Curso de Nivel Avanzado

La función Zeta de Dedekind y la fórmula para el número de clases

Nicolás Sirolli

Universidad de la República, Uruguay

VII Encuentro Nacional de Álgebra

La Falda, Sierras de Córdoba, Argentina

4 al 8 de Agosto de 2014

www.famaf.unc.edu.ar/~ciem/elena7

LA FUNCIÓN ZETA DE DEDEKIND Y LA FÓRMULA PARA EL NÚMERO DE CLASES

NICOLÁS SIROLLI

RESUMEN. En estas notas damos una demostración de la fórmula del número de clases, que relaciona el residuo de la función Zeta de Dedekind de un cuerpo de números con algunos de sus invariantes aritméticos, y comparamos esta fórmula con la conjetura de Birch y Swinnerton-Dyer.

ÍNDICE

INTRODUCCIÓN

Una de las ideas más fructíferas de la teoría analítica de números consiste en asociarle una función generatriz al objeto que se quiera estudiar, y obtener información aritmética de este objeto a partir de información analítica de la función. El ejemplo paradigmático de esto es la función Zeta de Riemann

$$\zeta(s) = \prod_{p \text{ primo}} \left(1 - p^{-s}\right)^{-1},$$

cuyas propiedades analíticas dan información sobre la distribución de los números primos. Por ejemplo, el Teorema de los Números Primos equivale a que $\zeta(s) \neq 0$ si $\Re(s) = 1$.

En este curso estudiaremos la generalización de esta función a cuerpos de números K, llamada función Zeta de Dedekind y denotada ζ_K. Si bien esta función también da información sobre la distribución de los ideales primos de K, nos concentraremos en la fórmula para el número de clases (Teorema 2.1). Esta fórmula relaciona el residuo de ζ_K en $s = 1$ con los invariantes aritméticos más importantes del cuerpo. Entre ellos, el número de clases de K.

Date: 15 de julio de 2014.

Agradezco a Daniel Kohen y a Emilio Lauret por haberme ayudado a mejorar estas notas. También agradezco al Área de Matemática del PEDECIBA por financiar los gastos de mi traslado a La Falda.

La utilidad de esta fórmula reside en que, para ciertos cuerpos de números, dicho residuo se puede calcular de manera explícita en términos de sumas de Gauss, por lo que nos da una herramienta para calcular números de clases.

En lugar de profundizar sobre la fórmula en esa dirección, terminaremos el curso enunciando una fórmula similar: la conjetura de Birch y Swinnerton-Dyer, uno de los problemas del milenio. Esta conjetura relaciona ciertos invariantes algebraicos asociados a una curva elíptica con el primer coeficiente de la función generatriz correspondiente. El parecido entre las dos fórmulas no es casualidad: son ambas casos particulares de las conjeturas de Beilison y de Bloch-Kato (ver [Sch88]).

En la primera sección de estas notas daremos los resultados básicos de la teoría algebraica de números que se precisan para definir los invariantes involucrados en la fórmula para el número de clases. Algunas referencias sobre este tema son, por ejemplo, [Mar77, Capítulos 2 y 5] y [Neu99, Capítulo 1].

En la segunda sección definimos la función Zeta de Dedekind, y enunciamos y demostramos el Teorema 2.1, siguiendo de cerca a [Mar77, Capítulos 6 y 7]. Tanto en [Mar77] como en [BS66, Capítulo 5] se pueden encontrar cálculos explícitos del residuo en el caso de cuerpos cuadráticos y cuerpos ciclotómicos.

En la tercera sección enunciamos la conjetura de Birch y Swinnerton-Dyer tras introducir (muy informalmente) los invariantes involucrados en esta, y nos ocupamos de comparar estos términos con los que aparecen en la fórmula para el número de clases. Se puede consultar a [Sil09] sobre la teoría básica de curvas elípticas, y a [Dar09], [Wil06] para profundizar sobre la conjetura de Birch y Swinnerton-Dyer.

1. Resultados básicos de la teoría algebraica de números

Un *cuerpo de números* es una extensión finita $K/\mathbb{Q}$. Algunos ejemplos interesantes de cuerpos de números son:

- $K = \mathbb{Q}(\sqrt{m})$, con $m \in \mathbb{Z} \setminus \{0, 1\}$ libre de cuadrados. Estos son los llamados *cuerpos cuadráticos*.
- $K = \mathbb{Q}(\xi_n)$, con $\xi_n \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad. Estos son los llamados *cuerpos ciclotómicos*.

Los cuerpos cuadráticos son, en términos del grado sobre $\mathbb{Q}$, los primeros cuerpos de números no triviales; a pesar de ello, ilustran la teoría que desarrollaremos sobradamente. Los cuerpos ciclotómicos son de interés, por ejemplo, porque toda extensión abeliana y finita de $\mathbb{Q}$ está contenida en uno de ellos.

Fijemos un cuerpo de números K, y denotemos por $d = [K : \mathbb{Q}]$ a la dimensión de K como $\mathbb{Q}$-espacio vectorial.

1.1. Aritmética de los cuerpos de números. El rol que juega $\mathbb{Z}$ como subanillo de $\mathbb{Q}$ es reemplazado en el cuerpo de números K por el *anillo de enteros*, que se define por

$$\mathcal{O}_K = \{\xi \in K : \exists\, f \in \mathbb{Z}[X] \text{ mónico tal que } f(\xi) = 0\}.$$

Este conjunto es en efecto un anillo, y sus elementos tienen norma y traza en $\mathbb{Z}$.

A los $\mathcal{O}_K$-módulos $\mathfrak{a} \subseteq K$ de tipo finito los llamaremos *ideales fraccionarios*. Aquellos que estén contenidos en $\mathcal{O}_K$ serán llamados *ideales*, a secas; son precisamente los ideales del anillo $\mathcal{O}_K$. El ideal $\{0\}$ quedará excluido de todo lo que sigue.

Proposición 1.1. *$\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango d. Más aún, todo ideal fraccionario de K lo es.*

Gracias a este resultado, podemos introducir el *discriminante* de K. Se define como el determinante de la forma bilineal en $\mathcal{O}_K$ dada por $(\xi_1, \xi_2) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\xi_1\xi_2)$, y se denota por $\mathrm{disc}(K)$.

Si bien el anillo de enteros no necesariamente es un dominio de factorización única (lo cual, en este caso, equivale a ser un dominio de ideales principales), sí se obtiene un resultado satisfactorio al considerar ideales en lugar de elementos. Más precisamente, se tiene el siguiente teorema.

Teorema 1.2. *Todo ideal fraccionario $\mathfrak{a} \subseteq K$ se escribe, de manera única, como*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n},$$

donde los $\mathfrak{p}_i$ son ideales primos de $\mathcal{O}_K$, y los e_i son enteros no nulos.

Es decir, el grupo de ideales fraccionarios de K, que denotamos por $\mathrm{Frac}(K)$, es el grupo abeliano libre generado por los ideales primos de $\mathcal{O}_K$.

La medida de cuán lejos está el anillo de ser enteros de ser un dominio de ideales principales está dada por el *grupo de clases*, definido por

$$Cl(K) = \mathrm{Frac}(K)/P(K),$$

donde $P(K) = \{\mathfrak{a} \in \mathrm{Frac}(K) : \exists \xi \in K^\times \text{ tal que } \mathfrak{a} = (\xi)_{\mathcal{O}_K}\}$ es el subgrupo de los ideales fraccionarios principales. El grupo de clases es finito y su orden, que llamamos *número de clases*, se denota por h_K.

Dado un ideal fraccionario $\mathfrak{a}$, definimos su *norma* por $N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$ (el índice de $\mathfrak{a}$ en $\mathcal{O}_K$). La función norma satisface las siguientes propiedades:

- $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}) \quad \forall\, \mathfrak{a}, \mathfrak{b} \in \mathrm{Frac}(K)$.
- $N((\xi)_{\mathcal{O}_K}) = |N_{K/\mathbb{Q}}(\xi)| \quad \forall\, \xi \in K^\times$.

1.2. Geometría de los cuerpos de números. A través de las inmersiones $K \hookrightarrow \mathbb{C}$, podemos utilizar herramientas de la geometría euclídea para estudiar a K, idea que se debe a Minkowski.

Distinguimos dos tipos de inmersiones.

- Las *reales*, aquellas $\sigma : K \hookrightarrow \mathbb{C}$ tales que $\sigma(K) \subseteq \mathbb{R}$.
- Las *complejas*, aquellas $\tau : K \hookrightarrow \mathbb{C}$ tales que $\tau(K) \not\subseteq \mathbb{R}$. Estas se pueden agrupar de a pares $(\tau, \bar{\tau})$.

Denotaremos entonces a las inmersiones de K por

$$\sigma_1, \ldots, \sigma_r, \tau_1, \bar{\tau_1}, \ldots, \tau_s, \bar{\tau_s},$$

con las σ_i reales y las τ_j complejas[1]. Aquí $r, s \in \mathbb{Z}_{\geq 0}$, y $r + 2s = d$.

A través de estas inmersiones definimos

$$\begin{aligned} \iota : K &\hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^d, \\ \xi &\mapsto (\sigma_1(\xi), \ldots, \sigma_r(\xi), \tau_1(\xi), \ldots, \tau_s(\xi)). \end{aligned}$$

En $\mathbb{R}^r \times \mathbb{C}^s$ definimos una función *norma* por $N(x, z) = \prod_{i=1}^r x_i \cdot \prod_{j=1}^s z_j\overline{z_j}$. De esta manera, se tiene que $N(\iota(\xi)) = N_{K/\mathbb{Q}}(\xi)$ para todo $\xi \in K$.

Proposición 1.3. *$\Lambda_{\mathcal{O}_K} := \iota(\mathcal{O}_K)$ es un retículo completo en $\mathbb{R}^d$. Más aún,*

$$\sqrt{|\operatorname{disc}(K)|} = 2^s \cdot \mathrm{vol}(\mathbb{R}^d/\iota(\mathcal{O}_K)). \tag{1.1}$$

[1]Usaremos la letra s tanto para denotar a la cantidad de inmersiones complejas de K como para denotar a la variable compleja de nuestras funciones generatrices. El lector sabrá disculparnos.

Consideremos el grupo de unidades $\mathcal{O}_K^\times$. Denotemos por $T(\mathcal{O}_K^\times)$ al subgrupo de elementos de torsión de este grupo. Notemos que $T(\mathcal{O}_K^\times)$ coincide con el grupo de raíces de la unidad de K. Denotamos el orden de este grupo por ω_K.

Se puede obtener un resultado similar a la Proposición 1.3 mediante la utilización de logaritmos. Para esto, consideramos el morfismo de grupos

$$\begin{aligned}\log :&(\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \to \mathbb{R}^{r+s}\\ &(x,z) \mapsto (\log(|x_1|),\dots,\log(|x_r|),2\log(|z_1|),\dots,2\log(|z_s|)),\end{aligned}$$

y denotamos $L = \log \circ \iota : K^\times \to \mathbb{R}^{r+s}$.

Como $N_{K/\mathbb{Q}}(\mathcal{O}_K^\times) \subseteq \mathbb{Z}^\times$, resulta que $L(\mathcal{O}_K^\times) \subseteq H$, donde H es el hiperplano dado por $H = \{v \in \mathbb{R}^{r+s} : \sum_k v_k = 0\}$. Además, como todo conjunto acotado de $\mathbb{R}^{r+s}$ tiene preimagen por L finita en $\mathcal{O}_K \setminus \{0\}$, se tiene que $\ker L = T(\mathcal{O}_K^\times)$.

Teorema 1.4 (Dirichlet)**.** *$\Lambda_{\mathcal{O}_K^\times} := L(\mathcal{O}_K^\times)$ es un retículo completo en H, y por lo tanto $\mathcal{O}_K^\times$ es producto directo de $T(\mathcal{O}_K^\times)$ y de un grupo abeliano libre de rango $r+s-1$.*

Este teorema nos permite definir otro de los invariantes importantes del cuerpo de números: el *regulador* de K, que se denota por $\operatorname{reg}(K)$ y está dado por

$$\operatorname{reg}(K) = \frac{\operatorname{vol}(H/\Lambda_{\mathcal{O}_K^\times})}{\sqrt{r+s}}. \tag{1.2}$$

Si $r+s=1$, por convención ponemos $\operatorname{reg}(K)=1$.

1.3. Ejercicios.

1. Sea $K = \mathbb{Q}(i)$.
   a) Probar que $\mathcal{O}_K = \mathbb{Z}[i]$, y calcular $\operatorname{disc}(K)$.
   b) Probar que $\mathbb{Z}[i]$ es un dominio euclídeo, utilizando como función "grado" a $\xi \mapsto N_{\mathbb{Q}(i)/\mathbb{Q}}(\xi)$.
   c) Probar que $T(\mathbb{Z}[i]^\times) = \{1,-1,i,-i\}$.
2. Sea p un primo distinto de 2. Probar que son equivalentes:
   a) p es reducible en $\mathbb{Z}[i]$.
   b) $p = a^2 + b^2$ con $a, b \in \mathbb{Z}$.
   c) -1 es un cuadrado en $\mathbb{Z}/p\mathbb{Z}$.
   d) $p \equiv 1 \mod 4$.
3. Sea $\mathfrak{p} = (1+i)$. Probar que $(2) = \mathfrak{p}^2$ es la factorización de (2) como producto de ideales primos de $\mathbb{Z}[i]$.
4. Sea p un primo distinto de 2.
   a) Probar que si $p \equiv 1 \mod 4$, entonces $(p) = \mathfrak{p}_1\mathfrak{p}_2$ con $\mathfrak{p}_1, \mathfrak{p}_2$ ideales primos (distintos) de $\mathbb{Z}[i]$.
   b) Probar que si $p \equiv 1 \mod 3$, entonces (p) es un ideal primo de $\mathbb{Z}[i]$.

2. La función Zeta de Dedekind y la fórmula para el número de clases

Sea K un cuerpo de números. Definimos la *función Zeta de Dedekind* de K por

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} \qquad (\Re(s) > 1), \tag{2.1}$$

donde $\mathfrak{a}$ recorre todos los ideales de $\mathcal{O}_K$. Para $K = \mathbb{Q}$, recuperamos la función Zeta de Riemann.

Al menos formalmente, el Teorema 1.2 nos permite escribir

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1}, \tag{2.2}$$

donde $\mathfrak{p}$ recorre todos los ideales primos de $\mathcal{O}_K$. Es decir, tal como le pasa a la función Zeta de Riemann, podemos desarrollar a ζ_K como un producto de Euler.

Veremos más adelante que (2.1) define una función holomorfa. Nuestro objetivo es probar el siguiente resultado.

Teorema 2.1. *La función ζ_K se puede extender de manera holomorfa a $\Re(s) > 1-1/d$, salvo por un polo simple en $s = 1$. El residuo en $s = 1$ está dado por*

$$\operatorname{Res}(\zeta_K, 1) = \frac{2^r(2\pi)^s}{\sqrt{|\operatorname{disc}(K)|}} \cdot h_K \cdot \frac{\operatorname{reg}(K)}{\omega_K}. \tag{2.3}$$

Probaremos un resultado algo más fuerte, que además muestra que los ideales están equidistribuidos en las clases de $Cl(K)$.

Teorema 2.2. *Sea κ la constante dada por*

$$\kappa = \frac{2^r(2\pi)^s}{\sqrt{|\operatorname{disc}(K)|}} \cdot \frac{\operatorname{reg}(K)}{\omega_K}.$$

Dada $\mathcal{C} \in Cl(K)$, consideremos la función $i_{\mathcal{C}}$ dada por

$$i_{\mathcal{C}}(t) = \#\left\{\mathfrak{a} \subseteq \mathcal{O}_K : \mathfrak{a} \in \mathcal{C}, N(\mathfrak{a}) \leq t\right\} \qquad (t \in \mathbb{R}_{\geq 0}).$$

Entonces, $i_{\mathcal{C}}(t) = \kappa t + O(t^{1-1/d})$.

Veamos cómo de este resultado se sigue el Teorema 2.1.

Para $n \in \mathbb{N}$, sea $j_n = \#\{\mathfrak{a} \subseteq \mathcal{O}_K : N(\mathfrak{a}) = n\}$. Reescribamos a ζ_K como la serie de Dirichlet

$$\zeta_K(s) = \sum_{n\geq 1} \frac{j_n}{n^s} = \sum_{n\geq 1} \frac{j_n - h_K\kappa}{n^s} + h_K\kappa\zeta(s). \tag{2.4}$$

Usaremos que el Teorema 2.1 es conocido para $K = \mathbb{Q}$. Esto es, la función ζ de Riemann $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$ converge uniformemente en compactos de $\Re(s) > 1$ (ver Lema 2.3), y se puede extender de manera holomorfa a $\Re(s) > 0$, salvo por un polo simple en $s = 1$ en el que se tiene que $\operatorname{Res}(\zeta, 1) = 1$.

En cuanto al primer sumando del miembro derecho de (2.4), el Teorema 2.2 nos dice que

$$\sum_{n\leq t} j_n - \kappa h_K = \left(\sum_{\mathcal{C}\in Cl(K)} i_{\mathcal{C}}(t)\right) - \kappa h_K \lfloor t \rfloor = O(t^{1-1/d}).$$

Entonces, el Teorema 2.1 se sigue de (2.4) más el siguiente resultado sobre la convergencia de series de Dirichlet.

Lema 2.3. *Sea $(a_n)_{n\geq 1} \subseteq \mathbb{C}$ una sucesión tal que $\sum_{n\leq t} a_n = O(t^\alpha)$ para algún $\alpha \in \mathbb{R}$. Entonces, la serie de Dirichlet $\sum_{n\geq 1} \frac{a_n}{n^s}$ converge uniformemente en compactos de $\Re(s) > \alpha$.*

Demostración. Fijemos constantes $A, \varepsilon > 0$, y tomemos $s \in \mathbb{C}$ con $\alpha + \varepsilon \leq \Re(s) \leq A$. Denotemos $A_n = \sum_{k \leq n} a_k$. Dados $m, M \in \mathbb{N}$ con $m \leq M$ tenemos que

$$\sum_{n=m}^{M} \frac{a_n}{n^s} = \sum_{n=m}^{M} \frac{A_n}{n^s} - \sum_{n=m}^{M} \frac{A_{n-1}}{n^s} = \frac{A_M}{M^s} - \frac{A_{m-1}}{(m-1)^s} + \sum_{n=m}^{M-1} A_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right).$$

Por hipótesis, existe $C > 0$ tal que $|A_n| \leq C n^\alpha$ para todo $n \in \mathbb{N}$. Por otra parte, se tiene que

$$\left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| = \left| s \int_n^{n+1} \frac{dt}{t^{s+1}} \right| \leq \frac{A}{n^{\Re(s)+1}}.$$

Entonces

$$\lim_{m,M \to \infty} \left| \sum_{n=m}^{M} \frac{a_n}{n^s} \right| \leq \lim_{m,M \to \infty} C \left(\frac{1}{M^\varepsilon} + \frac{1}{(m-1)^\varepsilon} + A \sum_{n=m}^{M} \frac{1}{n^{1+\varepsilon}} \right) = 0,$$

de lo que se sigue el resultado. □

Observación 2.4. Como la serie de Dirichlet en (2.4) converge en $\Re(s) > 1$, lo hace absolutamente (!). Esto le da sentido a la expresión de ζ_K dada en (2.1), ya que los ideales $\mathfrak{a}$ sobre los que se suma no están ordenados a priori.

Comencemos con la demostración del Teorema 2.2. Tomemos una clase $\mathcal{C} \in Cl(K)$ y fijemos $\mathfrak{b} \in \mathcal{C}^{-1}$ un ideal (entero). Gracias a la biyección

$$\begin{aligned} \#\{\mathfrak{a} \subseteq \mathcal{O}_K : \mathfrak{a} \in \mathcal{C}, N(\mathfrak{a}) \leq t\} &\xrightarrow{\simeq} \{(\xi)_{\mathcal{O}_K} \subseteq \mathfrak{b} : |N_{K/\mathbb{Q}}(\xi)| \leq t N(\mathfrak{b})\}, \\ \mathfrak{a} &\mapsto \mathfrak{a}\mathfrak{b}, \end{aligned}$$

pasamos de tener que contar *ideales* a tener que contar *elementos*, ya que nos dice que

$$i_{\mathcal{C}}(t) = \#\left\{\xi \in \mathfrak{b} : |N_{K/\mathbb{Q}}(\xi)| \leq t N(\mathfrak{b})\right\} / \mathcal{O}_K^\times.$$

Equivalentemente, si usando el Teorema 1.4 escribimos $\mathcal{O}_K^\times = T(\mathcal{O}_K^\times) \cdot V$ con V un grupo abeliano libre de rango $r + s - 1$, nos dice que

$$\omega_K \cdot i_{\mathcal{C}}(t) = \#\left\{\xi \in \mathfrak{b} : |N_{K/\mathbb{Q}}(\xi)| \leq t N(\mathfrak{b})\right\} / V.$$

Podemos calcular el miembro derecho de esta igualdad a través de la geometría, si hallamos un dominio fundamental D para la acción de $\iota(V)$ en $(\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$ y contamos los puntos de $\iota(\mathfrak{b})$ que estén en D. Siendo $\log|_{\iota(V)}$ un monomorfismo, se tiene que si D' es un dominio fundamental para la acción de $\Lambda_{\mathcal{O}_K^\times}$ en $\mathbb{R}^{r+s}$, entonces podemos tomar

$$D = \{(x, z) \in (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s : \log((x, z)) \in D'\}.$$

Como $\Lambda_{\mathcal{O}_K^\times}$ es un retículo completo en H, podemos tomar $D' = P \oplus \mathbb{R} \cdot v_0$, con P el paralelogramo fundamental para $\Lambda_{\mathcal{O}_K^\times}$ y $v_0 \in \mathbb{R}^{r+s} \setminus H$. De hecho, tomamos

$$v_0 = (\underbrace{1, \ldots, 1}_{r \text{ veces}}, \underbrace{2, \ldots, 2}_{s \text{ veces}})$$

porque así D resulta *homogéneo* (es decir, satisface que $D = \lambda D$ para todo $\lambda \in \mathbb{R}^\times$).

Para $a > 0$, denotemos $D_a = \{(x, z) \in D : |N(x, z)| \leq a\}$. Entonces, por la homogeneidad de D tenemos que

$$\omega_K \cdot \iota_{\mathcal{C}}(t) = \#\iota(\mathfrak{b}) \cap D_{tN(\mathfrak{b})} = \#\iota(\mathfrak{b}) \cap \sqrt[d]{tN(\mathfrak{b})} D_1. \tag{2.5}$$

Para calcular el miembro derecho de (2.5), utilizaremos el siguiente resultado, de naturaleza puramente geométrica. Diremos que un conjunto $B \subseteq \mathbb{R}^d$ tiene borde *suficientemente lindo* si $\partial B \subseteq \cup_{i\in I} f_i([0,1]^{d-1})$, donde las $f_i : [0,1]^{d-1} \to \mathbb{R}^d$ son funciones Lipschitz y el conjunto I es finito.

Proposición 2.5. *Sea $\Lambda \subseteq \mathbb{R}^d$ un retículo completo, y sea $B \subseteq \mathbb{R}^d$ un conjunto acotado y medible. Si el borde de B es suficientemente lindo, entonces*

$$\#\Lambda \cap aB = \frac{|B|}{\operatorname{vol}(\mathbb{R}^d/\Lambda)} \cdot a^d + O(a^{d-1}) \qquad (a > 0).$$

Demostración. Tomemos un isomorfismo $\varphi : \mathbb{R}^d \to \mathbb{R}^d$ tal que $\varphi(\Lambda) = \mathbb{Z}^d$. Entonces $\varphi(B)$ también tiene borde suficientemente lindo. Además, por ser φ lineal, se tiene que $|B| = |\varphi(B)| \cdot \operatorname{vol}(\mathbb{R}^d/\Lambda)$. Esto prueba que podemos suponer $\Lambda = \mathbb{Z}^d$.

Consideremos las traslaciones del cubo $[0,1]^d$ con centros en los puntos de $\mathbb{Z}^d$. Los llamaremos *d-cubos*. Denotemos por N_a a la cantidad de d-cubos que intersecan a $\partial(aB)$. Entonces

$$\big|\#\mathbb{Z}^d \cap aB - \text{cantidad de } d\text{-cubos contenidos en } aB\big| \le N_a, \quad \text{y}$$
$$\big||aB| - \text{cantidad de } d\text{-cubos contenidos en } aB\big| \le N_a,$$

por lo que, siendo $|aB| = a^d|B|$, basta con probar que $N_a = O(a^{d-1})$.

Por otra parte,

$$\partial B \subseteq \bigcup_{i\in I} f_i([0,1]^{d-1}) \Longrightarrow \partial(aB) \subseteq \bigcup_{i\in I} a \cdot f_i([0,1]^{d-1}).$$

Esto nos permite suponer que $\partial(aB) = a \cdot f([0,1]^{d-1})$ con f una función Lipschitz.

Subdividamos, de la manera natural, al cubo $[0,1]^{d-1}$ en $\lfloor a \rfloor^{d-1}$ pequeños cubos de lado $\frac{1}{\lfloor a \rfloor}$. Sea C uno de estos cubos. C tiene diámetro igual a $\frac{\sqrt{d-1}}{\lfloor a \rfloor}$, por lo que si λ es la constante Lipschitz de f, entonces $f(C)$ tiene diámetro acotado por $\frac{\lambda\sqrt{d-1}}{\lfloor a \rfloor}$. Por lo tanto, suponiendo que $a \ge 1$, resulta que $a \cdot f(C)$ tiene diámetro acotado por $2\lambda\sqrt{d-1}$. Si denotamos

$$M = \left(2 + 2\left\lceil 2\lambda\sqrt{d-1}\right\rceil\right)^n,$$

esto implica que $a \cdot f(C)$ interseca a lo sumo M de los d-cubos. Entonces, como la cantidad de cubos pequeños es $\lfloor a \rfloor^{d-1}$, tenemos que $N_a = O(\lfloor a \rfloor^{d-1}) = O(a^{d-1})$, lo que termina la demostración. □

Aplicando este resultado a $\Lambda = \iota(\mathfrak{b})$ y $B = D_1$, de (2.5) se sigue que

$$\omega_K \cdot \iota_{\mathcal{C}}(t) = \frac{|D_1|}{\operatorname{vol}(\mathbb{R}^d/\iota(\mathfrak{b}))} \cdot tN(\mathfrak{b}) + O(t^{1-1/d}) = \frac{2^s|D_1|}{\sqrt{|\operatorname{disc}(K)|}} \cdot t + O(t^{1-1/d}),$$

donde para obtener la última igualdad usamos que dados dos retículos completos $\Lambda \subseteq \Lambda' \subseteq \mathbb{R}^d$ se tiene que $\operatorname{vol}(\mathbb{R}^d/\Lambda) = [\Lambda' : \Lambda] \operatorname{vol}(\mathbb{R}^d/\Lambda')$, junto con (1.1). Entonces, el Teorema 2.2 quedará demostrado una vez que probemos el siguiente resultado.

Lema 2.6. *D_1 tiene borde suficientemente lindo, y $|D_1| = 2^r\pi^s \operatorname{reg}(K)$.*

Demostración. Como D_1 es simétrico respecto al 0 en su primera coordenada, basta con probar que

$$D_1^+ = \{(x,z) \in D_1 : x_1, \dots, x_r \ge 0\}$$

tiene borde suficientemente lindo y $|D_1^+| = \pi^s \operatorname{reg}(K)$, ya que $|D_1| = 2^r|D_1^+|$.

Para probar ambas afirmaciones, parametrizaremos a D_1^+. Empecemos notando que

$$D_1 = \{(x,z) \in (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s : \log(x,z) \in P \oplus (-\infty, 0] \cdot v_0\},$$

ya que $|N(x,z)| \leq 1$ si y solo si $\sum \log(x,z) \leq 0$, y las coordenadas de los puntos de P suman cero. Tomemos $v_1, \ldots, v_{r+s-1}$ base del retículo $\Lambda_{\mathcal{O}_K^\times}$. Escribamos $v_i = (v_i^{(1)}, \ldots, v_i^{(r+s)})$. Así, $(x,z) \in D_1^+$ si y solo si

$$\log(x_i) = \sum_{k=1}^{r+s-1} t_k v_k^{(i)} + u \qquad (1 \leq i \leq r),$$

$$2\log(|z_j|) = \sum_{k=1}^{r+s-1} t_k v_k^{(r+j)} + 2u \qquad (1 \leq j \leq s),$$

con $0 \leq t_k < 1$ y $-\infty < u \leq 0$. Pongamos $t_{r+s} = e^u$. Así, tenemos que $(x,z) \in D_1^+$ si y solo si

$$x_i = t_{r+s} \cdot \exp\left(\sum_{k=1}^{r+s-1} t_k v_k^{(i)}\right) \qquad (1 \leq i \leq r),$$

$$z_j = t_{r+s} \cdot \exp\left(\frac{1}{2}\sum_{k=1}^{r+s-1} t_k v_k^{(r+j)} + 2\pi i t_{r+s+j}\right), \qquad (1 \leq j \leq s),$$

con $t_{r+s} \in (0,1]$ y $t_k \in [0,1)$ para $1 \leq k \leq d, k \neq r+s$. La función $f : [0,1]^d \to \mathbb{R}^r \times \mathbb{C}^s$ dada por $t \mapsto (x,z)$ es Lipschitz, y se puede ver que $f([0,1]^d) = \overline{D_1^+}$ y $f(\partial([0,1]^d)) = \partial D_1^+$. Esto que muestra que D_1^+ es acotado, medible y tiene borde suficientemente lindo. Finalmente, utilizando esta parametrización se obtiene que $|D_1^+| = \pi^s \operatorname{reg}(K)$ (ver los ejercicios al final de esta sección). □

2.1. Ejercicios.

1. Sea $m \in \mathbb{N}$, y sea $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ un morfismo. Este induce naturalmente una función en los enteros coprimos con m, que extendemos por 0 a todos los enteros; la denotamos también por χ. Definimos la *L-serie* de χ por

$$L(s,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}.$$

   a) Probar que si el morfismo χ es no trivial, $L(s,\chi)$ define una función holomorfa en $\Re(s) > 0$. ¿Qué se puede decir cuando χ es trivial?
   b) Probar que

$$L(s,\chi) = \prod_{p \text{ primo}} \left(1 - \chi(p)p^{-s}\right)^{-1}.$$

2. Sea $K = \mathbb{Q}(i)$. Sea χ el carácter no trivial de $(\mathbb{Z}/4\mathbb{Z})^\times$. Probar que[2]

$$\zeta_K(s) = (1 - 2^{-s})^{-1} \cdot \zeta(s) \cdot L(s,\chi).$$

3. Probar la fórmula de Leibniz

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots$$

[2]Notar que $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \operatorname{Gal}(K/\mathbb{Q})$. Se puede obtener una fórmula similar a esta para cuerpos ciclotómicos cualesquiera.

4. En este ejercicio probaremos que $|D_1^+| = \pi^s \operatorname{reg}(K)$, completando así la demostración del Lema 2.6.
   a) Sea $\tilde{f} : (0,1)^d \to \mathbb{R}^r \times \mathbb{C}^s$ la restricción a $(0,1)^d$ de la función f introducida en la demostración de dicho lema. Verificar que $\tilde{f}$ es la composición de las funciones

   $$(0,1)^d \xrightarrow{f_1} \mathbb{R}^d \xrightarrow{f_2} \mathbb{R}^d = \mathbb{R}^r \times \mathbb{R}^s \times \mathbb{R}^s \xrightarrow{f_3} \mathbb{R}^r \times \mathbb{R}^s \times \mathbb{R}^s \xrightarrow{f_4} \mathbb{R}^r \times \mathbb{C}^s,$$

   donde:
   - $f_1(t) = (t_1, \dots, t_{r+s-1}, \log(t_{r+s}), t_{r+s+1}, \dots, t_d)$.
   - f_2 es la multiplicación a derecha por la matriz por bloques

   $$M = \left(\begin{array}{c|c} \begin{matrix} v_1 \\ \vdots \\ v_{r+s-1} \\ v_0 \end{matrix} & \begin{matrix} \\ 0 \\ \\ \end{matrix} \\ \hline 0 & I_s \end{array}\right) \in \mathbb{R}^{d\times d}.$$

   - $f_3(\alpha, \beta, \gamma) = (e^{\alpha_1}, \dots, e^{\alpha_r}, \frac{1}{2}e^{\beta_1}, \dots, \frac{1}{2}e^{\beta_s}, 2\pi\gamma_1, \dots, 2\pi\gamma_s)$.
   - $f_4(x, \rho, \theta) = (x, \rho_1 e^{i\theta_1}, \dots, \rho_s e^{i\theta_s})$.

   b) Deducir que $\tilde{f}$ es abierta e inyectiva, y probar que $f(\partial([0,1]^d)) = \partial D_1^+$.
   c) Sea $g = f_3 \circ f_2 \circ f_1$. Probar que

   $$\det Dg(t) = \frac{\pi^s \det(M) \prod_{i=1}^r x_i(t) \cdot \prod_{j=1}^s \rho_j(t)}{t_{r+s}}.$$

   d) Deducir que

   $$\left|D_1^+\right| = \int_{[0,1]^d} |\det Dg(t)| \prod_{j=1}^s \rho_j(t)\, dt = \pi^s \frac{|\det(M)|}{d}.$$

   e) Sean A, B dos matrices cuadradas cuyas filas, salvo tal vez la última, son vectores cuyas coordenadas suman cero. Probar que si las últimas filas de A y de B son vectores cuyas coordenadas suman lo mismo, entonces $\det A = \det B$.
   f) Deducir que $\frac{|\det(M)|}{d} = \operatorname{reg}(K)$.

3. Una fórmula similar: la conjetura de Birch y Swinnerton-Dyer

Sea K un cuerpo de números. Una *curva elíptica* E/K es una curva sobre K, no singular y de género 1, junto con un punto K-racional $O \in E(K)$. Toda tal curva puede ser descrita por una *ecuación de Weierstrass*

$$E: \quad y^2 = x^3 + Ax + B, \tag{3.1}$$

con $A, B \in K$ satisfaciendo $-16(4A^3 + 27B^2) \neq 0$.

Comenzaremos definiendo la función generatriz correspondiente. La idea básica es reducir la ecuación (3.1) módulo $\mathfrak{p}$ para cada primo $\mathfrak{p}$ de K, y para aquellos primos $\mathfrak{p}$ para los cuales se obtenga una curva elíptica $\overline{E}$ sobre $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ (los llamados primos de *buena reducción*), contar la cantidad de puntos de $\overline{E}(k_\mathfrak{p})$. Hacer dicha reducción requiere de algún cuidado; sólo diremos que el conjunto de primos de mala reducción es finito y se puede determinar con precisión.

Se la llama *L-serie* asociada a E/K, y se define como un producto de Euler:

$$L(E/K, s) = \prod_{\mathfrak{p} \text{ primo}} L_\mathfrak{p}(N(\mathfrak{p})^{-s})^{-1} \qquad (s \in \mathbb{C}), \tag{3.2}$$

donde el factor local $L_\mathfrak{p}$ es el polinomio dado por

$$L_\mathfrak{p}(T) = \begin{cases} 1 - a_\mathfrak{p} T + N(\mathfrak{p})T^2, & \text{si } \mathfrak{p} \text{ es de buena reducción,} \\ 1, 1+T \text{ ó } 1-T, & \text{si no,} \end{cases}$$

donde $a_\mathfrak{p} = N(\mathfrak{p}) + 1 - \#\overline{E}(k_\mathfrak{p})$, y el factor correspondiente a cada uno de los primos de mala reducción queda determinado en términos de cómo sea dicha reducción. Estos números satisfacen que $|a_\mathfrak{p}| \leq 2\sqrt{N(\mathfrak{p})}$ (cota de Hasse), de lo que se deduce que $L(E/K, s)$ converge uniformemente sobre compactos de $\Re(s) > 3/2$.

Notar el parecido entre (3.2) y (2.2). Podemos pensar a ζ_K como una L-serie en la que todos los factores locales son iguales a $1 - T$.

Ahora del lado aritmético,

Proposición 3.1. *$E(\overline{K})$ es un grupo abeliano. Más aún, es un grupo algebraico definido sobre K, del cual $E(K)$ es un subgrupo.*

El objeto que nos interesa es el grupo $E(K)$. El primer resultado importante sobre la estructura de este grupo es el siguiente teorema, que entenderemos como análogo a la descripción de $\mathcal{O}_K^\times$ que nos da el Teorema 1.4.

Teorema 3.2 (Mordell-Weil)**.** *El grupo abeliano $E(K)$ es finitamente generado.*

A diferencia de lo que ocurre con el rango de $\mathcal{O}_K^\times$, el rango de $E(K)$ es difícil de calcular. Lo denotaremos por r_{MW}.

Así como teníamos en $\mathrm{reg}(K)$ una medida del "tamaño" de la parte libre de $\mathcal{O}_K^\times$, en este contexto tenemos el *regulador* de E/K, que se define como

$$\mathrm{reg}(E/K) = \det\left(\langle P_i, P_j\rangle\right)_{i,j}, \tag{3.3}$$

donde $P_1, \ldots, P_{r_{MW}}$ es una base para la parte libre de $E(K)$, y $\langle\ ,\ \rangle$ es una forma bilineal en $E(K)$, que se calcula en términos de la *altura de Néron-Tate* definida en $E(K)$. Notar la similitud entre (3.3) y (1.2).

Sin dudas, de los invariantes involucrados en la conjetura de Birch y Swinnerton-Dyer, el más complicado es el *grupo de Tate-Shafarevich*, que juega un rol análogo al de $Cl(K)$ en la fórmula para el número de clases.

Para definirlo, consideramos la acción de $G_K := \mathrm{Gal}(\overline{K}/K)$ en $E(\overline{K})$. Cada primo $\mathfrak{p}$ de K induce una valuación en $K^\times$, dada por $x \mapsto e_\mathfrak{p}$, si $(x)_{\mathcal{O}_K} = \prod_\mathfrak{q} \mathfrak{q}^{e_\mathfrak{q}}$ con $\mathfrak{q}$ primo y $e_\mathfrak{q} \in \mathbb{Z}$. Denotamos por $K_\mathfrak{p}$ a la completación de K con respecto a esta valuación. Podemos entonces considerar también la acción de $G_{K_\mathfrak{p}} := \mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$ en $E(\overline{K_\mathfrak{p}})$. Como $G_{K_\mathfrak{p}}$ es un subgrupo de G_K, podemos considerar el morfismo

$$H^1(G_K, E(\overline{K})) \longrightarrow \prod_\mathfrak{p} H^1(G_{K_\mathfrak{p}}, E(\overline{K_\mathfrak{p}})),$$

que en cada coordenada viene dado por la restricción de G_K a $G_{K_\mathfrak{p}}$. El grupo de Tate-Shafarevich es el núcleo de este morfismo, y se denota por $Ш(E/K)$. Se conjetura que este grupo abeliano es finito.

¿Qué relación hay entre el grupo de Tate-Shafarevich y el grupo de clases? Ambos miden la obstrucción a que elementos localmente triviales (una clase de cohomología, o un ideal fraccionario) sean globalmente triviales. Más concretamente, si consideramos la acción de G_K en $\mathcal{O}_{\overline{K}}^\times$, se puede probar que $Cl(K)$ es isomorfo al núcleo del morfismo

$$H^1(G_K, \mathcal{O}_{\overline{K}}^\times) \longrightarrow \prod_\mathfrak{p} H^1(G_{K_\mathfrak{p}}, \mathcal{O}_{\overline{K_\mathfrak{p}}}^\times).$$

Sobre el último de los invariantes que hace falta introducir, la *constante de Tamagawa*, no entraremos en detalles. Se define como un producto de factores locales elementales, determinados por la geometría de la curva en los primos de mala reducción y en el infinito. La denotaremos por c.

Ahora sí, podemos enunciar el análogo al Teorema 2.1.

Conjetura 3.3 (Birch y Swinnerton-Dyer)**.**

1. *La función $L(E/K, s)$ se puede continuar de manera holomorfa a todo $\mathbb{C}$.*
2. *Sea r el orden con el que se anula $L(E/K, s)$ en $s = 1$. Entonces, $r = r_{MW}$.*
3.

$$\frac{L^{(r)}(E/K, 1)}{r!} = \frac{c}{\sqrt{|\operatorname{disc}(K)|}} \cdot |Ш(E/K)| \cdot \frac{\operatorname{reg}(E/K)}{|T(E(K))|^2}. \tag{3.4}$$

A diferencia de lo que sucede con la fórmula para el número de clases, esta conjetura dista mucho de ser un teorema[3]. La parte 1 se sabe cierta para cuerpos K totalmente reales (i.e. con $s = 0$), y solo a partir de los trabajos de Wiles, Taylor y otros sobre la demostración de la conjetura de Shimura-Taniyama. El resto de la conjetura, cuando $K = \mathbb{Q}$, se sabe cierta si $r \leq 1$.

Las funciones generatrices $\zeta_K(s)$ y $L(E/K, s)$ se definen como productos cuyos factores contienen información local de K y de E/K. La fórmula para el número de clases y la conjetura de Birch y Swinnerton-Dyer relacionan esta información local con invariantes globales de estos objetos.

Concluimos estas notas comparando las igualdades (2.3) y (3.4) término a término.

- El miembro izquierdo de la igualdad es el "primer" coeficiente de la función generatriz correspondiente.
- El denominador $\sqrt{|\operatorname{disc}(K)|}$ aparece en ambas fórmulas.
- $Cl(K)$ se corresponde con $Ш(E/K)$. Mientras que la finitud del primero es conocida (y fácil de demostrar), la del segundo es conjetural.
- $\operatorname{reg}(K)$ se corresponde con $\operatorname{reg}(E/K)$.
- ω_K se corresponde con $|T(E(K))|$ (aunque uno aparece elevado al cuadrado, y el otro no).
- El factor $2^r(2\pi)^s$ se corresponde con la constante de Tamagawa.

Referencias

[BS66] A. I. Borevich and I. R. Shafarevich. *Number theory*. Pure and Applied Mathematics, Vol. 20. Academic Press, New York-London, 1966.

[Dar09] Henri Darmon. Rational points on curves. In *Arithmetic geometry*, volume 8 of *Clay Math. Proc.*, pages 7–53. Amer. Math. Soc., Providence, RI, 2009.

[Mar77] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York-Heidelberg, 1977. Universitext.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Fundamental Principles of Mathematical Sciences*. Springer-Verlag, Berlin, 1999.

[Sch88] Peter Schneider. Introduction to the Beĭlinson conjectures. In *Beĭlinson's conjectures on special values of L-functions*, volume 4 of *Perspect. Math.*, pages 1–35. Academic Press, Boston, MA, 1988.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Wil06] Andrew Wiles. The Birch and Swinnerton-Dyer conjecture. In *The millennium prize problems*, pages 31–41. Clay Math. Inst., Cambridge, MA, 2006.

[3] De hecho, "esta fórmula relaciona el valor de una función en un punto en el que no está definida con el orden de un grupo cuya finitud no ha sido demostrada" (John Tate).

Instituto de Matemática y Estadística - Facultad de Ingeniería, Universidad de la República - Uruguay
E-mail address: nsirolli@fing.edu.uy