Historia

Sección a cargo de

Luis Español González

Aporto esta contribución personal a la sección para resolver el apuro de haberme quedado sin artículos que proponer a la dirección de la revista. Animo a los historiadores a enviar originales dirigidos a la amplia comunidad matemática de lectores de La Gaceta de la RSME*, extendida a ambos lados latinos del Atlántico y más allá.*

El lema de Gauss y sus variaciones durante el siglo XIX

por

Luis Español González

A Mateo Garnica, de Nájera,
que me prestó sus libros
traídos de Buenos Aires.

Introducción

En el Libro IV de *Elementos*, Euclides había mostrado la construcción con la regla y el compás de algunos polígonos regulares inscritos en una circunferencia: el triángulo equilátero, el cuadrado, el pentágono, el hexágono y el pentadecágono.[1] Hasta aquí llegó Euclides, parece que se tratara de un inicio a seguir con la construcción del heptágono, etc. Se puede suponer, aunque Euclides no lo dejara expresamente escrito, que la lista de los polígonos inscriptibles era más amplia. Como en la proposición 30 del Libro III quedó construida la bisección de un arco de circunferencia, una vez inscrito un polígono de n lados se puede inscribir el de $2n$ lados, así que disponían también de todos los de $2^k n$ lados con $n = 2, 3, 5$. El logro magnífico de

[1] En la primera proposición del Libro I, Euclides da la construcción del triángulo equilátero con un segmento dado como lado. En el Libro IV construye un triángulo inscrito en una circunferencia equiángulo con un triángulo dado. Uniendo ambos resultados sale la construcción del triángulo equilátero inscrito. La construcción de un cuadrado de lado dado aparece en el Libro I como paso necesario para el teorema de Pitágoras, pero en el Libro IV el cuadrado debe ser inscrito a una circunferencia dada.

Euclides en el Libro IV fue la construcción del pentágono, pero también fue sutil el salto a $n = 15 = 3 \cdot 5$, para el que Euclides apoyó en la figura 1 un argumento verbal que se condensa en la expresión fraccionaria $\frac{1}{3} - \frac{1}{5} = \frac{2}{15}$: si a partir de un punto de la circunferencia como vértice inicial para ambos y en el mismo sentido se construyen el lado del triángulo y el del pentágono, entre los vértices así obtenidos resulta un arco de circunferencia que es el doble de la circunferencia dividida en 15 partes iguales; dividiendo ese arco por la mitad resulta como cuerda el lado del pentadecágono.[2]

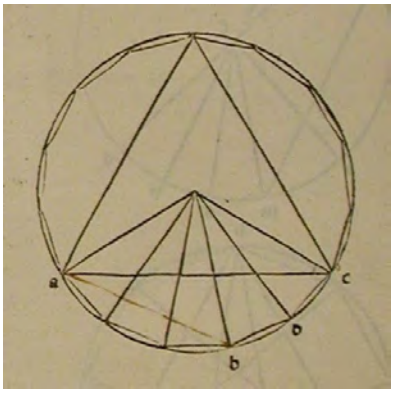


Figura 1: Corresponde a la proposición 16 del Libro IV de *Elementos*, que es la última de dicho libro, en la que se construye el heptadecágono. Tomada del ejemplar de la edición de Ratdolt (Venecia, 1482) conservado en la Biblioteca del Monasterio de San Millán de la Cogolla, La Rioja.

Los constructores con la regla y el compás se esforzaron al máximo en la resolución de los problemas de la duplicación del cubo, la trisección del ángulo y la cuadratura del círculo, pero se ocuparon menos de ampliar el elenco de los polígonos regulares inscriptibles en la circunferencia, parece que se conformaron con lo hecho por Euclides. Estos ufanos geómetras fueron perdiendo fuelle una vez que Vieta, Fermat y Descartes mostraron la posibilidad de analizar los problemas geométricos con el álgebra, lo que llevó con el tiempo a resolver algunos y a sospechar y demostrar, al fin, que otros no tenían solución si solo se usaban tan elementales instrumentos. En el caso de los polígonos, resultó que se podían construir más, pero para valores muy concretos del número de lados.

Gauss, nacido en 1777, demostró antes de tener veinte años que el heptadecágono regular se puede construir con regla y compás, pero no realizó la construcción efectiva

[2]Otra opción es usar la igualdad $\frac{2}{5} - \frac{1}{3} = \frac{1}{15}$, que se generaliza y ayuda a la proliferación de polígonos que se construyen a partir de otros ya logrados: si tenemos los de m y n lados con ambos números primos entre sí, entonces podemos construir el de mn lados. En efecto, hay una igualdad de la forma $hm = 1 + kn$ y por tanto $\frac{1}{mn} = \frac{h}{n} - \frac{k}{m}$, de modo que si a partir de un punto de la circunferencia como vértice inicial de ambos se construyen los polígonos dichos, tomando a partir del inicial común (vértice 0) h vértices consecutivos del n-gono y en el mismo sentido k del m-gono, entre los vértices así obtenidos resulta el lado del mn-gono.

dibujando con los instrumentos al modo antiguo, usó el álgebra para demostrar que tal construcción era posible, dejando que otros desarrollaran el algoritmo geométrico constructivo. El resultado aparece en la obra que lo consagró de inmediato como matemático genial, *Disquisitiones Arithmeticae* [11], publicada en Leipzig en 1801.[3] Llevaba trabajando en ella desde los años colegiales previos a sus estudios en la Universidad de Gotinga (1795–98), donde terminó de elaborarla y redactarla.[4] La primera anotación del diario matemático de Gauss[5] estaba fechada en «30-3-1796, Brunswick» y dice así:

> Principios sobre los que reposan la división del círculo y su divisibilidad geométrica en 17 partes, etc.. . .

Al final de *Disquisitiones*, Gauss demostró que se pueden construir con la regla y el compás los polígonos regulares inscritos con un número $n = 2^m p_1 \cdots p_k$ de lados, siendo los p_i números primos de la forma $2^{h_i} + 1$.[6] Dejó también escrito que tenía la demostración de la imposibilidad de construir los polígonos con otro número de lados, por ejemplo 7, 9, 11, 13, 14, 18, etc., pero ni la incluyó en *Disquisitiones* ni la publicó más tarde.[7]

En las páginas que siguen no voy a insistir en el tema de la construcción de polígonos regulares, sino que me voy a fijar en un resultado algebraico sobre polinomios con coeficientes enteros y racionales que fue crucial en la demostración por Gauss de la división del círculo en partes iguales y voy a exponer cómo este resultado, llamado *lema de Gauss*,[8] se perpetuó y generalizó con el tiempo como un enunciado meramente algebraico con aplicaciones a problemas de álgebra que los nuevos tiempos fueron planteando, según evolucionaban los objetivos esenciales del álgebra como rama de las matemáticas que iba cambiando desde la tradicional resolución de las ecuaciones, pasando por el cálculo con cantidades de diversa entidad, hacia la teoría de estructuras [4].

En la sección 1 me ocuparé de recoger lo que aparece en las *Disquisitiones Arithmeticae* y la forma personal como fue expuesto por Legendre en la segunda edición (1808) de su libro sobre teoría de números [19], aparecido un año después de la traducción de la obra de Gauss al francés. La sección 2 está dedicada a mostrar algunas

[3] La obra fue escrita en latín y se tradujo muy pronto al francés (1807). A lo largo de este artículo citaré diversas obras alemanas indicando sus traducciones al francés relativamente tempranas, un hecho muy característico del siglo XIX, cuando la matemática francesa seguía muy de cerca a la alemana que le iba arrebatando la hegemonía que tuvo durante el siglo anterior. Las versiones francesas ayudaron a la difusión de las obras alemanas. En algún caso indicaré otras traducciones. Una obra y sus traducciones aparecerán en el mismo registro de la sección final de referencias.

[4] Al mismo tiempo investigaba, entre otros temas, en los números complejos y el teorema fundamental del álgebra, objeto de su tesis doctoral defendida el año 1799 en la Universidad de Helmstedt.

[5] Cubre el periodo 1796–1814, fue descubierto en 1897 y editado por Klein en 1903 [14].

[6] No todos los números de esta forma son primos, los que lo son se llaman primos de Fermat y determinarlos es un problema de aritmética. Los primeros son 3, 5, 17, 257,... Para más detalles véase [24].

[7] Hay varias cuestiones que Gauss dejó anunciadas en *Disquisitiones*, sin demostrar ni desarrollar, decía que el libro se le estaba haciendo demasiado extenso. La imposibilidad de construcción con otro tipo de números es cierta, la demostración pendiente, fue expuesta en 1837 por Wantzel [25], un matemático también asociado a Gauss en el tema de los números complejos.

[8] Hay resultados con este mismo nombre en otros campos de la matemática, pero quizás este de los polinomios es el más conocido como tal.

variaciones sobre el tema, desde la primera modificación introducida por Eisenstein, hasta las que, desvinculadas ya del motivo geométrico inicial, fueron propiciadas por investigaciones algebraicas sobre la factorización única de entidades numéricas y no numéricas que heredaban algunas propiedades de las operaciones con los números enteros. Aunque mencionaré algunos trabajos esenciales de los investigadores más relevantes, mi propósito es indicar cómo el lema de Gauss quedó recogido en algunas obras de amplia difusión e influencia que ofrecen exposiciones generales de estas nuevas facetas del álgebra. Me referiré a dos libros de texto universitarios, el de Serret y el de Weber, y a una memoria de Hilbert de nivel más elevado pero también con carácter de síntesis de los avances previos recientes. La obra de Serret [21], con primera edición en 1849 y otras ampliadas posteriores, se mantuvo vigente durante la segunda mitad del siglo XIX, cuando le tomó el relevo un libro de Weber [26] que recoge parte de los avances del álgebra hasta la fecha finisecular de su aparición (1895), con una segunda edición en 1898 traducida al francés el mismo año.[9] En la sección 3 doy cuenta de la notable variación que experimenta el lema de Gauss cuando aparece en la obra de Hilbert sobre cuerpos de números algebraicos [12] publicada el año 1897, vinculado a la teoría de los ideales de números enteros algebraicos, elaborada principalmente por Dedekind a partir de un primer atisbo de Kummer, sin olvidar a Kronecker.[10] De este modo, la evolución del lema de Gauss quedará expuesta hasta poco antes de la llegada hacia 1920 del álgebra conmutativa abstracta y axiomática, en la que el lema de Gauss siguió teniendo una vida propia.[11]

1. El primer lema de Gauss

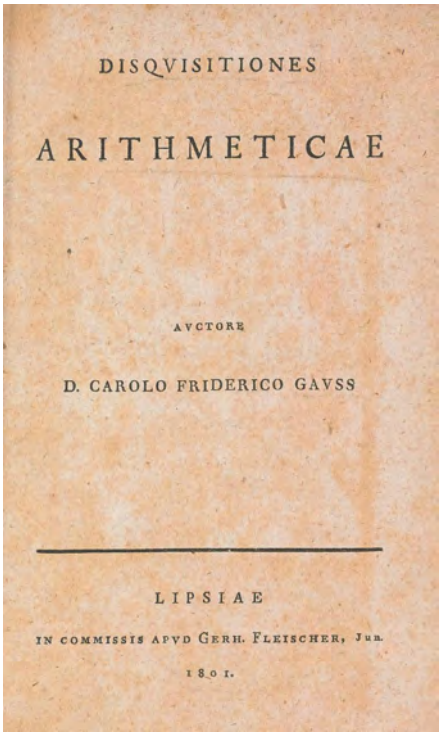
Disquisitiones Arithmeticae es una obra dividida en siete secciones y cada una de ellas en artículos hasta un total de 366. En el prefacio, Gauss escribe sobre la última de las secciones (arts. 335–366):

> La teoría de la división de un círculo o de polígonos regulares, tratada en la Sección VII, en sí misma no pertenece a la Aritmética, pero los principios involucrados dependen exclusivamente de la Aritmética Superior. Los geómetras pueden sorprenderse de este hecho en sí, tanto como espero que estarán complacidos con los nuevos resultados que se derivan de este tratamiento.

[9] El esfuerzo traductor fue relevante en estos años de internacionalismo matemático culminados en el primer Congreso Internacional de Matemáticos, Zürich, 1897. En 1898 se inició bajo la dirección de Klein la publicación de la *Encyclopädie der mathematischen Wissenschaften*, que los franceses, bajo la supervisión de Molk, iban traduciendo por fascículos; la Primera Guerra Mundial no interrumpió la publicación alemana, pero cortó el proceso de su traducción al francés.

[10] Esta obra de Hilbert tuvo también su traducción al francés en 1913.

[11] En 1983 publiqué una nota [10] sobre la evolución del lema de Gauss hasta esa fecha, incluyendo alguna noticia de su presencia en el álgebra abstracta y el álgebra constructiva interpretable en los topos, asunto en el que investigaba por entonces. El presente artículo es una versión ampliada de la primera parte de esa nota. En ella, las citas a *Disquisitiones* son mis traducciones de la edición francesa, pero en los años finales del siglo XX apareció la traducción al castellano [11] desde el latín original realizada en la República Dominicana y publicada con acceso libre en Colombia, así que ahora he preferido citar siguiendo a los traductores dominicanos. También en fecha todavía más próxima apareció otra traducción al catalán.


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Jun.

1801.

Figura 2: Portada del original en latín de *Disquisitiones Arithmeticae* de Gauss, 1801. Tomada del ejemplar digital de las Smithsonian Libraries.

Para Gauss, la teoría de la división de un círculo o de polígonos regulares consiste en el estudio de las raíces de la ecuación binomial $x^n - 1 = 0$. Sabe que la única raíz real es $x = 1$ y dividiendo la ecuación por $x - 1$ obtiene el polinomio que escribió

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0 \qquad (X)$$

cuyas $n - 1$ raíces son las complejas que faltan de la ecuación binomia. Se trata del punto de la circunferencia de radio 1 de coordenadas $\left(\cos \frac{P}{n}, \text{sen } \frac{P}{n}\right)$ y sus potencias sucesivas, siendo P, según denota Gauss, el arco completo de la circunferencia.[12] El polígono de n lados se podrá construir con regla y compás si $\cos \frac{P}{n}$ es un irracional cuadrático (y por tanto también sen $\frac{P}{n}$). Gauss se limita al caso en que $n = p$ es un número primo impar y da la expresión de $\cos \frac{P}{17}$ como irracional cuadrático en el art. 354. Los dos últimos artículos de la obra tienen estos contenidos:

365. El p-gono es construible si y solo si p es un primo de Fermat.

366. Se caracterizan los n para los que el n-gono es construible.

[12]Denotar la circunferencia con la letra P podría hacer referencia a la inicial de la palabra latina «Perimĕtros», como se hizo con la inicial griega π para su longitud medida por el diámetro. Luego Gauss usa la letra P con otro significado, denotando un polinomio en la variable x.

Para llegar a estos resultados, Gauss tuvo que demostrar otros previos, entre ellos uno de la misma sección séptima, sobre polinomios, que enuncia así:

> 341. Teorema. Si la función X es divisible por una función de grado más pequeño
> $$P = x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \text{etc.} + Kx + L$$
> los coeficientes $A, B, \ldots, L$ no pueden ser todos racionales.

Esto quiere decir que el polinomio ciclotómico X es irreducible, no se puede factorizar con coeficientes en $\mathbb{Q}$, luego tampoco en $\mathbb{Z}$.

Gauss procede por reducción al absurdo en su dilatada prueba del teorema 341, utilizando un resultado del final de la segunda sección, uno de los que califica como de «aplicación» de las cuestiones básicas sobre la divisibilidad tratadas antes. Este resultado, también con demostración laboriosa, es el siguiente:

> 42. Si los coeficientes $A, B, C, \ldots, N$; $a, b, c, \ldots, n$ de dos funciones de la forma
> $$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \cdots + N \qquad (P)$$
> $$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} + \cdots + n \qquad (Q)$$
> son todos racionales, y no todos enteros, y si el producto de (P) y (Q) es
> $$= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \text{etc.} + \mathfrak{Z},$$
> entonces no todos los coeficientes $\mathfrak{A}, \mathfrak{B}, \ldots, \mathfrak{Z}$ pueden ser enteros.

Este es el enunciado, o una de las variantes que tuvo con el tiempo, al que ahora me refiero como *lema de Gauss*, que recibe el calificativo de «lema» porque se supone que está al servicio del teorema sobre la irreducibilidad de la ecuación ciclotómica de grado primo. Con el tiempo, sus variantes siguieron siendo lemas para otros teoremas.

Gauss demostró que si un primo p tiene una aparición efectiva en el denominador de un coeficiente (fracción irreducible) de (P) entonces p aparece necesariamente de modo efectivo en el denominador de un coeficiente del producto,[13] independientemente de que p esté presente o no en algún denominador de (Q). Con notación moderna, decimos que, dados dos polinomios mónicos $f, g \in \mathbb{Q}[x]$, si $f \notin \mathbb{Z}[x]$ o $g \notin \mathbb{Z}[x]$ entonces $fg \notin \mathbb{Z}[x]$.

El gran matemático francés Legendre había publicado en 1798 *Essai sur la Théorie des Nombres* [19], el primer tratado sobre esta disciplina,[14] que Gauss conoció cuando ya tenía casi ultimada su obra *Disquisitiones Arithmeticae*, lo que mencionó de este modo en el preámbulo:

[13] Gauss no dio la definición general del producto de polinomios, pero la tenía bien clara, era simple consecuencia del cálculo. Para calcular el coeficiente de $x^{g+\gamma}$ en el producto, tomaba el coeficiente G de x^g en (P) y el Γ de x^γ en (Q) y los multiplicaba, luego tomaba los anteriores sucesivos $'G$, $''G$, etc. en (P) y los siguientes sucesivos Γ', Γ'', etc. en (Q), formaba los productos correlativos $'G\Gamma'$, $''G\Gamma''$, etc. y los sumaba; finalmente añadía la suma de los productos análogos por simetría $'\Gamma G'$, $''\Gamma G''$, etc. Ahora decimos que si los a_i son los coeficientes de (P) y los b_j son los de (Q), cada coeficiente c_k del producto es la suma de los productos $a_i b_j$ con $i + j = k$; lo mismo que Gauss.

[14] Cuyo prólogo contiene una interesante historia de la teoría de números hasta su tiempo.

> [...] apareció un trabajo sobresaliente obra de un hombre a quien la Aritmética Superior ya debe mucho, «Essai d'une théorie des nombres» (París, año VI) de Legendre, donde él reúne y sistematiza no solamente todo lo que había sido descubierto hasta esa fecha sino también muchos nuevos resultados propios. Ya que ese libro llegó a mis manos después de que gran parte de mi trabajo estaba levantado, no pude referirme a él en secciones análogas de mi libro. Sin embargo, me sentí obligado a agregar Notas Adicionales en algunos pasajes y confío que este comprensivo e ilustre hombre no se ofenderá.

Legendre tenía más de cincuenta años y andaba ultimando la segunda edición de su obra, aparecida en 1808, cuya portada aparece en la figura 3,[15] cuando llegó a sus manos *Disquisitiones*. En la «Advertencia» que colocó tras el prefacio de la segunda edición del *Essai* fue destacando las adiciones que la mejoraban y terminó escribiendo:

> [...] ha sido añadida una quinta parte donde se expone con todo el detalle necesario, la bella teoría de la resolución de la ecuación $x^n - 1 = 0$, dada por el Sr. Gauss, en sus Disquisitiones arithmeticae.
>
> Esta obra que apareció en Leipzig en 1801, y que colocó de un golpe a su autor en el rango de los Analistas más célebres, contiene muchas cosas análogas a las que son tratadas en el Ensayo sobre la Teoría de Números, publicado en 1798. Contiene particularmente una demostración directa y muy ingeniosa de la ley de reciprocidad ya citada; demostración que uno se proponía insertar con desarrollos más extensos en esta segunda Edición. Pero habiendo llegado después el Autor a encontrar una más simple y elegante, se ha expuesto con preferencia esta última en el §VII de la cuarta parte.
>
> Habría deseado enriquecer este Ensayo con un mayor número de los excelentes materiales que componen la obra del Sr. Gauss: pero los métodos de este autor le son de tal modo particulares que uno no habría podido, sin circuitos muy extensos, y sin someterse al simple papel de traductor, beneficiarse de sus otros descubrimientos.

La mencionada quinta parte añadida, la última del libro, tiene el título «Uso del análisis indeterminado en la resolución de la ecuación $x^n - 1 = 0$, siendo n un número primo». En ella Legendre señala (art. 435) que, hasta entonces, el conocimiento de la ecuación $x^n - 1 = 0$ se reducía a un teorema de Côtes: el polinomio ciclotómico X

[15] Este ejemplar de la obra de Legendre, el tratado de Serret y la memoria de Hilbert que se verá más tarde, me fueron prestados por Mateo Garnica Pérez, a quien acababa de conocer en Nájera cuando elaboré la nota [10]. También me prestó las traducciones francesas de *Disquisitiones* y del álgebra de Weber, aunque en las figuras respectivas he usado otros ejemplares. Mateo Garnica formó su biblioteca de matemáticas y física, con un notable fondo antiguo, en la capital argentina, a la que emigró a los 14 años por razones familiares. Fue estudiante en la Facultad de Ciencias de Buenos Aires y luego colaborador en sus laboratorios de física aplicada. Allí conoció a Rey Pastor y compitió con él en el mercado de libros de lance. Según Ortiz, «Garnica es quizás el más interesante de los bibliófilos científicos de Argentina del periodo 1940–1960» [2]. Por imposición de la política represiva en Argentina, volvió en 1965 a su Nájera natal, donde había nacido en 1920, incorporándose a su ámbito familiar como agricultor. Trajo de Buenos Aires una parte de su biblioteca, que guardaba con esmero hasta que la donó a la Universidad de La Rioja nada más ser fundada en 1992.

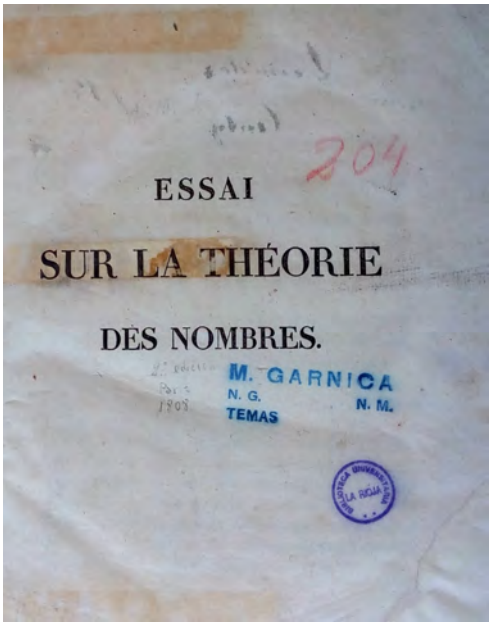


Figura 3: Portada del *Essai* de Legendre, 2.ª ed., 1808. Tomada del ejemplar de la Biblioteca de la Universidad de La Rioja, Fondo Mateo Garnica.

(el de Gauss, que Legendre denota con la misma letra) tiene por factor general

$$x^2 + 2x\cos\frac{2k\pi}{n} + 1$$

siendo k un número no divisible por n. Luego (art. 439) hace una exposición personal del lema de Gauss para a continuación (art. 440) utilizarlo para demostrar que X es irreducible en $\mathbb{Q}[x]$. Legendre califica por igual como «teorema» a ambas proposiciones, que enuncia así:

> (439) Teorema. Si el polinomio
>
> $$Z = x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \text{etc.},$$
>
> en el que los coeficientes A, B, C, etc. son enteros, es divisible por el polinomio
>
> $$P = x^n + ax^{n-1} + bx^{n-2} + \text{etc.},$$
>
> cuyos coeficientes a, b, c, etc. son todos racionales, digo que estos últimos deben ser también números enteros.
>
> (440) Teorema. El polinomio X, en el que n se supone siempre un número primo, no puede descomponerse en dos factores racionales.

Legendre puso su toque personal al exponer el lema de Gauss. La versión original del alemán es lógicamente equivalente a este enunciado directo: si $fg \in \mathbb{Z}[x]$ entonces

$f \in \mathbb{Z}[x]$ y $g \in \mathbb{Z}[x]$. Legendre cambia dos polinomios que se multiplican por uno con un divisor: si $f \in \mathbb{Z}[x]$ y $g \in \mathbb{Q}[x]$ divide a f entonces $g \in \mathbb{Z}[x]$. También simplificó la demostración haciendo uso de su art. (14), donde afirma que toda fracción cuyo denominador es el producto de dos números m y n primos entre sí se puede descomponer en suma de dos fracciones con m y n como denominadores respectivos, lo que extiende a un número finito de primos entre sí.[16]

2. El lema de Gauss en dos tratados

El camino que va del lema de Gauss al teorema de irreducibilidad fue refinado en 1850 por Eisenstein,[17] quien intercaló en el método de prueba el criterio de irreducibilidad de polinomios con coeficientes racionales que lleva a su nombre.[18]

No obstante, conviene advertir que se puede demostrar la irreducibilidad de la ecuación ciclotómica de grado primo sin usar el lema de Gauss. Así lo hizo Kronecker mientras realizaba en Berlín su tesis doctoral sobre las raíces de la unidad bajo la supervisión de Dirichlet. En un artículo muy corto [15] publicado el año 1845, comienza indicando:[19]

> Dada la importancia del tema, no debe dejar de tener interés agregar a la de Gauss en Disq. arithm. una segunda prueba muy simple. Para no perturbar el avance después, envío el siguiente teorema por delante [...]

El tema importante es la irreducibilidad de la ecuación ciclotómica de grado primo, para obtenerla propone un resultado previo que afirma que si p es un número primo y $\alpha \neq 1$ una raíz p-ésima de la unidad, entonces un polinomio con coeficientes enteros $f(x) = a + a_1x + a_2x^2 + \cdots + a_{p-1}x^{p-1}$ verifica la congruencia

$$f(\alpha)f(\alpha^2)\cdots f(\alpha^{p-1}) \equiv f(1)^{p-1} \pmod{p}.$$

Usando este que podríamos llamar «lema de Kronecker», demuestra la irreducibilidad de la ciclotómica de grado primo por reducción al absurdo, adjudicando con sendos argumentos valores contradictorios 0, 1 a la congruencia anterior.

Volviendo al camino trazado por Eisenstein, su método [9] fue seguido en muchas de las exposiciones del tema en la matemática clásica: primero se establece el lema de Gauss (sin que sea necesario suponer que los polinomios son mónicos) y con él

[16] Este es el mismo argumento que permite construir, como se vio antes, el mn-gono si ya se tienen construidos el m-gono y el n-gono, cuando los números son primos entre sí. Gauss no usó este argumento en la demostración del lema, pero sí que tenía demostrado en el art. 40 de *Disquisitiones* que si μ es el máximo común divisor de los números A, B, C, D etc., entonces se puede determinar una igualdad $\mu = aA + bB + cC +$ etc.

[17] Matemático berlinés nacido en 1823 que estaba desarrollando notablemente el contenido de las *Disquisitiones Arithmeticae* cuando falleció de tuberculosis a los 29 años en 1852, tres años antes de la muerte de Gauss. El año 1844 Eisenstein había visitado en Gotinga a Gauss, quien demostró una gran admiración por su trabajo.

[18] El criterio fue publicado antes por Schönemann [22], véase [5].

[19] Este comentario inicial no aparece en la traducción francesa de [15], que en una nota final añadida indica que la demostración de Kronecker parece más simple que las de Gauss y Legendre. Kronecker volvió sobre este asunto de la irreducibilidad en [16], con grado n arbitrario y usando el lema de Gauss; luego, en [17], insistió en la línea de [15].

se prueba el criterio de Eisenstein, del cual se deduce el teorema de irreducibilidad después de efectuar un cambio de variable $z = x + 1$. Klein lo siguió (con el lema de Gauss para polinomios mónicos) en su famoso opúsculo de 1985 sobre las construcciones geométricas, los polígonos regulares y la trascendencia de los números e y π [13]. Antes, a mediados de siglo, la huella de Eisenstein había quedado grabada en el primero de los dos tomos del *Course d'Algèbre supérieure* de Serret [21], aparecido en 1849, dos años después de que Liouville publicara los escritos inéditos de Galois. Fue uno de los textos de álgebra más difundidos durante la segunda mitad del siglo XIX. Lo comentaré siguiendo la tercera edición de 1866, en la que, al final de la obra, el autor expone resultados de Galois, Hermite y Kronecker formando tan solo un atisbo de la teoría de Galois.

Figura 4: Portada del *Cours* de Serret, 3.ª ed., 1866. Tomada del ejemplar de la Biblioteca de la Universidad de La Rioja, Fondo Mateo Garnica.

La obra está dividida en secciones y estas en capítulos. Serret empieza la sección primera («Las propiedades generales y la resolución numérica de las ecuaciones»)

dedicando dos capítulos a las fracciones continuas en general y al caso periódico. Siguen otros dos dedicados al teorema fundamental del álgebra (expuesto a la manera de Cauchy, usando la continuidad del polinomio como función compleja) y a la eliminación. El capítulo quinto trata de las «Propiedades de las raíces de la unidad», viendo la forma de las raíces, sus potencias, las que son primitivas y la reducción de la ecuación a las que tienen exponente primo o potencia de primo. En las últimas páginas del capítulo expone (art. 110, pág. 240) «Demostración de una propiedad notable de la ecuación $\frac{z^p-1}{z-1} = 0$, donde p designa un número primo». Se trata en efecto del teorema de irreducibilidad de la función ciclotómica de Gauss, del que afirma Serret que «esta importante propiedad es útil en un gran número de cuestiones». No procede exponer aquí las demostraciones, pero sí la secuencia de lemas previos al teorema de irreducibilidad:

> La demostración que vamos a presentar se debe a Eisenstein; reposa sobre los dos lemas siguientes:
>
> Lema I.— Si la función entera X de x con coeficientes enteros es descomponible en dos factores racionales X_1, X_2, de manera que se tenga $X = X_1X_2$, todos los coeficientes de los polinomios X_1 y X_2 serán enteros, o, si no lo son, se podrán encontrar enteros m y n tales, que todos los coeficientes de los polinomios $\frac{m}{n}X_1$, y $\frac{n}{m}X_2$, sean enteros.
>
> [...]
>
> Lema II.— Si en un polinomio X de grado cualquiera, el término más elevado en x tiene por coeficiente la unidad, suponemos que todos los otros coeficientes sean enteros divisibles por un número primo p, y también que el término independiente de x sea igual a $\pm p$, la ecuación $X = 0$ será irreducible.

El primer lema es una variación del original de Gauss y el segundo es el que llamamos criterio de Eisenstein.[20] La exposición sigue a Eisenstein sin mencionar la versión original de Gauss ni su vínculo con la construcciones con regla y compás de los polígonos regulares inscritos, el resultado se presenta como un caso especialmente interesante y bien resuelto de ecuación algebraica.

Serret tampoco relaciona este asunto con las congruencias, que expone en el segundo volumen. Este empieza con la sección tercera («Las propiedades de los números enteros»), en cuyos capítulos primero y segundo trata de las congruencias a la Legendre-Gauss, reconociendo que

> La notación de Gauss, para representar las congruencias, tiene la ventaja de poner en evidencia la analogía que existe entre las congruencias y las igualdades, sin que haya sin embargo temor a confusión. Vamos a hacer ver que la mayor parte de las transformaciones que uno puede llevar a cabo con las igualdades pueden ser aplicadas a las congruencias.

El capítulo tercero de la sección tercera («Propiedades de las funciones enteras de una variable, relativamente a un módulo primo») está dedicado a transferir la divisibilidad en $\mathbb{Z}$ a $\mathbb{Z}_p[x]$. La propiedad fundamental de la divisibilidad en $\mathbb{Z}$ es que todo entero se descompone de modo único (salvo el orden y el signo) en factores primos.

[20] En ambos lemas, X es un polinomio en general con las restricciones indicadas, ya no es el ciclotómico que Gauss denotó con dicha letra.

La existencia surge del concepto mismo de reducibilidad con ayuda del principio del tercero excluido (un elemento es irreducible o no es irreducible) y para demostrar la unicidad de la descomposición se ha de probar previamente que si un número primo divide a un producto de enteros divide al menos a uno de ellos. Este esquema metódico[21] es el que siguió Serret con $\mathbb{Z}_p[x]$, donde el papel de los números primos es jugado por los polinomios irreducibles módulo p. En el art. 343, Serret demuestra que $\mathbb{Z}_p[x]$ es, con terminología actual, un dominio de factorización única, probando antes con polinomios de $\mathbb{Z}_p[x]$ que si f es irreducible y divide a gh entonces f divide a g o f divide a h, proceso en el que interviene el lema de Gauss.

Los teoremas de carácter atomista extrapolados desde $\mathbb{Z}$, referidos a la descomposición de ciertos números o cantidades en otros análogos de naturaleza indescomponible, estaban en el corazón del álgebra del siglo XIX, en paralelo a la teoría de Galois; se trataba de extenderlos a la divisibilidad de polinomios y de otros conjuntos de números cerrados para las operaciones aritméticas usuales. En lo que a los polinomios se refiere, el modelo de prueba dada por Serret de la factorización única $\mathbb{Z}_p[x]$ sirve para polinomios con coeficientes en cualquiera de los cuerpos de números entonces en liza. Se sabía que $\mathbb{Q}[x]$ es dominio de factorización única y el lema de Gauss lleva a que también lo sea $\mathbb{Z}[x]$.

Extender estos resultados a polinomios en un número finito de variables tuvo que esperar a una notable memoria de Kronecker de 1882 [18] que quedó reflejada en el siguiente tratado de amplia difusión que voy a considerar, el *Lehrbuch der Algebra* de H. Weber (1898),[22] que incorporó, y sistematizó algunos, no todos, los avances del álgebra debidos principalmente a Kronecker y Dedekind.[23] De sus tres volúmenes solo mencionaré el primero y más difundido [26], cuya segunda edición fue rápidamente traducida al francés; fue en cierto modo el sucesor del *Course* de Serret por su influencia en la diseminación del álgebra superior. Dice Weber en el prefacio del *Lehrbuch*:

> El desarrollo tomado por el álgebra en estos últimos decenios parece justificar una exposición de conjunto de las diversas teorías de esta ciencia y de sus múltiples aplicaciones, incluso después del libro de Serret, tan excelente para la época en que fue publicado.

El mencionado primer volumen de Weber se compone de artículos numerados de 1 a 196, agrupados en dieciocho capítulos y estos en tres «Libros». Después de una introducción dedicada a presentar los sistemas de números desde los naturales a los complejos, inicia el Libro I («Los principios») con dos capítulos de cálculo algebraico con cantidades más allá de los números, como son primero los polinomios y sus fracciones y después los determinantes; luego inicia los preparativos para la resolución de las ecuaciones algebraicas y la teoría de Galois, tema protagonista del volumen.

El capítulo primero está dedicado a las «funciones racionales», que pueden ser «enteras» (los polinomios) o «fraccionarias» (los cocientes de polinomios). En el

[21] Que viene del Libro VII de los *Elementos* de Euclides, donde no está mencionada la unicidad pero sí el resultado que sirve para deducirla de modo inmediato.

[22] Un año después del primer Congreso Internacional de Matemáticos reunido en Zürich.

[23] Un análisis en contexto de la obra de Weber se encuentra en [4, 3].

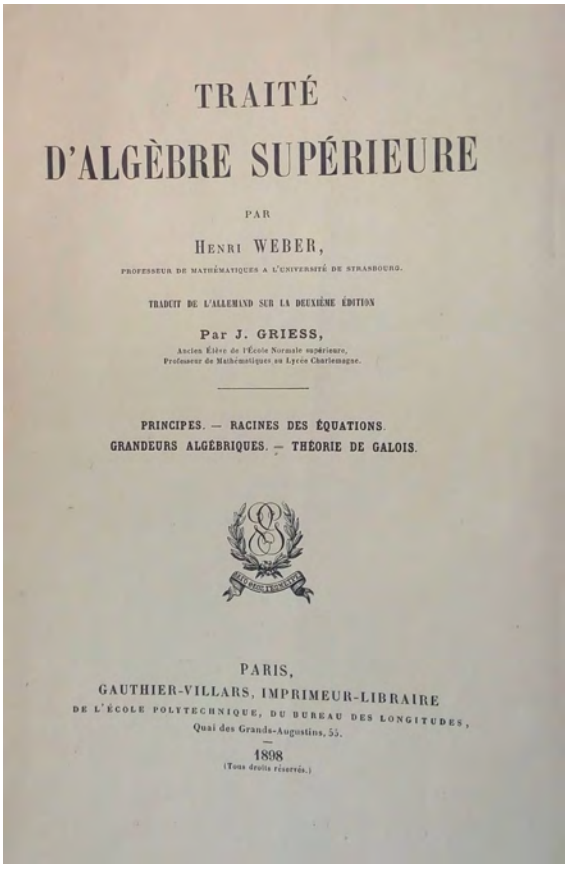

TRAITÉ
D'ALGÈBRE SUPÉRIEURE
PAR
HENRI WEBER,
PROFESSEUR DE MATHÉMATIQUES A L'UNIVERSITÉ DE STRASBOURG.
TRADUIT DE L'ALLEMAND SUR LA DEUXIÈME ÉDITION
Par J. GRIESS,
Ancien Élève de l'École Normale supérieure,
Professeur de Mathématiques au Lycée Charlemagne.
PRINCIPES. — RACINES DES ÉQUATIONS.
GRANDEURS ALGÉBRIQUES. — THÉORIE DE GALOIS.
PARIS,
GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE
DE L'ÉCOLE POLYTECHNIQUE, DU BUREAU DES LONGITUDES,
Quai des Grands-Augustins, 55.
1898
(Tous droits réservés.)

Figura 5: Portada de la traducción francesa del primer volumen del *Lehrbuch der Algebra* de Weber, 2.ª ed., 1898. Tomada de la biblioteca personal del autor.

«§1.– Funciones enteras» introduce directamente y de modo rápido las operaciones con los polinomios de una variable y señala la extensión a varias variables. En esta presentación general, los coeficientes de los polinomios son «símbolos de cantidades no determinadas, sobre las que se opera según las reglas del cálculo algebraico, y que se pueden reemplazar cuando proceda por valores determinados», de modo que lo dicho vale para cualquiera de los sistemas de cantidades con los que entonces se trabajaba con cierta ambigüedad, antes de la llegada de las precisas definiciones axiomáticas abstractas del siglo XX. Explica que el producto de dos funciones enteras es otra función entera dando la expresión habitual de sus coeficientes y asegura sin demostración que se cumplen las propiedades conmutativa, asociativa y distributiva respecto a la suma, precisando que la igualdad de funciones enteras se refiere a que «los términos del mismo exponente tengan el mismo coeficiente». En un párrafo de media página extiende lo dicho de una a varias variables $x, y, z, \ldots$, indicando que

> Estas funciones pueden ser consideradas como deducidas de una función de una sola variable x, en la que los coeficientes $a_0, a_1, \ldots, a_n$ se consideran como funciones de las otras variables $y, z, \ldots$. Es así como una función de m variables resulta de una función de $m-1$ variables.

A continuación llega el «§2.– Un teorema de Gauss», que el autor refiere al art. 42 de *Disquisitiones* que contiene el lema de Gauss, ahora convertido en el primer teorema del *Lehrbuch*. Weber le dedica estas líneas de presentación que señalan un rol de lema que se ejecutará más adelante en este volumen:

> Como aplicación de la regla de multiplicación de dos funciones racionales enteras, vamos a demostrar un teorema debido a Gauss, que nos será útil más tarde, pero que, por el momento, nos servirá de ejemplo sobre el modo de ejecutar el cálculo.

El cálculo al que se refiere es el producto de funciones enteras, pero esta vez está particularizado al caso en que los coeficientes son números enteros, se coloca pues en $\mathbb{Z}[x]$ (notación actual). Anuncia un teorema pero en realidad da tres, el último de los cuales es el lema de Gauss, que aparece después de dos resultados originados en Kronecker y que requieren definiciones previas. El máximo común divisor de los coeficientes de una función entera que los tiene enteros es el *divisor* de dicha función, que se llama *primitiva* si los coeficientes son primos entre sí (divisor igual a 1).

Weber afirma que «el teorema que quiere demostrar» es el siguiente:[24]

> (P1) Si las funciones $A(x)$ y $B(x)$ son funciones primitivas, también lo es su producto $C(x)$.

Una vez demostrado el teorema para una variable, Weber lo extiende dando en pocas palabras el argumento inductivo de Kronecker para transferir resultados de una a varias variables: las operaciones y argumentos que se hacen con los coeficientes en $\mathbb{Z}$ para probar (P1) se pueden hacer con coeficientes en $\mathbb{Z}[y, z, \ldots]$, así que si (P1) vale para $\mathbb{Z}[y, z, \ldots]$ también valdrá para $\mathbb{Z}[x, y, z, \ldots] = \mathbb{Z}[y, z, \ldots][x]$.

Aprovecha Weber el uso de este método para indicar que sirve para transferir otras propiedades: «Razonando de una manera análoga se prueba que un producto de dos o varias funciones enteras no puede ser nulo a menos que uno de sus factores sea nulo». Con este breve argumento supone el autor que el lector ha comprendido que $\mathbb{Z}[x, y, z, \ldots]$ es un dominio de integridad al igual que $\mathbb{Z}[x]$.

Hecho este inciso, Weber continúa con el tema principal afirmando que (P1) «se puede enunciar» de otra manera:

> (P2) El divisor del producto de dos funciones enteras es igual al producto de los divisores de estas dos funciones.

Que (P1) implica (P2) es muy sencillo de demostrar observando que cada función entera es el producto de su divisor por una función primitiva. La implicación inversa es obvia, ni la menciona. Weber deja apuntado que (P1) y (P2) son válidos con cualquier número finito de variables. Termina el §2 anunciando un tercer teorema:

[24] A lo largo del libro, los teoremas no llevan rótulo ni numeración, simplemente van en párrafo suelto y en cursiva. Previo al enunciado que sigue inserto la etiqueta (P1), con «P» de «Producto», para facilitar las referencias internas en este artículo. Lo mismo haré después con (P2).

> Colocándonos en el caso de una sola variable, se puede dar a este teorema la forma siguiente, bajo la cual es particularmente útil, sin cambiar notablemente su sentido.

El teorema al que el autor se refiere es (P1) y la nueva forma del mismo que inserta a continuación es el lema de Gauss (§42 de *Disquisitiones*). No vale la pena reproducirlo porque lo enuncia casi igual, seguido de una demostración muy sencilla usando (P1) y reducción al absurdo. En definitiva, Weber muestra el proceso metódico de Kronecker para llegar al lema de Gauss, en el que destaca el papel (lemas del lema) de los enunciados (P1) y (P2).

Estos resultados también serán usados como lemas en el «§20.– Funciones reducibles e irreducibles», para probar por inducción sobre el número de variables los enunciados siguientes:

> (I) Sean U, V, ν funciones enteras de cualesquiera variables; si la función ν divide al producto UV y si es prima con U, divide a V.
>
> (II) Un producto de varias funciones enteras no puede ser divisible por una función irreducible ν más que si uno de los factores es divisible por ν.
>
> (III) Abstracción hecha de ciertos factores constantes, una función entera no puede descomponerse en factores irreducibles más que de una sola manera.

Con las imprecisiones del lenguaje entonces usado, de camino hacia el dominio del simbolismo pero todavía muy retórico, lo que Weber ha demostrado es que ser un dominio de factorización única se transfiere a los polinomios sobre dicho dominio, en particular, $\mathbb{Z}[x_1, \ldots, x_n]$, $\mathbb{C}[x_1, \ldots, x_n]$ son dominios de factorización única.[25]

El lema de Gauss como herramienta para el teorema de irreducibilidad del polinomio ciclotómico X también está presente en el *Lehrbuch*, «§174.– Irreducibilidad de la ecuación de división». Weber no sigue como Serret en el método de Eisenstein, sino que incorpora variantes más recientes de la demostración. Primero prueba que X es irreducible en $\mathbb{Q}$ cualquiera que sea su grado siguiendo una demostración de Dedekind que utiliza el lema de Gauss; luego extiende la irreducibilidad demostrando que X también es irreducible en el cuerpo $\mathbb{Q}(\alpha)$ obtenido adjuntando una raíz primitiva de orden primo con n, teorema que Kronecker había obtenido de modo independiente en 1882.[26]

[25] Una vez formalizados en el siglo XX los conceptos de cuerpo, anillo (conmutativo y unitario) y dominio de factorización única, las demostraciones de Serret y de Weber, basadas en propiedades básicas de los casos que manejaban, inspiran las de dos teoremas abstractos: de Serret, que $K[x]$ es un dominio de factorización única cuando K es un cuerpo; de Weber, que si un anillo A es un un dominio de factorización única el anillo de polinomios $A[x]$ también lo es.

[26] Escribí [10] el año 1983, como homenaje por su jubilación a Rafael Rodríguez Vidal, mi profesor de álgebra en el tercer curso de matemáticas en Zaragoza (1968/69), donde uno de los textos a seguir era la traducción por dicho profesor de la influyente obra de los algebristas norteamericanos Birkhoff y Mac Lane [1]. La obra es posterior al libro de van der Waerden [23] que inauguró en 1930 la interminable serie de manuales de álgebra abstracta con el elenco de estructuras algebraicas y sin duda está influida por ella, pero mantiene un cierto recuerdo a los textos del periodo anterior; allí aprendí el lema de Gauss y sus usos. En el capítulo IV («Polinomios»), los autores llaman «lema de Gauss» al enunciado (P1), luego dan (P2) como segundo lema y a continuación su «Teorema 13» es el que vengo llamando lema de Gauss; esto aparece en el camino que lleva al «Teorema 14» de transferencia: si G es un dominio de factorización única, entonces $G[x]$ también

3. Ideales de enteros algebraicos

Falta, para terminar, adentrarnos por otra senda que parte de *Disquisitiones Arithmeticae* en la que el lema de Gauss caminó ofreciendo otra muestra de sus muy notables posibilidades. En su intento de generalizar la reciprocidad cuadrática, Gauss estudió los números complejos cuyas partes real e imaginaria son números enteros.[27] Gauss demostró que forman una extensión de los enteros ordinarios que admite muchas de las propiedades aritméticas de estos, la más importante es la divisibilidad que da lugar a un dominio de factorización única. Así como la reciprocidad cuadrática se quería extender a grados cada vez mayores, se buscaron extensiones sucesivas de los enteros dando lugar a la teoría de los enteros algebraicos, en la que trabajó Eisenstein mientras la salud se lo permitió y luego Kummer, el primer maestro de Kronecker. La propuesta de nuevos enteros algebraicos llevó a Kummer a encontrar casos en los que la factorización única no se verificaba, lo que le indujo a replantear la divisibilidad introduciendo unos «números ideales», luego llamados simplemente ideales, que son subconjuntos de números cumpliendo ciertas condiciones y que se pueden multiplicar. Trabajando la divisibilidad de estos ideales se restauran las buenas propiedades de los números originales, en particular la factorización única. En el estudio de la divisibilidad de los ideales de números enteros algebraicos Dedekind alcanzó la máxima jerarquía con la obra [6], en cuya versión inglesa el traductor Stillwell presenta una introducción muy recomendable a qué son y cómo se gestaron los enteros algebraicos. En su comunicación al congreso que la Sociedad Matemática Alemana celebró en Praga en 1892, Dedekind expuso [7] el desarrollo de «un teorema aritmético de Gauss» desde el lema de Gauss de *Disquisitiones* hasta sus formulaciones con la teoría de ideales. Los avances por esta senda fueron magistralmente sintetizados el año 1897 en una obra famosa de Hilbert, la memoria conocida como *Zahlenbegrift* [12], que contiene una nutrida lista de los artículos sobre el tema publicados hasta entonces.

Ya en 1888 Hilbert había usado los ideales en los anillos de polinomios que se usaban en la geometría algebraica, demostrando que esos ideales tenían siempre un conjunto finito de generadores, es decir, el ideal se forma a partir de un número finito $f_1, \ldots, f_r$ de polinomios juntando todos los de la forma $g_1 f_1 + \cdots + g_r f_r$ con los $g_1, \ldots, g_r$ polinomios cualesquiera. El ideal así formado se denota $(f_1, \ldots, f_r)$. El mérito del *teorema de la base* de Hilbert consiste en establecer que en los anillos de polinomios de la geometría algebraica todos los ideales (definidos por sus propiedades como subconjuntos respecto a las operaciones) son finitamente engendrados, lo que exige probar que el sistema generador o base existe. Los expertos en invariantes querían encontrar efectivamente la base, lo que solo lograban en casos sencillos y

lo es, y como corolario inductivo también $G[x_1, \ldots, x_n]$. A continuación, para ayudar a saber si un polinomio con coeficientes enteros es irreducible dan el criterio de Eisenstein («Teorema 15» que usa el «Teorema 13») y lo utilizan para indicar en un simple comentario al margen que el polinomio ciclotómico de grado primo es irreducible.

[27] Ahora denotamos $\mathbb{Z}[i]$ al conjunto que forman todos ellos y los denominamos *enteros de Gauss*. Forman un anillo (conmutativo y unitario) contenido en $\mathbb{Q}[i]$, que es un cuerpo intermedio entre el de los racionales $\mathbb{Q}$ y el de los complejos $\mathbb{C}$. Gauss mencionó estos números en dos de las últimas anotaciones de su diario (1813–14), pero no publicó sobre ellos hasta 1832.

mediante cálculos muy arduos, pero Hilbert cambió el método, con argumentos abstractos no constructivos demostró dicha existencia, el problema del cálculo efectivo quedaba para después.[28] Terminada su investigación sobre los ideales de polinomios de la geometría, Hilbert pasó a los ideales de enteros algebraicos de la teoría de números.[29]

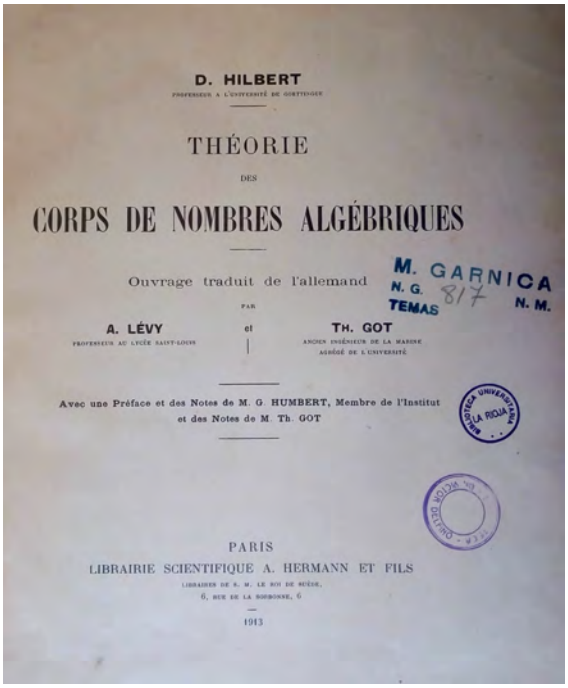


Figura 6: Portada de la traducción francesa del *Zahlenbegrift* de Hilbert, 1913. Tomada del ejemplar de la Biblioteca de la Universidad de La Rioja, Fondo Mateo Garnica.

En el prefacio de *Zahlenbegrift* Hilbert escribió: «La teoría de los números algebraicos y la teoría de las ecuaciones de Galois tienen sus raíces comunes en la teoría de los cuerpos algebraicos». Lejos de dar cuenta del alcance de la teoría, me limitaré a verificar la aparición de una variación del lema de Gauss en el capítulo segundo, todavía introductorio respecto al cuerpo central de la obra, organizada en cinco partes entre las que se distribuyen los 36 capítulos. A lo largo de toda ella mantiene una secuencia de teoremas de 1 a 169 que son los resultados importantes

[28] Algo similar había hecho Gauss, demostrar por razonamientos generales qué polígonos se podían construir y dejar que fueran los geómetras constructores los que cogieran la regla y el compás.

[29] Visto el paralelismo entre los métodos algebraicos usados en la geometría y en la teoría de números, la unificación de ambas teorías, vislumbrada por Kronecker y clarificada por Hilbert, culminó con la formulación abstracta del álgebra conmutativa a partir de los años 1920.

en sí mismos, pero en el preámbulo Hilbert dejó señalados los que «pueden ser tomados como punto de partida para incursiones en un país nuevo y no descubierto todavía». Mi aproximación a *Zahlenbegrift* solo llegará al primero de ellos.

El primer capítulo («El número algebraico y el cuerpo algebraico») es muy breve, limitándose a dar las primeras definiciones y propiedades (teoremas 1 a 5) que remite a los trabajos originales de Dedekind y Kronecker.[30] Los *números algebraicos* son las raíces de los polinomios con coeficientes racionales. Para formar un *cuerpo de números algebraicos*[31] se toman todas las funciones racionales con coeficientes enteros de ciertos números algebraicos dados en número finito, resultando así un dominio «invariante por las cuatro operaciones elementales: suma, resta, multiplicación, división». Los números algebraicos se llaman *números enteros algebraicos* cuando el polinomio del que son raíz tiene los coeficientes enteros y es mónico. Dentro de cada cuerpo de números algebraicos hay un sistema de enteros que es «invariante por las tres operaciones: suma, resta, multiplicación».[32] Los enteros algebraicos siempre se refieren a un cuerpo de números dado, son «los enteros del cuerpo».

El objetivo es estudiar la divisibilidad de los enteros algebraicos, para lo cual quedó claro desde Kummer que había que ampliar la divisibilidad de los números enteros algebraicos a la divisibilidad de los subconjuntos con ellos formados llamados ideales. El segundo capítulo de *Zahlenbegrift* («Los ideales del cuerpo») afronta esta tarea.[33] Un ideal de un cuerpo de números k es un «sistema» $\mathfrak{a}$ de números enteros algebraicos de k tal que siempre que tomemos un número finito de ellos $\alpha_1, \alpha_2, \ldots$ y el mismo número de enteros algebraicos $\lambda_1, \lambda_2, \ldots$ de k, el entero $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots$ también pertenece al ideal $\mathfrak{a}$. El primero de los teoremas que pueden ser «punto de partida para incursiones en un país nuevo» llega en el §5 de este segundo capítulo, presentado como «hecho fundamental»:

> Teorema 7. Todo ideal j puede ser descompuesto en un producto de ideales primos y puede serlo de una sola manera.

Naturalmente, antes ha tenido que introducir el producto y la divisibilidad de ideales, objetivo del §4 con el que se inicia del capítulo. Lo primero que demuestra («Teorema 6») es que cada ideal es finitamente engendrado, por lo que tiene la forma $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$. El ideal $\mathfrak{a}$ se multiplica por otro $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ poniendo

$$\mathfrak{ab} = (\alpha_1\beta_1, \ldots, \alpha_r\beta_1, \ldots, \alpha_1\beta_s, \ldots, \alpha_r\beta_s),$$

de modo que ya se puede decir lo que significa que un ideal divide a otro y que un ideal es primo. De inmediato demuestra que un ideal solo tiene un número finito de divisores, luego ya está listo para enunciar su teorema fundamental 7.[34] La demos-

[30] De Dedekind cita sus primeros trabajos sobre los enteros algebraicos: los suplementos a la obra de Dirichlet [8] la obra fundamental [6]; de Kronecker la famosa memoria de 1882 [18].

[31] Llamado también «cuerpo algebraico» o «dominio de racionalidad».

[32] Es decir, dentro del cuerpo de números algebraicos se tiene un anillo de enteros algebraicos.

[33] Denotando los ideales con letras góticas minúsculas, algo que ya hacía Dedekind y que se mantuvo como costumbre en muchos libros, no solo alemanes, del siglo siguiente.

[34] Hilbert expone las demostraciones primeras de Dedekind y Kronecker, aunque indica que el propio Dedekind dio otra prueba y también lo demostraron de manera diferente el propio Hilbert y Hurwitz.

tración de este teorema se inicia con un lema que adapta el lema de Gauss a los enteros algebraicos:

Lema 2. Cuando los coeficientes de dos funciones enteras de la variable x,

$$F(x) = \alpha_1 x^r + \alpha_2 x^{r-1} + \cdots,$$
$$G(x) = \beta_1 x^s + \beta_2 x^{s-1} + \cdots,$$

son números enteros algebraicos y los coeficientes $\gamma_1, \gamma_2, \gamma_3, \ldots$ del producto

$$F(x)G(x) = \gamma_1 x^{r+s} + \gamma_2 x^{r+s-1} + \cdots$$

son todos divisibles por el número entero algebraico ω, cada uno de los números $\alpha_1\beta_1$, $\alpha_1\beta_2, \ldots$, $\alpha_2\beta_1$, $\alpha_2\beta_2, \ldots$ es divisible por ω.

De este lema se deducen las siguientes propiedades que conducen a la demostración del teorema fundamental 7: Para cada ideal $\mathfrak{a}$ existe un ideal $\mathfrak{b}$ tal que $\mathfrak{ab}$ es principal. Si $\mathfrak{ac} = \mathfrak{bc}$ entonces $\mathfrak{a} = \mathfrak{b}$. Si todos los enteros de $\mathfrak{c}$ están en $\mathfrak{a}$ entonces $\mathfrak{c}$ divide a $\mathfrak{a}$. Si el producto de dos ideales $\mathfrak{ab}$ es divisible por un ideal primo $\mathfrak{p}$, uno de los dos ideales $\mathfrak{a}$, $\mathfrak{b}$ es divisible por $\mathfrak{p}$.

Por la analogía formal con la divisibilidad ordinaria, se comprende que la última de las propiedades anteriores dará la unicidad de la descomposición de un ideal en factores primos.

A continuación, en §6 («Las formas de los cuerpos algebraicos y sus contenidos») Hilbert, que hasta aquí ha seguido a Dedekind, se refiere a la teoría de Kronecker, en la que una *forma del cuerpo k* es un polinomio cuyos coeficientes son enteros algebraicos de k y se llama *contenido* de la forma al ideal engendrado por sus coeficientes. Entonces:

Teorema 13. El contenido del producto de dos formas es igual al producto de sus contenidos.

Si $\mathfrak{a}$ es el ideal engendrado por los coeficientes de un polinomio y $\mathfrak{b}$ el de otro, el ideal engendrado por los coeficientes del producto de ambos es $\mathfrak{c} = \mathfrak{ab}$. Este teorema compara el producto de formas (polinomios) y el producto de ideales, demostrando que dos sistemas finitos diferentes de generadores engendran el mismo ideal. La analogía formal con el enunciado (P2) visto en Weber salta a la vista, allí se llamaba divisor de un polinomio, que era el máximo común divisor de sus coeficientes, pero el ideal engendrado por los coeficientes coincide con el ideal principal engendrado por su máximo común divisor, así que (P2) es el mismo Teorema 13.

Este relato termina a las puertas del álgebra abstracta característica del siglo XX, que se puede considerar iniciada, desde el punto de vista de un proyecto de investigación, en 1921 con la teoría de los ideales en los anillos conmutativos introducidos de modo axiomático por Emmy Noether [20] y, desde el punto de vista de la difusión de la imagen del álgebra como teoría de estructuras, por el libro [26] publicado Van der Waerden en 1930. Toda esta corriente sigue el modelo formal de Dedekind y Hilbert, pero en el último cuarto del siglo XX apareció una nueva tendencia constructiva, más o menos heredera de Kronecker y Brouwer, que primero fue un álgebra constructiva intuicionista con modelos en topos de Grothendieck y enseguida un álgebra constructiva en el sentido de los algoritmos computables. También el lema de Gauss tiene su historia en este mundo más reciente de abstracción y cómputo.

REFERENCIAS

[1] G. BIRKHOFF Y S. MAC LANE, *A survey of modern algebra*, Macmillan, 1941. Trad. de R. Rodríguez Vidal: *Álgebra moderna*, Vicens-Vives, Barcelona, 1954.

[2] *Catálogo del Legado Mateo Garnica*, elaborado por J. León y M. Ruiz de la Cuesta, presentación de L. Español, apunte biográfico de M. Felip y estudio introductorio de E. L. Ortiz, Universidad de La Rioja, Logroño, 1994.

[3] L. CORRY, Estructuras algebraicas y textos algebraicos del siglo XIX, *Llull* **14** (1991), 7–30.

[4] L. CORRY, *Modern algebra and the rise of mathematical structures*, Birkhäuser, Basel, 1996.

[5] D. A. COX, Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first, *Amer. Math. Monthly* **118** (2011), 3–31.

[6] R. DEDEKIND, Sur la théorie des nombres entiers algébriques, *Bulletin des sciences mathématiques et astronomiques* **11** (1876), 278–288; **12** (1877), 17–41, 69–92, 144–164, 207–248. Trad. al inglés por J. Stillwell: *Theory of algebraic numbers*, Cambridge Univ. Press, 1996.

[7] R. DEDEKIND, Über einen arithmetischen Satz von Gauß, Mitteilungen der Deutschen mathematischen Gesellschaft in Prag, Jahrgang 1892, S. 1–11; und Über die Begründung der Idealtheorie, *Nachrichten von der Köning. Ges. der Wissenschaften zu Göttingen* (1895), 106–113. [*Werke*, Vol. 2, 103–147.]

[8] P. G. L. DIRICHLET, *Vorlesungen über Zahlentheorie*, Braunschweig, 1863 (otras ed., 1871, 1879, 1894), con suplementos de R. Dedekind. Trad. al inglés por J. Stillwell: *Lectures on number theory*, History of Mathematics 16, American Mathematical Society, Providence, RI; London Mathematical Society, London, 1999.

[9] G. EISENSTEIN, Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, *J. Reine Angew. Math. (Journal de Crelle)* **39** (1850), 160–179.

[10] L. ESPAÑOL, Nota sobre diversas versiones del lema de Gauss, *Homenaje al profesor D. Rafael Rodríguez Vidal*, 152–162, Secretariado de Publicaciones de la Universidad de Zaragoza, 1985.

[11] C. F. GAUSS, *Disquisitiones Arithmeticae*, Leipzig, 1801. Trad. al francés por A. C. M. Poullet-Delisle: *Recherches Arithmétiques*, Paris, 1807. Trad. al español por H. Barrantes, M. Josephy y A. Ruiz Zúñiga (Escuela de Matemáticas de la Universidad de Costa Rica): *Disquisitiones Arithmeticae*, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Colección Enrique Pérez Arbeláez No. 10, Bogotá, 1995. Trad. al catalán por Griselda Pascual Xufré: *Disquisicions Arithmètiques*, Institut d'Estudis Catalans, Barcelona, 1996.

[12] D. HILBERT, Die Theorie der algebraischen Zahlkörper, *Jahresber. Dtsch. Math.-Ver.* **4** (1897), 175–546. Trad. al francés por A. Lévi y Th. Got, con notas adicionales de G. Humbert y Th. Got: *Théorie des corps de nombres algébriques*, Librairie Scientifique A. Hermann et Fils, Paris, 1913.

[13] F. Klein, *Vorträge über ausgewählte Fragen der Elementargeometrie*, Ausgearb. F. Tägert, Leipzig, 1895. Trad. al francés por J. Griess: *Leçons sur certains questions de géométrie élémentaire*, Librairie Nony, Paris, 1896.

[14] F. Klein (ed.), Gauß wissenschaftliches Tagebuch 1796–1814, *Math. Ann.* **57** (1903), 1–34. Trad. al francés por P. Eymard y J. P. Lafon: Le journal mathématique de Gauss, *Revue d'histoire des sciences et de leurs applications* **9** (1956), 21–51.

[15] L. Kronecker, Beweis dass für jede Primzahl p die Gleichung $1 + x + x^2 + \cdots + x^{p-1} = 0$ irreductibel ist, *J. Reine Angew. Math. (Journal de Crelle)* **29** (1845), 280. [*Werke*, T. I, 1–4.] Trad. al francés: Nouvelle démonstration de l'irréductibilité de l'équation $1 + x + x^2 + \cdots + x^{p-1} = 0$, p étant un nombre premier, *Nouvelles Annales de Mathématiques* **8** (1849), 419–421.

[16] L. Kronecker, Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$, *J. Math. Pures Appl. (Journal de Liouville) Sér. I* **19** (1854), 177–192. [*Werke*, T. I, 75–92.]

[17] L. Kronecker, Démonstration de l'irréductibilité de l'équation $x^{n-1} + x^{n-2} + \cdots + 1 = 0$, ou n désigne un nombre premier, *J. Math. Pures Appl. (Journal de Liouville) Sér. II* **1** (1856), 399–400. [*Werke*, T. I, 99–102.]

[18] L. Kronecker, Grundüzge einer arithmetischen Theorie der algebraischen Grössen, *J. Reine Angew. Math. (Journal de Crelle)* **92** (1882), 1–122.

[19] L. Legendre, *Essai sur la Théorie des Nombres*, Paris, 1798 (2ème éd., 1808).

[20] E. Noether, Idealtheorie in Ringbereichen, *Math. Ann.* **83** (1921), 24–66.

[21] J. Serret, *Cours d'algèbre supérieure*, 3ème éd., Paris, 1866 (1e éd., 1849, 2ème éd., 1854).

[22] Th. Schönemann, Von denjenigen Moduln, welche Potenzen von Primzahlen sind, *J. Reine Angew. Math. (Journal de Crelle)* **32** (1846), 93–105.

[23] B. L. van der Waerden, *Moderne Algebre*, 2 vols., Berlin, Springer, 1930.

[24] J. L. Varona, *Recorridos por la teoría de números*, 2.ª ed., Textos Universitarios, Electolibris (coedición con RSME), Murcia, 2019.

[25] P. L. Wantzel, Recherches sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas, *J. Math. Pures Appl. (Journal de Liouville)* **1** (1837), 366–372.

[26] H. Weber, *Lehrbuch der Algebra*, vol. 1, F. Vieweg und Sohn, Braunschweig, 1895 (2d ed., 1898). Trad. de la 2d ed. al francés por J. Griess: *Traité d'Algèbre supérieure*, Gauthier-Villars, Paris, 1898.

Luis Español González, Dpto. de Matemáticas y Computación, Universidad de La Rioja
Correo electrónico: luis.espanol@unirioja.es