Miscelánea Matemática **53** (2011) 1–22 SMM

Las ecuaciones polinomiales como el origen de la teoría de Galois

Gabriel Villa Salvador

gvilla@ctrl.cinvestav.mx

Departamento de Control Automático
Centro de Investigación y de Estudios Avanzados del I.P.N.

Resumen

En este trabajo daremos un poco de historia sobre la vida de Galois para después presentar algo de historia sobre la solución de la ecuación cúbica y el Teorema de Abel–Ruffini sobre la imposibilidad de dar la solución por radicales a la ecuación general de quinto grado.
Después de estos antecedentes es donde entra el trabajo de Galois sobre cómo decidir si una ecuación polinomial dada es resoluble o no por medio de radicales.

1. A modo de excusa

La historia sobre la vida de Évariste Galois está llena de imprecisiones, diversas versiones, muchas veces no sólo encontradas sino francamente opuestas, de romanticismo, de medias verdades y muchas veces de total desconocimiento de los sucesos verdaderos. Hemos tratado de poner en este trabajo las versiones más o menos aceptadas sobre los diversos aspectos de la muy interesante y triste vida de uno de los matemáticos más grandes de toda la historia, pero no podemos asegurar que sean los verdaderos. No lo sabemos y posiblemente habrá aspectos que nunca serán aclarados del todo.

Asimismo, hemos incluido muchas páginas de la red con el fin de que el lector interesado pueda profundizar en algunos aspectos sobre la vida, la obra y la herencia de Évariste Galois. Sin embargo, por un lado, las páginas de la red cambian casi tan rápido como nuestros políticos de partido y es posible que lo que aquí pongamos haya desaparecido cuando el lector lo quiera consultar, y por otro lado, en realidad es más fácil encontrar innumerables referencias de cualquier tema con una

simple búsqueda que con páginas dadas de antemano. Sin embargo es nuestra obligación poner de la manera más precisa posible algunas de nuestras fuentes y por eso hemos incluido estas direcciones.

2. Antecedentes

Évariste Galois nació el 25 de octubre de 1811 en Bourg–la Reine, una comuna en las afueras de París, Francia, y murió el 31 de mayo de 1832 en París, a los 20 años, 7 meses y 6 días.

Su padre fue Nicholas-Gabriel Galois y su madre Adelade–Marie Demante. Su hermana mayor era Nathalie–Theodore y su hermano menor Alfred.

Fue educado hasta los 12 años por su madre y fue hasta ese entonces que empezó su educación académica formal en el liceo Royal de Louis–le–Grand de París. Ahí empezó el aspecto más importante de su personalidad, mucho más que su faceta de matemático: su pensamiento político y una rebeldía hacia la autoridad, sus sentimientos antieclesiásticos y antimonárquicos. Su primer contacto con las matemáticas fue hasta los 15 años, esto es, el trabajo matemático de toda su vida lo desarrolló en aproximadamente 5 años y es hasta nuestros días un tema relevante y de mucho interés en varias ramas de las matemáticas y en sí mismo.

Fue el curso impartido por M. Vernier el que despertó el genio matemático de Galois. En 1828 quiso entrar a la prestigiada École Polytechnique pero puesto que le faltaba mucha formación básica, fue rechazado. Siguió sus estudios en el Louis–le–Grand con el profesor M. Richard que apreció el potencial de Galois. Es por ese tiempo que publicó su primer trabajo: una demostración de un teorema sobre fracciones continuas periódicas; poco después encontró la clave para resolver el problema de la resolubilidad de las ecuaciones polinomiales por radicales. Sus avances más notables fueron en el desarrollo de la teoría de grupos (que aunque fue Galois el que más avances realizó en la teoría de grupos y le dio una forma diferente y estructurada, no fue el inventor de ella pues tanto Lagrange como Ruffini ya la habían estudiado e hicieron importantes contribuciones a ella).

Poco antes de presentarse a su segundo y definitivo examen de ingreso a la École Polytechnique, el padre de Galois se suicidó. Galois se presentó al examen en estas condiciones y, con sus maneras habituales de rebeldía y desprecio por la autoridad, se negó a seguir las indicaciones de los examinadores al rehusar justificar sus enunciados y, naturalmente, fue rechazado de manera definitiva.

294 FRACTIONS

ANALYSE ALGÉBRIQUE.

Démonstration d'un théorème sur les fractions continues périodiques ;

Par M. Evariste Galois, élève au Collége de Louis-le-Grand.

On sait que si, par la méthode de Lagrange, on développe en fraction continue une des racines d'une équation du second degré, cette fraction continue sera périodique, et qu'il en sera encore de même de l'une des racines d'une équation de degré quelconque, si cette racine est racine d'un facteur rationnel du second degré du premier membre de la proposée, auquel cas cette équation aura, tout au moins, une autre racine qui sera également périodique. Dans l'un et dans l'autre cas, la fraction continue pourra d'ailleurs être immédiatement périodique ou ne l'être pas immédiatement, mais, lorsque cette dernière circonstance aura lieu, il y aura du moins une des transformées dont une des racines sera immédiatement périodique.

Or, lorsqu'une équation a deux racines périodiques, répondant à un même facteur rationnel du second degré, et que l'une d'elles est immédiatement périodique, il existe entre ces deux racines une relation assez singulière qui paraît n'avoir pas encore été remarquée, et qui peut être exprimée par le théorème suivant :

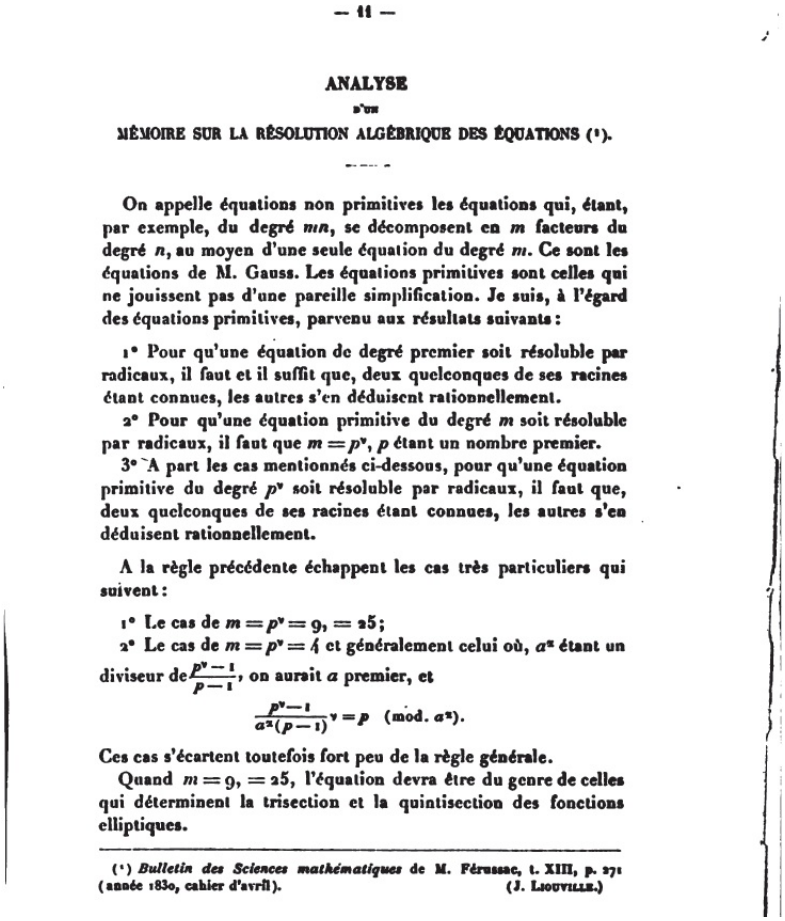
THÉORÈME. Si une des racines d'une équation de degré quelconque est une fraction continue immédiatement périodique, cette équation aura nécessairement une autre racine également périodique

Figura 1: "Analyse algébrique. Démonstration d'un théorme sur les fractions continues périodiques." *Annales de Gergonne*, **19** (1828-1829), p.294-301. Tomado de `http://archive.numdam.org/ARCHIVE/AMPA/AMPA_1828-1829__19_/AMPA_1828-1829__19__294_0/AMPA_1828-1829__19__294_0.pdf`, dominio público.

Entonces entró a la menos prestigiosa École Normale al mismo tiempo que sus trabajos sobre teoría de grupos eran evaluados por la Academia de Ciencias. Estos trabajos nunca fueron publicados en vida de Galois. Originalmente, el artículo sobre estos temas fue enviado a Cauchy quien lo rechazó pues el trabajo tenía puntos en común con los artículos de Abel de 1824 y 1826. Galois lo revisó y lo volvió a enviar y en esta ocasión, Cauchy lo remitió a la academia para su consideración.

Sin embargo Fourier, secretario vitalicio y encargado de su publicación, murió poco después de recibirlo y la memoria se traspapeló.

De cualquier manera Galois publicó 3 artículos en esos mismos años (1830–1831) en el *Bulletin des Sciences Mathématiques* de M. Férussac los cuales probaron sin ninguna duda que Galois había llegado mucho más lejos que cualquier matemático en la resolución de ecuaciones polinomiales.



— 11 —

ANALYSE

D'UN

MÉMOIRE SUR LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS (1).

On appelle équations non primitives les équations qui, étant, par exemple, du degré mn, se décomposent en m facteurs du degré n, au moyen d'une seule équation du degré m. Ce sont les équations de M. Gauss. Les équations primitives sont celles qui ne jouissent pas d'une pareille simplification. Je suis, à l'égard des équations primitives, parvenu aux résultats suivants :

1° Pour qu'une équation de degré premier soit résoluble par radicaux, il faut et il suffit que, deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement.

2° Pour qu'une équation primitive du degré m soit résoluble par radicaux, il faut que $m = p^\nu$, p étant un nombre premier.

3° A part les cas mentionnés ci-dessous, pour qu'une équation primitive du degré p^ν soit résoluble par radicaux, il faut que, deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement.

A la règle précédente échappent les cas très particuliers qui suivent :

1° Le cas de $m = p^\nu = 9, = 25$;

2° Le cas de $m = p^\nu = 4$ et généralement celui où, a^2 étant un diviseur de $\frac{p^\nu - 1}{p-1}$, on aurait a premier, et

$$\frac{p^\nu - 1}{a^2(p-1)}\nu = p \pmod{a^2}.$$

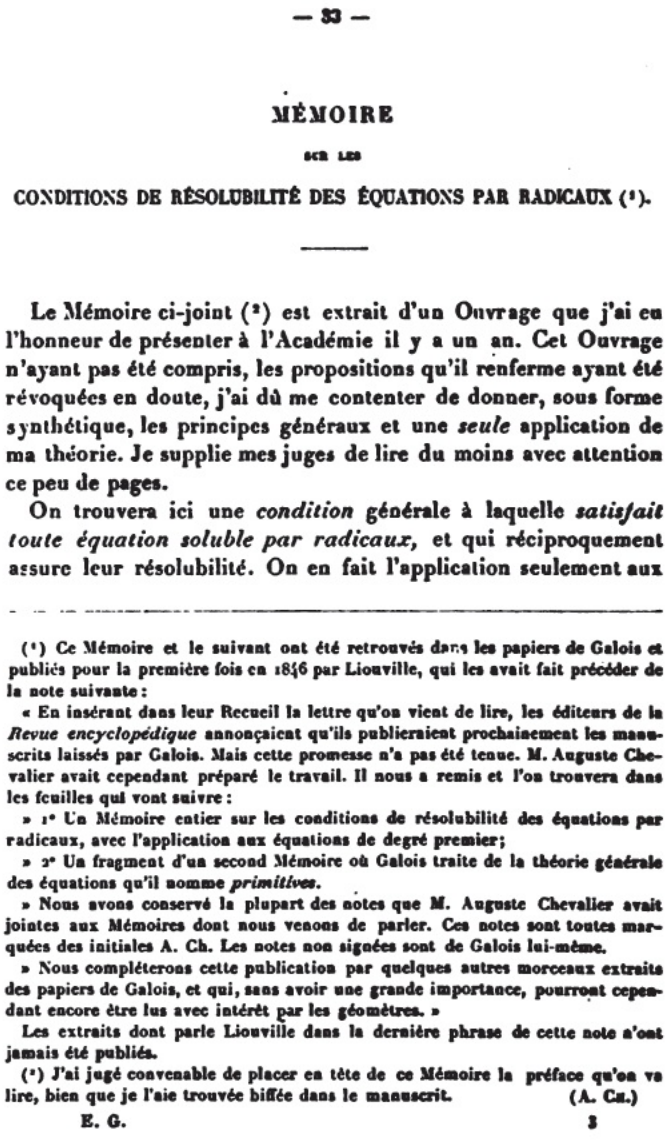
Ces cas s'écartent toutefois fort peu de la règle générale.

Quand $m = 9, = 25$, l'équation devra être du genre de celles qui déterminent la trisection et la quintisection des fonctions elliptiques.

(1) *Bulletin des Sciences mathématiques* de M. Férussac, t. XIII, p. 271 (année 1830, cahier d'avril). (J. LIOUVILLE.)

Figura 2: "Analyse d'un Mémoire sur la résolution algébrique des équations". *Bulletin des Sciences Mathématiques* XIII: 271 (1830). ŒUVERS MATHÉMATIQUES D'ÉVARISTE GALOIS, M. Émile Picard, Gauthier-Villars et Fils, Paris 1897. Tomado de
`http://openlibrary.org/books/OL6975080M/Œuvre_mathmatiques_d'Évariste_Galois`, dominio público.

En julio de 1830 los republicanos, entre ellos Galois, exiliaron al rey Carlos X pero fueron aplastados por el nuevo rey Luis Felipe de Orleans.



— 33 —

MÉMOIRE

SUR LES

CONDITIONS DE RÉSOLUBILITÉ DES ÉQUATIONS PAR RADICAUX (1).

Le Mémoire ci-joint (2) est extrait d'un Ouvrage que j'ai eu l'honneur de présenter à l'Académie il y a un an. Cet Ouvrage n'ayant pas été compris, les propositions qu'il renferme ayant été révoquées en doute, j'ai dû me contenter de donner, sous forme synthétique, les principes généraux et une *seule* application de ma théorie. Je supplie mes juges de lire du moins avec attention ce peu de pages.

On trouvera ici une *condition* générale à laquelle *satisfait toute équation soluble par radicaux,* et qui réciproquement assure leur résolubilité. On en fait l'application seulement aux

(1) Ce Mémoire et le suivant ont été retrouvés dans les papiers de Galois et publiés pour la première fois en 1846 par Liouville, qui les avait fait précéder de la note suivante :

« En insérant dans leur Recueil la lettre qu'on vient de lire, les éditeurs de la *Revue encyclopédique* annonçaient qu'ils publieraient prochainement les manuscrits laissés par Galois. Mais cette promesse n'a pas été tenue. M. Auguste Chevalier avait cependant préparé le travail. Il nous a remis et l'on trouvera dans les feuilles qui vont suivre :

» 1° Un Mémoire entier sur les conditions de résolubilité des équations par radicaux, avec l'application aux équations de degré premier;

» 2° Un fragment d'un second Mémoire où Galois traite de la théorie générale des équations qu'il nomme *primitives*.

» Nous avons conservé la plupart des notes que M. Auguste Chevalier avait jointes aux Mémoires dont nous venons de parler. Ces notes sont toutes marquées des initiales A. Ch. Les notes non signées sont de Galois lui-même.

» Nous compléterons cette publication par quelques autres morceaux extraits des papiers de Galois, et qui, sans avoir une grande importance, pourront cependant encore être lus avec intérêt par les géomètres. »

Les extraits dont parle Liouville dans la dernière phrase de cette note n'ont jamais été publiés.

(2) J'ai jugé convenable de placer en tête de ce Mémoire la préface qu'on va lire, bien que je l'aie trouvée biffée dans le manuscrit. (A. Ch.)

E. G. 3

Figura 3: "Mémoire sur les conditions de résolubilité des équations par radicaux". *Journal de Liouville*, tomo XI, 1846. ŒUVERS MATHÉMATIQUES D'ÉVARISTE GALOIS, M. Émile Picard, Gauthier-Villars et Fils, Paris 1897. Tomado de
`http://openlibrary.org/books/OL6975080M/Œuvre_mathmatiques_d'Évariste_Galois`, Dominio público.

Por participar activamente con los republicanos, Galois fue expulsado de la École Normale. A principios de 1831, y con apenas 19 años de

DES ÉQUATIONS PRIMITIVES
QUI SONT SOLUBLES PAR RADICAUX (1).
(Fragment.)

Cherchons, en général, dans quel cas une équation primitive est soluble par radicaux. Or, nous pouvons de suite établir un caractère général fondé sur le degré même de ces équations. Ce caractère est celui-ci : *Pour qu'une équation primitive soit résoluble par radicaux, il faut que son degré soit de la forme* p^n, *p étant premier*. Et de là suivra immédiatement que, lorsqu'on aura à résoudre par radicaux une équation irréductible dont le degré admettrait des facteurs premiers inégaux, on ne pourra le faire que par la méthode de décomposition due à M. Gauss; sinon l'équation sera insoluble.

Pour établir la propriété générale que nous venons d'énoncer relativement aux équations primitives qu'on peut résoudre par radicaux, nous pouvons supposer que l'équation que l'on veut résoudre soit primitive, mais cesse de l'être par l'adjonction d'un simple radical. En d'autres termes, nous pouvons supposer que, n étant premier, le groupe de l'équation se partage en n groupes irréductibles conjugués, mais non primitifs. Car, à moins que le degré de l'équation soit premier, un pareil groupe se présentera toujours dans la suite des décompositions.

Soit N le degré de l'équation, et supposons qu'après une extraction de racine de degré premier n, elle devienne non primitive et se partage en Q équations primitives de degré P, au moyen d'une seule équation de degré Q.

Si nous appelons G le groupe de l'équation, ce groupe devra se partager en n groupes conjugués non primitifs, dans lesquels les lettres se rangeront en systèmes composés de P lettres conjointes chacun. Voyons de combien de manières cela pourra se faire.

Soit H l'un des groupes conjugués non primitifs. Il est aisé de

(1) *Voir* la Note 1 de la page 33.

Figura 4: "Des équations primitives qui sont solubles par radicaux". *Journal de Liouville* Tome XI, 1846. Œuvers mathématiques d'Évariste Galois, M. Émile Picard, Gauthier-Villars et Fils, Paris 1897. Tomado de

`http://openlibrary.org/books/OL6975080M/Œuvers_mathematiques_d'Évariste_Galois`, dominio público.

edad, Galois fue encarcelado por sedición por un poco más de un mes y después de ser absuelto fue encarcelado nuevamente por sedición en julio (posiblemente encarcelado hasta octubre).

Durante 1831, Galois había redondeado su trabajo sobre grupos y lo había enviado a Poisson a la Academia de Ciencias, el cual primero lo sometió a la misma pero después recomendó su rechazo pues "sus argumentaciones no estaban ni lo suficientemente claras ni suficientemente desarrolladas para permitir juzgar su rigor". Galois recibió la carta de rechazo en prisión.

La parte final del reporte de Poisson dice:

> Hemos hecho todo esfuerzo posible para entender la prueba de Galois. Su razonamiento no es suficientemente claro ni suficientemente desarrollado para que nosotros podamos juzgar si es correcto y no podemos dar idea de ello en este reporte.
>
> El autor anuncia que la proposición que es el objeto especial de esta memoria, es parte de una teoría general susceptible de muchas aplicaciones. Posiblemente se comprobará que las diferentes partes de una teoría se aclaran mutuamente, y son más fáciles de captar en conjunto en lugar que cada una de manera aislada. Nos gustaría entonces sugerir al autor que debe publicar todo su trabajo completo para poder formarnos una opinión definitiva. Pero en el estado en que está la parte que él ha sometido a la academia, no podemos proponer su aceptación.

Dos días antes de su muerte, Galois fue liberado de su encarcelamiento. Los detalles de su muerte, supuestamente por un lío de faldas, no están claros y hay 2 ó 3 versiones totalmente distintas. Lo que sí sucedió la noche del 29 de mayo de 1832 es que Galois escribió varias cartas a los republicanos y escribió una copia de lo que había remitido a la academia junto con otros artículos a su amigo Auguste Chevalier.

En la madrugada del 30 de mayo de 1832, Galois perdió un duelo a pistola con Pescheux d'Herbinville, un artillero oficial (versión de Alejandro Dumas en sus memorias), falleciendo el 31 de mayo de 1832 a las 10 de la mañana en el hospital Cochin.

Sus últimas palabras, dirigidas a su hermano Alfred, fueron " ¡No llores! Necesito todo mi coraje para morir a los veinte años".

Su hermano y su amigo Auguste Chevalier recopilaron sus manuscritos. Es altamente probable que los hayan dado a conocer a muchos

II. — ŒUVRES POSTHUMES.

LETTRE A AUGUSTE CHEVALIER (1).

Mon cher ami,

J'ai fait en Analyse plusieurs choses nouvelles.

Les unes concernent la théorie des équations; les autres, les fonctions intégrales.

Dans la théorie des équations, j'ai recherché dans quels cas les équations étaient résolubles par des radicaux, ce qui m'a donné occasion d'approfondir cette théorie et de décrire toutes les transformations possibles sur une équation, lors même qu'elle n'est pas soluble par radicaux.

On pourra faire avec tout cela trois Mémoires.

Le premier est écrit, et, malgré ce qu'en a dit Poisson, je le maintiens, avec les corrections que j'y ai faites.

Le second contient des applications assez curieuses de la théorie des équations. Voici le résumé des choses les plus importantes :

1° D'après les propositions II et III du premier Mémoire, on voit une grande différence entre adjoindre à une équation une des racines d'une équation auxiliaire ou les adjoindre toutes.

Dans les deux cas, le groupe de l'équation se partage par l'adjonction en groupes tels, que l'on passe de l'un à l'autre par une même substitution; mais la condition que ces groupes aient les mêmes substitutions n'a lieu certainement que dans le second cas. Cela s'appelle la *décomposition propre*.

En d'autres termes, quand un groupe G en contient un autre H,

(1) Écrite la veille de la mort de l'auteur. (Insérée en 1832 dans la *Revue encyclopédique*, numéro de septembre, page 568.) (J. LIOUVILLE.)

Figura 5: "Lettre de Galois á M. Auguste Chevalier", *Journal des mathématiques pures et appliquées* XI: 408415. ŒUVERS MATHÉMATIQUES D'ÉVARISTE GALOIS, M. Émile Picard, Gauthier-Villars et Fils, Paris 1897. Tomado de
http://openlibrary.org/books/OL6975080M/Œuvre_mathmatiques_d'Évariste_Galois, Dominio público.

matemáticos de la época, pero únicamente atrajeron la atención de

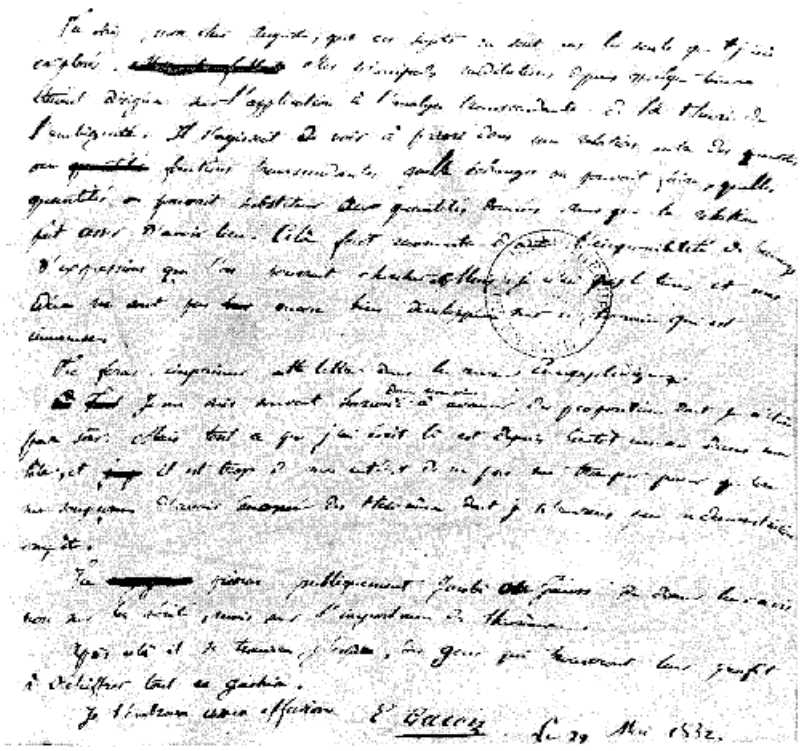


Figura 6: Tomada de `http://m759.net/wordpress/?p=8451`

Liouville en 1843.

Las obras de Galois fueron publicadas finalmente en el número de octubre de 1846 en *Journal des Mathematiques Pures et Appliquées* después de que Liouville revisó sus manuscritos y declaró que Galois había resuelto el problema de Abel. Gracias a Liouville es que ahora conocemos el trabajo de Galois.

3. Las ecuaciones de grado 3

Al principio del siglo XVI, Scipione del Ferro (1465–1526) encontró un método para resolver una clase de ecuaciones cúbicas: las del tipo $x^3 + ax = b$. De hecho todas las ecuaciones cúbicas pueden ser reducidas a esta forma si permitimos a a y a b ser negativos, pero los números negativos no eran conocidos por aquel entonces. Del Ferro mantuvo su resultado secreto hasta justo antes de su muerte cuando se lo comunicó a su estudiante Antonio Fiore.

En 1530 Niccolo Fontana conocido como *Tartaglia* (1500–1557) recibió dos problemas en ecuaciones cúbicas y anunció que podía resol-

Figura 7: Tomada de
http://www.librosmaravillosos.com/
grandesmatematicos/capitulo20.html

verlos. Pronto fue retado por Fiore. En el duelo, Tartaglia resolvió los problemas que eran de la forma $x^3 + ax = b$ para los cuales él había obtenido un método general mientras que Fiore fracasó en los problemas que recibió los cuales eran de la forma $x^3 + ax^2 = b$ que le resultaron muy difíciles y no los pudo resolver. Tartaglia ganó.

Más adelante Gerolamo Cardano (1501–1576) persuadió a Tartaglia de revelar su secreto para resolver ecuaciones cúbicas. Tartaglia accedió bajo la condición de que Cardano no los revelaría nunca y que en caso de que Cardano publicara un libro sobre ecuaciones cúbicas, le debería dar tiempo a Tartaglia para publicar sus resultados. Algunos años después, Cardano supo del trabajo previo de Del Ferro y publicó el método de Del Ferro en su libro "*Ars magna*" (el Gran Arte) en 1545, significando, posiblemente, que Cardano le dio 6 años a Tartaglia para publicar sus resultados y de cualquier forma dio debido crédito a Tartaglia por una solución independiente de las ecuaciones cúbicas. Aunque Cardano sintió que cumplió su promesa, no aceptó los retos de Tartaglia. El reto fue eventualmente aceptado por Lodovico Ferrari (1522–1565), originalmente sirviente de Cardano y posteriormente su colaborador. Ferrari superó en la competencia a Tartaglia y éste perdió su prestigio y su dinero.

Como dato curioso, Ferrari murió envenenado con arsénico por su hermana.

Cardano había notado que el método de Tartaglia requería de raíces cuadradas de números negativos. Cardano incluyó estos cálculos en Ars magna pero posiblemente sin entenderlos. Rafael Bombelli (1526–1572) estudió este problema en detalle y por esto es considerado a menudo como el descubridor de los números complejos.

Finalmente fue Ferrari en 1540 quien resolvió la ecuación de cuarto grado y este resultado también fue publicado en Ars Magna en 1545.

4. La ecuación de grado quinto

Es en el trabajo de Paolo Ruffini (1765–1822) donde se encuentra una prueba casi completa de que las ecuaciones generales de quinto grado en adelante no podían resolverse por radicales (1799).

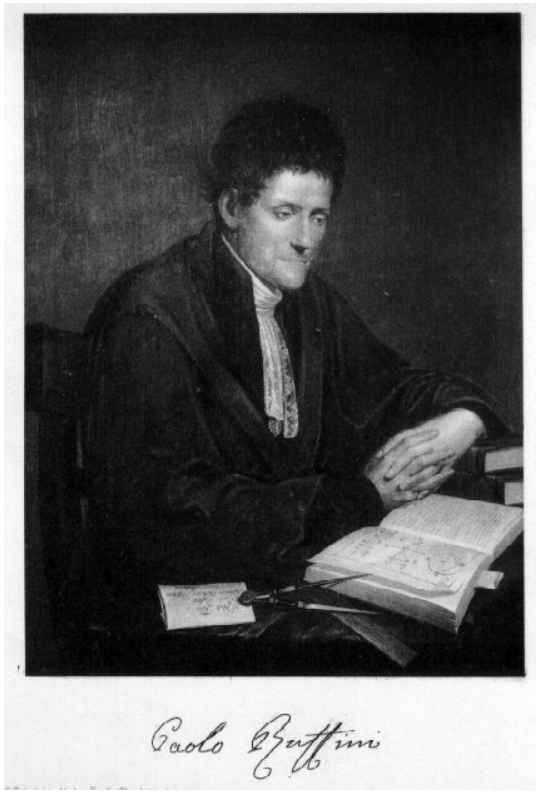
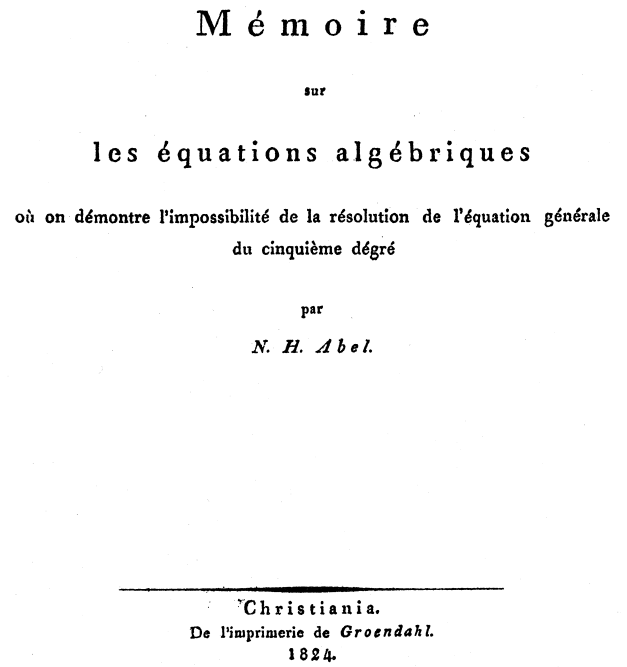


Figura 8: Tomada de
http://upload.wikimedia.org/wikipedia/commons/2/22/Ruffini_paolo.jpg

Ruffini usó teoría de grupos pero todo lo que usaba tenía que ser inventado y desarrollado por él mismo. Lagrange había usado permutaciones y se puede argumentar que ya los grupos habían aparecido en

el trabajo de Lagrange, sin embargo Lagrange nunca compuso permutaciones, por lo que no podemos decir que la teoría que usó Lagrange se pueda considerar totalmente como teoría de grupos. Ruffini fue el primero en introducir la noción de orden de un elemento, conjugación, la descomposición cíclica de elementos de los grupos de permutaciones y las nociones de primitividad e imprimitividad. También probó, entre otras cosas, que el orden de una permutación es el mínimo común múltiplo de las longitudes en la descomposición en ciclos disjuntos y que S_5 no tiene subgrupos de índice 3, 4 u 8.

En 1824 Niels Henrik Abel (1802–1829) publicó su demostración sobre la irresolubilidad de la ecuación de grado 5 [**1**] lo cual había obtenido en 1823. Puesto que no tenía dinero, Abel tuvo que presentar su resultado en únicamente 6 páginas y resultó ser muy obscuro y de forma difícil de leer. Una prueba más detallada la publicó en 1826 en el *Journal de Crelle* (*Journal für die reine und angewandte Mathematik*) [**2**]. Este artículo fue conocido por Galois pocos meses después de la muerte de Abel.



M é m o i r e

sur

les équations algébriques

où on démontre l'impossibilité de la résolution de l'équation générale du cinquième dégré

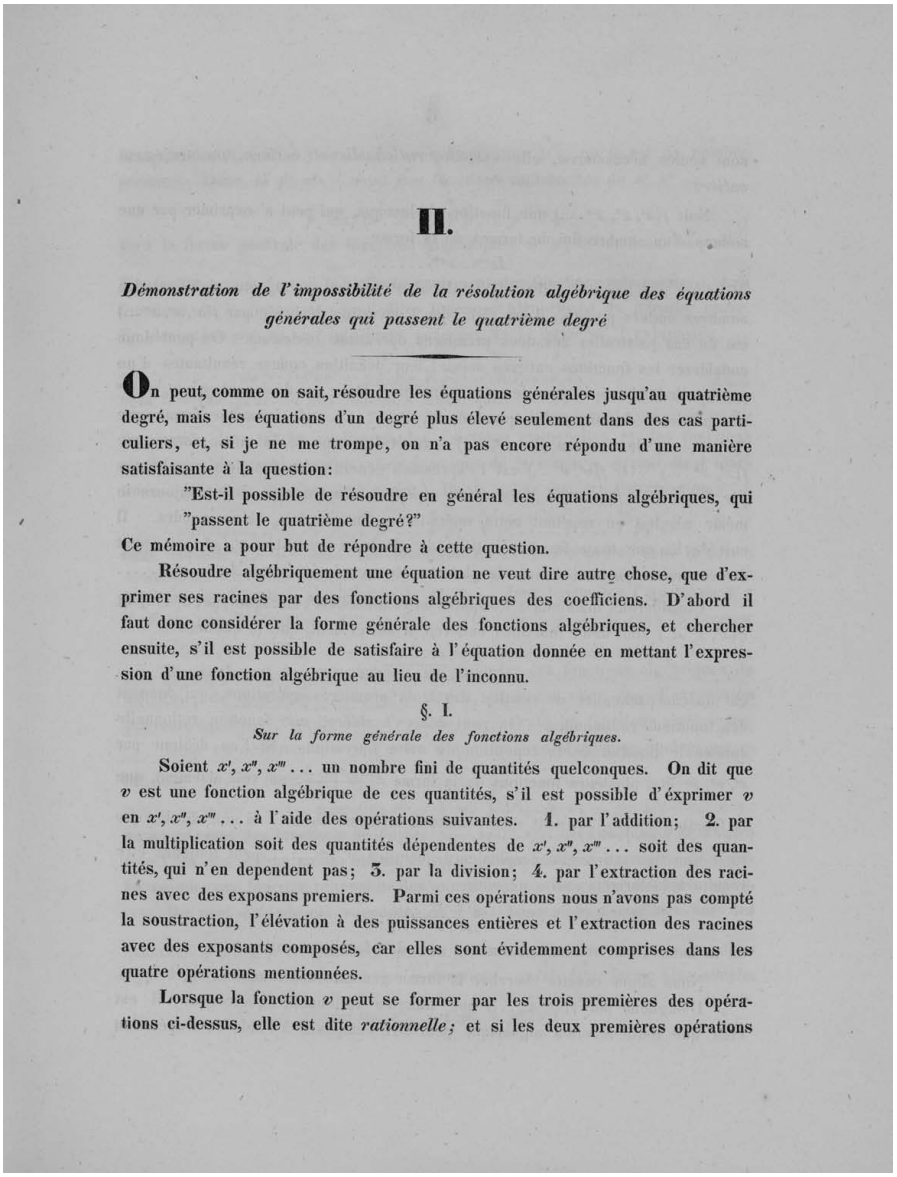
par

N. H. Abel.

Christiania.
De l'imprimerie de *Groendahl.*
1824.

Figura 9: Versión de 1824 del teorema de Abel, publicada por él mismo. Tomada de

`http://www.abelprisen.no/nedlastning/verker/1824_abel_memoir.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''' ... un nombre fini de quantités quelconques. On dit que v est une fonction algébrique de ces quantités, s'il est possible d'éxprimer v en x', x'', x''' ... à l'aide des opérations suivantes. 1. par l'addition; 2. par la multiplication soit des quantités dépendentes de x', x'', x''' ... 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

Figura 10: Publicado en *Journal für die reine und angewandte Mathematik* **1**, 1826. Tomada de

`http://www.abelprisen.no/verker/oeuvres_1839/oeuvres_completes_de_abel_1_kap02_opt.pdf`

5. El teorema de Galois

Como mencionamos antes, la noche previa a su duelo, o presunto duelo, no lo sabemos de cierto, Galois escribió parte de su trabajo en una carta enviada a Auguste Chevalier, en la cual incluyó un resumen del

manuscrito rechazado por la Academia y Poisson. Esta carta, junto con el manuscrito antes mencionado, es el gran legado de Galois. Es importante hacer notar que este trabajo de Galois está influenciado y motivado por trabajos de Lagrange, Ruffini y Abel. El trabajo de Lagrange sobre polinomios simétricos, es decir polinomios $p(x_1, \ldots, x_n)$ tales que para toda $\sigma \in S_n$, se tiene

$$\sigma(p(x_1, \ldots, x_n)) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = p(x_1, \ldots, x_n),$$

fue utilizado por Ruffini que usó los resultados de Lagrange para probar que en el caso en que $g(x_1, x_2, x_3, x_4, x_5)$ es un polinomio y $f(x_1, x_2, x_3, x_4, x_5) = g(x_1, x_2, x_3, x_4, x_5)^m$ para $m \in \mathbb{N}$, entonces si

$$f(x_1, x_2, x_3, x_4, x_5) = f(x_2, x_3, x_1, x_4, x_5) = f(x_1, x_2, x_4, x_5, x_3)$$

se tiene que g satisface las mismas igualdades. Notemos que en términos modernos, las igualdades satisfechas por el polinomio f son que $\tau(f) = \sigma(f) = f$ donde $\tau = (1, 2, 3)$ y $\sigma = (3, 4, 5)$, $\tau, \sigma \in A_5$. Se tiene que $\langle \tau, \sigma \rangle = A_5$.

Con este resultado, si la ecuación de quinto grado pudiese ser resuelta por radicales, entonces por lo descrito en el trabajo de Lagrange, la fórmula de la solución se obtiene, al principio con polinomios simétricos y a través de ellos determinando, paso por paso, polinomios $g_1, g_2, \ldots$ tales que para cada uno de ellos, una potencia puede ser determinada por los polinomios en el paso previo usando las 4 operaciones elementales (suma, resta, producto y cociente). El paso i–ésimo tiene la forma

$$g_i(x_1, x_2, \ldots)^{m_i} = f_i(x_1, x_2, \ldots),$$

donde f_i es expresado únicamente en términos de los polinomios $g_1, \ldots, g_{i-1}$ determinados en los pasos previos. Por tanto, aplicando el argumento de Ruffini de manera inductiva, se deduce que g_i satisface

$$g_i(x_1, x_2, x_3, x_4, x_5) = g_i(x_2, x_3, x_1, x_4, x_5) = g_i(x_1, x_2, x_4, x_5, x_3)$$

y por tanto todo polinomio en 5 variables satisfacen esta relación, lo cual es evidentemente absurdo: por ejemplo $h(x_1, x_2, x_3, x_4, x_5) = x_1$ no lo hace.

Como podemos apreciar, Ruffini no estaba nada lejos de una demostración completa de la imposibilidad de resolver por medio de radicales todas las ecuaciones polinomiales de quinto grado.

No cabe la menor duda de que Galois estuvo influenciado fuertemente por Abel, el cual fue el primero en dar una demostración completa sobre la irresolubilidad de la ecuación general de grado $n \geq 5$.

A diferencia del trabajo de Abel, Galois da una solución completa sobre exactamente qué ecuaciones son solubles por radicales. Actualmente, el teorema de Galois se enuncia de la siguiente forma.

Teorema 5.1 (Galois) *Sea $f(x) \in K[x]$ un polinomio separable e irreducible de grado n, K un campo cualquiera y L el campo de descomposición de f sobre K. Sea $G = \mathrm{Gal}(L/K)$. Entonces f es soluble por radicales si y sólo si G es un grupo soluble.*

Recordemos que un grupo G se llame *soluble* si existe una filtración $\{1\} \subseteq H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = G$ de subgrupos de G tales que cada grupo H_i es normal en H_{i+1}, $0 \leq i \leq n-1$ y H_{i+1}/H_i es un grupo abeliano de orden un número primo.

Observación 5.2 *Si $\mathrm{car}\, K = p > 0$ y $p \mid |G|$, entonces, puesto que en este caso la extensión $K(\sqrt[p]{a})/K$ no es separable, en lugar de entender por una raíz p–ésima de a a $\sqrt[p]{a}$, debe entenderse a una solución de la ecuación de Artin–Schreier: $x^p - x = a$.*

La ecuación general de grado n tiene como grupo S_n, el cual no es soluble para $n \geq 5$ (y si lo es para $1 \leq n \leq 4$).

6. La carta de Galois a Auguste Chevalier

La noche del 29 de mayo de 1832, la anterior al duelo, Galois escribió su famosa carta a Chevalier, describiendo en líneas generales sus descubrimientos. En esta carta Galois esbozó la conexión entre grupos y ecuaciones polinomiales. Pero esto no es todo, también menciona muchas otras ideas, acerca de funciones elípticas e integración de funciones algebraicas y otras cosas demasiado crípticas para ser identificables.

La carta empieza:

> Mi querido amigo. He hecho algunos nuevos descubrimientos en el campo del análisis matemático.

Además agregó un breve resumen de la memoria que había depositado en la Academia conteniendo lo que ahora conocemos como la *teoría de Galois* agregando algunos teoremas nuevos y conjeturas en 8 páginas manuscritas.

Galois concluye:

> No tengo tiempo y mis ideas no están suficientemente desarrolladas en esta área, la cual es enorme.

Agrega la siguiente petición:

> Pide a Jacobi o a Gauss, en público, dar su opinión, no sobre la veracidad, sino de la importancia de estos teoremas"

El documento es patético en más de una forma. Por ejemplo, está garabateado un comentario al margen que dice

> No tengo tiempo.

En el documento enviado a la Academia se tienen las siguientes afirmaciones:

> Hice varias cosas en análisis. Algunas de ellas acerca de la teoría de ecuaciones, otras acerca de integrales de funciones algebraicas.
>
> Sobre la teoría de ecuaciones, he tratado de averiguar bajo qué circunstancias las ecuaciones son solubles por radicales, lo cual me dio la oportunidad de investigarlas a fondo, y describir todas las posibles transformaciones de una ecuación, aún en el caso de que no sea soluble por radicales.
>
> Con este material podré escribir tres memorias.

En la carta a Chevalier usa las nociones de campos y extensiones sin definirlos ni denotarlas con algún nombre específico.

También es la primera vez que se considera al conjunto de sustituciones (concepto acuñado por Cauchy) cerrado con respecto al producto y se le llama *grupo* con un significado diferente a *conjunto*.

En el documento también aparece lo siguiente:

> ... cuando un grupo G contiene otro grupo H, el grupo G puede ser dividido entre grupos cada uno de ellos obtenido operando una misma sustitución sobre las permutaciones de H, de tal forma que
>
> $$G = H + HS + HS' + \cdots$$
>
> y puede ser descompuesto entre grupos teniendo la misma sustitución de tal forma que
>
> $$G = H + TH + T'H + \cdots$$
>
> En la mayoría de los casos estas descomposiciones no coinciden. Cuando ellas sí coinciden, la descomposición se llama propia.

Esta definición no es otra de que H *es normal en* G.
Uno de los resultados presentados es:

Teorema 6.1 *Para que una ecuación de grado primo p sea soluble por radicales, es necesario y suficientemente que una vez que dos de sus raíces son conocidas, las otras pueden deducirse de ellas racionalmente.*

Notemos que Galois no dice *irreducible*. Suponemos que Galois percibía que si una ecuación era reducible, su grupo sería no transitivo y sus raíces serían divididas en varios sistemas transitivos, correspondiendo a los factores irreducibles de la ecuación. Por tanto Galois se podría limitar a tener en consideración ecuaciones irreducibles sin mencionarlo explícitamente. Con esto en mente, su resultado puede ser reescrito de la siguiente forma:

Teorema 6.2 *Un polinomio irreducible $f(x)$ de grado primo es soluble por radicales si y solamente si para cualesquiera dos raíces α y β de f, el campo de descomposición de f es $K(\alpha, \beta)$.*

Hay material que únicamente se encuentra en la carta a Chevalier y en ningún otro manuscrito conocido. Por ejemplo lo referente a los períodos de una integral abeliana relativa a una función algebraica.

7. La herencia de Galois

Actualmente tenemos tres puntos de vista algo diferentes de cómo abordar la teoría de Galois:

- Como se dio originalmente, esto es, por medio de ecuaciones polinomiales, estudiando los grupos de Galois como grupos de permutaciones de las raíces del polinomio.

- El punto de vista "moderno" basado en estructuras algebraicas abstractas: grupos, campos, etc. Este punto de vista es más fácil de entender y estudiar, a pesar de la abstracción que se requiere para abordarlo.

- El punto de vista de Emil Artin. Este punto de vista está basado en el siguiente resultado: Si L es cualquier campo y G es un grupo finito de automorfismos de L, esto es, $\sigma\colon L \to L$ para todo $\sigma \in G$, entonces si $K^G := \{\alpha \in K \mid \sigma(\alpha) = \alpha \ \forall\ \sigma \in G\}$, se tiene que $[L : K] = |G|$.

El punto de vista de Artin es, desde mi muy personal punto de vista, la forma más elegante y eficiente de ver la teoría elemental de Galois.

En la actualidad hay innumerables teorías relacionadas con la teoría de Galois o con el nombre de Galois. Por ejemplo, si tenemos un objeto X relacionado con un cierto campo L de tal forma que el grupo de Galois $G = \mathrm{Gal}(L/K)$ de una extensión L/K actúa en X, se dice que la acción de G en X es de *Galois* o *galoisiana*.

En este orden de ideas, si la acción de G en X da lugar a grupos de cohomología, hablaremos de *cohomología de Galois*.

El problema abierto que en general se considera como el más difícil, es el llamado *problema inverso de la teoría de Galois*. El problema fue establecido inicialmente por Emmy Noether en los años treinta y consiste de la siguiente pregunta:

> *Dado un grupo finito G, ¿existe un campo numérico K que sea una extensión de Galois sobre $\mathbb{Q}$ y tal que $G \cong \mathrm{Gal}(K/\mathbb{Q})$?*

Este problema se generaliza de innumerables formas: a campos de funciones, con diversos campos de constantes, a la exacta realización de un grupo finito como el grupo completo de automorfismos de un campo de funciones $\mathrm{Aut}_k(K)$, etc.

Otra teoría relacionada con Galois es la llamada *teoría de cogalois*. La teoría de Galois es una correspondencia inversa entre la red de subgrupos de un grupo de Galois $G = \mathrm{Gal}(L/K)$ y la red de subcampos $K \subseteq E \subseteq L$ y la teoría de cogalois da una correspondencia directa entre los subgrupos de algún subgrupo

$$G \subseteq \mathrm{cog}(L/K) = T(L/K)/K^*,$$
$$T(L/K) := \{\alpha \in L^* \mid \alpha^m \in K \text{ para algún } m \in \mathbb{N}\}$$

y la red de subcampos $K \subseteq E \subseteq L$.

La teoría de cogalois está fuertemente relacionada con el estudio de las extensiones radicales de campos y por ende, es similar a la teoría de Galois en más de un sentido.

8. Los tres problemas griegos, Gauss y Galois

Desde la antigua Grecia, se habían planteado los siguientes tres problemas, ninguno de los cuales pudieron ser resueltos ni por ellos ni los

matemáticos posteriores. Fue hasta el siglo XIX que esos problemas fueron satisfactoriamente resueltos.

Los tres problemas a los que nos referimos fueron, es posible, usando únicamente regla y compás:

- ¿cuadrar un círculo?, esto es, dado un círculo, construir un cuadrado que tenga la misma área que el círculo dado;
- ¿trisectar un ángulo?, esto es, dado un ángulo, construir otro ángulo que sea la tercera parte del ángulo dado;
- ¿duplicar un cubo?, esto es, dado un cubo, construir otro cubo cuyo volumen sea el doble del cubo dado.

Notemos que para poder construir una figura geométrica o un número dado, a partir de un campo dado con regla y compás, necesitamos obtener, en un número finito de pasos, longitudes y segmentos de recta que se puedan dar mediante la intersección de circunferencias y rectas. Esto es equivalente a que podamos obtener la longitud del segmento deseado, o el punto dado en un campo que se pueda obtener mediante pasos de grado 1 (que no hicimos nada pero no nos dimos cuenta) o 2.

A finales del siglo XVIII (el 29 de marzo de 1796), el joven Karl Gauss (de 18 años) inicia su extraordinaria y única vida matemática construyendo, usando únicamente regla y compás, el polígono regular de 17 lados. No es este el lugar para describir los detalles de esta construcción, pero baste decir que $\zeta := \exp(2\pi i/17)$, la raíz décimo séptima de la unidad, satisface $\zeta^{17} = 1$, lo cual nos lleva a una ecuación de grado 16, esto es, se tiene:

$$P(\zeta) = 0, \quad \text{donde} \quad P(x) = \frac{x^{17} - 1}{x - 1} \in \mathbb{Q}[x].$$

Las 16 raíces forman un grupo cíclico y por ende, tiene subgrupos de índices 8, 4, y 2, los cuales nos indican que podemos ir haciendo construcciones cuadráticas hasta llegar al campo $\mathbb{Q}(\zeta)$ lo cual nos demuestra (más bien Gauss nos demostró) que ζ puede obtenerse en 4 pasos usando regla y compás.

De hecho, para construir el polígono regular de 17 lados se necesita construir el número

$$2\cos\frac{2\pi}{17} = -\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{34 - 2\sqrt{17}} + \frac{1}{4}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

Esto no se puede hacer con el héptagono (7 lados) regular, pues el grupo cíclico que obtenemos es de orden 6 y no podemos ir de 2 en 2. Similarmente, para el polígono regular de 9 lados, en el primer paso obtenemos la raíz cúbica de la unidad $\zeta_3 = \exp(2\pi i/3) = \frac{-1+\sqrt{-3}}{2}$ que es constructible pues es equivalente a obtener $\sqrt{-3}$. Sin embargo, en el segundo paso necesitamos construir $\zeta_9 := \exp(2\pi i/9)$, la raíz cúbica de ζ_3, el cual es un paso de grado 3 y por lo tanto no lo podemos hacer por medio de regla y compás. En otras palabras, para el polígono regular de 9 lados obtenemos nuevamente el grupo cíclico de orden 6 y no podemos ir de 2 en 2.

Estas ideas son las que nos llevan al teorema que nos determina que podemos y que no podemos construir, a partir de los racionales, usando únicamente regla y compás.

Teorema 8.1 *Un número α puede construirse con regla y compás si y solamente si $\mathbb{Q}(\alpha)$ es una extensión finita de $\mathbb{Q}$ tal que el grupo de Galois de la cerradura normal $K/\mathbb{Q}$ de $\mathbb{Q}(\alpha)/\mathbb{Q}$ es de orden una potencia de 2.*

Observación 8.2 *No basta que $\mathbb{Q}(\alpha)$ sea de grado una potencia de 2 sobre $\mathbb{Q}$ para que α sea constructible con regla y compás. Por ejemplo, si damos α tal que si K es la cerradura normal de $\mathbb{Q}(\alpha)/\mathbb{Q}$ satisface que $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$, el grupo alternante de 12 elementos, entonces α no es constructible a pesar de que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = 2^2$.*

Como corolario, tenemos que

Corolario 8.3 *Un polígono regular de n lados es constructible usando regla y compás si y solamente si $n = 2^m p_1 \cdots p_r$ donde $m, r \in \mathbb{N} \cup \{0\}$ y $p_1, \ldots, p_r$ son primos de Fermat* distintos.

Un primo p se llama *primo de Fermat* si $p = 2^{2^t} + 1$ para algún $t \in \mathbb{N} \cup \{0\}$.

Usando el teorema anterior, la teoría de Galois es usada para resolver los tres problemas griegos que fueron contestados hasta el siglo XIX.

Las respuestas a los problemas griegos son:

- No es posible cuadrar un círculo de radio 1 pues para hacerlo, necesitamos construir $\sqrt{\pi}$ el cual es transcendente (Ferdinand Lindemann (1852–1939) en 1882).

- No es posible trisectar el ángulo de 60 grados. Se tiene que $\alpha = \cos 20^\circ$ satisface la ecuación $8x^3 - 6x - 1$ que es irreducible de grado 3.

- No se puede duplicar el cubo, pues $\beta = \sqrt[3]{2}$ satisface el polinomio irreducible $x^3 - 2$.

Bibliografía

1. N. H. Abel, *Mémoire sur les équations algébriques, oú on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré*, Brochure imprimée chez Grøndahl, 1824.
2. _____, Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré, *Journal für die reine und angewandte Mathematik* **1** (1926) 1.
3. A. Chevalier, Nécrologie, *Révue Encyclopédique* **55** (1832) 744–754.
4. P. de la red, *Abel–Ruffini theorem - Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Abel–Ruffini_theorem.
5. _____, *Abel biography*, http://www-groups.dcs/st-and.ac.uk/ history/Biographies/Abel.html.
6. _____, *Ars Magna (Gerolamo Cardano) - Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Ars_Magna_(Gerolamo_Cardano).
7. _____, *BBC - h2g2 - Evariste Galois - Mathematical Genius*, http://www.bbc.co.uk/dna/h2g2/A679629.
8. _____, *Disputas Matemáticas En el Siglo XVI Tartaglia Cardano Del Ferro*, http://www.portalplanetasedna.com.ar/ disputas_matematicas.htm.
9. _____, *Evariste Galois*, http://www.evariste-galois.net.
10. _____, *Evariste Galois*, http://www.terabitcorp.com/galois.htm.
11. _____, *Évariste Galois - Wikipedia, la enciclopedia libre*, http://es.wikipedia.org/wiki/Évariste_Galois.
12. _____, *Galois biography*, http://www-history.mcs.st-andrews.ac.uk/ Biographies/Galois.html.
13. _____, *Galois, Évariste (1811-1832) – from Eric Weisstein's World of Scientific Biography*, http://scienceworld.wolfram.com/ biography/Galois.html.
14. _____, *Galois last letter neverendingbooks*, http://www.neverendingbooks.org/index.php/galois-last-letter.html.
15. _____, *Lodovico Ferrari - Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Lodovico_Ferrari.
16. _____, *Los Grandes Matemáticos*, http://www.librosmaravillosos.com/ grandesmatematicos/capitulo20.html.

17. _____, *Niels Henrik Abel - Wikipedia, la enciclopedia libre*, http://es.wikipedia.org/wiki/Niels_Henrik_Abel.
18. _____, *Niels Henrik Abel - Wikipedia, la enciclopedia libre*, http://www.abelprisen.no/no/.
19. _____, *Œuvres_mathématiques_d'Évariste_Galois (open library)s*, http://openlibrary.org/books/OL6975080M/Œuvres_mathématiques_d'Évariste_Galois.
20. _____, *Paolo Ruffini - Wikipedia, la enciclopedia libre*, http://es.wikipedia.org/wiki/Paolo_Ruffinil.
21. _____, *Paolo Ruffini - Wikipedia, la enciclopedia libre*, http://es.wikipedia.org/wiki/Paolo_Ruffini.
22. _____, *Rafael Bombelli - Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Rafael_Bombelli.
23. _____, *Recherche et téléchargement d'archives de revues mathématiques numérisées*, http://archive.numdam.org.
24. _____, *Tartaglia versus Cardan*, http://www-history.mcs.st-and.ac.uk/HistTopics/Tartaglia_v_Cardan.html.
25. _____, *Theory of Ambiguity Log24*, http://m759.net/wordpress/?p=8451.
26. _____, *video en youtube*, http://www.youtube.com/watch?v=WRhFW6p832o.
27. E. Galois, *Lettre de Galois à M. Auguste Chevalier*, Insérée en 1832 dans la Revue encyclopédique.
28. _____, *Galois, Évariste, Œuvres Mathématiques*, Journal de Liouville, 1846.
29. L. Infield, *Whom the Gods Love: The Story of Evariste Galois*, Whittlesey House, New York, 1948.
30. _____, *El Elegido de los Dioses*, Siglo XXI, 1978.
31. M. Livio, *The Equation That Couldn't Be Solved*, Simon & Schuster Paperbacks, 2005.
32. H. Maser, *Abhandlungen über die Algebraische Auflösung der Gleichungen von N. H. Abel und E. Galois*, Berlin, Verlag von Julius Springer, 1889.
33. J. Pierpont, Early history of galois' theory of equations, *Bull. Amer. Math. Soc.* **4** (1898) 332–340.
34. T. Rothman, Genius and biographers: the fictionalization of evariste galois, *American Mathematical Monthly* **89** (1982) 84–106.
35. I. Stewart, *Galois Theory*, Chapman and Hall, 1973.
36. R. Taton, Sur les relations scientifiques d'augustin cauchy et d'evariste galois, *Revue d'histoire des sciences* **24** (1971) 123–148.
37. L. Toti Rigatelli, *Evariste Galois 1811-1832*, Birkhäuser, 1996.