Estructura algebraica de los periodos de Gauss

Martin Azpillaga

13 de enero de 2014

Resumen

Lo que prosigue es un análisis sobre la estructura algebraica de los números complejos conocidos como periodos de Gauss. El contenido parte de un resumen de los resultados hallados en:
Travesa, Artur: *El teorema de Kronecker-Weber*.
CSIC Madrid, 2008. link
y continúa con la abstracción de los periodos de Gauss presente en:

N.J. Wildberger: *On the algebraic structure of Gaussian periods*. University of South Wales, 2003. link

El objetivo es mostrar la importancia de los periodos de Gauss en la teoria algebraica de números y dar una abstracción para su análisis desde el punto de vista del álgebra abstracta.

Motivación

Sea H un subgrupo de $(\mathbb{Z}/p\mathbb{Z})^*$ de índice n. Como $(\mathbb{Z}/p\mathbb{Z})^*$ es abeliano, H es normal y el cociente $(\mathbb{Z}/p\mathbb{Z})^*/H$ está bien definido. El subgrupo H particiona el conjunto $(\mathbb{Z}/p\mathbb{Z})^*$ en n clases laterales, las denotaremos por $C_1, ...C_n$.

Definamos ahora los objetos de nuestro estudio:

Definición. Periodos de Gauss.

Sea:

- H subgrupo de $\mathbb{Z}/p\mathbb{Z}^*$ de índice n
- $\{C_1, ..., C_n\}$ las clases laterales de $\mathbb{Z}/p\mathbb{Z}^*/H$
- $i \in \{1, ..., n\}$

Llamamos i-ésimo n-periodo de Gauss al numero complejo:

- $\sum_{x \in C_i} \zeta^x$

donde ζ es la raiz n-ésima primitiva: $e^{\frac{i\pi}{n}}$.

Cuando el valor de n se sobreentienda, denotaremos por η_i al i-ésimo n-periodo de Gauss.

El interes por los periodos de Gauss viene razonado por el siguiente teorema:

Teorema. Determinación de los subcuerpos ciclotómicos.

Sea:

- p primo impar
- ζ raíz p-ésima de la unidad
- K subcuerpo de $\mathbb{Q}(\zeta)$ tal que $[K : \mathbb{Q}] = n$

Entonces, se cumple:

$K = \mathbb{Q}(\eta_i) \qquad \forall i \in \{1, ..., n\}.$

En otras palabras, los n-periodos de Gauss son elementos primitivos de la única subextensión de $K|\mathbb{Q}$ de grado n.

Comenzaremos recordando tres resultados previos:

Resultado I.

Sea:

- p primo impar
- n divisor de $p-1$

Entonces, se cumple:

- $\exists!\ H < (\mathbb{Z}/p\mathbb{Z})^*$ tq $|(\mathbb{Z}/p\mathbb{Z})^* : H| = n$.

Resultado II.

Sea:

- $L|k$ extensión de Galois
- $\theta \in L$ elemento primitivo de $L|k$
- $K \subset L$ subcuerpo que contiene k
- $a_0, ..., a_n$ coeficientes de $Irr(\theta, K)$

Entonces, se cumple:

- $K = k(a_0, ..., a_n)$

Resultado III.

Sean:

- $n \in N$
- $s_k(X_1, ..., X_n)$ el k-ésimo polinomio simétrico
- $t_k(X_1, ..., X_n)$ el k-ésimo polinomio de Newton
- $x_1, ..., x_n$ elementos algebraicos sobre $\mathbb{Q}$

Entonces, se cumple:

- $\mathbb{Q}(s_1(x_1, ..., x_n), ..., s_n(x_1, ..., x_n)) = \mathbb{Q}(t_1(x_1, ..., x_n), ..., t_n(x_1, ..., x_n))$

Empecemos ahora con la demostración del teorema:
Sabemos que $\mathrm{Gal}(Q(\zeta)|Q)$ es isomorfo a $(\mathbb{Z}/p\mathbb{Z})^*$ que tiene orden $p-1$. Aplicando el resultado I, sabemos que existe un único subgrupo H de $\mathrm{Gal}(Q(\zeta)|Q)$ con índice n, y por la correspondencia de Artin, K ha de ser $\mathbb{Q}^H$.

Por el resultado II, el cuerpo K está generado sobre $\mathbb{Q}$ por los coeficientes del polinomio $Irr(\zeta, K)(X)$.
Como $Gal(Q(\zeta)|Q)$ es cíclico, H también. Sea σ un generador de H. Podemos expresar:

$$Irr(\zeta, K)(X) = \prod_{\tau \in H} (X - \tau(\zeta) = \prod_{j=1}^{d} (X - \sigma^{jn}(\zeta)$$

donde d es $p - 1/n$.

Para cada $j \in \{1, ..., d\}$, denotemos por a_j a $\sigma^{jn}(\zeta)$. Los coeficientes del polinomio irreductible vienen dados por los polinomios simétricos elementales evaluados sobre los a_j, esto es, son los valores: $s_1(a_1, ..., a_d), ..., s_d(a_1, ..., a_d)$.
Por el resultado III, los valores $t_1(a_1, ..., a_d), ..., t_d(a_1, ..., a_d)$ generan el mismo cuerpo sobre $\mathbb{Q}$ y resulta que cada uno de estos es un n-periodos de Gauss. Visualmente:

$$K = \mathbb{Q}(a_j)_j = \mathbb{Q}(s_j(a_1, ..., a_d))_j = \mathbb{Q}(t_j(a_1, ...a_d))_j \subset \mathbb{Q}(\eta_j)_j$$

Ahora, por la definición de periodos de Gauss se sigue que $\sigma(\eta_i) = \eta_i$ de manera que $\eta_i \in K$ para todo i y obtenemos la igualdad: $K = Q(\eta_1, ..., \eta_n)$
Finalmente, para todo i, j enteros, se satisface la igualdad $\sigma^j(\eta_i) = \eta_{i+j}$. Concluimos que todos los periodos η_i son conjugados entre sí y efectivamente:

$$K = Q(\eta_i)$$

Nuestro interes en estas paginas es estudiar la estructura de los periodos de Gauss. Para ello, analizaremos las propiedades que los caracterizan para despues abstraerlas y presentar una forma de estudiar los periodos de Gauss mediante álgebra abstracta. Volvamos a empezar:

Sea H el subgrupo de $\mathbb{Z}/p\mathbb{Z}^*$ de índice n. Como $(\mathbb{Z}/p\mathbb{Z})^*$ es abeliano, H es normal y el cociente $(\mathbb{Z}/p\mathbb{Z})^*/H$ está bien definido. El subgrupo H particiona el conjunto $(\mathbb{Z}/p\mathbb{Z})^*$ en n clases laterales, las denotaremos por $C_1, ...C_n$.

Ahora, podemos considerar $C_1 = H$. Dado un generador g de $\mathbb{Z}/p\mathbb{Z}^*$, para todo conjunto $C \in \{C_1, ..., C_n\}$ existe un k natural menor que n de manera que $C = g^k C_1$, y por ello podemos ordenar los conjuntos $C_1, ..., C_n$ mediante la regla:

$$C_i = g^i C_1 < C_j = g^j C_j \leftrightarrow i < j$$

Si añadimos el conjunto $C_0 = \{0\}$, definiendo $C_0 < C_i$ para todo i, obtenemos una particion totalmente ordenada de $\mathbb{Z}/p\mathbb{Z}$: $\{C_0, ..., C_n\}$. Denotaremos esta partición por $\mathcal{C}$.

Escojamos tres conjuntos $C_i, C_j, C_k \in \mathcal{C}$ y fijemos un x_k en C_k. Podemos considerar la cantidad de veces que x_k aparece como resultado de $x_i + x_j$ donde x_i y x_j varian en C_i y C_j respectivamente. El resultado no depende del x_k elegido y por ello tiene sentido denotar por N_{ij}^k a dicha cantidad.

Para todo i, j, se cumple la ecuación:

$$C_i C_j = \sum_{k=0}^{n} N_{ij}^k C_k$$

que llamaremos la ecuación característica de $\mathcal{C}$.

Consideremos ahora, $\mathbb{Z}\mathcal{C}$ el span de $\mathcal{C}$ por $\mathbb{Z}$, es decir:

$$\mathbb{Z}\mathcal{C} = \{\sum_{i=0}^{n} z_i C_i | z_i \in \mathbb{Z}, C_i \in \mathcal{C}\}$$

Gracias a la ecuación característica, $\mathbb{Z}\mathcal{C}$ con la suma y el producto ordinarios definidos sobre los coeficientes z_i, tiene estructura de anillo abeliano con unidad C_0.
Podemos considerar para cada C_i su inverso respecto la suma en $\mathbb{Z}\mathcal{C}$. Denotemoslo por C_i^*. Todos los C_i^* pertenecen a $\mathcal{C}$ y podemos considerar la aplicación:

$$\begin{aligned} * : \mathcal{C} &\longrightarrow \mathcal{C} \\ C_i &\longmapsto C_i^* \end{aligned}$$

que resulta ser un automorfismo sobre $\mathcal{C}$.

Hemos sido capaces de definir un conjunto de numeros naturales $\{N_{ij}^k\}$ que definen la ecuación carácterística y un automorfismo $*$ sobre $\mathcal{C}$. Estos dos conceptos quedan relacionados mediante la siguiente propiedad:

$$N_{ij}^0 > 0 \leftrightarrow C_j = C_i^*$$

Ahora, podemos abstraer estas propiedades y construir una nueva estructura algebraica del cual los periodos de Gauss formaran un ejemplo importante.

Ensamblajes

Abstraeremos las propiedades vistas bajo la definición de ensamblaje, *assembly* según el autor original:

Ensamblaje

Sea:

- $\mathcal{C} = \{C_i\}_{i=0}^{n}$ un conjunto totalmente ordenado.
- $N = \{N_{ij}^{k}\}_{i,j,k=0}^{n} \subset \mathbb{N}$.
- $* : \mathcal{C} \longrightarrow \mathcal{C}$.

Entonces, $(\mathcal{C}, N, *)$ es un ensamblaje de orden n si:

- $\mathbb{Z}\mathcal{C}$ es un anillo abeliano con unidad C_0.
- $N_{ij}^{k} > 0 \leftrightarrow C_j = C_i^{*}$.
- $*$ es un automorfismo sobre $\mathcal{C}$.
- Se cumple la ecuación característica:

$$C_i C_j = \sum_{k=0}^{n} N_{ij}^{k} C_k$$

- *Conservación de la masa:*

$$m(C_i)m(C_j) = \sum_{k=0}^{n} N_{ij}^{k} C_k$$

donde $m(C_i) = \sum_{j=0}^{n} N_{ij}^{0}$.

Nos referiremos con $\mathcal{C}$ a la terna $(\mathcal{C}, N, *)$ siempre que no cause confusión.

LLamamos **carácter masa** a la aplicación:

$$\begin{array}{rcl} m : \mathcal{C} & \longrightarrow & \mathbb{N} \\ C_i & \longmapsto & m(C_i) = \sum_{j=0}^{n} N_{ij}^{0} \end{array}$$

Antes de adentrarnos en el teorema principal, nos quedan unas cuantas definiciones más por considerar:

Masa Total

Sea:

- $(\mathcal{C}, N, *)$ un ensamblaje de orden n.

LLamamos masa total del ensamblaje $(\mathcal{C}, N, *)$ al natural:

- $\sum_{i=0}^{n} m(C_i)$

y lo denotamos por $m(\mathcal{C})$.

Ensamblaje Hermitiano

Sea:

- $(\mathcal{C}, N, *)$ un ensamblaje de orden n.

Entonces, $\mathcal{C}$ es un ensamblaje hermitiano si:

- $\forall i \in \{0, ..., n\} : C_i = C_i^*$.

Ensamblaje Ciclotómico

Sea:

- $(\mathcal{C}, N, *)$ un ensamblaje de orden n.
- $\sigma : \{0, .., n\} \longrightarrow \{0, ..., n\}$ una permutación definida por $\sigma(0) = 0, \sigma(n) = 1, \sigma(i) = i + 1$.

Entonces, $\mathcal{C}$ es un ensamblaje ciclotómico si:

- $\forall i, j, k \in \{0, ..., n\} : \quad N_{\sigma(i)\sigma(j)}^{\sigma(k)} = N_{ij}^{k}$.

Ensamblajes isomorfos

Sea:

- $(\mathcal{C}_1, N_1, *_1), (\mathcal{C}_2, N_2, *_2)$ ensamblajes de orden n.

Entonces, $\mathcal{C}_1, \mathcal{C}_2$ son isomorfos si $\exists\, \phi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ cumpliendo:

- $\phi(C_i C_j) = \phi(C_i)\phi(C_j)$.

- $\phi(C_i^*) = \phi(C_i)^*$

Teorema Principal

Retomemos los periodos Gaussianos. Sea $\mathcal{C} = \{\eta_0 = 1, \eta_1, ..., \eta_n\}$. Definamos N_{ij}^k como las apariciones de un elemento de C_k como suma de elementos de C_i y C_j y $*$ como la aplicación que asigna a cada periodo gaussiano su opuesto respecto la suma. Resulta que la terna $(\mathcal{C}, N, *)$ es un ensamblaje ciclotómico de orden n y masa total p.

El teorema principal asegura que, salvo isomorfismos, éste es el único ensamblaje que cumple estas condiciones:

Teorema Principal

Sea:

- p un primo.
- n un natural divisor de $p - 1$.

Entonces, se cumple salvo isomorfismos:

- $\exists!\, \mathcal{C}$ ensamblaje ciclotómico de orden n y masa total p

Esto permite establecer una correspondencia entre el único subcuerpo de grado n de $\mathbb{Q}(\zeta_p)$ y el único ensamblaje ciclotómico de orden n y masa total p.

Así, el estudio de periodos gaussianos se traslada al álgebra abstracta, ofreciendo la capacidad de analizar las propiedades de los periodos Gaussianos mediante los resultados obtenidos para los ensamblajes ciclotómicos.

La demostración de este teorema, así como el desarrollo de todos los conceptos colaterales que aparecen por el camino se encuentra en el artículo previamente citado:

N.J. Wildberger: *On the algebraic structure of Gaussian periods*. University of South Wales, 2003. link