Fórmulas de Traza en la Teoría de Funciones L

Martín Sombra

Departamento de Matemática
Universidad Nacional de La Plata

Introducción

En 1956, como consecuencia de investigaciones en la teoría de funciones automorfas, A. Selberg [Se] desarrolló una fórmula de traza general para subgrupos discretos Γ de covolumen finito de $SL(2, R)$. Esta fórmula relaciona los autovalores de un laplaciano con cierta data determinada por Γ.

Por otra parte, en 1952, A. Weil [We] encuentra las llamadas "fórmulas explícitas" de la teoría de números, que relaciona sumas sobre los ideales primos de un cuerpo de números con sumas sobre los ceros de las funciones L. La analogía formal entre estas fórmulas es sorprendente, y es objeto de muchas especulaciones.

Recientemente, D. Golfeld [Go] dio un paso en este sentido al construir ciertos operadores integrales cuya traza es precisamente la fórmulas explícitas de Weil. Goldfeld hace esta construcción sólo para la función zeta de Riemann clásica, usando como espacio base el producto semidirecto de los ideles de Q de norma uno con los adeles de Q, factorizado por el subgrupo discreto Q^*Q, y en general sólo enuncia los resultados. Nuestro trabajo consiste entonces en el desarrollo completo de estos resultados, junto con su generalización a todas las funciones L.

En las primeras secciones de este trabajo expongo las nociones generales de teoría algebraica de números que necesito para abordar el problema. El desarrollo de estas secciones está en su mayor parte basado en el libro de Lang [La].

En §1 y §3 describo la estructura general de un cuerpo de números K, es decir una extensión finita de Q. Luego estudio con más detalle las completaciones p-ádicas y arquimedianas de K y la construcción de los grupos de adeles y de ideles del cuerpo.

En §5 introduzco las funciones L de Hecke, y enuncio la fórmula explícita asociada.

En §6 estudio las propiedades generales del producto semidirecto, y las aplico a nuestro espacio base, que es el producto semidirecto $J_K^0 A_K$ factorizado por un subgrupo discreto.

En §8, finalmente, describo la construcción de los operadores, y demuestro la fórmula de traza.

Es necesario recalcar que en esta situación estamos muy lejos aún de haber establecido alguna conexión entre la teoría de funciones L y la fórmula

de traza de Selberg. En principio, no es claro que estos operadores sean los verdaderos análogos de los operadores intregrales que aparecen en la demostración de la fórmula de traza de Selberg. Aún en el caso de que sí lo fuera nos estaría faltando, principalmente, el análogo del laplaciano, y la relación entre los autovalores de los operadores integrales y los autovalores de este hipotético laplaciano.

Quiero agradecer a Alberto Dubson, quien me sugirió el tema que desarrollo en este trabajo y me señaló varios errores en la redacción final del mismo. También quiero agradecer a Martín Argerami y a Rodolfo Rodríguez por su asistencia técnica, a Marcela Sanmartino, Tomás Tetzlaff, Antonio Di Scala y Gerardo Oleaga por sus sugerencias y su apoyo en general, y a la Fundación Antorchas , que financió mis estudios durante los últimos años de la carrera.

Indice

Prerrequisitos

Los prerrequisitos necesarios son de un carácter básico, ya que esta exposición está en su mayor parte autocontenida.

Para la sección 1, sólo es necesario un cierto conocimiento de álgebra. En todo caso, las definiciones y propiedades utilizadas se pueden encontrar en el libro de S. Lang: *Algebra*.

En las secciones 2, 4 y 6 se asume algún grado de familiaridad con espacios topológicos y con teoría de la medida.

En la sección 7 se hace uso de la noción de espacio de Hilbert y de algunas de sus propiedades, que se encuentran en todos los textos standard de análisis funcional. Una referencia puede ser Conway: *A Course in Functional Analysis*.

Cuando es necesario algún resultado que está fuera de estos prerrequisitos básicos, se lo enuncia explícitamente junto con su referencia.

1 Enteros Algebraicos (parte 1)

En esta sección se describen los aspectos básicos del anillo de enteros algebraicos de un cuerpo de números. En general, se dan las demostraciones de los resultados que se enuncian en la medida que ayuden a entenderlos.

Se asume por anillo a un anillo conmutativo, íntegro, y con unidad.

1.1 Clausura integral

Proposición 1. *Sea A un anillo contenido en un cuerpo L, y x un elemento de L. Entonces las siguientes condiciones son equivalentes*

1. *Existe un A-módulo no nulo $M \subset L$ finitamente generado tal que $xM \subset M$.*

2. *El elemento x satisface una ecuación*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

con coeficientes $a_i \in A$, y un entero $n \geq 1$.

Esta ecuación se llama **ecuación integral** para x.

Dem. Asumamos 2.. El módulo $M = \langle 1, \ldots, x^{n-1} \rangle$ es cerrado por multiplicación por el elemento x. Recíprocamente, sea $M = \langle v_1, \ldots, v_n \rangle$ un A-módulo $\neq 0$ tal que $xM \subset M$. Luego

$$\begin{array}{ccccc} xv_1 = & a_{11}v_1 & + \cdots + & a_{1n}v_n \\ \vdots & \vdots & & \vdots \\ xv_n = & a_{n1}v_1 & + \cdots + & a_{nn}v_n \end{array}$$

con coeficientes $a_{ij} \in A$ y entonces el determinante

$$\begin{vmatrix} x - a_{11} & & -a_{1n} \\ & \ddots & \\ -a_{n1} & & x - a_{nn} \end{vmatrix}$$

es una ecuación integral para x sobre A.

Un elemento $x \in L$ que satisface alguna de estas condiciones se dice **entero** sobre A.

Sea B un anillo tal que $A \subset B \subset L$. Se dice que B es **entero** sobre A si todo elemento de B es entero sobre A.

Proposición 2. *Sea A un anillo, K su cuerpo cociente, y x un elemento algebraico sobre K. Entonces existe un elemento $c \neq 0$ en A tal que cx es entero sobre A.*

Dem. Sean $a_i \in A$ tales que

$$a_n x^n + \ldots + a_0 = 0$$

Luego

$$(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_0 a_n^{n-1} = 0$$

y por lo tanto $a_n x$ es entero sobre A.

Proposición 3. *Sean $A \subset B$ anillos, B entero sobre A. Sea σ un homomorfismo de B sobre A. Luego $\sigma(B)$ es entero sobre $\sigma(A)$.*

Dem. Sea $y \in \sigma(B)$, es decir, $y = \sigma(x)$ para algún $x \in B$. Sea

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

una ecuación entera para x sobre A. Luego

$$y^n + \sigma a_{n-1}x^{n-1} + \ldots + \sigma a_0 = 0$$

es una ecuación integral para y sobre $\sigma(A)$.

Proposición 4. *Sea A un anillo contenido en un cuerpo L. Sea B el conjunto de los elementos de L que son enteros sobre A. Luego B es un anillo.*

Este anillo se llama la **clausura integral** de A en L.

Dem. Sea $x, y \in B$ y $M, N \subset L$ dos A-módulos no nulos finitamente generados tales que $xM \subset M$, $yN \subset N$. Luego MN es finitamente generado, y para $\alpha \in MN$,

$$\alpha = \sum_{i=1}^{n} a_i b_i$$

con $a_i \in M$, $b_i \in N$, y entonces $(x \pm y)\alpha, xy\alpha \in MN$.

Corolario. *Sea A un anillo, K su cuerpo cociente, y L una extensión finita separable de K. Sea $x \in L$ entero sobre A, y sea*

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

el polinomio irreducible sobre K que anula a x. Luego los a_i son enteros sobre A.

Dem. Para cada K-isomorfismo σ de L, σx es entero sobre A. Los a_i se obtienen a partir de las funciones simétricas elementales, y por lo tanto son enteros sobre A.

Un anillo A se dice **integralmente cerrado en un cuerpo** L si todo elemento de L entero sobre A pertenece a A. Se dice que A es integralmente cerrado si es cerrado en su cuerpo cociente.

Proposición 5. *Sea A un anillo noetheriano e integralmente cerrado. Sea L una extensión finta separable del cuerpo cociente K. Entonces la clausura integral de A en L es finitamente generada sobre A.*

Dem. Sea $w_1, \ldots, w_n$ una base de L sobre K. Por la proposición 2 podemos suponer que los w_i son enteros sobre A

La traza tr de L a K es no-degenerada, y por lo tanto la aplicación

$$\begin{array}{rl} \varphi: & L \to L^* \\ & x \mapsto \varphi_x: \quad L \to K \\ & \qquad\qquad y \mapsto \text{tr } (xy) \end{array}$$

es un isomorfismo de L en su espacio dual. Sea $w_1', \ldots, w_n'$ la base dual de $w_1, \ldots, w_n$, i.e. tal que

$$\text{tr } (w_i' w_j) = \delta_{ij}$$

Sea $c \in A$, $c \neq 0$ tal que cw_i' es entero sobre A. Sea z entero sobre A. Luego

$$z = b_1 w_1 + \ldots + b_n w_n$$

para ciertos $b_i \in K$. Como $cw_i' z$ es entero sobre A, entonces

$$\text{tr } (cw_i' z) = cb_i \in A$$

por ser A integralmente cerrado. Luego, la clausura integral de A está contenida en el A-módulo $c^{-1}\langle w_1, \ldots, w_n \rangle$. Como A es noetheriano, todo A-módulo finitamente generado es noetheriano, y por lo tanto, la clausura integral es finitamente generada.

Proposición 6. *Si A es un dominio de factorización única, entonces A es integralmente cerrado.*

Dem. Supongamos que existe un elemento de la forma a/b, con $a, b \in A$, y un elemento primo p en A que divide a b y no a a. Sea

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \ldots + a_0 = 0$$

una ecuación integral para a/b. Luego

$$a^n + a_{n-1}a^{n-1}b + \ldots + a_0 b^n = 0$$

Como p divide a b, divide a a^n, y por lo tanto a a, contradicción.

Teorema 1. *Sea A un anillo principal, L una extensión finita separable de su cuerpo cociente K de grado n. Entonces la clausura integral de A en L es un A-módulo libre de rango n.*

Dem. A es un anillo principal, y por lo tanto noetheriano y de factorización única. Por la proposición 6, A es integralmente cerrado.

La clausura integral B está finitamente generada, no tiene torsión, y por la teoría de anillos principales, es un A-módulo libre.

Sea $w_1, \ldots, w_n$ una base de L sobre K con $w_i \in B$. Luego el A-módulo generado por los w_i está contenido en B, y es de rango n, y por lo tanto B es de rango n.

El teorema se aplica al anillo Z. Una extensión finita de los números racionales Q se llama un **cuerpo de números**. La clausura integral de Z en un cuerpo de números K es el anillo de los **enteros algebraicos** de K, y lo denotamos por A_K.

1.2 Ideales primos

Sean A, B anillos tales que $A \subset B$. Sean p, B ideales primos de A y de B respectivamente. Se dice que B **divide** a p si $\mathrm{B} \bigcap A = \mathrm{p}$, y se escribe B|p.

Proposición 7. *Sean A, B anillos tales que $A \subset B$, y B es entero sobre A. Sean p, B ideales primos de A y B respectivamente. Entonces B es maximal si y sólo si p es maximal.*

Proposición 8. *Sea A un anillo integralmente cerrado, L una extensión finita separable de su cuerpo cociente K, y B la clausura integral de A en L. Sea p un ideal primo de A. Luego el número de ideales primos $B|p$ de B es finita y positiva.*

1.3 Anillos de Dedekind

Sea A un anillo y K su cuerpo cociente. Un **ideal fraccionario** de A es un A-módulo $\mathrm{p} \subset K$ tal que existe un elemento $c \neq 0$ en A tal que $c\mathrm{p} \subset A$.

Un anillo A se dice de **Dedekind** si es noetheriano, integralmente cerrado en su cuerpo cociente, y tal que todo ideal primo no nulo es maximal. El anillo de los enteros algebraicos es un anillo de Dedekind.

Teorema 2. *Sea A un anillo de Dedekind. Entonces todo ideal de A se puede factorizar de una única manera en ideales primos, y el conjunto de los ideales fraccionarios no nulos forma un grupo por multiplicación.*

Proposición 8. *Sea A un anillo de Dedekind con un número finito de ideales primos. Entonces A es principal.*

Un **ideal fraccionario principal** es un ideal fraccionario generado por un único elemento α del curpo cociente de A.

Sea A un anillo de Dedekind. El grupo de los ideales fraccionarios módulo el grupo de los ideales fraccionarios principales se llama el **grupo de clases de ideales** de A.

Sea A un anillo de Dedekind, K su cuerpo cociente, L una extensión finita separable de K, y B la clausura integral de A en L. Si $\mathfrak{p}$ es un ideal primo de A, $\mathfrak{p}B$ es un ideal de B, y tiene una factorización

$$\mathfrak{p}B = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_r^{e_r}$$

en primos de B. Un primo $\mathfrak{B}$ de B ocurre en la factorización de $\mathfrak{p}B$ si y sólo si $\mathfrak{B}|\mathfrak{p}$.

Cada e_i se llama el **índice de ramificación** de $\mathfrak{B}_i$ sobre $\mathfrak{p}$

Si $\mathfrak{B}$ divide a $\mathfrak{p}$, se denota por $f_{\mathfrak{B}}$ al grado de la extensión $B/\mathfrak{B}$ sobre $A/\mathfrak{p}$, y se llama el **grado residual**.

Proposición 9. *Sea A un anillo de Dedekind, K su cuerpo cociente, L una extensión finita separable de K, y B la clausura integral de A en L. Sea p un ideal primo de A. Entonces*

$$[L : K] = \sum_{B|p} e_B f_B$$

Sea A un anillo de Dedekind tal que $A/\mathfrak{p}$ es finito para cada ideal primo $\mathfrak{p}$. Se define

$$N\mathfrak{p} = \#(A/\mathfrak{p})$$

para un ideal primo $\mathfrak{p}$, y se extiende esta aplicación al grupo de los ideales fraccionarios por multiplicación. Por la factorización única, esta aplicación está bien definida, y si $\mathfrak{p}$ es un ideal (entero) no nulo,

$$N\mathfrak{p} = \#(A/\mathfrak{p})$$

Si p es un ideal fraccionario principal generado por un elemento $\alpha \in K$, entonces

$$N\mathfrak{p} = N\alpha \ (= \prod_{\sigma} \sigma\alpha)$$

2 Completaciones de un Cuerpo de Números

En esta sección se estudia la estructura de las completaciones de un cuerpo de números bajo las topologías p-ádicas y de las completaciones obtenidas por la inmersión del cuerpo de números en los números reales o complejos.

2.1 Valores absolutos sobre un cuerpo de números

Sea K un cuerpo. Un **valor absoluto** sobre K es una función

$$\begin{aligned} v: \ & K \to R^+ \\ & x \mapsto |x|_v \end{aligned}$$

con las siguientes propiedades :

1. $|x|_v = 0$ si y sólo si $x = 0$.
2. $|xy|_v = |x|_v |y|_v$.
3. $|x + y|_v \leq |x|_v + |y|_v$.

Si en lugar de **3.** el valor absoluto satisface la condición más fuerte

4. $|x + y|_v \leq$ máx$(|x|_v, |y|_v)$,

entonces se dice que es una **valuación** o que es no arquimediano.

Lema 1. *Sea v una valuación sobre un cuerpo K. Sean $x, y \in K$ tales que $|x|_v < |y|_v$. Luego $|x + y| = |x|_v$*

Dem. Tenemos

$$\begin{aligned} |x+y| &\leq \max(|x|,|y|) = |x| \\ |x| &\leq \max(|y|,|x+y|) = |x+y| \end{aligned}$$

El valor absoluto tal que $|x| = 1$ para todo $x \neq 0$ se llama **trivial**.

Un valor absoluto v define una función distancia $(x,y) \mapsto |x-y|_v$,y por lo tanto, una topología sobre K. Dos valores absolutos se dicen **dependientes** si definen la misma topología; en otro caso se dice que son **independientes**.

Proposición 1. *Dos valores absolutos no triviales* $|\ |_1, |\ |_2$ *sobre* K *son dependientes si y sólo si existe algún* $\lambda > 0$ *tal que*

$$|x|_1 = |x|_2^{\lambda}$$

para todo $x \in K$.

Dem. Si tenemos que

$$|x|_1 = |x|_2^{\lambda}$$

para un $\lambda > 0$ es claro que $|\ |_1$ y $|\ |_2$ son valores absolutos dependientes. Recíprocamente, sea $x \in K$. Tenemos que $|x|_1 < 1$ si y sólo si $\lim_{n\to\infty} x^n = 0$, y por lo tanto $|x|_2 < 1$. Análogamente, si $|x|_1 > 1$, tenemos que $|x^{-1}| < 1$, y se sigue también que $|x|_2 > 1$.

Como $|\ |_1$ es no trivial, existe un $y \in K$ tal que $|y|_1 > 1$. Sea entonces $x \in K$, con $|x|_1 \geq 1$. Luego hay algún $\alpha > 0$ tal que $|x|_1 = |y|_1^{\alpha}$. Sean m, n enteros > 0 tales que $m/n > \alpha$. Tenemos que

$$|x|_1 < |y|_1^{m/n}$$

Luego $|x^n/y^m|_1 < 1$, $|x^n/y^m|_2 < 1$, y por lo tanto

$$|x|_2 < |y|_2^{m/n}$$

Análogamente, si $m/n < \alpha$, tenemos que

$$|x|_2 > |y|_2^{m/n}$$

y por lo tanto $|x|_2 = |y|^{\alpha}$. Se sigue entonces que

$$|x|_1 = |x|_2^{\lambda}$$

para todo $x \in K$, con $\lambda = \log|y|_1 / \log|y|_2$, cqd.

Sea v un valor absoluto sobre K. Decimos que K es **completo** (con respecto a v) si toda sucesión de Cauchy converge.

Sea K un cuerpo completo, E una extensión finita de K, y $|\ |_1$, $|\ |_2$ dos extensiones de v a E. Tenemos que

$$|\ |_1 = |\ |_2^{\lambda}$$

para algún $\lambda > 0$, y $|\ |_1 = |\ |_2$ para todo $x \in K$. Se sigue entonces que una extensión de v a E está unívocamente determinada.

Sea K un cuerpo de números algebraicos, y A_K el anillo de enteros de K. Dado un ideal fraccionario no nulo a de A_K tenemos una representación única

$$a = \prod_{\mathrm{p}} \mathrm{p}^{e\mathrm{p}(a)}$$

donde p recorre los ideales primos de A_K y los $e_{\mathrm{p}}(a)$ son enteros casi todos nulos. Definimos

$$\mathrm{ord}_{\mathrm{p}}(a) = e_{\mathrm{p}}(a)$$

para un ideal primo p, y extendemos esta definición a los elementos $a \in K^*$ haciendo

$$\mathrm{ord}_{\mathrm{p}}(x+y) \geq \min(\mathrm{ord}_{\mathrm{p}}x, ord_{\mathrm{p}}y)\mathrm{ord}_{\mathrm{p}}(a) = \mathrm{ord}_{\mathrm{p}}((a))$$

donde (a) es el ideal fraccionario principal generado por a.

Para x, $y \in K$ tenemos que

$$\mathrm{ord}_{\mathrm{p}}xy = \mathrm{ord}_{\mathrm{p}}x + \mathrm{ord}_{\mathrm{p}}y$$

Sea $c \in R$, $0 < c < 1$. Si definimos

$$|x| = c^{\mathrm{ord}_{\mathrm{p}}x}$$

para $x \in K^*$, tenemos entonces una valuación sobre K. La elección de la constante c es arbitraria. Sea p el número primo que genera $\mathrm{p} \cap Z$. Luego sea $e = \mathrm{ord}_{\mathrm{p}}p$ el índice de ramificación de p sobre p. Definimos entonces

$$|x|_{\mathrm{p}} = p^{\frac{-\mathrm{ord}_{\mathrm{p}}x}{e}}$$

y $|\ |_{\mathrm{p}}$ es entonces una extensión de la valuación $|\ |_p$ sobre Q.

Asimismo, toda inmersión de K en C induce un valor absoluto sobre K, que se llamará **real** o **complejo** según le caso.

Sea K un cuerpo de números. El conjunto de valores absolutos sobre K que consiste en las valuaciones p-adicas y en los valores absolutos reales y complejos se llama el **conjunto canónico**, que se denota M_K. Los valores absolutos reales y complejos en M_K se llaman también **arquimedianos**. Cada $w \in M_K$ es extensión de un $v \in M_Q$, y escribimos

$$w|v$$

2.2 Completaciones arquimedianas y p-ádicas

Sea K un cuerpo de números, y sea v un valor absoluto canónico sobre K. Podemos hacer entonces la completación de K con respecto a v. Consideramos $\mathcal{C}_K$ el anillo de las sucesiones de Cauchy de elementos en K. El conjunto $\mathcal{N}_K$ de las sucesiones nulas es un ideal maximal, y por lo tanto $\mathcal{C}_K/\mathcal{N}_K$ es un cuerpo, que denotamos K_v. K está naturalmente incluído en K_v por la aplicación $\alpha \mapsto (\alpha)_{n\in N}$, y el valor absoluto sobre K se extiende a K_v por continuidad. K_v es un cuerpo completo, que se llama la **completación** de K_v.

Sea v un valor absoluto arquimediano. Luego tenemos que K_v contiene a la clausura de Q, que es R, y por lo tanto $K \cdot R \subset K_v$. Como $K \cdot R$ es una extensión finita de R, es igual a R o a C, y es completa. Luego $K_v = K \cdot R$.

Sea v una valuación correspondiente a un ideal primo del anillo de enteros algebraicos de K, entonces se dice que K_v es el cuerpo de los números p-**ádicos**.

Sea $x \in K_v$, $x \neq 0$, y sea $x_0 \in K$ tal que

$$|x - x_0| < |x|$$

Por el carácter no arquimediano de $|\ |$, se sigue

$$|x_0| = |x - (x - x_0)| = |x|$$

Tenemos entonces que la imagen de K_v por $|\ |$ es igual a la de K, un grupo cíclico. Si π es un elemento de orden 1 en p, entonces $|\pi|$ genera a este grupo.

Denotamos por A_v la clausura de A_K en K_v. Sea $x \in K$ un elemento de valor absoluto ≥ 1. Por la proposición 2 de 1.1, existen $a \in \mathrm{A}_K$, $b \in Z - \mathrm{p}Z$

tales que $x = a/b$. Tenemos $\mathrm{p} + (b) = \mathrm{A}_K$ por ser p un ideal maximal. Sean $\alpha \in \mathrm{p}$, $\beta \in (b)$ tales que $\alpha + \beta = 1$. Luego $1 = (\alpha + \beta)^n = \alpha^n + \beta_0$, con $\alpha^n \in \mathrm{p}^n$, $\beta_0 \in (b)$, de donde se sigue

$$(b) + \mathrm{p}^n = \mathrm{A}_K$$

Sea $x_0 \in \mathrm{A}_K$ tal que $a - bx_0 \in \mathrm{p}^n$. Luego

$$|x - x_0| \leq |\mathrm{p}|^n$$

de donde se sigue que A_K es denso en $\{x \in K : |x| \leq 1\}$, y por lo tanto, $\mathrm{A}_v = \{x \in K_v : |x| \leq 1\}$.

De una manéra análoga, tenemos que la clausura de p consiste en los elementos de A_v de valor absoluto < 1, y es el único ideal maximal de A_v. A_v es un dominio de factorización única, con un único primo. Todo elemento $\alpha \neq 0$ en K_v se escribe como

$$\alpha = u\pi^r$$

donde $|u| = 1$, y por lo tanto u es unidad de A_v.

Los subgrupos p_v^r $(r = 1, 2, \ldots)$ son **abiertos** y **cerrados** en la topología de K_v, ya que

$$\mathrm{p}_v^r = \{x \in K_v : |x|_v < |\pi|^{r-1}\} = \{x \in K : |x|_v \leq |\pi|^r\}$$

y forman un sistema fundamental de entornos de 0 en K_v. Como grupos aditivos, tenemos que $\mathrm{p}_v^r/\mathrm{p}_v^{r-1}$ es isomorfo a $\mathrm{A}_v/\mathrm{p}_v$, por multiplicación a derecha por π^r.

Las unidades de A_v forman un grupo, que denotamos por U_v. para cada entero $i \geq 1$, sea

$$U_i = 1 + \mathrm{p}_v^i$$

Luego U_i es un grupo, porque si $x, y \in \mathrm{p}_v^i$, tenemos que

$$\begin{aligned} (1+x)(1+y) &= 1 + x + y + xy \ \in 1 + \mathrm{p}_v^i \\ (1-x)^{-1} &= 1 + x + x^2 + \ldots \ \in 1 + \mathrm{p}_v^i \end{aligned}$$

Tenemos que

$$U = \{x \in \mathrm{A}_v : |x| = 1\} = \mathrm{A}_v - \mathrm{p}_v$$

y por lo tanto es un abierto de A_v. Los U_i también son abiertos, y forman un sistema fundamental de entornos de 1 en K_v^*.

Bajo la aplicación canónica

$$\begin{array}{rl} \varphi: & \mathrm{A} \to \mathrm{A/p} \\ & x \mapsto x + \mathrm{p}_v \end{array}$$

tenemos el homomorfismo inducido

$$\varphi : U \to (\mathrm{A/p})^*$$

y su núcleo es U_1. Luego nos queda

$$U/U_1 \simeq (\mathrm{A/p})^*$$

También tenemos la aplicación

$$\begin{array}{l} \mathrm{p}^i/\mathrm{p}^{i+1} \to U_i/U_{i+1} \\ x + \mathrm{p} \mapsto (1+x)U_i \end{array}$$

que es un isomorfismo. El cuerpo residual A/p es una extensión finita de F_p, y es entonces un cuerpo finito.

Proposición 2. *A y U son grupos compactos.*

Dem. Tenemos que $\mathrm{A}_v/\mathrm{p}_v$ es un grupo finito, y por lo tanto compacto. La aplicación

$$\begin{array}{rl} \psi: & \mathrm{A} \to \prod_n \mathrm{A}_v/\mathrm{p}_v^n \\ & x \mapsto \prod_n (x + \mathrm{p}_v^n) \end{array}$$

es una inmersión, que identifica a A_v como un subgrupo de $\prod_n \mathrm{A}_v/\mathrm{p}_v^n$. Tenemos

$$\begin{array}{rcl} \psi(\mathrm{p}_v^N) & = & \{\{0\}^N \times \prod_{n>N}(x + \mathrm{p}^n) : x \in \mathrm{p}_v^n\} \\ & = & \psi(\mathrm{A}_v) \bigcap \{0\}^n \times \prod_{n>N} \mathrm{A}_v/\mathrm{p}_v^n \end{array}$$

y por tanto ψ es compatible con la topología de A_v. Se sigue que A_v es un subgrupo cerrado de $\prod_n (x + \mathrm{p}_v^n)$, y por lo tanto es compacto.

El grupo de unidades U_v es también compacto, por el mismo argumento, o bien por ser un subconjunto cerrado de A_v.

Sea v una valuación sobre Q correspondiente a un primo p, y sea Q_v la completación de Q. Para una extensión finita E de Q_v, sea A_E el anillo de los enteros algebraicos de E, es decir, los elementos $x \in E$ tales que

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

para ciertos $a_0, \ldots, a_{n-1} \in \mathrm{A}_v$. Luego existe un ideal primo p de A_E sobre p (i.e. $(p) = \mathrm{A}_v \bigcap \mathrm{p}$), y por lo tanto existe una extensión de la valuación v a

una valuación w sobre E, que es la inducida por el ideal primo p. De aquí se sigue que $\overline{Q}_v$, la clausura algebraica de Q_v, es un cuerpo valuado. Al ser Q_v un cuerpo completo, tenemos que la prolongación de v a una extensión finita está unívocamente determinada, y por lo tanto, también lo está la extensión de v a $\overline{Q}_v$.

Sea K un cuerpo de números, y w una valuación sobre K, extensión de la valuación v sobre Q. Luego $K \cdot Q_v$ es una extensión finita de Q_v contenida en K_w. Sabemos que $K \cdot Q_v$ es completo, y por lo tanto es igual a K_w. Entonces el valor absoluto w sobre K está dado por una inmersión de K en $\overline{Q}_v$. Lo mismo vale claramente para los valores absolutos arquimedianos.

Teorema 1. *Sea v un valor absoluto canónico sobre Q, K un cuerpo de números. Dos inmersiones*

$$\sigma, \tau : K \to \overline{Q}_v$$

sobre Q dan lugar al mismo valor absoluto sobre K si y sólo si el Q-isomorfismo

$$\sigma\tau^{-1} : \tau K \to \sigma K$$

se puede extender a un Q_v-isomorfismo

$$\sigma\tau^{-1} : \tau K \cdot Q_v \to \sigma K \cdot Q_v$$

En este caso decimos que las inmersiones son **conjugadas** sobre Q_v.

Dem. Supongamos que las dos inmersiones son conjugadas sobre Q_v. Por la unicidad de la extensión del valor absoluto de Q_v a $\overline{Q}_v$ tenemos

$$|x| = |\sigma\tau^{-1}x|$$

para todo elemento $x \in \tau K \cdot Q_v$. En particular, si $x \in K$

$$|\tau x| = |\sigma x|$$

es decir, que el valor absoluto inducido es igual. Supongamos ahora que este es el caso. Como τK es denso en $\tau K \cdot Q_v$, un elemento $x \in \tau K \cdot Q_v$ se puede escribir como

$$x = \lim_n \tau x_n$$

con $x_n \in K$. Como los valores absolutos coinciden, se sigue que la sucesión

$$\{\sigma\tau^{-1}\tau x_n\}_n = \{\sigma x_n\}_n$$

converge a un elemento $x \in \sigma K \cdot Q_v$, que denotamos por $\sigma\tau^{-1}x$. Este elemento no depende de la sucesión particular σx_n, y la aplicación

$$\sigma\tau^{-1} : \tau K \cdot Q_v \to \sigma K \cdot Q_v$$

es claramente un Q_v-isomorfismo.

Corolario 1. *Sea K un cuerpo de números, y sea $\alpha \in K$ un generador de K sobre Q, es decir $K = Q[\alpha]$. Si α tiene r_1 conjugados reales y r_2 pares de conjugados complejos, entonces K admite r_1 valores absolutos reales y r_2 valores absolutos complejos.*

Dem. Tenemos $\overline{Q}_\infty = C$, y el único R-isomorfismo no trivial de C es $z \mapsto \bar{z}$.

Corolario 2. *Sea K un cuerpo de números. Sea $v \in M_Q$, y para cada valor absoluto w sobre K que extiende a v, sea n_w el grado local,*

$$n_w = [K_w : Q_v]$$

Entonces

$$\sum_{w|v} n_w = n$$

Dem. Sea $\alpha \in K$ tal que $K = Q[\alpha]$, y sea F_α el polinomio irreducible asociado a α. Luego f_α tiene $n = [K : Q]$ raíces $\alpha_1, \ldots, \alpha_n$ distintas en $\bar{Q}_v$. Por el Teorema 1, cada completación está dada por algún α_i, es decir,

$$K_w = Q_v[\alpha_i]$$

y el grado de K_w sobre Q_v es igual a la cantidad de conjugados de α_i sobre Q_v. Cada Q_v-isomorfismo de K_w induce un Q-isomorfismo de K, y por lo tanto, los Q_v-conjugados de α_i son los α_j tales que el Q-isomorfismo inducido por α_j se puede extender a un Q_v-isomorfismo, y de aquíse sigue la fórmula.

Sea $\alpha \in K$, y v un valor absoluto en M_K. Definimos

$$\|\alpha\|_v = |\alpha|_v^{n_v}$$

Corolario 3. *Sea K un cuerpo de números, v un valor absoluto en M_Q. Sea $\alpha \in K$. Entonces*

$$\prod_{w|v} \|\alpha\|_w = |N_Q^K(\alpha)|_v$$

Dem.

$$N_Q^K(\alpha) = \prod_\sigma \sigma\alpha$$

donde σ recorre las Q-inmersiones de K en Q_v. Tomando valor absoluto en ambos miembros se sigue el corolario.

Sea q un número racional. Tenemos

$$\prod_{v \in M_Q} |q|_v = |q|_\infty \prod_{v \neq \infty} p^{-\mathrm{ord}_p q} = 1$$

Tenemos entonces por el corolario 3., para $\alpha \in K$ un cuerpo de números, que

$$\prod_{w \in M_K} \|\alpha\|_w = \prod_{v \in M_Q} |N_Q^K(\alpha)|_v = 1$$

Esta es la **fórmula del producto**.

3 Enteros Algebraicos (parte 2)

Esta sección es la continuación de la sección 1, y cubre aspectos no tan evidentes de un cuerpo de números.

En §1 se definen la diferente y el discriminante, que dan información acerca de los primos ramificados del anillo A_K.

En §2 se describen los teoremas clásicos sobre la finitud de las clases de ideales, y sobre la estructura del grupo de las unidades del anillo de enteros algebraicos.

3.1 La diferente y el discriminante

Sea A un anillo de Dedekind, K su cuerpo cociente, E una extensión finita separable de K, y B la clausura integral de A en E. El conjunto de los $x \in E$ tales que

$$\mathrm{tr}_K^E(xB) \subset A$$

es un ideal B'_E fraccionario que contiene a B. Se define la **diferente** $\mathcal{D}_E$ como ${B'_E}^{-1}$, que es entonces un ideal entero de B.

Sea K un cuerpo de números. Entonces la diferente de K se puede localizar en las completaciones p-ádicas para calcularla localmente.

Proposición 1. *Sea p un ideal primo de A_K, y v la valuación asociada a p. Entonces*

$$\mathcal{D}_K \cdot A_v = \mathcal{D}_{K_v}$$

Formalmente, se sigue

$$\mathcal{D} = \prod_{\mathrm{p}} \mathcal{D}_{\mathrm{p}}$$

Llamamos a $\mathcal{D}_K$ la **diferente local**, y a $\mathcal{D}_{K_v}$ la **diferente global**.

Proposición 2. *Un ideal primo p se ramifica sobre Z si y sólo si $p|\mathcal{D}_K$.*

Corolario . *La cantidad de ideales primos de A_K ramificados es finita.*

Sea $W = (w_1, \ldots, w_n)$ una base del Z- módulo A_K. Definimos el **discriminante** de W como

$$D_K(W) = \det(\sigma_i w_j)^2$$

donde σ_i recorre los n Q-isomorfismos de K en la clausura algebraica de Q.

Este número es un entero, y no depende de la base elegida. Lo llamaremos **el** discriminante del cuerpo, y lo denotamos por D_K.

Proposición 3.*La diferente y el discriminante están relacionados por la fórmula*

$$N\mathcal{D}_K = D_K$$

3.2 Clases de ideales, Teorema de las unidades

Sea K un cuerpo de números. Denotamos por I_K al grupo de los ideales fraccionarios no nulos, y por P_K al subgrupo de los ideales fraccionarios principales. El grupo cociente I_K/P_K es el grupo de las clases de ideales de K.

Teorema 1. (Finitud de número de clases de ideales) *I_K/P_K es finito.*

El cardinal h de I/P se llama el **número de clases** de K.

Ahora consideramos el grupo U_K de las unidades del anillo A_K. La parte de torsión de U_K está compuesta por las raíces de la unidad contenidas en K, y denotamos este subgrupo por G_K.

Sea S_∞ el conjunto de los valores absolutos arquimedianos en M_K. Sean r_1, r_2 el número de valores absolutos reales y complejos respectivamente. Luego

$$r_1 + 2r_2 = [K : Q]$$

El grado local n_v es 1 si v es real y 2 si v es complejo. Sea $r = r_1 + r_2 - 1$.

Teorema 2.(Teorema de las unidades) *El grupo G_K es finito, y U_K/G_K es un Z-módulo libre de rango r.*

Si $\alpha \in K$, sea $\alpha^{(i)}$ el j-ésimo conjugado de α para $j = 1, \ldots, r$.

Sean $u_1, \ldots, u_r$ una base de U_K/G_K. El valor absoluto del determinante

$$\begin{vmatrix} n_1 \log|u_1^{(1)}| & \cdots & n_1 \log|u_r^{(1)}| \\ \vdots & & \vdots \\ n_r \log|u_1^{(r)}| & \cdots & n_r \log|u_r^{(r)}| \end{vmatrix}$$

es no nulo, y no depende de la elección de la elección de la base. Este número es el **regulador** del cuerpo.

4 Adeles e Ideles

En la teoría clásica se considera la inmersión de un cuerpo de números en el producto cartesiano de sus completaciones bajo los valores absolutos arquimedianos. Actualmente se considera más conveniente tomar el producto sobre todas las completaciones, incluyendo las p-ádicas, con ciertas restricciones sobre las componentes. Esto conduce a los adeles y los ideles del cuerpo, que corresponden a las construcciones aditiva y multiplicativa respectivamente. En esta sección se describen sus aspectos básicos y su topología.

4.1

Sea K un cuerpo de números. Para cada valor absoluto canónico v sobre K tenemos la completación K_v de K, que es R, C o un cuerpo p-ádico.

El grupo aditivo K_v y el grupo multiplicativo K_v^* son localmente compactos. Cada uno contiene un subgrupo abierto y compacto, en el caso p-ádico. Estos son los enteros p-ádicos y las unidades p-ádicas respectivamente.

Sea M un conjunto de índices, y para cada $v \in M$, sea G_v un grupo conmutativo localmente compacto. Sea $S_0 \subset M$ un conjunto finito tal que para todo $v \notin S_0 H_v$ es un subgrupo abierto-compacto de G_v. El **producto directo restringido** de los G_v con respecto a los H_v es

$$G = \overline{\prod}_{v \in M} G_v/H_v = \{(x_v)_v : x_v \in H_v \text{ para casi todo } v\}$$

Donde "casi todo" significa "todos salvo finitos". Sea S un conjunto finito de índices que contiene a S_0. Luego

$$G_S = \prod_{v \in S} G_v \times \prod_{v \notin S} H_v$$

es el producto directo de grupos localmente compactos, donde casi todos son grupos compactos. Luego G_S es un grupo localmente compacto (con la topología producto). Entonces G es un grupo localmente compacto, haciendo que cada G_S sea un subgrupo abierto.

Sea para cada $v \in \{U_i^v\}_i$ una base de la topología de G_v. Luego, los conjuntos de la forma

$$\prod_{v \in S} U_{i_v}^v \times \prod_{v \notin S} H_v$$

forman una base de la topología de G. En particular, si para cada v, G_v es separable, entonces G es separable.

El producto directo restringido de los grupos K_v con respecto a los enteros locales A_v (que están definidos sólo cuando v es una valuación p-ádica) se llama el **grupo de adeles** de K, y se denota por A_K.

El producto directo restringido de los grupos K_v^* con respecto a las unidades U_v del anillo A_v se llama el **grupo de ideles** de K.

Un elemento $\alpha \in K$ es un entero p-ádico para casi todo p, y entonces podemos identificar a K dentro de los adeles mediante la aplicación

$$\alpha \mapsto (\alpha)_{v \in M}$$

Análogamente, un elemento no nulo de K^* es una unidad p-ádica para casi todo p, y por lo tanto K^* está incluído en los ideles.

Teorema 1. *K es un subgrupo discreto de los adeles A. K^* es un subgrupo discreto de J.*

Dem. Sea $\alpha \in K$. Que α esté cerca de 0 en la topología de A_K si $|\alpha|_v \leq 1$ para casi todo v, y $|\alpha|_v < \epsilon$ para un conjunto finito de índices v. Por la fórmula del producto, tenemos que $\alpha = 0$, y entonces 0 es un punto aislado de K en A.

Sea α un elemento tal que $|\alpha - 1| < \epsilon$ para v arquimediado. Por lo anterior, tenemos que $\alpha = 1$, y por lo tanto, K^* es discreto en J.

Introducimos ahora las nociones de grupo topológico y de medida de Haar.

Un **grupo topológico** G es un espacio de Hausdorff con una estructura de grupo tal que la aplicación

$$\begin{aligned} \phi: \quad & G \times G \to G \\ & (x, y) \mapsto xy^{-1} \end{aligned}$$

es continua.

Sea G un grupo localmente compacto. Una **medida de Haar** h es una medida de Borel[1] tal que $h(E) > 0$ para todo conjunto abierto de Borel E, y que satisface alguna de las siguientes propiedades

1. Para todo $a \in G,\ h(aA) = h(A)$
2. Para todo $a \in G,\ h(Aa) = h(A)$.

[1] [Ha] p.219

para todo conjunto de Borel A. Entonces se dice que h es invariante a **izquierda** o a **derecha** respectivamente.

Todo grupo localmente compacto G tiene una medida de Haar invariante a izquierda y medida de Haar invariante a derecha, únicas salvo multiplicación por una constante positiva[2]. Cuando estas medidas son iguales, decimos que el grupo G es **unimodular**. Los grupos compactos son unimodulares.

Sea v un valor absoluto arquimediano. Luego K_v es el cuerpo real o complejo, y si λ_v es la medida usual en la recta o en el plano, definimos

$$\mu_v = n_v \lambda_v$$

Sea v una valuación correspondiente a un primo p de A_K. En este caso, elegimos a μ_v como la medida de Haar sobre K_v tal que

$$\mu_v(\mathrm{A}_v) = (N\mathcal{D}_v)^{-1/2}$$

Proposición 1. *Sea v un valor absoluto canónico sobre K, μ la medida de Haar sobre K_v, y $a \in K_v^*$. Entonces*

$$\mu(aA) = \|a\|_v \mu(A)$$

para todo conjunto $A \subset K_v$ medible.

Dem. Si v es arquimediano la afirmación es clara. Luego sea v un valor absoluto p-ádico, y a un elemento de K_v^*. La aplicación del σ-anillo de Borel de K_v en R dada por

$$A \mapsto \mu_v(aA)$$

define una medida de Haar sobre K_v, y por lo tanto

$$\mu_v(aA) = c\mu_v(A)$$

para alguna constante c que no depende del conjunto A. Sea $a \in \mathrm{A}_v - \{0\}$. Tenemos entonces que $a\mathrm{A}_v$ es un subgrupo abierto de A_v de índice $N\mathrm{p}^{\mathrm{ord}_\mathrm{p} a}$, y por lo tanto

$$\mu(a\mathrm{A}_v) = N\mathrm{p}^{-\mathrm{ord}_\mathrm{p} a}\mu(\mathrm{A}_v) = \|a\|_v \mu(\mathrm{A})$$

ya que $n_v = e_v f_v$, donde e_v es el índice de ramificación de p sobre p, y f_v es el grado de la extensión A_K/p sobre F_p (ver §1.3). Tenemos entonces

$$\mu_v(a\mathrm{A}_v) = \|a\|_v \mu_v(A)$$

[2][Ha] cap. XI

para todo A. Si $a \in K_v - \mathrm{A}_v$, entonces $a^{-1} \in \mathrm{A}_v - \{0\}$, y de lo anterior se sigue

$$\mu_v(aA) = \|a^{-1}\|_v \mu_v(A)$$

con lo cual la fórmula queda probada para todo $a \in K_v^*$.

Ahora consideramos el grupo multiplicativo K_v^*, y definimos una medida λ_v sobre K_v^* como

$$\lambda_v(A) = \int_A \frac{d\mu_v(x)}{\|x\|_v}$$

Es fácil ves que la medida λ así definida es una medida de Haar sobre K_v^*, ya que

$$\lambda_v(A^{-1}) = \int_{A^{-1}} \frac{d\mu_v(x)}{\|x\|_v} = \int_A \|x\|_v \frac{d\mu_v(x)}{\|x\|_v^2} = \lambda_v(A)$$

$$\lambda_v(aA) = \int_A \frac{d\mu_v(x)}{\|x\|} = \frac{1}{\|a\|_v} \int_A \frac{d\mu_v(x)}{\|a^{-1}x\|_v} = \lambda_v(A)$$

Tomamos en definitiva

$$\mu_v^* = \lambda_v$$

si v es arquimediano, y

$$\mu_v^* = \frac{N\mathrm{p}}{N\mathrm{p} - 1} \lambda_v$$

si v es p-ádico. Tenemos entonces

$$\mu_v^*(\mathrm{A}_v) = (N\mathcal{D})^{-1/2}$$

Ahora vamos a considerar la medida de Haar sobre un producto directo restringido. Sea como antes, M un conjunto de índices, G_v un grupo conmutativo localmente compacto, y H_v un subgrupo de G_v abierto-compacto para casi todo v. Sea h_v una medida de Haar sobre G_v , tal que

$$h_v(H_v) = 1$$

para casi todo v. Entonces se define la medida de Haar h sobre una base de la topología de G como

$$h(\prod_{v \in S} A_v \times \prod_{v \notin S} H_v) = \prod_{v \in S} h_v(A_v) \times \prod_{v \notin S} h_v(H_v)$$

donde los A_v son abiertos medibles de G_v.

Sea G un grupo, y H un subgrupo de G. Se llama **clases a izquierda** al conjunto $G/H = \{xH : x \in G\}$. Análogamente, las **clases a derecha** son los elementos Hx, con $x \in G$. Todas las nociones referidas a G/H se transladan a $H\backslash G$.

Si H es un subgrupo normal, ambas nociones coinciden, y G/H tiene una estructura de grupo, con la operación

$$xH \cdot yH = xyH$$

Un R un subconjunto de G que contiene a un único elemento de cada una de las clases a izquierda se llama un **sistema de representantes** para G/H.

Sea ahora G un grupo localmente compacto, con una medida de Haar invariante a izquierda. Un sistema de representantes F de las clases a izquierda se dice un **dominio fundamental** si es un conjunto medible de Borel con interior no vacío.

Enunciamos el siguiente teorema sin dar su demostración.

Teorema 2[3]**.** *El grupo cociente A_K/K es compacto. Sea $w_1, \ldots, w_n$ una base de los enteros A_K sobre Z, y sea F_∞ el subconjunto de*

$$K_\infty = \prod_{v \in S_\infty} K_v$$

con $F_\infty = \{\sum_{i=1}^{r_1+r_2} t_i w_i : 0 \leq t_i < 1\}$. Luego

$$F = F_\infty \times \prod_{v \notin M_K} A_v$$

es un dominio fundamental de A_K/K.

Proposición 2. *F tiene medida 1.*

Dem. Sea μ_∞ la medida producto en K_∞, y σ la inclusión canónica de K en K_∞. Luego

$$\begin{aligned} \mu_\infty(F_\infty) &= 2^{r_2} |\det(\sigma w_i)| \\ &= |\det(\sigma_i w_j)| = |D_K|^{1/2} \end{aligned}$$

Luego

$$\mu(F) = |D_K|^{1/2} \prod_{v \notin S_\infty} (N\mathcal{D})^{-1/2} = 1$$

[3][La] p. 140

Ahora definimos

$$\|a\| = \prod_{v \in M_K} \|a\|_v$$

Como casi todos los factores del producto son iguales a 1, el producto está bien definido.

El grupo de los ideles actúa continuamente sobre los adeles, si definimos la multiplicación componente a componente. Sea

$$W = \prod_{v \in S} W_v \times \prod_{v \notin S} \mathrm{A}_v$$

donde S es un conjunto finito de índices que contiene a S_∞, y W_v es un conjunto medible de K_v. Tenemos entonces

$$\mu(aW) = \prod_{v \in S} \mu_v(a_v W_v) \times \prod_{v \notin S} \mu_v(a_v \mathrm{A}_v) = \|a\| \mu(W)$$

por las fórmulas de la proposición 1.

La aplicación

$$\begin{array}{rl} \| \ \| : & J \to R_+^* \\ & a \mapsto \|a\| \end{array}$$

define un homomorfismo continuo. Denotamos por J^0 al núcleo, que es un subgrupo cerrado de J.

$$J^0 = \{x \in J : \|x\| = 1\}$$

Por la fórmula del producto, K^* está contenido en J^0, y es un subgrupo discreto.

Dado un idele $a = (a_v)_v$ y un ideal primo p, definimos

$$\mathrm{ord}_{\mathrm{p}} a = \mathrm{ord}_{\mathrm{p}} a_v$$

Luego $\mathrm{ord}_{\mathrm{p}} a = 1$ para casi todo p, y por lo tanto

$$\prod_{\mathrm{p}} \mathrm{p}^{\mathrm{ord}_{\mathrm{p}} a}$$

es un ideal fraccionario, y tenemos entonces un homorfismo natural de J_K sobre I_K, el grupo de los ideales fraccionarios de A_K, definido por la aplicación

$$a \mapsto (a) = \prod_{\mathrm{p}} \mathrm{p}^{\mathrm{ord}_{\mathrm{p}} a_v}$$

El grupo I_K/P_K de clases de ideales es un grupo finito de orden h. Sean $b^{(1)}, \ldots, b^{(h)}$ un sistema de representantes de I_K/P_K. La restricción a J_K^0 del homomorfismo $a \mapsto (a)$ es suryectiva, y por lo tanto existen elementos $b^{(1)}, \ldots, b^{(h)}$ tales que $b^{(i)} = (b^{(i)})$. Sea entonces H_K el subgrupo de J_K^0 generado por K^* y por los $b^{(i)}$. Tenemos que H_K es un subgrupo discreto de J_K^0, y la aplicación $a \mapsto (a)$ de H_K en I_K es suryectiva.

La aplicación canónica

$$\begin{array}{rl} \varphi: & J \to J^0 \\ & a \mapsto a/\|a\| \end{array}$$

induce un isomorfismo algebraico y topológico entre J^0 y J/R_+^*, es decir que el producto directo restringido

$$(\prod_{v \in S_\infty} K_v^*)/R_+^* \times \overline{\prod}_{v \notin S_\infty} K_v^*/U_v$$

es isomorfo a J^0, y le asocia unívocamente a J^0 una medida de Haar μ^0. Ahora enunciamos para J^0 el resultado análogo al teorema 2.

Teorema 3[4]**.** *El grupo cociente J^0/H_K es compacto, y admite un dominio fundamental de la forma*

$$E_\infty \times \prod_{v \notin S_\infty} U_v$$

donde E_∞ es un conjunto de Borel de $(\prod_{v \in S_\infty} K_v^*)/R_+^*$.

[4][La] p 142,145

5 Funciones L de Hecke

Las funciones L ocupan un lugar preponderante dentro del estudio de los cuerpos numéricos. Estas funciones están directamente relacionadas con los ideales primos y con ciertas constantes intrínsecas del cuerpo, en particular con el número de clases de ideales. El estudio de estas funciones es entonces de mucha importancia, y aportan resultados acerca de los cuerpos de números que no son accesibles de otra forma.

En §1 se definen las funciones L asociadas a un caracter de Hecke, y mencionamos los aspectos analíticos básicos.

En §2 se exponen las fórmulas explícitas de Weil, de las que se desprende una hipótesis que es equivalente a la hipótesis de Riemann.

5.1 Caracteres de Hecke, series L

Sea G un grupo localmente compacto. Un **quasi-caracter** χ de G es un homomorfismo continuo

$$\chi : G \to C^*$$

Un **caracter de Hecke** es un quasi-caracter χ de las clases de ideles $C_K = J_K/K^*$.

Sea p un ideal primo de A_K, y consideramos al cuerpo local K_p con la inclusión canónica en J_K como

$$x \mapsto (\ldots, 1, x, 1, \ldots)$$

Se dice que χ es **no ramificado** sobre p si $\chi(U_\mathrm{p}) = 1$, donde U_p es el grupo de las unidades locales. Si p es no ramificado para χ, y π es un elemento primo de A_p, definimos

$$\chi(\mathrm{p}) = \chi(\pi)$$

Esta definición es independiente de la elección de π, ya que si π_1 es otro elemento primo de A_p, entonces $\pi_1 = u\pi$, con $u \in U_\mathrm{p}$, y $\chi(u) = 1$.

Si χ es ramificado sobre p, definimos $\chi(\mathrm{p}) = 0$, y por multiplicación extendemos esta definición al grupo I_K de los ideales no nulos.

Se define entonces las **funciones L de Hecke** como

$$L(s,\chi) = \prod_{\text{p no ram.}} (1 - \frac{\chi(\mathrm{p})}{N\mathrm{p}^s})^{-1}$$

Este producto converge absoluta y uniformemente para $\mathrm{Re}(s) \geq 1 + \delta$, y define entonces una función holomorfa en $\mathrm{Re}(s) > 1$.

Tenemos también la representación de L en serie de Dirchlet como

$$L(s,\chi) = \sum_{\mathrm{a}} \frac{\chi(\mathrm{a})}{N\mathrm{a}^s} \quad \sigma > 1$$

donde la suma se extiende a todos los ideales enteros $\neq 0$ de $\mathrm{A_p}$.

Esta función tiene una prolongación analítica a todo el plano complejo, con posibles polos simples en $s = 0$ y en $s = 1$. Más aún, satisface una ecuación funcional.

Sea $\chi = 1$ el caracter de Hecke trivial. La función L asociada a este caracter es

$$\zeta_K(s) = \prod_{\mathrm{p}} (1 - \frac{1}{N\mathrm{p}^s})^{-1}$$

y se llama a ζ_K la **función zeta** del cuerpo K. Hacemos

$$\Lambda(s) = (2^{-r_2} d_K^{1/2} \pi^{-n/2})^s \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} \zeta_K(s)$$

donde $n = [K : Q]$ y d_K es el valor absoluto del discriminante de K. Tenemos entonces la **ecuación funcional** para la función ζ_K, dada por

$$\Lambda(s) = \Lambda(1 - s)$$

Cuando χ es un caracter de Hecke no trivial, existe también una ecuación funcional análoga para la función $L(s,\chi)$, pero en este caso los factores asociados son un poco más difíciles de calcular[5].

5.2 La fórmula explícita

Sea una función $F : R \to C$ tal que

$$F(x)e^{(\frac{1}{2}+a)|x|} \in L^1$$

[5] [La] p. 300

para algún $a > 0$. Definimos entonces la **transformada de Mellin** de F como

$$\Phi(s) = \Phi_F(s) = \int_R F(x) e^{(s-\frac{1}{2})x} dx$$

que es holomorfa en la banda $-a < \mathrm{Re}(s) < 1 + a$. De acuerdo al uso corriente, $\Phi(s)$ es en realidad la transformada de Mellin de $x^{1/2}F(\log x)$. Asumimos las siguientes condiciones sobre F:

1. F es continua y con derivada continua, salvo en un conjunto finito de α_i, en donde tanto F como F' tienen una discontinuidad de salto, y es tal que
$$F(\alpha_i) = \frac{1}{2}\{F(\alpha_i^+) + F(\alpha_i^-)\}$$

2. Existe un $b > 0$ tal que $F(x)$ y $F'(x)$ son $O(e^{-(\frac{1}{2}+b)|x|})$, para $x \to \infty$.

Este es nuestro conjunto de funciones admisibles, que denotamos por $\mathrm{Ad}(R)$.

Sea $f : R \to C$ una función tal que $f \in L^1$ sobre $(-\infty, -1)$ y sobre $(1, \infty)$, y tal que $g(x) = |x|f(x)$ satisface la condición 1. Definimos entonces

$$\mathrm{P}f = \lim_{\lambda \to \infty} \{\int_R (1 - e^{-\lambda|x|}) f(x) dx - 2g(0) \log \lambda\}$$

que es una distribución, en el sentido de Schwartz. Sea v un valor absoluto arquimediano. Ponemos entonces

$$\Theta_v(F) = \mathrm{P}(F(x) K_{n_v, m_v}(x))$$

donde

$$K_{1,m}(x) = \frac{e^{(1/2-m)|x|}}{|e^x - e^{-x}|}, \quad K_{2,m}(x) = \frac{e^{-m|x|/2}}{|e^{x/2} - e^{-x/2}|}$$

y los m_v son enteros que dependen de v y del caracter χ.

Sea δ_χ definida como 1 si $\chi = 1$, y 0 en otro caso.

Enunciamos entonces la fórmula explícita, que relaciona ciertas sumas de la función F sobre los ideales primos de A_K con sumas de la transformada de Mellin Φ_F sobre los ceros de $L(s, \chi)$.

Teorema[6] *Sea $F \in Ad(x)$ y Φ su transformada de Mellin. La suma $\sum_\rho \Phi(\rho)$ sobre los ceros $\rho = \alpha + i\beta$ de $L(s, \chi)$ tales que $0 \le \alpha \le 1$ y $|\beta| < T$*

[6] [We]

converge cuando $T \to \infty$*, y tenemos que*

$$\begin{aligned}\textstyle\sum_{\rho:|\beta|<T} \Phi(\rho) &= \delta_\chi \textstyle\int_R F(x)(e^{\frac{x}{2}} + e^{-\frac{x}{2}})dx + F(0)\log A \\ &\quad - \textstyle\sum_{p,n} \frac{\log Np}{Np^{n/2}}[\chi(p)^{-n}F(\log Np^{-n}) + \chi(p)^n F(\log Np^n)] \\ &\quad - \textstyle\sum_{v\in S_\infty} \Theta_v(F_v) + O(1/T)\end{aligned}$$

donde $F_v = F(x)e^{-i\varphi x}$*, y* φ_v *y* A *son constantes que dependen del cuerpo* K *y de* χ*.*

Sea $F_t(x) = F(t+x)$ para $x \in R$. Es claro entonces que $F_t \in \mathrm{Ad}(R)$ y

$$\Phi_{F_t}(s) = \int_R F(x+t)e^{(s-\frac{1}{2})x}dx = e^{(\frac{1}{2}-s)t}\Phi_F(s)$$

Tenemos que

$$\Theta F_t = O(e^{mt})$$

Se sigue entonces

Corolario. *Con la misma notación,*

$$\begin{aligned}\textstyle\sum_{\rho:|\beta|<T} e^{(\rho-\frac{1}{2})t}\Phi(\rho) &= \delta_\chi \textstyle\int_R F(x)(e^{\frac{x-t}{2}} + e^{\frac{t-x}{2}})dx + F(t)\log A \\ &\quad - \textstyle\sum_{p,n} \frac{\log Np}{Np^{\frac{n}{2}}}[\chi(p)^{-n}F(t+\log Np^{-n}) + \chi(p)^n F(t+\log Np^n)] \\ &\quad + \textstyle\sum_{v\in S_\infty} \Theta_v(F_{t,v}) + O(1/T)\end{aligned}$$

Sean $f, g \in \mathrm{Ad}(R)$. Definimos la **convolución** de f con g como

$$f * g(x) = \int_R f(x-t)g(t)dt$$

Luego $f * g \in \mathrm{Ad}(R)$, y tenemos la conocida relación

$$\Phi_{f*g} = \Phi_f \cdot \Phi_g$$

La **hipótesis de Riemann** dice que dado un caracter de Hecke χ, los ceros de la función $L(s,\chi)$ con parte real > 0 están sobre la recta $\mathrm{Re}(s) = 1/2$. Es un problema abierto hasta el momento, y no está demostrada ni si quiera para una función L particular.

Hay una reformulación de la hipótesis de Riemann debida a Weil ([We]).

Proposición. *La función $L(s,\chi)$ satisface la hipótesis de Riemann si y sólo si la expresión del Teorema es ≥ 0 para toda función f de la forma*

$$f(x) = f_0(x) * \overline{f_0(-x)} = \int_R f_0(x+t)\overline{f_0(x)}dt$$

con $f_0 \in Ad(R)$.

6 Producto Semidirecto

A partir de un grupo S y un grupo R de automorfismos de G se define un grupo que llamamos el producto semidirecto de R con S.

En esta sección estudiamos la estructura general de este grupo, y aplicamos estos resultados al grupo de los adeles del cuerpo K, y al de los ideles de norma 1. Este es el grupo que voy a usar en mis consideraciones posteriores.

6.1 Definición y aspectos básicos

Sean S un grupo aditivo, y R un grupo multiplicativo que actúa a derecha sobre S, es decir

$$\begin{aligned} (x+y)\alpha &= x\alpha + y\alpha \\ x(\alpha\beta) &= (x\alpha)\beta \\ xe_R &= x \end{aligned}$$

donde $x = (x_1, x_2), y = (y_1, y_2) \in S$, $\alpha, \beta \in R$, y e_R es el elemento neutro de R. Se define en $R \times S$ la ley

$$xy = (x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_1 + y_2)$$

Tenemos que

$$\begin{aligned} (xy)z &= ((x_1y_1)z_1, (x_2y_1 + y_2)z_1 + z_2) \\ &= (x_1(y_1z_1), x_2(y_1z_1) + (y_2z_1 + z_2)) = x(yz) \\ (x_1, x_2)(e_R, e_S) &= (e_R, e_S)(x_1, x_2) = (x_1, x_2) \\ (x_1, x_2)(x_1^{-1}, -x_2x_1^{-1}) &= (x_1^{-1}, -x_2x_1 - 1) = (e_R, e_S) \end{aligned}$$

y se sigue entonces que $R \times S$ con esta ley es un grupo (no conmutativo), que se denota RS (**producto semidirecto**).

Consideremos a R y a S con una topología compatible, es decir, que R y S sean grupos topológicos tales que la función

$$\begin{aligned} \varphi: \quad & RS \to S \\ & (\alpha, x) \mapsto x\alpha \end{aligned}$$

es continua. Luego

$$\begin{aligned} \psi: \quad & (RS) \times (RS) \to RS \\ & (x, y) \mapsto xy^{-1} = (x_1 y_1^{-1}, (x_2 - y_2) y_1^{-1} \end{aligned}$$

es una aplicación continua, y por lo tanto RS es un grupo topológico, con la topología producto. En particular, si R y S son grupos localmente compactos, entonces RS también lo es.

Ahora necesitamos algunos resultados de teoría de la medida. Sean X, Y conjuntos, y A, B σ-anillos de conjuntos de X e Y respectivamente. Se define el σ-anillo A $\times$ B de conjuntos de $X \times Y$ como el σ-anillo generado por los conjuntos de la forma $A \times B$, con $A \in$ A, $B \in B$[7].

Sea $E \in X \times Y$. Una X-**sección** de E es un conjunto de la forma $E_x = \{y : (x, y) \in E\}$, para un elemento $x \in X$. Análogamente, una Y-**sección** es un conjunto $E^y = \{x : (x, y) \in E\}$ para un elemento $y \in Y$[8].

Teorema.[9] *Sean (X, A, λ), (Y, B, μ) espacios de medida σ-finita, y E un conjunto medible de $X \times Y$. Entonces*

1. *Dados $x \in X$, $y \in Y$, E_x, E_y son conjuntos medibles de Y y de X respectivamente.*

2. *Las funciones*

$$\begin{aligned} x &\mapsto \mu(E_x) \\ y &\mapsto \lambda(E^y) \end{aligned}$$

   son funciones medibles no negativas.

3. $$\int \mu(E_x) d\lambda(x) = \int \lambda(E^y) d\mu(y)$$

[7] [Ha] p. 140
[8] [Ha] p.141
[9] [Ha] p. 144

4. La aplicación

$$\lambda \times \mu : \quad A \times B \to R_+ \\ E \mapsto \int \mu(E_x) d\lambda(x) = \int \lambda(E^y) d\mu(y)$$

es una medida σ-finita, y si $A \in A$, $B \in B$,

$$\lambda \times \mu(A \times B) = \lambda(A)\mu(B)$$

Esta medida se llama la medida **producto** de λ y μ.

Lema 1.[10] *Sean X, Y espacios de Hausdorff localmente compactos, y sean A_0, B_0 y S_0 los σ-anillos de conjuntos de Baire*[11] *en X, Y y $X \times Y$ respectivamente. Luego $S_0 = A_0 \times B_0$.*

Lema 2.[12] *Sea X un espacio de Hausdorff separable y localmente compacto. Luego el σ-anillo de Borel de X coincide con el σ-anillo de Baire de X.*

Desde ahora suponemos que R y S son grupos separables y localmente compactos.

Proposición 1. *Sean λ, μ medidas de Haar sobre R y S respectivamente, invariantes a izquierda (resp. a derecha), σ-finitas, completas, y tales que*

$$\mu(A\alpha) = \mu(A)$$

para $\alpha \in R$ y $A \subset S$ conjunto medible. Entonces la medida producto $\lambda \times \mu$ es una medida de Haar sobre RS invariante a izquierda (resp. a derecha).

En particular, si R y S son grupos unimodulares, entonces RS es unimodular.

Dem. De los lemas 1 y 2 se sigue que la medida producto $\lambda \times \mu$ es una medida de Borel.

Sean λ y μ medidas invariantes a izquierda. Luego

$$\begin{aligned} \lambda \times \mu(aA) &= \int \mu(aA_x) d\lambda = \int \mu(\{y : (a_1^{-1}x, y - a_2 a_1^{-1}x) \in A\} d\lambda = \\ &= \int \mu(\{y + a_2 a_1^{-1}x : (a_1^{-1}x, y) \in A\} d\lambda = \\ &= \int \mu(\{y : (a_1^{-1}x, y) \in A\} d\lambda == \lambda \times \mu(\{(a_1 x, y) : (x, y) \in A\} = \\ &= \lambda \times \mu(A) \end{aligned}$$

[10] [Ha] p. 222
[11] [Ha] p. 220
[12] [Ha] p. 218

es decir, que $\lambda \times \mu$ es invariante a izquierda. Ahora supongamos que λ y μ son invariantes a derecha. Luego

$$\begin{aligned}
\lambda \times \mu(Aa) &= \int \mu(Aa_x)d\lambda = \int \mu(\{y : (xa_1^{-1}, (y-a_2)a_1^{-1}) \in A\}d\lambda = \\
&= \int \mu(\{ya_1 + a_2 : (xa_1^{-1}, y) \in A\}d\lambda = \\
&= \int \mu(\{y : (xa_1^{-1}, y) \in A\}d\lambda = \lambda \times \mu(\{(xa_1, y) : (x, y) \in A\} = \\
&= \lambda \times \mu(A)
\end{aligned}$$

y por lo tanto, $\lambda \times \mu$ es una medida de Haar sobre RS invariante a derecha.

6.2 Dominio fundamental de RS

Sea G un grupo topológico, H un subgrupo cerrado de G. Las clases a izquierda

$$G/H = \{xH : x \in G\}$$

es entonces un espacio topológico, con la topología cociente, i.e. sea

$$\begin{array}{rl} \varphi : & G \to G/H \\ & x \mapsto xH \end{array}$$

la aplicación canónica. Luego decimos que $A \subset G/H$ es un abierto si y sólo si $\varphi^{-1}(A)$ es un abierto de G.

De la misma manera, $H\backslash G$ es también un espacio topológico. En realidad, $H\backslash G$ es isomorfo a G/H, mediante la aplicación

$$\begin{array}{rl} \psi : & G/H \to H\backslash G \\ & xH \mapsto Hx^{-1} \end{array}$$

Sea G un grupo topológico, H un subgrupo cerrado de G. Sea $a \in G$. Hacemos

$$\begin{array}{rl} \varphi_a : & G/H \to G/H \\ & \bar{x} \mapsto \overline{ax} \end{array}$$

Si $y \in \bar{x}$, i.e. $y = xh$, con $h \in H$, entonces $ay = (ax)h \in \bar{x}$ y por lo tanto φ_a está bien definida. φ_a es claramente continua, y tenemos además

$$\varphi_{a^{-1}} \circ \varphi_a = \mathrm{id}_{G/H}$$

y por lo tanto φ_a es bicontinua, es decir, es un isomorfismo topológico de G/H sobre sí mismo. Resulta de aquí que la topología de G/H está determinada por una base local de entornos en un punto.

Lema. *Sea G un grupo topológico y H un subgrupo discreto de G. Entonces H es cerrado.*

Dem. Sea U un abierto de G tal que $U \bigcap H = \{e\}$. La aplicación

$$\begin{array}{rl} \phi: & G \times G \to G \\ & (xy^{-1}) \mapsto xy^{-1} \end{array}$$

es continua, y por lo tanto, $\phi^{-1}(U)$ es un abierto de $G \times G$. Luego existe un entorno abierto V de e tal que

$$\phi(V \times V) = VV^{-1} \subset U$$

Sea ahora $x \in G - H$. Tenemos entonces que

$$(Vx)(Vx)^{-1} \bigcap U = \{e\}$$

y por lo tanto, $Vx \bigcap H$ contiene a lo sumo un elemento $q \in H$. Luego $Vx - \{q\}$ es un entorno de x contenido en $G - H$, de donde se sigue que H es cerrado.

Sea H un subgrupo discreto de G. Recordemos que un dominio fundamental para G/H es un sistema de representantes F de las clases a izquierda que es un conjunto de Borel de G con interior no vacío. Es claro que F^{-1} es un dominio fundamental para $H\backslash G$.

Sea una medida h sobre G invariante a izquierda. Luego la restricción de esta medida al dominio fundamental F nos induce una medida $\hbar$ sobre G/H que es invariante por la acción a izquierda de G sobre G/H.

Si F es un dominio fundamental para G/H, en particular F es un entorno de un punto $x_0 \in G$. Es fácil entonces, ver que la biyección canónica

$$\begin{array}{rl} \varphi: & F \to G/H \\ & x \mapsto xH \end{array}$$

es un homeomorfismo local en x_0. Sea $A \in F$ un abierto de G. Luego $\varphi^{-1}(\varphi(A)) = AH$ es un abierto de G, y por lo tanto $\varphi(A)$ es un abierto de G/H. Sea ahora $B \in A \in F$ un conjunto tal que $\varphi(B)$ es un abierto de G/H. Luego $\varphi^{-1}\varphi(B) = BH$ es un abierto de G, y por lo tanto $B = A \bigcap \varphi^{-1}\varphi(B)$ es un abierto, c.q.d..

Se sigue entonces que toda base local en G/H en un punto es isomorfa a una base local en G en un punto.

Teorema 1. *Sean r,s subgrupos discretos de R y S respectivamente, tales que existen dominios fundamentales E,F para R/r y para S/s respectivamente.*

Entonces rs es un subgrupo discreto de RS,

$$rs \setminus RS \simeq RS/rs \simeq R/r \times S/s,$$

y $E \times F$ es un dominio fundamental para RS/rs.

Dem. Consideremos la aplicación

$$\begin{aligned} \Phi : \quad & E \times F \to RS/rs \\ & (x, y) \mapsto (x, y)rs \end{aligned}$$

Φ *es inyectiva* : Sean $x, y \in E \times F$, y elementos $q, q' \in rs$ tales que

$$xq = yq'$$

i.e.

$$(x_1q_1, x_2q_1 + q_2) = (y_1q_1', y_2q_1' + q_2')$$

Luego $x_1 = y_1$, $q_1 = q_1'$, y de

$$x_2 + q_1q_2^{-1} = y_2 + q_1^{-1}q_2'$$

seguimos que $x_2 = y_2$.

Φ *es suryectiva* : sea $\bar{x} \in RS/rs$

$$\text{i.e.} \quad \bar{x} = \{(x_1q_1, x_2q_2 + q_1) : q_1 \in r,\ q_2 \in s\}$$

Luego existe un elemento $q_1 \in r$ tal que $x_1q_1 \in E$, y existe también un elemento $q_2 \in s$ tal que $x_2q_1 + q_2 \in F$.

Tenemos entonces que Φ es una biyección, y por lo tanto $E \times F$ es un dominio fundamental para RS/rs.

Dadas dos bases locales $\mathcal{E}, \mathcal{F}$ contenidas en E y F respectivamente, son isomorfas a dos bases locales en R y en S respectivamente, y al mismo tiempo, $\mathcal{E} \times \mathcal{F}$ es isomorfa a una base local en $RS/r \times s$. Se sigue entonces que

$$rs \setminus RS \simeq RS/rs \simeq R/r \times S/s$$

como espacios topológicos.

Sea K un cuerpo de números, A_K los adeles sobre K, y J_K^0 los ideles sobre K de norma 1. Reuniendo los resultados de §2. y de §3., tenemos la siguiente proposición.

Proposición 2. *Sea K un cuerpo de números. Luego $J_K^0 A_K$ es un grupo localmente compacto y unimodular. La medida de Haar está dada por la medida producto.*

$H_K K$ es un subgrupo discreto de $J_K^0 A_K$, y el cociente $J_K^0 A_K / H_K K$ es un espacio topológico compacto. Tenemos que

$$H_K K \setminus J_K^0 A_K \simeq J_K^0 A_K / H_K K \backslash J_K^0 / H_K \times A_K / K$$

y si E_K, F_K son dominios fundamentales para J_K^0 / H_K y para A_K / K respectivamente, entonces $E_K \times F_K$ es un dominio fundamental para $J_K^0 A_K / H_K K$.

7 Operadores sobre $\mathcal{L}^2(\mathbf{M})$

7.1 Operadores de tipo traza

Sean X e Y espacios de Banach complejos. Denotamos por $B(X, Y)$ al espacio de las funciones lineales $A : X \to Y$ continuas. Para $A \in B(X, Y)$ se define la norma de A como

$$\|A\| = \sup\{\|Ax\| / \|x\| : x \neq 0\}$$

Esta aplicación está bien definida, y es fácil ver que es una norma en el sentido usual, y $(B(X, Y), \| \ \|)$ resulta ser un espacio de Banach[13].

Sea $A \in B(X, Y)$ y $U = \{x \in X : \|x\| < 1\}$ la bola unidad en X. Entonces A es un operador **compacto** si la clausura de $A(U)$ es compacta. El conjunto de los operadores compactos de X en Y se denota por $B_0(X, Y)$, y es un subespacio cerrado de $B(X, Y)$[14].

[13] [Co] p. 70
[14] [Co] p.178

Sea $A \in B(X)$ un operador continuo . Se dice que A es **invertible** si existe un operador $B \in B(X)$ tal que

$$AB = BA = \mathrm{id}_X$$

Este operador se denota por A^{-1}.

Se define el **espectro** $\sigma(A)$ como el conjunto de los $\lambda \in C$ tales que $A - \lambda I$ es **no** invertible.

Teorema 1[15]**.**(F. Riesz) *Sea X un espacio de Banach y $A \in B_0(X)$. Entonces ocurre alguna de las siguientes posibilidades:*

1. $\sigma(A) = \{0\}$.
2. $\sigma(A) = \{0, \lambda_1, \ldots, \lambda_n\}$, *donde* $\lambda_k \neq 0$ *para* $1 \leq k \leq n$, λ_k *es un autovalor de* A, *y* $dim(ker(A - \lambda I)) < \infty$.
3. $\sigma(A) = \{0, \lambda_1, \lambda_2, \ldots\}$, *donde para* $k \geq 1$ $\lambda_k \neq 0$, λ_k *es un autovalor de* A, $dim(ker(A - \lambda I))$, *y* $\lim \lambda_k = 0$.

Ahora sea H un espacio de Hilbert complejo.

Teorema 2[16]**.** *Sea $A \in B(H)$. Luego existe un único operador lineal $B \in B(H)$ tal que*

$$\langle Ax, y\rangle = \langle x, By\rangle$$

para todo $x, y \in H$. Más aún, $\|B\| = \|A\|$.

Este único operador asociado a A se llama el operador **adjunto** de A, y se denota A^*.

Un operador $A \in B(H)$ se dice **normal** si $AA^* = A^*A$. Un operador $A \in B(H)$ se dice **autoadjunto** si $A = A^*$.

Proposición 1[17]**.** *Sea $A \in B(H)$ un operador autoadjunto. Entonces $\sigma(A) \subset R$.*

Sea $\{e_i\}_{i \in I}$ una base ortonormal de H, y $A \in L(H)$. Tenemos entonces que la suma

$$\sum_{i \in I} \|Ae_i\|^2$$

[15][Co] p. 219
[16][Co] p. 31
[17][Du] p. 906

es independiente de la base elegida[18]. Si esta suma es finita, decimos que A es un operador de **Hilbert-Schmidt**. Denotamos por $B_2(H)$ al conjunto de los operadores de Hilbert-Schmidt.

Proposición 2[19]**.** *Todo operador de Hilbert-Schmidt es compacto.*

Proposición 3[20]**.** it Sean $A, B \in B_2(H)$, y sea $\{e_i\}_{i\in I}$ una base ortonormal de H. Luego la serie

$$\langle Ae_i, B^*e_i\rangle = \sum_{i\in I}\langle Ae_i, B^*e_i\rangle$$

converge absolutamente a un límite que es indendiente de la elección de la base.

Dados B, $C \in B_2(H)$, el operador $A = BC$ se llama operador **traza**. La clase de los operadores traza se denota por $B_1(H)$. Se tiene $B_1(H) \subset B_2(H)$.

Proposición 4[21]**.** *Sea $A \in B_1(H)$. Luego la suma*

$$\sum_{i\in I}\langle Ae_i, e_i\rangle$$

converge absolutamente, y si $B, C \in B_2(H)$ son tales que $A = BC$, entonces

$$\sum\langle Ae_i, e_i\rangle = \langle B, C\rangle$$

Se define entonces

$$\mathrm{tr}(A) = \sum\langle Ae_i, e_i\rangle$$

Teorema 3[22]**.** *Sea $A \in B_1(H)$, y sean λ_n los autovalores de A (con su multiplicidad). Entonces*

$$tr(A) = \sum_{n=1}^{\infty}\lambda_n$$

Sea $H = \mathcal{L}^2(X, \mu)$, donde X es un operador compacto y μ es una medida positiva sobre X. Sea $A \in B_1(H)$. A puede escribirse como $A = BC$, con $B, C \in B_2(H)$. Luego B y C son operadores integrales[23], con funciones

[18] [Du] p 1010
[19] [Du] p. 1012
[20] [Du] p. 1025
[21] [Du] p. 1025
[22] [Si] p. 50
[23] [Du] p. 1009

núcleo $b(x,y)$ y $c(x,y)$ respectivamente. Se sigue que A es un operador integral con núcleo

$$a(x,y) = \int_W b(x,t)c(t,y)$$

Luego tenemos la fórmula de traza[24]

$$\text{tr } A = \langle B, C^* \rangle = \int_{W\times W} b(x,t)c(t,x)dtdx = \int_W a(x,x)dx$$

Nota: Los operadores que vamos a estudiar están dados por núcleos continuos sobre un espacio de medida finita. Tenemos entonces que son operadores de Hilbert-Schmidt, pero no sabemos si son operadores de tipo traza.

En nuestro caso particular, por la analogía con el lema anterior, vamos a definir la traza de estos operadores como la integral sobre la diagonal del núcleo continuo que lo representa. De esta forma la traza queda bien definida, pero podríamos no tener las propiedades de los operadores traza, en particular el teorema 3.

7.2 Operadores integrales sobre $\mathcal{L}^2(\mathrm{M})$

Sea $\mathrm{M} = \mathrm{M}_K = J_K^0 A_K / H_K K$, que por lo que vimos en §4.1 es un espacio compacto. Ahora centraremos nuestra atención en $\mathcal{L}^2(M)$, el espacio de Hilbert de las funciones

$$f : \mathrm{M} \to C$$

de cuadrado integrable, con el producto interno definido como

$$\langle f, g \rangle = \int_{\mathrm{M}} f\bar{g}dx$$

Sea $K \in \mathcal{L}^2(\mathrm{M}\times\mathrm{M})$. La función

$$\begin{aligned} K_y : \quad & \mathrm{M} \to C \\ & x \mapsto K(x,y) \end{aligned}$$

está en $\mathcal{L}^2(\mathrm{M})$ para casi todo y, y podemos definir entonces

$$K_f(y) = \int_{\mathrm{M}} K(x,y)f(x)dx$$

[24][Ka] p. 522

para $f \in \mathcal{L}^2(\mathrm{M})$, que define un operador lineal $f \mapsto K_f$. Por la desigualdad de Cauchy, tenemos que

$$|K_f(y)|^2 = \int_{\mathrm{M}} |K(x,y)f(x)dx|^2 \leq \|f\|_2^2 \int_{\mathrm{M}} |K(x,y)|^2 dx$$

y se sigue entonces que $K \in B(\mathcal{L}^2(\mathrm{M}))$, y $\|K\| \leq \|K\|_2$

Sea $\{e_i\}_{i\in I}$ una base ortonormal de $\mathcal{L}^2(\mathrm{M})$. Luego $\{\bar{e}_i e_j\}$ es una base ortonormal de $\mathcal{L}^2(\mathrm{M}\times\mathrm{M})$, y por lo tanto existen elementos $a_{i,j} \in C$ tales que

$$K(x,y) = \sum_{i,j\in I} a_{i,j}\bar{e}_i(x)e_j(y)$$

con

$$\|K\| = (\sum_{i,j} |a_{i,j}|^2) < \infty$$

Sea K el operador integral inducido por K. Luego tenemos

$$\sum_{i\in I} \|Ke_i\|^2 = \sum_{i\in I} \|\sum_{j\in I} a_{i,j}e_j(y)\|_2^2 = \sum_{i,j\in I} |a_{i,j}|^2 < \infty$$

y K es entonces un operador de Hilbert-Schmidt.

Podemos pensar al grupo de adeles A_K como el producto directo restringido de R^n y los K_v, donde V recorre las valuaciones p-ádicas. Consideramos entonces $L \subset \mathcal{L}^2(\mathrm{M})$ el subespacio de las funciones

$$f : \mathrm{M} \to C$$

continuas y C^∞ con respecto a las variables reales de los adeles. Tenemos entonces que hay un conjunto medible $\mathcal{M}$ de R^N, y un conjunto medible $\mathcal{N}$ de $J_K^0(A_K/R^N)$ tales que $\mathcal{M}\times\mathcal{N}$ es un dominio fundamental para M. Tenemos que el espacio de las funciones C^∞ sobre M (con la topología cociente) es denso en $\mathcal{L}^2(\mathcal{M})$, y el espacio de las funciones continuas en $\mathcal{N}$ (con la topología cociente) es denso en $\mathcal{L}^2(\mathcal{N})$. Se sigue que L es un subespacio denso de $\mathcal{L}^2(\mathrm{M})$.

Sea $K : J_K^0 A_K \to C$ una función continua y C^∞ con respecto a las variables reales $x_{2,1}, \ldots, x_{2,n}$ de A_K. Supongamos que

$$\sum_{q\in H_K K} \frac{\partial^m}{\partial x_{2,i}^m} K(xqy^{-1})$$

converge uniformemente para $i = 1, \ldots, n,\ m = 0, 1, 2, \ldots$. Definimos entonces

$$K(x, y) = \sum_q K(xqy^{-1})$$

que es una función continua. Es claro que para $q_1, q_2 \in H_K K,\ K(xq_1, yq_2) = K(x, y)$, y el pasaje al cociente está entonces bien definido.

Tenemos que

$$xqy^{-1} = (q_1 \frac{x_1}{y_1}, \frac{q_1 x_2 - y_1 + q_2}{y_1})$$

y entonces nos queda que

$$(-y_1)^m \sum_{q \in F} \frac{\partial^m}{\partial x_{2,i}^m} K(xqy^{-1}) = \frac{\partial^m}{\partial y_{2,i}^m} \{\sum_{q \in F} K(xqy^{-1})\}$$

donde $F \subset H_K K$ es un conjunto finito. Supongamos entonces que $K(x, y)$ tiene $m - 1$ derivadas parciales continuas con respecto a $x_{2,i}$. Tenemos entonces

$$(-y_1)^{-m} \frac{\partial^{m-1}}{\partial y_{2,i}^{m-1}} K(x, y) = \sum_q \frac{\partial^{m-1}}{\partial x_{2,i}^{m-1}} K(xqy^{-1}) = c + \int_0^y \{\sum_q \frac{\partial^m}{\partial x_{2,i}^m} K(xqy^{-1})\} dt$$

de donde se sigue que

$$\frac{\partial^m}{\partial y_{2,i}^m} K(x, y) = (-y_1)^m \sum_{q \in K^* K} \frac{\partial^m}{\partial x_{2.i}^m} K(x, y)$$

y por lo tanto $K(x, y)$ es una función C^∞ con respecto a las variables $y_{2,1}, \ldots, y_{2,n}$. Entonces

$$K_f(y) = c + \int_0^y \{\int_{\mathrm{M}} \frac{\partial}{\partial t} K(x, t) f(x) dx\} dy$$

Se sigue luego que $K_f \in C^1$, y de una manera análoga, $K_f \in C^\infty$. Sea

$$\begin{array}{rl} \Delta : & L \to L \\ & f \mapsto \sum_{i=1}^n \frac{\partial^2}{\partial x_{2,i}^2} f \end{array}$$

Δ es un operador no acotado sobre L. Tenemos un dominio fundamental de la forma

$$[0, 1) \times F$$

hacemos entonces

$$\begin{array}{rl} f: & \mathrm{M} \to C \\ & x \mapsto e^{imx} \end{array}$$

Luego $f \in L$, $\|f\| = 1$, y $\|\Delta f\| = m^2$.

Sea K la función núcleo. Si tenemos que

$$\Delta_x K(x,y) = \Delta_y K(x,y)$$

entonces, si $f \in L$,

$$\begin{aligned} \Delta K_f(y) &= \Delta_y \int_{\mathrm{M}} K(x,y) f(x) dx = \int_{\mathrm{M}} \Delta_y K(x,y) f(x) dx \\ &= \int_{\mathrm{M}} \Delta_x K(x,y) f(x) dx = \int_{\mathrm{M}} K(x,y) \Delta f(x) dx = K_{\Delta f}(y) \end{aligned}$$

es decir, que en este caso, K conmuta con Δ.

8 La Fórmula de Traza

En esta sección definimos una función núcleo particular sobre M.

En §1. mostramos que la traza del operador integral asociado es precisamente la fórmula explícita de Weil. En base a este resultado, en §2. reformulamos la transformación de Weil de la hipótesis de Riemann como una hipótesis de positividad para la traza del operador.

8.1 Definición del operador, Fórmula de traza

Sea K un cuerpo de números. Sea M_K el conjunto de los valores absolutos canónicos sobre K, y S_∞ los valores absolutos arquimedianos en M_K.

Sea ψ_A la función característica de un conjunto A y para $(x_1, x_2) \in J_K^0 A_K$, y $v \notin S_\infty$, sea

$$\phi_v(x_1,x_2) = \begin{cases} 0 & \text{, si } x_{1,v} = 1 \\ \psi_{\mathrm{A}_v}(\frac{x_{2,v}}{x_{2,v}-1}) & \text{, si } x_v \neq 1 \text{ y } x_{1,v} - 1 \in \pi_v \mathrm{A}_v \\ \psi_{\mathrm{A}_v}(x_{2,v}) & \text{en otro caso.} \end{cases}$$

donde A_v denota los enteros locales, y π_v un elemento de orden 1 en A_v.

Para cada elemento $\alpha \in H_K$, la aplicación $\alpha \to (\alpha)$ es un homomorfismo sobre I_K. Sea $\{\mathrm{p}_i\}_{i\in I}$ un sistema de representantes de los ideales primos en I_K. Sea $x \in J^0$. Definimos

$$\nu(x) = \psi_{-E_\infty}(x_v/\prod_{v\notin S_\infty} \mathrm{p}_i^{\mathrm{ord}_v x})_{v\in S_\infty}$$

donde E_∞ es el conjunto mencionado en §4.1, tal que

$$E_\infty \times \prod_{v\notin S_\infty} U_v$$

es un dominio fundamental de J^0/H. Asumimos que E es un entorno de 1.

Sea ahora $S \supset S_\infty$ una familia finita de valores absolutos. Definimos entonces

$$\begin{aligned}\Psi_S :\ & J^0 A \to C\\ & (x_1,x_2) \mapsto \nu(x_1)\textstyle\prod_{v\in S-S_\infty} \psi_{\pi_v \mathrm{A}_v}(x_{1,v}) \prod_{v\notin S} \psi_{\mathrm{A}_v}(x_{1,v}) \prod_{v\notin S_\infty} \phi_v(x_1,x_2)\end{aligned}$$

El producto está evidentemente bien definido. Nos interesa saber cuándo $\Psi_S(xqy^{-1})$ es no nulo, si q recorre $H_K K$. Tenemos que

$$xqy^{-1} = (a\frac{x_1}{y_1}, \frac{ax_2 - y_2 + b}{y_1})$$

para $x = (x_1, x_2)$, $y = (y_1, y_2) \in J_K^0 A_K$, $q = (a, b) \in H_K K$.

Ahora nos basta con considerar $x = (x_1, x_2), y = (y_1, y_2) \in E \times F$, donde E y F son los dominios fundamentales de J^0/H y A/K respectivamente, que están descriptos en §4.1. Tenemos en particular $x_1, y_1 \in U_v$, $x_2, y_2 \in \mathrm{A}_v$ para todo v valuación p-ádica. Luego

$$a\frac{x_1}{y_1} \in U_v$$

para todo $v \notin S$ si y sólo si a es una S-unidad, es decir, $a = u\mathrm{p}_1^{n_1} \dots \mathrm{p}_r^{n_r}$, con $\mathrm{p}_i \in S$, $u \in U_K$. Si aparte pedimos

$$\nu(a\tfrac{x_1}{x_2}) = 1, \quad \textstyle\prod_{v\in S-S_\infty} \psi_{\pi \mathrm{A}_v}(x_{1,v}) = 1$$

entonces $a = -\mathrm{p}_1^{n_1} \dots \mathrm{p}_r^{n_r}$, con $n_i = 1, 2, \dots$. Tenemos que

$$\frac{ax_2 - y_2 + b}{y_1} \in (a-1)\mathrm{A}_v$$

para todo $v \in S_\infty$ si y sólo si $x_2 - y_2 + b \in (a-1)\mathrm{A}_v$. Para $x = (x_1, x_2) \in J^0 A$, sea $b(x)$ el (único) elemento de K/A_K tal que

$$x_2 + b(x) \in \mathrm{A}_v \quad \forall v \notin S_\infty$$

La aplicación $b : J^0 A \to K/\mathrm{A}_K$ está bien definida, y es continua.

Luego $x_2 - y_2 + b \in (a-1)\mathrm{A}_v$ si y sólo si

$$b \in (a-1)(b_0 + \mathrm{A}_K)$$

con $b_0 = b(\frac{x_2 - y_2}{a-1})$.

Sea $S \supset S_\infty$ una familia finita de valores absolutos en M_K, y una función continua $h_0 : \prod_{v \in S - S_\infty} K_v^* \times \prod_{v \in S_\infty} K_v \to C$. Hacemos

$$\begin{array}{rl} h: & J^0 A \to C \\ & x \mapsto h_0(x)\Psi_S(x) \end{array}$$

Supongamos que

$$\sum_{q \in H_K K} h(xqy^{-1})$$

converge absoluta y uniformemente para $x, y \in J^0 A$. Luego la función

$$\begin{array}{rl} \Upsilon_h: & \mathrm{M} \times \mathrm{M} \to C \\ & (x, y) \mapsto \sum_q h(xqy^{-1}) \end{array}$$

es continua. Ahora sea $h_0 : \prod_{v \in S - S_\infty} K_v^* \times R \to C$ una función continua, y hacemos

$$\begin{array}{rl} h: & J^0 A \to C \\ & (x_1, x_2) \mapsto h_0((x_{1,v})_{v \in S - S\infty}, \log \alpha(x))\psi_S(x) \end{array}$$

con $\alpha(x) = \prod_{v \in S_\infty} (\|\frac{x_2}{x_1 - 1}\|_v)\|\frac{x_2}{x_1 - 1}\|_v$. Se sigue entonces

$$\Upsilon_h(x, y) = \sum_{\substack{a = -\mathrm{p}_1^{n_1} \dots \mathrm{p}_r^{n_r} \\ b \in \mathrm{A}_K}} h_0((a\frac{x_1}{y_1})_{v \in S - S\infty}, \log \alpha(a\frac{x_1}{y_1}, ax_2 - y_2 + (a-1)(b_0 + b))$$

para $x, y \in E \times F$, dominio fundamental de $J^0 A / HK$.

De esta expresión se sigue que Υ_h es una función continua si la consideramos como definida sobre $(E \times F) \times (E \times F)$ con la topología inducida como subconjunto de $J^0 A$. Luego $\Upsilon_h : \mathrm{M} \times \mathrm{M} \to C$ es continua para todo $x, y \notin \partial(E \times F)$.

En particular, sea T_h el operador de Hilbert-Schmidt definido como

$$\begin{array}{rl} T_h: & \mathcal{L}^2(\mathrm{M}) \to \mathcal{L}^2(\mathrm{M}) \\ & f(x) \mapsto \int_{\mathrm{M}\times\mathrm{M}} \Upsilon_h(x,y) f(x) dx \end{array}$$

Luego

$$\mathrm{Tr}\ T_h = \int_{\mathrm{M}} \Upsilon_h(x,x) dx$$

Necesitamos hacer un cálculo.

Lema 1. *Con las mismas notaciones, sea*

$$h(x_1,x_2) = [h_0((x_1)_{v\in S-S_\infty}, -\log\alpha(x)) + h_0((x_1)_{v_i n S-S_\infty}, \log\alpha(x))]\Psi_S(x)$$

Entonces

$$Tr\ T_h = \mu \frac{2^{r_1}(2\pi)^{r_2}}{(r_1+r_2)!} \sum_a \int_R h_0(a,x) e^{|x|} |x|^{r_1+r_2-1} dx$$

con

$$\mu = \mu^*(E)$$

y E es el dominio fundamental de J^0/H.

Dem. Sin pérdida de generalidad, podemos suponer

$$h(x_1,x_2) = h_0(x_1, \log\alpha(x))\Psi_S(x)$$

Tenemos entonces

$$\Upsilon_h(x,x) = \sum_{a,b} h_0(a, \log \prod_{v\in S_i n f t y} \psi_{[1,\infty)}(\|x_2+b\|_v)\|x_2+b\|_v$$

Se sigue

$$\mathrm{Tr}\ T_h = \int_{\mathrm{M}} \Upsilon_h(x,x)dx = \mu \sum_a \int_{R^{r_1}\times C^{r^2}} h_0(a, \log \prod_{v\in S_\infty} \psi_{[1,\infty)}(\|x_2\|_v)\|x_2\|_v) dx_2$$

por la convergencia uniforme de la serie. Luego

$$\begin{array}{rl} & \int_{R^{r_1}\times C^{r_2}} h_0(a, \log\prod_{v\in S_\infty} \psi_{[1,\infty)}(\|x\|_v)\|x\|_v)dx = \\ = & 2^{r_1}(2\pi)^{r_2} \int_{[1,\infty)^{r_1+r_2}} x_1 \dots x_{r_2} h_0(a, \log\prod_{i=1}^{r_1+r_2} |x_i|) dx_1 \dots dx_{r_1+r_2} \\ = & 2^{r_1}(2\pi)^{r_2} \int_{R_+^{r_1+r_2}} e^{\sum t_i} h_0(a, \sum t_i) dt_1 \dots dt_{r_1+r_2} \end{array}$$

Ahora hacemos la sustitución

$$x = t_1 + \ldots + t_{r_1+r_2},\ t_2 = t_2,\ \ldots,\ t_{r_1+r_2} = t_{r_1+r_2}$$

y escribimos

$$W_x = \{t_2, \ldots, t_{r_1+r_2} : t_2 + \ldots + t_{r_1+r_2} \leq x\}$$

Tenemos entonces

$$\begin{aligned} \int_{R^{r_1+r_2}} e^{\sum t_i} h_0(a, \sum t_i) dt_1 \ldots dt_{r_1+r_2} &= \int_{R_+} \int_{W_x} h_0(a,x) e^x dt_1 \ldots dt_{r_1+r_2} \\ &= \tfrac{1}{(r_1+r_2)!} \int_{R_+} h(x) e^x x^{r_1+r_2} dx \end{aligned}$$

de donde se sigue la fórmula del lema.

Sea $k_1 : R \to C$ una función continua con derivada continua, y tal que hay algún $\delta > 0$ tal que

$$k_1(x), k_1'(x) = O(e^{-(\frac{1}{2}+\delta)|x|})$$

para $|x| \to \infty$. En particular, k_1 está en las condiciones del teorema de la Fórmula Explícita.

Sea $k_2 : R \to C$ una función test continua tal que

$$k_2(x) = O(e^{-m|x|})$$

para $|x| \to \infty$, y para un entero m sunficientemente grande.

Sea χ un caracter de Hecke (§5.1). Luego χ induce un quasi-caracter χ sobre el grupo I_K de los ideales fraccionarios no nulos de A_K.

Sea p un ideal primo del anillo de enteros A_K. Sea entonces

$$\begin{aligned} k_{\mathrm{p}}^0 :\ & \textstyle\prod_{v \in S_\infty \bigcup \{\mathrm{p}\}} K_v^* \times \prod_{v \in S_\infty} K_v \to C \\ & x \mapsto \|x_1\|_{\mathrm{p}}^{1/2} [\chi(x_{\mathrm{p}}^{-1}) k_1(\log \|x^{-1}\|_{\mathrm{p}} \alpha(x)) + \chi(x_{\mathrm{p}}) k_1(\log \|x\|_{\mathrm{p}} \alpha(x))] g(\log \alpha(x)) \end{aligned}$$

con

$$g(x) = \frac{(r_1+r_2)!}{2^{r_1}(2\pi)^{r_2}\mu} e^{-|x|} |x|^{1-r_1-r_2} k_2(x)$$

Hacemos

$$k_{\mathrm{p}}(x_1, x_2) = [k_{\mathrm{p}}^0(x_1, -x_2) + k_{\mathrm{p}}^0(x_1, x_2)] \Psi_S(x)$$

y se sigue entonces que

$$\Upsilon_{k\mathrm{p}}(x,y) = \sum_q k_{\mathrm{p}}(xqy^{-1})$$

converge absoluta y uniformemente, y también

$$\Upsilon_{k\mathrm{p}}(x,y) = O(N\mathrm{p}^{-(1+\delta)})$$

Análogamente, sea

$$\begin{array}{rl} h_{k_1}: & R \to C \\ & x \mapsto \delta_\chi \int_R k_1(t)(e^{\frac{x-t}{2}} + e^{\frac{t-x}{2}})dt + K_1(0)\log A + \sum_{v\in S_\infty} \Theta_v k_{1,x,v} \end{array}$$

y definimos

$$\begin{array}{rl} k_\infty: & J^0A \to C \\ & (x_1,x_2) \mapsto [h(-\log\alpha(x))g(\log\alpha(x)) + h(\log\alpha(x))g(\log\alpha(x))]\Psi_{S_\infty}(x) \end{array}$$

La suma

$$\sum_q k_\infty(xqy^{-1})$$

también converge uniformemente. Hacemos finalmente

$$k(x) = \sum_{\mathrm{p}} k_{\mathrm{p}}(x)$$

donde p recorre los ideales primos de A_K y el símbolo ∞. La suma es absolutamente convergente.

Proposición 1. *Sea* $\Upsilon_k(x,y) = \sum_q k(xqy^{-1})$*,y* T_k *el operador integral asociado. Entonces*

$$Tr\ T_k = \int_R k_0(x)k_2(x)dx$$

con

$$k_0(x) = h(x) - \sum_{p,n} \frac{\log Np}{Np^{n/2}}[\chi(p^{-n})k_1(\log Np^{-n} + x) + \chi(p^n)k_1(\log Np^n + x)]$$

La demostración es clara a partir del lema.

Proposición 2.

$$\mathrm{Tr}\ T_k = \lim_{T\to\infty} \sum_{|\rho|<T} \Phi_{k_1 * k_2}(\rho)$$

Dem. Por la proposición 1 y la fórmula explícita,

$$\begin{aligned} \text{Tr } T_k &= \int_R [\sum_{|\rho|<T} e^{(s-\frac{1}{2})x}\Phi_{k_1} + O(e^{|x|}/T)]k_2(x)dx \\ &= \lim_{T\to\infty} \sum_{|\rho|<T} \Phi_{k_1}(\rho)\Phi_{k_2}(\rho) \end{aligned}$$

de donde se sigue la proposición.

Si hacemos

$$\Upsilon^*(x,y) = \Upsilon(x,y) + \overline{\Upsilon(y,x)}$$

tenemos entonces

$$\langle T^* f, g\rangle = \int_{\mathrm{M}}\int_{\mathrm{M}} T^*(x,y)f(x)\overline{g(y)}dxdy = \langle f, T^* g\rangle$$

es decir, que T^* es un operador autoadjunto, y tenemos que

$$\text{Tr } T^* = 2\text{Re}(\text{Tr } T)$$

8.2 Relación con la hipótesis de Riemann

Ahora podemos reformular la equivalencia de Weil para la hipótesis de Riemann, que enunciamos en 5.2.

Proposición 3. *Sea T el operador asociado a $L(s,\chi)$ y a funciones k_1, k_2. La función $L(s,\chi)$ satisface la hipótesis de Riemann si y sólo si*

$$Tr\ T \geq 0$$

para todas las funciones

$$k_1(x) = f(x), \quad k_2(x) = \overline{f(-x)}$$

con $f \in Ad(R)$ tal que

$$f(x) = O(e^{-m|x|})$$

donde $m = m_\chi$ es un entero suficientemente grande.

References

[Co] Conway, J. "A course in functional analysis," Springer Verlag (1985).

[Du] Dunford, N. y Schwartz, J. "Linear operators," Interscience (1963).

[Go] Goldfeld, D. "Explicit formulae as trace formulae," *Number Theory, Trace Formulas and Discrete Groups, Symposium in Honor of Atle Selberg,* Academic Press (1989), 281-288.

[Ha] Halmos, P. "Measure theory," D. Van Nostrand, (1961).

[Ka] Kato, T. "Pertubation theory for linear operators," Springer Verlag (1966).

[La] Lang, S. "Algebraic number theory," Addison-Wesley (1970).

[Se] Selberg, A. "Harmonic analysis in discontinuous groups in weakly simmetric Riemannian spaces," *J. Indian Math. Soc.* **20** (1956), 47-87.

[Si] Simon, B. "Trace ideals and their applications," Cambridge University Press (1979).

[We] Weil, A. "Sur les 'formules explicites' dans la théorie des nombres premiers," *Comm. Sém. Math. Univ. Lund.* 1952, Tomme supplémentaire (1952), 252-265.