Universidad Nacional Autónoma de México

Facultad de Ciencias

Campos de números nolineales

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
ADRIÁN ZENTENO GUTIÉRREZ

DIRECTOR DE TESIS:
DR. TIMOTHY MOONEY GENDRON THORNTON

2009

1. Datos del alumno
   Zenteno
   Gutiérrez
   Adrián
   5709 4495
   Universidad Nacional Autónoma de México
   Facultad de Ciencias
   Matemáticas
   405031319

2. Datos del tutor
   Dr
   Timothy Mooney
   Gendron
   Thornton

3. Datos del Sinodal 1
   Dr
   Santiago Alberto
   Verjovsky
   Solá

4. Datos del Sinodal 2
   Dra
   María del Carmen
   Gómez
   Laveaga

5. Datos del Sinodal 3
   Dr
   Manuel
   Cruz
   López

6. Datos del Sinodal 4
   Dr
   Salvador
   Pérez
   Esteva

7. Datos de la tesis
   Campos de números nolineales
   120 p.
   2009

.

Dedicada a:
Guillermo Sienra Loera.

Agradecimientos

"Las matemáticas no son un recorrido prudente por una autopista despejada, sino un viaje a un terreno salvaje y extraño, en el cual los exploradores se pierden a menudo".
(W.S.Anglin)

Hacer una lista de todas las personas a las que quisiera agradecer por su ayuda en la realización de esta tesis implicaría es complicado. Así que seguramente se me escapara mencionar a más de una. De antemano, les ruego una disculpa por mi pésima memoria. Sin embargo, ustedes saben que este trabajo es de todos ustedes.

Se que no hay forma de agradecerle a un padre los miles de sacrificios que tienen que hacer por ver a su hijo realizado. Sin embargo de la manera más humilde agradezco a mis padres: Rufina y Jesús por mostrarme que no existe manera de ser los padres perfectos, pero que hay millones de ser buenos padres y ellos eligieron la mejor. A mis tíos: Víctor, Marco Antonio, Corina y Antonia por haberme aguatado en sus casas por tantos años, a Karla por su comprensión, apoyo y paciencia en este proceso y a toda mi familia por estar ahí.

Al Dr. Guillermo Sienra porque sin su ayuda simplemente no estaría aquí. A mi asesor el Dr. Timothy M. Gendron, por aceptarme como su hijo académico, por mostrarme que no hay que bajar la frente ante el problema más difícil, pero que aun el problema más humilde merece respeto. Por enseñarme que el hacer matemáticas es una bendición y una fiesta interminable que hay que disfrutar cada día.

De manera especial agradezco a Manuel Cruz, Carmen Gómez y Jesica Jaurez por escucharme y corregir muchos de mis errores cometidos en el presente trabajo.

A mis profesores: Azael del Mazo por ser el primero en mostrarme el camino de las matemáticas, a Jorge Nicolás, Yadira y Alfredo por mantener ese gusto por la mates durante la preparatoria y a Alberto Verjovsky por trasmitirme su entusiasmo. A mis profesores de la facultad: Leopoldo Morales por ser el primero en decirme - tienes que ser matemático -, Roció Vite por su formalidad, Emilio Lluis por su experiencia y a Jesús Falconi por la intuición. A Hugo Rincón, Israel Moreno, Ana Irene Ramírez, Juan José Alba, Carlos Prieto, Asunción Preiser; a mis ayudantes: Víctor Cruz, Gabriela Posadas, Omar Antolin, Hiroki Koike, Ernesto Mayorga, Rolando Gómez y muchos más que de

uno u otra manera influyeron en mi formación de matemático a través de la licenciatura.

A los profesores de la UAM-A Marina Salazar y Lino Reséndiz, a Jean Marc Gambaudo de la U. de Lille y a Luis Lomeli de la U. de Iowa, por dedicar parte de su tiempo a escucharme y compartir parte de sus conocimientos conmigo.

A mis amigos: Gloria Azuara, Iveth Bermeo, Axel Moreno, Natalia Ríos, Ilse Severino, Miriam Almeida, Alfredo Reyes, Itzel García, Nancy Castellanos, Ataulfo Anton, Cristóbal Falconi, Argenis, Roberto, Eduardo, la rubia, chomic, el choche, Violeta, Ilán, Fernando, Manuel, Angelito, Camilo, Valdimir, Adriana, el chuvy y tantos más que me acompañaron en este camino.

A todos mis estudiantes de la facultad de ciencias y de la UAM-A que contribuyeron a mostrarme que otra parte fundamental del ser matemático es la enseñanza y la transmisión de conocimientos.

A la UNAM, por darme una formación no solo académica sino también cultural y personal. Y a dios, por permitirme tener un gran motivo para vivir y disfrutar cada día de mi estancia en este mundo. Las matemáticas.

Indice

Introducción

"La matemática es la reina de las ciencias y la teoría de números es la reina de las matemáticas".
(Gauss)

El propósito de esta tesis es describir con detalle el concepto de campo de números no lineal $N(K)$ del artículo de T. Gendron y A. Verjovsky [1]. El cual como veremos es una extensión natural de un campo numérico K, en el sentido que extiende las dos operaciones de K a todo $N(K)$ y que además, resultara ser la proyectivización de una cierta álgebra graduada de funciones holomorfas $\mathrm{Har}_\bullet[K]$.

En particular, si $K = \mathbb{Q}$, veremos que $N(\mathbb{Q})$ contiene las clases proyectivas que corresponden a funciones zeta y L clásicas. Veremos también, que $N(K)$ es una variedad riemanniana, lo cual nos ayudara a construir una teoría de Galois para $N(K)$ que coincide con la teoría de Galois para las extensiones de K en el sentido clásico.

Empezaremos con un repaso breve de los números p-ádicos para posteriormente, de manera más general, estudiar los campos locales de característica 0, que como veremos son $\mathbb{R}$, $\mathbb{C}$ o una extensión finita de $\mathbb{Q}_p$ (*Cap.* 1).

Sea K un campo numérico de grado n sobre $\mathbb{Q}$ con anillo de enteros O_K. Una valuación de K es una función

$$|\cdot|_\nu : K \longrightarrow \mathbb{R}_{\geq 0},$$

que satisface las propiedades usuales del "valor absoluto". Se dice que dos valuaciones $|\cdot|_\nu$ y $|\cdot|_\mu$ son equivalentes si definen la misma topología. Esta relacion define un conjunto de clases de equivalencia que llamaremos los lugares de K. Luego, para cada lugar ν podemos completar a K con respecto a cada una de las valuaciones $|\cdot|_\nu$, en el sentido usual de análisis. A la completación de K en el lugar ν la denotaremos por K_ν. Luego, veremos que esta completación resulta ser un campo local de los mencionados anteriormente.

Considerando el producto directo restringido de K_ν sobre todos los lugares ν obtenemos el anillo de adéles de K

$$\mathbb{A}_K = \prod_\nu {}' K_\nu.$$

Veremos que K se puede sumergir diagonalmente en $\mathbb{A}_K$ como un subgrupo discreto y cocompacto con respecto a la adición. Luego, el cociente

$$\hat{\mathbb{S}}_K = \mathbb{A}_K/K,$$

es un solenoide que llamaremos el grupo de clases de adéles asociado a K y el cual es isomorfo a

- El cubriente universal algebraico del toro de Minkowski $\mathbb{T}_K$

$$\varprojlim \mathbb{T}_{\mathfrak{a}},$$

  donde $\mathfrak{a}$ corre sobre todos los ideales de O_K.

- La suspensión

$$(K_\infty \times \hat{O}_K)/O_K,$$

  donde $\hat{O}_K$ es la completación profinita de O_K.

Usando la suspensión anterior, construiremos la hiperbolización del grupo de clases de adéles $\hat{\mathfrak{S}}_K$, cuyas hojas son polidiscos isomorfos a $(\mathbb{H}^2)^n$ y cuya frontera distinguida es $\hat{\mathbb{S}}_K$ (*Cap.* 2).

Si $K/\mathbb{Q}$ es una extensión de Galois, mostraremos que $\mathrm{Char}(\hat{\mathbb{S}}_K)$, el grupo de caracteres de $\hat{\mathbb{S}}_K$, pose una segunda operación que le da estructura de campo. Luego, existe un isomorfismo canónico

$$\mathrm{Char}(\hat{\mathbb{S}}_K) \cong K. \quad (*)$$

Además, si $\mathfrak{d}_{O_K}^{-1} = O_K$, donde $\mathfrak{d}_{O_K}^{-1}$ es el diferente inverso asociado al anillo de enteros de K, se tiene que

$$\mathrm{Char}(\mathbb{T}_K) \cong O_K.$$

Sea $f \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$, por análisis armónico f tiene un desarrollo en series de Fourier

$$\sum a_q \phi_q,$$

donde $q \in K$, $a \in \mathbb{C}$ y $\phi_q \in \mathrm{Char}(\hat{\mathbb{S}}_K)$. De aquí y de $(*)$ tenemos la inclusión canónica

$$K \hookrightarrow L^2(\hat{\mathbb{S}}_K, \mathbb{C}),$$

la cual nos permite extender las dos operaciones de K a $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$. Para extender a $+_K$, usaremos el producto de Cauchy de funciones en $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$, siempre que este bien definido, y lo denotaremos por $\oplus$. Para el producto $\times_K$ usaremos el producto de Dirichlet, el cual denotaremos por $\otimes$. Con estas dos operaciones $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ adquiere una estructura de álgebra parcial, en el sentido de que las operaciones $\oplus$ y $\otimes$ son solo parcialmente definidas.

Una interpretación de $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ como valores frontera de funciones holomorfas en $\hat{\mathfrak{S}}_K$, puede ser introducida a través de la noción de holomorficidad

graduada, donde cada noción de holomorficidad esta dada en el sentido clásico. Si $K/\mathbb{Q}$ es una extensión de Galois real, tenemos el grupo de signos

$$\Theta = \{+,-\}^n,$$

donde n es el grado de la extensión de $K/\mathbb{Q}$. Luego f define una (2^n+1)-tupla de funciones $F = (F_\theta; F_0)$ en la hiperbolización $\tilde{\mathfrak{S}}_K$, donde para cada $\theta \in \Theta$, F_θ es "θ-holomorfa" y $F_0 = a_0$. Luego, al espacio de Hilbert de tales funciones holomorfa-graduadas F, lo denotaremos por

$$\mathrm{Har}_\bullet[K] = \bigoplus_{\theta\in\Theta} \mathrm{Har}_\theta[K] \oplus \mathbb{C},$$

el cual veremos es isomorfo a $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$. Para el caso de $K/\mathbb{Q}$ una extensión de Galois compleja tenemos una graduación similar aunque su construcción es un poco más delicada.

Dado $\mathrm{Har}_\bullet[K]$ visto como espacio vectorial, veremos que las operaciones $\oplus$ y $\otimes$ no están bien definidas cuando estas descienden a la proyectivización usual de de $\mathrm{Har}_\bullet[K]$. Así que definimos una nueva proyectivización quitando, además del 0, los elementos de traza 0 en $\mathrm{Har}_\bullet[K]$. Lo cual nos define un hiperplano de dimensión infinita

$$N(K) \subset \mathbb{P}\mathrm{Har}_\bullet[K],$$

que tiene estructura de doble semigrupo parcial con las operaciones $\oplus$ y $\otimes$. Entonces, $N(K)$ será nuestro "campo de números no lineales" asociado a K (*Cap.* 3).

Por otro lado, veremos que las funciones zeta y L definen elementos de $N(K)$ y el producto de Dirichlet de estas, coinside con el producto $\otimes$ de elementos de $\mathbb{N}(K)$. Esto nos ayudara a definir algunas nociones de lo que podría ser una especie de aritmética no lineal. En particular daremos algunas nociones básicas de una teoría de unidades con respecto a los productos $\oplus$ y $\otimes$ para el anillo de enteros no lineal $N(\mathbb{Z})$ (*Cap.* 4).

Por construcción $N(K)$ cuenta con las propiedad de ser una subvariedad Riemanniana de un espacio proyectivo de dimensión infinita con la métrica Fubini-Study. A partir de la graduación dada anteriormente, definimos un automorfismo de un campo de números no lineales $N(K)$ como una isometría Fubini-Study que permuta la graduación y preservan las operaciones $\oplus$ y $\otimes$.

Dado K un campo numérico, denotaremos por $\mathrm{Gal}(N(K)/K)$, al grupo de automorfismos de $N(K)$ que fijan a K. Ahora, si L/K es una extensión de Galois denotaremos por

$$\mathrm{Gal}(N(L)/N(K)),$$

al grupo de automorfismos de $N(L)$ que dejan fijo a $N(K)$ (*Cap.* 5). Finalmente, mostraremos que la teoría de Galois de las extensiones de los campos de números no lineales $N(K)$ coincide con la teoría de Galois de los campos clásicos en el sentido de que si tenemos L/K una extensión de Galois entonces

$$\mathrm{Gal}(N(L)/N(K)) \cong \mathrm{Gal}(L/K).$$

Notación

En el presente trabajo trataremos de apegarnos a la notación estándar en matemáticas, por ejemplo $\mathbb{Z}$ (resp. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$) denotara el conjunto de los números enteros (resp. racionales, reales y complejos).

Convendremos, que el conjunto de los números naturales será considerado como el conjunto $\mathbb{N} = \{1, 2, 3, \cdots\}$. Denotaremos por $\mathbb{R}_{\geq 0}$ (resp. $\mathbb{R}_{>0}$) al conjunto $\{x \in \mathbb{R} : x \geq 0\}$ (resp. $\{x \in \mathbb{R} : x > 0\}$).

Cuando escribamos una sucesión $\{x_i\}$ daremos por hecho que el conjunto de índices es el conjunto de los números naturales $\mathbb{N}$, salvo que se indique lo contrario. Dado un numero complejo $z = x + iy$ denotaremos por $\mathrm{Re}(z)$ (resp. $\mathrm{Im}(z)$) a la parte real (resp. parte imaginaria) de z y por Im a la imagen de una función dada.

Un anillo R en el contexto de esta tesis será entendido como anillo con 1. Diremos que K es un campo numérico si este es una extensión finita de $\mathbb{Q}$, en algunos textos a K se le llama también campo de números algebraicos. Cuando hablemos de extensiones de Galois daremos por hecho que son extensiones finitas, salvo que se indique lo contrario. Por otro lado, cuando nos refiramos a V un K-espacio vectorial, este puede ser de dimensión infinita.

Aquí diremos que un espacio topológico M es metrizable, si existe una métrica en M que induce la topología dada y M es separable si posee una base numerable de abiertos. Cuando hablemos de campos locales nos restringiremos al caso de característica 0.

Capítulo 1

Campos Locales

En este capítulo daremos un repaso general de los conceptos de teoría algebraica de números que utilizaremos en el resto de la tesis. En el presente trabajo asumiremos que el lector está familiarizado con la teoría de Galois y la teoría de campos finitos. Para una referencia ver [12].

1.1 Números p-ádicos

En esta sección estudiaremos las propiedades elementales de los números p-ádicos. Las referencias básicas de esta sección son [3] y [11].

Sea p un número primo. Un *entero p-ádico* es una serie formal infinita

$$a_0 + a_1 p + a_2 p^2 + \cdots ,$$

donde $0 \leq a_i \leq p-1$. Al conjunto de todos los enteros p-ádicos lo denotaremos por $\mathbb{Z}_p$.

Proposición 1.1. *Las clases de residuos* $a \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}$ *pueden ser representadas de manera única de la forma*

$$a \equiv a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} \bmod p^n,$$

donde $0 \leq a_i \leq p-1$*, para* $i = 0, 1, \cdots, n-1$.

Demostración. Por inducción sobre n. Para $n = 1$ es claro que se cumple la Proposición. Supongamos que la Proposición es cierta para $n-1$. Entonces, por hipótesis de inducción, tenemos una representación única

$$a \equiv a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-2} p^{n-2} + g p^{n-1},$$

para algún entero g. Si $g \equiv a_{n-1} \bmod p$ tal que $0 \leq a_{n-1} \leq p-1$, a_{n-1} es únicamente determinado por a y la congruencia de la Proposición se cumple. □

Cada $q \in \mathbb{Z}$, o de manera un poco más general, cada número racional $q = \frac{f}{g}$, donde p no divide a g, define una sucesión de clases de residuos

$$\bar{s}_n = q \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}, \quad n \in \mathbb{N}.$$

De la Proposición 1.1 tenemos que:

$$\begin{aligned} \bar{s}_1 &= a_0 \bmod p \\ \bar{s}_2 &= a_0 + a_1 p \bmod p^2 \\ \bar{s}_3 &= a_0 + a_1 p + a_2 p^2 \bmod p^3 \\ &\vdots \end{aligned}$$

donde los coeficiente $0 \leq a_i \leq p-1$, son determinados de manera única. Luego, la sucesión de números

$$s_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}, \quad n \in \mathbb{N},$$

define un entero p-ádico

$$\sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p.$$

A este le llamaremos la *expansión p-ádica* de q.

Con el fin de poder considerar a los racionales de la forma $\frac{f}{g}$, donde $g = p^n h$ con $n \geq 1$, extenderemos el dominio de los enteros p-ádicos a las series formales

$$\sum_{\nu=m}^{\infty} a_\nu p^\nu,$$

donde $m \in \mathbb{Z}$ y $0 \leq a_\nu \leq p-1$. A estas series las llamaremos *números p-ádicos* y usaremos $\mathbb{Q}_p$ para denotar al conjunto de dichos números.

Si tenemos un número racional arbitrario $q \in \mathbb{Q}$, lo podemos escribir como

$$q = \frac{f}{g} p^m \quad \text{donde } f, g, m \in \mathbb{Z}, \quad (fg, p) = 1.$$

Luego, dado que tenemos una expansión p-ádica para $\frac{f}{g}$, a saber

$$a_0 + a_1 p + a_2 p^2 + \cdots,$$

podemos asociarle a q el número p-ádico

$$a_0 p^m + a_1 p^{m+1} + a_2 p^{m+2} \cdots \in \mathbb{Q}_p,$$

como su expansión p-ádica.

Corolario 1.1. *Existe un mapeo canónico*

$$\mathbb{Q} \longrightarrow \mathbb{Q}_p,$$

el cual envía a $\mathbb{Z}$ en $\mathbb{Z}_p$ de forma inyectiva.

Demostración. El mapeo está dado por enviar a cada $q \in \mathbb{Q}$ a su expansión p-ádica. Luego, es claro que este mapeo envía a $\mathbb{Z}$ en $\mathbb{Z}_p$. Si $a, b \in \mathbb{Z}$ tienen la misma expansión p-ádica, se tiene que p^n divide a $a - b$ para cada n, por lo tanto $a = b$. □

Dado un número *p-ádico*

$$s = \sum a_\nu p^\nu,$$

lo podemos ver como una sucesión de clases de residuos

$$\bar{s}_n = s \bmod p^n,$$

donde los términos de dicha sucesión se encuentran en los diferentes anillos $\mathbb{Z}/p^n\mathbb{Z}$.

Para cada n tenemos las proyecciones canónicas

$$\begin{array}{rl} \phi_n : & \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z}, \\ & \bar{s}_n \longmapsto \bar{s}_{n-1}. \end{array}$$

Es claro que ϕ_n es suprayectiva y su kernel está formado por los elementos de $\mathbb{Z}/p^n\mathbb{Z}$ que son múltiplos de p^{n-1}. Entonces la sucesión,

$$\cdots \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z} \longrightarrow \cdots \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z},$$

forma un sistema proyectivo indexado por los enteros positivos.

Luego podemos definir el límite proyectivo

$$\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z},$$

del sistema $(\mathbb{Z}/p^n\mathbb{Z}, \phi_n)$ (Ver Apéndice B.1).

Asociando a cada entero p-ádico

$$s = \sum_{\nu=0}^{\infty} a_\nu p^\nu,$$

la sucesión $\{\bar{s}_n\}$ de clases de residuos

$$\bar{s}_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z},$$

obtenemos la siguiente biyección

$$\mathbb{Z}_p \xrightarrow{\sim} \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}.$$

Notemos que $\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$ es un subanillo del producto directo $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$, donde la adición y multiplicación son definidas componente a componente.

Luego identificando a $\mathbb{Z}_p$ con $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ obtenemos el *anillo de enteros p-ádicos*. Como cada elemento $q \in \mathbb{Q}_p$ admite una representación

$$q = p^m f,$$

con $f \in \mathbb{Z}_p$, la adición y multiplicación en $\mathbb{Z}_p$ se extiende a todo $\mathbb{Q}_p$ y $\mathbb{Q}_p$ se convierte en el campo de cocientes de $\mathbb{Z}_p$.

En $\mathbb{Z}_p$, un entero $a \in \mathbb{Z}$ es determinado por las congruencias

$$a \equiv a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} \bmod p^n,$$

con $0 \leq a_i \leq p-1$. Luego, haciendo la identificación

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z},$$

el subconjunto $\mathbb{Z}$ se identifica con las tuplas

$$(a \bmod p, a \bmod p^2, a \bmod p^3, \cdots) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}.$$

Así, tenemos que $\mathbb{Z}$ es un subanillo denso de $\mathbb{Z}_p$. De la misma forma, $\mathbb{Q}$ es un subcampo denso de $\mathbb{Q}_p$.

Otra ventaja de identificar a los números p-ádicos con $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ es que si consideramos a $\mathbb{Z}/p^n\mathbb{Z}$ como campo topológico con la topología discreta, esta induce una topología en el producto $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ conocida como topología producto o topología de Tychonoff [14]. Luego, $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ adquiere la topología relativa del producto, la cual es conocida como la *topología profinita* (Ver Apéndice B.2). En consecuencia, $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ es un grupo profinito y por lo tanto es un espacio de Hausdorff compacto con respecto a la topología profinita.

Ahora, daremos una definición alternativa de los números p-ádicos a partir del valor absoluto p-ádico.

Sea $a = \dfrac{b}{c}$; $b, c \in \mathbb{Z}$ distintos de cero. Para un primo p, fijo, podemos escribir

$$a = p^m \frac{a'}{b'}, \quad (b'c', p) = 1.$$

El *valor p-ádico* de a se define como

$$|a|_p = \frac{1}{p^m}.$$

Al exponente m, en el valor p-ádico anterior, lo denotaremos por $\nu_p(a)$. Luego, si definimos $\nu_p(0) = \infty$, tenemos la siguiente función

$$\nu_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\},$$

la cual satisface que

$$\nu_p(ab) = \nu_p(a) + \nu_p(b), \quad \nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}.$$

La función ν_p es llamada la *valuación exponencial p-ádica* de $\mathbb{Q}$.

Luego el *valor absoluto p-ádico* viene dado por

$$\begin{aligned} |\cdot|_p : \quad & \mathbb{Q} \longrightarrow \mathbb{R} \\ & a \longmapsto p^{-\nu_p(a)}. \end{aligned}$$

El cual, además, cumple la propiedad de ser no arquimediano o ultramétrico, *i.e.* satisface

$$|a+b|_p \leq \max\left\{|a|_p, |b|_p\right\},$$

para $a, b \in \mathbb{Q}$.

Una *sucesión de Cauchy* con respecto a $|\cdot|_p$ es por definición una sucesión de números racionales $\{x_n\}$, tal que para toda $\epsilon > 0$, existe un entero positivo n_0 que satisface

$$|x_n - x_m|_p < \epsilon,$$

para toda $n, m \geq n_0$. Una sucesión $\{x_n\}$ en $\mathbb{Q}$ es llamada una *nulsucesión* con respecto a $|\cdot|_p$ si $|x_n|_p$ es una sucesión que converge a 0 en el sentido usual.

Las sucesiones de Cauchy forman un anillo R, y las nulsucesiones un ideal maximal $\mathfrak{m}$. Luego definimos nuevamente el campo de los números p-ádicos como el campo de clases de residuos

$$\mathbb{Q}_p := R/\mathfrak{m}.$$

Nuevamente existe un mapeo de $\mathbb{Q}$ en $\mathbb{Q}_p$, el cual asocia a cada $a \in \mathbb{Q}$ las clases de residuos de la sucesión constante $(a, a, a, \cdots)$.

El valor absoluto p-ádico $|\cdot|_p$ en $\mathbb{Q}$ se extiende a $\mathbb{Q}_p$ asociando a cada elemento $x = \{x_n\} \bmod \mathfrak{m} \in R/\mathfrak{m}$ el valor absoluto

$$|x|_p := \lim_{n\to\infty} |x_n|_p \in \mathbb{R}.$$

Este límite existe porque $\left\{|x_n|_p\right\}$ es una sucesión de Cauchy en $\mathbb{R}$. Además, esta es independiente de la elección de la sucesión $\{x_n\}$ dentro de su clase mod $\mathfrak{m}$ porque toda nulsucesión p-ádica $y_n \in \mathfrak{m}$ satisface que $\lim_{n\to\infty} |y_n|_p = 0$.

La valuación exponencial p-ádica ν_p en $\mathbb{Q}$ se extiende a una valuación exponencial

$$\nu_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\},$$

que se define como sigue. Si $x \in \mathbb{Q}_p$ es la clase de la sucesión de Cauchy $\{x_n\}$, donde $x_n \neq 0$, entonces

$$\nu_p(x_n) = -\log |x_n|_p$$

la cual diverge a ∞ o es una sucesión de Cauchy en $\mathbb{Z}$ la cual eventualmente se hace constante para algún n suficientemente grande pues $\mathbb{Z}$ es discreto.

Luego definimos

$$\nu_p(x) = \lim_{n\to\infty} \nu_p(x_n) = \nu_p(x_n),$$

para $n \geq n_0$ y tenemos que para toda $x \in \mathbb{Q}_p$

$$|x|_p = p^{-\nu_p(x)}.$$

Por lo tanto, como en el caso de los números reales tenemos el siguiente resultado.

Proposición 1.2. *El campo $\mathbb{Q}_p$ de los números p-ádicos es completo con respecto al valor absoluto p-ádico $|\cdot|_p$. Es decir, toda sucesión de Cauchy en $\mathbb{Q}_p$ converge con respecto a $|\cdot|_p$.*

Una propiedad que diferencia a los números reales de los números p-ádicos, es que el valor absoluto p-ádico es ultramétrico. Este hecho nos da una nueva forma de definir los enteros p-ádicos.

Proposición 1.3. *El conjunto*

$$\mathbb{Z}_p := \left\{ x \in \mathbb{Q}_p : |x|_p \leq 1 \right\},$$

es un subanillo de $\mathbb{Q}_p$, el cual es la cerradura del anillo de enteros $\mathbb{Z}$ con respecto a $|\cdot|_p$ en el campo de números p-ádicos $\mathbb{Q}_p$.

Demostración. Sea $a, b \in \mathbb{Z}_p$, entonces

$$|a+b|_p \leq \max\left\{ |a|_p, |b|_p \right\} \leq 1,$$

por lo tanto $a + b \in \mathbb{Z}_p$. Además

$$|ab|_p = |a|_p |b|_p \leq 1,$$

luego $ab \in \mathbb{Z}_p$. Si $\{x_n\}$ es una sucesión de Cauchy en $\mathbb{Z}$ y $x = \lim_{n\to\infty} x_n$, entonces $|x_n|_p \leq 1$ implica que $|x|_p \leq 1$, luego $x \in \mathbb{Z}_p$. Conversamente, sea

$$x = \lim_{n\to\infty} x_n \in \mathbb{Z}_p,$$

para una sucesión de Cauchy $\{x_n\}$ en $\mathbb{Q}$. Como vimos en líneas anteriores $|x|_p = |x_n|_p \leq 1$ para $n \geq n_0$, *i.e.* $x_n = \dfrac{a_n}{b_n}$, con $a_n, b_n \in \mathbb{Z}$, $(b_n, p) = 1$. Eligiendo para cada $n \geq n_0$ una solución $y_n \in \mathbb{Z}$ de la congruencia $b_n y_n \equiv a_n \mod p^n$, tenemos que

$$|x_n - y_n|_p \leq \frac{1}{p^n},$$

por lo tanto $x = \lim_{n\to\infty} y_n$, de modo que x pertenece a la cerradura de $\mathbb{Z}$. □

Proposición 1.4. *El grupo de unidades de $\mathbb{Z}_p$ es*

$$\mathbb{Z}^* = \left\{ x \in \mathbb{Z}_p : |x|_p = 1 \right\}.$$

Además, para toda $x \in \mathbb{Q}_p^*$, x admite una única representación

$$x = p^m u,$$

con $m \in \mathbb{Z}$ y $u \in \mathbb{Z}_p^*$.

Demostración. Si $u \in \mathbb{Z}_p$ es invertible entonces existe $u' \in \mathbb{Z}_p$ tal que $uu' = 1$. Luego

$$1 = |uu'|_p = |u|_p |u'|_p ,$$

de donde se sigue que $|u|_p = 1$. Ahora, si $\nu_p(x) = m \in \mathbb{Z}$, entonces

$$\nu_p(xp^{-m}) = \nu_p(x)\nu_p(p^{-m}) = m - m = 0.$$

Lo cual implica que $|xp^{-m}| = 1$, *i.e.* $u = xp^{-m} \in \mathbb{Z}_p^*$. □

Proposición 1.5. *Los ideales, no cero, del anillo $\mathbb{Z}_p$ son los ideales principales*

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \nu_p(x) \geq n\} ,$$

con $n \geq 0$.

Demostración. Sea $\mathfrak{a} \neq \langle 0\rangle$ un ideal de $\mathbb{Z}_p$ y $x = p^m u u \in \mathbb{Z}_p^*$, un elemento del ideal $\mathfrak{a}$ con m lo más pequeño posible, esta se puede elegir así; pues $|x|_p \leq 1$, lo que implica que $m \geq 0$. Luego $\mathfrak{a} = p^m\mathbb{Z}_p$, pues $y = p^n u' \in \mathfrak{a}$ con $u' \in \mathbb{Z}_p^*$, implica que $n \geq m$, entonces $y = (p^{n-m}u')p^m \in p^m\mathbb{Z}_p$. □

Al principio de esta sección, definimos los enteros p-ádicos como las series formales

$$\sum_{\nu=0}^{\infty} a_\nu p^\nu, \quad 0 \leq a_\nu \leq p-1,$$

las cuales identificamos con las sucesiones

$$\bar{s}_n = s_n \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}, \quad n \in \mathbb{N},$$

donde los s_n eran las sumas parciales

$$s_n = \sum_{\nu=0}^{n-1} a_\nu p^{nu}.$$

El conjunto de estas sucesiones constituían el límite proyectivo

$$\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}.$$

luego nosotros podíamos ver a los enteros p-ádicos como elementos de este anillo.

Lema 1.1. *Para todo p primo y $n \geq 0$, existe el siguiente isomorfismo*

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Demostración. El homomorfismo

$$\mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$$

$$a \longmapsto a \bmod p^n\mathbb{Z}_p,$$

es suprayectivo y tiene como kernel a $p^n\mathbb{Z}$. De hecho, para todo $x \in \mathbb{Z}_p$, por la Proposición 1.3 existe un $a \in \mathbb{Z}$ tal que

$$|x-a|_p \leq \frac{1}{p^n},$$

dicho de otra manera $\nu_p(x-a) \geq n$. Por lo tanto, $x - a \in p^n\mathbb{Z}_p$ lo que implica que $x \equiv a \bmod p^n\mathbb{Z}_p$. Luego, tenemos el isomorfismo

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

□

Del Lema anterior se sigue que para cada $n \geq 1$, nosotros tenemos un homomorfismo suprayectivo

$$\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}.$$

Luego, es claro que la familia de estos homomorfismos induce un homomorfismo

$$\mathbb{Z}_p \longrightarrow \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

(Ver Apéndice B.1) Ahora veremos que es posible identificar nuestras dos definiciones dadas para $\mathbb{Z}_p$ vía la siguiente Proposición

Proposición 1.6. *El homomorfismo*

$$\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

es un isomorfismo.

Demostración. Si $x \in \mathbb{Z}_p$ va al cero, significa que $x \in p^n\mathbb{Z}_p$ para toda $n \geq 1$. Es decir,

$$|x|_p \leq \frac{1}{p^n},$$

para toda $n \geq 1$, lo que implica que $|x|_p = 0$ y entonces $x = 0$. Esto prueba la inyectividad.

Un elemento de $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ esta dado por una sucesión de sumas parciales

$$s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu, \quad 0 \leq a_\nu \leq p-1.$$

Como vimos anteriormente, esta es una sucesión de Cauchy en $\mathbb{Z}_p$, la cual converge a un elemento

$$x = \sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p.$$

Como

$$x - s_n = \sum_{\nu=n}^{\infty} a_\nu p^\nu \in p^n\mathbb{Z}_p,$$

uno tiene que $x \equiv s_n \bmod p^n$ para toda n, i.e. x es mapeado por el elemento de $\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$ que es definido por la sucesión $\{s_n\}$ lo que muestra la suprayectividad. □

Debemos notar que los elementos del lado derecho del isomorfismo

$$\mathbb{Z}_p \cong \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}.$$

están dados por series formales de sumas parciales

$$s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu, \quad n \in \mathbb{N}.$$

Mientras que en el lado izquierdo estas sucesiones convergen con respecto al valor absoluto p-ádico y muestran a los elementos de $\mathbb{Z}_p$ en el sentido usual como series convergentes

$$x = \sum_{\nu=0}^{\infty} a_\nu p^\nu.$$

Una ventaja de definir a los números p-ádicos como un espacio métrico es que $\mathbb{Q}_p$ se convierte en automático en un grupo topológico, el cual tiene una vecindad compacta al rededor de la identidad (a saber $\mathbb{Z}_p$). Luego dado que cualquier grupo topológico es homogéneo tenemos una vecindad compacta para todo punto en $\mathbb{Q}_p$ y por lo tanto $\mathbb{Q}_p$ es localmente compacto (Ver Apéndice A).

Definición 1. Una *valuación* de un campo K es una función

$$|\cdot| : K \longrightarrow \mathbb{R}$$

tal que para toda $x, y \in K$ cumple que

- $|x| \geq 0$, y $|x| = 0$ si y solo si $x = 0$,
- $|xy| = |x|\,|y|$,
- $|x + y| \leq |x| + |y|$.

El valor absoluto usual $|\cdot|_\infty$ en $\mathbb{Q}$ es el primer ejemplo de valuación. Otro ejemplo, es el valor absoluto p-ádico $|\cdot|_p$, el cual definimos en párrafos anteriores.

Se dice que un valor absoluto en K es trivial si cumple que $|x| = 1$ para toda $x \neq 0$ y $|0| = 0$.

Definiendo la distancia entre dos puntos $x, y \in K$ como

$$d(x, y) = |x - y|,$$

tenemos que K es un espacio métrico, y en particular un espacio topológico.

Diremos que dos valuaciones $|\cdot| = |\cdot|'$ son *equivalentes* si definen la misma topología, o equivalentemente, si existe una constante $s \in \mathbb{R}$, $s > 0$, tal que $|a|' = |a|^s$, para toda $a \in K$.

La valuación $|\cdot|$ es llamada *valuación no arquimediana* si $|n|$ es acotada para toda $n \in \mathbb{N}$, o equivalentemente, si satisface la propiedad

$$|x+y| \leq \max\{|x|, |y|\}.$$

En otro caso diremos que $|\cdot|$ es una *valuación arquimediana*.

Teorema 1.1 (Ostrowski)**.** *Toda valuación no trivial de $\mathbb{Q}$ es equivalente a una de las valuaciones $|\cdot|_p$ o $|\cdot|_\infty$.*

Demostración. Sea $\|\cdot\|$ una valuación no arquimediana de $\mathbb{Q}$. Luego

$$\|n\| = \|1 + \cdots + 1\| \leq 1,$$

y existe un número primo p tal que $\|p\| < 1$, de lo contrario, de la factorización única en primos, tendríamos que $\|x\| = 1$ para toda $x \in \mathbb{Q}^*$. Luego, $\|\cdot\|$ seria una valuación trivial. El conjunto

$$\mathfrak{a} = \{a \in \mathbb{Z} : \|a\| < 1\},$$

es un ideal de $\mathbb{Z}$ el cual cumple que $p\mathbb{Z} \subseteq \mathfrak{a} \neq \mathbb{Z}$. Luego, como $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$ tenemos que $\mathfrak{a} = p\mathbb{Z}$. Ahora si $a \in \mathbb{Z}$ y $a = bp^m$ con $(b,p) = 1$, de modo que $b \notin \mathfrak{a}$, entonces $\|b\| = 1$ y por lo tanto

$$\|a\| = \|p\|^m = |a|_p^s,$$

donde $s = -\log\|p\| / \log p$. En consecuencia $\|\cdot\|$ es equivalente a $|\cdot|_p$.

Ahora, sea $\|\cdot\|$ una valuación arquimediana de $\mathbb{Q}$. Entonces tenemos que, para cualesquiera dos números naturales $n, m > 1$,

$$\|m\|^{1/\log m} = \|n\|^{1/\log n}.$$

De hecho, podemos escribir

$$m = a_0 + a_1 n + \cdots + a_r n^r,$$

donde $0 \leq a_i \leq n-1$ y $n^r \leq m$. Por lo tanto, observando que $r \leq \log m / \log n$, pues

$$\|n\|^r \leq \|m\| = \|n\|^{\log m/\log n},$$

y que

$$\|a_i\| = \|1 + \cdots + 1\| \leq a_i \|1\| \leq n,$$

tenemos la siguiente desigualdad

$$\|m\| \leq \sum \|a_i\| \cdot \|n\|^i \leq \sum \|a_i\| \cdot \|n\|^r \leq \left(1 + \frac{\log m}{\log n}\right) n \cdot \|n\|^{\log m/\log n}.$$

Poniendo m^k en lugar de m en la desigualdad anterior y sacando raíz k-ésima en ambos lados

$$\|m\| \leq \left(1 + \frac{k\log m}{\log n}\right)^{1/k} n^{1/k} \cdot \|n\|^{\log m/\log n}.$$

Ahora si hacemos tender k a ∞ tenemos

$$\|m\| \leq \|n\|^{\log m/\log n},$$

o

$$\|m\|^{1/\log m} \leq \|n\|^{1/\log n}.$$

Cambiando los papeles de m y n se obtiene la identidad

$$\|m\|^{1/\log m} = \|n\|^{1/\log n}.$$

Poniendo $c = \|n\|^{1/\log n}$ tenemos que $\|n\| = c^{\log n}$, luego si escribimos a $c = e^s$, esto induce, para cada numero racional positivo $x = \dfrac{a}{b}$, una valuación

$$\|x\| = e^{s\log x} = |x|_\infty^s.$$

Por lo tanto $\|\cdot\|$ es equivalente al valor absoluto usual $|\cdot|_\infty$ en $\mathbb{Q}$. □

1.2 Espacios Vectoriales Localmente Compactos Sobre $\mathbb{Q}_p$

Sea V un $\mathbb{Q}_p$-espacio vectorial. Una *norma* en V, es un mapeo

$$\|\cdot\| : V - \{0\} \longrightarrow \mathbb{R}_{>0}$$

que se extiende a cero definiendo $\|0\| = 0$ y satisface las siguientes propiedades:

i) $\|ax\| = |a|\,\|x\|$ $(|\cdot| = |\cdot|_p,\ a \in \mathbb{Q}_p,\ x \in V)$.

ii) $\|x+y\| \leq \max\{\|x\|, \|y\|\}$ $(x, y \in V)$ (*i.e.* es ultramétrica).

Un $\mathbb{Q}_p$-*espacio vectorial normado* V, es simplemente un $\mathbb{Q}_p$-espacio vectorial equipado con una norma $\|\cdot\|$ $(V, \|\cdot\|)$. Esta norma define una topología en V, luego V se convierte en un grupo topológico con la adición. Además, la multiplicación por escalar

$$V \longrightarrow V$$
$$x \longmapsto ax$$

con $x \in V$ y $a \in \mathbb{Q}_p^*$ es un homeomorfismo.

Sea $V = \mathbb{Q}_p^n$ para algún entero positivo n. Luego para cada $x \in V$, definimos

$$\|x\|_\infty = \max_{1\leq i\leq n} |x_i|.$$

Esto define una norma ultramétrica en V la cual es conocida como la *norma infinita*.

Dos normas $\|\cdot\|$ y $\|\cdot\|'$ en V son *equivalentes* si existe un isomorfismo bicontinuo entre $(V, \|\cdot\|)$ y $(V, \|\cdot\|')$ o equivalentemente, si existen dos constantes $0 < c \leq C < \infty$, tal que

$$c\,\|x\| \leq \|x\|' \leq C\,\|x\|.$$

Teorema 1.2. *Sea V un $\mathbb{Q}_p$-espacio vectorial de dimensión finita. Entonces, todas las normas en V son equivalentes.*

Demostración. Sea $V = \mathbb{Q}_p^n$ con la norma infinita $\|\cdot\|_\infty$. Mostraremos que existe un isomorfismo bicontinuo de $(\mathbb{Q}_p^n, \|\cdot\|_\infty)$ en cualquier $\mathbb{Q}_p$-espacio vectorial normada $(V, \|\cdot\|)$ de dimensión n.

Sea (e_i) una base de V, con $i = 1, \cdots, n$ y $x = (x_i) \in V$. Definimos el mapeo

$$\varphi : \mathbb{Q}_p^n \to V$$

$$x \mapsto \sum x_i e_i,$$

el cual claramente es un isomorfismo algebraico. Así que basta ver que φ es un isomorfismo bicontinuo. Notemos que

$$\left\| \sum x_i e_i \right\| \leq \max \|x_i e_i\| = \max |x_i| \, \|e_i\| \leq \max \|e_i\| \cdot \max |x_i| = C \|x\|_\infty ,$$

donde $C = \max \|e_i\|$. Entonces, $\|\varphi(x)\| \leq C \|x\|_\infty$ luego φ es continuo. Finalmente, mostraremos que φ es un mapeo abierto.

Sea

$$B = \left\{ x \in \mathbb{Q}_p^n : \|x\|_\infty \leq 1 \right\},$$

la bola unitaria en $\mathbb{Q}_p^n$. Luego, tenemos que mostrar que $\varphi(B)$ contiene una bola abierta centrada en 0 de radio positivo en V.

Sea S_1 la esfera unitaria

$$S_1 = \left\{ x \in \mathbb{Q}_p^n : \|x\|_\infty = 1 \right\},$$

en $\mathbb{Q}_p^n$. Notemos que, S_1 es un subconjunto cerrado del conjunto compacto B, por lo tanto, S_1 es compacto. Lo que implica que $\varphi(S_1)$ es compacto. Como φ es biyectiva, $\varphi(S_1)$ no contiene al 0 de V. Por lo tanto, la distancia de 0 a $\varphi(S_1)$ es positiva y el mínimo es alcanzado por algún punto $\varphi(x_0)$, *i.e.* si $x \in S_1$ tenemos que

$$\|\varphi(x)\| \geq \|\varphi(x_0)\| = \epsilon > 0.$$

Si $v \in V - \{0\}$ tiene norma $\|v\| < \epsilon$ y λv un múltiplo de v, con $|\lambda| \leq 1$, Entonces tenemos que $\|\lambda v\| < \epsilon$. En particular, si $\|v\| < \epsilon$, $\lambda \in \mathbb{Q}$ y $|\lambda| \leq 1$, se tiene que $\lambda v \notin \varphi(S_1)$.

Como $\{e_i\}$ es una base de V, podemos escribir

$$v = \sum v_i e_i = \varphi((v_i)).$$

Sin pérdida de generalidad

$$0 \neq |v_n| = \max |v_i| = \|(v_i)\|_\infty .$$

Definiendo a $\lambda = 1/v_n$ tenemos que $\lambda v = \varphi((v_i/v_n)) = \varphi(w) \in \varphi(S_1)$. Lo que muestra que el escalar λ satisface $|\lambda| > 1$, de modo que

$$\|(v_i)\|_\infty = |v_n| = \frac{1}{|\lambda|} < 1.$$

Por lo tanto, $v = \varphi((v_i))$ con $\|(v_i)\|_\infty < 1$, luego se tiene que $v \in \varphi(B)$. En consecuencia

$$B_{<\epsilon}(V) \subset \varphi(B),$$

donde $B_{<\epsilon}(V)$ es la bola de radio ϵ con centro en 0 en V. □

Corolario 1.2. *Sea V y W dos $\mathbb{Q}_p$-espacios vectoriales normados, entonces cualquier mapeo lineal $T : V \to W$ es continuo.*

Corolario 1.3. *Un isomorfismo algebraico de $\mathbb{Q}_p$-espacios vectoriales de dimensión finita es bicontinuo.*

Corolario 1.4. *Sea V un $\mathbb{Q}_p$-espacio vectorial de dimensión finita. Un subconjunto $S \subset V$ que es acotado con respecto a una norma en V es acotada con respecto a cualquier otra norma en V.*

Lema 1.2. *El único $\mathbb{Q}_p$-espacio vectorial normado compacto, es el trivial $\{0\}$.*

Demostración. Sea $x \in \mathbb{Q}_p$ distinto de cero. Luego, x genera una línea y la norma es una función continua no acotada en esa línea ya que

$$\|\lambda x\| = |\lambda| \, \|x\| ,$$

donde $\lambda \in \mathbb{Q}_p$. Lo cual muestra que el único $\mathbb{Q}_p$-espacio vectorial normado compacto es el trivial $\{0\}$. □

Teorema 1.3. *Todo $\mathbb{Q}_p$-espacio vectorial normado V, que es localmente compacto, es de dimensión finita.*

Demostración. Sea Ω una vecindad compacta de 0 en V y escojamos un escalar $a \in \mathbb{Q}_p$ con $0 < |a| < 1$ (por ejemplo $a = p$ con $|a| = 1/p$). Notemos que, los *interiores* de las traslaciones $x + a\Omega$ $(x \in V)$ cubren todo el espacio. Luego, a fortiori existe una cubierta finita de Ω de la forma

$$\Omega \subset \bigcup_{\text{finta}} (a_i + a\Omega).$$

Sea L el subespacio de dimensión finita generado por los a_i. Luego este subespacio de dimensión finita es isomorfo a un espacio normado $\mathbb{Q}_p^d$ y por lo tanto, es completo. En consecuencia este subespacio L es cerrado, y en el espacio cociente Hausdorff V/L(Ver Apéndice A), la imagen A del conjunto Ω es una vecindad compacta de 0 que satisface

$$A \subset aA \quad (\text{ o } a^{-1}A \subset A),$$

por consiguiente, $a^{-n}A \subset A$ por inducción. Como, $|a^{-n}| \to \infty$, tenemos que

$$A \subset V/L \subset \bigcup_{n \geq 1} a^{-1}A \subset A.$$

En particular como V/L es compacto, por el Lema 1.2, $V/L = 0$, entonces $V = L$ es de dimensión finita. □

Corolario 1.5. *En un $\mathbb{Q}_p$-espacio vectorial normado localmente compacto, los subconjuntos compactos son cerrados y acotados.*

Demostración. Los subconjuntos compactos de cualquier espacio métrico son cerrados y acotados, por continuidad de la función distancia. Recíprocamente, si V es un $\mathbb{Q}_p$-espacio vectorial normado localmente compacto, este es de dimensión finita y su norma es equivalente a la norma del supremo. Pero en $\mathbb{Q}_p^n$ todo conjunto acotado está contenido en un (compacto) producto de bolas de $\mathbb{Q}_p$. Luego los conjuntos cerrados y acotados son subconjuntos compactos de $\mathbb{Q}_p^n$. □

Sea $K/\mathbb{Q}_p$ una extensión finita del campo $\mathbb{Q}_p$. Podemos considerar a K como un $\mathbb{Q}_p$-espacio vectorial de dimensión finita. Luego, cada valuación en K que extiende el valor absoluto p-ádico de $\mathbb{Q}_p$ es una norma en este $\mathbb{Q}_p$-espacio vectorial. Por lo que, podemos aplicar todos los resultados para $\mathbb{Q}_p$-espacios vectoriales vistos anteriormente.

Lema 1.3. *Existe a lo más una valuación en K que extiende el valor absoluto p-ádico de $\mathbb{Q}_p$.*

Demostración. Sea $|\cdot|$ y $|\cdot|'$ dos valuaciones en K que extienden el valor absoluto de $\mathbb{Q}_p$. Estas dos normas deben ser equivalentes. Luego, existen constantes $0 < c \leq C < \infty$ tal que

$$c\,|x| \leq |x|' \leq C\,|x| \quad (x \in K).$$

Remplazando a x por x^n en las desigualdades anteriores tenemos que

$$c\,|x^n| \leq |x^n|' \leq C\,|x^n|\,.$$

Por la multiplicidad de la valuación, se tiene que

$$c\,|x|^n \leq |x|'^n \leq C\,|x|^n\,,$$

o

$$c^{1/n}\,|x| \leq |x|' \leq C^{1/n}\,|x|\,.$$

Haciendo tender n a ∞, $c^{1/n} \to 1$ y $C^{1/n} \to 1$. Lo cual demuestra que $|\cdot| = |\cdot|'$. □

Consideremos K una extensión de Galois de $\mathbb{Q}_p$ y supongamos que el valor absoluto p-ádico de $\mathbb{Q}_p$ se extiende a una valuación en K. Luego para cada automorfismo σ de $K/\mathbb{Q}_p$, podemos considerar la valuación $|x|' = |\sigma x|$. Por la Proposición anterior, esta valuación debe coincidir con la valuación original. Sea $G = \mathrm{Gal}(K/\mathbb{Q}_p)$ y para cada $x \in K$, consideremos el elemento

$$N_p(x) = \prod_{\sigma \in G} \sigma x \in \mathbb{Q}_p,$$

luego, se tiene que

$$|N_p(x)| = \left| \prod_{\sigma \in G} \sigma x \right| = \prod_{\sigma \in G} |\sigma x| = |x|^n\,,$$

donde $n = |G| = [K : \mathbb{Q}_p] = \dim_{\mathbb{Q}_p}(K)$,

$$|x| = |N_p(x)|^{1/n}.$$

Como $N(x) \in \mathbb{Q}_p$, esta fórmula nos da una expresión explicita de como extender el valor absoluto de $\mathbb{Q}_p$.

Consideremos como antes K una extensión finita de grado n del campo $\mathbb{Q}_p$. La *norma* de $x \in K$ es un homeomorfismo multiplicativo

$$N_p : K^* \longrightarrow \mathbb{Q}_p^*$$

$$x \longmapsto N_p(x),$$

el cual coincide con la n-ésima potencia de $\mathbb{Q}_p^*$(Ver Apéndice E).

Teorema 1.4. *Sea K un una extensión finita de grado n sobre $\mathbb{Q}_p$. Para cada $x \in K$, sea T_x el $\mathbb{Q}_p$-operador lineal $y \to xy$ en K. Entonces*

$$f(x) = |N_p(x)|^{1/n} = |\det T_x|^{1/n},$$

define una valuación en K que extiende un valor absoluto p-ádico. Además, esta es la única valuación en K con esta propiedad.

Demostración. Si $a \in \mathbb{Q}_p$, es claro que $N_p(a) = a^n$, por lo tanto,

$$|N_p(a)|^{1/n} = |a|,$$

lo que muestra que la fórmula propuesta es una extensión del valor absoluto p-ádico. La multiplicatividad

$$f(xy) = f(x) \cdot f(y),$$

se sigue de la multiplicatividad del determinante. Veamos ahora, que se cumple la desigualdad ultramétrica. Para esto usaremos que K es localmente compacto, pues $\mathbb{Q}_p$ es localmente compacto y K es isomorfo a un producto finito de copias de $\mathbb{Q}_p$. Tomemos una norma arbitraria $\|\cdot\|$ en K. Por ejemplo, consideremos una base $e_1, \cdots, e_n$ de K sobre $\mathbb{Q}_p$ y usemos la norma infinita en los componentes de la base. Como la función continua f no se anula en el conjunto compacto

$$S_n = \{x \in K : \|x\| = 1\},$$

entonces f, es acotada tanto por arriba como por abajo en S_n, i.e.

$$0 < \epsilon \leq f(x) \leq A < \infty \quad (\|x\| = 1).$$

Para $x \in K^*$ elijamos $\lambda \in \mathbb{Q}_p$ con $\|x\| = |\lambda|$. Luego, el vector x/λ tiene norma 1,

$$\epsilon \leq f(x/\lambda) \leq A \quad (x \neq 0),$$

y como $f(x/\lambda) = f(x)/|\lambda|$,

$$\epsilon |\lambda| \leq f(x) \leq A |\lambda| \quad (x \neq 0),$$
$$\epsilon \|x\| \leq f(x) \leq A \|x\| \quad (x \neq 0).$$

Ahora, tomando $a = \epsilon^{-1}$ tenemos que

$$\|x\| \leq a f(x) \text{ y } f(x) \leq A \|x\|.$$

Supongamos que $f(x) \leq 1$ y por lo tanto $\|x\| \leq a$. Entonces, podemos inferir

$$\begin{aligned} f(1+x) &\leq A \|1+x\| \leq A \max\{\|1\|, \|x\|\}, \\ &\leq A \max\{\|1\|, a\} = C \max\{f(1), f(x)\}. \end{aligned}$$

De manera más general, si $f(y) \geq f(x)$, podemos dividir por y y aplicar la anterior desigualdad a x/y, ya que $f(x/y) = f(x)/f(y) \leq 1$, tenemos

$$f(1 + x/y) \leq C \max\{f(1), f(x/y)\}.$$

Por último, multiplicando en ambos lados por $f(y)$, obtenemos la desigualdad general

$$f(x+y) \leq C \max\{f(x), f(y)\}.$$

Lo cual prueba que f es una valuación. Además, como f extiende el valor absoluto p-ádico, f es acotada, luego es una valuación no arquimediana. Por lo tanto, la existencia y unicidad de una valuación en $K/\mathbb{Q}_p$ quedan probadas. □

Dado que existe una única extensión del valor absoluto p-ádico de $\mathbb{Q}_p$ a una valuación f en $K/\mathbb{Q}_p$, haciendo un abuso de notación, denotaremos a f como $|\cdot|_p$.

Recordemos, de la sección anterior, que $\mathbb{Z}_p$ es un anillo local con ideal maximal

$$p\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p : |x|_p < 1 \right\},$$

y que sus ideales son, los ideales principales

$$p^n\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p : |x|_p < p^{-n}, \text{ con } n \in \mathbb{N} \cup \{0\} \right\}.$$

Sea K una extensión finita de $\mathbb{Q}_p$ y sea O_p el conjunto de todas las $x \in K$ que satisfacen una ecuación de la forma $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ con $a_i \in \mathbb{Z}_p$, i.e. O_p es la cerradura algebraica de $\mathbb{Z}_p$ en K. Luego el siguiente resultado generaliza la noción de anillo de enteros $\mathbb{Z}_p$ de $\mathbb{Q}_p$ a un anillo O_p en $K/\mathbb{Q}_p$.

Proposición 1.7. *Sea K una extensión finita de $\mathbb{Q}_p$ de grado n y sea*

$$O_p = \left\{ x \in K : |x|_p \leq 1 \right\},$$
$$M = \left\{ x \in K : |x|_p < 1 \right\}.$$

Entonces O_p es un anillo el cual es la cerradura entera de $\mathbb{Z}_p$ en K, M es el único ideal maximal, y O_p/M es una extensión finita de $\mathbb{F}_p$ de grado a lo más n.

Demostración. De la aditividad y multiplicatividad de la norma ultramétrica, es claro que O_p es un anillo y M un ideal en O_p. Sea $\alpha \in K$ de grado m sobre $\mathbb{Q}_p$ y supongamos que α es entero sobre $\mathbb{Z}_p$, i.e. $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$, con $a_i \in \mathbb{Z}_p$. Si $|\alpha| > 1$, tendríamos:

$$|\alpha|_p^m = |\alpha^m|_p = \left|a_1\alpha^{m-1} + \cdots + a_m\right|_p \leq \max_{1\leq i\leq m} \left|a_i\alpha^{m-i}\right|_p$$

$$\leq \max_{1\leq i\leq m} \left|\alpha^{m-i}\right|_p = |\alpha|_p^{m-1}.$$

lo cual es una contradicción. Ahora, si $|\alpha|_p \leq 1$. Entonces, para todos los conjugados de $\alpha = \alpha_1$ sobre $\mathbb{Q}_p$ se tiene que

$$|\alpha_i|_p = \prod_{j=1}^{m} |\alpha_j|_p^{1/m} = |\alpha|_p,$$

ya que todos los coeficientes del polinomio mónico irreducible de α son sumas o diferencias de productos de α_i, luego se sigue que todos los coeficientes tienen norma $|\cdot|_p \leq 1$. Como estos están en $\mathbb{Q}_p$ entonces deben estar en $\mathbb{Z}_p$.

Ahora veremos que M contiene a todos los ideales de O_p. Supongamos que $\alpha \in O_p$ y $\alpha \notin M$. Luego $|\alpha|_p = 1$, de modo que $|1/\alpha|_p = 1$ y $1/\alpha \in O_p$. Luego todo ideal que contiene a α debe contener a $(1/\alpha)\alpha = 1$, lo cual es imposible.

Notemos que $M \cap \mathbb{Z}_p = p\mathbb{Z}_p$ lo cual se sigue de la definición. Consideremos el campo O_p/M. Recordemos que sus elementos son clases laterales izquierdas $a + M$ y notemos que si a y b están en $\mathbb{Z}_p$, entonces $a + M$ y $b + M$ están en la misma clase si y solo si $a - b \in M \cap \mathbb{Z}_p = p\mathbb{Z}_p$. Luego, existe una inclusión natural de $\mathbb{Z}_p/p\mathbb{Z}_p$ en O_p/M dado por el mapeo de clases $a+p\mathbb{Z}_p \mapsto \bar{a}+M$ para $a \in \mathbb{Z}_p$. Como $\mathbb{Z}_p/p\mathbb{Z}_p$ es el campo $\mathbb{F}_p$ de p elementos, esto significa que O_p/M es una extensión del campo $\mathbb{F}_p$.

Ahora, veamos que O_p/M es de grado finito sobre $\mathbb{F}_p$, de hecho, veremos que

$$[O_p/M : \mathbb{F}_p] \leq [K : \mathbb{Q}_p].$$

Si $n = [K : \mathbb{Q}_p]$ mostraremos que cualesquiera $n+1$ elementos $\bar{a}_1, \bar{a}_2, \cdots, \bar{a}_{n+1} \in O_p/M$ deben ser linealmente dependientes sobre $\mathbb{F}_p$. Para $i = 1, 2, \cdots, n+1$, sea a_i cualquier elemento en O_p que se mapea en $\bar{a}_i$ bajo la proyección $O_p \to O_p/M$. Como $[K : \mathbb{Q}_p] = n$, tenemos que $a_1, a_2 \cdots, a_{n+1}$ son linealmente dependientes sobre $\mathbb{Q}_p$:

$$a_1b_1 + a_2b_2 + \cdots + a_{n+1}b_{n+1} = 0, \quad b_i \in \mathbb{Q}_p.$$

Multiplicando por una potencia de p adecuada, podemos suponer que todos los $b_i \in \mathbb{Z}_p$, pero que al menos un $b_i \notin p\mathbb{Z}_p$. Entonces la imagen de la expresión anterior en O_p/M es

$$\bar{a}_1\bar{b}_1 + \bar{a}_2\bar{b}_2 + \cdots + \bar{a}_{n+1}\bar{b}_{n+1} = 0,$$

donde $\bar{b}_i$ es la imagen de b_i in $\mathbb{Z}_p/p\mathbb{Z}_p$. Como al menos algún b_i no está en $p\mathbb{Z}_p$. Se tiene que al menos un $\bar{b}_i$ no es 0, luego $\bar{a}_1, \bar{a}_2, \cdots, \bar{a}_{n+1}$ son linealmente dependientes. □

El campo O_p/M es llamado el *campo de residuos* de K. El cual es una extensión de $\mathbb{F}_p$ de grado finito, y O_p es llamado el *anillo de valuación* o *anillo de enteros* de $|\cdot|_p$ en K.

1.3 Medida de Haar

Para un estudio más detallado sobre la medida de Haar ver [13]. Una colección M de subconjuntos de un conjunto X es llamado una *σ-álgebra* si satisface las siguientes condiciones:

- $X \in M$,
- Si $A \in M$ entonces $A^c \in M$ donde A^c denota el complemento de A en X.
- Supongamos que $A_n \in M$ $(n \geq 1)$ y sea

$$A = \bigcup_{n=1}^{\infty} A_n,$$

entonces $A \in M$, *i.e.* M es cerrado bajo uniones numerables.

De estos axiomas se sigue fácilmente que el conjunto vació está en M y que M es cerrado bajo intersecciones finitas y numerables.

Un conjunto X con una σ- álgebra de subconjuntos M es llamado un *espacio medible*. Si además, X cumple la propiedad de ser espacio topológico entonces podemos considerar la más pequeña de las σ-álgebras $\mathcal{B}$ que contiene a todos los conjuntos abiertos de X. Los elementos del conjunto $\mathcal{B}$ son llamados *subconjuntos de Borel* de X.

Una medida positiva μ en un espacio medible arbitrario (X, M) es una función $\mu : M \to R_{\geq 0} \cup (\infty)$ que es numerablemente aditiva, i.e.

$$\mu(\bigcup_{n=1}^{\infty} A_n) = \sum_{n=1}^{\infty} \mu(A_n),$$

donde $\{A_n\}$ es una familia de conjuntos ajenos en M. En particular, una medida positiva definida en los conjuntos de Borel de un espacio Hausdorff localmente compacto X, es llamada *medida de Borel*.

Sea μ una medida de Borel en un espacio localmente compacto Hausdorff X y sea E un subconjunto de Borel de X. Diremos que μ es *regular exterior* en E si

$$\mu(E) = \inf \{\mu(U) : E \subseteq U,\ U \text{ abierto}\}.$$

Y diremos que es regular interior en E si:

$$\mu(E) = \sup \{\mu(K) : K \subseteq E,\ K \text{ compacto}\}.$$

Una *medida de Radon* en X es una medida de Borel que es finita sobre los conjuntos compactos, regular exterior en todos los conjuntos de Borel y regular interior en todos los conjuntos abiertos. Además, se puede demostrar que la medida de Radon es, regular interior en los conjuntos σ-$finitos$ (*i. e.* unión numerable de conjuntos μ-*medibles* de medida finita).

Sea G un grupo topológico y sea μ una medida de Borel en G. Diremos que μ es *traslación invariante por la izquierda* si para cada subconjunto de Borel E de G,

$$\mu(sE) = \mu(E),$$

para toda $s \in G$. La propiedad de ser *traslación invariante por la derecha* se define de manera análoga.

Definición 2. Sea G un grupo topológico localmente compacto. Entonces una *medida de Haar izquierda (*resp. *derecha)* en G, es una medida de Radon μ en G, distinta de cero, que además es una traslación invariante por la izquierda (resp. por la derecha). Una *medida de Haar bi-invariante* es una medida de Radon distinta de cero e invariante tanto por la izquierda como por la derecha.

Teorema 1.5. *Sea G un grupo localmente compacto, entonces G admite una medida de Haar izquierda (resp. derecha) además esta medida es única salvo multiplicación por escalares.*

Demostración. Una demostración de este resultado puede ser leída en [2]. □

Proposición 1.8. *Sea G un grupo localmente compacto con medida de Radon μ distinta de cero. Luego si μ es una medida de Haar izquierda en G entonces μ es positiva en todos los subconjuntos no vacíos de G y*

$$\int_G f d\mu > 0,$$

para toda $f \in \mathcal{C}_c^+(G)$, donde

$$\mathcal{C}_c^+(G) = \{f \in \mathcal{C}_c(G) : f(s) \geq 0 : \ \forall\ f(s) \in G \ y \ \|f\|_u > 0\}.$$

1.4 Módulo de un Automorfismo

En el estudio de los campos locales y en particular su clasificación, es esencial el concepto de módulo de un automorfismo. En esta sección estudiaremos este concepto para, posteriormente, dar una clasificación de los campos locales de característica 0. En esta y la siguiente sección, usaremos fuertemente las propiedades básicas de grupos topológicos las cuales pueden ser consultadas en el Apéndice A. Cabe mencionar que nuestro estudio de campos locales sigue la línea de André Well [5]. Otra cita que puede ser consultada para esta sección es [2].

Sea G un grupo localmente compacto abeliano con una medida de Haar[1] μ y consideremos un automorfismo (continuo) α de G. Si X es un subconjunto de Borel de G, entonces αX lo es y además $\mu \circ \alpha$ es una medida de Haar en G. Luego por la unicidad de la media de Haar $\mu \circ \alpha = c\mu$ para alguna constante positiva $c \in \mathbb{R}$. El factor constante c, el cual es claramente independiente de μ, es llamado el *módulo de* α y denotado $\mathrm{mod}_G(\alpha)$. Luego se sigue de la definición que

$$\mu(\alpha X) = \mathrm{mod}_G(\alpha)\mu(X).$$

Un campo K, sujeto a una topología dada, es llamado un *campo topológico* si la adición y multiplicación son continuas en $K \times K$. Un K-espacio vectorial V, sujeto a una topología dada, es llamado *K-espacio vectorial topológico* si las siguientes dos condiciones son satisfechas:

- El grupo aditivo $\langle V, + \rangle$ es un grupo topológico.
- El mapeo, multiplicación por escalar

$$K \times V \longrightarrow V$$

$$(\lambda, v) \longmapsto \lambda v,$$

  es continuo con respecto al producto topológico en $K \times V$.

En particular, si nuestro grupo es un campo localmente compacto K, que llamaremos mas brevemente *campo local*, cada $a \in K^*$ define un automorfismo continuo de K dado por

$$K^* \longrightarrow K^*$$

$$x \longmapsto ax,$$

luego podemos definir el módulo asociado a dicho automorfismo, el cual denotaremos por $\mathrm{mod}_K(a)$. Este, se puede extender a todo K definiendo $\mathrm{mod}_K(0) = 0$. De hecho, podemos generalizar esta idea a un K-espacio vectorial topológico V, donde cada automorfismo está dado por el mapeo $v \longmapsto av$, al cual le podemos asociar su módulo $\mathrm{mod}_V(a)$ y que, de igual manera, podemos extenderlo a todo V definiendo $\mathrm{mod}_V(0) = 0$.

Lema 1.4. *Dado K un campo local y $a, b \in K$ tenemos que:*

i) $\mathrm{mod}_K(ab) = \mathrm{mod}_K(a)\mathrm{mod}_K(b)$,

ii) $\mathrm{mod}_K(a^{-1}) = \mathrm{mod}_K(a)^{-1}$.

[1]Dado que G es abeliano la medida de Haar es izquierda y derecha por lo que solo nos referiremos a ella como medida de Haar.

Demostración. (i) Notemos que

$$\mu(abX) = \mu(a(bX)) = \mathrm{mod}_K(a)\mu(bX) = \mathrm{mod}_K(a)\mathrm{mod}_K(b)\mu(X),$$

por otro lado

$$\mu(abX) = \mu((ab)X) = \mathrm{mod}_K(ab)\mu(X),$$

luego como $\mu(X) > 0$, por la Proposición 1.8 podemos dividir todo entre $\mu(X)$, de donde se obtiene que

$$\mathrm{mod}_K(ab) = \mathrm{mod}_K(a)\mathrm{mod}_K(b).$$

(ii) La demostración de esta afirmación es equivalente a probar que

$$\mathrm{mod}_K(a^{-1})\mathrm{mod}_K(a) = 1.$$

Pero

$$\mu(X) = \mu((a^{-1}a)X) = \mathrm{mod}_K(a^{-1}a)\mu(X) = \mathrm{mod}_K(a^{-1})\mathrm{mod}_K(a)\mu(X),$$

luego, dividiendo todo entre $\mu(X)$ tenemos lo requerido. □

Proposición 1.9. *Sea K un campo localmente compacto con medida de Haar μ. Entonces $\mathrm{mod}_K : K \to \mathbb{R}_{\geq 0}$ es un homomorfismo continuo.*

Demostración. Por el Lema 1.4 tenemos que mod_K es un homomorfismo, así que solo falta probar la continuidad. Sea X una vecindad compacta de 0 en K. Como μ es regular exterior, para todo $a \in K$ y para cada $\epsilon > 0$ existe un abierto U, $aX \subseteq U$, tal que

$$\mu(U) \leq \mu(aX) + \epsilon,$$

Como la multiplicación es continua y X es compacto, existe una vecindad abierta W de a tal que $WX \subseteq U$. Luego $bX \subseteq U$ para todo $b \in W$. Entonces tenemos que

$$\mu(bX) \leq \mu(aX) + \epsilon,$$

que es equivalente a

$$\mathrm{mod}_K(b)\mu(X) \leq \mathrm{mod}_K(a)\mu(X) + \epsilon.$$

Luego, dividiendo entre $\mu(X)$ tenemos que

$$\mathrm{mod}_K(b) \leq \mathrm{mod}_K(a) + \mu(X)^{-1}\epsilon.$$

Por lo tanto, mod_K es continua en cero. Además, esto muestra que para toda x positivo la imagen inversa de $(0, x)$ bajo mod_K es abierta. Por el Lema 1.4 (ii) el siguiente diagrama conmuta

$$\begin{array}{ccc} K^* & \overset{\mathrm{mod}_K}{\to} & \mathbb{R}_{>0} \\ ()^{-1} \downarrow & & \downarrow ()^{-1} \\ K^* & \overset{\mathrm{mod}_K}{\to} & \mathbb{R}_{>0} \end{array}$$

luego, se sigue que para toda x positiva, la imagen inversa de (x, ∞) es abierta. Por lo tanto, la imagen inversa de todo intervalo abierto es abierta. Entonces mod_K es continuo. □

Corolario 1.6. *Sea K un campo local no discreto y sea U una vecindad abierta del cero. Entonces, para cada ϵ positivo existe $a \in U$ tal que $0 < \mathrm{mod}_K(a) < \epsilon$.*

Demostración. Notemos que la imagen inversa de $[0, \epsilon)$ es una vecindad abierta de cero. Luego, la intersección con U es también una vecindad abierta de cero. Además, K es no discreto, entonces la intersección contiene un elemento a distinto de cero, que por construcción tiene la propiedad requerida. □

A partir de aquí cuando hablemos de K nos referiremos a un campo local no discreto, ya que es trivial verificar que cualquier espacio topológico discreto es localmente compacto.

Proposición 1.10. *Sea K un campo local y sea m un número positivo definimos*

$$B_m = \{x \in K : \mathrm{mod}_K(x) \leq m\}.$$

Luego, B_m es compacto.

Demostración. Sea V una vecindad compacta de cero en K, y sea W una vecindad de cero tal que $WV \subset V$. Luego por el Corolario 1.6 existe $r \in W \cap V$ tal que $0 <\mathrm{mod}_K(r) < 1$ y por el Lema 1.4 (i) tenemos que

$$\mathrm{mod}_K(r^n) = \mathrm{mod}_K(r)^n < \mathrm{mod}_K(r),$$

entonces $r^n \in V$ para todo $n \geq 1$. Si r' es un punto límite de la sucesión $\{r^n\}_{n\geq 1}$, $\mathrm{mod}_K(r')$ debe ser cero, ya que $\mathrm{mod}_k(r^n)$ tiene límite 0 cuando n tiende a ∞. Luego la sucesión no puede tener otro punto límite más que el cero, pues está contenido en el conjunto compacto V, que tiene punto límite 0.

Ahora tomemos $m > 0$ y $a \in B_m$; como $r^n a$ tiende a cero, entonces existe un menor entero $\nu \geq 0$ tal que $r^\nu a \in V$; si a no está en V, entonces $r^{\nu-1}a \notin V$, luego multiplicando por r tenemos que $r^\nu a \in V - (rV)$.

Sea X la cerradura de $V - (rV)$, claramente X es compacto por ser un cerrado dentro de un compacto Hausdorff y además 0 no está en X. Luego si ponemos $\mu = \inf_{x\in X} \mathrm{mod}_K(x)$, tenemos que $\mu > 0$.

Sea N un entero tal que $\mathrm{mod}_K(r)^N \leq \mu/m$. Luego, si $a \in B_m$, $a \notin V$ y ν definida como antes, tenemos que

$$\mathrm{mod}_K(r)^N \cdot m \leq \mu \leq \mathrm{mod}_K(r^\nu a) = \mathrm{mod}_K(r)^\nu \mathrm{mod}_K(a) \leq \mathrm{mod}_K(r)^\nu \cdot m,$$

y como $0 < \mathrm{mod}(r) < 1$ debemos tener que $\nu \leq N$. Lo cual muestra que B_m está contenido en la unión de los conjuntos compactos, V, $r^{-1}V$, ..., $r^{-N}V$. Entonces, por la Proposición 1.9 tenemos que B_m es cerrado, luego como está dentro de un compacto Hausdorff, B_m es compacto. □

Corolario 1.7. *Para $a \in K$, $\lim_{n\to\infty} a^n = 0$ si y solo si $\mathrm{mod}_K(a) < 1$.*

Demostración. Si $\mathrm{mod}_K(a) < 1$, entonces los elementos a^n están en un compacto B_1 y además la sucesión $\{a^n\}$ converge. Por continuidad, el límite tiene módulo cero. El recíproco se sigue directamente de las propiedades de mod_K. □

Corolario 1.8. *Los conjuntos B_m constituyen un sistema fundamental de vecindades de cero en K.*

Demostración. Sea V una vecindad compacta de cero en K y tomemos

$$m > \sup_{x \in V} \mathrm{mod}_K(x),$$

de modo que $V \subset B_m$. Sea X la cerradura de $B_m - V$ y pongamos

$$m' = \inf_{x \in X} \mathrm{mod}_K(x) > 0.$$

Luego $0 \notin X$ y $X \subset B_m$. Entonces, por la Proposición 1.10 X es compacto, ya que X es cerrado y está en un compacto Hausdorff, y $0 < m' \leq m$. Por lo tanto, si escogemos $\gamma \in \mathbb{R}$ tal que $0 < \gamma \leq m'$; entonces $B_\gamma \subset B_{m'}$, $B_\gamma \cap X = \emptyset$ luego $B_\gamma \subset V$. □

Se dice que una función $F : \mathbb{N} \to \mathbb{R}$ es completamente multiplicativa si $F(mn) = F(m)F(n)$ para toda $m, n \in \mathbb{N}$.

Proposición 1.11. *Sea F una función completamente multiplicativa y supongamos que existe una constante A tal que*

$$F(m+n) \leq A \cdot \sup\{F(m), F(n)\},$$

para toda $m, n \in \mathbb{N}$. Entonces

i) $F(m) \leq 1$ para toda m, o

ii) $F(m) = m^\lambda$ para alguna constante positiva λ.

Demostración. Para una demostración ver [2] o [5]. □

Lema 1.5. *La función* mod_K *induce un homomorfismo abierto de K^* en un subgrupo cerrado Γ de $\mathbb{R}_{>0}$.*

Demostración. Sea Γ y Γ' las imágenes de K^* y K bajo el mapeo mod_K respectivamente. Claramente Γ es un subgrupo de $\mathbb{R}_{>0}$ y $\Gamma' = \Gamma \cup \{0\}$. Para cada $m > 0$, $\Gamma' \cap [0, m] = \mathrm{mod}_K(B_m)$, luego por las Proposiciones 1.9 y 1.10 la intersección es compacta y por tanto Γ' y Γ son cerrados en $\mathbb{R}_{\geq 0}$ y $\mathbb{R}_{>0}$ respectivamente.

Sea U el kernel de mod_K en K^* (*i.e.* el conjunto $\{x \in K : \mathrm{mod}_K(x) = 1\}$) y sea V una vecindad de 1 en K^* y V' su imagen bajo mod_K. A fin de probar que mod_K es un homomorfismo abierto de K^* en Γ, mostraremos que V' es vecindad de 1 en Γ. Supongamos que esto es falso, entonces existe una sucesión

$\{\gamma_n\} \in \Gamma - V'$ tal que $\lim\gamma_n = 1$. Para cada n, sea $a_n \in K^*$ tal que $\gamma_n = \mathrm{mod}_K(a_n)$. Por la Proposición 1.10, la sucesión $\{a_n\}$, tiene por lo menos un punto límite a. Luego, es claro $\mathrm{mod}_K(a) = 1$, es decir $a \in U$. Pero UV es una vecindad de U, por lo que existe algún n tal que $a_n \in UV$, luego $\gamma_n \in V'$. Lo cual, es una contradicción.

□

Teorema 1.6. *Sea K un campo local, no discreto con la medida de Haar μ entonces:*

i) Existe una constante positiva $A \geq 1$ tal que:

$$\mathrm{mod}_K(a+b) \leq A \cdot \sup\{\mathrm{mod}_K(a), \mathrm{mod}_K(b)\} \quad \forall a, b \in K.$$

ii) Si $A = 1$, entonces $\mathrm{mod}_K(K^*)$ es discreto.

Demostración. Definamos A por la fórmula

$$A = \sup_{b \in B_1} \{\mathrm{mod}_K(1+b)\}.$$

Como el supremo toma valores sobre un conjunto compacto (una traslación de B_1), entonces A es finito y mayor o igual que 1. Por otra parte, tomando $a = 1$ en la desigualdad del inciso (i) podemos ver que el número definido por está fórmula es claramente el menor valor positivo, para el cual la desigualdad establecida se mantiene.

Para mostrar que la desigualdad en (i) es valida para a y b, es suficiente considerar el caso en que cada a o b son distintos de cero. Supongamos que a es distinta de cero y que $\mathrm{mod}_K(b) \leq \mathrm{mod}_K(a)$(de otro modo b es distinta de cero y podemos cambiar los papeles de a y b). Luego, poniendo $c = a^{-1}b$, tenemos que $\mathrm{mod}_K(c) \leq 1$ y $a + b = a(1+c)$. Por construcción, $\mathrm{mod}_K(1+c) \leq A$ y por lo tanto

$$\begin{aligned} \mathrm{mod}_K(a+b) &= \mathrm{mod}_K(a)\mathrm{mod}_K(1+c) \leq A \cdot \mathrm{mod}_K(a) \\ &= A \cdot \sup\{\mathrm{mod}_K(a), \mathrm{mod}_K(b)\}. \end{aligned}$$

Con lo que queda demostrado (i). Supongamos $A = 1$ y sea U el interior de B_1, el cual obviamente contiene a cero. Entonces, mod_K mapea $1 + U$ en un subconjunto Γ que contiene a 1 y que también está contenido en $[0, 1]$. Esto muestra que $\mathrm{mod}_K(1+U)$ es la intersección de un subconjunto abierto de $\mathbb{R}$ con Γ. En particular, hay un intervalo abierto I que contiene a 1 cuya intersección con Γ está contenida en $[0, 1]$.

Sin embargo, 1 es un punto de acumulación por la izquierda de Γ si y solo si es un punto de acumulación por la derecha. Por lo tanto, no puede existir un intervalo I con estas características, amenos que 1 no sea punto de acumulación de Γ. Pero entonces el conjunto que consiste solo del 1 es abierto en Γ lo que nos dice que Γ tiene la topología discreta como queríamos. □

Si K satisface la desigualdad del Teorema 1.6 (i) de la Proposición anterior con $A = 1$, diremos que K (o mod_K) es *ultramétrico*, en este caso tenemos la siguiente desigualdad

$$\mathrm{mod}_K(a+b) = \sup\{\mathrm{mod}_K(a), \mathrm{mod}_K(b)\} \quad \forall a, b \in K,$$

a la cual llamaremos *desigualdad ultramétrica.*

1.5 Clasificación de los Campos Locales de Característica Cero

En esta sección mostraremos que los únicos campos locales de característica cero son $\mathbb{R}$, $\mathbb{C}$ o una extensión finita de $\mathbb{Q}_p$.

Para esto, enunciando algunas propiedades, sin demostrar, de los K-espacios vectoriales topológicos las cuales nos serán de utilidad en lo que sigue [2], [5].

Consideremos V un K-espacio vectorial topológico donde K es un campo local no discreto, y sea W un subespacio de V de dimensión finita n. Además, supongamos que W tiene una base $w_1, w_2, \ldots, w_n$.

Consideremos el mapeo

$$\varphi : K^n \longrightarrow W$$
$$(a_j) \longmapsto \sum a_j w_j.$$

Notemos que como φ es suma de funciones continuas, entonces se tiene que φ es un isomorfismo de K-espacios vectoriales topológicos.

Proposición 1.12. *Dado K, V, W y φ como antes, tenemos que φ es un isomorfismo de K-espacios vectoriales topológicos, además W es cerrado en V y localmente compacto.*

Proposición 1.13. *Todo K-espacio vectorial de dimensión finita, donde K es un campo local no discreto, puede ser equipado con una y solo una estructura de K-espacio vectorial topológico.*

Proposición 1.14. *Si V es un K-espacio vectorial topológico localmente compacto. Entonces V es de dimensión finita sobre K.*

Corolario 1.9. *Si V es un K-espacio vectorial topológico localmente compacto se cumple que*

$$\mathrm{mod}_V(a) = \mathrm{mod}_K(a)^{\dim(V)},$$

para toda $a \in K$.

Demostración. Como V es un K-espacio vectorial localmente compacto por la Proposición 1.14, V es de dimensión finita. Luego, por la Proposición 1.12 es suficiente probar el Corolario para $V = K^n$. Pero, por el Teorema de Fubini multiplicar por a(por la izquierda) en la medida de un subconjunto medible de K^n puede ser calculada iteradamente sobre cada una de las coordenadas. Luego, de esto se sigue que $\mathrm{mod}_V(a) = \mathrm{mod}_K(a)^{\dim(V)}$. □

Dado un campo local no discreto K, diremos que el *anillo primo* de K es un subanillo P de K que se define como

$$P_K = \{m \cdot 1_K \in K : m \in \mathbb{Z}\}.$$

Podemos notar que si $\text{char}(K) = p > 0$ entonces $p \cdot 1_K = 0$. En general para un campo local no discreto K nosotros podemos escribir $F(m \cdot 1_K) = \text{mod}_K(m \cdot 1_K)$. Luego de la Proposición 1.11 tenemos dos posibilidades para la función mod_K:

- $\text{mod}_K(m) \leq 1$ para toda m, o
- hay una constante positiva λ tal que $\text{mod}_K(m) = m^{\lambda}$.

Teorema 1.7. *Sea K un campo local no discreto de característica cero, entonces K es $\mathbb{R}$, $\mathbb{C}$ o una extensión finita de $\mathbb{Q}_p$.*

Demostración. Primero, dado que K es de característica 0 $\text{mod}_K(p) \neq 0$ para p primo, veamos ¿por qué? Supongamos que es falso entonces existe $p \in \mathbb{N}$ tal que $\text{mod}_K(p) = 0$ entonces como $\text{mod}_K(p) = \text{mod}_K(p \cdot 1_K)$ luego $p \cdot 1_K = \bar{0}$ pero esto nos diría que K es de característica p lo cual contradice el supuesto de que K era de característica 0. Por lo tanto, podemos escribir $\text{mod}_K(p) = p^{-t}$ con $t > 0$. Luego, dado que n se puede expresar como $n = mp^r$, con $(m, p) = 1$, tenemos que $\text{mod}_K(n) = |n|_p^t$ donde $|\cdot|_p$ es el valor absoluto $p-$ádico.

Sea $|\cdot|_\infty$ el valor absoluto usual en $\mathbb{R}$, entonces se tiene, en característica cero, que para todo $n \in \mathbb{N}$

$$\text{mod}_k(n) = |n|_\nu^t,$$

donde ν es un primo p o $\nu = \infty$.

Ahora, dado el siguiente isomorfismo algebraico

$$\mathbb{Z} \longrightarrow \mathbb{Z} \cdot 1_K$$

$$n \longmapsto n \cdot 1_K,$$

el cual es posible extender a un isomorfismo de

$$\mathbb{Q} \longrightarrow \mathbb{Q} \cdot 1_K \subseteq K$$

$$q \longmapsto q \cdot 1_K.$$

Luego, por lo visto al principio de la demostración, tenemos que mod_K induce un mapeo

$$x \mapsto |x|_p,$$

en $\mathbb{Q}$. Por el Corolario 1.8 el conjunto B_t constituye una base local de 0 en K. Luego, por la Proposición 1.13 la estructura topológica inducida en K es idéntica a la inducida por la función distancia $|x - y|_\nu$. Entonces, como K es localmente compacto la cerradura $\hat{\mathbb{Q}}$ de $\mathbb{Q}$ es precisamente la completación $\mathbb{Q}_\nu$ de $\mathbb{Q}$ en K con respecto a la métrica ν (Ver Apéndice A.2), por tanto $\hat{\mathbb{Q}} \cong \mathbb{Q}_\nu$ (como campos localmente compactos), luego por la Proposición 1.9, $\mathbb{Q}_\nu$ es de dimensión finita sobre K. Entonces si $\nu = \infty$, K es una extensión finita de $\mathbb{R}$ y por lo tanto es $\mathbb{R}$ o $\mathbb{C}$, en otro caso $\nu = p$, entonces K es una extensión finita de un campo $p-$ádico $\mathbb{Q}_p$.

□

1.6 Lugares

En esta sección definiremos el concepto de lugares de un campo numérico K. El cual será utilizado en el capítulo siguiente para definir el anillo de adeles $\mathbb{A}_K$ asociado a K. Aquí, daremos por hecho las propiedades básicas del anillo de enteros O_K de K y de las latices (Ver Apéndice E).

Recordemos que dos valuaciones $|\cdot|$ y $|\cdot|'$ en K son *equivalentes* si existe una constante positiva s tal que $|a|' = |a|^s$ para toda $a \in K$ o de manera equivalente si $|\cdot|$ y $|\cdot|'$ definen la misma topología.

Definición 3. Un lugar ν de un campo numérico K, es una clase de equivalencia de las valuaciones de K. A las clases de equivalencia no arquimedianas las llamaremos *lugares finitos,* mientras que a las clases de equivalencia arquimedianas las llamaremos *lugares infinitos.*

Por comodidad, y haciendo un abuso de notación, dada una valuación $|\cdot|_\nu$ la denotaremos simplemente por ν. Luego, la completación de K con respecto a ν puede ser denotada por K_ν. A la extensión canónica de la valuación ν a K_ν la denotaremos también por ν y la extensión de esta a $\overline{K}_\nu$, la cerradura algebraica de K_ν, la denotaremos por $\bar{\nu}$.

Sea L/K una extensión algebraica. Considerando un K-monomorfismo

$$\tau : L \longrightarrow \overline{K}_\nu,$$

obtenemos, restringiendo $\bar{\nu}$ a τL, una extensión

$$\omega = \bar{\nu} \circ \tau,$$

de la valuación ν a L. Es decir, si ν, resp. $\bar{\nu}$, dados por las valuaciones $|\cdot|_\nu$, resp. $|\cdot|_{\bar{\nu}}$, donde $|\cdot|_{\bar{\nu}}$ extiende la valuación $|\cdot|_\nu$ de K_ν a $\overline{K}_\nu$, entonces obtenemos en L la valuación multiplicativa

$$|x|_\omega = |\tau x|_{\bar{\nu}},$$

donde el mapeo $\tau : L \to \overline{K}_\nu$ es claramente continuo con respecto a esta valuación.

Teorema 1.8 (Teorema de extensión)**.** *Sea L/K una extensión algebraica y sea ν una valuación de K. Entonces*

i) Toda extensión ω de la valuación ν puede verse como la composición $\omega = \bar{\nu} \circ \tau$, donde τ es algún K-monomorfismo $\tau : L \to \overline{K}_\nu$.

ii) Dos extensiones $\bar{\nu} \circ \tau$ y $\bar{\nu} \circ \tau'$ son equivalentes si y solo si τ y τ' son conjugados sobre K_ν.

Demostración. Para una demostración de este Teorema ver [11]. □

Dado un campo numérico $K/\mathbb{Q}$, sabemos que existen n monomorfismos $\tau : K \to \mathbb{C}$ (Ver Apéndice E). Luego, de acuerdo con el Teorema 1.8 (Teorema de extensión) los lugares infinitos son obtenidos de los distintos monomorfismos $\tau : K \to \mathbb{C}$. Existen dos tipos de ellos, los *lugares reales* que son dados por los monomorfismos $\tau : K \to \mathbb{R}$ y los *lugares complejos* que son inducidos por las parejas de monomorfismos conjugados no reales de K en $\mathbb{C}$.

A continuación, daremos una interpretación geométrica de los lugares infinitos conocida como Teoría de Minkowski.

Consideremos el mapeo canónico

$$j : K \longrightarrow K_{\mathbb{C}} := \prod_{\tau} \mathbb{C}$$

$$a \longmapsto ja = (\tau a),$$

el cual resulta de los n monomorfismos $\tau : K \to \mathbb{C}$. Luego, el $\mathbb{C}$-espacio vectorial $K_{\mathbb{C}}$ puede ser equipada con un producto interior hermitiano

$$\langle x, y \rangle = \sum_{\tau} x_{\tau} \bar{y}_{\tau}.$$

Sea $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ el grupo de Galois de $\mathbb{C}$ sobre $\mathbb{R}$, el cual es generado por la conjugación compleja

$$\varphi : z \longrightarrow \bar{z}.$$

Podemos notar que φ actúa en los factores del producto $\prod_{\tau} \mathbb{C}$ y también actúa sobre el conjunto de índices τ, enviando a cada monomorfismo $\tau : K \to \mathbb{C}$ en su correspondiente complejo conjugado $\bar{\tau} : K \to \mathbb{C}$. Esto define una involución

$$\varphi : K_{\mathbb{C}} \longrightarrow K_{\mathbb{C}}$$

$$z = (z_{\tau}) \longmapsto \bar{z}_{\bar{\tau}}.$$

Notemos que el producto escalar $\langle \cdot, \cdot \rangle$, es equivariante bajo φ, *i.e.*

$$\langle \varphi x, \varphi y \rangle = \varphi \langle x, y \rangle .$$

Ahora consideremos el conjunto de los puntos φ-invariantes de $K_{\mathbb{C}}$.

$$K_{\infty} = \{ (z_{\tau}) \in K_{\mathbb{C}} : z_{\bar{\tau}} = \bar{z}_{\tau} \} .$$

La restricción del producto interior hermitiano $\langle \cdot, \cdot \rangle$ de $K_{\mathbb{C}}$ a K_{∞} induce un producto interior en el $\mathbb{R}$-espacio vectorial K_{∞},

$$\langle \cdot, \cdot \rangle : K_{\infty} \times K_{\infty} \longrightarrow \mathbb{R}.$$

Al espacio euclidiano K_{∞} lo llamaremos el *espacio de Minkowski*.

Sean

$$\rho_1, \cdots, \rho_r : K \longrightarrow \mathbb{R},$$

los monomorfismos reales y

$$\sigma_1, \bar{\sigma}_1, \cdots, \sigma_s, \bar{\sigma}_s : K \longrightarrow \mathbb{C},$$

las parejas conjugadas de monomorfismos complejos. Luego

$$n = r + 2s.$$

Sea ρ variando sobre todos los monomorfismos reales y consideremos σ un representante de la pareja $\sigma, \bar{\sigma}$ el cual varia sobre las distintas parejas de monomorfismos complejos. Luego como φ deja invariante a ρ e intercambia a σ por $\bar{\sigma}$ tenemos la siguiente descripción de

$$K_\infty = \left\{ (z_\tau) \in \prod_\tau \mathbb{C} : z_\rho \in \mathbb{R}, z_{\bar{\sigma}} = \bar{z}_\sigma \right\},$$

luego existe un isomorfismo

$$\phi : K_\infty \longrightarrow \prod_\tau \mathbb{R} = \mathbb{R}^{r+2s}$$

dado por el mapeo

$$(z_\tau) \longmapsto (x_\tau),$$

donde $x_\rho = z_\rho$, $x_\sigma = \Re(z_\sigma)$ y $x_{\bar{\sigma}} = \Im(z_\sigma)$.

A partir de ahora, denotaremos por $\mathcal{P}_\infty$ al conjunto de lugares infinitos

$$\mathcal{P}_\infty = \{\nu_1, \ldots, \nu_r, \mu_1, \ldots, \mu_s\},$$

donde ν_j, $j = 1, \ldots, r$ denota el lugar (real) asociados al monomorfismo real de $\rho_j : K \to \mathbb{R}$ y μ_k, $k = 1, \ldots, s$ denota el lugar (complejo) asociado al par conjugado de monomorfismos complejos $\sigma_k, \bar{\sigma}_K : K \to \mathbb{C}$.

Sea

$$S^1 = \{z \in \mathbb{C} : \|z\| = 1\},$$

El cual tiene estructura de grupo inducida por la restricción de la multiplicación usual en $\mathbb{C}$. A S^1 lo llamaremos el *grupo circular*. Dado el mapeo

$$\psi : \mathbb{R} \longrightarrow S^1$$

$$x \longmapsto e^{2\pi i x},$$

el cual es un homomorfismo suprayectivo con kernel $\mathbb{Z}$, luego tenemos que

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

Teorema 1.9. *Si L es una latiz de dimensión n en $\mathbb{R}^n$ entonces $\mathbb{R}^n/L$ es isomorfo al n-toro $\mathbb{T}^n$.*

Demostración. Sea $\{e_1, \ldots, e_n\}$ un conjunto de generadores de L. Entonces $\{e_1, \ldots, e_n\}$ es una base para $\mathbb{R}^n$. Definamos

$$\psi : \mathbb{R}^n \longrightarrow \mathbb{T}_K^n$$

$$(a_j e_j) \longmapsto (e^{2\pi i a_j}),$$

donde $j = 1, \cdots, n$. Luego ψ es suprayectiva y el kernel de ψ es L. □

Ahora considerando el mapeo $j : K \to K_\infty$, el cual resulta de tomar la restricción de $j : K \to K_{\mathbb{C}}$ a K_∞, tenemos que dado un ideal $\mathfrak{a}$ de O_K no trivial[2], $\Gamma = j\mathfrak{a}$ es una latiz completa en K_∞. Por lo tanto, dado que K_∞ es isomorfo a $\mathbb{R}^n$, donde n es el grado de K sobre $\mathbb{Q}$, y por el Teorema 1.9 tenemos que

$$\mathbb{T}_{\mathfrak{a}} = K^\infty/\mathfrak{a},$$

es isomorfo al n-toro $\mathbb{T}^n$. En particular

$$\mathbb{T}_K = K^\infty/O_K,$$

es conocido como el *toro de Minkowski* de dimensión real n.

Por otro lado, al conjunto de los lugares finitos lo denotaremos por $\mathcal{P}_{\text{fin}}$. En la sección 2 vimos que si $\nu \in \mathcal{P}_{\text{fin}}$, K_ν tienen un subanillo abierto maximal

$$O_\nu = \{x \in K_\nu : |x|_\nu \leq 1\},$$

al cual llamamos *anillo de enteros* de K_ν.

Recordemos que el conjunto de Cantor es naturalmente homeomorfo, como espacio topológico, al producto de una cantidad numerable de copias del espacio $\{0, 1\}$ donde cada una de las copias es equipada con la topología discreta. Este espacio puede ser identificado con el conjunto de los enteros 2-ádicos $\mathbb{Z}_2$. Luego, esta caracterización del conjunto de Cantor como producto de espacios compactos, proporciona una prueba rápida de que el conjunto de Cantor es compacto, vía el Teorema de Tychonoff [14].

Teorema 1.10. *Para todo $\nu \in \mathcal{P}_{\text{fin}}$, K_ν es localmente un conjunto de Cantor (i.e. totalmente disconexo, perfecto y localmente compacto). Además, O_ν es un conjunto de Cantor.*

Demostración. Basta probar el Teorema para $\mathbb{Q}_p$ pues K_ν puede ser visto como $\mathbb{Q}_p$-espacio vectorial de dimensión n, luego este es isomorfo a n copias de $\mathbb{Q}_p$. De la observación del párrafo anterior tenemos que $\mathbb{Z}_p$ es un conjunto de Cantor, luego dado que $\mathbb{Q}_p$ es homogéneo existe una vecindad homeomorfa a $\mathbb{Z}_p$ para todo punto $x \in \mathbb{Q}_p$, de donde se sigue que $\mathbb{Q}_p$ es localmente un conjunto de cantor. □

[2]Aquí entenderemos por ideal no trivial a un ideal $\mathfrak{a} \neq 0$.

Capítulo 2

Solenoides y Adéles

En este capítulo revisaremos el concepto de solenoide asociado a un campo numérico. Para esto describiremos tres estructuras matemáticas; la representación de una suspensión, el cubriente universal algebraico y el grupo de clase de adéles las cuales asociaremos a un campo numérico K y veremos que resultan ser isomorfas. Finalmente, daremos el concepto de solenoide hiperbolizado. En este capítulo daremos por hecho que el lector tiene conocimientos básicos de teoría de cubrientes. Para una referencia ver [14].

2.1 Cubriente Universal Algebraico

Sea $p : \mathbb{R} \to S^1$ definido por el mapeo exponencial $t \mapsto e^{2\pi it}$ y tomemos $U = S^1 - \{1\}$ entonces

$$p^{-1}(U) = \mathbb{R} - \mathbb{Z} = \coprod_{n\in\mathbb{Z}} (n, n+1),$$

y para cada n

$$p|_{(n,n+1)} : (n, n+1) \to U,$$

es un homeomorfismo. De manera más general, si $U \subset S^1$ es cualquier abierto distinto de S^1 entonces

$$p^{-1}(U) = \coprod_{n\in\mathbb{Z}} \tilde{U_n} \quad \text{y} \quad p|_{\tilde{U}_n} : \tilde{U}_n \to U,$$

es un homeomorfismo. Luego $p : \mathbb{R} \to S$ es una aplicación cubriente cuya fibra es equivalente a $\mathbb{Z}$. Por otro lado, sabemos que $\pi_1(S^1) \cong \mathbb{Z}$ y $\pi_1(\mathbb{R}) = 1$ entonces el subgrupo característico es la identidad, lo que implica que la clase de conjugación característica $C(\mathbb{R}, p)$ consta de un solo elemento y la multiplicidad de p coincide con $[\mathbb{Z} : 1] = |\mathbb{Z}|$. Luego $p : \mathbb{R} \to S^1$ es un cubriente universal.

Consideremos

$$p_n : S^1 \longrightarrow S^1$$
$$t \longmapsto t^n,$$

una aplicación cubriente de grado n, luego $p_{n^*} : \pi_1(S^1) \to \pi_1(S^1)$ corresponde al homomorfismo

$$\mu_n : \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$k \longmapsto nk.$$

De modo que, el subgrupo característico es $n\mathbb{Z}$ y la multiplicidad de p_n es $[\mathbb{Z} : n\mathbb{Z}] = n$. Este es un ejemplo de un cubriente de multiplicidad n.

Notemos que la aplicación p definida como antes, tiene como únicas transformaciones cubrientes a los homeomorfismos $\mathbb{R} \to \mathbb{R}$, $x \mapsto x + n$, $n \in \mathbb{Z}$ por lo que el grupo de transformaciones cubrientes

$$Dek_p(\mathbb{R}) \cong \mathbb{Z}.$$

Por otro lado, la aplicación cubriente p_n tiene como transformaciones cubrientes a las rotaciones de S^1 por ángulos múltiplos de $2\pi/n$ por lo que el grupo de transformaciones cubrientes

$$Dek_{p_n}(S^1) \cong \mathbb{Z}/n\mathbb{Z}.$$

Sea $\mathcal{I}$ el conjunto de todos los ideales de $\mathbb{Z}$, *i.e.* los conjuntos de la forma $\mathfrak{a}_n = n\mathbb{Z}$, y notemos que a cada ideal $\mathfrak{a}_n$ le podemos asociar un espacio cubriente de multiplicidad n, $p_n : \mathbb{R}/\mathfrak{a}_n \to S^1$. Luego para cualesquiera dos ideales $\mathfrak{a}_n, \mathfrak{a}_m \in \mathcal{I}$ con $\mathfrak{a}_n \leq \mathfrak{a}_m$, podemos asociarle sus correspondientes aplicaciones cubrientes

$$p_n : \mathbb{R}/\mathfrak{a}_n \to S^1,$$

y

$$p_m : \mathbb{R}/\mathfrak{a}_m \to S^1.$$

Entonces existe una única aplicación cubriente $p_{nm} : \mathbb{R}/\mathfrak{a}_m \to \mathbb{R}/\mathfrak{a}_n$ tal que $p_n \circ p_{nm} = p_m$. Esto determina un sistema proyectivo $\{\mathbb{R}/\mathfrak{a}_n, p_n\}$ cuyo límite proyectivo es conocido como el *cubriente universal algebraico de* S^1,

$$\mathcal{S}^1 = \varprojlim \mathbb{R}/n\mathbb{Z},$$

con proyección canónica $\pi : \mathcal{S}^1 \to S^1$, determinada por las proyecciones en las coordenadas. De la definición de limite inverso se sigue que $\mathcal{S}^1$ es un grupo topológico abeliano, compacto, conexo donde cada "*hoja*" es una variedad simplemente conexa de dimensión uno homeomorfa al cubriente universal $\mathbb{R}$ de S^1.

Dado que $\mathbb{T}^n$, puede ser visto como el producto de n copias de S^1 tenemos el cubriente universal $\rho : \mathbb{R}^n \to \mathbb{T}^n$ dado por el mapeo $(x_j) \mapsto (e^{2\pi i x_j})$.

Sea $\mathcal{I}$ el conjunto de subgrupos normales de índice finito de $\mathbb{Z}^n$. Entonces a cada $\mathfrak{a} \in \mathcal{I}$ le podemos asociar un espacio cubriente $\rho_{\mathfrak{a}} : \mathbb{R}^n/\mathfrak{a} \to \mathbb{T}^n$. Luego, para cualesquiera $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}$ con $\mathfrak{a} \leq \mathfrak{b}$, tenemos asociadas las correspondientes aplicaciones cubrientes

$$\rho_{\mathfrak{a}} : \mathbb{R}^n/\mathfrak{a} \to \mathbb{T}^n,$$

y

$$\rho_{\mathfrak{b}} : \mathbb{R}^n/\mathfrak{b} \to \mathbb{T}^n.$$

Entonces existe una única aplicación cubriente

$$\rho_{\mathfrak{ab}} : \mathbb{R}^n/\mathfrak{b} \to \mathbb{R}^n/\mathfrak{a}$$

tal que $\rho_{\mathfrak{a}} \circ \rho_{\mathfrak{ab}} = \rho_{\mathfrak{b}}$. Lo cual determina un sistema proyectivo $\{\mathbb{R}^n/\mathfrak{a}, \rho_{\mathfrak{a}}\}$ cuyo límite proyectivo llamaremos *cubriente Universal algebraico* de $\mathbb{T}^n$.

$$\mathcal{S}^n = \varprojlim \mathbb{R}^n/\mathfrak{a}.$$

con proyecciones canónicas $\pi : \mathcal{S}^n \to \mathbb{T}^n$ determinadas por las proyecciones en cada coordenada. Como en el caso anterior, es claro que $\mathcal{S}_n$ es un grupo topológico, abeliano, compacto y conexo donde cada "*hoja*" es una variedad simplemente conexa de dimensión n homeomorfa al espacio cubriente universal $\mathbb{R}^n$ de $\mathbb{T}^n$.

De manera similar, sea $K/\mathbb{Q}$ un campo numérico de grado n, luego como $\mathbb{Z}^n \cong O_K$, y dado que los subgrupos normales de índice finito de $\mathbb{Z}^n$ pueden ser identificados con ideales de O_K y viceversa, el cubriente universal algebraico del toro de Minkowski $\mathbb{T}_K$ está dado por

$$\varprojlim \mathbb{T}_{\mathfrak{a}}.$$

donde $\mathfrak{a}$ corre sobre todos los ideales de O_K.

2.2 Suspensión de una Representación

En esta sección y la siguiente seguiremos la línea de [29]. Una referencia alternativa es [30].

Una *n-laminación* L es un espacio Hausdorff, 2-numerable, equipado con un atlas maximal $\mathfrak{U} = \{(U_\alpha, \phi_\alpha)\}$ con homeomorfismos $\phi_\alpha : U_\alpha \to V_\alpha$, donde $U_\alpha \subset L$ y $V_\alpha \subset \mathbb{R}^n \times T$, T es un espacio Hausdorff 2-numerable. Donde cada cambio de coordenadas $\phi_{\alpha\beta} = \phi_\beta \circ \phi_\alpha^{-1}$ es de la forma:

$$\phi_{\alpha\beta}(x,t) = (h_{\alpha\beta}(x,t), f_{\alpha\beta}(t)),$$

con $t \mapsto h_{\alpha\beta}(\cdot, t)$ una familia continua de homeomorfismos y $f_{\alpha\beta}$ un homeomorfismo.

En particular, cuando $T = \mathbb{R}^n$ diremos que L es una $foliación$. Por otro lado, cuando T es un conjunto de cantor diremos que L es un *solenoide*. Una forma más de clasificar o nombrar las laminaciones es dependiendo de $h_{\alpha\beta}$. Por ejemplo, si $h_{\alpha\beta}(\cdot, t)$ es C^r (una familia de homeomorfismos diferenciables con r-ésima derivada continua) diremos que L es una $C^r - laminación$.

Dado D un disco abierto de $\mathbb{R}^n$ y (U_α, ϕ_α) una carta, a los subconjuntos de la forma $\phi_\alpha^{-1}(D \times \{t\})$ los llamaremos *hojas locales* o *placas* de la laminación. Luego, el supuesto en las funciones de transición, o de cambio de coordenadas, implica que las placas se "pegan" apropiadamente para determinar las que llamaremos *hojas* de la laminación. Las cuales definimos como la continuación

maximal de cambios de coordenadas de placas, que resultan ser variedades n-dimensionales inmersas inyectivamente en L.

Si además consideramos $T' \subset T$ abierto. Diremos que una *baraja* es un subconjunto de la forma $\phi_\alpha^{-1}(D \times T')$ y una *baraja transversal* es un subconjunto de la forma $\phi_\alpha^{-1}(x \times T')$.

Una *métrica Riemanniana* en una laminación suave es una familia $\gamma = \{\gamma_l\}$ de métricas Riemannianas, una en cada hoja l, que cuando la restringimos a una baraja nos da una familia continua $t \mapsto \gamma_t$ de métricas suaves. Si L tiene estructura de grupo topológico tal que los mapeos

$$(x, y) \mapsto xy \quad \text{y } x \mapsto x^{-1}$$

toman hojas en hojas, L es llamado *grupo topológico laminado*. Además, si L es suave y los mapeos anteriores son suaves a lo largo de las hojas, L es llamado un *grupo de Lie laminado*.

Sean $\mathfrak{U} = \{(U_\alpha, \phi_\alpha)\}$ y $\mathfrak{U}' = \{(U'_{\alpha'}, \phi'_{\alpha'})\}$ atlas maximales de las laminaciones L y L' respectivamente. El conjunto

$$\mathfrak{U} \times \mathfrak{U}' = \{(U_\alpha \times U'_{\alpha'}, \phi_\alpha \times \phi'_{\alpha'})\},$$

es un atlas del espacio producto $L \times L'$ el cual llamaremos *laminación producto*.

Sea G un grupo discreto de homeomorfismos de un espacio topológico Hausdorff 2-numerable L que actúa propia y libremente sobre L y π la proyección de L sobre el espacio cociente $M = L/G$. Si $\mathfrak{U}$ es un atlas maximal de L invariante por la acción de G, *i.e.* tal que $g\mathfrak{U} = \mathfrak{U}$ para todo elemento g de G. Entonces existe una laminación $\mathfrak{U}/G$ de M, de la misma naturaleza que $\mathfrak{U}$, y solo una tal que si π es un homeomorfismo de un abierto $U \in L$ sobre un abierto $V \in M$ entonces

$$(\mathfrak{U}/G)|_V = \pi_*(\mathfrak{U}|_U).$$

A esta laminación la llamaremos la *laminación cociente*.

Sea B una variedad y F un espacio Hausdorff 2-numerable. Una *representación* del grupo fundamental de B en el grupo de homeomorfismos de F, es un homomorfismo

$$\rho : \pi_1(B) \to \text{Homeo}(F).$$

Por teoría de cubrientes [14], sabemos que si $\alpha : \tilde{B} \to B$ designa el cubriente universal de B, entonces el grupo $\pi_1(B)$ actúa propia y libremente sobre el producto $\tilde{B} \times F$ por la acción canónica sobre el primer factor y a través de la representación ρ en el segundo factor *i.e.* tenemos la siguiente acción

$$\alpha \cdot (\tilde{x}, t) = (\alpha \cdot \tilde{x}, \rho_\alpha(t)).$$

Luego el espacio cociente

$$L_\rho = (\tilde{B} \times F)/\pi_1(B),$$

es una laminación llamada la *suspensión* de ρ. La proyección $L_\rho \to B$ muestra a L_ρ como una fibra acotado con fibra F y la restricción de la proyección a cada hoja es un mapeo cubriente.

En particular si $B = S^1$, el círculo unitario y $F = \hat{\mathbb{Z}}$ la completación profinita de $\mathbb{Z}$ (ver Apéndice B), tenemos la representación

$$\rho : \pi_1(S^1) = \mathbb{Z} \to \text{Homeo}(\hat{\mathbb{Z}}),$$

definida como $\rho_n(\hat{m}) = \hat{m} - n$.

Como vimos en la primera sección, $\tilde{S}^1 = \mathbb{R}$. Luego, $\pi_1(S^1) = \mathbb{Z}$ actúa propia y libremente sobre $\mathbb{R} \times \hat{\mathbb{Z}}$. Por lo tanto, tenemos la suspensión asociada

$$L_\rho = (\mathbb{R} \times \hat{\mathbb{Z}})/\mathbb{Z},$$

la cual llamaremos el *toro solenoidal dimensión* 1.

De manera más general, si tomamos $B = \mathbb{T}^n$ el n-toro y $F = \hat{\mathbb{Z}}^n$ la completación profinita de $\mathbb{Z}^n$. Tenemos la representación

$$\rho : \pi_1(\mathbb{T}^n) = \mathbb{Z}^n \to \text{Homeo}(\hat{\mathbb{Z}}^n),$$

definida como $\rho_n(\hat{m}) = \hat{m} - n$. Como $\pi_1(\mathbb{T}^n) = \mathbb{Z}^n$ actúa propia y libremente sobre $\mathbb{R}^n \times \hat{\mathbb{Z}}^n$. Entonces tenemos la suspensión asociada

$$L_\rho = (\mathbb{R}^n \times \hat{\mathbb{Z}^n})/\mathbb{Z}^n,$$

la cual llamaremos el *toro solenoidal de dimensión* n. Dado K un campo numérico de grado n sabemos que $\mathbb{T}_{\mathfrak{a}} \cong \mathbb{T}^n$ y $\mathbb{Z}^n \cong O_K$ entonces podemos construir la suspensión

$$(K_\infty \times \hat{O}_K)/O_K,$$

donde $\hat{O}_K = \lim_{\leftarrow} O_K/\mathfrak{a}$, con $\mathfrak{a}$ corriendo sobre todos los ideales de O_K.

2.3 Producto Directo Restringido

Sea $J = \{\nu\}$ un conjunto de índices y J_∞ un subconjunto fijo y finito de J. Además, asumamos que para cada índice ν tenemos un grupo localmente compacto G_ν no necesariamente abeliano y para cada $\nu \notin J_\infty$ tenemos un subgrupo compacto abierto (cerrado) H_ν de G_ν (Ver Apéndice A).

Definición 4. Definimos el *producto directo restringido* de G_ν con respecto de H_v como sigue:

$$\prod_{\nu \in J}{}' G_\nu = \{(x_\nu) : x_\nu \in G_\nu \text{ con } x_\nu \in H_\nu \text{ para casi toda } \nu\}.$$

Para abreviar, denotaremos por G al producto directo restringido de G_ν con respecto de H_ν. Luego, es claro que G es un subconjunto del producto directo de G_ν. Más aún, G es un subgrupo del grupo inducido por el producto directo de los grupos G_ν.

Una base de abiertos de la identidad e, consta de los conjuntos de la forma $\prod N_\nu$, donde N_ν es una vecindad de e en G_ν y $N_\nu = H_\nu$ para todos salvo un número finito de ν, luego esta define una topología para G.

Sea S un subconjunto finito de J que contiene a J_∞, y consideremos el subgrupo G_S de G definido como

$$G_S = \prod_{\nu \in S} G_\nu \times \prod_{\nu \notin S} H_\nu.$$

Lema 2.1. *La topología producto en G_S es idéntica a la topología inducida por la topología del producto directo restringido.*

Demostración. Los básicos en G_S inducidos por la topología producto son de la forma

$$\left(\prod_{\nu \in S} G_\nu \times \prod_{\nu \notin S} H_\nu \right) \cap \prod X_\nu, \quad \text{donde } X_\nu = G_\nu \ \text{ para casi toda } \nu,$$

luego tenemos la siguiente igualdad

$$\prod_{\nu \in S} G_\nu \cap X_\nu \times \prod_{\nu \notin S} H_\nu \cap X_\nu = \prod N_\nu \times \prod H_\nu.$$

Notemos que el producto de la derecha es precisamente un básico en la topología del producto restringido. La prueba de que un básico en la topología del producto restringido induce un básico en la topología producto es similar. □

Proposición 2.1. *Sea G_ν y H_ν como antes y sea G el producto directo restringido de G_ν con respecto de H_ν, entonces G es un grupo localmente compacto.*

Demostración. Notemos que como cada subgrupo de la forma G_S es localmente compacto y dado que cada $x \in G$ pertenece a un subgrupo de esa forma entonces G es localmente compacto. La operación de grupo en G es definida entrada a entrada por la operación en cada G_ν. Luego, como cada G_ν es un grupo topológico entonces la operación definida es continua, por lo tanto, G es un grupo topológico localmente compacto. □

2.4 Adéles

En el estudio de los campos locales y globales, un problema que a menudo se presenta es la necesidad de poder considerar varios campos diferentes simultáneamente, en la que cada ν puede ser un lugar finito o infinito. Como vimos en el capítulo 1 este problema puede ser resuelto para el caso de los lugares infinitos vía la teoría de Minkowski. En esta sección describiremos el concepto de Adéles, el cual nos permitirá considerar todas las completaciones de un campo numérico en una sola estructura. Las referencias básicas en esta sección son [2] y [6].

Sea K un campo numérico y sea K_ν la completación de K con respecto al lugar ν. Sabemos que $\langle K_\nu, + \rangle$ es un grupo localmente compacto abeliano. En

nuestro caso, K_ν corresponde a $\mathbb{R}$, $\mathbb{C}$ o una extensión finita de $\mathbb{Q}_p$. Además, para todos los lugares $\nu \in \mathcal{P}_{\text{fin}}$, K_ν admite a O_ν como un subgrupo abierto y compacto.

Al producto directo restringido de K_ν sobre todos los lugares ν con respecto a los subgrupos O_ν, $\nu \in \mathcal{P}_{\text{fin}}$, lo llamaremos *el grupo de adéles de* K, el cual se denota como $\mathbb{A}_K$.

Proposición 2.2. *$\mathbb{A}_K$ es un anillo topológico localmente compacto.*

Demostración. Por definición de producto directo restringido $\mathbb{A}_K$ es localmente compacto. La propiedad de ser anillo topológico se sigue directamente de la suma y el producto entrada a entrada inducida por la suma y el producto de cada una de las completaciones K_ν. □

Proposición 2.3. *Existe una inclusión diagonal de K en $\mathbb{A}_K$ dada por el siguiente mapeo*

$$K \longrightarrow \mathbb{A}_K$$
$$x \longmapsto (x, x, x, \cdots).$$

Demostración. El mapeo está bien definido porque siempre existe un monomorfismo inyectivo de K en K_ν. Además, cada elemento de $x \in K$ cumple que $x \in O_\nu$ para todos salvo un número finito de lugares ν. □

Sea $\mathbb{A}_\infty$ al conjunto de todos los elementos de $\mathbb{A}_K$ cuyas componentes en los lugares finitos tienen todos valor absoluto menor o igual a uno *i.e.*

$$\mathbb{A}_\infty = \prod_{\nu \in \mathcal{P}_\infty} K_\nu \times \prod_{\nu \in \mathcal{P}_{\text{fin}}} O_\nu.$$

Teorema 2.1. *Dado $\mathbb{A}$ el anillo de adéles de $\mathbb{Q}$ tenemos que*

$$\mathbb{A} = \mathbb{Q} + A_\infty = \mathbb{Q} + (\mathbb{R} \times \prod_{p \text{ primo}} \mathbb{Z}_p),$$

además $\mathbb{Q} \cap \mathbb{A}_\infty = \mathbb{Z}$.

Demostración. Por la Proposición anterior es claro que podemos identificar a $\mathbb{Q}$ con el subconjunto diagonal de $\mathbb{A}_\mathbb{Q}$. Luego basta mostrar que dado un elemento $x \in \mathbb{A}_\mathbb{Q}$, existe $\mu \in \mathbb{Q}$ tal que cada componente de la diferencia $x - \mu$ es entero en los lugares finitos.

Dado que cualquier $q \in \mathbb{Q}$ se factoriza como el producto de un número finito de potencias de primos, existe un número racional m tal que mx es entero en todos los lugares finitos. Sea $\{p_1, \cdots p_r\}$ el conjunto de primos que dividen a m, el cual claramente contiene a todos los primos cuya correspondiente componente de x no es entera, y sea $n_1, \cdots, n_r$ una sucesión finita de números naturales. Por el Teorema chino del residuo podemos elegir un $\lambda \in \mathbb{Z}$ tal que

$$mx_j \equiv \lambda (\text{mod} p_j^{n_j}),$$

donde x_j es el componente del adéle x correspondiente al lugar p_j.

Sea $\mu = \lambda/m$. Luego, si escogemos cada n_j al menos tan grande como el exponente de p_j en la factorización de m en $\mathbb{Z}$ se tiene que $x-\mu = m^{-1}(mx-\lambda)$ es entero en cada uno de los primos $p_1, \cdots p_r$ por construcción.

Para los otros primos el valor absoluto es idéntico al de $mx - \lambda$ y por tanto también son enteros, de donde tenemos la primera afirmación. La segunda es inmediata, pues $x \in \mathbb{Q}$ está en $\mathbb{A}_\infty$ si y solo si $x \in \mathbb{Z}_p$ para todo primo p, lo cual sucede si y solo si $x \in \mathbb{Z}$. □

De manera más general dado K un campo numérico se tiene el siguiente Teorema.

Teorema 2.2 (Teorema de Aproximación)**.** *Para cada campo numérico K*

$$\mathbb{A}_K = K + \mathbb{A}_\infty,$$

además, $K \cap \mathbb{A}_\infty = O_K$.

Demostración. la prueba es similar al caso en que $K = \mathbb{Q}$. □

Una consecuencia inmediata del Teorema de aproximación es que

$$A_K = K_\infty \times \prod_{\nu \in \mathcal{P}_{\text{fin}}}{}' K_\nu,$$

donde

$$\mathbb{A}_K^{\text{fin}} = \prod_{\nu \in \mathcal{P}_{\text{fin}}}{}' K_\nu,$$

lo llamaremos el *anillo de adéles finito.*

Sea K un campo numérico y

$$\mathcal{P}_K = \mathcal{P}_\infty \cup \mathcal{P}_{\text{fin}}\ ,$$

el conjunto de todos los lugares de K. Notemos que cada $\nu \in \mathcal{P}_K$ induce, por restricción, un lugar $u = \text{res}_{\mathbb{Q}} \in \mathcal{P}_{\mathbb{Q}}$. Luego, esto define un mapeo

$$\begin{aligned} r = r_{K/\mathbb{Q}}: \quad & \mathcal{P}_{\mathcal{K}} \longrightarrow \mathcal{P}_{\mathbb{Q}} \\ & \nu \longmapsto u, \end{aligned}$$

de los lugares de K en los lugares de $\mathbb{Q}$. Diremos que ν *se encuentra sobre* u o ν *divide a* u $(\nu|u)$, si $\nu \in r^{-1}(u)$.

Definamos M como

$$M = \prod_{\nu|u} K_\nu,$$

luego tenemos un monomorfismo

$$\begin{aligned} K &\xrightarrow{\psi} M \\ x &\mapsto \sum \psi_\nu(x), \end{aligned}$$

donde ψ_ν es el monomorfismo canónico dada por la completación en el lugar ν.

Teorema 2.3. *Sea $\{e_1, \ldots, e_n\}$ una $\mathbb{Q}$-base de K y sea u un lugar de $\mathbb{Q}$, luego $X = \{\psi(e_1), \cdots, \psi(e_n)\}$ es una $\mathbb{Q}_u$-base de M. Además, existe un conjunto finito S de lugares de $\mathbb{Q}$, que contiene a los lugares arquimedianos tal que para toda $u \notin S$*

$$O_M = \prod_{\nu|u} O_{K_\nu},$$

es libre sobre $O_{\mathbb{Q}_u}$ con base X.

Demostración. Para una prueba ver [2]. □

Lema 2.2. *Sea K un campo numérico de grado n sobre $\mathbb{Q}$, y fijemos una $\mathbb{Q}$-base $\{u_1, \cdots, u_n\}$ de K. El mapeo natural*

$$\alpha : \prod_{j=1}^{n} \mathbb{A}_{\mathbb{Q}} \longrightarrow \mathbb{A}_K$$

$$((x_{\nu,j})_\nu)_j \longmapsto \sum_j u_j (x_{\nu,j})_\nu,$$

es un isomorfismo de grupos topológico.

Demostración. El isomorfismo α es ciertamente un isomorfismo de espacios vectoriales, así que lo único que nos resta demostrar es la continuidad. Para cada lugar ν de $\mathbb{Q}$, definimos

$$K_\nu = \prod_{w|\nu} K_w,$$

donde w corre sobre todos los lugares de K que están sobre ν. Esto claramente no es un campo pero si es un espacio vectorial sobre $\mathbb{Q}_\nu$ donde $\mathbb{Q}_\nu$ se sumerge diagonalmente. Por el Teorema 2.3 tenemos que K_ν admite una $\mathbb{Q}_\nu$-base $\{u_1, \cdots, u_n\}$ y por tanto un isomorfismo algebraico

$$\alpha_\nu : \prod_{j=1}^{n} \mathbb{Q}_\nu \xrightarrow{\sim} K_\nu$$

$$(x_j) \mapsto \sum x_j u_j.$$

Por propiedades de espacios vectoriales topológicos α_ν es un isomorfismo topológico. Definamos un subconjunto O_{K_ν} de K_ν como sigue

$$O_{K_\nu} = \prod_{w|\nu} O_{K_w},$$

luego, por el Teorema 2.3 existe un conjunto finito de lugares S_0 de $\mathbb{Q}$, que contiene al lugar arquimediano, tal que para cada $\nu \notin S_0$ el mapeo α_ν definido antes induce, por restricción, un isomorfismo

$$\alpha_\nu : \prod_{j=1}^{n} O_\nu \xrightarrow{\sim} O_{K_\nu}.$$

Dado un conjunto finito S que contiene a S_0, consideremos los productos

$$\mathbb{A}_{\mathbb{Q}}^S = \prod_{\nu\in S} \mathbb{Q}_\nu \times \prod_{\nu\notin S} O_\nu \quad \text{y} \quad \mathbb{A}_K^S = \prod_{\nu\in S} K_\nu \times \prod_{\nu\notin S} O_{K_\nu},$$

luego, tomando el producto tenemos que

$$\prod_{j=1}^n \mathbb{A}_{\mathbb{Q}}^S = \prod_{j=1}^n \left(\prod_{\nu\in S} \mathbb{Q}_\nu \times \prod_{\nu\notin S} O_\nu \right) \cong \prod_{\nu\in S} K_\nu \times \prod_{\nu\notin S} O_{K_\nu} = \mathbb{A}_K^S,$$

para cada conjunto de lugares S. Luego la colección $\{\alpha_\nu\}$ induce un mapeo,

$$\alpha^S : \prod_{j=1}^n \mathbb{A}_{\mathbb{Q}}^S \xrightarrow{\sim} \mathbb{A}_K^S,$$

el cual es un isomorfismo topológico y por construcción, es compatible con la restricción de α. Luego esto es verdad para cada S que contiene a S_0 y los conjuntos abiertos $\mathbb{A}_K^S$ cubren a $\mathbb{A}_K$. Por tanto, α es un isomorfismo topológico. □

Si $K/\mathbb{Q}$ es una extensión de Galois de grado n, por el Lema anterior tenemos los siguientes monomorfismos de espacios vectorial o anillos según sea el caso,

$$\mathbb{R} \hookrightarrow K_\infty, \quad \mathbb{A}_{\mathbb{Q}}^{\text{fin}} \hookrightarrow \mathbb{A}_K^{\text{fin}}, \quad \mathbb{A}_{\mathbb{Q}} \hookrightarrow \mathbb{A}_K,$$

y el siguiente diagrama conmutativo de grupos topológicos, donde α y $\alpha|$ son isomorfismos topológicos.

$$\begin{array}{ccc} \prod_{j=1}^n \mathbb{A}_{\mathbb{Q}} & \xrightarrow{\alpha} & \mathbb{A}_K \\ \uparrow & & \uparrow \\ \prod_{j=1}^n \mathbb{Q} & \xrightarrow{\alpha|} & K \end{array}$$

Además, este diagrama induce los siguientes homomorfismos inyectivos

$$\mathbb{T}_{\mathbb{Q}} \hookrightarrow \mathbb{T}_K \quad \text{y} \quad \mathbb{A}_{\mathbb{Q}}/\mathbb{Q} \hookrightarrow \mathbb{A}_K/K.$$

Corolario 2.1. *Sea K un campo numérico de grado n sobre $\mathbb{Q}$, entonces*

$$K_\infty = \mathbb{R} \otimes_{\mathbb{Q}} K, \quad y \quad \mathbb{A}_K \cong (\mathbb{A}_{\mathbb{Q}})^n \cong \mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} K.$$

Demostración. Por Lema 2.2 tenemos que $\mathbb{A}_K \cong (\mathbb{A}_{\mathbb{Q}})^n$, además por propiedades de producto tensorial [12] tenemos que

$$(\mathbb{A}_{\mathbb{Q}})^n \cong (\mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q})^n \cong \mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}^n \cong \mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} K,$$

de manera análoga $K_\infty \cong \mathbb{R}^n \cong \mathbb{R} \otimes_{\mathbb{Q}} K$. □

Teorema 2.4. *K es discreto en $\mathbb{A}_K$ y $\mathbb{A}_K/K$ es compacto.*

Demostración. Por el Lema 2.2 basta dar una prueba para $K = \mathbb{Q}$. Por el Teorema 2.1 tenemos que

$$\mathbb{Q} \cap \left(\mathbb{R} \times \prod_{p \text{ primo}} \mathbb{Z}_p \right) = \mathbb{Q} \cap \mathbb{A}_\infty = \mathbb{Z},$$

luego definamos

$$C = \{x \in \mathbb{A}_\mathbb{Q} : |x_\infty|_\infty \leq 1/2 \text{ y } x_p \in \mathbb{Z}_p \text{ para todo primo } p\}.$$

Notemos que $C \subset \mathbb{A}_\infty$ entonces $\mathbb{Q} \cap C \subset \mathbb{Z}$, ahora si $b \in \mathbb{Q} \cap C$, $b \in \mathbb{Z}$ luego $b = 0$, ya que $|b|_\infty < 1$ por lo tanto $\mathbb{Q}$ es discreto.

Ahora probemos la compacidad. Para esto, basta ver que cada elemento $x' \in \mathbb{A}_\mathbb{Q}$ es de la forma $x' = q + x$ con $q \in \mathbb{Q}$ y $x \in C$. Observemos que para cada p podemos obtener un $r_p = z_p/p^{\alpha_p}$ donde $z_p \in \mathbb{Z}$, $\alpha_p \in \mathbb{N} \cup \{0\}$ y tal que $\left|x'_p - r_p\right|_p \leq 1$. Como $x \in \mathbb{A}_\mathbb{Q}$ podemos tomar $r_p = 0$ para casi todo p. Luego $r = \sum_p r_p$ está bien definida y $\left|x'_p - r\right| \leq 1$ para todo p. Ahora, escojamos $s \in \mathbb{Z}$ tal que $|x'_\infty - r - s| \leq 1/2$, entonces $q = r + s$ y $x' = x - b$ justo como queríamos.

Finalmente, por la continuidad de $C \to \mathbb{A}_\mathbb{Q}/\mathbb{Q}$, inducido por el mapeo cociente $\mathbb{A}_\mathbb{Q} \to \mathbb{A}_\mathbb{Q}/\mathbb{Q}$, es suprayectivo. Pero C es compacto, por ser producto de compactos, luego $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ es compacto. □

Al cociente $\hat{\mathbb{S}}_K = \mathbb{A}_K/K$ lo llamaremos el *grupo de clase de adéles*. Una interpretación geométrica de este grupo, es dada a continuación.

Teorema 2.5. *$\hat{\mathbb{S}}_\mathbb{Q}$ es un grupo de Lie solenoidal euclidiano de dimensión 1, isomorfo a*

i) El límite inverso de grupos de lie euclidianos

$$\varprojlim \mathbb{R}/n\mathbb{Z}.$$

ii) La suspensión

$$\left(\mathbb{R} \times \hat{\mathbb{Z}}\right)/\mathbb{Z},$$

donde $\hat{\mathbb{Z}}$ es la completación profinita de $\mathbb{Z}$.

Demostración. (i) Sea $n \in \mathbb{N}$ y definamos el conjunto

$$\mathcal{C}_n = \left\{ x \in \mathbb{A}_\mathbb{Q} : x_\infty = 0 \text{ y } x_p \in p^{\nu_p(n)}\mathbb{Z}_p \text{ para } p < \infty \right\}.$$

Es claro que cada $\mathcal{C}_n$ es un subgrupo compacto pues es producto de subgrupos compactos y además $\bigcap_{n \in \mathbb{N}} \mathcal{C}_n = \{0\}$. Luego, tenemos el siguiente isomorfismo (ver Apéndice A)

$$\varprojlim \mathbb{A}_\mathbb{Q}/\mathcal{C}_n \xrightarrow{\sim} \mathbb{A}_\mathbb{Q}$$

$$((\bar{x}_{p,n})_p)_n \mapsto (\lim_n x_{p,n})_p,$$

donde el límite directo es también tomado sobre $\mathbb{N}$ con respecto a la divisibilidad. Ahora consideremos el siguiente morfismo

$$\lim_{\leftarrow} \mathbb{A}_{\mathbb{Q}}/\mathcal{C}_n \xrightarrow{\varphi} \lim_{\leftarrow}(\mathbb{A}_{\mathbb{Q}})/\left(\mathcal{C}_n + \mathbb{Q}\right)$$

$$a_n + c_n \mapsto a_n + (c_n + \mathbb{Q}).$$

Si $q \in \mathbb{Q}$ entonces $q + c_n \mapsto 0 + c_n + \mathbb{Q}$, por lo tanto $\mathbb{Q} \subset ker\varphi$. Ahora, consideremos $a_n \in ker\varphi$ luego $a_n + c_n \mapsto 0 + c_n + \mathbb{Q}$, entonces para n suficientemente grande tenemos que $a_n \in \mathbb{Q}$ luego por el primer Teorema de isomorfismo tenemos que

$$(\lim_{\leftarrow} \mathbb{A}_{\mathbb{Q}}/\mathcal{C}_n)/\mathbb{Q} \cong \lim_{\leftarrow} \mathbb{A}_{\mathbb{Q}}/\mathbb{Q} + \mathcal{C}_n$$

de donde se sigue el isomorfismo topológico

$$\mathbb{A}_{\mathbb{Q}}/\mathbb{Q} \cong \lim_{\leftarrow} \mathbb{A}_{\mathbb{Q}}/(\mathbb{Q} + \mathcal{C}_n).$$

Ahora consideremos el siguiente mapeo

$$\mathbb{R}/n\mathbb{Z} \xrightarrow{\psi_n} \mathbb{A}_n/(\mathbb{Q} + \mathcal{C}_n)$$

$$(\bar{x}) \mapsto (\bar{x}, 0, 0, \ldots).$$

El cual está bien definido ya que para todo producto na, $a \in \mathbb{Z}$, tenemos la descomposición

$$(na, 0, 0, \ldots) = (na, na, na, \ldots) + (0, -na, -na, \ldots) \in \mathbb{Q} + \mathcal{C}_n,$$

de donde se sigue que ψ_n es inyectivo. La suprayectividad se sigue del Teorema 2.1. Luego de la existencia de los isomorfismos ψ_n tenemos que

$$\mathbb{A}_{\mathbb{Q}}/\mathbb{Q} \cong \lim_{\leftarrow} \mathbb{A}_{\mathbb{Q}}/(\mathbb{Q} + \mathcal{C}_n) \cong \lim_{\leftarrow} \mathbb{R}/n\mathbb{Z},$$

lo que prueba que

$$\hat{\mathbb{S}}_K \cong \lim_{\leftarrow} \mathbb{R}/n\mathbb{Z}.$$

(ii) Sea $(x, \hat{\gamma}) \in \mathbb{R} \times \hat{\mathbb{Z}}$, luego notemos que x define un elemento $\hat{x} = (x_n)$ de $\lim_{\leftarrow} \mathbb{R}/n\mathbb{Z}$ por la proyección en cada uno de los factores. Además, $\hat{\gamma}$ es por definición una sucesión coherente $\{\hat{\gamma}_n\}$ de transformaciones de cubrientes de $\mathbb{R}/n\mathbb{Z} \to S^1$. Luego, tenemos el siguiente homomorfismo

$$\varphi : \mathbb{R} \times \hat{\mathbb{Z}} \longrightarrow \hat{\mathbb{S}}_{\mathbb{Q}}$$

$$(x, \hat{\gamma}) \mapsto \hat{\gamma} \cdot \hat{x} = (\gamma_n(x_n)),$$

donde $ker\varphi = \mathbb{Z}$, entonces por el primer Teorema de isomorfismo [12] tenemos que

$$\left(\mathbb{R} \times \hat{\mathbb{Z}}\right)/\mathbb{Z} \cong \lim_{\leftarrow} \mathbb{R}/n\mathbb{Z}.$$

□

Teorema 2.6. *$\hat{\mathbb{S}}_K$ es un grupo de Lie solenoidal euclidiano de dimensión n isomorfo a*

i) El límite inverso de grupos de lie euclidianos

$$\varprojlim \mathbb{T}_{\mathfrak{a}}.$$

donde $\mathfrak{a}$ corre sobre todos los ideales de O_K.

ii) La suspensión

$$\left(K_\infty \times \hat{O}_K\right)/O_K.$$

donde $\hat{O}_K$ es la completación profinita de O_K.

Demostración. la prueba es similar a la del Teorema 2.5. □

Una *acción lineal* de G en un K-espacio vectorial V es aquella en donde cada transición $v \mapsto gv$ es lineal; es claro que toda acción lineal de G en V está determinada por una representación $G \to \mathrm{Aut}(V)$. En particular, la *acción ortogonal* de G en $\mathbb{R}^n$ será una acción lineal cuyas transiciones conservan el producto interno usual (es decir son isometrías) de R^n, esto es $\langle gu, gv\rangle = \langle v, w\rangle$ para todo $g \in G$ y todo par de vectores $u, v \in \mathbb{R}^n$.

Sea K un campo numérico, por el Teorema 2.1 podemos escribir

$$K_\infty \cong \mathbb{R} \otimes_{\mathbb{Q}} K \quad \mathbb{A}_K \cong \mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} K.$$

Luego podemos notar que si $K/\mathbb{Q}$ es una extensión de Galois, un elemento $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ actúa en K_∞ o en $\mathbb{A}_K$ a través del mapeo

$$x \otimes q \mapsto x \otimes \sigma(q)$$

, donde x está en $\mathbb{R}$ o en $\mathbb{A}_{\mathbb{Q}}$ según sea el caso.

De manera alternativa si $x = (x_\nu) \in K_\infty$ entonces $\sigma(x) = (x_{\sigma\nu})$. Esta última observación muestra el siguiente Corolario.

Corolario 2.2. $\mathrm{Gal}(K/\mathbb{Q})$ *actúa ortogonalmente en K_∞.*

Luego la acción de σ en $\mathbb{A}_K$ la podemos ver como el producto de las acciones en K_∞ y $\mathbb{A}_K^{\mathrm{fin}}$.

Proposición 2.4. *La imagen de O_K (resp. K) es preservada por σ y tenemos los isomorfismos isométricos (por hojas)*

$$\sigma : \mathbb{T}_K \to \mathbb{T}_K, \quad \hat{\sigma} : \hat{\mathbb{S}}_K \to \hat{\mathbb{S}}_K,$$

los cuales entrelazan la proyección $p : \hat{\mathbb{S}}_K \to \mathbb{T}_K$ en el sentido de que $p \circ \hat{\sigma} = \sigma \circ p$.

Demostración. Veamos primero que O_K es preservado bajo σ. Por el Corolario 2.2, $\mathrm{Gal}(K/\mathbb{Q})$ actúa ortogonalmente en $K_\infty \cong \mathbb{R}^n$. Entonces tenemos que $\sigma : K_\infty \to K_\infty$ preserva el producto interior. Por lo tanto, este mapeo induce un isomorfismo isométrico $\sigma : \mathbb{T}_K \to \mathbb{T}_K$. Además, dado que las hojas de $\mathbb{S}_K$ son homeomorfas a K_∞ tenemos que $\sigma : K_\infty \to K_\infty$ induce un isomorfismo isométrico por hojas $\hat{\sigma} : \hat{\mathbb{S}}_K \to \hat{\mathbb{S}}_K$. □

La Proposición anterior induce las siguientes representaciones

$$\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Isom}(\mathbb{T}_K), \quad \hat{\rho} : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Isom}(\hat{\mathbb{S}}_K)$$

donde $\mathrm{Isom}(\cdot)$ es el grupo de isomorfismos isométricos.

2.5 Hiperbolización

En esta sección daremos una hiperbolización del grupo de clases de adéles, la cual usaremos en el capítulo siguiente. Sea

$$\mathbb{H}^2 = \mathbb{R} \times i(0, \infty),$$

el semiplano superior del plano complejo. Entonces, definimos el *producto interior hiperbólico* de dos vectores $u, v \in \mathbb{H}_{\mathbb{Q}}$ anclados en un punto $z = x + it$, como

$$\langle u, v \rangle_h = \frac{\langle u, v \rangle}{t^2},$$

donde $\langle \cdot, \cdot \rangle$ es el producto interior usual en $\mathbb{R}^2$. Por lo tanto, $\langle \cdot, \cdot \rangle_h$ nos permite definir la norma de un vector v anclado en un punto z del semiplano superior como

$$\|v\|_h = \sqrt{\langle v, v \rangle_h}.$$

Luego podemos medir la longitud hiperbólica de una curva en $\mathbb{H}^2$ en forma análoga a la usual. Si $\gamma : [a, b] \to \mathbb{H}^2$ es una curva diferenciable, su longitud hiperbólica es

$$l_h(\gamma) = \int_a^b \|\gamma'(t)\|_h \, dt.$$

Notemos que la forma de calcular la norma varia con el punto $\gamma(t)$ en que esté anclado el vector tangente $\gamma'(t)$. Sin embargo, si la curva es suave la variación es continua y eso da sentido al integrando. Luego dados dos puntos $z_1, z_2 \in \mathbb{H}^2$ la distancia hiperbólica de z_1 a z_2 denotada por $\rho_h(z_1, z_2)$ es el ínfimo de las longitudes de las curvas en $\mathbb{H}^2$ que unen a estos dos puntos. Además, se puede ver que la distancia hiperbólica es una métrica riemanniana.

El semiplano superior $\mathbb{H}^2$, con la métrica hiperbólica es llamado el *plano hiperbólico*. Las rectas en $\mathbb{H}^2$, conocidas como geodésicas, son las curvas en $\mathbb{H}^2$ que minimizan la distancia hiperbólica entre sus puntos.

Una transformación de Möbius es una función

$$\begin{aligned} T : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto \frac{az + b}{cz + d}, \end{aligned}$$

donde $a, b, c, d \in \mathbb{C}$ y $ad - bc \neq 0$. Las transformaciones de Möbius, pueden ser extendidas a todo $\hat{\mathbb{C}}$, definiendo

$$T(-\frac{d}{c}) = \lim_{z \to -\frac{d}{c}} T(z) = \infty,$$

cuando $c \neq 0$ y

$$T(\infty) = \lim_{z\to\infty} T(z) = \frac{a}{c}.$$

Luego, estas transformaciones son holomorfas en todo $\hat{\mathbb{C}}$. Recíprocamente, todo biholomorfismo de $\hat{\mathbb{C}}$ está dado por una transformación de Möbius. Es claro de la definición, que las transformaciones de Möbius forman un grupo con la composición conocido como el grupo de Möbius, $\mathrm{Möb}(2,\mathbb{C})$.

Alternativamente, podemos pensar en el plano hiperbólico a través del modelo del *disco de Poincaré*. En este caso consideraremos el disco unitario

$$\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}.$$

La transformación de Möbius

$$G(z) = \frac{z-i}{-iz+1},$$

es una biyección que manda a $\mathbb{H}^2$ en $\mathbb{D}$. Luego, se puede definir producto interior de dos vectores $u, v \in \mathbb{R}^2$, anclados en $z \in \mathbb{D}$, como

$$\langle u, v\rangle_{\Delta} = \frac{4\langle u, v\rangle}{(1-r^2)^2},$$

donde r es la distancia del punto de apoyo de los vectores al centro del disco. Denotamos por Δ a $\mathbb{D}$ equipado con la métrica inducida por el producto interior.

Notemos que debido a que $\mathbb{Z}$ actúa por traslación en $\mathbb{R}$, esta acción se extiende trivialmente a todo $\mathbb{H}^2$. Lo cual da origen al *toro Hiperbolizado*

$$\mathfrak{T}_{\mathbb{Q}} = \mathbb{H}^2/\mathbb{Z} \cong \Delta^*,$$

donde $\Delta^* = \Delta - \{0\}$.

Más aún, podemos definir la hiperbolización del *grupo de clases de Adéles* asociado a $\mathbb{Q}$ como

$$\hat{\mathfrak{S}}_{\mathbb{Q}} = (\mathbb{H}^2 \times \hat{\mathbb{Z}})/\mathbb{Z} \cong \hat{\mathbb{S}}_{\mathbb{Q}} \times (0,\infty).$$

De forma similar, es posible generalizar la idea de hiperbolización a K un campo numérico de grado n sobre $\mathbb{Q}$. Para ν un lugar real $K_\nu \cong \mathbb{R}$, definimos

$$\mathbb{H}_\nu = \mathbb{R} \times i(0,\infty),$$

el cual se puede equipar con la métrica hiperbólica como antes.

Para los lugares complejos μ, haremos una ligerea modificación tomando en cuenta el álgebra del factor

$$\mathbb{C}_\mu = \{(z, \bar{z}) : z \in \mathbb{C}\} \cong \mathbb{C},$$

En este sentido, es conveniente ver al factor $(0,\infty)\times(0,\infty)$ que adjuntaremos a $\mathbb{C}_\mu$ como un factor complejo. Sea $\mathbb{B}$ el "espacio cuarto complejo"

$$\mathbb{B} = \{b = s + it \in \mathbb{C} : 0 < s, t\},$$

y definamos

$$\mathbb{H}_\mu = \left\{(z,\bar{z}) \times (b,-\bar{b}) : z \in \mathbb{C}, b \in \mathbb{B}\right\} \subset (\mathbb{C}\times\mathbb{B}) \times (\bar{C} \times (-\bar{\mathbb{B}})) \subset \mathbb{C}^2 \times \mathbb{C}^2.$$

Lema 2.3. *Dado $-i\mathbb{H}^2$ el semiplano derecho, podemos identificar a $\mathbb{H}_\mu$ con $\mathbb{H}^2 \oplus -i\mathbb{H}^2$.*

Demostración. Sea $z = x + iy$ y b como antes, definimos el mapeo

$$(z,\bar{z}) \times (b,-\bar{b}) \mapsto \frac{1}{2}(z + \bar{z} + b - \bar{b}, z - \bar{z} + b + \bar{b}),$$

luego

$$\frac{1}{2}(z + \bar{z} + b - \bar{b}, z - \bar{z} + b + \bar{b}) = (x + it, s + iy) \equiv (u, v),$$

y por lo tanto tenemos la identificación deseada. □

Luego podemos escribir

$$\mathbb{H}_\mu = \mathbb{H}_\mu^2 \oplus -i\mathbb{H}_\mu^2.$$

Esta identificación nos ayuda a inducir una métrica riemanniana en $\mathbb{H}_\mu$ como el producto de las métricas hiperbólicas de $\mathbb{H}^2$ y $-i\mathbb{H}^2$.

Diremos que una función en $\mathbb{H}_\mu$ es holomorfa si lo es en cada una de las variables $(u, v) = (x + it, s + iy)$ por separado.

Notemos que la acción, conjugación compleja en $\mathbb{C}_\mu$ se puede extender a $\mathbb{H}_\mu$ enviando a b en b, de donde tenemos que

$$(u, v) \mapsto (u, \bar{v})$$

lo cual define una isometría de $\mathbb{H}_\mu$.

Luego definimos la *hiperbolización*

$$\mathbb{H}_K = \prod \mathbb{H}_\nu \times \prod \mathbb{H}_\mu \cong \prod \mathbb{H}_\nu \times \left(\prod \mathbb{H}_\mu^2 \oplus -i\mathbb{H}_\mu^2\right) \cong K_\infty \times (0,\infty)^n.$$

Entonces $\mathbb{H}_K$ tiene una estructura de polidisco complejo n-dimensional equipado con la métrica riemanniana inducida por el producto de las métricas hiperbólicas de cada factor.

Si ν es un lugar real nosotros denotaremos por $z_\nu = x_\nu + it_\nu$ a los puntos de $\mathbb{H}_\nu$, y para un lugar complejo μ escribiremos

$$(w_\mu, \bar{w}_\mu) := ((z_\mu, b_\mu), (\bar{z}_\mu, -\bar{b}_\mu)) = (u_\mu, v_\mu).$$

Luego los puntos de $\mathbb{H}_K$ los podemos escribir como $z \times w$ donde $z = (z_1, \cdots, z_r)$, las coordenadas de la "hiperbolización real", y $w = ((w_1, \bar{w}_1), \cdots, (w_s, \bar{w}_s))$ las coordenadas de la "hiperbolización compleja".

Proposición 2.5. *La acción del grupo de Galois* $\mathrm{Gal}(K/\mathbb{Q})$ *en K_∞ se extiende a una acción isométrica en $\mathbb{H}_K$.*

Demostración. Como $\mathrm{Gal}(K/\mathbb{Q})$ actúa ortogonalmente en K_∞, entonces esta acción permuta isométricamente los factores de $K_\infty \cong \mathbb{R}^n$. Luego, $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ actúa en $\mathbb{H}_K$ de la siguiente forma

$$\sigma(x_j, t_j) = (\sigma(x_j), t_j).$$

Por lo tanto σ se extiende isométricamente a todo $\mathbb{H}_K$. □

Corolario 2.3. *Los subgrupos O_K y K de K_∞, vistos como grupos de traslaciones, se extienden a traslaciones de $\mathbb{H}_K$ las cuales son isometrías.*

Luego tenemos el *toro hiperbolizado* de K

$$\mathfrak{T}_K = \mathbb{H}_K/O_K \cong (\Delta^*)^n = \Delta^n - \{0\}.$$

Más aún tenemos la hiperbolización del grupo de clase de adéles de K a la cual llamaremos el *solenoide hiperbolizado.*

$$\hat{\mathfrak{S}} = (\mathbb{H}_K \times \hat{\mathbb{Z}}^n)/K \cong \hat{S}_K \times (0, \infty)^n.$$

Proposición 2.6. *Para K un campo numérico de grado n sobre $\mathbb{Q}$, las inclusiones canónicas*

$$\mathfrak{T}_\mathbb{Q} \hookrightarrow \mathfrak{T}_K \quad \hat{\mathfrak{S}_\mathbb{Q}} \hookrightarrow \hat{\mathfrak{S}_K},$$

son isométricas salvo un factor escalar de grado n.

Demostración. La prueba se sigue del Lema 2.2. □

Si $K/\mathbb{Q}$ es de Galois, la acción de $\mathrm{Gal}(K/\mathbb{Q})$ en $\mathbb{T}_K$ y $\hat{\mathbb{S}}_K$ se extiende por isometrías a $\mathfrak{T}_K$ y $\hat{\mathfrak{S}}_K$ restringiendo a la identidad en las imágenes de $\mathfrak{T}_\mathbb{Q}$ y $\hat{\mathfrak{S}}_\mathbb{Q}$.

Capítulo 3

Campos de Números No lineales

El propósito de este capítulo es describir con detalle el concepto de campo de números no lineal $N(K)$ del artículo de T. Gendron y A. Verjovsky [1]. El cual como veremos es una extensión natural de un campo numérico K en el sentido de que extiende las dos operaciones de K a todo $N(K)$ y que además resultara ser la proyectivización de una cierta álgebra graduada de funciones holomorfas $\mathrm{Har}_\bullet[K]$. En particular, veremos que en el caso cuando $K = \mathbb{Q}$, $N(K)$ contiene las clases proyectivas que corresponden a funciones zeta y L clásicas.

3.1 Construcción de $\mathbb{C}[K]$

Una *K-álgebra* A se define como un K-espacio vectorial con un producto K-bilineal

$$A \times A \to A$$
$$(x, y) \to xy,$$

tal que A obtiene una estructura de anillo con este producto y además cumple con las siguientes propiedades distributivas.

i) $(x + y)z = xz + yz, \quad \forall x, y, z \in A,$

ii) $x(y + z) = xy + xz, \quad \forall x, y, z \in A,$

iii) $\lambda(xy) = (\lambda x)y = x(\lambda y), \quad \forall x, y \in A$ y $\lambda \in K.$

Dado un grupo G y un campo K, definimos un *álgebra de grupo* $K[G]$ asociada a G como sigue

$$K[G] = \left\{ \sum_{g \in G} a_g g : a_g \in K \text{ es 0, para casi todo } g \right\},$$

donde $K[G]$ es un álgebra sobre K con las siguientes operaciones

i) la suma externa

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g)g,$$

ii) el producto

$$\left(\sum_{g\in G} a_g g\right) \odot \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} \left(\sum_{g_1 g_2 = g} a_{g_1} b_{g_2}\right) g,$$

iii) multiplicación por escalar

$$\lambda \sum_{g\in G} a_g g = \sum_{g\in G} (\lambda a_g) g.$$

De aquí se sigue que el elemento identidad en G corresponde al $1_\odot \in K[G]$ y que $K[G]$ es conmutativo si y solo si G es abeliano.

Cuando $K = \mathbb{C}$ y $G = (\mathbb{Q}, +)$ tenemos el álgebra de grupo $\mathbb{C}[\mathbb{Q}]$ con el producto

$$\oplus : \mathbb{C}[\mathbb{Q}] \times \mathbb{C}[\mathbb{Q}] \to \mathbb{C}[\mathbb{Q}]$$

definido como

$$\left(\sum_{q\in\mathbb{Q}} a_q q\right) \oplus \left(\sum_{q\in\mathbb{Q}} b_q q\right) = \sum_{q\in\mathbb{Q}} \left(\sum_{q_1+q_2=q} a_{q_1} b_{q_2}\right) q.$$

Ahora, sea $G = (\mathbb{Q}^*, \times)$ y $K = \mathbb{C}$, entonces se tiene el álgebra de grupo $\mathbb{C}[\mathbb{Q}^*]$ con el producto

$$\otimes : \mathbb{C}[\mathbb{Q}^*] \times \mathbb{C}[\mathbb{Q}^*] \to \mathbb{C}[\mathbb{Q}^*]$$

el cual definimos como,

$$\left(\sum_{q\in\mathbb{Q}} a_q q\right) \otimes \left(\sum_{q\in\mathbb{Q}} b_q q\right) = \sum_{q\in\mathbb{Q}} \left(\sum_{q_1\cdot q_2=q} a_{q_1} b_{q_2}\right) q.$$

Proposición 3.1. $\mathbb{C}[\mathbb{Q}]$ *tiene una doble estructura de álgebra inducida por los productos* $\oplus$ *y* $\otimes$.

Demostración. Por definición $(\mathbb{C}[\mathbb{Q}], \oplus)$ tiene estructura de álgebra de grupo, donde $1_\oplus = 0_\mathbb{Q}$. Por la misma razón, $(\mathbb{C}[\mathbb{Q}^*], \otimes)$ es un álgebra de grupo, con $1_\otimes = 1_\mathbb{Q}$, la cual puede extender la estructura de álgebra a todo $\mathbb{C}[\mathbb{Q}]$, pues $1_\oplus \otimes f = \mathrm{Tr}(f)$ el cual está bien definido en $\mathbb{C}[\mathbb{Q}]$. Además, es claro que se comporta bien con las propiedades de álgebra. □

Ahora, si consideramos el subespacio $\mathbb{C}[\mathbb{Z}]$, el conjunto de elementos $f \in \mathbb{C}[\mathbb{Q}]$ tal que todos sus $a_q \neq 0$ tienen indice $q \in \mathbb{Z}$, Como $\mathbb{Z}$ es cerrado bajo las operaciones $+_{\mathbb{Q}}$ y $\times_{\mathbb{Q}}$ restringidas a $\mathbb{Z}$ tenemos el siguiente Corolario.

Corolario 3.1. *El subespacio $\mathbb{C}[\mathbb{Z}]$ es cerrado con respecto a ambas estructuras de álgebra de grupo y por lo tanto es una doble subálgebra de $\mathbb{C}[\mathbb{Q}]$.*

Notemos que en todo el estudio de $\mathbb{C}[\mathbb{Q}]$ nunca utilizamos el hecho de que $K = \mathbb{Q}$ si no solo las propiedades de campo de este, por lo tanto, todas las Proposiciones anteriores son validas para K un campo numérico de grado n sobre $\mathbb{Q}$. Es decir, es cierto que $\mathbb{C}[K]$ es una doble álgebra de grupo y $\mathbb{C}[O_K]$ es una doble subálgebra de $\mathbb{C}[\mathbb{Q}]$, donde O_K es el anillo de enteros de K.

Teorema 3.1. *Las estructuras de $\mathbb{C}$-álgebra de $\mathbb{C}[\mathbb{Q}]$ no obedecen la ley distributiva, i.e. existen $a, b, c \in \mathbb{C}[K]$ tales que $(a \oplus b) \otimes c \neq (a \oplus c) \otimes (b \oplus c)$.*

Demostración. Para esto basta tomar $a = 1$, $b = 2$ y $c = (3 + 4)$. Por un lado tenemos que $(1 \oplus 2) \otimes (3 + 4) = 3 \otimes (3 + 4) = (3 \otimes 3) + (3 \otimes 4) = 9 + 12$, luego por otro lado $(1 \otimes (3 + 4)) \oplus (2 \otimes (3 + 4)) = (3 + 4) \oplus (6 + 8) = 9 + 11 + 10 + 12$ el cual es diferente de $(1 \oplus 2) \otimes (3 + 4) = 9 + 12$. □

3.2 Proyectivización

Sea V un K-espacio vectorial, diremos que x está relacionado con x', $x \sim x'$, si existe $\lambda \in K^*$ tal que $x_i = \lambda x'_i$, es claro que $\sim$ define una relación de equivalencia para los elementos $x \in V - \{0\}$.

Se define el *proyectivizado* $\mathbb{P}V$ de V un K-espacio vectorial, como

$$\mathbb{P}V = V - \{0\} / \sim = \ (V - \{0\})/K^*.$$

Note que $\mathbb{P}V$ no es un espacio vectorial, pues no tiene neutro aditivo, luego la estructura de grupo $(V, +)$ se pierde al tomar su proyectivización.

Dado que $\mathbb{C}[\mathbb{Q}]$ es un $\mathbb{C}$-espacio vectorial podemos hablar de su proyectivización,

$$\mathbb{PC}[\mathbb{Q}] = \mathbb{C}[\mathbb{Q}] - \{0\} / \mathbb{C}^*,$$

Por cuestiones de notación denotemos, por $[f]$ a los elementos de $\mathbb{PC}[\mathbb{Q}]$ donde $f \in \mathbb{C}[\mathbb{Q}]$.

Proposición 3.2. *El producto de Cauchy $\oplus$ está bien definido en $\mathbb{PC}[\mathbb{Q}]$.*

Demostración. Consideremos $f, f' \in [f]$ $(f = cf')$ y $g, g' \in [g]$ $(g = dg')$, con c y d distintos de cero,

$$\begin{aligned} f \oplus g &= \left(\sum_q a_q q\right) \oplus \left(\sum_q b_q q\right) = \left(\sum_q (ca'_q)q\right) \oplus \left(\sum_q (db'_q)q\right) \\ &= \sum_q \left(\sum_{q_1+q_2=q} (ca'_{q_1})(db'_{q_2})\right) q = cd \sum_q \left(\sum_{q_1+q_2=q} (a'_{q_1} b'_{q_2})\right) q \\ &= cd \left(\sum_q a'_q q\right) \oplus \left(\sum_q b'_q q\right) = cd(f' \oplus g'). \end{aligned}$$

Por lo tanto $f \oplus g$ está bien definido. □

Sea $T : \mathbb{C}[\mathbb{Q}] \to \mathbb{C}$ un mapeo definido como

$$T(f) = \sum_q a_q,$$

al cual llamaremos, *mapeo de aumentación*.

Sea $f \in \mathbb{C}[\mathbb{Q}]$, $f \neq 0$, tal que $T(f) = 0$, luego

$$1_\oplus \otimes f = 1_\oplus \otimes \sum_q a_q q = \left(\sum_q a_q\right) 1_\oplus = 0.$$

Por lo tanto, notemos que si proyectivizamos a $\mathbb{C}[\mathbb{Q}]$ de la manera usual el producto de Dirichlet $\otimes$ no está bien definido para los elementos f tales que $T(f) = 0$. Por lo tanto, definiremos una nueva proyectivización como sigue. Consideraremos el conjunto

$$\mathbb{C}[\mathbb{Q}]^* = \mathbb{C}[\mathbb{Q}] - \{f \in \mathbb{C}[\mathbb{Q}] : T(f) = 0\}$$

luego definimos nuestra proyectivización como la hipersuperficie,

$$\mathbb{PC}[\mathbb{Q}] \supseteq N_0[\mathbb{Q}] = \mathbb{C}[\mathbb{Q}]^* / \mathbb{C}^*.$$

Proposición 3.3. *Dados $f, g \in \mathbb{C}[\mathbb{Q}]$ tenemos que*

$$T(f) \cdot T(g) = T(f \oplus g) = T(f \otimes g).$$

Demostración. Para la primera igualdad tenemos que

$$T(f) \cdot T(g) = \left(\sum_q a_q\right) \cdot \left(\sum_q b_q\right) = \sum_q \left(\sum_{q_1+q_2=q} a_{q_1} b_{q_2}\right) = T(f \oplus g).$$

Ahora consideremos,

$$f = \sum_q a_q q = \sum_{q<0} a_q q + a_0 + \sum_{q>0} a_q q = f_- + f_0 + f_+.$$

Notemos que a cada f_+ le podemos asociar la serie de Dirichlet $D_f = \sum_{q>0} a_q q^{-s}$. Luego la traza de la serie de Dirichlet D_{f_+} asociada a f_+ es $T(D_{f_+}) = D_{f_+}(0)$ y considerando la identificación de f_+ con D_{f_+} tenemos que

$$\begin{aligned} T(D_{f_+\otimes g_+}) &= T(D_{f_+} * D_{g_+}) = (D_{f_+} * D_{g_+})(0) = D_{f_+}(0) * D_{g_+}(0) \\ &= T(D_{f_+})T(D_{g_+}) = T(f_+)T(g_+). \end{aligned}$$

Dado $f_- = \sum_{q<0} a_q q$, definamos

$$\tilde{f}_- = \sum_{|q|>0} a_q \left|q\right|,$$

luego $\tilde{f}_-$ define una serie de Dirichlet $D_{\tilde{f}_-}$, y además se cumple que $T(f_-) = T(\tilde{f}_-)$ entonces $T(f_- \otimes g_-) = T(\tilde{f}_- \otimes \tilde{g}_-) = T(\tilde{f}_-)T(\tilde{g}_-) = T(f_-)T(g_-)$. De manera análoga se tiene que $T(f_- \otimes g_+) = T(f_-)T(g_+)$.

$$\begin{aligned} T(f \otimes g) &= T((f_- + f_0 + f_+) \otimes (g_- + g_0 + g_+)) \\ &= T(f_- \otimes g_-) + T(f_- \otimes g_0) + T(f_- \otimes g_+) \\ &\quad + T(f_0 \otimes g_-) + T(f_0 \otimes g_0) + T(f_0 \otimes g_+) \\ &\quad + T(f_+ \otimes g_-) + T(f_+ \otimes g_0) + T(f_+ \otimes g_+) \\ &= T(f_-)T(g_-) + T(f_-)T(g_0) + T(f_-)T(g_+) \\ &\quad + T(f_0)T(g_-) + T(f_0)T(g_0) + T(f_0)T(g_+) \\ &\quad T(f_+)T(g_-) + T(f_+)T(g_0) + T(f_+)T(g_+) \\ &= T(f_- + f_0 + f_+)T(g_- + g_0 + g_+) \\ &= T(f)T(g). \end{aligned}$$

□

Corolario 3.2. *$\mathbb{C}[\mathbb{Q}]^*$ es cerrado con respecto a $\oplus$, $\otimes$ y la multiplicación por un escalar $\lambda \in \mathbb{C}^*$.*

Demostración. Consideremos $f, g \in \mathbb{C}[\mathbb{Q}]^*$ de donde tenemos que $T(f)\cdot T(g) \neq 0$ luego por la Proposición 3.3 tenemos que $T(f \oplus g) = T(f \otimes g) \neq 0$ lo que implica que $f \oplus g, f \otimes g \in \mathbb{C}[\mathbb{Q}]^*$. La multiplicación por escalar se sigue de la linealidad de T. □

Corolario 3.3. *$N_0(\mathbb{Q})$ es un doble semigrupo con las operaciones $\oplus$, $\otimes$ inducidas por $\mathbb{C}[\mathbb{Q}]^*$.*

Demostración. Por el Corolario 3.2, $\oplus$, $\otimes$ están bien definidas en $N_0(\mathbb{Q})$ y por la Proposición 3.1 tenemos la asociatividad. □

De manera análoga tenemos que $N_0(\mathbb{Z})$ es un doble subsemigrupo de $N_0(\mathbb{Q})$.

Proposición 3.4. *Existen dos monomorfismos canónicos*

$$\mathbb{Q} \hookrightarrow N_0(\mathbb{Q}) \quad y \quad \mathbb{Z} \hookrightarrow N_0(\mathbb{Z})$$

.

Demostración. El monomorfismo canónico de $\mathbb{Q} \hookrightarrow N_0(\mathbb{Q})$ está dado por el mapeo $q \mapsto [q]$, el cual es inyectivo ya que si tenemos dos elementos $[q] = [q']$ en $N_0(\mathbb{Q})$ esto implica que $q' = \lambda q$ para alguna $\lambda \in \mathbb{C}$ distinta de cero y por lo tanto $q = q'$ en $\mathbb{Q}$. Restringiendo este monomorfismo a $\mathbb{Z}$ se tiene el monomorfismo de $\mathbb{Z} \hookrightarrow N_0(\mathbb{Z})$. □

Nuevamente, como en la sección anterior todas las Proposiciones pueden ser reproducidas de manera similar si cambiamos a $\mathbb{Q}$ por un campo numérico K. Lo cual nos da $\mathbb{N}_0(K)$.

3.3 El espacio $N(K)$

Dada K una extensión de Galois de $\mathbb{Q}$ y O_K el anillo de enteros de K, tenemos una forma bilineal simétrica canónica en K visto como $\mathbb{Q}$-espacio vectorial inducida por la *traza*

$$(x, y) \mapsto \mathrm{Tr}(xy).$$

La cual nos permite asociar a cada ideal fraccional $\mathfrak{U}$ de K el O_K-módulo dual

$$\mathfrak{d}_{\mathfrak{U}}^{-1} = \{x \in K : \mathrm{Tr}(x\mathfrak{U}) \subset \mathbb{Z}\}.$$

El cual es también un ideal fraccional de K. La noción de dualidad se debe al isomorfismo

$$\mathfrak{d}_{\mathfrak{U}}^{-1} \to \mathrm{Hom}_{\mathbb{Z}}(\mathfrak{U}, \mathbb{Z}),$$

$$x \mapsto (y \mapsto \mathrm{Tr}(xy)).$$

En particular si $\mathfrak{U} = O_K$, tenemos el O_K-módulo

$$\mathfrak{d}_{O_K}^{-1} \cong \mathrm{Hom}_{\mathbb{Z}}(O_K, \mathbb{Z}).$$

Luego al ideal fraccional

$$\mathfrak{d}_K^{-1} = \mathfrak{d}_{O_K}^{-1} = \{x \in K : \mathrm{Tr}(xO_K) \subset \mathbb{Z}\} \supset O_K,$$

lo llamaremos el *diferente inverso* de K [11]. Nótese que el diferente inverso en general no es un anillo si no solo un O_K-módulo finitamente generado, de hecho $\mathfrak{d}_K^{-1}$ es un anillo si y solo si este coincide con el anillo de enteros O_K.

Consideremos el grupo circular,

$$S^1 = \{z \in \mathbb{C} : |z| = 1\},$$

con la topología usual. Y sea G un grupo abeliano localmente compacto. Luego un *caracter* de G se define como un homomorfismo continuo

$$\chi : G \to S^1.$$

El conjunto de caracteres de G forma un grupo multiplicativo con la operación $\oplus$ (producto puntual) definida como $(\chi \oplus \eta)(a) = \chi(a)\eta(a)$, que es inducida por el producto de S^1, y donde la identidad se define como el homomorfismo $\chi(a) = 1$ para toda $a \in G$, el cual se denota como $\mathrm{Char}(G)$ (Ver Apéndice C). Algunos ejemplos de grupos de caracteres son los siguientes.

Ejemplo 1. $\mathrm{Char}(\mathbb{Z}) = S^1 = \mathbb{R}/\mathbb{Z}$, de manera más general, $\mathrm{Char}(\mathbb{Z}^n) \cong \mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$ como grupos topológicos. Además, por el Teorema de dualidad de Pontryagin tenemos que,

$$\mathbb{Z}^n \cong \mathrm{Char}(\mathbb{T}^n) = \left\{\chi_N(x) = e^{2\pi i N\cdot x} : N \in \mathbb{Z}^n, x \in \mathbb{R}^n\right\}.$$

Ejemplo 2. Sea $K/\mathbb{Q}$ una extensión de grado n,

$$\mathbb{R}^n \cong \mathrm{Char}(K_\infty) = \left\{\chi_y(x) = e^{2\pi i \mathrm{Tr}(yx)} : y \in K_\infty\right\}.$$

Nótese que como K_∞ es localmente compacto por el Teorema de dualidad de Pontryagin su grupo de caracteres es isomorfo a sí mismo como grupo topológico.

Teorema 3.2. *Sea K una extensión de Galois de $\mathbb{Q}$. Entonces* $\mathrm{Char}(\hat{\mathbb{S}}_K)$ *pose una segunda operación $\otimes$, para la cual tenemos la siguiente identificación canónica*

$$\mathrm{Char}(\hat{\mathbb{S}}_K) \cong K.$$

Además, si $\mathfrak{d}_K^{-1} = O_K$, la operación $\otimes$ restringida a $\mathrm{Char}(\mathbb{T}_K)$ *hace de este un subanillo de* $\mathrm{Char}(\hat{\mathbb{S}}_K)$.

Demostración. Consideremos un caracter $\chi : \hat{\mathbb{S}}_K \to S^1$. Dado que $K_\infty \hookrightarrow \hat{\mathbb{S}}_K$ de manera densa entonces la restricción de un caracter de $\hat{\mathbb{S}}_K$ a K_∞ es de la forma

$$x \mapsto \exp(2\pi i \mathrm{Tr}(yx)),$$

para algún $y \in K_\infty$. Además, χ queda completamente determinado por su restricción a la hoja canónica K_∞, $\chi \mapsto \chi|_{K_\infty}$, y por lo tanto el mapeo es inyectivo. Por otro lado, el caracter χ restringido a $\hat{O}_K \subset \hat{\mathbb{S}}_K$, la completación profinita de O_K, se factoriza a través de un cociente finito. Es decir,

$$\chi|_{\hat{O}_K} : \hat{O}_K \to O_K/\mathfrak{a} \to \mathbb{C},$$

para algún ideal $\mathfrak{a} \subset O_K$. Lo que significa que χ se anula en $\hat{\mathfrak{a}}$, *i.e.* $\hat{\mathfrak{a}} \subset ker\chi$ luego para toda $x \in \hat{\mathbb{S}}_K$, $\chi(x+\hat{a}) = \chi(x)$, lo que significa que χ es constante a lo largo de las fibras de la proyección $\hat{\mathbb{S}}_K \to \mathbb{T}_\mathfrak{a} = K_\infty/\mathfrak{a}$. Entonces la restricción de χ a K_∞ debe de ser de la forma,

$$K_\infty \to \mathbb{T}_\mathfrak{a} \to \mathbb{C},$$

lo que implica que y está en $\{y \in K_\infty : \mathrm{Tr}(q \cdot \mathfrak{a}) \subset \mathbb{Z}\}$. Ahora, afirmamos que:

Sí $y \in K_\infty$ y cumple que $\mathrm{Tr}(y \cdot K) \subset \mathbb{Q}$ entonces $y \in K$.

Prueba de la afirmación: Consideremos una base entera $\alpha_1, \ldots, \alpha_n$ de K y sea A la matriz invertible de $n \times n$ cuyos ij-elementos son de la forma $\nu_j(\alpha_i)$, donde $\nu_1, \ldots, \nu_n$ son los lugares de K. Luego por hipótesis $Ay \in \mathbb{Q}^n$, o dado que A es invertible, $y \in A^{-1}\mathbb{Q}^n$. Como K es de Galois todas las entradas de A pertenecen a K, por lo tanto $y \in K \subset K_\infty$. Supongamos que es falso, es decir, supongamos que $y \notin K$. Luego existe algún automorfismo $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ y una coordenada y_ν tal que $\sigma(y_\nu) \neq y_{\sigma\nu}$. Sea A^ν el vector columna $(\nu(\alpha_1), \ldots, \nu(\alpha_n))^T$ de la matriz A indexada por el lugar ν. Luego

$$\sum A^\nu y_\nu = q \in \mathbb{Q}^n.$$

La acción de $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ permuta los vectores columna A^ν en la ecuación y fija a q, pero no permuta las entradas de y. Luego existe un vector $y' \neq y$ para el cual $Ay' = q$. Lo que implica que el núcleo de la transformación asociada a A es no trivial, lo cual es una contradicción pues A es invertible. Por lo tanto $y \in K$ ósea $Im(\chi \mapsto \chi|_{K_\infty}) \subset K$.

Ahora consideremos $\alpha \in K$, arbitraria, entonces el caracter en K_∞ definido por $\exp(2\pi i \mathrm{Tr}(\alpha x))$ se extiende a $\hat{\mathbb{S}}_K$. En efecto, por teoría algebraica de números [9], [11], existe un ideal entero $\mathfrak{a} \subset O_K$ tal que $\alpha \cdot \mathfrak{a} \subset O_K$. Luego el caracter $\exp(2\pi i \mathrm{Tr}(\alpha x))$ desciende a un caracter en $\mathbb{T}_\mathfrak{a}$ el cual compuesto con la proyección $K_\infty \to \mathbb{T}_\mathfrak{a}$ nos da la extensión de $\exp(2\pi i \mathrm{Tr}(\alpha x))$ a todo $\hat{\mathbb{S}}_K$. Por lo tanto, el mapeo $\chi \to \chi|_{K_\infty}$ identifica canónicamente a $\mathrm{Char}(\hat{\mathbb{S}}_K)$ con el grupo abeliano $(K, +)$. Luego la operación producto de K induce un producto $\otimes$ en $\mathrm{Char}(\hat{\mathbb{S}}_K)$ vía pull back.

Por último, si $\mathfrak{d}_K^{-1} = O_K$ el mapeo $x \mapsto \exp(2\pi i \mathrm{Tr}(yx))$ identifica a $\mathrm{Char}(\mathbb{T}_K)$ con O_K de modo que la restricción de $\otimes$ a $\mathrm{Char}(\mathbb{T}_K)$ es cerrada y le da estructura de anillo al grupo de caracteres de $\mathbb{T}_K$, el cual resulta isomorfo a O_K.

□

El conjunto de caracteres $\chi_q \in \mathrm{Char}(G)$ forma un sistema ortonormal completo en $L^2(G, \mathbb{C})$ [18]. Luego para todo $f \in L^2(G, \mathbb{C})$ existe una serie de Fourier convergente de la forma

$$f = \sum_{q \in \mathrm{Char}(G)} a_q \cdot \chi_q,$$

donde

$$a_n = \langle \chi_q, f \rangle = \int_G \chi_q(zw^{-1}) f(w) d\mu \in \mathbb{C}.$$

Ejemplo 3. Consideremos a $\mathbb{T}_K$ el toro de Minkowski con grupo de caracteres

$$\mathrm{Char}(\mathbb{T}_K) = \left\{ \chi_m(x) = \exp(2\pi i \mathrm{Tr}(mx)) : m \in \mathfrak{d}_K^{-1} \right\},$$

donde m se puede ver como un vector debido a la inclusión canónica que existe $\mathfrak{d}_K^{-1} \hookrightarrow K_\infty$. Donde $\mathrm{Char}(\mathbb{T}_K)$ es un sistema ortonormal completo en

$L^2(\mathbb{T}_K, \mathbb{C})$, y por tanto cada elemento $f \in L^2(\mathbb{T}_K, \mathbb{C})$ se puede escribir de la forma,

$$f(x) = \sum_{m \in \mathfrak{d}_K^{-1}} a_m \exp(2\pi i \mathrm{Tr}(mx)),$$

Otro ejemplo es el caso de $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ para el cual cada $f(\hat{x})$ se puede representar como

$$f(\hat{x}) = \sum_{q \in K} a_q \chi_q(\hat{x}),$$

donde $\chi_q \in \mathrm{Char}(\hat{\mathbb{S}}_K)$ y $\{a_q\} \in l^2$.

Lema 3.1. *$L^2(\mathbb{T}_K, \mathbb{C})$ es canónicamente un subespacio de $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$.*

Demostración. Notemos que como estamos en un espacio de Hilbert, la suma $\|f\|^2 = \sum |a_q|^2$ converge con respecto a cualquier subconjunto bien ordenado de índices de K. Luego podemos identificar a $L^2(\mathbb{T}_K, \mathbb{C})$ con el subespacio de $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ cuyas series de Fourier satisfacen que $a_q = 0$ para $q \notin \mathfrak{d}_K^{-1}$. □

Notemos del Ejemplo 3, que no es posible expresar a los elementos de $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ en términos de la función exponencial como en el caso de $L^2(\mathbb{T}_K, \mathbb{C})$. No obstante, si restringimos f a K_∞, la cual como vimos en el capítulo anterior es una hoja densa de $\hat{\mathbb{S}}_K$, podemos identificar a $\chi_q(x) = \exp(2\pi i \mathrm{Tr}(qx)) \equiv \eta^q$, y escribir a f como una L^2 serie de Puiseaux,

$$f(\eta) = \sum_{q \in K} a_q \eta^q.$$

Definición 5. Sea $K/\mathbb{Q}$ una extensión de Galois y sea $f, g \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ los cuales se puede desarrollar como: $f = \sum a_q \chi_q$, $g = \sum b_q \chi_q$. Entonces, definimos el *producto de Cauchy* como la L^2 extensión del producto puntual de funciones continuas, el cual está dado como:

$$f \oplus g = \sum_q \left(\sum_{q_1 + q_2 = q} a_{q_1} b_{q_2} \right) \chi_q,$$

siempre que la suma de la derecha sea convergente en $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$.

Dado $f \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ denotaremos por $Dom_\oplus(f)$, al conjunto de $g \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ para los cuales $f \oplus g$ está definido.

Proposición 3.5. *Existe un monomorfismo canónico con imagen densa de,*

$$(\mathbb{C}[K], \oplus) \hookrightarrow (L^2(\hat{\mathbb{S}}_K, \mathbb{C}), \oplus).$$

Demostración. Consideremos el mapeo dado por:

$$\sum_{q \in K} a_q q \mapsto \sum_{q \in K} a_q \eta^q,$$

de $\mathbb{C}[K] \hookrightarrow L^2(\hat{\mathbb{S}}_K, \mathbb{C})$, el cual induce el monomorfismo que deseamos. Además, el mapeo es denso ya que cualquier serie finita $\sum_q a_q \eta^q$ tiene asociado un representante $\sum_q a_q q$ en $\mathbb{C}[K]$ y dado que series finitas son densas en $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ hemos probado la Proposición. □

Recordemos del Teorema 3.2 que, $\chi_p \otimes \chi_q = \chi_{pq}$. En notación exponencial $\eta^p \otimes \eta^q = \eta^{qp} = (\eta^p)^q = (\eta^q)^p$, donde podemos notar que este producto corresponde a la composición de funciones usual $\eta^p \circ \eta^q$, luego podemos definir el siguiente producto.

Definición 6. Sea $K/\mathbb{Q}$ una extensión de Galois y sea $f, g \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ los cuales se puede desarrollar como: $f = \sum a_q \chi_q$, $g = \sum b_q \chi_q$. Definimos el *producto de Dirichlet* como:

$$f \otimes g = \sum_q \left(\sum_{q_1 q_2 = q} a_{q_1} b_{q_2} \right) \chi_q,$$

siempre que la suma de la derecha sea convergente en $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$.

Proposición 3.6. *Existe un monomorfismo canónico con imagen densa de*

$$(\mathbb{C}[K], \otimes) \hookrightarrow (L^2(\hat{\mathbb{S}}_K, \mathbb{C}), \otimes).$$

Demostración. La prueba es análoga a la prueba del Teorema 3.5. □

De manera similar, como en el producto de Cauchy, dado $f \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ denotaremos por $Dom_{\otimes}(f)$, al conjunto de $g \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ para los cuales $f \otimes g$ está definido.

Teorema 3.3. *Dado $f, g \in L^2(\hat{\mathbb{S}}_K, \mathbb{C}) \cap L^1(\hat{\mathbb{S}}_K, \mathbb{C})$ tenemos que $f \oplus g$ y $f \otimes g$ están en $L^2(\hat{\mathbb{S}}_K, \mathbb{C}) \cap L^1(\hat{\mathbb{S}}_K, \mathbb{C})$.*

Demostración. Usando la desigualdad de Schwarz [1]

$$|f \oplus g|_2^2 = |fg|_2^2 \leq \sum_q \left(\sum_{q_1 + q_2 = q} |a_{q_1}|^2 |b_{q_2}|^2 \right) \leq \sum_{q_1, q_2} |a_{q_1}|^2 |b_{q_2}|^2$$
$$= \sum_{q_1} |a_{q_1}|^2 \sum_{q_2} |b_{q_2}|^2 = \sum_q |a_q|^2 \sum_q |b_q|^2 < \infty.$$

ya que el producto de dos series absolutamente sumables es sumable. De la misma manera,

[1] La desigualdad de Schwarz dice que si f y $G \in L^2(G, \mathbb{C})$ entonces $\int_G |f\bar{g}|\, d\mu \leq \left\{ \int_G |f|^2 \, d\mu \right\}^{1/2} \left\{ \int_G |g|^2 \, d\mu \right\}^{1/2}$ [16].

$$|f \otimes g|_2^2 \leq \sum_q \sum_{q_1 q_2 = q} |a_{q_1}|^2 |b_{q_2}|^2 \leq \sum_{q_1, q_2} |a_{q_1}|^2 |b_{q_2}|^2 = \sum_q |a_q|^2 \sum_q |b_q|^2 < \infty.$$

□

Teorema 3.4. *Existe un conjunto denso $P \subset L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ para el cual está bien definido el producto de Cauchy $\oplus$ y el producto de Dirichlet $\otimes$.*

Demostración. Sea $P = C_0(\hat{\mathbb{S}}_K, \mathbb{C})$ el conjunto de funciones continuas de $\hat{\mathbb{S}}_K$ en $\mathbb{C}$ las cuales son densas en $L^p(\hat{\mathbb{S}}_K, \mathbb{C})$ para todo $p \in \mathbb{N}$. Luego, cualquier elemento $f \in C_0(\hat{\mathbb{S}}_K, \mathbb{C})$ está en $L^1(\hat{\mathbb{S}}_K, \mathbb{C}) \cap L^2(\hat{\mathbb{S}}_K, \mathbb{C})$, por lo tanto el producto de Cauchy $\oplus$ y el producto de Dirichlet $\otimes$ están bien definidos en $P = C_0(\hat{\mathbb{S}}_K, \mathbb{C})$. □

Un conjunto A se dice que es un *álgebra parcial* si A tiene estructura de K-álgebra con la excepción de que la operación $\odot$ que le da estructura de anillo a A solo está parcialmente definida.

Proposición 3.7. *$L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ tiene estructura de doble álgebra parcial de grupos con las operaciones $\oplus$ y $\otimes$.*

Demostración. Es claro que bajo el producto de Cauchy $\oplus$ $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$, es un álgebra parcial, pues coincide con el producto puntual de funciones el cual claramente es distributivo y conmutativo con respecto a la suma usual de funciones. Es claro que $(L^2(\hat{\mathbb{S}}_K, \mathbb{C}), \otimes)$ tiene estructura de anillo parcial con elemento identidad $1_\otimes$. Así que solo verificaremos la conmutatividad y distributividad con respecto a la suma usual.

$$(f \otimes g)(\eta) = \sum_q \left(\sum_{q = q_1 q_2} a_{q_1} b_{q_2} \right) \eta^q = \sum_q \left(\sum_{q = q_1 q_2} b_{q_1} a_{q_2} \right) \eta^q = (g \otimes f)(\eta).$$

Luego el producto de Dirichlet es conmutativo siempre que $f \otimes g$ sea convergente.

$$\begin{aligned} f \otimes (g + h) &= \sum_q \left(\sum_{q = q_1 q_2} a_{q_1} (b_{q_2} + c_{q_2}) \right) \eta^q \\ &= \sum_q \left(\sum_{q = q_1 q_2} a_{q_1} b_{q_2} + a_{q_1} c_{q_2}) \right) \eta^q \\ &= f \otimes g + f \otimes h, \end{aligned}$$

siempre que el producto sea convergente. Por tanto, $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ tiene estructura de doble álgebra parcial. □

Corolario 3.4. *Existe un doble monomorfismo canónico de álgebras de grupo*

$$\mathbb{C}[K] \hookrightarrow L^2(\hat{\mathbb{S}}_K, \mathbb{C}),$$

con imagen densa dado por el mapeo $q \mapsto \eta^q$.

Demostración. Tanto la existencia, como la densidad de la imagen del monomorfismo, se sigue de las Proposiciones 3.5 y 3.6. □

Dado que $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ es un espacio métrico completo y $\mathbb{C}[K]$ es denso en $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ tenemos que $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ es la L^2-*completación* de $\mathbb{C}[K]$.

Nótese que si restringimos el mapeo $q \mapsto \eta^q$ a $\mathfrak{d}_K^{-1}$ tenemos el monomorfismo

$$\mathbb{C}\left[\mathfrak{d}_K^{-1}\right] \hookrightarrow L^2(\mathbb{T}_K, \mathbb{C}).$$

En particular si $\mathfrak{d}_K^{-1} = O_K$ entonces tenemos que

$$\mathbb{C}[O_K] \hookrightarrow L^2(\mathbb{T}_K, \mathbb{C}).$$

Por otro lado, podemos hablar de la proyectivización de $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$. Definiendo

$$L^2(\hat{\mathbb{S}}_K, \mathbb{C})^* = L^2(\hat{\mathbb{S}}_K, \mathbb{C}) - \left\{ f : \mathrm{Tr}(f) = \sum_q a_q = 0 \right\},$$

y entonces tenemos que

$$N(K) = L^2(\hat{\mathbb{S}}_K, \mathbb{C})^* / \mathbb{C}^*,$$

Proposición 3.8. *N(K) es un doble semigrupo parcial con respecto a $\oplus$ y $\otimes$.*

Demostración. Sabemos que $T(f)T(g) = T(f \oplus g) = T(f \otimes g)$ lo cual nos muestra que el producto de Cauchy $\oplus$ (resp. el producto de Dirichlet $\otimes$) de dos elementos $f, g \in N(K)$ con traza distinta de cero tiene traza distinta de cero, siempre que $f \oplus g$ (resp. $f \otimes g$) sean convergentes. Luego el producto es cerrado. Además, es claro que cumple las propiedades de semigrupo parcial con respecto a $\oplus$ y (resp. $\otimes$) heredadas de $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$. □

Proposición 3.9. *Existe un monomorfismo canónico*

$$K \hookrightarrow N_0(K) \hookrightarrow N(K),$$

donde $N_0(K)$ tiene imagen densa en $N(K)$.

Demostración. El monomorfismo dado en el Corolario 3.4, $q \mapsto \eta^q$, de $\mathbb{C}[K]$ en $L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ induce un monomorfismo de clases $[q] \mapsto [\eta^q]$ de $N_0(K)$ en $N(K)$ el cual tiene imagen densa. □

Consideremos ahora el caso particular en que $K = \mathbb{Q}$ y consideremos $f, g \in C_0(\mathbb{T}_{\mathbb{Q}}, \mathbb{C}) \subset C_0(\hat{\mathbb{S}}_K, \mathbb{C})$ con $a_n = b_n = 0$ para $n \leq 0$. Luego de teoría analítica de números tenemos que f y g definen, vía una transformada de Mellin, las series de Dirichlet convergentes para $\Re(s) > 0$,

$$D_f(y) = \sum_n a_n n^{-2\pi i y} = \sum_{n=1}^{\infty} a_n n^{-s},$$

y

$$D_g(y) = \sum_n b_n n^{-2\pi i y} = \sum_{n=1}^{\infty} b_n n^{-s},$$

con $y \in \mathbb{R}$ y

$$D_{f\otimes g} = D_f * D_g,$$

el producto usual de series de Dirichlet [15]. Esto nos muestra que $N(\mathbb{Z})$ con el producto de Dirichlet codifica la aritmética de las series de Dirichlet, las L-funciones y las funciones zeta convergentes (salvo traslaciones) de teoría analítica de números clásica.

3.4 Espacios de Hardy

Sea $\hat{\mathfrak{S}}_{\mathbb{Q}}$ el solenoide hiperbolizado asociado a $\mathbb{Q}$, el cual como vimos es una laminación cuyas hojas densas L son isomorfas al disco de Poincaré. Diremos que una función continua $F : \hat{\mathfrak{S}}_{\mathbb{Q}} \to \mathbb{C}$ es $holomorfa$ si su restricción a L $(F|_L)$ es holomorfa para cada hoja L. De manera equivalente dado que todas las hojas son densas, F es holomorfa si su restricción a la hoja canónica $\mathbb{H}_{\mathbb{Q}}$, $(F|_{\mathbb{H}})$ es holomorfa.

Para cada elemento $t \in (0,\infty)$ consideremos $\hat{\mathbb{S}}_{\mathbb{Q}}(t) \subset \hat{\mathfrak{S}}_{\mathbb{Q}} \cong \hat{\mathbb{S}}_{\mathbb{Q}} \times (0,\infty)$ el subconjunto de puntos de $\hat{\mathfrak{S}}_{\mathbb{Q}}$ cuya coordenada imaginaria es igual a t. Dado que $\hat{\mathbb{S}}_{\mathbb{Q}}(t) \cong \hat{\mathbb{S}}_{\mathbb{Q}}$ podemos dotar a $\hat{\mathbb{S}}_{\mathbb{Q}}(t)$ de una medida de Haar unitaria, luego $\mathrm{Vol}(\mathbb{S}_{\mathbb{Q}}(t)) = 1$.

Ahora dadas $F, G : \hat{\mathfrak{S}}_{\mathbb{Q}} \to \mathbb{C}$ podemos definir el siguiente producto interior hermitiano

$$\langle F, G\rangle_t = \int_{\hat{\mathbb{S}}_{\mathbb{Q}}(t)} F\overline{G} d\mu.$$

Definición 7. El *espacio de Hardy* asociado a $\mathbb{Q}$ es el espacio de Hilbert definido como

$$\mathrm{Har}\,[\mathbb{Q}] = \left\{ F : \hat{\mathfrak{S}}_{\mathbb{Q}} \to \mathbb{C} : F \text{ es holomorfa y } \sup_t \langle F, F\rangle_t < \infty \right\},$$

con producto interior $\langle \cdot, \cdot \rangle = \sup_t \langle \cdot, \cdot \rangle_t$.

Notemos que dado $F \in \mathrm{Har}\,[\mathbb{Q}]$, F tiene un L^2-límite definido en casi todo punto cuando $t \to 0$ (*i.e.* salvo un conjunto de medida cero)[18]. Luego $\lim_{t\to 0} F(x+t) = \partial F(x)$ define un elemento frontera

$$\partial F := f \in L^2(\hat{\mathbb{S}}, \mathbb{C}).$$

Ahora utilizando el desarrollo en series de Fourier valido aquí podemos escribir la restricción $F|_{\mathbb{H}_{\mathbb{Q}}}$ como sigue,

$$F|_{\mathbb{H}_{\mathbb{Q}}} = \sum_q a_q \exp(2\pi i q \cdot z) = \sum_q a_q (\exp(2\pi i q x)\exp(-2\pi q y)) = \sum_q a_q \xi^q,$$

donde $\xi = e^{2\pi i z}$ la proyectivización de η. Definimos el *cono positivo* en $\mathbb{R}$, como el conjunto de las y tales que $y > 0$.

Luego notemos que las series anteriores definen un elemento de $\mathrm{Har}\,[\mathbb{Q}]$ si $a_q = 0$ para toda q que no este contenida en el cono positivo en $\mathbb{R}$. Luego se sigue que $\|F\| = \sum_q |a_q|$, donde $\|\cdot\|$ denota la norma de Hardy, lo que implica la siguiente Proposición

Proposición 3.10. *El mapeo $F \longmapsto \partial F$ induce una inclusión isométrica de espacios de Hilbert.*

$$\mathrm{Har}\,[\mathbb{Q}] \hookrightarrow L^2(\hat{\mathbb{S}}_{\mathbb{Q}}, \mathbb{C}).$$

Una idea natural después de esta discusión seria el intentar tratar de construir una especie de extensión holomorfa de $\mathbb{Q}$ a partir de $\mathrm{Har}\,[\mathbb{Q}]$. Lo cual es necesario para poder describir todos los elementos de $L^2(\hat{\mathbb{S}}, \mathbb{C})$ como límites (elementos frontera) de funciones holomorfas.

Sea $D \subset \mathbb{C}$ un dominio, diremos que una función $f : D \to \mathbb{C}$ es *antiholomorfa* en D si $\bar{f} : D \to \mathbb{C}$ es holomorfa en D.

Luego podemos notar que para cada función $F : \hat{\mathfrak{S}}_{\mathbb{Q}} \to \mathbb{C}$ de $\mathrm{Har}\,[\mathbb{Q}]$ podemos tomar su conjugada $\bar{F} : \hat{\mathfrak{S}}_{\mathbb{Q}} \to \mathbb{C}$ la cual al restringirla a $\mathbb{H}_{\mathbb{Q}}$ también tiene un desarrollo de Fourier

$$\bar{F}|_{\mathbb{H}_{\mathbb{Q}}} = \sum_q a_q \exp(2\pi i q \cdot \bar{z}) = \sum_q a_q \xi^q,$$

donde $\xi = e^{2\pi i \bar{z}}$. La cual es convergente si $a_q = 0$ para todo $q \geq 0$ luego estas funciones definen el espacio de Hardy de las funciones antiholomorfas (las cuales están definidas en el plano inferior $\mathbb{H}^- = \mathbb{R} \times (-\infty, 0)$ el cual es inducido por el mapeo conjugación $\overline{(\cdot)} : \mathbb{H} \to \mathbb{H}^-$) el cual denotaremos como $\mathrm{Har}_-\,[\mathbb{Q}]$.

Luego a estos dos espacios los podemos indexar por el grupo de signos $\{+, -\} \cong \mathbb{Z}/2\mathbb{Z}$. Esta forma de ver a los índices nos será de gran utilidad cuando extendamos la noción de espacios de Hardy para un campo numérico arbitrario.

Para fijar notación a partir de ahora denotaremos por F_+ (F_-) a los elementos de $\mathrm{Har}_+\,[\mathbb{Q}] = \mathrm{Har}\,[\mathbb{Q}]$ (resp. $\mathrm{Har}_-\,[\mathbb{Q}]$) y F_0 a las funciones tales que $a_q = 0$ para toda $q \neq 0$. Luego cada elemento $f \in L^2(\hat{\mathbb{S}}_{\mathbb{Q}}, \mathbb{C})$ queda completamente determinado por elementos de los espacios de Hardy antes definidos.

Corolario 3.5. *Cada elemento $f \in L^2(\hat{\mathbb{S}}_{\mathbb{Q}}, \mathbb{C})$ determina una terna (F_+, F_0, F_-) donde*

- $F_+ = \sum_{q>0} a_q \exp(2\pi i q \cdot z) \in \mathrm{Har}\,[\mathbb{Q}]$,
- $F_0 = a_0 \in \mathbb{C}$ *y*
- $F_- = \sum_{q<0} a_q \exp(2\pi i q \cdot \bar{z}) \in \mathrm{Har}_-\,[\mathbb{Q}]$.

i.e.

$$L^2(\hat{\mathbb{S}}_{\mathbb{Q}}, \mathbb{C}) \cong \mathrm{Har}_\bullet\,[\mathbb{Q}] = \mathrm{Har}_+\,[\mathbb{Q}] \oplus \mathbb{C} \oplus \mathrm{Har}_-\,[\mathbb{Q}]\,,$$

donde el producto interior es la suma directa de los productos en cada sumando.

Una función $f : \Omega \to \mathbb{C}$, con $\Omega \in \mathbb{C}^n$, es *holomorfa* si para cada $j = 1, \cdots, n$ y cada $z_1, \cdots, z_{j-1}, z_{j+1}, \cdots, z_n$, la función

$$\gamma \mapsto f(z_1, \cdots, z_{j-1}, \gamma, z_{j+1}, \cdots, z_n),$$

es holomorfa en el sentido clásico de una variable en el conjunto

$$\Omega(z_1, \cdots, z_{j-1}, z_{j+1}, \cdots, z_n) = \{\gamma \in \mathbb{C} : (z_1, \cdots, z_{j-1}, \gamma, z_{j+1}, \cdots, z_n) \in \Omega\},$$

[26]. Consideremos $K/\mathbb{Q}$ una extensión finita de Galois. Diremos que $F : \hat{\mathfrak{S}}_K \to \mathbb{C}$ es holomorfa si su restricción a cada hoja L (las cuales son isomorfas al polidisco de Poincaré definido como el conjunto $\{z \in \mathbb{C} : |z_j| < 1,\ j = 1, \cdots, n\}$) es holomorfa. En otras palabras F es holomorfa si su restricción a la hoja canónica $\mathbb{H}_K$ es holomorfa. Luego dado un vector $t \in (0, \infty)^n$ tenemos que $\hat{\mathbb{S}}_K(t) \cong \hat{\mathbb{S}}_K$ se puede dotar de una medida de Haar μ unitaria a $\hat{\mathbb{S}}_K(t)$, entonces $\mathrm{Vol}(\hat{\mathbb{S}}_K(t)) = 1$ y podemos definir el producto interior de $F, G : \hat{\mathfrak{S}}_K \to \mathbb{C}$ como

$$\langle F, G \rangle_t = \int_{\hat{\mathbb{S}}_K(t)} F\overline{G} d\mu.$$

Luego el espacio de Hardy asociado a K se define como:

$$\mathrm{Har}\,[K] = \left\{ F : \hat{\mathfrak{S}}_K \to \mathbb{C} : F \text{ es holomorfa y } \sup_t \langle F, F \rangle_t < \infty \right\},$$

con producto interior $\langle \cdot, \cdot \rangle_t = \sup_t \langle \cdot, \cdot \rangle_t$.

De manera similar dada $F \in \mathrm{Har}\,[K]$, esta tiene un L^2 límite definido para casi todo punto cuando $t \to 0$. Luego este límite define un elemento frontera $\partial F \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$.

Si $K/\mathbb{Q}$ es real podemos considerar el siguiente desarrollo en series de Fourier para los elementos de $\mathrm{Har}\,[K]$.

$$F|_{\mathbb{H}_K} = \sum_q a_q \exp(2\pi i \mathrm{Tr}(q \cdot z)) = \sum_q a_q \prod_\nu (\exp(2\pi i q_\nu x_\nu) \exp(-2\pi q_\nu y_\nu)),$$

luego podemos abreviar como sigue

$$F|_{\mathbb{H}_K} \equiv \sum_q a_q \xi^q,$$

donde $\xi \equiv \exp(2\pi i \mathrm{Tr}(z))$. Nuevamente tenemos que una serie de este tipo define un elemento de $\mathrm{Har}\,[K]$ si $a_q = 0$ para todo q que no está contenido en el cono positivo en K_∞. Luego tenemos el encaje

$$\mathrm{Har}\,[K] \hookrightarrow L^2(\hat{\mathbb{S}}_K, \mathbb{C}).$$

Tratando ahora de construir a partir de $\mathrm{Har}\,[K]$ una especie de extensión holomorfa de K, siguiendo la analogía con el caso de $\mathbb{Q}$, podemos remplazar nuestro grupo de signos $\{+, -\}$ por el grupo $\Theta = \{+, -\}^n \cong (\mathbb{Z}/2\mathbb{Z})^n$ y escribimos $\mathbb{C}_K = K_\infty \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{C} \cong (\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C})^n \cong \mathbb{C}^n$ donde cada elemento

lo podemos ver como $z = (x_1 + iy_1, \cdots, x_n + iy_n)$. Luego, para cada $\theta \in \Theta$, definimos

$$\mathbb{H}_K^\theta = \left\{ z \in \mathbb{C}^K : (\text{sign}(y_1), \cdots, \text{sign}(y_n)) = \theta \right\}.$$

Ahora asociaremos a θ un mapeo conjugación $c_\theta : \mathbb{C}_K \to \mathbb{C}_K$ tal que las coordenadas de $c_\theta(z) = z'$ satisfacen que $x'_j + iy'_j = x_j + \theta_j iy_j$ para $j = 1, \cdots, n$.

Proposición 3.11. *El mapeo conjugación satisface que*

$$c_{\theta_1} \circ c_{\theta_2} = c_{\theta_1 \theta_2}.$$

Demostración. Consideremos $z \in \mathbb{C}_K$. Entonces

$$c_{\theta_1} \circ c_{\theta_2}(z) = c_{\theta_1}\left((x_j + (\theta_1)_j iy_j)\right) = \left((x_j + (\theta_2)_j(\theta_1)_j iy_j)\right) = c_{\theta_1\theta_2}(z).$$

□

Sea K^θ el conjunto de elementos q cuyas coordenadas con respecto a la inclusión $K \hookrightarrow K_\infty$ satisface que $(\text{sign}(q_{\nu_1}), \cdots, \text{sign}(q_{\nu_n})) = \theta$.

Ahora observemos que para los K^θ, tenemos una especie de producto el cual, sigue la siguiente regla de multiplicación,

$$K^{\theta_1} \cdot K^{\theta_2} \subset K^{\theta_1\theta_2}.$$

Proposición 3.12. *Sea $K/\mathbb{Q}$ una extensión de Galois real. Entonces para toda pareja de signos $\theta_1, \theta_2 \in \Theta$,*

$$K^{\theta_1} \cdot K^{\theta_2} = K^{\theta_1\theta_2}.$$

Demostración. Solo falta verificar una contención, para esto vasta checar el caso en que $K = \mathbb{Q}$. Consideremos a $x \in \mathbb{Q}^{\theta_1\theta_2}$ luego es claro que x se puede descomponer como $x = ab$ donde $a \in \mathbb{Q}^{\theta_1}$ y $b \in \mathbb{Q}^{\theta_2}$, luego $x \in \mathbb{Q}^{\theta_1} \cdot \mathbb{Q}^{\theta_2}$ con lo que se tiene la otra contención, de manera similar se prueba el caso para K una extensión real. □

De aquí se sigue que cada elemento $f \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ determina una $(2^n + 1)$-tupla $(F_\theta; F_0)$, donde para cada $\theta \in \Theta$, $F_\theta : \hat{\mathfrak{S}}_K \to \mathbb{C}$ se define como una extensión a $\hat{\mathfrak{S}}_K$ de las siguientes funciones en $\mathbb{H}_K$:

$$F_\theta(z) = \sum_{q \in K^\theta} a_q \exp(2\pi i \text{Tr}(q c_\theta(z))) \equiv \sum_{q \in K^\theta} a_q (c_\theta(\xi))^q,$$

donde $c_\theta(\xi) \equiv \exp(2\pi i \text{Tr}(c_\theta(z)))$. El término análogo F_0 del caso de $\mathbb{Q}$ es la función constante a_0.

A las F_θ las llamaremos funciones θ-*holomorfas* y denotaremos por $\text{Har}_\theta[K]$ al espacio de Hardy de las funciones θ-holomorfas.

Teorema 3.5. *El espacio de las* (2^n+1)*-tuplas*

$$L^2(\hat{\mathbb{S}}_K, \mathbb{C}) \cong \mathrm{Har}_\bullet[K] = \left(\bigoplus_\theta \mathrm{Har}_\theta[K]\right) \oplus \mathbb{C},$$

es un espacio de Hilbert graduado cuyo producto interior es la suma directa de los productos interiores en cada sumando.

Como en el caso de $\mathbb{Q}$ nosotros denotaremos por $\mathrm{Har}[K]$ al sumando de $\mathrm{Har}_\bullet[K]$ con $\theta = (+, \cdots, +)$, el cual podemos notar es el espacio de Hardy de funciones holomorfas en $\hat{\mathfrak{S}}_K$ en el sentido ordinario de holomorficidad.

El producto de Dirichlet $\otimes$ se define de manera natural en $\mathrm{Har}_\bullet[K]$ vía una extensión de frontera, es decir, $F \otimes G$ se define como el único elemento de $\mathrm{Har}_\bullet[K]$ cuyo límite (frontera) es $\partial F \otimes \partial G$, siempre que este definido.

Proposición 3.13. *El producto de Dirichlet se descompone en* $\mathrm{Har}_\bullet[K]$ *como sigue:*

$$(F \otimes G)_\theta = \sum_{\theta=\theta_1\theta_2} F_{\theta_1} \otimes G_{\theta_2},$$

y

$$(F \otimes G)_0 = F(0)G_0 + G(0)F_0 - F_0G_0.$$

Demostración. Dado $F = \sum_{q\in K} a_q(\xi)^q$ y $G = \sum_{q\in K} b_q(\xi)^q$,

$$(F \otimes G)_\theta = \sum_{q\in K^\theta} \left(\sum_{q=q_1q_2} a_{q_1}b_{q_2}\right)\xi^q.$$

Luego por la Proposición 3.12 tenemos la descomposición $K^\theta = K^{\theta_1\theta_2} = K^{\theta_1} \cdot K^{\theta_2}$ de donde se sigue que:

$$(F \otimes G)_\theta = \sum_{\theta=\theta_1\theta_2} F_{\theta_1} \otimes G_{\theta_2}.$$

Para la segunda parte y por simplificar cálculos consideremos el caso en que $K = \mathbb{Q}$ y tomemos el producto.

$$(F \otimes G)_0 = \sum_{q=0} \left(\sum_{q=q_1q_2} a_{q_1}b_{q_2}\right)\xi^q.$$

Luego si $q = 0$ tenemos que $q_1 = 0$ y entonces q_2 puede tomar cualquier valor de q, o que $q_2 = 0$ y q_1 puede tomar cualquier valor de q luego tenemos que

$$(F \otimes G)_0 = \sum_{q_1} a_{q_1}b_0 + \sum_{q_2} a_0b_{q_2} - a_0b_0 = F(1)G_0 + G(1)F_0 - F_0G_0.$$

donde restamos el término a_0b_0 ya que al correr q_1 y q_2 sobre todo q el término a_0b_0 aparecía dos veces. □

Nota 1. El producto de Cauchy $\oplus$ se define de manera análoga al producto de Dirichlet vía una extensión de frontera. Sin embargo, notemos que el producto de Cauchy $\oplus$ no respeta la graduación en $\mathrm{Har}_\bullet[K]$, en el sentido de la Proposición 3.13. Por ejemplo: sea $K = \mathbb{Q}$ y tomemos, $F = \xi^{-1}$ y $G = \xi + \xi^2$. Luego

$$(F \oplus G)_+ = (\xi^{-1} \oplus (\xi + \xi^2))_+ = ((\xi^{-1} \oplus \xi) + (\xi^{-1} \oplus \xi^2))_+ = 1 + \xi.$$

Por otro lado

$$F_+ \oplus G_+ + F_- \oplus G_- = 0 \oplus (\xi + \xi^2) + \xi^{-1} \oplus 0 = 0.$$

Luego $(F \oplus G)_+ \neq F_+ \oplus G_+ + F_- \oplus G_-$.

Ahora, consideramos el caso cuando $K/\mathbb{Q}$ es complejo, dada $F \in \mathrm{Har}[K]$, esta tiene un L^2 límite, definido para casi todo punto, cuando $t \to 0$. Luego este límite define un elemento frontera $\partial F \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$.

Luego como en el caso real tenemos un desarrollo en series de Fourier para F como sigue:

$$\begin{aligned} F|_{\mathbb{H}_K} &= \sum_q a_q \exp(2\pi i \mathrm{Tr}(q \cdot (w))) \\ &= \sum_q a_q \prod_\mu (\exp(4\pi i \mathrm{Re}(q_\mu z_\mu)) \exp(-4\pi \mathrm{Im}(q_\mu b_\mu))). \end{aligned}$$

El cual abreviaremos como

$$F|_{\mathbb{H}_K} \equiv \sum_q a_q \varsigma^q,$$

donde $\varsigma \equiv \exp(2\pi i \mathrm{Tr}(w))$. Entonces tenemos que una serie de este tipo define un elemento de $\mathrm{Har}[K]$ si $a_q = 0$ para todo q que no está contenido en el cono positivo en K_∞. Aquí, el cono positivo de K_∞ se define como el conjunto de las z para las cuales $(z_\mu, \bar{z}_\mu) \in \mathbb{B} \times \overline{\mathbb{B}}$ para cada lugar μ. Luego tenemos el monomorfismo

$$\mathrm{Har}[K] \hookrightarrow L^2(\hat{\mathbb{S}}_K, \mathbb{C}).$$

A fin de extender la idea de construir a partir de $\mathrm{Har}[K]$ una especie de extensión holomorfa de K. Tenemos que hacer algunas modificaciones al grupo de signos para que nuestra graduación sea compatible con los lugares complejos.

Primero, conservaremos los signos que teníamos para el caso real

$$\Theta = \{-, +\}^s,$$

pero solo consideraremos s factores donde $s = n/2$, con n el grado de K sobre $\mathbb{Q}$. Lo cual nos ayuda a dotar de un signo (o signar) a los ejes reales. Ahora para los ejes imaginarios consideraremos el siguiente conjunto de signos.

$$\sqrt{-}\Theta = \left\{-\sqrt{-}, \sqrt{-}\right\}^s.$$

Ahora, considerando a todos estos signos juntos tenemos

$$\Theta_{\mathbb{C}} = \left\{\sqrt{-}, -, -\sqrt{-}, +\right\}^s,$$

la cual claramente tiene estructura de grupo con el producto multiplicación de signos y elemento identidad $+$. Diremos que $z \in (\mathbb{R} \cup i\mathbb{R}) - 0$ tiene signo $\sqrt{-}, -, -\sqrt{-}, +$ si z perteneces respectivamente a $i\mathbb{R}_+, -\mathbb{R}_+, -i\mathbb{R}_+, \mathbb{R}_+$. Luego a $\Theta_{\mathbb{C}}$ lo llamaremos el grupo de *signos singular*.

Ahora para los puntos que no están en $\mathbb{R} \cup i\mathbb{R}$, introduciremos el grupo cíclico de *signos complejo* de orden 4

$$\left\{\sqrt{-\epsilon}, -\epsilon, -\sqrt{-\epsilon}, +\epsilon\right\},$$

el cual es isomorfo al grupo $\mathbb{Z}/4\mathbb{Z}$, luego diremos que $z \in \mathbb{C} - (\mathbb{R} \cup i\mathbb{R})$ tiene signo complejo $\sqrt{-\epsilon}, -\epsilon, -\sqrt{-\epsilon}, +\epsilon$ si z pertenece a $i\mathbb{B}, -\mathbb{B}, -i\mathbb{B}, \mathbb{B}$ respectivamente. Luego podemos definir

$$\Omega = \left\{\sqrt{-\epsilon}, -\epsilon, -\sqrt{-\epsilon}, +\epsilon\right\}^s.$$

El cual tiene estructura de grupo equipado con una acción dada por $\Theta_{\mathbb{C}}$ donde s se entiende como la potencia con respecto a la operación suma directa de grupos.

Ahora consideremos el siguiente isomorfismo

$$\mathfrak{s} : \Omega \to \Theta_{\mathbb{C}},$$

dado por "borrar" u "olvidar" el símbolo ϵ.

Como en el caso real nosotros podemos escribir $\mathbb{C}_K = K_\infty \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}^n$, cuyos puntos ahora podemos expresar como: $w = ((z_1, b_1), \cdots, (z_s, b_s))$.

Para cada $\omega \in \Omega$,

$$\mathbb{H}_K^\omega = \{w \in \mathbb{C}_K : (\text{sign}(b_1), \cdots, \text{sign}(b_s)) = \omega\}.$$

Como en el caso real podemos asociar a cada ω una mapeo conjugación $c_\omega : \mathbb{C}_\omega \to \mathbb{C}_\omega$, donde las coordenadas de $c_\omega(w) = w'$ satisfacen que

$$(z_k', b_k') = (z_k, \omega_k b_k),$$

para $k = 1, \cdots, s$. Luego como en el caso real tenemos la siguiente Proposición.

Proposición 3.14. *El mapeo conjugación satisface que*

$$c_{\omega_1} \circ c_{\omega_2} = c_{\omega_1 \omega_2}.$$

Demostración. La prueba es análoga al caso real. □

Denotemos por K^ω los elementos q cuyas coordenadas con respecto a la inclusión $K \hookrightarrow K_\infty$ satisfacen que:

$$(\text{sign}(q_{\mu_1}), \cdots, \text{sign}(q_{\mu_s})) = \omega.$$

Cabe notar que si $q \in K^{\omega}$, $q \notin \mathbb{R} \cup i\mathbb{R}$. A diferencia del caso real la multiplicación graduada complexificada se comporta de la siguiente manera,

$$K^{\omega_1} \cdot K^{\omega_2} \subset K^{\omega_1\omega_2} \cup iK^{\omega_1\omega_2} \cup iK^{\mathfrak{s}(\omega_1\omega_2)}.$$

En este caso podemos escribir

$$\Re(K^{\omega_1} \cdot K^{\omega_2}) := (K^{\omega_1} \cdot K^{\omega_2}) \cap K^{\omega_1\omega_2},$$

la "*parte real*" de la graduación,

$$\Im(K^{\omega_1} \cdot K^{\omega_2}) := (K^{\omega_1} \cdot K^{\omega_2}) \cap iK^{\omega_1\omega_2},$$

la "*parte imaginaria*" de la graduación, y por último

$$\Im_{\Theta_{\mathbb{C}}}(K^{\omega_1} \cdot K^{\omega_2}) := (K^{\omega_1} \cdot K^{\omega_2}) \cap K^{\mathfrak{s}(\omega_1\omega_2)},$$

la " *parte singular*" de la graduación.

Proposición 3.15. *Sea K/Q una extensión de Galois compleja. Entonces para toda pareja de signos $\omega_1, \omega_2 \in \Omega$,*

$$K^{\omega_1} \cdot K^{\omega_2} = K^{\omega_1\omega_2} \cup iK^{\omega_1\omega_2} \cup iK^{\mathfrak{s}(\omega_1\omega_2)}.$$

Demostración. Notemos que solo nos falta probar una contención. Para esto como en el caso real, basta estudiar el caso en que $K/\mathbb{Q}$ es de grado 2. Consideremos a $x \in K^{\omega_1\omega_2} \cup iK^{\omega_1\omega_2} \cup iK^{\mathfrak{s}(\omega_1\omega_2)}$ y veamos que este x puede descomponerse como $x = ab$ con $a \in K^{\omega_1}$ y $b \in K^{\omega_2}$. Supongamos que $x \in K^{\omega_1\omega_2}$ escribiendo x, en notación exponencial

$$x = re^{i\alpha} = ste^{i(\alpha_1+\alpha_2)} = se^{i\alpha_1}re^{i\alpha_2},$$

donde es claro que $se^{i\alpha_1} \in K^{\omega_1}$ y $te^{i\alpha_2} \in K^{\omega_2}$. De manera análoga se prueba para los casos cuando $x \in iK^{\omega_1\omega_2}$ y $x \in K^{\mathfrak{s}(\omega_1\omega_2)}$. □

De aquí se sigue que cada elemento $f \in L^2(\hat{\mathbb{S}}_K, \mathbb{C})$ determina una $(4^s + 2 \cdot 2^s + 1)$-tupla $(F_\omega; F_\theta; F_0)$, donde para cada $\omega \in \Omega$, $F_\omega : \hat{\mathfrak{S}}_K \to \mathbb{C}$ se define como una extensión a $\hat{\mathfrak{S}}_K$ de las siguientes funciones en $\mathbb{H}_K$

$$F_\omega(w)|_{\mathbb{H}_K} = \sum_{q \in K^{\omega}} a_q \exp(2\pi i \mathrm{Tr}(q c_\omega(w))) \equiv \sum_{q \in K^{\omega}} a_q (c_\omega(\varsigma))^q,$$

donde $c_\omega(\varsigma) = \exp(2\pi i \mathrm{Tr}(c_\omega(w)))$ y el símbolo $(c_\omega(\varsigma))^q$ es entendido en el sentido de multi índices. A las F_ω las llamaremos funciones ω-$holomorfas$ y $F_0 = a_0$ es la función constante como en el caso real. Para el caso de las F_θ, que llamaremos funciones θ-holomorfas, notemos que estas son constantes en alguna de las variables u, v. Luego diremos que F_θ es degenerada en el sentido de que estas se reducen a funciones de u o v separadamente.

Aquí tenemos que para el morfismo conjugación se tiene que $c_+(u) = u$, $c_-(u) = \bar{u}$, la cual es la conjugación usual para la variable u, y $c_{\sqrt{=}}(v) = v$,

$c_{-\sqrt{-}}(v) = -s + iy$ la cual podemos interpretar como la conjugación del plano $-i\mathbb{H}^2$ en el plano $i\mathbb{H}^2$. Por lo que, podemos definir las multiconjugaciones c_θ, con $\theta \in \Theta_{\mathbb{C}}$, en el sentido obvio coordenada a coordenada. Luego tenemos la siguiente representación de las funciones θ-holomorfas. Para $\theta \in \Theta$,

$$F_\theta(w) = \sum_{q \in K^\theta} a_q \exp(4\pi i \mathrm{Tr}(q \cdot c_\theta(u))),$$

y para $\theta \in \sqrt{-}\Theta$,

$$F_\theta(w) = \sum_{q \in K^\theta} a_q \exp(-4\pi \mathrm{Tr}(q \cdot c_\theta(v))),$$

Como en el caso real aquí también tenemos los espacios de Hardy $\mathrm{Har}_\omega[K]$ y $\mathrm{Har}_\theta[K]$ de funciones ω-holomorfas y θ-holomorfas respectivamente.

Teorema 3.6. *El espacio de las* $(4^s + 2 \cdot 2^s + 1)$*-tuplas*

$$L^2(\hat{\mathbb{S}}_K, \mathbb{C}) \cong \mathrm{Har}_\bullet[K] = \left(\bigoplus_{\omega \in \Omega} \mathrm{Har}_\omega[K] \right) \oplus \left(\bigoplus_{\theta \in \Theta_{\mathbb{C}}} \mathrm{Har}_\theta[K] \right) \oplus \mathbb{C},$$

es un espacio de Hilbert graduado cuyo producto interior es la suma directa de los productos interiores de cada sumando.

Denotaremos por $\mathrm{Har}[K]$ al sumando de $\mathrm{Har}_\bullet[K]$ para el cual $\omega = (+, \cdots, +)$ el cual es, como en el caso real, el espacio de Hardy de funciones holomorfas en el sentido usual de holomorficidad. De manera análoga definimos el producto de Cauchy y el producto de Dirichlet en $\mathrm{Har}_\bullet[K]$, vía extensiones frontera.

Cuando $\omega_1\omega_2 = \omega$ y dado $F, G \in \mathrm{Har}_\bullet[K]$, escribiremos

$$\Re(F_{\omega_1} \otimes G_{\omega_2}),$$

para la proyección de $F_{\omega_1} \otimes G_{\omega_2}$ en la subserie indexada por $q \in \Re(K^{\omega_1} \cdot K^{\omega_2})$ y

$$\Im(F_{\omega_1} \otimes G_{\omega_2}),$$

para la proyección de $F_{\omega_1} \otimes G_{\omega_2}$ en la subserie indexada por $q \in \Im(K^{\omega_1} \cdot K^{\omega_2})$.

Proposición 3.16. *Dado* $K/\mathbb{Q}$ *una extensión de Galois compleja y* $F, G \in \mathrm{Har}_\bullet[K]$*, tenemos la siguiente descomposición,*

$$(F \otimes G)_\omega = \sum_{\omega = \omega_1\omega_2} \Re(F_{\omega_1} \otimes G_{\omega_2}) + \sum_{\omega = \sqrt{-}\omega_1'\omega_2'} \Im(F_{\omega_1'} \otimes G_{\omega_2'})$$

$$+ \sum_{\omega = \omega'\theta'} \left((F_{\omega'} \otimes G_{\theta'}) + (F_{\theta'} \otimes G_{\omega'}) \right).$$

De manera similar para los $\Theta_{\mathbb{C}}$ signos,

$$(F \otimes G)_\theta = \sum_{\theta=\theta_1\theta_2} (F_{\theta_1} \otimes G_{\theta_2}) + \sum_{\theta=\sqrt{-}\mathfrak{s}(\omega_1\omega_2)} \Im_{\Theta_{\mathbb{C}}}(F_{\omega_1} \otimes G_{\omega_2})$$

y

$$(F \otimes G)_0 = F(0)G_0 + G(0)F_0 - F_0G_0.$$

Demostración. Consideremos $F = \sum_q a_q \varsigma^q$ y $G = \sum_q b_q \varsigma^q$.

$$(F \otimes G)_\omega = \sum_{q \in K^\omega} \left(\sum_{q_1 q_2 = q} a_{q_1} b_{q_2} \right) \varsigma^q.$$

Luego los valores de los índices q_1 y q_2 son tales que cumplan la propiedad de que $q_1 q_2 \in K^\omega$.

Por la descomposición de $K^{\omega_1} \cdot K^{\omega_2}$ de la Proposición 3.15, q_1 y q_2 tienen que estar ya sea en la parte real o en la parte imaginaria de $K^{\omega_1} \cdot K^{\omega_2}$, ya que la parte singular solo contiene elementos que están en algún K^θ, los cuales no son de nuestro interés aquí.

Primero para la parte real de la graduación, se tiene que $q = q_1 q_2 \in K^{\omega_1\omega_2} = K^\omega$ lo cual nos da el factor

$$\sum_{\omega=\omega_1\omega_2} \Re(F_{\omega_1} \otimes G_{\omega_2}).$$

Ahora si $\omega = \sqrt{-}\omega_1\omega_2$ y $q \in \Im(K^{\omega_1} \cdot K^{\omega_1})$ tenemos que $q \in iK^{\omega_1'\omega_2} \subset K^{\sqrt{-}\omega_1\omega_2} = K^\omega$ de donde tenemos el factor,

$$\sum_{\omega=\sqrt{-}\omega_1\omega_2} \Im(F_{\omega_1} \otimes G_{\omega_2}).$$

Notemos sin embargo que debido a la acción de $\Theta_{\mathbb{C}}$ en Ω tenemos elementos $\theta' \in \Theta_{\mathbb{C}}$ que cumplen $\theta'\omega' = \omega$, lo cual nos da el último factor de la suma

$$\sum_{\omega=\omega'\theta'} \left((F_{\omega'} \otimes G_{\theta'}) + (F_{\theta'} \otimes G_{\omega'}) \right),$$

.

Para la segunda parte el primer factor

$$\sum_{\theta=\theta_1\theta_2} (F_{\theta_1} \otimes G_{\theta 2}),$$

se obtiene de manera análoga al caso real. Sin embargo, debido a la parte singular de la descomposición de $K^{\omega_1} \cdot K^{\omega_2}$ hay elementos $q_1 \in K^{\omega_1}$ y $q_2 \in K^{\omega_2}$ tal que $q_1 q_2 \in iK^\theta = K^{\sqrt{-}\theta}$ los cuales nos dan el factor

$$\sum_{\theta=\sqrt{-}\mathfrak{s}(\omega_1\omega_2)} \Im_{\Theta_C}(F_{\omega_1} \otimes G_{\omega 2}).$$

Por último, la tercera parte se prueba de manera análoga a la del caso real. □

Notemos que para cada K real o complejo tenemos una subdoble álgebra parcial $\mathrm{Har}_\bullet[O_K] \subset \mathrm{Har}_\bullet[K]$ definida por las series de Fourier indexadas por elementos de O_K. En particular si $\mathfrak{d}_K^{-1} = O_K$ los elementos de $\mathrm{Har}_\bullet[O_K]$ corresponden a las funciones holomorfas graduadas en el toro de Minkowski hiperbolizado $\mathfrak{T}_K$.

Teorema 3.7. *Sea $K/\mathbb{Q}$ una extensión de Galois. Entonces $\mathrm{Har}_\bullet[K]$ es un espacio de Hilbert equipado con una estructura de doble $\mathbb{C}$-álgebra parcial con respecto a las operaciones $\oplus$ y $\otimes$. En particular cuando $\mathfrak{d}_K^{-1} = O_K$ el correspondiente subespacio de funciones del toro de Minkowski hiperbolizado $\mathfrak{T}_K$, $\mathrm{Har}_\bullet[O_K]$ es un subespacio de Hilbert de $\mathrm{Har}_\bullet[K]$, el cual es una doble $\mathbb{C}$-subálgebra parcial.*

De manera análoga al Corolario 3.4 tenemos un monomorfismo con imagen densa

$$\mathbb{C}[K] \hookrightarrow \mathrm{Har}_\bullet[K].$$

Ahora si definimos $T(F) = F(0)$ un mapeo de $\mathrm{Har}_\bullet[K] \to \mathbb{C}$ tenemos nuevamente el mapeo de aumentación, luego podemos definir

$$\mathrm{Har}_\bullet^*[K] = \{F \in \mathrm{Har}_\bullet[K] : T(F) = 0\},$$

y por lo tanto una proyectivización

$$N_\bullet(K) = \mathrm{Har}_\bullet^*[K]/\mathbb{C}^*,$$

la cual es isomorfa a $N(K)$.

Luego siguiendo la filosofía de las Proposiciones 3.8 y 3.9, tenemos que $N_\bullet(K)$ tiene estructura de doble semigrupo parcial con los productos de Cauchy y Dirichlet. Además, se tiene el siguiente monomorfismo canónico

$$K \hookrightarrow N_0(K) \hookrightarrow N_\bullet(K),$$

donde $N_0(K)$ tiene imagen densa en $N_\bullet(K)$.

3.5 Campos de Números No lineales

La palabra *no lineal* (según [1]) proviene del hecho de la no linealidad del producto de Cauchy y el producto de Dirichlet vista en el Teorema 3.1.

Definición 8. Un **Campo de números no lineal** es un doble semigrupo parcial topológico abeliano $\mathcal{S}$ con respecto a dos operaciones $\oplus$ y $\otimes$ tales que cumple las siguientes condiciones

i) Existe un campo numérico K y una inclusión densa del doble semigrupo

$$i : N^0[K] \hookrightarrow \mathcal{S}$$

donde $i([f] \oplus [g]) = i([f]) \oplus i([g])$ y $i([f] \otimes [g]) = i([f]) \otimes i([g])$, siempre que $[f] \oplus [g]$ y $[f] \otimes [g]$ estén definidos.

ii) La identidad $1_{\oplus}$ es el aniquilador universal para $\otimes$ *i.e.* para toda $F \in \mathcal{S}$, $F \otimes 1_{\oplus} = 1_{\oplus}$.

A la cerradura $\mathcal{O}$ de la imagen de $i(N^0[O_K])$ la llamaremos **Anillo de Enteros No lineal**.

De manera inmediata de la definición de campo de números no lineal y de la discusión anterior tenemos.

Teorema 3.8. *Dado K un campo numérico, tenemos que $N[K]$ es un campo de números no lineal y $N[O_K]$ es su anillo de enteros no lineal.*

Una primera aproximación a tratar de hacer aritmética en los campos de números no lineales seria estudiar las unidades con respecto a alguno de los productos, para el producto de Cauchy $\oplus$ tenemos el siguiente resultado.

Proposición 3.17. *El grupo de unidades de Cauchy $N(K)^{\times}_{\oplus}$ es un subconjunto denso de $N(K)$.*

Demostración. Consideremos el caso de $K = \mathbb{Q}$, como hemos visto,

$$L^2(\hat{\mathbb{S}}_{\mathbb{Q}}, C) \cong \mathrm{Har}_{\bullet}[\mathbb{Q}] = \mathrm{Har}_{+}[K] \oplus \mathbb{C} \oplus \mathrm{Har}_{-}[K],$$

el cual contiene como subconjunto denso a $\mathrm{Har}^{an}_{+}[K] \oplus \mathbb{C}^* \oplus \mathrm{Har}^{an}_{-}[K]$ el conjunto de las funciones analíticas reales las cuales tienen como subconjunto denso a las funciones analíticas libres de cero las cuales son invertibles. Entonces, tenemos un conjunto denso de elementos invertibles de $L^2(\hat{\mathbb{S}}_{\mathbb{Q}}, \mathbb{C})$. Luego, tomando la proyectivización $N(K)$ la densidad es preservada luego tenemos lo requerido. Un argumento análogo se sigue para K arbitrario. □

El estudio de las unidades de *Dirichlet* es más complicado y estudiaremos estas de forma un poco más detallada en el siguiente capítulo.

Una de las ideas más importantes en la teoría algebraica de números es la construcción del campo de fracciones del anillo de enteros. Desafortunadamente en los campos de números no lineales no es posible reproducir fielmente este hecho, no obstante, el siguiente resultado muestra que existe un subconjunto denso P de $N(K)$ donde P funciona como una especie de campo de fracciones de $N(O_K)$.

Teorema 3.9. *Sea $K/\mathbb{Q}$ una extensión de Galois. Entonces hay un subconjunto denso $P \subset N(K)$ tal que para todo $[F] \in P$. Existe $[G] \in N(O_K)$ tal que*

$$[G] \otimes [F] \in N(O_K).$$

Demostración. Consideremos a $N(K)_{fin}$ el subespacio asociado a las funciones cuyos coeficientes de Fourier son indexados por q en algún ideal fraccional $\mathfrak{a}^{-1}O_K \subset K$.

Sea $\mathbb{T}_{\mathfrak{a}}$ el toro de Minkowski asociado a $\mathfrak{a}$, *i.e.* $\mathbb{T}_{\mathfrak{a}} = K_{\infty}/\mathfrak{a}$. Al cual podemos asociar el toro hiperbolizado $\mathfrak{T}_{\mathfrak{a}}$ y el doble subsemigrupo $N(\mathfrak{a})$. Luego por definición de $\mathfrak{a}^{-1}$

$$\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subset O_K\},$$

tenemos que dado $[F] \in N(K)_{fin}$ cuyos coeficiente de Fourier son indexados por $\mathfrak{a}^{-1}O_K$, basta considerar un elemento $[G]$ cuyos coeficientes no cero estén indexados por $\mathfrak{a}$, es decir, tenemos un $[G] \in N(\mathfrak{a})$ tal que $[F] \otimes [G] \in N(O_K)$. $\square$

Capítulo 4

Aritmética No lineal

Una cuestión fundamental en la teoría de números, es la aritmética de la estructura estudiada, en nuestro caso la aritmética de los campos de números no lineales. En este capítulo, y apoyados en la teoría de series de Dirichlet trataremos de construir una teoría de unidades en el caso particular del anillo de enteros no lineal $N(\mathbb{Z})$. Lo que nos dará algunas nociones primitivas de la aritmética los de enteros no lineales.

4.1 Funciones Aritméticas y Series de Dirichlet

El material que aparece en esta sección es clásico en teoría analítica de números. Luego, los detalles sobre los puntos tratados en esta sección pueden ser consultados en [15].

Una *función aritmética* f, se define como una sucesión de números reales o complejos, *i.e.* $f : \mathbb{N} \to \mathbb{C}$.

Un ejemplo de estas, es la función φ de Euler la cual se define mediante

$$\varphi(n) = |\{m : 0 < m \leq n,\ (m,n) = 1\}|\,.$$

Otro ejemplo, es la función μ de Möbius la cual es definida por la siguiente relación

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n = p_1 p_2 \cdots p_k, \text{ con } p_i \text{ distintos}\,, \\ 0 & \text{en otro caso.} \end{cases}$$

Dadas dos funciones aritméticas f y g definimos la *convolución de Dirichlet* $f * g$ como la función aritmética h, la cual esta dada por la siguiente ecuación

$$h(n) = \sum_{d|n} f(d) g(\frac{n}{d}).$$

Sean f, g, h funciones aritméticas luego, tenemos que

- $f * g = g * f$,

- $(f * g) * h = f * (g * h)$.

Ahora, si consideramos la función aritmética I definida como

$$I(n) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{en otro caso,} \end{cases}$$

la cual llamaremos *función identidad*, se puede demostrar que,

$$I * f = f * I = f.$$

Teorema 4.1. *Si f es una función aritmética con $f(1) \neq 0$ existe una única función aritmética f^{-1}, conocida como la inversa de Dirichlet de f, tal que*

$$f * f^{-1} = f^{-1} * f = I.$$

Más aún, f^{-1} está dada por la siguiente fórmula recursiva

$$f^{-1}(1) = \frac{1}{f(1)}, \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \text{ para } n > 1.$$

Esta fórmula es conocida como la fórmula de inversión de Möbius.

Corolario 4.1. *Una función aritmética f tiene inversa si y solo si $f(1) \neq 0$.*

Demostración. Por contradicción, supongamos que f tiene inversa y que $f(1) = 0$. Como f tiene inversa existe g función aritmética tal que

$$f * g = \sum_{d|n} f(d) g(\frac{n}{d}) = h(n) = I(n),$$

de donde se tiene que $h(1) = f(1)g(1) = 1$ para $n = 1$ y $h(n) = 0$ para toda $n \neq 1$. Por otro lado, de suponer que $f(1) = 0$ tenemos que $f(1)g(1) = 0$ lo cual es una contradicción. Recíprocamente, si $f(1) \neq 0$ tenemos por el Teorema 4.1 que existe f^{-1} tal que $f * f^{-1} = I$. □

Si definimos la función aritmética u que llamaremos *función unidad* definida por la ecuación $u(n) = 1$ para toda n y usando la igualdad

$$\sum_{d|n} \mu(d) = I(n),$$

tenemos que la función de Möbius es invertible, pues

$$\mu * u = I.$$

i.e. u y μ son inversas de Dirichlet una de la otra.

Notemos que $(f * g)(1) = f(1)g(1)$ luego, si $f(1) \neq 0$ y $g(1) \neq 0$ tenemos que $(f * g)(1) \neq 0$, entonces el conjunto de las funciones aritméticas f con $f(1) \neq 0$

forman un grupo con respecto a la convolución de Dirichlet $*$ y con elemento identidad I.

Un importante subgrupo de estas es el de las *funciones multiplicativas*. Diremos que una función aritmética f es multiplicativa si f no es idénticamente cero y sí

$$f(mn) = f(m)f(n),$$

siempre que $(m, n) = 1$. Diremos que f es *completamente multiplicativa* si se cumple que

$$f(mn) = f(m)f(n),$$

para toda m y n.

Notemos que el conjunto de las funciones completamente multiplicativas no forman un grupo. Por ejemplo, consideremos la función unidad u definida como antes. Esta, es completamente multiplicativa, pues

$$1 = u(nm) = u(n)u(m) = 1,$$

para toda m, n. Luego, como vimos antes, su inversa es la función $\mu(n)$ de Möbius la cual no es completamente multiplicativa pues $\mu(4) = 0$ y $\mu(2)\mu(2) = 1$.

Por otro lado, se puede probar que una función multiplicativa f es completamente multiplicativa si y solo si $f^{-1}(n) = \mu(n)f(n)$ para toda $n \geq 1$.

Una *series de Dirichlet* se define como una serie de la forma

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

donde $\{a_n\}$ es una sucesión de números complejos, y s es una variable compleja $s = \sigma + it$. Notemos que cada función aritmética f determina una serie de Dirichlet $D_f(s) = \sum f(n)/n^s$ y de hecho toda serie de Dirichlet es de está forma.

Teorema 4.2. *Si la serie de Dirichlet $D_f(s)$ converge para algún $s = s_0$ entonces esta converge para toda s con $Re(s) > \sigma_0$ donde $\sigma_0 = Re(s_0)$.*

Suponiendo que las series de Dirichlet convergen para alguna s, si σ_0 es el número real más chico tal que la serie converge para $\mathrm{Re}(s) > \sigma_0$ entonces llamaremos a σ_0 la *abscisa de convergencia*. Luego la serie de Dirichlet converge en el plano superior a la derecha de la línea $\sigma = \sigma_0$ el cual llamaremos *plano de convergencia*. Pero no converge para toda s con $\sigma < \sigma_0$.

Dadas dos series de Dirichlet

$$D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \text{ para } \sigma > a,$$

y

$$D_g(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \text{ para } \sigma > b,$$

en el plano donde ambas convergen tenemos que

$$D_f(s)D_g(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s},$$

donde $h = f * g$ es la convolución de f y g. Conversamente si

$$D_f(s)D_g(s) = \sum_{n=1}^{\infty} \alpha(n)n^{-s},$$

está definida para toda s de una sucesión $\{s_k\}$ con $\sigma_k \to \infty$ cuando $k \to \infty$, entonces $\alpha = f * g$.

Ahora mencionaremos algunos ejemplos de series de Dirichlet que usaremos mas adelante. Sean

$$D_u(s) = \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

y

$$D_\mu(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

dos series de Dirichlet, las cuales convergen absolutamente para $\sigma > 1$. Entonces, si tomamos $f(n) = u(n)$ y $g(n) = \mu(n)$ tenemos que $h(n) = I(n)$, luego

$$D_u(s)D_\mu(s) = \zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{(u * \mu)(n)}{n^s} = 1, \text{ si } \sigma > 1.$$

Lo que nos dice que la función zeta de Riemann $\zeta(s)$ es invertible si $\sigma > 1$. Y que su inversa está dada por la función

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^{-s}}.$$

De manera más general si suponemos que $f(1) \neq 0$, se tiene que existe $g = f^{-1}$ la inversa de Dirichlet de f. Luego, si consideremos sus series de Dirichlet asociadas

$$D_f(s) = \sum f(n)n^{-s} \quad \text{y} \quad D_g(s) = \sum g(n)n^{-s},$$

en el plano superior en el que ambas convergen absolutamente, entonces

$$D_f(s) \neq 0 \quad \text{y} \quad D_g(s) = 1/D_f(s).$$

En particular, si f es completamente multiplicativa se tiene que $f^{-1} = \mu(n)f(n)$. Luego, si $D_f(s) = \sum f(s)n^{-s}$ converge absolutamente para $\sigma > \sigma_0$ entonces la serie $\sum \mu(n)f(n)n^{-s}$ también converge absolutamente para $\sigma > \sigma_0$, pues $\left|f^{-1}(n)\right| \leq |f(n)|$, y tenemos que

$$\sum_{n=1}^{\infty} \frac{\mu(n)f(n)}{n^s} = \frac{1}{D_f(s)}, \text{ si } \sigma > \sigma_0.$$

Diremos que una función aritmética $\chi : \mathbb{N} \to \mathbb{C}$ es un carácter de Dirichlet módulo k, si satisface las siguientes condiciones

- $\chi(1) \neq 0$.
- Si $a \equiv b(\text{mod } k)$ entonces $\chi(a) = \chi(b)$.
- $\chi(ab) = \chi(a)\chi(b)$.
- Si $(a, k) > 1$ entonces $\chi(a) = 0$.

Es claro que χ es completamente multiplicativo. Luego para cada carácter, se tiene la serie de Dirichlet

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

la cual tiene inversa dada por:

$$\sum_{n=1}^{\infty} \frac{\mu(n)\chi(n)}{n^s} = \frac{1}{L(s, \chi)} \ , \text{ si } \sigma > 1.$$

Este tipo de series son conocidas como las *series L de Dirichlet*.

Sin embargo, cabe notar que no existe un criterio general para las series inversas de Dirichlet en lo que respecta a convergencia.

4.2 Unidades No Lineales en $N(\mathbb{Z})$

Consideremos el conjunto de las series de Dirichlet

$$D_f(s) = \sum_{n=1}^{\infty} a_n n^{-s} \ , \text{ para } \sigma > 0.$$

luego podemos identificar a $D_f(s)$ con un entero no lineal

$$f = \sum_{n=1}^{\infty} a_n z^n \in N_+(\mathbb{Z}),$$

donde $N_+(\mathbb{Z})$ es Har $[\mathbb{Z}]$ proyectivizado lo cual nos permite estudiar a los elementos de $N_+(\mathbb{Z})$ a través de las series de Dirichlet convergentes en $\sigma > 0$.

Una primera cuestión, seria estudiar bajo que condiciones un entero no lineal f es invertible con respecto $\otimes$ en $N_+(\mathbb{Z})$. Consideremos la función aritmética $f(n) = 1/n$ la cual define una serie de Dirichlet

$$D_f(s) = \sum_{n=1}^{\infty} \frac{1}{n} n^{-s} = \zeta(s + 1),$$

la cual, como podemos notar, es la función zeta de Riemann trasladada una unidad hacia la derecha. Por lo tanto, como $\zeta(s)$ converge para $\sigma > 1$ entonces $\zeta(s+1)$ converge para $\sigma > 0$, luego $\zeta(s+1)$ define un elemento en $N_+(\mathbb{Z}) \subset N(\mathbb{Z})$ el cual denotaremos por ζ

$$\zeta = \sum_{n=1}^{\infty} \frac{1}{n} z^n.$$

Proposición 4.1. *El entero no lineal ζ, es invertible en $N_+(\mathbb{Z}) \subset N(\mathbb{Z})$ y su inverso está dado por el número no lineal*

$$g = \sum_{n=1}^{\infty} b_n z^n,$$

donde $b_n = \mu(n)/n$.

Demostración. Consideremos la serie de Dirichlet

$$D_\mu(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} n^{-s},$$

la cual es convergente para $\sigma > 0$, pues de la teoría de series de Dirichlet sabemos que $\sum_{n=1}^{\infty} \mu(b) n^{-s}$ es convergente para $\sigma > 1$. Luego esta, también define un entero no lineal $g \in N_+(\mathbb{Z})$ dado por

$$g = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} z^n.$$

Ahora, considerando el producto $\zeta \otimes g$ el cual podemos identificar con el producto de Dirichlet de sus series de Dirichlet asociadas

$$\zeta(s+1) D_g(s) = \sum_{n=1}^{\infty} \left(\sum_{d|n} \frac{1}{\frac{n}{d}} \frac{\mu(d)}{d} \right) n^s = \sum_{n=1}^{\infty} \left(\sum_{d|n} \frac{\mu(d)}{n} \right) n^s$$

$$= \sum_{n=1}^{\infty} \frac{I(n)}{n} n^s = 1,$$

para $\sigma > 0$. □

De manera más general se tiene el siguiente resultado.

Proposición 4.2. *Dado un entero no lineal $f = \sum a_n z^n$ donde a_n es una función aritmética completamente multiplicativa entonces f es invertible en $N_+(\mathbb{Z}) \subset N(\mathbb{Z})$ y su inverso está dado por $f^{-1} = \sum \mu(n) a_n z^n$.*

Demostración. De teoría de series de Dirichlet tenemos que dada $D_f(s)$, la cual converge para $\sigma > 0$ y donde f es una función aritmética completamente multiplicativa. Se tiene $D_{f^{-1}}(s)$ la serie de Dirichlet asociada a la función aritmética $f^{-1} = \mu f$ la cual es la inversa de Dirichlet de f que converge para $\sigma > 0$ y donde $D_{f^{-1}}(s) D_f(s) = 1$. □

Al conjunto de números no lineales que cumplen las propiedades de la Proposición anterior, lo llamares, el conjunto de *unidades multiplicativas* de $N_+(\mathbb{Z})$.

Por otro lado, es conveniente notar que podemos tener dos tipos de unidades. Para esto definamos el producto $\oslash$ como sigue: Dado

$$f = \sum_{n\in\mathbb{Z}} a_n z^n \in N(\mathbb{Z})$$

y g una serie de la forma

$$g = \sum_{n\in\mathbb{Z}} b_n z^n$$

no necesariamente convergente, definimos

$$f \oslash g = \sum_n \left(\sum_{n_1 n_2 = n} a_{n_1} b_{n_2} \right) z^n,$$

el cual no es necesariamente convergente, pero que sin embargo define una serie formal.

Definición 9. Diremos que $f \in N(\mathbb{Z})$ es *unidad formal* si existe una serie

$$g = \sum_{n\in\mathbb{Z}} b_n z^n,$$

no necesariamente convergente, tal que $f \oslash g = 1_{\otimes}$.

Definición 10. Diremos que $f \in N(\mathbb{Z})$ es *unidad no lineal* si existe $g \in N(\mathbb{Z})$ tal que $f \otimes g = 1_{\otimes}$.

Gracias a la teoría de series de Dirichlet nosotros tenemos una forma de caracterizar las unidades formales en $N_+(\mathbb{Z})$ como sigue.

Teorema 4.3. *Dado un entero no lineal $f \in N_+(\mathbb{Z})$ de la forma $\sum_{n=1}^{\infty} a_n z^n$ es unidad formal si y solo si $a_1 \neq 0$.*

Demostración. Sabemos que dada una serie de Dirichlet $D_f(s)$ con $f(1) \neq 0$, existe $D_{f^{-1}}(s)$ donde f^{-1} es la inversa de Dirichlet de la función aritmética f, tal que $D_f(s)D_{f^{-1}}(s) = 1$ en la intersección de los planos de convergencia de ambas series.

Recíprocamente, si $D_f(s)$ es una serie de Dirichlet y supongamos por contradicción que $f(1) = 0$, entonces al hacer el producto de esta serie con cualquier otra, por ejemplo $D_g(s)$, tendríamos que $f(1)g(1) = 0$ es decir tendríamos que el primer coeficiente del producto $D_f(s)D_g(s)$ seria cero lo cual implica que $D_f(s)D_g(s) \neq 1$ lo cual contradice el hecho de ser unidad formal. □

Nota 2. Notemos que dada una serie de Dirichlet $D_f(s) = \sum f(n)n^{-s}$, con $f(1) \neq 0$, la cual converge para $\sigma > 0$ tiene inversa $D_{f^{-1}}(s) = \sum f^{-1}(n)n^{-1}$ siempre y cuando esta también converja para $\sigma > 0$, de lo contrario diremos que

$D_{f^{-1}}(s)$ es solo el inverso formal de $D_f(s)$, como vimos en el Teorema anterior. Luego es claro que estas series forman un grupo pues el producto de dos series convergentes en $\sigma > 0$ converge para $\sigma > 0$. Luego los enteros no lineales asociados a estas series de Dirichlet forman un grupo con $\otimes$ el cual llamaremos *grupo de unidades no lineales positivas* y el cual denotaremos por $N_+(\mathbb{Z})^\times$.

Nota 3. De manera análoga podemos estudiar el caso para $N_-(\mathbb{Z})$ sin embargo debemos notar que $N_-(\mathbb{Z})^\times$ no es un grupo pues dados dos números no lineales de la forma $f = \sum_{n=1}^{\infty} a_{-n} z^{-n}$ y $g = \sum_{n=1}^{\infty} b_{-n} z^{-n}$, tal que su producto de Dirichlet este bien definido, tenemos que $f \otimes g$ está en $N_+(\mathbb{Z})$. luego no podemos hablar de un grupo de unidades en $N_-(\mathbb{Z})$.

Ahora estudiaremos un poco el caso cuando los elementos son no homogéneos, los cuales son de la forma

$$\sum_{n\in\mathbb{Z}} a_n z^n,$$

donde existen $n_1 > 0$ y $n_2 < 0$ con $a_{n_1} \neq 0 \neq a_{n_2}$, además a_0 puede ser distinto de cero. Para esto estudiemos algunos casos particulares.

Ejemplo 4. El entero no lineal inhomogéneo $z + z^{-1}$ no es invertible en $N(\mathbb{Q})$ en particular no lo es en $N(\mathbb{Z})$.

Supongamos que es invertible. Entonces existen $f \in N(\mathbb{Q})$ tal que $f \otimes (z + z^{-1}) = z$ pero

$$f \otimes (z + z^{-1}) = f \otimes z + f \otimes z^{-1} = \sum_{q\in\mathbb{Q}} a_q z^q + \sum_{q\in\mathbb{Q}} a_{-q} z^q$$

$$= \sum_{q\in\mathbb{Q}} (a_q + a_{-q}) z^q = \sum_{q\in\mathbb{Q}} c_q z^q = z,$$

donde $c_q = a_q + a_{-q}$. Luego de la ecuación anterior tenemos que $c_q = 0$ para toda $q \neq 1$ y $c_1 = 1$. En particular si $n = 1$ se tiene que

$$1 = c_1 = a_1 + a_{-1} = a_{-1} + a_1 = c_{-1},$$

lo cual es una contradicción pues teníamos que $c_{-1} = 0$.

Nota 4. Si consideramos la función aritmética asociada a $z^{-1} + z$, dada por la siguiente relación,

$$f(n) = \begin{cases} 1 & si \ \ |n| = 1 \\ 0 & \text{en otro caso.} \end{cases}$$

la cual es completamente multiplicativa. Para demostrar esto basta considerar los siguientes casos; si $m = 0 = n$ es claro que $0 = f(mn) = f(m)f(n) = 0$. Si $m \neq 0$ y $n = 0$ entonces $0 = f(mn) = f(m)f(n) = 0$. Por último cuando $m \neq 0$ y $n \neq 0$ tenemos que $1 = f(mn) = f(m)f(n) = 1$ lo cual muestra que $f(n)$ efectivamente es completamente multiplicativa.

Notemos entonces que esta función aritmética nos da un ejemplo muy interesante pues en la Proposición 4.2 habíamos mostrado que si la función aritmética asociada a un entero no lineal $f \in N_+(\mathbb{Z})$ era completamente multiplicativa existía $f^{-1} \in N_+(\mathbb{Z})$ el inverso no lineal de f. Sin embargo, para elementos no homogéneos este criterio no funciona pues $z^{-1} + z$ tiene asociada una función aritmética completamente multiplicativa y sin embargo no tiene ni siquiera inverso formal.

Nota 5. Otro punto interesante que hay que notar es que este ejemplo nos muestra también un número no lineal tal que $a_1 \neq 0$ y sin embargo no es invertible formalmente lo cual muestra que el Teorema 4.3 no se puede extender a todo $N(\mathbb{Z})$.

Si consideráramos ahora *funciones aritméticas* de $\mathbb{Z} \to \mathbb{C}$ o más general de $\mathbb{Q} \to \mathbb{C}$ podríamos construir sus series de Dirichlet generalizadas asociadas. Sin embargo, el ejemplo anterior nos muestra que dos Teoremas importantes de las series de Dirichlet no podrían ser recuperados para esta generalización. Este podríamos considerarlo como uno de los primeros resultados para series de Dirichlet que es consecuencia del estudio de los campos de números no lineales.

Teorema 4.4. *Los polinomios de la forma* $f = z^{-k} + \cdots + z^{-1} + z + \cdots + z^k$ *no son unidades.*

Demostración. Supongamos que sí, entonces existe un $f \in N(\mathbb{Z})$ tal que

$$f \otimes (z^{-k} + \cdots + z^{-1} + z + \cdots + z^k) = 1,$$

desarrollando y agrupando por multiplicidad tendríamos que el coeficiente de z que es $a_1 + a_{-1}$ tendría que ser 1 pero por otro lado el coeficiente de z^{-1}, $a_{-1} + a_1 = a_1 + a_{-1}$ tendría que ser cero lo cual es una contradicción. □

Ejemplo 5. *El número no lineal inhomogéneo* $z^2 + z^{-1}$ *es unidad formal en* $N(\mathbb{Z})$ *pero su inverso no define un número no lineal.*

Vamos a construir f tal que $f \oslash (z^2 + z^{-1}) = z$. Primero, tenemos que

$$f \oslash (z^2 + z^{-1}) = f \oslash z^2 + f \oslash z^{-1} = \sum_{n\in\mathbb{Z}} a_n z^{2n} + \sum_{n\in\mathbb{Z}} a_{-n} z^n$$

$$= \sum_{n \text{ impar}} a_{-n} z^n + \sum_{n \text{ par}} a_{n/2} + a_{-n} z^n,$$

si igualamos esto con z tenemos que si n es impar $a_{-n} = 0$ para toda $n \neq 1$ y $a_{-1} = 1$. Ahora si n es par tenemos que $a_{n/2} + a_{-n} = 0$, o $a_{n/2} = -a_{-n}$

$$\begin{aligned}
a_2 &= -a_{-2/2} = -a_{-1} = -1,\\
a_{-4} &= -a_{4/2} = -a_2 = 1,\\
a_{-2} &= -a_{2/2} = -a_1 = 0,\\
a_4 &= -a_{-4/2} = -a_{-2} = 0,\\
a_8 &= -a_{-8/2} = -a_{-4} = -1,\\
a_{-8} &= -a_{8/2} = -a_4 = 0,\\
a_6 &= -a_{-6/2} = -a_{-3} = 0,\\
a_{-6} &= -a_{6/2} = -a_3 = 0.
\end{aligned}$$

de donde podemos deducir que si $n < 0$ entonces

$$a_n = \begin{cases} 1 & \text{si } n = -2^{2k},\ k = 0, 1, \cdots \\ 0 & \text{en otro caso.} \end{cases}$$

y si $n > 0$,

$$b_n = a_n = \begin{cases} -1 & \text{si } n = 2^{2k+1},\ k = 0, 1, \cdots \\ 0 & \text{en otro caso.} \end{cases}$$

Además del hecho de que $a_{n/2} + a_{-n} = 0$ para toda n par, tenemos que $a_0 = -a_0$ de donde se sigue que a_0 tiene que ser cero. Luego, el f que andábamos buscando es

$$f = \sum_{n<0} a_n z^n + \sum_{n>0} b_n z^n,$$

donde a_n y b_n son como antes, el cual satisface que $f \oslash (z^2 + z^{-1}) = z$, por construcción. Sin embargo, f no es convergente y por tanto no define un número no lineal. De manera más general.

Proposición 4.3. *Dado un número no lineal de la forma $z^m + z^{-1}$ con $m \in \mathbb{N}$ y $m \neq 1$, existe*

$$f = \sum_{n<0} a_n z^n + \sum_{n>0} b_n z^n \in N(\mathbb{Z}),$$

donde,

$$a_n = \begin{cases} 1 & \textit{si } n = -m^{2k},\ k = 0, 1, \cdots \\ 0 & \textit{en otro caso.} \end{cases}$$

$$b_n = a_n = \begin{cases} 1 & \textit{si } n = m^{2k+1},\ k = 0, 1, \cdots \\ 0 & \textit{en otro caso.} \end{cases}$$

tal que f es una unidad formal de $z^m + z^{-1}$.

Demostración. Vamos a construir f tal que $f \oslash (z^m + z^{-1}) = z$. Primero, tenemos que

$$f \oslash (z^m + z^{-1}) = f \oslash z^m + f \oslash z^{-1} = \sum_{n\in\mathbb{Z}} a_n z^{mn} + \sum_{n\in\mathbb{Z}} a_{-n} z^n$$

$$= \sum_{n=mk+r,\ r\neq 0} a_{-n} z^n + \sum_{n=mk} a_{n/m} + a_{-n} z^n,$$

si igualamos esto con z tenemos que si n no es múltiplo de m, $a_{-n} = 0$ para toda $n \neq 1$ y $a_{-1} = 1$. Ahora si n es múltiplo de m tenemos que $a_{n/m} + a_{-n} = 0$,

de donde siguiendo un procedimiento similar al del ejemplo anterior, podemos deducir que si $n < 0$ entonces

$$a_n = \begin{cases} 1 & \text{si } n = -m^{2k},\ k = 0, 1, \cdots \\ 0 & \text{en otro caso.} \end{cases}$$

y si $n > 0$,

$$b_n = a_n = \begin{cases} 1 & \text{si } n = m^{2k+1},\ k = 0, 1, \cdots \\ 0 & \text{en otro caso.} \end{cases}$$

Además del hecho de que $a_{n/m} + a_{-n} = 0$ para toda n múltiplo de m, tenemos que $a_0 = -a_0$ de donde se sigue que a_0 tiene que ser cero. Luego el f que andábamos buscando es

$$f = \sum_{n<0} a_n z^n + \sum_{n>0} b_n z^n,$$

donde a_n y b_n son como antes. El cual satisface que $f \oslash (z^m + z^{-1}) = z$ por construcción. Sin embargo, f no es convergente y por tanto no define un número no lineal.

□

La Proposición anterior nos muestra que tenemos elementos inhomogéneos con inversa formal y no invertibles, y que además el verificar si un elemento no homogéneo es invertible o no, depende mucho del número en particular, o al menos no se ve una forma clara de encontrar un criterio general para hallar las unidades en $N(\mathbb{Z})$.

Pregunta 1. *¿existen elementos inhomogéneos en $N(\mathbb{Z})$ con inverso?.*

Una discusión parecida para el caso de $N_+(\mathbb{Z}) \oplus N_0(\mathbb{Z})$ con el producto de Cauchy $\otimes$, puede ser dada vía el producto de series de potencias convergentes como en [27].

Para esto podríamos definir nuevamente dos tipos de unidades, las *unidades formales* respecto a $\oplus$ y las *unidades* respecto a $\oplus$ de manera análoga a las definidas para $\otimes$. Luego basados en los resultados para series de potencias tenemos los siguientes resultados para unidades formales en $N_+(\mathbb{Z}) \oplus N_0(\mathbb{Z})$.

Lema 4.1. *Todos los enteros no lineales de la forma*

$$f = 1 - \sum_{n \in \mathbb{N}} a_n z^n,$$

son unidades formales y su inverso viene dado por la serie formal

$$g = 1 + \sum_{n \in \mathbb{N}} b_n z^n,$$

donde $a_1 = b_1$ y $b_n = a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_{n-1} b_1 + a_n$.

De manera más general tenemos que,

Teorema 4.5. *El entero no lineal*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n,$$

tiene inverso formal si y solo si $f(0) \neq 0$.

Sin embargo, para el caso inhomogéneo cabe notar que a diferencia del caso del producto de Dirichlet, el principal problema con el cual podríamos encontrarnos es que cuando hacemos el producto de dos elementos $f = \sum_q a_q z^q$, $g = \sum_q b_q z^q$,

$$f \oplus g = \sum_q \left(\sum_{q_1+q_2=q} a_{q_1} b_{q_2} \right) z^q = \sum_q c_q z^q,$$

tenemos que para cada $q_1 \in \mathbb{Z}$ tal que $q_1 + q_2 = q$, podemos obtener un $q_2 = q - q_1 \in \mathbb{Z}$, por lo tanto, podemos tener una infinidad de productos de la forma $a_{q_1} b_{q_2}$ distintos de cero para cada q. Lo cual es muy diferente del caso de $\otimes$ donde el número de posibilidades de elegir q_1 y q_2 era finito, luego no tenemos ni siquiera la certeza de que todos los coeficientes c_q del producto $f \oplus g$ converjan. Lo cual hace del caso inhomogéneo de $N(\mathbb{Z})$ para el producto de Cauchy un problema más difícil.

Pregunta 2. *¿Existen elementos inhomogéneos en $N(\mathbb{Z})$ con inverso respecto al producto de Cauchy?*

La idea de desarrollar una teoría de unidad para anillos de enteros no lineales, asociados a una extensión $K/\mathbb{Q}$ de Galois, arbitrarios apoyado en series de Dirichlet como lo hemos hecho en esta sección nos llevaría a la necesidad de crear una teoría de multiseries de Dirichlet lo cual está fuera de nuestro alcance en este texto.

Capítulo 5

Teoría Geométrica de Galois

Otra parte importante en la teoría algebraica de números es la teoría de Galois. En este capítulo construiremos una teoría de Galois para $N(K)$ apoyándonos su estructura geométrica y exhibiremos el Teorema principal del artículo [1], el cual muestra que la teoría de Galois de $N(K)$ coincide con la teoría de Galois clásica del campo numérico K. Aquí, daremos por hecho las propiedades básicas de la teoría de variedades de Hilbert las cuales pueden ser consultadas en el Apéndice D.

5.1 El Espacio Proyectivo Complejo $\mathbb{P}H$

Sea H un espacio de Hilbert separable de dimensión infinita. Es claro que H es una variedad de Hilbert con el atlas (Id, H). Luego $\mathrm{Har}_\theta[K]$ y $\mathrm{Har}_\bullet[K]$ son variedades de Hilbert con los atlas $(Id, \mathrm{Har}_\theta[K])$ y $(Id, \mathrm{Har}_\bullet[K])$ respectivamente. donde los espacios $\mathrm{Har}_\theta[K]$ son sub-variedades de Hilbert de $\mathrm{Har}_\bullet[K]$. De hecho, son variedades riemannianas con la métrica inducida por el producto interior. Sin embargo, el hecho de que $N(K)$ sea una variedad riemanniana no es trivial. Para esto, construiremos el espacio proyectivo $\mathbb{P}H$ de un espacio de Hilbert H, así como una métrica para este espacio. Nuestra construcción sigue la línea de [25].

Consideremos a H un espacio de Hilbert complejo con $\langle \cdot, \cdot \rangle$, un producto interior hermitiano en H.

Notemos que $\langle x, y \rangle$ en general no es real. La parte real $\mathrm{Re}\langle x, y \rangle$ es un producto interior definido positivo en H visto como un $\mathbb{R}$-espacio vectorial. La parte imaginaria $\mathrm{Im}\langle x, y \rangle = \mathrm{Re}\langle x, iy \rangle$ es antisimétrica, $\mathrm{Re}\langle x, iy \rangle = -\mathrm{Re}\langle y, ix \rangle$. En particular $\mathrm{Re}\langle x, ix \rangle = 0$.

Sea

$$S_H = \{v \in H : \langle v, v \rangle = 1\},$$

la esfera unitaria en H, y por $H^* = H - \{0\}$. El *espacio proyectivo complejo* $\mathbb{P}H$ es definido como el conjunto de subespacios 1-dimensionales complejos de H el cual está dotado de la topología cociente.

Por $\pi : H^* \to \mathbb{P}H$ denotaremos al mapeo el cual asocia a cada $v \in H^*$ el elemento $v\mathbb{C} \in \mathbb{P}H$.

Sea $v \in S_H$, luego podemos definir la carta $(u_v, \mathbb{P}H_v)$ donde

$$\mathbb{P}H_v = \left\{p \in \mathbb{P}H : \langle v_p, v\rangle \neq 0,\ N_p \in \pi^{-1}(p)\right\},$$

y $u_v : \mathbb{P}H_v \to U_v \subset H$, es dada por

$$u_v(p) = \frac{v_p}{\langle v_p, v\rangle} - v.$$

Proposición 5.1. *$\mathbb{P}H$ es una variedad de Hilbert compleja.*

Demostración. Para dar un atlas para $\mathbb{P}H$ basta tomar las cartas $(u_v, \mathbb{P}H_v)$ donde v corre sobre una base ortonormal del espacio de Hilbert H. Por comodidad tomaremos la base canónica $\{e_i\}$. Entonces podemos definir

$$\mathbb{P}H_i = \mathbb{P}H_{e_i} = \left\{p \in \mathbb{P}H : \langle v_p, e\rangle \neq 0,\ v_p \in \pi^{-1}(p)\right\} = \left\{p = [v] \in \mathbb{P}H : v_i \neq 0\right\},$$

i.e el espacio de todas las líneas que no están contenidas en el hiperplano $\{v_i = 0\}$. Luego podemos escribir a $u_i = u_{e_i} : \mathbb{P}H_i \to U_i \subset H$ como

$$u_i(p) = \frac{v_p}{\langle v_p, e_i\rangle} - e_i = \left(\frac{v_0}{v_i}, \cdots, \frac{v_{i-1}}{v_i}, \frac{v_{i+1}}{v_i}, \cdots\right),$$

Luego tenemos el atlas $(u_i, \mathbb{P}H_i)$ el cual claramente cubre a todo $\mathbb{P}H$. Así que solo falta ver que los mapeos de cambio de coordenada sean biholomorfos. Sin perdida de generalidad podemos suponer $i < j$,

$$u_j \circ u_i^{-1} : u_i(\mathbb{P}H_i \cap \mathbb{P}H_j) \to u_j(\mathbb{P}H_i \cap \mathbb{P}H_j),$$

$$\begin{aligned} u_j \circ u_i^{-1}(v_1, \cdots, v_n, \cdots) &= u_j\left([v_1, \cdots, v_i, 1, v_{i+1}, \cdots]\right) \\ &= \left(\frac{v_1}{v_j}, \cdots, \frac{v_i}{v_j}, \frac{v_{i+1}}{v_j}, \cdots \frac{v_{j-1}}{v_j}, \frac{v_{j+1}}{v_j}, \cdots\right), \end{aligned}$$

de donde se sigue que $u_j \circ u_i$ es un biholomorfismo. Por lo tanto $\mathbb{P}H$ es una variedad de Hilbert compleja. □

Ahora, definiremos una *métrica riemanniana* g^* en H^* tomando como producto interior $g^*(v)(,)$ en T_vH^*

$$g^*(v)(x^*, y^*) = \frac{\operatorname{Re}\langle x^*, y^*\rangle}{\langle v, v\rangle}.$$

Nótese que la acción multiplicativa de $\mathbb{C}^* = \mathbb{C} - \{0\}$ en H^* es isométrica con respecto a esta métrica riemanniana.

Para cada $v \in H^*$ definimos la descomposición ortogonal

$$T_v H^* = T_v^n H^* \oplus T_v^h H^*,$$

donde $T_v^n H^* = v\mathbb{C}$ y $T_v^h H^* = \{x^* : \langle x^*, v\rangle = 0\}$. Luego

$$T_v\pi : T_v^h H^* \to T_{\pi(v)}\mathbb{P}H,$$

se convierte en un isomorfismo lineal. Para $v \in S_H$ la representación de $T_v\pi|_{T_v^h H^*}$ en las coordenadas (Id, H^*) de H^* y $(u_v, \mathbb{P}H_v)$ de $\mathbb{P}H$ es dado por $x^* \mapsto x^*$.

Definiremos una métrica riemanniana g en $\mathbb{P}H$ haciendo una submersión riemanniana $\pi : H^* \to \mathbb{P}H$. Si $p \in \pi(v)$; $v \in S_H$; $x, y \in T_p\mathbb{P}H$ y x^*, y^* sus imágenes inversas en $T_v^h H^*$ bajo $(T_v\pi|_{T_v^h H^*})^{-1}$ ponemos

$$g(p)(x, y) = g^*(v)(x^*, y^*) = \operatorname{Re}\langle x^*, y^*\rangle .$$

Como $z \in \mathbb{C}^*$ actúa en H^* como una isometría, la definición de g no depende de la elección de v.

Ahora queremos determinar la presentación $g(u)$ de g en una carta $(u, \mathbb{P}H_v) \equiv (u_v, \mathbb{P}H_v)$. Primero calculemos la parte principal x_u de un $x \in T_p\mathbb{P}H$, $p \in \mathbb{P}H_v$. Sea $x^* \in T_{v_p}^h H^*$ la imagen inversa de x, con $v_p \in S_H \cap \pi^{-1}(p)$. $c^*(s) = v_p + sx^*$, es una curva tal que $c(s) = \pi \circ c^*(s)$ tiene como vector tangente inicial a x. Por lo tanto,

$$x_u = \frac{d}{ds} u \circ c(s)|_0 = \frac{d}{ds}\left(\frac{v_p + sx^*}{\langle v_p + sx^*, v\rangle} - v\right)|_0$$

$$= \frac{\langle v_p, v\rangle\, x^* - \langle x^*, v\rangle\, v_p}{\langle v_p, v\rangle^2},$$

con

$$u(p) = \frac{v_p}{\langle v_p, v\rangle} - v,$$

luego usando el hecho de que $\langle x^*, v_p\rangle = \langle x_u, v\rangle = 0$ tenemos que

$$g(u)(x_u, x_u) = \frac{\langle x_u, x_u\rangle\,(1 + \langle u, u\rangle) - \langle x_u, u\rangle\,\langle u, x_u\rangle}{(1 + \langle u, u\rangle)^2}, \quad (*)$$

es igual a $\langle x^*, x^*\rangle = g(x, x)$. El elemento de la línea $(*)$ aparece por primera vez en [20] y [21] por lo cual la métrica riemanniana antes mencionada es conocida en la literatura como la *métrica Fubini-Study*.

Teorema 5.1. *$N(K)$ es una subvariedad riemanniana de $\mathbb{P}Har[K]$ abierta, densa y graduada con la métrica Fubini-Study inducida por $\mathbb{P}Har[K]$. La cual a su vez se descompone en subvariedades $N_\theta(K) = \operatorname{Har}_\theta^*[K]/\mathbb{C}^*$ donde $\operatorname{Har}_\theta^*[K]$ es el conjunto de las $F \in \operatorname{Har}_\theta[K]$ tal que $T(F) \neq 0$.*

5.2 Teoría de Galois No lineal

En la sección anterior vimos que $N(K)$ es una subvariedad riemanniana de $\mathbb{P}\mathrm{Har}\,[K]$ con la métrica Fubini-Study.

Definición 11. Un *automorfismo* $\Psi : N(K) \to N(K)$ es una isometría graduada con respecto a la métrica Fubini-Study que respeta las operaciones $\oplus$ y $\otimes$ siempre que estas estén definidas: *i.e.*

$$\Psi(f \oplus g) = \Psi(f) \oplus \Psi(g),$$

$$\Psi(f \otimes g) = \Psi(f) \otimes \Psi(g),$$

y para alguna permutación i de Θ se cumple que $\Psi(N_\theta(K)) = N_{i(\theta)}(K)$. Además, en los lugares complejos i debe satisfacer que $i(\Theta) = \Theta$ e $i(\Omega) = \Omega$.

Si L/K es una extensión de un campo numérico de grado finito sobre $\mathbb{Q}$ denotaremos por

$$\mathrm{Gal}(N(L)/N(K)),$$

el grupo de automorfismos de $N(L)$ que dejan fijo el subcampo no lineal $N(K)$ el cual llamaremos *grupo de Galois No Lineal*. Y denotaremos por

$$\mathrm{Gal}(N(K)/K),$$

al grupo de automorfismos de $N(K)$ que fijan a K.

Se dice que un operador lineal $T : X \to Y$, donde X, Y son espacios normados, es *acotado*, si existe $M > 0$ tal que

$$\|Tv\|_Y = M \|v\|_X ,$$

para toda $v \in X$. Sea H un espacio de Hilbert con producto interior $\langle \cdot, \cdot \rangle$ y consideremos un operador lineal acotado $T : H \to H$. Entonces se puede probar, utilizando el Teorema de Representación de Riez, que existe un único operador lineal acotado $T^* : H \to H$ con la siguiente propiedad

$$\langle Tx, y \rangle = \langle x, T^* y \rangle ,$$

para todo $x, y \in H$. Al operador T^* lo llamaremos operador *adjunto*.

Un *operador unitario* es un operador lineal acotado $U : H \to H$, en un espacio de Hilbert H el cual satisface que

$$U^*U = UU^* = I,$$

donde $I : H \to H$ denota el operador identidad. Luego, son equivalentes

i) El rango de U es denso, y

ii) U preserva producto interior $\langle \cdot, \cdot \rangle$ en el espacio de Hilbert H *i.e.* para toda $x, y \in H$ $\langle Ux, Uy \rangle = \langle x, y \rangle$.

Notemos de *ii*) que el hecho de que U preserve producto interior implica que U es una isometría. Además, de *i*) se tiene que existe un inverso U^{-1} de U acotado, definido en el rango de U, de donde se sigue que $U^{-1} = U^*$.

Se dice que un operador lineal $U : H \to H$, donde H es un espacio de Hilbert complejo, es *antiunitario* si cumple que

$$\langle Ux, Uy\rangle = \overline{\langle x, y\rangle} = \langle y, x\rangle \,,$$

para toda $x, y \in H$.

Teorema 5.2 (Wigner)**.** *Sea H un espacio de Hilbert complejo y $\mathbb{P}H = (H - \{0\})/\mathbb{C}^*$ su proyectivización. Sea $[h] : \mathbb{P}H \to \mathbb{P}H$ una biyección que preserva la métrica de Fubini-Study. Entonces $[h]$ es la proyectivización de un operador lineal unitario o antiunitario $h : H \to H$.*

Demostración. Para una prueba ver [22]. □

Teorema 5.3. *Sea K un campo numérico. Entonces*

$$\mathrm{Gal}(N(K)/K) \cong \{1\} \,.$$

Demostración. Sea $\sigma \in \mathrm{Gal}(N(K)/K)$. Consideremos $[F] \in \mathbb{P}\mathrm{Har}_\bullet\,[K] - N(K)$, y sea $l_{[F]}$ la única geodésica que comienza en $[\mathrm{id}_\oplus]$, la cual tiene traza distinta de cero y termina en$[F]$ en tiempo $t = 1$ (la cual tomamos con traza cero y por la densidad de $N(K)$ podemos aproximarla tanto como queramos por elementos de $N(K)$) y además no pasa por ∞. Luego podemos definir a $\sigma([F])$ como el punto final de $\sigma(l_{[F]})$. Esto tiene sentido pues

$$l^N_{[F]} = l_{[F]} \cap N(K),$$

es una geodésica en $N(K)$ luego su imagen $\sigma(l^N_{[F]})$ también es geodésica y por tanto $\sigma([F]) = \sigma(l^N_{[F]})(1)$. Luego esto extiende a σ isométrica y canónicamente a toda la proyectivización de $\mathrm{Har}_\bullet\,[K]$. Ahora por el Teorema de Wigner, σ es la proyectivización de un operador lineal (anti) unitario,

$$\tilde{\sigma} : \mathrm{Har}_\bullet\,[K] \to \mathrm{Har}_\bullet\,[K] \,.$$

Como σ fija a K, entonces existen múltiplos escalares $\lambda_q \in S^1$ tal que

$$\tilde{\sigma}(\xi^q) = \lambda_q \cdot \xi^q.$$

Pero σ es una isometría que respeta el producto de Cauchy y el producto de Dirichlet. Luego debemos tener que λ debe ser un caracter aditivo y multiplicativo simultáneamente, *i.e.*

$$\lambda_{q_1+q_2} = \lambda_{q_1}\lambda_{q_2} = \lambda_{q_1 q_2}.$$

Pero del isomorfismo de campos $\mathrm{Char}\hat{\mathbb{S}}_K \cong K$ se sigue que la única posibilidad de que este pase es que λ sea trivial. □

Nuestro siguiente paso es probar que nuestra teoría de Galois no lineal coincide con la teoría de Galois clásica en el sentido de que

$$\mathrm{Gal}(N(L)/N(K)) \cong \mathrm{Gal}(L/K).$$

Lema 5.1. *Dado $\theta \in \Theta$ y sea $F \in Har_\theta[\mathbb{Q}]$ tal que satisface la siguiente ecuación funcional*

$$F(rz) = (F(z))^r,$$

para toda $r \in \mathbb{R}_{>0}$ y $z \in \mathbb{H}_\mathbb{Q}$. Entonces $F \in \mathbb{Q}$.

Demostración. Sin perdida de generalidad podemos suponer $F \in \mathrm{Har}[\mathbb{Q}]$, *i.e.* $\theta = +$. Como $F \in \mathrm{Har}[\mathbb{Q}]$, tenemos que la restricción de F a $\mathbb{H}_\mathbb{Q}$ tiene el siguiente desarrollo:

$$F(z) = \sum_{q>0} a_q \exp(2\pi i q z) = \sum_{q>0} (a_q \exp(-2\pi q t)) \exp(2\pi i q x),$$

donde $\|F\| = \sum |a_q|^2 < \infty$ con la norma L^2.

De la ecuación funcional $F(rz) = (F(z))^r$ tenemos que

$$(F(z))^r = F(rz) = \sum_{q>0} (a_q \exp(-2\pi q r t)) \exp(2\pi i q r x),$$

Si $|F(z)| > 1$ para alguna z, entonces la parte izquierda de la ecuación anterior no es acotada en los puntos de la línea $l_{[z]} = \{rz : r \in \mathbb{R}_+\}$, mientras que la norma de la derecha es acotada por $\|F\| < \infty$. Por lo tanto $F(z)$ toma valores en el disco unitario en $\mathbb{C}$.

Sea

$$q_0 = \inf_{a_q \neq 0} q;$$

veamos que $q_0 \in \mathbb{Q}$ y $a_{q_0} \neq 0$. Supongamos que esto es falso y consideremos las aproximaciones definidas como

$$F_\epsilon(z) = \sum_{q \geq q_0 + \epsilon} a_q \exp(2\pi i q z),$$

las cuales convergen uniformemente en compactos a F. En particular, F^r está uniformemente cerca de F_ϵ^r en una vecindad compacta para $r \in [0, r_0]$. Por otro lado

$$|F^r(z)| = \left| \sum_q (a_q \exp(-2\pi q r t)) \exp(2\pi i q r x) \right| \leq \sum_q |a_q| \, |\exp(-2\pi q r t)| \, |\exp(2\pi i q r x)|$$

$$\leq \sum_q |a_q| \exp(-2\pi q r t) = \sum_q |a_q| \exp(-2\pi (q + \epsilon - \epsilon) r t)$$

$$\approx \exp(-2\pi \epsilon r t) \sum_{q \geq q_0 + \epsilon} |a_q| \exp(-2\pi (q - \epsilon) r t) \leq \exp(-2\pi \epsilon r t) \, \|F\| \to 0,$$

cuando $r \to 0$. Pero esto es imposible pues $|F^r(z)|$ tiene límite 1.

Es claro que el mismo argumento demuestra que cada $A \subset \{q : a_q \neq 0\}$ tiene elemento mínimo. Luego hemos reducido nuestro problema al caso donde el conjunto de q's para los cuales $a_q \neq 0$ es bien ordenado.

La expresión $F(z)\exp(-2\pi i q_0 z)$ define un elemento de Har $[\mathbb{Q}]$ el cual también satisface la ecuación funcional de la hipótesis, teniendo el siguiente desarrollo:

$$F(z)\exp(-2\pi i q_0 z) = \sum_q a_q \exp(2\pi i q z)\exp(-2\pi i q_0 z) = a_{q_0} + \sum_{q>q_0} a_q \exp(2\pi i (q-q_0) z).$$

Luego la ecuación funcional implica que la suma de los términos no constantes del lado derecho de la ecuación debe de ser cero. De modo que $F(z) = a_{q_0}\exp(-2\pi i q_0 z)$. Como

$$F(0) = \lim_{r\to 0} F(rz) = (F(z))^r = 1,$$

tenemos que $a_{q_0} = 1$. Lo que quiere decir que F es el caracter ξ^{q_0}. Luego $F \in \mathbb{Q}$. □

En el caso de una extensión finita $K/\mathbb{Q}$, se prueba de manera análoga. Lo que se muestra es que existe $q_0 \in K$ tomando $\inf_{a_q \neq 0} q$ (el cual es tomado en el conjunto parcialmente ordenado K_∞) para el cual $a_{q_0} \neq 0$, de donde se sigue que F es el caracter ξ^{q_0}.

Teorema 5.4. *Sea K una extensión de Galois real (compleja) de grado finito. Dado $\theta \in \Theta$ ($\theta \in \Theta_{\mathbb{C}}$ o $\omega \in \Omega$) y sea $F \in H_\theta[K]$ ($F \in H_\omega[K]$) tal que satisface la siguiente ecuación funcional*

$$F(rz) = (F(z))^r,$$

para toda $r \in \mathbb{R}_{>0}$ y $z \in \mathbb{H}_K$ ($w \in \mathbb{H}_K$). Entonces $F \in K$.

Teorema 5.5 (Gendron-Verjovsky)**.** *Sea L/K una extensión de Galois de un campo numérico de grado finito. Entonces*

$$\mathrm{Gal}(N(L)/N(K)) \cong \mathrm{Gal}(L/K).$$

Demostración. Sea $\sigma \in \mathrm{Gal}(N(L)/N(K))$. Mostraremos primero que $\sigma(L) = L$, donde a L lo podemos identificar con el campo de monomios $[\xi^q]$, $q \in L$.

Por definición tenemos que $\sigma(K) = K$. Como $\sigma(L)$ es un campo todos sus elementos obedecen a la ley distributiva. Entonces dado $[F] \in \sigma(L)$ y como $\sigma([\xi^m]) = [\xi^m]$, $m \in \mathbb{N}$, tenemos que

$$\begin{aligned}[F(\xi^m)] = [F] \otimes [\xi^m] &= [F] \otimes ([\xi] \oplus \cdots \oplus [\xi]) \\ &= ([F] \otimes [\xi]) \oplus \cdots \oplus ([F] \otimes [\xi]) \\ &= [F(\xi)] \oplus \cdots \oplus [F(\xi)]\,.\end{aligned}$$

Ahora dado $m/n \in \mathbb{Q}_{>0}$ y $(\cdot)^n$ la n-ésima potencia respecto a producto de Cauchy tenemos que

$$\begin{aligned}\left[F(\xi^{m/n})\right]^n &= \left([F] \otimes \left[\xi^{m/n}\right]\right)^n = \left([F] \otimes \left(\left[\xi^{1/n}\right] \oplus \cdots \oplus \left[\xi^{1/n}\right]\right)\right)^n \\ &= \left(([F] \otimes \left[\xi^{1/n}\right]) \oplus \cdots \oplus ([F] \otimes \left[\xi^{1/n}\right])\right)^n \\ &= \left[F(\xi^{1/n})\right]^n \oplus \cdots \oplus \left[F(\xi^{1/n})\right]^n \\ &= [F(\xi)] \oplus \cdots \oplus [F(\xi)] = ([F(\xi)])^m.\end{aligned}$$

Notemos, por definición de automorfismo, que dado que σ respeta la graduación y que cada elemento de L es homogéneo, *i.e.* está contenido en un sumando fijo $N_\theta(L)$, entonces $[F] \in N_{\theta'}(L)$, *i.e.* $[F]$ es homogéneo. Luego podemos encontrar $F \in [F]$, $F \in \mathrm{Har}_{\theta'}[L]$ tal que satisface la ecuación funcional $F(qz) = (F(z))^q$ para toda $z \in \mathbb{H}_L$ y $q \in \mathbb{Q}_{>0}$. La cual se extiende por continuidad a $\mathbb{R}_{>0}$. Luego por el Teorema 5.4 tenemos que $F \in L$ y $\sigma(L) = L$.

En este sentido, podemos inducir un homomorfismo

$$\Upsilon : \mathrm{Gal}(N(L)/N(K)) \to \mathrm{Gal}(L/K),$$

Pues $\tau \in \mathrm{Gal}(L/K)$ genera un automorfismo de $N(L)$ fijando $N(K)$ vía el mapeo $\xi^q \to \xi^{\tau(q)}$. Supongamos ahora que $\Upsilon(\sigma) = 1$ para algún automorfismo $\sigma \in \mathrm{Gal}(N(L)/N(K))$, luego sigma fija a L. Entonces $\sigma \in \mathrm{Gal}(N(L)/L) = \{1\}$. □

Ahora, centraremos nuestra atención en los campos numéricos K de grado n sobre $\mathbb{Q}$ y las operaciones $\oplus$ y $\otimes$ por separado.

Definición 12. Definimos $\mathrm{Gal}_\oplus(N(K)/K)$ el conjunto de isometrías que fijan a K y son un homomorfismo con respecto al producto de Cauchy $\oplus$. De manera análoga se define $\mathrm{Gal}_\otimes(N(K)/K)$ para el producto de Dirichlet.

Denotemos por $U(\mathrm{Har}_\bullet[K])$ el grupo de operadores unitarios de $\mathrm{Har}_\bullet[K]$. Notemos que la acción de $r \in K_\infty$ por traslación en $\mathbb{H}_K$, dado por $z \mapsto z + r$ induce una acción en $\mathrm{Har}_\bullet[K]$ dada por

$$\Phi_r(F) = \sum_q a_q \exp(2\pi i \langle q, z + r\rangle) = \sum_q a_q \exp(2\pi i \langle q, r\rangle)\xi^q,$$

para

$$F = \sum_q a_q \xi^q,$$

la cual induce la siguiente representación fiel

$$\Phi : K_\infty \to U(\mathrm{Har}_\bullet(K)).$$

i.e a cada $r \in K_\infty$ le asignamos el operador unitario Φ_r.

Teorema 5.6. *La proyectivización* $[\Phi]$ *de* Φ *define un monomorfismo*

$$[\Phi] : K_\infty \hookrightarrow \mathrm{Gal}_\oplus(N(K)/K).$$

Demostración. Para $[\exp(2\pi i \langle z, q\rangle)] = [\xi^q] \in K$ y $r \in K_\infty$, tenemos que

$$[\Phi]_r ([\xi^q]) = [\exp(2\pi i \langle q, r\rangle)\xi^q] = [\xi^q].$$

Para todo $[F]$, $[G] \in N(K)$, sean $[f]$ y $[g]$ las clases proyectivas de sus funciones frontera. Luego $[\Phi]_r ([F] \oplus [G])$ es un elemento de $N(K)$ cuyas funciones frontera son

$$[\Phi]_r ([f] \oplus [g]) = \left[\sum_q \left(\sum_{q_1+q_2=q} a_{q_1} b_{q_2}\right) \exp(2\pi i \langle q, r\rangle)\eta^q\right]$$

$$= \left[\sum_q \left(\sum_{q_1+q_2=q} a_{q_1} b_{q_2} \exp(2\pi i \langle q_1 + q_2, r\rangle)\right) \eta^q\right]$$

$$= \left[\sum_q \left(\sum_{q_1+q_2=q} a_{q_1} \exp(2\pi i \langle q_1, r\rangle) b_{q_2} \exp(2\pi i \langle q_2, r\rangle)\right) \eta^q\right]$$

$$= [\Phi]_r ([f]) \oplus [\Phi]_r ([g]),$$

la cual es la función frontera de $[\Phi]_r ([F]) \oplus [\Phi]_r ([G])$.

□

De la misma manera podemos definir un flujo en $N(K)$ con respecto a $\otimes$ como sigue. Para un vector $x \in K_\infty$ denotaremos por $\log|x|$ al vector

$$(\log|x_{\nu_1}|, \cdots, \log|x_{\nu_n}|).$$

si K es real o

$$(\log|x_{\mu_1}|, \log|x_{\mu_1}|, \cdots, \log|x_{\mu_s}|, \log|x_{\mu_s}|).$$

si K es complejo.

Luego para

$$F = \sum_q a_q \xi^q,$$

definimos

$$\Psi_r(F) = \sum_{q \in K} a_a \exp(2\pi i \langle \log|q|, r\rangle)\xi^q.$$

El cual define una representación fiel

$$\Psi : K_\infty \to U(\mathrm{Har}_\bullet [K]),$$

luego tenemos un Teorema análogo para $\otimes$

Teorema 5.7. *La proyectivización* $[\Psi]$ *de* Ψ *define un monomorfismo*

$$[\Psi] : K_\infty \hookrightarrow \mathrm{Gal}_\otimes(N(K)/K).$$

Demostración. Para $[\xi^q] \in K$ podemos identificar a $[\xi^q]$ con $[\exp(2\pi i \langle \log|q|, z\rangle)]$ y $r \in K_\infty$, luego tenemos que

$$[\Psi]_r([\xi^q]) = [\exp(2\pi i \langle \log|q|, r\rangle)\xi^q] = [\xi^q].$$

Para todo $[F]$, $[G] \in N(K)$, sean $[f]$ y $[g]$ las clases proyectivas de sus funciones frontera. Luego $[\Psi]_r([F] \otimes [G])$ es un elemento de $N(K)$ cuyas funciones frontera son

$$\begin{aligned}
[\Psi]_r([f] \otimes [g]) &= \left[\sum_q \left(\sum_{q_1 q_2 = q} a_{q_1} b_{q_2}\right) \exp(2\pi i \langle \log|q|, r\rangle)\eta^q\right] \\
&= \left[\sum_q \left(\sum_{q_1 q_2 = q} a_{q_1} b_{q_2} \exp(2\pi i \langle \log|q_1 q_2|, r\rangle)\right)\eta^q\right] \\
&= \left[\sum_q \left(\sum_{q_1 q_2 = q} a_{q_1} b_{q_2} \exp(2\pi i \langle \log|q_1| + \log|q_2|, r\rangle)\right)\eta^q\right] \\
&= \left[\sum_q \left(\sum_{q_1 q_2 = q} a_{q_1} \exp(2\pi i \langle \log|q_1|, r\rangle) b_{q_2} \exp(2\pi i \langle \log|q_2|, r\rangle)\right)\eta^q\right] \\
&= [\Psi]_r([f]) \otimes [\Psi]_r([g]),
\end{aligned}$$

la cual es la función frontera de $[\Psi]_r([F]) \otimes [\Psi]_r([G])$.

□

Apéndice A

Grupos Topológicos

En este apéndice damos un resumen de la teoría de grupos topológicos, necesaria para esta tesis. Las referencias básicas son [4], [2].

Un grupo topológico es un grupo G dotado de una topología y tal que cumple las siguientes propiedades:

- La operación de grupo
$$G \times G \to G$$
$$(g, h) \longmapsto gh,$$
es un mapeo continuo.
- El mapeo inverso
$$G \to G$$
$$g \longmapsto g^{-1},$$
es también continuo.

A.1 Propiedades Básicas

Notemos primero que la topología es *invariante bajo traslaciones* en el sentido de que para toda $g \in G$ y $U \subseteq G$: las siguientes tres afirmaciones son equivalentes:

- U es abierto.
- gU es abierto.
- Ug es abierto.

Además, dado que el mapeo inverso es también homeomorfismo, U es abierto si y solo si $U^{-1} = \left\{x : x^{-1} \in U\right\}$ es abierto. Un aspecto fundamental de los grupos topológicos es la *homogeneidad*. En general, si X es un espacio topológico,

Homeo(X) el conjunto de los homeomorfismos $X \to X$ y S un subconjunto de Homeo(X), entonces se dice que X es un *espacio homogéneo bajo* S si para todo $x, y \in X$, existe $f \in S$ tal que $f(x) = y$. Si no especificamos quien es S o si es todo Homeo(X) se dice simplemente que X es un *espacio homogéneo*. Es claro que un grupo topológico G es homogéneo en el sentido de que dados cualesquiera dos puntos $g, h \in G$, el homeomorfismo definido como traslación por la izquierda dado por hg^{-1} manda g en h. De aquí se sigue que una base local para la identidad $e \in G$ determina una base local en todos los puntos de G y por tanto la topología completa de G.

Algunos ejemplos de grupos topológicos son: $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{R}_{>0}$ y $\mathbb{C}^*$ con respecto a la multiplicación ordinaria y la topología euclidiana. También $\mathbb{R}^n$ y $\mathbb{C}^n$ son grupos topológicos con respecto a la suma de vectores y la topología euclidiana. Algunos ejemplos más complejos son: $\mathrm{GL}_n(k)$ y $\mathrm{SL}_n(k)$ definidos como sigue: dado $k = \mathbb{R}$ o $\mathbb{C}$, $n \geq 1$ y $M_n(k)$ el conjunto de matrices de $n \times n$, el grupo lineal general

$$\mathrm{GL}_n(k) = \{g \in M_n(k) : \det(g) \neq 0\},$$

es un grupo topológico con respecto a la multiplicación de matrices y la topología euclidiana. Luego el grupo especial lineal

$$\mathrm{SL}_n(k) = \{g \in \mathrm{GL}_n(k) : \det(g) = 1\},$$

es un subgrupo cerrado de $\mathrm{GL}_n(k)$. Decimos que un subconjunto S de G es *simétrico* si $S = S^{-1}$.

Proposición A.1. *Dado G un grupo topológico, tenemos las siguientes afirmaciones:*

i) Cada vecindad U de la identidad contiene una vecindad V de la identidad tal que $VV \subseteq U$.

ii) Cada vecindad U de la identidad contiene una vecindad simétrica V de la identidad.

iii) Si H es un subgrupo de G, también lo es su cerradura.

iv) Cada subgrupo abierto de G, es cerrado.

v) Si K_1 y K_2 son subconjuntos compactos de G, K_1K_2 es compacto.

Notemos que de 1 y 2 se sigue que, toda vecindad U de la identidad contiene una vecindad simétrica V tal que $VV \subseteq U$.

Proposición A.2. *Sea H un subgrupo de un grupo topológico G. Si H contiene una vecindad del elemento identidad e en G, entonces H es abierto y cerrado en G.*

dada función arbitraria f en un grupo topológico G, definimos sus *traslaciones izquierdas* y *derechas* por las fórmulas

$$L_h f(g) = f(h^{-1}g) \quad \text{y} \quad R_h f(g) = f(gh).$$

Si f es una función continua (real o complejo valuada) en un grupo topológico, diremos que f es *uniformemente continua* por la izquierda si para cada $\epsilon > 0$ existe una vecindad V de e tal que:

$$h \in V \Rightarrow \|L_h f - f\|_u < \epsilon,$$

donde $\|\cdot\|_u$ denota la norma uniforme o norma del supremo[1]. La continuidad uniforme por la derecha se define de manera análoga. Recordemos que $\mathcal{C}_c(G)$ denota el conjunto de las funciones continuas en G con soporte compacto.

Proposición A.3. *Sea G un grupo topológico. Entonces cada función f en $\mathcal{C}_c(G)$ es uniformemente continua tanto por la derecha como por la izquierda.*

Notemos, que la Proposición anterior caracteriza las funciones en un grupo topológico con soporte compacto.

Proposición A.4. *Sea un grupo topológico G. Luego las siguientes afirmaciones son equivalentes:*

i) G es T_1.

ii) G es Hausdorff.

iii) La identidad e es cerrada en G.

iv) Cada punto de G es cerrado.

Esta Proposición nos muestra que en los grupos topológicos los axiomas de separación T_1 y T_2 (Hausdorff) tienen la misma fuerza.

Si H es un subgrupo del grupo topológico G, el conjunto G/H de clases laterales izquierdas adquiere la *topología cociente*, definida como la topología más fuerte tal que la proyección canónica

$$\rho : g \longrightarrow gH,$$

es continua. Luego U es abierto en G/H si y solo si $\rho^{-1}(U)$ es abierto en G. Luego, es claro G/H constituye un grupo topológico con respecto a la topología cociente.

Proposición A.5. *Sea G un grupo topológico y sea H un subgrupo de G. Entonces, las siguientes afirmaciones son equivalentes:*

[1] La norma uniforme o del supremo de una función acotada f, real o complejo valuada, se define como

$$\|\cdot\|_u = \sup\{|f(x)| : x \text{ está en el dominio de } f\},$$

esta norma también es conocida como la norma de Chebyshev.

i) El espacio cociente G/H es homogéneo bajo G.

ii) La proyección canónica $\rho : G \longrightarrow G/H$ es un mapeo abierto.

iii) El espacio cociente G/H es T_1 si y solo si H es cerrado.

iv) El espacio cociente G/H es discreto si y solo si H es abierto. Además, si G es compacto, entonces H es abierto si y solo si G/H es finito.

v) Si H es normal en G, entonces G/H es grupo topológico con respecto a la operación cociente y la topología cociente.

vi) Sea H la cerradura de $\{e\}$ en G. Entonces H es normal en G, y el grupo cociente G/H es Hausdorff con respecto a la topología cociente.

Cabe notar que del último inciso se deduce que cada grupo topológico se proyecta por un homomorfismo continuo en un grupo topológico con la topología de Hausdorff.

Proposición A.6. *Sea G un grupo topológico Hausdorff. Luego las siguientes afirmaciones son verdaderas:*

i) El producto de un subconjunto cerrado F y un subconjunto compacto H es cerrado.

ii) Si H es un subgrupo compacto de G, entonces $\rho : G \longrightarrow G/H$ es un mapeo cerrado.

A.2 Grupos Localmente Compactos

Recordemos que un espacio topológico es llamado *localmente compacto* si cada punto admite una vecindad compacta.

Definición 13. Un grupo topológico G que es localmente compacto y Hausdorff es llamado *grupo localmente compacto.*

Notemos que dada la hipótesis de que el grupo es localmente compacto y Hausdorff, implica que todos sus puntos son cerrados.

Proposición A.7. *Sea G un grupo topológico Hausdorff. Entonces un subgrupo H de G que es localmente compacto es cerrado. En particular, cada subgrupo discreto de G es cerrado.*

Si un grupo topológico es *metrizable* entonces este es un espacio Hausdorff y tiene un sistema fundamental de vecindades numerable de la identidad e. Conversamente uno puede mostrar que esta condición es suficiente para la metrizabilidad [4].

Luego un grupo metrizable G puede ser siempre *completado i.e.* existe un grupo completo $\hat{G}$ y un homomorfismo $j : G \to \hat{G}$ tal que:

- La imagen $j(G)$ es densa en $\hat{G}$.
- j es un homeomorfismo de G en $j(G)$.
- Todo homomorfismo continuo $f : G \to G'$ en un grupo completo G' puede ser factorizado de manera única como $f = g \circ j : G \to G'$ con un homomorfismo continuo $g : \hat{G} \to G'$.

Dado que $\hat{G}$ la completación de G es un grupo topológico, entonces si G es localmente compacto este debe ser cerrado en su completación. Luego, se tiene que un grupo localmente compacto metrizable es completo.

Apéndice B

Grupos Profinitos

En este apéndice estudiamos a grandes rasgos el concepto de grupo profinito, para el cual es necesario entender antes el concepto de límite proyectivo. El material aquí presentado puede ser leído en [2] y [4].

B.1 Límites Proyectivos

Sea I un conjunto no vacío. Diremos que I es un *conjunto preordenado* con respecto a la relación $\leq$ si satisface que

- $i \leq j$, $\forall i \in I$ (Reflexividad),
- $i \leq j$ y $j \leq k \Rightarrow i \leq k$, $\forall i, j, k \in I$ (Transitividad).

Diremos que un conjunto preordenado I es un *conjunto directo* si cada subconjunto finito de I está acotado superiormente en I.

El conjunto de los números enteros $\mathbb{Z}$ es un conjunto preordenado con respecto a la divisibilidad. Más aún, es un conjunto directo, pues todo subconjunto finito de $\mathbb{Z}$ está acotado superiormente en $\mathbb{Z}$ por su mínimo común múltiplo.

Ahora supongamos que I es un conjunto preordenado de índices y sea $\{G_i\}_{i\in I}$ una familia de conjuntos. Supongamos, además, que para cada par de índices $i, j \in I$ con $i \leq j$ tenemos un mapeo asociado $\varphi_{ij} : G_j \to G_i$, sujeto a las siguientes condiciones

i) $\varphi_{ii} = 1_{G_i}, \forall i \in I$,

ii) $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$, $\forall i, j, k \in I$, $i \leq j \leq k$,

luego, el sistema (G_i, φ_{ij}) es llamado un *sistema proyectivo*.

Definición 14. Sea (G_i, φ_{ij}) un sistema proyectivo de conjuntos. Entonces definimos *el límite proyectivo* por el siguiente conjunto,

$$\varprojlim G_i = \left\{ (g_i) \in \prod_{i\in I} G_i : i \leq j \Rightarrow \varphi_{ij}(g_j) = g_i \right\}.$$

Notemos que dado que el límite inverso es un subconjunto del producto directo, puede ser naturalmente equipado con una familia de proyecciones,

$$p_j : \varprojlim G_i \to G_j.$$

Luego tenemos la siguiente propiedad universal del límite inverso.

Propiedad Universal : *Sea H un conjunto no vacío y un sistema de mapeos $\{\psi_i : H \to G_i\}_{i\in I}$ el cual es compatible con el sistema proyectivo en el sentido de que para cada par de índices $i, j \in I$, con $i \leq j$, existe*

$$\varphi_{ij} : G_j \longrightarrow G_i$$

tal que $\varphi_{ij} \circ \psi_j = \psi_i$. Entonces existe un único mapeo

$$\psi : H \longrightarrow \varprojlim G_i$$

tal que para cada $i \in I$ $p_i \circ \psi = \psi_i$.

Claramente el mapeo ψ está dado por

$$h \mapsto (\psi_i(h))_{i\in I}$$

como en el producto directo de conjuntos. Cabe notar que ni la definición ni la Propiedad Universal de límite proyectivo, afirma que dado un límite proyectivo de conjuntos este es o no vacío, en particular las proyecciones pueden tener dominio vacío. Pero es claro que si existe un sistema compatible $\{\psi : H \to G_i\}_{i\in I}$ con dominio no vacío H, entonces uno puede inferir la existencia de elementos de la forma $(\psi_i(h))_{i\in I}$ lo que implica que el límite proyectivo es no vacío.

Un caso de nuestro interés es cuando estos conjuntos son grupos en cuyo caso el conjunto de mapeos es remplazado por homomorfismos de grupos y la operación de grupos es definida entrada a entrada. Notemos, que este límite nunca puede ser vacío pues la identidad del producto directo está en el límite proyectivo. Es de nuestro interés también cuando nuestros conjuntos son espacios topológicos, luego nuestro conjunto de mapeos, deben ser las funciones continuas y la topología del límite proyectivo es la inducida por la topología producto del producto directo de espacios topológicos. De aquí podemos deducir que el límite proyectivo de un sistema proyectivo de grupos topológicos es un grupo topológico con respecto a la multiplicación entrada a entrada y la topología inducida por el producto topológico.

Sea G un grupo topológico y $\{H_n\}$ una sucesión decreciente de subgrupos normales de G. Luego podemos tomar $G_n = G/H_n$, como $H_{n+1} \subset H_n$ tenemos $\varphi_n : G/H_{n+1} \to G/H_n$ la proyección canónica. Entonces el límite proyectivo de esta sucesión es un subgrupo del producto topológico.

$$\hat{G} = \varprojlim G/H_n \subset \prod G/H_n,$$

junto con las proyecciones restringidas $\psi_n : \hat{G} \to G/H_n$. Como el sistema de mapeos cociente $f_n : G \to G/H_n$ es siempre un sistema compatible, obtenemos una factorización $f : G \to \hat{G}$ tal que $f_n = \psi_n \circ f$. Luego de la factorización de f podemos determinar el kernel fácilmente.

$$ker f = f^{-1}\left(\bigcap ker\psi_n\right) = \bigcap ker f_n = \bigcap H_n.$$

Proposición B.1. *Sea $G = \lim_{\leftarrow} G_n$ el límite proyectivo de grupos topológicos, y sean $\psi_n : G \to G_n$ los homomorfismos canónicos. Entonces, $\cap\ ker\ \psi_n = \{e\}$ y G es canónicamente isomorfo a $G = \lim\limits_{\leftarrow}(G/ker\psi_n)$.*

B.2 Grupos Profinitos

Consideremos un sistema proyectivo de grupos finitos cada uno dotado con la topología discreta. Luego el límite proyectivo tiene la topología inducida por la topología producto la cual llamaremos *topología profinita*. Luego, el límite proyectivo adquiere una estructura de grupo topológico.

Definición 15. Un grupo topológico isomorfo a un límite proyectivo de un sistema proyectivo de grupos finitos con la topología profinita es llamado *grupo profinito.*

Proposición B.2. *Sea G un grupo profinito, visto como el límite proyectivo del sistema proyectivo (G_i, φ_{ij}). Entonces las siguientes propiedades son equivalentes*

i) G es Hausdorff con respecto a la topología profinita.

ii) G es un subconjunto cerrado del producto directo $\prod G_i$.

iii) G es compacto.

Una caracterización de los grupos profinitos es dada por la siguiente Teorema.

Teorema B.1. *Sea G un grupo topológico. Entonces G es profinito si y solo si G es compacto y totalmente disconexo.*

Teorema B.2. *Sea G un grupo profinito y sea H un subgrupo de G. Entonces H es abierto si y solo si G/H es finito. Además, las siguientes tres propiedades son equivalentes.*

i) H es cerrado.

ii) H es profinito.

iii) H es la intersección de una familia de subgrupos abiertos.

Finalmente, si se satisfacen $(i) - (iii)$ entonces G/H es compacto y totalmente disconexo.

Un ejemplo de grupo profinito son los enteros p-ádicos $\mathbb{Z}_p$ los cuales construimos en el primer capítulo de esta tesis. Otro ejemplo de interés para nosotros, es el *anillo de Prüfer*. Consideremos los anillos $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$ los cuales forman un sistema proyectivo con respecto a las proyecciones $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, donde el orden parcial en $\mathbb{N}$ es dado por la divisibilidad $n|m$. Luego el límite proyectivo

$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z},$$

es conocido como el anillo de Prüfer o la *completación profinita de* $\mathbb{Z}$. Los grupos $n\hat{\mathbb{Z}}$, $n \in \mathbb{N}$, son los subgrupos abiertos de $\hat{\mathbb{Z}}$ y no es difícil verificar que

$$\hat{\mathbb{Z}}/n\hat{\mathbb{Z}} \cong \mathbb{Z}/\mathbb{Z}.$$

Para cada n consideremos su factorización en primos $n = \prod_p p^{\alpha_i}$, luego por el Teorema chino del residuo tenemos la siguiente descomposición

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_p \mathbb{Z}/p^{\alpha_i}\mathbb{Z},$$

luego, pasando al límite proyectivo tenemos que

$$\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p.$$

Además, podemos notar que hay inclusión natural de $\mathbb{Z}$ en $\hat{\mathbb{Z}}$ vía la inclusión diagonal

$$\begin{aligned} \mathbb{Z} &\longrightarrow \prod_p \mathbb{Z}_p \\ a &\longmapsto (a, a, \cdots). \end{aligned}$$

Apéndice C

Caracteres

En este apéndice revisaremos el concepto de caracter de un grupo abeliano localmente compacto. Las referencias básicas son [2] y [17].

Sea S^1 el grupo circular,

$$S^1 = \{z \in \mathbb{C} : |z| = 1\},$$

con la topología usual. Y sea G un grupo abeliano localmente compacto. Luego un caracter de G se define como un homomorfismo continuo

$$\chi : G \to S^1.$$

Es claro que los caracteres de G forman un grupo multiplicativo con la operación $\oplus$ (producto puntual) definido como $(\chi \oplus \eta)(a) = \chi(a)\eta(a)$, inducido por el producto de S^1, el cual denotaremos como $\mathrm{Char}(G)$.

Lema C.1. *Sea χ un caracter en un grupo compacto G y μ la medida de Haar, entonces*

$$\int_G \chi(x)d\mu = \begin{cases} \mu(G) & \text{si } \chi \text{ es trivial en } G, \\ 0 & \textit{en otro caso.} \end{cases}$$

Demostración. Escojamos algún $x_0 \in G$ tal que $\chi(x_0) \neq 1$ y escribamos xx_0 para x en la integral, luego

$$\int_G \chi(x)d\mu = \int_G \chi(xx_0)d\mu = \chi(x_0)\int_G \chi(x)d\mu.$$

□

Fijemos un caracter $\chi_0 \in \mathrm{Char}(G)$. Entonces una base de vecindades abiertas de χ_0 en $\mathrm{Char}(G)$ es dado por el conjunto de caracteres χ en $\mathrm{Char}(G)$ tal que

$$|\chi(g) - \chi_0(g)| < \epsilon \text{ para todo } g \in \mathcal{S},$$

donde $\epsilon > 0$ y $\mathcal{S}$ es un subconjunto compacto de G. Se puede probar que con esta topología $\mathrm{Char}(G)$ se convierte en un grupo topológico localmente compacto y que cada elemento de G induce un caracter en $\mathrm{Char}(G)$. Más aún, se tiene el siguiente resultado.

Teorema C.1 (Dualidad de Pontryagin)**.** *Dado G un grupo localmente compacto es cierto que*

i) $\mathrm{Char}(G)$ *es localmente compacto.*

ii) Es posible identificar el grupo de caracteres de $\mathrm{Char}(G)$ *con* G *i.e.*

$$\mathrm{Char}(\mathrm{Char}(G)) \cong G.$$

iii) Si G *es compacto entonces* $\mathrm{Char}(G)$ *es discreto.*

iv) Si G *es discreto entonces* $\mathrm{Char}(G)$ *es compacto.*

v) Si H *es un subgrupo cerrado de* G *y* $H^{\#}$ *(el aniquilador de* H*), consta de los elementos de* $\mathrm{Char}(G)$ *que son triviales en* H*. Entonces* $H^{\#}$ *es cerrado en* $\mathrm{Char}(G)$ *y existe un isomorfismo canónico* $\mathrm{Char}(H) \cong \mathrm{Char}(G)/H^{\#}$ *y* $\mathrm{Char}(G/H) \cong H^{\#}$*.*

Corolario C.1. *Todo caracter en un subgrupo cerrado de* G *puede ser extendido a todo* G*.*

Demostración. Consideremos H un subgrupo cerrado de G. Por el Teorema $C.1v$, $H^{\#}$ es un grupo cerrado de $\mathrm{Char}(G)$. Si $\xi \in H^{\#}$, ξ define un caracter en G/H. Luego cada caracter define canónicamente, por composición con el mapeo $G \mapsto G/H$, un caracter en G. □

Ejemplo 6. Sea $(\mathbb{Z}, +)$ con la topología discreta. Luego, podemos definir de forma arbitraria a $\chi(1)$ y definir $\chi(n) = \chi(1)^n$, donde claramente χ es continuo. Entonces $\mathrm{Char}(\mathbb{Z}) = S^1$. Además, por el Teorema de dualidad de Pontryagin $\mathrm{Char}(S^1) = \mathbb{Z}$. De manera más general dado que $O_K \cong \mathbb{Z}^n$ tenemos que $\mathrm{Char}(O_K) \cong \mathbb{T}^n$ como grupos topológicos.

Sea G un grupo topológico localmente compacto, μ su medida de Haar asociada y $f : G \to \mathbb{C}$ una función medible, entonces definimos la L^2-norma como

$$\|f\|_2 = \left\{ \int_G |f|^2 \, d\mu \right\}^{1/2}.$$

Luego el conjunto de todas estas funciones f tales que $\|f\| < \infty$ es llamado comúnmente el espacio de funciones cuadrado integrables y es denotado por $L^2(G, \mathbb{C})$.

Teorema C.2. $L^2(G, \mathbb{C})$ *es un espacio de Hilbert con producto interior*

$$\langle f, g \rangle = \int_G f \bar{g} d\mu.$$

Demostración. Primero notemos que el integrando de la derecha está en $L^1(G, \mathbb{C})$, pues sabemos que si p y q son exponentes conjugados $1 \leq p \leq \infty$ y si $f \in$

$L^p(G,\mathbb{C})$ y $g \in L^q(G,\mathbb{C})$ entonces $fg \in L^1(G,\mathbb{C})$[1]. Luego, $\langle f,g\rangle$ está bien definido. Notemos que

$$\|f\| = \langle f,f\rangle = \left\{\int_G |f|^2\, d\mu\right\}^{1/2} = \|f\|_2 .$$

Además, como $L^p(G,\mathbb{C})$es completo[2], tenemos que $L^2(G,\mathbb{C})$ es un espacio de Hilbert. □

Este resultado es valido incluso si G es un espacio medible arbitrario y μ una medida positiva [16].

Corolario C.2. *Si G es compacto entonces* $\mathrm{Char}(G) \subset L^2(G,\mathbb{C})$.

Demostración. Sea $\chi \in \mathrm{Char}(G)$, luego

$$\int_G |\chi|\, d\mu = \int_G d\mu = \mathrm{Vol}(G) < \infty.$$

□

Una propiedad importante de los espacios $L^2(G,\mathbb{C})$ es la posibilidad de desarrollar análisis de Fourier sobre ellos.

Teorema C.3. *El conjunto de caracteres $\chi_q \in \mathrm{Char}(G)$ forman un sistema ortonormal completo en $L^2(G,\mathbb{C})$. Luego, para todo $f \in L^2(G,\mathbb{C})$ existe una serie de Fourier convergente de la forma*

$$f = \sum_{q\in \mathrm{Char}(G)} a_q \cdot \chi_q,$$

donde

$$a_n = \langle \chi_q, f\rangle = \int_G \chi_q(zw^{-1}) f(w) d\mu \in \mathbb{C}.$$

Demostración. Para una prueba ver [18]. □

Por ejemplo, tomemos el toro $\mathbb{T}^n$ donde

$$\mathbb{Z}^n \cong \mathrm{Char}(\mathbb{T}^n) = \{\exp(2\pi N\cdot x) : N \in \mathbb{Z}^n \text{ y } x \in \mathbb{R}^n\}.$$

El cual es un sistema ortonormal completo en $L^2(\mathbb{T}^n,\mathbb{C})$ luego los elementos de $f \in L^2(\mathbb{T}^n,\mathbb{C})$ son todos de la forma

$$f(x) = \sum_{N\in\mathbb{Z}^n} a_n \exp(2\pi i N\cdot x).$$

En particular si $n = 1$ el conjunto

$$\mathrm{Char}(\mathbb{T}^1) = \mathrm{Char}(S^1) = \{\exp(2\pi i N\cdot x) : N \in \mathbb{Z} \text{ y } x \in \mathbb{R}\} = \{\cos Nx, \mathrm{sen} Nx\},$$

de donde tenemos la teoría de Fourier clásica.

[1] Ver [16] Teorema 3.8 .
[2] Ver [16] Teorema 3.11

Apéndice D

Geometría Diferencial

En este apéndice, introduciremos la noción de derivada en un espacio de Hilbert, para posteriormente dar las nociones básicas del concepto de variedad de Hilbert. Para un estudio detallado de calculo y geometría diferencial en espacios de Hilbert ver [23], [24], [25].

D.1 Calculo en Espacios de Hilbert

Sean H y H' espacios de Hilbert separables, U, V conjuntos abiertos de H y H' respectivamente y consideremos el mapeo $f : U \to V$. Se dice que f es *diferenciable* en $u_0 \in U$ si existe $Df(u_0) \in L(H, H')$ tal que

$$f(u) - f(u_0) - Df(u_0) \cdot (u - u_0) = o(|u - u_0|),$$

donde o_r satisface

$$\lim_{r \to 0} \left\| \frac{o(r)}{r} \right\| = 0.$$

Diremos que f es *diferenciable de clase* C^1 si es diferenciable para toda $u \in U$ y el mapeo $u \mapsto Df(u)$ es continuo.

Sea $f : U \to V$ y supongamos que tenemos definido el mapeo $D^{r-1}f : U \to L(H, L(H, \cdots, L(H, H') \cdots))$ (H, $r-1$ veces). Si $D^{r-1}f$ es diferenciable de clase C^1, entonces podemos escribir $D(D^{r-1})f = D^r f$ y diremos que f es *diferenciable de clase* C^r. Luego, diremos que $f : U \to V$ es *diferenciable* si es diferenciable de clase C^r para toda r.

Sea $U \subset H$ un abierto. Para cada $u_0 \in U$ definimos el *espacio tangente* $T_{u_0}U$ *de* U *en* u_0 como el conjunto

$$T_{u_0}U = \{(u_0, X) : X \in H\}.$$

Dotado con la estructura de espacio vectorial que proviene del mapeo canónico

$$\rho : (u_0, X) \in T_{u_0}U \mapsto X \in H.$$

La colección de espacios tangentes $T_{u_0}U$, $u_0 \in U$, es denotado por TU. El isomorfismo canónico $TU \cong U \times H$ hace que podamos ver a TU como un abierto en $H \times H$. La proyección $p : U \times H \to U$ en el primer factor puede ser escrita también como

$$\tau \equiv \tau_U : TU \to U$$

$$(u_0, X) \mapsto u_0,$$

luego, a τ_U lo llamaremos el *haz tangente* de U, TU el *espacio tangente total* de U y τ la *proyección* del haz tangente.

D.2 Variedades de Hilbert

Una *variedad topológica* M, modelada en un espacio de Hilbert separable H es un espacio metrizable el cual es localmente homeomorfo a H, i.e. para cada punto de M existe una vecindad V la cual es homeomorfa a H.

Sea M una variedad topológica modelada en H. Un *atlas diferenciable* para M es una familia

$$(u_i, M_i)_{i \in I},$$

de cartas, con las siguientes propiedades

i) $(M_i)_{i \in I}$ es una cubierta abierta de M.

ii) Para cada $i \in I$, la pareja (u_i, U_i) implica un homeomorfismo

$$u_i : M_i \to U_i,$$

de M_i en un abierto $U_i \subset H$.

iii) Si tenemos $M_i \cap M_j = M_{ij}$ y $u_i(M_{ij}) = U_{ij}$, el *mapeo de cambio de coordenadas*

$$u_j \circ u_i^{-1} : U_{ij} \to U_{ji},$$

es un difeomorfismo, *i.e.* $u_j \circ u_i^{-1}$ tiene inversa diferenciable.

Diremos que dos atlas diferenciables $(u_i, M_i)_{i \in I}$, $(u_j, M_j)_{i \in J}$ para una variedad topológica M son *equivalentes* si su unión da un atlas diferenciable. Luego una *estructura diferenciable* es una clase de equivalencia de atlas diferenciables.

Definición 16. Una *variedad de Hilbert* es una variedad topológica equipada con una estructura diferenciable.

Corolario D.1. *Un espacio de Hilbert H es una variedad de Hilbert con el atlas (Id, H).*

Sea M una variedad de Hilbert. Sea (u, M') una carta que cubre el punto $p \in M$ y sea $u(M') = U \subset H$. Entonces $T_{u(p)}U$ es llamado un *representante del espacio tangente de M* en p, dado por la carta (u, M'). Los elementos de

$T_{u(p)}U$ son denotados por $(u(p), X_{u(p)})$ con $X_{u(p)} \in H$. A X_{u_p} lo llamaremos la parte *principal* del vector $(u(p), X_{u(p)})$. Sean (u, M') y (u', M'') dos cartas que cubren a $p \in M$. Y pongamos $u(M') = U$, $u'(M'') = U'$. Entonces el mapeo de cambio de coordenadas

$$u' \circ u^{-1} : u(M' \cap M'') \longrightarrow u'(M'' \cap M'),$$

determina el isomorfismo lineal

$$T_{u(p)}(u' \circ u^{-1}) : T_{u(p)}U \longrightarrow T_{u'(p)}U'.$$

Diremos que $(u(p), X_{u(p)})$ y $(u'(p), X_{u'(p)})$ representan el mismo vector tangente de M en p si el último es la imagen del primero bajo $T_{u(p)}(u' \circ u^{-1})$.

Un *vector tangente* de M en p es definido por la familia de representantes dado por las cartas que cubren a p. El *espacio tangente* T_pM es el conjunto de vectores tangentes a M en p. T_pM tiene estructura de espacio vectorial isomorfo a H dado por el mapeo representante

$$T_p u : T_pM \longrightarrow T_{u(p)}U,$$

el cual es un isomorfismo lineal. Se puede probar que la estructura de espacio vectorial de T_pM es independiente del mapeo representante elegido.

Dada una variedad de Hilbert M. Por TM denotaremos a la colección de espacios tangentes T_pM, $p \in M$. Definimos

$$\tau \equiv \tau_M : TM \longrightarrow M,$$

asociando a cada vector $X \in T_pM$ su *punto base* $p \in M$. τ_M es llamado *proyección*.

El *haz tangente de una variedad de Hilbert* M es el mapeo

$$\tau : TM \to M.$$

A TM, considerado como una variedad de Hilbert, lo llamaremos el *espacio tangente total* de M.

Sea $f : M \to N$ diferenciable. Diremos que f es una *inmersión en* $p \in M$ si T_pf es inyectivo y cerrado. Luego, diremos que f es una *inmersión* si T_pf es una inmersión para todo $p \in M$.

Diremos que f es una *submersión* en p si T_pf es suprayectivo, luego si T_pf es suprayectivo para todo $p \in M$, entonces llamaremos a f *submersión*.

$f : M \to N$ es llamando un *encaje* si este es una inmersión y si $f : M \to f(M)$ es un homeomorfismo, donde $f(M) \subset N$ está equipado con la topología inducida. Si un subconjunto M de una variedad de Hilbert N puede ser equipada con una estructura de variedad de Hilbert tal que la inclusión $i : M \to N$ es un encaje, entonces M es una *sub-variedad* de N.

Apéndice E

Teoría Agebraica de Números

El material aquí presentado es clásico en teoría algebraica de números (para un estudio más detallado ver [9] o [7]).

E.1 Campos Numéricos

Un número complejo α es llamado *número algebraico* si es algebraico sobre $\mathbb{Q}$, *i.e.*, si satisface un polinomio con coeficientes en $\mathbb{Q}$. Se puede probar que el conjunto de los números algebraicos es un subcampo de $\mathbb{C}$ el cual denotaremos por $\mathcal{A}$. Un subcampo $K \subset \mathbb{C}$ es un *campo numérico* si cumple que $[K : \mathbb{Q}]$ es finito, luego dado que todos los elementos de K son números algebraicos, $K \subset \mathcal{A}$.

Si K es un campo numérico entonces $K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ para un número finito de números algebraicos $\alpha_1, \cdots, \alpha_n$. Más aún se puede demostrar que $K = \mathbb{Q}(\theta)$ para algún número algebraico θ.

Si $K = \mathbb{Q}(\theta)$ un campo numérico, en general, pueden existir varios monomorfismos de $\tau : K \to \mathbb{C}$. Por ejemplo, si $K = \mathbb{Q}(i)$ tenemos dos posibilidades,

$$\tau_1 : K \to \mathbb{C}, \quad x + iy \mapsto x + iy,$$

y

$$\tau_2 : K \to \mathbb{C}, \quad x + iy \mapsto x - iy,$$

para $x, y \in \mathbb{Q}$. De manera más general tenemos el siguiente Teorema.

Teorema E.1. *Sea $K = \mathbb{Q}(\theta)$ un campo numérico de grado n sobre $\mathbb{Q}$. Entonces, existen exactamente n monomorfismos distintos $\tau_i : K \to \mathbb{C}$, $i = 1, \ldots, n$. Además, los elementos $\tau_i(\theta) = \theta_i$ son las raíces distintas del polinomio mínimo de θ sobre $\mathbb{Q}$.*

Demostración. Sea $\theta_1, \ldots, \theta_n$ el conjunto de raíces del polinomio mínimo p de θ [1]. Luego cada θ_i tiene un polinomio mínimo p_i el cual divide a p, pero p es irreducible, luego existe un único isomorfismo de campos $\tau_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ tal que $\tau(\theta) = \theta_i$. De hecho, si $\alpha \in \mathbb{Q}(\theta)$ entonces $\alpha = r(\theta)$ para un único $r \in \mathbb{Q}[x]$ con $\text{grad}(r) < n$ luego tenemos que

$$\tau_i(\alpha) = r(\theta_i).$$

Recíprocamente, si tenemos un monomorfismo $\tau : K \to \mathbb{C}$, entonces τ es la identidad en $\mathbb{Q}$ luego tenemos que

$$0 = \tau(p(\theta)) = p(\tau(\theta)),$$

de modo que $\tau(\theta)$ es una de las θ_i, luego τ es una de las τ_i. □

Sea $K = \mathbb{Q}(\theta)$ un campo numérico de grado n sobre $\mathbb{Q}$ y sea $\alpha = \{\alpha_1, \ldots, \alpha_n\}$ una base de K visto como $\mathbb{Q}$-espacio vectorial. Definimos el *discriminante* de α como

$$\Delta[\alpha_1, \ldots, \alpha_n] = \{\det[\tau_i(\alpha_j)]\}^2.$$

Ahora si escogemos otra base $\beta = \{\beta_1, \ldots, \beta_n\}$ entonces

$$\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i \quad (c_{ik} \in \mathbb{Q}),$$

para $k = 1, \ldots, n$ y $\det(c_{ik}) \neq 0$. Luego, de las propiedades del producto de determinantes y de las propiedades de τ_i tenemos que

$$\Delta[\beta_1, \ldots, \beta_n] = [\det(c_{ik})]^2 \Delta[\alpha_1, \ldots, \alpha_n].$$

Además, se puede demostrar que el discriminante de cualquier base para $K = \mathbb{Q}(\theta)$ es racional y distinto de cero.

Un número complejo θ es un *entero algebraico* si existe un polinomio mónico $p(t)$ con coeficientes enteros tal que $p(\theta) = 0$. Este conjunto forma un subanillo de los números algebraicos $\mathcal{A}$ y lo denotaremos por $\mathcal{B}$.

Para un campo numérico K escribiremos $O_K = K \cap \mathcal{B}$ y llamaremos a O_K el anillo de enteros de K. Notemos que K y $\mathcal{B}$ son subanillos de $\mathbb{C}$. Luego tenemos que O_K es subanillo de $\mathbb{C}$. Además, $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ y $\mathbb{Z} \subseteq \mathcal{B}$ luego $\mathbb{Z} \subseteq O_K$.

Proposición E.1. *Si $\alpha \in K$ entonces para algún $c \in \mathbb{Z}$ distinto de cero tenemos que $c\alpha \in O_K$.*

Corolario E.1. *Si K es un campo numérico entonces $K = \mathbb{Q}(\theta)$ para algún entero algebraico θ.*

[1] De álgebra sabemos que un polinomio irreducible sobre un subcampo K de $\mathbb{C}$ tiene todas sus raíces distintas [12]

Demostración. Sabemos que $K = \mathbb{Q}(\phi)$ para algún número algebraico ϕ. Luego, por la Proposición anterior, $\theta = c\phi$ es un entero algebraico para algún $0 \neq c \in \mathbb{Z}$. Luego $\mathbb{Q}(\theta) = \mathbb{Q}(\phi)$. □

Un criterio útil para ver cuando un número es entero algebraico en término de su polinomio mínimo es el siguiente.

Proposición E.2. *Un número algebraico α es entero algebraico si y solo si su polinomio mínimo sobre $\mathbb{Q}$ tiene todos sus coeficientes en $\mathbb{Z}$.*

Sea K un campo numérico de grado n sobre $\mathbb{Q}$, por el Corolario anterior tenemos que $K = \mathbb{Q}(\theta)$ donde θ es un entero algebraico, luego tenemos que el polinomio mínimo $p(\theta)$ tiene grado n y $\left\{1, \theta, \ldots, \theta^{n-1}\right\}$ es una base para K visto como $\mathbb{Q}$-espacio vectorial.

El anillo O_K de enteros de K es un grupo abeliano con la adición. Una $\mathbb{Z}$-base para $(O_K, +)$ es llamada una *base entera* para K (o para O_K). Luego $\{\alpha_1, \ldots, \alpha_s\}$ es una base entera si y solo si toda $\alpha_i \in O_K$ y cada elemento de O_K es expresado de manera única de la forma

$$a_1\alpha_1 + \cdots + a_s\alpha_s,$$

para $a_1, \ldots, a_s \in \mathbb{Z}$. Luego de la Proposición E.1 se sigue que toda base entera para K es una $\mathbb{Q}$-base. En particular $s = n$.

Teorema E.2. *Cada campo numérico K pose una base entera, y el grupo aditivo de O_K es un grupo abeliano libre de rango n igual al grado de K.*

Corolario E.2. *La pareja $O_K \subset K$ es isomorfa a la pareja $\mathbb{Z}^n \subset \mathbb{Q}^n$ como grupos abelianos.*

Sea L/K una extensión finita, *la traza* y *la norma* de un elemento $x \in L$ se define como la traza y el determinante, respectivamente, del endomorfismo

$$T_x : L \longrightarrow L$$

$$a \longmapsto xa,$$

del K-espacio vectorial L, *i.e.*

$$\mathrm{Tr}_{L|K}(x) = \mathrm{Tr}(T_x), \quad N_{L|K}(x) = \mathrm{Det}(T_x).$$

Sea $K \subset L \subset M$ una torre de extensiones de campos finitas. Entonces

$$\mathrm{Tr}_{L|K} \circ \mathrm{Tr}_{M|L} = \mathrm{Tr}_{M|K}$$

y

$$N_{L|K} \circ N_{M|L} = N_{M|K}$$

En particular si K es un campo numérico tenemos que

$$\mathrm{Tr}_K(x) = \prod_{i=1}^{n} \tau_i(x), \quad N_K(x) = \sum_{i=1}^{n} \tau_i(x),$$

con $x \in K$ y τ_i los n monomorfismos de $K \to \mathbb{C}$.

E.2 Latices

Sea V un $\mathbb{R}$-espacio vectorial de dimensión n. Una *latiz* en V es un subgrupo de la forma

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

donde los vectores $v_1, \cdots, v_m$ son linealmente independientes. A la m-tupla $\{v_1, \cdots, v_m\}$ la llamaremos una *base* para la latiz Γ y al conjunto

$$M = \{x_1v_1 + \cdots + x_mv_m : x_i \in \mathbb{R},\ 0 \leq x_i < 1\},$$

lo llamaremos un *dominio fundamental* para Γ. Se dice que la latiz Γ es *completa* si $m = n$.

Como podemos observar Γ es un subgrupo del grupo aditivo $(\mathbb{R}, +)$. Luego, una latiz de dimensión m es un grupo abeliano libre de rango m por lo que podemos aplicar toda la teoría y terminología de grupos libres abelianos al estudio de las latices.

Por otro lado, también es posible dar una caracterización topológica de las latices. Sea $V = \mathbb{R}^n$ equipado con la métrica usual, donde $\|x - y\|$ denota la distancia entre x y y, y denotemos la bola cerrada de radio r y centro x por $B_r[x]$. Recordemos que un subconjunto $X \subseteq \mathbb{R}^n$ es *acotado* si $X \subseteq B_r[0]$ para alguna r. Diremos que un subconjunto de $\mathbb{R}^n$ es *discreto* si y solo si interseca a cada $B_r[0]$ en un conjunto finito. Luego tenemos la siguiente caracterización topológica de las latices.

Teorema E.3. *Un subgrupo $\Gamma \subset V$ es una latiz si y solo si Γ es discreto.*

Proposición E.3. *Una latiz Γ es completa si y solo si existe un subconjunto acotado $M \subset V$ tal que el conjunto de traslaciones $M + \gamma$, donde $\gamma \in \Gamma$, cubre a todo V.*

Teorema E.4. *El anillo de enteros O_K de un campo numérico K de grado n sobre $\mathbb{Q}$ es una latiz completa en V. Más aún, todo ideal $\mathfrak{a} \in O_K$, distinto de 0, es una latiz completa en V.*

Bibliografía

[1] T.M. Gendron and A. Verjovsky *Geometric Galois Theory, Nonlinear Number Fields and a Galois Group Interpretation of the Idele Class Group* (World Scientific, 2005)

[2] D. Ramakrishnan and R. J. Valenza, *Fourier Analysis on Number Fields* (Springer-Verlag, 1999)

[3] J.P. Serre, *A course in arithmetic* (Springer-Verlag, 1973)

[4] N. Bourbaki, *Topologie Générale* (Hermann, Editeurs des Sciences et des Paris, 1974)

[5] A. Weil, *Basic Number Theory* (Springer-Verlag, 1973)

[6] J. W. S. Cassels y A. Frolich (eds.),*Algebraic Number Theory* (Academic Press, 1986)

[7] P. Samuel,*Théorie Algébraique des Nombres* (Herman, Editeurs des Sciences et des Paris, 1966)

[8] A.M. Robert,*A Course in p-adic Analysis* (Springer, 2000)

[9] I. Stewart, *Algebraic Number Theory* (chapman and Hall, 1987)

[10] S. Lang, *Algebraic Number Theory* (Springer-Verlag, 1994)

[11] J. Neukirch, *Algebraic Number theory* (Springer-Verlag, 1999)

[12] S. Lang, *Algebra* (Springer-Verlag, 2002)

[13] P. R. Halmos, *Measure Theory* (Springer-Verlag, 1974)

[14] C. Prieto, *Topología Básica* (Fondo de Cultura Economica, 2003)

[15] T. M. Apostol, *Introduction to Analytic Number Theory* (Springer-Verlag, 1976)

[16] W. Rudin, *Real and Complex Analysis* (McGraw-Hill, 1991)

[17] H.P.F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory* (Cambridge University Press, 2001)

[18] Y. Katznelson, *An Introduction to Harmonic Analysis* (Cambridge University Press, 2004)

[19] S. de Neymet, *Introducción a los grupos topológicos de transformaciones* (SMM 2005)

[20] G. Fubini, *Sulle metriche definite da una forma Hermitiana* (att; Ist. Veneto 6, pp 501-513, 1904)

[21] E. Study, *Kürzeste Wegeimkomplexen Gebiet,* (math. Ann 60, pp 312-377 1905)

[22] E. Wigner, *Gruppentheorie und ihre anwendung auf die Quantenmechanik der Atomspektren* (J.W. Edwards, 1944)

[23] J. Dieudonné *Foundations of Modern Analysis* (Academic Press, 1969)

[24] S. Lang, *Foundamentals of Diferential Geometry* (Springer-Verlag, 1999)

[25] W.P.A. Klingenberg *Riemannian Geometry* (Walter de Gruyter, 1995)

[26] S.G. Krantz *Function Theory of Several Complex Variables* (AMS, 2001)

[27] R. Remmert, *Theory of Complex Functions* (Springer-Verlag, 1990)

[28] G.D. Villa, *Introducción a la Teoría de las Funciones Algebraicas* (Fondo de Cultura Economica, 1990)

[29] C. Godbillon, *Feuilletages. Études géométriques* (Birkhäuser, 1991)

[30] A. Candel y L. Conlon, *Foliations I* (AMS, 2000)