Miscelánea Matemática **63** (2016) 1-28 SMM

La demostración de Abel

Martha Rzedowski Calderón
Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados del I. P. N.
mrzedowski@ctrl.cinvestav.mx

Para encontrar las raíces de la ecuación cuadrática

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

usamos la famosa fórmula general

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

Para las ecuaciones cúbicas se pueden usar las fórmulas conocidas como fórmulas de Cardano y para las cuárticas el método de Ferrari. Para la ecuación polinomial de grado cinco **no existe** una fórmula que nos dé sus raíces en términos de las operaciones elementales y de radicales. Abel fue el primero en dar una demostración completa y correcta de que la ecuación general de grado cinco no es soluble por medio de radicales.

Este trabajo está dedicado a la memoria de Jaime Cruz Sampedro quien con sus preguntas me motivó a profundizar en el tema.

1. Introducción

La ecuación polinomial general (con coeficientes arbitrarios) de grado n no es soluble por medio de radicales para $n \geq 5$. Es importante aclarar que las raíces de tales ecuaciones existen (esto lo garantiza el Teorema Fundamental del Álgebra), podrían obtenerse bajo otros criterios y hay métodos para aproximarlas. Entre los primeros en estudiar las soluciones de las ecuaciones polinomiales de grado mayor o igual a cinco están Joseph–Louis Lagrange, Paolo Ruffini, Niels Henrik Abel, Augustin Louis Cauchy y Évariste Galois.

Se presenta un contexto histórico tanto del problema como del personaje y un bosquejo de demostración del hecho. Para la parte histórica se consultaron diversas fuentes, entre otras los trabajos de Shirley Bromberg y Juan José Rivaud [1], Peter Pesic [4] y José Manuel Sánchez Muñoz [6], así como diversas páginas de Wikipedia. El bosquejo de demostración se basa en una prueba debida a Michael Rosen [5], la cual coincide en espíritu con la de Abel, usa lenguaje moderno y no utiliza la teoría de Galois. Finalmente, se reproduce la primera página tanto de la versión de 1824 como de la de 1826 de la demostración original de Abel, disponibles en la red [7].

2. Ecuaciones polinomiales

2.1 Grado 1

La ecuación de primer grado

$$ax + b = 0,$$

con $a \neq 0$, tiene una única raíz, la cual es

$$x = -\frac{b}{a}.$$

Los orígenes de la obtención de soluciones para la ecuación lineal se remontan probablemente a los albores de la humanidad. En el **papiro Rhind**, el escriba Ahmes (en el antiguo Egipto, $\sim$ 1650 a.C.) dice basarse en un documento original escrito unos 200 años antes. El problema 26 del papiro pide el valor de *aha* si *aha* y su cuarto son añadidos para obtener 15.

En notación moderna, para solucionar el problema, se ha de resolver la ecuación

$$x + \frac{1}{4}x = 15,$$

cuya solución es $x = 12$.

2.2 Grado 2

La ecuación cuadrática

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

Figura 1. Papiro Rhind.

con $a \neq 0$, se puede resolver utilizando la fórmula general

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

Los orígenes de la obtención de soluciones para la ecuación cuadrática se remontan probablemente al Neolítico, habiendo evidencias de resolución de este tipo de ecuaciones en la cultura china («Nueve Capítulos en el Arte Matemático» elaborado durante el periodo Han, de 206 a.C. a 221 d.C.), en la cultura babilónica (texto BM 13901, $\sim$ 1600 a.C.), en la cultura griega (Proposiciones 28 y 29 de libro VI y Proposición 11 del libro II de «Los Elementos» de Euclides, c 300 a.C. y Libro 6 de la Aritmética de Diofanto, $\sim$ 280 d.C.) y en la cultura hindú (II 4 del Aryabhatiya, $\sim$ 500 d.C.)

El antiguo texto babilónico de la tablilla **BM 13 901** ($\sim$ 1600 a.C.) traducido (al alemán) y publicado por O. Neugebauer contiene problemas como:

He restado el (lado del) cuadrado del área, y es $14,30$.
El número $14,30$ está en base 60, que en base 10 corresponde a
$14 \times 60 + 30 = 870$. El problema es resolver la ecuación
$x^2 - x = 870$.
La solución está dada en palabras:
Tome 1, el coeficiente del (lado del cuadrado). Divida 1 *en dos partes*
$0:30 \times 0:30 = 0:15$ *añada* $14,30$
$14,30:15$ *tiene raíz cuadrada* $29:30$
Añada a $29:30$ *el* $0:30$ *que había multiplicado por él mismo,*
y 30 *es el (lado del) cuadrado.*
Lo anterior corresponde a $x = \frac{1}{2}(1) + \sqrt{(\frac{1}{2}(1))^2 + 870}$,
por lo tanto $x = 30$.

2.3 Grado 3

Aunque hubo algunas soluciones particulares con anterioridad, no fue sino hasta el siglo XVI que los algebristas italianos Scipione dal Ferro, Niccolò Tartaglia y Gerolamo Cardano obtuvieron la solución para la ecuación cúbica general.

Alrededor de 1515 Scipione **dal Ferro**, probablemente influenciado por Luca Pacioli, resolvió la ecuación cúbica de la forma $ax^3 + bx = c$. No hizo público su resultado, pero lo comunicó a su alumno y yerno Annibale **della Nave** y al menos a otro alumno, Antonio Maria **Fiore**.

Niccolò Fontana (apodado **Tartaglia**), quien llegó a vivir a Venecia en 1534, era famoso por resolver ecuaciones cúbicas. Fiore retó a Tartaglia a un concurso, para resolver ecuaciones cúbicas, mismo que ganó Tartaglia. El médico Gerolamo (o Girolamo) **Cardano** estaba completando un libro matemático y, teniendo noticias del concurso entre Fiore y Tartaglia, le interesó incluir la solución de la ecuación cúbica. Intentó convencer a Tartaglia de que le diera su solución. Al fin lo hizo, pero, de acuerdo con Tartaglia, Cardano juró por el Espíritu Santo y su fe como caballero, no publicar el descubrimiento. En 1539 apareció el libro de Cardano sin la solución de Tartaglia.

Versos en que explica **Tartaglia** su método para resolver las ecuaciones

$$x^3 + px = q, x^3 = px + q \text{ y } x^3 + q = px$$

(1534)

dal Ferro

Tartaglia

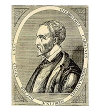
Quando chel cubo con le cose appresso	Del numer farai due tal part'á uolo
Se agguaglia á qualche numero discreto	Che l'una in l'altra si produca schietto
Trouan dui altri differenti in esso.	El terzo cubo delle cose in stolo
Dapoi terrai questo per consueto	Delle qual poi, per communprecetto
Che'llor produtto sempre sia eguale	Torrai li lati cubi insieme gionti
Alterzo cubo delle cose neto,	Et cotal somma sara il tuo concetto.
El residuo poi suo generale	El terzo poi de questi nostri conti
Delli lor lati cubi ben sottratti	Se solue col secondo se ben guardi
Varra la tua cosa principale.	Che per natura son quasi congionti.
In el secondo de cotestiatti	Questi trouai, & non con paßi tardi
Quando che'l cubo restasse lui solo	Nel mille cinquecentè, quatroe trenta
Tu osseruarai quest'altri contratti,	Con fondamenti ben sald'è gagliardi

Nella citta dal mar'intorno centa.

Con ayuda de su alumno Ludovico **Ferrari**, Cardano obtuvo una demostración del resultado y lo generalizó. En 1540 Ferrari descubrió que la ecuación de grado cuatro $x^4 + 6x^2 + 36 = 60x$ puede resolverse con ayuda de una ecuación cúbica.

Había el rumor de que dal Ferro había dejado su fórmula original con su yerno. Cardano y Ferrari visitaron a della Nave y confirmaron que dal Ferro había descubierto, con 20 años de antelación, la misma fórmula que encontró Tartaglia. En 1545 Cardano publicó su libro «Ars Magna» en el cual presenta las ecuaciones cúbica y cuártica, y sus soluciones, dando crédito a dal Ferro, a Tartaglia y a Ferrari.

Raíces de la ecuación cúbica
(Método de **Cardano**)



Ars Magna Cardano

Consideremos la ecuación cúbica $x^3 + ax^2 + bx + c = 0$.
Al tomar $x = y - \frac{a}{3}$ obtenemos una ecuación de la forma
$y^3 + py + q = 0$, donde $p = \frac{1}{3}(3b - a^2)$ y $q = \frac{1}{27}(2a^3 - 9ab + 27c)$.
Para resolverla hacemos $y = u + v$, obteniendo la ecuación

$$u^3 + v^3 + (p + 3uv)(u + v) + q = 0.$$

Supongamos que u y v satisfacen que $p + 3uv = 0$, entonces $uv = -\frac{p}{3}$.
Por lo tanto

$$u^3 + v^3 = -q \text{ y } u^3v^3 = -\frac{p^3}{27},$$

así pues u^3 y v^3 satisfacen la ecuación $t^2 + qt - \frac{p^3}{27} = 0$,
la cual es una ***ecuación resolvente*** y sus raíces son:

$$t_1 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \text{ y } t_2 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Sea $A = \sqrt[3]{t_1}$. Los valores para u son: $A, \omega A$ y $\omega^2 A$, donde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.
Como $uv = -\frac{p}{3}$, sea $B = \sqrt[3]{t_2}$ tal que $AB = -\frac{p}{3}$.
Entonces las raíces de la ecuación $y^3 + py + q = 0$ son:

$$y_1 = A + B,\ y_2 = \omega A + \omega^2 B \text{ y } y_3 = \omega^2 A + \omega B.$$

De donde pueden obtenerse las raíces de la ecuación cúbica original.

2.4 Grado 4

El alumno y secretario de Cardano, Ludovico **Ferrari** descubrió que la ecuación general de grado cuatro se puede reducir a una ecuación cúbica y por tanto ser resuelta por medio de raíces cuadradas y raíces cúbicas. Cardano explica el método de Ferrari en su obra «Ars Magna», el cual empieza con un teorema sobre cuadrados y rectángulos y usa en dos ocasiones la completación de cuadrados.

Raíces de la ecuación cuártica

De la ecuación cuártica $x^4 + ax^3 + bx^2 + cx + d = 0$, al sustituir $x = y - \frac{a}{4}$,
obtenemos la ecuación $y^4 + py^2 + qy + r = 0$, donde
$p = \frac{1}{8}(-3a^2 + 8b)$, $q = \frac{1}{8}(a^3 - 4ab + 8c)$ y $r = \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d)$
Sean y_1, y_2, y_3, y_4 las raíces de la ecuación en y.
Sean $\alpha = (y_1 + y_2)(y_3 + y_4) = -(y_1 + y_2)^2$,
$\beta = (y_1 + y_3)(y_2 + y_4) = -(y_1 + y_3)^2, \gamma = (y_1 + y_4)(y_2 + y_3) = -(y_2 + y_3)^2$,
observándose que $y_1 + y_2 + y_3 + y_4 = 0$. Consideramos
$h(t) = (t - \alpha)(t - \beta)(t - \gamma) = t^3 - (\alpha + \beta + \gamma)t^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)t - \alpha\beta\gamma$.
Se escribe este polinomio en términos de los coeficientes p, q y r y resulta
una ***ecuación resolvente***
para este caso: $t^3 - 2pt^2 + (p^2 - 4r)t + q^2 = 0$.
Observamos que $\sqrt{-\alpha}\sqrt{-\beta}\sqrt{-\gamma} = -q$.
Resolviendo esta ecuación cúbica obtenemos α, β y γ.
Debido a que $y_1 + y_2 = \sqrt{-\alpha}, y_1 + y_3 = \sqrt{-\beta}, y_1 + y_4 = \sqrt{-\gamma}$,
tenemos $2y_1 = \sqrt{-\alpha} + \sqrt{-\beta} + \sqrt{-\gamma}$ y de manera análoga se tiene que
$2y_2 = \sqrt{-\alpha} - \sqrt{-\beta} - \sqrt{-\gamma}, 2y_3 = -\sqrt{-\alpha} + \sqrt{-\beta} - \sqrt{-\gamma}$,
$2y_4 = -\sqrt{-\alpha} - \sqrt{-\beta} + \sqrt{-\gamma}$.
De donde pueden obtenerse las raíces de la ecuación cuártica original.

2.5 Grado 5

Una vez obtenidas las fórmulas para las raíces de las ecuaciones de grados 3 y 4, siguieron infructuosos intentos para resolver las ecuaciones de grado 5 por medio de radicales, es decir, obtener una fórmula del mismo estilo (que involucrara solamente operaciones elementales y extracción de raíces, a partir de los coeficientes de la ecuación).

Las raíces de tales ecuaciones existen (por el Teorema Fundamental del Álgebra), podrían obtenerse bajo otros criterios y hay métodos para acotarlas, separarlas y aproximarlas.

2.6 General

En su memoria de 1771 «Reflexiones sobre la resolución algebraica de ecuaciones», Joseph Louis **Lagrange** considera, para la ecuación cúbica $y^3 + py + q$, la resolvente $(y_1 + \omega y_2 + \omega^2 y_3)^3$, donde y_1, y_2, y_3 son las raíces de la ecuación original y ω es una raíz primitiva cúbica de 1. Los dos valores de la resolvente corresponden a t_1 y t_2 en la solución de Cardano.

Para la ecuación cuártica $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ considera la resolvente $R = (x_1 + x_2 - x_3 - x_4)^2$, donde x_1, x_2, x_3, x_4 son las raíces de la ecuación. Al aplicar las permutaciones se obtienen solamente 3

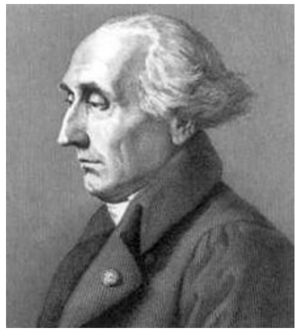


Figura 2. Joseph Louis Lagrange (1736 - 1813).

valores distintos. Las cuatro raíces de la ecuación original se pueden expresar como combinaciones sencillas de los diferentes valores de $\sqrt{R}$. Usando las identidades de Newton, Lagrange mostró que R satisface una ecuación cúbica. Resolviendo esta ecuación se obtienen sus 3 raíces, de las cuales se pueden obtener x_1, x_2, x_3, x_4, como en la fórmula de Ferrari (en la lámina se usó la resolvente $(y_1+y_2)(y_3+y_4) = -(y_1+y_2)^2$, donde y_1, y_2, y_3, y_4 son las raíces de la ecuación $y^4 + py^2 + qy + r = 0$).

En el «Teorema 100», Lagrange dice que si todas las permutaciones que dejan invariante a t también dejan invariante a y, entonces y puede ser expresado como función racional de t y los coeficientes de la ecuación dada. Cuando Lagrange usó el **método de resolventes** con la ecuación quíntica, obtuvo una ecuación de grado 6. **Por lo anterior, consideró que era necesario un nuevo camino para atacar la quíntica.**

Figura 3. Carl F. Gauss (1777 - 1855).

En el apartado 365 de sus *Disquisitiones Artithmeticae* [2], (1798-1801) llamado «Secciones del círculo que pueden realizarse por ecuaciones cuadráticas o sea por construcciones geométricas», Carl F. Gauss presenta una construcción del polígono regular de 17 lados e **indica que los polígonos regulares construibles con regla y compás son los que tienen n lados, donde $n \geq 3$ y $n = 2^m p_1 \cdots p_n$, con m y n enteros mayores o iguales que 0 y $p_1, \ldots, p_n$ son primos de Fermat** (los cuales son primos de la forma $p = 2^{2^\nu} + 1$, se conocen solamente 5, a saber 3, 5, 17, 257, 65537 y se conjetura que son todos).

> Gauss advierte: Siempre que $p-1$ contenga otros factores primos distintos de 2, somos llevados a ecuaciones de mayor grado, a saber, a una o más ecuaciones cúbicas cuando 3 aparece una o varias veces entre los factores primos de $p-1$, a ecuaciones de quinto grado cuando $p-1$ es divisible por 5, etc. **Podemos probar con todo rigor que las ecuaciones de mayor grado no pueden ser eludidas de ninguna manera ni pueden ser reducidas a ecuaciones de menor grado.** Los límites de este trabajo excluyen aquí esta demostración, pero emitimos esta advertencia no sea que alguien intente llevar a cabo otras construcciones geométricas que no son las sugeridas por nuestra teoría (e.g., secciones en 7, 11, 13, 19, etc. partes) y así gaste su tiempo inútilmente.

En la introducción de su primera demostración (1797-1799) del Teorema Fundamental del Álgebra, Gauss comenta:

> En pocas palabras, **se supone sin suficiente razón que la solución de cualquier ecuación se puede reducir a la resolución de ecuaciones puras. Tal vez no sería demasiado difícil demostrar la imposibilidad para el grado cinco con todo rigor**, comunicaré mis investigaciones sobre este tema en otra ocasión. Aquí es suficiente **enfatizar que la solución general de ecuaciones, en este sentido, se mantiene muy dudosa**, y consecuentemente que cualquier demostración que dependa totalmente de esta suposición, en el estado actual de las cosas no tiene peso.

En el apartado 359 de sus *Disquisitiones*, Gauss también aborda el problema:

Las investigaciones precedentes trataban del *descubrimiento* de ecuaciones auxiliares. Ahora explicaremos una propiedad muy notable concerniente a sus *soluciones.* **Consta que todos los trabajos de los geómetras eminentes han fracasado en la búsqueda de una solución general de ecuaciones de grado mayor que cuatro o (para definir lo que se desea más exactamente, de la reducción de ecuaciones mixtas a ecuaciones puras. Existe la pequeña duda de si este problema no solamente está más allá de las facultades del análisis contemporáneo sino que propone lo imposible** (cf. lo que dijimos de este asunto en *Demonstr. nova etc., art. 9*). No obstante es cierto que existen innumerables ecuaciones mixtas de todos los grados que admiten una reducción a ecuaciones puras, y esperamos que los geómetras encontrarán esto gratificante si demostramos que nuestras ecuaciones auxiliares son siempre de esta clase. Pero a causa de la longitud de esta discusión, presentaremos aquí solamente los principios más importantes para demostrar que la reducción es posible; reservamos para otra ocasión una consideración más completa, la que el tema merece.

2.7 Grado 5

Figura 4. (1765 - 1822).

Hasta donde sabemos Paolo **Ruffini** fue **el primero (1799 - 1813) en tratar de probar (y casi probar) que la ecuación general de grado** 5 **o mayor no se puede resolver por medio de radicales.**

Ruffini se basaba en los métodos de Lagrange. Consideraba funciones racionales de las raíces de una ecuación general de grado n. Si m es el número de permutaciones que dejan tal función inalterada, m es un divisor de $n!$, y el número de valores diferentes que toma la función, si se permutan las raíces, es $\frac{n!}{m}$. Lagrange había probado que tal función es raíz de una ecuación de grado $\frac{n!}{m}$. Ruffini mostró que en el caso de la quíntica $\frac{5!}{m}$ puede ser 2 o 5, pero no 3 o 4, lo que significa que una resolvente en el sentido de Lagrange que satisfaga una ecuación de grado 3 o 4 es imposible. Su demostración no era totalmente correcta pues faltaba justificar que los radicales se pudieran expresar como funciones racionales de las raíces de la ecuación.

Cauchy parece haber considerado conclusiva la demostración de Ruffini, no así otros como el mismo Lagrange, Malfatti, Legendre y Abel.

Se conoce como *Regla de Ruffini* a la división sintética para dividir un polinomio entre un monomio de la forma $x - a$.

2.8 General

Figura 5. Augustin Cauchy (1789 - 1857).

Sean n el número de variables independientes y p el número primo más grande que divida a n. Augustin **Cauchy** probó, en su artículo de 1815, que el número de valores diferentes de una función racional no simétrica de n variables no puede ser menor que p, a menos que sea 2. **Cauchy distinguía entre permutaciones y sustituciones.** Escribir $1, 2, 3, 4$ en cualquier orden como 1 2 4 3 y 2 4 3 1 serían *permutaciones*, mientras que el pasar de una a otra como

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

sería una *sustitución*. Galois usó la misma terminología, aunque no de manera consistente.

Cauchy definió el producto de sustituciones. En sus trabajos de 1844 - 1846, llamó a dos sustituciones P y Q «semejantes» si se descomponen en ciclos de la misma manera. Probó que P y Q son semejantes si y solamente si $Q = R^{-1}PR$. También probó que el orden de cualquier grupo de sustituciones es divisible por el orden de cualquier sustitución en el grupo.

La teoría de **Galois** describe, entre otras cosas, precisamente cuándo una ecuación polinomial es soluble por medio de radicales. Todo polinomio tiene asociado un grupo, conocido como *grupo de Galois* del polinomio o de la ecuación polinomial correspondiente. **Una ecuación polinomial es soluble por medio de radicales si y solamente si su grupo de Galois es soluble.**

Figura 6. Évariste Galois (1811-1832).

El grupo G es *soluble* si existe una cadena de subgrupos

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_s = G$$

de manera que G_i es subgrupo normal de G_{i+1} y G_{i+1}/G_i es abeliano para $i \in \{0, 1, \ldots, s-1\}$.

La ecuación general de grado n tiene como grupo de Galois al grupo simétrico S_n. El grupo simétrico S_n no es soluble para $n \geq 5$. Por lo que concluimos que **la ecuación general de grado n no puede ser resuelta por medio de radicales para $n \geq 5$.**

Para grado 5 consideramos algunos ejemplos (notemos que si el polinomio de grado 5 que define a la extensión de Galois es irreducible, el grupo de Galois es un subgrupo transitivo de S_5):

- La ecuación polinomial $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0$ tiene como grupo de Galois al grupo *cíclico* C_5 con 5 elementos, el cual es soluble, por lo que el polinomio es soluble por medio de radicales.
- La ecuación polinomial $x^5 - 5x + 12 = 0$ tiene grupo de Galois D_{10}, el grupo *diédrico* con 10 elementos, el cual es soluble, por lo tanto el polinomio es soluble por medio de radicales.
- La ecuación polinomial $x^5 - 2 = 0$ tiene grupo de Galois F_{20}, el grupo *de Frobenius* con 20 elementos, el cual es soluble, luego el polinomio es soluble por medio de radicales. De hecho, sus 5 soluciones son $\zeta^k \cdot \sqrt[5]{2}$, con $\zeta = e^{\frac{2\pi i}{5}}$ y $k \in \{0, 1, 2, 3, 4\}$.
- El grupo de Galois asociado al polinomio $x^5 + 20x + 16$ es el grupo *alternante* en 5 letras A_5 con 60 elementos, el cual no es soluble, por lo que el polinomio no es soluble por medio de radicales.
- El grupo de Galois asociado al polinomio $x^5 - x + 1$ es el grupo *simétrico* en 5 letras S_5 con 120 elementos, el cual no es soluble, por lo tanto el polinomio no es soluble por medio de radicales.
- La ecuación polinomial $x^5 = 0$ tiene grupo de Galois $\{id\}$, el grupo *trivial* con un elemento, el cual es soluble, luego el polinomio es soluble por medio de radicales. Su única solución es 0, es una raíz de multiplicidad 5, pertenece al campo $\mathbb{Q}$.
- El grupo de Galois asociado al polinomio $x^5 + x^2 - x + 1 = (x^2 + 1)(x^3 - x + 1)$ es el grupo $C_2 \times S_3$ con 12 elementos, el cual es soluble, por lo que el polinomio es soluble por medio de radicales.
- La ecuación polinomial $x^5 + x^4 - x^3 + -2x - 1 = (x^3 + x^2 - 2x - 1)(x^2 + 1) = 0$ tiene como grupo de Galois al grupo $C_2 \times C_3 \cong C_6$ con 6 elementos, el cual es soluble, por lo tanto el polinomio es soluble por medio de radicales.

3. Niels Henrik Abel

3.1 Primeros años

Niels Henrik Abel nació el 5 de agosto de 1802 en Finnøy (aunque algunos indican que fue en Nedstrand), Noruega. En aquella época Noruega se separaba de Dinamarca y había intenciones de que se integrara a Suecia. Abel fue hijo del pastor protestante Søren Georg Abel y de Anne Marie Simonsen.

Sus primeros estudios estuvieron a cargo de su padre y de un maestro particular. Cuando tenía 13 años lo enviaron a estudiar a la escuela de la Catedral de Christiania (ahora, y desde 1923, llamada Oslo).

En 1818 tuvo la suerte de tener como maestro de matemáticas a Bernt Michael **Holmboe**, quien motivó a algunos de sus alumnos retándolos a resolver diversos problemas de álgebra y geometría.

Figura 7. Niels Henrik Abel (1802-1829).

Figura 8. Christiania.

Figura 9. Bernt Holmboe (1795 - 1850).

Abel se destaca y su maestro le plantea problemas especiales. En poco tiempo va más allá y empieza a trabajar solo. Se interesó en los trabajos de Euler, Lagrange y Laplace. Solicitó en préstamo de la biblioteca obras de Newton, Gauss y Lagrange, entre otras.

De esta época data su interés por encontrar la solución general de la ecuación de grado cinco. Muestra su solución a su maestro y se consulta a algunos especialistas. Antes de recibir la respuesta, él mismo encuentra un error. Uno de los consultados, el danés Ferdinand **Degen** le aconseja estudiar las integrales elípticas.

En 1821, a pesar de la muerte de su padre el año anterior y de los graves problemas económicos de la familia, ingresó a la Universidad de Christiania, donde permaneció durante cuatro años, con la ayuda económica de parte de algunos profesores. En 1823, el profesor Søren

Rasmussen le apoyó económicamente para que hiciera una visita de dos meses a Copenhague, donde conoció a Degen.

También ahí, en un baile, conoció a Christine (Crelly) Kemp, con quien se comprometería en 1824. Ella viajó a Noruega el año siguiente y trabajó como institutriz para estar cerca de él.

Figura 10. Christine Kemp (1804 - 1862).

Abel trabajó sobre el Último Teorema de Fermat e inició su estudio de las funciones elípticas. Publicó su primer trabajo importante sobre integrales definidas. Por parte de sus profesores, se tenía la idea de que Abel viajara a Alemania y a Francia para continuar sus estudios y establecer contactos.

3.2 Viajero

Le apoyaron en su solicitud de fondos estatales para viajar. Sin embargo, se consideró necesario que permaneciera un tiempo más en la universidad preparándose mejor, entre otras cosas en idiomas. En 1824 demostró que no existe una fórmula algebraica para obtener las soluciones de la ecuación general de grado cinco. Abel utilizó parte del apoyo recibido para imprimir su trabajo sobre la quíntica. Para que fuera su carta de presentación, lo preparó en francés, pero tratando de economizar, lo condensó en seis páginas. Se lo envió a Gauss.

En septiembre de 1825 inició su viaje, junto con otros 4 estudiantes noruegos. Entre ellos estaba el geólogo Baltazar Mathias Keilhaus.

A su paso por Dinamarca, Abel quiso visitar a Degen, pero se encontró con que ya había fallecido.

Viajó a Berlín, donde tuvo la fortuna de conocer a August Leopold Crelle, quien inició en 1826 la publicación de su célebre revista *Journal für die reine und angewandte Mathematik*, incorporando seis trabajos de Abel. El segundo fue una versión ampliada de su trabajo sobre la quíntica. Ese mismo año se publicaron otros siete trabajos de Abel en la revista.

Figura 11. Baltazar Keilhaus (1797 - 1858).

Figura 12. August Crelle (1780 - 1855).

Visitó algunas ciudades de Europa y en agosto de 1826 llegó a París. Tenía reservado para la Academia de Ciencias lo que se conoce como el Tratado de París: «Memoria sobre una propiedad general de una clase muy amplia de funciones trascendentes», un teorema de adición sobre integrales elípticas, mismo que entregó con fecha del 30 de octubre. La academia encargó la revisión del trabajo a Legendre y a Cauchy. El manuscrito fue olvidado hasta que, a instancias de Jacobi, su gran competidor en el tema, finalmente fue publicado en 1841.

A fines de 1826 dejó París y visitó Berlín nuevamente. Volvió a Noruega en mayo de 1827, donde se encontró sin empleo, con deudas propias y familiares y además enfermo de tuberculosis. En la primavera de 1828 tuvo un empleo temporal. Decidió aceptar alguna oferta de trabajo que pudiera llegar de Berlín. Su salud continuó deteriorándose y él continuó trabajando en matemáticas. Para Navidad decidió viajar (en trineo) a Frøland a visitar a su prometida y amigos. Su enfermedad se agravó. Abel pidió a su amigo Keilhaus que cuidara a Christine, su prometida (se casaron un año y medio después). Abel falleció el 6 de abril de 1829, tenía 26 años.

3.3 Aportaciones y reconocimientos

El 8 de abril de ese mismo año de 1828 llegaron noticias de París, se había encontrado el extraviado Tratado de París y se iniciaba el reconocimiento a su trabajo. Al año siguiente se le otorgó el premio de la Academia de Ciencias, que compartió con Jacobi. También el 8 de abril, Crelle le escribió una carta anunciándole que había obtenido un empleo permanente en Berlín. En 1828 habían escrito Legendre, Poisson, Lacroix y Maurice al rey de Suecia solicitando apoyo para Abel.

En una carta a Crelle de fecha 8 de octubre de 1828, Abel escribe: Si (cada) tres raíces de una ecuación irreducible cualquiera de grado primo, están relacionadas entre ellas de manera que una de esas raíces puede ser expresada racionalmente por las otras dos, la ecuación en cuestión será siempre soluble con la ayuda de radicales.

En su último trabajo Abel demostró que si las raíces de una ecuación son tales que todas las raíces se pueden expresar como funciones racionales de una de ellas, digamos x, y si cualquiera dos de ellas, digamos $\theta(x)$ y $\theta_1(x)$ son tales que

$$\theta\theta_1(x) = \theta_1\theta(x),$$

entonces la ecuación se puede resolver por medio de radicales.
Un ejemplo de tal ecuación es $x^n - 1$.
Los grupos en los que la operación es conmutativa se llaman *abelianos*.

En la introducción de su artículo inconcluso *Sur la théorie algébrique des équations*, Abel explica su pensamiento: Uno debe dar a un problema una forma tal que siempre sea posible resolverlo, cosa que siempre puede hacerse con cualquier problema. En lugar de buscar una solución que uno no sabe si existe o no, uno debe preguntarse si tal relación es realmente posible.
Además formula los siguientes problemas:

- Encontrar todas las ecuaciones de un grado dado que son algebraicamente solubles.
- Juzgar cuándo una ecuación dada es algebraicamente soluble.
- Encontrar todas las ecuaciones que una función algebraica dada puede satisfacer.

Entre sus trabajos se encuentran los siguientes:

- Almindelig Methode til at finde Funktioner af een variabel Stórrelse, naar en Egenskab af disse Functioner er udtrykt ved en Ligning imellem to Variable, Magazin for Naturvidenskaberne bind I, 1823, pp. 216–229

- Oplösning af et Par Opgaver ved Hjelp af bestemte Integraler (del 1), Magazin for Naturvidenskaberne bind II, 1823, pp. 55–68
- Oplösning af nogle Opgaver ved Hjelp af bestemte Integraler (del 2), Magazin for Naturvidenskaberne bind II, 1823, pp. 205–215
- Om Maanens Indflydelse paa Pendelens Bev$\frac{3}{4}$gelse, Magazin for Naturvidenskaberne bind I, 1824, pp. 219–226, Berigtigelse, bind II, 1824, pp. 143–1144
- Mémoire sur les équations algébriques où on démontre l'impossibilité de la résolution de l'équation générale du cinquième dégré, Groendahl, Christiania 1824
- Det endelige Integral $\Sigma^n\phi$x udtrykt ved et enkelt bestemt Integral, Magazin for Naturvidenskaberne bind II, 1825, pp. 182–189
- Et lidet Bidrag til L$\frac{3}{4}$ren om adskillige transcendente Functioner, Det Kongelige Norske Videnskabers Selskabs Skrifter 2, 1826, pp. 177–207

En el *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1, 1826:

- Untersuchung der Functionen zweier unabhängig veränderlichen Größen x und y, wie f(x, y), welche die Eigenschaft haben, daß f(z,f(x,y)) eine symmetrische Function von z, x und y ist, pp. 11–15
- Beweis der Unmöglichkeit algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen, pp. 65–84
- Bemerkungen über die Abhandlung Nr. 4, Seite 37. im ersten Heft dieses Journals, pp. 117–118
- Auflösung einer mechanischen Aufgabe, pp. 153–157
- Beweis eines Ausdruckes, von welchem die Binomial-Formel ein einzelner Fall ist, pp. 159–160
- Ueber die Integration der Differential-Formel $\rho dx/\sqrt{}R$, wenn R und ρ ganze Functionen sind, pp. 185–221
- Untersuchungen über die Reihe: $1 + (m/1)x + m(m-1)/(12)x^2 + m(m-1)(m-2)/(123)x^3+$ u.s.w., pp. 311–339

En el *Journal für die reine und angewandte Mathematik (Crelles Journal)* 2, 1827:

- Ueber einige bestimmte Integrale, pp. 22–30
- Recherches sur les fonctions elliptiques, pp. 101–181
- Théorèmes et problèmes, p. 286
- Ueber die Functionen welche der Gleichung $\phi x + \phi y = \psi(xfy + yfx)$ genugthun, pp. 386–394

En el *Journal für die reine und angewandte Mathematik (Crelles Journal)* 3, 1828:

- Note sur le mémoire de Mr. L. Olivier No. 4. du second tome de ce journal, ayant pour titre «remarques sur les séries infinies et leur convergence», pp. 79–82
- Recherches sur les fonctions elliptiques. (Suite du mémoire Nr. 12. tom. II. cah. 2. de ce journal), pp. 160–190
- Aufgabe aus der Zahlentheorie, p. 212
- Remarques sur quelques propriétés générales d'une certaine sorte de fonctions transcendantes, pp. 313–323
- Sur le nombre des transformations différentes, qu'on peut faire subir à une fonction elliptique par la substitution d'une fonction donné de premier degré, pp. 394–401
- Théorème général sur la transformation des fonctions elliptiques de la seconde et de la troisième espèce, p. 402

En el *Journal für die reine und angewandte Mathematik (Crelles Journal)* 4, 1829:

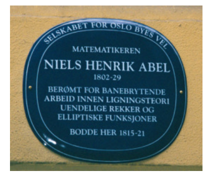
- Note sur quelques formules elliptiques, pp. 85–93
- Mémoire sur une classe particulière d'équations résolubles algébriquement, pp. 131–156
- Théorèmes sur les fonctions elliptiques, pp. 194–199
- Démonstration d'une propriété générale d'une certaine classe de fonctions transcendentes, pp. 200–201
- Précis d'une théorie des fonctions elliptiques, pp. 236–277
- Précis d'une théorie des fonctions elliptiques. (Suite), pp. 309–348

Entre sus aportaciones mencionamos:

- Ecuaciones funcionales
- Transformadas integrales e integrales definidas (un problema mecánico)
- Ecuaciones algebraicas («quíntica», ejemplos de ecuaciones solubles, formulación general)
- Teorema de irreducibilidad
- Funciones elípticas
- Integrales elípticas
- Integrales hiperelípticas
- Integrales abelianas
- Teorema de Abel (teorema de adición)
- Series (y el rigor)

En la actualidad se usan los términos grupo abeliano, extensión abeliana, variedad abeliana, función abeliana, categoría abeliana, integral abeliana, esquema abeliano, ...

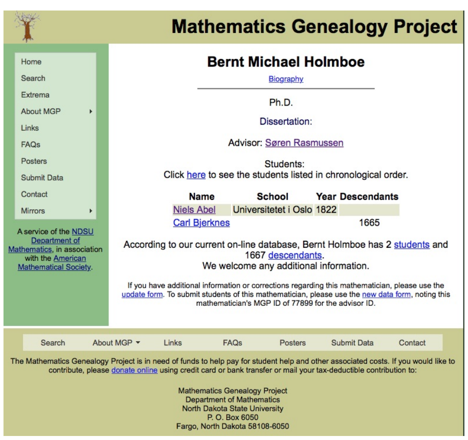
El conjunto de sus trabajos fue editado por Holmboe y publicado en 1839 por el gobierno noruego. Una edición más completa de su obra fue preparada por Ludwig Sylow y Sophus Lie y publicada en 1881.

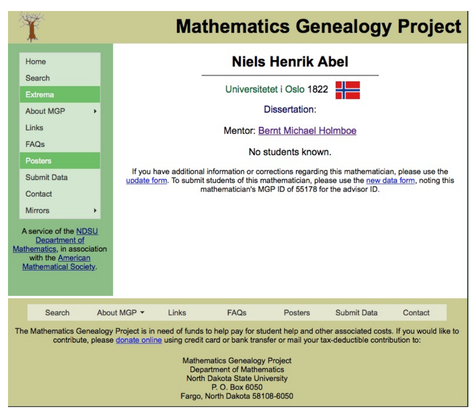


En 1902 y en 2002 hubo grandes homenajes. En 2002 se estableció el **Premio Abel** en su honor. El objetivo es otorgar el Premio Abel por trabajo científico destacado en el campo de las matemáticas. El premio es por 6 millones de coronas noruegas (aproximadamente 750 000 euros) y fue otorgado por primera vez el 3 de junio de 2003, a Jean–Pierre Serre.

Llevan el nombre de Abel un asteroide, un cráter en la Luna y también una aeronave.

Aparece en el *Mathematics Genealogy Project* [3].





4. Demostración del teorema de Abel

Como se dijo en la introducción, se presentará un bosquejo de demostración basado en el punto de vista de Michael Rosen [5], que tiene el espíritu de la demostración de Abel, que usa lenguaje moderno y no utiliza la teoría de Galois.

Sea k un campo con suficientes raíces de la unidad, por ejemplo, puede tomarse $k = \mathbb{C}$.

Sea $f(x) \in k[x]$ un polinomio mónico. Si $f(x) = (x - \theta_1)(x - \theta_2)\dots(x - \theta_n)$, llamamos a $F = k(\theta_1, \theta_2, \dots, \theta_n)$ un **campo de descomposición de** $f(x)$ **sobre** k.

Una extensión algebraica finita E/k es llamada **torre de radicales** si existe una serie de campos intermedios

$$k = E_0 \subset E_1 \subset \cdots \subset E_{m-1} \subset E_m = E$$

tal que para cada $0 \leq i \leq m, E_{i+1} = E(\sqrt[p_i]{\alpha_i})$ donde p_i es primo y $\alpha_i \in E_i^*$.

La ecuación $f(x) = 0$ es **soluble por medio de radicales** si existe una torre de radicales E/k tal que $F \subseteq E$.

Observamos que si $f(x) = 0$ es soluble por medio de radicales, no necesariamente se tiene que F/k sea una torre de radicales (por ejemplo, para $f(x) = x^3 + x^2 - 2x - 1$ la extensión $F/\mathbb{Q}$ es una extensión de Galois de grado 3 que no es radical pues las tres raíces de $f(x)$ son reales y las raíces primitivas cúbicas de la unidad no son reales, pero que sí es soluble por medio de radicales).

Supongamos que k es de característica cero y sean $s_1, s_2, \dots, s_n$ algebraicamente independientes sobre k. Sea $K = k(s_1, s_2, \dots, s_n)$. La **ecuación general de grado** n **sobre** k es

$$x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n = 0.$$

Supongamos $x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n = (x - x_1)(x - x_2)\dots(x - x_n)$ en alguna extensión de K. Sea $L = K(x_1, x_2, \dots, x_n)$. Estas definiciones de K y L se mantendrán en lo que resta de esta sección.

El **grupo simétrico** S_n actúa sobre L permutando las raíces $x_1, x_2, \dots, x_n$ y $K = k(s_1, s_2, \dots, s_n)$ es el campo fijo.

Si $\sigma \in S_n$ y $f \in L$,

$$(\sigma f)(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

Sean

$$\delta = \Pi_{i<j}(x_i - x_j) \ \text{ y } \ \Delta = \delta^2.$$

Para $\sigma \in S_n$, $\sigma\delta = \pm\delta$. Si σ es una trasposición, $\sigma\delta = -\delta$. El **grupo alternante** A_n es el subgrupo de S_n que consiste de los elementos $\sigma \in S_n$ tales que $\sigma\delta = \delta$.

Se tienen los siguientes resultados acerca de permutaciones. El tercero se sigue del segundo observando que

$$(a_1 a_2 a_3) = (a_2 a_1 a_3 a_4 \dots a_m)(a_m a_{m-1} \dots a_4 a_3 a_2 a_1).$$

- El grupo S_n está generado por trasposiciones.
- El grupo A_n está generado por 3-ciclos.

- El grupo A_n está generado por m-ciclos, donde m es cualquier número impar entre 3 y n.

La demostración del teorema se llevará a cabo en cuatro pasos.

PASO 1. *Si L está contenido en una torre de radicales sobre K, entonces L/K es una torre de radicales.*

PASO 2 (Teorema de Cauchy sobre permutaciones)**.** *Sea p el primo más grande menor o igual que n. Si $f \in L$ toma menos de p valores bajo la acción de S_n, entonces f puede tomar solamente* 1 *o* 2 *valores.*

PASO 3. *Si $n = 5$, entonces L/K no es una torre de radicales.*

PASO 4 (Teorema de Abel)**.** *La ecuación general de grado* 5 *sobre k no es soluble por medio de radicales.*

Necesitaremos los siguientes cuatro lemas y un lema crucial. Consideremos un número primo q.

Lema 4.1. *Sea F un campo que contenga una raíz q-ésima primitiva de la unidad. Si $a \in F^*$ no es una q-ésima potencia, entonces $x^q - a$ es irreducible.*

Demostración. Denotamos por ζ a una raíz q-ésima primitiva de la unidad en F y por α a una raíz de $x^q - a$. Las raíces de la ecuación son de la forma $\zeta^i\alpha$ con $0 \le i < q$, por lo que cualquier factor de $x^q - a$ es de la forma $h(x) = \prod_{i\in\mathcal{A}}(x - \zeta^i\alpha)$ para algún subconjunto $\mathcal{A}$ de $\{0, \ldots, q-1\}$. Notemos que si $h(x) \in F[x]$, entonces $h(0) = \pm\prod_{i\in\mathcal{A}}(\zeta^i\alpha) = \pm\zeta^{i_0}\alpha^{|\mathcal{A}|}$ es un elemento de F, luego $\alpha^{|\mathcal{A}|}$ también es un elemento de F. Puesto que $\alpha \notin F$ y q es primo, obligadamente $h(x) = x^q - a$. Por lo que $x^q - a$ es irreducible. □

Lema 4.2. *Supóngase que $x^q - a \in F[x]$ es irreducible y que α es una raíz. Sea $\gamma \in F(\alpha)\backslash F$. Entonces existe $\beta \in F(\alpha)$ tal que $\beta^q \in F$ y*

$$\gamma = b_0 + \beta + b_2\beta^2 + \ldots + b_{q-1}\beta^{q-1},$$

donde $b_0, b_2, \ldots, b_{q-1} \in F$.

Demostración. Sea α una raíz de $x^q - a$. Entonces $\gamma = a_o + a_1\alpha + \cdots + a_{q-1}\alpha^{q-1}$ para algunos $a_i \in F$. Sea k el natural más pequeño tal que $a_k \neq 0$. Pongamos $\beta := a_k\alpha^k$. Entonces $\beta^q \in F(\alpha)$. Para $2 \le m < q$ podemos encontrar enteros r y s tales que $0 \le s < q$ y $rq + sk = m$. Luego $\alpha^m = (\alpha^q)^r(\alpha^k)^s = c_s\beta^s$ con $c_s \in F$. Sustituyendo en la ecuación para γ se obtiene la expresión deseada. □

Lema 4.3. *Sea ζ una raíz q-ésima primitiva de la unidad. Entonces*

$$1 + \zeta^i + \zeta^{2i} + \ldots + \zeta^{(q-1)i} = \begin{cases} 0 & si\ q \nmid i, \\ q & si\ q \mid i. \end{cases}$$

Demostración. Si q divide a i se tiene $\zeta^i = 1$, de donde se sigue el resultado. Mientras que si q no divide a i, entonces ζ^i es una raíz q-ésima primitiva de la unidad. De $(\zeta^i-1)(1+\zeta^i+\zeta^{2i}+\ldots+\zeta^{(q-1)i}) = \zeta^{iq}-1 = 0$ y $\zeta^i - 1 \neq 0$, se obtiene lo requerido. □

Lema 4.4. *Sean K y L como al principio de esta sección. Sea $y \in L$. Entonces el polinomio irreducible de y sobre K se descompone en factores lineales en $L[x]$.*

Demostración. Sean $y_1, y_2, \ldots, y_m$ los distintos valores de y bajo la acción del grupo simétrico S_n. Entonces $g(x) = (x-y_1)(x-y_2)\ldots(x-y_m)$ tiene coeficientes que quedan fijos bajo S_n y por tanto son elementos de K (hecho conocido en ese tiempo). Luego el polinomio irreducible de y sobre K debe dividir a $g(x)$, de donde se sigue el resultado. □

Lema crucial. *Sean E/K una extensión de campos, q un primo y $a \in E$ tales que $x^q-a \in E[x]$ es irreducible. Sea α una raíz de $x^q-a = 0$. Sean $M := E(\alpha) \cap L$ y $M_0 := E \cap L$. Entonces M/M_0 es una extensión radical. Más precisamente, existe $\beta \in M$ tal que $\beta^q \in M_0$ y β genera a M sobre M_0.*

Demostración. Si $M_0 = M$ se tiene el resultado. Suponemos $M_0 \neq M$. Sea $y \in M \setminus M_0$. Por el lema 4.2, existe $\beta \in E(\alpha)$ tal que $\beta^q = b \in E$ y

$$y = b_0 + \beta + b_2\beta^2 + \ldots + b_{q-1}\beta^{q-1},$$

donde $b_i \in E$. Sea $g(x) \in K[x]$ el polinomio irreducible de y sobre K y póngase

$$G(x) = g(b_0 + x + b_2x^2 + \ldots + b_{q-1}x^{q-1}).$$

Tenemos $G(x) \in E[x]$ y tiene a β como raíz. Por el lema 4.1, $x^q - b \in E[x]$ es irreducible. Luego x^q-b divide a $G(x)$. Se sigue que $G(\zeta^i\beta) = 0$, donde i es cualquier entero y así los elementos

$$\begin{aligned}
y = y_1 &= b_0 + \beta + b_2\beta^2 + \ldots + b_{q-1}\beta^{q-1} \\
y_2 &= b_0 + \zeta\beta + b_2\zeta^2\beta^2 + \ldots + b_{q-1}\zeta^{q-1}\beta^{q-1} \\
&\vdots \\
y_q &= b_0 + \zeta^{q-1}\beta + b_2\zeta^{2(q-1)}\beta^2 + \ldots + b_{q-1}\zeta^{(q-1)(q-1)}\beta^{q-1}
\end{aligned}$$

son todos raíces de $g(x)$. Por el lema 4.4, tenemos que $y_1, y_2, \ldots, y_q$ son elementos de L. Multiplicamos cada i-ésima ecuación por ζ^{i-1} y sumamos. Usando el lema 4.3, tenemos

$$\beta = \frac{1}{q}\sum_{i=1}^{q} \zeta^{1-i} y_i \in L.$$

Luego $\beta \in L \cap E(\alpha) = M$ y $\beta^q = b \in L \cap E = M_0$. Probemos que β genera a M sobre M_0. Sea $\gamma \in M$.

Tenemos

$$\gamma = c_0 + c_1\beta + c_2\beta^2 + \ldots + c_{q-1}\beta^{q-1},$$

para algunos $c_i \in E$. Resta probar que $c_i \in E \cap L = M_0$. Con el argumento anterior tenemos

$$\gamma_i = c_0 + c_1\zeta^{i-1}\beta + c_2\zeta^{2(i-1)}\beta^2 + \ldots + c_{q-1}\zeta^{(q-1)(i-1)}\beta^{q-1} \in L \cap E(\alpha) = M,$$

para $i = 1, 2, \ldots, q$. Multiplicamos γ_i por $\zeta^{k(1-i)}$ y sumamos sobre i. Por el lema 4.3, obtenemos

$$c_k\beta^k = \sum_{i=1}^{q} \zeta^{k(1-i)\gamma_i} \in M.$$

Puesto que $\beta \in M$, se sigue que $c_k \in M \cap E = M_0$, con lo que se concluye la demostración. □

PASO 1. *Si L está contenido en una torre de radicales sobre K, entonces L/K es una torre de radicales.*

Demostración. Supongamos que E/K es una torre de radicales tal que $L \subseteq E$. Entonces

$$K = E_0 \subset E_1 \subset \cdots \subset E_{m-1} \subset E_m = E,$$

tal que para cada $E_{i+1} = E(\sqrt[q_i]{a_i})$ donde q_i es primo y $a_i \in E_i^*$. Consideramos la torre

$$K \subseteq E_1 \cap L \subseteq \cdots \subseteq E_{m-1} \cap L \subseteq L.$$

Por el lema crucial $E_{i+1} \cap L/E_i \cap L$ es trivial o bien es una extensión radical de grado q_i. Eliminando igualdades, la última torre muestra que L/K es una torre de radicales. □

PASO 2 (Teorema de Cauchy sobre permutaciones)**.** *Sea p el primo más grande menor o igual que n. Si $f \in L$ toma menos de p valores bajo la acción de S_n, entonces f puede tomar solamente* 1 *o* 2 *valores.*

Demostración. Sean $\sigma \in S_n$ un p-ciclo y $< \sigma >$ el subgrupo generado por σ. Sea $H = \{\tau \in < \sigma > \mid \tau f = f\}$. Como p es primo, $H = < \sigma >$ o $H = < e >$. Luego, o bien $f, \sigma f, \ldots, \sigma^{p-1}$ son todos distintos, o bien $\sigma f = f$. Como f toma menos de p valores, ha de tenerse que $\sigma f = f$ para todos los p-ciclos. El tercer resultado sobre permutaciones implica que f es fijado por A_n. Puesto que $[S_n : A_n] = 2$, se sigue el resultado. □

El anterior es una generalización del siguiente resultado de Ruffini.

Proposición 4.5. *Si $n = 5$ y f toma menos de 5 valores, entonces f puede tomar solamente 2 valores diferentes o un valor, pero nunca 3 o 4 valores.*

PASO 3. *Si $n = 5$, entonces L/K no es una torre de radicales.*

Demostración. Probaremos primero que cualquier extensión radical de K dentro de L tiene grado 2. Consideremos $K \subset K_1 \subset L$ y supongamos $K_1 = K(\alpha)$, donde $\alpha^q = a \in K$ y q es primo. Sea m el número de valores que toma α bajo la acción de S_5 (es decir, el número de distintos conjugados de α). Tenemos que m es el grado del irreducible de α sobre K. Como $x^q - a$ es irreducible, se tiene que $m = q$. Puesto que $|S_5| = 120$, m divide a 120 (Teorema de Lagrange), luego $q = 2, 3$ o 5. Por el paso 2, $q \neq 3$. Así $q = 2$ o $q = 5$. Veamos que $q \neq 5$. Supongamos que $q = 5$ y sean $x_1, \ldots, x_5$ las raíces de $x^5 - a$. Por el lema 4.2, existe $\beta \in K(\alpha)$ tal que $\beta^5 \in K$ y

$$x_1 = b_0 + \beta + \ldots + b_4\beta^4,$$

donde $b_0, \ldots, b_4 \in K$. Como en la demostración del lema crucial, obtenemos

$$\beta = \frac{1}{5}\sum_{i=1}^{5} \zeta^{1-i} x_i.$$

Esta relación es imposible, pues el lado izquierdo puede tomar 5 valores, mientras que el derecho puede tomar 120. Así pues, $q = 2$. Abel muestra que entonces $K_1 = K(\sqrt{\Delta})$ y de manera análoga a como se hizo antes, prueba que $K(\sqrt{\Delta})$ no tiene extensiones radicales en L. $\square$

PASO 4 (Teorema de Abel)**.** *La ecuación general de grado* 5 *sobre* k *no es soluble por medio de radicales.*

Demostración. Supongamos que la ecuación general de grado 5 sobre k es soluble por medio de radicales. Entonces, por definición, existe una torre de radicales E/K tal que $L \subseteq E$. Luego, por el paso 1, L/K es una torre de radicales. Esto contradice el paso 3, luego la ecuación general de grado 5 sobre k no es soluble por medio de radicales. $\square$

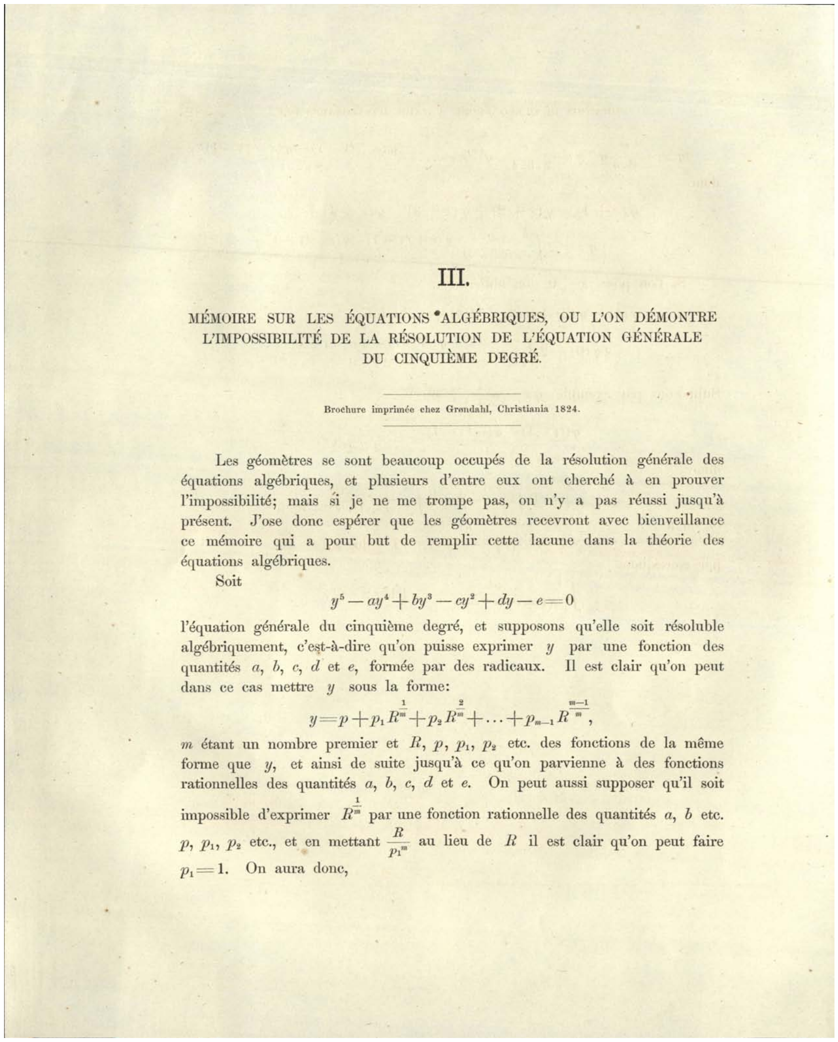
Abel termina mencionando: «De este teorema se deduce inmediatamente que resulta también imposible resolver por medio de radicales ecuaciones de grado superior a 5.»

5. La demostración original de Abel

5.1 La demostración de Abel, versión de 1824

Se reproduce a continuación la primera de las 6 páginas de la versión de 1824 que está en la edición de Sylow y Lie de los trabajos de Abel, el documento completo se obtuvo de la siguiente liga:

`http://www.abelprize.no/nedlastning/verker/oeuvres_1881_del1/oeuvres_\completes_de_abel_nouv_ed_1_kap03_opt.pdf`



III.

MÉMOIRE SUR LES ÉQUATIONS ALGÉBRIQUES, OU L'ON DÉMONTRE L'IMPOSSIBILITÉ DE LA RÉSOLUTION DE L'ÉQUATION GÉNÉRALE DU CINQUIÈME DEGRÉ.

Brochure imprimée chez Grøndahl, Christiania 1824.

Les géomètres se sont beaucoup occupés de la résolution générale des équations algébriques, et plusieurs d'entre eux ont cherché à en prouver l'impossibilité; mais si je ne me trompe pas, on n'y a pas réussi jusqu'à présent. J'ose donc espérer que les géomètres recevront avec bienveillance ce mémoire qui a pour but de remplir cette lacune dans la théorie des équations algébriques.

Soit

$$y^5 - ay^4 + by^3 - cy^2 + dy - e = 0$$

l'équation générale du cinquième degré, et supposons qu'elle soit résoluble algébriquement, c'est-à-dire qu'on puisse exprimer y par une fonction des quantités a, b, c, d et e, formée par des radicaux. Il est clair qu'on peut dans ce cas mettre y sous la forme:

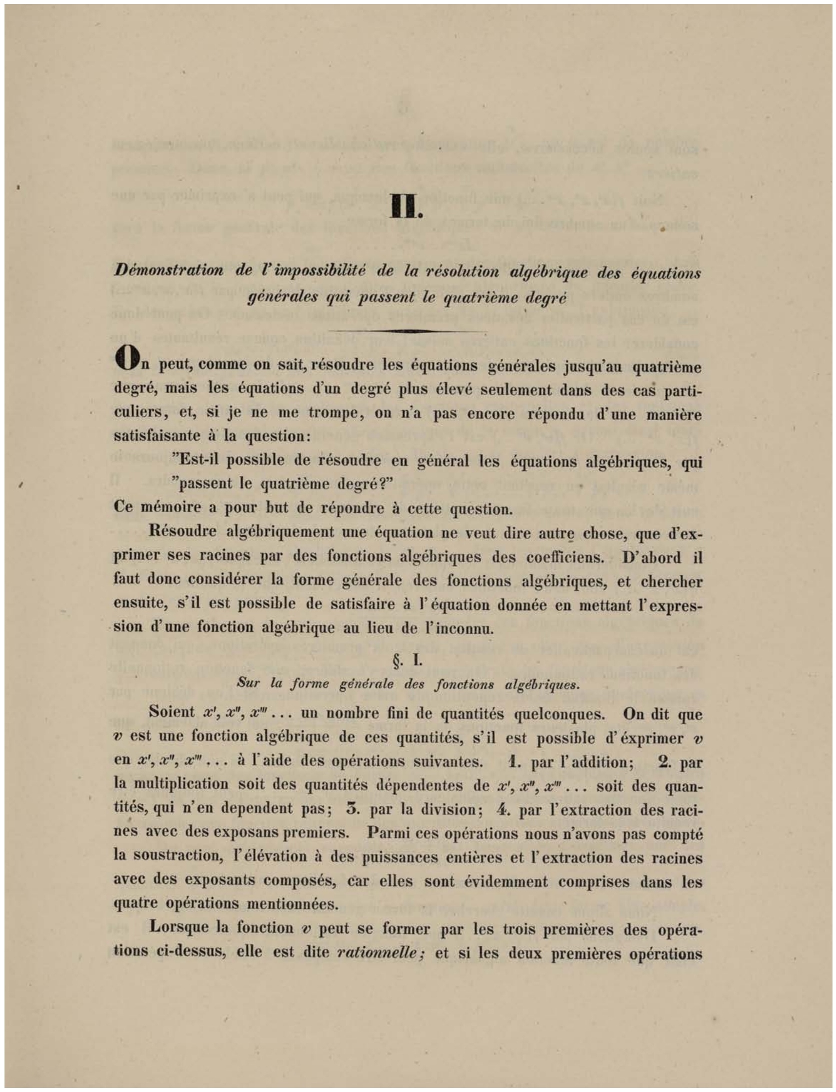
$$y = p + p_1 R^{\frac{1}{m}} + p_2 R^{\frac{2}{m}} + \ldots + p_{m-1} R^{\frac{m-1}{m}},$$

m étant un nombre premier et R, p, p_1, p_2 etc. des fonctions de la même forme que y, et ainsi de suite jusqu'à ce qu'on parvienne à des fonctions rationnelles des quantités a, b, c, d et e. On peut aussi supposer qu'il soit impossible d'exprimer $R^{\frac{1}{m}}$ par une fonction rationnelle des quantités a, b etc. p, p_1, p_2 etc., et en mettant $\frac{R}{p_1^m}$ au lieu de R il est clair qu'on peut faire $p_1 = 1$. On aura donc,

5.2 La demostración de Abel, versión de 1826

Se reproduce a continuación la primera de las 20 páginas de la versión de 1826 que está en la edición de Holmboe de los trabajos de Abel, el documento completo se obtuvo de la siguiente liga:

`http://www.abelprize.no/nedlastning/verker/oeuvres_1839/oeuvres_completes_de_abel_1_kap02_opt.pdf`



II.

Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré

On peut, comme on sait, résoudre les équations générales jusqu'au quatrième degré, mais les équations d'un degré plus élevé seulement dans des cas particuliers, et, si je ne me trompe, on n'a pas encore répondu d'une manière satisfaisante à la question:

"Est-il possible de résoudre en général les équations algébriques, qui "passent le quatrième degré?"

Ce mémoire a pour but de répondre à cette question.

Résoudre algébriquement une équation ne veut dire autre chose, que d'exprimer ses racines par des fonctions algébriques des coefficiens. D'abord il faut donc considérer la forme générale des fonctions algébriques, et chercher ensuite, s'il est possible de satisfaire à l'équation donnée en mettant l'expression d'une fonction algébrique au lieu de l'inconnu.

§. I.

Sur la forme générale des fonctions algébriques.

Soient $x', x'', x''' \ldots$ un nombre fini de quantités quelconques. On dit que v est une fonction algébrique de ces quantités, s'il est possible d'exprimer v en $x', x'', x''' \ldots$ à l'aide des opérations suivantes. 1. par l'addition; 2. par la multiplication soit des quantités dépendentes de $x', x'', x''' \ldots$ soit des quantités, qui n'en dependent pas; 3. par la division; 4. par l'extraction des racines avec des exposans premiers. Parmi ces opérations nous n'avons pas compté la soustraction, l'élévation à des puissances entières et l'extraction des racines avec des exposants composés, car elles sont évidemment comprises dans les quatre opérations mentionnées.

Lorsque la fonction v peut se former par les trois premières des opérations ci-dessus, elle est dite *rationnelle;* et si les deux premières opérations

Bibliografía

[1] S. Bromberg y J. J. Rivaud, «Vida y Obra de Niels Henrik Abel», *Miscelánea Matemática*, núm. 36, 2002, 1–27.

[2] C. F. Gauss, *Disquisitiones Arithmeticae*, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, 1995, Traducción al español hecha por Hugo Barrantes, Michael Josephy, Ángel Ruiz Zúñiga.

[3] Mathematics Genealogy Project, «https://genealogy.math.ndsu.nodak.edu», consultado por última vez el 22 de septiembre de 2016.

[4] P. Pesic, *Abel's Proof*, MIT Press, 1983.

[5] M. I. Rosen y N. Hendrik, «Abel and Equations of the Fifth Degree», *American Mathematical Monthly*, núm. 102, 1995, 495–505.

[6] J. M. Sánchez Muñoz, «Historias de Matemáticas, Abel y la imposibilidad de resolver la "quíntica" por radicales», *Pensamiento Matemático*, 2011, 1–31.

[7] The Abel Prize Website, «http://www.abelprize.no», consultado por última vez el 22 de septiembre de 2016.