GAUSS Y EL ALGEBRA DE SU TIEMPO

IGNACIO SOLS LUCIA

Catedrático de la Universidad Complutense

I. VIDA Y OBRA DE GAUSS

Johann Friedrich Carl Gauss nace de humilde familia el 30 de Abril de 1777 en la pequeña ciudad alemana de Brunswick. Fue un talento precoz. A los 12 años, concibió sus ideas sobre la distribución de los números primos y sobre la media aritmético-geométrica de dos números, lo que inspiró más tarde su estudio de las integrales elípticas, en lo que pudiéramos llamar albores de la geometría algebraica.

En el período de 1792-1795 estudia en el colegio carolino de Brunswick donde, al ser instruido en los elementos de Euclides, concibe la idea de las geometrías no euclídeas. Finalizado este período, decide consagrarse a las matemáticas más bien que a la filología al demostrar la constructibilidad por regla y compás del polinomio regular de 17 lados, del cual pensaban los griegos - y también Fermat y Euler - que era inconstructible (cfr. anexo II).

Siempre apoyado por el príncipe Fernando de Brunswick elige Göttingen para sus tres años universitarios 1796-1798, especialmente por su buena biblioteca. Prácticamente sin profesores, ni exámenes, ni obligación de asistir a clase, desarrolló su creatividad en solitario o en largos paseos silenciosos, a veces con su amigo Wolfgang Bolyai, sin otro testigo de este período que las eventuales entradas en su famoso diario matemático (1796-1814), descubierto en 1898. Tesis doctoral: el teorema fundamental del algebra (1799). Vuelto a Brunswick en ese mismo año, redacta las principales ideas concebidas en aquel período en sus Disquisitiones Arithmeticae, cuya publicación en 1801 e inmediata traducción al francés le valen una temprana reputación de genialidad.

En las disquisiciones: Teoría de la divisibilidad y estudio del número de enteros menores que un número y primos con él; Primera demostración correcta de la ley de reciprocidad cuadrática entre números primos p, q. En símbolos de Legendre

$$\left(\frac{p}{q}\right) = \left\{\begin{matrix} 1 \text{ si existe un entero } x \text{ tal que } x^2 \equiv q \ (mod\, p\,) \\ -1 \text{ en caso contrario} \end{matrix}\right\}$$

la ley expresa que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ (Esta ley fue previamente enunciada y discutida por Euler y Legendre); Estudio de formas binarias $ax^2 + bxy + cy^2$, así como de formas ternarias. Solución de ecuaciones diofánticas de 2º grado con dos incógnitas y teoremas de tipo Fermat, como el que afirma que todo número primo congruente con 1, módulo 4, es suma de cuadrados de modo único, y que todo número es suma de tres números triangulares (o sea, del tipo $\frac{1}{2}n\ (n+1)$). Por último el más famoso capítulo VII es de contenido algebraico: resolución de la ecuación ciclotómica y constructibilidad de polígonos regulares por regla y compás (anexo II).

Diciembre de 1801. El planetoide Ceres recién hallado y perdido luego tras el sol no reaparece donde lo esperaban los astrónomos de la época sino donde lo predicen los cálculos del joven Gauss. Consiguiente popularidad e inicio de una carrera de astrónomo, de momento con las escasas posibilidades de su ciudad natal. No se decide a dejar Brunswick a pesar de las invitaciones de universidades y observatorios de otras ciudades y países. Siguen años de interminables observaciones y cálculos: "Lieber der Tod als ein solches Leben" escribió al margen de un borrador en su investigación de la órbita de Palas.

En 1809 publicará su celebrada memoria de más de trescientas páginas "Theoria Motus corporum coelestium in sectionibus conicis Solem ambientium". Expone en esta memoria las técnicas por él introducidas en astronomía y en particular la ley de cuadrados mínimos que Gauss había utilizado antes de enunciarla Legendre: La suma de los cuadrados de los errores, es decir de las diferencias entre los valores calculados y los valores observados debe ser mínima. Esta ley será objeto más tarde de una monografía "Theoria combinationis observationum erroribus minimis obnoxiae" (1823) en la que introduce su famosa distribución normal $\exp\left(-\frac{1}{x^2}\right)$ como la más natural distribución en que acontecen los errores (campana de Gauss). Al desarrollar en serie trigonomética las perturbaciones de algunas órbitas planetarias se adelanta en este tipo de desarrollo al mismo Fourier (o al menos, a su tardía publicación).

Durante sus años de astrónomo en Brunswick y luego en Göttingen publicará (o dejará en fragmentos) importantes hallazgos aritméticos que hubieran constituido, de hallarse menos ocupado, su anhelada prolongación de las Disquisiciones: segunda demostración (algebraica) del teorema fundamental del Algebra (anexo I); irreducibilidad de $x^3 + y^3 + z^3$, algoritmo de división - y consecuente factorialidad - de $Q\left[\sqrt{3}\ \right]$; teorema de Fermat para $n = 3, 5$.

Son años verdaderamente felices en que se casó muy enamorado con Johanna (1805), una muchacha de su vecindario, de la que nacen Joseph y Minna. En 1808, a los 31 años, vuelve definitivamente a Göttingen como director del laboratorio astronómico de la universidad, creado para él. El año siguiente es el más amargo de su vida: muere Johanna al alumbrar a su tercer hijo, quien muere meses después. Leemos en una hoja medio borrada por sus lágrimas: "Por favor, pide al Eterno - no podría negártelo - tan solo esto: que su bondad infinita permanezca siempre viva ante mi mente, para que también yo, pobre hombre, pueda esforzarme en seguirte a tí". Le preocupa el hogar que necesitan sus hijos y vuelve a casarse poco después con Minna, hija de un catedrático de derecho de Göttingen de la que nacerán Eugen, Wilhelm y Theresa.

En esos años (1808-1818), y entre innumerables cálculos de calendario y tablas astronómicas, no abandona la matemática pura, y es tiempo de excelentes ideas: se adelanta a Cauchy en su fórmula integral para demostrar una vez más el teorema fundamental del Algebra (1816): Si f no tuviese ceros, entonces $\frac{f'(z)}{f(z)}$ no tendría polos y contradictoriamente $f(0) = \frac{1}{2\pi i}\int_0 \frac{f'(z)}{f(z)}dz$ sería cero.

Un ensayo de Schlessinger en las obras completas de Gauss analiza su importante trabajo inédito en estos años, adelantándose al trabajo independiente de Abel y Jacobi en Berlín en el estudio de las integrales elípticas y funciones θ, semillas de la geometría algebraica. Recordemos que el pequeño Carl había concebido a los doce años - independientemente de Lagrange (1785) - la idea de la media aritmético-geométrica $M(n,m)$ de dos números n y m: Por media aritmética y por media geométrica de $n = n_1$ y $m = m_1$ se obtienen otros dos números n_2, m_2 y se itera el proceso siendo en el límite ambos n_∞ y m_∞ iguales a un mismo número $M(n, m)$. Para calcular la órbita de Pallas observa en su "Determinatio atractionis quam in punctum quodvis positionis datae exerceret planeta si eius massa per totam orbitam ratione temporis, quo singula partes describuntur, uniformiter esse dispertita" (1818) que $\frac{1}{M(1+x, 1-x)}$ coincide sorprendentemente con la integral elíptica $\frac{1}{n}\int \frac{d\varphi}{\sqrt{1-x^2\cos^2\varphi}}$ para cuya inversión usó Gauss por vez primera la función θ. Admirable resultó para Gauss esta inesperada irrupción de la aritmética en su musa Naturaleza para el cálculo de la longitud de elipses y otras órbitas. Las sumas de Gauss introducidas al final del cap. VII de las disquisiciones y discutidas en detalle en "Summatio quarundam serierum singularium" (1811) parecen indicar que ya al escribir sus disquisiciones conocía Gauss las funciones θ. Su función hipergeométrica $\pi(x)$ inspirará más tarde a Weierstrass la función $\Gamma(x)$; y sus definiciones y estudios fragmentarios e inéditos de las funciones modulares (en relación con la media aritmético-geométrica) y de los dominios fundamentales inspiraron la investigación posterior de Dedekind. Hoy son de ordinario uso en la teoría de moduli de la Geometría Algebraica.

En el periodo de 1818 hasta 1832 (¡mucho más largo de lo previsto!) vemos a Gauss geodesta, no limitándose a los cálculos de laboratorio, sino inventando también el heliotropo y sufriendo frío y sobre todo calor por los campos del reino de Hannover en el proyecto de su cartografía. Su mujer Minna padece una larga enfermedad hasta su muerte en 1831. Se añaden los problemas de los hijos, ya mayores. Ninguno de ellos es muy brillante. Joseph, que le había ayudado en el trabajo geodésico, puede colocarse al fin como ingeniero en el ferrocarril. Eugen, jugador empedernido a quien debe mostrar el rostro del padre severo, conlleva demasiados problemas y amarguras, hasta que - muy entrampado - debe emigrar a América, siguiéndole después Wilhelm, dedicado a los trabajos de granja (y sólo en América queda descendencia de Gauss en nuestros días). Aunque siguen escribiéndose, no volverá a verlos más.

Frutos de este trabajo geodésico: "Allgemeinste Auflösung des Problems der Abwickelung der Flächen" de 1822 donde introduce las ecuaciones llamadas de Cauchy-Riemann y el mapeo en geometría diferencial, así como al tratamiento de las aplicaciones conformes mediante el uso de la variable compleja; en 1827 publica su célebre y breve memoria "Disquisitiones generales circa superficies curvas" descubriendo su curvatura y geometría intrínsecas y el famoso teorema, - ampliado luego por Bonet - que relaciona la curvatura de una superficie con la suma de los ángulos de sus triángulos geodésicos. Finalmente, en 1829, publica su método geodésico en su trabajo "Bestimmung des Breitenunterschiedes zwischen den Sternwarten von Göttingen und Altona" prolongado más tarde en sus dos largas memorias "Untersuchungen über Gegenstände der höheren Geodäsie I, II" de 1844 y 1847, básicas en geodesia teórica y práctica.

Del profundo desánimo y pérdida del deseo de vivir tras la muerte de Minna le levantará en 1832 la llegada a Göttingen del joven físico Webber, único colaborador de Gauss. A los cincuenta y cinco años resucita pues Gauss como físico que debe cultivar y desarrollar la teoría del magnetismo por el encargo oficial de dirigir la búsqueda del polo magnético terrestre. Ya tres años antes, en 1829, había publicado "Über ein neues allgemeines Grundgesetz der Mechanik" sobre desplazamientos virtuales y el principio de ligaduras mínimas, así como sus "Principia generalia theoriae figurae fluidorum in statu aequilibrium" (1830), sobre el cálculo de variaciones y principios extremales, siendo su matematización rigurosa independiente del trabajo de Poisson. Desarrollando la teoría del potencial demuestra los teoremas de Green y de la divergencia, y explica cualitativa y cuantitativamente las fuerzas de capilaridad.

Este trabajo con Webber sobre magnetismo comprenderá desde la corrección por Gauss de las agujas de la brújula, e invención e instalación del primer telégrafo entre los laboratorios de Gauss y Webber, hasta el uso en "Intensitas vis magneticae terrestris ad mensuram absolutam revocata" (1841) del posteriormente llamado principio de Dirichlet: una distribución de masas en un área determina unívocamente el potencial en cada punto del área.

Irreparable fue para Gauss la pérdida de Webber expulsado de Göttingen en 1838, al tiempo que su yerno y otros profesores, por motivos políticos. Publica Gauss entonces su memoria "Allgemeine Theorie des Erdmagnetismus" (1939) método que le llevó a predecir la situación del polo magnético precisamente donde el explorador Wilkes lo encuentra después en 1841. En 1840 demuestra rigurosamente la expresión del potencial en el interior de un cuerpo como 4π veces su densidad, que generalizará más tarde Einstein a la famosa ecuación de campo $G=8\pi T$ como base de la relatividad general. En este mismo año publica sus "Dioptrische Untersuchungen", investigaciones también por encargo y que mucho influyeron en la teoría óptica y en la industria óptica alemana.

A partir de ahora empiezan a ser frecuentes sus clases y comienza a formar alumnos de modo más o menos directo (entre ellos R. Dedekind); redacta también memorias atrasadas, como las antes aludidas sobre geodesia. Como recensionista activo alaba la obra sobre geometría no euclídea de Lobachevski pero poco encuentra ahí nuevo para él, como no lo encontró en la obra del hijo Janos de su amigo de juventud Bolyai, pues Gauss conocía estas geometrías desde los 14 años y las silenció "por temor al grito de los beocios".

Seis años de matemáticas del seguro, desde 1845, por encargo de la universidad de Göttingen, es la última aportación a la ciencia de este hombre honrado que entrega su espíritu en 1855 a los 78 años y medio, simpar científico que bajo el lema "pauca, sed matura" ha sido semilla e inspiración de las posteriores generaciones de matemáticos.

II. ECUACIONES ALGEBRAICAS EN LA EPOCA DE GAUSS

La tendencia de Gauss a trabajar en problemas concretos más bien que en marcos generales, lo ha configurado más como sembrador de semillas que como cosechador de frutos. El trabajo posterior de prosecución y generalización de las ideas iniciadas en su obra, en tantos campos de las matemáticas y de la física, ha correspondido pues a otros que en cierto modo cosecharon lo que él sembró. Podríamos seguir la pista a cada una de estas ideas seminales en muy variadas perspectivas históricas, lo cual requeriría una mayor cultura científica y mayor espacio que esta conferencia. Esta labor resulta pues más sencilla si nos restringimos a un campo, el Algebra, y más todavía a un problema, el que más parecía interesar a los algebristas de su tiempo: la resolución de ecuaciones algebraicas.

Un aspecto del problema era la demostración correcta de la existencia de raíces complejas de un polinomio de grado n. Ya se han comentado las circunstancias en que Gauss proveyó la primera y hasta tres demostraciones distintas a este fundacional teorema y ensayaremos en un anexo una aproximación a la lectura de la demostración más desconocida y de mayor interés para nosotros: la demostración algebraica.

El aspecto, sin embargo, que más interesaba a los algebristas del tiempo de Gauss era la obtención de las raíces de una ecuación como expresiones racionales de sus coeficientes envolviendo también radicales $\sqrt[n]{\ }$ y más en particular radicales cuadráticos $\sqrt{\ }$. En efecto, este último era el problema motivador pendiente desde la matemática helénica, pues equivalía al de constructibilidad geométrica - y en general solución de problemas geométricos - por regla y compás. Este es el tema que rastrearemos históricamente y al que dedicaremos los otros dos anexos: uno acerca del ensayo de Gauss sobre la ciclotomía o división de la circunferencia, y otro en torno a la memoria de Galois sobre resolubilidad de una ecuación por radicales. Veremos pues un mismo problema tratado en un caso particular - aunque ciertamente el más relevante: la construcción de polígonos regulares - y más tarde su aclaración final en la memoria de Evariste Galois. La consideración de esta memoria sería el término cabal de una perspectiva de futuro desde la obra de cualquier algebrista de la época anterior.

Los griegos dejaron irresueltas construcciones geométricas tales como la ciclotomía o la duplicación del cubo o la trisección de un ángulo, cuestiones que los matemáticos posteriores al renacimiento clásico acertaron a expresar como problemas de extracción de raíces de ecuaciones algebraicas. Era bien conocida la solución por radicales de las ecuaciones de grado 2, 3 y 4, y Edward Waring en "Miscellanea Analytica" (1762) y Alexandre Théophile Vandermonde, en "sur la resolution des equations" (1770) habían estudiado la ecuación ciclotómica $x^n-1 = 0$. Vandermonde la resuelve en el caso $n = 11$, y al mismo tiempo dilucida las conocidas soluciones de la ecuación general de grados 2,3,4 mediante una función lineal de las raíces $x_1, \dots, x_n$

$$\varphi = \lambda_1 x_1 + \dots + \lambda_n x_n$$

llamada "resolvente de Lagrange" (pero que al menos debe atribuirse a ambos autores de modo dependiente y simultáneo: a Vandermonde en 1770 y a Lagrange en 1771, en sus "Reflections sur la resolution algébrique des equations"): Se toman $\lambda_1, \dots, \lambda_n$ de modo que φ adquiera $n!$ valores distintos $\varphi_1, \dots, \varphi_{n!}$ al permutar $x_1, \dots, x_n$ (Por ejemplo, basta tomar como $\lambda_1, \dots, \lambda_n$ las raíces n-ésimas de la unidad). Esto permite escribir las raíces buscadas $x_1, \dots, x_n$ como funciones racionales de los valores $\varphi_1, \dots, \varphi_{n!}$ de φ, soluciones a su vez de la ecuación

$$(x - \varphi_1) \dots (x - \varphi_{n!}) = 0$$

Esta ecuación es de coeficientes simétricos en $x_1, \dots, x_n$, y por tanto es función racional de sus funciones simétricas elementales, es decir de los coeficientes de $f(x)$. No nos sirve como ecuación auxiliar pues su grado $n!$ es muy alto, pero una potencia $\alpha = \varphi^m$ podría reducir el número de valores hasta ser $< n$, obteniéndose α (y por tanto $\varphi = \sqrt[m]{\alpha}$) como solución de una ecuación auxiliar de grado inferior a n. Esto es factible para $n = 2, 3, 4$ y la ecuación ciclotómica $x^{11} - 1 = 0$, y se especulaba sobre la viabilidad del método en el caso general.

En cuanto a la ecuación general, Paolo Ruffini obtiene un resultado negativo en su "Teoría generale delle equazioni, in cui si dimostra imposibile la soluzione algebraica delle equazioni generale di grado superiore al quarto" (1789).Demuestra en realidad la irresolubilidad por radicales naturales, es decir, tales que son función racional de las raíces, como por ejemplo $\sqrt{b^2 - 4ac} = x_1 - x_2$ en el caso de la ecuación general de 2º grado $ax^2 + bx + c = 0$, o más en general el discriminante $\Delta = \Pi\,(x_i - x_j)$ en cualquier ecuación (Esto es sencillo de probar en términos debidos ya a Galois: Supuesta ya resuelta la ecuación, la expresión final de las raíces como función de los coeficientes, envolviendo estos radicales, varía obviamente con cualquier permutación de las raíces, y en particular con el ciclo

$$(1\,2\,3\,4\,5) = (1\,2\,3) \circ (1\,4\,5)$$

Por tanto, algún radical de la expresión deberá variar al efectuar esta permutación, quedando entonces multiplicado por una raíz quíntica de 1, si atendemos al primer miembro, y por el producto de dos raíces cúbicas, si atendemos al segundo miembro: contradicción.

En cuanto a la ecuación ciclotómica

$$0 = x^n - 1 = (x-1)\,(x^{n-1} + x^{n-2} + \dots + 1)$$

Carl Gauss, en el capítulo VII de sus Disquisitiones Arithmeticae (ver anexo II), reduce su resolución al caso en que n es primo y demuestra que si $n - 1 = \alpha\,.\,\beta\,.\,\gamma \dots$ entonces la resolución se reduce a la de ecuaciones auxiliares de grados $\alpha, \beta, \gamma, \dots$ que son resolubles por radicales mediante el método de la resolvente de Langrage, observación que es innecesaria en el caso más interesante en que $n - 1$ es una potencia de 2, y en el que se concluye la ciclotomía de la circunferencía por regla y compás. Apostilla Gauss: "Siempre que $n - 1$ encierra factores distintos de 2 se llega siempre a ecuaciones más elevadas (....) y NOSOTROS PODEMOS DEMOSTRAR CON TODO RIGOR QUE ESTAS ECUACIONES NO PUEDEN SER EVITADAS NI REBAJADAS EN GRADO, aunque los límites de esta Obra no nos permiten desarrollar aquí la demostración de esta verdad".

El trabajo del joven danés Niels Abel (1802-1829) está conectado con el de Ruffini y el de Gauss: En primer lugar objeta a Ruffini, en su "Démonstration de l'impossibilité de la résolution algébrique des equations genérales qui passent le 4^{me} degré" de 1826, que implícitamente había supuesto la naturalidad en todos los radicales. Completa, pues, el teorema de irresolubilidad de la ecuación general de grado ≥ 5, al probar que si ésta es resoluble por radicales, entonces lo es por radicales naturales.

En 1829 muere Abel con veintisiete años. Dos meses antes había escrito y enviado a publicación su "Mémoire sur une classe particulière d'equations resolubles algébriquement". En ella demuestra que si todas las raíces r_i de una ecuación son expresables como función $\varphi_i r$ de una raíz r de modo que $\varphi_i \varphi_j r = \varphi_j \varphi_i r$, entonces la ecuación es resoluble por radicales. En el lenguaje de Galois, esto significará que el grupo de la ecuación es abeliano, y será mejor que esperemos a aquel contexto para comprender la razón de este hecho.

En el año 1815, Cauchy había publicado en París su "Mémoire sur les nombres des valeurs qu'une fonction peut acquérir lorsqu'on y permute de tous les manières possibles les quantités qu'elle renferme". En ella estudia la relación entre los valores que toma una función de las raíces y el número de permutaciones que la dejan invariante, llegando así a la noción de índice, que veremos ocupar un lugar clave en la idea de Galois.

El genial matemático francés, muerto estúpidamente a los veinte años, tan solo se reconoció influido en su teoría - presentada a la Academia de París en 1929 y seguida de la "Mémoire sur les conditions de resolubilité des equations par radicaux" (1830) - por la obra de Lagrange, Ruffini, Gauss y Cauchy, pero en modo alguno por el trabajo de Abel de 1929 de quien, escribe, "desconocía hasta el nombre". Sin embargo esta es la concatenación lógica de la aportación de los tres jóvenes geniales: Gauss resuelve por radicales las ecuaciones de grupo cíclico; Abel resuelve las de grupo abeliano; y Galois resuelve las de grupo recursivamente abeliano, es decir, resoluble; y enuncia - dejando en esencia indemostrado, aunque en su marco adecuado - el teorema inverso.

Con Galois termina una línea de investigación en álgebra - y otras muchas se abren - cosechando en uno de tantos campos donde Gauss había sepultado su semilla.

ANEXO 1: LA DEMOSTRACION ALGEBRAICA DEL TEOREMA FUNDAMENTAL DEL ALGEBRA

Exponemos la "Demonstratio nova altera theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse" de 1816. Aunque algo extensa - veinticuatro páginas de los Gesammelte Werke -, esta prueba es la más interesante desde el punto de vista algebraico. Sin embargo, es la más desconocida de las tres, y si se trata de ella suele ser en forma simplificada - utilizando muy esencialmente el cuerpo de descomposición - perdiéndose así la línea argumental de Gauss. Mi propósito en este anexo es facilitar la lectura directa presentando el mismo discurso del autor, y reduciendo el uso de las raíces en el cuerpo de descomposición (construido posteriormente por Kronecker) a un mínimo esencial: tan sólo en unos lemas que el lector bien puede acotar y separar del resto del razonamiento para encontrar su demostración más larga - sin uso del cuerpo de descomposición - en el artículo original.

Teorema.- Todo polinomio $y(x) \in R[x] \leq C[x]$ posee al menos una raíz compleja, y por tanto descompone en $C[x]$ como $y(x) = \prod_{i=1}^{m} (x - a_i)$.

Obviamente el número complejo conjugado de una raíz también es raíz, por lo que el teorema es equivalente al enunciado en el título latino.

Demostración.- Supuesta la descomposición del enunciado (o en un cuerpo de descomposición) podríamos escribir

$$(y(x))^m = \prod_{i,j} (x - a_i)(x - a_j) = \prod_{i,j} (x^2 - (a_i + a_j)x + a_i a_j) = f(x^2, x)$$

si se denota por

$$f(u, x) = \prod_{i,j} (u - (a_i + a_j)x + a_i a_j)$$

el correspondiente polinomio "auxiliar" $f_x(u) = f(u, x) \in R[x, u]$. Los coeficientes de este polinomio son reales, porque son claramente función simétrica de las raíces a_i de $y(x)$, luego son función racional de sus funciones simétricas elementales, esto es de los coeficientes de $y(x)$. Podemos pues formar la función $f(u, x)$ independientemente de la suposición de existencia de raíces.

Esta es la inspiración de Gauss en su argumento: la forma lineal $(a_i + a_j)x + a_i a_j$ toma $m' = \frac{m(m-1)}{2}$ valores distintos al hacer variar $i, j = 1, \dots m$ y por tanto es solución de un polinomio, a saber $f(u, x)$ que tiene grado m' en u. Conocida esta solución, es decir, conocidos $a_i + a_j$ y $a_i a_j$ podemos deducir el par de raíces a_i, a_j *de* $y(x)$. Esto sigue siendo cierto si especializamos la variable x a un valor complejo $x_o \in C$, de tal modo que los valores $(a_i + a_j)x_o + a_i a_j$, o sea las raíces de $f(u, x_o) \in R[u]$ sean distintas, es decir de modo que el discriminante $\Delta f(u, x_o)$ sea no nulo. Probará Gauss en un lema que $\Delta f(u, x) \in R[x]$ es un polinomio no nulo y que por tanto puede escogerse x_o de esta forma. Al poseer "obviamente" solución las ecuaciones de grado impar, y al ser el contenido del 2 en m' (potencia del 2 en la descomposición factorial de m') inferior en una unidad al contenido del 2 en m, podemos suponer que $f(u, x_o) \in R[u]$ posee una raíz, luego también $y(x)$.

LEMA 1.- Todo polinomio es producto de polinomios separables (es decir sin raíces múltiples) y así pues, puede suponerse $y(x)$ separable en el enunciado del teorema.

LEMA 2.- Si $y(x)$ es separable, los polinomios $y(x)$, $\frac{dy}{dx}$ no tienen raíces en común.

LEMA 3.- El discriminante $\Delta f(u,x) \in C[x]$ es no nulo.
Dem: Usando las raíces a_i de f en el cuerpo de descomposición podemos escribir $\Delta f(x,u)$ como producto de todas las diferencias que se pueden formar entre los $(a_i + a_j)x - a_{ij}$. Si este producto fuera nulo, alguna de estas diferencias $[(a_i + a_j)x - a_{ij}] - [(a'_i + a'_j)x - a'_{ij}]$ sería idénticamente nula, concluyéndose que $a_i = a'_i$, $a_j = a'_j$, contra la separabilidad de $y(x)$.

Denotemos $x' = \dfrac{\partial f}{\partial x}$, $u' = \dfrac{\partial f}{\partial u}$ para el

LEMA 4.- En $C[u,x,w]$, el polinomio $f(u,x)$ divide a $f(u + wx', x - wu')$
Dem: Abreviemos $a_i + a_j$ como b_{ij}, y también $a_i a_j$ como c_{ij} . Ya que

$$x' = \frac{\partial}{\partial x}(u - b_{ij}x + c_{ij})\,Q_{ij} = -\,b_{ij}\,Q_{ij} + (u - b_{ij}x + c_{ij})\frac{\partial Q_{ij}}{\partial x}$$

$$u' = \frac{\partial}{\partial u}(u - b_{ij}x + c_{ij})\,Q_{ij} = Q_{ij} + (u - b_{ij}x + c_{ij})\frac{\partial Q_{ij}}{\partial u}$$

se tiene que $f(u + wx', x' - wf')$ es

$$\prod_{i,j}(u + wx' - b_{ij}x - b_{ij}wu' + c_{ij}) = \prod_{i,j}(u - b_{ij}x + c_{ij})\left(1 + w\frac{\partial Q}{\partial x} + b_{ij}\,w\frac{\partial Q}{\partial u}\right)$$

y por tanto contiene a $f(u,x)$ como factor.

Sea pues $x_o \in C$ tal que $\Delta f_{x_o}(u) \in C - \{0\}$. Como señalamos más arriba si μ es el contenido del 2 en el grado $m = 2^{\mu}K$ de $y(x)$, entonces μ - 1 es su contenido en el grado $\dfrac{m(m-1)}{2} = 2^{\mu-1}K'$ de $f_{x_o}(u)$. Sabemos que si este contenido es cero, es decir si $y(x)$ es de grado impar, entonces por fuerza tiene una solución real (conocido es que esta concesión a la intuición fue garantizada más tarde por demostración de Bolzano). Así pues, por inducción en el contenido μ del 2 en el grado de la ecuación podemos suponer que $f_{x_o}(u)$ posee una solución u_o , siendo por tanto $u'_o = \dfrac{\partial f}{\partial u}(x_o, u_o)$ no nulo, de modo que tiene sentido sustituir w por $\dfrac{x_o - x}{u'_o}$ en el polinomio nulo $f(u_o + w x'_o, x_o - w u'_o)$ de $C[w]$ obtenido al tomar valores x_o, u_o para x, u en el lema 1. Resulta entonces

$$f\left(u_o + \frac{x_o x'_o}{u'_o} - \frac{x x'_o}{u'_o}, x\right) = 0$$

Luego

$$u - \left(u_o + \frac{x_o x'_o}{u'_o} - \frac{x'_o}{u'_o}x\right) \text{ divide a } f_x(u)$$

de donde

$$x^2 + \left(\frac{x'_o}{u'_o}\right)x - \left(u_o + \frac{x_o x'_o}{u'_o}\right) \text{ divide a } f_x(x^2) = (y(x))^m$$

obteniéndose, pues, para $(y(x))^m$, y por tanto para $y(x)$, un par de raíces complejas.

ANEXO 2: LAS ECUACIONES QUE DETERMINAN LAS SECCIONES CIRCULARES

Este histórico ensayo de Gauss constituye el capítulo VII de sus famosas "Disquisitiones Arithmeticae", estudio prácticamente autónomo de la ecuación ciclotómica $x^n - 1 = 0$, que expresa la división de la circunferencia unidad en partes iguales, es decir la inscripción del polígono regular de n lados. Observando que el exponente n puede suponerse primo, demuestra Gauss que si n-1 $=\alpha\ \beta\ \gamma$... entonces puede resolverse la ecuación ciclotómica mediante la resolución de ecuacones auxiliares de menor grado α, β, γ, ... (que además prueba, al final, ser resolubles por radicales). En particular - y éste fue el problema motivador - si (p - 1) es una potencia de dos, entonces la ecuación puede resolverse por radicales cuadráticos, es decir que la construcción del polígono regular de p lados puede ser llevada a cabo geométricamente (mediante regla y compás). Estos son los números primos de tipo $p = 2^m + 1$ que presenta Gauss y que actualmente conocemos: 3, 5, 17, 157, 65537.

El planteamiento del capítulo está basado en investigaciones en previos capítulos sobre clases de restos, que son al principio recordadas.

Las p raíces del polinomio x^n-1 pueden expresarse como potencias $1, r, r^2, \dots, r^{p-1}$ de cualquiera de ellas (distinta de 1), y sus exponentes enteros pueden ser mejor comprendidos en (Z / p) - {0}, el producto de raíces correspondiendo entonces a la suma de exponentes en (Z / p). Las p-1 raíces $r, r^2, \dots, r^{n-1}$, denotadas por Gauss [1] [2]...[p-1], de

$$\frac{x^{p-1}}{x-1} = x^{p-1} + x^{p-2} + \dots + x + 1$$

corresponden pues al subconjunto (Z / p) - {0} formado por las clases de restos no nulas, el cual tiene la estructura multiplicativa de un grupo cíclico de orden p-1. Sea g un generador de este grupo (raíz primitiva), que aparece ahora reordenado cíclicamente así: $[1][g][g^2]\dots[g^{p-2}]$

Gauss ejemplifica en detalle, a lo largo del capítulo, el caso $p = 19$. La reordenación de las raíces de $x^{18} + x^{17} + ... + 1 = 0$ al tomar, por ejemplo, el $[2]$ como generador, es $[2^i]$, $i = 0, 1, ..., 18$:

$$1\ \underline{2}\ 4\ 8\ \underline{16}\ 13\ 7\ \underline{14}\ 9\ 18\ \underline{17}\ 15\ 11\ \underline{3}\ 6\ 12\ \underline{5}\ 10$$

Hemos omitido aquí los corchetes por brevedad y hemos subrayado los elementos del conjunto período $(f,\lambda) = (6,1)$, como ejemplo de la noción de conjunto período en λ de longitud f (siendo f un divisor de p -1 $= fe$), definido éste formalmente como el subconjunto

$$(f,\lambda) = [\lambda], [\lambda h], ..., [\lambda h^{f}],\ con\ h = g^{e},$$

(e informalmente como el subconjunto obtenido en la reordenación de arriba " desde λ, saltando de e en e").

Igualmente llama Gauss período y denota aún como (f,λ) a la suma de los elementos del conjunto período (f,λ), pues ello nunca da lugar a equívoco. La clave de la memoria de Gauss está en observar que el producto de dos períodos de igual longitud se puede expresar fácilmente como una suma de períodos de esa misma longitud, a saber:

$$(f,\lambda).(f.\mu) = (f,\lambda+\mu) + (f,\lambda'+\mu) + (f,\lambda''+\mu) + \ldots$$

donde $[\lambda]$, $[\lambda']$, ... son los elementos del conjunto (f,λ). Por su importancia y brevedad traducimos literalmente la demostración de Gauss:

"Sea como más arriba ρ -1 $= ef$, y sea g una raíz primitiva módulo ρ, y sea $h = g^{e}$. Se tendrá por lo que precede

$$(f,\lambda) = (f,\lambda h) = (f,\lambda h^{2}),\ \text{etc.} \ldots$$

El producto buscado será pues

$$[\mu].(f,\lambda) + [\mu h](f,\lambda h) + [\mu h^{2}](f,\lambda h^{2}) + \text{etc.},$$

y por tanto

$$\begin{gathered}[\lambda+\mu] + [\lambda h+\mu] + [\lambda h^{2}+\mu] + \ldots + [\lambda h^{f-1}+\mu] + \\ + [\lambda h+\mu h] + [\lambda h^{2}+\mu h] + [\lambda h^{3}+\mu h] + \ldots + [\lambda h^{f}\mu h] + \\ + [\lambda h^{2}+\mu h^{2}] + [\lambda h^{3}+\mu h^{2}] + [\lambda h^{4}+\mu h^{2}] + \ldots + [\lambda h^{f+1}+\mu h^{2}] + \text{etc.}\end{gathered}$$

Esta expresión contendrá en total f^{2} raíces, y si se toma separadamente la suma de cada columna vertical, se encuentra que la suma total es, como lo habíamos anunciado, igual a

$$(f,\lambda+\mu)+(f,\lambda h+\mu)+(f,\lambda h^{2}+\mu)+\ldots+(f,\lambda h^{f-1}+\mu);$$

Ahora bien, $\lambda' \equiv \lambda h$, $\lambda'' \equiv \lambda h^2$, etc. ..., módulo ρ, y por tanto

$$\lambda'+\mu \equiv \lambda h+\mu,\ \lambda''+\mu = \lambda h^{2}+\mu, \text{ etc. "}$$

Gauss aplica este teorema para la resolución de la ecuación ciclotómica siguiendo un método general que luego ilustra con dos ejemplos: $p=19$ y $p=17$. Por razones de brevedad expondremos el caso $p=19$ en cuya resolución late el espíritu del método general. Como $19-1=2\cdot3\cdot3$ el método de Gauss reducirá su resolución a la de ecuaciones auxiliares de grado 2 y 3.

De las definiciones se sigue la siguiente distribución del conjunto Ω de todas las raíces

$$\Omega=(18,1)\begin{cases}(6,1)\begin{cases}(2,1)= & [1],[18]\\(2,8)= & [8],[11]\\(2,7)= & [7],[12]\end{cases}\\[2ex](6,2)\begin{cases}(2,2)= & [2],[17]\\(2,16)= & [3],[16]\\(2,14)= & [5],[14]\end{cases}\\[2ex](6,4)\begin{cases}(2,4)= & [4],[15]\\(2,13)= & [6],[13]\\(2,9)= & [9],[10]\end{cases}\end{cases}$$

de las cuales conocemos las sumas

$$-1=(18,1)=(6,1)+(6,2)+(6,4)$$

$$(6,1)=(2,1)+(2,8)+(2,7);\text{ etc. ...}$$

$$(2,1)=[1]+[18];\text{ etc. ...}$$

y gracias al teorema conocemos también los productos, de modo que podemos formar las ecuaciones auxiliares de las cuales estos períodos son raíces, obteniendo así en particular los períodos $(1,\lambda)=[\lambda]$, es decir las raíces todas de la ecuación ciclotómica.

La ecuación que tiene por raíces $p=(6,1)$, $p'=(6,2)$, $p''=(6,4)$ es

$$0=(x-p)(x-p')(x-p'')=$$

$$=x^{3}-(p+p'+p'')x^{2}+(pp'+pp''+p'p'')x-pp'p''=x^{3}+x^{2}-6x-7$$

y al ser ésta de tercer grado podemos suponer conocidos estos tres períodos.

La ecuación cuyas raíces son $q = (2,1)$, $q' = (2,8)$, $q'' = (2,7)$ es

$$0 = x^3 - (q + q' + q'')x^2 + (qq' + qq'' + q'q'')x - qq'q'' =$$
$$= x^3 - (6,1)x^2 + ((6,1) + (6,4))x - (2 + (6,2))$$

luego podemos suponer conocidos estos períodos, y análogamente los períodos $q = (2,2), q' = (2,16), q'' = (2,14)$ y los períodos $q = (2,4), q' = (2,13)$, $q'' = (2,16)$.

Para terminar, [1] y [18] son las dos raíces de $x^2 - (2,1)x + 1 = 0$, y análogamente se hallan todas las demás raíces de la ecuación ciclotómica.

ANEXO 3: LA MEMORIA DE GALOIS SOBRE LAS CONDICIONES DE RESOLUBILIDAD DE ECUACIONES POR RADICALES

La famosa memoria de Evariste Galois "sobre las condiciones de resolubilidad de ecuaciones por radicales", aun siendo una de las piezas de literatura matemática más significativas jamás escritas, es a menudo desconocida por los matemáticos, o al menos, por nuestros estudiantes. La memoria resulta sin embargo asequible a cualquier alumno que conozca la teoría de Galois en su forma actual, con tal que no haya perdido en su aprendizaje un contacto mínimo con su formulación clásica; a este lector potencial pretendo facilitar su tarea con los comentarios que siguen.

PRINCIPIOS. En este párrafo introductorio, explica Galois lo que entiende por función racional de los coeficientes de una ecuación $f(x) = 0$ (Estos coeficientes pueden ser números o letras, de modo que la teoría estudia tanto ecuaciones particulares como generales). Se trata simplemente de un elemento arbitrario del cuerpo K al que se supone pertenecen los coeficientes del polinomio: $f(x) \in K[x]$. Una ampliación $K(\alpha) \geq K$ donde $\alpha^n = a \in K$, es decir $\alpha = \sqrt[n]{a}$, se llama ampliación de K por adjunción del radical α (llamado natural si α es función racional de las raíces $x_1, \dots, x_n$ de $f(x)$ es decir si $\alpha \in K(x_1, \dots, x_n)$).

Si después de un número finito de ampliaciones de este tipo, el cuerpo de coeficientes llega a contener a todas las raíces de f, decimos entonces que f es resoluble por radicales, es decir cuando existen $\alpha_1, \dots, \alpha_m$ tales que

$$K(x_1, \dots, x_n) \subseteq K(\alpha_1, \dots, \alpha_m) \text{ y } \alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1}),$$

(siendo pues $K(x_1, \dots, x_n) = K(\alpha_1, \dots, \alpha_m)$ la condición de resolubilidad por radicales naturales que Abel había demostrado ser equivalente).

Siguen cuatro lemas bien conocidos para nosotros:

I) Si un polinomio irreducible comparte una raíz con otro polinomio, necesariamente lo divide (en efecto: en caso contrario, ambos compartirían como factor común no trivial al polinomio mínimo de esta raíz).

II) Supongamos que $f(x) = 0$ es separable, es decir que no tiene raíces múltiples (esto puede suponerse y así lo hacemos en adelante, pues todo polinomio es fácilmente expresable como producto de separables). Puede encontrarse siempre una función lineal (resolvente de Lagrange) $V = a_1x_1 + \ldots + a_nx_n$, con coeficientes $a_i \in K$, de las raíces x_i de f, de tal modo asimétrica que las $n!$ distintas permutaciones de $x_1, \ldots, x_n$ dan lugar a $n!$ valores distintos de V.

Es obvio que si φ es función de una función racional ψ de las raíces $\varphi(\psi(x_1, \ldots, x_n))$, las permutaciones de las raíces que dejan a ψ invariante, también dejan invariante a φ. Lagrange observó en el artículo 100 de sus "Reflexions" que, recíprocamente siempre que esto ocurre, es φ función de ψ (en términos actuales: $K(x_1, \ldots, x_n)$, es ampliación normal de $k(\varphi)$ para todo $\varphi \in k(x_1, \ldots, x_n)$, es decir que $K(\varphi)$ es el cuerpo fijo del grupo Gal $(K(x_1, \ldots, x_n), K(\varphi))$ de automorfismos de $K(x_1, \ldots, x_n)$ que fijan $K(\varphi)$; ya que una extensión es normal si y solo si es obtenida por adjunción de todas las raíces de una ecuación). Así pues, de II) se obtiene el lema III): Toda raíz x_1 es de forma $f_1(V) \in K(V)$ es decir que $K(x_1, \ldots, x_n) = K(V)$ (teorema del elemento primitivo).

IV) Si además V' es conjugado de V (raíz con V de un mismo polinomio irreducible g) entonces $x'_i = f_i(V')$ es también raíz de la ecuación dada f (por tener $f(f_i(x)) = 0$ una raíz V en común con el polinomio irreducible g, tiene en común con g todas sus raíces: $V, V', V'', \ldots$).

Esta es la observación clave que permite a Galois asociar un grupo a la ecuación de f :

PROPOSICIONES I, II, III: Asociado a la ecuación f existe un grupo $G_f \leq \Sigma_n$ tal que una función $\varphi(x_1, \ldots, x_n) \in K(x_1, \ldots, x_n)$ de las raíces de f es función $\varphi \in K$ de los coeficientes de f si y solo si es invariante por las permutaciones de G_f entre las raíces $x_1, \ldots, x_n$.

En lenguaje moderno, al ser $K \subset K(x_1, \ldots, x_n)$ una extensión normal, el grupo $G_f = Gal(K(x_1, \ldots, x_n), K)$ de automorfismos de $K(x_1, \ldots, x_n)$ que fijan K tiene esta propiedad (que caracteriza al grupo G_f). Si $x_1 = \phi_1(V), \ldots, x_n = \phi_n(V)$ son las raíces de f, para un conjugado V' de V se obtiene una permutación $x'_1 = \phi_1(V'), \ldots, x'_n = \phi_n(V')$ de las raíces de f. Al considerar todos los conjugados $V, V', V'', \ldots$ de V, obtiene Galois un grupo de permutaciones que posee obviamente la propiedad requerida.

La proposición II, en términos actuales, afirma para $K \subseteq K' \subseteq K(x_1, \dots, x_n)$ la normalidad de $G_{f,K'} \subseteq G_{f,K}$ si $K' \supseteq K$ es ampliación normal. Se trata de la proposición principal pues Galois puede suponer sin mención explícita (gracias al trabajo de Gauss) que al adjuntar $\sqrt[p]{\alpha}$ al cuerpo de una ecuación se le han añadido previamente las raíces p-ésimas de la unidad 1, $\varepsilon, \dots, \varepsilon^{p-1}$ y por lo tanto la ampliación que se obtiene es la misma que al añadir todas las raíces de $x^p - \alpha = 0$, luego la reducción $G \supseteq G'$ es normal, siendo además p el índice de G' en G (lo que Galois tampoco demuestra). En consecuencia si la ecuación es resoluble por radicales se obtendrá (en el siguiente apartado) para el grupo $G = G_f$ una cadena

$$G \supseteq G_1 \supseteq, \dots, \supseteq G_n = 1$$

de reducciones normales acabando en la identidad, y siendo $(G_i / G_{i+1}) = p_i$: es decir que G_f es resoluble.

Basados en la elaboración posterior, pero aún en lenguaje fácilmente traducible al de Evariste Galois podríamos "susurrarle" al joven genial la siguiente demostración:

Recordemos que ya en su época, después de la primera memoria de Abel, se sabía que la resolubilidad por radicales es equivalente a la resolución por radicales naturales y éstos de orden primo. Supongamos pues que $G' \subseteq G$ es la reducción de G al adjuntar el radical natural $\alpha = \sqrt[p]{a}$ solución de $x^p - a$, donde $a \in K$. Sea ε una raíz primitiva p-ésima de 1, de modo que $\alpha_o = \alpha$, $\alpha_1 = \varepsilon\,\alpha$, $\alpha_2 = \varepsilon^2\alpha, \dots, \alpha_{p-1} = \varepsilon^{p-1}\alpha$ son todas las raíces p-ésimas de a, luego $K(\alpha) = K(\alpha_o, \dots, \alpha_{p-1})$. El grupo $G = Gal(K(x_1, \dots, x_n), K)$ actúa sobre el conjunto $\{\alpha_o, \dots, \alpha_{p-1}\}$ de raíces de $x^p - \alpha = 0$ y, al ser primo el número de elementos de este conjunto, actúa transitivamente, esto es con solo una órbita. Los estabilizados $G_i' = Gal(K(x_1, \dots, x_n), K(\alpha_i))$ de cada elemento α_i son pues una clase completa de subgrupos de G conjugados entre sí y, por ser $K(\alpha_i) = K(\alpha_o, \dots, \alpha_{p-1})$, todos ellos son iguales, es decir que $G_i' = G'$. Queda así probado que G' es normal y de índice igual al número p de elementos de la órbita, y por tanto primo.

¿Cuándo es una ecuación resoluble por radicales?

Expone su celebrada respuesta: cuando su grupo G_f es resoluble.

Habiendo ya tratado la parte directa al comentar las proposiciones anteriores, tratemos ahora de la parte recíproca, aclarando el razonamiento de Galois.

Supongamos que G_f admite un subgrupo normal H siendo G_f / H un grupo de orden primo p , y por tanto formado por las potencias de un solo elemento S , de modo que G_f es unión disjunta de subconjuntos (clases módulo H)

$$H \quad SH \quad S^2H \quad S^3H \dots \quad S^{p-1}H$$

Sea $\theta \in K(x_1, \dots, x_n)$ invariante por H y $\varepsilon \neq 1$ una raíz primitiva p-ésima de la unidad. La p-ésima potencia de la "resolvente de Lagrange"

$$\xi = \theta + \varepsilon \theta S + \varepsilon^2 \theta S^2 + \dots + \varepsilon^{p-1} \theta S^{p-1}$$

es invariante por G_f, y por tanto está en K, es decir que $\xi = \sqrt[p]{\lambda}$ con $\lambda \in$ K. En efecto, $\xi S = \varepsilon \xi$ implica que $\xi^p S = \varepsilon^p \xi^p = \xi^p$, y así pues ξ^p es invariante por S, luego por $S^2, S^3, \dots$ y por tanto lo es por G_f.

Si adjuntamos a K este radical $\xi = \sqrt[p]{\lambda}$, el grupo que obtenemos $Gal\,(K(x_1, \dots, x_n), K(\xi)) \subseteq G$ contiene a H, y por ser primo el índice de H coincide con él, de modo que el grupo de la ecuación se ha reducido a H.

Iterando el proceso, se deduce que si G es resoluble, la ecuación f es resoluble por adjunción de radicales.

****

La memoria de Galois termina con esta aplicación: Las ecuaciones generales de grado tres y cuatro son resolubles por radicales y no así las de grado ≥ 5 (aplicación que Galois formula de este modo más general: para que una ecuación irreducible de grado primo sea resoluble por radicales, es necesario y suficiente que todas las raíces sean funciones racionales de <u>dos</u> cualesquiera de ellas). No me molestaré en seguir a Galois en esta última parte por no alargar estos comentarios. Cualquier alumno que haya seguido un curso sobre teoría de grupos sabe bien que los grupos simétricos $\Sigma_2, \Sigma_3, \Sigma_4$, son resolubles, pero no así el grupo Σ_n , para $n \geq 5$. No es difícil por otra parte demostrar rigurosamente el hecho intuitivo de que el grupo simétrico Σ_n es el grupo de la ecuación general de grado n , y se concluyen pues esa aplicación desde el teorema de Galois que hemos comentado.

COMENTARIOS BIBLIOGRAFICOS

1) Los Gessamelte Werke de Gauss, editados por Félix Klein, no se encuentran íntegros en ninguna biblioteca española, aunque los volúmenes esenciales I-VI pueden encontrarse por ejemplo en la biblioteca de la Universidad Complutense. Falta en particular el tomo X que contiene, entre otros ensayos críticos, un estudio de Schlessinger sobre las ideas inéditas de Gauss acerca de las funciones θ, formas modulares y sus dominios fundamentales (ideas, pues, germinales de la geometría algebraica).
2) La más importante referencia sobre Gauss es hasta ahora la colección de ensayos "Gauss zum Gadächtniss" (Lipsiae 1957, ed. W. Reichardt), y ésta es accesible en nuestras bibliotecas. De especial interés para nuestro tema resulta el ensayo de Kochendörfer "Gauss algebraische Arbeiten", en el cual se analizan los conceptos algebraicos actuales que tienen su raíz en Gauss.
3) La bibliografía más actual para la obra de Gauss y para la obra acerca de Gauss es la publicada en el libro de W. K. Bühler "Gauss. A biographical study", de Springer Verlag (1981). Muchos de nuestros comentarios biográficos han sido tomados de esta amena y bien documentada lectura.
4) En cuanto al Algebra de Gauss, pueden encontrarse en muchas bibliotecas españolas las "Recherches arithmetiques", traducción al francés de Poullet-Delisle de las Disquisitiones Arithmeticae (Blanchard, reeditado en 1979).
5) Una muy legible historia, con referencias bien documentadas, sobre el álgebra en el entorno temporal de Gauss puede hallarse en "A History of Algebra" de B. L. Van der Waerden (Springer Verlag, 1985).
6) La escasa obra completa (e incompleta) de Galois fue publicada -y recientemente reeditada- en forma de opúsculo "Oeuvres Mathématiques de Evariste Galois" por Gauthiers-Villars en 1897, sin más comentarios que una breve introducción de Emil Piccard.
7) Una edición crítica de todas las cartas y manuscritos de E. Galois ha sido publicada por Gauthier - Villars en 1962 : "Ecrits et mémories mathématiques d'Evariste Galois".
8) La "Mémoire sur les conditions de résolubilité des équations por radicaux" de E. Galois, que hemos comentado en el anexo III, se halla también, en versión inglesa, como apéndice del libro de H. M. Edwards "Galois Theory" de Springer-Verlag (1984). El contenido de este libro es la exposición moderna de la teoría de Galois que más se acerca a su versión original.