alpha) = \sigma(\alpha)$ porque τ' deja fijo a α. Por lo tanto $\alpha \in E^H$ implica que $\sigma(\alpha) \in E^H$; esto es, $\sigma(E^H) \subset E^H$; efectivamente $\sigma(E^H) = E^H$ porque ambos tienen la misma dimensión sobre F. Finalmente, por el Lema 43, E^H/F es Galois.

□

4. Problemas Abiertos en Teoría de Galois

La teoría de Galois sigue siendo una línea activa de investigación. Mencionamos ahora algunos de los problemas que se tratan en la investigación en Teoría de Galois.

4.1. El Problema Inverso de Galois

Luego de plantear la definición de grupo de Galois, es natural que surja la siguiente pregunta: dado un grupo finito G, ¿podemos realizar a G como el grupo de Galois de una extensión E/F? no es difícil ver que, con lo mencionado en esta monografía, la respuesta a esta pregunta es afirmativa. Al final de la Sección 3.7 mencionamos que todos los grupos simétricos se pueden realizar como el grupo de Galois de una extensión E/F. El lector familiarizado con el Teorema de Cayley recordara que debe existir un $n \in \mathbb{N}$ tal que exista un subgrupo de $\mathbb{S}_n$ isomorfo a G. Para simplificar, identificaremos a este subgrupo con G. Luego, si E/F es una extensión de Galois tal que $\mathrm{Gal}(E/F) = \mathbb{S}_n$; consideramos el cuerpo fijo E^G y, por el Teorema 45, $\mathrm{Gal}(E/E^G) = G$.

Mucho mas interesante es plantear la pregunta restringiendo el cuerpo de base F : dado un grupo G y un cuerpo F, ¿existe una extensión de Galois E/F tal que el grupo de Galois de la extensión sea isomorfo a G? Si una tal extensión existe, G se dice **realizable sobre F.**

El problema inverso de Galois plantea si todo grupo finito puede ser el grupo de Galois de alguna extensión de $\mathbb{Q}$. Este problema, propuesto inicialmente por Hilbert en el siglo XIX, permanece sin resolver.

La siguiente pregunta interesante a hacerse puede ser: si G es realizable Sobre un cuerpo F ¿se puede construir una familia explicita de polinomios sobre F que tengan a G como grupo de Galois o mas aún, se puede construir la familia de todos los polinomios sobre F que tienen a G como grupo de Galois? Esta pregunta resulta en muchas otras: dado un grupo G y un cuerpo F ¿se puede escribir a la familia de todos los polinomios sobre F que tengan a G como grupo de Galois como un polinomio genérico? En tal caso, ¿cuál es el menor número de parámetros necesarios para describir explícitamente esta familia?

Algunos hitos importantes en la búsqueda de responder a estas preguntas son los siguientes:

1. **Teorema de Kronecker-Weber:** Todo grupo abeliano finito es realizable sobre $\mathbb{Q}$. Más aún, este se puede realizar como el grupo de Galois de un subcuerpo de un cuerpo ciclotómico (es decir, $\mathbb{Q}(\omega)$, donde ω es una raíz de la unidad).

2. Como ya se mencionó antes, Hilbert probó un cierto resultado conocido como el **Teorema de Irreducibilidad de Hilbert** para concluir el siguiente resultado: para todo $n \geq 1$ el grupo simétrico $\mathbb{S}_n$ y el grupo alternante $\mathbb{A}_n$ son realizables sobre $\mathbb{Q}$.

3. El siguiente paso importante fue realizado por A. Scholz y H. Reichard en 1937 al probar que todo p-grupo finito es realizable sobre $\mathbb{Q}$.

4. El último gran avance en esta teoría fue quizás el que hizo Shafarevich en 1989, que probó que todo grupo soluble es realizable sobre $\mathbb{Q}$. El único inconveniente es que

su argumento no es constructivo, por lo que no produce un polinomio que tenga a grupo prefijado como grupo de Galois.

5. Con respecto a los grupos simples, se tienen algunos resultados. Los grupos $\mathrm{PSL}(2,p)$ para algunos primos impares, fueron unos en de los primeros en ser realizados. Existen ciertas condiciones para p bajo las cuales se sabe que este grupo es realizable sobre $\mathbb{Q}$. Matzat probó que cuatro de los grupos de Mathieu, M_{11}, M_{12}, M_{22} y M_{24} son realizables sobre $\mathbb{Q}$. Quizás el resultado más espectacular en esta teoría para grupos simples se debe a Thompson, que logró probar que el grupo Monstruo es realizable sobre $\mathbb{Q}$.

Más resultados y una exposición más detallada de los métodos empleados en esta teoría se pueden encontrar en [Ran] y en [Mal].

Un caso particular del problema inverso de Galois es la conjetura de Malle. Esta involucra un invariante crucial de la extensiones algebraicas de $\mathbb{Q}$: el discriminante. El discriminante es un elemento de $\mathbb{Q}$ que se le asocia a una extensión $E/\mathbb{Q}$ y se puede definir en términos de una forma bilineal que a su vez usa la traza $E/\mathbb{Q}$ como $\mathbb{Q}$-espacio vectorial. La conjetura de Malle estudia la densidad de estas extensiones, cuando se fija el grupo de Galois y el determinante de la misma. En otras palabras, establece aproximadamente cuántas extensiones de $\mathbb{Q}$ tienen grupo de Galois G y discriminante menor o igual que un cierto $X \in \mathbb{Q}$ prefijado. Esta conjetura fue publicada en [Mal02]. Si bien está planteada en característica 0, se puede plantear en característica p; por ejemplo, para el cuerpo de funciones racionales $\mathbb{F}_p(t)$. En estos casos, el problema toma una naturaleza más geométrica. Una parte de la conjetura en este caso fue probada en marzo de 2023 en [ETW23].

4.2. El Grupo de Galois Absoluto

Dado un cuerpo F, definimos su **Grupo de Galois Absoluto** como $\mathrm{Gal}(\overline{F}/F)$, sonde $\overline{F}$ es la clausura algebraica de F. En particular, nos interesa estudiar $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Se puede probar que este es un grupo **pro-finito.** Esto quiere decir que es un grupo topológico que, en cierto sentido, se puede construir a partir de un sistema de grupos finitos. En este caso, se puede construir a partir de los grupos finitos $\mathrm{Gal}(E/\mathbb{Q})$ donde $E/\mathbb{Q}$ es una extensión finta de $\mathbb{Q}$. Por esto mismo, quizás el problema más importante de la Teoría de Galois sea entender la estructura de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, ya que dentro de este grupo, se codifica toda la teoría de Galois para extensiones finitas.

Uno de los intentos es el del reconocido Programa de Langlands. Este programa fue descripto por el matemático Edward Frenkel como "una especie de gran teoría unificada de las matemáticas". Tratar de resumir esta proeza matemática en solo tres párrafos constituye una verdadera falta de respeto, pero más aún lo sería ni siquiera mencionarlo, así que damos un panorama sobre-simplificado.

La gran tragedia de los grupos es que no son objetos lineales, por lo que muchas veces estudiarlos requiere un herramientas sofisticadas. Sin embargo, la Teoría de Representaciones nos permite "linealizarlos"; es decir, estudiarlos como si fueran grupos de matrices. Existe un importante teorema del matemático japones Tadao Tannaka, que dio origen a toda una filosofía dentro del álgebra moderna. En un sentido muy general, el teorema nos dice que entender toda la teoría de representaciones de un grupo es equivalente a

entender el grupo. Por lo que nos permite navegar con las herramientas del mundo lineal para recuperar luego información sobre grupos. En el caso particular de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, estas representaciones son conocidas como **Representaciones de Galois.**

Siendo desgraciadamente vago, el programa de Lagnlands pretende establecer una conexión entre estos objetos algebraicos (representaciones de Galois), una familia de objetos geométricos; las conocidas **curvas elípticas** y una familia de objetos analíticos, las igual de famosas **formas modulares**. Juntos, estos conceptos forman un tridente al que generaciones enteras de matemáticos y matemáticas han dedicado su vida a comprender. Para pintar lo gigantesco y ambicioso de esta propuesta basta mencionar que la aclamada prueba del último Teorema de Fermat, publicada por Andrew Wiles, se trato casi por completo sobre navegar en el centro de este triangulo de las matemáticas.

Otro intento de estudiar este grupo fue el de Alexander Grothendieck, con su programa "Esquisse d'un programme". Allí, Grothendieck nota que existe una acción fiel de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ en cierta colección de grafos incrustados en superficies compactas, a los les puso el simpático nombre *dessins d'enfants* o dibujos de niños, debido a su aparente simplicidad.

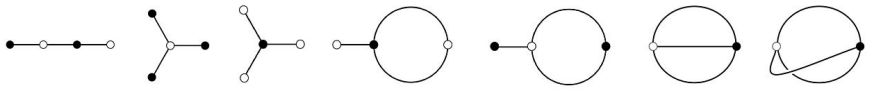

Figura 1: Ejemplos de dessins d'enfants.

Si se pudiese entender esta acción, podríamos representar a los elementos de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ como permutaciones de dessins d'enfants. Por lo tanto, uno de los problemas abiertos mas relevantes en la teoría de dessins d'enfants es clasificar suficientes invariantes de dessins d'enfants de forma tal que dos orbitas de la acción de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ se puedan distinguir.

Poco tiempo después de que Grothendieck publicara su Esquisse d'un programme, Drinfeld probó que $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ se inyecta en un grupo conocido como el **Grupo de Grothendieck-Teichmuller.** Este grupo surgió originalmente de la física teórica y se puede describir en términos de generadores y relaciones. Una pregunta aún abierta es si este grupo es isomorfo a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Incluso definir los elementos del grupo absoluto de Galois de $\mathbb{Q}$ ya desafía los límites conocidos del sistema axiomático de las matemáticas. Grandes avances se han producido en entender este grupo, pero parecen minúsculos comparados a lo que aún no sabemos. Galois sin saberlo, abrió una gran caja de Pandora, que deja perplejos a los matemáticos incluso siglos después de su muerte.

5. Epílogo

Pienso mucho en la vida. El prólogo que comienza este trabajo se puede leer al revés para descubrir algo sorprendente. Quizás la vida es tan inevitable como la muerte. Pues, ningún muerto estaría leyendo esto. ¿Qué hay de mí? Dijo Evariste atrás mio. Le pedí que deje de columpiarse en estas confusas palabras entre la vida y la muerte. "Vos no estás muerto, sos eterno. Tu teoría es eterna. Tus teoremas son una condena lógica, ¡venciste a la muerte!". Me miró inconcluso. De repente sonrió. Notó el libro que llevaba en la mano. "Me alegro mucho", me dijo y se desvaneció entre en la estantería número 12 de la biblioteca. No lo entendí. "¡Estamos por cerrar!" me asustó el bibliotecario por atrás. Creo que habían pasado varias horas. Dejé el libro donde estaba, saludé y me fui.

Volví a casa pensando. Pensé en la vida. Pensé en la muerte. Pensé en las matemáticas. Vi las caras de la gente en el colectivo. Las luces de los autos. Los carteles de la calle. Vi el sol ponerse y la luna salir. Todo era finito. La gente moriría. Los autos se romperían. Los carteles sería reemplazados por otros. La luna volvería a ponerse y el sol volvería a salir. De repente el pensamiento fue interrumpido. Pasó un taxi que tenía el número interno 3125. "¡Ja! 5^5" gritó esa parte insoportable de mi cabeza. "5..." recordé. Recordé el misterio. El misterio de vislumbrar a lo lejos que había algo intrínseco del número 5, que no permitía que los malditos polinomios con ese grado admitieran una solución por radicales. Recordé la carcajada que solté cuando sentí la adrenalina del abismo que significaba ese pensamiento. Recordé la sonrisa de Evariste. Cuando pinté esa imagen noté que en el revés de la suya estaba mi sonrisa. Aquella que sonreí mientras leía por primera vez un libro de Teoría de Galois. Fue la misma sonrisa de mi amigo cuando le conté desordenadas estas ideas recién aprendidas en un pizarrón de la facultad. Toda alma matemática la conoce. La siente aparecer cada vez que se coloca la última pieza de un rompecabezas matemático y tenemos ese adorado momento "¡A-já!". Somos almas adictas. Devoramos voraces tomos enteros con tal de quemarnos con ese fuego sagrado.

Esa era la clave. Entendí todo a la perfección. La eternidad de Galois fue su sonrisa. La que tuvo al leer a Lagrange, la misma que tuve yo al leer su obra. Ese minúsculo intervalo de tiempo tiene más sabor a eterno que cualquier teorema. Ese instante, tan efímero e inmortal, es la matemática.

Referencias

[Cor] Fernando Corbalán. *La invención de la teoría de grupos - Galois*. Genios de las matemáticas. ISBN: 9788447390656.

[ETW23] Jordan S. Ellenberg, TriThang Tran y Craig Westerland. *Fox-Neuwirth-Fuks cells, quantum shuffle algebras, and Malle's conjecture for function fields*. 2023. arXiv: 1701.04541 [math.NT].

[Hun] Thomas W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer. ISBN: 0387905189.

[Inf] Leopold Infeld. *Elegido de los dioses: la historia de Evariste Galois*. Siglo ventiuno. ISBN: 9682300452.

[Lan] Serge Lang. *Algebra, 3rd edition*. Graduate Texts in Mathematics. Springer. ISBN: 038795385X.

[Mal] Gunter Malle. *Inverse Galois Theory*. Springer Monographs in Mathematics. Springer. ISBN: 3540628908.

[Mal02] Gunter Malle. «On the Distribution of Galois Groups». En: *Journal of Number Theory* 92.2 (2002), págs. 315-329. ISSN: 0022-314X. DOI: https://doi.org/10.1006/jnth.2001.2713. URL: https://www.sciencedirect.com/science/article/pii/S0022314X01927131.

[Ran] Fariba Ranjbar. *Inverse Galois Problem and Significant Methods*. URL: https://arxiv.org/ftp/arxiv/papers/1512/1512.08708.pdf.

[Rot] Joseph Rotman. *Galois Theory*. Universitext. Springer. ISBN: 0387973052.

[San] Jorge Calero Sanz. *La revolución algebraica: el nacimiento de la teoría de grupos*. Grandes ideas de las matemáticas. ISBN: 8417811419.

[Wel] Jake Wellens. *A Friendly Introduction to Group Theory*. URL: https://math.mit.edu/~jwellens/Group%20Theory%20Forum.pdf.

Índice

Página