Series de Poincaré Multivariable de singularidades de curvas algebraicas y análisis p-ádico

TESIS MASTER

Anibal Fernando Álvarez Pérez

Escuela de Matemáticas

Facultad de Ciencias

Universidad Nacional de Colombia sede Medellín

2014

Documento maquetado con TeXiS v.1.0.

Este documento está preparado para ser imprimido a doble cara.

Series de Poincaré Multivariable de singularidades de curvas algebraicas y análisis p-ádico

Memoria que se presenta para optar al título de Master en Matemáticas

Dirigida por el Doctor John Jader Mira Albanes

Escuela de Matemáticas

Facultad de Ciencias

Universidad Nacional de Colombia sede Medellín

2014

A mi madre Isabel

y mi hermana Elizabeth

Agradecimientos

A todos los que la presente vieren y entendieren.

Inicio de las Leyes Orgánicas. Juan Carlos I

A mi familia y en especial a mi hermana Elizabeth, por todo su apoyo incondicional, tanto en los momento buenos como en los momentos difíciles.

Expreso mis senceros agradecimentos a mi asesor, Jhon Jader Mira, por sus valiosos consejos, por sus grandes contribuciones a mi formación académica, por su dedicación, paciencia y valentia en afrontar un tema inexplorado como el estudiado en este trabajo. Finalmente le agradezco por ser un amigo y por aportar inmensamente en mi crecimiento como ser humano.

A todos mis compañeros en la Universidad Nacional de Colombia sede Medellín, a quienes tengo el placer de conocer y con quienes he compartido buenos momentos. En especial, a mis grandes amigos: Sebastián Vélez y Juan Sebastián Díaz por sus valiosos comentarios y gran apoyo en la ejecución de este trabajo.

A todos los profesores de la Universidad Nacional de Colombia sede Medellín quienes contribuyeron tanto a mi formación académica como a mi formación profesional. En particular, agradezco a los profesores: Débora Tejada, Sigifredo Herrón, John Bayron Baena y Fernando Puerta. Además, al profesor Karl Otto Stöhr del IMPA por sus comentarios acerca del tema.

A los funcionarios de la Universidad Nacional de Colombia sede Medellín que con su amabilidad hacen más agradable nuestros estudios en la escuela de matemáticas.

Finalmente, agradezco a muchas otras personas que no cito, más con quienes me siento inmensamente agradecido, su amistad a contribuido verdaderamente a culminar este trabajo.

Índice

Introducción

Wars come and go, my soldiers, stay eternal.

Tupac Amaru Shakur

A finales del siglo diecinueve Kurl Hensel (1861-1941) descubrió los números p-ádicos. A pesar de haber pasado más de cien años de su nacimiento, estos números aun hoy siguen envueltos en un aura de misterio dentro de la comunidad científica. Una de las grandes motivaciones para estudiar dicho sistema numérico es su intrincada topología, en donde por ejemplo, las bolas son conjuntos abiertos y cerrados y cualquier punto en ella puede ser su centro. Su riqueza algebraica también hace de los números p-ádicos campo atractivo, por ejemplo la completación algebraica de los números p-ádicos es una extensión algebraica de grado infinito, haciendo que no sea localmente compacto. Parte de este trabajo trata de desenvolver sus propiedades analíticas, topológicas y algebraicas. Las conexiones entre las extensiones algebraicas de los números p-ádicos y los campos finitos de característica prima p, hacen pensar que definiciones y resultados de la geometría algebraica sobre campos finitos pueden tener análogos en los campos p-ádicos.

Es así como en este trabajo estudiamos las series de Poincaré Multivariable $P(\mathfrak{a}, \mathfrak{b}, \mathfrak{t})$ asociada a un anillo local $\mathcal{O}$, de una curva algebraica singular X definida sobre un campo finito $\mathbb{F}_q$. Dicha serie se puede expresar como una integral usando la medida de Haar $\widehat{\mu}$ sobre el anillo de fracciones de la completacion de $\widetilde{\mathcal{O}}$, donde $\widetilde{\mathcal{O}}$ es la clausura entera de $\mathcal{O}$, ya que dicho anillo de fracciones resulta ser localmente compacto

En esta tesis mostramos que dado un anillo local $\mathcal{O}$ de una curva algebraica singular X

definida sobre el campo de los números p-ádicos, el anillo de fracciones de la completacion de la clausura de $\mathcal{O}$ es un grupo topológico, el cual, no es un espacio topológico localmente compacto, lo cual imposibilita obtener una medida de Haar en él, usando las tecnicas desarrolladas en el Apéndice. Así la definición de la serie de Poincaré multivariable para singularidades sobre $\mathbb{Q}_p$ no es posible apartir de una representación integral como en el caso de campos finitos.

La organización de esta tesis es la siguiente.

En el Capítulo 1, se empieza definiendo los número p-ádicos como la completación de $\mathbb{Q}$ con respecto a la norma p-ádica $\| \, \|_p$. Mostramos algunas de sus rarezas topológicas y analíticas siguiendo los libros [9] y [7]. Como uno de los resultados interesantes, probamos que una serie converge, si y sólo si, sus términos n-ésimos convergen a cero. Además, vemos que $\mathbb{Q}_p$ es un espacio topológico localmente compacto, lo que nos permite tener una medida de Haar en $\mathbb{Q}_p$. Luego terminamos con el Lema de Hensel, el cual es un método útil a la hora de mostrar la existencia de raíces de polinomios sobre $\mathbb{Q}_p$. Después de esto, la tarea será construir una análogo p-ádico de los números complejos, es decir; una extensión algebraica de $\mathbb{Q}_p$, la cual sea completa con respecto a la norma inducida por la norma en $\mathbb{Q}_p$ y algebraicamente cerrada. Esto nos lleva a estudiar como extender la norma p-ádicas a extensiones finitas $K|\mathbb{Q}_p$. Un primer intento para hallar dicho campo, es pensar en la clausura algebraica de $\mathbb{Q}_p$, denotada por $\mathbb{Q}_p^{alg}$, pero este campo no es completo. El paso siguiente es considerar la completación de $\mathbb{Q}_p^{alg}$, de suerte que obtenemos nuestro campo completo y algebraicamente cerrado, denotado por $\mathbb{C}_p$. Para finalizar el estudio de los números p-ádicos mostramos que $\widehat{\mathbb{Q}_p}$ y $\mathbb{C}_p$ no son localmente compactos, lo que muestra la complejidad del estudio del análisis p-ádicos, seguimos para esto a [16].

En el Capítulo 2, estudiamos las series de Poincaré multivariable de singularidades de curvas sobre un campo finito, tales series fueron definidad por Karl Otto Stöhr. Damos una definición puramente algebraica de lo que entenderemos por curva algebraica, exploramos algunas propiedades de las series de Poincaré y por último expresamos dicha serie como una integral.

Finalmente, en el Capítulo 3, vemos que no es posible la definir las series de Poincaré sobre $\mathbb{Q}_p$ usando una representación integral siguiendo el caso de $\mathbb{F}_p$ y damos algunas concluciones.

En el Apéndice estudiamos la medida de Haar, la cual muestra que la integración abstracta y la integración sobre espacios localmente compactos es equivalente. En otras palabras, la medida de Haar resuelve la pregunta:

¿Cuales son las condiciones necesarias para poder tener una teoria de la medida tan generales como la ideada Henri Léon Lebesgue (1875-1941)?

Para esto estudiamos algunas nociones topológicas siguiendo [8]. Luego mostramos la existencia y unicidad de esta medida de Haar en grupos topológicos localmente compactos [14]. La prueba de la existencia sigue las ideas de André Weil [24] y la prueba de la unicidad está basada en un computo inteligente debido independientemente a Weil y a Von Neumann [15].

Capítulo 1

Números p-ádicos

Resumen: En este capítulo construiremos los números p-ádicos, exploraremos algunas de sus propiedades análiticas, topológicas y algebraicas. Además, construiremos el análogo p-ádico de los números complejos.

1.1. Construcción

Consideremos $p \in \mathbb{Z}$ un número primo fijo. Entonces para cada $a \in \mathbb{Z}$, no nulo, por el teorema fundamental de la aritmetica $a = p^n q$, donde $p \nmid q$, definimos $ord_p(a) = n$, así esta es una valuación discreta sobre $\mathbb{Q}$, donde para cada $\frac{a}{b} \in \mathbb{Q}$,

$$ord_p\left(\frac{a}{b}\right) = ord_p(a) - ord_p(b), \quad \text{y} \quad ord_p(0) = \infty.$$

De la definición se sigue que, para todo $x, y \in \mathbb{Q}$

1. $ord_p(-x) = ord_p(x)$
2. $ord_p(xy) = ord_p(x) + ord_p(y)$
3. $ord_p(x + y) \geq \text{mín}\{ord_p(x), ord_p(y)\}$.

Ahora, definimos la **norma p-ádica** como: para cada $x \in \mathbb{Q}$,

$$\|x\|_p = \begin{cases} p^{-ord_p(x)} & si \quad x \neq 0 \\ 0 & si \quad x = 0 \end{cases}$$

Veamos que $\| \cdot \|_p$ es una norma:

1. $\|x\|_p = 0$ sí, y solo si, $x = 0$. Es claro de la definición.
2. $\|xy\| = \|x\|\|y\|$, se sigue de $ord_p(xy) = ord_p(x) + ord_p(y)$
3. $\|x+y\| \leq \text{máx}\{\|x\|, \|y\|\} \leq \|x\|+\|y\|$, se sigue de $ord_p(x+y) \geq \text{mín}\{ord_p(x), ord_p(y)\}$.

Mostremos un lema muy útil:

Lema 1.1.1. *Sea $a_1, \ldots, a_n \in \mathbb{Q}$, entonces:*

(a) $ord_p(a_1 + \cdots + a_n) \geq \text{mín}\{ord_p(a_1), \ldots, ord_p(a_n)\}$

(b) Si $\text{mín}\{ord_p(a_1), \ldots, ord_p(a_n)\}$ *es alcanzado sólo una vez, entonces,*

$$ord_p(a_1 + \cdots + a_n) = \text{mín}\{ord_p(a_1), \ldots, ord_p(a_n)\}.$$

(c) Si $a_1 + \cdots + a_n = 0$, entonces $\text{mín}\{ord_p(a_1), \ldots, ord_p(a_n)\}$ *es alcanzado por lo menos dos veces.*

Demostración. (a) se sigue por inducción de $ord_p(x + y) \geq \text{mín}\{ord_p(x), ord_p(y)\}$.

Veamos (b). Supongamos que $ord_p(a_1) < ord_p(a_i)$, para $i = 2, 3, \ldots, n$. Supongamos por el absurdo que $ord_p(a_1 + \cdots + a_n) > ord_p(a_1)$. Entonces

$$\begin{aligned} ord_p(a_1) &= ord_p(a_1 + a_2 + \cdots + a_n - a_2 - \cdots - a_n) \\ &\geq \text{mín}\{ord_p(a_1 + a_2 + \cdots + a_n), ord_p(a_2), \ldots, ord_p(a_n)\} \\ &> ord_p(a_1). \end{aligned}$$

Es decir, $ord_p(a_1) > ord_p(a_1)$, lo cual es una contradicción.

Veamos (c). Supongamos por el contrario que el mínimo se obtiene una única vez, digamos, $ord_p(a_1) < ord_p(a_i)$, para $i = 2, 3, \ldots, n$, entonces,

$$\begin{aligned} ord_p(a_1) &= ord_p(-a_2 - \cdots - a_n) \\ &\geq \text{mín}\{ord_p(a_2), \ldots, ord_p(a_n)\} \\ &> ord_p(a_1). \end{aligned}$$

lo cual constituye un absurdo. □

Corolario 1.1.2. *Sea $a_1, \ldots, a_n \in \mathbb{Q}$. Entonces:*

(a) $\|a_1 + \cdots + a_n\|_p \leq \text{máx}\{\|a_1\|_p, \ldots, \|a_n\|_p\}$

(b) Si $\text{máx}\{\|a_1\|_p, \ldots, \|a_n\|_p\}$ *es alcanzado solo una vez, entonces,*

$$\|a_1 + \cdots + a_n\|_p = \text{máx}\{\|a_1\|_p, \ldots, \|a_n\|_p\}$$

(c) Si $a_1 + \cdots + a_n = 0$, entonces $\text{máx}\{\|a_1\|_p, \ldots, \|a_n\|_p\}$ *es alcanzado por lo menos dos veces.*

Demostración. Es inmediata del Lema anterior. □

Se definen los **los racionales p-ádicos**, *denotados por $\mathbb{Q}_p$ como la completación topológica de $\mathbb{Q}$ con respecto a la norma $\|\cdot\|_p$ y definimos los enteros p-ádicos como*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \,/\, \|x\|_p \leq 1\}.$$

1.2. Propiedades Topológicas

Extendemos la norma p-ádica en $\mathbb{Q}$ a $\mathbb{Q}_p$ de la siguiente manera: definimos la norma $\|\cdot\|_p$ de cada clase de equivalencia a como $\|a\|_p = \text{lím}_{n\to\infty} \|a_n\|_p$, donde $\{a_n\}$ es cualquier representante de a. Tal límite no depende del representante y siempre converge, pues

1. Si $a = 0$, entonces por definición $\lim_{n\to\infty} \|a_n\|_p = 0$.

2. Si $a \neq 0$, entonces para algún $\epsilon > 0$ y para todo $N \in \mathbb{N}$ existe $m_N > N$, tal que $\|a_{m_N}\|_p > \epsilon$. Tomado N suficientemente grande, tendremos que, para todo $n, m > N$, $\|a_n - a_m\|_p < \epsilon$, de donde:

$$\|a_n - a_{m_N}\|_p < \epsilon, \quad \text{para todo} \quad n > N.$$

Dado que $\|a_{m_N}\|_p > \epsilon$, se sigue que $\|a_n\|_p = \max\{\|a_n - a_{m_N}\|_p, \|a_{m_N}\|_p\} = \|a_{m_N}\|_p$, Corolario 1.1.2. Luego, para todo $n > N$, $\|a_n\|_p$ tiene el valor constante $\|a_{m_N}\|_p$.

Una importante diferencia entre la completación de $(\mathbb{Q}, |\cdot|)$ con respecto a $|\cdot|$ su valor absoluto usual, $(\mathbb{R}, |\cdot|_\infty)$, es que la norma extendida $|\cdot|_\infty$ toma muchos más valores que los tomados por $|\cdot|$ en $\mathbb{Q}$. Pero al pasar de $\mathbb{Q}$ a $\mathbb{Q}_p$ la norma extendida sigue tomando los mismo valores que la norma sobre $\mathbb{Q}$, a saber, $\{p^n\}_{n\in\mathbb{Z}} \cup \{0\}$.

Dadas dos clases de equivalencia a y b de sucesiones de Cauchy en $\mathbb{Q}_p$, tomamos representantes $\{a_n\} \in a$ y $\{b_n\} \in b$, definimos:

- $a + b = \lim_{n\to\infty}(a_n + b_n)$
- $a \cdot b = \lim_{n\to\infty}(a_n b_n)$

Para definir la multiplicación por inversos debemos de tener un poco de cuidado pues es posible que aparezcan terminos nulos en la sucesion de Cauchy. Sin embargo, si $a \in \mathbb{Q}_p$ entonces a tiene un representante sin ceros.

Así $\mathbb{Q}_p$ es un campo, el cual, es completo con respecto a la norma $\|\cdot\|_p$, es decir, cualquier sucesión de Cauchy converge a un punto en $\mathbb{Q}_p$.

En lo siguiente probaremos un teorema que hará más simple la comprensión de $\mathbb{Q}_p$.

Lema 1.2.1. *Si $x \in \mathbb{Q}$ y $\|x\|_p \leq 1$, entonces para todo n existe un entero $y \in \mathbb{Z}$ tal que $\|y - x\|_p \leq p^{-n}$. El entero y puede ser escogido del conjunto* $\{0, 1, 2, \ldots, p^n - 1\}$

Demostración. Sea $x = \dfrac{a}{b}$, donde a y b son primos relativos, es decir, a y b no tienen factores primos comunes. Dado que $\|x\|_p \leq 1$, se sigue que p no divide a b, de donde,

b y p^n son también primos relativos. Luego existen $l, m \in \mathbb{Z}$ tales que $lb + mp^n = 1$, multiplicando esta ecuaciones por $\frac{a}{b}$, tenemos que, $al - \frac{a}{b} = -\frac{a}{b}mp^n$, de donde, definiendo $y = al$, tenemos que:

$$\begin{aligned} \|y - x\|_p &= \left\|\frac{a}{b}\right\|_p \|m\|_p \|p^n\|_p \\ &\leq p^{-n} \end{aligned}$$

Además, $y = qp^n + r$, donde $0 \leq r < p^n$ y $q \in \mathbb{Z}$, así;

$$\begin{aligned} \|r - x\|_p &= \|y - x + (-qp^n)\|_p \\ &\leq \max\{\|y - x\|_p, \|qp^n\|_p\} \\ &\leq p^{-n}. \end{aligned}$$

Lo cual completa la prueba. □

Teorema 1.2.2. *Cada clase de equivalencia $a \in \mathbb{Q}_p$, con $\|a\|_p \leq 1$ tiene exactamente un representante de la forma $\{a_n\}$ para el cual:*

1. $0 \leq a_n < p^n$ *para cada* $n = 1, 2, \ldots$
2. $a_n = a_{n+1} \mod p^n$ *para cada* $n = 1, 2, \ldots$

Demostración. Veamos primero la unicidad. Sea $\{a'_n\}$ otra sucesión que representa a a y satisface *1* y *2*. Además, supongamos que $a_{n_0} \neq a'_{n_0}$. Dado que, tanto a_{n_0} como a'_{n_0} están entre 0 y p^{n_0}, se sigue que $a_{n_0} \neq a'_{n_0} \mod p^{n_0}$. De donde, para todo $n \geq n_0$, tenemos

$$a_n \mod p^{n_0} = a_{n_0} \neq a'_{n_0} = a'_n \mod p^{n_0}$$

es decir; $a_n \neq a'_n \mod p^{n_0}$. Luego

$$\|a_n - a'_n\|_p > p^{-n_0}$$

para todo $n \geq n_0$, de donde $\{a_n\}$ y $\{a'_n\}$ no son sucesiones de Cauchy equivalentes, lo cual es un absurdo.

Veamos ahora la existencia. Sea $\{b_i\}$ una sucesión de Cauchy que representa a a. Para cada $m = 1, 2, \ldots$. sea N_m tal que $\|b_n - b_{n'}\|_p \leq p^{-N_m}$ para todo $n, n' > N_m$, Además, tomamos la sucesión de los $N_{m'}$s estrictamente creciente y $N_m \geq m$. Así, para todo $n, n' > N_1$ tenemos que

$$\begin{aligned}\|b_n\|_p &\leq \text{máx}\{\|b_{n'}\|_p, \|b_n - b_{n'}\|_p\} \\ &\leq \text{máx}\{\|b_{n'}\|_p, p^{-1}\}\end{aligned}$$

y dado que $\|b_{n'}\|_p \longrightarrow \|a\|_p \leq 1$, cuando $n' \to \infty$, se cumple, $\|b_n\|_p \leq 1$, para todo $n \geq N_1$. Por el lema anterior, para cada b_{N_n} existe un $0 \leq a_n < p^{-n}$, tal que

$$\|a_n - b_{N_n}\|_p \leq p^{-n}.$$

Veamos que $\{a_n\}$ es la sucesión pedida.

(i) $a_n = a_{n+1} \mod p^n$, pues

$$\begin{aligned}\|a_{n+1} - a_n\|_p &= \|a_{n+1} - b_{N_{n+1}} + b_{N_{n+1}} - b_{N_n} - (a_n - b_{N_n})\|_p \\ &\leq \text{máx}\{\|a_{n+1} - b_{N_{n+1}}\|_p, \|b_{N_{n+1}} - b_{N_n}\|_p, \|a_n - b_{N_n}\|_p\} \\ &\leq \text{máx}\{p^{-n-1}, p^{-n}, p^{-n}\} \\ &= p^{-n}.\end{aligned}$$

(ii) $\{a_n\} \sim \{b_n\}$, pues, dado cualquier m, para $n \geq N_m$ tenemos

$$\begin{aligned}\|a_n - b_n\|_p &= \|a_n - a_m + a_m - b_{N_n} - (b_n - b_{N_n})\|_p \\ &\leq \text{máx}\{\|a_n - a_m\|_p, \|a_m - b_{N_n}\|_p, \|b_n - b_{N_n}\|_p\} \\ &\leq \text{máx}\{p^{-n}, p^{-n}, p^{-n}\} \\ &= p^{-n}.\end{aligned}$$

De ahí que $\|a_n - b_n\|_p \to 0$ cuando $n \to \infty$.

Lo cual prueba el teorema. □

Ahora bien, si $a \in \mathbb{Q}_p$ y $\|a\|_p > 1$, entonces $\dfrac{a}{\|a\|_p} = ap^{ord_p(a)}$ tiene norma p-ádica menor o igual a 1, y por el teorema anterior, existe un representante $\{a'_n\}$ con las condiciones *1.* y *2.* para $ap^{ord_p(a)}$, así, a tiene como representante a $\{a_n\}$ donde $a_n = a'_n p^{-ord_p(a)}$. Escribiendo todos los a'_n en la sucesión representante de $ap^{ord_p(a)}$ en base p, la condición *2*, se traduce como, si

$$a'_n = b_0 + b_1 p + \cdots + b_{n-1} p^{n-1},$$

donde los $b_{i's}$ son números en $\{0, 1, \ldots, p-1\}$, entonces

$$a'_{n+1} = b_0 + b_1 p + \cdots + b_{n-1} p^{n-1} + b_n p^n,$$

donde los dígitos b_0 hasta b_{n-1} son los mismo que para a'_n. De lo anterior, se sigue que

$$\frac{a}{\|a\|_p} = b_0 + b_1 p + \cdots + b_{n-1} p^{n-1} + b_n p^n + \cdots$$

Por tanto, obtenemos una forma de escribir todo $a \in \mathbb{Q}_p$, llamada "la expansión p-ádica de a"

$$a = b_0 p^{-n} + b_1 p^{-n+1} + \cdots + b_{n-1} p^{-1} + b_n + b_{n+1} p + b_{n+2} p^2 + \cdots \qquad (\dagger)$$

donde $n = ord_p(a)$.

Por otro lado, sean $\{b_m\}_{m=-n}^{\infty}$ una sucesión de entero p-ádicos, $\|b_m\|_p \leq 1$. Consiredemos la suma parcial

$$S_N = b_{-n} p^{-n} + b_{-n+1} p^{-n+1} + \cdots + b_0 + b_1 p^1 + b_2 p^2 + \cdots + b_N p^N.$$

La sucesión de sumas parciales es claramente Cauchy, pues si $M > N$, entonces,

$$\begin{aligned} \|S_M - S_N\|_p &= \|b_{N+1} p^{N+1} + \cdots + b_M p^M\|_p \\ &\leq \text{máx}\{\|b_{N+1} p^{N+1}\|_p, \ldots, \|b_M p^M\|_p\} \\ &\leq \text{máx}\{\|p^{N+1}\|_p, \ldots, \|p^M\|_p\} \\ &< \frac{1}{p^N}. \end{aligned}$$

De donde converge a un elemento de $\mathbb{Q}_p$, definimos el límite de $\{S_N\}$ como $\sum_{m=-n}^{\infty} b_m p^m$. Similarmente, si $\{c_m\}$ es una sucesión cualquiera de elementos en $\mathbb{Q}_p$, tales que $\|c_m\|_p \to 0$

cuando $m \to \infty$, entonces la sucesión de sumas parciales $S_N = \sum_{m=1}^{N} c_m$ es una sucesión convergente, ya que

$$\|S_M - S_N\|_p \leq \text{máx}\{\|c_{N+1}\|_p, \ldots, \|c_M\|_p\} \to 0, \quad \text{cuando} \;\; N \to \infty.$$

Obtenemos entonces la siguiente proposición.

Proposición 1.2.3. *Una serie $\sum c_m$ en $\mathbb{Q}_p$ converge sí, y solo si, la sucesión de términos c_m convergen a 0.*

Retornando de nuevo a la expansión p-ádica, nosotros vemos que la serie a la derecha de la definición (†) converge a a, y así, la igualdad puede ser tomada en el sentido de convergencia de series.

Importante: La unicidad en el Teorema 1.2.2 es algo que no se tiene en el caso de los números reales, denotados por $\mathbb{R}$. A saber, existen varias representaciones decimales para un mismo número, por ejemplo: $1{,}000\cdots = 0{,}999\cdots$. Pero si dos expansiones p-ádicas convergen al mismo número en $\mathbb{Q}_p$, entonces ellas son iguales, es decir, todos sus dígitos son los mismos.

Recordemos que $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \ / \ \|a\|_p \leq 1\}$, este es el conjunto de números en $\mathbb{Q}_p$ cuya expansión p-ádica no contiene potencias negativas de p, los cuales llamamos **"enteros p-ádicos"**. La suma y producto de elementos en $\mathbb{Z}_p$ de elementos en $\mathbb{Z}_p$ es de nuevo un elemento en $\mathbb{Z}_p$, de donde, $\mathbb{Z}_p$ es una subanillo del campo $\mathbb{Q}_p$. Definimos el conjunto de unidades de $\mathbb{Z}_p$ como $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \,/\, \frac{1}{x} \in \mathbb{Z}_p\}$ lo cual es equivalente a $\{x \in \mathbb{Z}_p/\|x\|_p = 1\}$. Sea $p\mathbb{Z}_p := \mathbb{Z}_p - \mathbb{Z}_p^*$, es decir, $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p \ / \ \|x\|_p < 1\}$. Entonces $p\mathbb{Z}_p$ es el único ideal maximal de $\mathbb{Z}_p$, ya que si $a \in \mathbb{Z}_p$ y $b \in p\mathbb{Z}_p$, $\|ab\|_p = \|a\|_p\|b\|_p < 1$ y si $x, y \in \mathbb{Z}_p$, entonces,

$$\|x + y\|_p \leq \text{máx}\{\|x\|_p, \|y\|_p\} < 1.$$

La maximalidad es dada ya que el complemento de $p\mathbb{Z}_p$ son las unidades de $\mathbb{Z}_p$. Además, el Lema 1.2.1 dice que $\mathbb{Z}$ es denso en $\mathbb{Z}_p$.

Sean $a, b \in \mathbb{Q}_p$, escribimos $a = b \mod p^n$ si $\|a - b\|_p \leq p^{-n}$, lo que equivale a decir que, $(a - b)p^{-n} \in \mathbb{Z}_p$, i.e., el primer digito no nulo en la expansión p-ádica de $a - b$ no ocurre antes del lugar p^n-ésimo. Si a y b están en $\mathbb{Z}$, entonces la noción de igualdad $a = b$ mód p^n coincide con la de igualdad modular en $\mathbb{Z}$, es decir; $a = b \mod c$ sí, y solo si, c divide a $a - b$. En esta forma podemos expresar $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ / \ x \neq 0 \mod p\}$. De lo anterior concluimos

Corolario 1.2.4. $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$, *esto es, dado* $x \in \mathbb{Q}_p$, *existe* $n \geq 0$ *tal que* $p^n x \in \mathbb{Z}_p$. *La multiplicación por p es un homeomorfismo de* $\mathbb{Q}_p \longrightarrow \mathbb{Q}_p$. *Los conjuntos de* $p^n\mathbb{Z}_p$ *con* $n \in \mathbb{Z}$ *forman un sistema de vecindades de* $0 \in \mathbb{Q}_p$, *que cubren a* $\mathbb{Q}_p$.

Corolario 1.2.5. *Para cualquier* $n \geq 1$ *la secuencia*

$$0 \longrightarrow p^n\mathbb{Z}_p \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

es una secuencia exacta con morfismos continuos, donde la topología en $\mathbb{Z}/p^n\mathbb{Z}$ *es la topología discreta. En particular,*

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

Demostración. Definamos claramente los morfismos. El primer morfismo $i : p^n\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$, es tal que $i(a) = a$, es inyectivo y continuo. Una forma explicita para el segundo morfismo puede darse usando la expansión p-ádica. Para todo $a \in \mathbb{Z}_p$

$$a = b_0 + b_1 p + \cdots + b_{n-1}p^{n-1} + b_n p^n + \cdots$$

donde los $b_{i'}s$ son números en $\{0, 1, \ldots, p-1\}$, definimos $\pi : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ como

$$\pi(a) = b_0 + b_1 p + \cdots + b_{n-1}p^{n-1} + b_n p^n.$$

La unicidad de la serie anterior hace que π este bien definida y la sobreyectividad es clara. Además, para todo $t \in \mathbb{Z}/p^n\mathbb{Z}$, $\pi^{-1}(t) = t + p^n\mathbb{Z}_p$, de donde, en particular

$$\ker(\pi) = \pi^{-1}(0) = p^n\mathbb{Z}_p.$$

□

Corolario 1.2.6. $\mathbb{Z}_p$ *es secuencialmente compacto, es decir, toda sucesión en* $\mathbb{Z}_p$ *posee una subsucesión convergente.*

Demostración. Sea $\{a_n\}_{n=0}^{\infty}$ una sucesión de enteros p-ádicos, es decir, $\|a_n\|_p \leq 1$ para todo $n \in \mathbb{N}$, así, la expansión p-ádica de cada a_n es de la forma

$$\begin{aligned} a_1 = &\quad a_{10} + a_{11}p + a_{12}p^2 + \cdots \\ a_2 = &\quad a_{20} + a_{21}p + a_{22}p^2 + \cdots \\ \vdots \\ a_n = &\quad a_{n0} + a_{n1}p + a_{n2}p^2 + \cdots \end{aligned}$$

Dado que los $a_{n0'}s \in \{0, 1, \ldots, p-1\}$, deben haber infinitos $a_{n'}s$ cuyo primer dígito son iguales, es decir, existe un subconjunto $S_1 \subseteq \{a_n\}$ cuyo primer dígito es igual. Sea $n_1 = \text{mín}\{n /\ a_n \in S_1\}$. Similarmente, existe un subconjunto infinito $S_2 \subseteq S_1$ cuyo segundo dígito es igual, sea $n_2 = \text{mín}\{n/a_n \in S_1 - a_{n_1}\}$. De esta forma obtenemos $n_1 < n_2 < \cdots < n_k < \cdots$, y donde

$$a_{n_k} = a_{n_{k+1}} \quad \text{mód } p^k.$$

La subsucesión $\{a_{n_k}\}_{k=1}^{\infty}$ es una sucesión de Cauchy, ya que, si $m < l$, entonces,

$$\|a_{n_l} - a_{n_m}\|_p \leq p^{-m}.$$

Dado que $\mathbb{Q}_p$ es completo, existe $a \in \mathbb{Q}_p$ talque $\lim\limits_{k\to\infty} a_{n_k} = a$. Por tanto, existe $N \in \mathbb{N}$, tal que, para todo $k \geq N$, $\|a - a_{n_k}\|_p \leq 1$, de donde

$$\|a\|_p \leq \text{máx}\{\|a_{n_k}\|_p, \|a - a_{n_k}\|_p\} \leq 1$$

es decir; $a \in \mathbb{Z}_p$, lo cual concluye la prueba. □

Ahora definiremos los abiertos básicos de los números p-ádicos. En cualquier espacio métrico las bolas definidas por $B_r(a) = \{x\ /\ \|x - a\| < r\}$ forman una base para la topología, pero en nuestro caso los únicos posibles valores para la norma son $\{p^n\}_{n\in\mathbb{Z}} \cup \{0\}$. Así que definimos, para todo $r \in \mathbb{Z}$ y para todo $a \in \mathbb{Q}$

$$B_r(a) = \{x \in \mathbb{Q}_p\ /\ \|x - a\|_p \leq p^{-r}\}$$

como **la bola con centro en a y radio p^{-r}** y

$$S_r(a) = \{x \in \mathbb{Q}_p\ /\ \|x - a\|_p = p^{-r}\}$$

como **la esfera con centro en a y radio p^{-r}**.

Notemos que en la definición la escogencia de " $<$" o " $\leq$" no es relevante, pues

$$\{x \in \mathbb{Q}_p \ / \ \|x-a\|_p < p^{-r}\} = \{x \in \mathbb{Q}_p \ / \ \|x-a\|_p \leq p^{-r-1}\} = B_{r+1}(a) \subset B_r(a).$$

Proposición 1.2.7. *Sea $a, b \in \mathbb{Q}_p$ y $r, s \in \mathbb{Z}$, entonces:*

1. *Si $b \in B_r(a)$, entonces $B_r(b) = B_r(a)$.*
2. *$B_r(a) \cap B_s(b) \neq \emptyset$ sí, y solo si, $B_s(b) \subseteq B_r(a)$ o $B_s(b) \supseteq B_r(a)$.*
3. *$B_r(a)$ es abierto y cerrado en la topológia inducida por $\| \cdot \|_p$.*
4. *$S_r(a)$ es abierto y cerrado en la topológia inducida por $\| \cdot \|_p$.*

Demostración.

1. " $\subseteq$ " Sea $x \in B_r(b)$, es decir; $\|x-b\|_p \leq p^{-r}$. Por tanto,

   $$\|x-a\|_p \leq \text{máx}\{\|x-b\|_p, \|b-a\|_p\} \leq p^{-r}$$

   de donde, $x \in B_r(a)$

   " $\supseteq$ " Se sigue de la anterior, ya que $a \in B_r(b)$. Esto nos dice que cualquier punto en una bola puede ser su centro.

2. " $\Rightarrow$ " Supongamos que $B_r(a) \cap B_s(b) \neq \emptyset$. Entonces, existe $c \in B_r(a) \cap B_s(b)$, así $B_r(a) = B_r(c) \subseteq B_s(c) = B_s(b)$, si $r > s$. De igual forma, si $r < s$, entonces $B_r(a) \supseteq B_s(b)$.

   " $\Leftarrow$ " Es claro, pues $B_r(a) \cap B_s(b)$, es igual $B_r(a)$ ó $B_s(b)$ dependiendo del caso.

3. $B_r(a)$ es abierto ya que $B_r(a) = \{x \in \mathbb{Q}_p \ / \ \|x-a\|_p < p^{-r+1}\}$ el cual es abierto en cualquier espacio métrico. Ahora, para ver que $B_r(a)$ es cerrado, mostremos que $B_r(a) = \overline{B_r(a)}$ (donde para cualquier conjunto A, $\overline{A}$ es la clausura topológia, es decir; si C es un cerrado tal que $A \subseteq C$, entonces, $\overline{A} \subseteq C$). Sea $x \in \overline{B_r(a)}$, entonces para cualquier abierto U de $\mathbb{Q}_p$, con $x \in U$, se satisface que $B_r(a) \cap U \neq \emptyset$, en particular, tomando $s > r$, tenemos que $B_r(a) \cap B_s(a) \neq \emptyset$, de donde por *2.*, tenemos, $B_s(a) \subseteq B_r(a)$, de ahí que, $x \in B_r(a)$.

4. Esto es claro, ya que

$$S_r(a) = B_r(a) \cap (B_{r+1}(a))^c \quad [1]$$

$\square$

Observación: Es claro de la definición de bola y de esfera que:

$$B_r(a) = a + p^r\mathbb{Z}_p$$

$$S_r(a) = a + p^r\mathbb{Z}_p^*$$

Ahora veremos unos cuantos proposiciones las cuales son corolarios del Teorema 1.2.2.

Corolario 1.2.8. *$\mathbb{Z}_p$ es compacto y $\mathbb{Q}_p$ es localmente compacto.*

Demostración. De la Proposición 1.2.7 y la observación anterior, vemos que para todo $a \in \mathbb{Q}_p$, $a+\mathbb{Z}_p$ es una vecindad de a, así, basta probar que $\mathbb{Z}_p$ es compacto. En el Corolario 1.2.6 vimos que $\mathbb{Z}_p$ es secuencialmente compacto, y como $\mathbb{Q}_p$ es un espacio metrico, esto equivale a que $\mathbb{Z}_p$ es compacto (vea [13]). Otra forma de mostrar que $\mathbb{Z}_p$ es compacto, es darse cuenta que $\mathbb{Z}_p$ es completo y totalmente acotado. Por la Proposición 1.2.7, $\mathbb{Z}_p$ es completo, ya que es un subconjunto cerrado de un espacio completo $\mathbb{Q}_p$. Para mostrar que es totalmente acotado, debemos mostrar que, dado $\epsilon > 0$, existe un cubrimiento de $\mathbb{Z}_p$ por bolas de radio ϵ, observemos que por la limitación de los valores de nuestra norma p-ádica, basta tomar $\epsilon = p^{-n}$, para $n \geq 0$. Ahora, dado que

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

es un conjunto finito y la proyección π, en el Corolario 1.2.5 es continua, se sigue que $\mathbb{Z}_p$ es totalmente acotado. $\square$

Lema de Hensel

El siguiente teorema llamado Lema de Hensel da condiciones para que un polinomio con coeficientes en $\mathbb{Z}_p$ tenga raíces en $\mathbb{Z}_p$. Este teorema será esencial en la construcción de la completación algebraica de $\mathbb{Q}_p$.

[1] dado un conjunto A, A^c denota su complemento en el espacio ambiente.

Teorema 1.2.9. *Sea* $F(x) = c_0 + c_1x + \cdots + c_nx^n$ *un polinomio cuyos coeficientes están en* $\mathbb{Z}_p$*, es decir,* $\|c_i\|_p \leq 1$ *para todo* i *y definamos* $F'(x) = c_1 + 2c_2x + \cdots + nc_nx^{n-1}$ *como la derivada formal de* F*. Sea* $a_0 \in \mathbb{Z}_p$ *tal que*

$$F(a_0) = 0 \mod p \quad y \quad F'(a_0) \neq 0 \mod p.$$

Entonces existe un único $a \in \mathbb{Z}_p$ *tal que*

$$F(a) = 0 \quad y \quad a = a_0 \mod p.$$

Demostración. Para mostrar la existencia de a, construiremos una sucesión de Cauchy (sobre $\mathbb{Q}_p$), usando esencialmente el "método de Newton" para hallar raíces de polinomios.

Deseamos construir una sucesión $a_0, a_1, a_2, \ldots$, tal que

1. $F(a_n) = 0 \mod p^{n+1}$
2. $a_n = a_{n+1} \mod p^{n+1}$
3. $0 \leq a_n \leq p - 1$.

La prueba de la existencia de dichos $a_{n'}$s se hará por inducción. Observe que la condición 2. nos dice que la sucesión es en efecto una sucesión de Cauchy.

Paso Base: Por hipótesis tenemos la existencia de a_0 y sin perdida de generalidad podemos suponer que $a_0 \in \{0, 1, 2, \ldots, p-1\}$ de otra forma reemplazamos a_0 por a_0 $\mod p$. Esto último no afecta las hipótesis, pues si $a_0 = a_0' + q$ con $\|q\|_p \geq 1$, entonces

$$\begin{aligned} F(a_0') &= F(a_0 - q) \\ &= F(a_0) + F'(a_0)(-q) + \cdots \\ &= F(a_0) \mod p \\ &= 0 \mod p. \end{aligned}$$

Similarmente $F'(a_0') \neq 0 \mod p$. Ahora vamos a definir a_1, de tal forma que cumpla las propiedades deseadas. Para que a_1 cumpla 2. y 3. debe ser de la forma

$$a_1 = a_0 + b_1p, \quad \text{donde} \quad 0 \leq b_1 \leq p - 1.$$

Evaluando F en a_1 y expandiendo en serie formal de Taylor, tenemos:

$$\begin{aligned} F(a_1) &= F(a_0 + b_1 p) \\ &= F(a_0) + F'(a_0)(b_1 p) + \ (\textit{términos en} \quad p^n), \quad n \geq 2 \\ &= (F(a_0) + F'(a_0)(b_1 p)) \mod p^2. \end{aligned}$$

Dado que $F(a_0) = 0 \mod p$, podemos suponer que $F(a_0) = \alpha p \mod p^2$, para algún $\alpha \in \{0, 1, 2, \ldots, p-1\}$. Así, para obtener 3., es decir; $F(a_1) = 0 \mod p^2$ debemos tener:

$$\begin{aligned} (\alpha p + F'(a_0) b_1 p) &= 0 \mod p^2 \\ (\alpha + F'(a_0) b_1) &= 0 \mod p \end{aligned}$$

y dado que $F'(a_0) \neq 0 \mod p$, definimos

$$b_1 = -\frac{\alpha}{F'(a_0)} \mod p,$$

con lo cual también definimos a a_1.

Ahora procedemos por inducción, supongamos que ya definimos $a_1, a_2, \ldots, a_{n-1}$. Definamos a a_n, por 2. y 3., necesitamos que sea de la forma

$$a_n = a_{n-1} + b_n p^n, \quad \text{con} \quad b_n \in \{0, 1, \ldots, p-1\}.$$

Similarmente al paso base, evaluamos F en a_n y expandiendo en serie formal de Taylor, para obtener:

$$\begin{aligned} F(a_n) &= F(a_{n-1} + b_n p^n) \\ &= (F(a_{n-1}) + F'(a_{n-1})(b_n p^n)) \mod p^{n+1}. \end{aligned}$$

Dado que $F(a_{n-1}) = 0 \mod p^n$, por hipótesis inductiva, nosotros podemos suponer que $F(a_{n-1}) = \alpha' p \mod p^{n+1}$, para algún $\alpha' \in \{0, 1, 2, \ldots, p-1\}$. Así, $F(a_n) = 0 \mod p^{n+1}$ es:

$$\begin{aligned} (\alpha' p^n + F'(a_{n-1}) b_n p^n) &= 0 \mod p^{n+1} \\ (\alpha + F'(a_{n-1}) b_n) &= 0 \mod p. \end{aligned}$$

Además, $a_{n-1} = a_0 \mod p$, se sigue que $F'(a_{n-1}) = F'(a_0) \neq 0 \mod p$, y por tanto podemos definir

$$b_n = -\frac{\alpha'}{F'(a_{n-1})} \mod p,$$

Esto completa el paso inductivo.

Definimos $a = a_0 + a_1 p + a_2 p^2 + \cdots$ dado que para todo n, $F(a) = F(a_n) \mod p^{n+1} = 0 \mod p^{n+1}$, concluimos que $F(a) = 0$. La unicidad de a se sigue de la unicidad de la expansión p-ádica.

$\square$

1.3. Propiedades Algebraicas

Cuando completamos a $\mathbb{Q}$ con respecto a la norma valor absoluto obtenemos el campo de los número reales denotado por $\mathbb{R}$, el cual no resulta ser algebraicamente cerrado, ya que por ejemplo el polinomio $x^2 + a$ con $a > 0$ no tiene soluciones en $\mathbb{R}$. Así es como al tratar de hallar las raíces de este estilo de polinomios construimos el campo de los número complejos $\mathbb{C}$ formado por los números de la forma $a + bi$ donde $a, b \in \mathbb{R}$ y $i^2 = -1$, el cual satisface:

(1) $\mathbb{C}$ es algebraicamente cerrado, es decir; todo polinomio con coeficientes complejos tiene solución en $\mathbb{C}$.

(2) $\mathbb{C}$ es completo con respecto a la única norma la cual extiende a la norma $\| \ \|_\infty$ en $\mathbb{R}$, la cuál es dada por $\|a + bi\| = \sqrt{a^2 + b^2}$. Es decir, cualquier sucesión de Cauchy de números complejos tiene límite en $\mathbb{C}$.

El proceso finaliza en $\mathbb{C}$, ya que este resulta ser lo suficientemente agradable, es decir, es un campo algebraicamente cerrado y completo.

Este no es el caso con $(\mathbb{Q}, \| \cdot \|_p)$. Después de completar a $\mathbb{Q}$ respecto a la norma p-ádica $\| \ \|_p$, obtenemos a $\mathbb{Q}_p$, el cual es completo, pero no es algebraicamente cerrado, por ejemplo las ecuaciones $x^2 - 2 = 0$ o $x^2 + 1 = 0$ no tiene solución en $\mathbb{Q}_p$. Para obtener la clausura algebraica de $\mathbb{Q}_p$, debemos formar una secuencia infinita de extensiones de campo obtenidas al adjuntar soluciones de polinomios de grados cada vez más altos, lo cual es diferente con respecto a $\mathbb{C}$. Por desgracia, la clausura algebraica de $\mathbb{Q}_p$ no es un campo completo respecto a la norma inducida por la norma p-ádica en $\mathbb{Q}_p$. Así es como debemos completar dicha clausura algebraica para obtener al fin un campo el cual es algebraica cerrado y completo respecto a la norma que extiende a $\| \|_p$. Tal campo será denotado por $\mathbb{C}_p$, el cual es el analogo p-ádico de $\mathbb{C}$ y es el sistema numerico conveniente en el cual estudiar el cálculo y el análisis p-ádico, el cual es mucho menos comprendido que $\mathbb{C}$, por ejemplo, caracterizar los autoformismos de campo $\mathbb{Q}_p$-lineales de $\mathbb{C}_p$, aún sigue siendo una preguntar por resolver.

1.4. Construcción de $\mathbb{C}_p$

Antes de mostrar el campo $\mathbb{C}_p$, veremos las propiedades de la clausura algebraica de $\mathbb{Q}_p$, para lo cual necesitamos algunos resultados de campos finitos y teoría de extensiones de campos.

Campos Finitos

En adelante el campo de p elementos (de característica p) será denotado por $\mathbb{F}_p$, es decir;

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}.$$

Para las prueba de las siguientes afirmaciones damos como referencia [9] y [16].

Teorema 1.4.1. *Sea F un campo finito de q elementos tal que $\mathbb{F}_p \subseteq F$ y $f = [F : \mathbb{F}_p]$ i.e., la dimensión de F como un $\mathbb{F}_p$-espacio vectorial es f. Sea K la clausura algebraica de $\mathbb{F}_p$ tal que $F \subseteq K$. Entonces, $q = p^f$, F es el único campo de q elementos contenido en K y F es el conjunto de todos los elementos de K que satisfacen la ecuación $X^q - X = 0$.*

Inversamente, para cualquier potencia $q = p^f$, las raíces de la ecuación $X^q - X = 0$ en K son un campo de q elementos.

Observación 1.4.2. Dado que cualquier dos clausuras algebraicas de $\mathbb{F}_p$ son isomorfas, se sigue que cualquier dos campos de $q = p^f$ elementos son isomorfos. Denotaremos por $\mathbb{F}_q$ el único campo (salvo isomorfismos) de q elementos. Si F es un campo, $F^\times$, denota el grupo multiplicativo de los elementos diferentes del cero en F.

Definimos $\varphi(d) = \#\{l \;/\; l \text{ es primo relativo a } d,\ l \leq d\}$.

Lema 1.4.3. $\displaystyle\sum_{d\,|\,n} \varphi(d) = n.$

Proposición 1.4.4. $\mathbb{F}_q^\times$ *es un grupo cíclico de orden* $q-1$.

Por último en esta sección veamos una proposición que usaremos más tarde

Proposición 1.4.5. *Sea* $q = p^f$ *y sea* a *un elemento generador del grupo* $\mathbb{F}_p^\times$. *Sea* $P(X)$ *el polinomio minimal de* a *sobre* $\mathbb{F}_p$. *Entonces* $\deg(P) = f$.

Extensión de Normas

En esta sección estudiaremos la forma de extender la norma no arquimedeana $\|\ \|_p$ de $\mathbb{Q}_p$ a cualquier extensión de campos finita.

Sabemos que sobre un espacio métrico y en particular sobre cualquier espacio normado, la definición de compacidad y secuencialmente compacto son equivalentes ([13] Teorema 7.4), recordemos que decimos que un conjunto X es **secuencialmente compacto** si cada sucesión de elementos en X tiene una subsucesión convergente. En adelante podremos trabajar con esta equivalencia de compacidad.

Durante esta sección F denotará un campo con una norma no arquimedeana $\|\ \|$ el cual es localmente compacto. Es decir, para todo $x, y \in F$, $\|x+y\| \leq \text{máx}\{\|x\|, \|y\|\}$ y además para todo $x \in F$ existe un compacto $E \subseteq F$ tal que $x \in \text{int}(E) \subseteq E$.

Definición 1.4.6. Sea V un espacio vectorial sobre F de dimensión finita ($\dim_F V < \infty$), una **norma** sobre V es una función $\|\ \|_V : V \longrightarrow \mathbb{R}^{\geq 0}$ tal que para todo $x, y \in V$ y $\alpha \in F$

(1) $\|x\|_V = 0$ si y sólo si, $x = 0$

(2) $\|\alpha x\|_V = \|a\|\ \|x\|_V$

(3) $\|x+y\|_V \leq \|x\|_V + \|y\|_V$

Proposición 1.4.7. *Todo espacio vectorial normado $(V, \|\cdot\|_V)$ localmente compacto, es completo.*

Demostración. Supongamos que $\{a_n\}$ es una sucesión de Cauchy de elementos en V, entonces existe $M > 0$, tal que para todo $n \geq N$, $\|a_n\| \leq M$, es decir, $\{a_n\}_{n\geq N} \subseteq \overline{B}(0, M)$ el cual es compacto. Así, existe una subsucesión convergente, lo cual implica que $\{a_n\}$ converge. □

Teorema 1.4.8. *Si V es un espacio vectorial finito dimensional sobre un campo localmente compacto F, entonces todas las normas sobre V son equivalentes.*

Demostración. Por la proposición anterior F es completo, así que el resultado se sigue igual que en [10] Teorema 2.4-2. □

Sea L una extensión de campos de k decimos que una norma $\| \ \|_L$ en L **extiende la norma** $\| \ \|_k$ en k, si para todo $a \in k$, $\|a\|_L = \|a\|_k$).

Corolario 1.4.9. *Sea K una extensión de campos finita de F. Entonces existe a lo sumo una única norma $\| \ \|_K$ sobre K que extiende a la norma $\| \ \|$ sobre F.*

Demostración. Sean $\| \ \|_1$ y $\| \ \|_2$ normas sobre K que extienden a $\| \ \|$. Por el teorema anterior $\| \ \|_1$ y $\| \ \|_2$ son normas equivalentes, así, existen $c_1, c_2 \in \mathbb{R}$ con $c_1 > 0$ y $c_2 > 0$ tales que

$$c_1\|x\|_1 \leq \|x\|_2 \leq c_2\|x\|_1, \text{ para todo } x \in K.$$

Supongamos que existe $x \in K$ tal que $\|x\|_1 \neq \|x\|_2$, sin perdida de generalidad, digamos que $0 < \|x\|_1 < \|x\|_2$, entonces $1 < \dfrac{\|x\|_2}{\|x\|_1}$, de ahí que, para algún n lo suficientemente grande,

$$\left(\frac{\|x\|_2}{\|x\|_1}\right)^n > c_2$$

así, $\|x^n\|_2 > c_2\|x^n\|_1$, lo cual es un absurdo. □

Esto aún deja la pregunta: ¿Dada una extensión finita de campos $K|F$, existe alguna norma sobre K que extienda la norma en F?

Es momento entonces de recordar un concepto básico en extensiones de campos, la “norma” de un elemento. Este uso de la palabra norma no debe ser confundido con el uso hasta aquí en el sentido métrico. La **“Norma”** en el nuevo sentido siempre será denotado por $\mathbf{N}$.

Sea $F(\alpha)|F$ una extensión simple de un campo F generado por un elemento α algebraico sobre F, es decir, α satisface un polinomio mónico irreducible sobre F llamado **el polinomio minimal** de α sobre F.

$$P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \text{ con } a_i \in F.$$

Definición 1.4.10. sea K una extensión finita del campo F. Las siguientes tres definiciones de la “**norma** de α desde K a F” denotada por $\mathbf{N}_{K|F}(\alpha)$, son equivalentes:

(1) Si $K = \langle x_1, x_2, \ldots, x_n \rangle_F$ como un espacio vectorial sobre F n-dimensional, entonces la multiplicación por α, es una transformación lineal de K en K con matriz asociada A_α. Definimos:
$\mathbf{N}_{K|F}(\alpha) = \det(A_\alpha)$.

(2) $\mathbf{N}_{K|F}(\alpha) = (-1)^n a_0$ donde a_0 es el coeficiente constante del polinomio minimal de α.

(3) $\mathbf{N}_{K|F}(\alpha) = \prod_{i=1}^{n} \alpha_i$ donde los α_i son los conjugados de $\alpha = \alpha_1$ sobre F. Es decir, α_i son las raíces sobre alguna clausura algebraica de F del polinomio minimal de α.

Veamos que en efecto tales definiciones son equivalentes:

(2) $\Leftrightarrow$ **(3)** Se sigue claramente del hecho que

$$P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 = \prod_{i}^{n}(X - \alpha_i)$$

pues, así $P(0) = a_0 = \prod_{i=1}^{n}(-\alpha_i)$.

(1) $\Leftrightarrow$ **(2)** Si usamos como base para K el conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Entonces, la matriz asociada a la transformación lineal multiplicación por α, es claramente (usando $\alpha^n = -a_{n-1}X^{n-1} - \ldots - a_1X - a_0$)

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & & -a_0 \\ 1 & 0 & 0 & & & -a_1 \\ 0 & 1 & 0 & & & -a_2 \\ & & & \ddots & & \vdots \\ & & & & 0 & -a_{n-2} \\ & & & & 1 & -a_{n-1} \end{pmatrix}$$

la cual, tiene determinante $(-1)^n a_0$, al calcular dicho determinante expandiendo usando la primera fila.

Si $\beta \in K = F(\alpha)$, podemos definir $\mathbf{N}_{K|F}(\beta)$ como en **(1)** el determinante de la matriz multiplicación por β o, equivalentemente como

$$(\mathbf{N}_{F(\beta)|F}(\alpha))^{[K:F(\beta)]}.$$

Ambas definiciones son equivalentes ya que si escogemos una base $\{\lambda_1, \ldots, \lambda_l\}$ para $F(\beta)$ como espacio vectorial sobre F y una base $\{\gamma_1, \ldots, \gamma_m\}$ para K como espacio vectorial sobre $F(\beta)$, entonces, una base para K como F espacio vectorial es

$$\{\lambda_i\gamma_j \ / \ i = 1, \ldots, l, \ j = 1, \ldots, m\}.$$

Usando esta base para K sobre F, vemos que si la matriz de multiplicación por β en $F(\beta)$ es A_β, entonces la matriz de multiplicación por β, pero ahora en K, tiene la forma:

$$\begin{pmatrix} A_\beta & 0 & & \\ 0 & A_\beta & & \\ & & \ddots & \\ & & & A_\beta \end{pmatrix}$$

el determinante de la matriz anterior es precisamente $(\det(A_\beta))^{[K:F(\beta)]}$, es decir;

$$\mathbf{N}_{K|F}(\beta) = \left(\mathbf{N}_{F(\beta)|F}(\beta)\right)^{[K:F(\beta)]}.$$

Dado que $\mathbf{N}_{K|F}(\alpha)$ es definido para cualquier $\alpha \in K$ como el determinante de la matriz de multiplicación por α en K, se sigue que $\mathbf{N}_{K|F}$ es una función multiplicativa desde K en F, es decir; para todo $\alpha, \beta \in K$

$$\mathbf{N}_{K|F}(\alpha\beta) = \mathbf{N}_{K|F}(\alpha)\mathbf{N}_{K|F}(\beta) \tag{$\dagger$}$$

Podemos ahora imaginar como extender la norma $\| \ \|_p$ a cualquier α algebraico sobre $\mathbb{Q}_p$. Supongamos que $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = n$, es decir; el polinomio minimal de α sobre $\mathbb{Q}_p$ tiene grado n. Si K es cualquier extensión finita de Galois de $\mathbb{Q}_p$ que contiene a α, por ejemplo K puede ser el campo de descomposición de α, obtenido al adjuntar α y todos sus conjugados a $\mathbb{Q}_p$. Supongamos que encontramos una norma $\| \ \|$ la cual extiende a $\| \ \|_p$ a K. Por el Corolario 1.4.9 la norma $\| \ \|$ es la única norma en el campo K extendiendo a $\| \ \|_p$. Ahora, sea α' cualquier conjugado de α, y sea σ el automorfismo de K que envia α en α'. Claramente, $\| \ \|' : K \longrightarrow \mathbb{R}^{\geq 0}$ definida por $\|x\|' = \|\sigma(x)\|$ es una norma en el campo K la cual extiende a $\| \ \|_p$, de ahí que, $\| \ \|' = \| \ \|$ y así,

$$\|\alpha\| = \|\alpha\|' = \|\sigma(x)\| = \|\alpha'\|.$$

Concluimos que la norma de α es igual a la norma de sus conjugados. Por tanto, se sigue que

$$\begin{aligned}
\|\mathbf{N}_{\mathbb{Q}_p(\alpha)|\mathbb{Q}_p}(\alpha)\|_p &= \left\|\mathbf{N}_{\mathbb{Q}_p(\alpha)|\mathbb{Q}_p}(\alpha)\right\| \\
&= \left\|\prod \alpha'\right\| \quad \alpha' \text{ conjugado de } \alpha \\
&= \prod \|\alpha'\| \\
&= \|\alpha\|^n.
\end{aligned}$$

Luego tenemos que

$$\|\alpha\| = \sqrt[n]{\left\|\mathbf{N}_{\mathbb{Q}_p(\alpha)|\mathbb{Q}_p}(\alpha)\right\|_p} \tag{1.4.1}$$

Por tanto, para hallar la norma p-ádica de α, debemos mirar el polinomio minimal de α sobre $\mathbb{Q}_p$, si este tiene grado n y término constante a_0, entonces la norma p-ádica de α será $\sqrt[n]{\|a_0\|_p}$.
Notemos que la ecuación anterior es equivalente a

$$\|\alpha\| = \left(\|\mathbf{N}_{K|\mathbb{Q}_p}(\alpha)\|_p\right)^{1/[K:\mathbb{Q}_p]} \tag{1.4.2}$$

En esta forma las raíces se mantienen fijas, donde K es cualquier campo que contiene a α, esto ocurre ya que

$$\|\mathbf{N}_{K|\mathbb{Q}_p}(\alpha)\|_p = \left(\mathbf{N}_{\mathbb{Q}_p(\alpha)|\mathbb{Q}_p}(\alpha)\right)^{[K:\mathbb{Q}_p]}$$

y

$$[K:\mathbb{Q}_p] = [K:\mathbb{Q}_p(\alpha)][\mathbb{Q}_p(\alpha):\mathbb{Q}_p] = [K:\mathbb{Q}_p(\alpha)]\cdot n.$$

Lo siguiente será probar que en realidad sí tenemos una norma con las propiedades requeridas. Para ello veamos un par de lemas.

Sea γ un elemento algebraico sobre $\mathbb{Q}_p$, para cualquier $\alpha = \sum_{i=0}^{n-1} a_i\gamma^i \in \mathbb{Q}_p(\gamma)$, denotaremos por $\|\alpha\|_{\sup}$ la norma del supremos en esta base, esto significa;

$$\|\alpha\|_{\sup} := \max\{\|a_i\|_p \;/\; i = 0,1,\ldots,n-1\}.$$

Similarmente, si $A = (a_{ij})_{n\times n}$ es una matriz con entradas en $\mathbb{Q}_p$

$$\|A\|_{\sup} := \max\{\|a_{ij}\|_p \;/\; i,j = 0,1,\ldots,n-1\}.$$

Lema 1.4.11. *Sea $\|\ \|$ sobre K definida como arriba (Ecuaciones 1.4.1). Para todo $\gamma\in K$ tal que $\|\gamma\|\leq 1$ se tiene que $\|1+\gamma\|\leq 1$*

Demostración. Notemos que podemos definir $\|\gamma\|$ y $\|1+\gamma\|$ usando el campo $\mathbb{Q}_p(\gamma) = \mathbb{Q}_p(1+\gamma)$ en lugar de K. Es decir,

$$\begin{aligned}\|\gamma\| &= \left(\mathbf{N}_{\mathbb{Q}_p(\gamma)|\mathbb{Q}_p}(\gamma)\right)^{1/[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]}\\ \|1+\gamma\| &= \left(\mathbf{N}_{\mathbb{Q}_p(\gamma)|\mathbb{Q}_p}(1+\gamma)\right)^{1/[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]}.\end{aligned}$$

Sin perdida de generalidad podemos suponer que $K = \mathbb{Q}_p(\gamma)$, así que $\{1, \gamma, \gamma^2, \dots, \gamma^{n-1}\}$ es una base para K como un espacio vectorial sobre $\mathbb{Q}_p$, donde $n = [\mathbb{Q}_p(\gamma) : \mathbb{Q}_p]$.

Sea A_γ la matriz correspondiente a la transformación $\mathbb{Q}_p$-lineal multiplicación por γ. En esta forma, la matriz A_γ^i es la matriz correspondiente a la transformación $\mathbb{Q}_p$-lineal multiplicación por γ^i y la matriz $I + A_\gamma$ es la matriz correspondiente a la transformación $\mathbb{Q}_p$-lineal multiplicación por $1 + \gamma^i$ (en general, la matriz $P(A)$ corresponde a la multiplicación por $P(\gamma)$ para cualquier polinomio $P(X) \in \mathbb{Q}_p[X]$).

Afirmación: La sucesión de números reales $\{\|A_\gamma^i\|_{\text{sup}}\}_k$ es acotada.
Supongamos lo contrario, entonces podemos encontrar una subsucesión $\{\|A_\gamma^{i_k}\|_{sup}\}_k$, tal que

$$\|A_\gamma^{i_k}\|_{sup} > k.$$

Sea $b_k = \|A_\gamma^{i_k}\|_{sup}$, el cual es el máximo de las normas p-ádicas de las n^2 entradas de $A_\gamma^{i_k}$ y sea β_k una entrada de $A_\gamma^{i_k}$ con $\| \|_p$ máximo, es decir;

$$\|\beta_k\|_p = \|A_\gamma^{i_k}\|_{sup} = b_k.$$

Definimos

$$B_k = \frac{1}{\beta_k} A_\gamma^{i_k}, \text{ entonces } \|B_k\|_{\text{sup}} = 1.$$

Dado que en la norma del supremo la esfera unitaria es compacta, podemos encontrar una subsucesión $\{B_{k_j}\}_j$, la cual converge a alguna matriz B.Como
$\det(B_k) = \dfrac{1}{\beta_k^n} \det(A_\gamma^{i_k})$, tenemos que

$$\begin{aligned}
\|\det(B_k)\|_p &< \frac{\|\det((A_\gamma^{i_k})\|_p}{k^n} \\
&\leq \frac{\left\| \left(\mathbf{N}_{\mathbb{Q}_p(\gamma)|\mathbb{Q}_p}(\gamma)\right)^{i_k} \right\|_p}{k^n} \\
&\leq \frac{\|\gamma\|^{n\, i_k}}{k^n} \\
&< \frac{1}{k^n}
\end{aligned}$$

Por la definición de convergencia en la norma del supremo, cada entrada de B es el límite cuando $j \to \infty$ de la correspondiente entrada de B_{k_j} y de ahí que

$$\det(B) = \lim_{j\to\infty} \det(B_{k_j}) = 0.$$

Por tanto, $\det(B) = 0$, de donde existe un elemento $X \in K$, considerado como un vector escrito con respecto a la base $\{1, \gamma, \gamma^2, \dots, \gamma^{n-1}\}$, tal que $BX = 0$. El conjunto $\{\gamma^i X\}_{i=0}^{n-1}$ es una base para el $\mathbb{Q}_p$-espacio vectorial K. Mostraremos que para todo $i = 0, \dots, n-1$ se tiene que $B\gamma^i X = 0$, lo cual implica que $B = 0$. En efecto la matriz multiplicación por γ^i viene dada por la matriz A_γ^i, tenemos que

$$\begin{aligned} B\gamma^i X &= BA_\gamma^i X \\ &= A_\gamma^i BX \\ &= 0 \end{aligned}$$

donde la conmutatividad $BA_\gamma^i = A_\gamma^i B$ es dada por el hecho de que B es el límite de las matrices $B_k = \dfrac{1}{\beta_k} A_\gamma^{i_k}$.
Concluimos que $B = 0$, pero esto contradice el hecho que $\|B\|_{sup} = 1$.

Así, hemos probado que existe una constante $C > 0$ tal que para todo i

$$\|A_\gamma^i\|_{\sup} \leq C.$$

Notemos que al expandir el $\det(A_\gamma)$ y usar las propiedades de la norma no arquimedeana (ver 1.1.2), tenemos

$$\|\det(A_\gamma)\|_p \leq (\max \|a_{ij}\|_p)^n = (\|A_\gamma\|_{\sup})^n.$$

Sea N lo suficientemente grande y consideremos

$$(I + A_\gamma)^N = I + \binom{N}{1} A + \cdots + \binom{N}{N-1} A^{N-1} + A^N.$$

Tenemos que

$$\begin{aligned}
\|1+\gamma\|^N &= \|\det(I+A)^N\|_p^{1/n} \\
&\leq \|(I+A)^N\|_{\sup} \\
&\leq \max_{0\leq i\leq N} \left\| \binom{N}{i} A^i \right\|_{\sup} \\
&\leq \max_{0\leq i\leq N} \|A^i\|_{\sup} \quad \text{ya que} \quad \left\| \binom{N}{i} a_{ij} \right\|_p = \|a_{ij}\|_p \\
&\leq C
\end{aligned}$$

Por tanto, $\|1+\gamma\| \leq \sqrt[N]{C}$, tomando $N \to \infty$ tenemos el resultado requerido

$$\|1+\gamma\| \leq 1.$$

□

Teorema 1.4.12. *Sea K una extensión finita de $\mathbb{Q}_p$. Entonces existe una norma sobre K la cual extiende la norma $\| \ \|_p$ en $\mathbb{Q}_p$.*

Demostración. Sea $n = [K : \mathbb{Q}_p]$. Definimos para todo $\alpha \in K$, $\|\alpha\|$ como:

$$\|\alpha\| = \left(\|\mathbf{N}_{K|\mathbb{Q}_p}(\alpha)\|_p\right)^{1/n}$$

Veamos que en efecto $\| \ \|$ es una norma que extiende a $\| \ \|_p$:

(i) $\|\alpha\| = 0$, si y sólo si, $\alpha = 0$.
$\|\alpha\| = 0$, es equivalente a decir que, $\|\mathbf{N}_{K|\mathbb{Q}_p}(\alpha)\|_p = 0$ y ya que $\| \ \|_p$ es una norma, esto ocurre sii $\mathbf{N}_{K|\mathbb{Q}_p}(\alpha) = 0$, es decir; el polinomio minimal de α es $m_\alpha(X) = X-0$, de ahí que, $\alpha = 0$.

(ii) Sean $\alpha, \beta \in K$, entonces

$$\begin{aligned}
\|\alpha\beta\| &= \left(\|\mathbf{N}_{K|\mathbb{Q}_p}(\alpha\beta)\|_p\right)^{1/n} \\
&= \left(\|\mathbf{N}_{K|\mathbb{Q}_p}(\alpha)\ \mathbf{N}_{K|\mathbb{Q}_p}(\beta)\|_p\right)^{1/n} \\
&= \left(\|\mathbf{N}_{K|\mathbb{Q}_p}(\alpha)\|_p\right)^{1/n}\left(\|\mathbf{N}_{K|\mathbb{Q}_p}(\beta)\|_p\right)^{1/n} \\
&= \|\alpha\|\ \|\beta\|.
\end{aligned}$$

(iii) $\|\alpha + \beta\| \leq \text{máx}\{\|\alpha\|, \|\beta\|\}$.

Supongamos sin perdida de generalidad que $\|\alpha\| \leq \|\beta\|$, usando el lema anterior con $\gamma = \dfrac{\alpha}{\beta}$, tenemos $\|\gamma\| \leq 1$, de donde $\|1 + \dfrac{\alpha}{\beta}\| = \|1 + \gamma\| \leq 1$, es decir

$$\|\alpha + \beta\| \leq \|\beta\|.$$

(iv) Ahora, sea $\alpha \in \mathbb{Q}_p$ entonces el polinomio minimal de α, es $m_\alpha(X) = X - \alpha$, así que

$$\mathbf{N}_{K|\mathbb{Q}_p}(\alpha) = \left(\mathbf{N}_{\mathbb{Q}_p(\alpha)|\mathbb{Q}_p}(\alpha)\right)^{[K:\mathbb{Q}_p(\alpha)]} = (-1)^n\alpha^n,$$

de donde $\|\alpha\| = (\|(-1)^n\alpha^n\|_p)^{1/n} = \|\alpha\|_p$.

□

Observación: Sea K una extensión finita de $\mathbb{Q}_p$. A la única norma $\| \ \|$ sobre K, la cual extiende la norma p-ádica sobre $\mathbb{Q}_p$, la seguiremos denotando por $\| \ \|_p$.

Proposición 1.4.13. *Sea K una extensión finita de $\mathbb{Q}_p$ de grado n, y sean*

$$A = \{x \in K \ / \ \|x\|_p \leq 1\}$$

$$M = \{x \in K \ / \ \|x\|_p < 1\}.$$

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

Demostración. Que A es un anillo y M es un ideal es consecuencia de las propiedades de la norma no arquimedeana $\| \ \|_p$.

Veamos que A es la clausura entera de $\mathbb{Z}_p$ en K. Sea $\alpha \in K$ un elemento entero sobre $\mathbb{Z}_p$, es decir; existen $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_p$ tal que

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0 = 0.$$

De la igualdad anterior se tiene que

$$\begin{aligned}
\|\alpha\|_p^m &= \|\alpha^m\|_p \\
&= \|-(+a_{m-1}\alpha^{m-1} + \cdots + a_0)\|_p \\
&\leq \text{máx}\{\|a_i\alpha^i\|_p \;/\; i = 0, \ldots, m-1\} \\
&\leq \text{máx}\{\|\alpha^i\|_p \;/\; i = 0, \ldots, m-1\} \\
&= \|\alpha\|_p^{i_0} \text{ para algún } \quad 0 \leq i_0 \leq m-1.
\end{aligned}$$

es decir, $\|\alpha\|_p^{m-i_0} \leq 1$. Por tanto, $\|\alpha\|_p \leq 1$, ya que $m - i_0 > 0$.

Ahora, sea $\alpha \in A$, entonces como todos los conjugados de $\alpha = \alpha_1$ sobre $\mathbb{Q}_p$ también están en A ya que si α_i es un conjugado de α

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

Dado que los coeficientes en el polinomio minimal de α son sumas o diferencias de productos de los α_i's se sigue que estos coeficientes tienen norma menor o igual a uno, así, ellos están en $\mathbb{Z}_p$.

M es el único ideal maximal de A, ya que si $\alpha \in A$ y $\alpha \notin M$, entonces, $\|\alpha\|_p = 1$, lo cual implica que α es invertible en A, pues $\|1/\alpha\|_p = 1$. Notemos que

$$M \cap \mathbb{Z}_p = p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \;/\; \|x\|_p \leq 1\}.$$

Por último veamos que A/M es una extensión finita de $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$. Consideremos el homomorfismo

$$\begin{aligned}
\varphi : \quad \mathbb{F}_p \quad &\longrightarrow \quad A/M \\
a + p\mathbb{Z}_p \quad &\longmapsto \quad a + M
\end{aligned}$$

entonces φ es una inclusión, ya que si $a + M = b + M$ entonces $a - b \in M$, como $a, b \in \mathbb{Z}_p$, así que $a - b \in M \cap \mathbb{Z}_p = p\mathbb{Z}_p$, de ahí que, $a + p\mathbb{Z}_p = b + p\mathbb{Z}_p$. Veamos que

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

Supongamos que $[K : \mathbb{Q}_p] = n$, mostremos que cualquier conjunto de $n + 1$ elementos $\{\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_{n+1}\}$ en A/M es linealmente dependiente sobre $\mathbb{F}_p$. Dado que $[K : \mathbb{Q}_p] = n$,

$\{a_1, a_2, \ldots, a_{n+1}\}$ son linealmente dependientes sobre $\mathbb{Q}_p$, es decir; existen

$$b_1, \ldots, b_{n+1} \in \mathbb{Q}_p$$

no todos iguales a cero, tal que

$$a_1b_1 + a_2b_2 + \ldots + a_{n+1}b_{n+1} = 0.$$

Multiplicando por p^{-l} donde $l = \text{máx}\{\|b_i\|_p \;/\; i = 1, \ldots, n+1\}$ podemos suponer que los $b_i \in \mathbb{Z}_p$, donde al menos un $b_i \notin p\mathbb{Z}_p$. Así,

$$\overline{a}_1\overline{b}_1 + \overline{a}_2\overline{b}_2 + \ldots + \overline{a}_{n+1}\overline{b}_{n+1} = 0$$

es una expresión en A/M que muestra que $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_{n+1}$ son linealmente dependientes sobre $\mathbb{F}_p$. $\square$

Nota: El campo A/M es llamado **el campo residual** de K sobre $\mathbb{Q}_p$. Es usual llamar a A el "**anillo de valuación**" de $\| \; \|_p$ en K.

1.4.1. Estructura de campos p-ádicos.

Sea K una extensión finita de $\mathbb{Q}_p$ de grado n, definimos

$$A_K = \{x \in K \;/\; \|x\|_p \leq 1\}$$

$$M_K = \{x \in K \;/\; \|x\|_p < 1\}.$$

En la sección anterior probamos que A_K es un anillo local con ideal maximal M_K y además, que A_K/M_K es una extensión finita de $\mathbb{F}_p$ de grado a lo sumo n.
Sea $\alpha \in K - \mathbb{Q}_p$, entonces α es algebraico sobre $\mathbb{Q}_p$ de grado m, con $2 \leq m \leq n$, es decir; α satisface una ecuación polinomial sobre $\mathbb{Q}_p$ de la forma

$$a_mX^m + \cdots + a_0 = 0$$

con $a_m \neq 0$, $a_i \in \mathbb{Q}_p \;\; i = 0, \ldots, m$. Esto implica que existe $0 \leq i < j$ tal que $\|a_i\alpha^i\|_p = \|a_j\alpha^j\|_p \neq 0$, esto es el Corolario 1.1.2 para la norma extendida a K. De ahí que,

$$\begin{aligned}\|\alpha\|_p^{j-i} &= \left\|\frac{a_i}{a_j}\right\|_p \\ &= p^d\end{aligned}$$

para algún $d \in \mathbb{Z}$, así $\|\alpha\|_p = p^{d/c}$, donde $c = j - i$. De lo anterior, vemos que al extender a K la definición de **orden** de un elemento $\alpha \in K$ como:

$$ord_p(\alpha) = -\log_p \|\alpha\|_p = -\frac{1}{n}\log_p \|\mathbf{N}_{K|\mathbb{Q}_p}(\alpha)\|_p. \tag{1.4.3}$$

Esta definición concuerda con la dada para cuando $\alpha \in \mathbb{Q}_p$, pues si $\alpha = p^m\beta$, donde $\beta \in \mathbb{Z}_p^\times$, entonces

$$ord_p(\alpha) = -\log_p(\|p^m\beta\|_p) = -\log_p(p^{-m}) = -(-m) = m.$$

Además, es claro que está es una función multiplicativa, es decir, $ord_p(\alpha\beta) = ord_p(\alpha) + ord_p(\beta)$, lo cual nos dice ord_p es una valuación sobre K. La imagen de $K^\times$ bajo la valuación esta contenida en $\frac{1}{n}\mathbb{Z} = \{x \in \mathbb{Q} \ / \ nx \in \mathbb{Z}\}$, igualdad 1.4.3. Dado que esta imagen es un subgrupo aditivo de $\frac{1}{n}\mathbb{Z}$, está imagen debe ser $\frac{1}{e}\mathbb{Z}$ para algún entero positivo e que divide a n. Sea $\pi \in K$ un elemento de norma maximal menor que 1, entonces se tiene que $M_K = \pi A_K$, así, tenemos que $\frac{1}{p} = \|p\|_p = (\|\pi\|_p)^e$, es decir; $\|\pi\|_p = p^{-1/e}$.

Definición 1.4.14. El **Grado Residual** de una extensión finita K de $\mathbb{Q}_p$ es el entero

$$f = [A_K/M_K : \mathbb{F}_p].$$

El **índice de Ramificación** de K sobre $\mathbb{Q}_p$ es el entero

$$e = [\|K^\times\|_p : \|\mathbb{Q}^\times\|_p]$$

donde $\|K^\times\|_p$ y $\|\mathbb{Q}^\times\|_p$ denotan el grupo de valores de $K^\times$ y $\mathbb{Q}^\times$ respectivamente.

De la definición de e y la definición de f, vemos que $e \leq n$ y $f \leq n$, ahora, mostraremos que tenemos más que esta relación de desigualdad.

Proposición 1.4.15. *Sea K una extensión finita de $\mathbb{Q}_p$ de grado n, entonces $n \geq e\,f$, donde f es el grado residual y e es el índice de ramificación.*

Demostración. Sea $\{a_1, \ldots, a_f\}$ elementos en A_K tal que la imagen en el cociente $\{\overline{a}_1, \ldots, \overline{a}_f\}$ es una base para A_K/M_K como espacio vectorial sobre el campo $\mathbb{F}_p$.

Afirmación: El conjunto $\{a_i\pi^j \ / \ i = 1, \ldots, f, \quad j = 0, \ldots, e-1\}$ es linealmente independiente sobre $\mathbb{Q}_p$, donde π es un elemento de norma maximal en M_K, es dedir, $\|\pi\|_p = p^{-1/e}$

Consideremos una combinación lineal no trivial

$$\sum c_{ij}a_i\pi^j = \sum x_j\pi^j, \quad \text{con} \quad c_{ij} \in \mathbb{Q}_p$$

donde $x_j = \sum c_{ij}a_i$. Entonces para cada j existe un índice $l = l_j$, tal que

$$\|c_{lj}\|_p \geq \|c_{ij}\|_p \ \text{ para todo } \ i$$

y así, $\dfrac{x_j}{c_{lj}} = \sum \left(\dfrac{c_{ij}}{c_{lj}}\right) a_i = \sum \gamma_i a_i$ es una combinación lineal no trivial con coeficientes en A_K y $\gamma_l = 1$. Consideremos esta relación $\mod M_K$. Definamos $\overline{\gamma}_i = \gamma_i \mod p$. Dado que $\{\overline{a}_1, \ldots, \overline{a}_f\}$ es una base para el campo residual A_K/M_K tenemos que

$$0 \neq \sum \overline{\gamma}_i\overline{a}_i \in A_K/M_K$$

simplemente porque $\overline{\gamma}_l = 1$. De ahí que

$$\sum \gamma_i a_i \notin M_K$$

lo cual implica que

$$\left\|\sum \gamma_i a_i\right\|_p = 1$$

es decir; $\|x_j\|_p = \|c_{lj}\|_p \in \|\mathbb{Q}_p^\times\|$ es una potencia entera de p. Si $\sum x_j\pi^j = 0$ implicaría que existen $\|x_j\pi^j\|_p = \|x_{j'}\pi^{j'}\|_p$, de ahí que, $\|x_j\|_p\|\pi\|_p^j = \|x_{j'}\|_p\|\pi\|_p^{j'}$, es decir; $p^m = \|\pi\|_p^{j'-j}$, esto contradice la maximalidad de la norma de π en M_K. Así, todas las normas de los elementos $x_j\pi^j$ son diferentes, implicando que

$$\sum x_j\pi^j \neq 0, \quad \text{Corolario 1.1.2}$$

es decir, $\sum c_{ij} a_i \pi^j \neq 0$. Esto prueba la afirmación, además se concluye que

$$e\,f \leq [K : \mathbb{Q}_p] = n.$$

□

Teorema 1.4.16. *Para cada extensión finita K de $\mathbb{Q}_p$, tenemos*

$$e\,f = [K : \mathbb{Q}_p] = n. \text{ (Igualdad fundamental)}$$

Demostración. Por la proposición anterior es suficiente mostrar la existencia de un conjunto generador de K sobre $\mathbb{Q}_p$ que contenga $e\,f$ elementos.

Afirmación: El conjunto $\{a_i \pi^j \;/\; i = 1, \ldots, f,\;\; j = 0, \ldots, e-1\}$ es un conjunto generador para K como $\mathbb{Q}_p$-espacio vectorial.

Sea $x \in A_K$. Entonces x se puede escribir como

$$x = \sum_{l=0}^{\infty} c_l p^l, \quad \text{donde} \quad c_l = \sum_{i=1}^{f} \sum_{j=0}^{e-1} c_{ij} a_i \pi^j, \quad \text{cada} \quad c_{ijl} \in \mathbb{Z}_p \tag{1.4.4}$$

es decir,

$$x = \sum_{l=0}^{\infty} \sum_{i=1}^{f} \sum_{j=0}^{e-1} c_{ij} a_i \pi^j p^l$$

observemos que l es el único índice con infinitos valores y además, $p^l \to 0$, así podemos cambiar el orden de la serie, entonces:

$$x = \sum_{i=1}^{f} \sum_{j=0}^{e-1} \left(\sum_{l \geq 0} c_{ij} p^l \right) a_i \pi^j$$

definiendo $c_{ij} = \sum_{l \geq 0} c_{ij} p^l \in \mathbb{Z}_p$, tenemos que $x = \sum_{ij} c_{ij} a_i \pi^j$, como A_K es un anillo de valuación en K, esto prueba que $\{a_i \pi^j \;/\; i = 1, \ldots, f,\;\; j = 0, \ldots, e-1\}$ genera a K como un espacio vectorial sobre $\mathbb{Q}_p$ y se sigue que $e\,f \geq n$. Por la proposición anterior $n \geq e\,f$, así, $n = e\,f$. □

Nota. Sea K una extensión finita de $\mathbb{Q}_p$ decimos que:

- K es **no ramificada** cuando $e = 1$, i.e., cuando $[K : \mathbb{Q}_p] = f$.

- K es **totalmente ramificada** cuando $f = 1$, i.e., $[K : \mathbb{Q}_p] = e$.
- K es **dócilmente ramificada** si $p \nmid e$.
- K es **salvajemente ramificada** si e es una potencia de p.

En otras palabra, una extensión finita K de $\mathbb{Q}_p$ es no ramificada cuando p es un generador del ideal maximal $M_K \subseteq A_K$ y K es una extensión totalmente ramificada cuando el campo residual no crece.

En adelante la clausura algebraica de $\mathbb{Q}_p$, será denotada por $\mathbb{Q}_p^{alg}$, su anillo de valuación de $\mathbb{Q}_p^{alg}$, es denotado por $\mathbb{Z}_p^{alg}$, es decir,

$$\mathbb{Z}_p^{alg} = \{x \in \mathbb{Q}_p^{alg} \ / \ \|x\|_p \leq 1\}$$

y su único ideal maximal por

$$p\mathbb{Z}_p^{alg} = \{x \in \mathbb{Q}_p^{alg} \ / \ \|x\|_p < 1\}$$

Una consecuencia de la Proposición 1.4.13 nos dice que

$$\mathbb{Z}_p^{alg}/p\mathbb{Z}_p^{alg} \cong \mathbb{F}_p^{alg} = \cup_{f=1}^{\infty}\mathbb{F}_{p^f}.$$

1.4.2. La completación del campo $\mathbb{Q}_p^{alg}$, $\mathbb{C}_p$

El objetivo principal de esta sección es mostrar la existencia de un campo completo y algebraicamente cerrado, el cual, contenga a $\mathbb{Q}_p$, es decir, un campo análogo a los números complejos $\mathbb{C}$. Primero, veamos que la clausura algebraica $\mathbb{Q}_p^{alg}$, de $\mathbb{Q}_p$ no es completa con respecto a la norma inducida.

Lema 1.4.17. *Sea α un elemento algebraico sobre $\mathbb{Q}_p$ de grado n, esto es, $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = n$. Entonces existe un entero positivo N, tal que α no satisface ninguna congruencia*

$$a_m\alpha^m + \cdots + a_1\alpha + a_0 = 0 \mod p^N$$

en la cual $a_j \in \mathbb{Z}_p$ no todos divisibles por p.

Demostración. Sea $P(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0$ el polinomio minimal de α sobre $\mathbb{Q}_p$, multiplicando por p^{-k} donde $k = \text{mín}\{ord_p(b_i) \,/\, i = 0, \ldots, n-1\}$, tenemos que

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0, \text{ con } a_n = p^{-k},$$

así, $a_n \in \mathbb{Z}_p$ y no todos los $a_0, \ldots, a_{n-1}$ son divisibles por p. De la ecuación anterior, se sigue que

$$-a_n\alpha^n = a_{n-1}\alpha^n - 1 + \cdots + a_1\alpha + a_0,$$

de ahí que, si para todo N, se tiene que, $a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0 = 0 \mod p^N$. Se tendría que, $-a_n\alpha^n = 0 \mod p^N$ para todo N, de donde, $a_n = 0$, lo cual es un absurdo. $\square$

Teorema 1.4.18. *La clausura algebraica $\mathbb{Q}_p^{alg}$ no es un espacio métrico completo.*

Demostración. Mostraremos la existencia de una sucesión de Cauchy $\{a_n\}_{n\in\mathbb{N}}$ en $\mathbb{Q}_p^{alg}$, tal que $\{a_n\}_{n\in\mathbb{N}}$ no tiene límite en $\mathbb{Q}_p^{alg}$. Es decir, no existe $a \in \mathbb{Q}_p$, tal que, $\text{lím}_{n\to\infty} a_n = a$.

Sea b_i una $(p^{2^i} - 1)$-raíz de la unidad en $\mathbb{Q}_p^{alg}$ esto es, $b_i^{p^{2^i}-1} = 1$, tal que, $b_i^m \neq 1$, para todo $m < p^{2^i} - 1$. Notemos que si $k > i$, entonces $b_i^{p^{2^k}-1} = 1$, ya que $2^i | 2^k$, implica que $p^{2^i} - 1 | p^{2^i} - 1$. Por tanto, si $k > i$, b_i es una potencia de b_k. Definimos

$$a_n := \sum_{i=0}^{n} b_i p^{N_i},$$

donde $0 = N_0 < N_1 < N_2 < \cdots$, es una sucesión de enteros no negativos, los cuales, escogeremos inductivamente. Supongamos que ya tenemos N_k, para todo $k \leq n$, es decir, tenemos $a_n = \sum_{i=0}^{n} b_i p^{N_i}$. Sea $K = \mathbb{Q}_p(b_n)$, en la sección anterior mostramos que K es una extensión no ramificada, de grado 2^n. Además, mostramos todos los conjugados de b_n están en K, [9]. Así, K es también una extensión de Galois. De ahí que, $K = \mathbb{Q}_p(a_n)$, de lo contrario, se tendría $\mathbb{Q}_p \not\subseteq \mathbb{Q}_p(a_n) \not\subseteq \mathbb{Q}_p(b_n)$, por tanto, existe un automorfismo σ de K el cual deja fijo a $\mathbb{Q}_p(a_n)$, es decir, $\sigma(a_n) = a_n$. Por otro lado, $\sigma(a_n)$ tiene expansión p-ádica $\sum_{i=0}^{n} \sigma(b_i)p^{N_i}$ y dado que, $\sigma(b_n) \neq b_n$, se sigue que, $\sigma(a_n) \neq a_n$, puesto que tienen expansiones p-ádicas distintas. Notemos que los b_i con $i = 0, 1, \ldots, n$ son los digitos en la expansión p-ádica de a_n en la extensión no ramificada $\mathbb{Q}_p(b_n)$, dado que $b_i^{p^{2^i}} = b_i$, y así $\{a_n\}$ es una sucesión de Cauchy.

Por el Lema anterior, existe $N_{n+1} > N_n$ tal que a_n no satisface ninguna congruencia

$$\beta_k a_n^k + \beta_{k-1} a_n^{k-1} + \cdots + \beta_1 a_n + \beta_0 = 0 \mod p^{N_{n+1}},$$

para todo $k < 2^n$ y $\beta_j \in \mathbb{Z}_p$, no todos divisibles por p. Esto nos da la existencia de nuestra sucesión $\{a_n\}$. Por último, basta ver que no tiene límite en $\mathbb{Q}_p^{alg}$. Supongamos por el contrario que existe $a \in \mathbb{Q}_p^{alg}$, tal que

$$\lim_{n\to\infty} a_n = a.$$

Dado que a es algebraico sobre $\mathbb{Q}_p$, a satisface una ecuación polinomial de la forma

$$\beta_m a^m + \beta_{m-1} a^{m-1} + \cdots + \beta_1 a + \beta_0 = 0,$$

para algún $m \geq 0$, donde podemos suponer que todos los $\beta_j \in \mathbb{Z}_p$ y no todos son divisibles por p, estas dos condiciones se logran al multiplicar por una potencia adecuada de p. Ahora, sea n tal que $2^n > m$. Dado que $a = a_i \mod p^{N_{n+1}}$, tenemos que

$$\beta_m (a_n)^m + \beta_{m-1} (a_n)^{m-1} + \cdots + \beta_1 a_n + \beta_0 = 0 \mod p^{N_{n+1}},$$

lo cual contradice la definición de a_n. □

Proposición 1.4.19. *El conjunto de los posibles valores para la norma p-ádica sobre $\mathbb{Q}_p^{alg}$ son todas las potencias racionales de p, es decir, para todo $\alpha \in \mathbb{Q}_{alg}^p$ existe $r \in \mathbb{Q}$ tal que $\|\alpha\|_p = p^r$. Esto lo denotaremos por $\|(\mathbb{Q}_p^{alg})^\times\|_p = p^{\mathbb{Q}}$.*

Demostración. Si $\alpha \in \mathbb{Q}_p$, esto es claro. Sea $\alpha \in \mathbb{Q}_p^{alg} - \mathbb{Q}_p$, entonces α es algebraico sobre $\mathbb{Q}_p$ de grado $2 \leq n$, es decir; α satisface una ecuación polinomial sobre $\mathbb{Q}_p$ de la forma

$$a_n \alpha^n + \cdots + a_0 = 0$$

con $a_n \neq 0$, $a_i \in \mathbb{Q}_p$ $i = 0, \ldots, n$. Esto implica que existe $0 \leq i < j$ tal que $\|a_i \alpha^i\|_p = \|a_j \alpha^j\|_p \neq 0$ (esto es el corolario 1.1.2 para la norma extendida a $\mathbb{Q}_p^{alg}$). De ahí que,

$$\begin{aligned} \|\alpha\|_p^{j-i} &= \left\| \frac{a_i}{a_j} \right\|_p \\ &= p^d \end{aligned}$$

para algún $d \in \mathbb{Z}$, se que concluye $\|\alpha\|_p = p^{d/c}$, donde $c = j - i$. □

Definición 1.4.20. Definimos $\mathbb{C}_p$ como la completación de $\mathbb{Q}_p^{alg}$ con respecto a la norma p-ádica, $\| \|_p$, esto es,

$$\mathbb{C}_p = \widehat{\mathbb{Q}_p^{alg}}$$

Justo como extendimos la norma $\| \|_p$ en $\mathbb{Q}$ a $\mathbb{Q}_p$, extendemos la norma $\| \|_p$ en $\mathbb{Q}_p^{alg}$ a $\mathbb{C}_p$, al definir, para cada $a \in \mathbb{C}_p$, $\|a\|_p = \lim_{n\to\infty} \|a_n\|_p$, donde $\{a_n\}$ es una sucesión de Cauchy de elementos en $\mathbb{Q}_p^{alg}$ que converge a a.

Al igual que al pasar de $\mathbb{Q}$ a $\mathbb{Q}_p$, es sencillo mostrar que para todo $a \in \mathbb{C}_p$, $a \neq 0$, se tiene que, $\|a\|_p = \|a_n\|_p$ para n suficientemente grande. De ahí que, el conjunto de valores de $\| \|_p$ sobre $\mathbb{C}_p$ es también $p^{\mathbb{Q}}$.

También, extendemos ord_p a $\mathbb{C}_p$ como

$$ord_p(a) = -\log_p \|a\|_p \text{ para todo } a \in \mathbb{C}_p.$$

El próximo teorema nos dice que $\mathbb{C}_p$ es el campo p-ádico análogo de los número complejos $\mathbb{C}$.

Teorema 1.4.21. *El campo $\mathbb{C}_p$ es algebraicamente cerrado.*

Demostración. Sea $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polinomio en $\mathbb{C}_p[X]$. Basta mostrar que f tiene una raíz en $\mathbb{C}_p$. Para cada $i = 0, 1, \ldots, n-1$, sea $\{a_m^{(i)}\}$ una sucesión de $\mathbb{Q}_p^{alg}$ que converge a a_i, esto es, $\lim_{m\to\infty} a_m^{(i)} = a_i$. Definimos para todo $m = 0, 1, 2, \ldots$

$$g_m(X) := X^n + a_{n-1,m}X^{n-1} + \cdots a_{1,m}X + a_{0,m}$$

Entonces $g_m \longrightarrow f$, ya que cada coeficiente lo hace. Además, para cada m, $g_m(X) \in \mathbb{Q}_p^{alg}[X]$, por tanto, g_m tiene todas sus raíces en $\mathbb{Q}_p^{alg}$, sean $r_{1,m}, r_{2,m}, \ldots, r_{n,m} \in \mathbb{Q}_p^{alg}$ las raíces de $g_m(X)$.

Afirmación. Existe una subsucesión $\{r_{k_m,m}\}$ la cual es una sucesión de Cauchy para algún $1 \leq k_m \leq n$.

Veamos esto por inducción. Supongamos que tenemos $r_{k_m,m}$ y deseamos hallar $r_{k_{m+1},m+1}$. Sea $\delta_m = \|g_m - g_{m+1}\|_p = \max\{\|a_m^{(i)} - a_{m+1}^{(i)}\|_p \ / \ i = 0, \ldots, n\}$. Note que $\delta_m \to 0$, cuando

$m \to \infty$, ya que $g_m \to f$, cuando $m \to \infty$. Si $A_m = \text{máx}\{1, \|r_{i,m}\|_p^n \ / \ i = 0, \ldots, n\}$, existe una constante A, tal que, para todo m $A_m \leq A$. Por consiguiente,

$$\begin{aligned}
\prod \|r_{k_m,m} - r_{i,m+1}\|_p &= \|g_{m+1}(r_{k_m,m})\|_p \\
&= \|g_{m+1}(r_{k_m,m}) - g_m(r_{k_m,m})\|_p \\
&\leq \text{máx}\{\|a_m^{(i)} - a_{m+1}^{(i)}\|_p, \|r_{k_m,m}\|_p^i \ / \ i = 0, \ldots, n\} \\
&\leq \delta_m A.
\end{aligned}$$

De donde, existe al menos un i tal que

$$\|r_{k_m,m} - r_{i,m+1}\|_p \leq \sqrt[n]{\delta_m A}. \quad (\dagger)$$

Sea $r_{k_{m+1},m+1}$ cualquiera de tales $r_{i,m+1}$ que satisface ($\dagger$). Por las propiedades de $\| \ \|_p$ es claro que $\{r_{k_m,m}\}$ es una sucesión de Cauchy. Ahora si definimos $r = \text{lím}_{m\to\infty} r_{k_m,m} \in \mathbb{C}_p$, $r \in \mathbb{C}_p$ y se sigue que

$$f(r) = \lim_{m\to\infty} f(r_{k_m,m}) = \lim_{m\to\infty} g_m(r_{k_m,m}) = 0.$$

Como se deseaba. □

Finalizamos este estudio de los números p-ádicos mostrando que $\mathbb{Q}_p^{alg}$ y $\mathbb{C}_p$ **no** son localmente compactos, lo que los separa radicalmente de $\mathbb{C}$, por ejemplo, no podemos usar el procedimiento expuesto en el Apendice A para definir una medida de Haar en $\mathbb{Q}_p^{alg}$ o en $\mathbb{C}_p$.

Teorema 1.4.22. *Los campos $\mathbb{Q}_p^{alg}$ y $\mathbb{C}_p$ no son localmente compactos.*

Demostración. Topológicamente los campos $\mathbb{Q}_p^{alg}$ y $\mathbb{C}_p$ de $\mathbb{Q}_p$ son homeomorfos a $\prod_{\mathbb{N}} \mathbb{Q}_p$, y sabemos que el producto de espacios topológicos es localmente compacto, si y sólo si excepto un número finito de ellos son compactos [9]. □

Resumimos este capítulo en una tabla con los hechos más importantes:

Campo$\supseteq$ A $\supseteq$ M	**Campo Residual**	**Valores** $\| \ \|_p$	**Propiedades**
$\mathbb{Q}_p \supseteq \mathbb{Z}_p \supseteq p\mathbb{Z}_p$	$\mathbb{F}_p$	$p^{\mathbb{Z}}$	Completo y locamente Compacto.
$\mathbb{Q}_p^{alg} \supseteq \mathbb{Z}_p^{alg} \supseteq p\mathbb{Z}_p^{alg}$	$\mathbb{F}_p^{alg}$	$p^{\mathbb{Q}}$	Algebraicamente Cerrado, No completo y No localmente compacto.
$\mathbb{C}_p \supseteq \widehat{A} \supseteq \widehat{M}$	$\mathbb{F}_p^{alg}$	$p^{\mathbb{Q}}$	Algebraicamente Cerrado, Completo y No localmente compacto.

Capítulo 2

Series de Poincaré de Singularidades de curvas sobre $\mathbb{F}_q$

Resumen: En este capítulo motivaremos la noción de curva geométrica [21] y daremos la definición de series de Poincaré multi-variable de singularidades de curvas definida por Karl Stöhr.

2.1. Curvas Singulares

Sea k un campo algebraicamente cerrado y sea C una curva algebraica afín sobre k. En otras palabras, C es una variedad algebraica cuyo anillo de coordenads $k[C]$ (vea [3] pag 661) es un dominio entero, tal que el campo de funciones racionales $k(C) = \mathrm{Frac}(k[C])$ tiene grado de transcendencia 1 sobre k.

Decimos que un punto $v \in C$ es no singular, sí $\mathfrak{m}_{v,C}/\mathfrak{m}_{v,C}^2$ es k-espacio vectorial de dimensión 1, donde $m_{v,C}$ es el único ideal maximal del anillo local $\mathcal{O}_{v,C}$, de funciones racionales sobre C definidas en v, (vea [3] pag 722). Entonces sabemos que v es un punto no singular de C sobre k sí, y solo si, el anillo local $\mathcal{O}_{v,C}$ es un anillo de valuación discreta (vea [3] Proposición 12 pag 763). Además, sabemos que al hacer **Blow up** en cada punto de C, obtenemos el modelo no singular de C, denotado por $\widetilde{C}$. Cada punto $\widetilde{v} \in \widetilde{C}$ se proyecta en un único punto $v \in C$ y cada punto singular de $v \in C$, al hacer blow up sobre él, se convierte a lo sumo en un número finito de puntos $\widetilde{v}_1, \ldots, \widetilde{v}_m \in \widetilde{C}$.

Lo anterior motiva a definir en términos más algebraicos que geométricos la noción de curva algebraica.

Sea $K|k$ un cuerpo de funciones en una variable con campo de constantes k, donde k no necesita ser algebraicamente cerrado. Diremos que X es una curva algebraica, geométricamente irreducible y completa, si X es el conjunto de índices de $\{\mathcal{O}_P\}_{P \in X}$, donde los $\mathcal{O}_P$ son k-algebras locales propiamente contenidas en K y con campo de fracciones K, con las siguientes dos propiedades:

(i) Para casi todo $P \in X$, el anillo de local $\mathcal{O}_P$ es un anillo de valuación discreta.

(ii) Para cada anillo de valuación discreta R de $K|k$ existe un único $P \in X$ tal que $\mathcal{O}_P \subseteq R$.

Por la primera propiedad el número de posibles singularidades de X es finito. Y por la segunda propiedad, existe un morfismo $\pi : \widetilde{X} \longrightarrow X$, donde $\widetilde{X}$ denota el conjunto de índices de todas las valuaciones discretas de $K|k$, llamado el **modelo no singular** o **normalización** de X sobre k. Para cada $P \in X$ los elementos de la fibra $\pi^{-1}(P)$ son llamados la **ramas de X centradas en** P. Por el teorema de existencia de valuaciones (vea [6]), el morfismo $\pi : \widetilde{X} \longrightarrow X$ es sobreyectivo, es decir, para todo $\mathcal{O}_P$ existe un anillo de valuación discreta R por encima de $\mathcal{O}_P$. Además, el número de ramas centradas en P es finito, veamos esta última afirmación en detalle.

Proposición 2.1.1. *Sea $K|k$ un campo de funciones en una variable sobre k. Si $\mathcal{O}$ una k-algebra local propiamente contenida en K, tal que Frac$(\mathcal{O}) = K$, entonces existen finitos anillos de valuación discreta de $K|k$ sobre $\mathcal{O}$.*

Demostración. Sabemos que la clausura entera de $\mathcal{O}$, denotada por $\widetilde{\mathcal{O}}$, es la intersección de todos los anillos de valuación que contienen a $\mathcal{O}$ (vea Corolario 5.22 [1]), así, que todo anillo de valuación sobre $\mathcal{O}$ es también un anillo de valuación sobre $\widetilde{\mathcal{O}}$. Por tanto, probar que existen finitos anillos de valuación discreta sobre $\mathcal{O}$, es equivalente a probar la existencia de finitos anillos de valuación disreta sobre $\widetilde{\mathcal{O}}$. El Teorema 7 pag 755 y el Corolario 8 pag 758 [3], nos dicen que si I es un ideal primo minimal de $\widetilde{\mathcal{O}}$ con respecto a la inclusión, entonces la localización de $\widetilde{\mathcal{O}}$ en I, $\widetilde{\mathcal{O}}_I$ es un anillo de valuación discreta y dado que los anillos de valuación discreta son anillos maximales, entonces existe una correspondencia biyectiva entre los ideales primos minimales de $\widetilde{\mathcal{O}}$ y los anillos de valuación discreta que contienen a $\widetilde{\mathcal{O}}$. Por tanto, basta probar que en un dominio noetheriano existen finitos ideales primos minimales, lo cual es una consecuencia directa del Teorema de Descomposición Primaria en anillos noetherianos (vea Corolario 22 pag 685 [3]) $\square$

Sea $Q_1, \ldots, Q_m \in \widetilde{X}$ las ramas centradas en P, esto es, $\pi^{-1}(P) = \{\mathcal{O}_{Q_1}, \ldots, \mathcal{O}_{Q_m}\}$ donde $\mathcal{O}_{Q_1}, \ldots, \mathcal{O}_{Q_m}$ son los correspondientes anillos locales a estos puntos. Dado que K es el campo de funciones de $\widetilde{X}$ y de X y $\widetilde{X}$ es una curva no singular, los anillos locales $\mathcal{O}_{Q_1}, \ldots, \mathcal{O}_{Q_m}$ son precisamente los anillos de valuación discreta de $K|k$ sobre $\mathcal{O}_P$. La clausura entera de $\mathcal{O}_P$, denotada por $\widetilde{\mathcal{O}}_P$ es

$$\widetilde{\mathcal{O}}_P = \mathcal{O}_{Q_1} \cap \cdots \cap \mathcal{O}_{Q_m}$$

y por tanto, $\widetilde{\mathcal{O}}_P$ es un dominio de ideales principales semilocal, cuyos ideales maximales $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ corresponden biyectivamente a las ramas $Q_1, \ldots, Q_m$. Es decir, para cada $i = 1, \ldots, m$

$$\mathfrak{p}_i = \widetilde{\mathcal{O}}_P \cap \mathfrak{m}_{Q_i} = \{z \in \widetilde{\mathcal{O}}_P \ / \ v_i(z) > 1\}$$

donde $v_i = ord_{Q_i}$ es la valuación discreta correspondiente a $\mathcal{O}_{Q_i}$ en el campo de funciones $K|k$ y $\mathfrak{m}_{Q_i} = \{z \in \mathcal{O}_{Q_i} \ / \ v_i(z) > 1\}$ es el único ideal maximal de $\mathcal{O}_{Q_i}$.

Ahora bien, la completación del anillo local $(\mathcal{O}_P, \mathfrak{m}_p)$ será denotada por $\widehat{\mathcal{O}_P}$ y la completación del anillo semi local $\widetilde{\mathcal{O}}_P$ con respecto a su ideal de Jacopson $\mathcal{J} = \cap \mathfrak{p}_i$ es denotada por $\widehat{\widetilde{\mathcal{O}}}_P$. Dado que $\mathcal{O}_P$ tiene k-codimensión finita en $\widetilde{\mathcal{O}}_P$, esto es, $\delta_P = \dim(\widetilde{\mathcal{O}}_P/\mathcal{O}_P)$ (vea Capítulo 4 [20]), de ahí que, $\widetilde{\mathcal{O}}_P$ es un $\mathcal{O}_P$-módulo finitamente generado. Tomando la filtración

$$\widetilde{\mathcal{O}}_P \supseteq \mathcal{J} \supseteq \mathcal{J}^2 \supseteq \mathcal{J}^3 \supseteq \cdots$$

tal filtración es $\mathfrak{m}_P$-estable, ya que:

(i) Para todo $n \geq 1$, $\mathfrak{m}_P \mathcal{J}^n \subseteq \mathcal{J}^{n+1}$, esto es equivalente a mostrar que $\mathfrak{m}_P \subseteq \mathcal{J}$. Sea $z \in \mathfrak{m}_P$. Entonces $1+z$ es un elemento invertible en $\mathcal{O}_P \subseteq \mathcal{O}_{Q_i}$, por tanto es invertible en $\mathcal{O}_{Q_i}$, esto significa que $z \in \mathfrak{m}_{Q_i}$, de ahi que $z \in \mathcal{J}$.

(ii) Existe un $n \geq 1$ tal que $\mathfrak{m}_P \mathcal{J}^n = \mathcal{J}^{n+1}$. Basta mostrar que existe un $n \geq 1$ tal que $\mathfrak{m}_P \widetilde{\mathcal{O}}_P \supseteq \mathcal{J}^n$. Tomando $n_i = \text{mín}\{v_i(z) \ / \ z \in \mathfrak{m}_P \widetilde{\mathcal{O}}_P\}$, tenemos que

$$\mathfrak{m}_P \widetilde{\mathcal{O}}_P = \widetilde{\mathcal{O}}_P t_1^{n_1} \cdots t_m^{n_m}$$

donde t_i es un **parámetro local** de $\mathcal{O}_{Q_i}$, es decir, $v_i(t_i) = 1$ y es claro que $\mathcal{J} = \widetilde{\mathcal{O}}_P t_1 \cdots t_m$. De ahí que tomando $n = n_1 + \cdots + n_m$, tenemos

$$\begin{aligned} \mathcal{J}^n &= \widetilde{\mathcal{O}}_P t_1^n \cdots t_m^n \\ &= \left(\widetilde{\mathcal{O}}_P t_1^{n_1} \cdots t_m^{n_m}\right)\left(t_1^{n-n_1} \cdots t_m^{n-n_m}\right) \\ &= \mathfrak{m}_P \widetilde{\mathcal{O}}_P \left(t_1^{n-n_1} \cdots t_m^{n-n_m}\right) \\ &\subseteq \mathfrak{m}_P \widetilde{\mathcal{O}}_P. \end{aligned}$$

Por tanto por el Lema de Artin-Rees (Proposición 10.9 [1]), la filtración inducida

$$\mathcal{O}_P \cap \widetilde{\mathcal{O}}_P \supseteq \mathcal{O}_P \cap \mathcal{J} \supseteq \mathcal{O}_P \cap \mathcal{J}^2 \supseteq \mathcal{O}_P \cap \mathcal{J}^3 \supseteq \cdots$$

es $\mathfrak{m}_P$-estable, es decir, existe n tal que

$$\begin{aligned} \mathfrak{m}_P (\mathcal{O}_P \cap \mathcal{J}^n) &= \mathcal{O}_P \cap \mathcal{J}^{n+1} \\ \mathfrak{m}_P^{n+1} &= \mathcal{O}_P \cap \mathcal{J}^{n+1}. \end{aligned}$$

De lo anterior, tenemos la siguiente proposición:

Proposición 2.1.2. *La topología de $\mathcal{O}_P$ es inducida por la topología de $\widetilde{\mathcal{O}}_P$ y así $\widehat{\mathcal{O}_P}$ es un subanillo cerrado de $\widehat{\widetilde{\mathcal{O}}}_P$ de k-codimensión δ_P*

Ahora nos concentraremos en $\widetilde{\mathcal{O}}_P$ y en su completación $\widehat{\widetilde{\mathcal{O}}}_P$. Dado que dos ideales maximales diferentes son comaximales, se tiene que $\mathfrak{p}_i$ y $\mathfrak{p}_j$ son comaximales si $i \neq j$, de ahí que $\mathcal{J} = \mathfrak{p}_1 \cdots \mathfrak{p}_m = \widetilde{\mathcal{O}}_P \mathfrak{m}_{Q_1} \cdots \mathfrak{m}_{Q_m}$, usando el Teorema Chino del Residuo, tenemos:

$$\begin{aligned}
\frac{\widetilde{\mathcal{O}}_P}{\mathcal{J}} &= \frac{\widetilde{\mathcal{O}}_P}{\widetilde{\mathcal{O}}_P \cap \mathfrak{m}_{Q_1} \cap \cdots \cap \mathfrak{m}_{Q_m}} \\
&\cong \frac{\widetilde{\mathcal{O}}_P}{\widetilde{\mathcal{O}}_P \cap \mathfrak{m}_{Q_1}} \times \cdots \times \frac{\widetilde{\mathcal{O}}_P}{\widetilde{\mathcal{O}}_P \cap \mathfrak{m}_{Q_m}}.
\end{aligned}$$

Analogamente, $\mathfrak{p}_i^n$ y $\mathfrak{p}_j^n$ son comaximales si $i \neq j$,

$$\frac{\widetilde{\mathcal{O}}_P}{\mathcal{J}^n} \cong \frac{\widetilde{\mathcal{O}}_P}{\widetilde{\mathcal{O}}_P \cap \mathfrak{m}_{Q_1}^n} \times \cdots \times \frac{\widetilde{\mathcal{O}}_P}{\widetilde{\mathcal{O}}_P \cap \mathfrak{m}_{Q_m}^n}.$$

Por tanto, tenemos que para todo $n \neq 1$

$$\frac{\widetilde{\mathcal{O}}_P}{\mathcal{J}^n} \cong \frac{\mathcal{O}_{Q_1}}{\mathfrak{m}_{Q_1}^n} \times \cdots \times \frac{\mathcal{O}_{Q_m}}{\mathfrak{m}_{Q_m}^n}.$$

Ahora, pasando al límite inverso (vea Capítulo 10 [1]) tenemos que:

$$\begin{aligned}
\widehat{\widetilde{\mathcal{O}}}_P &= \lim_{\leftarrow} \frac{\widetilde{\mathcal{O}}_P}{\mathcal{J}^n} \\
\widehat{\widetilde{\mathcal{O}}}_P &\cong \lim_{\leftarrow} \frac{\mathcal{O}_{Q_1}}{\mathfrak{m}_{Q_1}^n} \times \cdots \times \frac{\mathcal{O}_{Q_m}}{\mathfrak{m}_{Q_m}^n} \\
\widehat{\widetilde{\mathcal{O}}}_P &\cong \lim_{\leftarrow} \frac{\mathcal{O}_{Q_1}}{\mathfrak{m}_{Q_1}^n} \times \cdots \times \lim_{\leftarrow} \frac{\mathcal{O}_{Q_m}}{\mathfrak{m}_{Q_m}^n} \\
\widehat{\widetilde{\mathcal{O}}}_P &\cong \widehat{\mathcal{O}}_{Q_1} \times \cdots \times \widehat{\mathcal{O}}_{Q_m}.
\end{aligned}$$

Donde $\widehat{\mathcal{O}}_{Q_i}$ es la completación del anillo de valuación discreta con respecto a su único ideal maximal $\mathfrak{m}_{Q_i}$. Además, si $\widehat{K}_{v_i}$ es la completación de K con respecto a la valuación v_i correspondiente a $\mathcal{O}_{Q_m}$, entonces

$$\widehat{\widetilde{\mathcal{O}}}_P \subseteq \widehat{K}_{v_1} \times \cdots \times \widehat{K}_{v_m}.$$

Ahora, sea $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ los primos minimales de $\widehat{\mathcal{O}}_P$ y sea $\widehat{\mathcal{O}}_{P\mathfrak{P}_i}$ la completación de $\widehat{\mathcal{O}}_P$ con respecto a $\mathfrak{P}_i$, si $\psi : \widehat{\mathcal{O}}_P \longrightarrow \widehat{\mathcal{O}}_{P\mathfrak{P}_1} \times \cdots \times \widehat{\mathcal{O}}_{P\mathfrak{P}_m}$ denota el homomorfismo diagonal, entonces dado que $\widehat{\mathcal{O}}_P$ es un anillo reducido (vea Teorema 1 [18]) ψ es inyectiva. Lo cual implica que el siguiente diagrama conmuta:

$$\begin{tikzcd}
\widehat{\widehat{\mathcal{O}}}_P \arrow[r, "\sim"] & \widehat{\mathcal{O}}_{Q_1} \times \cdots \times \widehat{\mathcal{O}}_{Q_m} \\
\widehat{\mathcal{O}}_P \arrow[u] \arrow[r, "\psi"] & \widehat{\mathcal{O}}_{P\mathfrak{P}_1} \times \cdots \times \widehat{\mathcal{O}}_{P\mathfrak{P}_m} \arrow[u]
\end{tikzcd}$$

Luego tenemos una correspondencia biyectiva entre los $\widehat{\mathcal{O}}_{Q_i}$ y los $\widehat{\mathcal{O}}_{P\mathfrak{P}_i}$. Nosotros llamamos a los anillos $\widehat{\mathcal{O}}_{P\mathfrak{P}_i}$ las ramas centradas en $\widehat{\mathcal{O}}_P$. Por el Teorema Estructural de Cohen para anillos locales regulares (vea Proposición 10.16 [4]) cada $\widehat{\mathcal{O}}_{Q_i}$ es isomorfo a $k_i[|t_i|]$, donde $k_i = \widehat{\mathcal{O}}_{Q_i}/\widehat{\mathfrak{m}}_{Q_i}$ es el **campo residual** de $\widehat{\mathcal{O}}_{Q_i}$, es claro que $k_i = \mathcal{O}_{Q_i}/\mathfrak{m}_{Q_i} = \widetilde{\mathcal{O}}_P/\mathfrak{p}_i$.

Concluimos que

$$\widehat{\widehat{\mathcal{O}}}_P \cong k_1[|t_1|] \times \cdots \times k_m[|t_m|].$$

Este isomorfismo es una herramienta esencial en nuestro estudio de las series de Poincaré definidas a continuación.

2.2. Series de Poincaré Multi-variables de Singularidades de curvas algebraicas

En esta sección definiremos las series de Poincaré multi-variable $P(\mathfrak{a}, \mathfrak{b}, \mathfrak{t})$. Usamos como referencias [23], [22].

Sea $\mathcal{O}$ un anillo local de una curva algebraica geometricamente irreducible definida sobre un campo finito $k = \mathbb{F}_q$, con campo de funciones racionales K, esto es, $k \subseteq \mathcal{O} \subsetneq K$ con $\mathrm{Frac}(\mathcal{O}) = K$. La clausura entera $\widetilde{\mathcal{O}}$ de $\mathcal{O}$ es un dominio de ideales principales semilocal, cuyos ideales maximales $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ se corresponden biyectivamente con las ramas centradas en $\mathcal{O}$ de la singularidad de la curva. Sea $v_1 = ord_{\mathfrak{p}_1}, \dots, v_m = ord_{\mathfrak{p}_m}$ las correspondientes valuaciones discretas del campo de funciones $K|\mathbb{F}_q$. Para cada $\mathcal{O}$-ideal, digamos

$$\mathfrak{p}^{\mathbf{n}} := \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_m^{n_m} \quad \text{con} \;\; \mathbf{n} := (n_1, \dots, n_m) \in \mathbb{Z}^m$$

definimos su multiexponente como $\mathbf{v}(\mathfrak{p}^{\mathbf{n}}) := \mathbf{n}$. Y para cada función racional no nula $z \in K^*$, sea

$$\mathbf{v}(z) = \mathbf{v}(z\widetilde{\mathcal{O}}) = (v_1(z), \ldots, v_m(z)) \in \mathbb{Z}^m.$$

Sea $\mathbf{t}$ el vector de longitud m cuyas entradas son las variables $t_1, \ldots, t_m$. Abreviamos el **monomio de Laurent**, por

$$\mathbf{t}^{\mathbf{n}} := t_1^{n_1} \cdots t_m^{n_m}, \quad \text{para todo } \mathbf{n} := (n_1, \ldots, n_m) \in \mathbb{Z}^m.$$

Definición 2.2.1. La **Serie de Poincaré Multivariable** asociada a un par de clases de $\mathcal{O}$-ideales $[\mathfrak{a}]$ y $[\mathfrak{b}]$ es definida por la serie de potencias multivariable

$$P(\mathfrak{a}, \mathfrak{b}, \mathbf{t}) := \sum \eta_{\mathbf{n}}(\mathfrak{a}, \mathfrak{b})\mathbf{t}^{\mathbf{n}} \in \mathbb{Z}[|t_1, \ldots, t_m|]$$

cuyos coeficientes son los cardinales

$$\eta_{\mathbf{n}}(\mathfrak{a}, \mathfrak{b}) = \#\{\mathcal{O}\text{-ideales } \mathfrak{d} \;/\; \mathfrak{d} \supseteq \mathfrak{a}, \mathfrak{d} \sim \mathfrak{b} \text{ y } \mathfrak{d} \cdot \widetilde{\mathcal{O}} = \mathfrak{a} \cdot \mathfrak{p}^{-\mathbf{n}}\}$$

donde dos $\mathcal{O}$-ideales $\mathfrak{d}$ y $\mathfrak{b}$ están relacionados $\mathfrak{d} \sim \mathfrak{b}$, si existe $z \in K^*$ tal que $z\mathfrak{d} = \mathfrak{b}$.

En adelante probaremos que dichos cardinales son finitos y que el dominio de convergencia de esta serie multivariable es el polidisco unidad. Esta serie sólo depende de las clases de equivalencia de los $\mathcal{O}$-ideales $[\mathfrak{a}]$ y $[\mathfrak{b}]$, así que la podemos expresar alternativamente como:

$$P(\mathfrak{a}, \mathfrak{b}, \mathbf{t}) = \sum_{\substack{\mathfrak{d} \supseteq \mathfrak{a} \\ \mathfrak{d} \sim \mathfrak{b}}} \mathbf{t}^{\mathbf{v}(\mathfrak{a} \cdot \widetilde{\mathcal{O}}) - \mathbf{v}(\mathfrak{d} \cdot \widetilde{\mathcal{O}})} \tag{2.2.1}$$

Dado que cada $\widetilde{\mathcal{O}}$-ideales es equivalente a el $\mathcal{O}$-ideales $\widetilde{\mathcal{O}}$ y que los $\widetilde{\mathcal{O}}$-ideales que contiene a $\mathfrak{a}$ son exactamente de la forma $\mathfrak{a} \cdot \mathfrak{p}^{-\mathbf{n}}$, donde $\mathbf{n} := (n_1, \ldots, n_m) \in \mathbb{N}^m$, entonces en el caso particular en el cual $\mathfrak{b}$ es simultaneamente un $\mathcal{O}$-ideal y un $\widetilde{\mathcal{O}}$-ideal, entonces

$$\begin{aligned} P(\mathfrak{a}, \mathfrak{b}, \mathbf{t}) &= P(\mathfrak{a}, \widetilde{\mathcal{O}}, \mathbf{t}) \\ &= \sum_{n_1 \ldots n_m = 0}^{\infty} t_1^{n_1} \cdots t_m^{n_m} \\ &= \frac{1}{(1-t_1) \cdots (1-t_m)}. \end{aligned}$$

Notación: Definimos

$$\rho := \dim(\mathcal{O}/\mathfrak{m}_{\mathcal{O}}) < \infty$$

como **el grado del campo residual** de $\mathcal{O}$ sobre el campo de constantes $\mathbb{F}_q$ y por

$$r_i := \dim(\widetilde{\mathcal{O}}/\mathfrak{p}_i) < \infty$$

el **grado del campo residual** de $\widetilde{\mathcal{O}}$ en $\mathfrak{p}_i$ para $i = 1, \ldots, m$. Por el Teorema Chino del Residuo

$$\begin{aligned} \frac{\widetilde{\mathcal{O}}}{\mathfrak{p}^{\mathbf{n}}} &= \frac{\widetilde{\mathcal{O}}}{\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_m^{n_m}} \\ &= \frac{\widetilde{\mathcal{O}}}{\mathfrak{p}_1^{n_1}} \times \cdots \times \frac{\widetilde{\mathcal{O}}}{\mathfrak{p}_m^{n_m}} \end{aligned}$$

y así,

$$\dim(\widetilde{\mathcal{O}}/\mathfrak{p}^{\mathbf{n}}) = \sum_{i=1}^{m} r_i n_i = \mathbf{r} \cdot \mathbf{n}. \tag{2.2.2}$$

El grado de un $\mathcal{O}$-ideal $\mathfrak{d}$, denotado por $\deg(\mathfrak{d})$, es definido por las siguientes propiedades:

1. $\deg(\mathcal{O}) = 0$
2. $\dim(\mathfrak{d}/\mathfrak{a}) = \deg(\mathfrak{d}) - \deg(\mathfrak{a})$, siempre que $\mathfrak{d} \supseteq \mathfrak{a}$.

Sea $\delta = \deg(\widetilde{\mathcal{O}}) = \dim(\widetilde{\mathcal{O}}/\mathcal{O})$ el **grado de singularidad** del anillo $\mathcal{O}$. Entonces por 2.2.2

$$\deg(\mathfrak{p}^{\mathbf{n}}) = \delta - \mathbf{r} \cdot \mathbf{n}.$$

Lema 2.2.2. *Para cada función racional no nula $z \in K^*$ y para cada $\mathcal{O}$-ideal $\mathfrak{a}$ tenemos que*

$$\deg(\mathfrak{a}) - \deg(z\mathfrak{a}) = \sum_{i=1}^{m} r_i v_i(z) = \mathbf{r} \cdot \mathbf{v}(z)$$

y en particular, $\deg(z\mathcal{O}) = -\mathbf{r} \cdot \mathbf{v}(z)$.

Demostración. Sea $\mathfrak{b}$ otro $\mathcal{O}$-ideal y $\mathfrak{d} = \mathfrak{a} \cap \mathfrak{b}$. Dado que la multiplicación por z define un automorfismo de K como k-espacio vectorial, se tiene un isomorfismo de k espacios vectoriales

$$\mathfrak{a}/\mathfrak{d} \cong z\mathfrak{a}/z\mathfrak{d} \ \text{ y } \ \mathfrak{b}/\mathfrak{d} \cong z\mathfrak{b}/z\mathfrak{d}.$$

Por consiguiente,

$$\begin{aligned} \deg(\mathfrak{a}) - \deg(\mathfrak{d}) &= \deg(z\mathfrak{a}) - \deg(z\mathfrak{d}) \\ \deg(\mathfrak{b}) - \deg(\mathfrak{d}) &= \deg(z\mathfrak{b}) - \deg(z\mathfrak{d}), \end{aligned}$$

Restando ambas ecuaciones, tenemos $\deg(\mathfrak{a}) - \deg(z\mathfrak{a}) = \deg(\mathfrak{b}) - \deg(z\mathfrak{b})$, lo cual nos dice que el valor de $\deg(\mathfrak{a}) - \deg(z\mathfrak{a})$ no depende del $\mathcal{O}$-ideal $\mathfrak{a}$. Tomando $\mathfrak{a} = \widetilde{\mathcal{O}}$, por la Ecuación 2.2.2

$$\begin{aligned} \deg(\mathfrak{a}) - \deg(z\mathfrak{a}) &= \deg(\widetilde{\mathcal{O}}) - \deg(z\widetilde{\mathcal{O}}) \\ &= \dim(\widetilde{\mathcal{O}}/z\widetilde{\mathcal{O}}) \\ &= r_1 v_1(z) + \cdots + r_m v_m(z). \end{aligned}$$

□

Ahora daremos una forma alternativa de expresar los coeficientes de la serie de Poincaré $P(\mathfrak{a}, \mathfrak{b}, \mathbf{t})$.

Definición 2.2.3. Sea $\mathfrak{a}$ y $\mathfrak{b}$ $\mathcal{O}$-ideales, definimos el cociente $\mathfrak{b} : \mathfrak{a}$, como el submódulo

$$\mathfrak{b} : \mathfrak{a} = \{z \in K \ / \ z\mathfrak{a} \subseteq \mathfrak{b}\}.$$

Para cada $\mathcal{O}$-ideal $\mathfrak{b}$ consideremos el $\widetilde{\mathcal{O}}$-ideal

$$(\mathfrak{b} : \widetilde{\mathcal{O}}) : \mathfrak{b} = (\mathfrak{b} : \widetilde{\mathcal{O}}) : (\mathfrak{b} \cdot \widetilde{\mathcal{O}}) = (\mathfrak{b} : \widetilde{\mathcal{O}}) \cdot (\mathfrak{b}.\widetilde{\mathcal{O}})^{-1}$$

el cual, es el cociente de $(\mathfrak{b} : \widetilde{\mathcal{O}})$, el $\widetilde{\mathcal{O}}$-ideal más grande contenido en $\mathfrak{b}$, por $\mathfrak{b} \cdot \widetilde{\mathcal{O}}$, el $\widetilde{\mathcal{O}}$-ideal más pequeño que contiene a $\mathfrak{b}$. Este cociente sólo depende de la clase $[\mathfrak{b}]$. Dado que $\widetilde{\mathcal{O}}$ es un dominio de ideales principales, podemos escoger $\mathfrak{b}$ en su clase tal que $\mathfrak{b} \cdot \widetilde{\mathcal{O}} = \widetilde{\mathcal{O}}$.

Lema 2.2.4. *Sea* $\mathfrak{f} = \mathcal{O} : \widetilde{\mathcal{O}}$ *el* $\mathcal{O}$*-ideal conductor, entonces*

$$\mathfrak{f} \subseteq (\mathfrak{b} : \widetilde{\mathcal{O}}) : (\mathfrak{b} \cdot \widetilde{\mathcal{O}}) \subseteq \widetilde{\mathcal{O}}.$$

Demostración. Dado que $(\mathfrak{b} : \widetilde{\mathcal{O}})$ esta contenido en $\mathfrak{b}$ y a su vez $\mathfrak{b}$ esta contenido en $\mathfrak{b} \cdot \widetilde{\mathcal{O}}$, se tiene que $(\mathfrak{b} : \widetilde{\mathcal{O}}) \subseteq \mathfrak{b} \cdot \widetilde{\mathcal{O}}$ y por tanto

$$(\mathfrak{b} : \widetilde{\mathcal{O}}) : (\mathfrak{b} \cdot \widetilde{\mathcal{O}}) \subseteq (\mathfrak{b} \cdot \widetilde{\mathcal{O}}) : (\mathfrak{b} \cdot \widetilde{\mathcal{O}}) \subseteq \widetilde{\mathcal{O}}.$$

Ahora tomando $\mathfrak{b}$ en su clase de equivalencia tal que $\mathfrak{b} \cdot \widetilde{\mathcal{O}} = \widetilde{\mathcal{O}}$, contiene el $\widetilde{\mathcal{O}}$-ideal $\mathfrak{b} \cdot \mathfrak{f}$, así mismo lo hace $\mathfrak{b} : \widetilde{\mathcal{O}}$ y por tanto

$$(\mathfrak{b} : \widetilde{\mathcal{O}}) : (\mathfrak{b} \cdot \widetilde{\mathcal{O}}) \supseteq (\mathfrak{b} \cdot \mathfrak{f}) : \mathfrak{b} \cdot \widetilde{\mathcal{O}}) \supseteq \mathfrak{f}.$$

□

Si $\mathfrak{b} \cdot \widetilde{\mathcal{O}} = \widetilde{\mathcal{O}}$, entonces $\mathfrak{f} \subseteq \mathfrak{b} \subseteq \widetilde{\mathcal{O}}$. Dado que el anillo $\widetilde{\mathcal{O}}/\mathfrak{f}$ es finito, se sigue que el semigrupo de clases de $\mathcal{O}$ es finito (vea [5]). También, deducimos que el índice $(U_{\widetilde{\mathcal{O}}} : U_{\mathfrak{b}})$ del subgrupo de unidades de $\mathfrak{b}$, $U_{\mathfrak{b}}$ en $U_{\widetilde{\mathcal{O}}}$ el subgrupo de unidades de $\widetilde{\mathcal{O}}$ es finito. En realidad, los finitos $\mathcal{O}$-ideales $\mathfrak{d}$ que satisfacen $\mathfrak{d} \cdot \widetilde{\mathcal{O}} = \widetilde{\mathcal{O}}$ y $\mathfrak{d} \sim \mathfrak{b}$ son justamente de la forma $z^{-1}\mathfrak{b}$ donde $z \in U_{\widetilde{\mathcal{O}}}$ es únicamente determinado módulo $U_{\mathfrak{b}}$, siempre que se tenga $\mathfrak{b} \cdot \widetilde{\mathcal{O}} = \widetilde{\mathcal{O}}$. Sea

$$\mathbf{b} = (b_1, \ldots, b_m) := \mathbf{v}((\mathfrak{b} : \widetilde{\mathcal{O}}) : \mathfrak{b}) = \mathbf{v}(\mathfrak{b} : \widetilde{\mathcal{O}}) - \mathbf{v}(\mathfrak{b})$$

el multiexponete de $(\mathfrak{b} : \widetilde{\mathcal{O}}) : \mathfrak{b}$. Por el lema anterior tenemos que

$$\mathbf{0} := (0, \ldots, 0) \leq \mathbf{b} \leq \mathbf{f} := \mathbf{v}(\mathfrak{f})$$

donde $\leq$ es el orden parcial en el producto $\mathbb{Z}^m$. Si $\mathfrak{b} \cdot \widetilde{\mathcal{O}} = \widetilde{\mathcal{O}}$, entonces $(\mathfrak{b} : \widetilde{\mathcal{O}}) : \mathfrak{b}$ es el $\widetilde{\mathcal{O}}$-ideal más grande contenido en $\mathfrak{b}$, y $\mathbf{b}$ es el vector más pequeño en el orden parcial de $\mathbb{Z}^m$ tal que $\mathfrak{p}^{\mathbf{b}} \subseteq \mathfrak{b}$. El vector $\mathbf{b}$ y el conjunto

$$S(\mathfrak{b}) := \{\mathbf{v}(z) - \mathbf{v}(\mathfrak{b} \cdot \widetilde{\mathcal{O}}) \ / \ z \in \mathfrak{b}, z \neq 0\}$$

sólo dependen de la clase del ideal $\mathfrak{b}$. Es claro que

$$\mathbf{b} + \mathbb{N}^m \subseteq S(\mathfrak{b}) \subseteq \mathbb{N}^m$$

y $S(\mathcal{O}) + S(\mathbf{b}) \subseteq S(\mathbf{b})$. En particular, $S(\mathcal{O})$ es un semigrupo intermedio entre $\mathbf{f} + \mathbb{N}^m$ y $\mathbb{N}^m$, llamado el **semigrupo asociado** al anillo local $\mathcal{O}$.

Para cada $\mathbf{b}$ y para cada $\mathbf{n} \in \mathbb{Z}^m$, definimos

$$\mathfrak{b}_{\mathbf{n}} := \{z \in \mathfrak{b} \ / \ \mathbf{v}(z) = \mathbf{n}\}.$$

Teorema 2.2.5. *La serie de Poincaré multivariable $P(\mathfrak{a}, \mathfrak{b}, \mathbf{t})$ tiene coeficientes*

$$\eta_{\mathbf{n}}(\mathfrak{a}, \mathfrak{b}) = \frac{\#((\mathfrak{b} : \mathfrak{a})_{\mathbf{j}}/U_{\mathcal{O}})}{(U_{\mathfrak{b}} : U_{\mathcal{O}})}$$

donde $\mathbf{j} = \mathbf{n} - \mathbf{v}(\mathfrak{a} \cdot \widetilde{\mathcal{O}}) + \mathbf{v}(\mathfrak{b} \cdot \widetilde{\mathcal{O}})$*. Además,*

1. $\eta_{\mathbf{n}}(\mathcal{O}, \mathfrak{b}) > 0$*, sí, y solo si* $n \in S(\mathfrak{b})$

2. $0 \leq \eta_{\mathbf{n}}(\mathfrak{a}, \mathfrak{b}) \leq (U_{\widetilde{\mathcal{O}}} : U_{\mathfrak{b}})$ *para todo* n

3. $\mathbf{b}$ *es el vector más pequeño en el orden parcial de* $\mathbb{N}^m$ *con la propiedad:*

$$\textit{Si} \quad \mathbf{n} \geq \mathbf{b} \quad \textit{entonces} \quad \eta_{\mathbf{n}}(\mathfrak{a}, \mathfrak{b}) = (U_{\widetilde{\mathcal{O}}} : U_{\mathfrak{b}}).$$

Demostración. Al reescribir la serie como

$$P(\mathfrak{a}, \mathfrak{b}, \mathbf{t}) = \sum_{z \in (\mathfrak{b}:\mathfrak{a}) \setminus 0/U_{\mathfrak{b}}} \mathbf{t}^{\mathbf{v}(\mathfrak{a}\cdot\widetilde{\mathcal{O}}) - \mathbf{v}(\mathfrak{b}\cdot\widetilde{\mathcal{O}}) + \mathbf{v}(z)}$$

donde $U_{\mathfrak{b}} = \{z \in K^* \ / \ z\mathfrak{b} = \mathfrak{b}\}$ y $(\mathfrak{b} : \mathfrak{a}) \setminus 0/U_{\mathfrak{b}}$ denota el cociente de $(\mathfrak{b} : \mathfrak{a}) \setminus 0$ por la acción del grupo $U_{\mathfrak{b}}$. Vemos que

$$P(\mathfrak{a}, \mathfrak{b}, \mathbf{t}) = \sum_{j \in \mathbb{Z}^m} \#((\mathfrak{b} : \mathfrak{a})_{\mathbf{j}}/U_{\mathfrak{b}}) \mathbf{t}^{\mathbf{v}(\mathfrak{a}\cdot\widetilde{\mathcal{O}}) - \mathbf{v}(\mathfrak{b}\cdot\widetilde{\mathcal{O}}) + \mathbf{j}},$$

es decir, $\eta_{\mathbf{n}}(\mathfrak{a}, \mathfrak{b}) = \#((\mathfrak{b} : \mathfrak{a})_{\mathbf{j}}/U_{\mathfrak{b}})$ donde $\mathbf{n} = \mathbf{v}(\mathfrak{a} \cdot \widetilde{\mathcal{O}}) - \mathbf{v}(\mathfrak{b} \cdot \widetilde{\mathcal{O}}) + \mathbf{j}$. Dado que

$$\#((\mathfrak{b} : \mathfrak{a})_{\mathbf{j}}/U_{\mathcal{O}}) = \#((\mathfrak{b} : \mathfrak{a})_{\mathbf{j}}/U_{\mathfrak{b}})(U_{\mathfrak{b}} : U_{\mathcal{O}})$$

tenemos la expresión deseada para $\eta_{\mathbf{n}}$. Ahora bien, los coeficientes $\eta_{\mathbf{n}}(\mathfrak{a}, \mathfrak{b}) > 0$, sii, $\mathfrak{b}_{\mathbf{n}+\mathbf{v}(\mathfrak{b}\cdot\widetilde{\mathcal{O}})}$ es no vacio, esto es, $\mathbf{n} \in S(\mathfrak{b})$. Para probar las dos afirmaciones restantes, asumiremos sin perdida de generalidad que $\mathfrak{a}\cdot\widetilde{\mathcal{O}} = \mathfrak{b}\cdot\widetilde{\mathcal{O}} = \widetilde{\mathcal{O}}$ y por consiguiente, tenemos que $(\mathfrak{b}:\mathfrak{b}) \subseteq \widetilde{\mathcal{O}}$, $\mathfrak{b}:\widetilde{\mathcal{O}} = \mathfrak{p}^{\mathbf{b}}$ y

$$\eta_{\mathbf{n}}(\mathfrak{a},\mathfrak{b}) = \#((\mathfrak{b}:\mathfrak{a})_{\mathbf{n}}/U_{\mathfrak{b}}) \leq \#(\widetilde{\mathcal{O}}_{\mathbf{n}}/U_{\mathfrak{b}}) = (U_{\widetilde{\mathcal{O}}} : U_{\mathfrak{b}})$$

para cada $\mathbf{n} \in \mathbb{N}^m$. La igualdad ocurre, sii, $(\mathfrak{b}:\mathfrak{a})_{\mathbf{n}} = \widetilde{\mathcal{O}}_{\mathbf{n}}$, es decir, $\widetilde{\mathcal{O}}_{\mathbf{n}} \subseteq \mathfrak{b}:\mathfrak{a}$. Luego esto ocurre para todo $\mathbf{n}$ y para cualquier vector más grande, sii, $\mathfrak{p}^{\mathbf{n}} \subseteq \mathfrak{b}:\mathfrak{a}$, es decir, $\mathfrak{a}\cdot\mathfrak{b}^{\mathbf{n}} \subseteq \mathfrak{b}$, lo que equivale a $\mathfrak{p}^{\mathbf{n}} \subseteq \mathfrak{b}$ ya que $\mathfrak{a}\cdot\widetilde{\mathcal{O}} = \widetilde{\mathcal{O}}$, lo que finalmente nos dice que $\mathfrak{p}^{\mathbf{n}} \subseteq \mathfrak{b}:\widetilde{\mathcal{O}}$, es decir $\mathbf{n} \geq \mathbf{b}$. □

En particular, este teorema nos dice que nuestra serie en realidad esta bien definida y dado que desde cierto vector en adelante todos los coeficientes de la serie son constantes, tenemos una serie geométrica lo que nos lleva a concluir que el dominio de convergencia de la serie de Poincaré Multivariable es el polidisco unidad, esto es, $|t_1| < 1, \ldots, |t_m| < 1$.

2.3. Representación Integral

En sección daremos una representación integral de la Serie de Poincaré, para esto debemos considerar un espacio en el cual podamos hallar una medida útil (vea A.2.5). Sea

$$\mathcal{R} := \prod_{i=1}^{m} \widehat{K}_{v_i}$$

el anillo de fracciones de la completación de $\widehat{\mathcal{O}}$ del anillo local $\mathcal{O}$. Sea $U_{\mathcal{R}} := \prod_{i=1}^{m} \widehat{K}_{v_i}^*$ su grupo de unidades. La asignación que a cada $\mathcal{O}$-ideal $\mathfrak{a}$ le asigna el $\widehat{\mathcal{O}}$-ideal $\widehat{\mathfrak{a}} := \mathfrak{a}\cdot\widehat{\mathcal{O}}$, $\mathfrak{a} \longmapsto \widehat{\mathfrak{a}} := \mathfrak{a}\cdot\widehat{\mathcal{O}}$, define una correspondencia inyectiva y monotona la cual preserva el grado entre los $\mathcal{O}$-ideales y los $\widehat{\mathcal{O}}$-ideales, el morfismo inverso está dado por $\widehat{\mathfrak{a}} \longmapsto \widehat{\mathfrak{a}} \cap K$. Dos $\mathcal{O}$-ideales $\mathfrak{a}$, $\mathfrak{b}$ son equivalentes, sí y solo si, los correspondientes $\widehat{\mathcal{O}}$-ideales $\widehat{\mathfrak{a}}$, $\widehat{\mathfrak{b}}$ son equivalentes, esto es; $\mathfrak{a} = z\mathfrak{b}$ para algún $z \in K^*$, sii, $\widehat{\mathfrak{a}} = z\widehat{\mathfrak{b}}$ para algún $z \in U_{\mathcal{R}}$ (vea [5] sección 3)

Lema 2.3.1. *Sea $\mathfrak{a}$ y $\mathfrak{b}$ $\mathcal{O}$-ideales, entonces*

$$\widehat{\mathfrak{b}:\mathfrak{a}} = \widehat{\mathfrak{b}}:\widehat{\mathfrak{a}}$$

Demostración. Sea $z \in \mathfrak{b} : \mathfrak{a}$, entonces por definición $z\mathfrak{a} \subseteq \mathfrak{b}$, de ahí que por continuidad $z\widehat{\mathfrak{a}} \subseteq \widehat{\mathfrak{b}}$, esto nos dice que $z \in \widehat{\mathfrak{b}} : \widehat{\mathfrak{a}}$, por tanto $\mathfrak{b} : \mathfrak{a} \subseteq \widehat{\mathfrak{b}} : \widehat{\mathfrak{a}}$, lo cual implica que $\widehat{\mathfrak{b} : \mathfrak{a}} \subseteq \widehat{\mathfrak{b}} : \widehat{\mathfrak{a}}$.

Dado que $\widehat{\mathfrak{b} : \mathfrak{a}} \cap K = \mathfrak{b} : \mathfrak{a}$, es sufienciente mostrar que $(\widehat{\mathfrak{b}} : \widehat{\mathfrak{a}}) \cap K \subseteq \mathfrak{b} : \mathfrak{a}$. Sea $z \in K$ tal que $z\widehat{\mathfrak{a}} \subseteq \widehat{\mathfrak{b}}$, entonces $z\mathfrak{a} = z\widehat{\mathfrak{a}} \cap K \subseteq z\widehat{\mathfrak{b}} \cap K = \mathfrak{b}$ y por consiguiente $z \in \mathfrak{b} : \mathfrak{a}$. □

El homomorfismo $\mathbf{v} : K^* \longrightarrow \mathbb{Z}^m$ se extiende naturalmente al homomorfismo de grupos $\mathbf{v} : U_{\mathcal{R}} \longrightarrow \mathbb{Z}^m$ que envia cada elemento $z = (z_1, \ldots, z_m)$ de $U_{\mathcal{R}}$ al vector $\mathbf{v}(z) := (\widehat{v}_1(z), \ldots, \widehat{v}_m(z))$, donde $\widehat{v}_i$ es la valuación en $\widehat{K}_{v_i}$ que extiende a v_i.

Teorema 2.3.2. *$\mathcal{R}$ es un grupo topológico localmente compacto.*

Demostración. Veamos en principio que en realidad $\mathcal{R}$ es el anillo de fraciones de $\mathcal{O}$, es decir,

$$\mathrm{Frac}(\widehat{\mathcal{O}}) \cong \prod_{i=1}^{m} \widehat{K}_{v_i}.$$

Es claro que $\mathrm{Frac}(\mathcal{O}) = \mathrm{Frac}(\widetilde{\mathcal{O}})$, de donde se sigue que

$$\begin{aligned} \mathrm{Frac}(\widehat{\mathcal{O}}) &= \mathrm{Frac}(\widehat{\widetilde{\mathcal{O}}}) \\ &\cong \mathrm{Frac}(\widehat{\mathcal{O}}_{Q_1} \times \cdots \times \widehat{\mathcal{O}}_{Q_m}) \\ &\cong \mathrm{Frac}(\widehat{\mathcal{O}}_{Q_1}) \times \cdots \times \mathrm{Frac}(\widehat{\mathcal{O}}_{Q_m}) \\ &\cong \widehat{K}_{v_1} \times \cdots \times \widehat{K}_{v_m} \end{aligned}$$

Que $\mathcal{R}$ es un grupo topológico se sigue del hecho que su topología esta dada por una norma. Ahora dado que $\mathcal{R}$ es el producto finito de los $\widehat{K}_{v_i}$ con $i = 1, \ldots, m$, basta ver que cada $\widehat{K}_{v_i}$ es localmente compacto. Por el teorema estructural de Cohen, tenemos que cada $\widehat{\mathcal{O}}_{Q_i} \cong k_i[|t_i|]$ donde $k_i = \widetilde{\mathcal{O}}/\mathfrak{p}_i$, de ahí que

$$\begin{aligned} \widehat{K}_{v_i} &= \mathrm{Frac}(\widehat{\mathcal{O}}_{Q_i}) \\ &\cong \mathrm{Frac}(k_i[|t_i|]) \\ &\cong k_i((t_i)) \end{aligned}$$

donde $k_i((t_i))$ denotan las series de Laurent en la variable t_i con campo de constantes k_i. Dado que k_i es una extensión finita de $\mathbb{F}_q$, $k_i \cong \mathbb{F}_{q^{r_i}}$, k_i es compacto, además, sabemos que si k es un campo localmente compacto, entonces un producto de espacio vectoriales sobre k, es localmente compacto, sí y solo si, casi todos son espacios compacto. Así $k_i((t_i)) \cong \prod_{\mathbb{Z}} k_i$ es localmente compacto y por tanto $\widehat{K}_{v_i}$ también lo es. $\square$

Del teorema anterior $\mathcal{R}$ es un grupo topológico aditivo, el cual es una $\mathbb{F}_q$-álgebra localmente compacta. Por el teorema de Haar (vea A.2.5) existe una única medida de Haar $\widehat{\mu}$ sobre $\mathcal{R}$, normalizada tal que $\widehat{\mu}(\widehat{\mathcal{O}}) = 1$. Ahora bien, si $\mathfrak{a} \subseteq \mathfrak{b}$ son $\mathcal{O}$-ideales, entonces el $\widehat{\mathcal{O}}$-ideal $\widehat{\mathfrak{b}}$ es una unión disjunta de clases laterales de $\widehat{\mathfrak{a}}$, esto es, $\widehat{\mathfrak{b}} = \bigcup_{z\in\widehat{\mathfrak{b}}/\widehat{\mathfrak{a}}} z + \widehat{\mathfrak{a}}$ y dado que $\widehat{\mathfrak{b}}/\widehat{\mathfrak{a}}$ es una $\mathbb{F}_q$-álgebra de dimensión finita,

$$\begin{aligned}
\widehat{\mu}(\widehat{\mathfrak{b}}) &= \widehat{\mu}(\bigcup_{z\in\widehat{\mathfrak{b}}/\widehat{\mathfrak{a}}} z + \widehat{\mathfrak{a}}) \\
&= \#(\widehat{\mathfrak{b}}/\widehat{\mathfrak{a}})\widehat{\mu}(\widehat{\mathfrak{a}}) \\
&= q^{\dim(\widehat{\mathfrak{b}}/\widehat{\mathfrak{a}})}\widehat{\mu}(\widehat{\mathfrak{a}}) \\
&= q^{\dim(\mathfrak{b}/\mathfrak{a})}\widehat{\mu}(\widehat{\mathfrak{a}}).
\end{aligned}$$

Luego, dado que la normalización es $\widehat{\mu}(\widehat{\mathcal{O}}) = 1$, tenemos que $\widehat{\mu}(\widehat{\mathfrak{b}}) = q^{\deg(\mathfrak{b})}$, para todo $\mathcal{O}$-ideal $\mathfrak{b}$. En particular, $\widehat{\mu}(\widehat{\overline{\mathcal{O}}}) = q^{\delta}$. Además, dado que el grupo de unidades $U_{\widehat{\mathcal{O}}}$ del anillo local $\widehat{\mathcal{O}}$ es el complemento del ideal maximal $\widehat{\mathfrak{m}}$ de $\widehat{\mathcal{O}}$, concluimos que

$$\begin{aligned}
\widehat{\mu}(U_{\widehat{\mathcal{O}}}) &= \widehat{\mu}(\widehat{\mathcal{O}} \setminus \widehat{\mathfrak{m}}) \\
&= 1 - \widehat{\mu}(\widehat{\mathfrak{m}}) \\
&= 1 - q^{-\rho}.
\end{aligned}$$

Además, por el lema 2.2.2 se sigue que, para toda $z \in K^*$, $\widehat{\mu}(z\widehat{\mathcal{O}}) = q^{-\mathbf{r}\cdot\mathbf{v}(z)}$ y aun más para cada $z \in U_{\mathcal{R}}$. Ahora por la unicidad de la medida de Haar, tenemos que

$$\widehat{\mu}(zM) = q^{-\mathbf{r}\cdot\mathbf{v}(z)}\widehat{\mu}(M)$$

para todo $z \in U_{\mathcal{R}}$ y para todo conjunto medible M.

Sea $h : \mathbb{Z}^m \longrightarrow \mathbb{C}$ una función. Definimos

$$\widehat{\mathfrak{b}}_{\mathrm{reg}} = \widehat{\mathfrak{b}} \cap U_{\mathcal{R}}$$

dado que $\widehat{\mathfrak{b}}_{\mathrm{reg}}$ es la unión disjunta de los conjuntos $\widehat{\mathfrak{b}}_{\mathbf{n}} = \{z \in \widehat{\mathfrak{b}} \ / \ \mathbf{v}(z) = \mathbf{n}\}$, y dado que $\mathbf{v}(z)$ asume sobre $\widehat{\mathfrak{b}}_{\mathbf{n}}$ el valor constante $\mathbf{n}$, tenemos que:

$$\begin{aligned}\int\limits_{\widehat{\mathfrak{b}}_{\mathrm{reg}}} h(\mathbf{v}(z))\mathbf{t}^{\mathbf{v}(z)}\, d\widehat{\mu}(z) &= \sum_{\mathbf{n}\in\mathbb{Z}^m} \int\limits_{\widehat{\mathfrak{b}}_{\mathbf{n}}} h(\mathbf{v}(z))\mathbf{t}^{\mathbf{v}(z)}\, d\widehat{\mu}(z) \\ &= \sum_{\mathbf{n}\in\mathbb{Z}^m} h(\mathbf{n})\mathbf{t}^{\mathbf{n}}\widehat{\mu}(\widehat{\mathfrak{b}}_{\mathbf{n}}) \in \mathbb{C}[|t_1,\ldots,t_m|]\mathbf{t}^{\mathfrak{b}\cdot\widehat{\mathcal{O}}}\end{aligned}$$

en el dominio de convergencia absoluta de la serie de Laurent formal al lado derecho. Aún si el dominio de convergencia es vacío, la serie de Laurent formal aún puede ser interpretada como alguna clase de integral en el espiritu de la integración motivica (vea [11]).

Dado que $\widehat{\mathfrak{b}}_{\mathbf{n}}$ es la unión disjunta de clases $zU_{\widehat{\mathcal{O}}}$, donde z varía sobre un sistema completo de representantes del cociente $\widehat{\mathfrak{b}}_{\mathbf{n}}/U_{\widehat{\mathcal{O}}}$ y dado que cada una de estas clases tiene medida

$$\widehat{\mu}(zU_{\widehat{\mathcal{O}}}) = q^{-\mathbf{r}\cdot\mathbf{v}(z)}\widehat{\mu}(U_{\widehat{\mathcal{O}}}) = q^{-\mathbf{r}\cdot\mathbf{v}(z)}(1-q^{-\rho})$$

obtenemos

$$\widehat{\mu}(\widehat{\mathfrak{b}}_{\mathbf{n}}) = \#(\mathfrak{b}_{\mathbf{n}}/U_{\mathcal{O}})q^{-\mathbf{r}\cdot\mathbf{n}}(1-q^{-\rho}).$$

De ahí que

$$\int\limits_{\widehat{\mathfrak{b}}_{\mathrm{reg}}} h(\mathbf{v}(z))\mathbf{t}^{\mathbf{v}(z)}\, d\widehat{\mu}(z) = (1-q^{-\rho})\sum_{\mathbf{n}\in\mathbb{Z}^m} \#(\mathfrak{b}_{\mathbf{n}}/U_{\mathcal{O}})h(\mathbf{n})q^{-\mathbf{r}\cdot\mathbf{n}}\mathbf{t}^{\mathbf{n}}.$$

En el cado particular que $h(\mathbf{n}) = q^{\mathbf{r}\cdot\mathbf{n}}$,tenemos que

$$(1-q^{-\rho})\sum_{\mathbf{n}\in\mathbb{Z}^m} \#(\mathfrak{b}_{\mathbf{n}}/U_{\mathcal{O}})\mathbf{t}^{\mathbf{n}} = \int\limits_{\widehat{\mathfrak{b}}_{\mathrm{reg}}} q^{\mathbf{r}\cdot\mathbf{v}(z)}\mathbf{t}^{\mathbf{v}(z)}\, d\widehat{\mu}(z). \tag{2.3.1}$$

Teorema 2.3.3 (Rerensetación Integral de la serie de Poincaré.)**.**

$$P(\mathfrak{a},\mathfrak{b},\mathbf{t}) = \frac{q^{\rho}}{(U_{\mathfrak{b}}:U_{\mathcal{O}})(q^{\rho}-1)}\mathbf{t}^{\mathbf{v}(\mathfrak{a}\cdot\widetilde{\mathcal{O}})-\mathbf{v}(\mathfrak{b}\cdot\widetilde{\mathcal{O}})} \int\limits_{(\widehat{\mathfrak{b}}:\widehat{\mathfrak{a}})_{reg}} q^{\mathbf{r}\cdot\mathbf{v}(z)}\mathbf{t}^{\mathbf{v}(z)}\, d\widehat{\mu}(z).$$

en el polidisco unidad $|t_1| < 1, \ldots, |t_m| < 1$.

Demostración. Por el Teorema 2.2.5, los coeficientes de la serie de Poincaré multivariable, son tales que

$$\eta_{\mathbf{n}}(\mathfrak{a},\mathfrak{b}) = \frac{\#((\mathfrak{b}:\mathfrak{a})_{\mathbf{j}}/U_{\mathcal{O}})}{(U_{\mathfrak{b}}:U_{\mathcal{O}})}$$

donde $\mathbf{j} = \mathbf{n} - \mathbf{v}(\mathfrak{a}\cdot\widetilde{\mathcal{O}}) + \mathbf{v}(\mathfrak{b}\cdot\widetilde{\mathcal{O}})$. Reemplazando en la ecuación 2.3 $\widehat{\mathfrak{b}}_{\mathrm{reg}}$ por $\widehat{(\mathfrak{b}:\mathfrak{a})}_{\mathrm{reg}} = (\widehat{\mathfrak{b}}:\widehat{\mathfrak{a}})_{\mathrm{reg}}$, obtenemos:

$$\begin{aligned}
P(\mathfrak{a},\mathfrak{b},\mathbf{t}) &= \sum_{\mathbf{n}\in\mathbb{Z}^m} \eta_{\mathbf{n}}(\mathfrak{a},\mathfrak{b})\mathbf{t}^{\mathbf{n}} \\
&= \sum_{\mathbf{n}\in\mathbb{Z}^m} \frac{\#((\mathfrak{b}:\mathfrak{a})_{\mathbf{j}}/U_{\mathcal{O}})}{(U_{\mathfrak{b}}:U_{\mathcal{O}})}\mathbf{t}^{\mathbf{n}} \\
&= \frac{\mathbf{t}^{\mathbf{v}(\mathfrak{a}\cdot\widetilde{\mathcal{O}})-\mathbf{v}(\mathfrak{b}\cdot\widetilde{\mathcal{O}})}}{(U_{\mathfrak{b}}:U_{\mathcal{O}})} \sum_{\mathbf{n}\in\mathbb{Z}^m} \#((\mathfrak{b}:\mathfrak{a})_{\mathbf{j}}/U_{\mathcal{O}})\mathbf{t}^{\mathbf{j}} \\
&= \frac{\mathbf{t}^{\mathbf{v}(\mathfrak{a}\cdot\widetilde{\mathcal{O}})-\mathbf{v}(\mathfrak{b}\cdot\widetilde{\mathcal{O}})}}{(U_{\mathfrak{b}}:U_{\mathcal{O}})} \frac{1}{(1-q^{-\rho})} \int_{\widehat{(\mathfrak{b}:\mathfrak{a})}_{\mathrm{reg}}} q^{\mathbf{r}\cdot\mathbf{v}(z)}\mathbf{t}^{\mathbf{v}(z)}\, d\widehat{\mu}(z) \\
&= \frac{q^{\rho}}{(U_{\mathfrak{b}}:U_{\mathcal{O}})(q^{\rho}-1)} \mathbf{t}^{\mathbf{v}(\mathfrak{a}\cdot\widetilde{\mathcal{O}})-\mathbf{v}(\mathfrak{b}\cdot\widetilde{\mathcal{O}})} \int_{(\widehat{\mathfrak{b}}:\widehat{\mathfrak{a}})_{\mathrm{reg}}} q^{\mathbf{r}\cdot\mathbf{v}(z)}\mathbf{t}^{\mathbf{v}(z)}\, d\widehat{\mu}(z)
\end{aligned}$$

□

Capítulo 3

Conclusiones

3.1. Series de Poincaré sobre $\mathbb{Q}_p$

Como vimos en el Capítulo 2, la serie de Poincaré multivariable de singularidades de curvas definidas sobre el campo de constantes $\mathbb{F}_q$, puede ser representado como una integral:

$$P(\mathfrak{a}, \mathfrak{b}, \mathbf{t}) = \frac{q^\rho}{(U_\mathfrak{b} : U_\mathcal{O})(q^\rho - 1)} \mathbf{t}^{\mathbf{v}(\mathfrak{a}\cdot\widetilde{\mathcal{O}}) - \mathbf{v}(\mathfrak{b}\cdot\widetilde{\mathcal{O}})} \int\limits_{(\widehat{\mathfrak{b}}:\widehat{\mathfrak{a}})_{\mathrm{reg}}} q^{\mathbf{r}\cdot\mathbf{v}(z)} \mathbf{t}^{\mathbf{v}(z)} \, d\widehat{\mu}(z).$$

donde $\widehat{\mu}$ es la medida de Haar sobre $\mathcal{R} := \prod_{i=1}^{m} \widehat{K}_{v_i}$ normalizada tal que $\widehat{\mu}(\widehat{\mathcal{O}}) = 1$. El principal propósito de este trabajo era dar una definición de serie de Poincaré multivariable de singularidades de curvas definidas sobre el campo de los números p-ádicos, $\mathbb{Q}_p$, a través de una posible representación integral. Vimos en la Sección 2.1, que dado un campo de constantes cualquiera k y un cuerpo de funciones en una variable K sobre k, para un anillo local $\mathcal{O}$ propiamente contenido en K tal que $\mathrm{Frac}(\mathcal{O}) = K$, tenemos que

$$\widehat{\widetilde{\mathcal{O}}} \cong k_1[|t_1|] \times \cdots \times k_m[|t_m|]$$

donde $k_i = \widetilde{\mathcal{O}}/\mathfrak{p}_i$ es el campo residual de $\widetilde{\mathcal{O}}$ respecto al ideal maximal $\mathfrak{p}_i$. Al definir $\mathcal{R} := \prod_{i=1}^{m} \widehat{K}_{v_i}$, tenemos que $\mathcal{R} \cong \mathrm{Frac}(\widehat{\widetilde{\mathcal{O}}})$. En particular, que tomando $k = \mathbb{F}_q$, $\mathcal{R}$ es un grupo topológico localmente compacto lo cual nos permite usar el Teorema A.2.5 para obtener una medida de Haar sobre $\mathcal{R}$.

Al tratar de simular dichas ideas tomando $k = \mathbb{Q}_p$ encontramos que $\mathcal{R}$ no es localmente compacto ya que cada $\widehat{K}_{v_i}$ es homeomorfo al producto infinito contable $\prod k_i$ donde $k_i = \widetilde{\mathcal{O}}/\mathfrak{p}_i$ es una extensión finita de $\mathbb{Q}_p$. Lo cual implica que k_i es localmente compacto, pero el producto $\prod k_i$ **NO** lo es. Lo anterior debido a que existe un número infinito de factores, los cuales no son compactos. Al no tener la propiedad de localmente compacto, no podemos usar el Teorema A.2.5 para obtener una medida de Haar en $\mathcal{R}$ para anillos locales definidos sobre $\mathbb{Q}_p$.

Otra posible complicación es: la completacion algebraica de $\mathbb{Q}_p$ denotada por $\mathbb{Q}_p^{alg}$, no es localmente compacta, más aún, no es completo respecto a la topología inducida por $\mathbb{Q}_p$.

Conclusiones y posibles desarrollos consecuentes

1. La definición de serie de Poincaré multivariable de singularidades de curvas definidas sobre $\mathbb{Q}_p$ no es posible a partir de una representación integral como en el caso de $\mathbb{F}_q$.

2. La clausura algebraica $\mathbb{Q}_p^{alg}$, de $\mathbb{Q}_p$, la completación topológica $\mathbb{C}_p$, de $\mathbb{Q}_p^{alg}$, y el campo de fracciones $\mathcal{R}$, de $\widehat{\mathcal{O}}$, son grupos topológicos, los cuales, **no** son localmente compactos, lo cual imposibilita usar el Teorema A.2.5 para obtener una medida de Haar sobre dichos espacios.

Preguntas abiertas y desafíos que esta tesis deja son:

- ¿Podemos hallar una medida de Haar sobre algunos de los campos $\mathbb{Q}_p^{alg}$, $\mathbb{C}_p$ y $\mathcal{R}$? Aún más, la siguiente pregunta en el área de la teoría de la medida, ¿Cuales son las condiciones necesarias y suficientes sobre un grupo topológico para poder definir una medida de Haar sobre él?. Ambas preguntas son de gran importancia, dado que el estudio de la estructura analítica y algebraica de $\mathbb{Q}_p$ y sus extensiones tiene grandes aplicaciones físicas y matemáticas (vea [9], [16], [2], [17]). Y dado el gran número de espacios topológicos que no son localmente compactos, definidos en áreas como geometría algebraica y diferencial. Hace falta una herramienta que nos permita decidir la existencia o no de una medida "útil" sobre dichos espacios.

- Otra pregunta es, ¿Existe un análogo de la Serie de Poincaré Multivariable de singularidades de curvas $P(\mathfrak{a}, \mathfrak{b}, \mathfrak{t})$, definida por Karl Otto Stöhr sobre el campo de los números p-ádicos?

  Otra definiciones de series de Poincaré similares están dadas por Zúñiga en [12], [25]. En dónde integramos sobre $\mathbb{Q}_p$ o sobre alguna extensión finita de $\mathbb{Q}_p$ y se toman anillos locales $\mathcal{O}$ los cuales están entre $\mathbb{Q}_p$ y extensiones finitas K de $\mathbb{Q}_p$, además de tomar $\mathcal{O}$-ideales triviales.

Veamos una de las posibles definiciones de serie de Poincaré multivariable dada en [12], la cual se fundamenta en la teoría de la integración motivica.

Integración respecto a la característica de Euler generalizada.

Sea k un campo de constantes. Empecemos denotando por Var_k la categoría de las variedades algebraicas sobre k y por $K_0(\mathrm{Var}_k)$ **el anillo de Grothendieck** correspondiente a Var_k, esto es, el cociente del grupo abeliano libre por las clases de isomorfismo $[X]$ de una variedad algebraica sobre k, con las siguientes relaciones:

- $[X] = [Y]$ si X es isomorfa a Y, para $X, Y \in \mathrm{Var}_k$
- $[X] - [Z] = [X \setminus Z]$ si Z es un subconjunto cerrado Zariski en X
- $[X \times_k Y] = [X][Y]$, para $X, Y \in \mathrm{Var}_k$

donde $X \times_k Y$ denota el producto fibrado de X y Y. Denotemos por $\mathbb{L} = [\mathbb{A}_k^1]$ y $\mathbb{1} = [x]$ la clase de equivalencia de un punto. Definimos $\mathcal{M}_k := K_0(\mathrm{Var}_k)[\mathbb{L}^{-1}]$ como el anillo obtenido por la localización de $K_0(\mathrm{Var}_k)$ con respecto al sistema multiplicativo $\{\mathbb{1}, \mathbb{L}^1, \mathbb{L}^2, \mathbb{L}^3, \ldots\}$.

Asociado al anillo local $\mathcal{O}$ (vea la sección 2.2) se define el conjunto de $\mathbf{n}-jets$ como

$$\mathcal{J}_{\widetilde{\mathcal{O}}}^{\mathbf{n}} := \widetilde{\mathcal{O}}/\mathbf{t}^{\mathbf{n+1}}\widetilde{\mathcal{O}} \cong k^{\|\mathbf{n+1}\|},$$

donde $\mathbf{n} := (n_1, \ldots, n_m) \in \mathbb{N}^m, \mathbf{1} := (1, \ldots, 1)$, $\|\mathbf{n}+\mathbf{1}\| = (\mathbf{n}+\mathbf{1}) \cdot \mathbf{1}$ y $\mathbf{t} := (t_1, \ldots, t_m)$ con los t_i's son uniformizantes locales de las valuaciones por encima de $\mathcal{O}$. La proyección canónica $\widetilde{\mathcal{O}} \longrightarrow \widetilde{\mathcal{O}}/\mathbf{t}^{\mathbf{n+1}}\widetilde{\mathcal{O}}$ es denotada por $\pi_{\mathbf{n}}$.

En estos términos, un subconjunto X de $\widetilde{\mathcal{O}}$ se dice **cilíndrico** si $X = \pi_{\mathbf{n}}^{-1}(Y)$ para algún subconjunto constructible Y de $\mathcal{J}_{\widetilde{\mathcal{O}}}^{\mathbf{n}}$, *i.e.*, Y es una unión finita disjunta de subespacios localmente cerrados.

La característica de Euler generalizada (o medida motivica) de un subconjunto cilíndrico $X \subseteq \mathcal{O}$, $X = \pi_{\mathbf{n}}^{-1}(Y)$, con $Y \subseteq \mathcal{J}_{\widetilde{\mathcal{O}}}^{\mathbf{n}}$ constructible, es:

$$\chi_g(X) := [Y]\mathbb{L}^{-\|\mathbf{n+1}\|} \in \mathcal{M}_k$$

la cual esta bien definida. Esta definición la extendemos a cualquier subconjunto de $X \subseteq K$, esto es, X es llamado **cilíndrico** si existe un elemento $z \in \mathcal{O}$ no divisor del cero tal que el conjunto zX es un subconjunto de $\mathcal{O}$ y es cilíndrico, por ejemplo, los $\mathcal{O}$-ideales. En este situación, la característica de Euler generalizada es

$$\chi_g(X) := \frac{\chi_g(zX)}{\chi_g(z\mathcal{O})} \quad \text{(vea [11])}$$

Ahora, la integral respecto a la característica de Euler generalizada es difinida como: Sea $(G, +, 0)$ un grupo abeliano, y sea X un subconjunto cilíndrico de $\widetilde{\mathcal{O}}$. Una función $\psi : \widetilde{\mathcal{O}} \longrightarrow G$ es llamada **cilíndrica** si ella tiene rango finito y para cada $a \in G$, $a \neq 0$, el conjunto $\pi_{\mathbf{n}}(\psi(a))$ es cilíndrico,

$$\int_X \psi \, d\chi_g := \sum_{\substack{a \in G \\ a \neq 0}} \chi_g(X \cap \psi(a)) \otimes a$$

si la suma tiene sentido en $\mathcal{M}_k \otimes G$. En tal caso, la función ψ se dice **integrable** sobre X.

Ahora bien, tomando $\mathfrak{a} = \mathcal{O}$, en la representación integral de $P(\mathfrak{a}, \mathfrak{b}, \mathbf{t})$ (vea Teorema 2.3.3) y tomando en la clase $[\mathfrak{b}]$ un represente tal que $\mathfrak{b} \cdot \widetilde{\mathcal{O}} = \widetilde{\mathcal{O}}$, tenemos que:

$$P(\mathcal{O}, \mathfrak{b}, \mathbf{t}) = \frac{q^{\rho}}{(U_{\mathfrak{b}} : U_{\mathcal{O}})(q^{\rho} - 1)} \int_{\widehat{\mathfrak{b}}_{\mathrm{reg}}} q^{\mathbf{r}\cdot\mathbf{v}(z)} \mathbf{t}^{\mathbf{v}(z)} \, d\widehat{\mu}(z).$$

Además, tomando $k = \mathbb{F}_q$ en la definición de característica de Euler generalizada, tenemos que la medida de Haar de un $\mathcal{O}$-ideal y su característica de Euler generalizada coinciden, es decir

$$\chi_g(\mathfrak{a}) = \widehat{\mu}(\widehat{\mathfrak{a}}) \ \ \text{(vea } \mathbf{2.8}[11])$$

Y así, la serie de Poincaré multivariable de singularidades de una curva algebraica se puede expresar como

$$P(\mathcal{O}, \mathfrak{b}, \mathbf{t}) = \frac{\chi_g(U_{\mathcal{O}})}{(U_{\mathfrak{b}} : U_{\mathcal{O}})} \int_{\widehat{\mathfrak{b}}_{\mathrm{reg}}} \mathbb{L}^{\mathbf{r}\cdot\mathbf{v}(z)} \mathbf{t}^{\mathbf{v}(z)} \, d\chi_g$$

Lo anterior nos motiva a definir en general, la Serie de Poincaré Multivariable de Singularidades de una curva como

$$\widetilde{\mathcal{P}}(\mathcal{O}, \mathfrak{b}, \mathbf{t}) = \chi_g(U_{\mathcal{O}}) \int_{\widehat{\mathfrak{b}}_{\mathrm{reg}}} \mathbb{L}^{\mathbf{r}\cdot\mathbf{v}(z)} \mathbf{t}^{\mathbf{v}(z)} \, d\chi_g \tag{3.1.1}$$

la cual en el caso finito $k = \mathbb{F}_q$ es un multiplo entero de $P(\mathcal{O}, \mathfrak{b}, \mathbf{t})$, a saber,

$$(U_{\mathfrak{b}} : U_{\mathcal{O}}) P(\mathcal{O}, \mathfrak{b}, \mathbf{t}).$$

Notemos que la ecuación 3.1.1 tiene sentido en el caso $k = \mathbb{Q}_p$, es decir, está es una forma de definir $P(\mathcal{O}, \mathfrak{b}, \mathbf{t})$ en el caso p-ádico, la pregunta es: ¿Es esta definición el análogo de la Serie de Poincaré Multivariable de una Singularidad definidad por Stöhr [23]? La complejidad de esta pregunta yace en el formalismo de dicha definición y en la poco información de las propiedades de la característica de Euler generalizada en el caso p-ádico.

Apéndice A

Medida de Haar

Resumen: Mostraremos la existencia y unicidad de la medida de Haar en cada grupo topológico localmente compacto. La medida de Haar se obtendrá a partir del teorema de representación de Riezs, así, que se mostraremos un funcional que inducirá nuestra forma de medir. Este tratamiento, esta basado en los libros [14] y [8].

A.1. Espacios Localmente Compactos

Definición A.1.1. Espacio Completamente Regular: Sea X espacio topológico Hausdorff, diremos que X es Completamente Regular si para todo $x_0 \in X$ y $F \subseteq X$ cerrado, con $x_0 \notin F$, existe una función continua $f : X \to [0,1]$ tal que $f(x_0) = 1$ y para todo $y \in F$ $f(y) = 0$.

Espacio Localmente Compacto: Un espacio topológico X se dice localmente compacto si para todo elemento $x \in X$ existe un abierto U, tal que $x \in U$ y la clausura de U es compacta. Esto es claramente equivalente a que para todo $x \in X$ existe un compacto C tal que $x \in \operatorname{int}(C)$.

Definición A.1.2. Un grupo topológico (G, Γ), es un grupo G con una topología Γ, con la cual resulta ser un espacio topológico Hausdorff, y tal que las funciones

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (\alpha, \beta) & \longmapsto & \alpha\beta \end{array} \qquad \begin{array}{rcl} G & \longrightarrow & G \\ \alpha & \longmapsto & \alpha^{-1} \end{array}$$

son funciones continuas.

Proposición A.1.3. *Si A y B son subconjuntos compactos disjuntos de un espacio topológico Hausdorff X, entonces existen abiertos disjuntos U y V tal que $A \subseteq U$ y $B \subseteq V$.*

Demostración. Primero, supongamos que $B = \{b\}$ y A es un conjunto compacto arbitrario. Como el espacio ambiente es Hausdorff, para cada $a \in A$ existen abiertos disjuntos V_a y U_a tales que $b \in V_a$ y $a \in U_a$. La colección $\{U_a \ / \ a \in A\}$ forma un cubrimiento abierto de A y dado que A es compacto, $A \subseteq \bigcup_{i=1}^{n} U_{a_i} = U$, además es claro que $\{b\} \subset \bigcap_{i=1}^{n} V_{a_i} = V$ y tanto U como V son abiertos disjuntos.

Ahora pasemos al caso general, donde A y B son compactos arbitrarios. Por el caso anterior, para cada $b \in B$, existen abiertos disjuntos U_b y V_b tales que $A \subset U_b$ y $b \in V_b$. La colección $\{V_b \ / \ b \in B\}$ forma un cubrimiento abierto de B y dado que B es compacto, $B \subseteq \bigcup_{i=1}^{m} V_{b_i}$, y $A \subseteq U = \bigcap_{i=1}^{m} U_{b_i}$. $\square$

Proposición A.1.4. *Sea X un espacio topológico localmente compacto y $K \subseteq X$ un conjunto compacto. Entonces existe un compacto $V \subseteq X$ y un abierto $U \subset V$ tal que $K \subseteq U$ en este caso decimos que V es una* ***vecindad compacta*** *de K*

Demostración. Sea $K \subseteq X$ un conjunto compacto. Como X es un espacio localmente compacto, para cada $x \in K$, existe un compacto $C_x \subseteq X$ tal que $x \in \text{int}(C_x)$. Es claro que $K \subseteq \cup_{x \in K} \text{int}(C_x)$. Dado que K es compacto, existen $x_1, \ldots, x_n \in K$ tal que $K \subseteq \cup_{i=1}^{n} \text{int}(C_{x_i})$. Tomando $V = \cup_{i=1}^{n} C_{x_i}$ y $U = \cup_{i=1}^{n} \text{int}(C_{x_i})$, tenemos que V es compacto, U es abierto contenido en V y $K \subseteq U$ como se pedia. $\square$

Proposición A.1.5. *Sea X un espacio topológico localmente compacto y $K \subseteq X$ un conjunto compacto. Entonces para toda vecindad W de K, existe una vecindad compacta U con $K \subseteq U \subseteq W$.*

Demostración. Sea W una vecindad de K la cual, sin perdida de generalidad, podemos suponer que W es abierta. Por la proposición anterior existe una vecindad compacta C de K, entonces $Z = C \cap W \subseteq C$ es una vecindad de K, la cual es un abierto en C (tomando la topología inducida). Sea $Y = Z^c \cap C$ entonces Y es un cerrado contenido en C, por lo cual Y es compacto. Por la Proposición A.1.3 aplicada a K y a Yexisten abiertos disjuntos U' y V' (los cuales los podemos tomar abiertos en C) tales que $K \subseteq U'$ y $Y \subseteq V'$. Como $U' \subseteq (V')^c$, entonces $\overline{U'} \subseteq (V')^c$, además, $(V')^c \subseteq Y^c = Z = C \cap W$, de ahí que, $\overline{U'} \subseteq W$. Tomando $U = \overline{U'}$, tenemos que U es una vecindad compacta de K pues $U \subseteq C$, la cual está contenida en W. $\square$

Lema A.1.6. *Todo espacio topológico X, el cual es Hausdorff y localmente compacto, es completamente regular.*

Demostración. Sabemos de topología básica (ver [13] Corolario 8.4 pag 186) que todo espacio Hausdorff locamente compacto es homeomorfo a un subespacio abierto de un espacio Hausdorff compacto (por ejemplo, la compactificación por un punto de X) y como todo espacio Hausdorff compacto es completamente regular, X es homeomorfo a un subespacio abierto de un espacio completamente regular, lo cual implica que X es completamente regular. $\square$

Proposición A.1.7. *Sea X un espacio localmente compacto. Si C es un compacto y F un cerrado en X tales que $C \cap F = \emptyset$, entonces existe una función continua $f : X \to \mathbb{R}$ con $0 \leq f \leq 1$ tal que $f(x) = 1$ para todo $x \in C$ y $f(x) = 0$ para todo $x \in F$.*

Demostración. Por el lema anterior para todo $c \in C$ existe una función continua $f_c : X \to [0, 1]$ tal que $f_c(c) = 1$ y para todo $x \in F$, $f_c(x) = 0$. La colección de conjuntos $A_c = \{x \in X \ / \ f_c(x) > \frac{1}{2}\}$, con $c \in C$, es un cubrimiento abierto de C. Dado que C es compacto existen $c_1, \ldots, c_n \in C$ tales que

$$C \subseteq \bigcup_{i=1}^{n} A_{c_i}$$

Definamos $g := \prod_{i=1}^{n} f_{c_i}$, entonces es claro que g es una función continua y para todo $x \in X$, $0 \leq g(x) \leq 1$, además se sigue que:

- para todo $x \in C$, $g(x) > \dfrac{1}{2^n}$
- para todo $x \in F$, $g(x) = 0$.

Ahora definamos $f : X \to [0,1]$ como

$$f(x) = \begin{cases} 1, & x \in C \\ g(x), & x \notin C \end{cases}.$$

Claramente, $0 \leq f(x) \leq 1$, para todo $x \in X$ y por definición, para todo $x \in C$, $f(x) = 1$ y para todo $x \in F$, $f(x) = 0$. Basta ver que f es continua. Esto se sigue si $x \in \mathrm{int}C$ o si $x \notin C$, f es constante igual a cero o $f(x) = g(x)$, respectivamente. Ahora, sea $x \in \overline{C} \cap \overline{C^c} = \mathrm{Front}(C)$. Como C es compacto, entonces C es cerrado, de donde $x \in C$ de ahí que $f(x) = 1$. Para mostrar la continuidad de f en x basta tomar vecindades de la forma $(\alpha, 1]$, con $\alpha > 0$. Como cada f_{c_i}, con $i = 1, \ldots, n$, es continua, existe una vecindad B_i de x tal que $f_{c_i}(B_i) \subseteq (\sqrt[n]{\alpha}, 1]$. Tomando $B = \cap_{i=1}^n B_i$, vemos que $f_{c_i}(B) \subseteq (\sqrt[n]{\alpha}, 1]$, de donde se sigue $f(B) \subseteq (\alpha, 1]$, como se pedia. $\square$

Otra forma de llegar a este resultado es introducir la compactificación por un punto de X, usar el hecho conocido de que todo espacio compacto Hausdorff es normal y aplicar el Lema de Urysohn.

Definición A.1.8. Sea $f : G \to \mathbb{R}$ una función de valor real definida sobre un grupo topológico G:

- Decimos que f es **uniformemente continua a izquierda**, si para todo $\epsilon > 0$, existe una vecindad V de la identidad e tal que para todo $x, y \in G$ con $x^{-1}y \in V$, se satisface $|f(x) - f(y)| < \epsilon$.
- Decimos que f **es uniformemente continua a derecha**, si para todo $\epsilon > 0$, existe una vecindad V de la identidad e tal que para todo $x, y \in G$ con $yx^{-1} \in V$, se satisface $|f(x) - f(y)| < \epsilon$.
- Decimos que f es **uniformemente continua**, si es tanto a izquierda como a derecha.

Proposición A.1.9. *Sea G un grupo topológico localmente compacto. Toda función continua de valor real con soporte compacto, es uniformemente continua.*

Demostración. En la prueba mostraremos que f es uniformemente continua a izquierda. La prueba de la continuidad uniforme a derecha es análoga y ya teniendo ambas podemos concluir que f es uniformemente continua.

Sustituyendo $x^{-1}y = s$, vemos que la definición de continuidad uniforme a izquierda es equivalente a que para todo $\epsilon > 0$, existe una vecindad de la identidad tal que para todo $x \in G$ y para todo $s \in V$, se satisface $|f(x) - f(xs)| < \epsilon$. Probemos esta última sentencia, sea $\epsilon > 0$ y $K = \text{support}(f) = \overline{\{x \,/\, f(x) \neq 0\}}$. Dado que f es continua en G, (en particular en K), para todo $x \in K$ existe un abierto U_x de x y un abierto V_x de la identidad e tal que para todo $y \in U_x$ y para todo $s \in V_x$, se tiene $|f(y) - f(ys)| < \epsilon$. Claramente, la colección $\{U_x \;/\; x \in K\}$ es un cubrimiento abierto para K. Al ser K compacto existen $x_1, \dots, x_n \in K$ tal que $K \subseteq \cup_{i=1}^{n} U_{x_i}$. Definiendo $V' = \cap_{i=1}^{n} V_{x_i}$ donde cada V_{x_i} es el abierto de la identidad correspondient a U_{x_i}. Tenemos que V' es un abierto de la identidad, en donde para todo $x \in K$ y para todo $s \in V'$, se tiene $|f(x) - f(xs)| < \epsilon$.

Ahora, veamos que existe un abierto V'' de la identidad tal que para todo $x \notin K$ y para todo $s \in V''$, $|f(x) - f(xs)| < \epsilon$, es decir, $|f(xs)| < \epsilon$. Sea $J = \{x \in G \;/\; f(x) \geq \epsilon\}$, por la continuidad de f, J es cerrado, él cual está contenido en K y por tanto J es compacto. Para cada $x \in J$, existe un abierto V_x de la identidad tal que $xV_x \subset K$. Sea W_x otro abierto de la identidad tal que $W_x W_x \subseteq V_x$. Dado que J es compacto y $\{xW_x\}_{x \in J}$ es un cubrimiento abierto para J, existen $x_1, \dots, x_n \in J$ tales que $J \subseteq \cup_{i=1}^{n} x_i W_{x_i}$. Tomado $W := \cap_{i=1}^{n} W_{x_i}$, se sigue que para todo $z \in J$ y para todo $w \in W$, existe un x_i tal que $z \in x_i W_{x_i}$, de donde $zw \in x_i W_{x_i} W_{x_i} \subseteq x_i V_{x_i} \subseteq K$, es decir, $JW \subseteq K$. Sea $V'' := W^{-1} = \{w^{-1} \;/\; w \in W\}$. Entonces, V'' es un abierto de la identidad, pues estamos en un grupo topológico y si $x \notin K$ y $s \in V$, se sigue que, $xs \notin J$ (pues si $xs = z \in J$, $x = zs^{-1} \in JW \subseteq K$), por consiguiente $|f(xs)| < \epsilon$. Finalmente, definimos $V = V' \bigcap V''$, y así, obtenemos que para todo $x \in G$ y para todo $s \in V$, se satisface $|f(x) - f(xs)| < \epsilon$. $\square$

Notación: Definimos $\mathcal{C}_c(X)$ como el conjunto de funciones continuas de valor real con soporte compacto en X y por $\mathcal{C}_c(X, K) = \{f \in \mathcal{C}_c \ / \ \text{support}(f) \subseteq K\}$.

Proposición A.1.10. *Sea X un espacio hausdorff localmente compacto, y sea Λ un funcional lineal sobre $\mathcal{C}_c(X)$. Entonces Λ es continua respecto a la norma uniforme en cada subespacio vectorial $\mathcal{C}_c(X, K)$ tal que K es un compacto en X.*

Demostración. Sea K un subconjunto compacto de X. Entonces por la Proposición A.1.4, existe una vecindad compacta V de K. Además, por la Proposición A.1.7, existe una función F continua $0 \leq F(x) \leq 1$ tal que $F(x) = 1$ para todo $x \in K$ y $F(x) = 0$ para toda $x \in (\text{int}(V))^c$, lo cual implica que $F(x) = 0$ para toda $x \in V^c$. Claramente $\text{support}(F) \subseteq V$ y como V es compacto, se sigue que $F \in \mathcal{C}_c^+(X) = \{f \in \mathcal{C}_c(X) \ / \ f \geq 0\}$. Desde el análisis funcional sabemos que la continuidad de un funcional, es equivalente a la continuidad del funcional en el origen, veamos esto último para Λ. Sea $f \in \mathcal{C}_c(X, K)$. Entonces, si $x \in K$, $F(x) = 1$ y, por tanto,

$$-\|f\| \cdot F(x) \leq f(x) \leq F(x) \cdot \|f\|$$

ó, si $x \in K^c$, entonces $f(x) = 0$ y $-\|f\| \cdot F(x) \leq f(x) \leq F(x) \cdot \|f\|$, pues $\|f\| \geq 0$ y $F(x) \geq 0$. Así, para todo $x \in X$,

$$-\|f\| \cdot F(x) \leq f(x) \leq F(x) \cdot \|f\|.$$

Como Λ es un funcional positivo,

$$-\|f\|\Lambda(\cdot F) \leq \Lambda(f) \leq \Lambda(F) \cdot \|f\|$$

es decir;

$$|\Lambda(f)| \leq \Lambda(F) \cdot \|f\|.$$

Por tanto, es claro que, si $\|f\| \to 0$, entonces $\Lambda(f) \to 0$. □

A.2. Medida de Haar

El propósito de esta sección es mostrar la existencia y unicidad de la medida de Haar en cualquier grupo topológico localmente compacto. Antes de continuar con la prueba daremos unas cuantas definiciones para entrar en contexto.

Definición A.2.1. Una colección $\mathfrak{M}$ de subconjuntos de un conjunto X es llamada una $\boldsymbol{\sigma}$**-álgebra** en X, si $\mathfrak{M}$ satisface las siguientes propiedades:

1. $X \in \mathfrak{M}$
2. Si $A \in \mathfrak{M}$, entonces $A^c \in \mathfrak{M}$
3. Si $A_1, A_2, \ldots, A_n, \ldots$ es una sucolección contable de elemento en $\mathfrak{M}$, entonces $\bigcup_{n=1}^{\infty} A_n \in \mathfrak{M}$.

Si $\mathfrak{M}$ es una σ-álgebra en X, entonces X es llamado **un espacio de medida**, y los conjuntos en $\mathfrak{M}$ son llamados **los conjuntos medibles** en X.

Definición A.2.2. Sea X un conjunto y $\mathfrak{M}$ es una σ-álgebra en X, una función $\mu : \mathfrak{M} \longrightarrow [0, \infty]$ es llamada **una Medida**, si satisface las siguientes propiedades:

1. Pata todo $A \in \mathfrak{M}$, $\mu(A) \geq 0$.
2. $\mu(\emptyset) = 0$.
3. Para cada colección contable $\{A_n\}_{n \in \mathbb{N}}$ de $\mathfrak{M}$ disjunta par a par ($A_m \cap A_n = \emptyset$ si $m \neq n$), se tiene que
$$\mu\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \mu(A_n).$$

Definición A.2.3. Sea X un espacio topológico. El $\boldsymbol{\sigma}$**-álgebra de Borel**, es la σ-álgebra generada por los conjuntos compactos de X, es decir, es una σ-álgebra $\mathfrak{M}$, la cual contiene a todos los conjuntos compactos de X y si $\mathfrak{M}'$ es otra σ-álgebra que contiene a todos los compactos, entonces $\mathfrak{M} \subseteq \mathfrak{M}'$.

Notación: $\mathcal{C}(G)$ denota las funciones continuas sobre G de valor real, es decir;

$$\mathcal{C}(G) = \{f : G \longrightarrow \mathbb{R} \,/\, f \text{ es continua}\}.$$

$\mathcal{C}_c(G)$ denotará las funciones continuas sobre G de valor real con soporte compacto. Además, definimos para cada $\alpha \in G$ las funciones $L_\alpha, R_\alpha, J : \mathcal{C}(G) \longrightarrow \mathcal{C}(G)$ de la siguiente manera para cada $f \in G$,

$$\begin{array}{rcl} L_\alpha f : G & \longrightarrow & G \\ x & \longmapsto & L_\alpha f(x) = f(\alpha^{-1}x) \end{array} \qquad \begin{array}{rcl} R_\alpha f : G & \longrightarrow & G \\ x & \longmapsto & R_\alpha f(x) = f(x\alpha) \end{array}$$

$$\begin{array}{rcl} Jf : G & \longrightarrow & G \\ x & \longmapsto & Jf(x) = f(x^{-1}) \end{array}$$

Teorema A.2.4. *Teorema de Representación de Riesz Sea X un espacio hausdorff localmente compacto y sea Λ un funcional lineal sobre $\mathcal{C}_c(X)$. Entonces existe una σ- álgebra $\mathfrak{M}$ en X la cual contiene todos los conjuntos de Borel en X, y existe una única medida positiva μ en X la cual representa a Λ en el sentido que*

1.
$$\Lambda(f) = \int_X f \, d\mu$$
para toda $f \in \mathcal{C}_c(X)$, la cual, tiene las siguientes propiedades adicionales:

2. *$\mu(K) < \infty$, para todo conjunto compacto $K \subseteq X$.*

El anterior es un resultado famoso el cual se encuentra en [19]

Teorema A.2.5. *Sea G un grupo topológico localmente compacto, entonces*

(1) *Existe un único funcional lineal positivo $\Lambda : \mathcal{C}_c(G) \to \mathbb{R}$, tal que $\Lambda(R_\alpha f) = \Lambda(f)$, para todo $\alpha \in G$ y para toda $f \in \mathcal{C}_c(G)$. Además, para todo $\alpha \in G$ y para toda $f \in \mathcal{C}_c(G)$*
$$\Lambda(L_\alpha f) = \Lambda(Jf) = \Lambda(f)$$

(2) *Existe una σ-álgebra Σ, de subconjuntos de G que contiene a la σ-álgebra de borel de G, la cual, es invariante bajo multiplicación a izquierda, a derecha y bajo inversión, i.e., para todo $S \in \Sigma$ y para todo $\gamma \in G$:*

$$\begin{aligned} \gamma S &= \{\gamma x \,/\, x \in S\} \in \Sigma. \\ S\gamma &= \{x\gamma \,/\, x \in S\} \in \Sigma. \\ S^{-1} &= \{x^{-1} \,/\, x \in S\} \in \Sigma. \end{aligned}$$

Y existe una medida μ sobre Σ tal que

(i) *Para todo $S \in \Sigma$, $\mu(\gamma S) = \mu(S\gamma) = \mu(S^{-1}) = \mu(S)$.*

(ii) *Para toda $f \in \mathcal{C}_c(G)$, $\Lambda(f) = \displaystyle\int_G f(\gamma)\, d\mu(\gamma)$.*

Una medida con las anteriores características es llamada **Medida de Haar sobre G**. Primero veamos la prueba de la existencia de dicha medida. Desde ahora G denotará un grupo topológico localmente compacto. Dado que el Teorema de Representación de Riesz A.2.4 nos da una conexión entre funcionales y medidas, usaremos μ para denotar tanto funcionales como medidas. La prueba debida a André Weil usa algunos hechos topológicos que serán vistos brevemente, para el resto daremos referencias.

Lema A.2.6. *Sea G un grupo localmente compacto $f, g \in \mathcal{C}_c(G)$ con $f \geq 0$ y $g > 0$. Entonces existen $\alpha_1, \alpha_2, \ldots, \alpha_n \in G$ y $c_1, c_2, \ldots, c_n \in \mathbb{R}$, con $c_i > 0$ para todo $i = 1, \ldots, n$; tales que, para todo $x \in G$, se satisface*

$$f(x) \leq \sum_{i=1}^{n} c_i L_{\alpha_i} g(x)$$

Demostración. Sea $K = \text{support}(f)$ y sea $u \in G$ tal que $g(u) > 0$. Sea $t \in G$, si $\alpha = tu^{-1}$ entonces $L_\alpha g(t) > 0$, pues $L_\alpha g(t) = g(\alpha^{-1}t) = g(u) > 0$. Dado $\epsilon > 0$, como $L_\alpha g$ es continua, existe una vecindad V_t de t tal que para todo $x \in V_t$, $L_\alpha g(x) \geq \epsilon$. Sea $a = \max\left\{\dfrac{f(x)}{L_\alpha g(x)} \,/\, x \in V_t\right\}$, el cual, existe pues $f \in \mathcal{C}_c(G)$, $L_\alpha g$ es una función continua y $L_\alpha g(x) \geq \epsilon$ en V_t. Así, para todo $x \in V_t$, $f(x) \leq aL_\alpha g(x)$. Claramente $K \subseteq \bigcup_{t\in G} V_t$, al ser K compacto, existen $t_1, \ldots, t_n \in G$ tales que $K \subseteq \bigcup_{i=1}^{n} V_{t_i}$. Por consiguiente, existen

$\alpha_i \in G$ y $c_i > 0$ tales que $f(x) \leq c_i L_{\alpha_i} g(x)$, para todo $x \in V_{t_i}$. De donde, para todo $x \in K$, se tiene

$$f(x) \leq \sum_{i=1}^{n} c_i L_{\alpha_i} g(x) \quad (*)$$

Dado que $f = 0$ para x fuera de K, se sigue que la relación $(*)$ se cumple en todo G. $\square$

Por el lema anterior, si $f, g \in \mathcal{C}_c(G)$, con $f \geq 0$ y $g > 0$, entonces podemos tener

$$f(x) \leq \sum_{i=1}^{n} c_i L_{\alpha_i} g(x),$$

donde $\alpha_1, \alpha_2, \ldots, \alpha_n \in G$ y $c_1, c_2, \ldots, c_n \in \mathbb{R}$ con $c_i \geq 0$ para todo $i = 1, \ldots, n$. Si tenemos una medida de Haar invariante a izquierda μ sobre G, podemos concluir de la desigualdad $(*)$ que

$$\sum_{i=1}^{n} c_i \geq \frac{\int f \, d\mu}{\int g \, d\mu}$$

lo cual motiva la siguiente definición.

Definición A.2.7. Si $f, g \in \mathcal{C}_c(G)$, con $f \geq 0$ y $g > 0$, definimos $(f : g)$ como el infimo de las sumas $\sum_{finita} c_i$ tales que $f \leq \sum_{finita} c_i L_{\alpha_i} g$, es decir;

$$(f : g) := \text{ínf} \left\{ \sum_{i=1}^{n} c_i \ / \text{ existe } n \in \mathbb{N} \text{ tal que } f \leq \sum_{i=1}^{n} c_i L_{\alpha_i} g \right\}.$$

con α_i y c_i como en el Lema A.2.6.

Notemos que en la definición A.2.7 el n varía, además, como los $c_i \geq 0$, se sigue que $0 \leq (f : g) < \infty$. En adelante cuando escribimos el símbolo $(f : g)$, se sobreentenderá que $f, g \in \mathcal{C}_c(G)$ con $f \geq 0$ y $g > 0$.

Lema A.2.8. *Con la notación de la definición anterior, se tiene:*

1. *Si $f > 0$, entonces $(f : g) > 0$.*

2. *Para todo $\alpha \in G$, $(L_\alpha f : g) = (f : g)$.*

3. *$(f_1 + f_2 : g) \leq (f_1 : g) + (f_2 : g)$.*

4. *Para todo* $\lambda \in \mathbb{R}$, *con* $\lambda > 0$; $(\lambda f : g) = \lambda(f : g)$.

5. *Si* $f_1 \leq f_2$, *entonces* $(f_1 : g) \leq (f_2 : g)$.

6. $(f : h) \leq (f : g)(g : h)$.

Demostración. 1. Sea $a = \sup f$ y $b = \sup g$ en G, entonces tanto a como b son estrictamente mayores que 0. Ahora si $f(x) \leq \sum_{i=1}^{n} c_i L_{\alpha_i} g(x)$ para toda $x \in G$, entonces dado que $g(\alpha^{-1}x) \leq b$, se sigue que $f(x) \leq b \sum_{i=1}^{n} c_i$, de donde $a \leq b \sum_{i=1}^{n} c_i$, esto es $\sum_{i=1}^{n} c_i \geq \dfrac{b}{a} > 0$, por tanto, tomando infimo, se sigue $(f : g) \geq \dfrac{b}{a} > 0$.

2. Si $f(x) \leq \sum_{i=1}^{n} c_i L_{\alpha_i} g(x)$, para toda $x \in G$, obtenemos en particular, $f(\alpha^{-1}y) \leq \sum_{i=1}^{n} c_i L_{\alpha_i} g(\alpha^{-1}y)$ para toda $y \in G$, es decir, $L_\alpha f \leq \sum_{i=1}^{n} c_i L_{\alpha\alpha_i} g$. Así, $(L_\alpha f : g) \leq (f : g)$. Utilizando esta última desigualdad vemos que

$$\begin{aligned} (f : g) &= (L_{\alpha\alpha^{-1}} f : g) \\ &= (L_{\alpha^{-1}} L_\alpha f : g) \\ &\leq (L_\alpha f : g). \end{aligned}$$

3. Sean $f_1 \leq \sum_{i=1}^{n} a_i L_{\alpha_i} g$ y $f_2 \leq \sum_{j=1}^{m} b_j L_{\beta_j} g$. Entonces

$$f_1 + f_2 \leq \sum_{i=1}^{n} a_i L_{\alpha_i} g + \sum_{j=1}^{m} b_j L_{\beta_j} g = \sum_{k=1}^{m+n} c_k L_{\gamma_k} g,$$

donde, $c_k = a_k$ y $\gamma_k = \alpha_k$ si $k = 1, \ldots, n$ y $c_k = b_{k-n}$ y $\gamma_k = \beta_{k-n}$ si $k = n+1, \ldots, m+n$, por tanto,

$$(f_1 + f_2 : g) \leq \sum_{k=1}^{m+n} c_k = \sum_{i=1}^{n} a_i + \sum_{j=1}^{m} b_j.$$

En consecuencia, $(f_1 + f_2 : g) \leq (f_1 : g) + (f_2 : g)$.

4. Si $f \leq \sum_{i=1}^{n} a_i L_{\alpha_i} g$, entonces como $\lambda > 0$, $\lambda f \leq \sum_{i=1}^{n} \lambda a_i L_{\alpha_i} g$. Así, $(\lambda f : g) \leq \lambda \sum_{i=1}^{n} a_i$, lo cual implica, $(\lambda f : g) \leq \lambda(f : g)$. Usando está última

desigualdad tenemos que

$$\begin{aligned}(f:g) &= (\lambda^{-1}\lambda f:g)\\ &\leq \lambda^{-1}(\lambda f:g)\end{aligned}$$

es decir; $\lambda(f:g)\leq(\lambda f:g)$.

5. Si $f_2 \leq \sum_{i=1}^{n} a_i L_{\alpha_i} g$, entonces $f_1 \leq \sum_{i=1}^{n} a_i L_{\alpha_i} g$ pues $f_1 \leq f_2$, luego, $(f_1:g)\leq \sum_{i=1}^{n} a_i$, de donde, $(f_1:g)\leq(f_2:g)$.

6. Suponga que $f\leq \sum_{i=1}^{n} a_i L_{\alpha_i} g$ y que $g\leq \sum_{j=1}^{m} b_j L_{\beta_j} h$. Entonces

$$L_{\alpha_i} g \leq \sum_{j=1}^{m} b_j L_{\alpha_i} L_{\beta_j} h = \sum_{j=1}^{m} b_j L_{\beta_j \alpha_i} h$$

de donde $f\leq \sum_{i=1}^{n} a_i \sum_{j=1}^{m} b_j L_{\beta_j\alpha_i} h$, luego $(f:h)\leq \sum_{i=1}^{n} a_i \sum_{j=1}^{m} b_j$. Por tanto, $(f:h)\leq(f:g)(g:h)$.

□

Ahora fijaremos nuestra atención en una función $f^* \in \mathcal{C}_c(G)$, con $f^*>0$. Si $F\in\mathcal{C}_c(G)$, con $F>0$, definimos para cada $f\in\mathcal{C}_c(G)$ con $f\geq 0$ la integral aproximada $\mu_F(f)$ por

$$\mu_F(f)=\frac{(f:F)}{(f^*:F)}$$

notemos que por el Lema A.2.8 tenemos que $(f^*:F)>0$. Cuando escribimos el símbolo $\mu_F(f)$, se entiende que $f,F\in\mathcal{C}_c(G)$ con $f\geq 0$ y $F>0$. Es claro que de la definición que $\mu_F(f^*)=1$, lo cual nos dirá luego que $\int_G f^*\, f\mu = 1$, esto es el análogo a decir que dado un subconjunto compacto E de G, podemos hallar una medida μ tal que $\mu(E)=1$ Ahora daremos el analogo del Lema A.2.8, para $\mu_F(f)$.

Lema A.2.9. *Con la notación anterior, se tiene:*

1. *Si $f>0$, entonces $\mu_F(f)>0$.*

2. *Para todo $\alpha\in G$, $\mu_F(L_\alpha f)=\mu_F(f)$.*

3. $\mu_F(f_1 + f_2) \leq \mu_F(f_1) + \mu_F(f_2)$.

4. *Para todo* $\lambda \in \mathbb{R}$, *con* $\lambda > 0$, $\mu_F(\lambda f) = \lambda \mu_F(f)$.

5. *Si* $f_1 \leq f_2$, *entonces* $\mu_F(f_1) \leq \mu_F(f_2)$.

6. *Si* $f > 0$, *entonces* $\dfrac{1}{(f^* : f)} \leq \mu_F(f) \leq (f : f^*)$.

Demostración. Este lema es una consecuencia inmediata del Lema A.2.8, veamos sólo *6.* Tenemos que $(f : F) \leq (f : f^*)(f^* : F)$ y $(f^* : F) \leq (f^* : f)(f : F)$, lo cual implica, $\mu_F(f) \leq (f^* : F)$ y $\dfrac{1}{(f^* : f)} \leq \mu_F(f)$. □

El siguiente lema indica que la integral aproximada $\mu_F(f)$, la cual, es subaditiva por el Lema A.2.8, tiende a ser aditiva cuando el soporte de F tiende a la identidad de G. Es decir,

$$\mu_F(f_1 + f_2) \longrightarrow \mu_F(f_1) + \mu_F(f_2), \text{ si support}(F) \longrightarrow e.$$

Lema A.2.10. *Dadas* $f_1, f_2 \in \mathcal{C}_c(G)$, *con* $f_1 \geq 0, f_2 \geq 0$, *y dado* $\epsilon > 0$, *existe una vecindad* V *de la identidad de* G, *tal que*

$$\mu_F(f_1 + f_2) = \mu_F(f_1) + \mu_F(f_2) + \epsilon$$

siempre y cuando $F \in \mathcal{C}_c(G)$, *con* $F > 0$ *y support*$(F) \subseteq V$.

Demostración. Sea K compacto en G tal que $\text{support}(f_1) \cup \text{support}(f_2) \subseteq K$. Como G es localmente compacto, existe $f' \in \mathcal{C}_c(G)$, con $f \geq 0$, tal que $f'\big|_K = 1$. Definamos $f = f_1 + f_2 + \delta f'$, donde $\delta > 0$. Sean $h_1(x) := \dfrac{f_1(x)}{f(x)}$, $h_2(x) := \dfrac{f_2(x)}{f(x)}$ si $f(x) \neq 0$ y $h_1(x) = h_2(x) = 0$ si $f(x) = 0$. Por definición h_i es continua en el abierto $U = \{x \in G \;/\; f(x) \neq 0\}$. Además, $h_i\big|_{K^c} = 0$, pues $\text{support}(f_i) \subseteq K$. Así h_i es continua en el abierto K^c (es abierto dado que K es compacto). Como $G = U \cup K^c$, se sigue que h_i es continua en todo G, es decir, $h_i \in \mathcal{C}_c(G)$. Notemos que $h_i \geq 0$ y $h_1 + h_2 = \dfrac{f_1 + f_2}{f_1 + f_2 + \delta f'} \leq 1$.

Dado $\epsilon' > 0$, por la Proposición A.1.9, h_i es uniformemente continua. Por tanto existe una vecindad V de la identidad de G, tal que, para todo $x, y \in G$ con $y^{-1}x \in V$, se tiene

$|h_i(x) - h_i(y)| < \epsilon'$ para $i = 1, 2$. Ahora, supongamos que $F \in \mathcal{C}_c(G)$, con $F > 0$ y support$(F) \subseteq V$. Sean $c_1, \ldots, c_n \in \mathbb{R}$, con cada $c_i \geq 0$ y $\alpha_1, \ldots, \alpha_n \in G$ tales que

$$f \leq \sum c_i L_{\alpha_i} F, \quad (*)$$

es decir, $f(x) \leq \sum c_i F(\alpha_i^{-1}x)$, esta desigualdad junto con la continuidad uniforme de h_j, implican

$$\begin{aligned} f(x)h_j(x) &\leq \sum c_i F(\alpha_i^{-1}x)h_j(x) \\ &\leq \sum c_i F(\alpha_i^{-1}x)(h_j(s_i) + \epsilon') \end{aligned}$$

pues, $h_j(x) \leq h_j(\alpha_i) + \epsilon'$ o $F(\alpha_i^{-1}x) = 0$ de acuerdo a si $\alpha_i^1 x \in V$ o si $\alpha_i^1 x \notin V$. Luego

$$f_j = fh_j \leq \sum c_i(h_j(s_i) + \epsilon')L_{\alpha_i}F,$$

de ahí que,

$$(f_j : F) \leq \sum c_i(h_j(s_i) + \epsilon').$$

Sumando para $j = 1, 2$, tenemos que

$$(f_1 : F) + (f_2 : F) \leq \sum c_i(1 + 2\epsilon'),$$

lo cual, implica que, para todo $\sum c_i$ que satisfacen $(*)$, se tiene

$$(f_1 : F) + (f_2 : F) \leq (1 + 2\epsilon')\sum c_i.$$

Así, tomando infimo

$$(f_1 : F) + (f_2 : F) \leq (1 + 2\epsilon')(f : F),$$

dividiendo ambos lados por $(f^* : F)$, tenemos

$$\begin{aligned} \mu_F(f_1) + \mu_F(f_2) &\leq (1 + 2\epsilon')\mu_F(f) \\ &\leq (1 + 2\epsilon')(\mu_F(f_1 + f_2) + \delta\mu_F(f')). \end{aligned}$$

Aplicando el Lema A.2.9(6), vemos que,

$$\mu_F(f_1) + \mu_F(f_2) \leq \mu_F(f_1 + f_2) + 2\epsilon'(f_1 + f_2 : f^*) + \delta(1 + 2\epsilon')(f' : f^*).$$

Ahora debemos tomar δ y ϵ' lo suficientemente "pequeños" para que

$$2\epsilon'(f_1 + f_2 : f^*) + \delta(1 + 2\epsilon')(f' : f^*) < \epsilon.$$

Por ejemplo, si $(f' : f^*) \neq 0$, tomamos $\delta = \text{mín}\left\{\frac{\epsilon}{2(f' : f^*)}, 1\right\}$ y así podemos tomar $\epsilon' \leq \frac{\epsilon}{4((f_1 + f_2 : f^*) + (f' : f^*))}$, de otra forma tomamos $\epsilon' \leq \frac{\epsilon}{2(f_1 + f_2 : f^*)}$. Así se obtiene el resultado pedido

$$\mu_F(f_1 + f_2) = \mu_F(f_1) + \mu_F(f_2) + \epsilon.$$

□

A.2.1. Prueba de la existencia de la medida de Haar.

Demostración. Sea $D = \{f \in \mathcal{C}_c(G) \ / \ f > 0\}$. Para cada $f \in D$ definimos $J(f)$ como el intervalo compacto $\left[\frac{1}{(f^* : f)}, (f : f^*)\right] \subseteq \mathbb{R}$. Por el teorema de Tychonoff el producto cartesiano

$$J = \prod_{f \in D} J(f)$$

es compacto. Para cada $F \in D$, fijo, los valores tomados por $\mu_F(f)$ cuando $f \in D$, son las coordenadas de un punto a_F de J, es decir; $a_F = (\mu_F(f))_{f \in D}$, pues por el Lema A.2.9(6) $\mu_F(f) \in J(f)$. Para cada vecindad V de la identidad, definimos

$$A_V = \{a_F \in J \ / \ F \in \mathcal{C}_c(G), F > 0, \text{support}(F) \subseteq V\}.$$

Notemos que ningún A_V es vacío. Además, si V_1, V_2, V son vecindades de la identidad tales que $V \subseteq V_1 \cup V_2$, entonces $A_V \subseteq A_{V_1} \cap A_{V_2}$. Dado que J es compacto, se tiene que

$$\bigcap \overline{A_V} \neq \emptyset$$

es decir, existe $a = (\mu(f))_{f \in D} \in J$ tal que $a \in \overline{A_V}$, lo cual significa que dadas $f_1, f_2, \ldots, f_n \in D$ y $\epsilon > 0$ y una vecindad V de la identidad, existe una función $F \in \mathcal{C}_c(G)$ tal que $F > 0$, $\text{support}(F) \subseteq V$ y $|\mu(f_i) - \mu_F(f_i)| < \epsilon$, para todo $i = 1, 2, \ldots, n$. Así (2),(3),(4) y (6) del Lema A.2.9 y Lema A.2.10 demuestrán inmediatamente que

1. $\mu(L_\alpha f) = \mu(f)$

2. $\mu(\lambda f) = \lambda\mu(f)$

3. $\mu(f_1 + f_2) = \mu(f_1) + \mu(f_2)$

4. $\mu(f) \geq \dfrac{1}{(f^* : f)} > 0$

donde $\alpha \in G$, $f, f_1, f_2 \in D$ y $\lambda > 0$. Definiendo $\mu(0) = 0$, podemos extender μ a $\mathcal{C}_c(G)$ y por el teorema de representación de Riesz, obtenemos una medida Borel, la cual, resulta ser una medida de Haar por las propiedades antes enumeradas. Note que $\mu(f^*) = 1$. $\square$

A.2.2. Prueba de la unicidad de la medida de Haar.

Ahora pasamos a la prueba de la unicidad de la medida de Haar invariante a izquierda, esta unicidad será entendida como se explica en el Teorema A.2.5.

Si μ es una medida de Haar invariante a izquierda en G, la función representada por $f * g$ y definida por

$$(f * g)(x) = \int f(y)g(y^{-1}x)d\mu(y), \quad \text{para todo} \quad x \in G$$

es la convolución de f y g con respecto a μ, donde $f, g \in \mathcal{C}_c(G)$. Notemos que la función de dos variables, definida por

$$(x, y) \longmapsto f(y)g(y^{-1}x),$$

pertenece a $\mathcal{C}_c(G \times G)$ y es claramente continua. Además, si $S_f = \text{support}(f)$ y $S_g = \text{support}(g)$, entonces el soporte de la función de dos variables en cuestión estará contenido en $S_f S_g \times S_f$, pues, si (x, y) son tales que $f(y)g(y^{-1}x) \neq 0$, entonces $f(y) \neq 0$ y $g(y^{-1}x) \neq 0$, así, $y \in S_f$ y $y^{-1}x \in S_g$. Por tanto, $(x, y) = (y(y^{-1}x), y) \in S_f S_g \times S_f$, de donde la clausura de tales elementos está contenida en $S_f S_g \times S_f$.

Vemos que $f * g \in \mathcal{C}_c(G)$ y que $S_{f*g} \subseteq S_f S_g$. La invarianza a izquierda de μ nos permite escribir como

$$(f * g)(x) = \int f(xy)g(y^{-1})\, d\mu(y) \quad \text{para todo} \quad x \in G$$

El concepto de convolución, definido arriba para funciones continuas con soporte compacto, se generaliza para funciones integrables y tiene propiedades importantes. Nosotros debemos limitarnos a unas pocas ideas rudimentarias las cuales son suficientes para nuestro objetivo inmediato. Los dos lemas siguientes forman parte de un importante método conocido como el proceso de regularización.

Lema A.2.11. *Sea E un espacio localmente compacto, μ una medida positiva en E, f una función continua de valor real sobre E y $a \in E$. Dado $\epsilon > 0$, existe una vecindad V de a tal que, si $g \in \mathcal{C}_c(E)$ con $g \geq 0$, support$(g) \subseteq V$ y $\int g d\mu = 1$; entonces*

$$\left| \int fg \, d\mu - f(a) \right| \leq \epsilon.$$

Demostración. Dado $\epsilon > 0$, existe una vecindad V de a tal que para todo $y \in V$, se tiene $|f(y) - f(a)| \leq \epsilon$, ya que f es continua. Ahora, Si $g \in \mathcal{C}_c(E)$, con $g \geq 0$, support$(g) \subseteq V$ y $\int g d\mu = 1$, entonces, para todo $y \in E$ se satisface $|f(y) - f(a)|g(y) \leq \epsilon g(y)$. De donde

$$\begin{aligned} \left| \int fg \, d\mu - f(a) \right| &= \left| \int (f(y) - f(a))g(y) \, d\mu(y) \right| \\ &\leq \int |f(y) - f(a)| \, g(y) \, d\mu(y) \\ &\leq \int \epsilon g(y) \, d\mu(y) \\ &\leq \epsilon. \end{aligned}$$

□

Lema A.2.12. *Sea G un grupo topológico localmente compacto, μ una medida de Haar invariante a izquierda en G y $f \in Cc(G)$. Dado $\epsilon > 0$, existe una vecindad V de la identidad tal que, si $g \in \mathcal{C}_c(G)$ con $g \geq 0$, support$(g) \subseteq V$ y $\int g \, d\mu = 1$; entonces*

$$|(f * Jg)(x) - f(x)| \leq \epsilon \quad \textit{para todo} \quad x \in G.$$

Demostración. Dado $\epsilon > 0$, como $f \in \mathcal{C}_c(G)$ f es uniformemente continua, existe una vecindad V de la identidad de G, tal que para todo $x \in G$ y $y \in V$, se tiene $|f(xy) -$

$f(x)| \leq \epsilon$. Sea $g \in \mathcal{C}_c(G)$ con $g \geq 0$, support$(g) \subseteq V$ y $\int g d\mu = 1$, entonces

$$\begin{aligned}
|(f * Jg)(x) - f(x)| &= \left| \int f(xy) Jg(y^{-1})\, d\mu(y) - f(x) \right| \\
&= \left| \int f(xy) g(y)\, d\mu(y) - \int f(x) g(y)\, d\mu(y) \right| \\
&= \left| \int (f(xy) - f(x)) g(y)\, d\mu(y) \right| \\
&\leq \int |f(xy) - f(x)|\, g(y)\, d\mu(y) \\
&= \int_V |f(xy) - f(x)|\, g(y)\, d\mu(y) \\
&\leq \epsilon.
\end{aligned}$$

□

Ahora, finalmente probemos la parte del Teorema A.2.5, la cual trata de la unicidad. Sean μ, ν dos medidas de Haar invariantes a izquierda en G. Primero asumiremos que existe $f^* \in \mathcal{C}_c(G)$, con $f^* \geq 0$ tal que $\int f^* d\mu = \int f^* d\nu = 1$, en base a esta suposición probaremos que $\mu = \nu$. El caso general de dos medidas de Haar invariantes a izquierda, es entonces inmediata.

Si $f, g \in \mathcal{C}_c(G)$, formamos la convolución $h = f * Jg \in \mathcal{C}_c(G)$ relativa a μ. Por la primera expresión para la convolución tenemos que

$$h(x) = (f * Jg)(x) = \int f(y) Jg(y^{-1}x)\, d\mu(y)$$

así,

$$\begin{aligned}
\int h(x)\, d\nu(x) &= \iint f(y) Jg(y^{-1}x)\, d\mu(y) d\nu(x) \\
&= \iint f(y) Jg(y^{-1}x)\, d\nu(x) d\mu(y) \\
&= \int f(y) \int Jg(y^{-1}x)\, d\nu(x) d\mu(y)
\end{aligned}$$

de donde,

$$\int h\, d\nu = \int f\, d\mu \int Jg\, d\nu \tag{A.2.1}$$

Ahora, dado $\epsilon > 0$, por el Lema A.2.12 existe una vecindad V de la identidad, la cual, puede asumirse compacta y tal que para toda $g \in \mathcal{C}_c(G)$, con $g \geq 0$, $\text{support}(g) \subseteq V$ y $\int g\, d\mu = 1$, se tiene

$$\|h - f\| := \sup\{|h(x) - f(x)| \;/\; x \in G\} \leq \epsilon.$$

Proposición A.2.13. *Sea μ es una medida de Haar invariante a izquierda sobre un grupo localmente compacto G. Si $f \in \mathcal{C}_c(G)$, con $f \geq 0$ no idénticamente igual a cero, entonces $\int f\, d\mu > 0$.*

Demostración. Como $\mu \neq 0$, existe $g \in \mathcal{C}_c(G)$, con $g \geq 0$ no identicamente cero, tal que $\int g\, d\mu > 0$. Por el Lema A.2.6 existen $\alpha_1, \ldots, \alpha_n \in G$ y $a_1, \ldots, a_n \in \mathbb{R}$, con $a_i > 0$, tales que $g \leq \sum a_i L_{\alpha_i} f$. Por tanto,

$$\int g\, d\mu \leq \sum a_i \int f\, d\mu \quad \text{lo cual implica} \quad \int f\, d\mu \leq \frac{\int g\, d\mu}{\sum a_i} > 0.$$

$\square$

La proposición anterior es independiente del Teorema A.2.5 y consecuentemente, por esta proposición para cada vecindad V de la identidad existe una función $g \in \mathcal{C}_c(G)$, con $g \geq 0$, $\text{support}(g) \subseteq V$ y $\int g d\mu = 1$. Dado que el soporte de h esta contenido en el compacto $S_f V^{-1}$, es decir, $S_h \subseteq S_f V^{-1}$, donde $V^{-1} := \{v^{-1}/v \in V\}$, el cual, es compacto, ya que V es compacto y la función $x \longmapsto x^{-1}$ es continua, se sigue desde la continuidad de las medidas positivas, que $\int h\, d\nu$ puede ser llevada tan cerca de $\int f\, d\nu$ como se desee, siempre y cuando V sea una vecindad de la identidad lo suficientemente pequeña y $g \in \mathcal{C}_c(G)$, con $g \geq 0$, $\text{support}(g) \subseteq V$ y $\int g d\mu = 1$. Cuando nosotros aplicamos esta observación a $f = f^*$ y tomamos en cuenta que

$$\int f^*\, d\mu = \int f^*\, d\nu = 1$$

la Ecuación A.2.1 resulta ser

$$\int h\, d\nu = \int Jg\, d\nu$$

y dado que $\int h\, d\nu \longrightarrow \int f^*\, d\nu = 1$, se sigue que $\int Jg\, d\nu \longrightarrow 1$. Cuando aplicamos esta nueva observación, la Ecuación A.2.1, pasando al límite, produce que

$$\int f\, d\mu = \int f\, d\nu \quad \text{así } \mu = \nu.$$

Finalmente, notamos que si μ y ν son medidas de Haar invariantes a izquierda, seleccionamos una función $f^* \in \mathcal{C}_c(G)$ con $f^* \geq 0$ no idénticamente igual a cero, entonces por la Proposición A.2.13 tenemos que $u = \int f\, d\mu > 0$ y $v = \int f\, d\nu > 0$. Definimos $\mu' = \dfrac{\mu}{u}$ y $\nu' = \dfrac{\nu}{v}$. Así, $\int f^*\, d\mu' = \int f^*\, d\nu' = 1$ y por lo anterior, $\mu' = \nu'$, es decir, $\mu = c\nu$ donde $c = \dfrac{u}{v}$.

Indicaremos una segunda prueba de la unicidad de la medida de Haar, es decir, del funcional que hemos definido, basada en un inteligente computo debido independientemente a Weil y a Von Neumann.

Sea μ una medida de Haar invariante a izquierda en G y $f' \in \mathcal{C}_c(G)$, $f' \geq 0$ no identicamente igual a cero, tal que $\int f'\, d\mu = 1$, definimos

$$\Delta(s) = \int f'(xs^{-1})\, d\mu(x), \qquad \text{para todo } \ s \in G.$$

Por la Proposición A.2.13 $\Delta(s) > 0$ y Δ es un homomorfismo continuo. Consideremos las dos expresiones para la convolución $(f' * f)(x)$ en x:

$$\int f'(y) f(y^{-1}x)\, d\mu(y) = \int f'(xy) f(y^{-1})\, d\mu(y)$$

donde $f \in \mathcal{C}_c(G)$. Integrando con respecto a x, tenemos:

$$\begin{aligned}
\iint f'(y) f(y^{-1}x)\, d\mu(y)\, d\mu(x) &= \iint f'(xy) f(y^{-1})\, d\mu(y)\, d\mu(x) \\
\int f'(y) \int f(y^{-1}x)\, d\mu(x)\, d\mu(y) &= \int f(y^{-1}) \int f'(xy)\, d\mu(x)\, d\mu(y) \\
\int f'(y) \int f(x)\, d\mu(x)\, d\mu(y) &= \int f(y^{-1}) \Delta(y^{-1})\, d\mu(y) \\
\int f(x)\, d\mu(x) \int f'(y)\, d\mu(y) &= \int f(y^{-1}) \Delta(y^{-1})\, d\mu(y) \\
\int f(x)\, d\mu(x) &= \int f(y^{-1}) \Delta(y^{-1})\, d\mu(y) \\
\int f(x)\, d\mu(x) &= \int f(x^{-1}) \Delta(x^{-1})\, d\mu(x). \ \ (\dagger)
\end{aligned}$$

Reemplazamos en la anterior identidad f por $L_s f$, tenemos:

$$\begin{aligned}
\int L_s f(x)\, d\mu(x) &= \int L_s f(x^{-1})\Delta(x^{-1})\, d\mu(x) \\
\int f(xs^{-1})\, d\mu(x) &= \int f(x^{-1}s^{-1})\Delta(x^{-1})\, d\mu(x) \\
&= \Delta(s) \int f(x^{-1}s^{-1})\Delta(x^{-1})\Delta(s^{-1})\, d\mu(x) \\
&= \Delta(s) \int f(x^{-1}s^{-1})\Delta((sx)^{-1})\, d\mu(x).
\end{aligned}$$

Cambiando la variable x por la variable sx, por el Lema A.2.9, tenemos que $\mu(x) = \mu(sx)$, de donde $d\mu(x) = d\mu(sx)$, obteniendo:

$$\begin{aligned}
\int f(xs^{-1})\, d\mu(x) &= \Delta(s) \int f(x^{-1}s^{-1})\Delta((sx)^{-1})\, d\mu(sx) \\
\int f(xs^{-1})\, d\mu(x) &= \Delta(s) \int f(x^{-1})\Delta(x^{-1})\, d\mu(x)
\end{aligned}$$

De nuevo por (†), se sigue que

$$\begin{aligned}
\int f(xs^{-1})\, d\mu(x) &= \Delta(s) \int f(x)\, d\mu(x) \\
\Delta(s^{-1}) \int f(xs^{-1})\, d\mu(x) &= \int f(x)\, d\mu(x) \quad (\ddagger)
\end{aligned}$$

Observación: En la deducción de las ecuaciones anteriores se han usado las siguientes propiedades:

(i) $\Delta(e) = 1$, donde e es la identidad de G.

(ii) $\Delta(ab) = \Delta(a)\Delta(b)$.

(iii) $\Delta(s)\Delta(s^{-1}) = 1$.

La prueba de (i) es inmediata y (iii) es consecuencia de las dos anteriores, veamos (ii):

$$\begin{aligned}
\Delta(a)\Delta(b) &= \int f'(xa^{-1})\,d\mu(x)\int f'(yb^{-1})\,d\mu(y)\\
&= \iint f'(xa^{-1})f'(yb^{-1})\,d\mu(x)\,d\mu(y)\\
&= \iint f'(xa^{-1})f'(yb^{-1})\,d\mu(x)\,d\mu(y)\\
&= \iint f'(yb^{-1}a^{-1})f'(yb^{-1})\,d\mu(yb^{-1})\,d\mu(y)\\
&= \int f'(yb^{-1}a^{-1})\left(\int f'(yb^{-1})\,d\mu(yb^{-1})\right)d\mu(y)\\
&= \int f'(yb^{-1}a^{-1})\,d\mu(y)\\
&= \Delta(ab)
\end{aligned}$$

Las dos propiedades establecidas (†)(‡) inducen la unicidad de la medida de Haar en la siguiente forma. Consideremos dos medidas de Haar μ y ν y definamos Δ en términos de μ. Entonces para toda $f, g \in \mathcal{C}_c(G)$

$$\begin{aligned}
\int f(x)\,d\mu(x)\int g(y)\,d\nu(y) &= \iint f(x)\,d\mu(x)\,g(y)\,d\mu(y)\\
&= \iint f(xy)\,d\mu(x)\Delta(y)g(y)\,d\nu(y) \quad \text{por } (\ddagger)\\
&= \iint f(xy)g(y)\Delta(y)\,d\nu(y)\,d\mu(x)\\
&= \iint f(w)g(x^{-1}w)\Delta(x^{-1}w)\,d\nu(w)\,d\mu(x)\\
&= \iint g((w^{-1}x)^{-1})\Delta((w^{-1}x)^{-1})\,d\mu(x)\,f(w)\,d\nu(w)\\
&= \iint g(z^{-1})\Delta(z^{-1})\,d\mu(z)\,f(w)\,d\nu(w)\\
&= \iint g(z)\,d\mu(z)\,f(w)\,d\nu(w) \quad \text{por } (\dagger)\\
&= \int g(z)\,d\mu(z)\int f(w)\,d\nu(w).
\end{aligned}$$

Es decir,

$$\int f\,d\mu\int g\,d\nu = \int g\,d\mu\int f\,d\nu,$$

tomando $g \in \mathcal{C}_c(G)$, con $g \geq 0$ no identicamente igual a cero, $c = \dfrac{\int g\, d\nu}{\int g\, d\mu} > 0$, y así,

$$\int f\, d\nu = c \int f\, d\mu$$

para toda $f \in \mathcal{C}_c(G)$, lo cual prueba la unicidad.

Por último, veremos una forma útil de interpretar la medida de Haar. En la prueba de la existencia consideramos el conjunto A_V y observamos que un punto $a \in \cap\overline{A_V}$ corresponde a una medida de Haar invariante a izquierda μ tal que $\int f\, d\mu = 1$. Sabemos que μ es única, de donde a también debe ser único.

Lema A.2.14. *Sea E un espacio compacto y $\{X_i\}$ una familia de subconjuntos no vacíos de E con la propiedad que dados X_i y X_j existe un X_k tal que $X_k \subseteq X_i \cap X_j$.*

$\bigcap \overline{X_i} = \{a\}$ sí, y solo si, cada vecindad de a contiene algún X_i.

Demostración. ($\Leftarrow$) Por la Proposición **??**, $\bigcap \overline{X_i} \neq \emptyset$. Sean $a, b \in \bigcap \overline{X_i}$, si ocurriera que $a \neq b$, como E es Hausdorff, existen vecindades V_a y V_b de a y b respectivamente, con $V_a \cap V_b = \emptyset$. Por hipótesis existe X_i tal que $a \in \overline{X_i} \subseteq V_a$, así, $b \notin \overline{X_i}$, lo cual es un absurdo. Por tanto, debe ser $a = b$.

($\Rightarrow$) Supongamos por el contrario que existe una vecindad abierta V de a, tal que ningún X_i esta contenido en V. Sea $F = V^c$ y definamos $Y_i = X_i \cap F \neq \emptyset$ y es claro que dados Y_i y Y_j existe Y_k tal que $Y_k \subseteq Y_i \cap Y_j$. Por la Proposición **??** existe

$$b \in \bigcap \overline{Y_i} = \bigcap \overline{X_i \cap F} \subset \bigcap \overline{X_i} \cap F,$$

de ahí que, $b \in \bigcap \overline{X_i}$ y $b \in F = V^c$, por tanto $b \neq a$ y $\overline{X_i}$ consta al menos de dos puntos. □

Proposición A.2.15. *Para cada $f \in \mathcal{C}_c^+(G)$ existe un número $\mu(f)$ tal que, dado $\epsilon > 0$, existe una vecindad V de la identidad, tal que para toda $F \in \mathcal{C}_c^+ G$ con support(F) $\subseteq V$ y F no identicamente igual cero, se tiene*

$$|\mu_F(f) - \mu(f)| < \epsilon.$$

El número $\mu(f)$ es único para cada $f \in \mathcal{C}_c^+(G)$.

Demostración. Si f es identicamente igual a cero, $f = 0$, entonces $\mu_F(f) = 0$ y definimos entonces $\mu(f) = 0$. Sea $f \neq 0$, como $a \in J$ es el único punto en la clausura de todos los A_V, es decir; $\{a\} = \bigcap \overline{A_V}$, el lema anterior nos dice que toda vecindad de a contiene a algún A_V. Sea $\epsilon > 0$, para la vecindad $(a - \epsilon, a + \epsilon) = \prod_{f\in D}(\mu(f) - \epsilon, \mu(f) + \epsilon)$, existe una vecindad de la identidad, tal que $\overline{A_V} \subseteq (a - \epsilon, a + \epsilon)$. Es decir, para toda $F \in \mathcal{C}_c^+(G)$ con support$(F) \subseteq V$ y F no identicamente igual cero, se tiene $a_F \in (a - \epsilon, a + \epsilon)$, lo cual es equivalente a

$$|\mu_F(f) - \mu(f)| < \epsilon.$$

Veamos la unicidad. Supongamos que $\mu'(f)$ también satisface que para todo $\epsilon > 0$, existe una vecindad V de la identidad, tal que para toda $F \in \mathcal{C}_c^+G$ con support$(F) \subseteq V$ y F no identicamente igual cero, se tiene

$$|\mu'_F(f) - \mu'(f)| < \epsilon,$$

entonces, es claro que para todo $\epsilon > 0$

$$|\mu'(f) - \mu(f)| < \epsilon,$$

de donde $\mu(f) = \mu'(f)$. □

La proposición anterior nos dice que:

$$\mu(f) = \lim_{S_F \to e} \mu_F(f), \quad \text{donde} \quad S_F = \text{support}(F).$$

Es decir; si $F \in \mathcal{C}_c^+(G)$ con $F \neq 0$, entonces a medida que support(F) tiende a la identidad de G, la integral aproximada $\mu_F(f)$ tiende a $\mu(f)$, para toda $f \in \mathcal{C}_c^+(G)$.

Bibliografía

Y así, del mucho leer y del poco dormir, se le secó el celebro de manera que vino a perder el juicio.

Miguel de Cervantes Saavedra

[1] Atiyah, M. *Introduction To Commutative Algebra*. Addison-Wesley series in mathematics. Westview Press, 1994. ISBN 9780813345444.

[2] Casas-Sánchez, O. y Zúñiga-Galindo, W. p-adic elliptic quadratic forms, parabolic-type pseudodifferential equations with variable coefficients and markov processes. *P-Adic Numbers, Ultrametric Analysis, and Applications*, vol. 6(1), páginas 1–20, 2014.

[3] Dummit, D. y Foote, R. *Abstract Algebra*. Wiley, 2003.

[4] Eisenbud, D. *Commutative Algebra: With a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995. ISBN 9780387942698.

[5] Galkin, V. M. Zeta functions of some one-dimensional rings. *Mathematics of the USSR-Izvestiya*, vol. 7(1), página 1, 1973.

[6] Goldschmidt, D. *Algebraic Functions and Projective Curves*. Graduate Texts in Mathematics. Springer, 2003. ISBN 9780387954325.

[7] GOUVÊA, F. Q. *Primeiros Passos p-ádicos*. Instituto de Matemática Pura e Aplicada, 1989.

[8] HALMOS, P. *Measure Theory*. Número v. 9 en Graduate Texts in Mathematics. Springer, 1974.

[9] KOBLITZ, N. *P-adic numbers, p-adic analysis, and zeta-functions*. Graduate texts in mathematics. Springer-Verlag, 1977.

[10] KREYSZIG, E. *Introductory functional analysis with applications*, vol. 81. wiley New York, 1989.

[11] DE LA MATA, F. y MOYANO FERNÁNDEZ, J. On the relation between the generalized poincaré series and the stöhr zeta function. *Proceedings of the American Mathematical Society*, vol. 137(1), páginas 51–59, 2009.

[12] MOYANO-FERNÁNDEZ, J., ZÚÑIGA-GALINDO, W. ET AL. Motivic zeta functions for curve singularities. *Nagoya Mathematical Journal*, vol. 198, páginas 47–75, 2010.

[13] MUNKRES, J. *Topology*. Prentice Hall, Incorporated, 2000.

[14] NACHBIN, L. *The Haar Integral*. D. Van Nostrand Company, 1965.

[15] NEUMANN, J. V. The uniqueness of haar's measure. *Matematicheskii Sbornik*, vol. 1(5), páginas 721–734, 1936.

[16] ROBERT, A. *A Course in p-adic Analysis*. Graduate Texts in Mathematics. Springer, 2000.

[17] RODRÍGUEZ-VEGA, J. y ZÚÑIGA-GALINDO, W. Elliptic pseudodifferential equations and sobolev spaces over p-adic fields. *Pacific journal of mathematics*, vol. 246(2), páginas 407–420, 2010.

[18] ROSENLICHT, M. Equivalence relations on algebraic curves. *Annals of Mathematics*, páginas 169–191, 1952.

[19] Rudin, W. *Real and Complex Analysis*. Tata McGraw-Hill, 1987.

[20] Serre, J. *Algebraic Groups and Class Fields*. Graduate Texts in Mathematics. Springer New York, 1997. ISBN 9780387966489.

[21] Stöhr, K.-O. On the poles of regular differentials of singular curves. *Boletim da Sociedade Brasileira de Matemática - Bulletin/Brazilian Mathematical Society*, vol. 24(1), páginas 105–136, 1993. ISSN 0100-3569.

[22] Stöhr, K.-O. Local and global zeta-functions of singular algebraic curves. *Journal of Number Theory*, vol. 71(2), páginas 172 – 202, 1998. ISSN 0022-314X.

[23] Stöhr, K.-O. Multi-variable poincaré series of algebraic curve singularities over finite fields. *Mathematische Zeitschrift*, vol. 262(4), páginas 849–866, 2009. ISSN 0025-5874.

[24] Weil, A. *Líntégration dans les groupes topologiques et ses applications*. Actualités scientifiques et industrielles. Hermann, 1979.

[25] Zúñiga-Galindo, W. Local zeta functions and fundamental solutions for pseudo-differential operators over p-adic fields. *P-Adic Numbers, Ultrametric Analysis, and Applications*, vol. 3(4), páginas 344–358, 2011.

–¿Qué te parece desto, Sancho? – Dijo Don Quijote –
Bien podrán los encantadores quitarme la ventura,
pero el esfuerzo y el ánimo, será imposible.

Segunda parte del Ingenioso Caballero
Don Quijote de la Mancha
Miguel de Cervantes

–Buena está – dijo Sancho –; fírmela vuestra merced.
–No es menester firmarla – dijo Don Quijote–,
sino solamente poner mi rúbrica.

Primera parte del Ingenioso Caballero
Don Quijote de la Mancha
Miguel de Cervantes