Universidad Autónoma de Madrid
Departamento de Matemáticas

La ciclotomía de Gauss

David Portuondo Muñoz

Trabajo de fin de grado dirigido por Fernando Chamizo

6 de junio de 2017

Índice

Resumen.

Gauss probó en el último capítulo, la sección VII, de su obra maestra *Disquisitiones Arithmeticae*, un bello teorema que caracteriza los polígonos regulares que se pueden construir con regla y compás. Desde el punto de vista actual, esto requiere la teoría de Galois abeliana, pero entonces ni Galois ni Abel habían nacido. Los argumentos de Gauss son bastante elementales y a su vez la base de varias ideas que inspiraron a Abel y Galois. El propósito del trabajo es explicar estos argumentos siguiendo el esquema del original. Parte de la dificultad radica en leer a Gauss dado que la notación que utiliza resulta a veces extraña, y dado que en la época no existían programas tipográficos de la eficiencia de LaTeX, lo cual dificulta enormemente su comprensión. Por otro lado, Gauss tiende a detenerse en explicaciones de cosas que en la actualidad nos parecen claras porque ahora forman parte de los temarios del grado. De este modo, lo que vamos a hacer es tomar lo que escribió Gauss como un esquema pero cambiaremos la notación cuando sea conveniente y utilizaremos atajos que hoy en día sean bien conocidos.

Abstract.

Gauss proved in the last chapter, section VII, of his masterpiece *Disquisitiones Arithmeticae*, a beautiful theorem that characterizes the regular polygons that can be constructed with ruler and compass. From the current point of view, this requires the Galois Abelian theory, but then neither Galois or Abel were born. Gauss's arguments are quite elementary and the basis of several ideas that inspired Abel and Galois. The purpose of the project is to explain these arguments following the original scheme. Part of the difficulty is reading Gauss because of the notation he uses, which is sometimes strange, and the absence of typographic programs of the efficiency of LaTeX that greatly complicate its understanding. On the other hand, Gauss tends to dwell on explanations of things that in the present seem clear to us because they are now part of the mathematics degree programs. Thus, what we are going to do is take what Gauss wrote as a scheme, but we will change the notation where appropriated and we will use currently well-known shortcuts.

1. La idea básica en breve

El trabajo consiste en entender con detalle la sección VII, el último capítulo, de las Disquisitiones Arithmeticae de Gauss. Allí se estudia qué polígonos regulares se pueden construir con regla y compás.

Construir un polígono regular equivale a encontrar los vértices del polígono inscrito en la circunferencia unidad. Es decir, basta con resolver la ecuación $x^n - 1 = 0$, donde n es el número de vértices. Sus soluciones son claramente $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ con $\zeta = e^{\frac{2\pi i}{n}}$. Vamos a considerar el caso $n = p$ con $p \neq 2$ primo, y ya veremos que el caso general se reduce de alguna forma a éste.

Esencialmente lo que probó Gauss es que si la factorización en primos de $p - 1$ es $p - 1 = q_1 q_2 \cdots q_s$ con $q_1 \leq q_2 \leq \cdots \leq q_s$, entonces, se puede expresar ζ como solución de una "cadena"de ecuaciones de grados $q_1, q_2, \ldots, q_s$. En este caso "cadena"significa que la primera ecuación tiene coeficientes racionales y en cada uno de los pasos siguientes uno puede tener coeficientes más complicados dados por combinaciones de raíces de las ecuaciones anteriores. Ahora, nosotros estamos limitados a utilizar regla y compás, lo cual requiere ecuaciones de segundo grado, por lo que parece natural reducir el problema al caso $p-1 = 2^n$. De esta forma, según el resultado, podríamos calcular $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ con ecuaciones cuadráticas y construir el polígono regular de p lados. En el resto de la introducción veremos cómo proceder algorítmicamente para calcular dichas ecuaciones.

Lo interesante de este resultado es que conecta temas en principio muy alejados de álgebra y de geometría plana de los griegos basándose en ideas simples de simetría que son la base de la teoría de Galois.

Tratemos por encima el ejemplo del polígono ($p = 5$) para ver cómo entran en juego las simetrías:

Antes de nada recordar un resultado básico de teoría de números. Para cualquier primo p existe un $1 \leq g < p$ tal que $g^0, g^1, \ldots, g^{p-2}$ da el conjunto de restos $1, 2, \ldots, p-1$ (quizá en otro orden) módulo p. En nuestro caso (cogiendo $g = 3$) tendríamos: $3^0 \equiv 1, 3^1 \equiv 3, 3^2 \equiv 4$ y $3^3 \equiv 2$ (mód 5).

Vamos ahora con las simetrías. Diremos que una expresión $P(\zeta)$ con $P \in \mathbb{Q}[x]$ tiene la simetría S_d con $d \mid p - 1$ si $P(\zeta) = P(\zeta^{g^d})$. Vamos a ir reduciendo las simetrías de $P(\zeta) = \zeta + \zeta^2 + \zeta^3 + \zeta^4$. Para ello ordenamos los exponentes según aparecen en

$g^k, k = 0, \ldots, 3$ módulo 5 y vamos tomando uno de cada dos elementos como sigue

$$\begin{array}{ll} S_1: & \zeta^1+\zeta^3+\zeta^4+\zeta^2 \\ & \quad /\qquad\quad \backslash \\ S_2: & \zeta+\zeta^4 \qquad \zeta^3+\zeta^2 \\ & \quad /\quad \backslash \qquad /\quad \backslash \\ S_4: & \zeta \quad \zeta^4 \quad \zeta^3 \quad \zeta^2 \end{array}$$

En general, siempre que $p-1=2^n$, procediendo de esta forma se pasa de $\sum \zeta^k$ hasta las raíces sueltas en n pasos con simetrías $S_{2^k}, k = 1, \ldots, 2^n$.

El resultado fundamental es que cualquier expresión que tenga la simetría S_d, se puede escribir como combinación lineal (con coeficientes racionales) de las expresiones que aparecen en el piso S_d del árbol.

Gauss observó que la suma y el producto de dos expresiones que tengan el mismo padre en el árbol adquieren las simetrías del piso de arriba. Esto es debido a que al aplicar la simetría S_d, es decir al cambiar ζ por ζ^{g^d}, a uno de los hijos del piso S_{2d}, éste se transforma en el otro hijo. Por ello tanto el producto como la suma de los hijos tienen simetría S_d.

Otra observación importante es que dado que $\zeta^p \equiv 1 (\text{mód } p)$ y que estamos ante una serie geométrica, entonces

$$1+\sum_{k=1}^{p-1}\zeta^k = \sum_{k=1}^{p}\zeta^k = \frac{1-\zeta^p}{1-\zeta} = 0. \tag{1.1}$$

Es decir, que el piso superior del árbol es $\sum_{k=1}^{p-1}\zeta^k = -1$.

Entonces, en el caso que estamos tratando,

$$S = (\zeta+\zeta^4)+(\zeta^3+\zeta^2) \quad y \quad P = (\zeta+\zeta^4)(\zeta^3+\zeta^2)$$

tienen simetría S_1 y por tanto son una combinación lineal racional de un sólo número (un múltiplo racional) de $\zeta^1+\zeta^3+\zeta^4+\zeta^2 = -1$. Es decir, son números racionales que podemos calcular:

$$S = -1 \quad y \quad P = -1.$$

Ahora, nótese que ambos términos, $\zeta+\zeta^4$ y $\zeta^3+\zeta^2$, son solución de la ecuación cuadrática $x^2 - Sx + P = 0$. Y resolviéndola llegamos a

$$r_1 = \zeta+\zeta^4 = \tfrac{-1+\sqrt{5}}{2} \qquad r_2 = \zeta^3+\zeta^2 = \tfrac{-1-\sqrt{5}}{2}$$

Haciendo lo mismo con el piso inferior del árbol tenemos que la suma y el producto de ζ y ζ^4 tienen las simetrías de su padre, S_2, y son combinación lineal de r_1 y r_2

$$\zeta+\zeta^4 = r_1 \qquad \zeta\cdot\zeta^4 = 1 = -r_1 - r_2$$

Y, repitiendo el argumento de antes, tenemos que ζ y ζ^4 son raíces de la ecuación $x^2 - r_1 x - r_1 - r_2 = x^2 - r_1 x + 1 = 0$, y de esta forma obtenemos una fórmula con raíces cuadradas para $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$

$$\cos\tfrac{2\pi}{p} = \tfrac{-1+\sqrt{5}}{4} \quad y \quad \sin\tfrac{2\pi}{p} = \tfrac{\sqrt{\sqrt{5}+5}}{2\sqrt{2}} \ .$$

Veamos telegráficamente el primer paso del caso $p = 17$ para terminar de aclarar el algoritmo:

En este caso, si H_1 y H_2 son los hijos,

$$H_1 = (\zeta^1 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2)$$
$$H_2 = (\zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6)$$

entonces:

$$S = H_1 + H_2 \quad y \quad P = H_1 \cdot H_2$$

y haciendo los cálculos obtenemos:

$$S = -1 \quad y \quad P = -4$$

Luego tanto H_1 como H_2 son soluciones de la ecuación $x^2 + x - 4 = 0$. Y resolviendo obtenemos:

$$H_1 = \tfrac{-1+\sqrt{17}}{2} \quad y \quad H_2 = \tfrac{-1-\sqrt{17}}{2} \ .$$

2. Algunas construcciones geométricas con regla y compás

En esta sección vamos a tratar el apartado geométrico del problema. Antes de nada, ¿qué significa que una medida es construible? Desde el punto de vista geométrico sería que podemos construir dicha distancia utilizando exclusivamente regla y compás. ¿Y desde el punto de vista algebraico? Hay varias maneras de traducir el problema de construcción al problema algebraico. Una drástica y rápida pasa por tomar éste último como definición de construible después de algunas explicaciones iniciales:

Fijemos una unidad de medida, por ejemplo, la dada por $(0,0)$ y $(1,0)$. Sabemos que las rectas tienen ecuaciones de primer grado y las circunferencias de segundo grado, por lo que, como mencionamos en la sección anterior (y es lo que esencialmente probó Gauss), todos los puntos construibles con regla y compás provienen de cadenas de ecuaciones cuadráticas.

Traduzcamos esto al lenguaje de la teoría de Galois: las coordenadas de todos los puntos construibles están en sucesivas extensiones cuadráticas de cuerpos. Por lo tanto, si $(x,y) \in \mathbb{R}^2$ es un punto construible con regla y compás, entonces existe una cadena de cuerpos

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n = L$$

con $[L_{k+1} : L_k] = 2$ y $x, y \in L \subset \mathbb{R}$.

Si a esto le añadimos que la suma, resta, división, multiplicación y raíces cuadradas de longitudes construibles también son construibles (fácil de ver en el diagrama de la figura 1),

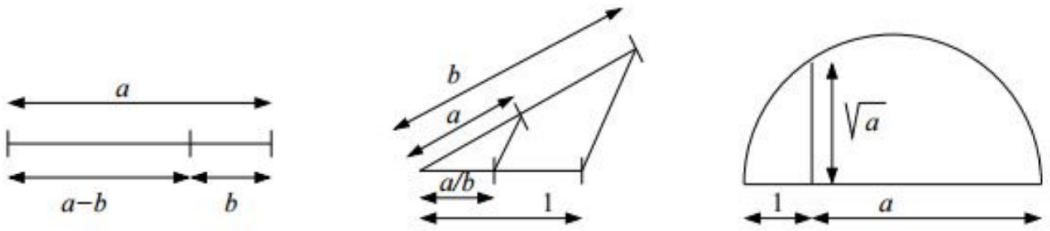

Figura 1:

1. Construcción de $a - b$ 2. Construcción de a/b 3. Construcción de $\sqrt{a}$

entonces cualquier elemento de un cuerpo real, L, para el que exista una cadena de subcuerpos como la anterior, puede ser obtenido como coordenada de un punto construible con regla y compás, es decir, se tiene la siguiente caracterización que tomaremos como definición:

Definición 2.1. Un punto $(x, y) \in \mathbb{R}$ es construible con regla y compás si y solo si x e y pertenecen a un cuerpo $L \subset \mathbb{R}$ tal que existe una cadena de subcuerpos

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n = L$$

donde todas las extensiones son de grado dos.

Definido ya lo que es una medida construible, pasemos a ver algún ejemplo de construcción de polígonos construibles:

Los casos del triángulo y del cuadrado son tan fáciles que los vamos a ver rápidamente con un simple diagrama

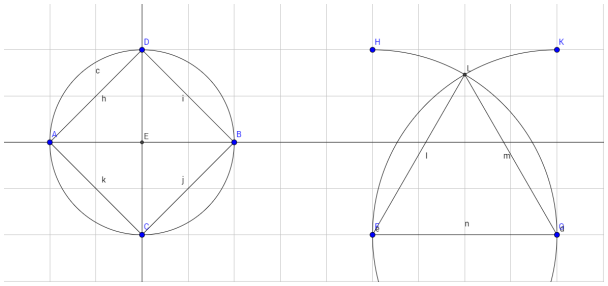

Figura 2:

Para el caso del pentágono vamos a servirnos de los cálculos realizados en la sección anterior, en donde llegamos a calcular

$$\cos \tfrac{2\pi}{5} = \tfrac{-1+\sqrt{5}}{4} \quad y \quad \sin \tfrac{2\pi}{5} = \tfrac{\sqrt{\sqrt{5}+5}}{2\sqrt{2}} \ .$$

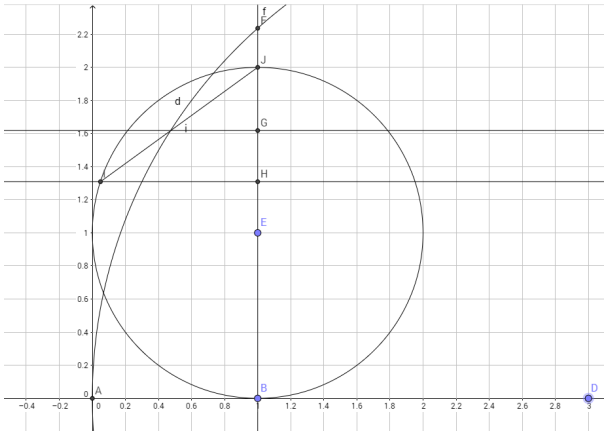

Figura 3:

Ahora, dado que en ambas expresiones solo hay sumas, restas, multiplicaciones, divisiones y raíces cuadradas de números naturales (distancias construibles), tenemos que tanto $\cos\frac{2\pi}{5}$ como $\sin\frac{2\pi}{5}$ son construibles. Hallamos $\cos\frac{2\pi}{5}$ geométricamente reproduciendo las operaciones (ver figura 2). Calculamos $\overline{BF} = \sqrt{5}$. A esa distancia le restamos 1 y nos queda $\overline{EF} = \sqrt{5} - 1$. Calculamos 2 mediatrices y llegamos a $\overline{EH} = \frac{\sqrt{5}-1}{4} = \cos\frac{2\pi}{5}$. Y la perpendicular en H interseca a la circunferencia unidad en I. Por lo que $\widehat{IEJ} = \zeta$ e $\overline{IJ}$ es uno de los lados del pentágono.

El teorema que anuncia Gauss es el siguiente:

Teorema 2.2. *El polígono regular de n lados es construible con regla y compás si y sólo si $n = 2^r p_1 p_2 \cdots p_k$ con p_i primos distintos tales que $p_i - 1$ es una potencia de dos (llamados primos de Fermat).*

Deduzcamos éste a partir de la versión simplificada del teorema que vimos en la sección anterior que dice que un polígono de un número primo impar de lados n es construible si n es un primo de Fermat.

Si nos fijamos, los teoremas difieren únicamente en dos cosas:

1. En la versión extendida aparece el factor 2^r.
2. En la versión extendida no sólo se consideran los primos de Fermat, sino también el producto de ellos.

Tratemos cada diferencia por separado:

1. Pasar de un polígono de n lados a uno de $2n$ lados se consigue haciendo la bisectriz de cada lado.
2. Queremos llegar a la conclusión de que para tratar el problema de $n = p_1 p_2 \cdots p_k$ con p_i primos de Fermat distintos entre sí, podemos tratar cada primo por separado. Para ello, hacemos uso del lema 2.3, con el que tenemos (quitando los exponentes) que si $n = p_1 \cdots p_k$, entonces el ángulo $\zeta = 2\pi/n$ se puede obtener como combinación lineal de los ángulos de considerar un único primo de Fermat. Esto es
$$\zeta = \frac{2\pi}{n} = \sum_{j=1}^{k} \frac{m_j 2\pi}{p_j}.$$

Lema 2.3. *Sea $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la factorización en primos de n, entonces existen números $m_j \in \mathbb{Z}$ tales que*
$$\frac{2\pi}{n} = \sum_{j=1}^{k} \frac{m_j 2\pi}{p_j^{\alpha_j}}.$$

Demostración. Veamos el caso de descomponer la fracción $\frac{m}{n}$ donde n es el producto de los números p_1, p_2 primos entre sí en suma de dos fracciones con denominadores p_1 y p_2. Es decir, el caso $\frac{m}{n} = \frac{x}{p_1} + \frac{y}{p_2}$ con $x, y \in \mathcal{N}$:

Está claro que para que se dé la igualdad $\frac{m}{n} = \frac{x}{p_1} + \frac{y}{p_2}$, se tiene que cumplir la ecuación $p_2x + p_1y = m$. Por lo que resolvemos la congruencia $p_2x \equiv m (\text{mod } p_1)$, y nos queda $x \equiv mp_2^{-1} (\text{mod } p_1)$ ya que p_1 y p_2 son coprimos. Y calculamos y con, $y = \frac{m-p_2x}{p_1}$.

Sea ahora el caso general en el que $n = p_1p_2 \cdots p_k$ con p_j coprimos entre sí $\forall j$. Separamos n en p_1, $p_2 \cdots p_k$ coprimos y aplicamos lo que acabamos de ver. Procediendo de esta forma llegamos a donde queríamos. □

Ahora, ¿qué pasa si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ con algún $\alpha_i \neq 1$? Es decir, ¿por qué Gauss no considera las posibles potencias de los primos de Fermat en su teorema? Porque en ese caso el polígono no sería construible, veámoslo:

Observación 2.4. Si el polígono regular de p^α lados es construible, $p > 2$ primo, $\alpha > 1$, entonces también lo es el de p^2 lados.

Demostración. Construyendo $p^{\alpha-2}$ ángulos adosados que midan $\frac{2\pi}{p^\alpha}$ radianes tenemos uno de $\frac{2\pi}{p^2}$. □

De esta forma, para poder restringirnos a n primo, sólo falta justificar que el polígono regular de p^2 lados con $p > 2$ primo no es construible. Para ello, bastaría con probar que la extensión de cuerpos $[\mathbb{Q}(e^{2\pi i/p^2}) : \mathbb{Q}]$ no es una potencia de dos, ya que por la caracterización de polinomio construible (teorema 2.2) tendríamos que $e^{2\pi i/p^2}$ no se podría construir con regla y compás.

Observación 2.5. El polinomio $P(x) = x^{p(p-1)} + x^{p(p-2)} + x^{p(p-3)} + \cdots + x^p + 1$ es irreducible sobre $\mathbb{Q}$.

Demostración. Lo probamos aplicando el criterio de Eisenstein a $P(x+1)$

$$P(x+1) = (x+1)^{p(p-1)} + (x+1)^{p(p-2)} + (x+1)^{p(p-3)} + \cdots + (x+1)^p + 1.$$

Y desarrollando los binomios nos queda algo de la forma

$$P(x+1) = a_{p(p-1)}x^{p(p-1)} + a_{p(p-2)}x^{p(p-2)} + a_{p(p-3)}x^{p(p-3)} + \cdots + a_2x^2 + a_1x + a_0$$

donde $a_{p(p-1)} = 1$, $a_0 = p$ y el resto de a_i son sumas de números combinatorios $\binom{p}{k}$ donde $k < p$. Por lo que existe un primo, en este caso p, tal que $p^2 \nmid a_0$, $p \nmid a_{p-1}$ y $p \mid a_i \ \forall i \neq 0, p-1$. Y $p \mid a_i$ ya que $p \mid \binom{p}{k}$ al ser $k < p$ y p primo. □

Veamos que $e^{2\pi i/p^2}$ es solución de $P(x)$. Esto se ve directamente utilizando que $\sum_{k=1}^{p} \zeta^k = 0$ (observación 1.1) ya que al evaluar nos queda $P(e^{2\pi i/p^2}) = \sum_{k=1}^{p} \zeta^k = 0$. Por tanto, tenemos un polinomio irreducible de grado $p(p-1)$ sobre $\mathbb{Q}$ en el que $e^{2\pi i/p^2}$ es raíz, es decir, tenemos lo que queríamos

$$[\mathbb{Q}(e^{2\pi i/p^2}) : \mathbb{Q}] = p(p-1) \tag{2.1}$$

donde p es impar, y por consiguiente, no es una potencia de dos.

Es decir, en esta sección hemos visto que podemos tratar la versión simplificada en la que n es un primo de Fermat para probar el caso general donde $n = 2^r p_1 p_2 \cdots p_k$ con p_i primos de Fermat.

A partir de ahora empezaremos a seguir fielmente lo que escribió Gauss.

3. El polinomio ciclotómico (Art. 337-341)

Estamos tratando la ecuación

$$x^n - 1 = 0,$$

y queremos ver cuales son sus posibles soluciones. Para ello obviamos la solución elemental $x = 1$. De esta forma reducimos el problema a ver los ceros del polinomio

$$p[x] = x^{n-1} + x^{n-2} + \cdots + x + 1 \qquad \text{con } n > 2 \text{ primo}, \tag{3.1}$$

el que es conocido como *polinomio ciclotómico*.

En esta sección nos ocuparemos de los artículos 337-341, donde Gauss demuestra la irreducibilidad de (3.1).

Teorema 3.1. *El polinómio ciclotómico (3.1) es irreducible en* $\mathbb{Q}[x]$.

En la actualidad, dicha prueba apenas ocupa unas escasas líneas haciendo uso del criterio de Eisenstein.

Demostración. (*Actual*) Es esencialmente la misma que la de la observación 2.5 de la hoja anterior (aplicar el criterio de Eisenstein al polinomio $p(x + 1)$). □

Centrémonos ahora en la prueba que dio Gauss. En ella utiliza dos resultados auxiliares

- Lema de Gauss
- Potencias de raíces.

El primero de ellos, el Lema de Gauss, aparece en el artículo 42 y dice que al factorizar polinomios con coeficientes enteros no pueden aparecer denominadores de la nada, veámoslo:

Lema 3.2. ***Lema de Gauss*** *Sea* $q[x]$ *un polinomio no constante con coeficientes enteros. Si* $q[x]$ *es irreducible sobre* $\mathbb{Z}[x]$*, entonces también lo es sobre* $\mathbb{Q}[x]$.

Demostración. Véase el artículo 42 de [Gau86] para la prueba de Gauss o [Ste89] para una prueba moderna. □

La otra observación dice que si tenemos un polinomio con coeficientes racionales o enteros, entonces al elevar sus raíces a una potencia entera positiva, esa propiedad no cambia:

Observación 3.3. Potencias de raíces

$$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\in A[x] \quad \Rightarrow \quad (x-\alpha_1^k)(x-\alpha_2^k)\cdots(x-\alpha_n^k)\in A[x],$$

donde $A=\mathbb{Q}$ ó $A=\mathbb{Z}$.

Demostración. Véase un esbozo en el artículo 338 ó una prueba actual en [Cha12]. □

La prueba en sí comienza en el artículo 340 en el que se trata el siguiente lema:

Lema 3.4. *Sea p un polinomio tal que $p\in\mathbb{Z}[x_1,x_2,\ldots,x_n]$ y sea $\zeta=e^{\frac{2\pi i}{n}}$ una raíz de la unidad. Entonces, $\forall\lambda\in\mathbb{Z}$ existen $A_i\in\mathbb{Z}$ tal que:*

- $p[(\zeta)^\lambda,(\zeta^2)^\lambda,\ldots,(\zeta^n)^\lambda]=A+A_1\zeta^\lambda+A_2\zeta^{2\lambda}+\cdots+A_{n-1}\zeta^{(n-1)\lambda}$
- $\sum_{\lambda=1}^n p[(\zeta)^\lambda,(\zeta^2)^\lambda,\ldots,(\zeta^n)^\lambda]=nA$

Demostración. Dado que productos entre raíces de la unidad vuelven a dar raíces de la unidad, es decir, $\prod_k\zeta^k=\zeta^j$, para ciertos $k's$ y cierta j, al evaluar el polinomio $p[x_1,x_2,\ldots,x_n]$ en $(\zeta,\zeta^2,\ldots,\zeta^n)$, nos quedará una expresión de la forma

$$p[\zeta,\zeta^2,\ldots,\zeta^n]=A+A_1\zeta+A_2\zeta^2+\cdots+A_{n-1}\zeta^{(n-1)},$$

donde los $A_j\in\mathbb{Z}$ al estar $p\in\mathbb{Z}[x_1,x_2,\ldots,x_n]$.

Evaluando ahora en $((\zeta)^\lambda,(\zeta^2)^\lambda,\ldots,(\zeta^n)^\lambda)$ vemos que lo que se había reducido a ζ^r en la expresión anterior, se hace ahora $\zeta^{\lambda r}$, de modo que:

$$p[(\zeta)^\lambda,(\zeta^2)^\lambda,\ldots,(\zeta^n)^\lambda]=A+A_1\zeta^\lambda+A_2\zeta^{2\lambda}+\cdots+A_{n-1}\zeta^{(n-1)\lambda},$$

y los coeficientes siguen estando en $\mathbb{Z}$.

Veamos ahora por qué

$$\sum_{\lambda=1}^n p[(\zeta)^\lambda,(\zeta^2)^\lambda,\ldots,(\zeta^n)^\lambda]=nA.$$

Esto es así debido a que n es primo y por ello dada cualquier raíz de la unidad $\zeta=e^{\frac{2\pi ki}{n}}$, para cierto valor $k\in[1,\ldots,n-1]$; $\zeta\neq\zeta^k\ \forall k\in[2,\ldots,n-1]$, es decir, se recorren todas las posibles soluciones. Llamando $\gamma=\sum_{k=1}^n\zeta^k$ tenemos

$$\sum_{\lambda=1}^n p[(\zeta)^\lambda,(\zeta^2)^\lambda,\ldots,(\zeta^n)^\lambda]=nA+A_1\gamma+A_2\gamma+\cdots+A_{n-1}\gamma.$$

Y, aplicando que $\gamma=\sum_{k=1}^p\zeta^k=0$ (por la ecuación (1.1)), nos queda

$$\sum_{\lambda=1}^n p[(\zeta)^\lambda,(\zeta^2)^\lambda,\ldots,(\zeta^n)^\lambda]=nA.$$

□

En el artículo 341 se enuncia el teorema (3.1) y se demuestra:

Demostración. ***Teorema 3.1.***

Supongamos que el polinomio ciclotómico $p[x] = x^{n-1} + x^{n-2} + \cdots + x + 1$ es divisible por el polinomio $q[x] \in \mathbb{Q}[x]$ de grado $\lambda < n - 1$

$$q[x] = x^{\lambda} + A_{\lambda-1}x^{\lambda-1} + A_{\lambda-2}x^{\lambda-2} + \cdots + A_1 x + A_0.$$

Entonces, por el lema 3.2, $q[x] \in \mathbb{Z}[x]$.

Cada raíz de $q[x]$ es a la vez una raíz de $p[x]$, luego es de la forma $\zeta = e^{\frac{2\pi k i}{n}}$ para cierto $k \in 1, \ldots, n-1$, y será $q[\zeta] = 0$. Esto implica que su conjugado $\frac{1}{\zeta}$ también es raíz, $q[\frac{1}{\zeta}] = 0$.

Y así, podríamos reescribir $q[x]$ como producto de $\frac{1}{2}\lambda$ factores dobles de la forma $(x^2 - 2x\cos\zeta^k + 1)$, con $k \in 1, \ldots, \frac{n-1}{2}$. Y, observando que $(x^2 - 2x\cos\zeta^k + 1)$ se puede expresar como $((x - \cos\zeta^k)^2 + (\sin\zeta^k)^2)$, llegamos a que $\forall x \in \mathbb{R}$, $q[x] \in \mathbb{R} > 0$.

Sean $q_1, q_2, \ldots, q_{n-1}$ los polinomios cuyas raíces son las raíces de $q[x]$ elevadas a $1, 2, \ldots, n-1$ respectivamente (nótese que con esta notación $q_1 = q[x]$).

Observando que cada raíz de $q_j[x]$ es a su vez una raíz de $p[x]$ y repitiendo el argumento que acabamos de ver para $q[x]$, tenemos que $\forall x \in \mathbb{R}$, $q_j[x] \in \mathbb{R} > 0$.

Por el lema 3.4,

$$q_1[1] + q_2[1] + \cdots + q_{n-1}[1] = A_0 n. \tag{3.2}$$

Veamos ahora que $\prod_{j=1}^{n-1} q_j = p^{\lambda}$:

Sean $\zeta^{k_1}, \zeta^{k_2}, \ldots, \zeta^{k_{n-1}}$ las raíces de $q[x]$, entonces tenemos:

$$\begin{array}{rcccccc}
q_1[x] & = & (x-\zeta^{k_1}) & (x-\zeta^{k_2}) & \cdots & (x-\zeta^{k_\lambda}) \\
q_2[x] & = & (x-(\zeta^{k_1})^2) & (x-(\zeta^{k_2})^2) & \cdots & (x-(\zeta^{k_\lambda})^2) \\
\vdots & & \vdots & \vdots & & \vdots \\
q_{n-1}[x] & = & (x-(\zeta^{k_1})^{n-1}) & (x-(\zeta^{k_2})^{n-1}) & \cdots & (x-(\zeta^{k_\lambda})^{n-1}) \\
 & & \downarrow & \downarrow & & \downarrow \\
 & & c_1 & c_2 & & c_\lambda
\end{array}$$

Si c_k son el producto de los términos de cada columna, es fácil ver que $c_k = c_j \forall k, j$ ya que en cada c_k están todas las raíces de $p[x]$ y ninguna repetida. Y agrupando adecuadamente los términos nos queda

$$\prod_{j=1}^{n-1} q_j = p^{\lambda}.$$

También tenemos que $\prod_{j=1}^{n-1} q_j[1] = n^{\lambda}$, ya que $p[1] = n$.

Ahora, dado que todos los coeficientes de $q[x]$ son enteros (observación 3.3), los coeficientes de $q_j[x]$ también lo son. Y como $\prod_{j=1}^{n-1} q_j[1] = n^\lambda$ y hay $n-1$ productos en un lado y λ en el otro y $\lambda < n-1$; por lo que habrá más de un $q_j[1]$ que sea 1 (al ser n primo) y el resto serán n o potencias de n. Nótese que $q_j[1]$ es mayor que 0, por lo que $q_j[1]$ no puede ser -1, que estropearía la prueba.

Así, la suma

$$q_1[1] + q_2[1] + \cdots + q_{n-1}[1] \equiv g \qquad (\text{mod. } n),$$

con $g \in 1, \ldots, n-1$. Por lo que tenemos contradicción con la ecuación (3.2),

$$q_1[1] + q_2[1] + \cdots + q_{n-1}[1] \equiv 0 \qquad (\text{mod. } n).$$

□

4. Periodos y sus propiedades (Art. 342-346)

El objetivo de esta sección es enunciar y demostrar el teorema 4.7 del artículo 346. Para ello, vamos a introducir los periodos, su notación y algunas propiedades.

Los periodos ya aparecieron en la primera sección del trabajo, pero sólo en el caso en que $n-1$ era una potencia de dos. Veamos el caso general:

Definición 4.1. Sea n un número primo, e un divisor de $n-1$ y $f = \frac{n-1}{e}$ (i.e. $n-1 = ef$). Sea g un generador de $\mathcal{U}(\mathbb{Z}_n)$, el grupo multiplicativo de unidades de $\mathbb{Z}_n$. Entonces, definimos el periodo (f, λ) como,

$$(f, \lambda) = \sum_{k=0}^{f-1} \zeta^{\lambda g^{ek}}, \qquad \text{para} \quad \lambda \in \mathbb{Z} \quad \text{dado y } \zeta = e^{2\pi i/n}.$$

Por ejemplo, cogiendo $n = 19$ tenemos, $n - 1 = 19 - 1 = 3 \cdot 6$, es decir, podemos coger $f = 6$ y $e = 3$. Y para $\lambda = 2$ y $\lambda = 3$ nos quedan periodos iguales cogiendo una raíz primitiva cualquiera como $g = 2$,

$$(6, 2) = (6, 3) = \zeta^2 + \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{16} + \zeta^{17}.$$

Aparentemente la definición depende del generador g que escojamos, pero no es así.

Observación 4.2. El periodo (f, λ) no depende del generador g que escojamos.

Demostración. Sean g, G generadores de $\mathcal{U}(\mathbb{Z}_n)$. Queremos ver que

$$\sum_{k=0}^{f-1} \zeta^{\lambda g^{ek}} = \sum_{k=0}^{f-1} \zeta^{\lambda G^{ek}}.$$

Dado que $g, G \in \mathcal{U}(\mathbb{Z}_n)$, podemos escribir $G \equiv g^w (\text{mod n})$, para cierto w.
Sea $\mu \in 1, \ldots, f-1$ tal que $\mu w \equiv v \pmod f$. Entonces tenemos,

$$ve \equiv \mu we \pmod{n-1}.$$

Y de esta forma, aplicando el Pequeño Teorema de Fermat ($g^{n-1} \equiv 1 (\text{mod } n)$, $\forall n$ primo) tenemos,

$$g^{ve} \equiv g^{\mu we} \equiv G^{\mu e} \pmod n.$$

Es decir, cualquier número de la primera serie será congruente con alguno de la segunda, y viceversa. Y de esta forma ambas sumas tienen las mismas raíces, y por tanto, son iguales. □

Todos los resultados que veremos serán para periodos similares.

Definición 4.3. Para un n dado, a los periodos con el mismo f (y por tanto e) se les llama periodos similares.

Observación 4.4. $(f,\lambda) \equiv (f,\lambda g^e) \equiv (f,\lambda(g^e)^2) \equiv \cdots \equiv (f,\lambda(g^e)^{f-1})$.

Demostración. Aplicando el Pequeño Teorema de Fermat vemos que podemos reducir el exponente de (g^e) módulo f,

$$\lambda(g^e)^f \equiv \lambda g^{n-1} \equiv \lambda \qquad (\text{mod } n).$$

Y es fácil ver que las f raíces de cada suma van a ser siempre las mismas independientemente de la raíz por la que se empiece. □

En el artículo 345 aparece un resultado importante en el que se ve que el conjunto

$$\mathcal{B} = \big\{1, (f,1), (f,g), (f,g^2), \ldots, (f,g^{e-1})\big\},$$

es una especie de "base entera" al hacer sumas, restas y multiplicaciones de periodos similares.

Teorema 4.5. *Cualquier polinomio en* $\mathbb{Z}[x_1,\ldots,x_m]$ *al ser evaluado en periodos similares da una expresión de la forma*

$$a_0 + b_0(f,1) + b_1(f,g) + \cdots + b_{e-1}(f,g^{e-1}) \qquad \textit{donde } a_0, b_0, \ldots b_{e-1} \in \mathbb{Z}.$$

Demostración. Sean (f,λ) y (f,μ) dos periodos similares. Entonces,

$$(f,\lambda)(f,\mu) = \zeta^{\mu}(f,\lambda) + \zeta^{\mu g^e}(f,\lambda) + \zeta^{\mu(g^e)^2}(f,\lambda) + \ldots.$$

Y, gracias a la observación 4.4 sabemos que $(f,\lambda) = (f,\lambda g^{te})$, $\forall t = 1,2,\ldots$, luego podemos escribirlo de la forma,

$$(f,\lambda)(f,\mu) = \zeta^{\mu}(f,\lambda) + \zeta^{\mu g^e}(f,\lambda g^e) + \zeta^{\mu(g^e)^2}(f,\lambda(g^e)^2) + \ldots.$$

Desarrollando cada $(f,\lambda(g^e)^t)$ $\forall t$, tenemos,

$$\begin{array}{rcccccccc}
(f,\lambda)(f,\mu) & = & \zeta^{\lambda+\mu} & + & \zeta^{\lambda g^e+\mu} & + & \cdots & + & \zeta^{\lambda(g^e)^{f-1}+\mu} + \\
 & & \zeta^{\lambda g^e+\mu g^e} & + & \zeta^{\lambda(g^e)^2+\mu g^e} & + & \cdots & + & \zeta^{\lambda(g^e)^f+\mu g^e} + \\
 & & \zeta^{\lambda(g^e)^2+\mu(g^e)^2} & + & \zeta^{\lambda(g^e)^3+\mu(g^e)^2} & + & \cdots & + & \zeta^{\lambda(g^e)^{f+1}+\mu(g^e)^2} + \\
 & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}$$

Y sumando cada columna llegamos a

$$(f,\lambda)(f,\mu) = (f,\lambda+\mu) + (f,\lambda g^e+\mu) + \cdots + (f,\lambda(g^e)^{f-1}+\mu). \tag{4.1}$$

Ahora, dado que los términos particulares de (4.1) coinciden con alguna de las sumas $(f,0),(f,1),\ldots,(f,g^{e-1})$; podemos reescribir la expresión de la siguiente forma,

$$(f,\lambda)(f,\mu) = a_0 f + b_0(f,1) + b_1(f,g) + \cdots + b_{e-1}(f,g^{e-1}),$$

con $a_0, b_0, b_1 \cdots \in \mathbb{Z}$.

Por inducción concluimos que el resultado es cierto para cualquier número finito de productos.

Y nos falta ver qué pasa con la suma de periodos similares. Pero se ve directamente que agrupando términos llegamos a una expresión de la forma que buscábamos. □

Corolario 4.6. *Además, en una identidad de este tipo se pueden multiplicar todos los segundos argumentos de los periodos por una misma constante k no divisible por n y la identidad se sigue cumpliendo, esto es, sea $p \in \mathbb{Z}[x_1,\ldots,x_m]$,*

$$p[1,(f,k),(f,kg)\ldots,(f,kg^{e-1})] = a_0 + b_0(f,k) + b_1(f,kg) + \cdots + b_{e-1}(f,kg^{e-1}).$$

Demostración. Basta notar que al multiplicar λ y μ por k, k sale como factor común,

$$(f,k\lambda)(f,k\mu) = (f,k(\lambda+\mu))+(f,k(\lambda g^e+\mu))+(f,k[\lambda(g^e)^2+\mu])+\cdots+(f,k[\lambda(g^e)^{f-1}+\mu]),$$

y seguir la demostración del teorema 4.5. □

Vamos ahora con el teorema que hemos mencionado al principio de la sección y que ha motivado todos los pasos que hemos dado hasta el momento:

Teorema 4.7. *Suponiendo que λ es un número no divisible por n, y escribiendo por brevedad p en lugar de (f,λ), cualquier otro periodo similar (f,μ), en el cual μ no es divisible por n, puede ser reducido a la forma*

$$(f,\mu) = a_0 + a_1 p + a_2 p^2 + \cdots + a_{e-1}p^{e-1}, \qquad \textit{donde} \quad a_0, a_1 \cdots \in \mathbb{Q}.$$

Veamos un ejemplo para ilustrar lo visto hasta ahora y para facilitar el entendimiento de la demostración del teorema:

Supongamos que $n = 13$ y $f = 3$, con ello $e = 4$. Podemos tomar $g = 2$ (aunque otros generadores dan el mismo resultado). La lista de los periodos, destacando a la izquierda los que aparecen en $\mathcal{B}$ con esta elección de g, es:

$$\begin{array}{rcccc} X := (3,1) & = & \zeta+\zeta^3+\zeta^9 & = & (3,3) = (3,9) \\ Y := (3,2) & = & \zeta^2+\zeta^6+\zeta^5 & = & (3,6) = (3,5) \\ Z := (3,4) & = & \zeta^4+\zeta^{12}+\zeta^{10} & = & (3,12) = (3,10) \\ T := (3,8) & = & \zeta^8+\zeta^{11}+\zeta^7 & = & (3,11) = (3,7) \end{array}$$

Supongamos que queremos expresar T en términos de X. Gauss nos dice que tomemos las potencias de 1 a $e-1$ de $X=(3,1)$ y las expresemos como combinación lineal entera de los elementos de $\mathcal{B}$, que en nuestro caso es $\{1,X,Y,Z,T\}$. Esto es posible (y algorítmico) por el teorema 4.5. En la primera ecuación no usa X evitando la tautología $X=X$. Simplemente emplea que las suma de todas las raíces de la unidad, incluyendo el uno, es cero y por tanto $X=-1-Y-Z-T$. Haciendo las cuentas lo que sale es

$$\begin{array}{lcccccc} (3,1)^1 & = & -1 & & -Y & -Z & -T \\ (3,1)^2 & = & & & Y & +2Z & \\ (3,1)^3 & = & 6 & +X & +3Y & & +3T \end{array}$$

Tenemos 3 ecuaciones, entonces podemos eliminar $3-1$ variables, por "métodos conocidos", según Gauss (¡hoy diríamos por eliminación de Gauss!). Al eliminar la Y y la Z nos quedamos con algo que involucra la X y la T y potencias de X en el primer miembro. De ello se deduce

$$T=-\frac{5}{3}X-X^2-\frac{1}{3}X^3.$$

Vamos ahora con la demostración del teorema 4.7:

Demostración. Designamos por $p,p_1,p_2,\ldots,p_{e-1}$ a los periodos

$$(f,\lambda),(f,\lambda g),(f,\lambda g^2),\ldots,(f,\lambda g^{e-1}).$$

Obsérvese que $0=1+p+p_1+\cdots+p_{e-1}$, dado que están todas las raíces de la unidad.

Tomando ahora potencias en p y teniendo en mente el teorema (4.5), nos quedan expresiones de este tipo

$$\begin{array}{rcl} 0 & = & p^2+a+a_0p+a_1p_1+\cdots+a_{e-1}p_{e-1} \\ 0 & = & p^3+b+b_0p+b_1p_1+\cdots+b_{e-1}p_{e-1} \\ 0 & = & p^4+c+c_0p+c_1p_1+\cdots+c_{e-1}p_{e-1} \\ & & \vdots \\ 0 & = & p^{e-1}+d+d_0p+d_1p_1+\cdots+d_{e-1}p_{e-1} \end{array}$$

donde los $a,b,d,\cdots\in\mathbb{Z}$, y observamos que son independientes de λ, es decir, se obtienen las mismas ecuaciones independientemente del valor que le demos.

Ahora, dado que en $p_1,p_2,\ldots,p_{e-1}$ están todos los periodos similares a p, (f,μ) deberá coincidir con alguno de ellos. Podemos suponer $(f,\mu)=p_1$.

Ya que tenemos $e-1$ ecuaciones, podemos quitarnos $e-2$ incógnitas por eliminación de Gauss. Y llegar a una expresión de la forma

$$0=A+Bp+Cp^2+\cdots+Dp^{e-1}+Ep_1,$$

donde $A, B, C, \ldots, D \in \mathbb{Z}$ y al menos uno de ellos $\neq 0$.

Nos falta probar que E no se anula.

Supongamos $E = 0$, entonces:

$$0 = A + Bp + Cp^2 + \cdots + Dp^{e-1}. \tag{4.2}$$

Esta ecuación en p, al tener grado $e-1$, tendrá a lo sumo $e-1$ soluciones distintas. Pero dado que las ecuaciones de las cuales se deduce (4.2) son independientes de λ, tenemos que $(f,1),(f,g),\ldots,(f,g^{e-1})$ son soluciones. Es decir, tenemos e soluciones para una ecuación de grado $e-1$, por lo que al menos dos de estas sumas deben ser iguales.

Supongamos que una de estas sumas contiene las raíces $\zeta^{\sigma_0}, \zeta^{\sigma_1}, \ldots, \zeta^{\sigma_{f-1}}$, y la otra las raíces $\zeta^{\eta_0}, \zeta^{\eta_1}, \ldots, \zeta^{\eta_{f-1}}$, donde todos los exponentes son positivos y menores que n.

Consideramos ahora el polinomio

$$r[x] = x^{\sigma_0} + x^{\sigma_1} + \cdots + x^{\sigma_{f-1}} + x^{\eta_0} + x^{\eta_1} + \cdots + x^{\eta_{f-1}},$$

que es un polinomio de grado menor que n, donde $r[0] = 0$ y $r[\zeta] = 0$.

De esta forma $r[x]$ tiene el factor $(x-\zeta)$ en común con el polinomio ciclotómico $p[x]$, y vamos a ver que esto es absurdo.

Dado que $r[x]$ y $p[x]$ son polinomios con coeficientes racionales, al calcular el máximo común divisor entre ellos tiene que dar otro polinomio con coeficientes racionales. Pero este polinomio no puede ser 1 al tener una raíz en común, ni puede tener grado $n-1$ al ser ambos de grado $n-1$ y con una raíz diferente ($r[0] = 0$ y $p[0] \neq 0$).

Y así, llegamos a una contradicción ya que $p[x]$ es irreducible en $Q[x]$ por el teorema 3.1.

□

5. Periodos y sus propiedades (Art. 347-358)

En esta sección probaremos que cada periodo compuesto por f raíces de la unidad es raíz de un polinomio de grado d cuyos coeficientes son periodos compuestos por df raíces.

Empezamos por el artículo 347, en el que se enuncia el siguiente teorema:

Teorema 5.1. *Si $F \in \mathbb{Q}[x_1, \ldots, x_f]$ es un polinomio simétrico, entonces*

$$F(\zeta^{\lambda}, \zeta^{\lambda g^e}, \zeta^{\lambda g^{2e}}, \ldots, \zeta^{\lambda g^{e(f-1)}}) = A + \sum_{j=0}^{e-1} a_j (f, g^j) \qquad \text{con } A, a_j \in \mathbb{Q}.$$

Demostración. Por el lema 3.4, $F(\zeta^{\lambda}, \zeta^{\lambda g^e}, \zeta^{\lambda g^{2e}}, \ldots, \zeta^{\lambda g^{e(f-1)}})$ es reducido a la forma

$$F(\zeta^{\lambda}, \zeta^{\lambda g^e}, \zeta^{\lambda g^{2e}}, \ldots, \zeta^{\lambda g^{e(f-1)}}) = A + \sum_{j=1}^{n-1} a_j \zeta^{j\lambda}, \tag{5.1}$$

y tenemos que ver que las raíces que pertenecen al mismo periodo de f términos tienen los mismos coeficientes en esta expresión.

Al ser F un polinomio simétrico, podemos permutar ζ^{λ} por $\zeta^{\lambda g^{me}}$ al evaluar, obteniendo el mismo resultado. De esta forma, si al operar y simplificar sale en algún sitio un $a\zeta^{\lambda b}$, también sale un $a\zeta^{\lambda b g^{me}}$. Y repitiendo el proceso con el resto de valores llegamos a la conclusión de que todas las raíces contenidas en $(f, \lambda b)$ tienen el mismo coeficiente en la ecuación (5.1).

□

Veamos un ejemplo:
Sea $n = 7$, $e = 2$, $f = 3$ y $F = x(y + 2) + z(x + 2) + y(z + 2)$. Calculamos,

$$F(\zeta^{\lambda}, \zeta^{\lambda g^e}, \zeta^{\lambda g^{2e}}, \ldots, \zeta^{\lambda g^{e(f-1)}}) = F(\zeta, \zeta^2, \zeta^4) = (\zeta^3 + \zeta^5 + \zeta^6) + 2(\zeta + \zeta^2 + \zeta^4),$$

y de esta forma nos queda,

$$F(\zeta, \zeta^2, \zeta^4) = 2(3, 1) + (3, 3).$$

En el artículo 348 Gauss muestra cómo aplicar el teorema 5.1 a polinomios:

Al operar $P = (x - x_1)(x - x_2) \cdots (x - x_f)$, los coeficientes de P son funciones simétricas en $x_1, x_2, \ldots, x_f$. Por ejemplo, el coeficiente de x^{f-1} es $-(x_1 + x_2 + \cdots + x_n)$ y el término independiente es $(-1)^f x_1 x_2 \cdots x_f$. Entonces tomando como x_i las raíces de la unidad que aparecen en (f, λ) se tiene, a partir del teorema 5.1, que los coeficientes se pueden escribir en términos de los $(f, \lambda g^j)$, $\forall j \in 0, \ldots, e - 1$.

De esta forma, podemos descomponer el polinomio ciclotómico en e polinomios de grado f en el que cada uno de ellos contiene a las f raíces de cada periodo (f, g^j). Y estos polinomios son fáciles de especificar una vez encontrada una de las e sumas $(f, \lambda g^j)$, ya que todos los coeficientes de estos polinomios son combinación lineal de dichas sumas y todas ellas se deducen de una sola por el teorema 4.7.

Veamos un ejemplo:

En el caso $n = 7$, se tiene $(3, 1) = \zeta + \zeta^2 + \zeta^4$. Vamos a calcular los coeficientes de $P = (x - \zeta)(x - \zeta^2)(x - \zeta^4)$ en términos de los periodos:

$$P = x^3 - (\zeta + \zeta^2 + \zeta^4)x^2 + (\zeta^3 + \zeta^5 + \zeta^6)x - 1 = x^3 - (3, 1)x^2 + (3, 3)x - 1.$$

En el artículo 350 se extiende el teorema 5.1 evaluando en periodos en lugar de en raíces separadas.

Teorema 5.2. *Si $F \in \mathbb{Q}[x_1, \ldots, x_{e'}]$ es un polinomio simétrico y $f = e'f'$, entonces*

$$F((f', \lambda), (f', \lambda g^e), (f', \lambda g^{2e}), \ldots, (f', \lambda g^{e(e'-1)}) = A + \sum_{j=0}^{e-1} a_j (f, g^j) \qquad \text{con } A, a_j \in \mathbb{Q}.$$

Lema 5.3. *Sea $n - 1 = ef$ y $f = e'f'$, entonces cada periodo (f, λ) está compuesto por periodos (f', λ) de la siguiente forma:*

$$(f, \lambda) = \sum_{l=0}^{e'-1} (f', \lambda g^{el}).$$

Demostración. La clave de la demostración está en fijarnos en que los números menores que $f = e'f'$ siempre se pueden escribir de la forma $l + e'k$, con $0 \leq l < e'$ y $0 \leq k < f'$. De esta forma, podemos reescribir $(f, \lambda) = \sum_{k=0}^{f-1} \zeta^{\lambda g^{ek}}$ como,

$$(f, \lambda) = \sum_{l=0}^{e'-1} (\sum_{k=0}^{f'-1} \zeta^{\lambda g^{e(l+e'k)}}) = \sum_{l=0}^{e'-1} (f', \lambda g^{el}).$$

□

Demostración del Teorema 5.2. Aplicando el teorema 4.5 tenemos

$$F((f', \lambda), (f', \lambda g^e), (f', \lambda g^{2e}), \ldots, (f', \lambda g^{e(e'-1)}) = A + \sum_{j=0}^{ee'-1} a_j (f', g^j) \qquad \text{con } A, a_j \in \mathbb{Q}.$$

Y tenemos que ver que el coeficiente de (f', g^j) es el mismo que el de $(f', g^j g^{ev})$ $\forall v \in \mathbb{Z}$, ya que por la observación 5.3 esto supone que todas las raíces de (f, g^j) tienen el mismo coeficiente.

Al ser F un polinomio simétrico, podemos permutar (f', λ) por $(f', \lambda g^{ev})$ al evaluar, obteniendo el mismo resultado. De esta forma, si al operar y simplificar sale en algún sitio un $a\zeta^{\lambda b}$, también sale un $a\zeta^{\lambda b g^{ev}}$. De esto se sigue que el coeficiente de $(f', \lambda b)$ es igual que el de $(f', \lambda b g^{ev})$. Y repitiendo el proceso para todo $v \in 0, \ldots, e' - 1$ y por el lema 5.3 tenemos el mismo coeficiente para todas las raíces de $(f, \lambda b)$.

□

Ahora, procediendo como antes con el polinomio simétrico $P = (x-x_1)(x-x_2)\cdots(x-x_{e'})$ nos queda el siguiente corolario:

Corolario 5.4. *Consideramos el polinomio simétrico $P = (x - x_1)(x - x_2)\cdots(x - x_{e'})$ y tomamos como x_j los periodos $(f', \lambda g^{(j-1)e})$, entonces los coeficientes de P se escriben en términos de los periodos (f, μ), donde $f = e'f'$.*

Juntando todo lo visto hasta el momento podemos crear un algoritmo para calcular ζ resolviendo ecuaciones del grado más pequeño posible. De hecho, si $n-1$ factoriza como $p_1 \cdot p_2 \cdots p_k$, entonces ζ se puede expresar como solución de una cadena de ecuaciones de grados $p_1, \ldots, p_k$ como anunciamos al principio del trabajo. Veamos cómo en el siguiente ejemplo.

Analicemos con detalle el caso $n = 13$. Seleccionamos la factorización $12 = 2 \cdot 2 \cdot 3$ (escogemos esta factorización para que nos queden las ecuaciones con el grado más pequeño posible). De esta forma, los f correspondientes son $12 = 12/1$, $6 = 12/2$, $3 = 12/(2 \cdot 2)$ y $1 = 12/(2 \cdot 2 \cdot 3)$. El árbol que indica la relación entre estos periodos (los que forman parte de otros) es:

$$-1 = \zeta + \zeta^2 + \zeta^3 + \ldots \zeta^{12} = (12,1) = \begin{cases} (6,1) \begin{cases} (3,1) \begin{cases} (1,1) = \zeta \\ (1,3) = \zeta^3 \\ (1,9) = \zeta^9 \end{cases} \\ (3,4) \begin{cases} (1,4) = \zeta^4 \\ (1,10) = \zeta^{10} \\ (1,12) = \zeta^{12} \end{cases} \end{cases} \\ (6,2) \begin{cases} (3,2) \begin{cases} (1,2) = \zeta^2 \\ (1,5) = \zeta^5 \\ (1,6) = \zeta^6 \end{cases} \\ (3,7) \begin{cases} (1,7) = \zeta^7 \\ (1,8) = \zeta^8 \\ (1,11) = \zeta^{11} \end{cases} \end{cases} \end{cases}$$

Este árbol se ha formado de derecha a izquierda fijándonos en qué periodos contienen a las raíces de cada periodo inicial. De esta forma, por ejemplo, las raíces del periodo $(1,1) = \zeta$ están contenidas en $(3,1) = \zeta + \zeta^3 + \zeta^9$, que a su vez están contenidas en $(6,1) = \zeta + \zeta^3 + \zeta^9 + \zeta^4 + \zeta^{10} + \zeta^{12}$ y estás en $(12,1)$, que contiene a todas.

Hallemos una expresión de $(6,1)$ y $(6,2)$. Para ello tomamos el polinomio $P = \big(x - (6,1)\big)\big(x - (6,2)\big)$. Por el teorema 5.2, al ser P simétrico, sabemos que los coeficientes de P son combinaciones lineales de los periodos superiores (en este caso solo hay un periodo superior $(12,1) = -1$). Nos queda, $P = x^2 - (12,1)x + 3(12,1) = x^2 + x - 3$. Y resolviendo la ecuación, tenemos que $(6,1)$ y $(6,2)$ son $(-1 \pm \sqrt{13})/2$. Para saber cuál es cuál, se usa una calculadora comprobando cuál es positivo y se obtiene,

$$(6,1) = (-1 + \sqrt{13})/2 \quad \text{y} \quad (6,2) = (-1 - \sqrt{13})/2.$$

Hagamos lo mismo para hallar una expresión de $(3,1)$. Sabemos que $(3,1)$ es solución del polinomio $P = \big(x - (3,1)\big)\big(x - (3,4)\big)$, y que los coeficientes de dicho polinomio son combinaciones lineales de los periodos $(6,1)$ y $(6,2)$. Nos queda,

$$P = x^2 - (6,1)x + (6,2) + 3.$$

Y resolviendo y escogiendo la raíz adecuada para cada periodo tenemos que

$$(3,1) = \tfrac{-1+\sqrt{13}+(26-7\sqrt{13})i}{4} \quad \text{y} \quad (3,4) = \tfrac{-1+\sqrt{13}-(26-7\sqrt{13})i}{4}.$$

Y por último, para hallar la raíz de $(1,1) = \zeta$, tendríamos que repetir el proceso resolviendo la ecuación $(x - \zeta)(x - \zeta^3)(x - \zeta^9) = 0$, que en término de los periodos anteriores sería resolver,

$$x^3 - (3,1)x^2 + (3,4)x - 1 = 0.$$

De esta forma hemos descrito un algoritmo para hallar ζ. Y todas las demás raíces se obtienen a partir de ésta por una combinación lineal de sus potencias por el teorema 4.7.

En este ejemplo se ve la necesidad a la hora de construir polígonos con regla y compás de que solo aparezca el factor 2 en la descomposición de $n-1$, ya que si aparece cualquier otro factor tendríamos que resolver ecuaciones de orden mayor que 2, lo que es imposible en general al estar limitados a regla y compás.

6. Reducción de la ecuación ciclotómica

Gauss dedica los artículos 359 y 360 a la resolubilidad del problema por radicales.

Por el corolario 5.4 sabemos que los periodos $(f', \lambda g^{el})$ son soluciones de una ecuación de grado e' con coeficientes que dependen de los periodos (f, μ), con $n-1 = ef$ y $f = e'f'$.

Gauss dedica el artículo 360 a probar que esta ecuación se puede resolver utilizando sólo $\sqrt[e']{1}$ y con otras raíces e'-ésimas que dependen de los coeficientes. La situación es que suponemos los (f, λ) conocidos y queremos resolver la ecuación para los (f', ν) que están contenidos en ellos según el lema 5.3. Consideramos los polinomios

$$L_j(x) = \sum_{l=0}^{e'-1} (f', \lambda g^{e(l+j)}) x^l \quad j = 0, 1, 2, \dots e' - 1 \qquad \text{y} \qquad P(x) = \frac{1}{e'} \sum_{j=0}^{e'-1} \big(L_j(x)\big)^{e'}.$$

Ahora, dado que los L_j son los mismos polinomios pero permutando cíclicamente los coeficientes, al expandir las potencias de P y escribir los coeficientes en términos de los (f', ν), todos los $(f', \lambda g^{e(l+j)})$ aparecerán multiplicados por lo mismo. Y por el lema 5.3 tenemos que $P(x) = \sum_{k=0}^{e-1} (f, g^k) p_k(x)$, para ciertos polinomios $p_k \in \mathbb{Q}[x]$.

De la permutación cíclica de los coeficientes de los L_j tenemos, llamando $\xi = e^{\frac{2\pi i}{e'}}$,

$$L_0(\xi) = \xi^j L_j(\xi).$$

E introduciendo esto en la definición de P,

$$(L_0(\xi))^{e'} = P(\xi) = \sum_{k=0}^{e-1} (f, g^k) p_k(\xi)$$

que es una cantidad conocida si lo son los (f, λ) y ξ, porque los p_k son polinomios con coeficientes racionales. Si llamamos $T_1 = \sum_{k=0}^{e-1} (f, g^k) p_k(\xi)$ tenemos

$$\sqrt[e']{T_1} = \sum_{l=0}^{e'-1} (f', \lambda g^{el}) \xi^l$$

para alguna elección del argumento, y si en vez de tomar ξ hubiéramos tomado otra raíz e'-ésima ξ^j se tendría en general

$$\sqrt[e']{T_j} = \sum_{l=0}^{e'-1} (f', \lambda g^{el}) \xi^{jl} \qquad \text{para} \quad j = 1, 2, \dots, e' \qquad \text{y} \qquad T_j = (L_0(\xi^j))^{e'}.$$

Y escribiendo $x_l = (f', \lambda g^{el})$ esto es un sistema lineal de e' ecuaciones con e' incógnitas con determinante de Vandermonde y, por tanto no singular. De esta forma, cada periodo

x_l se expresa en términos de las raíces e'-ésimas $\sqrt[e']{T_j}$ y ξ. En definitiva, las ecuaciones que dan los (f', ν) en términos de los (f, λ) se resuelven utilizando solo radicales de índice e'.

De esta forma, las ecuaciones de grado mayor que cuatro, que en general no son resolubles por radicales, para los periodos sí lo son.

Los artículos 365 y 366 son una especie de resumen y conclusión de todo el trabajo. Veamos su contenido conectándolo con todas las secciones anteriores:

El objetivo es autoconvencernos de que hemos probado lo que queríamos, es decir, que el polígono regular de n lados es construible con regla y compás si y sólo si $n = 2^r p_1 p_2 \cdots p_k$ con p_i primos de Fermat distintos. Veamos primero el caso en el que n es primo para tratar luego el caso compuesto:

- n primo: por la discusión precedente, hemos reducido la división del círculo en n partes a la solución de tantas ecuaciones como factores haya en el número $n-1$, donde el grado de cada ecuación se determina por el tamaño de los factores. Por lo tanto, necesitamos que $n-1$ sea una potencia de dos para que la división del círculo se reduzca únicamente a la resolución de ecuaciones cuadráticas y, de este modo, por la definición 2.1, sea construible.

  Tenemos entonces que n es primo y de la forma $n = 2^m + 1$. Pero para ello, el exponente m tiene que ser de la forma $m = 2^\nu$. De otro modo, si $m = \varsigma\eta$, donde ς es impar, es fácil probar que $2^m + 1$ es divisible por $2^\eta + 1$ y así necesariamente compuesto.

  De esta modo tenemos que n es de la forma $n = 2^{2^\nu} + 1$ (aunque no todos estos números son primos $\forall \nu \in \mathcal{N}$).

  Siempre que $n-1$ contengan otros factores primos distintos de dos, somos llevados a ecuaciones de mayor grado. Gauss afirma que puede probar con todo rigor que estas ecuaciones de mayor grado no pueden ser eludidas de ninguna forma ni pueden ser reducidas a ecuaciones de menor grado, pero no incluye la demostración. Hoy sería tan fácil como decir que al añadir raíces cuadradas siempre el grado de la extensión es una potencia de dos, por lo que este caso no se podría dar.

- n compuesto: la extensión al caso $n = p_1 p_2 \cdots p_k$ con p_i primos de Fermat distintos entre sí la podemos hacer gracias al lema 2.3. Y de estos primos p_i, los que aceptan potencias de grado mayor que 1 son aquellos en los que la extensión dada por la ecuación (2.1),
$$[\mathbb{Q}(e^{2\pi i/p^2}) : \mathbb{Q}] = p(p-1),$$
es una potencia de dos. Por lo que el único primo p que cumple esta condición es

el dos.

De este modo, los polígonos construibles con regla y compás son aquellos de la forma,

$$n = 2^r p_1 p_2 \cdots p_k$$

con p_i primos de Fermat distintos y $r \in \mathcal{N}$.

7. Polígono de 17 lados

En el artículo 365 tenemos un formulón gigantesco para el coseno de $2\pi/17$.

$$-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

Con mucha paciencia, podríamos ir construyendo poco a poco cada una de las raíces cuadradas y las operaciones aritméticas correspondientes para llegar finalmente a un segmento de longitud $\cos(2\pi/17)$. Cuando su perpendicular en el extremo derecho interseca una circunferencia unidad con centro en el otro extremo, tendremos el ángulo de $2\pi/17$. Todo esto parece muy laborioso y surge la pregunta de si no es posible algo más práctico para construir el polígono de 17 lados.

En esta sección veremos una posible sencilla solución del problema:

Llamamos $\theta=\frac{2\pi}{17}$ y $\zeta_k=\cos k\theta+i\sin k\theta$. Calculamos los periodos

$$\begin{array}{rcrcl}
x_1 & = & (8,1) & = & \zeta_1+\zeta_9+\zeta_{13}+\zeta_{15}+\zeta_{16}+\zeta_8+\zeta_4+\zeta_2\\
x_2 & = & (8,3) & = & \zeta_3+\zeta_{10}+\zeta_5+\zeta_{11}+\zeta_{14}+\zeta_7+\zeta_{12}+\zeta_6\\
y_1 & = & (4,1) & = & \zeta_1+\zeta_{13}+\zeta_{16}+\zeta_4\\
y_2 & = & (4,2) & = & \zeta_9+\zeta_{15}+\zeta_8+\zeta_2\\
y_3 & = & (4,3) & = & \zeta_3+\zeta_5+\zeta_{14}+\zeta_{12}\\
y_4 & = & (4,6) & = & \zeta_{10}+\zeta_{11}+\zeta_7+\zeta_6.
\end{array}$$

Ahora, como $\zeta_k+\zeta_{17-k}=2\cos k\theta$, tenemos

$$\begin{array}{rcl}
x_1 & = & 2(\cos\theta+\cos 8\theta+\cos 4\theta+\cos 2\theta)\\
x_2 & = & 2(\cos 3\theta+\cos 7\theta+\cos 5\theta+\cos 6\theta)\\
y_1 & = & 2(\cos\theta+\cos 4\theta)\\
y_2 & = & 2(\cos 8\theta+\cos 2\theta)\\
y_3 & = & 2(\cos 3\theta+\cos 5\theta)\\
y_4 & = & 2(\cos 7\theta+\cos 6\theta).
\end{array}$$

Sabemos que $x_1+x_2=-1$. Y utilizando la identidad

$$2\cos(m\theta)\cos(n\theta)=\cos((m+n)\theta)+\cos((m-n)\theta),$$

también tenemos que $x_1x_2=4(x_1+x_2)=-4$.

De esta forma, x_1 y x_2 son ceros del polinomio $p(t)=t^2-(x_1+x_2)t+(x_1x_2)$, es decir, de

$$p(t)=t^2+t-4. \tag{7.1}$$

De forma similar obtenemos que $y_1 + y_2 = x_1$ y que $y_1 y_2 = -1$. Por lo que y_1, y_2 son ceros de $t^2 - x_1 t - 1$.

Y análogamente y_3, y_4 son ceros de $t^2 - x_2 t - 1$.

Ahora, reescribimos y_3 y nos queda,

$$\begin{array}{rcl} y_1 & = & 2\cos\theta + 2\cos 4\theta \\ y_3 & = & 2\cos 5\theta + 2\cos 3\theta \quad = \quad 4\cos\theta\cos 4\theta, \end{array}$$

por lo que, $z_1 = 2\cos\theta$ y $z_2 = 2\cos 4\theta$, son ceros del polinomio cuadrático $t^2 - y_1 t + y_3$.

De esta forma, hemos llegado a una cadena de ecuaciones cuadráticas. La resolvemos y llegamos a la expresión que aparece en el artículo 365,

$$\cos\theta = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

Hasta aquí no hemos hecho más que seguir a Gauss. La clave de esta ingeniosa construcción radica en considerar el menor ángulo agudo ϕ tal que $\tan 4\phi = 4$. Entonces ϕ, 2ϕ y 4ϕ son agudos y podemos reescribir el polinomio 7.1 como,

$$p(t) = t^2 + 4t\cot 4\phi - 4,$$

cuyos ceros son $2\tan 2\phi$ y $-\cot 2\phi$. Por lo que,

$$x_1 = 2\tan 2\phi \qquad \text{y} \qquad x_2 = -2\cot 2\phi.$$

De esto se sigue que,

$$y_1 = \tan(\phi + \frac{\pi}{4}) \qquad y_2 = \tan(\phi - \frac{\pi}{4}) \qquad y_3 = \tan\phi \qquad y_4 = -\cot\phi.$$

E igualando estas expresiones de y_2 e y_3 con las obtenidas en función de θ nos queda,

$$\begin{array}{rcccl} y_2 & = & \tan\phi & = & 2(\cos 3\theta + \cos 5\theta) \\ y_3 & = & \tan(\phi - \frac{\pi}{4}) & = & 2(\cos 2\theta + 2\cos 8\theta) \quad = \quad 4\cos 3\theta\cos 5\theta. \end{array}$$

Ahora la idea es jugar con estas expresiones para construir los ángulos 3θ y 5θ como sigue:

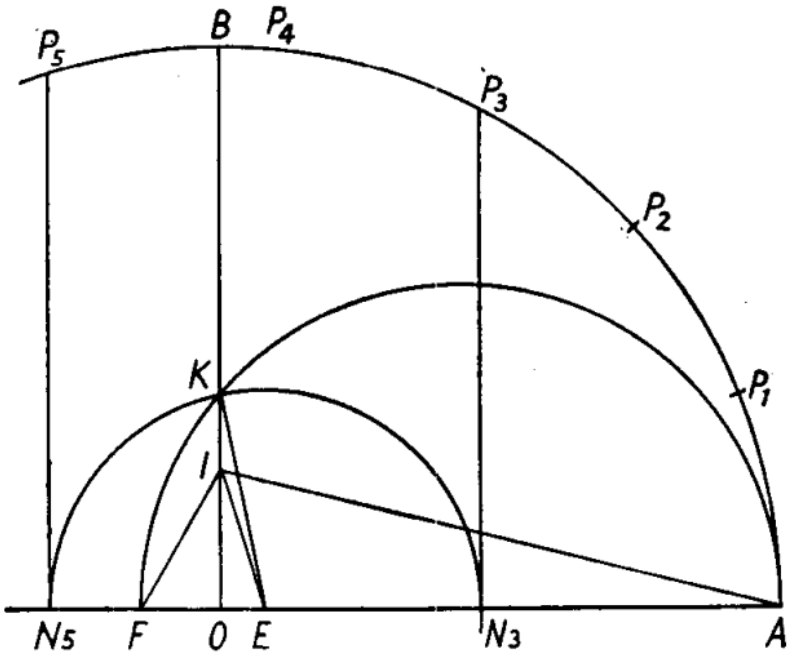

Figura 4:

Sean OA y OB dos radios perpendiculares de una circunferencia. Hacemos $OI = \frac{1}{4}OB$ y $\widehat{OIE} = \frac{1}{4}\widehat{OIA}$. Encontramos F en AO tal que $\widehat{EIF} = \frac{\pi}{4}$. Sea K el punto de corte entre $\overline{OB}$ y la circunferencia de diámetro $\overline{AF}$. Hallamos N_3 y N_5 intersecando la circunferencia de centro E que pasa por K con OA. Trazamos las perpendiculares a OA en N_3 y N_5 hallando P_3 y P_5.

De esta forma, si $\overline{OA} = 1$, tenemos que, $\tan(\widehat{OIA}) = 4$, $\widehat{OIA} = 4\phi$ y $\widehat{OIE} = \phi$. Y también,

$$2(\cos(\widehat{AOP_3}) + \cos(\widehat{AOP_5})) = 2\frac{\overline{ON_3}-\overline{ON_5}}{\overline{OA}} = 4\frac{\overline{OE}}{\overline{OA}} = \frac{\overline{OE}}{\overline{OI}} = \tan\phi$$

$$4\cos(\widehat{AOP_3})\cos(\widehat{AOP_5})) = -4\frac{\overline{ON_3}\times\overline{ON_5}}{\overline{OA}\times\overline{OA}} = -4\frac{\overline{OK}^2}{\overline{OA}^2} = -4\frac{\overline{OF}}{\overline{OA}} = -\frac{\overline{OF}}{\overline{OI}} = \tan(\phi - \tfrac{\pi}{4}).$$

Comparando esto con lo que ya teníamos vemos que,

$$\widehat{AOP_3} = 3\theta \qquad y \qquad \widehat{AOP_5} = 5\theta.$$

De esta forma tenemos que P_3 y P_5 son el tercer y quinto vértices de un polígono regular de 17 lados. Y ahora, el resto de vértices son fáciles de hallar.

Referencias

[Cla84] A. Clark. *Elements of Abstract Algebra*. Dover Books on Mathematics Series. Dover Publications, 1984.

[DH96] J. R. Dorronsoro and E. Hernández. *Números grupos y anillos*. Addison-Wesley Iberoamericana-UAM, 1996.

[Gau86] C. F. Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[HW08] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[kle55] *Famous Problems and other monographs*. Chelsea Publishing Co., New York, 1955. Famous problems of elementary geometry, by F. Klein, From determinant to tensor, by W. F. Sheppard, Introduction to combinatory analysis, by P. A. MacMahon, Three lectures on Fermat's last theorem, by L. J. Mordell.

[Rot90] J. Rotman. *Galois theory*. Universitext. Springer-Verlag, New York, 1990.

[Ste89] I. Stewart. *Galois theory*. Chapman and Hall, Ltd., London, second edition, 1989.

[Cha12] F. Chamizo. ¡Qué bonita es la teoría de Galois! `http://www.uam.es/fernando.chamizo/libreria/libreria.html`, 2012.