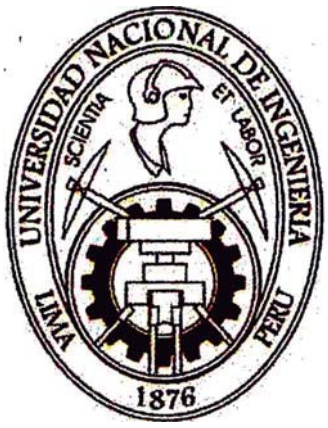
Universidad Nacional de Ingeniería
Facultad de Ciencias
Escuela Profesional de Matemática



Números p-ádicos y racionalidad de la función zeta de una hipersuperficie afín

Por

Rodolfo Canto Torres

Tesis para optar el título profesional de

Licenciado en Matemática

Dr. Christian Holger Valqui Haase

Asesor

Diciembre de 2008

Para a mi abuela
Brigida Condor Guere.

Agradecimientos: A mi asesor Dr. Christian Valqui, por su confianza y orientación durante estos dos ultimos años; a mi amigo Dr. Oswaldo Velasquez, por su invaluable ayuda en la corrección de esta monografía; y a mi familia, por su apoyo incondicional.

Tabla de Símbolos

A continuación enunciaremos las notaciones y símbolos que utilizaremos en este trabajo, algunos son utilizados con frecuencia en el algebra, pero otros seran introducidos para fines específicos.

Símbolo	Significado	Página
$A^\times$	el grupo multiplicativo de elementos invertibles de un anillo A	4
$\mathbb{N}$	el conjunto de números naturales	4
$\mathbb{R}$	el cuerpo de los números reales	4
$\lfloor x \rfloor$	el mayor entero menor al número real x	4
$\text{sen}(x)$	el seno del número real x	5
$\square$	demostración terminada	7
$\mathbb{N}_0$	el conjunto de números naturales unido con 0	9
$\mathfrak{N}$	el conjunto de n-multiindices	9
$A[X_1, \ldots, X_n]$	anillo de polinomios en n variables con coeficientes en A	10
$A[[X_1, \ldots, X_n]]$	anillo de series formales en n variables con coeficientes en A	10
grad $(f(X))$	grado de polinomio $f(X)$	11
$f(X) \mid g(X)$	el polinomio $f(X)$ divide a $g(X)$	11
$\sigma f(X)$	aplicar σ a los coeficientes de $f(X)$	11
$x \equiv y$ mód $\mathfrak{a}$	x es congruente a y módulo el ideal $\mathfrak{a}$	11
$\langle a \rangle$	el ideal generado por a	11
$\mathbb{C}$	el cuerpo de los números complejos	11
$K^{n \times n}$	el conjunto de matrices cuadradas de orden n con entradas en K	12
$\mathcal{S}(B)$	el conjunto de permutaciones de B	12
sig (σ)	el signo de la permutación σ	12
L/K	L es una extensión sobre K	15
$\mathbb{Q}$	el cuerpo de los números racionales	15
$[L : K]$	el grado de la extensión L sobre K	15
$S[A]$	la adjunción de A al anillo S	16
$K(A)$	la adjunción de A al cuerpo K	16
Irr (K, a)	el polinomio minimal de a sobre K	18
L^a	la clausura álgebraica de K en L	19

Símbolo	Significado	Página
$\mathbb{Z}/n\mathbb{Z}$	el anillo cociente de $\mathbb{Z}$ con el ideal $n\mathbb{Z}$	20
$\mathrm{Nu}(\sigma)$	el núcleo de un homomorfismo σ entre anillos (cuerpos o grupos)	22
$A \cong B$	A, B son isomorfos como anillos (cuerpos o grupos)	22
$\mathrm{car}\, K$	la característica del cuerpo K	22
$\binom{m}{n}$	la combinación de m en n	23
$\#A$	el cardinal del conjunto A	31
$G(L/K)$	el grupo de Galois de la extensión de cuerpos	31
$N_{L/K}(a)$	la norma de a sobre la extensión de cuerpos	33
$T_{L/K}(a)$	la traza de a sobre la extensión de cuerpos	33
$\mathbb{F}_q$	un cuerpo de q elementos	38
$\mathrm{ord}\,(x)$	orden de x como elemento de un grupo	40
$\mathrm{mcd}\,(x, y)$	el maximo común divisor de x e y	42
$\lvert\cdot\rvert$	un valor absoluto	46
$\log_c$	la función real logaritmo con base c	48
$(D, \lvert\cdot\rvert)$	dominio provisto de un valor absoluto	47
$\lvert D\rvert$	la imagen de dominio via $\lvert\cdot\rvert$	47
	la base del logaritmo neperiano	49
v_p	la valuación p-ádica	68
$\lvert\cdot\rvert_p$	el valor absoluto p-ádico	70
$\lvert x\rvert_\infty$	el maximo entre x y $-x$	71
$\mathrm{im}\,(\sigma)$	la imagen del homomorfismo σ	75
$\mathbb{Q}_p$	el cuerpo de números p-ádicos	56
$\mathbb{Z}_p$	el anillo de enteros p-ádicos	73
$\mathbb{Q}_p^{alg}$	la clausura algebraica de $\mathbb{Q}_p$	99
$\mathcal{O}_L$	el anillo de valuación sobre una extensión algebraica L sobre $\mathbb{Q}_p$	103
$\mathfrak{p}_L$	el anillo de valuación sobre una extensión algebraica L sobre $\mathbb{Q}_p$	103
$\Bbbk_L$	el cuerpo residual de una extensión algebraica L sobre $\mathbb{Q}_p$	103
$\mu(L)$	el conjunto de raíces de la unidad de L extesión algebraica de $\mathbb{Q}_p$	109
$\mu_{p^\infty}(L)$	el subconjunto de raíces de la unidad de orden una potencia de p en L	109
$\mu_{(p)}(L)$	el subconjunto de raíces de la unidad de orden coprimo a p en L	109
$\mathcal{L}_f$	la extensión no ramificada de grado f sobre $\mathbb{Q}_p$	103

Símbolo	Significado	Página
$\mathbb{C}_p$	el cuerpo de números complejos p-ádicos	121
$\mathfrak{D}_p$	el anillo de valuación de $\mathbb{C}_p$	122
$\mathfrak{d}_p$	el ideal de valuación de $\mathbb{C}_p$	122
$\mathfrak{K}_p$	el cuerpo residual de $\mathbb{C}_p$	122
$\mathfrak{U}_p^m$	el conjunto de raíces m-ésimas de la unidad	122
$\mathcal{T}_p$	el conjunto de representantes de Teichmüller	122
ω_X	la valuación X-ádica sobre $D[[X]]$	126
$\lvert\cdot\rvert_X$	el valor absoluto X-ádico sobre $D[[X]]$	127
$\mathfrak{p}_X$	el ideal de valuación de ω_X	130
$f(X) \circ g(X)$	la composición de las series formales $f(X)$ y $g(X)$	130
$\exp(X)$	la serie formal exponencial	142
$\log(1+X)$	la serie formal logaritmo	142
$\binom{X}{n}$	el n-ésimo polinomio combinatorio	144
$B(X,Y)$	la serie binomial	144
$\mathcal{H}_{f(X)}(L)$	la hipersuperficie afín determinada por $f(X)$ en L	188
$\mathcal{Z}(\mathcal{H}_f/\mathbb{F}_q;T)$	la función zeta de la hipersuperficie afín generada por $f(X)$ sobre $\mathbb{F}_q$	189

Índice general

Capítulo 1

Introducción

Los números p-ádicos fueron creados por el matemático alemán Kurt Hensel alrededor de 1899, publicando el artículo titulado "New foundations of the theory of algebraic numbers". La idea con la cual Hensel desarrolló los números p-ádicos era la de dotar de un desarrollo a los números algebraicos en series de potencias de elementos primos.

En 1907, Hensel introdujo conceptos topológicos al cuerpo de números p-ádicos y desarrolló el análisis correspondiente aplicado a teoría de números. Luego, en 1913, el matemático húngaro József Kürschák introdujo la noción de "valuación", con la cual los números p-ádicos fueron generalizados.

No fue sino hasta 1921 que se dio el primer gran aporte de los números p-ádicos. El matemático alemán Helmut Haase, alumno de Hensel, publicó una disertación acerca de las formas cuadráticas sobre cuerpos numéricos, enunciando el ahora conocido como "principio local-global". Este principio establece la suficiencia de que una forma cuadrática homogénea posea ceros no triviales en los cuerpos p-ádicos y el cuerpo de los números reales para que posea ceros racionales. Otra aplicación de los números p-ádicos fue dada por el matemático noruego Thoralf Skolem. Skolem desarrolló un auto-denominado metódo p-ádico para resolver ciertas ecuaciones diofánticas (estas dos aplicaciones se pueden ver en [1]).

De la resolución de ecuaciones diofánticas derivó el estudio de las soluciones de ecuaciones polinomiales en diversos cuerpos, lo cual produjo el concepto de *hipersuperficie afín* y *variedad algebraica* como la reunión de estas soluciones; de manera similar se definió la noción de variedad proyectiva. En el caso que el cuerpo en cuestion fuese finito, el conteo de estas soluciones originó lo que se conoce como *funciones zeta*, que son series de potencias en una variable. En 1940, André Weil conjeturó propiedades acerca de las funciones zeta sobre variedades projectivas. La primera de esta conjeturas era la racionalidad (como función en una variable) de las

funciones zeta. En 1959, Bernard Dwork dió la primera demostración de esta incógnita, para lo cual utilizó el análisis p-ádico para probar la racionalidad de toda función zeta para el caso de una hipersuperficie afín, lo cual es suficiente para establecer la afirmación en otros casos.

El objetivo de esta tesis es estudiar las herramientas p-ádicas necesarias para demostrar la racionalidad de una función zeta, siguiendo un desarrollo similar al dado en [9].

En la actualidad los números p-ádicos constituyen una herramienta avanzada en diversas ramas de la matemática, por ejemplo en el análisis harmónico y la teoría de ondiculas (ver el reciente libro [14]). Del mismo modo, los números p-ádicos han despertado interés dentro de la física matemática (vea por ejemplo [15]).

1.1. Organización del trabajo

Este trabajo está dividido en ocho capítulos, repartidos de la siguiente forma:

- En el primer capítulo revisaremos algunas nociones elementales y notaciones del álgebra y del análisis real que se estudian de manera superficial en cursos de pregrado, siendo tal vez el ítem menos conocido una fórmula de los coeficientes del polinomio característico de una matriz.

- El segundo capítulo esta dedicado a las nociones básicas de teoría de cuerpos, constituyendo parte del lenguaje con el que desarrollaremos la teoría algebraica del cuerpo de números p-ádicos, que denotaremos por $\mathbb{Q}_p$. Entre estos se encuentran los diferentes tipos de extensiones de un cuerpo, las importantísimas nociones de norma y traza de una extensión finita y un breve resumen sobre los cuerpos finitos.

- El tercer capítulo contiene las ideas de valuación y valor absoluto sobre un dominio, siendo de mayor interés para nosotros el estudio de los valores absolutos no arquimedianos. Daremos la noción de cuerpo completo y compleción, con la cual construiremos $\mathbb{Q}_p$. También definiremos y estudiaremos la noción de serie convergente respecto a un valor absoluto no arquimediano.

- En el cuarto capítulo empezaremos con nuestro principal objeto de estudio, definiendo la valuación p-ádica. Luego, definiremos el cuerpo de números p-ádicos como la compleción de $\mathbb{Q}$ con el valor absoluto p-ádico $|\cdot|_p$. Luego, llevaremos a cabo nuestro estudio de $\mathbb{Q}_p$ por medio del importantísimo anillo de enteros p-ádicos $\mathbb{Z}_p$, por medio del cual estudiaremos a $\mathbb{Q}_p$. Mostraremos que los elementos de este anillo se expresan de manera única como

serie de potencias en base p. Estableceremos el célebre lema de Hensel y otros resultados acerca de factorización en $\mathbb{Z}_p[X]$.

- Iniciaremos el quinto capítulo con una breve mirada a los espacios normados sobre un cuerpo completo arbitrario, con el objetivo de extender $|\cdot|_p$ sobre las extensiones finitas de $\mathbb{Q}_p$. Luego, estudiaremos los distintos tipos de extensiones bajo la nocion de "índice de ramificación", estableciendo resultados importantes sobre la clausura algebraica de $\mathbb{Q}_p$. Finalizamos construyendo el cuerpo más transcendente de este trabajo, el cuerpo de números complejos p-ádicos, que es el análogo p-ádico de $\mathbb{C}$.

- En el sexto capítulo, desarrollaremos herramientas formales para establecer distintas propiedades sobre el anillo de series formales en varias variables, entre estas la composición de series formales y el producto infinito de estas. Presentamos además la serie formal más útil de nuestro trabajo, la *serie binomial*, así como su relación con las series formales exponencial y logaritmo.

- En el penúltimo capítulo, desarrollaremos una breve introdución al análisis p-ádico introduciendo series de potencias p-ádicas. Luego, estableceremos uno de los más importantes resultados acerca de series de potencias en $\mathbb{Q}_p$: el teorema p-ádico de preparación de Weierstrass. Aquí también construiremos una importante serie formal para nuestro trabajo, la cual pertenecerá a $\mathbb{Z}_p[[X,Y]]$. Finalizamos el capítulo con un breve estudio acerca $\mathbb{C}_p[[X]]$ como espacio vectorial y estableciendo una noción, conveniente para nosotros, de traza y serie característica para cierto conjunto de operadores lineales.

- Culminamos este trabajo cumpliendo el objetivo principal: demostrar el teorema de Dwork para hipersuperficies afines por medio del análisis p-ádico. Empezaremos por establecer algunas propiedades de la función zeta de una hipersuperficie. Luego utilizaremos tanto nociones algebraicas como analíticas acerca de $\mathbb{C}_p$ para establecer que toda función zeta es cociente de series de potencias que convergen en todo $\mathbb{C}_p$, con lo cual culminaremos la demostración del teorema de Dwork.

Capítulo 2

Preliminares

En este trabajo sólo estaremos interesados en anillos conmutativos con unidad, a los cuales denominaremos simplemente *anillos*. Además denotaremos al conjunto de los elementos invertibles de un anillo A por $A^\times$.

2.1. Series dobles

En esta sección, entederemos por *sucesión doble en* $\mathbb{R}$ a toda función $a : \mathbb{N} \times \mathbb{N} \to \mathbb{R}$. Denotaremos cada elemento $a(m,n)$ por $a_{m,n}$, y a la función a por $(a_{m,n}) \subset \mathbb{R}$.

La siguiente definición generaliza el concepto de límite de una sucesión.

Definición 2.1.1 Dada una sucesión doble $(a_{m,n}) \subset \mathbb{R}$, diremos que esta *converge a* $\alpha \in \mathbb{R}$, cuando para cada $\epsilon > 0$, exista $T \in \mathbb{N}$ tal que $|a_{m,n} - \alpha| < \epsilon$, siempre que $m, n \geq T$. En caso que $(a_{m,n})$ converja a algún número real, simplemente diremos que es *convergente*.

Ejemplos 2.1.2

1. Sea $(a_{m,n}) \subset \mathbb{R}$ definida por $a_{m,n} = 2^{-m-n}$ para cada $m, n \in \mathbb{N}$. Esta sucesión converge a 0; pues, dado $\epsilon > 0$, basta tomar $T \in \mathbb{N}$ tal que $2^{-T} < \epsilon$ para obtener que $m, n \geq T$ implique $|a_{m,n}| \leq 2^m \leq 2^T < \epsilon$.

2. Sea $(b_{m,n}) \subset \mathbb{R}$ definida por $b_{m,n} = \frac{m+n}{mn}$. Esta sucesión también converge a cero. De hecho, dado $\epsilon > 0$, eligimos $T \in \mathbb{N}$ tal que $1/\epsilon < T$ para obtener que la condición $m \geq n \geq T$ implica $|b_{m,n}| \leq \frac{2m}{mn} \leq 1/T < \epsilon$.

3. Si $(c_{m,n}) \subset \mathbb{R}$ es dada por $c_{m,n} = n/m$, entonces para cualquier $\alpha \in \mathbb{R}$ y $T \in \mathbb{N}$, basta tomar $m = T$ y $n = (\lfloor |\alpha| \rfloor + 2)T$ para obtener que $|\alpha - c_{m,n}| \geq |c_{m,n}| - |\alpha| \geq \lfloor |\alpha| \rfloor + 2 - |\alpha| > 1$, aunque $m, n \geq T$. Por lo tanto, la sucesión doble $(c_{m,n})$ no converge.

Otro posible proceso de límite en una sucesión doble es el siguiente. Sea $(a_{m,n}) \subset \mathbb{R}$, si existiese $\lim_m a_{m,n}$ para cada $n \in \mathbb{N}$, entonces podríamos definir una sucesión $(b_n) \subset$ tomando $b_n = \lim_m a_{m,n}$ y establecer si esta sucesión posee límite. Análogamente, si existe $\lim_n a_{m,n}$ para cada $m \in \mathbb{N}$, entonces podemos estudiar la convergencia de la sucesión conformada por $c_m = \lim_n a_{m,n}$. De existir la sucesión (b_n) o (c_m), y/o sus límites correspondientes, nos referiremos a estos por *límites iterados.*

Ejemplos 2.1.3

- En los ejemplos previo, la tercera sucesión doble $(c_{m,n})$ no posee los límites $\lim_n c_{m,n}$, para ningún $m \in \mathbb{N}$. Sin embargo, existen los límites $\lim_m c_{m,n}$ para cada $n \in \mathbb{N}$, siendo todos estos nulos. Así pues, se da el caso en que un límite iterado existe y el otro ni siquiera se puede formular.

- Si $(d_{m,n}) \subset \mathbb{R}$, es dado por $d_{m,n} = m/(m+n)$. Entonces, dado $r, s \in \mathbb{N}$ se tiene que $a_r = \lim_{n\to\infty} d_{r,n} = 0$ y $b_s = \lim_{m\to\infty} d_{m,s} = 1$. Por lo tanto, $d_{m,n}$ posee límites iterados distintos.

Observaciones 2.1.4

- Puede darse el caso que los límites iterados no existan y sin embargo exista el límite de una sucesión doble, vea por ejemplo $a_{m,n} = \dfrac{\operatorname{sen}(\max\{m,n\})}{\min\{m,n\}}$.

- Si una sucesin doble $(a_{m,n})$ converge a $\alpha \in \mathbb{R}$, entonces la sucesión *diagonal* $(a_{n,n})$ converge también a α.

Otro concepto que generalizaremos es el de serie.

Definición 2.1.5 Sea $(a_{m,n}) \subset \mathbb{R}$.

- La *serie doble de sumandos* $a_{m,n}$ es la sucesión doble $(s_{m,n})$ determinada por las sumas parciales $s_{m,n} = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{m,n}$, a este serie doble la denotaremos por $\sum a_{m,n}$.

- Una serie $\sum a_{m,n}$ converja si $\alpha \in \mathbb{R}$ significa que la sucesión doble $s_{m,n}$ converge, al número real al cual converge esta serie lo denotamos por $\sum_{m,n} a_{m,n}$.

Análogamente al caso de sucesiones dobles, también podríamos definir la noción de límites iterados, para cuando existan los límites correspondientes a cada natural n y m, que vendrían a ser los límites iterados de la sucesión de sumas parciales. Sin embargo necesitaremos de una noción más fuerte.

Definición 2.1.6 Sea $\sum a_{m,n}$ una serie doble. Supongamos que existen los límites

$$\sum_{m=1}^{\infty} a_{m,n}, \text{ para todo } n \in \mathbb{N} \qquad \text{y} \qquad \sum_{n=1}^{\infty} a_{m,n}, \quad \text{para cada } m \in \mathbb{N}.$$

Denominaremos a los límites $\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} a_{m,n}$ y $\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} a_{m,n}$, los *límites iterados* de $\sum a_{m,n}$.

Observación 2.1.7 Esta definición es un caso particular de que existan los límites iterados de la sucesión de sumas parciales.

Ahora enfocaremos nuestra atención al caso en que la serie doble sea construida a partir de sumandos no negativos. Estudiar este caso particular nos brindará propiedades con respecto a otro tipo de serie que necesitaremos analizar.

Proposición 2.1.8 *Sea $(a_{m,n}) \subset \mathbb{R}$ con términos no negativos, y $(s_{m,n})$ la respectiva sucesión doble de sumas parciales. Entonces*

1. *Si $(s_{n,n}) \subset \mathbb{R}$ converge a $S \in \mathbb{R}$, entonces $\sum a_{m,n} = s_{m,n}$ también converge a S.*
2. *Si $\sum a_{m,n}$ es convergente, entonces las series iteradas $\sum_m \sum_n a_{m,n}$ y $\sum_n \sum_m a_{m,n}$ existen y coinciden con $\sum_{m,n} a_{m,n}$.*
3. *Si alguna serie iterada converge, entonces la otra serie iterada y la serie doble también convergen; más aún estas convergen al mismo número real.*

Demostración.- Denotemos a cada $s_{n,n}$ por σ_n, para todo $n \in \mathbb{N}$, obteniendo asi una sucesión de números reales positivos.

1. Por hipótesis (σ_n) converge a S, de modo que para cada $\epsilon > 0$, existe $T \in \mathbb{N}$ tal que

   $$|\sigma_n - S| < \epsilon, \text{ para todo } n \geq T.$$

   Entonces, dados $m, n \geq T$ obtenemos que $\sigma_T \leq s_{m,n} \leq \sigma_{m+n} \leq S$, por lo tanto $|s_{m,n} - S| \leq |\sigma_T - S| < \epsilon$.

2. Por las observaciones 2.1.4, tendremos que la sucesión $(\sigma_n) \subset \mathbb{R}$ converge a $\sum_{m,n} a_{m,n}$ que denotamos por S. Dado $m \in \mathbb{N}$, tenemos que

   $$\sum_{j=0}^{n} a_{m,j} \leq \sum_{i=0}^{m}\sum_{j=0}^{n} a_{m,n} = s_{m,n} \leq \sigma_{m+n} \leq S, \quad \text{para todo } n \in \mathbb{N};$$

por tanto existe $\sum_n a_{m,n} \leq S$. Más aun,

$$\sigma_m \leq \sum_{i=1}^{m} \sum_{n} a_{i,n} = \lim_{n\to\infty} \sum_{j=1}^{n} \sum_{i=1}^{m} a_{i,j} \leq \lim_{n\to\infty} \sum_{j=1}^{n} \sum_{i=1}^{n} a_{i,j} = \lim_{n} \sigma_n = S,$$

Gracias a esta última desigualdad, la sucesión $(\sum_n a_{m,n})_{m\in\mathbb{N}} \subset \mathbb{R}$ es convergente, por lo tanto existe $\sum_m \sum_n^n a_{i,j}$ y coincide con S; de forma análoga verificamos que la otra serie iterada converge y es igual S.

3. Supongamos que $\sum_m \sum_n a_{m,n}$ es convergente, entonces

$$\sigma_m \leq \sum_{i=1}^{m} \sum_{n} a_{i,n} \sum_{m} \sum_{n} a_{m,n}, \quad \text{para cada } m \in \mathbb{N};$$

porque $a_{m,n} \geq 0$. Por lo tanto, la sucesión creciente $(\sigma_m) \subset \mathbb{R}$ es acotada, luego será convergente a $S \in \mathbb{R}$, y utilizando *1.* y *2.* concluimos.

□

El siguiente tipo de serie es el motivo por el cual se hizo la presente sección, pues como veremos su convergencia conservará las mismas propiedades que menciona la proposición previa acerca de las series dobles de sumandos no negativos.

Definición 2.1.9 Sea $\sum a_{m,n}$ una serie doble en $\mathbb{R}$, diremos que es *absolutamente convergente* si la serie doble $\sum |a_{m,n}|$ es convergente.

Proposición 2.1.10 *Si $\sum a_{m,n}$ una serie doble en $\mathbb{R}$ es absolutamente convergente, entonces*

1. *$\sum a_{m,n}$ es convergente.*
2. *las series iteradas existen y convergen hacia $\sum_{m,n} a_{m,n}$.*

Demostración.-

1. Denotemos por $s_{m,n}$ y $\bar{s}_{m,n}$ las sumas parciales $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{m,n}$ y $\sum_{j=1}^{n} \sum_{i=1}^{m} |a_{m,n}|$, respectivamente; así también denotamos $\sigma_n = s_{n,n}$ y $\bar{\sigma}_n = \bar{s}_{n,n}$, para cada $n \in \mathbb{N}$. Entonces, cuando $m \geq n$ tendremos que

$$|\sigma_m - \sigma_n| \leq |\sum_{i=n+1}^{m} \sum_{j=1}^{n} a_{i,j} + \sum_{i=1}^{m} \sum_{j=n+1}^{m} a_{i,j}| \leq \sum_{i=n+1}^{m} \sum_{j=1}^{n} |a_{i,j}| + \sum_{i=1}^{m} \sum_{j=n+1}^{m} |a_{i,j}| = \bar{\sigma}_m - \bar{\sigma}_n,$$

por lo tanto $|\sigma_m - \sigma_n| \leq \bar{\sigma}_m - \bar{\sigma}_n$, para $m \geq n$. Es claro que esto es suficiente para concluir que $(\sigma_n) \subset \mathbb{R}$ es de Cauchy, por lo tanto convergente a algún $S \in \mathbb{R}$. Más aun, dados $m \geq n$ tendremos que

$$|s_{m,n} - \sigma_n| = |\sum_{i=n+1}^{m} \sum_{j=1}^{n} a_{i,j}| \leq \sum_{i=n+1}^{m} \sum_{j=1}^{n} |a_{i,j}| = \bar{\sigma}_m - \bar{\sigma}_n. \tag{2.1}$$

Ahora, dado $\epsilon > 0$ tomemos $T \in \mathbb{N}$ tal que $m, n \geq T$ impliquen $|\bar{\sigma}_m - \bar{\sigma}_n| < \epsilon/2$ y $|S - \sigma_n| < \epsilon/2$. Entonces, si $m \geq n \geq T$ tendremos que

$$|s_{m,n} - S| \leq |s_{m,n} - \sigma_n| + |\sigma_n - S| \leq |\bar{\sigma}_m - \bar{\sigma}_n| + |\sigma_n - S| < \epsilon.$$

Esta misma desigualdad se cumple cuando $n \geq m \geq T$, gracias a la desigualdad análoga a (2.1).

2. Tan sólo verifiquemos que $\sum_m \sum_n a_{m,n} = \sum_{m,n} a_{m,n}$, pues de manera análoga se muestra la igualdad de $\sum_{m,n} a_{m,n}$ con la otra serie iterada, y por tanto la igualdad entre estas series iteradas. Puesto que la serie doble $\sum |a_{m,n}|$ es convergente, sus respectivas series iteradas también convergen. En particular, como existe $\sum_m \sum_n |a_{m,n}|$, dado $m \in \mathbb{N}$ la serie $(\sum_{j=1}^{n} a_{m,n})_{n \in \mathbb{N}} \subset \mathbb{R}$ es absolutamente convergente, más aun

$$\sum_{i=1}^{m} |\sum_{j=1}^{\infty} a_{i,j}| \leq \sum_{i=1}^{m} \sum_{j=1}^{\infty} |a_{i,j}| \leq \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} |a_{i,j}|, \quad \text{para cualquer } m \in \mathbb{N};$$

por tanto $(\sum_{i=1}^{m} (\sum_n a_{i,n}))_{m \in \mathbb{N}} \subset \mathbb{R}$ es absolutamente convergente, y en consecuencia existe $\sum_m \sum_n a_{m,n}$. Finalmente, dado $m \in \mathbb{N}$

$$\begin{aligned} \Big|\sum_{i=1}^{m} \sum_{j=1}^{\infty} a_{i,j} - \sum_{i=1}^{m} \sum_{j=1}^{m} a_{i,j}\Big| &= \Big|\sum_{i=1}^{m} \sum_{j=m+1}^{\infty} a_{i,j}\Big| \leq \sum_{j=m+1}^{\infty} \sum_{i=1}^{m} |a_{i,j}| \\ &\leq \sum_{j=m+1}^{\infty} \sum_{i=1}^{\infty} |a_{i,j}| \\ &\leq \Big|\sum_{j=1}^{\infty} \sum_{i=1}^{\infty} a_{i,j} - \sum_{j=1}^{m} \sum_{i=1}^{\infty} a_{i,j}\Big|. \end{aligned}$$

Esta última desigualdad nos ayuda a concluir que

$$\lim_{m \to \infty} (\sum_{j=1}^{m} \sum_{i=1}^{\infty} a_{i,j} - \sigma_m) = 0, \quad \text{y por lo tanto } \sum_m \sum_n a_{m,n} = \sum_{m,n} a_{m,n}.$$

□

Corolario 2.1.11 *Si $\sum a_{m,n}$ es una serie doble tal que alguna de las series iteradas de la serie doble $\sum |a_{m,n}|$ sea convergente, entonces las series iteradas de $\sum a_{m,n}$ existen y convergen al mismo número real.*

Demostración.- Por la proposición 2.1.8, obtendremos la convergencia de la serie doble $\sum |a_{m,n}|$, lo que significará que $\sum a_{m,n}$ es absolutamente convergente. Luego, las series iteradas $\sum_m \sum_n a_{m,n}$ y $\sum_m \sum_n a_{m,n}$ existen y son iguales. □

2.2. Anillo de series formales y anillo de polinomios de varias variables

En esta sección formalizaremos la noción de polinomios y series de potencias que conocemos del cálculo, donde son funciones que se expresan por sumas de potencias de la variable en cuestión (que en el caso de series de potencias es una suma infinita). Apelaremos al conocimiento previo de la construcción del anillos de polinomios en una variable para poder realizar esta construcción que es mucho más general.

Empecemos por recordar que una sucesión en un conjunto A no es más que una función de $\mathbb{N}$ en A. Esto se generaliza a sucesiones cuyo primer término es indexado por cualquier entero fijo. En particular, cuando empieza en 0, tendremos una función de $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ en A. Así tambiénemplearemos la terminologia de *sucesión multiindexada* para denominar a una función $x : N_0^n \to A$, para algún $n \in \mathbb{N}$ fijo; además denotaremos a $x(u)$ por x_u, para todo $u \in \mathbb{N}_0^n$.

Fijemos $n \in \mathbb{N}$ y A un anillo, tomemos $\mathfrak{N} = \mathbb{N}_0^n$ y denotemos por $\mathfrak{A}_n$ al conjunto de las sucesiones multiindexadas por $\mathfrak{N}$ con términos en A.

Definamos las operaciones $\oplus$ y $\odot$ en $\mathfrak{A}$ por

$$(f \oplus g)_w = f_w + g_w \qquad \text{y} \quad (f \odot g)_u = \sum_{u+v=w} f_u g_v \qquad \text{para todo } w \in \mathfrak{N},$$

para todo par de elementos $f, g \in \mathfrak{A}_n$. Es fácil ver que $(\mathfrak{A}_n, \oplus)$ es un grupo abeliano cuyo elemento nulo $\mathbf{0}$ es la sucesión que posee sólo términos nulos. Así también se puede verificar $(\mathfrak{A}, \odot)$ es un monoide conmutativo[1] con elemento neutro, el cual es dado por la sucesión que posee como único término no nulo al primero con valor 1.

Denotemos por $\mathfrak{A}_{(n)}$ al conjunto de las sucesiones nulas salvo un número finito de términos, esto es

$$\mathfrak{A}_{(n)} = \{f \in \mathfrak{A}_m \,;\, \{u \in \mathfrak{N} \,,\, a_u \neq 0\} \text{ es finito}\}.$$

Veamos que este conjunto es un subanillo de $\mathfrak{A}_n$. Para esto, dado $f \in \mathfrak{A}_{(n)}$ escribiremos $\mathcal{Z}_f = \{u \in \mathfrak{N} \,;\, f_u \neq 0\}$, de donde para $f, g \in \mathfrak{A}_{(n)}$, tendremos que

$$\mathcal{Z}_{f \oplus g} \subset \mathcal{Z}_f \cup \mathcal{Z}_g \quad \text{y} \quad \mathcal{Z}_{f \odot g} \subset \{u = (u_1, \ldots, u_n) \in \mathfrak{N} \,;\, u_i \leq M + N\}$$

donde M, N son cotas para $\mathcal{Z}_f$ y $\mathcal{Z}_g$.

Procedamos a realizar algunas notaciones con el objetivo de comprender mejor este anillo.

[1] Un monoide $(M, *)$ es un par conformado por un conjunto M y una operación $* : M \times M \to M$ que es asociativa.

- La sucesión $\delta^{(u)} \in \mathfrak{A}_{(n)}$ es aquella que posee un único término no nulo se posiciona en u con valor 1.

- El elemento $e_i \in \mathfrak{N}$ es aquella que posee $i-$ésima componente es igual a 1 y es la única no nula.

- Para cada $i \in \{1, 2, \ldots, n\}$ definamos $X_i \in \mathfrak{A}_{(n)}$ como $X_i = \delta^{(u)}$.

De la definición de producto en $\mathfrak{A}_{(n)}$, no es dificil ver que

$$\delta^{(u)} \odot \delta^{(v)} = \delta^{(u+v)}, \qquad \text{para todo } u, v \in \mathfrak{N}.$$

Que en el caso particular de u de la forma e_i nos da

- $X_i^m = \underbrace{X_i \odot X_i \odot \cdots \odot X_i}_{m\text{veces}} = \delta^{(me_i)}$., para todo $m \in \mathbb{N}_0$.

- $X_1^{m_1} \odot X_2^{m_2} \odot \cdots \odot X_n^{m_n} = \delta^{(u)}, \qquad$ para todo $u = (m_1, m_2, \ldots, m_n) \in \mathfrak{N}$.

  Esto nos induce a escribir $X^u = X^{m_1} \odot \cdots \odot X^{m_n} = \delta^{(u)}$, que cumple

$$X^{u+v} = X^u \odot X^v \qquad \text{para cualesquiera } u, v \in \mathfrak{N}.$$

Por otra parte, podemos inducir un monomorfismo ι de A hacia $\mathfrak{A}_{(n)}$ tomando como $\iota(a)$ la sucesión cuyo primer término es igual a a y es el único no nulo; por lo tanto podemos suponer que $A \subset \mathfrak{A}_{(n)}$. De esto, podemos inferir que $(a \odot f)_u = af_u$, para todo $u \in \mathfrak{N}, f \in \mathfrak{A}_n$. En consecuencia, tomando $f \in \mathfrak{A}_{(n)}$ tendremos que

$$f = \sum_{u \in \mathcal{Z}_f} (f(u) \odot X^u),$$

teniendo sentido la anterior suma por la finitud de $\mathcal{Z}_f$. En adelante, abusando de la notación, expresaremos a un elemento f de $\mathfrak{A}_n$ por

$$f = \sum_{u \in \mathfrak{N}} f_u X^u,$$

lo cual se conoce como una suma formal.

Definición 2.2.1 El anillo $\mathfrak{A}_n$ es denominado *anillo de series formales en n variables con coeficientes en A*, que denotaremos por $A[[X_1, \ldots, X_n]]$. De forma similar $\mathfrak{A}_{(n)}$ es denominado *el anillo de polinomios* y es denotado por $A[X_1, \ldots, X_n]$.

2.3. Anillo de polinomios en una variable

Definición 2.3.1 Sea A un anillo y $f(X) = a_0X + \cdots + a_nX^n \in A[X]$ no nulo. Denominaremos *grado* de $f(X)$ a $\max\{m; a_m \neq 0\}$, a este número entero lo denotaremos por grad $f(X)$.

Definición 2.3.2 Dados $f(X), g(X) \in A[X]$, donde A es un anillo, diremos que $f(X)$ *divide* a $g(X)$ si existe algún $h(X) \in A[X]$ tal que $g(X) = f(X)h(X)$; este hecho lo denotará por $f(X) \mid g(X)$.

De manera natural, podemos asociar a todo polinomio $f(X) = a_0 + \cdots + a_nX^n \in A[X]$ una función $\widetilde{f} : A[X] \to A[X]$ definida por $\widetilde{f}(a) = a_0 + \cdots + a_na^n$. En adelante, cuando haya peligro de confusión denotaremos por $\mathcal{E}(f, a)$ la evaluación de $\widetilde{f}$ en a; en caso contrario simplemente utilizaremos la notación f para denotar $\widetilde{f}$.

Dado un homomorfismo de anillos $\sigma : A \to B$, podemos obtener una extensión $\widetilde{\sigma} : A[X] \to B[X]$, definiendo

$$\widetilde{\sigma}(f(X)) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n,$$

cuando $f(X) = a_0 + a_1X + \cdots + a_nX^n$. En adelante, siempre que el contexto lo permita, simplificaremos $\widetilde{\sigma}\big(f(X)\big)$ por $\sigma f(X)$. Con esta notación podemos obtener $\mathcal{E}(\sigma f(X), \cdot) : B \to B$; más aun

$$\sigma\big(f(a)\big) = \sigma\Big(\mathcal{E}\big(f(X), a\big)\Big) = \mathcal{E}\big(\sigma f(X), \sigma(a)\big) = \sigma f\big(\sigma(a)\big), \quad \text{para todo } a \in A.$$

Ejemplo 2.3.3 Si A es un anillo y $\mathfrak{a}$ es un ideal de A, entonces la proyección $\pi : A \to A/\mathfrak{a}$ se extiende a $\widetilde{\pi} : A[X] \to A/\mathfrak{a}[X]$. Es clara la equivalencia entre

$$f(X) - g(X) \in \mathfrak{a}[X] \quad \text{y} \quad \pi f(X) = \pi g(X),$$

la cual será denotada por

$$f(X) \equiv g(X) \text{ mód } \mathfrak{a}.$$

Más aun, cuando $\mathfrak{a}$ sea principal, esto es $\mathfrak{a} = \langle a \rangle$ la notación quedará simplificada a

$$f(X) \equiv g(X) \text{ mód } a.$$

2.4. Tópicos de álgebra lineal

En lo que sigue, K denotará un cuerpo cualquiera. Si bien muchas de las demostraciones de los hechos a detallar en la presente sección se encuentran sus contextos originales (ver [5, 6, 11]) establecidas en el caso real o complejo ($K = \mathbb{R}$ o $K = \mathbb{C}$), estas son válidas en el caso general; haremos las restricciones necesarias en casos particulares.

Definición 2.4.1 Sea K un cuerpo, V un K-espacio vectorial y $n \in \mathbb{N}$. Diremos que una n-multilineal $\varphi : V^n \to K$ es *alternada* si

$\varphi(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = 0$ siempre que existan $i \neq j, 1 \leq i, j \leq n$ tales que $x_i = x_j$.

Observación 2.4.2 En el caso que la característica de K sea distinta de 2, una n-multilineal φ será alternada si y sólo si

$$\varphi(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = -\varphi(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n), \text{ para todo } i \neq j \, , 1 \leq i, j \leq n. \tag{2.2}$$

La condición anterior es necesaria en el caso que la característica de K sea 2, mas no suficiente. De hecho, la bilineal simétrica $b : (\mathbb{Z}/2\mathbb{Z})^2 \to (\mathbb{Z}/2\mathbb{Z})$ definida por $b\big((x_1, y_1), (x_2, y_2)\big) = x_1x_2 + y_1y_2$ satisface (2.2), pero no es alternada.

Definición 2.4.3 Sea K un cuerpo y $n \in \mathbb{N}$. Definimos la función *determinante* $\det : K^{n\times n} \to K$ como la única n-multilineal alternada sobre las filas de una matriz tal que $\det(I) = 1$, donde I denota la matriz identidad.

En adelante, asumiremos muchos hechos acerca del determinante que son ampliamente utilizados en $\mathbb{R}$ o $\mathbb{C}$, tales como la caracterización de matrices invertibles como aquellas con determinante no nulo, el hecho que el determinante es una función alternada respecto a las filas, su comportamiento respecto a las operaciones elementales, etc.

Definición 2.4.4 Sean K un cuerpo y $A \in K^{n\times n}$.

- El *polinomio característico* de A es $\det(A - XI) \in K[X]$.
- Un *autovalor* de A es una raíz del polinomio característico de A.

Lema 2.4.5 *Sean K un cuerpo y $A = [a_{i,j}] \in K^{n\times n}$, el polinomio característico de A posee coeficiente principal igual a $(-1)^n$ y grado n, y su coeficiente m-ésimo es de la forma*

$$(-1)^m \sum_{B\in\mathcal{P}_{n-m}} \sum_{\sigma\in\mathcal{S}(B)} (-1)^{\operatorname{sig}(\sigma)} \prod_{i\in B} a_{i\sigma(i)}, \qquad \text{para } m = 0, 1, \ldots, n-1;$$

donde $\mathcal{P}_k$ es la colección de subconjuntos de $\{1, 2, \ldots, n\}$ con k elementos, $\mathcal{S}(B)$ es el conjunto de permutaciones de B y $\operatorname{sig}(\sigma)$ es el signo de la permutación σ.

Demostración.- Denotemos por $\mathcal{S}_n$ el conjunto de permutaciones de $1, 2, \ldots, n$ y definamos, para $i, j \in \{1, 2, \ldots, n\}$, $\delta_{ij} = 0$ cuando $i \neq j$ y $\delta_{ij} = 1$ cuando $i = j$. Entonces,

$$\det(A - XI) = \sum_{\sigma\in\mathcal{S}_n} (-1)^{\operatorname{sig}(\sigma)} (a_{1\sigma(1)} - \delta_{1\sigma(1)})(a_{2\sigma(2)} - \delta_{2\sigma(2)}) \cdots (a_{n\sigma(n)} - \delta_{n\sigma(n)}).$$

Por tanto, $\det(A - XI)$ es la suma de monomios de grado a lo más n. Ahora, para $i \in \{1, 2, \ldots, n\}$, $\sigma \in \mathcal{S}_n$ definamos

$$f_{i,\sigma}(X) = a_{i,\sigma(i)} - \delta_{i\sigma(i)}X = d_{i\sigma}^{(0)} + d_{i\sigma}^{(1)}X.$$

Esta notación nos permite escribir

$$\det(A - XI) = \sum_{\sigma \in \mathcal{S}_n} (-1)^m f_{1,\sigma}(X) f_{2,\sigma}(X) \cdots f_{n,\sigma}(X);$$

en consecuencia, si c_m es el coeficiente m-ésimo de $\det(A - XI)$, este será de la forma

$$c = \sum_{\sigma \in \mathcal{S}_n} \sum_{j_1 + \cdots + j_n = m} d_{1\sigma}^{(j_1)} d_{2\sigma}^{(j_1)} \cdots d_{n\sigma}^{(j_n)} = \sum_{j_1 + \cdots + j_n = m} \sum_{\sigma \in \mathcal{S}_n} d_{1\sigma}^{(j_1)} d_{2\sigma}^{(j_1)} \cdots d_{n\sigma}^{(j_n)},$$

pues la colección de $n-$adas $(j_1, \ldots, j_n)$ cuyas componentes suman m no depende de σ. Más aun, puesto que cada j_i puede ser 0 o 1, podemos establecer una correspondencia entre las n-adas $(j_1, \ldots, j_n)$ cuyas componentes suman m y los elementos de $\mathcal{P}_{m-n}$ por $(j_1, \ldots, j_n) \mapsto \{i \,;\, j_i = 0\}$. Luego

$$c_m = \sum_{B \subset \mathcal{P}_{n-m}} \sum_{\sigma \in \mathcal{S}_n} \prod_{i \in B} a_{i\sigma(i)} \prod_{i \notin B} (-\delta_{i\sigma(i)}).$$

Ahora, podemos ver que los sumandos no nulos correspondientes a un subconjunto B serán nulos siempre que σ no sea la identidad en el complemento de B. En caso que esto no ocurra, tendremos que $\sigma_{|B} \in \mathcal{S}(B)$. Denotemos por $\mathcal{S}'(B)$ al conjunto de todas estas permutaciones. Cuando $m = n$, tendremos que $\mathcal{P}_0 = \{\emptyset\}$, $\mathcal{S}'() = \{\mathrm{id}\}$ y $c_m = (-1)^n$. Si $m < n$, vemos que $\sigma \mapsto \sigma_{|B}$ es una biyección entre $\mathcal{S}'(B)$ y $\mathcal{S}(B)$, además conserva el signo de la permutación. Esto concluye la demostración. □

La siguiente definición será la "versión" de polinomio característico que utilizaremos en este texto.

Definición 2.4.6 Sean K un cuerpo y $A \in K^{n \times n}$, definimos el *polinomio característico conjugado de* A por $\det(I - XA) \in K[X]$.

Corolario 2.4.7 *Sean K un cuerpo y $A = [a_{i,j}] \in K^{n \times n}$, el polinomio característico conjugado de A posee coeficiente independiente igual a 1, grado a lo más n y su coeficiente m-ésimo es de la forma*

$$(-1)^m \sum_{B \in \mathcal{P}_m} \sum_{\sigma \in \mathcal{S}(B)} \left((-1)^{\mathrm{sig}(\sigma)} \prod_{i \in B} a_{i\sigma(i)} \right), \qquad \text{para } m = 1, 2, \ldots, n.$$

Demostración.- No es difícil ver que $\det(I - XA) = (-1)^n\Big(X^n \det\big(A - (1/X)I\big)\Big)$, luego el coeficiente m-ésimo del polinomio característico conjugado de A es el coeficiente $(n-m)$-ésimo del polinomio característico de A multiplicado por $(-1)^n$. El lema anterior concluye esta prueba. □

Capítulo 3

Teoría de cuerpos

Este capítulo es un resumen de las definiciones y resultados acerca de extensiones de cuerpos que utilizaremos más adelante. Puesto que no forman parte del objetivo de esta monografía, obviaremos las demostraciones de la mayoria de lemas, teoremas, etc., las cuales pueden ser encontradas en muchos libros, tales como [4] y [13]. Sin embargo, daremos la prueba de algunos resultados que construimos con fines muy particulares.

3.1. Extensión de un cuerpo

Definición 3.1.1 Sean L y K cuerpos, L se denomina *extensión de* K cuando K es subcuerpo de L, y lo denotaremos por L/K. Más generalmente, el par (L, i) es llamado extensión de K, cuando $i : K \to L$ es un monomorfismo.

Ejemplos 3.1.2

- $\mathbb{R}$ es una extensión de $\mathbb{Q}$, $\mathbb{C}$ una extensión de $\mathbb{R}$.
- $(\mathcal{Q}(K[X]), i)$ es una extensión de K con el homomorfismo canónico de injección i, donde $\mathcal{Q}(\mathcal{D})$ denota al cuerpo de fracciones del dominio D.

No es difícil ver que una extensión de un cuerpo K puede ser vista como un K-espacio vectorial. Por tanto la siguiente definición tiene sentido.

Definición 3.1.3 Dada una extensión L de K, la dimensión de L como K-espacio vectorial se denomina *grado* de L sobre K, lo que denotaremos por $[L : K]$. Si el grado $[L : K]$ es finito diremos que L/K es *finita*, en caso contrario L/K será denominado *infinita*.

Ejemplos 3.1.4

- La extensión $\mathcal{Q}(K[X])/K$ es infinita, pues contiene a un conjunto $l.i.$ infinito $\{1, x, x^2, .., x^n, ..\}$.

- Si $L = \{a + bi; a, b \in \mathbb{Q}\} \subset \mathbb{C}$ y $K = \mathbb{Q}$, es fácil ver que L es un cuerpo y que $\{1, i\}$ es base de L sobre K, por tal motivo $[L : K] = 2$.

Observación 3.1.5 El caso $[L : K] = 1$ sólo ocurre cuando $L = K$.

Teorema 3.1.6 (Regla de torres) *Sean M una extensión de L y L una extensión de K. Entonces M es una extensión de K y M/K es finito si y sólo si M/L y L/K son finitos, y en este caso se cumple*

$$[M : K] = [M : L][L : K].$$

Demostración.- Vea [4, capítulo 1, sección 1, teorema 1]. □

Dada una extensión L de K y $A \subset L$, podemos tomar la colección $\mathscr{A}$ de subcuerpos de L que contengan a K y A (que no sera vacía, pues $L \in \mathscr{A}$), e intersectando todos sus elementos obtendremos un subcuerpo que contenga a K y A; a esta extensión de K la denotaremos $K(A)$ y denominaremos *adjunción de A a K*. Análogamente, si R es un anillo, S un subanillo de R y $A \subset R$ cualquiera, existe un " menor"subanillo de R que contiene a S y A, que denotaremos por $S[A]$. Con estas notaciones tendremos el siguiente resultado.

Proposición 3.1.7 *Se cumplen la siguientes igualdades:*

a) $S[A] = \{p(a_1, \ldots, a_n); n \geq 0, p \in S[x_1, \ldots, x_n], a_i \in A\}$;

b) $K(A) = \left\{\frac{p(a_1,\ldots,a_n)}{q(a_1,\ldots,a_n)}; n \geq 0, p, q \in K[x_1, \ldots, x_n], a_i \in A, q(a_1, \ldots, a_n) \neq 0\right\}$;

c) $\mathcal{Q}(K[A]) = K(A)$;

d) $S[A][B] = S[A \cup B] = S[B][A]$, *para todo* $A, B \subset R$;

e) $K(A)(B) = K(A \cup B) = K(B)(A)$, *para todo* $A, B \subset L$.

Demostración.- El conjunto a la derecha de la igualdad en *a)*, denotémoslo por T, el cual es un subanillo de R que contiene a S y A, esto da $S[A] \subset T$; y si un subanillo de R que contiene a S y A, también contendrá a T, de donde $T \subset S[A]$, por lo tanto se da la igualdad entre estos subanillos. El ítem *b)*, se comprueba de forma análoga. El ítem *c)* es cierto a la luz de *a)* y *b)*, aunque estrictamente hablando tan sólo se cumple $\mathcal{Q}(K[A])$ es isomorfo a $K(A)$. Y para *d)*, observe que de la definición de $S[A \cup B]$ y $S[A][B]$ tenemos, respectivamente, $S[A \cup B] \subset S[A][B]$ y $S[A][B] \subset S[A \cup B]$; análogamente obtenemos *e.* □

En lo siguiente, si $A = \{a_1, \ldots, a_n\} \subset L$ es finito entonces denotaremos $K(a_1, \ldots a_n)$ en lugar de $K(A)$.

Ejemplo 3.1.8 El cuerpo $\mathbb{Q}(i) \subset \mathbb{C}$ es el subconjunto de los elementos de la forma $c + di$ con $c, d \in \mathbb{Q}$.

Lema 3.1.9 *Si L/K es finita con $n = [L : K]$, entonces existen $a_1, \ldots, a_n \in L$ tales que $L = K(a_1, \ldots, a_n)$.*

Demostración.- Basta tomar una base $\{a_1, \ldots, a_n\} \subset L$ sobre K. □

Sean L un cuerpo y M, N subcuerpos de L. Entenderemos por *composición de M y N (en L)* a la intersección de todos los subcuerpos L que contienen a M y N. Este es el menor subcuerpo que contiene a M y N, y lo denotaremos por MN.

Observación 3.1.10 Sean L un cuerpo y M, N subcuerpos de L, entonces $MN = M(N) = N(M)$. Además, si F es subcuerpo de M y N, y existe $S \subset L$ tal que $M = F(S)$, de donde $MN = N(S)$.

3.2. Elementos algebraicos

Definición 3.2.1 Sean L/K y $a \in L$, diremos que a es *algebraico sobre K* si existe $p(X) \in K[X]$ no nulo tal que $p(a) = 0$; en el caso contrario, diremos que a es *trascendental sobre K*. Si todo elemento $a \in L$ es algebraico sobre L, diremos que L es una *extensión algebraica sobre K* (o más brevemente L/K es algebraico); en el caso contrario L será una *extensión trascendental sobre K* (o simplemente L/K es trascendental).

Ejemplos 3.2.2

- Todo elemento de un cuerpo es algebraico sobre él.
- Dado $a + bi \in \mathbb{Q}(i)$, el polinomio $p(X) = (X - a)^2 + b^2 \in \mathbb{Q}[X]$ es no nulo y cumple que $p(a + bi) = 0$, luego $\mathbb{Q}(i)/\mathbb{Q}$ es algebraico.
- Dado $a \in \mathbb{Q}$ no negativo, tenemos que $\sqrt[n]{a} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$. Sin embargo, existen elementos transcedentales en $\mathbb{R}$ sobre $\mathbb{Q}$ como e (vea por ejemplo [5, capítulo 5, sección 2, teorema 5.f]).
- Si $\alpha \in L$ es trascendental sobre K y $p(X) \in K[X]$ es no constante, entonces $p(\alpha) \in L$ es trascendentales.

Teorema 3.2.3 *Si L es una extensión finita de K, entonces L será algebraica sobre K.*

Demostración.- Vea [4, capítulo 1, sección 2, teorema 2]. □

El teorema anterior nos da innumerables ejemplos de extensiones algebraicas de un cuerpo K; sin embargo depende de extensiones finitas. El siguiente nos dice mucho más de su estructura.

Teorema 3.2.4 *Sea L una extensión de K y $a \in L$ algebraico sobre K, entonces existe un único polinomio mónico irreductible $p(X) \in K[X]$ tal que $p(a) = 0$. Se satisface que*

- *Si $q(X) \in K[X]$ se anula en a, entonces $p(X) \mid q(X)$ en $K[X]$.*
- *Si $b \in K(a) \setminus \{0\}$, existe un único $r(X) \in K[X]$ con* grad $r(X) <$ grad $p(X)$ *tal que $r(a) = b$. En particular $K[a] = K(a)$.*

Demostración.- Vea [4, capítulo 1, sección 2, teorema 3]. □

En adelante, dado $a \in L$ algebraico sobre K, denotaremos por $\mathrm{Irr}\,(K, a)$ al polinomio descrito en el teorema anterior. A este polinomio se le conoce como *polinomio minimal de a sobre K*. Un resultado inmediato del anterior teorema que nos sera útil en adelante es el siguiente.

Corolario 3.2.5 *Sea L extensión de K y $a \in L$, si a es algebraico sobre K, entonces $1, a, ..., a^{n-1}$ es una base de $K(a)$ sobre K, donde $n =$* grad $\mathrm{Irr}\,(K, a)$*).*

Corolario 3.2.6 *Si L es una extensión algebraica de K, entonces L es la unión de las extensiones finitas sobre K contenidas en L.*

Demostración.- Puesto que todo elemento $a \in L$ genera a la extensión finita $K(a)/K$, tendremos que $L = \bigcup_{a \in L} K(a)$. □

Proposición 3.2.7 *Sea M/K, L un cuerpo tal que $K \subset L \subset M$. Si $a \in M$ es algebraico sobre K, tambien será algebraico sobre L.*

Demostración.- Basta observar que a se anula en el polinomio no nulo $\mathrm{Irr}\,(K, a) \in M[X]$. □

Proposición 3.2.8 *Sea L una extensión de K y $a_1, \ldots, a_n \in L$ algebraicos sobre K. Entonces, la extensión $K(a_1, \ldots, a_n)/K$ es finita, y por lo tanto algebraica.*

Demostración.- Vea [4, capítulo 1, sección 2, corolario 2].

Corolario 3.2.9 *Sea L/K una extensión y $a, b \in L$ algebraicos sobre K, se cumple que $a + b, a - b$ y $a \cdot b$ son algebraicos sobre K, y si $b \neq 0$ entonces a/b es algebraico sobre K.*

Dada una extensión L de K, por el corolario anterior $L^a = \{b \in L;\ b \text{ es algebraico sobre } K\}$ será un subcuerpo de L que contiene a K. Más aun será la mayor extensión algebraica de K contenida en L; a dicho conjunto lo llamaremos *clausura álgebraica de K en L.*

La siguiente proposición muestra la especie de transitividad con la que cuenta el concepto de elemento algebraico.

Teorema 3.2.10 *Sea M una extensión de K y L un cuerpo entre ellos (es decir $K \subset L \subset M$) tal que L/K sea algebraica. Si $a \in M$ es algebraico sobre L entonces a es algebraico sobre K.*

Demostración.- Vea por ejemplo [13, capítulo 1, sección 1, proposición 1.23]. □

Ahora nos preocuparemos por encontrar una extensión que contenga al menos una raíz para un polinomio especifico.

Teorema 3.2.11 (Kronecker) *Sea K un cuerpo y $f(x) \in K[x]$ irreductible, entonces existe una extensión L sobre K que contiene a un elemento a tal que $L = K(a)$ y $f(a) = 0$*

Demostración.- Vea [4, capítulo 1, sección 2, teorema 5].

3.3. Homomorfismos entre extensiones

El comportamiento de los homomorfismos respecto a los elementos algebraicos es interesante y natural, pues como veremos conserva la propiedad de elemento algebraico.

Empecemos por suponer que tenemos dos extensiones L y $\bar{L}$ de los cuerpos K y $\bar{K}$, respectivamente, y un monomorfismo $\sigma : L \to \bar{L}$ tal que $\sigma(K) \subset \bar{K}$. Tomemos $\alpha \in L$ algebraico sobre K, $p(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ no nulo tal que $p(\alpha) = 0$. Entonces

$$0 = \sigma\big(p(\alpha)\big) = \sigma(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0) = \sigma(a_n)\sigma(\alpha)^n + \cdots + \sigma(a_0) = \sigma p\big(\sigma(\alpha)\big).$$

Puesto que σ es un homomorfismo entre cuerpos, este será inyectivo, así pues $\sigma p(X) \in \bar{K}[X]$ será no nulo; por lo tanto $\sigma(\alpha) \in \bar{L}$ sera algebraico sobre $\bar{K}$. Resumimos nuestro anterior análisis en la siguiente proposición.

Proposición 3.3.1 *Sean L y $\bar{L}$ extensiones sobre K y $\bar{K}$ respectivamente, y $\sigma : L \to \bar{L}$ un momomorfismo tal que $\sigma(K) \subset \bar{K}$.*

- *Si $\alpha \in L$ es raíz de $f(X) \in K[X]$, entonces $\sigma(\alpha)$ es raíz del polimonio $\sigma f(X)$.*

- *Si $\alpha \in L$ es algebraico sobre K, entonces $\sigma(\alpha) \in \bar{L}$ es algebraico sobre $\bar{K}$.*

Definición 3.3.2 Sean L una extensión de K y $a, b \in L$ algebraicos sobre K, diremos que a y b son *K-conjugados sobre K* cuando $\operatorname{Irr}(L, a) = \operatorname{Irr}(L, b)$.

Ejemplo 3.3.3 Sea $K = \mathbb{Z}/2\mathbb{Z}$ y $f(X) = X^2 + X + 1 \in K[X]$. Este polinomio de segundo grado no tiene raíces en K, luego es irreductible. El teorema 3.2.11 nos permite elegir una extensión L sobre K donde exista una raíz u de $f(X)$, y vemos facilmente que $u + 1$ es raíz de $f(X)$. Como $f(X)$ es mónico, se tiene que $\operatorname{Irr}(K, u) = f(X)$, por lo cual u y $u + 1$ son $K-$conjugados.

Definición 3.3.4 Sean L y M extensiones de K y $\sigma : M \to L$ homomorfismo, σ será un K-homomorfismo (resp. K-isomorfismo) de L en M, si $\sigma(c) = c$, para todo $c \in K$. En caso de existir un $K-$isomorfismo $\sigma : L \to M$ diremos que L y M son $K-$isomorfos.

Ahora, tomemos K y $\bar{K}$ cuerpos isomorfos via el isomorfismo $\sigma : K \to \bar{K}$ isomorfismo, y su respectiva extensión $\tilde{\sigma} : K[x] \to \bar{K}[x]$ definida por $\tilde{\sigma}\big(f(x)\big) = \sigma f(x)$. Puesto que $\tilde{\sigma}$ es un isomorfismo, tenemos que $f(x) \in K[x]$ es irreductible si y sólo si $\sigma f(x) \in \bar{K}$ es irreductible.

Lema 3.3.5 *Sean L/K y $\bar{L}/\bar{K}$ tales que exista un isomorfismo $\sigma : K \to \bar{K}$. Tomemos $a \in L$ y $b \in \bar{L}$ algebraicos sobre K y $\bar{K}$ respectivamente. Si $\operatorname{Irr}(\bar{K}, b) = \sigma \operatorname{Irr}(K, a)$ entonces existe un único isomorfismo $\tau : K(a) \to \bar{K}(b)$ que extiende σ tal que $\tau(a) = b$.*

Demostración.- La función $\Psi : K[X] \to K(a)$, $\Psi\big(f(X)\big) = f(a)$ es un homomorfismo sobreyectivo, la cual poseerá núcleo igual al ideal generado por $p(X) = \operatorname{Irr}(K, a)$ (por el teorema 3.2.4). Por lo tanto, tenemos un isomorfismo $\dot{\Psi}$ entre $K[X]/\langle p(X)\rangle$ y $K(a)$ tal que $\dot{\Psi}\big(X + \langle X\rangle\big) = a$; análogamente podemos construir un isomorfismo $\dot{\Phi}$ entre $\bar{K}[X]/\langle \sigma p(X)\rangle$ y $\bar{K}(b)$ tal que $\dot{\Phi}\big(X + \langle X\rangle\big) = b$. Tomando el isomorfismo $\dot{\sigma} : K[x]/\langle p(x)\rangle \to \bar{K}[x]/\langle q(x)\rangle$ que nos induce $\tilde{\sigma}$ definida arriba, tenemos que $\tau = \dot{\Phi} \circ \dot{\sigma} \circ \dot{\Psi}^{-1} : K(a) \to \bar{K}(b)$ cumple $\tau(a) = \dot{\Phi}\Big(\dot{\sigma}\big([x]_1\big)\Big) = \dot{\Phi}([x]_2) = b$ y $\tau(c) = \dot{\Phi}\Big(\dot{\sigma}\big([c]_1\big)\Big) = \dot{\Phi}\Big(\big[\sigma(c)\big]\Big) = \sigma(c)$, para todo $c \in K$.

Si existiese otro, por decir $\rho : K(a) \to K(b)$ con las mismas características, entonces dado $d \in K(a)$ tenemos, por el teorema 3.2.4, que existe $r(x) = c_0 + \cdots + c_n x^n \in K[x]$ tal que $r(a) = d$, de donde

$$\rho(d) = \rho(c_0 + \cdots + c_n a^n) = \rho(c_0) + \cdots + \rho c_n b^n = \tau(c_0) + \cdots + \tau(c_n a^n) = \tau(d),$$

por lo tanto $\tau = \sigma$ lo que finaliza la prueba. □

Observación 3.3.6 Asumamos las notaciones del lema previo, y supongamos que $[K(a) : K] = \text{grad Irr}\,(K,a) = n$. Si $\alpha \in L$, entonces existen únicos $c_0, c_1, \ldots, c_{n-1} \in K$ tales que $\alpha = c_0 + c_1 a + \cdots + c_{n-1}a^{n-1}$, por lo tanto

$$\tau(c) = \tau(c_0) + \tau(c_1)\tau(a) + \cdots + \tau(c_{n-1})\tau(a^{n-1}) = \sigma(c_0) + \sigma(c_1)b + \cdots + \sigma(c_{n-1})b^{n-1}.$$

Esta será la forma que tendrán estas extensiones de isomorfismos que asignan elementos algebraicos que cumplen la hipótesis del lema.

En el caso particular de $\bar{K} = K$ y $\sigma = \text{id}$ tendremos el siguiente resultado.

Corolario 3.3.7 *Si $a, b \in L/K$ son K-conjugados, entonces existe un $K-$isomorfismo $\tau : K(a) \to K(b)$ tal que $\tau(a) = b$.*

Observación 3.3.8 La afirmación recíproca tambien es cierta, es decir

> si $a, b \in L$ son algebraicos sobre K, y existe un K-monomorfismo $\sigma : K(a) \to K(b)$ tal que $\sigma(a) = b$, entonces a, b son $K-$conjugados.

En efecto, si $f(x) = \text{Irr}\,(K,a)$ entonces $f(b) = f\big(\sigma(a)\big) = \sigma\big(f(a)\big) = 0$; luego $\text{Irr}\,(K,b) \mid f(x)$. Como $f(x)$ es irreductible, deducimos que estos polinomios son elementos conjugados en $K[X]$, y como ambos son mónicos concluimos que son iguales.

3.4. Característica de un cuerpo

Empecemos con un pequeño análisis sobre la estructura aditiva de un cuerpo K. Denotemos por Δ a la intersección de todos los subcuerpos de K, que será un subcuerpo de K. Más aun será el "menor"subcuerpo de K y lo llamaremos el *cuerpo primo de K*. Nótese que Δ contendrá a la unidad del cuerpo, que en esta sección denotamos por e.

Observación 3.4.1 Si L es extensión de K entonces L posee el mismo cuerpo primo que K.

Ahora tomemos $\eta : \mathbb{Z} \to K$ definido por

$$\eta(n) = \begin{cases} \underbrace{e + \cdots + e}_{n\text{elementos}} & n > 0, \\ 0 & n = 0, \\ -\underbrace{(e + \cdots + e)}_{-n\text{elementos}} & n < 0. \end{cases}$$

Unos cálculos directos nos muestran que es un homomorfismo de anillos no nulo. Con igual facilidad, obtenemos que $\eta(n) \in \Delta$,para todo $n \in \mathbb{Z}$ (pues $e \in \Delta$ y Δ es un subanillo), esto es $\eta(\mathbb{Z}) \subset \Delta$ y $\eta(\Delta)$ es un dominio. Sin embargo, no sabemos nada de su núcleo, así que separaremos dos casos:

1. $\mathrm{Nu}(\eta) = \langle 0 \rangle$: entonces $\mathbb{Z} \cong \mathbb{Z}/\mathrm{Nu}(\eta) \cong \eta(\mathbb{Z})$. Podemos tomar $\mathcal{Q}(\eta(\mathbb{Z})) \subset K$ subcuerpo, luego $\Delta \subset \mathcal{Q}(\eta(\mathbb{Z}))$; pero este es el menor subcuerpo que contiene a $\eta(\mathbb{Z})$ (salvo isomorfismo), entonces $\mathcal{Q}(\eta(\mathbb{Z})) \subset \Delta$ y serán iguales. Así tenemos que $\mathbb{Q} = \mathcal{Q}(\mathbb{Z}) \cong \mathcal{Q}(\eta(\mathbb{Z})) = \Delta$.

2. $\mathrm{Nu}(\eta) \neq \langle 0 \rangle$: entonces $\mathrm{Nu}(\eta) = \langle p \rangle$ con $p \neq 0$ ($\mathbb{Z}$ es *dominio de ideales principales*), y se cumple $\mathbb{Z}/\langle p \rangle \cong \eta(\mathbb{Z})$, de ahí que $\mathbb{Z}/\langle p \rangle$ es un dominio, luego $\langle p \rangle$ debe ser un ideal primo y en consecuencia $p \in \mathbb{N}$ es primo. Así $\mathbb{Z}/\langle p \rangle$ es un cuerpo, y como $\eta(\mathbb{Z}) \cong \mathbb{Z}/\langle p \rangle$ tendremos que $\eta(\mathbb{Z})$ es un subcuerpo de K, esto nos da $\Delta \subset \eta(\mathbb{Z})$. Resumiendo, $\mathbb{Z}/\langle p \rangle \cong \eta(\mathbb{Z}) = \Delta$. Este análisis nos da el siguiente resultado.

Teorema 3.4.2 *Para cualquier cuerpo K, su cuerpo primo es, o bien isomorfo a $\mathbb{Q}$, o bien isomorfo a $\mathbb{Z}/\langle p \rangle$ para algún $p \in \mathbb{N}$ primo.*

Definición 3.4.3 Sea K un cuerpo, si $\Delta \cong \mathbb{Q}$ diremos que K tiene *caracterítisca* 0, y en el caso contrario diremos que posee característica p. A la característica de K la denotaremos por $\mathrm{car}\, K$.

Observación 3.4.4 Si σ es un automorfismo de un cuerpo K, entonces es Δ-automorfismo.

Utilizando el anterior homomorfismo η, dado $n \in \mathbb{Z}$ y $a \in K$ denotemos por $n \cdot a$ a $\eta(n)a$. En lo siguiente omitiremos el punto $\cdot$ en esta notación siempre que no exista peligro de confusión.

Observación 3.4.5 Con esta nueva notación tenemos que:

- Si $\mathrm{car}\, K = 0$: $na = 0$ implica $\eta(n) = 0$ o $a = 0$, esto es $n = 0$ o $a = 0$. *Asumiendo $n \neq 0$ tenemos que $na = 0$ si y sólo si $a = 0$.*

- Si $\mathrm{car}\, K = p$: $na = 0$ implica $n \in \mathrm{Nu}(\eta)$ o $a = 0$, esto es $p \mid n$ o $a = 0$. *Asumiendo $a \neq 0$ tenemos que $na = 0$ si y sólo si $p \mid n$.*

Proposición 3.4.6 *Sea K un cuerpo con característica $p \in \mathbb{N}$ primo. La función $\xi : K \to K$ definida por $\xi(a) = a^p$, para todo $a \in K$ es un monomorfismo de anillos.*

Esta función ξ es llamada *homomorfismo de Frobenius en* K.

Demostración.- Sean $a, b \in K$ cualesquiera, por tanto K tiene producto conmutativo podemos aplicar el teorema del binomio de Newton a $(a+b)^p = \xi(a+b)$ y obtendremos que

$$\xi(a+b) = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i},$$

pero si $1 \leq i \leq p-1$ entonces $p \nmid i!, p \nmid (p-i)!$, y de ahí $p \mid p! = \binom{p}{i} i!(p-i)!$ implica que $p \mid \binom{p}{i}$, para $1 \leq i \leq n$. Entonces $\xi(a+b) = a^p + b^p = \xi(a) + \xi(b)$, para todo $a, b \in K$. Finalmente, es claro que ξ respeta la multiplicación de elementos, por lo cual es homomorfismo de anillos, con ello deducimos rápidamente que es un monomorfismo. □

Observación 3.4.7

- Es consecuencia inmediata, via inducción, que: *dado* $t \in \mathbb{N}$ *se cumple*

$$(a+b)^{p^t} = a^{p^t} + b^{p^t}, \qquad \text{para todo } a, b \in K.$$

- Dados $a, b \in K$, se tiene que $a^{p^t} = b^{p^t}$ implica $a = b$.

- Si K es un cuerpo finito, tendremos que ξ es un automorfismo (pues ξ sería una función inyectiva entre cuerpos finitos del mismo cardinal).

3.5. Elementos separables

Sean K un cuerpo, $f(X) \in K[X]$ y $a \in K$. Por el algortimo euclidiano de la división en $K[X]$ tenemos que existen $q(X), r(X) \in K[X]$ tales que $f(X) = q(X)(X-a) + r(X)$ con $r(X) = 0$ o grad $r(X) <$ grad $(X-a)$; en ambos casos $r(X)$ es un polinomio constante. De este modo, $f(X) = q(X)(X-a) + r$ con $r \in K$, de ahí que $f(a) = 0$ si y sólo si $r = 0$, esto es $(X-a) \mid f(X)$.

Lema 3.5.1 *Sean* K *un cuerpo,* $a \in K$ *y* $f(X) \in K[X]$. *Entonces,* a *es una raíz de* $f(X)$ *si y sólo si* $(X-a)$ *divide a* $f(X)$.

Definición 3.5.2 Sean K un cuerpo, $f \in K[X]$ y $a \in K$. Decimos que a es una *raíz de* $f(X)$ *con multiplicidad* $m \in \mathbb{N}$ si $(X-a)^m \mid f(X)$ y $(X-a)^{m+1} \nmid f(X)$. En el caso particular que $m = 1$, decimos que a es una *raíz simple de* $f(X)$.

El objeto en la siguiente definición será una herramienta de mucha utilidad en el futuro.

Definición 3.5.3 Dado $f(X) = a_0 + a_1 \cdots + a_n X^n \in K[X]$, definimos $f'(X) \in K[X]$, *la derivada formal de* $f(X)$ por $f'(X) = a_1 + \cdots + n a_n X^{n-1}$.

No es difícil obtener las propiedades de la derivada formal de polinomios, que muestra similitud con las existentes con la derivada tradicional de funciones reales de variable real.

Proposición 3.5.4 *Sean* $f(X), g(X) \in K[X]$, *se cumplen:*

1 $(f+g)'(X) = f'(X) + g'(X)$,

2 $(cf)'(X) = cf'(X)$, *para todo* $c \in K$,

3 $(f \cdot g)'(X) = g(X)f'(X) + f(X)g'(X)$,

4 *si* $f(X) = (X-a)^m$, *entonces* $f'(X) = m(X-a)^{m-1}$, *para todo* $m \in \mathbb{N}$.

Teorema 3.5.5 *Sea* L *una extensión de* K, $f(X) \in K[X]$ *no nulo y* $a \in L$ *una raíz de* $f(X)$. *Entonces* a *es raíz simple de* $f(X)$ *si y sólo* $f'(a) \neq 0$.

Demostración.- Vea [4, capítulo 1, sección 3, proposición]. □

Observación 3.5.6 Se rescata que $f'(X) = 0$ no implica que $f(X) = c \in K$. En efecto, basta tomar $K = \mathbb{Z}/p\mathbb{Z}$ y $f(X) = X^p - 1$, entonces $f'(X) = pX^{p-1} = 0$.

Definición 3.5.7 Sea L una extensión de K y $a \in L$ algebraico sobre K. Decimos que a es *separable sobre* K si es raíz simple de su polinomio minimal. Si L/K es algebraica, diremos que L es una *extensión separable sobre* K cuando todo $a \in L$ sea separable sobre K, en el caso contrario diremos que es *inseparable sobre* K.

Ejemplos 3.5.8

- Sea $K = \mathbb{Z}/3\mathbb{Z}$ y $f(X) = X^2+1$. Vemos que $f(X)$ es un polinomio irreductible en $K[X]$. Tomando L una extensión sobre K que contienen a una raíz a de $f(X)$, tendremos que las raíces de $f(X)$ son $a, -a \in L$, y a es separable sobre K.

- Si tomamos $p \in \mathbb{N}$ primo, $K = \mathbb{Z}/p\mathbb{Z}(X)$ y $p(Y) = Y^p - X \in K[Y]$, las raíces de $p(Y)$ serán inseparables. En efecto, sea L un cuerpo de la forma $K(u)$ con u raíz de $f(Y)$. Entonces $f(u) = 0$, lo que implicará que $p(u) = 0$, luego $u^p = X$ y $p(Y) = (Y-u)^p$ (por proposición 3.4.6); de esta forma $f(Y) = (Y-u)^m$, para cierto $m \in \mathbb{N}$. Si $m = 1$, entonces $u \in K$ y existirán $g(X), h(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ tales que $u = g(X)/h(X)$, así $X = u^p = \big(g(X)/h(X)\big)^p$ y

  $$p \operatorname{grad} h(X) + 1 = \operatorname{grad}\Big(X\big(h(X)\big)^p\Big) = \operatorname{grad}\,(g(X)^p) = p \operatorname{grad} g(X),$$

  de donde $p \mid 1$, lo que contradice que p es primo. Luego $m > 1$ y u no es raíz simple de $f(Y)$ (que es su polinomio minimal), por tanto u no es separable sobre K, y como toda raíz de $p(Y)$ es raíz de alguno de sus factores irredutibles, concluimos.

La siguiente proposición es una propiedad similar a la transitividad que posee el concepto de separabilidad.

Proposición 3.5.9 *Sean M extensión de K, $a \in M$ separable sobre K. Si L es un cuerpo entre K y M, entonces a es separable sobre L.*

Demostración.- Por la proposición 3.2.7, tenemos que a es algebraico sobre L, por lo cual existen $\operatorname{Irr}(L,a)$ y $\operatorname{Irr}(K,a)$. Desde que $\operatorname{Irr}(K,a) \in L[x]$ y se anula en a, se tiene que $\operatorname{Irr}(L,a) \mid \operatorname{Irr}(K,a)$. Luego, si a no es separable sobre L, por definición tendríamos que $(x-a)^2 \mid \operatorname{Irr}(L,a)$, de ahí $(x-a)^2 \mid \operatorname{Irr}(K,a)$ y a no será separable sobre K, que es una contradicción. □

Definición 3.5.10 Sea K un cuerpo. Diremos que K es *perfecto* si toda extensión algebraica sobre K es separable.

Proposición 3.5.11 *Dado un cuerpo perfecto K, toda extensión algebraica L sobre K es perfecta.*

Demostración.- Sea M una extensión algebraica sobre K. Por el teorema 3.2.10 tendremos que M/K es algebraica, por tanto M/K es separable. Por la proposición 3.5.9 concluimos que M/L es separable, por lo tanto L es perfecto. □

Dado un cuerpo K de característica $p \in \mathbb{N}$, definimos $K^p = \xi(K)$, donde ξ es el homomorfismo de Frobenius definido en la sección anterior.

Teorema 3.5.12 *Sea K un cuerpo. Si $\operatorname{car} K = 0$, entonces K es perfecto. En el caso de $\operatorname{car} K = p$ primo, K será perfecto si y sólo si $K^p = K$.*

Demostración.- Vea [4, capítulo 1, sección 3, teorema 7]. □

Corolario 3.5.13 *Todo cuerpo finito es perfecto.*

3.6. Descomposición de polinomios

Empecemos por el siguiente lema muy conocido y básico.

Lema 3.6.1 *Sea K un cuerpo y $p(X) \in K[X]$, si $n = \operatorname{grad} p(X)$ entonces $p(X)$ posee a lo más n raíces en K.*

Demostración.- Basta con usar inducción sobre el grado del polinomio y el lema 3.5.1. □

Nótese que dado un polinomio $f(X) \in K[X]$ de grado n, por el teorema de Kronecker, podemos encontrar una extensión L_1 sobre K que contenga al menos una raíz u de $f(X)$, luego $f(X) = (X - u)g_1(X)$ donde $g_1(X) \in L_1[X]$, que será de grado igual a $n - 1$. Procediendo de igual manera con $g_1(X) \in L_1[X]$, encontraremos una L_2 que contendra a u_2 raíz de $g(X)$, así tendremos que $f(X) = (X - u_1)(X - u_2)g_2(X)$ con grad $g_2(X) = n - 2$. Como podemos apreciar el grado de los polinomios decrece, y si seguimos construyendo extensiones sobre K que contengan raíces de $f(X)$ entonces lograremos factorizar $f(X)$ en n factores lineales. Con esta idea, la siguiente definición será plausible.

Definición 3.6.2 Sea L una extensión de K y $f(X) \in K[X]$, decimos que $f(X)$ *se descompone en* $L[X]$ si $f(X)$ se descompone en factores lineales con coeficientes en $L[X]$, esto es $f(X) = c(X - a_1)(X - a_2)\cdots(X - a_n)$, donde $c, a_1, a_2, \ldots, a_n \in L$.

El siguiente lema nos asegura que cuando logramos descomponer un polinomio en una extensión L, esta descomposición se conservará a pesar de extender L.

Lema 3.6.3 *Sean $f(X) \in K[X]$ y L una extensión de K tal que $f(X)$ se descompone en $L[X]$. Tomemos $A = \{a \in ;\ f(a) = 0\}$ y M una extensión de L. Si $b \in M$ es una raíz de $f(x)$ entonces $b \in A$.*

Demostración.- Si $f(x) = c(x-a_1)(x-a_2)\cdots(x-a_n)$ donde $c, a_1, a_2, \ldots, a_n \in L$ y $c \neq 0$, entonces

$$c(b-a_1)(b-a_2)\cdots(b-a_n) = f(b) = 0,$$

y puesto que M es un cuerpo, b debe ser algún a_i. □

En el siguiente lema determinaremos la multiplicidad de cada a_i en la anterior descomposición; para esto nos restringiremos al caso $f(X)$ irreductible y mónico (que es el caso base y sencillo).

Lema 3.6.4 *Sean K un cuerpo perfecto, L una extensión de K y $f(X) \in K[X]$ irreductible. Si $f(X)$ descompone en $L[X]$, entonces la multiplicidad de cada factor lineal es 1.*

Demostración.- Vea [4, capítulo 1, sección 5, teorema 14]. □

Como hemos visto podemos obtener un cuerpo lo "suficientemente grande"para que contenga todas las posibles raíces de un polinomio $f(X)$ y así este polinomio se descomponga sobre $L[X]$; pero podemos tomar una extensión más pequeña sobre K que posea estas cualidades.

Definición 3.6.5 Sea L una extensión de K y $f(X) \in K[X]$. Decimos que L es un *cuerpo de descomposición*, que abreviaremos por *c.d.*, de $f(X)$ sobre K si $f(X) = c(X-a_1)\cdots(X-a_n)$ con $a_1, \ldots, a_n$ y $L = K(a_1, a_2, \ldots, a_n)$.

Observación 3.6.6 Notamos que: L/K sera un *c.d.* de $f(X) \in K[X]$ si y sólo si:

- el polinomio $f(X)$ se descompone en $L[X]$,
- si $f(X)$ se descompone en un subcuerpo L' de L con $K \subset L'$, entonces $L' = L$.

El siguiente teorema muestra que siempre podemos obtener un *c.d.* para un polinomio dado, esto será de importancia en sucesivas construcciones y caracterizaciones.

Teorema 3.6.7 *Dado un cuerpo K, todo polinomio $f(x) \in K[x]$ tiene un c.d. sobre K.*

Demostración.- Vea [4, capítulo 1, sección 5, teorema 15]. □

Ejemplo 3.6.8 Algunas veces no es necesario agregar raíz tras raíz para obtener un cuerpo de dscomposición. En efecto, tomemos $p(X) = X^4+1 \in \mathbb{Q}[X]$ y un cuerpo L que contiene una raíz de $p(X)$. Sea $u \in L$ una raíz de $p(X)$, entonces $p(-u) = 0$ y $-u$ será otra raíz de $p(X)$ (es claro que $u \neq -u$, puesto car $\mathbb{Q} \neq 2$). Tambien se tiene $p(u^3) = (-1)^3 + 1 = 0$, y como $\pm u = u^3$ implica $\pm 1 = u^2$ (lo cual no es cierto), entonces $u, -u, u^3$ no son iguales. Asimismo, $p(-u^3) = 0$ y $-u^3$ es otra raíz de $p(X)$ en L. Puesto que $L = K(u)$ (vea el teorema 3.2.11), tenemos que L es un *c.d.* de $p(X)$ sobre $\mathbb{Q}$.

Proposición 3.6.9 *Sean L un c.d. de $f(X)$ sobre K y M un subcuerpo entre L y K. Entonces L es un c.d. de $f(X)$ sobre M.*

Demostración.- En efecto, como $K \subset M$ entonces $f(X) \in M[X]$ y se descompone sobre $L[X]$. Si L' es subcuerpo de L que contiene a M y $f(X)$ se escinde sobre L', entonces L' es un subcuerpo entre K y L tal que $f(X)$ se descompone sobre L', entonces $L' = L$ (por la observación 3.6.6). Luego, por la observación 3.6.6, concluimos que L es un *c.d.* de $f(X)$ sobre M. □

Pueden existir distintos *c.d.* de $f(X)$ sobre K, puesto estos pueden ser resultado de reiteradas construcciones de cuerpos de con una nueva raíz sobre K, los cuales no son únicos, en un orden totalmente arbitrario. Sin embargo, podemos rescatar un tipo de unicidad puesto que tan sólo se agregan raíces del mismo polinomio, aunque sean de extensiones posiblemente distintas.

Teorema 3.6.10 *Sean K y $\bar{K}$ cuerpos isomorfos por $\sigma : K \to \bar{K}$ y $f(x) \in K[x]$. Si L y $\bar{L}$ son c.d. de $f(x)$ y $\sigma f(x)$ respectivamente, entonces existe un isomorfismo $\tau : L \to \bar{L}$ tal que $\tau(c) = \sigma(c)$; para todo $c \in K$.*

La demostración de este teorema puede ser encontrada en [13, capítulo 1, sección 3, teorema 3.20]. En el caso particular de $\bar{K} = K$ y σ la identidad en K tenemos el siguiente.

Corolario 3.6.11 *Dado K cuerpo y $f(X) \in K[X]$, todo par de cuerpos de descomposición de $f(X)$ sobre K son $K-$isomorfos.*

3.7. Extensiones normales

Las extensiones normales son un tipo de extensión sumamente importante, pues constituyen el concepto más cercano a algebraicamente cerrado (que veremos más adelante). En este tipo de extensión desarrollaremos más las propiedades de $K-$monomorfismo.

Definición 3.7.1 Sea L una extensión de K. Decimos que L es una *extensión normal sobre K*, si es algebraica y si todo $p(X) \in K[X]$ irreductible que tenga una raíz en L necesariamente se descompone en $L[X]$. En este caso también diremos que L es normal sobre K o, más brevemente, L/K es normal.

Ejemplo 3.7.2 *Toda extensión cuadrática L de K es normal.*

En efecto, sea L/K una extensión cuadrática L/K. Para empezar, esta extensión es finita, y por lo tanto algebraica sobre K. Sea $p(X) \in K[X]$ irreducible con una raíz $a \in L$. Como $K(a) \subset L$, por el teorema 3.1.6 se tiene que $[L : K(a)][K(a) : K] = [L : K] = 2$, y de ahí que $[K(a) : K] = 1$ o 2. Por otra parte, $\operatorname{Irr}(K, a)$ y $p(X)$ se diferencian por una constante, luego $\operatorname{grad} p(X) = \operatorname{grad} \operatorname{Irr}(K, a) = [K(a) : K]$ (por el teorema 3.2.4). Luego, el $\operatorname{grad} p(x) = 1$ o 2; en el primer caso tenemos que $p(X)$ se descompone en $K[X]$, y en el segundo $p(x) = (X - a)q(X)$ con $q(X) \in L[X]$, y como $\operatorname{grad} q(x) = 1$ se tiene que $p(X)$ se escinde en $L[X]$. Por lo tanto L/K es normal.

Observación 3.7.3 La definición de extensión normal sólo se rige sobre polinomios irreductibles, pues podemos tomar $L = \mathbb{Q}(\sqrt{2})$ normal sobre $\mathbb{Q}$ y $p(X) = (X^2 - 2)(X^2 + 2)$, el cual tendrá una raíz en L, pero no se descompone sobre L.

Ejemplo 3.7.4 La extensión $L = \mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}$ no es normal. En efecto, basta observar que $p(X) = X^3 - 2 \in \mathbb{Q}[X]$ es irreductible (si tuviese un factor no constante en $\mathbb{Q}$, entonces tendría un factor lineal y por tanto una raíz cúbica de 2 en $\mathbb{Q}$). Este polinomio tiene una raíz en L, aunque

$$p(X) = (X - \sqrt[3]{2})(x^2 + \sqrt[3]{2}X + \sqrt[3]{4}) = (X - \sqrt[3]{2})q(X),$$

donde $q(X) = X^2 + \sqrt[3]{2}X + \sqrt[3]{4}$, lo que nos trae como consecuencia que no exista otra raíz de $p(X)$ en L. En efecto, si $b \in L \subset \mathbb{R}$ es otra raíz de $p(X)$, entonces lo será de $q(X)$; sin embargo $q(b) = (b + \sqrt[3]{2}/2)^2 + (3/4)\sqrt[3]{4} > 0$, ahí que $p(X)$ no se descompone sobre $L[X]$ y L/K no es normal.

Proposición 3.7.5 *Si L es una extensión normal de K y M un subcuerpo entre K y L, entonces L/M es normal.*

Demostración.- En primer lugar, por la proposición 3.2.7 tenemos que L/M es algebraica. Sea $p(X) \in M[X]$ irreductible con una raíz en $b \in L$. Tendremos que $p(X) = c \operatorname{Irr}(M, b)$ para algún $c \in M$. Puesto que L/K es normal, el polinomio $\operatorname{Irr}(K, b)$ se descompone en $L[X]$, y, como $\operatorname{Irr}(M, b) \mid \operatorname{Irr}(K, b)$, concluimos que $\operatorname{Irr}(M, b)$ se descompone en $L[X]$; con esto concluimos que L/M es normal. □

Observación 3.7.6 En adelante, según nos sea conveniente, verificaremos que una extensión L es normal mostrando la descomposición de polinomios irreducibles (con una raíz en L) sólo para el caso en que los polinomios sean mónicos. Asumido esto, tendremos la siguiente equivalencia:

una *extensión algebraica* L/K, *será* normal *si y sólo si todo polinomio minimal en* $K[X]$ *se descompone en* $L[X]$.

Ahora veamos la relación entre cuerpos de descomposición sobre un cuerpo K y las extensiones normales sobre K, la cual nos sera muy útil en el futuro; la demostración de este hecho puede ser encontrada en [4, capítulo 1, sección 5, teorema 16].

Teorema 3.7.7 *Sean* $f(X) \in K[X]$ *y* L *un c.d. de* $f(X)$ *sobre* K. *Entonces* L *es una extensión normal sobre* K.

El siguiente teorema es el recíproca del teorema anterior en el caso finito (para el caso infinito puede revisar [13, capítulo 1, sección 3, proposición 3.28]), lo que tendrá importante repercusión cuando queramos encontrar automorfismos que extiendan ciertos monomorfimos.

Teorema 3.7.8 *Sea* L *un extensión finita y normal sobre* K. *Entonces* L *es un c.d. para un* $p(X) \in K[X]$.

Demostración.- Vea [4, capítulo 1, sección 5, teorema 17]. □

Proposición 3.7.9 *Sean* M *y* L *extensiones de* K *tales que* $K \subset L \subset M$ *con* L/K *normal. Si* σ *es un* K*-automorfismo de* M *entonces* $\sigma(L) \subset L$.

Demostración.- Sean $a \in L$ y $p(X) = \text{Irr}\,(K, a)$. Por la proposición 3.3.1 $\sigma(a)$ será una raíz de $\sigma p(X) = p(X)$, el cual se descompone en L (pues L/K es normal). Entonces, por el lema 3.6.3, tendremos que $\sigma(a) \in L$; como $a \in L$ fue arbitrário, concluimos la demostración. □

Teorema 3.7.10 *Sea* L/K *finito normal y* M, N *subcuerpos* $K-$*isomorfos de* L. *Si* $\sigma : M \to N$ *es un* $K-$*isomorfismo, entonces existe un* K*-automorfismo* τ *que* τ *extiende* σ.

Demostración.-Vea [4, capítulo 1, sección 5, teorema 18]. □

El siguiente teorema será trascendente en la construcción de las funciones norma y traza en una extensión finita, dichas funciones seran piezas claves en la demostración del teorema principal de este trabajo.

Teorema 3.7.11 *Sea* L *una extensión finita de* K. *Existe un cuerpo* $F \supset L$, *finito y normal sobre* K *que es la menor extensión normal sobre* K *posible, en el siguiente sentido:*

si E *es una extensión normal de* K *que contiene a* L, *entonces existe un* $L-$*monomorfismo de* F *en* E.

A este tipo de extensión F, la denominaremos una *clausura normal de L sobre K*, más brevemente una clausura normal de L/K.

Demostración.- Vea [4, capítulo 1, sección 5, teorema 18]. □

3.8. K-automorfismos y K-inmersiones

En esta sección atenderemos unos de los aspectos más importantes en teoría de cuerpos: los automorfismos. Ya hemos visto que, dado un cuerpo K, los $K-$isomorfismos influyen en las propiedades de sus extensiones (por ejemplo, la normalidad de una extensión); ahora profundizaremos este topico. Antes mostremos una proposición que nos una idea del comportamiento de estos K-automorfismos.

Lema 3.8.1 *Sea L un extensión algebraica de K y $\sigma : L \to L$ un K-monomorfismo. Entonces*

- *Si $a \in L$, $p(x) = \text{Irr}\,(K, a)$ y $A = \{b \in L; p(b) = 0\}$, se tiene que $\#\sigma(A) \leq \text{grad}\, p(x)$ y $\sigma(A) = A$.*
- *σ es un $K-$automorfismo de L.*

Demostración.

- Por el lema 3.6.1, el conjunto A es finito y, por la proposición 3.3.1, tenemos que $\sigma(A) \subset A$. Entonces podemos restringir a σ a $\sigma_{|A} : A \to A$, la cual será inyectiva; y por ser A finito, deducimos que esta función será sobreyectiva.
- Dado $b \in L$, tomemos $q(x) = \text{Irr}\,(K, b)$ y $B = \{c \in L; q(c) = 0\}$, entonces $\sigma(B) = B$, así que $b \in \sigma(L)$, por lo tanto σ es un K-automorfismo.

Sean K un cuerpo y los K-automorfismos $\sigma, \eta : L \to L$. Es claro que $\sigma \circ \eta$ es un automorfismo, más aun será un $K-$automorfismo. Así tambien las inversas σ^{-1}, τ^{-1} serán K-automorfismos. Por lo tanto, el conjunto de $K-$automorfismos provisto de la operación de composición de funciones será un subgrupo del grupo de automorfismos de L. Rescatemos este análisis en la siguiente definición.

Definición 3.8.2 Sea L una extensión algebraica sobre K, denotamos

$$G(L/K) = \{\sigma : L \to L \,;\, \sigma \text{ es un } K\text{-automorfismo}\},$$

que es denominado *grupo de Galois de L/K*.

Observación 3.8.3 *Si L/K es finito y normal, entonces $G(L/K)$ es finito.*

En efecto, fijemos una base $a_1, a_2, \ldots, a_n \in L$ sobre K y tomemos $p_1(x) = \text{Irr}\,(K, a_1), \ldots,$ $p_n(x) = \text{Irr}\,(K, a_n)$. Dado $\sigma \in G(L/K)$, por el último lema, la cantidad de valores posibles para cada $\sigma(a_i)$ es a lo más grad $p_i(x)$. Además, puesto que σ es un $K-$homomorfismo, puede ser visto como un $K-$endomorfismo lineal de L, luego σ está totalmente determinado por los valores de $\sigma(a_1), \ldots, \sigma(a_n)$. Por lo tanto, la cantidad máxima de posibles $K-$automorfismos es $(\text{grad}\, p_1) \cdots (\text{grad}\, p_n)$, de donde $G(L/K)$ es finito.

Ejemplo 3.8.4 Sean $K = \mathbb{Q}$ y $L = K(\sqrt{2}, \sqrt{3})$. La extensión L será normal sobre K, pues L es un *c.d.* de $(X^2 - 2)(X^2 - 3)$ sobre $K[X]$, además es una extensión de grado 4. Procederemos a calcular los $K-$automorfismos de L, que en este caso particular, simplemente serán automorfismos (por la observación 3.4.4); para este fin utilizaremos las observaciones 3.3.6 y la anterior. Sean σ_1, el automorfismo identidad de $K(\sqrt{2})$, y un $K-$isomorfismo $\sigma_2 : K(\sqrt{2}) \to K(-\sqrt{2})$ tal que $\sigma_2(\sqrt{2}) = -\sqrt{2}$ (que existe pues $\sqrt{2}$ y -$\sqrt{2}$ son $K-$conjugados), nótese que estos serán todos los $K-$automorfismos de $K(\sqrt{2})$, puesto que $[K(\sqrt{2}) : K] = 2$. Tomemos $M = K(\sqrt{3})$, vemos que $\text{Irr}\,(M, \sqrt{3}) = X^2 - 3$, por lo cual $\sqrt{3}$ y $-\sqrt{3}$ son M-conjugados, luego existen dos $M-$automorfismos $\tau_{1,1}, \tau_{1,2} : M(\sqrt{3}) \to M(-\sqrt{3})$ tales que $\tau_{1,1}(\sqrt{3}) = \sqrt{3}$ y $\tau_{1,2}(\sqrt{3}) = -\sqrt{3}$ (notese que $\tau_{1,1}$ llega a ser la identidad sobre L). Ahora, tomando un automorfismo σ en M y el lema 3.3.5, tenemos dos automorfismos $\tau_{2,1}$ y $\tau_{2,2}$ que extienden a σ sobre L tales que $\tau_{2,1}(\sqrt{3}) = \sqrt{3}$ y $\tau_{2,2}(\sqrt{3}) = -\sqrt{3}$. Así obtenemos cuatro automorfismos sobre L, que es la cantidad máxima de automorfimos, por lo tanto $G(L/K) = \{\tau_{1,1}, \tau_{1,2}, \tau_{2,1}, \tau_{2,2}\}$

En lo siguiente, dada una extensión L/K, necesitaremos conocer acerca $K-$homomorfismos que parten de L hacia alguna extensión de K. Este es un caso más general que el que hasta ahora hemos visto, por lo cual nos brindará mayor flexibilidad en los pasos de demostraciones siguientes.

Definición 3.8.5 Sean L, M extensiones de un cuerpo K. Si $\sigma : L \to$ es un $K-$monomorfismo, será llamado *$K-$inmersión de L en M*. Al conjunto de todas las K-inmersiones de L en M lo denotaremos por $\text{In}_K(L, M)$.

Observación 3.8.6 Si L es una extensión algebraica sobre K, entonces $\text{In}\,(L/L) = G(L/K)$ por el lema 3.8.1.

Puesto que en nuestro trabajo tán solo encontraremos extensiones separables, el siguiente resultado será suficiente para el desarrollo del presente estudio; cabe mencionar que éste es un caso particular de un teorema que se puede encontrar en [4, capítulo 1, sección 5, teorema 20].

Teorema 3.8.7 *Sea L una extensión finita y separable sobre K y M una extensión normal de K tal que $K \subset L \subset M$. Entonces $\#\mathrm{In}_K(L, M) = [L : K]$.*

Corolario 3.8.8 *Sea L una extensión finita, normal y separable sobre K. Entonces $\#G(L/K) = [L : K]$.*

Corolario 3.8.9 *Sea L una extensión finita y separable de K, entonces $G(L/K)$ es finito.*

Demostración.- Sea F una clausura normal de K en L, entonces $\#\mathrm{In}_K(L, F) = [L : K]$. Dado $\tau \in G(L/K)$, reemplazamos el codominio de L por F para obtener una K-inmersión de L sobre F. Así obtendremos $\Theta : G(L/K) \to \mathrm{In}_K(L, F)$, definida $\Theta(\tau)(a) = \tau(a), \forall\, a \in L$. Puesto que Θ es inyectiva y su codominio es finito se sigue el corolario. □

Observación 3.8.10 Sea L un extensión de K y M, N cuerpos entre K y L. Si asumimos la convención de llamar a M y N como *$K-$conjugados* cuando existe un K-isomorfismo entre ellos, concluiremos por este último teorema que si L/K es normal, y M es un subcuerpo entre ellos, finito y separable sobre K, entonces M tiene a lo más $[M : K]$ $K-$conjugados en L.

Para terminar con esta sección, presentamos el siguiente teorema que es muy importante para la teoría de Galois, aunque no se refiere a extensiones algebraicas. En el futuro, nosotros tan sólo lo utilizaremos para garantizar la no nulidad de cierta función en algunas extensiones.

Teorema 3.8.11 (Dedekind) *Sean L y M dos cuerpos, y $\tau_1, \tau_2, \ldots, \tau_n : L \to M$ monomorfismos distintos. Entonces $\tau_1, \tau_2, \ldots, \tau_n$ son l.i. en el sentido siguiente:*

si $a_1, a_2, \ldots, a_n \in M$ y $\sum_{i=1}^{n} a_i \tau_i(b) = 0$, para todo $b \in L$, entonces $a_1 = a_2 = \cdots = a_n = 0$.

Demostración.- Vea [4, capítulo 2, sección 1, teorema 1]. □

3.9. Norma y traza

En esta sección tambien nos restringiremos a extensiones finitas y separables, para lo cual tan sólo estudiaremos extensiones finitas de cuerpos perfectos. De este modo serán validos los teoremas de la sección anterior. Supongamos que L es una extensión de un cuerpo perfecto K de grado $n \in \mathbb{N}$. Tomemos una clausura normal F de L/K, entonces existirán exactamente n K-inmersiones $\sigma_1, \sigma_2, \ldots, \sigma_n : L \to F$. Para esta clausura normal de L/K, dado un elemento $a \in L$ definimos la *norma de a sobre L/K* y la *traza de a sobre L/K* como

$$N_{L/K}(a) = \prod_{i=1}^{n} \sigma_i(a) \qquad \text{y} \qquad T_{L/K}(a) = \sum_{i=1}^{n} \sigma_i(a),$$

respectivamente. El siguiente teorema muestra la independencia de los valores que toman la norma y la traza respecto a la clausura normal eligida.

Teorema 3.9.1 *Sea L una extensión finita de un cuerpo perfecto K. Si $a \in L$ y* $\operatorname{Irr}(K,a) = x^r + c_{r-1}x^{r-1} + \cdots + c_0$, *entonces*

$$N_{L/K}(a) = ((-1)^r c_0)^{[L:K(a)]} \qquad y \qquad T_{L/K}(a) = -[L:K(a)]c_{r-1}.$$

Demostración.- Vea [4, capítulo 1, sección 9, teorema 26]. □

Observación 3.9.2

- Las funciones norma y traza no dependen de la clausura normal elegida.
- Dada una extensión L sobre un cuerpo K perfecto, los valores de las funciones norma y traza son elementos de K.
- Si L/K es normal, al igual que en el corolario 3.8.8, tendremos que $\operatorname{In}_K(L/L) = G(L/K)$, luego

$$N_{L/K}(a) = \prod_{\sigma \in G(L/K)} \sigma(a) \qquad \text{y} \qquad T_{L/K}(a) = \sum_{\sigma \in G(L/K)} \sigma(a)\,, \quad \text{para todo } a \in L.$$

Ejemplo 3.9.3 Si $d \in \mathbb{Z}$ no es cuadrado perfecto, tendremos que $\sqrt{d} \in \mathbb{C} \setminus \mathbb{Q}$ y $L = \mathbb{Q}(\sqrt{d})$ será una extensión cuadratica sobre $K = \mathbb{Q}$, por lo tanto normal sobre K. Como en el ejemplo 3.8.4, podemos deducir que $G(L/K) = \{\mathrm{id}, \tau\}$, donde $\tau(a + b\sqrt{d}) = a - b\sqrt{d}, \forall\ a, b \in \mathbb{Q}$ (la conjugación respecto a $\sqrt{2}$), luego $N_{L/K}(a) = \mathrm{id}\,(a+b\sqrt{d})\tau(a+b\sqrt{d}) = a^2 - b^2 d$. Nótese que en el caso $d := -1, 2, 3, \ldots$, esta "norma" coindice con la norma del respectivo dominio euclidano $\mathbb{Z}[\sqrt{d}]$.

Proposición 3.9.4 *Sea L una extensión finita de un cuerpo perfecto K, entonces*

1. *Dados $a, b \in L$ se tiene que*

$$N_{L/K}(ab) = N_{L/K}(a)N_{L/K}(b) \qquad y \qquad T_{L/K}(a+b) = T_{L/K}(a) + N_{L/K}(b)$$

2. *Si $a \in K$, se cumple que $N_{L/K}(a) = a^{[L:K]}$ y $T_{L/K}(a) = [L:K]a$.*

3. *Si η es un isomorfismo de L con otro cuerpo, entonces*

$$N_{\eta(L)/\eta(K)}\big(\eta(a)\big) = \eta\big(N_{L/K}(a)\big) \qquad y \qquad T_{\eta(L)/\eta(K)}\big(\eta(a)\big) = \eta\big(T_{L/K}(a)\big),$$

para todo $a \in L$.

4. Si M/L es una extensión finita y $a \in M$, entonces

$$N_{M/K}(a) = N_{L/K}(N_{M/L}(a)) \qquad y \qquad T_{M/K}(a) = T_{L/K}(T_{M/L}(a)).$$

Demostración.- Vea [4, capítulo 1, sección 9, teorema 27]. □

El siguiente lema indica la no trivialidad del concepto de traza. Este resultado será útil en un caso a tratar en el futuro.

Lema 3.9.5 *Sea L una extensión finita de un cuerpo perfecto K. Entonces la traza no es idénticamente nula.*

Demostración.- Sea N una clausura normal de L/K y $\sigma_1, \sigma_2, \ldots, \sigma_n$ todas las $K-$ inmersiones de L en M. Entonces $T_{L/K} = \sigma_1 + \sigma_2 + \cdots + \sigma_n$, y como esta es una combinación lineal no trivial de monomorfismos, el teorema 3.8.11 nos dice que es no nula. □

3.10. Clausura algebraica de un cuerpo

En el cuerpo $\mathbb{C}$ satisface el famoso teorema fundamental del álgebra, que fue demostrado por primera vez en 1821 por Cauchy, que nos dice que todo polinomio no constante con coeficientes en $\mathbb{C}$ tiene al menos una raíz en $\mathbb{C}$. Generalicemos esta propiedad por una serie de equivalencias.

Proposición 3.10.1 *Dado un cuerpo Ω, son equivalentes:*

- *Todo polinomio con coeficientes en Ω tiene al menos una raíz en Ω.*
- *Todo polinomio con coeficientes en Ω se descompone en Ω.*
- *Los únicos polinomios irreducibles en $\Omega[x]$ son lineales.*
- *No existen extensiones algebraicas sobre Ω distinta de éste mismo cuerpo.*

Demostración.- Vea [13, capítulo 1, sección 3, lema 3.10]. □

Definición 3.10.2 Diremos que un cuerpo es algebraicamente cerrado si satisface alguna de las condiciones de la proposición 3.10.1.

La siguiente proposición mostrará la repercusión y estabilidad de esta definición, en el sentido de mantener la característica de algebraicamente cerrado si se toma el conjunto adecuado.

Proposición 3.10.3 *Sea Ω un cuerpo algebraicamente cerrada que contenga a un cuerpo K. Si $L = \Omega^a$ es la clausura algebraica de K en Ω, entonces L también es algebraicamente cerrado.*

Demostración.- Por el corolario 3.2.9, L será una extensión de K, veamos que todo polinomio en L tiene al menos una raíz. Sea $f(X) \in L[X]$, por hipótesis se anula en algún $\alpha \in \Omega$, de donde α será algebraico sobre L. Como L/K es algebraica, por la proposición 3.2.10 tendremos que α es algebraico sobre K, por lo tanto $\alpha \in L$ y L es algebraicamente cerrado. □

Esta proposición nos menciona la posibilidad de encontrar un cuerpo algebraicamente cerrado y que únicamente contenga elementos algebraicos del cuerpo más pequeño, lo que será útil en los caso de $\mathbb{C}$ y $\mathbb{Q}$.

Definición 3.10.4 Dado L una extensión de un cuerpo K. Diremos que L es una *Clausura Algebraica de K*, si es una extensión algebraica de K algebraicamente cerrada.

Proposición 3.10.5 *Sea L una extensión algebraica de K tal que todo polinomio de K se descomponga en $L[X]$, entonces L es una clausura algebraica de K.*

Demostración.- Dado $f(X) \in L[X]$, encontremos una raíz de $f(X)$ en L. Sea M una extensión de L tal que exista una raíz α de $f(X)$. Entonces α es algebraico de L, luego α es algebraico sobre K. Como $\text{Irr}(K, \alpha)$ se descompone en L, por el lema 3.6.3 tendremos que $\alpha \in L$. □

Teorema 3.10.6 *Todo cuerpo K tiene una clausura algebraica.*

Demostración.- Vea [13, capítulo 1, sección 3, teorema 3.14]. □

Ahora cabe una pregunta: si tenemos dos clausuras algebraicas de un mismo cuerpo y encontramos propiedades algebraicas en ambos cuerpos, ¿estas pueden diferenciarse de manera radical?. El siguiente lema nos brinda el grado de generalidad que obtenemos si trabajamos con una sola clausura algebraica, esto es, la medida de unicidad de un cuerpo con esas características.

Lema 3.10.7 *Sean $\mathbb{A}$ y $\mathbb{B}$ clausuras algebraicas de un mismo cuerpo K, entonces estos cuerpos son $K-$isomorfos.*

Demostración.- Vea [4, capítulo 1, sección 3, corolario 3.21]. □

Corolario 3.10.8 *Sea L una extensión algebraica sobre un cuerpo K y $\mathbb{A}$ una clausura algebraica de este último. Entonces existe una $K-$inmersión $\sigma : L \to \mathbb{A}$.*

Demostración.- Tomemos una clausura algebraica $\mathbb{B}$ sobre L, la cual tambien sera también una extensión algebraica de K y, por lo tanto, otra clausura algebraica de K. Tomando la restricción a L de un isomorfismo entre $\mathbb{B}$ y $\mathbb{A}$, concluimos el corolario. □

Este corolario responde a la observación previa, pues nos dice que el análisis de las propiedades algebraicas de una extensión se puede realizar dentro de una clausura algebraica del cuerpo inicial. Veremos que este tipo de análisis es más fuerte en el caso de cuerpos finitos, como veremos en la siguiente sección.

Un resultado importante para nuestro trabajo que se puede generalizar pertenece al ambito del algebra lineal, el cual es un conocido lema acerca de formas canónicas de las matrices en $\mathbb{C}$.

Lema 3.10.9 *Sea K un cuerpo completo y $A \in K^{n\times n}$. Entonces existe $P \in K^{n\times n}$ inversible tal que $P^{-1}AP$ es una matriz triangular superior.*

Una demostración de este teorema puede ser encontrada en [5, capítulo 6, sección 4, teorema 6.j]; también se puede seguir el razonamiento empleado en [11, parte 1, capítulo 5, sección 3, proposición 2] para el caso $K = \mathbb{C}$, válido para este contexto puesto que tan sólo utiliza la existencia de un autovalor de la matriz A en K.

3.11. Cuerpos finitos

En secciones anteriores habíamos hablado acerca del cuerpo primo de un cuerpo, que en caso de característica p veíamos que era un cuerpo isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Luego, aparecía la pregunta: ¿qué otro cuerpo finito puede existir? Durante esta sección estudiaremos la estructura de estos cuerpos, más aún veremos que estas condiciones caracterizan totalmente este tipo de cuerpo y brindandonos un método de construcción. Empecemos la sección con un resultado que nos muestra la restrinción que posee la cardinal de un cuerpo finito.

Proposición 3.11.1 *Sea L una extensión sobre el cuerpo finito K, entonces $[L : K] = n$ si y sólo si $\#L = (\#K)^n$.*

Demostración.- Supongamos que $\{a_1, \ldots, a_n\} \subset L$ es una base sobre K. Entonces $L = Ka_1 \oplus \cdots \oplus Ka_n$, y $\#L = p^n$; de esta forma se verifica la equivalencia propuesta. □

Puesto que todo cuerpo de característica positiva p posee un subcuerpo primo isomorfo a $\mathbb{Z}/p\mathbb{Z}$, podemos establecer el siguiente resultado.

Corolario 3.11.2 *Dado un cuerpo finito K con $p = \operatorname{car} K$, entonces $\#K = p^n$ para algún $n \in \mathbb{N}$.*

Teorema 3.11.3 *Sean K un cuerpo y G un subgrupo finito de $K^\times$. Entonces G es cíclico.*

Demostración.- Vea por ejemplo [4, capítulo 1, sección 6, teorema 23]. □

Corolario 3.11.4 *Dada L/K una extensión de cuerpos finitos, esta extensión será simple.*

Dado un cuerpo K con característica $p > 0$, esté tendra un cuerpo primo isomorfo a $\mathbb{Z}/p\mathbb{Z}$; por lo tanto, sin perdida de generalidad, supondremos que estos cuerpos son siempre extensiones de $\mathbb{Z}/p\mathbb{Z}$.

El siguiente teorema caracteriza la estructura de los cuerpos finitos como cuerpos de descomposición de un cierto polinomio en $\mathbb{Z}/p\mathbb{Z}$.

Teorema 3.11.5 *Dado $p, n \in \mathbb{N}$ con p primo, salvo isomorfismo, existe un único cuerpo F con p^n elementos, el cual será un c.d. de $X^{p^n} - X$ sobre $(\mathbb{Z}/p\mathbb{Z})$.*

Demostración.- Vea [4, capítulo 1, sección 6, teorema 22]. □

El siguiente teorema nos da la estructura de todo cuerpo finito como extensión de uno más pequeño; en el caso de su cuerpo primo nos da una extensión de $\mathbb{Z}/p\mathbb{Z}$

Teorema 3.11.6 *Sea L es una extensión de grado n sobre un cuerpo finito K de $q = p^r$ elementos, donde $p = \operatorname{car} K$. Entonces*

1. *el cuerpo L es un c.d. de $X^{q^n} - X \in K[x]$, donde $n = [L : K]$; en particular es normal;*
2. *el grupo de Galois $G(L/K)$ es generado por el automorfismo ξ^r, donde ξ es el automorfismo de Frobenius.*

Demostración.- El primer ítem es una reformulación del teorema previo, el segundo se encuentra en [13, capítulo 2, sección 6, corolario 7]. □

De ahora en adelante, denotaremos por $\mathbb{F}_{p^n}$ al cuerpo de p^n elementos, el cual es único salvo isomorfismos. Asi pues, $\mathbb{F}_p$ se confundirá con el cuerpo $\mathbb{Z}/p\mathbb{Z}$. A continuación veremos que esta condición de unicidad salvo isomorfismo se refuerza si suponemos que los cuerpos en cuestión estan contenidos en una clausura algebraica de un $\mathbb{F}_q$, donde $q = p^n$ con p como la característica del cuerpo. Recordando que las extensiones de $\mathbb{F}_q$ seran del tipo $\mathbb{F}_{p^n}$ (por la proposición 3.11.1), presentamos el siguiente resultado.

Teorema 3.11.7 *Sea Ω una clausura algebraica de $\mathbb{F}_q$. Entonces*

- *Dado $n \in \mathbb{N}$, existe un único cuerpo $\mathbb{F}_{q^n}$ de q^n elementos en Ω, que es el conjunto de raíces en Ω del polinomio $X^{q^n} - X \in \mathbb{F}_q[X]$.*

- *Se tiene que* $\Omega = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{q^n}$.
- *Dados* $n, m \in \mathbb{N}$, $\mathbb{F}_{q^n} \subset \mathbb{F}_{q^m}$ *si y sólo* $n \mid m$.

Demostración.- El primer ítem y tercer í pueden ser encontrados en [13, capítulo 2, sección 6, teorema 8], siendo el segundo consecuencia del corolario 3.2.6. □

Esto nos trae resultados atractivos, como el siguiente lema.

Lema 3.11.8 *Sea* $a \in L$ *extensión de* $\mathbb{F}_q$. *Entonces:*

(1) si $f(X) = \mathrm{Irr}(K, a)$ *y tiene grado* n, *entonces* $a^q, a^{q^2}, \ldots, a^{q^n}$ *son todas las raíces de* $f(x)$, *en el sentido que estos conforman todos los factores lineales de* $f(X)$;

(2) si a *es raíz de* $f(X)$, *entonces* a^q *también es raíz de* $f(X)$.

Demostración.- Vea [13, capítulo 2, sección 6, corolario 9]. □

Lema 3.11.9 *Sean* σ *un* $\mathbb{F}_q-$*automorfismo de* $\mathbb{F}_{q^n}$ *distinto de la identidad, entonces* $\mathcal{F}(\sigma) = \{a \in \mathbb{F}_{q^n} \ , \ \sigma(a) = a\}$ *será una extensión de* $\mathbb{F}_q$ *estrictamente contenida en* $\mathbb{F}_{q^n}$.

Demostración.- Sea $q = p^r$ con $p \in \mathbb{N}$, y $\sigma = \chi^j = (\xi^r)^j$ donde $j \in \{1, 2 \ldots, n-1\}$ (en virtud del teorema 3.11.6), lo que significa que $\sigma(a) = (\xi^r)^j(a) = a^{p^{rj}}$, para todo $a \in \mathbb{F}_q$. Nótese que $\mathcal{F}(\sigma)$ es cerrado bajo la suma, el producto e inversión, por lo tanto un subcuerpo de $\mathbb{F}_{q^n}$. Más aun, este cuerpo será el conjunto de los ceros de $X^{q^j} - X \in \mathbb{F}_q[X]$, el único cuerpo que contenido en $\mathbb{F}_{q^n}$ (pues podemos asumir que $\mathbb{F}_{q^n}$ esta contenido en una clausura algebraica de $\mathbb{F}_q$, vea el corolario 3.10.8). Entonces $\mathcal{F}(\sigma) = \mathbb{F}_{q^j}$ con $j < n$ y $\mathcal{F}(\sigma)$ está contenido propiamente en $\mathbb{F}_q^n$. □

El siguiente punto a tratar es el comportamiento de la traza de las extensiones finitas de cuerpos finitos.

Lema 3.11.10 *Dado* $q = p^r$, *la traza* $T_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ *es dada por*

$$T_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{r-1}}, \quad \text{para cada } \alpha \in \mathbb{F}_p,$$

y es un epimorfismo entre los grupos $(\mathbb{F}_q, +)$ *y* $(\mathbb{F}_p, +)$.

Demostración.- Puesto que $\mathbb{F}_q/\mathbb{F}_p$ es normal y separable (pues $\mathbb{F}_p$ es finito), la traza se expresa como la suma de los $\mathbb{F}_p$-automorfismos de $\mathbb{F}_q$. Puesto que el segundo ítem del teorema 3.11.6 indica que este grupo es generado por el automorfimos de Frobenius, concluimos que la igualdad de arriba es cierta. Y, como $\mathbb{F}_q/\mathbb{F}_p$ es separable, tendremos que $T_{\mathbb{F}_q/\mathbb{F}_p}$ es no nula, por lo tanto

existe $\alpha_0 \in \mathbb{F}_p$ tal que $T_{\mathbb{F}_q/\mathbb{F}_p}(\alpha_0) = a \in \mathbb{F}_p^\times$. Como $\mathbb{F}_p$ es generado es cuerpo primo de $\mathbb{F}_q$, es generado por $1 \in \mathbb{F}_p$, entonces $T_{\mathbb{F}_q/\mathbb{F}_p}(\alpha_0) = n_0 \cdot 1$ para algún $n_0 \in \mathbb{N}$ coprimo con p (de lo contrario esta evaluación sería nula). Luego, dado $a \in \mathbb{F}_p$ tomamos $n, m \in \mathbb{N}$ tales que

$$a = n \cdot 1 \quad \text{y} \quad mn_0 \equiv n \text{ mód } p,$$

de donde tendremos que

$$T_{\mathbb{F}_q/\mathbb{F}_p}(m\alpha_0) = mT_{\mathbb{F}_q/\mathbb{F}_p}(\alpha_0) = m(n_0 \cdot 1) = n \cdot 1 = a.$$

3.12. Raíces de la unidad

El concepto raíz de la unidad nos es familiar en el ambito de $\mathbb{C}$, a decir, un elemento de $u \in \mathbb{C}$ es una raíz de la unidad si $u^n = 1$ para algún $n \in \mathbb{N}$. Ahora extenderemos este concepto y sus propiedades a cuerpos de característica 0. La siguiente definición tendrá sentido si recordamos la estructura de grupo abeliano que posee su conjunto de elementos no nulos.

Definición 3.12.1 Sea K un cuerpo de característica 0. Dado $u \in K^\times$, este será una *raíz n-ésima de la unidad* si $u^n = 1$. En el caso que $\text{ord}(u) = n$ (respecto al grupo $(K^\times, \cdot)$), diremos que u es una *raíz primitiva n−ésima de la unidad.*

Observación 3.12.2

- Por definición, toda raíz n−ésima de la unidad será un cero del polinomio $X^n - 1$. Por lo tanto, existen a lo más n raíces de la unidad en K.
- Si Ω es una clausura algebraica de K, entonces existen a lo más n raíces n−ésimas de la unidad en Ω.
- Para cada $n \in \mathbb{N}$, el conjunto $G = \{u \in K,\ u^n = 1\}$ es un subgrupo finito multiplicativo de $K^\times$. Luego, en virtud del lema 3.11.3, G posee un generador u_0, el cual será una raíz primitiva m−ésima de la unidad, donde $m = \#G$.
- De la definición previa, si u es una raíz n−ésima primitiva de la unidad, entonces $u^m = 1$ si y sólo si n divide a m. En consecuencia, las potencias $u, u^2, \ldots, u^n = 1$ son distintas.
- Si K posee n raíces n−ésimas de la unidad, entonces K poseerá una raíz primitiva n−ésima de la unidad.

- Si $u \in K^\times$ es una raíz primitiva $n-$ésima de la unidad, entonces u^m será raíz primitiva $t-$ésima de la unidad, donde $t = (m, n)$.

- Si $u, v \in K^\times$ son raíces de la unidad de orden n y m respectivamente y m divide a n, entonces u es una potencia de v.

- Si K es extensión de k y $u \in K$ es una raíz n-ésima, entonces todo k-conjugado de u en K tambien es una raíz $n-$ésima.

El siguiente resultado, nos establece una propiedad cuantitativa e inherente de las raíces de la unidad.

Lema 3.12.3 *Sea K un cuerpo de característica 0, y $u_1, u_2, \ldots, u_r \in K$ las raíces $n-$ésimas de la unidad en K. Entonces, dado $s \in \mathbb{N}$ tendremos que*

$$\sum_{i=1}^{r} u_i = \begin{cases} r & , \text{ si } r \text{ divide as;} \\ 0 & , \text{ en caso contrario.} \end{cases}$$

Demostración.- Por la observación previa, el grupo de las raíces n-ésimas de la unidad admite un generador $u_0 \in K$. Entonces $u_0^r = 1$, y $u_0^r \neq 1$ cuando $r \nmid s$. Como es claro que la identidad de arriba es cierta para el primer caso, suponemos que $r \nmid s$. Entonces,

$$\sum_{i=1}^{r} u_i^s = \sum_{j=1}^{r} (u^j)^s = \sum_{j=0}^{r} (u^s)^j = \frac{(u^s)^r - 1}{u^s - 1} = 0.$$

Capítulo 4

Valuación y valores absolutos sobre dominios

4.1. Valuación

Definición 4.1.1 Dado un dominio D, diremos que $v : D \to \mathbb{R} \cup \{+\infty\}$ es una *valuación sobre* D, si

1. $v(0) = +\infty$;
2. $v(ab) = v(a) + v(b)$, para todo $a, b \in D$;
3. $v(a+b) \geq \text{mín}\{v(a), v(b)\}$, para todo $a, b \in D$.

Observaciones 4.1.2

1. Usualmente una valuación es una funcion definida en los elementos no nulos de un anillo en donde se cumplen las propiedades 2. y 3. (en la propiedad 3. sólo se considera el caso en el que $a + b \neq 0$); por tanto, nuestra definición es un caso particular.
2. En lo siguiente, para demostrar que una función v es una valuación sobre un dominio, tan sólo asumiremos $v(0) = +\infty$ y demostraremos las propiedades 2. y 3. de la definición anterior en el caso $a, b, a+b$ no nulos, pues en caso contrario se verifican inmediatamente.

La siguiente proposición nos describe el tipo de valuación más importante en este trabajo.

Proposición 4.1.3 *Supongamos que D es un dominio de factorización única (d.f.u.) y p un elemento irreductible de D. Entonces $v : D \to \mathbb{R}$ definida por*

$$v(x) = \text{máx}\{m \ : \ p^m \mid x\}, \qquad \textit{para todo } x \in D \setminus \{0\},$$

es una valuación.

Demostración.- Tomemos x e y no nulos, $r = v(x)$ y $s = v(y)$; entonces $p^{r+s} \mid xy$, por lo cual $r+s \leq v(xy)$. Si $v(xy) > r+s$ entonces $p^{r+s+1} \mid xy$, luego $p^{s+1} \mid \frac{x}{p^r}y$, y como mcd $(p, \frac{x}{p^r}) = 1$, tendremos que $p^{s+1} \mid y$, lo que contradice la definición de $v(y)$. Si además $x+y \neq 0$ entonces tomando $u = \text{mín}\{r,s\}$ tendremos que $x+y = p^u(\frac{x}{p^u} + \frac{y}{p^u})$ donde los factores son no nulos; luego, por la propiedad ya demostrada, se concluye que

$$v(x+y) = v(p^u) + v(\frac{x}{p^u} + \frac{y}{p^u}) \geq u + 0.$$

Ejemplo 4.1.4 Para cualquier K cuerpo, el anillo $K[X]$ es un dominio euclidiano, por lo tanto un *d.f.u.* que contiene al polinomio X como elemento irreductible. Luego, la función $v_X : K[X] \to \mathbb{R}$, definida por $v_X(t) = \text{máx}\{m\,;\ X^m \mid t\}$ es una valuación.

Proposición 4.1.5 *Sea D un dominio y v una valuación en D, entonces v se extiende de manera única a una valuación sobre su cuerpo de fracciones.*

Demostración.- Si K es el cuerpo de fracciones de D y $x \in K$, definimos $v(x) = v(a) - v(b)$ para $a, b \in D$ con $x = a/b$; está sera una buena definición. En efecto, si $a, b, c, d \in D$ tales que $a/b = c/d$, entonces $ad = cb$, por tanto $v(a) + v(d) = v(c) + v(b)$, con lo cual se concluye su buena definición. La verificación de las propiedades 2. y 3. y la unicidad son inmediatas. □

Por otra parte, se puede extender una valuación de un cuerpo K a su anillo de polinomios $K[X]$, de la siguiente manera.

Proposición 4.1.6 *Dada una valuación v sobre un cuerpo K y $c \in \mathbb{R}$, podemos extender la valuación v a $K[X]$ tomando $w : K[X] \to \mathbb{R} \cup \{+\infty\}$ definida por*

$$w(a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0) = \text{mín}\{ci + v(a_i), i = 0, 1, \ldots, n\},$$

para $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \neq 0$.

Demostración.- Sean $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ y $g(X) = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_0$ en $K[X]$, verifiquemos que se cumplen las propiedades enunciadas en la definición de valuación. Empecemos por la propiedad 3, para esto supongamos que $n < m$ y tomemos $a_{n+1} = a_{n+2} =$

$\cdots = a_m = 0$, entonces $w\big(f(X)\big) = \min\{ci + v(a_i); i = 0, 1, \ldots, m\}$ y por lo tanto

$$\begin{aligned} w(f(X)+g(X)) &= \min\{cj + v(a_j + b_j);\ j = 0, 1, \ldots, m\} \\ &= cj_0 + v(a_{j_0} + b_{j_0}), \qquad \text{para algún } j_0, \\ &> \min\{c_{j_0} + v(a_{j_0}), c_{j_0} + v(b_{j_0})\} \\ &> \min\Big\{ \min_{1\le i\le m}\{ci + v(a_i)\}, \min_{1\le i\le m}\{cj + v(b_j)\} \Big\} \end{aligned}$$

y tendremos la propiedad buscada. Y para mostrar la propiedad 2., tomamos

$$f(X)g(X) = c_{n+m}X^{n+m} + c_{n+m-1}X^{n+m-1} + \cdots + c_0,$$

tendremos que

$$\begin{aligned} w\big(f(X)g(X)\big) &= \min\Big\{ck + v\Big(\sum_{i+j=k} a_i b_j\Big), k = 0, 1, \ldots, n+m\Big\} \\ &= ck_0 + v\Big(\sum_{i+j=k_0} a_i b_j\Big), \quad \text{para algún } k_0 \\ &> ck_0 + \min\{v(a_i) + v(b_j), i + j = k_0\} \\ &= \min\big\{ci + v(a_i) + cj + v(b_j), i + j = k_0\big\} \geq w\big(f(x)\big) + w\big(g(x)\big). \end{aligned}$$

Finalmente, demostraremos la desigualdad contraria. Elijamos

$$i_0 = \min\Big\{i; ci + v(a_i) = w\big(f(x)\big)\Big\} \quad \text{y} \quad j_0 = \min\Big\{j; cj + v(b_j) = w\big(g(X)\big)\Big\}$$

para analizar cada sumando de $c_{i_0+j_0}$, cuyos índices i y j suman $k_0 = i_0 + j_0$, de la forma siguiente:

- Si $i < i_0$, entonces $ci + v(a_i) > ci_0 + v(a_{i_0})$ de donde

  $$ck_0 + v(a_i b_j) = ci + cj + v(a_i) + v(b_j) > ci_0 + cj_0 + v(a_{i_0}) + v(b_{j_0}) = ck_0 + v(a_{i_0} b_{j_0}),$$

  por lo cual $v(a_i b_j) > v(a_{i_0} b_{j_0})$.

- Si $i = i_0$, entonces $j = k_0 - i = j_0$ y tenemos que el sumando es $a_{i_0} b_{j_0}$.

- Si $i > i_0$, entonces $k_0 - j > k_0 - j_0$ y por lo tanto $j > j_0$, luego $cj + v(b_j) > cj_0 + v(b_{j_0})$ y $ck_0 + v(a_i b_j) > ck_0 + v(a_{i_0} b_{j_0})$, de modo que $v(a_i b_j) > v(a_{i_0} b_{j_0})$.

Concluimos que

$$v\Big(\sum_{i+j=k_0} a_i b_j\Big) = \min\{v(a_i b_j), i + j = k_0\} = v(a_{i_0} b_{j_0}),$$

y por lo tanto

$$w\big(f(X)g(X)\big) \leq c_{k_0} + v(c_{k_0}) = ck_0 + v(a_{i_0}b_{j_0}) = w\big(f(X)\big) + w\big(g(X)\big),$$

y conseguimos demostrar 2. □

Si restringimos una valuación v sobre un cuerpo K a su grupo multiplicativo $K^\times$, tendremos que esta función es un homomorfismo de grupos, por lo tanto $v(K^\times)$ será un subgrupo aditivo de $\mathbb{R}$.

Definición 4.1.7 Sea v una valuación sobre un cuerpo K, el conjunto $v(K^\times)$ es denominado *grupo de valuación de v sobre K.*

Ejemplos 4.1.8

- Podemos extender la valuación v_X definida en el ejemplo 4. 1. 4sobre $K[X]$ a su cuerpo de fracciones $K(X)$, como indica la proposición 4. 1. 5,así tendremos de manera inmediata que $v_X\big(K(X)^\times\big) = \mathbb{Z}$.
- Supongamos que v es una valuación sobre un cuerpo K tal que $v(K^\times) = \mathbb{Z}$ y $c \notin \mathbb{Q}$. Tomando la valuación w definida en $K[X]$ por la proposición 4. 1. 6,la extendemos sobre $K(X)$. Entonces $w\big(K(X) \setminus \{0\}\big) = \{m + nc\ ;\ m, n \in \mathbb{Z}\}$, y como es bien conocido este grupo aditivo será denso en $\mathbb{R}$.

Una valuación sobre un cuerpo provee al cuerpo de estructura algebraica adicional la cual será beneficiosa en el futuro.

Proposición 4.1.9 *Sea v una valuación sobre un cuerpo K, entonces*

$$\mathcal{O} = \{x \in K\ :\ v(x) \geq 0\}$$

es un anillo y

$$\mathfrak{p} = \{x \in K; v(x) > 0\}$$

es su ideal propio más grande. En particular $\mathfrak{p}$ es el único ideal maximal y $\mathcal{O}/\mathfrak{p}$.

Demostración.- A partir de las propiedades de valuación de v es fácil mostrar que $\mathcal{O}$ es un anillo y $\mathfrak{p}$ es un ideal; por tanto, sólo verificaremos que $\mathfrak{p}$ contiene a todo ideal propio. En efecto, si $I \subset \mathcal{O}_K$ es un ideal, el hecho que exista $x \in \mathcal{O} \setminus \mathfrak{p}$, implica que $v(x) = 0$, luego $x \neq 0$ y $v(x^{-1}) = 0$. Por tanto, $x^{-1} \in \mathcal{O}$ y $1 = x^{-1}x \in I$, de este modo $I = \mathcal{O}$; así concluimos que si I es propio, entonces $I \subset \mathfrak{p}$. Esto implica que $\mathfrak{p}$ es maximal, y que si existe otro ideal maximal J, entonces $J \subset \mathfrak{p}$, y por tanto $J = \mathfrak{p}$. □

Definición 4.1.10 Dada una valuación v sobre cuerpo K, el *anillo de valuación de* v es

$$\mathcal{O} = \{x \in K \quad v(x) \geq 0\},$$

su *ideal de valuación* es

$$\mathfrak{p} = \{x \in K; v(x) > 0\},$$

y su *cuerpo residual* es $\kappa = \mathcal{O}/\mathfrak{p}$.

Ahora veremos un lema muy interesante que describe una propiedad estructural que nos brinda una valuación.

Lema 4.1.11 *Sea v una valuación sobre un cuerpo L_2 que es extensión de L_1. Denotemos por $\mathcal{O}_i, \mathfrak{p}_i$ y κ_i al anillo de valuación, ideal de valuación y cuerpo residual de K_i, respectivamente. Entonces, se cumplen:*

(i) $\mathcal{O}_1 \subset \mathcal{O}_2$ *y* $\mathfrak{p}_1 \subset \mathfrak{p}_2$;

(ii) la función $a+\mathfrak{p}_1 \mapsto a+\mathfrak{p}_2$ *es un monomorfismo entre los cuerpos* K_1 *y* K_2. *En particular,* κ_2 *es una extensión de* κ_1.

Demostración.- El ítem *(i)* es consecuencia inmediata de las definiciones de anillo e ideal de valuación, lo que nos da el homomorfismo de inclusión $j : \mathcal{O}_1 \to \mathcal{O}_2$, y tomando la proyección canónica $\phi : \mathcal{O}_2 \to \mathcal{O}_2/\mathfrak{p}_2$, tendremos el homomorfismo $\lambda : \mathcal{O}_1 \to \mathcal{O}_2/\mathfrak{p}_2$ definido por $\lambda(a) = a + \mathfrak{p}_2$. Como

$$\mathrm{Nu}(\lambda) = \{a \in \mathcal{O}_1 \ : \ a \in \mathfrak{p}_2\} = \mathfrak{p}_1,$$

el homomorfismo λ induce, de manera natural, un monomorfismo $\widetilde{\lambda} : \mathcal{O}_1/\mathfrak{p}_1 \to \mathcal{O}_2/\mathfrak{p}_2$ definido por $\widetilde{\lambda}(a + \mathfrak{p}_1) = a + \mathfrak{p}_2$. Así concluimos que $\kappa_2 = \mathcal{O}_2/\mathfrak{p}_2$ es una extensión de $\kappa_1 = \mathcal{O}_1/\mathfrak{p}_1$. □

4.2. Valores absolutos

Definición 4.2.1 Sea D un dominio, diremos que $|\cdot| : D \to \mathbb{R}$ es un *valor absoluto sobre* D si cumple:

1. $|x| \geq 0$ para todo $x \in D$;
2. $|x| = 0$ si y sólo si $x = 0$;
3. $|xy| = |x||y|$ para todo $x, y \in D$;

4. $|x+y| \leq |x| + |y|$ para todo $x, y \in D$ (*Desigualdad triangular*);
   Si además $|\cdot|$ cumple

5. $|x+y| \leq \max\{|x|, |y|\}$. para todo $x, y \in D$.

diremos que $|\cdot|$ es *no arquimediano*, sino que es *arquimediano.*

Escribiremos $(D, |\cdot|)$ para referirnos al dominio provisto de un valor absoluto en particular; más aun, dependiendo de que $|\cdot|$ sea arquimediano o no, diremos que $(D, |\cdot|)$ es arquimediano o no. Además $|D|$ denotará al conjunto $\{|x| \; ; \; x \in D\}$.

Proposición 4.2.2 *Sea $|\cdot|$ un valor absoluto sobre D, se cumple:*

(i) $|1| = 1$;

(ii) Si $x^n = 1$, *entonces* $|x| = 1$; *en particular* $|-1| = 1$.;

(iii) $|x| = |-x|$, *para todo* $x \in D$;.

(iv) Si $|\cdot|$ es no arquimediano, entonces

$$|a_1 + a_2 + \cdots + a_n| \leq \max\{|a_1|, |a_2|, \ldots |a_n|\}, \quad \textit{para todo } a_1, a_2 \ldots a_n \in D.$$

(v) Dados $a, b \in D$ *se tiene que* $||a| - |b|| \leq |a - b|$.

Demostración.- Como $|1| \neq 0$ y $|1| = |1 \cdot 1| = |1||1|$, se tiene que $|1| = 1$; por lo tanto (i) es cierto. Suponiendo que $x^n = 1$ obtendremos que $x \neq 0$, $|x| > 0$. luego, por inducción, $|x|^n = |x^n| = |1| = 1$; por lo tanto $|x|$ es una raíz positiva real de 1, de modo que $|x| = 1$; de este modo tenemos (ii). Tenemos (iii) a partir de (ii), y los ítems (iv) y (v) son inmediatos. □

Observaciones 4.2.3

1. En la definición 4.2.1, La propiedad 5 implica 4.

2. *El cuarto ítem de la definición 4.2.1 para un valor absoluto $|\cdot|$ puede ser reemplazado por*

   $4'$ $|x+1| \leq \max\{|x|, 1\}$, para todo $x \in K$.

   En efecto, es claro que esta propiedad es una condición necesaria; procedamos a verificar el cuarto ítem, a partir de los tres primeros y esta propiedad. Sean $x, y \in K$, si $y = 0$ entonces la propiedad no arquimediana se satisface. En caso contrario, existe $z = x/y$ y tendremos que $|x/y + 1| \leq \max\{|x/y|, 1\}$, y por lo tanto $|x+y| \leq \max\{|x|, |y|\}$.

3. De igual modo que en la proposición 4.1.5, un valor absoluto $|\cdot| : D \to \mathbb{R}$ se puede extender a su cuerpo de fracciones de manera natural definiendo $|x| = |a|/|b|$ para $a, b \in D$ tales $x = a/b$. Se puede mostrar que es una buena definición y es un valor absoluto sobre K, siendo arquimediana si lo era antes, o no si antes no lo era.

Proposición 4.2.4 *Sea D un dominio y $|\cdot|$ un valor absoluto sobre D, entonces $|\cdot|$ se extiende de manera única a un valor absoluto sobre su cuerpo de fracciones.*

Demostración.- Si K es el cuerpo de fracciones de D y $x \in K$, definimos $\|x\| = |a||b|$ para $a, b \in D$ con $x = a/b$; la cual es una buena definición. Verificar que $\|\cdot\|$ es un valor absoluto y su unicidad como extensión de $|\cdot|$ son inmediatas. □

Proposición 4.2.5 *Sea D un dominio y $c > 1$.*

1. *Si v es una valuación sobre D y $|\cdot| : D \to \mathbb{R}$ es definido por*

$$|x| = \begin{cases} c^{-v(x)} & , \ si\ x \neq 0, \\ 0 & , \ si\ x = 0, \end{cases},$$

   entonces $|\cdot|$ es un valor absoluto no arquimediano sobre D.

2. *Si $|\cdot|$ es un valor absoluto no arquimediano sobre D y $v : D \to \mathbb{R}$ es definido por*

$$v(x) = -\log_c(|x|), \ \ para\ cada\ x \in D \setminus \{0\},$$

   entonces v es una valuación.

Demostración.- Es de verificación inmediata.

Observaciones 4.2.6

- Esta proposición nos dice que fijado $c > 1$, todo valor absoluto no arquimediano induce una valuación y que toda valuación nos induce un valor absoluto no arquimediano. Utilizaremos la denominación de *inducido por* para referirnos a las anteriores funciones construidas utilizando $c > 1$.

- Fijemos $c > 1$. Si $|\cdot|$ es un valor absoluto y v es una valuación inducida por $|\cdot|$ como en la proposición anterior (con parámetro c), entonces el valor absoluto que induce v (con parámetro c) es $|\cdot|$; esto también es cierto para el caso de una valuación.

- Sea v una valuación sobre D y $|\cdot|$ el valor absoluto inducido por v, entonces el anillo e ideal de valuación están dados por

$$\mathcal{O}_v = \{x \in D\,;\ |x| \leq 1\} \quad \text{y} \quad \mathfrak{p}_v = \{x \in D\,;\ |x| < 1\}.$$

Ejemplos 4.2.7

1. Siguiendo las notaciones del ejemplo 4.1.4, por la proposición anterior, tomando $c = e$ la base del logaritmo neperiano y $v = v_X$, tenemos que $|\cdot|_X : K[X] \to \mathbb{R}$ definido por $|t|_X = e^{-v_X(t)}$ para todo $t \in K[X] \setminus \{0\}$ es un valor absoluto no arquimediano.

2. Por la proposición 4.2.4, el valor absoluto $|\cdot|_X$ sobre $K[X]$ se puede extender a su cuerpo de fracciones; a este valor absoluto también lo denotaremos por $|\cdot|_X$.

3. Si $(K, |\cdot|)$ es no arquimediano, entonces la función $v : K \to \mathbb{R}$ definida por $v(a) = -\log(|a|)$, para $a \in K \setminus \{0\}$, nos da una valuación. Luego, tomando $c \in \mathbb{R}$ (fijo), esta valuación se puede extender al anillo $K[X]$ tomando

$$w\big(f(X)\big) = \min\{ci + v(a_i), i = 0, 1, \ldots, a_n\}, \quad \text{cuando } f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \neq 0.$$

   Esta nueva valuación nos genera una extensión del valor absoluto original en $K[X]$ tomando $\|f(X)\| = e^{-v\left(f(X)\right)}$, para todo $f(X) \in K[X] \setminus \{0\}$. Veamos algunas propiedades de este nuevo valor absoluto en el caso de $c = 0$, que luego serán utilizadas en las demostraciones sucesivas.

Proposición 4.2.8 *Sea $(K, |\cdot|)$ no arquimediano y $\|\cdot\|$ el valor absoluto no arquimediano definido por $\|f(X)\| = \max\{|a_i|, i = 0, 1, \ldots, n\}$ cuando $f(X) = a_n X^n + \cdots + a_1 X + a_0 \neq 0$. Entonces, se cumplen las siguientes propiedades:*

(i) Dados $\alpha \in K$, $f(X) \in K[X]$, ocurre que $|f(\alpha)| \leq \|f(X)\| \max\{1, |\alpha|^n\}$.

(ii) Si $\alpha \in K$ es una raíz de $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$, entonces

$$|\alpha| \leq \max\{1, \|f(X)\|/|a_n|\}.$$

(iii) Si $f(X), g(X) \in K[X]$ son mónicos de grado n con raíces distintas $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ y $\beta_1, \beta_2, \ldots, \beta_n \in K$ (respectivamente), entonces $D\big(f(X), g(X)\big) = \prod_{i,j=1}^{n}(\alpha_i - \beta_j)$, el producto de las diferencias de la raíces de $f(X)$ y $g(X)$, satisface

$$|D(f(X), g(X))| \leq \Big(\|f(X) - g(X)\| \max\{1, \|f(X)\|^n\}\Big)^n.$$

Demostración.

(i) Escribamos $f(X) = a_nX^n + a_{n-1}X^{n-1} \cdots + a_0$, por la propiedad no arquimediana de $|\cdot|$ obtenemos que

$$f(\alpha) \leq \max\{|a_i\alpha^i| \ , \ i = 0, 1, \cdots, n\} = \max\{|a_i||\alpha|^i \ , \ i = 0, 1, \cdots, n\}.$$

Si $|\alpha| \geq 1$, tendremos que

$$|f(\alpha)| \leq \max\{|a_i||\alpha|^n \ , \ i = 0, 1, \ldots, n\} = \|f(X)\||\alpha|^n;$$

y en el caso que $|\alpha| < 1$ también se satisface (i).

(ii) Se tiene que

$$|a_n||\alpha|^n = |-a_{n-1}\alpha^{n-1} - \cdots - a_0| \leq \max\{|a_i||\alpha|^i \ , \ i = 0, 1, 2, \ldots, n-1\}.$$

Si $|\alpha| \geq 1$, se tendrá que

$$|a_n||\alpha|^n \leq \|f(X)\||\alpha|^{n-1},$$

y en consecuencia $|\alpha| \leq \|f(X)\|/|a_n|$, de lo cual se concluye (ii).

(iii) Puesto que $g(X) = (X - \beta_1) \cdots (X - \beta_n)$, se tendrá que

$$D\big(f(X), g(X)\big) = \prod_{i=1}^{n} g(\alpha_i) = \prod_{i=1}^{n} \big(g(\alpha_i) - f(\alpha_i)\big),$$

de donde

$$|D(f(X), g(X))| \leq \prod_{i=1}^{n} \Big(\|f(X) - g(X)\| \max\{1, |\alpha_i|^n\}\Big).$$

Como $|\alpha_i| \leq \max\{1, \|f(X)\|\}$, se tiene que $\max\{1, |\alpha_i|^n\} \leq \max\{1, \|f(X)\|^n\}$, para todo $i \in \{1, 2, \ldots, n\}$, con lo que concluimos.

□

Definición 4.2.9 Sean D un cuerpo, dos valores absolutos $|\cdot|_1, |\cdot|_2$ sobre D se le llamarán *equivalentes* si dado $x \in D$ se cumple que $|x|_1 < 1$ si y sólo si $|x|_2 < 1$.

Ejemplo 4.2.10 Toda valuación induce valores absolutos no arquimedianos que son equivalentes. De hecho, más adelante veremos que este caso de equivalencia entre valores absolutos es estándar.

Proposición 4.2.11 *Sean $|\cdot|_1$ y $|\cdot|_2$ valores absolutos sobre un dominio D. Si $|\cdot|_1$ y $|\cdot|_2$ son equivalentes, entonces*

1. $|x|_1 > 1$ *si y sólo si* $|x|_2 > 1$.

2. $|x|_1 = 1$ *si y sólo si* $|x|_2 = 1$.

Demostración.- Por la simetría de los ítems, basta verificar que una condición implica la otra. Supongamos que $|x|_1 > 1$, entonces $x \neq 0$ y $|x^{-1}|_1 < 1$, por tanto $|x^{-1}|_2 < 1$, esto es $|x|_1 > 1$ implica $|x|_2 > 1$. Si se tiene $|x|_1 = 1$, tendremos que $|x|_2 = 1$ o $|x|_2 > 1$, luego por *1.* tendremos que $|x|_2 = 1$ es la única posibilidad. □

Proposición 4.2.12 *Sean* $|\cdot|_1$ *y* $|\cdot|_2$ *valores absolutos sobre un cuerpo* K. *Entonces,* $|\cdot|_1$ *y* $|\cdot|_2$ *son equivalentes si y sólo si existe* $\alpha > 0$ *tal que* $|x|_1 = |x|_2^\alpha$, *para todo* $x \in K$.

*Demostración.-*Supongamos que $|\cdot|_1$ y $|\cdot|_2$ son equivalentes. En el caso $|x|_1 = 1$ para todo $x \in K^\times$, tendremos que $|x|_2$=1, por tanto basta tomar $\alpha = 1$. Si existe $x \in K^\times$ tal que $|x|_1 \neq 1$ entonces tomamos $z = x$ cuando $|x|_1 < 1$ y en otro caso $z = x^{-1}$, para obtener $0 < |z|_1 < 1$. Sea $r \in \mathbb{R}$ tal que $|z|_2^\alpha = |z|_1$, este número es positivo porque $|z|_2 < 1$. Dado $y \in K^\times$ verificaremos que $|y|_1^\alpha = |y|_2$, lo que será cierto en el caso $|y|_1 = 0$ o 1, pues en el segundo caso el argumento anterior muestra que $|y|_2 = 1$. En el caso $|y|_1 > 1$, tomemos $r \in \mathbb{R}$ tal que $|y|_1^r = |z|_1$ y para cada $n \in \mathbb{N}$ tomamos $a_n, b_n \in \mathbb{Z}$ tales que $r - 1/n < a_n/b_n < r$, con lo que tendriamos

$$|y|_1^{a_n/b_n} < |z|_1, \quad \text{para todo } n \in \mathbb{N}.$$

Esto equivale a $|y^{a_n}/z^{b_n}|_1 < 1$, por tanto $|y^{a_n}/z^{b_n}|_2 < 1$ y luego $|y|_2^{a_n/b_n} < |z|_2$, para cada $n \in \mathbb{N}$. Así concluimos, cuando $n \to +\infty$, que $|y|_2^r \leq |z|_2$. Por un razonamiento análogo, si para cada $n \in \mathbb{N}$ tomamos $c_n, d_n \in \mathbb{Z}$ tales que $r < c_n/d_n < r + 1/n$, concluiremos que $|y|_2^r \geq |z|_2$. Por lo tanto $|y|_2^r = |z|_2$, luego

$$|y|_2^\alpha = |z|_2^{\alpha/r} = |z|_1^{1/r} = |y|_1.$$

En el caso restante $0 < |y|_1 < 1$, basta observar que $|1/y|_1 < 1$ y concluir que $|1/y|_1^\alpha = |1/y|_2$ (por el caso ya demostrado). La afirmación recíproca es inmediata, lo termina la demostración. □

4.3. Estructura topológica inducida por un valor absoluto

Todo valor absoluto $|\cdot|$ induce una métrica $d : D \times D \to \mathbb{R}$ dada por

$$d(x, y) = |x - y|, \qquad x, y \in D.$$

En el caso no arquimediano tendremos que

$$d(x,z) \leq \max\{d(x,y), d(y,z)\}, \quad \text{para todo } x,y,z \in K. \tag{4.1}$$

A una métrica que cumple la propiedad (4.1) se le denomina *ultramétrica* y al espacio correspondiente, espacio ultramétrico.

Lema 4.3.1 *Tres puntos cualesquiera $a, b, c \in M$ sobre un espacio ultramétrico M determinan un triángulo isósceles, esto es*

$$d(x,y) = d(z,x) \quad \text{o} \quad d(y,z) = d(z,x) \quad \text{o} \quad d(x,y) = d(y,z);$$

o equivalentemente, si $d(x,y) > d(x,z)$, entonces $d(y,z) = d(x,y)$.

Demostración.- Si $d(x,y) < d(y,z)$, entonces $d(x,z) \leq \max\{d(x,y), d(y,z)\} = d(y,z)$, y como $d(y,z) \leq \max\{d(y,x), d(x,z)\}$ es imposible $d(x,z) < d(y,z)$; por tanto, si una de las distancias es distinta a otra, las restantes son iguales. □

Corolario 4.3.2 *Sea D un dominio y $a_1, a_2, \ldots, a_n \in D$. Se cumple:*

- *si $|\cdot| : D \to \mathbb{R}$ es un valor absoluto no arquimediano y $|a_1|$ es mayor que $|a_2|, |a_3|, \ldots, |a_n|$, entonces $|a_1 + \cdots + a_n| = |a_1|$;*
- *si v es una valuación sobre D y $v(a_1)$ es menor que $v(a_2), \ldots, v(a_n)$, entonces $v(a_1 + \cdots + a_n) = v(a_1)$.*

Demostración.- Observemos que (D,d) con $d(x,y) = |x-y|$ es un espacio ultramétrico y $|x| = d(x,0)$ para todo $x \in D$. □

Proposición 4.3.3 *Sea (M,d) un espacio ultramétrico, si tomamos en cuenta la topología inducida por su ultramétrica d, se cumple:*

1. *toda bola abierta es un conjunto cerrado y abierto. Toda bola cerrada de radio positivo es un conjunto cerrado y abierto;*
2. *los únicos conjuntos conexos son los unitarios, esto es, M es totalmente disconexo.*

Demostración.- Empecemos por mostrar *1.*, tomando $x \in M$ y $r \geq 0$ veremos que la bola abierta $B(x,r)$ es un cerrado; pues siempre es un conjunto abierto en la topología inducida por la métrica. Si $r = 0$ entonces es el conjunto vacío, por tanto el conjunto es abierto y cerrado. Si $r > 0$, dado $y \notin B(x,r)$ tomamos $s = r/2$, y entonces para todo $z \in B(y,s)$ se

cumple que $d(z,x) = \max\{d(x,y), d(y,z)\} = d(x,y) > r$ (por el lema previo), con lo cual concluimos que $M \setminus B(x,r)$ es abierto; de manera análoga se prueba el otro caso enunciado. Ahora es fácil demostrar *2*, pues dado $X \subset M$ con al menos dos elementos, x e y, tomamos $r = d(x,y)/2$, entonces $X \cap B(x,r)$ y $X \setminus B(x,r)$ es una escisión no trivial de X. □

Corolario 4.3.4 *Sea $|\cdot|$ un valor absoluto sobre un dominio D y v una valuación inducida por $|\cdot|$. Entonces el anillo e ideal de valuación son conjuntos cerrados.*

La siguiente proposición dice que las operaciones de suma, producto e inversión son continuas en la métrica inducida por un valor absoluto, esto es inducen un *anillo topológico*. La prueba de esta proposición es idéntica a la realizada en $\mathbb{R}$, por lo que la obviaremos.

Proposición 4.3.5 *Sean $|\cdot|$ un valor absoluto sobre un dominio D con valor absoluto $|\cdot|$ y $(a_n), (b_n) \subset D$.*

1. *Si $\lim_{n\to\infty} a_n = a$ entonces $\lim_{n\to\infty} |a_n| = |a|$.*
2. *Si $\lim_n a_n = 0$ equivale a $\lim_{n\to\infty} |a_n| = 0$.*
3. *Si $\lim_{n\to\infty} a_n = a$ y $\lim_{n\to\infty} b_n = b$, entonces $\lim_{n\to\infty} a_n + b_n = a + b$ y $\lim_{n\to\infty} a_n \cdot b_n = a \cdot b$.*
4. *Si $(a_n)_n \in D^\times$ y $\lim_{n\to\infty} a_n = a \in D^\times$ entonces $\lim a_n^{-1} = a^{-1}$.*

El tercer ítem, de este teorema nos dice que un dominio con un valor absoluto es anillo topológico; y *4.*, que un cuerpo con un valor absoluto es un cuerpo topológico.

El siguiente lema establece una de las consecuencias más importantes de que el valor absoluto sobre el dominio sea no arquimediano. El lema subsiguiente ilustra otra gran diferencia entre valores absolutos arquimedianos y los no arquimedianos.

Lema 4.3.6 *Sean $(D, |\cdot|)$ no arquimediano y $(a_n) \subset D$, entonces (a_n) es de Cauchy si y sólo si $\lim_{n\to\infty} |a_{n+1} - a_n| = 0$.*

Demostración.- Es claro que $\lim_{n\to\infty} |a_{n+1} - a_n| = 0$ es una condición necesaria para que (a_n) sea de Cauchy, así que probemos la suficiencia. Dado $\epsilon > 0$, existe $N_0 \in \mathbb{N}$ tal que $n > N_0$ implica que $|a_{n+1} - a_n| < \epsilon$. Así concluimos, por las observaciones 4.2.3, que si $m > n > N_0$ entonces

$$|a_m - a_n| \leq \max\{|a_m - a_{m-1}|, |a_{m-1} - a_{m-2}|, \ldots, |a_{n+1} - a_n|\} < \epsilon,$$

de lo cual se deduce que (a_n) es de Cauchy.

Lema 4.3.7 *Sean $(D, |\cdot|)$ no arquimediano y $(a_n) \subset D$ una secuencia de Cauchy que no converge a 0, entonces $(|a_n|) \subset \mathbb{R}$ es una secuencia estacionaria, es decir, existe $N_0 \in \mathbb{N}$ tal que $|a_m| = |a_{N_0}|$ para todo $m > N_0$.*

Demostración.- Veamos que existe $d > 0$ tal que $|a_n| > d$, para todo n suficientemente grande. Puesto que (a_n) no converge a 0, existirá $c > 0$ y una subsucesión $(a_{n_j}) \subset (a_n)$ tal que $|a_{n_j}| > c$ para todo $j \in \mathbb{N}$. Como (a_n) es de Cauchy, también que $N_0 \in \mathbb{N}$ tal que $n, m > N_0$ implica $|a_m - a_n| < c/2$. Tomando $n_j > N_0$ y cualquier $n > N_0$ tenemos que

$$c/2 > |a_{n_j} - a_n| \geq |a_{n_j}| - |a_n| \geq c - |a_n|,$$

así que $|a_n| > c/2$, para todo $n > N_0$; con lo cual lo afirmado será cierto para $d = c/2$.

Ahora, elijamos $N_1 \in \mathbb{N}$ tal que $|a_m - a_n| < d/2$ para todo $n > N_1$, tomando $N_2 = \text{máx}\{N_0, N_1\} + 1$ tendremos que para $m > N_2$ se cumple $|a_m| = |a_{N_2} - (a_m - a_{N_2})| = \text{máx}\{|a_{N_2}|, |a_m - a_{N_2}|\} = |a_{N_2}|$. □

Definición 4.3.8 Diremos que un dominio D con valor absoluto es *completo* si toda sucesión de Cauchy es convergente en K, esto es, D es un espacio métrico completo bajo la métrica inducida por el valor absoluto.

En lo que sigue de la sección sólo analizaremos cuerpos con un valor absoluto. Dado un valor absoluto $|\cdot|$ sobre un cuerpo K, tomaremos $\mathfrak{S}(K) = \{(a_n)_{n\in\mathbb{N}} \subset X\}$ y las operaciones de suma $+ : \mathfrak{S}(K) \times \mathfrak{S}(K)$ y producto $\cdot : \mathfrak{S}(K) \times \mathfrak{S}(K)$ entre secuencias definidas por

$$(a_n) + (b_n) = (a_n + b_n) \qquad (a_n) \cdot (b_n) = (a_n b_n).$$

Es fácil mostrar que con estas operaciones $\mathfrak{S}(C)$ es un anillo conmutativo, mas no es dominio. También consideraremos los subconjuntos

$$\mathfrak{C}(K) = \{(a_n) \subset K \ : \ (a_n) \quad \text{es una secuencia de Cauchy}\}$$

y

$$\mathfrak{N}(K) = \{(a_n) \subset K \ : \lim_n a_n = 0 \ \}.$$

Ahora veremos cómo el conjunto de las secuencias de Cauchy adquiere una estructura algebraica inducida por el valor absoluto tomado.

Proposición 4.3.9 *Sea K cuerpo con $|\cdot|$ como valor absoluto, se cumple:*

1. *el conjunto $\mathfrak{C}(K)$ es un subanillo de $\mathfrak{S}(K)$;*

2. *el conjunto* $\mathfrak{N}(K)$ *es un ideal maximal de* $\mathfrak{C}(K)$.

Demostración.-

Denotemos por $\mathfrak{C}$ y $\mathfrak{N}$ a $\mathfrak{C}(K)$ y $\mathfrak{N}(K)$, respectivamente. La demostración de estos ítems es rutinaria, pues es ejercicios de álgebra y análisis, salvo el hecho que $\mathfrak{N}$, como ideal de $\mathfrak{C}$, es maximal. Ello lo demostraremos tomando $x \in \mathfrak{C} \setminus \mathfrak{N}$ y probando que $\mathfrak{J}$, el ideal generado por x y $\mathfrak{N}$ es $\mathfrak{C}$. Por el lema anterior, ya que $(a_n) \in \mathfrak{C} \setminus \mathfrak{N}$, existirá $N_0 \in \mathbb{N}$ y $d > 0$ tales que $|a_n| = d$, para todo $n \geq N_0$. Tomemos $d = c/2$ e $y = (b_n) \in \mathfrak{S}$ definido por

$$b_n = \begin{cases} 0, & \text{si} \quad n \leq N_0 \\ a_n^{-1}, & \text{si} \quad n > N_0 \end{cases},$$

que afirmamos pertenece a $\mathfrak{C}$. En efecto, dado $\epsilon > 0$, existe $N_1 \in \mathbb{N}$ tal que $|a_m - a_n| < \epsilon d^2$ cuando $m, n > N_1$; por tanto, si $n, m > \text{máx}\{N_0, N_1\}$ entonces

$$|b_n - b_m| = \frac{|a_n - a_m|}{|a_m||a_n|} < \epsilon d^2 d^{-2} = \epsilon.$$

Si tomamos $u_n = 1$ para todo $n \in \mathbb{N}$, entonces $u = (u_n)$ es la unidad en $\mathfrak{C}$, más aun $u - xy \in \mathfrak{N}(K)$; por lo tanto $u \in \mathfrak{J}$ y hemos demostrado 2. □

Ejemplo 4.3.10 Un ejemplo clave de cuerpo completo es $\mathbb{R}$ con el valor absoluto tradicional $|\cdot|$ dado por $|x| = \text{máx}\{x, -x\}$; pues es el *único cuerpo ordenado completo.* Un caso sencillo de cuerpo no completo es $(K(X), |\cdot|_X)$ (puede verlo en los ejemplos 4.2.7). En efecto, la sucesión $(s_n)_{n\in\mathbb{N}} \subset K[X]$ formada por $s_n = \sum_{j=0}^{n} X^j$ cumple $|s_{n+1} - s_n| = e^{-n}$ para todo $n \in \mathbb{N}$, por tanto es de Cauchy (ver lema 4.3.6), y sin embargo no tiene límite en $K[X]$. De hecho, si $\lim_n s_n = p(X) = a_0 + a_1 + \cdots + a_r X^r \in K[X]$, entonces existe $n_0 \in \mathbb{N}$ tal que $n \geq n_0$ implica $|s_n - p(X)|_x < e^{-r-2}$. Tomando $n = \text{máx}\{n_0, r+1\}$, tendremos que

$$s_n - p(X) = \sum_{j=r}^{n} X^j + (s_t - p(X)) = s(X) + q(X),$$

donde $s(X)$ y $q(X)$ son el primer y segundo sumando de la segunda expresión de arriba, además $|s_n - p(X)|_X < e^{-r-2}$. Si $q(X) = 0$, entonces $|s_n - p(X)|_X = |s(X)|_X = e^{-r-1}$; en otro caso $|q(X)|_X \leq e^r$, y por tanto $|s_n - p(X)| \geq e^{-r-1}$, lo que contradice la elección de n.

Definición 4.3.11 Sean L y K cuerpos y $|\cdot|, \|\cdot\|$ valores absolutos sobre K y L, respectivamente, diremos que L es una *compleción de* K si $(L, \|\cdot\|)$ es completo y existe un monomorfismo $\sigma : K \to L$ que cumple

1. El conjunto $\sigma(K)$ es denso en L.

2. Para todo $x \in K$ tenemos que $\|\sigma(x)\| = |x|$, esto es $\|\cdot\|$ extiende a $|\cdot|$ en L.

La definición anterior nos dice que L es una compleción de K si L es un cuerpo completo, una extensión de K, que extiende el valor absoluto y que no es más grande que K (K es denso en L). El ejemplo más conocido es $\mathbb{R}$, que es una compleción de $\mathbb{Q}$, más aun se conoce la unicidad de $\mathbb{R}$ como cuerpo arquimediano ordenado, salvo isomorfismos que conserven el orden. Veamos que esa unicidad es consecuencia del siguiente resultado.

Teorema 4.3.12 *Todo cuerpo tiene una compleción, y esta es única salvo $K-$isomorfismos isometricos.*

Demostración.- Tomemos un valor absoluto $|\cdot|$ en un cuerpo K y construyamos un valor absoluto sobre el cuerpo $L = \mathfrak{C}(K)/\mathfrak{N}(K)$.

Afirmación 1: *Si $(a_n) \in \mathfrak{C}(K)$, existe $\lim_n |a_n|$, más aun si $(a_n) \equiv (b_n)$ mód $\mathfrak{N}(K)$, entonces $\lim_n |a_n| = \lim_n |b_n|$.*

Dados $m, n \in \mathbb{N}$ tenemos que se cumple que $\big||a_m| - |a_n|\big| \leq |a_m - a_n|$; de modo que si $(a_n) \in \mathfrak{C}(K)$, concluimos facilmente que $(|a_n|) \in \mathfrak{C}(\mathbb{R})$, y por tanto $(|a_n|)$ es convergente en $\mathbb{R}$. Si $(a_n) - (b_n) \in \mathfrak{N}(K)$, entonces $(a_n - b_n) \in \mathfrak{N}(K)$, esto es $\lim_n (a_n - b_n) = 0$, lo que equivale a que $\lim_n |b_n - a_n| = 0$, pero esto implica que $\lim_n ||b_n| - |a_n|| = 0$. Por lo tanto $\lim_n |b_n|$ existe, pues

$$\lim_n |b_n| = \lim_n [|b_n| + (|a_n| - |b_n|)] = \lim_n |a_n|.$$

Ahora podemos construir nuestro candidato a valor absoluto sobre L.

Afirmación 2: *La función $\|\cdot\| \to \mathbb{R}$, definida por $\|(a_n) + \mathfrak{N}(K)\| = \lim_n |a_n|$ es un valor absoluto sobre K.*

La primera afirmación nos asegura que existe el límite y que este no depende del representante. Mostremos que $\|\cdot\|$ satisface las propiedades de un valor absoluto; la no negatividad es verificada por definición. Tomemos $x = (a_n) + \mathfrak{N}(K)$ tal que $\|x\| = 0$; en este caso tendremos que $\lim_n |a_n| = 0$, lo que equivale a que $\lim_n (a_n) = 0$, esto es $(a_n) \in \mathfrak{N}(K)$ y $x = \mathfrak{N}(K)$, como el recíproco es inmediato tenemos que $\|\cdot\|$ satisface la segunda propiedad de la definición 4.2.1. Tomando $x = (a_n) + \mathfrak{N}(K)$, $y = (b_n) + \mathfrak{N}(K) \in L$ tendremos que

$$\|xy\| = \|(a_n)(b_n) + \mathfrak{N}(K)\| = \lim_n |a_n b_n| = \lim_n |a_n| \lim_n |b_n| = \|x\|\|y\|,$$

y por lo tanto $\|\cdot\|$ cumple la tercera propiedad. Así también se tiene que

$$\|x + y\| = \|(a_n) + (b_n) + \mathfrak{N}(K)\| = \lim_n |a_n + b_n| \leq \lim_n |a_n| + \lim_n |b_n| = \|x\| + \|y\|,$$

luego la cuarta propiedad de la definición 4.2.1. Y en el caso que $|\cdot|$ sea no arquimediano tenemos que

$$\|x+y\| = \|(a_n+b_n)+\mathfrak{N}(K)\| = \lim_n |a_n+b_n| \leq \lim_n \max\{|a_n|,|b_n|\} = \max\{\|x\|,\|y\|\}.$$

En lo que sigue de esta demostración denotaremos la sucesión de términos constantes iguales a $a \in K$ por $(a)_{n\in\mathbb{N}}$, es claro que este tipo de sucesión es de Cauchy, por tanto tenemos una función $\sigma : K \to L$ definida por $\sigma(a) = (a)_{n\in\mathbb{N}} + \mathfrak{N}(K)$, que es un monomorfismo. En efecto, es fácil ver que es un homomorfismo, y si $\sigma(a) = \mathfrak{N}(K)$ entonces $\lim_n a = 0$, lo que significa $a = 0$, esto muestra que es inyectiva.

Afirmación 3: La función σ *cumple las propiedades enunciadas en la definición 4.3.11*

Dado $x \in L$, existe $(a_n) \in \mathfrak{C}(K)$ tal que $x = (a_n) + \mathfrak{N}(K)$. Si tomamos $\epsilon > 0$ entonces existe $n_0 \in \mathbb{N}$ tal que $|a_m - a_n| < \epsilon/2$ para todo $n, m \geq n_0$. Por otra parte, se tiene que

$$\big||a_m - a_{n_0}| - |a_n - a_{n_0}|\big| \leq |a_m - a_n|$$

para todo $m, n \in \mathbb{N}$, por lo cual la sucesión $(|a_m - a_{n_0}|)_{m\in\mathbb{N}} \in \mathfrak{C}(\mathbb{R})$ y será convergente. Por tanto, tenemos que $b = a_{n_0}$ cumple que

$$\|x - \sigma(b)\| = \big\|(a_m - b)_{m\in\mathbb{N}} + \mathfrak{N}(K)\big\| = \lim_m |a_m - a_{n_0}| \leq \epsilon/2 < \epsilon,$$

muestra que $\sigma(K)$ es denso en L. También se tiene que para cada $a \in K$ se cumple $\big\|\sigma(a)\big\| = \big\|(a)_{n\in\mathbb{N}} + \mathfrak{N}(K)\big\| = \lim_n |a| = |a|$, luego σ cumple las condiciones de la definición 4.3.11.

Ahora, demostremos que $(L, \|\cdot\|)$ es completo, para esto consideremos $(x_m)_{m\in\mathbb{N}} \in \mathfrak{C}(L)$. Para cada $m \in \mathbb{N}$ escribamos $x_m = (a_{mn})_{n\in\mathbb{N}} + \mathfrak{N}(K)$ y, tomando en cuenta la densidad de $\sigma(b)$ seleccionemos $b_m \in K$ tal que $\|\sigma(b_m) - x_m\| < 1/m$.

Afirmación 4: $(b_m) \in \mathfrak{C}(K)$ *y* (x_m) *converge a* $(b_m) + \mathfrak{N}(K)$.

Dado $\epsilon > 0$, existe $m_0 \in \mathbb{N}$ tal que $\|x_m - x_n\| < \epsilon/3$ para todo $m, n \geq m_0$, por tanto

$$\lim_t \|a_{mt} - a_{nt}\| < \epsilon/3.$$

Por otra parte, dado $t \in \mathbb{N}$ tenemos que

$$|b_m - b_n| \leq |b_m - a_{mt}| + |a_{mt} - a_{nt}| + |a_{nt} - b_n|,$$

y tomando límite cuando $t \to \infty$ tendremos

$$|b_m - b_n| \leq \lim_t |b_m - a_{mt}| + \lim_t |a_{mt} - a_{nt}| + \lim_t |a_{nt} - b_n| = \|\sigma(b_m) - x_m\| + \|x_m - x_n\| + \|x_n - \sigma(b_n)\|.$$

Por lo tanto $|b_m - b_n| < \epsilon$ siempre que $m, n \geq \max\{m_0, 3/\epsilon\}$; esto demuestra que (b_m) es de Cauchy.

Ahora tomemos $x = (b_m) + \mathfrak{N}(K) \in L$ y verifiquemos que $\lim_m x_m = x$. Para cualquier $m, t, s \in \mathbb{N}$ tendremos que

$$|a_{mt} - b_t| \leq |a_{mt} - a_{ms}| + |a_{ms} - a_{ts}| + |a_{ts} - b_t| \tag{4.2}$$

Dado $\epsilon > 0$, sea $M \in \mathbb{N}$ tal que $\lim_s |a_{ms} - a_{ts}| < \epsilon/3$ cuando $m, t \geq M$. Fijemos $m \geq M$, entonces existe $M_1 = M_1(\epsilon, m) \in \mathbb{N}$ tal que

$$t, s \geq M_1 \quad \text{implique} \quad |a_{mt} - a_{ms}| < \epsilon/3.$$

Ahora, fijando $t \geq M' = \max\{M_1, M, 3/\epsilon\}$ podemos tomar $M_2 = M_2(t) \in \mathbb{N}$ tal que

$$|a_{ts} - b_t| < 1/t \leq \epsilon/3, \quad \text{siempre que} \quad s \geq M_2;$$

así también existe $M_3 = M_3(t, m) \in \mathbb{N}$ tal que

$$|a_{ms} - a_{ts}| < \epsilon/3 \quad \text{cuando} \quad s \geq M_3.$$

Por tanto, si $s \geq \max\{M_1, M_2, M_3\}$ tendremos en 4.2 que

$$|a_{mt} - b_t| < \epsilon + \epsilon + \epsilon = \epsilon \quad \text{para todo } t \geq M';$$

luego para cada $m \geq M_0$ hacemos $t \to \infty$ para obtener que $\lim_t |a_{mt} - b_t| \leq \epsilon/3$, esto es $\|x_m - x\| \leq \epsilon$ para todo $m \leq M_0$, con esto se concluye lo afirmado.

Finalmente, supongamos que $(M, \|\cdot\|_0)$ es otra compleción de K y $\tau : K \to M$ el monomorfismo respectivo (que cumple la definición 4.3.11). Dado $(a_n) \in \mathfrak{C}(K)$, tendremos que $(\tau(a_n)) \in \mathfrak{C}(M)$ (pues τ es isométrico), por lo tanto $(\tau(a_n))$ es convergente en M. Más aun, si $(a_n) \equiv (b_n)$ mód $\mathfrak{N}(K)$ tendremos $(b_n) - (a_n) \in \mathfrak{N}(K)$, por tanto $\lim |b_n - a_n| = 0$ y $\lim_n \|\lim_n \tau(b_n - a_n)\|_0 = 0$, con lo que tendremos que

$$0 = \lim_n \tau(b_n - a_n) = \lim_n \tau(b_n) - \lim_n \tau(a_n).$$

Por lo tanto, el límite obtenido es el mismo para todo representante de una clase en L. Así podemos definir $\Psi : L \to M$ por $\Psi((a_n) + \mathfrak{N}(K)) = \lim_n \tau(a_n)$.

Afirmación 5 Ψ *es un isomorfismo isometrico.*

Es fácil demostrar que Ψ es un homomorfismo, así que procedamos a demostrar que es biyectivo. Si $x = (a_n) + \mathfrak{N}(K) \in L$ cumple que $\Psi(x) = 0$ entonces $\lim_n \tau(a_n) = 0$, de donde $\lim_n |a_n| = \lim_n \|\tau(a_n)\|_0 = 0$, luego $(a_n) \in \mathfrak{N}(K)$ y $x = \mathfrak{N}(K)$, por tanto Ψ es inyectivo.

Dado $y \in M$, puesto que $\tau(K)$ es denso en M, podemos encontrar $(a_n) \subset K$ tal que $\|\tau(a_n) - y\| < 1/n$ para todo $n \in \mathbb{N}$. Por tanto $\tau(a_n)$ converge a y, en particular $(\tau(a_n)) \in$

$\mathfrak{C}(M)$, entonces es inmediato que $(a_n) \in \mathfrak{C}(K)$; tomando $x = (a_n) + \mathfrak{N}(K)$ tendremos que $\Psi(x) = y$, esto nos dice que Ψ es sobreyectivo. Finalmente, las igualdades

$$\|(a_n) + \mathfrak{N}(K)\| = \lim_n |a_n| = \lim_n \|\tau(a_n)\|_0 = \|\lim_n \tau(a_n)\|_0 = \|\Psi(x)\|,$$

muestran que Ψ es una isometría. □

Proposición 4.3.13 *Sean $(M, \|\cdot\|)$ una compleción de $(K, |\cdot|)$ no arquimediano y un monomorfismo $\sigma : K \to M$ que satisface la definición 4.3.11. Entonces*

1. $|K| = \|M\|$.

2. *Sean $c > 1$ y $v : K \to \mathbb{R}$ la valuación inducida por $|\cdot|$ con parámetro c, entonces la valuación inducida por $\|\cdot\|$ con parámetro cumple que $v(K) = w(M)$ y $v(x) = w\big(\sigma(x)\big)$, para todo $x \in K$.*

Demostración.- Sea $\sigma : K \to M$ un monomorfismo tal que $|x| = \|\sigma(x)\|$, para todo $x \in K$.

1. Se tiene que $|K| = \|\sigma K\| \subset \|M\|$. Recíprocamente, dado $x \in M$ no nulo, por la densidad de $\sigma(K)$ en M, existe una sucesión $(x_n)_{n\in\mathbb{N}} \in K$ tal que $\lim_{n\to\infty} \sigma(x_n) = x$. Entonces $\big(\sigma(x_n)\big)_{n\in\mathbb{N}}$ es una sucesión de Cauchy en M que no converge a 0; por lo tanto, en virtud del lema 4.3.7, existe $n_0 \in \mathbb{N}$ tal que $\big\|\sigma(x_n)\big\| = \big\|\sigma(x_{n_0})\big\|$, para todo $n \geq n_0$. Luego

$$\|x\| = \big\|\lim_{n\to\infty} \sigma(x_n)\big\| = \big\|\sigma(x_{n_0})\big\| = |x_{n_0}| \in |K|.$$

2. Dado $c > 0$, sean $v : K \to \mathbb{R} \cup \{+\infty\}$ y $w : L \to \mathbb{R} \cup \{+\infty\}$ las valuaciones inducidas por $|\cdot|$ y $\|\cdot\|$ (con parámetro c). Dado $x \in K \setminus \{0\}$ se tiene

$$v(x) = -\log_c(|x|) = -\log_c\Big(\big\|\sigma(x)\big\|\Big) = w\big(\sigma(x)\big);$$

por lo tanto w extiende Además

$$w(L) = -\log_c(\{\|x\| \ : \ x \in L\}) = -\log_c(\{|x| \ ; \ x \in K\}) = v(K).$$

□

Proposición 4.3.14 *Sea $\big(L_2, |\cdot|_2\big)$ una compleción de un cuerpo no arquimediano $\big(L_1, |\cdot|_1\big)$. Dado $c > 1$, sean $v_j : L_j \to \mathbb{R} \cup \{\infty\}$ las valuaciones inducidas por $|\cdot|_j$, respectivamente. Entonces los cuerpos residuales de v_1 y v_2 son isomorfismos.*

Demostración.- Denotemos por $\mathcal{O}_j, \mathfrak{p}_j$ y κ_j al anillo de valuación, ideal de valuación y cuerpo residual de v_j, respectivamente. Sean $\sigma : L_1 \to L_2$ un monomorfismo que satisface la definición 4.3.11, $L = \sigma(L_1)$ y v la valuación v_2 restringida a L. Por la proposición anterior, tenemos que $v_1(x) = v_2(\sigma(x))$, para todo L_1. Entonces, el anillo e ideal de valuación de v son $\sigma(\mathcal{O}_1)$ y $\sigma(\mathfrak{p}_1)$, respectivamente. Luego, σ induce un isomorfismo entre κ_1 y el cuerpo residual κ de v; por lo tanto, resta demostrar que el κ es isomorfo a κ_2. En virtud del lema 4.1.11, la función $\phi : \kappa \to \kappa_2$, definida por $\phi\big(\sigma(a) + \sigma(\mathfrak{p}_1)\big) = \sigma(a) + \mathfrak{p}_2$ es un monomorfismo; verifiquemos que es sobreyectiva. Dado $x \in \mathcal{O}_2$, por la densidad de $\sigma(L_1)$ en L_2, existe $a \in L_1$ tal que $|x - \sigma(a)|_2 < 1$. Entonces,

$$|a|_1 = |\sigma(a)|_2 \leq \text{máx}\big\{|x - \sigma(a)|_2, |-x|_2\big\} \leq 1,$$

y $a \in \mathcal{O}_1$. También deducimos que $v_2\big(x - \sigma(a)\big) > 0$ y $x - \sigma(a) \in \mathfrak{p}_2$, por lo tanto $x + \mathfrak{p}_2 = \sigma(a) + \mathfrak{p}_2 = \phi\big(\sigma(a) + \sigma(\mathfrak{p}_1)\big)$. □

4.4. Series en dominios completos no arquimedianos

Durante esta sección, fijemos un dominio completo D respecto a un valor absoluto no arquimediano $|\cdot|$. Empecemos por enunciar el siguiente lema, que es una reformulación del lema 4.3.6.

Lema 4.4.1 *Sea $(x_k)_{k\in\mathbb{N}} \subset D$. Son equivalentes:*

1. $\lim_{k\to\infty}(x_{k+1} - x_k) = 0$;
2. *la sucesión (x_k) es de Cauchy;*
3. *la sucesión (x_k) es convergente.*

Definición 4.4.2 Sea $(x_k)_{k\in\mathbb{N}} \subset D$ definimos la *serie* de sumandos en (x_k), denotada por $\sum_k x_k$, a la sucesión de sumas o sumandos parciales $(\sum_{k=1}^n x_k)_n \in \mathbb{N}$. Con estas notaciones, la serie $\sum_k x_k$ es convergente si y sólo si existe $\lim_n \sum_{k=1}^n x_k$; en el caso de existir este límite lo denotaremos por $\sum_{k=1}^\infty x_k$.

Lema 4.4.3 *Sea $(x_k)_{k\in\mathbb{N}} \subset D$. Son equivalentes:*

1. $\lim_k x_k = 0$;
2. $\lim_k |x_k| = 0$;

3. la serie $\sum_k x_k$ es convergente.

Demostración.- Sea $y_n = \sum_{k=1}^{n} x_k$, para cada $n \in \mathbb{N}$. Entonces existe $\sum_{k=1}^{\infty} x_k$ que es $\lim_n y_n$ si y sólo si $\lim_n |y_{n+1} - y_n| = 0$, que simplemente es $\lim |x_k| = 0$; y como ya hemos visto, esto equivale al primer ítem. □

Corolario 4.4.4 *Sea $(x_k)_{k\in\mathbb{N}} \subset X$. Si $\sum_k |x_k|$ es convergente en $\mathbb{R}$, entonces $\sum_k x_k$ converge en D.*

Demostración.- Puesto que la existencia $\sum_{k=1}^{\infty} |x_k|$ en $\mathbb{R}$ implica que $\lim_k |x_k| = 0$, tendremos que $\lim_{k\to\infty} x_k = 0$ y que $\sum_k x_k$ es convergente. □

Observaciones 4.4.5

- Durante la sección, para cada $m \in \mathbb{N}$, denotaremos $I_m = \{1, 2, \ldots, m\} \subset \mathbb{N}$.
- El último lema muestra otra diferencia sustancial de los valores absolutos no arquimedianos con los arquimedianos, pues en en $\mathbb{R}$ existen series como la armónica que satisfacen el primer ítem del lema anterior y no el segundo.
- El corolario nos muestra un nexo claro entre el concepto entre cuerpos como $\mathbb{R}$ o $\mathbb{C}$ y los no arquimedianos, el hecho que la convergencia de la serie conformada por el valor absoluto de cada sumando implica la convergencia de la serie misma.
- El recíproco del enunciado del corolario anterior no es cierto; un ejemplo de esto lo veremos en el capítulo 5 y sección 6.

Lema 4.4.6 *Sea $(x_k)_{k\in\mathbb{N}} \subset D$ tal que $\sum_k x_k$ es convergente. Si $\sigma : \mathbb{N} \to \mathbb{N}$ es una biyección, entonces la serie $\sum_k x_{\sigma(k)}$ es convergente, más aun $\sum_{k=1}^{\infty} x_{\sigma(k)} = \sum_{k=1}^{\infty} x_k$.*

Demostración.- Verifiquemos que $\sum_k x_{\sigma(k)}$ es convergente. Fijemos $\epsilon > 0$. En virtud del lema anterior existe $k_0 \in \mathbb{N}$ tal que $k \geq k_0$ implica $|x_k| \leq \epsilon$; luego, tomando $m_0 = \max\{\sigma^{-1}(1), \ldots, \sigma^{-1}(k_0)\}$ tendremos que para todo $k \geq m_0 + 1$ se cumple que $\sigma_k > k_0$, por lo cual $|x_{\sigma(k)}| < \epsilon$; como $\epsilon > 0$ fue arbitrario, concluimos la convergencia de $\sum_k x_{\sigma(k)}$. Más aun, para todo $n \geq k_0$ y $m \geq m_0 + 1$ ocurre que

$$\begin{aligned}
\Big|\sum_{k=1}^{n} x_k - \sum_{k=1}^{m} x_{\sigma(k)}\Big| &= \Big|\sum_{k=k_0+1}^{n} x_k - \sum_{k\in I_m \setminus \sigma^{-1}(I_{k_0})} x_{\sigma(k)}\Big| \\
&\leq \max\Big\{\max_{k_0+1\leq k\leq n} |x_k|, \max_{j\in\sigma(I_{m_0})\setminus I_{k_0}} |x_j|\Big\} \\
&< \epsilon,
\end{aligned}$$

puesto que $I_{k_0} \subset \sigma(I_{m_0}) \subset \sigma(I_m)$. Luego,

$$\left|\sum_{k=1}^{\infty} x_k - \sum_{k=1}^{m} x_{\sigma(k)}\right| = \lim_{n\to\infty}\left|\sum_{k=1}^{n} x_k - \sum_{k=1}^{m} x_{\sigma(k)}\right| < \epsilon, \qquad \text{para todo } m \geq m_0;$$

puesto que $\epsilon > 0$ era arbitrario, esta ultima desigualdad demuestra que $\sum_{k=1}^{\infty} x_{\sigma(k)}$ converge a $\sum_{k=1}^{\infty} x_k$. □

Observación 4.4.7 Este lema nos muestra que las series convergentes no son condicionalmente convergentes, a pesar que no son necesariamente absolutamente convergentes en el sentido de $\mathbb{R}$.

Motivados por este último lema presentamos a continuación un estudio acerca de como podemos extender esta noción de "suma infinita "para series indexadas por un conjunto un poco más general que $\mathbb{N}$, esto será de vital importancia en el desarrollo de esta monografía.

Definición 4.4.8 Dado un conjunto infinito numerable $\mathcal{N}$, toda función $X : \mathcal{N} \to D$ será denominada *sucesión indexada por* $\mathcal{N}$. Denotaremos a cada evaluación $x(u)$ por x_u; y a la sucesión será por $(x_u)_{u\in\mathcal{N}} \subset D$.

Proposición 4.4.9 *Sea $\mathcal{N}$ infinito numerable y $(x_u)_{u\in\mathcal{N}} \subset D$. Si existe una biyección $\varphi : \mathbb{N} \to \mathcal{N}$ tal que la serie $\sum_k x_{\varphi(k)}$ es convergente entonces, para cada biyección $\psi : \mathbb{N} \to \mathcal{N}$, la serie $\sum_k x_{\psi(k)}$ es convergente y su límite coindice con $\sum_{k=1}^{\infty} x_{\varphi(k)}$.*

Demostración.-Es sólo una reformulación del lema 4.4.6. □

Definición 4.4.10 Dado $\mathcal{N}$ infinito numerable y una sucesión $x : \mathcal{N} \to D$, siempre que exista una biyección $\varphi : \mathbb{N} \to \mathcal{N}$ tal que $\sum_k x_{\varphi(k)}$ sea convergente definimos *la suma de* (x_u) como el límite $\sum_{k=1}^{\infty} x_{\varphi(k)}$, que denotaremos por $\sum_{u\in\mathcal{N}} x_u$.

La proposición anterior asegura la buena definición de la suma de este tipo más general de sucesión. El siguiente lema nos brinda herramientas para el cálculo de este nuevo concepto que nos independiza de la elección de una biyección $\varphi : \mathbb{N} \to \mathcal{N}$.

Proposición 4.4.11 *Sean $\mathcal{N}$ un conjunto infinito numerable y $(x_u)_{u\in\mathcal{N}} \subset D$ una sucesión.*

(1) Existe $\sum_{u\in\mathcal{N}} x_u$ si y sólo si para todo $\epsilon > 0$, existe un subconjunto finito $F_0 \subset \mathcal{N}$ tal que $u \notin F_0$ implica $|x_u| < \epsilon$.

(2) Existe $\sum_{u\in\mathcal{N}} x_u$ y es igual a $s \in D$ si y sólo si para todo $\epsilon > 0$ existe $F_0 \subset \mathcal{N}$ finito tal que todo $F \subset \mathcal{N}$ finito que satisfaga $F_0 \subset F$ necesariamente cumple que $|s - \sum_{u\in F} x_u| < \epsilon$.

Demostración.

1. Supongamos que exista $\varphi : \mathbb{N} \to \mathcal{N}$ tal que $\sum_k x_k$ sea convergente y tomemos $\epsilon > 0$. Entonces, existe $k_0 \in \mathbb{N}$ tal que $k \geq k_0$ implica $|x_{\varphi(k)}| < \epsilon$; luego tomando $F_0 = \varphi(I_{k_0})$ tendremos que si $u \notin F_0$, se tiene que $\varphi^{-1}(u) > k_0$ y $|x_u| = \left|x_{\varphi\left(\varphi^{-1}(u)\right)}\right| < \epsilon$; por lo tanto la primera condición es suficiente. Procedamos a verificar que es necesaria para la veracidad de la segunda. Fijemos $\varphi : \mathbb{N} \to \mathcal{N}$ y tomemos cualquier $\epsilon > 0$. Entonces, existe $F_0 \subset \mathcal{N}$ tal que $|x_u| < \epsilon$ para todo $u \notin F_0$. Elijiendo $k_0 = \max \varphi^{-1}(F_0)$ sucede que todo $k \geq k_0 + 1$ cumple que $\varphi(k) \neq u$, para todo $u \in F_0$; por lo tanto $|x_{\varphi(k)}| < \epsilon$ siempre que $k \geq k_0 + 1$, con esto concluimos la demostración de *(1)*.

2. Supongamos que existe $\varphi : \mathbb{N} \to \mathcal{N}$ tal que $s = \sum_{k=1}^{\infty} x_u$ esté bien definido. Dado $\epsilon > 0$, sea $k_0 \in \mathbb{N}$ tal que $n \geq k_0$ implique

$$\left|s - \sum_{k=1}^{n} x_{\varphi(k)}\right| < \epsilon \qquad \text{y} \qquad |x_{\varphi(n)}| < \epsilon,$$

que existe a causa del lema 4.4.3. Para cualquier $F \subset \mathcal{N}$ finito y que contenga a F_0, ocurre que todo $u \in F \setminus F_0$ cumple que $\varphi^{-1}(u) > k_0$, y por tanto $|x_u| = |x_{\varphi(\varphi^{-1}(u))}| < \epsilon$. En consecuencia

$$\left|s - \sum_{u \in F} x_u\right| \leq \max\left\{\left|s - \sum_{u \in F_0} x_u\right|, \left|\sum_{u \in F \setminus F_0} x_u\right|\right\} \leq \max\left\{\epsilon, \max_{u \in F \setminus F_0} |x_u|\right\} < \epsilon.$$

Recíprocamente, fijemos una biyección $\varphi : \mathbb{N} \to \mathcal{N}$, elijamos cualquier $\epsilon > 0$ y verifiquemos la primera condición a partir de la segunda. Existe $F_0 \subset \mathcal{N}$ tal que todo $F \subset \mathcal{N}$ finito conteniendo a F_0 cumple necesariamente $\left|s - \sum_{u \in F} x_u\right| < \epsilon$. Entonces, tomando $n_0 = \max \varphi^{-1}(\mathcal{N})$, para todo $n \geq n_0$ se tiene que $\varphi(I_n)$ es finito y contiene a F_0, por lo que

$$\left|s - \sum_{k=1}^{n} x_{\varphi(k)}\right| = \left|s - \sum_{u \in \varphi(I_n)} x_u\right| < \epsilon$$

siempre que $n \geq n_0$.

Proposición 4.4.12 *Sean $\mathcal{N}$ un conjunto infinito numerable y $(x_u)_{u \in \mathcal{N}} \subset D$ una sucesión. Si $\sum_{u \in \mathcal{N}} x_u$ existe , entonces*

(1) Dados $t \in D$ y $\epsilon > 0$, si existe $F_0 \subset \mathcal{N}$ finito tal que $F \supseteq F_0$ implica $\left|\sum_{u \in F} x_u - t\right| \leq \epsilon$, entonces $\left|\sum_{u \in \mathcal{N}} x_u - t\right| \leq \epsilon$. En consecuencia, el hecho que $|x_u| \leq \epsilon$ para todo $u \in \mathcal{N}$, es suficiente para que $\left|\sum_{u \in \mathcal{N}} x_u\right| \leq \epsilon$.

(2) Para cada $\mathcal{N}_0 \subset \mathcal{N}$ *existe* $\sum_{u\in\mathcal{N}_0} x_u$.

(3) Para cada $F_0 \subset \mathcal{N}$ *finito, existe* $\sum_{\in\mathcal{N}\setminus F_0} x_u$ *y satisface*

$$\sum_{u\in\mathcal{N}} x_u - \sum_{u\in F_0} x_u = \sum_{u\in\mathcal{N}\setminus F_0} x_u.$$

Demostración.-

1. Sea $\varphi : \mathbb{N} \to \mathcal{N}$ una biyección, entonces $\sum_k x_{\varphi(k)}$ es convergente. Tomando $n_0 = \max \varphi^{-1}(F_0)$, tendremos que $\varphi(I_{n_0}) \supseteq F_0$; por lo tanto, para cada $n \leq n_0$ se cumple que $\varphi(I_n) \supseteq F_0$ y

$$|\sum_{k=1}^{n} x_{\varphi(k)} - t| \leq \epsilon.$$

Así concluimos que

$$|\sum_{u\in\mathcal{N}} x_u - t| = \lim_{n\to\infty} |\sum_{k=1}^{n} x_{\varphi(k)} - t| \leq \epsilon.$$

En particular, si $|x_u| \leq \epsilon$ para todo $u \in \mathcal{N}$, entonces fijando algún $u_0 \in \mathcal{N}$ y $F_0 = \{u_0\}$, tendremos que todo subsconjunto finito $F \supseteq F_0$ cumple

$$|\sum_{u\in F} x_u| \leq \max\{|x_u| \,;\, u \in F\} \leq \epsilon,$$

de lo cual deducimos la última afirmación de *(1)*.

2. La afirmación es trivialmente cierta cuando $\mathcal{N}_0$ es finito; procedamos a verificar cuando $\mathcal{N}_0$ es infinito. Puesto que existe la suma de (x_u), dado $\epsilon > 0$, existirá $F_0 \subset \mathcal{N}$ tal que $|x_u| < \epsilon$ para todo $u \notin F_0$. Entonces, tomando $F_1 = \mathcal{N} \cap F_0$ obtendremos que F_1 es un subconjunto finito tal que $|x_u| < \epsilon$, para todo $u \in \mathcal{N}_0 \setminus F_1$; por lo tanto existe $\sum_{u\in\mathcal{N}_0} x_n$.

3. De las hipótesis obtenemos que $\mathcal{N}_0 = \mathcal{N} \setminus F_0$ es un conjunto infinito numerable y que $\sum_{u\in\mathcal{N}_0} x_n$ existe (por *(2)*.). Dado $\epsilon > 0$, existe $F_1 \subset \mathcal{N}$ finito tal que

$$\Big|\sum_{u\in\mathcal{N}} x_u - \sum_{u\in F} x_u\Big| < \epsilon, \quad \text{para todo subconjunto finito } F \supseteq F_1.$$

Entonces, todo subconjunto finito $F \subset \mathcal{N} \setminus F_0$ tal que $F \supseteq (F_1 \setminus F_0)$ cumple que $F \cup F_0 \supseteq F_1 \cup F_0$ y

$$\Big|\sum_{u\in\mathcal{N}} x_u - \sum_{u\in F_0} x_u - \sum_{u\in F} x_u\Big| = \Big|\sum_{u\in\mathcal{N}} x_u - \sum_{u\in F\cup F_0} x_u\Big| < \epsilon.$$

Con esta desigualdad y el primer ítem de la anterior proposición, tendremos que

$$|\sum_{u\in\mathcal{N}} x_u - \sum_{u\in F_0} x_u - \sum_{u\in F} x_u| < \epsilon,$$

para $\epsilon > 0$ arbitrario, con lo que concluimos la demostración.

□

Proposición 4.4.13 *Sean $\mathcal{N}$ un conjunto numerable, $t \in D$ y $(x_u)_{u\in\mathcal{N}}$, $(y_u)_{u\in\mathcal{N}} \subset D$ tales que $\sum_{u\in\mathcal{N}} x_u$, $\sum_{u\in\mathcal{N}} y_u$ existen en D. Entonces*

$$\sum_{u\in\mathcal{N}}(x_u+y_u)=\sum_{u\in\mathcal{N}}x_u+\sum_{u\in\mathcal{N}}z_u \quad y \quad \sum_{u\in\mathcal{N}}tx_u=t\sum_{u\in\mathcal{N}}x_u.$$

Demostración.- Dado $\epsilon > 0$, existe $F_0 \subset \mathcal{N}$ finito tal que $F \supset F_0$ finito implica que

$$\left|\sum_{u\in\mathcal{N}}x_u-\sum_{u\in F}x_u\right|<\epsilon/2 \quad \text{y} \quad \left|\sum_{u\in\mathcal{N}}y_u-\sum_{u\in F}y_u\right|<\epsilon/2.$$

Entonces $F \supset F_0$ finito implica

$$\left|\left(\sum_{u\in\mathcal{N}}x_u+\sum_{u\in\mathcal{N}}y_u\right)-\sum_{u\in F}z_u\right| \le \left|\sum_{u\in\mathcal{N}}x_u-\sum_{u\in F}x_u\right|+\left|\sum_{u\in\mathcal{N}}y_u-\sum_{u\in F}y_u\right|<\epsilon;$$

como $\epsilon > 0$ fue arbitrario concluimos lo enunciado para $\sum_{u\in\mathcal{N}} z_u$. De manera similar se demuestra lo afirmado para $\sum_{u\in\mathcal{N}} w_u$, pues la demostración es semejante a la realizada si el cuerpo en cuestión fuese $\mathbb{R}$. □

Lema 4.4.14 *Sean $\mathcal{N}$ un conjunto numerable infinito y $(x_u)_{u\in\mathcal{N}}$ tal que $\sum_{u\in\mathcal{N}} x_u$ existe. Si $\{\mathcal{N}_k\}_{k\in\mathbb{N}}$ es una familia de subconjuntos finitos de $\mathcal{N}$ tal que $\bigcup_{k\in\mathbb{N}} \mathcal{N}_k = \mathcal{N}$ y $\mathcal{N}_k \subset \mathcal{N}_{k+1}$, para todo $k \in \mathbb{N}$. Entonces*

$$\sum_{u\in\mathcal{N}}x_u=\lim_{k\to\infty}\sum_{u\in\mathcal{N}_k}x_u.$$

Demostración.- Puesto que $\sum_{u\in\mathcal{N}}$ existe, entonces podemos tomar $F_0 \subset \mathcal{N}$ tal que todo subconjunto finito $F \supseteq F_0$ necesariamente cumple que

$$\left|\sum_{u\in\mathcal{N}}x_u-\sum_{u\in F}x_u\right|<\epsilon.$$

Como $\mathcal{N} \subset \bigcup_{k\in\mathbb{N}} \mathcal{N}_k$ y F_0 es finito, existirá $n_0 \in \mathbb{N}$ tal que $F_0 \subset \bigcup_{k=1}^{n_0} \mathcal{N}_{n_0}$; más aun podemos decir que $F_0 \subset \mathcal{N}_{n_0}$. Por lo tanto, todo $k \ge n_0$ cumple que $\mathcal{N}_k \supseteq F_0$ y, en consecuencia,

$$\left|s-\sum_{u\in\mathcal{N}_k}x_u\right|<\epsilon;$$

de esta forma obtenemos la convergencia de la sucesión de sumas parciales $\sum_{u\in\mathcal{N}_k} x_u$ y que su límite es igual a la suma de (x_u). □

El siguiente lema es el resultado más importante de la sección, el cual se podria resumir diciendo que en toda serie convergente es posible agrupar los sumandos de manera arbitraria sin variar el límite de la serie.

Lema 4.4.15 *Sean $\mathcal{N}$ un conjunto numerable y $(x_u)_{u\in\mathcal{N}} \subset D$ tal que exista $\sum_{u\in\mathcal{N}} x_u$. Si $\{\mathcal{N}_v\}_{v\in\mathcal{M}}$ es una partición de $\mathcal{N}$, entonces $\mathcal{M}$ es numerable y*

$$\sum_{u\in\mathcal{N}} x_u = \sum_{v\in\mathcal{M}} \sum_{u\in\mathcal{N}_v} x_u.$$

Demostración.- Puesto que los conjuntos que conforman la partición son disjuntos, por el axioma de elección podemos construir una función $f : \mathcal{M} \to \mathcal{N}$ que será inyectiva, por tanto $\mathcal{M}$ es numerable. La anterior proposición nos garantiza la existencia de cada suma $\sum_{u\in\mathcal{N}_v} x_u$, por lo tanto nos resta demostrar que la suma de todas estas es igual a $\sum_{u\in\mathcal{N}} x_u$. Definamos $s = \sum_{u\in\mathcal{N}} x_u$, fijemos $\epsilon > 0$ y tomemos $F_0 \subset \mathcal{N}$ finito tal que:

- $|x_u| < \epsilon$, para todo $u \notin F_0$;
- $F \supseteq F_0$ finito implique $|s - \sum_{u\in F} x_u| < \epsilon$.

Si $G_0 = \{v \in \mathcal{M} \ , \ F_0 \cap \mathcal{N}_v \neq \emptyset\}$ entonces G_0 será finito y $F_0 = \bigcup_{v\in G_0} \mathcal{N}_v$, puesto que la familia $\{\mathcal{N}_v\}_{v\in\mathcal{M}}$ forma una partición de $\mathcal{N}$. Dado $G \subset G_0$ finito, se satisface que

$$\begin{aligned}
\Big|s - \sum_{v\in G}\sum_{u\in\mathcal{N}_v} x_u\Big| &\leq \text{máx}\Big\{\Big|s - \sum_{u\in F_0} x_u\Big|, \Big|\sum_{u\in F_0} x_u - \sum_{v\in G}\sum_{u\in\mathcal{N}_v} x_u\Big|\Big\} \\
&< \text{máx}\Big\{\epsilon, \Big|\sum_{u\in F_0} x_u - \sum_{v\in G_0}\sum_{u\in G_v} x_u\Big|, \Big|\sum_{v\in G\setminus G_0}\sum_{u\in G_v} x_u\Big|\Big\} \\
&= \text{máx}\Big\{\epsilon, \Big|\sum_{v\in G_0}\sum_{u\in\mathcal{N}_v\setminus(\mathcal{N}_v\cap F_0)} x_u\Big|, \Big|\sum_{v\in G\setminus G_0}\sum_{u\in G_v} x_u\Big|\Big\}.
\end{aligned}$$

Dado $v \in G_v$, sucede que cada sumando x_u indexado por $u \in \mathcal{N}_v \setminus F_0$ posee valor absoluto menor que ϵ, entonces se tiene inmediatamente que $|\sum_{u\in G_v\setminus F_0}| < \epsilon$, si son finitos; sino será a causa de *1.* y *2.* de la proposición anterior. Análogamente, para todo $v \in G \setminus G_0$, deducimos que $|\sum_{u\in\mathcal{N}_v} x_u| \leq \epsilon$, pues en ese caso todo índice u no pertenece a F_0. Por lo tanto,

$$\Big|s - \sum_{v\in G}\sum_{u\in\mathcal{N}_v} x_u\Big| < \text{máx}\Big\{\epsilon, \max_{v\in G_0}\Big|\sum_{u\in\mathcal{N}_v\setminus(\mathcal{N}_v\cap F_0)} x_u\Big|, \max_{v\in G\setminus G_0}\Big|\sum_{u\in\mathcal{N}_v} x_u\Big|\Big\} \leq \epsilon.$$

Como $\epsilon > 0$ fue arbitrario, en caso $\mathcal{M}$ sea infinito tendriamos que existe $\sum_{v\in\mathcal{M}}\sum_{u\in\mathcal{N}_v} x_u$ y es igual a s (por la proposición anterior). En caso $\mathcal{M}$ sea finito, simplemente podemos reemplazar $G = \mathcal{M}$ y verificará la desigualdad anterior para cada $\epsilon > 0$, y también será cierto el lema. □

Las siguientes proposiciones son un ejemplo de la utilidad de la generalidad con que hemos abordado el tema de series, del potencial del lema anterior y donde estableceremos series que abordarán la segunda parte de esta monografía.

Proposición 4.4.16 *Sean* $n \in \mathbb{N}$, $\mathfrak{N} = \mathbb{N}_0^n$ *y* $(x_u)_{u\in\mathfrak{N}}$, $(y_u)_{u\in\mathfrak{N}} \subset D$ *tales que existan* $\sum_{u\in\mathfrak{N}} x_u$ *y* $\sum_{u\in\mathfrak{N}} y_u$. *Definamos* $(z_w)_{w\in\mathfrak{N}} \subset D$ *por* $z_w = \sum_{u+v=w} x_u y_v$; *entonces existe la suma de* (z_w) *y*

$$\sum_{w\in\mathfrak{N}} z_w = \sum_{u\in\mathbb{N}} x_u \sum_{v\in\mathbb{N}} y_v.$$

Demostración.- Definamos el conjunto (infinito numerable) $\mathcal{N}' = \mathfrak{N}\times\mathfrak{N}$ y la sucesión $(x_u y_v)_{(u,v)\in\mathcal{N}'}$. Comprobemos que existe la suma de $(x_u y_v)$ en D. Puesto que $\sum_{u\in\mathfrak{N}} x_u$ y $\sum_{v\in\mathfrak{N}} y_u$ existen, pódemos elegir algún $c > 0$ tal que

$$|x_u| < c \text{ y } |y_u| < c \text{ para todo } u, v \in \mathfrak{N};$$

pues $\sum_k x_{\varphi(k)}$ y $\sum_k y_{\varphi(k)}$ existen para alguna $\varphi : \mathbb{N} \to \mathfrak{N}$ biyección. Dado $\epsilon > 0$, existen subconjuntos finitos $F_1, F_2 \subset \mathfrak{N}$ tales que $|x_u| < \epsilon/c$ e $|y_u| < \epsilon/c$ para todo $u \notin F_1$ y $v \notin F_2$. Luego, el conjunto $F_0 = F_1 \times F_2$ será finito y todo $(u, v) \in \mathcal{N}' \setminus F_0$ cumple que $u \notin F_1$ o $v \notin F_2$, lo que a su vez implica que $|uv| < (\epsilon/c)c = \epsilon$; por lo tanto, en virtud de la proposición 4.4.11, existe $\sum_{(u,v)\in\mathcal{N}'} x_u y_v$. Como $\{(u, v)\ ;\ v \in \mathfrak{N}\}_{u\in\mathfrak{N}}$ y $\{(u, v)\ ;\ u + v = w\}_{w\in\mathfrak{N}}$ son familias de subconjuntos de $\mathcal{N}'$ que lo particionan, entonces existirá la suma en cada subconjunto de estas familias y

$$\sum_{(u,v)\in\mathcal{N}'} = \sum_{u\in\mathfrak{N}} \sum_{(u,v)\ ;\ v\in\mathfrak{N}} x_u y_v = \sum_{w\in\mathfrak{N}} \sum_{u+v=w} x_u y_v.$$

Gracias a la proposición 4.4.13, podemos ver que

$$\sum_{u\in\mathfrak{N}} \sum_{(u,v)\ ;\ v\in\mathfrak{N}} x_u y_v = \sum_{u\in\mathfrak{N}} (x_u \sum_{v\in\mathfrak{N}} y_v) = \sum_{v\in\mathfrak{N}} y_v \sum_{u\in\mathfrak{N}} x_u,$$

con lo cual concluimos la proposición. □

Proposición 4.4.17 *Sean* $\mathfrak{N} = \mathbb{N}_0^2$ *y* $(x_u)_{u\in\mathfrak{N}} \subset D$ *tal que* $\sum_{u\in\mathfrak{N}} x_u$ *existe, entonces existen*

$$\sum_{m=0}^{\infty} x_{n,m} \quad y \quad \sum_{n=0}^{\infty} x_{n,m}, \qquad \text{para todo } n, m \geq 0.$$

Más aun

$$\sum_{u\in\mathfrak{N}} x_u = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} x_{n,m} = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} x_{n,m}.$$

Demostración.- Sea $\mathcal{N}_n = \{n\} \times \mathbb{N}_0$, para todo $n \in \mathbb{N}_0$. Entonces, por el lema 4.4.15 tendremos que, para cada $n \in \mathbb{N}_0$, existe $\sum_{v\in\{n\}\times\mathbb{N}_0} x_v \in D$; el cual es igual a $\sum_{m=0}^{\infty} x_{n,m}$. Más aun, se tiene que

$$\sum_{u\in\mathfrak{N}} x_u = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} x_{n,m};$$

de manera análoga se demuestra que $\sum_{u\in\mathfrak{N}} x_u = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} x_{n,m}$. □

Capítulo 5

El cuerpo de números p−ádicos

En este capítulo empezaremos con el tema de trabajo: los números p-ádicos. Construiremos un valor absoluto sobre $\mathbb{Q}$ y veremos que no es completo. Su compleción, a la que denotaremos $\mathbb{Q}_p$, será un cuerpo que goza de muchas propiedades algebraicas que serán estudiadas a partir de su anillo de valuación $\mathbb{Z}_p$.

5.1. El valor absoluto p-ádico

En este capítulo p denotará un número primo; recordando la proposición 4.1.3 podemos enunciar la siguiente definición.

Definición 5.1.1 La *valuación p−ádica sobre* $\mathbb{Z}$ es definida por $v_p(n) = \text{máx}\{m; p^m | n\}$, para todo $n \in \mathbb{Z} \setminus \{0\}$.

Un valor muy conocido de v_p en teoría de números es su evaluación en $n!$, a saber

$$v_p(n!) = \sum_{m=1}^{\infty} \left\lfloor \frac{n}{p^m} \right\rfloor,$$

la demostración de esta fórmula se puede encontrar en [2, capítulo 4, sección 1, teorema 4.2]. Nosotros necesitaremos otra versión un poco más algebraica. Denotemos por $\overline{a_t a_{t-1} \dots a_0}_p$ a un *numeral en base p*, esto es $n = a_0 + a_1 p + \cdots + a_t p^t$, donde $a_0, \dots, a_t \in \{0, 1, \dots, p-1\}$.

Lema 5.1.2 *Dado* $n = \overline{a_t a_{t-1} \dots a_0}_p$ *no nulo, se tiene*

1. $v_p(n) = \text{mín}\{0 \leq j \leq t \ : \ a_j \neq 0\}$;
2. $v_p(n!) = \dfrac{n - (a_t + \cdots + a_1 + a_0)}{p-1}$.

Demostración.- Tomando $k = \min\{j \ : \ a_j \neq 0\}$ vemos que

$$v_p(n) = v_p(p^k(a_k + \cdots + a_t p^{t-k})) = k + v_p(a_k + \cdots + a_t p^{t-k}) = k + 0,$$

porque $p \nmid a_j$. Realicemos la prueba por inducción sobre n; vemos que es cierta para $n = 1$, así que supongamos cierto el lema para $n = \overline{a_t a_{t-1} \ldots a_0}_p$ e intentemos demostrarlo para $n+1$, dividiéndolo en dos casos. Si $a_j < p-1$, para algún j entre 1 y t, tomamos $k = \min\{j; a_j < p-1\} \leq t$. Tenemos que $0 \leq a_k \leq p-2$ y $a_0 = a_1 = \cdots = a_{k-1} = p-1$, luego $1 \leq a_k + 1 \leq p-1$ y

$$n+1 = a_t p^t + a_{t-1}p^{t-1} + \cdots + a_{k+1}p^{k+1} + (a_k+1)p^k + 0 \cdot p^{k-1} + \cdots + 0 \cdot p + 0 \cdot 1,$$

por tanto $n+1 = \overline{b_t b_{t-1} \cdots b_0}_p$ con $b_0 = \cdots = b_{k-1} = 0$, $b_k = a_k + 1$ y $a_{k+1} = b_{k+1}, \ldots, a_t = b_t$; entonces

$$\begin{aligned} v_p((n+1)!) &= v_p(n!) + v_p(n+1) \\ &= \frac{n - (a_t + \cdots + a_0)}{p-1} + k \\ &= \frac{n - (a_t + \cdots + a_0)}{p-1} - (p-1)\frac{k}{p-1} + k \\ &= \frac{n+1 - \left(b_t + \cdots + b_{k+1} + (a_k+1)\right)}{p-1} \\ &= \frac{n - (b_t + \cdots + b_0)}{p-1}; \end{aligned}$$

por tanto, en este caso la igualdad es cierta. En el otro caso, $a_0 = a_1 = \cdots = a_t = (p-1)$ y entonces

$$n = (p-1)p^t + (p-1)p^{t-1} + \cdots + (p-1) = (p-1)\frac{(p^{t+1}-1)}{p-1} = p^{t+1} - 1,$$

por tanto $n+1 = p^t$ y $n+1 = \overline{10\ldots0}$ (con t ceros en esta representación), luego

$$v_p\big((n+1)!\big) = v_p(n!) + v_p(n+1) = \frac{n - \sum_{j=1}^{t} a_j}{p-1} + (t+1) = \frac{n+1-1}{p-1},$$

por lo que el lema también se cumple en este caso. □

Observación 5.1.3 Sea $n \geq 1$. Como $p^{v_p(n)} \mid n$, tendremos que $v_p(n)\log(p) \leq \log(n)$ por lo tanto $v_p(n) \leq \log(n)/\log(p)$.

La valuación valuación $p-$ádica sobre $\mathbb{Z}$ se extiende a una valuación sobre $\mathbb{Q}$ (por la proposición 4.1.5), y a esta nueva valuación también la denotaremos por v_p y la denominaremos $p-$ádica. Luego, en virtud de la proposición 4.2.5, podemos construir un valor absoluto no arquimediano.

Definición 5.1.4 El *valor absoluto p−ádico* $|x|_p$ sobre $\mathbb{Q}$ es definido por $|x|_p = p^{-v_p(x)}$.

Tomando en cuenta la valuación $p-$ádica sobre $\mathbb{Q}$, denotemos por $\mathbb{Z}_{(p)}$ al anillo de valuación, esto es

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \,:\, v_p(x) \geq 0\} = \{x \in \mathbb{Q} \,:\, |x|_p \leq 1\}$$

y $\mathfrak{p}_0$ al ideal de valuación,

$$\mathfrak{p}_0 = \{x \in \mathbb{Q}_p \,:\, v_p(x) > 0\} = \{x \in \mathbb{Q}_p \,:\, |x|_p < 1\}.$$

Con estas notaciones presentamos el siguiente resultado.

Proposición 5.1.5

(i) Dado $x \in \mathbb{Q} \setminus \{0\}$, *se tiene que* $x = p^{v_p(x)}a/b$ *con* $a, b \in \mathbb{Z} \setminus \{0\}$ *coprimos con* p.

(ii) $\mathbb{Z}_{(p)} = \{a/b \,:\, a, b \in \mathbb{Z},\ con\ p \nmid b\}$.

(iii) $\mathfrak{p}_0 = p\mathbb{Z}_{(p)}$.

(iv) El cuerpo residual $\kappa_0 = \mathbb{Z}_{(p)}/\mathfrak{p}_0$ *es isomorfo a* $\mathbb{F}_p$.

(v) $\mathbb{Z}$ *es denso en* $\mathbb{Z}_{(p)}$.

Demostración.-

- Dado $x = c/d$, basta tomar $a = p^{-v_p(c)}c$ y $b = p^{-v_p(d)}d$ para obtener la anterior representación .
- El conjunto de la derecha de *(ii)* está contenido en $\mathbb{Z}_{(p)}$, y si $x \in \mathbb{Z}_{(p)}$ tendremos que $v_p(x) \geq 0$. Por tanto, si $x = p_p^v(x)a/b$ con a, b coprimos con p, entonces $c = ap^{v_p(x)} \in \mathbb{Z}$ y $x = c/b$ con $p \nmid b$.
- Es análogo al anterior ítem.
- Sea $x = a/b \in \mathbb{Z}_{(p)}$ con $p \nmid b$, tomemos $c \in \mathbb{Z}$ representante de la clase de $(a + p\mathbb{Z})(b + p\mathbb{Z})^{-1}$, entonces $a - bc \equiv a - 1 \cdot a \equiv 0 \pmod{p}$; por lo tanto $v_p(a/b - c) > 0$, nótese esto ocurre para cualquier representante de $(a + p\mathbb{Z})(b + p\mathbb{Z})^{-1}$. Recíprocamente, si $v_p(a/b - c) > 0$ con $c \in \mathbb{Z}$ y $a/b \in \mathbb{Z}_{(p)}$, entonces $v(a - bc) > 0$ y $a \equiv bc \bmod p$, esto es $c \equiv ab^{-1} \bmod p$; esto caracteriza la clase $(a + p\mathbb{Z})(b + p\mathbb{Z})^{-1}$ como la única clase tal que todo elemento c en ella cumple $v_p(x - c) > 0$ (o equivalentemente $|x - c|_p \leq 1$).

  Esto nos permite definir $\psi : \mathbb{Z}_{(p)} \to \mathbb{Z}/p\mathbb{Z}$ como $\psi(x) = (a + p\mathbb{Z})(b + p\mathbb{Z})^{-1}$, para $x = a/b$ con $(b, p) = 1$; procedamos a verificar que es un homomorfismo. De hecho, dados

$x = a_1/b_1$, $y = a_2/b_2 \in \mathbb{Z}_{(p)}$, tomemos $c_1 \in \psi(x)$ y $c_2 \in \psi(y)$, por la propiedad no arquimediana tendremos entonces

$$\left|\frac{a_1}{b_1} + \frac{a_2}{b_2} - (c_1 + c_2)\right|_p = \max\left\{\left|\frac{a_1}{b_1} - c_1\right|_p, \left|\frac{a_2}{b_2} - c_2\right|_p\right\} \leq 1,$$

y además

$$\begin{aligned}\left|\frac{a_1a_2}{b_1b_2} - c_1c_2\right|_p &= \left|\frac{a_1}{b_1}\left(\frac{a_2}{b_2} - c_2\right) + c_2\left(\frac{a_1}{b_1} - c_1\right)\right|_p \\ &\leq \max\left\{\left|\frac{a_1}{b_1}(\frac{a_2}{b_2} - c_2)\right|_p, \left|c_2(\frac{a_1}{b_1} - c_1)\right|_p\right\} \\ &\leq \max\left\{\left|\frac{a_2}{b_2} - c_2\right|_p, \left|\frac{a_1}{b_1} - c_1\right|_p\right\} \leq 1,\end{aligned}$$

esto nos dice que $c_1 + c_2 \in \psi(x+y)$ y $c_1c_2 \in \psi(xy)$ (por la caracterización de ψ). Puesto que se trata clases de equivalencia, concluimos que $\psi(a_1/b_1 + a_2/b_2) = \psi(a_1/b_1) + \psi(a_2/b_2)$ y $\psi(a_1a_2/b_1b_2) = \psi(a_1/b_1)\psi(a_2/b_2)$. Como $\mathrm{Nu}(\psi) = \mathfrak{p}_0$ e $\mathrm{Im}(\psi) = \mathbb{Z}/p\mathbb{Z}$, por el teorema fundamental de homomorfismos tendremos que $\mathbb{Z}_{(p)} \cong \mathbb{F}_p$.

- Sea $x = a/b \in Z_{(p)}$ donde $p \nmid b$, y $\epsilon > 0$. Entonces escogemos $n \in \mathbb{N}$ tal que $p^{-n} < \epsilon$, y $c \in \mathbb{Z}$ representante de $(a + p^n\mathbb{Z})(b + p^n\mathbb{Z})^{-1}$ para obtener que $a - bc \equiv 0$ mód $p^n\mathbb{Z}$ y $|a/b - c|_p \leq p^{-n} < \epsilon$; por tanto $\mathbb{Z}$ es denso en $\mathbb{Z}_{(p)}$.

□

Una propiedad que relaciona al valor absoluto tradicional $|\cdot|_\infty$ y al valor absoluto p-ádico es el siguiente resultado.

Lema 5.1.6 *El único entero n tal que $|n|_p|n|_\infty < 1$ es el número 0, para todo $p \in \mathbb{N}$ primo.*

Demostración.- Dado $n \in \mathbb{Z}$ no nulo, supongamos que $n = p_1^{e_1} \cdots p_r^{e_r}$ es su descomposición en potencias de números primos distintos. Luego, si $p \in \mathbb{N}$ es primo, entonces $|n|_p$ es 1, si $p \notin \{p_1, \ldots, p_r\}$, en caso contrario $|n|_p = p_r^{-e_r}$. Como en ambos casos ocurre que $|n|_p|n|_\infty \geq 1$, concluimos el lema. □

Recordemos que $\mathbb{Q}$ no es completo con respecto al valor absoluto tradicional, por ejemplo $X = \{x \ : x^2 \leq 2\}$ no tiene ínfimo en $\mathbb{Q}$, de lo cual se puede deducir que X contiene una sucesión de Cauchy no convergente en $\mathbb{Q}$. Ahora veremos que $\mathbb{Q}$ tampoco es completo respecto a cualquier valor absoluto $p-$ádico, pero antes daremos un lema acerca de la existencia de raíces módulo p sobre $\mathbb{Z}$ de enteros que no la tienen en $\mathbb{Q}$.

Lema 5.1.7 *Dado p primo, existen $a, m \in \mathbb{Z}$ coprimos con p tales que:*

1. *no existe $x \in \mathbb{Q}$ tal que $x^m = a$;*

2. *existe* $x_1 \in \mathbb{Q}$ *tal que* $x_1^m \equiv a \bmod p$.

Demostración.- Empecemos por mostrar que si $a \in \mathbb{Z}$ no tiene raíces $n-$ésimas en $\mathbb{Z}$, tampoco las tendrá en $\mathbb{Q}$. En efecto, de lo contrario existirán $b, c \in \mathbb{Z}$ coprimos tal que $(b/c)^n = a$, entonces $b^n = c^n a$. Dado $q \in \mathbb{N}$ primo se cumple $nv_q(b) = nv_q(c) + v_q(a)$; luego, si $c \neq 1$ entonces existe $q_0 \in \mathbb{N}$ primo tal que $q_0 \mid c$ (lo que equivale a $v_{q_0}(c) > 0$), por ello $q \nmid b$ y $v_q(b) = 0$, por lo que $0 = nv_q(c) + v_q(a)$ y $v_q(a) = -nv_q(c) < 0$, lo que es absurdo.

Ahora demostremos el caso p impar. Verificaremos que $m = 2$ y $a = p^2 + 1$ satisfacen las propiedades enunciadas. Supongamos que existe $b \in \mathbb{Z}$ tal que $b^2 = a = p^2 + 1$, entonces $2 \mid b^2$, luego $2 \mid b$ y $4 \mid b^2$. Así tenemos que $(p+1)^2 \equiv b^2 + 2p \bmod 4$, y como $(p+1)^2 \equiv 0 \bmod 4$, concluimos que $2p \equiv 0 \bmod 4$, lo que es absurdo. El caso $p = 2$ se revuelve para $a = 7$, $m = 3$ y $x_1 = 1$. □

Teorema 5.1.8 *El cuerpo* $(\mathbb{Q}, |\cdot|_p)$ *no es completo.*

Demostración.- La idea de esta demostración es construir un secuencia de Cauchy de modo tal que si existe el límite en $\mathbb{Q}$, este será una raíz de cierta ecuación previamente establecida, pero imponiendo condiciones sobre esta ecuación imposibilitaremos la existencia de tal límite en $\mathbb{Q}$. Tomemos $a, m, x_1 \in \mathbb{Z}$ cumpliendo las condiciones del del lema anterior, y definamos $B = \{(n, b), b^m \equiv a \bmod p^n\}$. Este conjunto será no vacío, pues $(1, x_1) \in B$, más aun podemos contruir por inducción una sucesión $(c_n)_{n\in\mathbb{N}} \subset B$ tal que su segunda componente forme una sucesión de Cauchy respecto al valor absoluto p-ádico. En efecto, empecemos por tomar $c_1 = (1, x_1)$; supongamos que tenemos $c_n = (n, b_n) \in B$ y procedamos a construir el siguiente término c_{n+1}. Sea $d \in \mathbb{Z}$, tomando $x = b_n + dp^n$ obtenemos que

$$x^m = (b_n + dp^n)^m = b_n^m + b_n^{m-1} dp^n + \sum_{i=0}^{m-2} \binom{m}{i} b_n^i (dp^n)^{m-i}.$$

Como $n(m-i) \geq n+1$ cuando $i = 0, 1, \ldots, m-2$, tendremos $x^m \equiv b_n^m + a_n^{m-1} dp^n \bmod p^{n+1}$. Puesto que $b_n^m \equiv a \bmod p^n$, se tiene que $b_n^m \equiv a \bmod p$; luego, como $p \nmid a$, tenemos que $p \nmid b_n^m$ y $b_n \in (\mathbb{Z}/p\mathbb{Z})^\times$. Por tanto, existe $t = t(b_n) \in \mathbb{Z}$ tal que $b_n t \equiv 1 \bmod p$. Por otra parte, existe $r = r(n, b_n) \in \mathbb{Z}$ tal que $p^n r = b_n^m - a$; por lo tanto tomando a d como un representante de la clase $-rt^{m-1} + p\mathbb{Z}$ tendremos que

$$r + db_n^{m-1} \equiv r - rt^{m-1} b^{m-1} \equiv r - r1 \equiv 0 \bmod p,$$

luego

$$x^m \equiv a + (b_n^m - a) + db_n^{m-1} p^n \equiv a + p^n (r + db_n^{m-1}) \equiv a \bmod p^{n+1}.$$

Así tomamos $b_{n+1} = b_n + dp^n$ con el anterior $d = d(n, b_n)$, obteniendo $(n+1, b_{n+1}) \in B$ con $b_{n+1} \equiv b_n$ mód p^n. Por inducción, obtenemos la existencia de $(b_n)_{n\in\mathbb{N}} \subset \mathbb{Z}$ tal que

(1) $(n, b_n) \in B$, para todo $n \in \mathbb{N}$.

(2) $b_{n+1} \equiv b_n$ mód p^n, para todo $n \in \mathbb{N}$.

El segundo ítem nos da $|b_{n+1} - b_n|_p \leq p^{-n}$ para cada $n \in N$, asi concluimos que $\lim_n |b_{n+1} - b_n|_p = 0$ y (b_n) es de Cauchy. Si (b_n) converge a algún $\alpha \in \mathbb{Q}$, entonces

$$|\alpha^m - a|_p = \lim_n |b_n^m - a|_p = 0.$$

Esto nos dice que $\alpha^m = a$, lo que contradice el lema anterior; por lo tanto, (b_n) no es convergente y $(\mathbb{Q}, |\cdot|_p)$ no es completo. □

Utilizando el teorema 4.3.12, podemos construir $\mathbb{Q}_p$, una compleción de $(\mathbb{Q}, |\cdot|_p)$; más aún si en la prueba de cada teorema acerca de $\mathbb{Q}_p$ nos restringimos a sólo utilizar sus propiedades de compleción (las mencionadas en la definición 4.3.11), entonces podemos afirmar que se cumplen para toda compleción y tratar a $\mathbb{Q}_p$ como la única compleción de $(\mathbb{Q}, |\cdot|_p)$. El siguiente teorema nos mostrará la generalidad de los cuerpos $\mathbb{Q}_p$ como compleciones no arquimedianas de $\mathbb{Q}$, el cual no demostraremos porque no tendrá repercusión en nuestro trabajo (puede encontrar su demostración en [4, capítulo 3, sección 2]).

Teorema 5.1.9 (Ostrowski) *Todo valor absoluto no trivial sobre $\mathbb{Q}$ es equivalente al valor absoluto tradicional o a algún valor absoluto $p-$ádico.*

La compleción $\mathbb{Q}_p$ contiene un cuerpo isomorfo e isométrico a $\mathbb{Q}$, que podemos suponer igual a $\mathbb{Q}$. De hecho, si $\sigma : \mathbb{Q} \to \mathbb{Q}_p$ es un monomorfismo que satisface la definición 4.3.11, entonces podemos construir un cuerpo isomorfo e isométrico a $\mathbb{Q}_p$ de la forma $(\mathbb{Q}_p - \sigma(\mathbb{Q})) \uplus \mathbb{Q}$ (este tipo de construcción es análoga a realizada en [3, páginas 52 y 53] para "colocar" un dominio dentro de su cuerpo de fracciones).

El valor absoluto $p-$ádico se extiende a $\mathbb{Q}_p$ y lo hace completo; a este valor absoluto también le denominaremos $p-$ádico y denotaremos por $|\cdot|_p$. Además, por la proposición 4.3.13 se cumple que

$$|\mathbb{Q}_p|_p = |\mathbb{Q}|_p = \{p^n; n \in \mathbb{Z}\};$$

así también se extiende v_p sobre $\mathbb{Q}_p$, definiendo $v_p(x) = -\log_p(|x|_p)$ (el logaritmo real en base p). Al anillo de valuación de $\mathbb{Q}_p$ lo denotaremos por $\mathbb{Z}_p$, es decir

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ : \ v_p(x) \geq 0\} = \{x \in \mathbb{Q}_p \ : \ |x|_p \leq 1\}$$

y al ideal de valuación por $\mathfrak{p}$, así

$$\mathfrak{p} = \{x \in \mathbb{Q}_p \,:\, v_p(x) > 0\} = \{x \in \mathbb{Q}_p \,:\, |x|_p > 1\}.$$

Como indica la proposición 4.1.9, $\mathfrak{p}$ es el único ideal maximal de $\mathbb{Z}_p$. Sin embargo, pero podemos decir mucho más.

Teorema 5.1.10 *Dado p primo, se cumplen:*

(1) $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$.

(2) $\mathfrak{p} = p\mathbb{Z}_p$.

(3) $\mathbb{Z}$ *es denso en* $\mathbb{Z}_p$.

(4) $\mathbb{Z}_p/\mathfrak{p} \cong \mathbb{F}_p$.

Demostración.- Son claras la veracidad de *(1)* y que $p\mathbb{Z}_p \subset \mathfrak{p}$. Más aún, si $x \in \mathfrak{p}$ entonces $|x|_p = p^{-n}$ con $n > 0$, luego $|p^{-n}x|_p = 1$ y $p^{-n}x \in \mathbb{Z}_p$, en particular $x \in p\mathbb{Z}_p$, por lo tanto *(2)* también es cierto. Para demostrar el *(3)*, verificaremos que $\mathbb{Z}_{(p)}$ es denso en $\mathbb{Z}_p$, lo cual, por la proposición 5.1.5, implicará que $\mathbb{Z}$ es denso en $\mathbb{Z}_p$. Dado $x \in \mathbb{Z}_p$ y $\epsilon \in]0,1[$, existe $a/b \in \mathbb{Q}$ tal que $|x - a/b|_p < \epsilon$, por tanto $|a/b|_p = \max\{|x - a/b|_p, |x|_p\} \leq 1$. Luego $a/b \in \mathbb{Z}_{(p)}$ con $|x - a/b|_p < \epsilon$; por tanto $\mathbb{Z}_{(p)}$ es denso en $\mathbb{Z}_p$. El cuarto ítem es consecuencia directa de la proposición 4.3.14. □

Observaciones 5.1.11

- Las unidades del anillo $\mathbb{Z}_p$ son los elementos $u \in \mathbb{Z}_p$ tales que $|u|_p = 1$ (o equivalentemente $v_(u) = 0$), esto es $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p;\ |x|_p = 1\}$.
- *El único elemento irreducible de* $\mathbb{Z}_p$ *es p (salvo conjugados).* En efecto, si $t \in \mathbb{Z}_p$ fuese otro elemento irreducible no conjugado con p tendriamos que $p \nmid t$, por tanto $t \in \mathbb{Z}_p \setminus \mathfrak{p}$, luego seria inversible sobre $\mathbb{Z}_p$.
- Como en el segundo ítem de la proposición anterior, recordamos que si $|x|_p = p^{-n}$ con $n \geq 1$ obtendremos que $|xp^{-n}|_p = 1$, luego $xp^{-n} = u$ con $u \in \mathbb{Z}_p$ y $x \in p^n\mathbb{Z}_p$. Por tanto, en el caso que $|x - y|_p \leq p^{-n} < 1$ tendremos que $p^n \mid x - y$ en $\mathbb{Z}_p$.
- En el caso $|x_p| = 1$, no se puede cumplir que $p \mid x$ en $\mathbb{Z}_p$.

La relevancia de p como elemento irreducible en $\mathbb{Z}_p$ y su importancia como factor de los elementos de $\mathbb{Z}_p$ nos induce a denotar $|x-y|_p \leq p^{-n}$, lo que equivale a $p^n \mid x-y$ en $\mathbb{Z}_p$, por $x \equiv y$ mód p^n.

Observaciones 5.1.12

- Nótese que esto generaliza lo que sucede en $\mathbb{Z}$. En efecto, si $a, b \in \mathbb{Z}$ son tales que $p^n \mid a-b$ en $\mathbb{Z}_p$, esto es, existe $c \in \mathbb{Z}$ tal que $p^n c = a-b$ con $c \in \mathbb{Z}_p$, entonces $|a-b|_p \leq p^{-n}$. Como esta relación en elementos de $\mathbb{Z}$ significa que existe $c' \in \mathbb{Z}$ tal que $p^n c = a-b$, deducimos que $c = c'$. Por lo tanto

$$a + p^n\mathbb{Z}_p = b + p^n\mathbb{Z}_p \qquad \text{equivale a} \qquad a + p^n\mathbb{Z} = b + p^n\mathbb{Z}.$$

- Esta notación resume $x + p^n\mathbb{Z}_p = y + p^n\mathbb{Z}_p$ igual entre clases de equivalencia el anillo $\mathbb{Z}_p$ por el ideal generado por p^n, luego esta notación es una relación de equivalencia y respeta las operaciones de suma y producto entre clases.

Proposición 5.1.13 *Dado $\alpha \in \mathbb{Z}_p$, se tiene que $|\alpha^p - \alpha|_p < 1$, o equivalentemente $\alpha^p = \alpha$ mód p.*

Demostración.- Puesto que $\mathbb{Z}_p/\mathfrak{p}$ es isomorfo a $\mathbb{Z}/p\mathbb{Z}$, ocurre que $\alpha^p + \mathfrak{p} = (\alpha + \mathfrak{p})^p = \alpha + \mathfrak{p}$, por tanto $\alpha^p \equiv \alpha \mod p$. □

Ahora, daremos la primera caracterización de $\mathbb{Z}_p$, para esto recordemos que dado $n \in \mathbb{N}$, existe un homomorfismo de anillos $\chi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ definido por $\chi_n(a + p^{n+1}\mathbb{Z}) = a + p^n\mathbb{Z}$.

Definición 5.1.14 Una sucesión del tipo $(E_n, \chi_n)_{n\in\mathbb{N}}$ con $\chi_n : E_{n+1} \to E_n$ homomorfismo entre anillos es llamado *sistema proyectivo.* Un *límite proyectivo* (E, π_n) del sistema proyectivo (E_n, χ_n) es un anillo E con una sucesión de homomorfismos $\pi_n : E \to E_n$ tal que $\pi_{n+1} = \chi_n \circ \pi_n$, para todo $n \in \mathbb{N}$, que además satisfacen

> Si un anillo X junto con los homomorfismos $(f_n)_{n\in\mathbb{N}}$ satisfacen $f_n = \chi_n \circ f_{n+1}$ para todo $n \in \mathbb{N}$, entonces existe un homomorfismo $f : X \to E$ tal que $f_n = \pi_n \circ f$.

Proposición 5.1.15 *Dado $n \in \mathbb{N}$, la función $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ definida por*

$$\pi_n(x) = \left\{a \in \mathbb{Z}; |x-a|_p \leq p^{-n}\right\} = (x + p^n\mathbb{Z}_p) \cap \mathbb{Z},$$

es un homomorfismo de anillos tal que $Nu(\pi_n) = p^n\mathbb{Z}_p$ e $\operatorname{im}(\pi_n) = \mathbb{Z}/p^n\mathbb{Z}$. Además, la sucesión formada por estos homomorfimos satisface $\pi_n = \chi_n \circ \pi_{n+1}$.

Demostración.- Dado $x \in \mathbb{Z}_p$, el conjunto $\pi_n(x)$ es no vacío por el tercer ítem del teorema (5.1.10), y con la última notación tenemos que

$$\pi_n(x) = \{a \in \mathbb{Z}; x \equiv a \text{ mód } p^n\},$$

el cual es la clase de equivalencia de a módulo p^n. Ahora la verificación de que es homomorfismo es la verificación del segundo ítem en la última observación. En efecto, dados $x, y \in \mathbb{Z}_p$ tomando $a \in \pi_n(x)$ y $b \in \pi_n(y)$ tenemos que

$$\big|(x+y)-(a+b)\big|_p \leq \text{máx}\{|x-a|_p, |y-b|_p\} \leq p^{-n},$$

por tanto $a+b \in \pi_n(x+y)$ y $\pi_n(x)+\pi(y) \subset \pi_n(x+y)$, y como se trata de clases de equivalencia se concluyen las igualdades. De forma análoga,

$$|xy-ab|_p \leq \text{máx}\big\{|x|_p|y-b|_p, |b|_p|x-a|_p\big\} \leq p^{-n},$$

por tanto $\pi_n(xy) \subset \pi_n(x)\pi_n(y)$, luego los últimos conjuntos son iguales y π_n es un homomorfismo de anillos.

Ahora, veamos las afirmaciones acerca del núcleo e imagen. Dado $x \in \text{Nu}(\pi_n)$, tenemos que $0 \in \pi_n(x)$, luego $|x|_p \leq p^{-n}$ asi que $\text{Nu}(\pi_n) \subset p^n\mathbb{Z}_p$. Recíprocamente, si $x \in p^n\mathbb{Z}$, entonces cualquier $a \in \pi_n(x)$ cumple $|a|_p \leq \text{máx}\{|x-a|_p, |a|_p\} \leq p^{-n}$, de modo que $a \in 0+p^n\mathbb{Z}$ y $\pi_n(x) \subset 0+p^n\mathbb{Z}$; como se trata de clases, concluimos que $\pi_n(x) = p^n\mathbb{Z}$; luego $\text{Nu}(\pi_n) = p^n\mathbb{Z}_p$. Más aun, como $\pi_n(m) = m+p^n\mathbb{Z}$ para todo $m \in \mathbb{Z}$ tendremos que π_n es sobreyectiva.

Finalmente, dado $n \in \mathbb{N}$ tenemos que $\pi_{n+1}(x) = a+p^{n+1}\mathbb{Z}$ para algún $a \in \mathbb{Z}$, luego $\chi_n\big(\pi_{n+1}(x)\big) = a+p^n\mathbb{Z}$. Como $\pi_{n+1}(x) \subset \pi_n(x)$, concluimos que $a \in \pi_n(x)$ y $\pi_n(x) = a+p^n\mathbb{Z}$; por lo tanto $\pi_n(x) = \chi_n\big(\pi_{n+1}(x)\big)$ para todo $x \in \mathbb{Z}_p$. □

Teorema 5.1.16 *El conjunto de enteros p−ádicos $\mathbb{Z}_p$ es un límite inverso de $(\mathbb{Z}/p^n\mathbb{Z}, \chi_n)$.*

Demostración.- Sean X un anillo y una sucesión de homomorfismos $f_n : X \to \mathbb{Z}/p^n\mathbb{Z}$ como en la definición 5.1.14. Dado $x \in X$, para cada $n \in \mathbb{N}$ elijamos $a_n \in f_n(x)$. Entonces, dado $n \in \mathbb{N}$ tenemos

$$a_{n+1}+p^{n+1}\mathbb{Z} = f_{n+1}(x) \quad \text{y} \quad \chi_n(f_{n+1}(x)) = a_{n+1}+p^n\mathbb{Z},$$

como $f_n(x) = a_n + p^n\mathbb{Z}$ satisface la definición 5.1.14, tendremos que $a_n \equiv a_{n+1}$ mód p^n. Por tanto $(a_n) \subset \mathbb{Z}$ es una sucesión de Cauchy, luego existe $\lim_n a_n \in \mathbb{Q}_p$ que denotamos f_x. Puesto que $\mathbb{Z}_p$ es cerrado, tendremos que $f_x \in \mathbb{Z}_p$.

Veamos que f_x no depende de la elección de la sucesión (a_n) escogida y sólo de x. En efecto, sea $(b_n) \subset \mathbb{Z}$ tal que $b_n \in f_n(x)$ para todo $n \in \mathbb{N}$; entonces, dado $n \in \mathbb{N}$ tenemos $|b_n - a_n|_p \leq p^{-n}$, luego

$$\lim_n b_n = \lim_n b_n - a_n + \lim_n a_n = \lim_n a_n = f_x,$$

por tanto, f_x depende únicamente de x, así definimos $f : x \to \mathbb{Z}_p$ por $f(x) = f_x$.

Es rutinario demostrar que f es un homomorfismo, así que tan sólo veamos que f es satisface el enunciado del teorema. Tomemos $n \in \mathbb{N}$ y $x \in X$, sea $(a_m) \subset \mathbb{Z}$ tal que $a_m \in f_m(x)$, para todo $m \in \mathbb{N}$. Entonces, por inducción sobre $m \geq n$, tendremos que $a_m \equiv a_n \mod p^n$, luego $\left|f(x) - a_n\right|_p = \lim_n |a_m - a_n| \leq p^{-n}$. Por tanto, $a_n \in \pi_n\big(f(x)\big)$ y en consecuencia $f_n(x) \subset a_n + p^n\mathbb{Z} = \pi_n\big(f(x)\big)$; como se trata de clases de equivalencia se tiene la igualdad. □

5.2. La expansión p -ádica

Denotaremos por $\mathbb{Z}[[x]]$ al anillo de series formales con coeficientes en $\mathbb{Z}$. El lema siguiente, nos dice que estas series pueden ser evaluadas en p y que su suma pertenece a $\mathbb{Z}_p$. Más aun, el siguiente teorema nos dirá que los elementos así obtenidos son en realidad todos los que existen en $\mathbb{Z}_p$.

Lema 5.2.1 *Si* $(a_n)_{n\geq 0} \subset \mathbb{Z}$, *entonces* $\sum_{n\geq 0} a_n p^n$ *es convergente en* $\mathbb{Z}_p$.

Demostración.- Como $\mathbb{Z}_p$ es una bola cerrada en un espacio métrico completo, entonces $\mathbb{Z}_p$ es un dominio completo. Luego, por el lema 4.4.3 concluimos. □

Teorema 5.2.2 (expansión p-ádica) *Dado* $a \in \mathbb{Z}_p$, *existe una única sucesión* $(a_n)_{n\geq 0} \subset \{0, 1, \ldots, p-1\}$ *tal que* $a = \sum_{n\geq 0} a_n p^n$; *más aun, si* $a \neq 0$ *entonces* $v_p(a) = \min\{n; a_n \neq 0\}$.

Demostración.- Empecemos demostrando la unicidad de este tipo de sucesión. Sean $(a_n)_{n\geq 0}$, $(b_n)_{n\geq 0} \subset \{0, 1, \ldots, p-1\}$ tales que $a = \sum_{n\geq 0} a_n p^n = \sum_{n\geq 0} b_n p^n$. Entonces, dado $m \in \mathbb{N}$ tenemos que

$$x = \sum_{n=0}^{m-1} a_n p^n + \sum_{n\geq m} a_n p^n = \sum_{n=0}^{m-1} a_n p^n + p^m \alpha$$

donde $\alpha = \sum_{n\geq m} a_n p^{m-n}$, el cual es convergente en $\mathbb{Z}_p$ (por el lema anterior); análogamente existe $\beta \in \mathbb{Z}_p$ tal que $x = b_0 + \cdots + b_{m-1}p^{m-1} + p^m\beta$. Luego

$$x \equiv a_0 + \cdots + a_{m-1}p^{m-1} \equiv b_0 + \cdots + b_m p^{m-1} \mod p^m,$$

como los dos últimos miembros de esa congruencias son enteros entre 1 y $p^m - 1$, tenemos que son iguales. Como se tratan de representaciones en base p del mismo natural, concluimos que $a_0 = b_0, \ldots, a_{m-1} = b_{m-1}$, y puesto que $m \in \mathbb{N}$ fue arbitrario concluimos que $a_n = b_n$, para todo $n \geq 0$.

Mostremos la existencia con ayuda del teorema 5.1.16, Para cada $n \in \mathbb{N}$ tomamos b_n como el único representante de $\pi_n(x)$ entre 1 y $p^n - 1$, y $a_{n,0}, \ldots, a_{n,n-1} \in \{0, 1, \cdots, p-1\}$ tales que $b_n = a_{n,0} + \cdots + a_{n,n-1}p^{n-1}$, nótese que los $a_{n,m}$ son dígitos de b_n en base p y que algunos pueden ser ceros.

Afirmación. *Dados $n, k \in \mathbb{N}$ se tiene que $a_{n,m} = a_{n+k,m}$ para todo $m = 0, 1, \ldots, n-1$.*

En efecto, como $|a - b_n|_p < p^{-n}$ y $|a - b_{n+k}|_p < p^{-(n+k)}$ concluimos que $|b_{n+k} - b_n|_p \leq p^{-n}$, o equivalentemente $b_{n+k} \equiv b_n \bmod p^n$; por lo tanto concluimos que $a_{n,0} = a_{n+k,0}, \cdots, a_{n,n-1} = a_{n+k,n-1}$.

Ahora, escojamos $(a_n)_{n\geq 0}$ definiendo $a_n = b_{n+1,n}$ para cada $n \geq 0$ y verifiquemos que satisfacen el teorema. Dados $m \in \mathbb{N}$ y $n \leq m$ tendremos que $a_n = b_{n+1,n} = b_{m+1,n}$, por tanto

$$a_0 + a_1 p \cdots + a_m p^m = a_{m+1,0} + \cdots + a_{m+1,m}p^m = b_{m+1},$$

luego $\left|a - (a_0 + \cdots + a_m p^m)\right|_p \leq p^{-m-1}$, para todo $m \in \mathbb{N}$; con esta desigualdad se concluye la afirmación.

Finalmente, si $a \neq 0$ y el conjunto $\{n; a_n \neq 0\}$ debe ser no vacío, por tanto podemos tomar su menor elemento que denotamos por r. Luego

$$a = \sum_{n\leq r} a_n p^n = p^r\Big(a_r + p\big(\sum_{n=r+1}^{\infty} a_n p^{n-(r+1)}\big)\Big) = p^r(a_r + p\alpha)$$

donde $\alpha = \sum_{n\geq r+1} a_n p^{n-(r+1)} \in \mathbb{Z}_p$ (por el lema previo). Como $v_p(a_r) = 0$ y $v_p(p\alpha) \geq 1$, tendremos que $v_p(a_r + p\alpha) = v_p(a_r) = 0$ y $v_p(a) = r$. □

Corolario 5.2.3 *Dado $x \in \mathbb{Q}_p^\times$ y $r = v_p(x) \in \mathbb{Z}$, existe una única sucesión $(c_n)_{n\geq r} \subset \{0, 1, \ldots, p-1\}$ tal que $x = \sum_{n\geq r} c_n p^n$. con $c_r \neq 0$.*

Demostración.- Escribamos $x = p^r a$ con $a \in \mathbb{Z}_p^\times$, entonces existe una única sucesión $(a_n)_{n\in\mathbb{N}} \subset \{0, 1, \ldots, p-1\}$ tales que $a = \sum_{n\leq 0} a_n p^n$ con $a_0 \neq 0$ (pues $v_p(a) = 0$). Asi escribiendo, para cada $n \geq r$, $c_n = a_{n-r}$ tendremos que $x = \sum_{n\geq r} c_n p^n$ con $c_0 \geq 0$. Más aun, si $(d_n)_{n\in\mathbb{N}} \subset \{0, 1, \ldots, p-1\}$ también satisface el corolario, entonces $a = \sum_{n\geq 0} d_{n+r} p^n$. Luego por la unicidad de $(a_n)_{n\in\mathbb{N}}$ tendremos que $c_n = a_{n-r} = d_n$ para todo $n \geq r$, con lo cual concluimos el corolario. □

Ejemplos 5.2.4 Presentamos algunas representaciones $p-$ádicas que provienen de sencillas relaciones algebraicas sobre un cuerpo.

1. Como
$$\frac{1-p^{(n+1)r}}{1-p^r} = 1 + p^r + p^{2r} + \cdots + p^{nr} \qquad \text{para todo } n \in \mathbb{N},$$
haciendo $n \to +\infty$ tendremos que
$$\frac{1}{1-p^r} = 1 + p^r + p^{2r} + \cdots + p^{rn} + \cdots .$$

2. Dado $\hat{a} = \sum_{n \geq r} a_n p^n$ con $a_r \neq 0$, tomando $m > r$ tendremos que
$$a + (p - a_r)p^r + (p - 1 - a_{r+1})p^{r+1} + \cdots + (p - 1 - a_n)p^n = \sum_{n>m} a_n p^n,$$
y tomando límite vemos que
$$-a = (p - a_r)p^r + (p - 1 - a_{r+1})p^{r+1} + \cdots + (p - 1 - a_n)p^n + \cdots .$$

3. Se tiene que
$$-1 = (p-1) + (p-1)p + \cdots + (p-1)p^n + \cdots .$$

4. Dado p primo impar, se tiene que
$$\frac{1}{2} = \frac{p+1}{2} - \frac{p}{2} = \frac{p+1}{2} + \frac{p}{2}\Big(\sum_{n\geq 0}(p-1)p^n\Big),$$
por lo tanto
$$\frac{1}{2} = \frac{p+1}{2} + \frac{p-1}{2}p + \cdots + \frac{p-1}{2}p^n \cdots .$$

Corolario 5.2.5 *El anillo de enteros $p-$ádicos $\mathbb{Z}_p$ es no numerable, por tanto el cuerpo de números p-ádicos $\mathbb{Q}_p$ tampoco lo es.*

Demostración.- El teorema precedente nos dice que $\mathbb{Z}_p$ y $\prod_{n=0}^{\infty}\{0, 1, \ldots, p-1\}$ son equipotentes, y como el cardinal de $\{0, 1, \ldots, p-1\}$ es mayor o igual a 2 tenemos que $\mathbb{Z}_p$ es no numerable. □

Observación 5.2.6 Utilizando el teorema 5.1.9 tendremos que ninguna compleción de $\mathbb{Q}$ con una métrica inducida por un valor absoluto no trivial es numerable.

5.3. Lema de Hensel

Este lema establece una de las propiedades más importantes y útiles de $\mathbb{Z}_p$, pues afirma la existencia de una raíz de un polinomio siempre que inicialmente tengamos una raíz aproximada módulo p^n. El lema es conocido como la versión $p-$ádica del método iterativo de Newton, pues utiliza una sucesión (a_n) de la forma $a_{n+1} = a_n - F(a_n)/F'(a_n)$. Si bien en la versión en $\mathbb{R}$ de este método se utiliza la noción de derivada como un límite (de lo cual hablaremos mas adelante), en esta sección sólo nos remitiremos a la derivada formal de los polinomios a tomar, aunque utilizaremos el siguiente lema que es una suerte de teorema de Taylor en $\mathbb{Z}_p$.

Lema 5.3.1 *Sea $f(X) \in \mathbb{Z}_p[X]$ un polinomio. Entonces existe $g(X,Y) \in \mathbb{Z}_p[X,Y]$ tal que*

$$f(X+Y) = f(X) + Yf'(X) + y^2 g(X,Y).$$

En particular, si $\alpha, \beta \in \mathbb{Z}_p$ entonces $\left|f(\alpha) - f(\beta)\right|_p \leq |\alpha - \beta|_p$.

Nótese que la primera afirmación se cumple en cualquier anillo.

Demostración.- Tomemos $f(X) = a_m X^m + \cdots + a_0$, entonces

$$\begin{aligned} f(X+Y) &= \sum_{i=0}^{m} a_i (X+Y)^i = \sum_{i=0}^{m} a_i \left(\sum_{j=0}^{i} \binom{i}{j} X^{i-j} Y^j \right) \\ &= \sum_{i=0}^{m} a_i X^i + Y \sum_{i=1}^{m} i a_i X^{i-1} + Y^2 \sum_{i=2}^{m} a_i \left(\sum_{j=0}^{i} \binom{i}{j} X^{i-j} Y^{j-2} \right). \end{aligned}$$

Por lo tanto, tomando $g(X,Y) = \sum_{i=2}^{m} a_i \left(\sum_{j=0}^{i} \binom{i}{j} X^{i-j} Y^{j-2} \right) \in \mathbb{Z}_p[X,Y]$ tenemos mostrada la primera parte. Para mostrar la segunda parte nótese que $X = \alpha$, $Y = \beta - \alpha$ nos da

$$|f(\beta) - f(\alpha)|_p \leq \text{máx}\left\{ \left|f'(\alpha)(\alpha - \beta)\right|_p, \left|g(\alpha, \beta - \alpha)(\beta - \alpha)^2\right|_p \right\} \leq |\beta - \alpha|.$$

□

Teorema 5.3.2 (Hensel) *Sean $f(X) \in \mathbb{Z}_p[X]$ y $\alpha_1 \in \mathbb{Z}_p$ tales que $v_p\big(f'(\alpha_1)\big) = r < \infty$ y $v_p\big(f(\alpha_1)\big) \geq 2r+1$. Entonces, existe un único $\alpha \in \mathbb{Z}_p$ tal que $f(\alpha) = 0$ y $\alpha_1 \equiv \alpha$ mód p^{r+1}.*

Demostración.- Empecemos por observar qué ocurre en una iteración $p-$ádica del metodo de Newton para nuestro caso.

Afirmación. *Sea $\alpha \in \mathbb{Z}_p$ y n un entero positivo tales que $\left|f(\alpha)\right|_p \leq p^{-(2r+n)}$ y $\left|f'(\alpha)\right|_p = p^{-r}$, entonces $\beta = \alpha - f(\alpha)/f'(\alpha)$* satisface

1. $|\beta - \alpha|_p \leq p^{-(r+n)}$.

2. $|f'(\beta)|_p = p^{-r}$.

3. $|f(\beta)|_p \leq p^{-(2r+2n)}$.

En efecto tomemos $h = \beta - \alpha$, entonces

$$|h|_p = |f(\alpha)|_p / |f'(\alpha)|_p \leq p^{-(r+n)},$$

y el primer ítem es cierto. Para mostrar el segundo, utilicemos el lema previo. Con sus mismas notaciones, obtenemos que $f(\beta) = f(\alpha) + f'(\alpha)h + g(\alpha, h)h^2$ con $g(X, Y) \in \mathbb{Z}_p[X, Y]$. Aplicando este lema al polinomio $f'(X) \in \mathbb{Z}_p[X]$ obtenemos que

$$\left|f'(\alpha) - f'(\beta)\right|_p \leq |\alpha - \beta|_p \leq p^{-r-n} < p^{-r} = \left|f'(\alpha)\right|,$$

por tanto $\left|f'(\beta)\right|_p = \text{máx}\left\{\left|f'(\alpha)\right|_p, \left|f'(\beta) - f'(\alpha)\right|_p\right\} = \left|f'(\alpha)\right|_p$. Además,

$$|f(\beta)| = |g(\alpha, h)h^2|_p \leq |h|_p^2 \leq p^{-2(r+n)},$$

puesto que $g(X, Y) \in \mathbb{Z}_p[X, Y]$.

Por esta afirmación, al tomar

$$A = \left\{\alpha \in \mathbb{Z}_p; \left|f'(\alpha)\right|_p \leq p^{-r} \quad \text{y} \quad \left|f'(\alpha)\right|_p < p^{2r}\right\},$$

que es no vacío por hipótesis, podemos asegurar que $t : A \to A$, definido por $t(a) = a - f(a)/f'(a)$ esta bien definido. Luego, por inducción construimos una sucesión $(a_n)_{n\in\mathbb{N}} \subset A$ tal que

(i) $a_1 = \alpha_1$,

(ii) $a_{n+1} = t(a_n)$, para todo $n \in \mathbb{N}$.

La afirmación también nos asegura, aplicando inducción sobre n, que se tiene

(i') $|a_n - a_{n+1}|_p \leq p^{-(r+2^{n-1})}$,

(ii') $|f'(a_n)|_p = p^{-r}$, para todo $n \in \mathbb{N}$.

Luego (a_n) será una sucesión de Cauchy en $\mathbb{Z}_p$, por tanto convergente a $\alpha \in \mathbb{Z}_p$; y como las funciones $\mathcal{E}(f, \cdot)$ y $\mathcal{E}(f', \cdot)$ son continuas (por la proposición 4.3.5) concluimos que

$$f(\alpha) = \lim_n f(a_n) = 0 \quad \text{y} \quad |f'(\alpha)|_p = \lim_n |f'(a_n)| = 1.$$

Además, dado $n \in \mathbb{N}$ tendremos que

$$|a_n - \alpha_1|_p \leq \max\{|a_1 - a_2|_p, |a_2 - a_3|_p, \ldots, |a_{n-1} - a_n|_p\} \leq p^{-r-1};$$

por tanto, tomando límite cuando $n \to +\infty$, concluimos que $|\alpha - \alpha_1|_p \leq p^{-r-1}$, y la existencia de α está garantizada.

Finalmente, veamos la unicidad del α construido. Supongamos que $\beta \in \mathbb{Z}_p$ es distinto a α y $f(\beta) = 0$, $|\beta - \alpha_0|_p \leq p^{-r-1}$. Entonces, $\beta \equiv \alpha \bmod p^{-r-1}$ y $k = \beta - \alpha$ satisface $|\beta - \alpha|_p \leq p^{-r-1}$. Luego

$$f(\beta) = f(\alpha) + kf'(\alpha) + k^2 g(\alpha, k),$$

donde $g(X, Y) \in \mathbb{Z}_p[X, Y]$ por el lema previo, por tanto

$$|f'(\alpha)|_p = |-kg(\alpha, k)|_p \leq p^{-r-1} \cdot 1$$

y $v_p(f'(\alpha)) \geq r + 1$, lo que es absurdo, lo que prueba la unicidad de α. □

En el caso párticular de $r = 0$ y de elementos en $\mathbb{Z}$ obtenemos el siguiente resultado.

Corolario 5.3.3 *Sean $f(X) \in \mathbb{Z}[X]$ y $a \in \mathbb{Z}$ tales que $f(a) \equiv 0 \bmod p$ y $f'(a) \not\equiv 0 \bmod p$, entonces existe un único $\alpha \in \mathbb{Z}_p$ que satisface $f(\alpha) = 0$ y $\alpha \equiv a \bmod p$.*

5.3.1. Raíces de la unidad

En esta sección utilizaremos el lema de Hensel para estudiar la existencia de raíces de la unidad, pues como dijimos anteriormente estas no son más que ceros de polinomios del tipo $X^n - 1$.

Para empezar, si recordamos la proposición 4.2.2, tendremos que toda raíz de la unidad estará en $\mathbb{Z}_p^\times$. Por tal motivo tendremos que $\alpha \not\equiv 0 \bmod p$, o equivalentemente $\alpha \equiv a \bmod p$ para algún $a \in \{1, 2, \ldots, p-1\}$.

Un hecho trivial, pero importante para $\mathbb{Q}_p$, es que todo elemento no nulo de $\mathbb{Z}/p\mathbb{Z}$ es una raíz de la unidad. Más aun se tiene el hecho que el grupo $(\mathbb{Z}/p\mathbb{Z})^\times$ siempre es cíclico (por el teorema 3.11.3). De este modo, en el caso p impar tenemos la existencia de $b \in \mathbb{Z}$ tal que $b^t \not\equiv 1 \bmod p$ para $t = 1, 2, \ldots, p-2$. Luego dado $m \mid p-1$ tomando $a = b^{(p-1)/m}$ tendremos que $a^m \equiv 1 \bmod p$ y $a^t \equiv 1 \bmod p$ para $t = 1, 2, \ldots, m-1$.

Proposición 5.3.4 *Dado $p \in \mathbb{N}$ primo y $m > 1$ coprimo con p, entonces existen raíces de la unidad de orden m si y sólo si $m \mid p-1$.*

Demostración.- Empecemos por suponer que existe $\alpha \in \mathbb{Q}_p$ que sea una raíz primitiva $m-$ésima de la unidad. Tomemos $a \in \{0,1,\ldots,p-1\}$ tal que $\alpha \equiv a \text{ mód } p$ y $t = \text{ord}\,(a+p\mathbb{Z})$. Porque $a^m \equiv \alpha^m \equiv 1$, tendremos que $t \mid m$; más aun, tomando $p(X) = X^m - 1$, por el corolario 5.3.3 concluimos que existe un único $\theta \in \mathbb{Z}_p$ tal que $p(\theta) = 0$ y $\theta \equiv a \text{ mód } p$. Por un motivo análogo, si $q(X) = X^t - 1$ entonces existirá $\beta \in \mathbb{Z}_p$ tal que $\beta^t = 1$ y $\beta \equiv a \text{ mód } p$. Como $t \mid m$, se cumple que $q(X) \mid p(X)$, por tanto $p(\beta) = 0$ y $\beta = \theta$; así concluimos que $m = \text{ord}\,(\theta) = \text{ord}\,(\beta) = t$, y $m \mid p-1$.

Ahora supongamos que $m \mid p-1$ para el caso en que $p > 2$ sea impar. Por la observación precedente, tomemos $a \in \mathbb{Z}$ tal que $a^m \equiv 1 \text{ mód } p$ y $a^t \not\equiv 1 \text{ mód } p$ para $t = 1,2,\ldots,m-1$, entonces por el corolario 5.3.3 existe $\alpha \in \mathbb{Z}_p$, una $m-$ésima raíz de la unidad, tal que $\alpha \equiv a \text{ mód } p$. Más aun, para cada $t = 1,2,\ldots,m-1$ se tiene que $\alpha^t \equiv a^t \not\equiv 1 \text{ mód } p$; en particular $\alpha^t \neq 1$ para todo $t \in \{1,2,\ldots,m-1\}$; así concluimos que $\text{ord}\,(\alpha) = m$. □

5.3.2. Segunda forma del lema de Hensel

El siguiente análisis tiene como fin extender el lema de Hensel para el caso $r = 0$, tomando en cuenta polinomios "módulo p" y la de multiciplicidad de una raíz.

Primeramente, expresando las hipótesis del teorema 5.3.2 en términos clase de equivalencia tendremos que

$$|f(\alpha_0)|_p < 1 \quad \text{equivale a} \quad f(\alpha_0) = 0 \text{ mód } p, \quad \text{o bien} \quad (\pi f)(\pi(a)) = 0,$$

esto es, $\pi(a) \in \mathbb{F}_p$ es raíz de $\pi f(X) \in \mathbb{F}_p[X]$. Así también

$$|f'(\alpha_0)|_p = 1 \quad \text{es lo mismo que} \quad f'(\alpha_0) \not\equiv 0 \text{ mód } p, \quad \text{o bien} \quad (\pi f)(\pi(\alpha_0)) \neq 0,$$

por lo tanto, $\pi(\alpha_0)$ sea una raíz es simple. Ahora, por definición de raíz simple, tendremos que existe $h_1(X) \in \mathbb{F}_p[X]$ tal que

$$\pi f(X) = \big(X - \pi(\alpha_0)\big)h_1(X) \quad \text{y} \quad h_1(\pi(\alpha_0)) \neq 0,$$

pero esto nos indica que $\big(X - \pi(\alpha_0)\big) \nmid h_1(X)$, el cual es irreductible en $\mathbb{F}_p[X]$, por tanto concluimos que la hipótesis equivale a la existencia de $h_1(X) \in \mathbb{F}_p[X]$ tal que

$$\pi f(X) = \big(X - \pi(\alpha_0)\big)h_1(X), \qquad \text{con} \quad \text{mcd}\,\big(X - \pi(\alpha_0), h_1(X)\big).$$

La tesis simplemente nos dice que existirán $\alpha \in \mathbb{Z}_p$ y $h(X) \in \mathbb{Z}_p[X]$ tales que

$$f(X) = (X-\alpha)h(X) \quad \text{y} \quad \pi(X - \alpha_0) = \pi(X - \alpha).$$

En conclusión, ciertas factorizaciones en $\mathbb{F}_p[X]$ de la proyección $\pi f(X)$ pueden ser "elevadas" hacia factorizaciones en $\mathbb{Z}_p[X]$ del polinomio $f(X)$, el siguiente teorema presenta algunas condiciones suficientes para que esto ocurra.

Teorema 5.3.5 (Segunda forma del lema de Hensel) *Dado $f(X) \in \mathbb{Z}_p[X]$, si existen $g_1(X), h_1(X) \in \mathbb{Z}_p[X]$ tales que*

(1) $f(X) = g_1(X)h_1(X) \mod p$

(2) $g_1(X)$ *y* $h_1(X)$ *son coprimos módulo p, esto es mcd* $(g_1(X), h_1(X)) = 1$.

(3) $g_1(X)$ *es mónico.*

Entonces, existen $g(X), h(X) \in \mathbb{Z}_p$ tales que

(a) $f(X) = g(X)h(X)$.

(b) $g(X) \equiv g_1(X) \mod p$ *y* $h(X) \equiv h_1(X) \mod p$.

(c) $g(X)$ *es mónico.*

Demostración.-

Construiremos dos sucesiones en $\mathbb{Z}_p[X]$ adecuadas para proporcionarnos los polinomios esperados, via un proceso de "aproximación módulo p". Empecemos, fijando $r(X), s(X) \in \mathbb{Z}_p[X]$ tales que

$$r(X)g_1(X) + s(X)h_1(X) \equiv 1 \mod p;$$

que existen porque $\pi g_1(X), \pi h_1(X) \in \mathbb{F}_p[X]$ son coprimos y $\mathbb{F}_p[X]$ es un dominio ideales principales. Ahora definimos el conjunto B de las ternas $\big(n, g(X), h(X)\big) \in \mathbb{N} \times \mathbb{Z}_p[X] \times \mathbb{Z}_p[X]$ que satisfacen

1. $f(X) \equiv g(X)h(X) \mod p^n$;
2. $r(X)g(X) + s(X)h(X) \equiv 1 \mod p$;
3. $g(X)$ es mónico.

Sobre este conjunto definiremos una sucesión cuya segunda y tercera componente formen sucesiones adecuadas a nuestros fines. Dado $(n, g(X), h(X)) \in B$, elijamos los únicos $t(X), r(X)$, $s(X) \in \mathbb{Z}_p[X]$ tales que $p^n t(X) = f(X) - g(X)h(X)$, pues $\mathbb{Z}_p[X]$ es un dominio. Para cualesquiera $a(X), b(X) \in \mathbb{Z}_p[X]$ tendremos que

$$f(X) - \big(g(X) + p^n a(X)\big)\big(h(X) + p^n b(X)\big) = p^n\big(t(X) - g(X)b(X) - a(X)h(X)\big) + p^{2n}a(X)b(X).$$

Por tanto, si elegimos $a_0(X) = s(X)t(X)$ y $b_0(X) = r(X)t(X)$ obtenemos que

$$f(X) - \big(g(X) + p^n a_0(X)\big)\big(h(X) + p^n b_0(X)\big) \equiv 0 \text{ mód } p^{n+1}.$$

Sin embargo $g(X) + p^n a_0(X)$ no es candidato a ser una segunda componente de un elemento en B, pues no necesariamente es mónico, aunque no está lejos de serlo. En efecto, como $g(X)$ es mónico podemos aplicar el algoritmo euclidiano de división para encontrar los únicos $q(X), \alpha(X) \in \mathbb{Z}_p[X]$ tales que

$$a_0(X) = g(X)q(X) + \alpha(X) \qquad \text{con } \alpha(X) = 0 \text{ o grad } \big(\alpha(X)\big) < \text{grad } \big(g(X)\big);$$

tomando $g_0(X) = g(X) + p^n \alpha(X)$, obtenemos un polinomio mónico, que junto a $h_0(X) = h(X) + p^n \beta(X)$ con $\beta(X) = h(X)q(X) + b_0(X)$, cumplen

$$\begin{aligned} f(X) - g_0(X)h_0(X) &= p^n\big(t(X) - a_0(X)h(X) - g(X)b_0(X)\big) \\ &+ -p^n\big(g(X)h(X)q(X) - g(X)q(X)h(X)\big) \\ &+ p^{2n}\big(a_0(X) - g(X)q(X)\big)\big(b_0(X) + h(X)q(X)\big) \\ &\equiv 0 \text{ mód } p^{n+1}; \end{aligned}$$

y como

$$g_0(X) \equiv g(X) \text{ mód } p \qquad \text{y} \qquad h_0(X) \equiv h(X) \text{ mód } p,$$

$g_0(X)$ y $h_0(X)$ también satisfacen el ítem 2) de la definición de B, por lo tanto $\big(n+1, g_0(X), h_0(X)\big) \in B$; lo cual nos definide una función $\ell : B \to B$ tal que $\ell\big(n, g(X), h_n(X)\big) = \big(n+1, g_0(X), h_0(X)\big)$, donde $g_0(X)$ y $h_0(X)$ son determinados, de manera única, por el procedimiento previo. Aplicando inducción, podemos construir $\big(g_n(X)\big)_{n\in\mathbb{N}}, \big(h_n(X)\big)_{n\in\mathbb{N}} \subset \mathbb{Z}_p[X]$ tales que

(a) $g_1(X)$ y $h_1(X)$ son exactamente los polinomios en las hipótesis del teorema.

(b) $\big(n+1, g_{n+1}(X), h_{n+1}(X)\big) = \ell\big(n, g_n(X), h_n(X)\big)$, para todo $n \in \mathbb{N}$.

(c) $\big(n, g_n(X), h_n(X)\big) \in B$, para todo $n \in \mathbb{N}$.

Por este ítem (b) tenemos que

$$g_{n+1}(X) \equiv g_n(X) \text{ mód } p^n \quad \text{y} \quad h_{n+1}(X) \equiv h_n(X) \text{ mód } p^n \tag{5.1}$$

para todo $n \in \mathbb{N}$. Y por el ítem (c), sabemos que todo $g_n(X)$ es mónico, por tanto

$$\text{grad } g_n(X) = \text{grad } \pi g_n(X), \quad \text{para todo } n \in \mathbb{N};$$

así concluimos que

$$\text{grad } g_1(X) = \text{grad } \pi g_1(X) = \text{grad } \pi g_n(X) = \text{grad } g_n(X) = \text{grad } \pi_n g_n(X); \quad \text{para todo } n \in \mathbb{N}.$$

Fijamos $r = \text{grad } g_1(X) \in \mathbb{Z}$. Ahora, si $f(X) = a^t X^t + \cdots + a_1 X + a_0$ entonces, para cada $n > v_p(a_t)$, obtendremos $a_t \not\equiv 0 \text{ mód } p^n$; luego grad $\pi_n f(X) = t$, para cada $n > v_p(a_t)$. Por tanto, como $g_n(X)$ es mónico, claramente tendremos que

$$t = \text{grad } \pi_n f(X) = \text{grad } \pi_n g_n(X) + \text{grad } \pi_n h_n(X) = r + \text{grad } \pi_n h_n(X), \quad \text{para todo } n \in \mathbb{N};$$

y $s = t - r \in \mathbb{Z}$ cumple que grad $\pi_n h_n(X) = s$, para todo $n > v_p(a_t)$. Para cada $n \in \mathbb{N}$, denotemos

$$g_n(X) = X^r + b_{r-1}X^{r-1} + \cdots + b_0 \quad \text{y} \quad h_n(X) = c_{s_n}X^{s_n} + c_{s_n-1}X^{s_n-1} + \cdots + c_0.$$

Entonces

$$c_{s_n} \equiv c_{s_n-1} \equiv \cdots \equiv c_{s+1} \equiv 0 \text{ mód } p^n, \quad \text{para todo } n > v_p(a_t),$$

lo que nos dice que los coeficientes de orden mayor a s "no cuentan módulo p^n ".

Luego, utilizando el ítem (c), y las propiedades de r y s cuando $n > v_p(a_t)$, tendremos que

$$a_k \equiv \sum_{i+j=k} b_{i,n}c_{j,n} \text{ mód } p^n \qquad \text{para todo } k = 0, 1, \ldots, t. \tag{5.2}$$

Por otra parte, las congruencias (5.1) nos dan

$$b_{i,n+1} \equiv b_{i,n} \text{ mód } p^n \quad \text{y} \quad c_{j,n+1} \equiv c_{j,n} \text{ mód } p^n$$

para todo $i = 0, 1, \ldots, r$, $j = 0, 1, \ldots, s$ y $n \in \mathbb{N}$. Por lo tanto, las sucesiones $(b_{i,n})_{n\in\mathbb{N}}, (c_{j,n})_{n\in\mathbb{N}} \subset \mathbb{Z}_p$ son de Cauchy y serán convergentes a $b_i \in \mathbb{Z}_p$ y $c_j \in \mathbb{Z}_p$ para cada $i = 0, 1, \ldots, r$ y $j = 0, 1, \ldots, s$. Luego, por las congruencias (5.2) se obtiene

$$a_k - \sum_{i+j=k} b_i c_j = \lim_n (a_k - \sum_{i+j=k} b_{i,n}c_{j,n}) = 0$$

para cada $k = 0, 1, \ldots, t$; así tenemos que $g(X) = b_r X^r + b_{r-1}X^{r-1} + \cdots + b_0$ y $h(X) = c_s X^s + c_{s-1}X^{s-1} + \cdots + c_0$ satisfacen $f(X) = g(X)h(X)$. Recuerde que cada $b_{r,n}$ era igual a 1, por tal motivo $g(X)$ es mónico. Además, un proceso de inducción nos asegura por el ítem (c) que

$$|b_{j,1} - b_{j,n}|_p \leq p^{-1}, \text{ y luego } |b_{j,1} - b_j| \leq p^{-1},$$

para todo $j = 0, 1, \ldots, r$; esto es $g_1(X) \equiv g(X) \text{ mód } p^n$. De manera análoga, para $m = v_p(a_t + 1)$ se demuestra que $|h_m(X) - h(X)|_p \leq p^m$, y como $h_1(X) \equiv h_m(X) \text{ mód } p$ concluimos que $h_1(X) \equiv h(X) \text{ mód } p$, este último paso termina la prueba. □

Observación 5.3.6 Al igual que en el lema de Hensel, en este teorema podemos demostrar la unicidad de los elementos $g(X), h(X) \in \mathbb{Z}_p[X]$ mencionados. Para esto utilicemos el lema de Gauss para *d.f.u.*:

Si D es un *d.f.u.* entonces $D[X]$ también lo es.

Empecemos recordando que $(\mathbb{Z}_p, |\cdot|_p)$ es un dominio euclidiano, y por tal es un *d.f.u.*, así que $\mathbb{Z}_p[X]$ también lo será (puede ver esto en [3, capítulo 2, sección 3, teorema 1]). Así también notemos que es probable que $g(X)$ y $h(X)$ no sean coprimos en $\mathbb{Z}_p[X]$, pero esto en realidad si ocurre. En efecto, al ser $d(X) \in \mathbb{Z}_p[X]$ es un divisor común de $g(X)$ y $h(X)$, tendremos que el coeficiente principal de $d(X)$ es un elemento invertible de $\mathbb{Z}_p$, por tanto grad $d(X) =$ grad $\pi d(X)$. Por otra parte $\pi d(X) \in \mathbb{F}_p[X]$ será un divisor común de $\pi g(X) = \pi g_1(X)$ y $\pi h(X) = \pi h_1(X)$, por lo cual es una constante; por lo tanto concluimos que mcd $(g(X), h(X)) = 1$.

Ahora, supongamos $g_0(X), h_0(X) \in Z_p[X]$ también cumplen las condiciones del teorema anterior, entonces análogamente mcd $\big(g_0(X), h_0(X)\big) = 1$. De manera similar, si $t(X) \in \mathbb{Z}_p[X]$ es un factor irreductible de $g(X)$ y $l(X) = t(X)^e$ es la mayor potencia que divide a $g(X)$, entonces $l(X)$ tiene como coeficiente principal a una unidad de $\mathbb{Z}_p$, por tanto grad $l(X) =$ grad $\pi l(X)$. Esto implica que $\pi l(X)$ es un factor no trivial de $\pi g_1(X)$, luego $\pi l(X)$ no es un factor de $\pi h_1(X) = \pi h_0(X)$; así concluimos que $l(X) \nmid h_0(X)$. Como $l(X) \mid f(X) = g_0(X)h_0(X)$, y $t(X)$ es irreductible (por tanto primo) concluimos que $l(X) \mid g_0(X)$. De esta manera obtenemos

$$\big(g(X)/l(X)\big)h(X) = f(X)/l(X) = \big(g_0(X)/l(X)\big)h_0(X),$$

y como el lado derecho no presenta ningun factor irreducible asociado a $t(X)$, entonces el lado izquierdo tampoco debe tenerlo, lo que prueba que $l(X)$ es la mayor potencia de $t(X)$ que divide a $g_0(X)$, con esto concluimos que $g(X)$ y $g_0(X)$ presentan la misma descomposición en factores irreducibles en $\mathbb{Z}_p[X]$, luego $g(X) = cg_0(X)$ con $c \in \mathbb{Z}_p^\times$, y como ambos son mónicos, estos deben ser iguales; con esto tendremos que $h(X) = h_0(X)$, y la unicidad de $g(X)$ y $h(X)$ está comprobada.

Ahora mostraremos la aplicación más importante en este trabajo de esta segunda versión del lema de Hensel, que será de vital importancia en el siguiente capítulo.

Lema 5.3.7 *Sea* $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Q}_p[X]$ *irreductible. Si* $a_0 \in \mathbb{Z}_p$, *entonces* $f(X) \in \mathbb{Z}_p[X]$.

Demostración.- Por reducción al absurdo, supongamos que algún $a_j \notin \mathbb{Z}_p$. Por tal motivo $r = \min\{v_p(a_j),\ j = 0,1,\ldots,n\}$ es un entero negativo. Tomemos $k = \min\{j,\ v_p(a_j) = r\}$ que debe cumplir $0 < k < n$, puesto que $f(X)$ es mónico y $a_0 \in \mathbb{Z}_p$. Si escogemos $t(X) = p^{-r}f(X) = b_nX^n + \cdots + b_1X + b_0$, obtendremos que:

- para cada $j \in \{0,1,\ldots,n\}$ se tiene que $v_p(b_j) = v_p(a_j) - r \geq 0$;
- para cada $j \in \{0,1,\ldots,k-1\}$ se cumple que $v_p(b_j) > 0$ y $v_p(a_k) = 0$.

Por lo tanto $t(X) \in \mathbb{Z}_p[X]$ y

$$t(X) \equiv b_nX^n + b_{n-1}X^{n-1} + \cdots + b_kX^k \equiv g(X)h(X) \text{ mód } p,$$

donde $g(X) = X^k$ y $h(X) = b_nX^{n-k} + \cdots + b_k$. Nótese que mcd $\big(\pi g(X), \pi h(X)\big) = 1$, pues el único factor irreducible de $\pi g(X)$ es πX, el cual no lo es de $\pi h(X)$, puesto que esto indicaría que $0+p\mathbb{Z}_p$ es una raíz de $\pi h(X)$, y este polinomio tiene coeficiente independiente $b_0+p\mathbb{Z}_p \neq 0+p\mathbb{Z}_p$. Con esto presente, podemos utilizar el teorema 5.3.5 para obtener $g_0(X), h_0(X)$ tales que

(i) $g_0(X)$ es mónico y $g_0(X) \equiv X^k$ mód p;

(ii) $t(X) = g_0(X)h_0(X)$.

Por (i) tendremos que grad $g_0(X)$ será igual a k, luego $t(X)$ tendrá un factor no trivial y $f(X)$ será reducible en $\mathbb{Q}_p[X]$ (lo que es absurdo), luego es necesario que $f(X) \in \mathbb{Z}_p[X]$. □

El segundo aporte de la segunda forma del lema de Hensel a este trabajo necesitará de una suerte de lema de Gauss para números p-ádicos.

Lema 5.3.8 *Si $f(X) \in \mathbb{Z}_p[X]$ tiene una factorización no trivial en $\mathbb{Q}_p[X]$, entonces también tiene una factorización no trivial en $\mathbb{Z}_p[X]$.*

Demostración.- Para demostrar este lema construiremos una factorización no trivial de $f(X)$ en $\mathbb{Z}_p[X]$ a partir de una factorización en $\mathbb{Q}_p[X]$, para esto utilizaremos la proposición 4.1.6 tomando la valuación $w_p : \mathbb{Q}_p[X] \to \mathbb{R} \cup \{+\infty\}$ definida por

$$w_p(a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0) = \min\{v_p(a_i); i = 0,1,\ldots,n\}.$$

Lo más importante a observar es que dado $h(X) \in \mathbb{Q}[X]$, se tiene que $w_p\big(f(X)\big) \geq 0$ si y sólo si $f(X) \in \mathbb{Z}_p[X]$. Ahora, supongamos que $f(X) = g(X)h(X)$ con $0 <$ grad $g(X) <$ grad $f(X)$ y $0 <$ grad $h(X) < n$, entonces $w_p\big(f(X)\big) = w_p\big(g(X)\big) + w_p\big(h(X)\big)$. Luego, si denotamos

$n = w_p\big(g(X)\big)$ y $m = w_p\big(h(X)\big)$, tendremos que $n + m \geq 0$. Tomando $g_0(X) = p^{-n}g(X)$ y $h_0(X) = p^n h(X)$, se tiene que

$$w_p\big(g_0(X)\big) = -n + w_p\big(g(X)\big) = 0 \quad \text{y} \quad w_p\big(h_0(X)\big) = n + w\big(h(X)\big) \geq 0,$$

esto es, $g_0(X), h_0(X) \in \mathbb{Z}_p[X]$, que factorizan de manera no trivial a $f(X)$.

Corolario 5.3.9 *Sea $f(X) \in \mathbb{Z}_p[X]$ mónico. Si $\pi_1 f(X)$ es irreductible en $\mathbb{F}_p[X]$ (coreferencia a la proposición 5.1.15), entonces $f(X)$ es irreductible en $\mathbb{Q}_p[X]$.*

Demostración.- Realicemos la prueba por reducción al absurdo, asumiendo que existen $g(X)$, $h(X) \in \mathbb{Q}_p[X]$ no constantes tales que $f(X) = g(X)h(X)$. Por el lema anterior, podemos asumir que $g(X), h(X) \in \mathbb{Z}_p[X]$; como $f(X)$ es mónico concluimos que $g(X)$ y $h(X)$ tienen coeficientes principales que son unidades en $\mathbb{Z}_p$ (pues uno será el inverso multiplicativo del otro). Por lo tanto $\pi_1 g(X)$ y $\pi_1 h(X)$ tendrán el mismo grado que $g(X)$ y $h(X)$, respectivamente, y factorizarán de manera no trivial a $\pi_1 f(X)$, lo que es absurdo; por lo tanto $f(X)$ es irreductible en $\mathbb{Q}_p[X]$. □

Capítulo 6

Extensiones algebraicas de $\mathbb{Q}_p$

Nuestro objetivo en este capítulo es construir el cuerpo $\mathbb{C}_p$ que es una extensión de $\mathbb{Q}_p$, analaga a $\mathbb{C}$ para $\mathbb{Q}$, esto es, una extensión que sea completa y a la vez cerrada algebraica. Empezaremos estudiando espacios normados sobre un cuerpo completo, los cuales son una la generalización adecuada para obtener resultados de extensiones algebraicas de $\mathbb{Q}_p$ que posean un valor absoluto extendiendo a $|\cdot|_p$, puesto que un valor absoluto es un caso muy particular de norma.

6.1. Espacios normados

En esta sección denotaremos por $(K, |\cdot|)$ a un cuerpo completo, arquimediano o no, y nos restringiremos a K-espacios vectoriales.

Definición 6.1.1 Sea V un K-espacio vectorial, decimos que $\|\cdot\| : V \to \mathbb{R}$ es una norma sobre V si

1. Dado $v \in V$, $\|v\| = 0$.
2. Dado $v \in V$, $\|v\| = 0$ si y sólo $v = 0$.
3. Dados $v \in V$ y $\lambda \in K$ se cumple $\|\lambda v\| = |\lambda|\|v\|$.
4. Dados $v, w \in V$ se tiene que $\|v + w\| \leq \|v\| + \|w\|$.

Ejemplos 6.1.2 Supongamos que V es un $k-e.v.$ y $v_1, v_2, \ldots, v_n \in V$ una base de V. Con esto presente, dado $v \in V$, existen $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ tales que $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$, que además son los únicos escalares que satisfacen esta ecuación, por tanto las siguientes definiciones seran buenas.

- $\|v\|_0 = \max\{|\lambda_1|, |\lambda_2|, \ldots, |\lambda_n|\}$.
- $\|v\|_1 = |\lambda_1| + |\lambda_2| + \cdots + |\lambda_n|$.

Como en el caso real, es fácil demostrar que $\|\cdot\|_0, \|\cdot\|_1$ son normas en V.

Al igual que en el caso de valor absoluto, una norma $\|\cdot\|$ nos induce una métrica d en V definida por $d(x,y) = \|x-y\|$, es por ello que establecemos la siguiente definición.

Definición 6.1.3 Diremos que $(V, \|\cdot\|)$ es completo si es completo con la métrica inducida por $\|\cdot\|$.

Ejemplo 6.1.4 Con las notaciones del ejemplo anterior, tenemos que $(V, \|\cdot\|_0)$ es un espacio metrico completo. En efecto, tomemos una sucesión de Cauchy $(w_m)_{m\in N} \subset V$ y veamos que converge en V. Para cada $m \in \mathbb{N}$ tomemos $\lambda_{1,m}, \lambda_{2,m}, \ldots, \lambda_{n,m} \in K$ tales que

$$w_m = \lambda_{1,m}v_1 + \lambda_{2,m}v_2 + \cdots + \lambda_{n,m}v_n.$$

Procederemos a demostrar que $(\lambda_{i,m})_{m\in\mathbb{N}}$ es de Cauchy para $i = 1, 2, \ldots, n$. Dado $\epsilon > 0$, existe $m_0 \in \mathbb{N}$ tal que $\|w_r - w_s\| < \epsilon$, para todo $r, s \geq m_0$. Entonces, para $i = 1, 2, \ldots, n$ tendremos que

$$|\lambda_{i,r} - \lambda_{i,s}| \leq \max\{|\lambda_{1,r} - \lambda_{1,s}|, |\lambda_{2,r} - \lambda_{2,s}|, \ldots, |\lambda_{n,r} - \lambda_{n,s}|\} < \epsilon,$$

cuando $r, s \geq m_0$. Como K es completo, cada sucesión $(\lambda_{i,m})$ converge a algún $\lambda_i \in K$, con lo cual definimos que $w = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n \in V$. Concluiremos lo afirmado, mostrando que $\lim_m w_m = w$; para esto basta observar que

$$\|w_m - w\| = \max\{|\lambda_{1,m} - \lambda_1|, |\lambda_{2,m} - \lambda_2|, \cdots, |\lambda_{n,m} - \lambda_n|\}$$

y que el miembro derecho de esta desigualdad tiende a cero.

Definición 6.1.5 Dados $\|\cdot\|_1$ y $\|\cdot\|_2$ normas en V, un K-espacios vectoriales, diremos que estas son equivalentes si existen $C, D > 0$ tales que

$$C\|x\|_1 < \|x\|_2 < D\|x\|_1; \quad \text{para todo } x \in V.$$

Ejemplo 6.1.6 En las notaciones de los ejemplos 6.1.2, tendremos que $\|\cdot\|_1$ y $\|\cdot\|_2$ son normas equivalentes. En efecto, dado $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$ ocurre que

$$\|v\|_0 \leq \|v\|_1 \leq \sum_{k=1} \|v\|_0 = n\|v\|_0.$$

Con igual facilidad se puede comprobar las siguientes equivalencias.

Proposición 6.1.7 *Sean V un K-espacios vectorial con normas $\|\cdot\|_1, \|\cdot\|_2$ y $(v_n)_{n\in\mathbb{N}} \subset V$. Si $\|\cdot\|_1$ y $\|\cdot\|_2$ son equivalentes, se cumple*

- *La sucesión (x_n) es de Cauchy respecto a $\|\cdot\|_1$ si y sólo si lo es respecto a $\|\cdot\|_2$.*
- *La sucesión (x_n) converge a $x \in V$ respecto a $\|\cdot\|_1$ si y sólo si converge a x respecto a $\|\cdot\|_2$.*

En consecuencia, $(V, \|\cdot\|_1)$ es completo si y sólo si $(V, \|\cdot\|_2)$ lo es.

Observación 6.1.8 En un espacio vectorial, motivados por la proposición anterior, podemos definir la relación $\|\cdot\|_1 \sim \|\cdot\|_2$ si $\|\cdot\|_1$ y $\|\cdot\|_2$ son equivalentes, es una relación de equivalencia. Esta noción de equivalencia es muy importante, puesto que separa a las normas entre si o bien la reune. Veamos que en el caso finito dimensional no existe "demasiada variedad" respecto a las normas existentes.

Teorema 6.1.9 *En cualquier K-espacio vectorial de dimensión finita, todas las normas son equivalentes entre si.*

Demostración.- Empecemos por demostrar que todo espacio unidimensional cumple el teorema. En efecto, si V es generado por v_0 y $\|\cdot\|_1$ y $\|\cdot\|_2$ son normas sobre V, entonces $\|v_0\|_1$ y $\|v_0\|_2$ son no nulos. Tomando $C = \|v_0\|_1/\|v_0\|_2 > 0$ y $D = \|v_0\|_2/\|v_0\|_1 > 0$ se satisface

$$C\|v\|_2 = \|v\|_1 = D\|v\|_2, \text{ para todo } v = \lambda v_0, \text{ con } \lambda \in K.$$

Ahora, si suponemos que no es cierto el teorema, existira $n \geq 2$ el menor número natural tal que este teorema sea falso para espacios de dimensión finita; por ello poder tomar V un $K-$espacio vectorial de dimensión n para el cual existan normas $\|\cdot\|_1$ y $\|\cdot\|_2$ sobre V, las cuales no sean equivalentes.

Sea $\{v_1, v_2, \ldots, v_n\} \subset\in V$ una base, y definamos $\|\cdot\|_0$ como en los ejemplos 6.1.2. Ahora, si $\|\cdot\|_1$ y $\|\cdot\|_2$ fueran equivalentes a $\|\cdot\|_0$, entonces por la observación anterior, tendriamos que éstas son equivalentes entre sí; por lo tanto al menos una de estas no lo es, y sin perdida de generalidad, supondremos que $\|x\|_1$ no es equivalente a $\|\cdot\|_0$. Vemos que todo $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$, cumple que

$$\|v\|_1 \leq \sum_{i=1} |\lambda_i| \|v_i\|_1 \leq n\|v\|_0 \max_{1\leq i\leq n} \{v_i\}_1 = C\|v\|_0,$$

donde $c = n\,\text{máx}\{\|v_i\|_1; i = 1, 2, \ldots, n\}$. Asi concluimos que se satisface $1/C\|v\|_1 \leq \|v\|_0$, para todo $v \in V$; como estas normas no son equivalentes, deducimos que no existe $D > 0$ tal que $\|v\|_0 \leq D\|v\|_1$ para todo $v \in V$. Por ello podemos construir una sucesión $(w_n) \subset V$ tal que

$$\|v\|_1 < 1/m\|v\|_0, \quad \text{para todo } m \in \mathbb{N}.$$

Es fácil ver que esta condición garantiza que ningun w_n sea nulo. Para cada $m \in \mathbb{N}$ escribamos $w_m = \lambda_{1,m}v_1 + \cdots + \lambda_{n,m}v_n$, y definamos

$$\mathcal{M}_i = \{m \in \mathbb{N}; |\lambda_{i,m}| = \|w_m\|_0\} \qquad \text{para cada } i = 1, 2, \ldots n.$$

Como $\mathbb{N} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \cdots \cup \mathcal{M}_n$, tendremos que al menos uno de estos conjuntos es infinito, el cual podemos suponer que es $\mathcal{M}_n$, de lo contrario podemos renombrar a los vectores v_i's y obtener dicho caso. Luego, escribamos $\mathcal{M}_n = \{m_1, m_2, \ldots, m_k, \ldots\}$ en orden ascendente; de esta forma $|\lambda_{n,m_k}| = \|w_{m_k}\|_0 > 0$, para todo $k \in \mathbb{N}$. Entonces, para cada $k \in \mathbb{N}$ se tiene

$$\lambda_{n,m_k}^{-1} w_{m_k} = (\lambda_{1,m_k}/\lambda_{n,m_k})v_1 + \cdots + (\lambda_{1,m_k}/\lambda_{n,m_k}v_{n-1}) + v_n = u_k + v_n,$$

donde u_k es la suma de de los $n-1$ primeros sumandos, por lo cual cada u_k pertencerá al subsespacio generado por $\{v_1, v_2, \ldots, v_{n-1}\}$ que denotamos por $\mathcal{W}$. En estos términos tenemos

$$\|u_k + v_n\|_1 < 1/m_k, \quad \text{para todo } k \in \mathbb{N}.$$

Entonces, la sucesión (u_k) convergerá en $\|\cdot\|_1$ a $-v_n$, así como que la sucesión $(u_k)_{k\in\mathcal{W}}$ es de Cauchy respecto a $\|\cdot\|_1$.

Por otro lado, la minimalidad de n nos implica que en el $K-$espacio vectorial $\mathcal{W}$ de dimensión $n-1$, las restricciones de $\|\cdot\|_1$ y $\|\cdot\|_0$ seran normas equivalentes. Recordando la proposición 6.1.7, inferimos que (u_k) es de Cauchy respecto a $\|\cdot\|_0$, y por el ejemplo 6.1.4 concluimos que la sucesión (u_k) converge a algún $u \in \mathcal{W}$ respecto a $\|\cdot\|_0$. Por la equivalencia de $\|\cdot\|_0$ y $\|\cdot\|_1$ en $\mathcal{W}$, deducimos que (u_k) converge a u en $\|\cdot\|_1$, por lo tanto

$$\|u - (-v_n)\| \leq \|u - u_k\|_1 + \|u_k + v_n\|_1; \qquad \text{para todo } k \in \mathbb{N}.$$

Esta última desigualdad es motivo por el cual $v = -u \in \mathcal{W}$, lo que contradice la independencia lineal de la base establecida, y como este absurdo se produjo por suponer la existencia de n, concluimos que el teorema era cierto. □

6.2. Extensión de $|\cdot|_p$

Nuestro objetivo en esta sección será extender $|\cdot|_p$ a extensiones finitas de $\mathbb{Q}_p$, esto es dado $K/\mathbb{Q}_p$ finita encontrar alguna función $\|\cdot\| : K \to \mathbb{R}$ sobre tal que

- La función $\|\cdot\|$ es un valor absoluto sobre K.
- Para cada $x \in \mathbb{Q}_p$, $\|x\| = |x|_p$.

Para este fin, empecemos por asumir su existencia y mostrar la unicidad de esta extensión, lo cual nos ayudara para encontrar un candidato a este valor absoluto.

Proposición 6.2.1 *En una extensión finita de $\mathbb{Q}_p$, a lo mas existe una extensión de $|\cdot|_p$.*

Demostración.- Sean $K/\mathbb{Q}_p$ finita, $\|\cdot\|_1$ y $\|\cdot\|_2$ valores abslutos sobre K que extienden a $|\cdot|_p$. Puesto que estas funciones son normas sobre K como un $\mathbb{Q}_p$-espacio vectorial y $\mathbb{Q}_p$ es completo, deducimos que estos valores absolutos son equivalentes como normas; procedamos a verificar que también lo son comó valores absolutos.

Dado $x \in K$ con $\|x\|_1 < 1$, se tendra que la sucesión $(x^n)_{n\in\mathbb{N}} \subset K$ converge a 0 respecto $\|\cdot\|_1$; luego, por la proposición 6.1.7, obtendremos que (x^n) converge a 0 respecto $\|\cdot\|_2$, lo cual implica que $\|x^m\|_2 < 1$ para algún $m \in \mathbb{N}$, y de ahi que $\|x\|_2 < 1$. Análogamente podemos demostrar lo recíproco. Entonces, por la proposición 4.2.12 existirá $\alpha > 0$ tal que $\|x\|_1 = \|x\|_2^\alpha$, para todo $x \in K$, en particular

$$p^{-1} = |p|_p = \|p\|_1 = \|p\|_2^\alpha = |p|_p^\alpha = p^{-\alpha}.$$

Así concluimos que $\alpha = 1$ y que los valores absolutos son identicos. □

Otra aplicación importante de la proposición 6.1.7, aunque no apunta a nuestro objetivo, es la siguiente proposición.

Proposición 6.2.2 *Si $K/\mathbb{Q}_p$ es finita y $\|\cdot\|$ es una extensión de $|\cdot|_p$, entonces el cuerpo $(K, \|\cdot\|)$ es completo*

Demostración.- Puesto que en estas condiciones K es un $\mathbb{Q}_p$-espacio normado deducimos que es un espacio normado completo. □

Construyamos ahora la anunciada extensión de $|\cdot|_p$, para esto empecemos por tomar una extensión L que sea normal y finita sobre $\mathbb{Q}_p$ y que posea un valor absoluto $\|\cdot\|$ que extiende $|\cdot|_p$. Entonces, dado $\sigma \in G(L/\mathbb{Q}_p)$ vemos claramente que $\|\sigma(\cdot)\|$ define un valor absoluto que extiende a $|\cdot|_p$; por tanto $\|\sigma(\cdot)\|$ debe coincidir con $\|\cdot\|$ (por la proposición 6.2.1). Como $G(L/\mathbb{Q}_p)$ tiene cardinalidad $n = [L : \mathbb{Q}_p]$, para cada $a \in L$ se cumple que

$$\|a\|^n = \prod_{\sigma\in G(L/\mathbb{Q}_p)} \|\sigma(a)\| = \| \prod_{\sigma\in G(L/\mathbb{Q}_p)} \sigma(a)\| = \|N_{L/\mathbb{Q}_p}(a)\| = |N_{L/\mathbb{Q}_p}(a)|_p,$$

pues $N_{L/\mathbb{Q}_p}(a) \in \mathbb{Q}_p$ (como mencionamos en la observación 3.9.2); por lo tanto $\|\cdot\| = \sqrt[n]{|N_{L/\mathbb{Q}_p}(\cdot)|_p}$. Así pues, de existir un valor absoluto sobre L que extienda al $p-$ádico, aquel

debe tener esa forma; nótese que este tipo de función extiende a $|\cdot|_p$, pues dado $a \in \mathbb{Q}_p$, tenemos que

$$\|a\| = \sqrt[n]{|N_{L/\mathbb{Q}_p}(a)|_p} = \sqrt[n]{|a^n|_p} = \sqrt[n]{|a|_p^n} = |a|_p.$$

Finalmente, no supongamos que $L/\mathbb{Q}_p$ sea normal y tomemos F una clausura normal de $L/\mathbb{Q}_p$, la cual sera una extensión normal y finita sobre $\mathbb{Q}_p$ (vea el teorema 3.7.11), escribamos $m = [F : \mathbb{Q}_p]$. Nuevamente, asumamos que existe un valor absoluto $\|\cdot\|_1 : F \to \mathbb{R}$ extendiendo a $|\cdot|_p$, entonces $\|\cdot\|_1$ restringido a L nos brindará un valor absoluto (extendiendo al $p-$ádico), por lo cual $\|\cdot\|_1$ necesariamente coincide con $\|\cdot\|$ sobre L, esto es

$$\|a\| = \|a\|_1 = \sqrt[m]{|N_{F/\mathbb{Q}_p}(a)|_p}, \quad \text{para cada } a \in L.$$

Como $m = [F : \mathbb{Q}_p] = [F : L][L : \mathbb{Q}_p] = [F : L]n$, tendremos que todo $a \in L$ cumple

$$\|a\| = |N_{F/L}(N_{L/\mathbb{Q}_p}(a))|_p^{\frac{1}{[F:L]n}} = |(N_{L/\mathbb{Q}_p}(a))^{[F:L]}|_p^{\frac{1}{[F:L]n}} = \sqrt[n]{|(N_{L/\mathbb{Q}_p}(a))|_p},$$

esto comprueba que toda posible extensión del valor absoluto presenta esa forma.

Resumimos y concluimos este análisis un teorema.

Teorema 6.2.3 *Sea L una extensión sobre $\mathbb{Q}_p$ de grado $n \in \mathbb{N}$, entonces existe un único valor absoluto $\|\cdot\|$ que extiende $|\cdot|_p$, que es dado por*

$$\|a\| = \sqrt[n]{|(N_{L/\mathbb{Q}_p}(a))|_p}, \quad \textit{para todo } a \in L.$$

Demostración.- En el razonamiento previo obtuvimos este candidato, ahora resta verificar que es un valor absoluto sobre L. Vemos con facilidad que $\|\cdot\|$ satisface las primeras tres cualidades de la definición 4.2.1 (acerca de valores absolutos); procedamos a garantizar que

$$\|a + 1\| \leq \text{máx}\{\|a\|, 1\}, \quad \text{para todo } a \in L,$$

que como hemos visto en las observaciones 4.2.3, es suficiente para garantizar que $\|\cdot\|$ es un valor absoluto no arquimediano. Supongamos que $\|a\| \leq 1$, entonces por definición $|N_{L/\mathbb{Q}_p}(a)|_p \leq 1$. Luego, si escribimos

$$f(X) = \text{Irr}\,(\mathbb{Q}_p, a) = X^r + c_{r-1}X^{r-1} + \cdots + c_0,$$

por el teorema 3.9.1 tendremos que

$$|c_0|_p^{[L:\mathbb{Q}_p(a)]} = |((-1)^r c_0)^{[L:\mathbb{Q}_p(a)]}|_p = |N_{L/\mathbb{Q}_p}(a)|_p \leq 1,$$

por tanto $|c_0|_p \leq 1$. Asi vemos que el polinomio minimal de a tiene término constante en $\mathbb{Z}_p$, luego, en virtud del lema 5.3.7 tendremos que $c_1, c_2, \ldots, c_{r-1} \in \mathbb{Z}_p$. Como $f(X - 1)$ es un

polinomio mónico e irreductible que se anula en $a+1$, tendremos que $\mathrm{Irr}\,(K, a+1) = f(F-1)$. Este polinomio posee término constante

$$(-1)^r + c_{r-1}(-1)^{r-1} + \cdots + c_1(-1) + c_0 \in \mathbb{Z}_p;$$

por tanto $N_{L/\mathbb{Q}_p}(a) \in \mathbb{Z}_p$ y, en consecuencia, $\|a+1\| \leq 1$. En el caso que $\|a\| > 1$, tedremos que $\|a^{-1}\| < 1$ y $\|a^{-1}+1\| \leq \max\{\|a^{-1}\|, 1\}$; de ahí que $\|1+a\| \leq \max\{1, \|a\|\}$; con esto queda demostrado que $\|\cdot\|$ es un valor absoluto no arquimediano. □

Definición 6.2.4 Dada L una extensión sobre $\mathbb{Q}_p$ de grado n, definimos el valor absoluto p-ádico $|\cdot|_p$ por

$$|a|_p = \sqrt[n]{|(N_{L/\mathbb{Q}_p}(a))|_p}, \quad \text{para todo } a \in L.$$

Observaciones 6.2.5 Supongamos que L es una extensión finita de $\mathbb{Q}_p$.

- Todo $\sigma \in G(L/\mathbb{Q}_p)$ es una isometria de L. De hecho, $|\sigma(\cdot)|_p$ es otro valor absoluto sobre L que extiende a $|\cdot|$, por tanto $|\cdot| = |\sigma(\cdot)|_p$ y $|a|_p = |\sigma(a)|_p$ para todo $a \in L$.
- Del análisis previo, tenemos que si L y M son extensiones finitas sobre $\mathbb{Q}_p$ tales que $L \subset M$, entonces el valor absoluto p-ádico sobre L es la restricción en L del valor absoluto p-ádico sobre M.
- *Si $a, b \in L$ son $\mathbb{Q}_p$-conjugados, entonces $|a|_p = |b|_p$.* En efecto, tomando N una clausura normal de $L/\mathbb{Q}_p$, tendremos que el $\mathbb{Q}_p$-isomorfismo σ entre $\mathbb{Q}_p(a)$ y $\mathbb{Q}_p(b)$ que asigna b a a, se puede extender a un un $\mathbb{Q}_p-$automorfismo τ de N, luego $|a|_p = |\tau(a)|_p = |\sigma(a)|_p = |b|_p$.

Ejemplos 6.2.6 A continuación construiremos extensiones finitas de $\mathbb{Q}_p$ tomando ceros de polinomios cuadraticos que no se anulan en $\mathbb{Q}_p$, razon por la cual estos seran irreductibles.

$F_1 = \mathbb{Q}_5(\sqrt{3})$ Veamos que es imposible la existencia de un elemento $\alpha \in \mathbb{Q}_5$ tal que $\alpha^2 = 3$, asumamos esto y encontremos una contradicción. Si $\alpha^2 = 3$ entonces $|\alpha|_5 = 1$ y $\alpha \in \mathbb{Z}_5$; por tanto es admisible la existencia de $a \in \mathbb{Z}$ tal que $a \equiv \alpha \bmod 5$, lo que implica $a^2 \equiv 3 \bmod 5$ con $a \in \mathbb{Z}$ (imposible). Luego $f_1(X) = X^2 - 3 \in \mathbb{Q}_5[X]$ no tendra raíces y será irreductible; por tanto tomando $F_1 = \mathbb{Q}_5(u)$ un cuerpo que contiene una raíz u de $f_1(X)$ tendremos que $f_1(X) = \mathrm{Irr}\,(\mathbb{Q}_5, u)$ y $[F_1 : \mathbb{Q}_5] = 2$.

$F_2 = \mathbb{Q}_7(\sqrt{7})$ En general, si $p \in \mathbb{N}$ primo entonces no existe $u \in \mathbb{Q}_p$ tal que $u^2 = p$, pues de haberlo se tiene $2v_p(u) = v_p(u^2) = 1$ y $v_p(u) \notin \mathbb{Z}$. En particular, tomando $F_2 = \mathbb{Q}_7(u)$ tendremos que $\mathrm{Irr}\,(\mathbb{Q}_7, u) = X^2 - 7$ y $[F_2 : \mathbb{Q}_7] = 2$.

$F_3 = \mathbb{Q}_3(\zeta, \sqrt{5})$ Empecemos por mostrar que no existen raíces de la unidad distintas a 1 en $\mathbb{Q}_3$. Supongamos que $u \in \mathbb{Q}_3 \setminus \{1\}$ tal que $u^3 = 1$. Entonces $|u|_3 = 1$, de ahi que u es de la forma $u = a + 3b$ con $a \in 1, 2$ y $b \in \mathbb{Z}_p$. Pero al ser u distinta de 1, tendremos que $u^2 + u + 1 = 0$, lo cual no se satisface porque

$$(1 + 3b)^2 + (1 + 3b) + 1 \equiv 3 + 9b + b^2 \equiv 3 \text{ mód } 9, \quad \text{si } a = 1$$

y

$$(2 + 3b)^2 + (2 + 3b) + 1 \equiv 1 + 2 + 1 \equiv 1 \text{ mód } 3, \quad \text{si } a = 2.$$

De esta forma $g_3(X) = X^2 + X + 1 \in \mathbb{Q}_3[X]$ es irreductible, luego tomando $L = \mathbb{Q}_3(\zeta)$ un cuerpo con una raíz ζ de $g_3(X)$, obtenemos que $\text{Irr}\,(\mathbb{Q} - 3, \zeta) = g_3(X)$ y $[\mathbb{Q}_3(\zeta), \mathbb{Q}_3] = 2$. El siguiente paso será mostrar la inexistencia de raíces de cuadradas de 5 en $\mathbb{Q}_3(\zeta)$. Supongamos que existe $\alpha \in \mathbb{Q}_3(\zeta)$ tal que $\alpha^2 = 5$; escogiendo $a, b \in \mathbb{Q}_3$ que satisfagan $\alpha = a + b\zeta$ obtendremos $a^2 + 2ab\zeta + b^2\zeta^2 = 5$. Puesto que $\zeta^2 + \zeta + 1 = 0$, se tiene que $(a^2 - b^2 - 5)1 + (2ab - b^2)\zeta = 0$, luego se tiene que $a^2 - b^2 = 5$ y $b(2a - b) = 0$. Si b fuese nulo, entonces $a^2 = 5$ con $a \in \mathbb{Q}_3$, lo que es imposible (por motivos similares al primer caso). Entonces $2a = b$ y $-3b^2 = 5$, lo que nos da $v_p(b) = 1/2(v_p(5) - v_p(-3)) = 1/2 \notin \mathbb{Z}_3$. Por lo tanto $X^2 - 5 \in \mathbb{Q}_3(\zeta)$ es irreductible y $[\mathbb{Q}_3(\zeta, \alpha) : \mathbb{Q}_3] = [\mathbb{Q}_3(\zeta, \alpha) : \mathbb{Q}_3(\zeta)][\mathbb{Q}_3(\zeta) : \mathbb{Q}_3] = 4$.

Ahora, calculemos las extensiones de $|\cdot|_p$ en uno de estos cuerpos, los cuales mostraremos que son extensiones normales sobre $\mathbb{Q}_p$, por tanto este calculo se basará en encontrar su grupo de Galois, y con él su norma sobre $\mathbb{Q}_p$.

$F_1 = \mathbb{Q}_5(\sqrt{3})$ Es claro que F_1 es un *c.e.* de $x^2 - 3$ sobre $\mathbb{Q}_5$, por tanto es una extensión normal sobre $\mathbb{Q}_5$, y $\#G(F_1/\mathbb{Q}_5) = 2$ (por el corolario 3.8.8). Más aún, como F_1 es una extensión simple de $\mathbb{Q}_5$, los automorfismos quedan determinados por sus evaluaciones de $\sqrt{3}$, las cuales deben de ser $\mathbb{Q}_5$–conjugados en F_1. Así $G(F_1/\mathbb{Q}_5) = \{\sigma_1, \sigma_2\}$ con σ_1, σ_2 determinados por $\sigma_1(\sqrt{3}) = \sqrt{3}$ y $\sigma_2(\sqrt{3}) = -\sqrt{3}$ (en este caso $\sigma_1 = \text{id}_{F_1}$). Luego, dados $a, b \in \mathbb{Q}_5$ se tiene que

$$|a + b\sqrt{3}|_5 = |\mathbb{N}_{F_1/\mathbb{Q}_5}(a + b\sqrt{3})|_5^{1/2} = |\sigma_1(a + b\sqrt{3})\sigma_2(a + b\sqrt{3})|_5^{1/2} = |a^2 - 3b^2|_5^{1/2}.$$

Asi por ejemplo, $|1 + \sqrt{3}|_5 = \sqrt{|-2|_5} = 1$ y $|5 + 5\sqrt{3}|_5 = \sqrt{|-50|_5} = 1/5$.

$F_2 = \mathbb{Q}_7(\sqrt{7})$ De manera análoga al ítem anterior, obtenemos que $F_2/\mathbb{Q}_7$ es normal y que $G(F_2/\mathbb{Q}_7) = \{\tau_1, \tau_2\}$, donde τ_1, τ_2 son determinados por $\tau_1(\sqrt{7}) = \sqrt{7}$ y $\tau_2(\sqrt{7}) = -\sqrt{7}$.

Luego,

$$|a+b\sqrt{7}|_7 = |\mathbb{N}_{F_2/\mathbb{Q}_7}(a+b\sqrt{7})|_7^{1/2} = |\tau_1(a+b\sqrt{7})\tau_2(a+b\sqrt{7})|_7^{1/2} = |a^2-7b^2|_7^{1/2};$$

para todo $a, b \in \mathbb{Q}_7$. En particular $|10+\sqrt{7}|_7 = \sqrt{|93|_7} = 1$ y $|7+\sqrt{7}|_7 = \sqrt{|42|_7} = \sqrt{1/7}$.

$F_3 = \mathbb{Q}_3(\zeta, \sqrt{5})$ Notemos que ζ^2 también es una raíz de $g_3(x) = \text{Irr}\,(\mathbb{Q}_3, \zeta)$, pues $\zeta^4+\zeta^2+1 = \zeta+\zeta^2+1 = 0$; por lo que $\mathbb{Q}_3(\zeta, \sqrt{5})$ es un *c.e.* de $(x^2+x+1)(x^2-5)$ sobre $\mathbb{Q}_3$, así $F_3/\mathbb{Q}_3$ es normal. Por el corolario 3.8.8, se tiene que $\#G(F_3/\mathbb{Q}_3) = [F_3 : \mathbb{Q}_3] = 4$; procedamos a calcular este grupo de manera análoga al ejemplo 3.8.4, por ello los pasos tendran jusificaciones similares a las relizadas en el anterior ejemplo. En $\mathbb{Q}_3(\zeta)$ existen dos $\mathbb{Q}_3-$automorfismos, a decir τ_1, τ_2 determinados por $\tau_1(\zeta) = \zeta$ y $\tau_2(\zeta) = \zeta^2$, respectivamente. El primer $\mathbb{Q}_3$-automorfismo se puede extender sobre F_3 en dos automorfismos: $\tau_{1,1}$ y $\tau_{1,2}$ determinados por $\tau_{1,1}(\sqrt{5}) = \sqrt{5}$ y $\tau_{1,2}(\sqrt{5}) = -\sqrt{5}$. Igualmente, el automorfismo τ_2 se extiende sobre F_3 a $\tau_{2,1}$ y $\tau_{2,2}$ tales que $\tau_{2,1}(\sqrt{5}) = \sqrt{5}$ y $\tau_{2,2}(\sqrt{5}) = -\sqrt{5}$. Luego, si $a, b \in \mathbb{Q}_p(\zeta)$ entonces

$$\begin{aligned} |a+b\sqrt{5}|_3 &= |\prod_{i=1}^{2}\prod_{j=1}^{2}\tau_{i,j}(a+b\sqrt{5})|_3^{1/4} = \sqrt[4]{|(a^2-5b^2)(\tau(a)^2-5\tau(b)^2))|_3} \\ &= \sqrt[4]{|(a^2-5b^2)\tau(a^2-5b^2)|_3} = \sqrt[4]{|N_{\mathbb{Q}_3(\zeta)/\mathbb{Q}_3}(a^2-5b^2)|_3} \\ &= \sqrt{\sqrt{|N_{\mathbb{Q}_3(\zeta)/\mathbb{Q}_3}(a^2-5b^2)|_3} = \sqrt{|a^2-5b^2|_3}}; \end{aligned}$$

pues $\mathbb{Q}_3(\zeta)/\mathbb{Q}_3$ es normal y $G(\mathbb{Q}_3(\zeta)/\mathbb{Q}_3) = \{\text{id}, \tau\}$. Ya que este valor absoluto queda expresado en términos de $N_{\mathbb{Q}_3(\zeta)/\mathbb{Q}_3}$, es oportuno mencionar que

$$N_{\mathbb{Q}_3(\zeta)/\mathbb{Q}_3}(c+d\zeta) = (c+d\zeta)(c+d\zeta^2) = c^2+d^2\zeta^3+cd(\zeta+\zeta^2) = c^2+d^2-cd,$$

para todo $c, d \in \mathbb{Q}_3$. Así por ejemplo se tendrá

$$|1+\zeta|_3 = |N_{F_3/\mathbb{Q}_3}(1+\zeta)|_3^{1/4} = |(1+\zeta)^2|_3^{1/4} = |1+1+1|_3^{1/2} = 3^{-1/2}$$

y

$$|\zeta+\sqrt{5}|_3 = |N_{\mathbb{Q}_3(\zeta)/\mathbb{Q}_3}(\zeta^2-5)|_3^{1/4} = |N_{F_3/\mathbb{Q}_3}(-6-\zeta)|_3^{1/4} = |36+1-6|_3^{1/4} = 1^{1/4} = 1.$$

Estos dos últimos casos muestran que la imagen de $|\cdot|_p$ ya no esta contenida en $0 \cup \{p^n;\ n \in \mathbb{Z}\}$ como ocurrio cuando extendimos este valor absoluto de $\mathbb{Q}$ a $\mathbb{Q}_p$. Este hecho será el tema principal de la siguiente sección.

Si recordamos que toda clausura algebraica Ω de un cuerpo K se puede obtener por reunir todas las extensiones finitas sobre K (contenidas en la misma Ω), entonces la proposición anterior nos sugerirá que $|\cdot|_p$ se puede extender a una clausura algebraica de $\mathbb{Q}_p$.

Proposición 6.2.7 *El valor absoluto p−ádico $|\cdot|_p$ se puede extender a una clausura algebraica $\mathbb{Q}_p^{alg}$ sobre $\mathbb{Q}_p$ de manera única con la regla de correspondencia*

$$\|a\| = |N_{\mathbb{Q}_p(a)/\mathbb{Q}_p}(a)|_p^{1/[\mathbb{Q}_p(a):\mathbb{Q}_p]}, \qquad a \in \mathbb{Q}_p^{alg}.$$

Demostración.- Es claro que $\|\cdot\|$ cumple las dos primeras caracteristicas enunciadas en la definición 4.2.1 acerca de valor absoluto, veamos que $\|\cdot\|$ respeta el producto. Para esto forzaremos la notación escribiendo $|a|_{p|L}$ cuando nos referiramos a la extensión de $|\cdot|_p$ sobre L, una extensión finita de $\mathbb{Q}_p$ que contenga a a; por tanto $\|a\| = |a|_{p|\mathbb{Q}_p(a)}$, para todo $a \in \mathbb{Q}_p^{alg}$. Dados $a, b \in \mathbb{Q}_p^{alg}$ se tiene que

$$\begin{aligned} ||a \cdot b|| &= |a \cdot b|_{p|\mathbb{Q}_p(a\cdot b)} = |a \cdot b|_{p|\mathbb{Q}_p(a,b)} = |a|_{p|\mathbb{Q}_p(a,b)}|b|_{p|\mathbb{Q}_p(a,b)} \\ &= |a|_{p|\mathbb{Q}_p(a)}|b|_{p|\mathbb{Q}_p(b)} = \|a\|\|b\|; \end{aligned}$$

de forma análoga se demuestra la propiedad no arquimediana, por tanto $\|\cdot\|$ es un valor absoluto que extiende a $|\cdot|_p$. Más aun, $|\cdot|$ es otro valor absoluto que extiende a $|\cdot|_p$ sobre $\mathbb{Q}_p^{alg}$, entonces, para cada $a \in \mathbb{Q}_p^{alg}$, se tiene que $|a| = |a|_{\mathbb{Q}_p(a)} = |a|_{p|\mathbb{Q}_p(a)} = \|a\|$, puesto que existe un único valor absoluto extendiendo a $|\cdot|_p$ sobre $\mathbb{Q}_p(a)$; por lo tanto $|\cdot| = \|\cdot\|$ y $\|\cdot\|$ es único. □

De ahora en adelante tan sólo estudiaremos extensiones de algebraicas sobre $\mathbb{Q}_p$ contenida en esta clausura algebraica $\mathbb{Q}_p^{alg}$. Extenderemos el dominio de $|\cdot|_p$ sobre $\mathbb{Q}_p^{alg}$ con la regla de correspondencia escrita en la anterior proposición; de este modo "toda" extensión algebraica sobre $\mathbb{Q}_p$ posee un valor absoluto que extiende al p-ádico.

6.3. Índice de ramificación

Al igual que extendimos el valor absoluto $p-$ádico, ahora extenderemos la valuación $p-$adica para extensiones finitas de $\mathbb{Q}_p$, pero esta vez partiremos de la ya obtenida extensión de $|\cdot|_p$.

Sea L es una extensión de $\mathbb{Q}_p$ de grado n, por la proposición 4.2.5 podemos definir una valuación v sobre L tomando $v = \log_p(|\cdot|_p)$. Así pues, tendremos que

$$v(a) = -\log_p(|N_{L/\mathbb{Q}_p}(a)|_p^{1/n}) = -1/n \log_p(|N_{L/\mathbb{Q}_p}(a)|_p), \quad \text{para todo } a \in L^\times.$$

También podemos deducir que cada $a \in \mathbb{Q}_p^\times$ satisface $v(a) = -1/n \log_p(|a^n|_p) = v_p(a)$; esto es, v extiende a v_p. Verifiquemos que ésta será la única valuación sobre L que extiende a v_p. De hecho, si w es una valuación que extiende a v_p, definiendo $\|\cdot\| : L \to \mathbb{R}$ por $\|x\| = p^{-w(x)}$,

obtendremos un valor absoluto que extiende a $|\cdot|_p$ sobre L. De ahí que $\|\cdot\| = |\cdot|_p$ y en consecuencia

$$w(a) = -\log_p(\|a\|) = -\log_p(|a|_p) = v(a), \quad \text{para todo } a \in L^\times;$$

este hecho lo resumimos.

Definición 6.3.1 Sea L una extensión de $\mathbb{Q}_p$ de grado n. *La valuación $p-$adica sobre L*, denotado por v_p, es definida por $v_p(a) = -\log_p(|a|_p)$.

Observaciones 6.3.2 Asumiendo las anteriores notaciones establecemos los siguientes comentarios.

- La valuación $p-$ádica de un elemento no nulo x de una extensión de $\mathbb{Q}_p$ se puede entender como el único real y tal que $|x|_p = p^{-y}$.
- También podemos extender v_p sobre $\mathbb{Q}_p^{alg}$ por la misma definición y estará dotada de unicidad (esto se puede verificar por medio de los mismos pasos pasos que acabamos de hacer).
- Si $\alpha, \beta \in \mathbb{Q}_p^{alg}$ son $\mathbb{Q}_p-$conjugados, entonces $v_p(\alpha) = v_p(\beta)$.
- Si recordamos la definición de valuación $p-$ádica sobre $\mathbb{Q}_p$, podemos obtener que $v_p(a) = 1/nv_p(N_{L/K}(a))$, para todo $a \in L$.
- Podemos ver que $v_p(L^\times) \subset 1/n\mathbb{Z}$; más aun los dos últimos casos del ejemplo 6.2.6 nos muestran que ya no es cierto que $v_p(L^\times) \subset \mathbb{Z}$. Sin embargo, tenemos claro que $\mathbb{Z} \subset v_p(L^\times) \subset 1/n\mathbb{Z}$, por lo cual se puede esperar que el enunciado de la siguiente proposición sea verdadero.

Proposición 6.3.3 *Sea L una extensión sobre $\mathbb{Q}_p$ de grado n. Existe $e \in \mathbb{N}$ tal que $v_p(L^\times) = 1/e\mathbb{Z}$; en particular e es un divisor de n.*

Demostración.- Tomemos $e = \text{máx}\{m \in \mathbb{N}; 1/m \in v_p(L^\times)\}$, con el cual generamos el subgrupo aditivo $H = \{m/e; m \in \mathbb{Z}\} \subset v_p(L^\times)$; nuestra tarea será demostrar que $v_p(L^\times) \subset H$. Dado $q \in v_p(L^\times)$, podemos escribir q de la forma a/b con $a, b \in \mathbb{Z}$ coprimos con $b > 0$. Existen $s, t \in \mathbb{Z}$ tales que $sa + tb = 1$, entonces

$$\frac{1}{b} = \frac{sa + tb}{b} = s(\frac{a}{b}) + t \in v_p(L^\times),$$

pues $\mathbb{Z} \subset v_p(L^\times)$. Ahora deseamos mostrar que $1/b \in H$ (lo que será suficiente para verificar que $q \in H$), pero esto equivale a la existencia de $m \in \mathbb{Z}$ tal que $1/b = m/e$, lo cual no es más que $b \mid e$. Si esto no es cierto, entonces existen $q, r \in \mathbb{Z}$ que satisfacen $e = bq + r$ con $0 < r < b$; luego

$$\frac{r}{eb} = \frac{e - qb}{eb} = \frac{1}{b} - q\frac{1}{e} \in v_p(L^\times).$$

Escojamos $x, y \in \mathbb{Z}$ tales que $xr + yb = (b, r)$ (el maximo común divisor de r y b), para obtener que

$$x\frac{r}{eb} + y\frac{1}{e} = \frac{xr + yb}{eb} = \frac{(b, r)}{eb} \in v_p(L^\times).$$

Pero, por la definición de e tendremos que $e(b/(b, r)) \leq e$ y, en consecuencia, $b \leq (b, r) \leq r$ (contradi cción). Por tanto $m \mid b$, entonces $q \in H$. □

Definición 6.3.4 Sea L una extensión de $\mathbb{Q}_p$ de grado $n > 1$. *El índice de ramificación* $e = e(L)$ es aquel entero positivo que verifica $v_p(L^\times) = 1/e\mathbb{Z}$. Diremos que L es una *extensión ramificada* si $e > 1$; más aún la denominaremos *totalmente ramificada* si $e = n$. En el caso que $e = 1$, diremos que L es una extensión *no ramificada.*

Ejemplos 6.3.5 Tomemos en cuenta los ejemplos 6.2.6.

$F_1 = \mathbb{Q}_5(\sqrt{3})$: Es una extensión no ramificada, esto es $v_5(F_1^\times) = \mathbb{Z}$; esto significa que todo $\alpha \in \mathbb{F}_1^\times$ cumple $v_5(\alpha) \in \mathbb{Z}$, o lo mismo que $v_5(N_{F_1/\mathbb{Q}_5}(\alpha)) \in 2\mathbb{Z}$. Por reducción al absurdo, asumamos que existe α no nulo tal que $v_5(N_{F_1/\mathbb{Q}_5}(\alpha)) = 2m+1$ con $m \in \mathbb{Z}$. Si escribimos $\alpha = a + b\sqrt{3}$ con $a, b \in \mathbb{Q}_5$, podemos deducir que $v_5(a) = v_5(b)$. En efecto, en el caso que $v_5(a) < v_5(b)$ (por lo cual $a \neq 0$), tendremos que $v_5(a^2) = 2v_5(a) < 2v_5(b) = v_5(-3b^2)$ luego

$$2v_5(a) = \text{mín}\{v_5(a^2), v_5(-3b^2)\} = v_5(a^2 - 3b^2) = 2m + 1,$$

obteniendo que $v_5(a) \notin \mathbb{Z}$ con $a \in \mathbb{Q}_5^\times$; análogamente, en el caso $v_5(b) < v_p(a)$ podemos encontrar una contradicción. Luego, si b es nulo entonces a también lo será ($v_5(a) = v_5(b)$); por lo tanto, podemos tomar $\beta = \alpha b^{-1} = c + \sqrt{3}$ donde $c = a/b$, y tendremos $v_5(c) = 0$ y $c \in \mathbb{Z}_5$. Luego

$$v_5(\beta) = v_5\big(N_{F_1/\mathbb{Q}_5}(\alpha b^{-1})\big) = v_5\big(N_{F_1/\mathbb{Q}_5}(\alpha)b^{-2}\big) = 2m + 1 - 2v_5(b) = 2t + 1,$$

donde $t = m - v_5(b) \in \mathbb{Z}$. Más aún, $2t + 1 = v_5(c^2 - 3) \geq \text{mín}\{v_5(c^2), v_5(-3)\} \geq 0$, de lo cual concluimos que $t \geq 0$ y $v_5(c^2 - 3) \geq 1$. Luego, tomando $d \in \mathbb{Z}$ tal que $d \equiv c \bmod 5$ tendremos que $d^2 \equiv c^2 \equiv 3 \bmod 5$ (lo que es falso).

$F_2 = \mathbb{Q}_7(\sqrt{7})$: Es una extensión totalmente ramificada; pues

$$v_7(\sqrt{7}) = 1/2 v_7\big(N_{F_2/\mathbb{Q}_7}(\sqrt{7})\big) = 1/2 v_7(-7) = 1/2;$$

de ahi que $1/2\mathbb{Z} \subset v_p(F_2^\times) \subset 1/2\mathbb{Z}$.

$F_3 = \mathbb{Q}_3(\zeta, \sqrt{5})$: Es una extensión ramificada, pero no totalmente ramificada. De hecho, como hemos visto en los ejemplos 6.2.6, tenemos

$$v_3(1-\zeta) = 1/4 v_3(N_{F_3/\mathbb{Q}_3}(1-\zeta)) = 1/4 v_p(N_{\mathbb{Q}_3(\zeta)/\mathbb{Q}_3}((1-\zeta)^2)) = 1/4 v_3(9) = 1/2,$$

y, por tanto, $1/2\mathbb{Z} \subset v_3(F_3^\times)$; veamos que esta inclusión es en realidad una igualdad, para esto necesitaremos reformular la valuación $p-$ádica en términos de $N_{\mathbb{Q}_3(\sqrt{5})/\mathbb{Q}_3}$. Denotemos por λ y η a $\tau_{1,2}$ y $\tau_{2,1}$, respectivamente; entonces $\mathrm{id}, \lambda, \eta$ y $\eta\lambda$ son cuatros $\mathbb{Q}_3$-automorfismos distintos de F_3, por tanto estos conforman a $G(F_3/\mathbb{Q}_3)$. Luego, dado $\alpha = a + b\zeta \in F_3$ con $a, b \in \mathbb{Q}_3(\sqrt{5})$, tendremos que

$$\begin{aligned} N_{F_3/\mathbb{Q}_3}(\alpha) &= (\alpha \cdot \lambda(\alpha))(\eta(\alpha) \cdot \eta(\lambda(\alpha))) \\ &= (a^2 + b^2 - ab)(\eta(a)^2 + \eta(b)^2 - \eta(a)\eta(b)) \\ &= N_{\mathbb{Q}_3(\sqrt{5}/\mathbb{Q}_3)}(a^2 + b^2 - ab). \end{aligned}$$

puesto que $\mathbb{Q}_3(\sqrt{5})/\mathbb{Q}_3$ es normal y $G(\mathbb{Q}_3(\sqrt{5})/\mathbb{Q}_3) = \{\mathrm{id}, \eta_{|\mathbb{Q}_3(\sqrt{5})}\}$. Ahora, por reducción al absurdo, supongamos que existe $\alpha \in F_3^\times$ tal que $v_3(\alpha) \notin 1/2\mathbb{Z}$. Como $v_3(\alpha) \in 1/4\mathbb{Z}$, concluimos que $4v_3(\alpha) \in \mathbb{Z}$ y su mitad no; por tanto $4v_3(\alpha) = 2m+1$ con $m \in \mathbb{Z}$. Luego, escribiendo $\alpha = a + b\zeta$ con $a, b \in \mathbb{Q}_3(\sqrt{5})$ obtendremos

$$\frac{2m+1}{4} = v_3(\alpha) = \frac{1}{4} v_3\big(N_{F_3/\mathbb{Q}_3}(a+b\zeta)\big) = \frac{1}{4} v_3\big(N_{\mathbb{Q}_3(\sqrt{5})/\mathbb{Q}_3}(a^2+b^2-ab)\big) = \frac{1}{2} v_3(\theta),$$

esto es $v_3(\theta) = m + 1/2$ donde $\theta = a^2 + b^2 - ab \in \mathbb{Q}_2(\sqrt{5})$. Sin embargo $v_3(\mathbb{Q}_3(\sqrt{5})^\times) = \mathbb{Z}$ (lo cual se puede demostrar con los mismos pasos que en el primer caso), esta contradicción nos muestra que desde un principio no existia $\alpha \in F_3$ con esas propiedades.

Estos ejemplos nos sugiere un hecho no trivial, aunque posiblemente obvio en nuestro caso, que el grupo de valuación de v_p sobre una extensión finita L de $\mathbb{Q}_p$ es un grupo simple, pues $v_p(L^\times)$ es generado por todo $\pi \in L^\times$ que cumpla $v(\pi) = 1/e$ (donde $e = e(L/\mathbb{Q}_p)$). Este tipo de elemento se tendrá una importancia considerable tanto como la tuvo p en $\mathbb{Q}_p$, por ello damos la siguiente definición.

Definición 6.3.6 Sea L una extensión finita de $\mathbb{Q}_p$ y $e = e(L/\mathbb{Q}_p)$. Diremos que $\pi \in L$ es un uniformizador cuando $v_p(\pi) = 1/e$.

Observaciones 6.3.7

1. La primera deducción en la demostración de la proposición 6.3.3, nos dice que:

   > Si $x \in L$ una extensión algebraica de $\mathbb{Q}_p$ y $v_p(x) = a/b$ donde $a, b \in \mathbb{N}$ son coprimos con $b > 0$, entonces existe $\pi_0 \in L$ tal que $v_p(\pi_0) = 1/b$.

   Esto nos dará una suerte de uniformizador "provisional" en la siguiente sección. Con las mismas notaciones, podemos deducir que si $a > 0$ tendremos que $x = \pi_0 y$ con $v_p(\pi_0) = 1/b$ y $v_p(y) \geq 0$ (basta tomar $y = x\pi_0^{-1}$).

2. El número de uniformizadores es infinito, pues si $\pi \in L$ es un uniformizador entonces πu será un uniformizador para todo $u \in L$ con $v(u) = 0$.

3. El grupo $v_p(\mathbb{Q}_p^{alg})$ no será finitamente generado, más aun es $\mathbb{Q}$. De hecho, dado $n \in \mathbb{N}$, tenemos que, si $u \in \mathbb{Q}_p^{alg}$ es un cero del polinomio $f_n(X) = X^n - p$ entonces $|u|_p^n = p^{-1}$. Así deducimos que $v_p(u) = 1/n$ con $u \in \mathbb{Q}_p^{alg}$; esto a su vez implica que $v(\mathbb{Q}_p^{alg}) = \mathbb{Q}$.

Dada L una extensión algebraica de $\mathbb{Q}_p$, como vimos en la proposición 4.1.9, la valuación $p-$ádica nos brinda un subanillo en L, a decir

$$\mathcal{O} = \mathcal{O}_L = \{x \in K \ ; \ v_p(x) \geq 0\} = \{x \in K \ ; \ |x|_p \leq 1\}$$

que es conocido como el *anillo de valuación de* K; así también, obtenemos su único ideal maximal

$$\mathfrak{p} = \mathfrak{p}_L = \{x \in K \ ; \ v_p(x) > 0\} = \{x \in K \ ; \ |x|_p < 1\}$$

el *ideal de valuación*, y podemos construir el *cuerpo residual* $\Bbbk = \Bbbk_L = \mathcal{O}/\mathfrak{p}$. Resumiremos las propiedades básicas de estas estructuras para el caso finito.

Proposición 6.3.8 *Sea L una extensión finita de $\mathbb{Q}_p$, $e = e(L/\mathbb{Q}_p)$ y π un uniformizador en L, entonces*

i) El ideal $\mathfrak{p}_L$ es principal y π es un generador.

ii) Dado $\alpha \in L$, se expresar como $\pi^n u$ con $n \in \mathbb{Z}$ y $u \in L$ tal que $v_p(u) = 0$, en particular $L = \mathcal{O}[1/\pi]$.

iii) El cuerpo $\Bbbk$ es una extensión de $\mathbb{F}_p$ de grado menor o igual a $[L : \mathbb{Q}_p]$.

iv) Dado $x \in L$, $x \in \mathcal{O}$ si y sólo si $\mathrm{Irr}\,(\mathbb{Q}_p, x) \in \mathbb{Z}_p[X]$.

v) *Sea* $A = \{0, c_1, c_2, \cdots, c_r\} \subset \mathcal{O}$ *un conjunto de representantes de* $\Bbbk$. *Entonces, para cada* $x \in L$ *existe una única expansión* $p-$*ádica de la forma*

$$x = \sum_{i \leq m} a_i \pi^i \qquad \textit{donde cada } a_i \in A.$$

Demostración.

i) Dado $x \in \mathfrak{p} \setminus \{0\}$, tenemos que $v_p(x) = ne > 0$ y que $x\pi^{-n} \in \mathcal{O}$, por tanto $x \in \pi^n \mathcal{O}$ y $x \in \langle \pi \rangle$.

ii) Dado $x \in L \setminus \mathcal{O}$, tenemos que $n = v_p(x)e < 0$ y $u = x\pi^{-n}$ es tal que $v_p(u) = 0$, por tanto $x = u\pi^n \in [1/\pi]$; esto y el ítem previo nos implican este ítem.

iii) Puesto que $\mathbb{Q}_p \subset L$, por la lema 4.1.11 obtenemos que $\Bbbk$ es una extensión $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$. Denotemos como n al grado de la extensión $L/\mathbb{Q}_p$ y comprobemos que a lo más existen n elementos *l.i.* sobre $\mathbb{Q}_p$. Dados $v_1, v_2, \ldots, v_{n+1} \in \Bbbk$, elijamos $x_1, \ldots, x_{n+1} \in \mathcal{O}$ tales que $x_i + \mathfrak{p} = v_i$, para $i \in 1, 2, \ldots, n+1$. Entonces, existen $a_1, a_2, \ldots, a_{n+1} \in \mathbb{Q}_p$ no todos nulos tales que $a_1x_1 + a_2x_2 + \cdots + a_{n+1}x_{n+1} = 0$. Tomemos $j \in \{1, 2, \ldots, n+1\}$ tal que $v_p(a_j) = \min\{v_p(a_i); i = 1, 2, \ldots, n+1\}$, en este caso a_j es no nulo (de lo contrario todos lo serian), y para cada $i = 1, 2, \ldots, n+1$ tomemos $b_i = a_i/a_j$; de modo que $v_p(b_i) = v_p(a_i) - v_p(a_j) \geq 0$, esto es $b_i \in \mathbb{Z}_p$ (para todo i). Luego, $b_1x_1 + b_2x_2 \cdots + b_{n+1}x_{n+1} = 0$, tomando módulo el ideal $\mathfrak{p}$ tendremos que

$$(b_1 + \mathfrak{p})v_1 + (b_2 + \mathfrak{p})v_2 \cdots + (b_{n+1} + \mathfrak{p})v_{n+1} = 0$$

donde al menos $b_j + \mathfrak{p} = 1 + \mathfrak{p} \neq \mathfrak{p}$; así concluimos que cualesquiera $n+1$ elementos de $\Bbbk$ son *l.d.*.

iv) Dado $\alpha \in L$, escribamos $\mathrm{Irr}\,(\mathbb{Q}_p, \alpha) = x + a_{r-1}x_{r-1} + \cdots + a_0$. Entonces $|\alpha|_p \leq 1$ si y sólo si $|N_{L/\mathbb{Q}_p}(\alpha)| \leq 1$, o bien $|a_0| \leq 1$ (por el teorema 3.9.1), lo cual ,via el lema 5.3.7, equivale a que $a_0, a_1, \ldots, a_{r-1} \in \mathbb{Z}_p$.

v) Empecemos demostrando por inducción la siguiente afirmación.

Afirmación : *Dados* $x \in \mathcal{O}$, $n \in \mathbb{N}$ *existen únicos* $a_0^{(n)}, a_1^{(n)}, \ldots, a_{n-1}^{(n)} \in A$ *tales* $x \equiv a_0^{(n)} + a_1^{(n)}\pi + \cdots + a_{n-1}^{(n)}\pi^{n-1}$ mód π^n.

Es claro, que tomando $a_0 \in A$ tal que $x \equiv a_0 \mod \pi$ la afirmación es cierta para el caso $n = 1$. Supongamos que es cierto para algún $n \in \mathbb{N}$, entonces existen $a_0, a_1, \ldots, a_{n-1} \in A$ tales que π^n divide a $x - (a_0 + a_1\pi \cdots + a_{n-1}\pi^{n-1})$. Elijamos $y = (x - (a_0 + a_1\pi +$

$\cdots + a_{n-1}\pi^{n-1}))/\pi^n \in \mathcal{O}$ y a_n el único elemento de A tal que $y \equiv a_n$ mód π (estamos utilizando la base de inducción, que ya hemos demostrado). Entonces

$$x - (a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}) \equiv a_n\pi^n \text{ mód } \pi^{n+1},$$

y deducimos la existencia de estos elementos, veamos su unicidad. Sean $b_0, b_1, \ldots, b_n \in A$ que satisface la congruencia de la afirmación, entonces

$$x \equiv a_0 + \cdots + a_{n-1}\pi^{n-1} \equiv b_0 + \cdots + b_{n-1}\pi^{n-1} \text{ mód } \pi^n;$$

de esta congruencia podemos deducir que $a_i = b_i$, para $i = 0, 1, \ldots, n-1$; luego $a_n \equiv y \equiv b_n$ mód π, por tanto $a_n = b_n$.

Notemos que cada una de estas sucesiones es parte de la siguiente, es decir, dado $n \in \mathbb{N}$ se tiene que $a_i^{(n)} = a_i^{(n+1)}$ para $i = 0, 1, \ldots, n-1$. En consecuencia, $(c_n)_{n\geq 0} \in A$ definido por $c_n = a_n^{(n+1)}$ satisfacerá $c_n = a_n^{(m)}$, para todo $n \in 0, 1, \ldots, m-1$, $m \in \mathbb{N}$. Luego,

$$|x - c_0 + c_1\pi + \cdots + c_{m-1}\pi^{m-1}|_p = |x - a_0^{(m)} - \cdots - a_{m-1}^{(m)}\pi^{m-1}|_p \leq p^{-em},$$

para todo $m \in \mathbb{N}$. Por esta desigualdad, deducimos que $x = \sum_n c^n\pi^n$. La demostración de la unicidad de esta expansión, como su generalización para cualquier elemento de $L = \mathcal{O}[1/\pi]$ son analogas a las dadas en el teorema 5.2.2.

Observaciones 6.3.9

- Segun se necesite especificar o acentuar a que extensión pertenece el anillo, el ideal de valuación o el cuerpo residual, utilizaremos como subíndice la misma letra con que se denota a dicha extensión, así también la obviaremos con el fin de simplicar la notación.

- El cuarto de esta proposición se puede resumir en: " $\mathbb{Z}_p$ es integralmente cerrado en $\mathcal{O}_L$"(vea [10] para más información).

- Dado L extensión algebraica sobre $\mathbb{Q}_p$, tendremos que $\Bbbk_L$ es un extensión algebraica sobre $\mathbb{F}_p$. De hecho, dado $\alpha \in \Bbbk_L$, existen $a \in \mathcal{O}_L$ y $c_0, \ldots, c_r \in \mathbb{Z}_p$ tales que $a + \mathfrak{p}_L = \alpha$ y $c_0 + \cdots + c_r a^r = 0$; por lo tanto,

$$(c_0 + \mathfrak{p}_L) + \cdots + (c_r + \mathfrak{p}_L)(a + \mathfrak{p}_L)^r = (c_0 + \cdots + c_r a^r) + \mathfrak{p}_L = 0 + \mathfrak{p}_L = \mathfrak{p}_L,$$

  y α es algebraico sobre $\mathbb{Z}_p/(\mathbb{Z}_p \cap \mathfrak{p}_L) \cong \mathbb{F}_p$ (vea la proposición 4.1.9).

- Supongamos que $L \subset M$ son extensiones algebraicas de $\mathbb{Q}_p$ y que $x, y \in L$, entonces

$$x \equiv y \text{ mód } \mathfrak{p}_L \quad \text{equivale a} \quad x \equiv y \text{ mód } \mathfrak{p}_M;$$

  pues la primera congruencia equivale a $|x - y|_p$, que significa exactamente lo mismo que la segunda congruencia (lo cual es cierto desde $|\cdot|_p$ es único en $\mathbb{Q}_p^{alg}$).

Mejoramos la información mencionada acerca del cuerpo residual de una extensión finita con el siguiente resultado.

Teorema 6.3.10 *Sea L una extensión de grado n sobre $\mathbb{Q}_p$, $e = e(L/\mathbb{Q}_p)$ el índice de ramificación y $f \in \mathbb{N}$ tal que $ef = n$. Entonces, el grado de $\Bbbk$ sobre $\mathbb{F}_p$ es f.*

Demostración.- Si escribimos $m = [\Bbbk : \mathbb{F}_p]$, que como sabemos es menor o igual a n, entonces buscamos demostrar que $em = n$; para realizar esto bastar demostrar que existe una base de L sobre K de em elementos. Tomemos $\pi \in L$ un uniformizador, $\{\alpha_1, \alpha_2, \ldots, \alpha_m\} \subset \mathcal{O}$ tal que $\{\alpha_1 + \mathfrak{p}, \alpha_2 + \mathfrak{p}, \ldots, \alpha_m + \mathfrak{p}\} \subset \Bbbk$ sea una base, y

$$\mathcal{B} = \{\alpha_i \pi^j \ ; \ i = 1, 2, \ldots, m \ , \ j = 0, 1 \ldots, e-1\}.$$

Afirmación 1: *$\mathcal{B}$ es l.i. sobre $\mathbb{F}_p$*

Sean $\lambda_{i,j} \in \mathbb{Q}_p$ no todos nulos y $x = \sum_{j=0}^{e-1} \sum_{i=1}^{m} \lambda_{i,j} \alpha_i \pi^j$, verifiquemos que x es no nulo. Elijamos i_0 y j_0 tales que λ_{i_0,j_0} posea la menor valuación entre estos coeficientes, entonces

λ_{i_0,j_0} será no nulo (pues de lo contrario todos los coeficientes tendran valuación infinita y, por tanto, serian nulos). Para cada i y j tomemos $\eta_{i,j} = \lambda_{i,j}\lambda_{i_0,j_0}^{-1}$, obteniendo que $v_p(\eta_{i,j}) \geq 0$ (para cada i y j), y , en consecuencia, $y = x\lambda_{i_0,j_0}^{-1} \in \mathcal{O}$. Luego, si $k_0 \in \{0, 1, \ldots, e-1\}$ como el menor índice tal que $v_p(\eta_{i,k_0}) = 0$ para algún i. Entonces, dados $i \in \{1, \ldots, e\}$, $j < k_0$, tendremos que $v_p(\eta_{i,j}) > 0$ con $\eta_{i,j} \in \mathbb{Z}_p$, luego $\eta_{i,j} \equiv 0 \,\text{mód}\, \pi^e$. Con esto podemos deducir que $\pi^{k_0} \mid y$ en $\mathcal{O}$, entonces

$$y\pi^{-k_0} \equiv \eta_{1,k_0}\alpha_1 + \cdots + \eta_{m,k_0}\alpha_m \not\equiv 0 \,\text{mód}\, \pi,$$

puesto que no todo $\eta_{i,k_0} \equiv 0 \,\text{mód}\, \pi$ y $\alpha_1 + \mathfrak{p}, \ldots, \alpha_1 + \mathfrak{p}$ son *l.i.*; luego $v_p(y\pi^{-k_0}) = 0$ y $v_p(x) = k_0/e + v_p(\lambda_{i_0,j_0})$, en particular x es no nulo.

Afirmación 2: *El conjunto B genera L*

En primer lugar, tenemos que $W = \text{Span}(\mathcal{B})$ es un $\mathbb{Q}_p$-espacio normado finito dimensional, por tanto completo, de este modo es un subespacio cerrado en L. Para probar esta afirmación y finalizar la demostración, deduciremos la densidad de W en L.

Afirmación 3: *Dado $x \in \mathcal{O}$ y $n \in \mathbb{N}$, existe $w \in W$ tal que $v_p(x - w) \geq n$.*

Nótese que ocurrir esto, ocurria que $v_p(w) \geq \text{mín}\{v_p(x), v)p(w - x)\} \geq 0$, $w \in \mathcal{O}$. Demostraremos este hecho por inducción sobre $n \in \mathbb{N}$. Dado $x \in W$, existen $a_0, a_1, \ldots, a_{e-1} \in \mathcal{O}$ tales que

$$x \equiv a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1} \,\text{mód}\, \pi^e,$$

estos coeficientes a_i pueden ser aquellos que aparezcan en una expansión $p-$ádica de x. Como $a_0 \in \mathcal{O}$, existen $a_{0,1}, \ldots, a_{0,m} \in \mathbb{Z}_p$ tales que $b_1 = a_0 - (a_{0,1}\alpha_1 + \cdots + a_{0,m}\alpha_m)$ sea congruente a 0 módulo π, luego

$$y \equiv \sum_{i=1}^{m} a_{0,i}\alpha_i + (a_1 + b_1/\pi)\pi + \sum_{i=2}^{e-1} a_i\pi^i \,\text{mód}\, \pi^e.$$

Tomando $a_{0,1}, \ldots, a_{0,m} \in \mathbb{Z}_p$ tales que $b_2 = a_2 + b_1/\pi - \sum a_{1,i}\alpha_i$ sea congruente a 0 módulo π, tendremos

$$y \equiv \sum_{i=1}^{m} a_{0,i}\alpha_i + \sum_{i=1}^{m} a_{1,i}\alpha_i\pi + (a_2 + b_2/\pi)\pi^2 + \sum_{i=3}^{e-1} a_i\pi^i \,\text{mód}\, \pi^e;$$

repitiendo este proceso obtenemos coeficientes $a_{i,j} \in \mathbb{Z}_p$ tales que

$$y \equiv \sum_{j=0}^{e-1}\sum_{i=1}^{m} a_{0,i}\alpha_i\pi^j + (b_e/\pi)\pi^e \,\text{mód}\, \pi^e,$$

donde $b_e \equiv 0$ mód π. Si denotamos por w a la suma del lado derecho de esta última congruencia, tendremos que $w \in W$ y que $v_p(x - w) \geq e \cdot 1/e = 1$. Ahora supongamos que existe $w \in W$

tal que $v_p(x-w) \geq n$. Entonces $z = (x-w)/p^n$ poseerá valuación p-ádica positiva, por lo que $z \in \mathcal{O}$. Luego, por el caso ya demostrado, existirá $u \in W$ tal que $v_p(z-u) \geq 1$, por lo tanto

$$v_p\big(x-(w+p^n u)\big) = v_p\big(p^n(z-u)\big) \geq n+1, \quad \text{donde } w+p^n u \in W;$$

esto demuestra que la veracidad de la afirmación en algún $n \in \mathbb{N}$ implica la del caso $n+1$.

Veamos que W es denso en L, dado $y \in L$ no nulo y $\epsilon > 0$, tomemos $m \in \mathbb{Z}$ tal que $v_p(y) \geq m$, para obtener que $x = yp^{-m} \in \mathcal{O}$. Elijamos $n \in \mathbb{N}$ y $w \in V$ tales que $p^{-n} < p^m \epsilon$ y $v_p(x-w) \geq n$. Entonces,

$$|y - p^m w|_p = |p^m|_p |x-w|_p \leq p^{-n-m} < \epsilon, \qquad \text{con} \quad p^m w \in V.$$

□

Observación 6.3.11 Nótese que la tercera afirmación de esta demostración nos un metodo para encontrar una sucesión $(w_n)_{n\in\mathbb{N}} \subset W$ que convergen a elemento $x \in L$ (preestablecido). Más aun, los términos de la sucesión con combinaciones lineales de elementos de $\mathcal{B}$ con coeficientes en $\mathbb{Z}_p$; por lo tanto deducimos que $\mathcal{B}$ es una base para el $\mathbb{Z}_p-$modulo $\mathcal{O}$, esto es lo que se conoce como "base integral" de $\mathcal{O}$ sobre $\mathbb{Z}_p$ (vea [10]).

Definición 6.3.12 Sean L una extensión de $\mathbb{Q}_p$ de grado n y $e = e(L/\mathbb{Q}_p)$ el índice de ramificación. El entero $f = n/e$ se denomina como *Grado Residual de* L.

Corolario 6.3.13 *Dado $g(X) \in \mathbb{F}_p[x]$ mónico e irreductible de grado n, existe una extensión no ramificada de grado n sobre $\mathbb{Q}_p$ tal que $g(X)$ tiene una raíz en $\Bbbk_L$.*

Demostración.- Escribamos $g(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0$ y tomemos $b_0, b_1, \ldots, b_{r-1} \in \mathbb{Z}_p$ tales que $b_i + \mathfrak{p}_{\mathbb{Q}_p} = a_i$, para todo i; entonces, $h(X) = X^r + b_{r-1}X^{r-1} + \cdots + b_0 \in \mathbb{Q}_p[x]$ es irreductible (por el corolario 5.3.9). Si $\alpha \in \mathbb{Q}_p^{alg}$ es una raíz de $h(x)$, entonces $L = \mathbb{Q}_p(\alpha)$ tiene grado r sobre $\mathbb{Q}_p$. Más aun, por la proposición anterior $\alpha \in \mathcal{O}_L$, así tenemos que $\alpha + \mathfrak{p}_L \in \Bbbk$ es un cero de $g(X)$. Luego $\mathbb{F}_p(\alpha) \subset \Bbbk$ y $r \leq [\Bbbk : \mathbb{F}_p] \leq [L : \mathbb{Q}_p] = r$, en consecuencia, el grado residual coincide con el grado de la extensión de L; por el teorema anterior tendremos $e(L/\mathbb{Q}_p) = 1$. □

Terminamos esta sección rescatando un sencillo y util hecho acerca de la Traza y Norma de una extensión finita de $\mathbb{Q}_p$ con respecto al anillo de valuación.

Proposición 6.3.14 *Sea L una extensión finita sobre $\mathbb{Q}_p$. Entonces la traza $T_{L/\mathbb{Q}_p}$ y la norma $N_{L/\mathbb{Q}_p}$ de $L/\mathbb{Q}_p$ cumplen $T_{L/\mathbb{Q}_p}(\mathcal{O}_L) \subset \mathbb{Z}_p$ y $N_{L/\mathbb{Q}_p}(\mathcal{O}_L) \subset \mathbb{Z}_p$.*

Demostración.- Dado $\alpha \in \mathcal{O}_L$, tomemos $f(X) = \text{Irr}\,(\mathbb{Q}_p, \alpha) = X^r + c_{r-1}X^{r-1} + \cdots + c_0 \in \mathbb{Q}_p[X]$. Por la proposición 6.3.8, tendremos que $f(X) \in \mathbb{Z}_p[X]$, luego por el teorema 3.9.1 tendremos que $T_{L/\mathbb{Q}_p}(\alpha) = -[L : K(a)]c_{r-1}$ y $N_{L/K}(a) = ((-1)^r c_0)^{[L:K(a)]}$, verificando la proposición. □

6.4. Raices de la unidad e índice de ramificación

Sea L una extensión algebraica de $\mathbb{Q}_p$. Denotaremos el conjunto de raíces de la unidad por

$$\mu(L) = \{x \in L\ ;\ x^n = 1\ ,\ n \in \mathbb{N}\},$$

este es sugbrupo multiplicativo de $L^\times$ formado por los elementos de orden finito, así también denotaremos los subconjuntos

$$\mu_{p^\infty}(L) = \{x \in L^\times\ ;\ \text{ord}\,(x) = p^n\ ,\ n \in \mathbb{N}\} \quad \text{y} \quad \mu_{(p)}(L) = \{x \in L^\times\ ;\ \text{mcd}\,(\text{ord}\,(x), p) = 1\ ,\}.$$

Se puede demostrar que $\psi : \mu(L) \to \mu_{p^\infty}(L) \times \mu_{(p)}(L)$ definido por $\psi(x) = (x^{\text{ord}\,(x)/m}, x^{\text{ord}\,(x)/p^n})$ cuando $\text{ord}\,(x) = p^n m$ con $\text{mcd}\ (p, m) = 1$, es un homomorfismo de grupos (basta utilizar que $\text{ord}\,(xy) = \text{ord}\,(x)\text{ord}\,(y)/\text{mcd}\ (\text{ord}\,(x), \text{ord}\,(y))$); más aun un isomorfismo. De hecho, si $\psi(x) = (1, 1)$ entonces, con las anteriores notaciones, se tiene que $\text{ord}\,(x)/p^n = 1$ y $\text{ord}\,(x)/m = 1$, lo que implica que $m = p^n$, $\text{ord}\,(x) = 1$ y $x = 1$; y como es sobreyectvo, ψ es un isomorfismo.

El siguiente lema nos será mucha utilidad en el futuro, tanto a nivel clasificatorio, como en nuestras cuentas.

Lema 6.4.1 *Sea L una extensión algebraica de $\mathbb{Q}_p$, entonces*

$$\mu_{p^\infty}(L) = \mu(L) \cap (1 + \mathfrak{p}_L).$$

Demostración.- Sea $u \in \mu(L)$ con $\text{ord}\,(u) = p^n$, entonces $(u + \mathfrak{p})^{p^n} = u^{p^n} + \mathfrak{p} = 1 + \mathfrak{p}$; como $\text{car}\,(\Bbbk) = p$, necesariamente $u + \mathfrak{p} = 1 + \mathfrak{p}$. Recíprocamente, sea $u \in \mu(L)$ tal que $u \in 1 + \mathfrak{p}$, tomemos $\text{ord}\,(u) = p^n m$ con $\text{mcd}\ (m, p) = 1$. Veamos que es imposible que $m > 1$, pues de serlo $w = u^{p^n}$ poseerá orden igual 1 y $w + \mathfrak{p} = (u + \mathfrak{p})^{p^n} = 1 + \mathfrak{p}$. Escribamos $w = 1 + \beta$ con $\beta \in \mathfrak{p}$, que será no nulo (porque $m > 1$), entonces $v_p(\beta) = c/d > 0$ con $c, d \in \mathbb{N}$ coprimos. Por las observaciones 6.3.7, existen $\pi_0, a_1 \in L$ tales que $\beta = \pi_0 a_1$ con $v_p(\pi_0) = 1/d > 0$ y $v_p(a_1) \geq 0$, con los cuales obtenemos que

$$w^p = 1 + p\pi_0 a_1 + \sum_{k=2}^{p} \binom{p}{k} \pi_0^k a_1^{p-k} = 1 + \pi_0^2 a_2,$$

donde $a_2 = (p/\pi_0)a_1 + \sum \binom{p}{k}\pi_0^{k-2}a_1^{p-k} \in \mathcal{O}_L$, pues $v_p(p) = 1 \geq v_p(\pi_0)$. Por los mismos cálculos podemos realizar un proceso de inducción e inferir que: para todo $r \in \mathbb{N}$, existe a_r tal que $w^{p^r} = 1 + \pi_0^{r+1}a_r$. Por otra parte, como mcd $(m, p) = 1$, por el teorema de Lagrange, tenemos que existe $s \in \mathbb{N}$ tal que $m \mid (p^s - 1)$; de ahi que, nuevamente por inducción, que $w^{p^{sr}} = w$, para todo $r \in \mathbb{N}$. Luego, para cada $r \in \mathbb{N}$ se cumple que

$$w = w^{p^{sr}} = 1 + \pi_0^{sr+1}a_r \quad \text{para algún} \quad a_r \in \mathcal{O}_L.$$

esto nos dice que $|w - 1|_p \leq p^{-(\frac{sr+1}{d})}$, para todo $r \in \mathbb{N}$; luego, $|w - 1|_p = 0$ y $m = 1$ (contradicción). □

Corolario 6.4.2 *Si $m \in \mathbb{N}$ es coprimo con p y $u, v \in \mathbb{Q}_p^{alg}$ son m-ésimas raíces distintas de la unidad, entonces $v_p(u - v) = 0$.*

Demostración.- Tomando $w = u/v$ obtenemos una $m-$ésima raíz de unidad distinta de 1, por tanto $w \notin \mu_{p^\infty}(\mathbb{Q}_p^{alg})$ y $v_p(w - 1) \neq 0$, lo que implica que $v_p(u - v) \neq 0$. □

Observación 6.4.3 Asumiendo las mismas notación que en el lema anterior, pero añadiendo una perspectiva de grupos y homomorfismos, obtendremos que:

> La proyección canónica π de anillo de valuación entre el ideal de valuación restringido a $\mu(L)$ es un homomorfismo de grupos multiplicativos hacia $\Bbbk_L^\times$, lleva exactamente al subgrupo $\mu_{p^\infty}(L)$ al elemento neutro $1 + \mathfrak{p}_L$, esto significa que $\mathrm{Nu}(\pi) = \mu_{p^\infty}(L)$.

Podemos mejorar este resultado, pero para hacerlo necesitaremos una extensión del lema Hensel para extensiones finitas.

Lema 6.4.4 (Hensel) *Sean L una extensión finita de $\mathbb{Q}_p$, $f(X) \in \mathcal{O}_L[X]$ y $\alpha_1 \in \mathcal{O}_L$ tales que $v_p(f'(\alpha_1)) = 0$ y $v_p(f(\alpha_1)) > 0$. Entonces, existe un único $\alpha \in \mathcal{O}_L$ tal que $f(\alpha) = 0$ y $\alpha \equiv \alpha_1$ mód $\mathfrak{p}_L$.*

Demostración.- En primer lugar, nótese que las hipótesis sobre las valuaciones de $f(\alpha_1)$ y $f'(\alpha_1)$ son un caso particular que la presentadas en el teorema 5.3.2 (aunque a su vez en un contexto más general); así son aplicables a la afirmación realizada. De hecho, la demostración de esa afirmación fue argumentada por las propiedades del valor absoluto no arquimediano de $|\cdot_p|$, las cuales hemos extendido en $\mathcal{O}_L$; por lo tanto se puede repetir los pasos anteriores, con los cambios adecuados, y obtener las siguientes propiedades.

Afirmación : *Sea $\alpha \in \mathcal{O}_L$ y $s > 0$ tales que $|f(\alpha)|_p \leq p^{-s}$ y $|f'(\alpha)|_p = 1$ entonces $\beta = \alpha - f(\alpha)/f'(\alpha)$ satisface*

- $|\beta - \alpha|_p \leq p^{-s}$.
- $|f'(\beta)|_p = 1$.
- $|f(\beta)|_p \leq p^{-2s}$.

Tomando $s = v_p(f(\alpha_1)) > 0$, contruimos $(a_n) \subset \mathcal{O}_L$ tal que

- $a_1 = \alpha_1$.
- $|a_n - a_{n+1}|_p \leq p^{-2^{n-1}s}$.
- $|f'(a_n)|_p = 1$, para todo $n \in \mathbb{N}$.

Esta sucesión será de Cauchy, por tanto será convergente a algún $\alpha \in \mathcal{O}_L$ (puesto que L es completo al ser una extensión finita de $\mathbb{Q}_p$). Luego, es similar deducir la existencia y unicidad de α como raíz de $f(x)$ que satisfaga $\alpha \equiv \alpha_1$ mód $\mathfrak{p}_L$. □

Teorema 6.4.5 *Sea L una extensión algebraica de $\mathbb{Q}_p$ y la proyección canónica $\pi : \mathcal{O}_p \to \Bbbk_L$. Entonces la restricción $\pi_{|\mu(L)} : \mu(L) \to \Bbbk_L^\times$ es un epimorfismo de grupos multiplicativos, cuyo nucleo es μ_{p^∞}. En particular $\mu_{(p)}(L) \cong \Bbbk_L^\times$.*

Demostración.- Por el lema 6.4.1 y su observación nos resta demostrar que la sobreyectividad de $\pi_{|\mu(L)}$. Dado $a \in \Bbbk_L^\times$, este elemento es algebraico sobre $\mathbb{F}_p$, luego $a \in \mathbb{F}_q$ con $q = p^n$ para algún $n \in \mathbb{N}$, y por tanto $a^{q-1} = 1 + \mathfrak{p}_L$ (por el teorema de Lagrange). Si tomamos $u_0 \in \mathcal{O}_L$ tal que $u_0 + \mathfrak{p}_L = a$ entonces $u_0^{q-1} + \mathfrak{p}_L = (u_0 + \mathfrak{p}_L)^{q-1} = 1 + \mathfrak{p}_L$, y como $(q-1)u_0^{q-2} \not\equiv 0$ mód $\mathfrak{p}$, todo esto significará se resume en

$$v_p(u_0^{q-1} - 1) > 0 \quad \text{y} \quad v_p\big((q-1)u_0^{q-2}\big) = 0.$$

Luego, tomando $M = \mathbb{Q}_p(u_0)$ podemos aplicar el lema de Hensel en el polinomio $x^{q-1} - 1$, para obtener $u \in \mathbb{Q}_p(u_0)$ tal que $v_p(u - u_0) > 0$ y $u^{q-1} = 1$; así es como obtenemos $u \in \mu_{(p)}(L)$ y $\pi(u) = a$. Finalmente la última afirmación es justificada por

$$\Bbbk_L^\times \cong \frac{\mu(L)}{\mu_{p^\infty}(L)} \cong \frac{\mu_{p^\infty}(L) \times \mu_{(p)}(L)}{\mu_{p^\infty}(L)} \cong \mu_{(p)}(L).$$

□

Observaciones 6.4.6

- Si L en la anterior fuese una extensión finita de $\mathbb{Q}_p$, entonces $\Bbbk_L$ sería finito y $\#\mu_{(p)}(L) = \#\Bbbk_L^\times = p^s - 1$ para algún $s \in \mathbb{N}$.

- Tenemos que

$$\mu_{(p)}(\mathbb{Q}_p^{alg}) = \{u \in \mathbb{Q}_p^{alg} \ ; \ u \text{ es una raíz } p^s - 1\text{-ésima de la unidad, para algún } s \in \mathbb{N}\}.$$

  De hecho, dado $u \in \mu_{(p)}(L)$, el elemento $\pi(u) \in \Bbbk_{\mathbb{Q}_p^{alg}}^{\times}$ posee su mismo orden. Puesto que $\Bbbk_{\mathbb{Q}_p^{alg}}^{\times}$ es algebraico sobre $\mathbb{F}_p$, existe $s \in \mathbb{N}$ tal que $\pi(u) \in \mathbb{F}_{p^s}$; por lo tanto, $\pi(u)^{p^s-1} = 1$.

- El isomorfismo que acabamos de demostrar nos da una condición suficiente y necesaria para que una extensión posea un cuerpo residual mas grande que $\mathbb{F}_p$ (que en nuestro caso significa que posea con más de $p-1$ elemento), la cual sería es que contenga más raíces de la unidad que las $p-1$ raíces de la unidad que ya pertenecian a $\mathbb{Q}_p$. En resumen, la creación de una extensión (algebraica) no ramificada de $\mathbb{Q}_p$ supone un cuerpo residual mayor, por tanto se debe haber añadido raíces de la unidad a $\mathbb{Q}_p$. El siguiente corolario, muestra que la sufiencia de añadir raíces de la unidad a $\mathbb{Q}_p$ para obtener una extensión no ramificada.

Corolario 6.4.7 *Existe una única extensión no ramificada de grado $f \in \mathbb{N}$, la cual es generada por adjuntar una $p^f - 1$-ésima raíz primitiva de la unidad a $\mathbb{Q}_p$.*

Demostración.- Por el corolario 6.3.13, sabemos que existen extensiones no ramificadas de grado f sobre $\mathbb{Q}_p$, tomemos a L como una de estas. Por el teorema previo, sabemos que $\mu_{(p)}(L) \cong \Bbbk_L^{\times}$; por tanto $\mu_{(p)}(L)$ es un subgrupo multiplicativo finito de $L^{\times}$, así que existe $u \in L^{\times}$ que genera a $\mu_{(p)}(L)$ (por lo cual tiene orden $p^f - 1$). Sea $M = \mathbb{Q}_p(u)$, entonces $u, u^2, \ldots, u^{p^f-1} \in M$ no son congruentes dos a dos módulo $\mathfrak{p}_M$ (por el corolario 6.4.2), lo que implica que $\#\Bbbk_M \geq p^f - 1$ y $\mathbb{F}_{p^f} \subset \Bbbk_M$. Luego, se tiene que

$$f = [\mathbb{F}_{p^f} : \mathbb{F}_p] \leq [\Bbbk_M : \mathbb{F}_p] \leq [M : \mathbb{Q}_p] \leq [L : \mathbb{Q}_p] = f,$$

en conclusión $L = M = \mathbb{Q}_p(u)$.

Finalmente, si L_0 es otra extensión no ramificada de grado f sobre $\mathbb{Q}_p$, entonces existirá $v \in L_0$ raíz no ramificada de orden $p^f - 1$. Luego, podemos encontrar $r, s \in \mathbb{N}$ coprimos con $p^f - 1$ tales que $v^r = u$ y $u^s = v$; por tanto $L_0 = \mathbb{Q}_p(v) = \mathbb{Q}_p(u) = L$. □

Observación 6.4.8 Dado $f \in \mathbb{N}$, denotaremos a $\mathcal{L}_f$ a la extensión no ramificada de grado f sobre $\mathbb{Q}_p$.

Este último corolario clasifica todas las extensiones ramificadas como aquellas generadas por adjuntar una raíz de la unidad, la siguiente proposición nos menciona aun más de este importante tipo de raíz de la unidad.

Proposición 6.4.9 *Dado $f \in \mathbb{N}$, sea $u \in \mathbb{Q}_p^{alg}$ una raíz primitiva $p^f - 1$-ésima de la unidad, entonces $\mathcal{L}_f = \mathbb{Q}_p(u)$ es normal sobre $\mathbb{Q}_p$ y $G(\mathcal{L}_f/\mathbb{Q}_p)$ es generado por el $\mathbb{Q}_p-$automorfismo ψ determinado por $\psi(u) = u^p$.*

Demostración.- Como ya sabemos $L_f = \mathbb{Q}_p(u)$ es normal sobre $\mathbb{Q}_p$, así que resta verificar que ψ es $\mathbb{Q}_p-$automorfismo y que genera a $G(L_f, \mathbb{Q}_p)$. Para mostrar que ψ determina un $\mathbb{Q}_p-$monomorfismo bastaria mostrar que u^p también es una raíz de $\operatorname{Irr}(\mathbb{Q}_p, u)$ (por el lema 3.3.5); más aun, esto significaria que ψ es un $\mathbb{Q}_p-$automorfismo (por el lema 3.8.1, o también porque u^p también es una raíz primitiva). Tomemos $g(X) = \operatorname{Irr}(\mathbb{Q}_p, u) \in \mathbb{Q}_p[X]$ como $X^f + a_{f-1}X^{f-1} + \cdots + a_0$ (pues grad $\operatorname{Irr}(\mathbb{Q}_p, u) = [\mathbb{Q}_p(u) : \mathbb{Q}_p] = f$), entonces $a_0, a_1, \ldots, a_{r-1} \in \mathbb{Z}_p$ (por la proposición 6.3.8); de esta forma tiene sentido $\pi g(X)$, donde π es la proyección canónica de $\mathcal{O}$ entre $\mathfrak{p}$.

Afirmación : $\operatorname{Irr}(\mathbb{F}_p, u + \mathfrak{p}) = \pi g(X)$

Como $\pi g(X)$ se anula en $u + \mathfrak{p}$ tendremos que $\operatorname{Irr}(\mathbb{F}_p, u + \mathfrak{p})$ divide a $g(X)$. Por otra parte, el corolario 6.4.2 nos garantiza que $u + \mathfrak{p}, u^2 + \mathfrak{p}, \ldots, u^{p^f - 1} + \mathfrak{p}$ son distintos, por tanto $\#\mathbb{F}_p(u + \mathfrak{p}) \geq p^f - 1$ y $\mathbb{F}_{p^f} \subset \mathbb{F}_p(u + \mathfrak{p})$; así conluimos que grad $\operatorname{Irr}(\mathbb{F}_p, u + \mathfrak{p}) = [\mathbb{F}_p(u + \mathfrak{p}) : \mathbb{F}_p] \geq f$. Por lo tanto $\operatorname{Irr}(\mathbb{F}_p, u + \mathfrak{p})$ y $\pi g(x)$ tienen el mismo grado, y como ambos son mónicos estos polinomios son iguales.

Por el lema 3.11.8, $(u+\mathfrak{p})^p$ también sera un cero de $\pi g(x)$, así que $g(u^p) \equiv 0$ mód $\mathfrak{p}$; más aun, como $\mathbb{F}_p$ es perfecto y $\pi g(X)$ es irreducible tendremos que $(u + \mathfrak{p})^p$ es una raíz simple, así que $g'(u^p) \not\equiv 0$ mód $\mathfrak{p}$. De ahí que podemos aplicar el lema de Hensel a $u^p \in \mathbb{Q}_p(u)$ y $g(x) \in \mathbb{Z}_p[x]$ y para obtener $v \in \mathbb{Q}_p(u)$ tal que $v \equiv u^p$ mód $\mathfrak{p}$ y $g(v) = 0$. Asi tenemos que v es un $\mathbb{Q}_p$-conjugado de u, por lo que también una raíz $p^f - 1$-ésima de la unidad. Como $v \equiv u^p$ mód $\mathfrak{p}$ tendremos que v necesearíamente es u^p, por tanto u^p es un $\mathbb{Q}_p-$conjugado de u. Finalmente, $\psi, \psi^2, \ldots, \psi^f$ seran $\mathbb{Q}_p$-automorfismos distintos, pues $\psi(u), \psi^2(u), \ldots, \psi^f(u)$ son distintos, y como $\#G(\mathbb{Q}_p(u)/\mathbb{Q}_p) = [\mathbb{Q}_p(u) : \mathbb{Q}_p] = f$ (como $\mathbb{Q}_p(u)/\mathbb{Q}_p$ es normal), concluiremos que ψ genera a $G(\mathbb{Q}_p(u)/\mathbb{Q}_p)$. □

Corolario 6.4.10 *Dado $f \in \mathbb{N}$, tenemos que la traza $T_{\mathcal{L}_f/\mathbb{Q}_p}$ de la extensión $\mathcal{L}_f/\mathbb{Q}_p$ cumple que*

$$T_{\mathcal{L}_f/\mathbb{Q}_p}(v) = v^p + v^{p^2} + \cdots + v^{p^r}, \quad \textit{para todo } v \in \mu_{(p)}(L).$$

Nótese que esta ecuación también es valida para $v = 0$.

Demostración.- Sea $u \in \mu_{(p)}$ una raíz primitiva $p^f - 1$-ésima de la unidad, entonces $G(\mathcal{L}_f/\mathbb{Q}_p) = \{\psi, \psi^2, \ldots, \psi^f\}$ donde ψ es determinado por $\psi(u) = u$. Dado $v \in \mu_{(p)}(L)$ existe $s \in \mathbb{N}$ tal que

$u^s = v$ (puesto que u es un generador de $\mu_{(p)}(L)$), luego

$$T_{\mathcal{L}_f/\mathbb{Q}_p}(v) = \sum_{i=1}^{f} \psi^i(v) = \sum_{i=1}^{f} (\psi^i(u))^s = \sum_{i=1}^{f} (u^{p^i})^s = \sum_{i=1}^{f} (u^s)^{p^i} = \sum_{i=1}^{f} v^{p^i}.$$

□

Si recordamos el lema 3.11.6 vemos un gran parecido con lo que acabamos de obtener acerca del grupo de automorfismo de $\mathcal{L}_f/\mathbb{Q}_p$. Con esta idea llegamos al siguiente lema, el cual nos muestra una estrecha relación que comparten una extensión no ramificada con su cuerpo residual con respecto a sus trazas. Esta relación sera vital para desarrollar en un posterior capítulo una extensión analítica de un concepto totalmente algebraico.

Lema 6.4.11 *Dado $f \in \mathbb{N}$, sean $\Bbbk_f$ el cuerpo residual de $\mathcal{L}_f$, $\mathcal{Z}_f$ el conjunto de ceros de $X^{p^f} - X \in \mathbb{Q}_p[X]$ y π la proyección canónica del anillo de valuación de $\mathcal{L}_f$ en $\Bbbk_f$. Entonces la restricción $\pi_{|\mathcal{Z}_f} : \mathcal{Z}_f \to \Bbbk_f$ es una biyección que respeta el producto. Más aún, si $\zeta = \pi^{-1}_{|\mathcal{Z}_f} : \Bbbk_f \to \mathcal{Z}_f$ tendremos que*

1. *Dado $A \in \Bbbk_f$, $\zeta(A)$ es una raíz $p^f - 1$-ésima de la unidad, cuando $A \neq 0$; en otro caso es igual a 0.*

2. *Dado $A \in \Bbbk_f$, se tiene que $A = \zeta(A) + \mathfrak{p}$.*

3. *Dados $A, B \in \Bbbk_f$, se cumple que*

$$\zeta(AB) = \zeta(A)\zeta(B) \quad y \quad \zeta(A+B) \equiv \zeta(A) + \zeta(B) \text{ mód } \mathfrak{p}.$$

4. *Si $T_{\mathcal{L}_f/\mathbb{Q}_p}$ y $T_{\Bbbk_f/\mathbb{F}_p}$ son las trazas de las extensiones $\mathcal{L}_f/\mathbb{Q}_p$ y $\Bbbk/\mathbb{F}_p$, respectivamente, entonces*

$$T_{\Bbbk_f/\mathbb{F}_p}(A) = T_{\mathcal{L}_f/\mathbb{Q}_p}(\zeta(A)) + \mathfrak{p}, \quad \textit{para todo } A \in \Bbbk_f.$$

Demostración.- Empecemos por mencionar que $\mu_{(p)}(L)$ es un grupo de $p^f - 1$ elementos; luego, por el teorema 6.4.5, tendremos $\pi(\mu_{(p)}(L)) = \Bbbk_f^\times$. Como $\mathcal{Z}_f = \mu_{(p)}(L) \cup \{0\}$, tendremos que $\pi_{|\mathcal{Z}_f}$ es una biyección, que respetará el producto.

Como $\pi(0) = 0$, se tendrá $\zeta(0) = 0$ y $\zeta(\Bbbk_f^\times) = \mu_{(p)}(L)$, de esta forma hemos probado el primer ítem. El segundo ítem no es mas que otra reformulación de la igualdad $\pi_{|\mathcal{Z}_f} \circ \zeta = \mathrm{id}$. Ahora, dados $A, B \in \Bbbk_f$, tenemos que

$$\zeta(AB) = \zeta\Big(\pi\big(\zeta(A)\big)\pi\big(\zeta(B)\big)\Big) = \zeta\Big(\pi\big(\zeta(A)\zeta(B)\big)\Big) = \zeta(A)\zeta(B).$$

Así también

$$\pi(\zeta(A)+\zeta(B)) = \pi(\zeta(A)) + \pi(\zeta(B)) = A + B = \pi(\zeta(A+B)),$$

por tanto $\zeta(A)+\zeta(B) \equiv \zeta(A+B)$ mód $\mathfrak{p}$. Y, finalmente, como esta descrito en el lema 3.11.10, dado $A \in \Bbbk_f$ se cumple que $T_{\Bbbk_f/\mathbb{F}_p}(A) = A + A^p \cdots + A^{p^{f-1}}$, lo cual unido al segundo ítem nos da

$$\begin{aligned} T_{\Bbbk_f/\mathbb{F}_p}(A) &= \zeta(A) + \mathfrak{p} + (\zeta(A)+\mathfrak{p})^p + \cdots + (\zeta(A)+\mathfrak{p})^{p^{f-1}} \\ &= \zeta(A) + \zeta(A)^p + \cdots + \zeta(A)^{p^{f-1}} + \mathfrak{p}. \end{aligned}$$

Puesto que $\zeta(A)$ es cero o una raíz $p^f - 1$–ésima de la unidad; por la proposición anterior verificamos que , en ambos casos, se obtiene $T_{\Bbbk_f/\mathbb{F}_p}(A) = T_{\mathcal{L}_f/\mathbb{Q}_p}(\zeta(A)) + \mathfrak{p}$. □

Ya hemos visto que el cuerpo residual sólo crece si es que se añaden elementos de $\mu_{(p)}$, el siguiente paso será mostrar que cuando adjuntamos elementos de $\mu_{p^\infty}(\mathbb{Q}_p^{alg})$, el índice de ramificación aumenta, pero antes daremos un lema que nos ayudará en este proposito.

Lema 6.4.12 *[Versión p–ádica del criterio de Eisenstein] Sea* $f(X) = a_r X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in \mathbb{Q}_p[X]$ *tal que*

- $v_p(a_r) = 0$,
- *Para* $i = 1, 2 \ldots, r-1$ *se tiene que* $v_p(a_i) \geq 1$,
- $v_p(a_0) = 1$.

Entonces $f(X)$ *es irreductible.*

Demostración.- Supongamos que existen $g(X) = b_s X^s + b^{s-1}X^{s-1} + \cdots + b_0$ y $h(x) = c_t X^t + c_{t-1}X^{t-1} + \cdots + c_0$ con coeficientes en $\mathbb{Z}_p[X]$ tales que $f(X) = g(X)h(x)$ (por tanto $s = r+t$). Entonces $a_r = b_s c_t$ y $a_0 = b_0 c_0$, por tanto $v_p(b_s) = v_p(c_t) = 0$ y alguno de los coeficientes independientes es divisible por p y el otro, no; supongamos que $v_p(c_0) = 1$ y $v_p(b_0) = 0$. Entonces, tomando $j_0 = \min\{j \; v_p(c_j) = 0\}$ tendremos que

$$a_{j_0+s} \equiv \sum_{i+k=j_0+s} c_i b_k \equiv c_{j_0} b_s + \sum_{i=0}^{j_0-1} c_i b_{j_0-i} \equiv c_{j_0} b_r \not\equiv 0 \text{ mód } p,$$

de ahi que $j_0 + s$ debe ser r y $j_0 = t$. Luego

$$a_r X^r \equiv f(x) \equiv c_t X^t (b_s X^s + \cdots + b_0) \equiv b_s c_t X^r + \cdots + b_0 c_t X^t \text{ mód } p,$$

por tanto $s = 0$ y la factorización necesariamente es trivial. Con esto, la versión p–ádica del lema de Gauss nos asegura la irreductibilidad en $\mathbb{Q}_p[X]$. □

Definición 6.4.13 Si $f(X) \in \mathbb{Q}_p[X]$ es un polinomio que satisface las hipótesis del lema anterior, entonces $f(X)$ es denominado *polinomio de Eisenstein.*

Lema 6.4.14 *Sea $\zeta \in \mathbb{Q}_p^{alg}$ una raíz p-ésima de la unidad distinta de 1, se cumple que:*

- $\mathrm{Irr}\,(\zeta) = X^{p-1} + \cdots + 1$.
- $v_p(\zeta - 1) = 1/(p-1)$, *por lo tanto* $\zeta - 1$ *es un uniformizador de* $\mathbb{Q}_p(\zeta)$.
- *Para cada* $i \in \{1, 2, \ldots, p-1\}$, *se cumple que* $1 + \zeta + \zeta^2 + \cdots + \zeta^{i-1} \equiv i \bmod p$.

Demostración.- Como ζ es una raíz de $X^p - 1 = (X-1)(X^{p-1} + \cdots + X + 1)$, tendremos que ζ es raíz de $f(X) = X^{p-1} + \cdots + X + 1 \in \mathbb{Z}_p$. Realizando la composición de este último polinomio con $X + 1$ obtenemos que

$$f(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{X^p + \sum_{k=2}^{p} \binom{p}{k} X^k + pX}{X} = X^{p-1} + \sum_{k=2} \binom{p}{k} X^{k-1} + p.$$

Puesto que $p \mid \binom{p}{k}$ para k entre 1 y $p-1$, tendremos que $f(x+1)$ es un polinomio de Eisentein, por tanto irreductible en $\mathbb{Q}_p[X]$; en consecuencia, $f(X)$ también lo es, y será el polinomio minimal de ζ. Así también, $f(X+1)$ es el polinomio minimal de $\zeta - 1$ (pues es mónico e irreductible), lo que implica que $N_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}(\zeta - 1) = ((-1)^{p-1}p)^1$ (por el teorema 3.9.1), por tanto $v_p(\zeta - 1) = 1/(p-1) \cdot 1$ y se sigue el segundo ítem. Lo último es claro si recordamos el lema 6.4.1. □

Este lema muestra un caso donde el uniformizador de la extensión totalmente ramificada, que fue $\zeta - 1$ de $\mathbb{Q}_p(\zeta)$, posee un polinomio minimal que es de Eisenstein, veamos que esto es cierto en general.

Proposición 6.4.15 *Si π es un uniformizador de L una extensión finita totalmente de $\mathbb{Q}_p$, entonces* $\mathrm{Irr}\,(\mathbb{Q}_p, \pi)$ *es un polinomio de Eisenstein.*

Demostración.- Sea $n = [L : \mathbb{Q}_p] = e(L/\mathbb{Q}_p)$ y $\mathrm{Irr}\,(\mathbb{Q}_p, \pi) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}_p[x]$. Como $\mathrm{Irr}\,(\mathbb{Q}_p, \pi)$ es mónico, nuestra meta es mostrar, para cada $i \in \{1, 2, \ldots, n-1\}$, que $v_p(a_i) \geq 1$, y que $v_p(a_0) = 1$. Tomemos N una clausura normal de $L/\mathbb{Q}_p$ y $\alpha_1 = \pi, \alpha_2, \ldots, \alpha_n \in L$ como todas las raíces de $\mathrm{Irr}\,(\mathbb{Q}_p, \pi)$ en N (pues este polinomio irreductible se descompone en N); luego,

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n).$$

Por tanto, cada a_i es suma y producto de α_i's, en consecuencia

$$v_p(a_i) \geq \min\{v_p(\alpha_i), i = 1, 2, \ldots, n\} = v_p(\pi) = 1/n > 0,$$

y como son números $p-$ádicos, se tiene $v_p(a_i) \geq 1$, para cada i. Más aun, se puede ver que $a_0 = (-1)^n \alpha_1 \alpha_2 \cdots \alpha_n$, por tanto $v_p(a_0) = 1/n v_p(\alpha_1 \cdots \alpha_n) = n \cdot 1/n = 1$. □

6.5. Más acerca de $\mathbb{Q}_p^{alg}$

La siguiente proposición comenta algunos otros hechos que no hemos resaltado.

Proposición 6.5.1 *El cuerpo $\mathbb{Q}_p^{alg}$ es una extensión infinita de $\mathbb{Q}_p$, cuyo cuerpo residual $\Bbbk = \Bbbk_{\mathbb{Q}_p^{alg}}$ es una clausura algebraica de $\mathbb{F}_p$.*

Demostración.- Por el lema 6.4.12, tendremos que el polinomio $X^n - p \in \mathbb{Z}_p[X]$ es irreductible sobre $\mathbb{Q}_p[X]$, para todo $n \in \mathbb{N}$; por lo tanto $\mathbb{Q}_p^{alg}$ contiene subcuerpos que son extensiones de $\mathbb{Q}_p$ de grado n, para todo $n \in \mathbb{N}$. De esta manera hemos probado que $\mathbb{Q}_p$ es de infinito dimensional con $\mathbb{Q}_p$-espacio vectorial.

Veamos que $\Bbbk$ es una clausura algebraica de $\mathbb{F}_p$, como ya es cierto que es algebraica, demostremos que estas en las misma condiciones supuestas en la proposición 3.10.5. Sea $f(X) = X^r + \alpha_{r-1}X^{r-1} + \cdots + \alpha_0 \in \mathbb{F}_p[X]$ irreductible, verifiquemos que se descompone en $\Bbbk$, con lo cual culminaremos esta demostración. Existen $a_0, a_1, \ldots, a_{r-1} \in \mathbb{Z}_p$ tales que $\alpha_i = a_i + \mathfrak{p}$, para $i = 0, 1, \ldots, r-1$; luego, por el lema 5.3.9, tendremos que $g(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in \mathbb{Z}_p[X]$ es irreductible en $\mathbb{Q}_p[X]$. Como $\mathbb{Q}_p^{alg}$ es una clausura algebraica de $\mathbb{Q}_p$, exitiran $b_1, \ldots, b_r \in \mathbb{Q}_p^{alg}$ tales que $g(X) = (X - b_1)(X - b_2) \cdots (X - b_r)$. Puesto que $g(X)$ tiene coeficientes enteros p-ádicos y es el polinomio minimal de $b_1, \ldots, b_r$, entonces estos elementos pertenecen a $\mathcal{O}$; por lo tanto

$$f(X) = X^r + (a_{r-1} + \mathfrak{p})X^{r-1} + \cdots + (a_0 + \mathfrak{p}) = \big(X - (b_1 + \mathfrak{p})\big)\big(X - (b_2 + \mathfrak{p})\big) \cdots \big(X - (b_r + \mathfrak{p})\big),$$

con $b_i + \mathfrak{p} \in \Bbbk$, para $i = 1, 2, \ldots, r$. □

Observación 6.5.2 La primera afirmación de este teorema muestra otra diferencia entre $\mathbb{Q}_p$ y $\mathbb{R}$, ambas compleciones de $\mathbb{Q}$ bajo distintos valores absolutos. Mientras $\mathbb{R}$ posee una clausura algebraica de grado finito sobre él, el cuerpo $\mathbb{Q}_p$ posee una clausura algebraica de grado infinito.

Desde la segunda sección hemos utilizado propiedades y conceptos acerca de extensiones algebraicas sobre $\mathbb{Q}_p$ (ya sean la norma o grado de la extensión, por ejemplo), para obtener información de $|\cdot|_p$. Ahora haremos lo inverso, utilizaremos información sobre $|\cdot|_p$ en un elemento para conocer la extensión generada por este elemento. Así pues, recordando que toda extensión algebraica de $\mathbb{Q}_p$ tiene a $\mathbb{Q}_p^{alg}$ también como clasura algebraica, empecemos por el mostrar el siguiente utíl resultado.

Lema 6.5.3 *[Krasner] Sean L una extensión de $\mathbb{Q}_p$, $\alpha \in \mathbb{Q}_p^{alg}$ y sus $L-$conjugadas $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ en $\mathbb{Q}_p^{alg}$. Si $\beta \in \mathbb{Q}_p^{alg}$ satisface la desigualdad*

$$|\beta - \alpha|_p < \text{mín}\{|\alpha - \alpha_i|_p, i = 2, 3 \ldots, n\},$$

entonces $L(\alpha) \subset L(\beta)$

Demostración.- Comprobemos la proposición contrarecíproca. Sea $\beta \in \mathbb{Q}_p^{alg}$ tal que $L(\alpha) \not\subset L(\beta)$, o equivalentemente $\alpha \notin L(\beta)$. Entonces el grado de la extensión generada por α sobre $L(\beta)$ es mayor o igual a 2, por tanto α tiene una $L(\beta)-$conjugada en $\mathbb{Q}_p^{alg}$ distinta de si misma, por decir α_j. Sea σ el $L(\beta)$-isomorfismo que asigna α_i a α, entonces σ es un $\mathbb{Q}_p$-isomorfismo y enviará elementos algebraicos sobre $\mathbb{Q}_p$ en sus $\mathbb{Q}_p-$conjugados, y por tanto que es una isometria (recordar las observaciones 6.2.5). De ahí que $|\beta - \alpha_j|_p = |\sigma(\beta - \alpha)|_p = |\beta - \alpha)|_p$, en consecuencia

$$|\alpha_j - \alpha|_p \leq \text{máx}\{|\alpha_j - \beta|_p, |\beta - \alpha|_p\} = |\beta - \alpha_i|.$$

□

Corolario 6.5.4 *Sea $p \in \mathbb{N}$ un primo impar y $b \in \mathbb{Q}_p$ que no sea cuadrado perfecto. Entonces todo $a \in \mathbb{Q}_p$ tal que $|a - b|_p \leq |b|_p$ no es cuadrado perfecto y $\mathbb{Q}_p(\sqrt{b}) = \mathbb{Q}_p(\sqrt{a})$.*

Demostración.- Sean $\alpha, \beta \in \mathbb{Q}_p^{alg}$ tales que $\alpha^2 = a$ y $\beta^2 = b$, entonces $\beta \notin \mathbb{Q}_p$ y posee a $-\beta$ como $\mathbb{Q}_p$-coonjugada. Vemos que

$$|\alpha - \beta|_p|\alpha + \beta|_p = |a - b|_p < |\beta^2|_p = |\beta|_p^2,$$

por lo cual podémos decir que $|\alpha - \beta|_p < |\beta|_p$ o $|\alpha - (-\beta)|_p < |\beta|_p$. En el primer caso, tendremos que $|\alpha - \beta|_p < |2\beta|_p = |\beta - (-\beta)|_p$, por tanto $\mathbb{Q}_p(\beta) \subset \mathbb{Q}_p(\alpha)$, y como $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = \text{grad Irr}\,(\mathbb{Q}_p, \alpha) \leq 2$ (pues $x^2 - a$ se anula en α), conluimos que $\mathbb{Q}(\beta) = \mathbb{Q}_p(\alpha)$ y que $\alpha \notin \mathbb{Q}_p$. En el segundo caso, por el mismo razocinio deducimos que $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(-\beta)$ y llegamos a la misma conclusión. □

La siguiente proposición utilizaremos la extensión de $|\cdot|_p$ sobre una extensión algebraica L hacia su anillo de polinomios, por definir $\|f(x)\| = \text{máx}\{|a_i|_p\ ,\ i = 0, 1, \ldots, n\}$ para $f(x) = a_n x^n + \cdots + a_1 x + a_0$; así también utilizaremos la proposición 4.2.8.

Proposición 6.5.5 *Dado $\alpha \in \mathbb{Q}_p^{alg}$ y L una extensión algebraica de $\mathbb{Q}_p$, existe $\epsilon > 0$ tal que todo $g(x) \in L[x]$ mónico del mismo grado que α que satisfaga $\|\text{Irr}\,(L, \alpha) - g(x)\| < \epsilon$ necesariamente es irreducible y tiene una raíz β que cumple $L(\alpha) = L(\beta)$.*

Demostración.- Denotemos $f(X) = \text{Irr}\,(L, \alpha)$, $n = \text{grad}\, f(X)$ y a sus $L-$conjugados de *alpha* por $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n \in \mathbb{Q}_p^{alg}$. Estas raíces serán distintas, porque L es perfecto; por tanto $r = \text{mín}\{|\alpha_i - \alpha_j|_p\ ,\ 1 \leq i < j \leq n\} > 0$; tomemos $\epsilon = r^n/(2\,\text{máx}\{1, \|f(x)\|^n\})$. Sea $g(x) \in L[x]$ como en el enunciado, y sus n raíces $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{Q}_p^{alg}$. Entonces, por la proposición 4.2.8, tendremos que

$$\Big|\prod_{i,j=1}^{n}(\alpha_i - \beta_j)\Big|_p \leq \big(\epsilon\,\text{máx}\{1, \|f(x)\|^n\}\big)^n = \frac{r^{n^2}}{2^n} < r^{n^2}.$$

En consecuencia, se debe cumplir que $|\alpha_{i_0} - \beta_{j_0}| < r$ para algún $i_0, j_0 \in \{1, 2, \ldots, n\}$; luego en virtud del lema de Krasner obtenemos que $L(\alpha_{i_0}) \subset L(\beta_{j_0})$. Este última relación implica

$$n = \text{grad}\, f(X) = [L(\alpha_{i_0}) : L] \leq [L(\beta_{j_0}) : L] = \text{grad Irr}\,(L, \beta_{j_0}) \leq \text{grad}\, g(x) = n,$$

pues $\text{Irr}\,(L, \beta_{j_0}) \mid g(x)$ y los $L-$conjugados comporten el mismo grado sobre L. De esta forma, hemos concluido que $[L(\alpha_{i_0}) : L] = [L(\beta_{j_0}) : L]$ y $\text{grad Irr}\,(L, \beta_{j_0}) = \text{grad}\ g(X)$, por lo tanto $L(\alpha_{i_0}) = L(\beta_{j_0})$ y $g(x) = \text{Irr}\,(L, \beta_{j_0})$. Finalmente, tomando $\sigma : L(\alpha) \to L(\alpha_{i_0})$ el $L-$isomorfismo tal que $\sigma(\alpha) = \alpha_{i_0}$, obtenemos que

$$L(\alpha) = \sigma\big(L(\alpha_{i_0})\big) = L\big(\sigma(\beta_{j_0})\big) = L(\beta),$$

donde β es un $L-$conjugado de β_{j_0}. □

Corolario 6.5.6 *Dado $\alpha \in \mathbb{Q}_p^{alg}$, la extensión $\mathbb{Q}_p(\alpha)$ admite un subcuerpo F que es una extensión finita sobre $\mathbb{Q}$ tal que $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = [F : \mathbb{Q}]$*

Demostración.- Como $\mathbb{Q}_p$ es denso en $\mathbb{Q}$, podemos encontrar $g(X) \in \mathbb{Q}[X]$ mónico y de grado $n = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$ que satisfaga $\|\text{Irr}\,(\mathbb{Q}_p, \alpha) - g(X)\| < \epsilon$, donde $\epsilon > 0$ es como en la proposición previa. Luego, $g(X)$ es el polinomio minimal de algún $\beta \in \mathbb{Q}_p^{alg}$ tal que $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$. Como $g(X)$ es irreductible en $\mathbb{Q}_p[X]$, también lo sera $\mathbb{Q}[X]$; por tanto $F = \mathbb{Q}(\beta)$ tendra grado n sobre $\mathbb{Q}$, veamos que F es denso en $\mathbb{Q}_p(\alpha)$. Sea $x \in \mathbb{Q}_p(\alpha)$, existen $a_0, a_1, \ldots, a_n \in \mathbb{Q}_p$ tales que $x = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$. Dado $\epsilon > 0$, tomemos $r_0, r_1, \ldots, r_{n-1} \in \mathbb{Q}$ tales que $|r_i - a_i|_p < \epsilon/(2\,\text{máx}\{1, |\alpha|_p^{n-1}\})$ para $i = 0, 1, 2, \ldots, n-1$, entonces

$$|x - r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}|_p \leq \text{máx}\{|r_i - a_i|_p|\alpha|^i\ ,\ i = 0, 1, \ldots, n-1\} \leq \epsilon/2 < \epsilon.$$

□

Observación 6.5.7 Este último resultado sobre extensiones simples de $\mathbb{Q}_p$ ocurre en general para cualquier extensión finita. De hecho, uno de los resultados iniciales de la teoría de Galois dice que toda extensión finita y separable es una extensión simple.

Acerca de $\mathbb{R}$, la compleción arquimediana de $\mathbb{Q}$, sabemos que su clausura algebraica $\mathbb{C}$ es un cuerpo completo, por lo cual se podria esperar lo mismo de $\mathbb{Q}_p$, que su clausura algebraica $\mathbb{Q}_p^{alg}$ también fuese un cuerpo completo. Sin embargo esto no ocurre, dandonos así otra marcada diferencia con $\mathbb{R}$.

Proposición 6.5.8 *EL cuerpo $\mathbb{Q}_p^{alg}$ no es completo.*

Demostración.- Nuestra tarea es encontrar una sucesión de Cauchy en $\mathbb{Q}_p^{alg}$ que no sea convergente, y como sabemos que toda extensión finita de $\mathbb{Q}_p$ es completa, deberiamos procurar que cada término de la sucesión pertenezca a un cuerpo " más grande" que a la que pertenece el término anterior, para este fin utlizaremos $\mu_{(p)}$ el grupo de raíces de orden coprimo a p.

Para cada $i \in \mathbb{N}$, tomemos $m_i = p^{(i+1)!} - 1 \in \mathbb{N}$ y $\zeta_i \in \mu_{(p)}$ una m_i-ésima raíz primitiva de la unidad; además denotemos por ζ_0 a 1. Entonces, para cada $i \in \mathbb{N}$, se tendrá que

- $\mathbb{Q}_p(\zeta_{i-1}) \subset \mathbb{Q}_p(\zeta_i)$, pues ζ_{i-1} es una potencia ζ_i (por la observación 3.12.2).
- $[\mathbb{Q}_p(\zeta_i) : \mathbb{Q}_p(\zeta_{i-1})] = \dfrac{[\mathbb{Q}_p(\zeta_i) : \mathbb{Q}_p]}{[\mathbb{Q}_p(\zeta_{i-1}) : \mathbb{Q}_p]} = \dfrac{(i+1)!}{i!} = i+1.$

Definamos $(c_n)_{n\in\mathbb{N}} \subset \mathbb{Q}_p^{alg}$ por $c_n = \sum_{i=0}^{n} \zeta_i p^i$ para cada $n \in \mathbb{N}$. Esta sucesión sera de Cauchy pues $\lim |\zeta_i p^i|_p = 0$ (y $\mathbb{Q}_p^{alg}$ es no arquimediano); veamos que no es convergente, asumiendo su convergencia a $c \in \mathbb{Q}_p^{alg}$ con $k = [\mathbb{Q}_p(c) : \mathbb{Q}_p] \in \mathbb{N}$. Puesto que $\mathbb{Q}_p(\zeta_k)$ es normal sobre $\mathbb{Q}_p$, tendremos que $\mathbb{Q}_p(\zeta_k)/\mathbb{Q}_p(\zeta_{k-1})$ será normal (por la proposición 3.7.5), por tanto, el corolario 3.8.8 nos asegura que $\#G\big(\mathbb{Q}_p(\zeta_k)/\mathbb{Q}_p(\zeta_{k-1})\big) = [\mathbb{Q}_p(\zeta_k) : \mathbb{Q}_p(\zeta_{k-1})] = k+1$, denotemos a los elementos de este grupo por $\sigma_1, \sigma_2, \ldots, \sigma_{k+1}$. Tomando una clausura normal N de $\mathbb{Q}_p(\zeta_k, c)/\mathbb{Q}_p(\zeta_{k-1})$, podemos encontrar $\mathbb{Q}_p(\zeta_{k-1})-$automorfimos $\tau_1, \tau_2, \ldots, \tau_{d+1}$ de N que extiende a los anteriores automorfismos (por el teorema 3.7.10).

Afirmación : *Para $i, j \in \{1, 2, \ldots, d+1\}$ distintos se cumple $|\tau_i(c) - \tau_j(c)|_p = p^{-(k+1)}$.*

Como ζ_k define los $\mathbb{Q}_p(\zeta_{k-1})-$automorfismos de $\mathbb{Q}_p(\zeta_k)$ es necesario que $\sigma_i(\zeta_k) \neq \sigma_j(\zeta_k)$ para $i \neq j$; por lo tanto seran m_i-raíces distintas de la unidad. Luego, en virtud del lema 6.4.2, tenemos que $|\sigma_i(\zeta_k) - \sigma_j(\zeta_k)|_p = 1$ para distintos $i, j \in \{1, 2, \ldots, k+1\}$. Como

$$\sigma_i(c_k) = \sigma_i\Big(\sum_{i=0}^{k} \zeta_i p^i\Big) = \sum_{i=0}^{k-1} \zeta_i p^i + \sigma_i(\zeta_k) p^k, \quad \text{para todo } i = 1, 2, \ldots, d+1,$$

se cumple que

$$|\sigma_i(c_k) - \sigma_j(c_k)|_p = |\sigma_i(\zeta_k) - \sigma_j(\zeta_k)|_p p^{-k} = p^{-k}, \quad \text{para } 1 \leq i < j \leq n. \tag{6.1}$$

Por otra parte, las observaciones 6.2.5, se tendra que

$$|\tau_i(c) - \tau_j(c_k)|_p = |c - c_k|_p = |\sum_{i=k+1}^{\infty} \zeta_i p^i|_p = \lim_{n\to\infty} |\sum_{i=k+1}^{n} \zeta_i p^i|_p = p^{-k}, \tag{6.2}$$

para $1 \leq i < j \leq n$. Por las ecuaciones (6.1) y (6.2) tendremos, para i y j distintos, que

$$|\tau_i(c) - \tau_j(c)| = \text{máx}\{|\tau_i(c) - \tau_i(c_k)|_p, |\tau_i(c_k) - \tau_j(c_k)|_p, |\tau_i(c_k) - \tau_i(c)|_p\} = 1.$$

De esta afirmación deducimos que $\tau_1(c), \tau_2(c), \ldots, \tau_{k+1}(c)$ son distintos $\mathbb{Q}_p(\zeta_{k-1})$-conjugados; por lo tanto grad Irr $(\mathbb{Q}_p(\zeta_{k-1}), c) \geq k+1$. Como grad Irr $(\mathbb{Q}_p(\zeta_{k-1}), c) \leq$ grad Irr $(\mathbb{Q}_p, c) = k$, vemos que hemos llegado a un absurdo; por lo tanto (c_n) no es converge en $\mathbb{Q}_p^{alg}$. □

6.6. El cuerpo de números complejos p-ádicos $\mathbb{C}_p$

Con el fin de obtener un cuerpo completo que contenga a $\mathbb{Q}_p^{alg}$ tomamos denotamos por $\mathbb{C}_p$ una compleción de éste, cuyo valor absoluto (no arquimediano) también lo denotamos $|\cdot|_p$. Este último paso genera incertidumbre respecto al comportamiento algebraico de $\mathbb{C}_p$, pues como acabamos de ver en $\mathbb{Q}_p^{alg}$, podemos obtener un cuerpo algebraicamente cerrado que no es completo, ahora que $\mathbb{C}_p$ es completo, ?' sucederá que $\mathbb{C}_p$ no es algebraicamente cerrado?. El siguiente teorema responde esta duda y además muestra el por qué de la notación para este nuevo cuerpo.

Teorema 6.6.1 *El cuerpo $\mathbb{C}_p$ es algebraicamente cerrado.*

Demostración.- Aqui también haremos uso de la extensión de $|\cdot|_p$ sobre $\mathbb{C}_p[X]$, es decir $\|f(X)\| = \text{máx}\{|a_0|_p, |a_1|_p, \ldots, |a_n|_p\}$ para todo $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}_p[X]$, así como también de los resultados de la proposición 4.2.8. Dado $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{C}_p[X]$, encontremos una raíz en $\mathbb{C}_p$. Puesto que $\mathbb{Q}_p^{alg}$ es denso en $\mathbb{C}_p$ (por ser $\mathbb{C}_p$ una compleción de $\mathbb{Q}_p^{alg}$), podemos encontrar $(a_{0,j})_{j\in\mathbb{N}}, (a_{1,j})_{j\in\mathbb{N}}, \ldots, (a_{n-1,j})_{j\in\mathbb{N}} \subset \mathbb{Q}_p^{alg}$ tales que $\lim_{j\to\infty} a_{i,j} = a_i$, para cada $i \in \{0, 1, \ldots, n-1\}$. Tomando, para cada $j \in \mathbb{N}$, $g_j(x) = x^n + a_{n-1,j}x^{n-1} + \cdots + a_{1,j}x + a_{0,j} \in \mathbb{Q}_p^{alg}[x]$, tendremos claramente que la sucesión $(A_j)_{j\in\mathbb{N}}$, formada por $A_j = \|f(x) - g_j(x)\|$, converge a cero. De lo cual, tomando $(B_j) \subset \mathbb{R}$ definida por $B_j = \text{máx}\{A_j, A_{j+1}\}$ para cada $j \in \mathbb{N}$, obtenemos una sucesión que converge a cero. Además, podemos ver que $(\|g_j(x)\|)_{j\in\mathbb{N}}$ converge a $\|f(x)\|$; en particular, esta acotada por algún $C > 0$.

Afirmación : *Dado $j \in \mathbb{N}$ y $r_j \in \mathbb{Q}_p^{alg}$ una raíz de $g_j(x)$, existirá una raíz $r_{j+1} \in \mathbb{Q}_p^{alg}$ de $g_{j+1}(x)$ tal que $|r_j - r_{j+1}|_p \leq \sqrt[n]{B_j}\,\text{máx}\{1, C\}$.*

Denotando por $r_{1,j+1}, r_{2,j+1}, \ldots, r_{n,j+1}$ a las raíces de $g_{j+1}(x)$ en $\mathbb{Q}_p^{alg}$, obtendremos $g_j(x) = (x - r_{1,j+1})(x - r_{2,j+1}) \cdots (x - r_{n,j+1})$ y

$$\prod_{i=1}^{n} |r_j - r_{i,j+1}|_p = |g_{j+1}(r_j)|_p = |g_{j+1}(r_j) - g_j(r_j)|_p \leq \text{máx}\{\|g_{j+1}(r_j) - f(r_j)\|, \|f(r_j) - g_j(r_j)\|\};$$

por tanto

$$\prod_{i=1}^{n} |r_j - r_{i,j+1}|_p \leq B_j \,\text{máx}\{1, |r_j|_p^n\} \leq B_j \,\text{máx}\{1, \|g_j(x)\|^n\} \leq B_j \,\text{máx}\{1, C^n\}.$$

De esta última desigualdad, podemos inferir que para algún $i_j \in \{1, 2, \ldots, n\}$ verifica la afirmación.

Gracias a esta afirmación podemos construir una sucesión $(r_j)_{j\in\mathbb{N}} \subset \mathbb{Q}_p^{alg}$ que cumple $\lim_{j\to\infty} |r_j - r_{j+1}|_p = 0$. Como $\mathbb{Q}_p^{alg}$ es no arquimediano, la sucesión (r_j) sera de Cauchy, por tanto será convergente a algún $r \in \mathbb{C}_p$. Recordando la proposición 4.2.8, tendremos que

$$|f(r_j)|_p = |f(r_j) - g_j(r_j)|_p \leq A_j \,\text{máx}\{1, |r_j|_p^n\} \leq A_j \,\text{máx}\{1, C^n\},$$

para todo $j \in \mathbb{N}$; por lo tanto, $f(r) = \lim_{j\to\infty} f(r_j) = 0$. □

Observación 6.6.2 Al cuerpo $\mathbb{C}_p$ se le conoce como el *cuerpo de números p-ádicos complejos.*

De esta forma encontramos un cuerpo que extienda al valor absoluto sobre $\mathbb{Q}_p$ donde podemos estudiar aspectos algebraicos como analíticos. Más aún podemos ver que es el menor de estos.

Proposición 6.6.3 *Si Ω es un cuerpo completo y algebraicamente cerrado que contiene a $(\mathbb{Q}, |\cdot|_p)$, entonces Ω contiene a un cuerpo isometrico e isomoformo a $\mathbb{C}_p$.*

Demostración.- Como $(\mathbb{Q}, |\cdot|_p)$ esta contenido en Ω y éste es completo, la cerradura topológica F de $\mathbb{Q}$ en Ω será una compleción de $(\mathbb{Q}, |\cdot|_p)$; por tanto F será isomorfo e isometrico a $(\mathbb{Q}_p, |\cdot|_p$. Puesto que Ω es algebraicamente cerrado, el cuerpo F^{alg}, conjunto de elementos algebraicos sobre F, será una clausura algebraica para éste mismo y por tanto será isomorfaa $\mathbb{Q}_p^{alg}$; también será isometrica, como la definición de las extensiones de $|\cdot|_p$ sobre extensiones algebraicas sólo esta sujetas a las propiedades algebraicas de estas mismas. Luego tomando la cerradura topológica de F^{alg} respecto a Ω, tendremos un cuerpo isometrico e isomorfo a $\mathbb{C}_p$. □

Definición 6.6.4 En el cuerpo $\mathbb{C}_p$ establecemos:

- El anillo y ideal de valuación de $\mathbb{C}_p$ denotado por $\mathfrak{D}_p$ y $\mathfrak{d}_p$, respectivamente; y al cuerpo residual, por $\mathfrak{K}_p$.

- Dado $m \in \mathbb{N}$, al conjunto de raíces de la unidad de orden m en se le denotará por $\mathfrak{U}_p^m$.

- El conjunto

$$\mathcal{T}_p = \{a \in \mathbb{C}_p \; ; \; a^{p^s} = a \text{ , para algún } s \in \mathbb{N}\}.$$

A cada elemento de $\mathcal{T}_p$ se le denominará representante de Teichmüller.

La siguiente proposición es resultado inmediato de las proposiciones 4.3.14 y 6.5.1.

Proposición 6.6.5 *El cuerpo $\mathfrak{K}_p$ es una clausura algebraica de $\mathbb{F}_p$.*

El siguiente resultado es semejante al lema 6.4.11 y muestra la importancia de los representantes de Teichmüller en $\mathbb{C}_p$.

Lema 6.6.6 *Sea $\pi : \mathcal{T}_p \to \mathfrak{K}_p$ la proyección canónica restringida a $\mathcal{T}_p$, entonces π es una biyección que respeta el producto. Si $\zeta = \pi^{-1} : \mathfrak{K}_p \to \mathcal{T}_p$ tendremos que*

1. *Dado $A \in \mathfrak{K}_p$, se tiene que $A = \zeta(A) + \mathfrak{d}_p$.*

2. *Dados $A, B \in \mathfrak{K}_p$, se cumple que*

$$\zeta(AB) = \zeta(A)\zeta(B) \quad y \quad \zeta(A+B) \equiv \zeta(A) + \zeta(B) \text{ mód } \mathfrak{d}_p.$$

Además, si $f \in \mathbb{N}$ y $\widetilde{\mathbb{k}}_f$ es el subcuerpo de p^f elementos contenido en $\mathfrak{K}_p$ entonces

3. $\zeta(\mathfrak{d}_p) = 0$ *y* $\zeta(\widetilde{\mathbb{k}}_f^{\times}) = \mathfrak{U}_p^{p^f-1}$.

4. $T_{\widetilde{\mathbb{k}}_f/\mathbb{F}_p}(A) = T_{\mathcal{L}_f/\mathbb{Q}_p}(\zeta(A)) + \mathfrak{d}_p$, *para todo $A \in \mathbb{k}_f$, donde $\mathcal{L}_f$ es la extensión no ramificada de grado f.*

Demostración.- Sean $f \in \mathbb{N}$, $\mathbb{k}_f$ el cuerpo residual de $\mathcal{L}_f$, $\mathcal{Z}_f$ el conjunto de ceros de $X^p - X$ en $\mathbb{C}_p$ y $\pi_f : \mathcal{Z}_f \to \mathbb{k}_f$ la restricción de la proyección canónica de $\mathcal{O}_f$ sobre $\mathbb{k}_f$. Por el lema 4.1.11, tendremos que $j : a + \mathfrak{p} \mapsto a + \mathfrak{K}_p$ es un monomorfismo $\mathbb{k}_f$ entre $\mathfrak{K}_p$, cumpliendosé entonces $\pi_{|\mathcal{Z}_f} = j \circ \pi_f$.

Por el lema 6.4.11, tendremos que π_f sera una biyección entre $\mathcal{Z}_f$ y $\mathbb{k}_f$. Entonces $\pi_{|\mathcal{Z}_f} = j \circ \pi_f$ será inyectiva, y $\pi(\mathcal{Z}_f) = j(\mathbb{k}_f) \subset \mathfrak{K}_p$ será un cuerpo de p^f de elementos, para todo $f \in \mathbb{N}$. Puesto que $\bigcup_{f\in\mathbb{N}} \mathcal{Z}_f = \mathcal{T}_p$, tendremos que π es una función inyectiva que respeta el producto. Como $\mathfrak{K}_p$ es una clausura algebraica de $\mathbb{F}_p$, por el teorema 3.11.7 concluimos que π es sobreyectiva.

Si $\zeta = \pi^{-1} : \mathcal{R}_p \to \mathcal{T}_p$, entonces el primer y segundo ítem son demostrados de la misma forma que sus analogos en el lema 6.4.11. Dado $f \in \mathbb{N}$, denotemos $\zeta_f = \pi_f^{-1} : \mathbb{k}_f \to \mathcal{Z}_f$. Se tiene que $\zeta \circ \pi_{|\mathcal{Z}_f} = \mathrm{id}_{\mathcal{Z}_f}$, por tanto $(\zeta \circ j) \circ \pi_f = \mathrm{id}_{\mathcal{Z}_f}$. Asi obtenemos que

$$\zeta \circ j = (\zeta \circ j) \circ (\pi_f \circ \zeta_f) = ((\zeta \circ j) \circ \pi_f) \circ \zeta_f = \zeta_f. \tag{6.3}$$

Como $j(\mathbb{k}_f)$ es un cuerpo de p^f elementos y $\mathcal{R}_p$ es una clausura algebraica de $\mathbb{F}_p$ tendremos que $j(\mathbb{k}_f) = \tilde{\mathbb{k}}_f$ y j es un isomorfismo. Este hecho junto con la ecuación (6.3) y el lema 6.4.11 implican al ítem 3.. Así también, si $A \in \tilde{\mathbb{k}}_f$ entonces

$$T_{\tilde{\mathbb{k}}_f/\mathbb{F}_p}(A) = \sum_{i=1}^{f} A^{p^i} = j\Big(\sum_{i=1}^{f} j^{-1}(A)^{p^i}\Big) = j\Big(T_{\mathbb{k}_f/\mathbb{F}_p}\big(j^{-1}(A)\big)\Big) = j\Big(T_{\mathcal{L}_f/\mathbb{Q}_p}\big(\zeta_f(j^{-1}(A))\big) + \mathfrak{p}_{\mathcal{L}_f}\Big),$$

por tanto $T_{\tilde{\mathbb{k}}_f/\mathbb{F}_p}(A) = T_{\mathcal{L}_f/\mathbb{Q}_p}(\zeta(A)) + \mathfrak{d}_p$. □

Capítulo 7

La valuación X-ádica y el anillo de series formales

Este capítulo sera el sustento riguroso al manejo intuitivo de series formales y sus evaluaciones en estas. La cuarta sección ejempliza las tres primeras cuya notación y cálculo es grande. Y, en la última sección, estudiaremos tres importantes series formales provenientes del cálculo: serie exponencial, la serie logaritmo y la serie binomial.

Durante estas tres primeras secciones fijaremos un dominio D y un número natural n. Denotemos al anillo de series de potencias en variables las variables $X_1, X_2, \ldots, X_n$ simplemente por $D[[X]]$; nuevamente, $\mathfrak{N}$ denotará al conjunto de multiíndices respectivos.

7.1. La valuación $X-$ádica y el anillo de series formales

Definición 7.1.1 El *peso* de un multiíndice $u = (u_1, u_2, \ldots, u_n) \in \mathfrak{N}$, denotado por $|u|$, es $u_1 + u_2 + \cdots + u_n$.

Observaciones 7.1.2

- Dados $u, v \in \mathfrak{N}$ se tiene que $|u + v| = |u| + |v|$.
- Sea $f(X) = \sum_u a_u X^u, g(X) = \sum_v b_v X^v \in D[[X]]$ y $f(X)g(X) = c_w X^w$. Como $c_w = \sum_{u+v=w} a_u b_v$, entonces que estos multindices u y v poseen pesos no mayores w (por ejemplo, tenemos que $|u| \leq |u| + |v| = |w|$).

A continuación daremos algunas otras definiciones acerca del conjunto de índices, las cuales seran muy utiles en futuras demostraciones.

Definición 7.1.3 Sean $m \in \mathbb{N}$ y $u = (u_1, u_2, \ldots, u_n) \in \mathfrak{N}$.

- El *orden lexicografico en* $\mathfrak{N}$, es aquel orden parcial que ordena a dos elementos comparando sucesivamente las componentes de estos hasta encontrar una componente que sea menor o igual a la otra componente correspondiente.
- Diremos que m *divide a* u si m divide a $u_1, u_2, \ldots, u_n$. Este hecho sera denotado como $m \mid u$; en caso contrario, escribiremos $m \nmid u$.
- Denotaremos por mu al multiindice $(mu_1, mu_2, \ldots, mu_n)$.
- El multiindice $u^m \in \mathfrak{N}$ esta definido por $(u_1^m, u_2^m, \ldots, u_n^m)$.
- Cuando no haya peligro de confusión, los simbolos 0 y 1 también denotaran a los multiindices $(0, 0, \ldots, 0)$ y $(1, 1, \ldots, 1)$, respectivamente.

Definición 7.1.4 La *valuación X-ádica sobre* $D[[X]]$ es definida por $\omega_X(f(X)) = \min\{|u| \; ; \; a_u \neq 0\}$ cuando $f = \sum_u a_u X^u$.

Proposición 7.1.5 *La función* ω_X *es una valuación sobre* $D[[X]]$.

Demostración.- Sean $f(X) = \sum_u a_u X^u, g(X) = \sum_v b_u X^u \in D[[X]]$ no nulos. Tomemos u_0 y v_0 tal que $|u_0| = \omega_X(f(X))$ y $|v_0| = \omega_X(g(X))$, entonces cuando $w \in \mathfrak{N}$ con $|w| < \min\{|u_0|, |v_0|\}$, ocurrirá que $a_w + b_w = 0$; por lo tanto

$$\omega_X(f(X) + g(X)) = \min\{|w| \; ; \; a_w + b_w \neq 0\} \geq \min\{\omega_X(f(X)), \omega_X(g(X))\}.$$

Ahora, denotemos $f(X)g(X)$ por $\sum_w c_w X^w$, y elijamos $u^0, v^0 \in \mathfrak{N}$ como

$$u^0 = \max\{u \in \mathfrak{N} \; ; \; |u| = \omega_X(f(X))\} \quad \text{y} \quad v^0 = \max\{v \in \mathfrak{N} \; ; \; |v| = \omega_X(f(X))\},$$

donde el orden en el cual se compara es el lexicografico, nótese que existen estos multiindices indexan un coeficiente no nulo de $f(X)$ y $g(X)$, respectivamente; afirmamos que el multiindice $w^0 = u^0 + v^0$ indexa un coeficiente no nulo. En efecto, el coeficiente c_{w^0} es $\sum a_u b_v$, donde los índices u y v son tales que $u + v = w^0$. entonces cuando $|u| < |u^0| = |u_0|$ tendremos que el sumando $a_u b_v$ sería nulo; pero también lo sería cuando $|u| > |u^0|$ (pues en ese caso $|v| < |v^0| = |v_0|$). Por lo tanto, los únicos sumandos posiblemente no nulos son aquellos indexados por los multiindices u y v que satisafagan $|u| = |u^0|$ y, en consecuencia, $|v| = |v^0|$; procedamos a evaluar un par de estos multiindices: $u = (u_1, \ldots, u_n)$ y $v = (v_1, \ldots, v_n)$. Denotando $w^0 = (w_1^0, \ldots, w_n^0)$, deducimos que si $u_1 < u_1^0$ entonces

$$w_1^0 = u_1 + v_1 < u_1^0 + v_1^0 = w_1^0,$$

pues $v_1 \leq v_1^0$ (por definición de v^0); por lo cual es necesario que $u_1 = u_1^0$, y, en consecuencia, $v_1 = w_1^0 - u_1 = w_1^0 - u_1^0 = v_1^0$. De igual forma podemos deducir, sucesivamente, que $u_i = u_i^0$ y $v_i = v_i^0$ para $i = 2, 3, \ldots, n$. Por lo tanto, el único sumando en la anterior suma es $a_{u^0} b_{v^0}$, el cual es no nulo; así es como concluimos que $\omega_X(f(X)g(X)) \geq \omega_X(f(X)) + \omega_X(g(X))$. Más aun, siguiendo el mismo razonamiento acerca de los multiindices que aparecen en c_{w^0}, obtendremos que no existen sumandos $a_u b_v$ no nulos con $u + v = w$ cuando $|w| < |w^0|$. Por lo tanto $c_w = 0$, para todo $w \in \mathfrak{N}$ con $|w| < |w^0|$; de esta forma concluimos que $\omega_X(f(X)g(X)) = \omega(f(X)) + \omega(g(X))$. □

Observaciones 7.1.6

- Una consecuencia inmediata es que $D[[X]]$ es un dominio.
- Dado $f(X) \in D[[X]]$ y $n \geq 0$, vemos que $\omega_X(f(X)) > n$ si y sólo si $f(X)$ no presenta términos de grado menores o iguales a n.

La proposición anterior y la proposición 4.2.5 brindan sentido a la siguiente definición.

Definición 7.1.7 El *valor absoluto $X-$ádico sobre $D[[X]]$* es definida por $|f(X)|_X = e^{-\omega_X(f(X))}$ para cada $f(X) \in D[[X]]$.

Proposición 7.1.8 *El dominio $(D[[X]], |\cdot|_X)$ es completo.*

Demostración.- Sea $(f_k(X)) \subset D[[X]]$ una sucesión de Cauchy. Puesto que la sucesión es de Cauchy, podemos escojer una secuencia escritamente creciente $(N_k) \subset \mathbb{N}$ tal que

$$|f_m(X) - f_{N_k}(X)|_X < e^{-k} \quad \text{para todo } m \geq N_k.$$

Si escribiremos $f_m(X) = \sum_u a_u^{(m)} X^u$ para cada $m \in \mathbb{N}$, esta última desigualdad significará que dados $k \in \mathbb{N}_0$ y $|u| \leq k$, se tendra que

$$a_u^{(m)} = a_u^{(N_k)}, \quad \text{cuando } m \geq N_k.$$

Con esto presente, definamos $a_u = a_u^{N_k}$ para cada $u \in \mathfrak{N}$ tal que $|u| = k$, y $f(X) = \sum_u a_u X^u$. Entonces, dado $k \geq 0$ tendremos que

$$\begin{aligned} f(X) - f_{N_k}(X) &= \sum_{j=0}^{k} \Big(\sum_{|u|=k} (a_u - a_u^{(N_k)}) X^u \Big) + \sum_{|u|>k} (a_u - a_u^{(N_k)}) X^u \\ &= \sum_{j=0}^{k} \Big(\sum_{|u|=k} (a_u - a_u^{(N_j)}) X^u \Big) + \sum_{|u|>k} (a_u - a_u^{(N_k)}) X^u; \end{aligned}$$

pues $N_j \leq N_k$ para cada $j \leq k$. Luego, $|f(X) - f_{N_k}(X)|_X < e^{-k-1}$, para cada $k \in \mathbb{N}_0$; por lo cual la subsucesión $(f_{N_k}(X))$ converge a $f(X)$. Como es bien sabido, al ser (f_m) una sucesión de Cauchy, está debe de ser convergente y converger al mismo elemento que cualquiera de la subsucesión convergente. □

Observaciones 7.1.9

- Esta demostración nos permite concluir lo siguiente

  > Una sucesión $(f_m(X)) \subset D[[X]]$ converge a $f(X) \in D[[X]]$, respecto a $|\cdot|_X$, si y sólo si para cada multiindice $u \in \mathfrak{N}$, el coeficiente indexado por u de estas series se estabilizan, para un $m \in \mathbb{N}$ suficientemente grande.

- Dado $f(X) \in D[[X]]$ y $(f_m(X)) \subset D[[X]]$ tal que $f(X) = \lim_{m\to\infty} f_m(X)$. Dado $r \geq 0$, existe $M > 0$ tal que los coeficientes de $f(X)$ y $f_m(X)$ indexados por multiindices de peso menor a o igual a r coinciden. De hecho, basta tomar $M > 0$ tal que $m \geq M$ implique $|f_m(X) - f(X)|_X < e^{-r}$, y utilizar el segundo ítem de la anterior observación.

- El valor absoluto $X-$ádico es no arquimediano, pues proviene de una valuación. Más aun vemos que $|\cdot|_X$ no extiende a $|\cdot|_p$ sobre $\mathbb{Q}_p[[X]]$; de hecho, este valor absoluto extiende al trivial.

Proposición 7.1.10 *El subespacio $D[X]$ es denso $D[[X]]$. Más aun, todo elemento $f(X) \in D[[X]]$ existe una única secuencia $(\alpha_u)_{u\in\mathfrak{N}} \subset D$ tales que $f(X)$ es el límite $\sum_{u\in\mathfrak{N}} \alpha_u X^u \in D[[X]]$.*

Demostración.- Si $f(X) = \sum \alpha_u X^u$, entonces tomamos $a_u = \alpha_u$ para todo $u \in \mathfrak{N}$. Dado $\epsilon > 0$, elegimos $n_0 \in \mathbb{N}$ tal que $e^{-n_0} < \epsilon$ y $F_0 = \{u \in \mathfrak{N}; |u| < n_0\}$ (que es finito). Entonces para cada subconjunto finito $F \supset F_0$ se cumple que $f(X) - \sum_{u\in F} a_u X^u$ es una serie sin ningun monomio de grado menor a n_0; por lo tanto $|f(X) - \sum_{u\in F} a_u X^u|_x \leq e^{-n_0} < \epsilon$. Como $\epsilon > 0$ fue arbitrario, concluimos que existe la suma de $(a_u X^u)_{u\in\mathfrak{N}}$ y $\sum_{u\in\mathfrak{N}} a_u X^u = f(X)$ (por la proposición 4.4.11). Finalmente verifiquemos la unicidad, suponiendo que existe otra sucesión $(b_u)_{u\in\mathfrak{N}} \subset D$ distinta de $(a_u)_{u\in\mathfrak{N}}$ tal que $f(X) = \sum_{u\in\mathfrak{N}} b_u X^u$. Entonces, tomando $u_0 \in \mathfrak{N}$ tal que $a_{u_0} \neq b_{u_0}$ y $F_0 \subset \mathfrak{N}$ finito tal que

$$|f(X) - \sum_{u\in F_0} a_u X^u|_X < \epsilon \qquad \text{y} \qquad |f(X) - \sum_{u\in F_0} b_u X^u|_X < e^{-|u_0|}.$$

entonces

$$|\sum_{u\in F_0} (a_u - b_u) X^u| \leq \text{máx}\{|f(X) - \sum_{u\in F_0} a_u X^u|_X, |f(X) - \sum_{u\in F_0} b_u X^u|_X\} < e^{|u_0|},$$

lo que contradice que $\omega\left(\sum_{u\in F_0}(a_u-b_u)X^u\right)\leq|u_0|$; esta contradiccón muestra la unicidad de la sucesión $(a_u)_{u\in\mathfrak{N}}$. □

Observación 7.1.11 Esta proposición simplemente se puede enunciar como: " $\{X^u\ ;\ u\in\mathfrak{N}\}$ es una base Schauder de $(D[[X]],|\cdot|_X)$"(para encontrar esta terminologia puede ver [12]).

7.2. Composición entre series formales

Este valor absoluto nos permitirá definir nuevas operaciones entre series de potencias. Por ejemplo, si $f(X)=\sum_u a_uX^u\in D[X]$ y $g_1(X),\ldots,g_n(X)\in D[[X]]$ entonces es natural definir

$$f(g_1(X),\ldots,g_n(X))=\sum_u a_u(g_1(X)^{u_1}\cdots g_n(X)^{u_n}),$$

veamos que podemos extender esta definición para el caso en que $f(X)\in D[[X]]$.

Proposición 7.2.1 *Sean* $f(X)=\sum_u a_uX^u\in D[[X]]$ *y* $g_1(X),\ldots,g_n(X)\in D[[X]]$ *tales que* $\omega_X(g_i(X))>0$ *para cada* $i\in\{1,2,\ldots,n\}$. *Si* $f_d(X)=\sum_{|u|\leq d}a_uX^u\in D[X]$, *entonces existe* $\lim_{d\to\infty}f_d(g_1(X),\ldots,g_n(X))$

Demostración.- Dado $d\in\mathbb{N}$, tenemos que

$$\begin{aligned}|f_{d+1}(X)-f_d(X)|_X &= \Big|\sum_{|u|=d+1}a_u(g_1(X))^{u_1}\cdots(g_n(X))^{u_n}\Big|_X\\ &\leq \text{máx}\{|g_1(X)|_X^{u_1}\cdots|g_n(X)|_X^{u_n}\ ;\ |u|=d+1\},\end{aligned}$$

y gracias a la hipótesis acerca de cada $\omega_X(g_i(X))$ deducimos que

$$|f_{d+1}(X)-f_d(X)|_X\leq\text{máx}\{(e^{-1})^{u_1}\cdots(e^{-1})^{u_n}\ ;\ |u|=d+1\}=e^{-d-1};$$

por lo tanto $(f_d(X))_{d\in\mathbb{N}}$ es de Cauchy, luego convergente en $D[[X]]$. □

Observación 7.2.2 El segundo ítem de esta última proposición se puede mejorar. Admitiendo las mismas notaciones de la proposición, tendremos que

$$\lim_{d\to\infty}f_d(g_1(X),\ldots,g_n(X))=\sum_{u\in\mathfrak{N}}a_ug_n(X)^{u_n}\cdots g_1(X)^{u_1}$$

como suma en $D[[X]]$ de sumandos indexados por el conjunto infinito numerable $\mathfrak{N}$. De hecho, dado $u\in\mathfrak{N}$ tendremos que

$$|a_ug_1(X)^{u_1}\cdots g_n(X)^{u_n}|_X\leq e^{-u_1}\cdots e^{-u_n}=e^{-|u|}.$$

Por lo tanto, dado $\epsilon > 0$, basta tomar $r \in \mathbb{N}$ tal que $e^{-r} < \epsilon$, para obtener que todo $u \in \mathfrak{N}$ y $|u| > r$ cumple

$$|a_u g_1(X)^{u_1} \cdots g_n(X)^{u_n}|_X \leq e^{-|u|} < \epsilon;$$

de este modo, en virtud de la proposición 4.4.11 concluimos que existe la suma mencionada, y por el lema 4.4.14 concluimos la igualdad mencionada.

De ahora en adelante, denotaremos por $\mathfrak{p}_X$ al *ideal de valuación de* ω_X. Por lo tanto, dado $f(X) \in D[[X]]$, tendremos $\omega_X(f(X)) > 0$ si solo si $f(X) \in \mathfrak{p}_X$.

Definición 7.2.3 Sean $f(X), g_1(X), g_2(X) \ldots, g_n(X) \in D[[X_1, \ldots, X_n]]$ donde $g_i(X) \in \mathfrak{p}_X$, para $1 \leq i \leq n$. Definimos la *composición de series de* $f(X)$ y $g(X)$ por

$$f(X) \circ (g_1(X), g_2(X), \cdots, g_n(X)) = \sum_{u \in \mathfrak{N}} a_u g_1(X)^{u_1} g_2(X)^{u_2} \cdots g_n(X)^{u_n}.$$

Observaciones 7.2.4

- Como vemos, resulta engorrosa esta notación, la cual menciona un concepto muy sencillo, por lo tanto la reduciremos. Cada $n-$ada de series formales $(g_1(X), g_2(X), \cdots, g_n(X))$ sera representada como $g(X) \in D[[X]]^n$, siempre y cuando no haya peligro a confución; por tanto la anterior notación se reduce $f(X) \circ g(X)$ para mencionar a la composición de la serie formal $f(X)$ con la n-ada $g(X) = (g_1(X), g_2(X), \cdots, g_n(X))$.

- Con el mismo espiritu del ítem anterior, dado $u = (u_1, \ldots, u_n) \in \mathfrak{N}$ y $g(X) = (g_1(X), \ldots, g_n(X))$ definimos $g(X)^u = g_1(X)^{u_1} \cdots g_n(X)^{u_n}$. Más aun, si $u = (m, m, \cdots, m)$ entonces escribiremos $g(X)^m$ en vez de $g(X)^u$.

Proposición 7.2.5

1. *Sea* $g(x) = (g_1(X), g_2(X), \ldots, g_n(X)) \in D[[X]]$ *con* $g_k(X) \in \mathfrak{p}_X$, *para* $1 \leq k \leq, n$. *Definiendo* $C_{g(X)} : D[[X]] \to D[[X]]$ *por* $C_{g(X)}(f(X)) = f(X) \circ g(X)$ *obtendremos un homomorfismo de anillos que es continuo respecto a la métrica inducida por* $|\cdot|_X$.

2. *Sean* $(g_{1,k}(X))_{k \in \mathbb{N}}, \cdots, (g_{n,k}(X))_{k \in \mathbb{N}} \subset D[[X]]$. *Si para cada* $i \in \{1, 2, \ldots, n\}$ *la secuencia* $(g_{i,k}(X))$ *converge a algún* $g_i(X) \in D[[X]]$, *y* $g_{i,k}(X) \in \mathfrak{p}_X$ *para todo* $k \in \mathbb{N}$; *entonces existe* $f(X) \circ (g_1(X), g_2(X), \cdots, g_n(X))$ *y*

$$f(X) \circ (g_1(X), g_2(X), \cdots, g_n(X)) = \lim_{k \to \infty} f(X) \circ (g_{1,k}(X), g_{2,k}(X), \cdots, g_{n,k}(X))$$

para todo $f(X) \in D[[X]]$.

Demostración.-

1. No es dificil probar que $C_{g(X)}$ es un homomorfismo de anillos. Por ejemplo, dados $f(X)$, $h(X) \in D[[X]]$, si escribimos $f(X) = \sum_u a_u X^u$ y $h(X) \sum b_v X^v$, por definición tendremos que

$$\begin{aligned}(f(X)\cdot h(X))\circ g(X) &= \sum_{w\in\mathfrak{N}}\Big(\big(\sum_{u+v=w} a_u b_v\big) g_1(X)^{w_1}\cdots g_n(X)^{w_n}\Big)\\ &= \sum_{w\in\mathfrak{N}}\Big(\sum_{u+v=w}\big(a_u g_1(X)^{u_1}\cdots g_n(X)^{u_n}\big)\big(b_v g_1(X)^{v_1}\cdots g_n(X)^{v_n}\big)\Big),\end{aligned}$$

y por tratarse de series en un dominio no arquimediano, la proposición 4.4.16 nos garantiza que

$$(f(X)\cdot h(X))\circ g(X) = \big(\sum_{u\in\mathfrak{N}} a_u g(X)^u\big)\big(\sum_{v\in\mathfrak{N}} b_v g(X)^v\big).$$

Ahora veamos que $C_{g(X)}$ es continua. Dado $f(X) = \sum_u a_u X^u \in D[[X]]$, por el primer ítem de la proposición 4.4.12 tendremos que

$$\begin{aligned}|f(X)\circ g(X)|_X &\leq \text{máx}\{|a_u g_1(X)^{u_1}\cdots g_n(X)^{u_n}|_X \,;\, u\in\mathfrak{N}\}\\ &\leq \text{máx}\{e^{-u_1}\cdots e^{-u_n} \,;\, u\in\mathfrak{N}\,,\ a_u\neq 0\}\\ &= e^{-\min\{|u|,a_u\neq 0\}};\end{aligned}$$

por tanto

$$|f(X)\circ g(X)|_X \leq |f(X)|_X \tag{7.1}$$

Luego, para cada $f(X), h(X) \in D[[X]]$ se tiene que

$$|f(X)\circ g(X) - h(X)\circ g(X)|_X = |(f(X)-h(X))\circ g(X)|_X \leq |(f(X)-h(X))|_X;$$

lo que significa que $C_{g(X)}$ es de Lipschitz, por tanto es continua.

2. Puesto que el ideal de valuación de ω_X es un conjunto cerrado, tendremos que $\omega_X(g_j(X)) > 0$, para $j = 1, 2, \ldots, n$; por lo tanto $f(X)\circ(g_1(X),\ldots,g_n(X))$ puede ser definido. Denotemos $h_k(X) = (g_{1,k}(X),\cdots,g_{n,k}(X))$, $h(X) = (g_1(X),\ldots,g_n(X))$ y $f(X) = \sum_u a_u X^u$. Dados $u\in\mathfrak{N}, k\in\mathbb{N}$, por la desigualdad triangular tenemos que $|a_u h_k(X)^u - a_u h(X)^u|_X$ es menor o igual a

$$\max_{1\leq j\leq n}\big\{|a_u (g_1(X))^{u_1}\cdots(g_{j-1}(X))^{u_{j-1}}((g_{j,k}(X))^{u_j} - g_j(X)^{u_j})(g_{j+1,k}(X))^{u_{j+1}}\cdots g_{j,k}(X)^{u_n}|_X\big\}.$$

De este modo

$$|a_u h_k(X)^u - a_u h(X)^u|_X \leq \max_{1\leq j\leq n}\big\{|g_{j,k}(X)^{u_j} - g_j(X)^{u_j}|_X\big\}, \quad \text{para todo } k\in\mathbb{N}, u\in\mathfrak{N}.$$

Pero, para cada término del segundo miembro con $u_j > 0$ ocurre que

$$|g_{j,k}(X)^{u_j} - g_j(X)^{u_j}|_X = |g_{j,k}(X) - g_j(X)|_X \Big| \sum_{r+s=u_j} (g_{j,k}(X))^r (g_j(X))^s \Big|_X \leq |g_{j,k}(X) - g_j(X)|_X;$$

por lo tanto, concluimos que

$$|a_u h_k(X)^u - a_u h(X)^u|_X \leq \max_{1 \leq j \leq n} \{|(g_{j,k}(X))^{u_j} - g_j(X)^{u_j}|_X\}, \quad \text{para todo } k \in \mathbb{N}, u \in \mathfrak{N}.$$

Por la hipótesis de este ítem, dado $\epsilon > 0$, existe $k_0 \in \mathbb{N}$ tal que $k \geq k_0$ implica que $|(g_{j,k}(X)) - g_j(X)|_X < \epsilon$, para $j = 1, 2, \ldots, n$. Entonces, para $d, k \geq k_0$, se cumple que

$$\Big| \sum_{|u| \leq d} a_u h_k(X)^u - \sum_{|u| \leq d} a_u h(X)^u \Big|_X \leq \max\{\epsilon, \Big| \sum_{k_0 < |u| \leq d} a_u h_k(X)^u - \sum_{k_0 < |u| \leq d} a_u h(X)^u \Big|_X\};$$

y por la desigualdad (7.1) concluimos que

$$\Big| \sum_{|u| \leq d} a_u h_k(X)^u - \sum_{|u| \leq d} a_u h(X)^u \Big|_X \leq \max\{\epsilon, e^{-k_0}\}.$$

Luego, por la proposición 4.4.13 y el primer ítem de la proposición 4.4.12 tendremos que

$$|f(X) \circ h_k(X) - f(X) \circ h(X)|_X \leq \max\{\epsilon, e^{-k_0}\}, \quad \text{para todo } k \geq k_0;$$

con esta última desigualdad concluimos este ítem.

□

El siguiente lema nos muestra que la operación composición entre series formales presenta un tipo de asociatividad (lo cual sucederá exactamente lo que sucede en el caso de series formales de una variable).

Lema 7.2.6 *Sean* $f(X) \in D[[X]]$ *y* $g(X) = (g_1(X), g_2(X), \cdots, g_n(X))$, $h(X) = (h_1(X), h_2(X), \cdots, h_n(X)) \in D[[X]]^n$ *con con* $g_k(X)), h_k(X) \in \mathfrak{p}_X$ *para* $k = 1, 2, \ldots, n$. *Se tiene que*

$$(f(X) \circ g(X)) \circ h(X) = f(X) \circ (g_1 \circ h(X), \ldots, g_n \circ h(X)).$$

Demostración.- Para empezar, debemos verificar que el segundo miembro de la igualda planteada tiene sentido, es decir, para cada $i \in \{1, 2, \ldots, n\}$, se cumple $g_i(X) \circ h(X) \in \mathfrak{p}_X$. De hecho, dado $i \in \{1, 2, \ldots, n\}$,por la desigualdad (7.1) obtendremos que

$$|g_i(X) \circ h(X)|_X \leq |g_i(X)|_X < 1,$$

por tanto, $\omega_X(g_i(X) \circ h(X)) > 0$. Enumerando $\mathfrak{N} = \{u^{(1)}, u^{(2)}, \ldots, u^{(k)}, \ldots\}$, tendremos que

$$\begin{aligned}(f(X) \circ g(X)) \circ h(X) &= (\lim_{m\to\infty} \sum_{k=1}^{m} a_{u^{(k)}} g_1(X)^{u_1^{(k)}} \cdots g_n(X)^{u_n^{(k)}}) \circ h(X) \\ &= \lim_{m\to\infty} (\sum_{k=1}^{m} a_{u^{(k)}} g_1(X)^{u_1^{(k)}} \cdots g_n(X)^{u_n^{(k)}}) \circ h(X)\end{aligned}$$

por la continuidad y linealidad de $C_{h(X)}$; así también, porque $C_{h(X)}$ es un homomorfismo de anillos obtenemos que el segundo miembro de arriba es igual

$$\lim_{m\to\infty} (\sum_{k=1}^{m} a_{u^{(k)}} (g_1(X) \circ h(X))^{u_1^{(k)}} \cdots (g_n(X) \circ h(X))^{u_n^{(k)}}),$$

que es exactamente $f(X) \circ (g_1(X) \circ h(X), \ldots, g_n(X) \circ h(X))$, con lo que conluimos la prueba. □

El siguiente lema muestra condiciones suficientes y necesarias para que una serie formal en una variable elemento sea "invertible" respecto a la operación composición.

Lema 7.2.7 *Sea* $f(X) = \sum_{k=0}^{\infty} a_k X^k \in D[[X]]$. *Son equivalentes*

i) Existe $g(X) \in D[[X]]$ *tal que* $g(X) \in \mathfrak{p}_X$ *y* $f(X) \circ g(X) = X$.

ii) $a_0 = 0$ *y* $a_1 \in D^\times$.

En el caso que se satisfagan estos ítems, es única la serie formal $g(X)$ *que satisface i), la cual también satisfacerá* $g(X) \circ f(X) = X$.

Demostración.- Durante esta demostración utilizaremos las funciones $\pi_m : D[[X]] \to D$ definidas por $\pi_m(\sum_{k=0} a_k X^k) = a_m$, para cada $m \geq 0$.

Supongamos que existe $g(X) \in D[[X]]$ con $\omega_X(g(X)) > 0$ y procedamos a verificar *ii)*. Como $\sum_{k=0}^{\infty} a_k g(X)^k$ converge a $f(X) \circ g(X)$, por las observaciones 7.1.9 tendremos que existe $M > 0$ tal que $m \geq M$ implica que los dos primeros coeficientes de $f(x) \circ g(X)$ y $\sum_{k=0}^{m} a_k (g(X))^k$ coinciden. Como $\omega_X(g(x)) \geq 1$, tendremos que

$$0 = \pi_0(f(X) \circ g(X)) = \pi_0(\sum_{k=0}^{m} a_k (g(X))^k) = a_0,$$

porque $\omega_X(a_k g(X)^k) \geq k\omega_X(g(X)) \geq k$, para $k = 1, \ldots, m$. Por el mismo motivo,

$$1 = \pi_1(f(X) \circ g(X)) = \pi_1(\sum_{k=0}^{m} a_k (g(X))^k) = \pi_1(a_1 g(X)) = a_1 \pi_1(g(X));$$

por lo tanto $a_1 \in D^\times$ (nótese que lo mismo sucede para $g(X)$).

Recíprocamente, asumamos que $a_0 = 0$ y $a_1 \in D^\times$, construiremos una serie formal $g(X)$ como límite de una sucesión adecuada a nuestros fines.

Afirmación : *Dado $m \geq 1$, existe $g_m(X) \subset D[X]$ de grado m tal que $g_m(X) \in \mathfrak{p}_X$ y $w_X(f(X) \circ g_m(X)) > m$.*

Nótese que $g_m(X) \in D[X]$ de grado m con $w_X(g_m(X)) > 0$ satisface la afirmación si y sólo si

$$\pi_l(f(X) \circ g_m(X)) = \begin{cases} 1 & , \text{ si } l = 1, \\ 0 & , \text{ si } l = 0 \text{ o } l = 2, 3, \ldots, m, \end{cases}$$

Para el caso $m = 1$ basta tomar $g_1(X) = a_1^{-1}X$, pues

$$f(X) \circ g_1(X) = \sum_{k=0}^{\infty} a_k (a_1^{-1}X)^k = X + \sum_{k=2}^{\infty} a_1^{-k} a_k X^k,$$

por lo tanto $g_1(X)$. Ahora, supongamos que existe $g_m(X)$ que satisface la afirmación en el caso $m \geq 1$. Sean $b \in D$ y $h(X) = g_m(X) + bX^{m+1}$. Para cada $l \leq m$ vemos que

$$\pi_l(f(X) \circ h(X)) = \pi_l\Big(\sum_{k=1}^{\infty} a_k (h(X))^k\Big) = \pi_l\Big(\sum_{k=1}^{\infty} a_k (h(X))^k\Big),$$

puesto que $\omega_X(h(X)) > 0$; luego

$$\pi_l(f(X) \circ h(X)) = \pi_l\Big(\sum_{k=1}^{m} a_k \sum_{j=0}^{k} \binom{k}{j} (bX^{m+1})^j g_m(X)^{k-j}\Big) = \pi_l\Big(\sum_{k=1}^{m} a_k g_m(X)^k\Big) = \pi_l\Big(f(X) \circ g_m(X)\Big).$$

Por lo tanto, $h(X)$ satisface la afirmación en el caso $m+1$ si y sólo si $0 = \pi_{m+1}(f(X) \circ h(X))$, esto es

$$\begin{aligned} 0 &= \pi_{m+1}\Big(\sum_{k=1}^{m+1} a_k \sum_{j=0}^{k} \binom{k}{j} (bX^{m+1})^j g_m(X)^{k-j}\Big) \\ &= \pi_{m+1}\Big(\sum_{k=1}^{m+1} a_k \big(g_m(X)^k + kbX^{m+1} g_m(X)^{k-1}\big)\Big) \\ &= 0 + a_1 b + \pi_{m+1}\Big(\sum_{k=2}^{m+1} a_k g_m(X)^k\Big), \end{aligned}$$

pues $w_X(g_m(X)^{k-1}) \geq 1$, para $k \geq 2$. Por lo tanto, $h(X)$ satisface la afirmación en el caso $m+1$ cuando $b = -a_1^{-1}\pi_{m+1}(\sum_{k=2}^{m+1} a_k g_m(X)^k)$; nótese que este polinomio $h(X)$ es tal $\omega_X(g_m(X) - h(X)) \geq m + 1$.

Gracias a esta afirmación y su último comentario, podemos construir por inducción sobre m una sucesión $(g_m(X))_m \subset D[X]$ tal que $\omega_X(g_m(X)) > 0$ y $\omega_X(f(X) \circ g_m(X) - X) > m$ y

$\omega_X(g_{m+1}(X)-g_m(X)) \geq m+1$, para todo $m \geq 1$. Por lo tanto, $\lim_{m\to\infty} |g_{m+1}(X) - g_m(X)|_X = 0$, $(g_m(X))$ es de Cauchy y existe $\lim_{m\to\infty} g_m(X) = g(X)$. Puesto que el ideal de valuación de ω_X es cerrado, tendremos que $\omega_X(g(X)) > 0$. Como $|f(X)\circ g(X) - X|_X < e^m$ para todo $m \geq 1$, tendremos que $\lim_{m\to\infty} f(X)\circ g_m(X) = X$. Por lo tanto $f(X)\circ g(X) = f(X)\circ \lim_{m\to\infty} g_m(X) = X$, en virtud de la proposición 7.2.5.

Finalmente, supongamos que $g(X)$ satisface el ítem *i)*, entonces como mencionamos antes $\pi_1(g(X))$ es un elemento invertible en D, por lo cual existe $h(X) \in D[[X]]$ con $\omega_X(h(X)) > 0$ tal que $g(X) \circ h(X)$. Luego,

$$f(X) = f(X) \circ (g(X) \circ h(X)) = (f(X) \circ g(X)) \circ h(X) = h(X),$$

por lo cual $g(X) \circ f(X) = X$. Si existiese $t(X) \in D[[X]]$ que también satisface *i)* tendremos que

$$g(X) = g(X) \circ (f(X) \circ t(X)) = (g(X) \circ f(X)) \circ t(X) = t(X);$$

así es como concluimos la unicidad de $g(X)$. □

La siguiente definición que encierra algunos casos particulares de la composición entre series.

Definición 7.2.8 Sea $f(X) = \sum b_u X^u \in D[[X_1, \cdots, X_n]]$ y $g(X) = (g_1(X_1, \ldots, X_m), \ldots, g_n(X_1, \ldots, X_m)) \in D[[X_1, \ldots, X_m]]^m$.

- Si $n > m$, definimos $f(X) \circ g(X)$ como $f(X) \circ h(X)$ con $h(X) = (g_1(X), \ldots, g_m(X), X_{m+1}, \ldots, X_n)$.
- Si $m > n$, definimos $f(X)\circ g(X)$ como $h(X)\circ g(X)$ con $h(X) = \sum_{v\in\mathbb{N}_0^m} b_X^v \in D[X_1, \ldots, X_m]$ tal que b_v es $a_{(u_1,\ldots,u_n)}$ cuando $v = (u_1, \ldots, u_n, 0, \ldots, 0)$; y 0, en otro caso.

Observación 7.2.9 Cuando no haya peligro de ambigüedad, resumiremos de otra forma nuestra notación. Dado $f(X) \in D[[X_1, \ldots, X_n]]$ y $g(X) = (g_1(X), \ldots, g_m(X)) \in D[[X_1, \ldots, X_m]]$, escribiremos $f(X) \circ g(X)$ como $f(g(X))$.

7.3. Producto entre series de potencias

Otra elemento que se puede definir como límite de una sucesión de series formales es el producto infinito de series formales.

Proposición 7.3.1 *Sea* $(f_k) \subset D[[X]]$, *la sucesión* $(\prod_{k=1}^m f_k(X))_{m\in\mathbb{N}} \subset D[[X]]$ *converge a una serie no nula si y sólo si cada* $f_k(X)$ *es no nulo y* $\lim |f_k(X) - 1|_X = 0$.

Demostración.- Supongamos que $(\prod_{k=1}^{m} f_k)$ converge a una serie no nula $f(X)$.

Como $\lim_m |\prod_{k=1}^{m} f_k(X)|_X = |f(X)|_X > 0$, fijando $C > 0$ tal que $1/C < |f(X)|_X$, existirá $M \in \mathbb{N}$ tal que

$$|\prod_{k=1} f_k(X)|_X > 1/C, \quad \text{para todo } m \geq M;$$

lo cual seria imposible si algún término $f_k(X)$ fuese nulo. Por parte, esta sucesión sera de Cauchy, y por tanto, dado $\epsilon > 0$ existirá $N \in \mathbb{N}$ tal que

$$|\prod_{k=1}^{m+1} f_k(X) - \prod_{k=1}^{m} f_k(X)|_X < \epsilon/C, \quad \text{cuando } m \geq N.$$

Luego, siempre que $m \geq \text{máx}\{M, N\}$, tendremos que

$$|f_{m+1}(X) - 1|_X < C|\prod_{k=1} f_k(X)|_X |f_{m+1}(X) - 1|_X < C(\epsilon/C) = \epsilon.$$

Recíprocamente, supongamos que $\lim_{m\to\infty} |f_m(X) - 1|_X = 0$ y que cada $f_m(X)$ sea no nulo. Dado $m \in \mathbb{N}$ se cumple

$$|\prod_{k=1}^{m+1} f_k(X) - \prod_{k=1}^{m} f_k(X)|_X \leq 1 \cdot |f_m(X) - 1|_X,$$

por tanto, al ser no arquimediano $|\cdot|_X$, tendremos que la sucesión de productos finitos es de Cauchy, de ahí que es convergente a $f(X) \in D[[X]]$; procedamos a verificar que $f(X)$ es no nula. Existe $M \in \mathbb{N}$ tal que $|f_k(X) - 1|_X < 1$, para todo $k \geq M$; por tanto $|f_k(X)| = \text{máx}\{|f_k(X) - 1|_X, |1|_X\}$=1, y se tendra que

$$|\prod_{k=1}^{m} f_k(X)|_X = \prod_{k=1}^{M} |f_k(X)|_X > 0, \quad \text{siempre que } m \geq M.$$

En consecuencia, tomando límite tendremos que

$$|f(X)|_X = \lim_m |\prod_{k=1}^{m} f_k(X)|_X = \prod_{k=1}^{M} |f_k(X)|_X > 0.$$

La siguiente proposición muestra la forma de las unidades en $D[[X]]$.

Proposición 7.3.2 *Sea $f(X) \in a_0 + \mathfrak{p}_X$ con a_0 un elemento invertible, entonces existe $g(X) \in a_0^{-1} + \mathfrak{p}_X$ tal que $f(X)g(X) = g(X)f(X) = 1$.*

Demostración.- Escribamos $f(X) = \sum_u a_u X^u$. Construiremos por inducción una sucesión $(g_d(X))_{d\geq 0} \subset a_0^{-1} + \mathfrak{p}_X$ tal que $\omega_x(f(X)g_d(X) - 1) > d$. Para $d = 0$, basta tomar $g_0(X) = a_0^{-1}$.

Ahora supongamos que existe $g_d(X) = \sum_{|u|\leq d} a_u X^u \in a_0^{-1} + \mathfrak{p}_X$ tal que $\omega_x(f(X)g_d(X) - 1) > d$. Dado $w \in \mathfrak{N}$ con $|w| = d+1$, definamos $b_w = -a_0^{-1} \sum_{\substack{u+v=w \\ u\neq 0}} a_u b_v$. Nótese que esta definición es buena, puesto que sólo aparecen multiindices de peso menor o igual a d en la sumatoria (recuerde las observaciones 7.1.2). Luego, tomando $g_{d+1}(X) = g_d(X) + \sum_{|v|=d+1} X^v \in 1 + \mathfrak{p}_X$ tenemos que lo coeficiente del término X^w de $f(X)g_{d+1}(X)$ es 1, para $w = 0$; o 0, para $0 < |w| \leq d+1$. De este modo concluimos la construcción por inducción sobre d. Asi tendremos que $\lim_{d\to\infty} f(X)g_d(X) = 1$; en particular $(f(X)g_d(X))_{d\geq 0}$ es de Cauchy. Puesto que

$$|f(X)g_r(X) - f(X)g_s(X)|_X = |f(X)|_X |g_r(X) - g_s(X)|_X = |g_r(X) - g_s(X)|_X, \quad \text{para todo } r, s \in \mathbb{N},$$

concluimos que $(g_d(X))_{d\leq 0}$ es Cauchy, por tanto converge a algún $g(X) \in D[[X]]$. Además, puesto que $g_d(X) - a_0^{-1} \in \mathfrak{p}_X$, para cualquier $d \geq 0$; tendremos que $g(X) - a_0^{-1} \in \mathfrak{p}_X$. □

Corolario 7.3.3 *Si K es un cuerpo, entonces el conjunto de elementos invertibles de $K[[X]]$ es $K[[X]] \setminus \mathfrak{p}_X$.*

Observaciones 7.3.4

- Este corolario tiene como consecuencia que $\mathfrak{p}_X$ es un ideal maximal, más aun es único. Por lo tanto, $K[[X]]$ es un *anillo local.*
- la condición mencionada en la proposición anterior también es necesaria.
- De ahora en adelante, si $f(X), g(X) \in D[[X]]$ con $g[[X]]$ invertible, el producto $f(X)g(X)^{-1}$ lo expresaremos por $\dfrac{f(X)}{g(X)}$.

Ejemplo 7.3.5 Si $a \in D$ es nulo y $d \geq 1$ entonces $(1 - aX^d)^{-1} = \sum_{s=1}^{\infty} a^s (X^d)^s \in D[[X]]$. De hecho, para cada $n \in \mathbb{N}$, tenemos que

$$(1 - aX^d) \sum_{s=0} a^s (X^d)^s = 1 - a^{n+1}(X^d)^n + 1,$$

por tanto $|(1 - aX^d)\sum_{s=0}^{n} a^s (X^d)^s - 1|_X = e^{-n-1}$; por tanto,

$$1 = \lim_{n\infty}(1 - aX^d) \sum_{s=0}^{n} a^s (X^d)^s = (1 - aX^d) \lim_{n\infty} \sum_{s=0}^{n} a^s (X^d)^s = (1 - aX^d) \sum_{s=0}^{\infty} a^s (X^d)^s.$$

En caso de series formales de una variable, podemos obtener condiciones para que una serie formal sea el resultado del cociente de dos polinomios, esto es el producto de la inversa. Cabe mencionar que la condición a demostrar es también necesaria, su demostración puede encontrarla en [9].

Lema 7.3.6 *Sea K un cuerpo y $f(X) = \sum_{i=0}^{\infty} a_i X^i \in K[[X]]$. Dado $s, m \geq 0$ enteros, definimos $A_{s,m} = [a_{s+i+j}]_{0 \leq i,j \leq m} \in K^{(m+1)\times(m+1)}$.*

$$\begin{pmatrix} a_s & a_{s+1} & a_{s+2} & \cdots & a_{s+m} \\ a_{s+1} & a_{s+2} & a_{s+3} & \cdots & a_{s+m+1} \\ a_{s+2} & a_{s+3} & a_{s+4} & \cdots & a_{s+m+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m} \end{pmatrix}$$

y $D_{s,m} = \det(A_{s,m})$. Si existen $m, S \geq 0$ para los cuales $s \geq S$ implique $D_{s,m} = 0$, entonces $f(X) = P(X)/Q(T)$.con $P(T), Q(T) \in K[X]$.

Demostración.- Antes de realizar de la prueba de este lema, rescatemos algunas relaciones entre estas matrices $A_{s,m}$. Denotemos a la fila $i-$ésima de $A_{s,m}$ por $A_{s,m}^{(i)}$, entonces tenemos que

(i) $A_{s,m}^{(i)} = A_{s+1,m}^{(i-1)}$, para $1 \leq 1 \leq m$.

(¨) $A_{s,m}^{(i)} = [A_{s,m-1}^{(i)}, a_{s+i+m}]$, para $0 \leq i \leq m$, $m \geq 1$.

( ) $A_{s,m}^{(i)} = [a_{s+i}, A_{s+1,m-1}^{(i-1)}]$, para $1 \leq i \leq m$, $m \geq 1$.

Sea $m_0 = \min\{m \ ; \ \exists S \geq 0 \ , \ D_{s,m} = 0 \ , \forall \ s \geq S\}$ y $S_0 \geq 0$ tal que $s \geq S_0$ implique $D_{s,m_0} = 0$. Si $m_0 = 0$, entonces $a_s = 0$ para todo $s \geq S_0$, por lo cual $f(X) \in K[X]$ y el lema estara demostrado; por lo cual asumamos que $m_0 \geq 1$.

Afirmación : *Dado $s \geq S_0$, $D_{s,m_0-1} = 0$ implica $D_{s+1,m_0-1} = 0$.*

En efecto, como $D_{s,m_0-1} = 0$, las filas $A_{s,m_0-1}^{(0)}$, $A_{s,m_0-1}^{(1)}, \ldots, A_{s,m_0-1}^{(m_0-1)}$ son *l.d.*, por lo cual existen $\alpha_0, \ldots, \alpha_{m_0-1} \in K$ no todos nulos tales que

$$\alpha_0 A_{s,m_0-1}^{(0)} + \alpha_1 A_{s,m_0-1}^{(1)} + \cdots + \alpha_{m_0-1} A_{s,m_0-1}^{(m_0-1)} = 0 \in K^{1\times m}.$$

Tomemos $i_0 = \min\{i \ ; \ \alpha_i \neq 0\}$, entonces

$$A_{s,m_0-1}^{(i_0)} - \beta_{i_0+1} A_{s,m_0-1}^{(i_0+1)} + \cdots + \beta_{m_0-1} A_{s,m_0-1}^{(m_0-1)} = 0,$$

si eligimos $\beta_i = \alpha_i/\alpha_0$ para $i = 1, 2, \ldots, m_0 - 1$. Si $i_0 \geq 1$, por el ítem tendremos que

$$A_{s+1,m_0-1}^{(i_0-1)} - \beta_{i_0+1} A_{s+1,m_0-1}^{(i_0)} + \cdots + \beta_{m_0-1} A_{s+1,m_0-1}^{(m_0-2)} = 0,$$

lo signfica que las m últimas filas de A_{s+1,m_0-1} son *l.d.* y que $D_{s+1,m_0-1} = 0$. En el caso $i_0 = 0$, utilizamos el ítem (ii) para obtener que

$$A_{s,m_0}^{(0)} - \beta_1 A_{s,m_0}^{(1)} + \cdots + \beta_{m_0-1} A_{s,m_0}^{(m_0-1)} = [0, 0, \ldots, 0, b]; \tag{7.2}$$

tomemos $v = [0, \ldots, 0, b] \in K^{1\times(m+1)}$. Como $D_{s,m_0} = 0$, las filas $A^{(0)}_{s,m_0}, A^{(1)}_{s,m_0}, \ldots, A^{(m_0)}_{s,m_0}$ son *l.d.*, entonces $v, A^{(1)}_{s,m_0}, \ldots, A^{(m_0)}_{s,m_0}$ también son *l.d.*. Por tanto, existiran $\lambda_0, \lambda_1, \ldots, \lambda_{m_0} \in K$ no todos nulos tales que

$$\lambda_0 v + \lambda_1 A^{(1)}_{s,m_0} + \cdots + \lambda_{m_0} A^{(m_0)}_{s,m_0} = 0. \tag{7.3}$$

Si algún λ_i fuese no nulos para $i \geq 1$, entonces tomando las m primeras componentes de los vectores fila en (7.3) y el ítem (iii) tendremos que

$$0 + \lambda_1 A^{(0)}_{s+1,m_0-1} + \cdots + \lambda_{m_0} A^{(m_0-1)}_{s+1,m_0-1} = 0,$$

por lo cual las filas de A_{s+1,m_0-1} son *l.d.* y $D_{s+1,m_0-1} = 0$. En caso contrario, simplemente tendriamos que $\lambda_0 v = 0$ con $\lambda \neq 0$, y $b = 0$. Aplicando el ítem (ii) a la igualdad (7.2), vemos que $A^{(0)}_{s+1,m_0-1}$ es combinación lineal de $A^{(1)}_{s+1,m_0-1}, \ldots, A^{(m_0-1)}_{s+1,m_0-1}$, por lo cual $D_{s+1,m_0-1} = 0$.

Si existiese $\widetilde{s} \geq S_0$ tal que $D_{\widetilde{s},m_0-1} = 0$, entonces la afirmación anterior nos permite realizar inducción sobre $D_{s,m_0-1} = 0$ para todo $s \geq \widetilde{s}$; lo cual contradeciria la minimalidad de $\widetilde{s}$, por lo tanto concluimos que $D_{s,m_0-1} \neq 0$ para todo $s \geq S_0$. Luego, dada una matriz $A_{s,m}$ con $s \leq S_0$, existirán $\lambda_0, \ldots, \lambda_m$ tales que $\lambda_0 A^{(0)}_{s,m_0} + \cdots + \lambda_{m_0} A^{(m_0)}_{s,m_0} = 0$. Si λ_{m_0} fuese nulo, por el ítem (ii) ocurriria que las filas de A_{s,m_0-1} son *l.d.*; por lo tanto $\lambda_{m_0} \neq 0$ y la última fila de A_{s,m_0} es combinación lineal de las m primeras filas, para todo $s \geq S_0$.

Tomemos $u = [u_{m_0}, u_{m_0-1}, \ldots, u_0] \in K^{(m_0+1)\times 1}$ no nulo tal que $A_{S_0,m_0} u = 0$, entonces

$$A^{(0)}_{S_0,m_0} u = 0, \qquad \text{para } i = 0, 1, \ldots m_0.$$

Por lo que acabamos de mencionar y el ítem (i), la fila $A^{m_0}_{S_0+1,m_0}$ es combinación lineal de ocurre $A^{(1)}_{S_0,m_0}, \cdots, A^{(m_0-1)}_{S_0,m_0}$, y en consecuencia $A^{m_0}_{S_0+1,m_0} u = 0$. Este mismo razonamiento, manteniendo el mismo vector columna $u \neq 0$, nos permite realizar inducción sobre

$$a_s u_{m_0} + a_{s+1} u_{m_0-1} + \cdots a_{s+m_0} u_0 = A^{m_0}_{s,m_0} u = 0, \qquad \text{para todos} \geq S_0.$$

Entonces, definiendo $h(X) = \sum_{i=0}^{S_0} u_i \in K[X]$ no nulo tendremos que $g(X) = f(X)h(X)$ tiene todos sus coeficientes nulos desde $S_0 + m_0$, por lo tanto $f(X) = g(X)/h(X)$ con $g(X), h(X) \in K[X]$.

7.4. Series Formales de una y dos variables

En esta sección daremos unas cuantas convenciones y propiedades acerca de series formales de una o dos variables, las cuales ejemplizaran el sencillo uso de lo ya desarrollado.

Durante esta sección, D seguira denotando un dominio cualquiera y $\mathfrak{N}$ será $\mathbb{N}_0^2$. Empecemos por mencionar una sencilla proposición acerca de algunos conocidos subanillos que podemos encontrar en $D[[X,Y]]$.

Proposición 7.4.1 *El dominio $D[[X,Y]]$ contiene subanillos isomorfos a $D[X]$, $D[Y]$, $D[[X]]$, $D[[Y]]$, $D[X][[Y]]$, $D[Y][[X]]$, $D[[X]][[Y]]$ y $D[[X]][[Y]]$.*

Demostración.- Para demostrar esta proposición es suficiente mostrar que $D[[X]][[Y]]$ es isomorfo a $D[[X,Y]]$. Establescamos $\Xi : D[[X,Y]] \to D[[X]][[Y]]$ definido por $\Xi(f) : \mathbb{N}_0 \to D[[X]]$ como $\Xi(f)(n) = f(\cdot, n)$; esta definición esta basada en el hecho que una serie en dos variables en tan solo una función de $\mathfrak{N}$ en D. Como es rutinario demostrar que Ξ es un isomorfismo, damos por concluida esta demostración. □

Observación 7.4.2 En el caso de series formales de dos variables X e Y, denotaremos a la valuación que hemos definido en la sección anterior y al valor absoluto inducido por ésta como $\omega_{(X,Y)}$ y $|\cdot|_{(X,Y)}$, respectivamente. Así también el ideal de valuación de $\omega_{(X,Y)}$ será denotado por $\mathfrak{p}_{(X,Y)}$.

Gracias al valor absoluto $|\cdot|_{(X,Y)}$, a las proposiciones 7.1.10 y 4.4.17 podemos expresar de una manera más "natural" el significado de la anterior proposición.

Proposición 7.4.3 *Dado $f(X,Y) = \sum_{(m,n)\in\mathfrak{N}} a_{m,n}X^mY^n \in D[[X,Y]]$, se tiene que*

$$f(X,Y) = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} a_{m,n}X^mY^n = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} a_{m,n}X^mY^n.$$

Definición 7.4.4 Dados $f(X) \in D[[X,Y]]$ y $g(X,Y) \in D[[X,Y]]$, entonces denotaremos $f(X) \circ g(X,Y)$ por $f(g(X,Y))$.

A continuación estudiaremos un muy importante tipo de series formales: el anillo $D[X][[Y]]$. Por la proposición 7.4.1, asumiremos la inclusión $D[X][[Y]] \subset D[[X,Y]]$. Por tanto, tendremos que $\omega_{(X,Y)}$ y $|\cdot|_{(X,Y)}$ son una valuación y un valor absoluto sobre $D[X][[Y]]$.

Sin embargo, estableceremos la valuación ω_Y sobre $D[X][[Y]]$ como anillo de series formales en la variable Y con coeficientes en $D[X]$. El siguiente lema nos da una sencilla, pero importante relación entre estas valuaciones.

Proposición 7.4.5 *Dado $f(X,Y) \in D[X][[Y]]$ no nulo, se tiene que*

$$\omega_Y(f(X,Y)) \leq \omega_{(X,Y)}(f(X,Y)) \qquad y \qquad |f(X,Y)|_{(X,Y)} \leq |f(X,Y)|_Y.$$

Demostración.- Sean $f(X,Y) = \sum_{(m,n)\in\mathfrak{N}} X^m Y^n$ y $N = \{n \geq 0;\ \exists m \geq 0,\ \omega_{(X,Y)}(f(X,Y)) = m+n\}$. Entonces, tomando $n_0 = \min N$ tendremos que $n_0 \geq \omega_Y(f(X,Y))$. Si $m_0 \geq 0$ es tal que $n_0 + m_0 = \omega_{(X,Y)}(f(X,Y))$, tendremos que

$$\omega_Y(f(X,Y)) \leq n_0 \leq n_0 + m_0 = \omega_{(X,Y)}(f(X,Y)).$$

Puesto que la segunda inecuación es consecuencia inmediata de la primera, damos por terminada la demostración. □

Corolario 7.4.6 *Sea $(f_n(X,Y)) \subset D[X][[Y]]$. Si $(f_n(X,Y))$ converge a $f(X,Y) \in D[X][[Y]]$ respecto a $|\cdot|_Y$, entonces también converge a $f(X,Y)$ respecto a $|\cdot|_{(X,Y)}$.*

Este último corolario nos garantiza que si se pueden definir una serie formal en $D[X][[Y]]$ como límite de una sucesión en $D[X][[Y]]$ bajo $|\cdot|_Y$, tendremos que es la misma serie formal si tratamos a esta sucesión en $D[[X,Y]]$; entre estas, se encuentran las productorias infinitas.

Un caso similar al anterior, pero no exactamente el mismo lo da el siguiente resultado.

Proposición 7.4.7 *Sea $f(X,Y) \in D[X][[Y]]$, $g(X) \in XD[X]$ y $h(Y) \in YD[[Y]]$ entonces $f(X,Y) \circ (g(X), h(Y))$ existe y pertenece a $D[X][[Y]]$.*

Demostración.- Como $\omega_{X,Y}(g(X)) \geq 0$ y $\omega_{X,Y}(h(y)) \geq 0$, entonces $f(X,Y) \circ (g(X), h(Y)) \in D[[X,Y]]$. Si escribimos $f(X,Y) = \sum_{(m,n)} a_{m,n} X^m Y^n \in D[[X,Y]]$, entonces

$$f(X,Y)\circ(g(X),h(Y)) = \sum_{(m,n)} a_{m,n} g(X)^m h(Y)^n = \sum_n \sum_m a_{m,n} g(X)^m h(Y)^n = \sum_n t_n(X) h(Y)^n$$

con $t_n(X) = \sum_m a_{m,n} g(X)^m \in D[X]$, para $n \geq 0$. Como $\omega_Y(h(Y)) \geq 1$, tendremos que la suma de arriba converge respecto a $|\cdot|_Y$ en $D[X][[Y]]$. □

La siguiente función sera de mucha utilidad para construir series de potencias en una variable desde series formales en $D[X][[Y]]$. Esta función será otra extensión de la función $\mathcal{E}_t$ que vimos en la sección de preliminares.

Definición 7.4.8 Dado $t \in D$, definimos la función *evalución parcial en t* por $\mathcal{E}_t : D[X][[Y]] \to D[[Y]]$ por $\mathcal{E}_t\left(\sum_n f_n(X)Y^n\right) = \sum_n f_n(t)Y^n$.

Observación 7.4.9 Cuando no haya peligro de ambigüedad, por ejemplo con las indeterminadas, denotaremos por $f(t,Y)$ a la serie formal $\mathcal{E}_t(f(X,Y)) \in D[[Y]]$.

El siguiente lema le sumará importancia a esta definición.

Lema 7.4.10 *Dado $t \in \mathbb{N}$, la función $\mathcal{E}_t$ es un homomorfismo continuo respecto $|\cdot|_Y$.*

Demostración.- A partir que $\mathcal{E}_t$ es un homomorfismo sobre $D[X]$, resulta sencillo ver que $\mathcal{E}_t$ lo es sobre $D[X][[Y]]$; procedamos a verificar que es continuo respecto a $|\cdot|_Y$. Dado $f(X,Y) \in D[X][[Y]]$, vemos que $w_Y\big(\mathcal{E}_t(f(X,Y))\big) \geq w_Y(f(X,Y))$. Por lo tanto, si $g(X,Y), h(X,Y) \in D[X][[Y]]$ entonces

$$|\mathcal{E}_t(g(X,Y)) - \mathcal{E}_t(h(X,Y))|_Y = |\mathcal{E}_t(g(X,Y) - h(X,Y))|_Y \leq |g(X,Y) - h(X,Y)|_Y;$$

de este modo concluimos que $\mathcal{E}_t$ es Lipschitz, por tanto continua. □

Proposición 7.4.11 *Sea $f(X,Y) \in D[X][[Y]]$, $g(X) \in XD[X]$ y $h(Y) \in YD[[Y]]$. Dado $t \in D$, se cumple $\mathcal{E}_t(f(g(X),h(Y))) = \mathcal{E}_{g(t)}(f(X,h(Y)))$*

Demostración.- Por las hipótesis acerca de $g(X)$ y $h(Y)$, existe $f(g(X),h(Y)) \in D[X][[Y]]$. Luego, escribiendo $f(X,Y) = \sum_{(m,n)} a_{m,n}X^mY^n$ tendremos que

$$\begin{aligned}
\mathcal{E}_t(f(X,Y) \circ (g(X),h(Y))) &= \mathcal{E}_t\Big(\sum_{m,n} a_{m,n}g(X)^m h(Y)^n\Big) \\
&= \sum_{m,n} \mathcal{E}_t\Big(a_{m,n}g(X)^m h(Y)^n\Big) \\
&= \sum_{m,n} a_{m,n}g(t)^m h(Y)^n,
\end{aligned}$$

estas igualdades son ciertas en virtud del lema anterior. Como el último de esta igual es $\mathcal{E}_{g(t)}(f(X,h(Y)))$ concluimos la demostración. □

7.5. La serie binomial

Empezamos esta sección expresando a las series de Taylor de las funciones exp y log como series formales.

Definición 7.5.1 La *serie formal exponencial* y *la serie formal logaritmo* son definidos, respectivamente, como

$$\exp(X) = \sum_{k=0}^{\infty} \frac{1}{k!}X^k \in \mathbb{Q}[[X]] \qquad \text{y} \qquad \log(1+X) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k}X^k \in \mathbb{Q}[[X]].$$

Observaciones 7.5.2

- Nótese que en el caso de la serie formal logaritmo, no tiene sentido la expresión $\log(X)$, puesto que la composición $\log(1+X) \circ (X-1)$ no converge respecto al valor absoluto X-ádico.

- Más aun, en adelante asumerimos la convención de escribir

$$\log(f(X)) = \log(1+X) \circ (f(X)-1) \quad \text{para todo } f(X) \in 1 + \mathfrak{p}_{(X,Y)}.$$

Veamos que la serie formal $\exp(X)$ también cumple una propiedad semejante a la que posee la función compleja exponencial.

Proposición 7.5.3 *La serie formal exponencial cumple*

$$\exp(f(X,Y))\exp(g(X,Y)) = \exp(f(X,Y)+g(X,Y)), \quad \textit{para todo } f(X,Y), g(X,Y) \in \mathfrak{p}_{X,Y}.$$

Demostración.- Por las hipótesis sobre $f(X,Y)$ y $g(X,Y)$, la composición de series $\exp(X) \circ (f(X,Y)+g(X,Y))$ existe; así también nos encontramos en la posibilidad de utilizar la proposición 4.4.16 y obtener que

$$\begin{aligned}
\exp\big(f(X,Y)\big)\exp\big(g(X,Y)\big) &= \Big(\sum_{k=0}^{\infty}\frac{1}{k!}f(X,Y)^k\Big)\Big(\sum_{l=0}^{\infty}\frac{1}{l!}g(X,Y)^l\Big) \\
&= \sum_{m=0}^{\infty}\sum_{k+l=m}\big(\frac{1}{k!}f(X,Y)^k\big)\big(\frac{1}{l!}g(X,Y)^l\big) \\
&= \sum_{m=0}^{\infty}\frac{1}{m!}\big(f(X,Y)+g(X,Y)\big)^m \\
&= \exp\big(f(X,Y)+g(X,Y)\big).
\end{aligned}$$

El siguiente lema encierra un cáculo que estrá presente en varias demostraciones.

Lema 7.5.4 *Sea D un dominio que contiene a $\mathbb{Q}$ y $f(X) = \sum_{s=1}^{\infty} c_s X^s$, entonces el coeficiente s-ésimo de $\exp(X) \circ f(X)$ esta dado por*

$$\sum_{k=1}^{s}\sum_{i_1+\cdots+i_k=s}\frac{1}{k!}c_{i_1}\cdots c_{i_k}, \qquad \textit{para todo } s \geq 1.$$

Demostración.- Tenemos que

$$\exp(X)\circ f(X) = 1 + \sum_{s=1}^{\infty}\frac{f(X)^m}{m!} = 1 + \sum_{m=1}^{\infty}\frac{1}{m!}\Big(\sum_{k=1}^{\infty}c_k X^k\Big)^m.$$

Denotemos por $\pi_s : D[[X]] \to D$ a la proyección en el s-ésimo coeficiente, para cada $s \geq 1$. Entonces, obviando los términos que no aportan monomios de grado s tendremos que

$$\pi_s(\exp(X)\circ f(X)) = \pi_s\Big(\sum_{m=1}^{s}\frac{1}{m!}\Big(\sum_{k=1}^{\infty}c_k X^k\Big)^m\Big) = \sum_{m=1}^{s}\pi_s\Big(\frac{1}{m!}\Big(\sum_{k=1}^{s}c_k X^k\Big)^m\Big).$$

Por definición de productos de polinomos obtenemos

$$\pi_s\left(\frac{1}{m!}\left(\sum_{k=1}^{s} c_k X^k\right)^m\right) = \frac{1}{m!} \sum_{i_1+\cdots+i_k=s} c_{i_1} \cdots c_{i_k}, \quad \text{para } m = 1, 2, \ldots, s;$$

con lo cual finalizamos la demostración. □

La siguiente serie formal tendrá un papel sumamente importante en construcciones posteriores, a decir como sustento para generalizar la potenciación en exponentes no enteros de ciertas series.

Definición 7.5.5

- Dado $n \in \mathbb{Z}$ no negativo definimos *el n-ésimo polinomio combinatorio* como

$$\binom{X}{n} = \begin{cases} \frac{x(x-1)\cdots(x-n+1)}{n!} & ; \ n \in \mathbb{N} \\ 1 & ; \ n = 0 \end{cases};$$

- *la serie binomial* $B(X, Y) \in \mathbb{Q}[[X, Y]]$ viene dada por

$$B(X, Y) = \sum_{n=0}^{\infty} \binom{X}{n} Y^n.$$

Posiblemente el nombre de esta serie se deba a que dado $m \in \mathbb{N}$, los polinomios $\binom{X}{n}$ evaluados en m seran los coeficientes binomiales para $n \leq m$, e identicamente nulos para $n > m$. Por lo tanto,

$$B(m, Y) = \sum_{n=0}^{m} \binom{m}{n} Y^n = (1 + Y)^m.$$

El siguiente teorema encierra la más importante propiedad de esta serie. La demostración de este hecho será el tema de toda esta sección, pues es larga y conlleva muchos pasos. Más aun, encierra la idea de utilizar diversas propiedades análiticas en $\mathbb{R}$ y $\mathbb{C}$ para obtener resultados algebraicos en su subcuerpo $\mathbb{Q}$.

Teorema 7.5.6 *Se cumple que* $B(X, Y) = \exp(X \log(1 + Y))$.

Cuya consecuencia primordial es el siguiente resultado.

Corolario 7.5.7 *Dado* $f(x), g(X) \in \mathbb{Q}[X]$ *y* $n \in \mathbb{N}$, *se tiene que*

$$B(f(X), Y^n) B(g(X), Y^n) = B(f(X) + g(X), Y^n).$$

Demostración.- Por la asociatividad en la composición de series formales obtendremos que

$$\begin{aligned} B(X,Y)\circ(f(X),Y^n) &= \exp(X)\circ\big((X\log(1+Y))\circ(f(X),Y^n)\big) \\ &= \exp\big(X\circ(f(X),Y^n)\log(1+Y)\circ(f(X),Y^n)\big) \\ &= \exp\big(f(X)\log(1+Y^n)\big). \end{aligned}$$

Por lo tanto,

$$B(f(X),Y^n)B(g(X),Y^n) = \exp(f(X)\log(1+Y^n)+g(X)\log(1+Y^n)) = B(f(X)+g(X),Y$$

Empecemos por encontrar un nexo entre estas dos series.

Lema 7.5.8 *Dado $m \geq 2$ entero, se cumple que $B(1/m,Y)$ converge uniformemente a la funcion $y \to \sqrt[m]{1+y}$ en $(-1/2,1/2)$.*

Demostración.- Tomemos $I=(-1/2,1/2)$ y $f: I \to \mathbb{R}$ definido por $f(y)=\sqrt[m]{1+y}$. Entonces f es una función de clase C^∞; más aun, dado $c \in I$ tenemos que

$$f^{(k)}(c) = (\frac{1}{m})(\frac{1}{m}-1)\cdots(\frac{1}{m}-(k-1))(1+c)^{\frac{1}{m}-k}, \quad \text{para todo } k \geq 1.$$

Por lo tanto, si $c, h \in I$, tendremos que

$$\Big|\frac{h^k f^{(k)}(c)}{k!}\Big| \leq \frac{|h|^k(k-1)!(1+c)^{\frac{1}{m}-k}}{mk!} \leq \frac{2^{-k}(1/2)^{\frac{1}{m}-k}}{mk} \leq \frac{1}{\sqrt[m]{2}mk}.$$

Luego, utilizando la formula de Taylor con resto de Lagrange obtenemos que dado $h \in I$ y $n \in \mathbb{N}$ existirá $c=c(h) \in I$ tal que

$$f(h) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} + \frac{f^{(n+1)}(c)h^{n+1}}{(n+1)!}.$$

Entonces, para cualquier $h \in I$, tendremos que

$$\Big|f(h) - \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!}\Big| \leq \frac{1}{\sqrt[m]{2}m(n+1)}.$$

Por esta desigualdad y el Test M de Weierstrass deducimos que la serie de Taylos de $f(x)$ con centro en 0 converge uniformente a $f(x)$ en I, y como el coeficiente $n-$ésimo de está de potencias es igual a $\binom{1/m}{n}$, hemos terminado la demostración. □

El anterior lema se puede traducir a

Dado $y \in I$ y $m \geq 2$ entero, se cumple que $B(1/m,y) = \exp(1/m\log(1+y))$.

Ahora, fijando $y \in I$, definamos las funciones $g_n : \mathbb{C} \to \mathbb{C}$ por $g_0(z) = 1$, y $g_n(z) = \binom{z}{n} y^n$, para cada $n \in \mathbb{N}$. Establescamos la convergencia de la serie de funciones $\sum_{n\geq 0} g_n(z)$ en el disco $D = \{z \in \mathbb{C} \,;\, |z| \leq 1/2\}$. De hecho, dado $n \in \mathbb{N}$ y $z \in D$ se tiene que

$$g_n(z) \leq \frac{|z|(|z|+1)\cdots(|z|+n-1)}{n!}|y|^n \leq \frac{(1/2)n!(1/2)^n}{n!} = 2^{-n-1};$$

por lo tanto, en virtud del Test-M de Weierstrass inferimos la convergencia de la serie mencionada en D a una función $g(z)$. Como cada uno de los sumandos era una función holomorfa, su límite uniforme g también lo será. Entonces, por el lema anterior, tenemos que $g(z)$ coincide con $\exp(z\log(1+y))$ en el conjunto $\{1/m \,;\, m \geq 2 \text{ entero}\}$ con punto de acumulación $0 \in D$; por lo tanto estas funciones son identicas en D (por el teorema de la identidad de funciones holomorfas). De este modo podemos concluir que

Dados $x, y \in I$, es cierto que $B(x,y) = \exp(x\log(1+y))$.

Es momento de enfocarnos en la serie formal $\exp\big(X\log(1+Y)\big) \in \mathbb{Q}[[X,Y]]$. Para empezar,

$$\exp\big(X\log(1+Y)\big) = 1 + \sum_{m=1}^{\infty} \frac{\big(X\log(1+Y)\big)^m}{m!} = 1 + \sum_{m=1}^{\infty} \frac{1}{m!} X^m \left(\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} Y^k\right)^m.$$

Para cada $m \geq 1$, denotemos

$$\left(\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} Y^k\right)^m = \sum_{n=1}^{\infty} c_{m,n} Y^n, \quad \text{donde } c_{m,n} = \sum_{i_1+\cdots+i_m=n} \frac{(-1)^{m+n}}{i_1 \cdot \cdots \cdot i_m},$$

por definición de productos de polinomos. Luego, por la proposición 7.4.3 obtenemos que

$$\exp\big(X\log(1+Y)\big) = 1 + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} \frac{c_{m,n}}{m!} X^m Y^n = 1 + \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{c_{m,n}}{m!} X^m Y^n,$$

y como $c_{m,n} = 0$ cuando $m > n$, obtenemos

$$\exp(X\log(1+Y)) = 1 + \sum_{n=1}^{\infty}\sum_{m=1}^{n} \frac{c_{m,n}}{m!} X^m Y^n \in \mathbb{Q}[X][[Y]]. \tag{7.4}$$

El siguiente paso será mostrar que cuando $\exp(X\log(1+Y))$ es evaluada en puntos de $I \times I$, el valor es el mismo que el obtenido si se evaluasé en esta última serie. Esto se puede entender como que la permutación realizada a nivel de series formales también es valida a nivel de números reales.

Dado $y \in I$, tenemos que $\sum_n 1/n|y|^n$ es convergente, y denotamos a su límite por $\gamma(y)$. Se sigue que la serie de taylor de $\log(1+y)$ es absolutamente convergente, por tanto podemos aplicar el producto de Cauchy para series de potencias para obtener que

$$\log(1+y)^m = \Big(\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} y^k\Big)^m = \sum_{n=1}^{\infty} c_{m,n} y^n, \quad \text{para todo } y \in I,\ m \geq 1.$$

Así también, por ser $\gamma(y)$ una serie convergente de términos positivos obtenemos que

$$\gamma(y)^m = (\sum_{k=1}^{\infty} \frac{1}{k}|y|^k)^m = \sum_{n=1}^{\infty}\Big(\sum_{i_1+i_2+\cdots+i_m=n} \frac{1}{i_1\cdots i_m}\Big)|y|^n = \sum_{n=1}^{\infty} d_{m,n}|y|^n,$$

para todo $y \in I$, $m \geq 1$. Nótese que $d_{m,n} = |c_{m,n}|$ para cada $m, n \geq 1$.

Luego, dados $x \in I$ y $t \in \mathbb{N}$ tendremos que

$$\left|\sum_{m=0}^{t} \frac{(x\log(1+y))^m}{m!}\right| \leq \sum_{m=0}^{t} \frac{|x|^m}{m!}|\sum_{n=0}^{\infty} c_{m,n}y^n| \leq \sum_{m=0}^{t} \frac{|x|^m}{m!}\sum_{n=0}^{\infty} d_{m,n}|y|^n.$$

De ahí que

$$\left|\sum_{m=0}^{t} \frac{(x\log(1+y))^m}{m!}\right| \leq \sum_{m=0}^{t} \frac{\big(|x|\gamma(y)\big)^m}{m!} \leq \exp(|x|\log(1+|y|)),$$

para todo $t \in \mathbb{N}$; de lo cual concluimos que la serie iterada $\sum_m \sum_n (c_{m,n}/m!)x^m y^n$ es absolutamente convergente. Entonces, en virtud del corolario 2.1.11, el valor de esta serie coincide con el valor de su otra iteración $\sum_n \sum_m (c_{m,n}/m!)x^m y^n$. Esto nos trae como consecuencia que

$$H(X,Y) = \exp\big(X\log(1+Y)\big) - B(X,Y) \in \mathbb{R}[X][[Y]]$$

es se anula en la region $I \times I$; de esta forma, el siguiente lema finaliza todo este analísis.

Lema 7.5.9 *Sea $H(X,Y) \in \mathbb{R}[X][[Y]]$, $c > 0$ e $J = (-c, c)$. Si $H(X,Y)$ se anula en $I \times I$ entonces $H(X,Y)$ es la serie formal identicamente nula.*

Demostración.- Por reducción al absurdo, supongamos que existe algún polinomio $f_n(X)$ no nulo, y tomemos a t como el menor índice en el cual ocurre esto. Entonces

$$H(X,Y) = Y^t\big(\sum_{n=0}^{\infty} f_{n+t}(X)Y^n\big) = Y^t G(X,Y),$$

donde $G(X,Y) = \sum_{n=0}^{\infty} f_{n+t}(X)Y^n$. Fijemos $a \in J$, como la serie $H(a,Y)$ converge en J, entonces también lo hace $G(a,Y)$ en J, de ahí que J esta contenido en el intervalo de convergencia de $G(a,Y)$. Además, para $b \in J$ se da

$$G(a,b) = \begin{cases} 0 & ; \ b \neq 0 \\ f_t(a) & ; \ b = 0 \end{cases}$$

Como una serie de potencias define una función continua en su intervalo de convergencia, tendremos que $G(a,Y)$ es continua en J; por lo tanto

$$f_t(a) = G(a,0) = \lim_{b\to 0} G(a,b) = 0,$$

para cualquier $a \in I$. Como un polinomio no nulo sólo tiene un número finito de cero llegamos a una contradicción, por tanto todos los polinomios $f_n(X)$ son identicamente nulos. □

Proposición 7.5.10 *Las series formales* $\exp(X)$ *y* $\log(1+X)$ *satisfacen*

$$\exp(\log(1+Y)) = Y \quad y \quad \log(\exp(Y)) = 1+Y.$$

Demostración.- Tomando $\mathcal{E}_1$ el homomorfismo evaluación $X = 1$, por la expresión de $\exp(X\log(1+Y))$ en la ecuación (7.4), deducimos que

$$1+Y = B(1,Y) = \mathcal{E}_1(B(X,Y)) = \mathcal{E}_1\big(\exp(X\log(1+Y))\big) = \exp(\log(1+Y)).$$

Esta igualdad nos dice que $E(X) = \exp(X) - 1 \in \mathbb{Q}[[X]]$ cumple que $E(Y) \circ \log(1+Y)) = Y$, luego por el lema 7.2.7 tendremos que $\log(1+Y) \circ E(Y) = Y$, esto es $\log(\exp(Y)) = Y$. □

Corolario 7.5.11 *Dados* $f(Y), g(Y) \in 1 + Y\mathbb{Q}[[Y]]$, *entonces*

$$\log(f(Y)) + \log(g(Y)) = \log(f(Y)g(Y)).$$

Demostración.- Se tiene que

$$\exp\big(\log(f(Y))+\log(g(Y))\big) = \exp\big(\log(f(Y))\big)\exp\big(\log(g(Y))\big) = \big(1+(f(Y)-1)\big)\big(1+(g(Y)-1)\big);$$

luego, componiendo con la función $\log(1+Y)$ concluimos que

$$\log(f(Y)) + \log(g(Y)) = \log(f(Y))\log(g(Y)).$$

□

Este corolario trae como consecuencia las siguientes igualdades

Proposición 7.5.12

- *Dado* $n \in \mathbb{N}$, *se tiene que* $n\log(1+Y) = \log((1+Y)^n)$.
- *Si* $f(Y) \in 1 + Y\mathbb{Q}[[Y]]$, *entonces* $-\log(f(Y)) = \log(f(Y)^{-1})$.
- *Sean* D *un dominio que contiene a* $\mathbb{Q}$, $a \in D$ *y* $d \geq 1$. *Entonces*

$$\exp\Big(\sum_{s=1}^{\infty} \frac{a^s}{s}(X^d)^s\Big) = (1-aX^d)^{-1} = \sum_{s=0}^{\infty} a^s(X^d)^s.$$

Demostración.- En virtud del anterior corolario las demostraciones del primer y segundo ítem son rutinarias, por tanto procedamos a verificar el tercer. Como

$$\sum_{s=1}^{\infty} \frac{a^s}{s}(T^d)^s = -\sum_{s=1}^{\infty} \frac{(-1)^{s+1}}{s}(-aT^d)^s = -\log(1+T)\circ(-aT^d) = -\log(1-aT^d),$$

por tanto

$$\exp\Big(\sum_{s=1}^{\infty} \frac{a^s}{s}(X^d)^s\Big) = \exp\big(\log((1-aT^d)^{-1})\big) = (1-aT^d)^{-1};$$

la última igualdad se consecuencia de un ejemplo anterior.

Capítulo 8

Análisis p-ádico

En este capítulo estudiaremos las propiedades analíticas de $\mathbb{C}_p$ explotando la propiedad no arquimediana. Empezaremos en el caso general de un cuerpo completo no arquimediano, pues nos generalizará resultados utiles tanto para series formales como para las mismas series en $\mathbb{C}_p$.

8.1. Series de potencias en una variable

De manera semenjante a los polinomios con coeficientes en un anillo, las series formales pueden brindar funciones sobre un dominio; así también nos brindará información acerca de la serie formal que la produjó.

En esta sección asumiremos que K es un subcuerpo completo de $\mathbb{C}_p$ y que $|\cdot|$ es el valor absoluto p-ádico sobre K. Empezaremos estudiando sólo series formales en una sola variable.

Dado $f(X) = \sum a_n X^n \in K[[X]]$ y $\alpha \in K$, la evaluación " más natural "de α respecto a $f(X)$ seria dada por el límite $\sum a_n \alpha^n$. Sin embargo, este límite puede no existir para algunos valores especificos en K, con el fín de determinar el dominio de este candidato de función damos la siguiente definición.

Definición 8.1.1 Dado $f(X) = \sum a_n X^n \in K[[X]]$, definimos el *el radio de convergencia de* $f(X)$ como el real extendido **(esta bien decir como, en lugar de: por??)**

$$\mathcal{R}_{f(X)} = \sup\{r \geq 0 \,;\, \lim_{n\to\infty} |a_n| r^n = 0\}.$$

Ejemplos 8.1.2 Los siguientes casos son el menor y el mayor valor posible que un radio de convergencia puede tomar.

- Tomemos $(a_n) \subset \mathbb{C}_p$ como $a_n = p^{-n^2}$, para todo $n \geq 0$; y $f(X) = \sum a_n X^n$. Entonces, dado $r > 0$ y $s = \log(r)/\log(p)$ se tiene que

$$\lim_{n\to\infty} v_p(a_n) + ns = \lim_{n\to\infty} n^2 + ns = +\infty;$$

por tanto $\lim_{n\to\infty} |a_n|_p r^n = +\infty$, para todo $r > 0$. De esta forma concluimos que $\mathcal{R}_{f(X)} = 0$.

- Sea $g(X) = \sum b_n X^n \in \mathbb{C}_p[[X]]$ con $b_n = p^{n^2}$ para todo $n \geq 0$. Entonces, para cada $r > 0$, tenemos que $s = \log r/\log p$ cumple

$$\lim_{n\to\infty} v_p(b_n) + ns = \lim_{n\to\infty} -n^2 + ns = -\infty \quad \text{y} \quad \lim_{n\to\infty} |a_n|_p r^n = 0;$$

así concluimos que $\mathcal{R}_{f(X)} = \infty$.

Observación 8.1.3 Dado $r \geq 0$ un real extendido, denotaremos

$$\mathcal{D}(r) = \{x \in K\,;|x| < r\} \qquad \text{y} \qquad \mathcal{D}(r) = \{x \in K\,;|x| \leq r\}$$

Definición 8.1.4 Sea $f(X) = \sum a_n X^n \in K[[X]]$.

- Diremos que $f(X)$ *converge en* $\alpha \in K$ si existe $\sum a_n \alpha^n$; a este límite lo denotaremos por $f(\alpha)$. En caso de no existir este límite, diremos que $f(X)$ *diverge en* α.
- Dado $A \subset K$, diremos que $f(X)$ *converge en* A si $f(X)$ converge en a, para todo $a \in A$; en este caso diremos que A es una *region de convergencia de* $f(X)$.
- La función $\mathfrak{f} : \{\alpha \in K\,;\, \exists f(\alpha)\} \to K$ definida por $\mathfrak{f}(\alpha) = f(\alpha)$ se le denomina *serie de potencias.*
- Una serie de potencias con radio de convergencia infinito será denominada *función entera p-ádica.*
- Una serie de potencias es una *función meromorfa p-ádica* si la serie formal que la define es cociente de dos series formales cuyo radio de convergencia sea infinito.

Proposición 8.1.5 *Sea* $f(X) = \sum a_n X^n \in K[[X]]$.

- *La serie formal* $f(X)$ *converge en* $\mathcal{D}(\mathcal{R}_{f(X)})$.
- *La serie formal* $f(X)$ *diverge en* α, *cuando* $\alpha \notin \mathcal{D}[\mathcal{R}_{f(X)}]$.
- *Si* $f(X)$ *converge para algún* $\alpha_0 \in K$ *con* $|\alpha_0| = \mathcal{R}_{f(X)}$, *entonces* $f(X)$ *converge en* $\mathcal{D}[\mathcal{R}_{f(X)}]$.

- *Si $f(X)$ diverge para algún $\alpha_0 \in K$ con $|\alpha_0| = \mathcal{R}_{f(X)}$, entonces $f(X)$ diverge en todo $\alpha \notin \mathcal{D}[\mathcal{R}_{f(X)}]$.*

Demostración.- Estas cuatro afirmaciones son resultado directo de la siguiente equivalencia:

Dado $\alpha \in K$, existe $f(\alpha)$ si y sólo si $\lim_{n\to\infty} |a_n||\alpha|^n = 0$.

La veracidad de esta afirmación se ampara en el lema 4.4.3 □

Observación 8.1.6 Sea $f(X) = \sum a_n X^n \in K[[X]]$. Una definición alternativa de $\mathcal{R}_{f(X)}$ es la siguiente:

$$\mathcal{R}_{f(X)} = \sup\{r \geq 0 \ ; \ (|a_n|r^n) \subset \mathbb{R} \text{ esta acotada}\}.$$

En efecto, es claro que el radio de convergencia es menor o igual que este supremo; además si $r > 0$ es tal que $(|a_n|r^n)$ es acotada entonces tomando $s < r$ tendremos que

$$\lim_{n\to\infty} |a_n|s^n = \lim_{n\to\infty} |a_n|r^n(r/s)^n = 0,$$

por tanto $s \leq \mathcal{R}_{f(X)}$, para todo $s < r$. Luego, $r \leq \mathcal{R}_{f(X)}$ y que $\mathcal{R}_{f(X)}$ es mayor o igual al supremo enunciado.

La siguiente proposición nos muestra otra similitud entre los cuerpos arquimedianos y los no arquimedianos, la cual es una versión de la conocida formula de Hadamard para el radio de convergencia de una serie de potencias en $\mathbb{R}$ o $\mathbb{C}$. Para el enunciado y demostración admitiremos las convenciones $\infty^{-1} = 0$ y $0^{-1} = \infty$.

Proposición 8.1.7 *Sea $f(X) = \sum a_n X^n \in K[[X]]$, entonces $\mathcal{R}_{f(X)} = (\limsup \sqrt[n]{|a_n|})^{-1}$.*

Demostración.- Sea $\rho = \limsup \sqrt[n]{|a_n|}$. Supongamos que $\rho = 0$ y fijemos $r > 0$. Dado $\epsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $\sup\{\sqrt[n]{|a_n|} \ ; \ n \geq n_0\} < \epsilon/r$, por lo tanto $|a_n|r^n < \epsilon$, para todo $n \geq n_0$. De este modo verificamos que $\lim_{n\to\infty} |a_n|r^n = 0$, para cualquier $r > 0$; así $\mathcal{R}_{f(X)} = \infty$ y que la formula es valida para este caso.

Asumamos que $\rho = \infty$ y tomemos $r > 0$ cualquiera. Entonces existe $n_0 \in \mathbb{N}$ tal que $1/r < \sup\{\sqrt[n]{|a_n|} \ ; \ n \geq n_0\}$; esto es $1 < |a_n|r^n$ para todo $n \geq n_0$. Así concluimos que $\lim |a_n|r^n \neq 0$ para todo $r > 0$; por lo tanto $\mathcal{R}_{f(X)} = 0$.

Finalmente, verifiquemos el caso en que ρ es un número real positivo. Dado $r > \rho$ se cumple que existe $n_0 \in \mathbb{N}$ tal que $\sup\{\sqrt[n]{|a_n|} \ ; \ n \geq n_0\} < r$; luego $|a_n|(1/r)^n < 1$, paratodo $n \geq n_0$. De esta forma $\left(|a_n|(1/r)^n\right) \subset \mathbb{R}$ esta acotada y $1/r \leq \mathcal{R}_{f(X)}$, por lo tanto $\rho^{-1} \leq \mathcal{R}_{f(X)}$. Recíprocamente, si $r > 0$ tal que $\lim |a_n|r^n = 0$, entonces existe $n_0 \in \mathbb{N}$ tal que $|a_n|r^n < 1$, para todo $n \geq n_0$; luego $\sup\{\sqrt[n]{|a_n|} \ ; \ n \geq n_0\} < r^{-1}$. Entonces, $\rho \leq r^{-1}$, o bien $r \leq \rho^{-1}$; tomando en cuenta la definición de $\mathcal{R}_{f(X)}$ concluimos este caso. □

Corolario 8.1.8 *Sea* $f(X) = \sum_n a_n X^n \in K[X]$. *Si* $|a_n| \leq 1$ *para todo* $n \geq 0$, *entonces* $f(X)$ *converge en* $\mathcal{D}(1)$.

Ejemplos 8.1.9 Al igual que en análisis real y complejo, podemos definir la función exponencial y logaritmo en $\mathbb{C}_p$.

1. *La función exponencial* p-ádica $\exp_p$ es la función que se obtiene por evaluar a la serie formal $f(X) = \sum a_n X^n$ con $a_n = 1/n!$, para todo $n \geq 0$.

2. *La función logaritmo* p-ádica $\log_p$ es la función que se obtiene por evaluar a la serie formal $g(X) = \sum b_n X^n$ con $b_n = (-1)^{n+1}/n$, para todo $n \geq 0$.

Determinemos con precisión sus regiones de convergencia.

1. Por el lema 5.1.2, dado $n \geq 1$ se tiene que $|a_n|_p = p^{-v_p(a_n)} = p^{\frac{n-s(n)}{p-1}}$, donde $s(n)$ es la suma de las cifras del numeral en base p que representa a n. Por lo tanto, $\sqrt[n]{|a_n|_p} \leq p^{\frac{1}{p-1}}$, para todo $n \geq 1$; de esta forma $p^{\frac{1}{1-p}} \leq \mathcal{R}_f(X)$. Sin embargo, dado $\alpha \in \mathbb{C}_p$ con $|\alpha|_p = p^{\frac{-1}{p-1}}$, para cada $m \geq 1$ vemos que $|a_{p^m}\alpha^{p^m}|_p = p^{\frac{p^m-1}{p-1}\frac{-p^m}{p-1}} = p^{\frac{1}{1-p}}$; por lo tanto $\lim_{n\to\infty}(a_n\alpha^n) \neq 0$ y $\exp_p$ esta definida exactamente en $\mathcal{D}(p^{\frac{1}{p-1}})$.

2. Para cada $n \geq 1$ tenemos que $\sqrt[n]{|b_n|_p} = p^{v_p(n)/n} \leq p^{\log(n)/n\log(p)}$ (por la observación 5.1.3), luego $\limsup \sqrt[n]{|b_n|_p} \leq p^0 = 1$ y $\mathcal{R}_{g(X)} \geq 1$. Más aun, puesto que $|b_{p^m}|_p = p^m$ para todo $m \geq 1$, concluimos que $(b_n \cdot 1^n)_{n\geq 0} \subset \mathbb{C}_p$ posee una subsucesión que no converge a cero. Por lo tanto $g(X)$ diverge en todo α con $|\alpha|_p = 1$ y $\log_p$ esta definido exactamente en $\mathcal{D}(1)$.

8.2. Series de potencias en varias variables

Extenderemos las definiciones de la sección de forma natural utilizando las nociones de series indexadas por conjuntos numerables. Fijemos $n \geq 1$ entero, $\mathfrak{N} = \mathbb{N}_0^n$ y $(K, |\cdot|)$ como un subcuerpo completo de $(\mathbb{C}_p, |\cdot|_p)$.

Definición 8.2.1 Sea $f(X) = \sum_{u\in\mathfrak{N}} a_u X^u \in K[[X]]$.

- Dado $\alpha \in K^n$, diremos que $f(X)$ converge en α si existe $\sum_{u\in\mathfrak{N}} a_u\alpha^u$ (respecto al valor absoluto $|\cdot|$); en este caso denotaremos a este límite como $f(\alpha)$.

- Dado $X \subset K^n$, diremos que $f(X)$ converge en X si existe $f(\alpha)$, para todo $\alpha \in X$.

Observación 8.2.2 Dado $f(X) \in K[[X]]$, podemos construir una función sobre un subconjunto de K^n, por asignar a $\alpha \in K^n$ el valor de $f(\alpha)$, siempre que $f(X)$ converja en α. A este tipo de funciones se les conoce como *serie de potencias en varias variables.*

Las siguientes igualdades muestran el buen comportamiento de la serie de potencias respecto a las serie formales que las generan, las cuales son resultado inmediato de las proposiciones 4.4.13 y 4.4.16.

Proposición 8.2.3 *Sean $f(X), g(X) \in K[[X]]$. Si $f(X)$ y $g(X)$ convergen en $\alpha \in K^n$ entonces también lo hacen $f(X)+g(X)$ y $f(X)g(X)$; más aun sus límites respectivos son $f(\alpha)+g(\alpha)$ y $f(\alpha)g(\alpha)$.*

Proposición 8.2.4 *Sean $f(X,Y) = \sum a_{m,n}X^mY^n \in K[[X,Y]]$ y $(\alpha,\beta) \in K^2$. Si $F(X,Y)$ converge en $(\alpha.\beta)$, entonces*

$$f(\alpha,\beta) = \sum_{m=0}^{\infty}\Big(\sum_{n=0}^{\infty} a_{m,n}\beta^n\Big)\alpha^m = \sum_{n=0}^{\infty}\Big(\sum_{m=0}^{\infty} a_{m,n}\alpha^m\Big)\beta^n.$$

Demostración.- Por la proposición 4.4.17, tendremos que

$$\sum_{n=0}^{\infty} a_{m,n}\alpha^m\beta^n \quad \text{y} \quad \sum_{m=0}^{\infty} a_{m,n}\alpha^m\beta^n, \quad \text{para todo } m,n \geq 0.$$

Por lo tanto,

$$f(\alpha,\beta) = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} a_{m,n}\alpha^m\beta^n = \sum_{m=0}^{\infty}\Big(\sum_{n=0}^{\infty} a_{m,n}\beta^n\Big)\alpha^m;$$

la otra igualdad se demuestra de manera análoga. □

Lema 8.2.5 *Sean $f(T) \in K[[T]]$, $g(X_1,\ldots,X_n) = bX_1^{u_1}\cdots X^{u_n} \in K[[X_1,\ldots,X_n]]$ con $g(X) \in \mathfrak{p}_X$. Si $\alpha \in K^n$ es tal que $f(T)$ converge en $g(\alpha)$, entonces $f(T)\circ g(X)$ es convergente en α y su valor es $f(g(\alpha))$.*

Demostración.- Tan sólo tomaremos el caso en que $b \neq 0$, el cual no es trivial. Sean $f(T) = \sum_m^{\infty} a_m T^m$, $\alpha = (\alpha_1,\ldots,\alpha_n)$, $u = (u_1,\ldots,u_n)$ y $h(X_1,\ldots,X_n) = f(T)\circ g(X_1,\ldots,X_n) \in K[[X_1,\ldots,X_n]]$. Entonces

$$h(X_1,\ldots,X_n) = \sum_{m=0}^{\infty} a_m b_u^m X_1^{mu_1}\cdots X_n^{mu_n} = \sum_v c_v X^v,$$

donde

$$c_v = \begin{cases} a_0 & , \text{ si } v = 0 \\ a_m b^m & , \text{ si } v \neq 0 \text{ y } v = mu, \quad \text{para algún } m \in \mathbb{N} \\ 0 & , \text{ si } v \neq 0 \text{ y } v \neq mu, \quad \text{para todo } m \in \mathbb{N} \end{cases}$$

Nótese que esta definición es buena porque existe a lo mas existe un natural m tal que $v = mu$. De hecho, como $\omega_X(g(X)) > 0$, existe algún índice no nulo, digamos u_j es no nulo. Por lo tanto, si existe otro $m' \in \mathbb{N}$ tal que $v = m'u$, tendremos que $mu_j = m'u_j$, luego $m = m'$ y m es único.

Como $f(T)$ converge en $g(\alpha)$, dado $\epsilon > 0$ existe $l_0 \in \mathbb{N}$ tal que $l \geq l_0$ implica $|f(\alpha) - \sum_{m=0}^{l} a_m g(\alpha)^m| < \epsilon$. Definamos $F_0 = \{v\ ,\ |v| \leq l_0|u|\}$. Si un subconjunto finito de multiindices F contiene a F_0 y $l = \text{máx}\{m \geq 0\ ,\ mu \in F\}$ entonces $l \geq l_0$ y $\displaystyle\sum_{v\in F} c_v\alpha^v = \sum_{m=0}^{l} a_m b^m \alpha_1^{mu_1} \ldots \alpha_n^{mu_n}$. Por lo tanto $|\sum_{v\in F} c_v\alpha^v - f(\alpha)| < \epsilon$, para todo subconjunto finito $F \supset F_0$; luego, por la proposición 4.4.11 concluimos el lema. □

Corolario 8.2.6 *Sean $f(T) \in K[[T]]$ y $a \in K$. Si $f(T)$ posee radio de convergencia infinito, entonces $f(aT)$ también posee radio de convergencia infinito.*

8.3. El teorema p-ádico de preparación de Weierstrass

En esta sección estudiaremos más las propiedades que satisface una función analítica p-ádica en una bola cerrada en el origen. Para esto utilizaremos un valor absoluto adecuado que provendrá del mismo hecho que la serie formal sea convergente esta región.

Al igual que en anteriores secciones aquí también supondremos que K es cuerpo completo contenido $\mathbb{C}_p$ y que $|\cdot|$ es una restricción del valor absoluto p-ádico, los cuales se mantedran durante toda la sección; así también fijaremos un número real $c > 0$.

Supongamos que $f(X) = \sum_n a_n X^n \in K[[X]]$ converge en $\alpha \in K$, entonces, nombrando c a $|\alpha|$, tendremos que

$$\lim_{n\to\infty} |a_n|c^n = \lim_{n\to\infty} |a_n\alpha^n| = 0.$$

Si un número real $c > 0$ cumple esta relación con los coeficientes de $f(X)$, entonces existe $\text{máx}\{|a_n|\ ,\ n \in \mathbb{N}\}$. De hecho, en el caso que exista algún $m \in \mathbb{N}$ tal que $a_m \neq 0$ (el único caso a tener en cuenta), existirá $N \in \mathbb{N}$ tal que

$$|a_n|c^n < |a_m|c^m \qquad \text{siempre que } n \geq N;$$

nótese que sera necesario que $m < N$. Por tanto

$$\sup\{|a_n|c^n\ ,\ n \in \mathbb{N}\} = \sup\{|a_n|c^n\ ,\ n < N\} = \text{máx}\{|a_n|c^n\ ,\ n < N\}.$$

Definición 8.3.1 Definimos

1. El conjunto $\mathfrak{A}_c = \{\sum_n a_n X^n \in K[[X]]\ ;\ \lim |a_n|c^n = 0\}$.

2. La función $\|\cdot\|_c : \mathfrak{A}_c \to \mathbb{R}$ por $\max\{|a_n|c^n \ ; \ n \in \mathbb{N}\}$.

La siguiente proposición nos da una idea de la relación de estas series formales con sus radios de convergencia.

Proposición 8.3.2 *Para todo $c > 0$, se cumple*

$$\mathfrak{A}_c \subset \{f(X) \in K[[X]] \ ; \ f(X) \text{ es convergente en } \mathcal{D}[c]\}.$$

En el caso que $c \in |K|$ sea da la igualdad.

Demostración.- Es claro que resta verificar que toda serie de potencias que converge en $\mathcal{D}[c]$ pertenece a $\mathfrak{A}_c$, para esto tomemos una de estas series $f(X) = \sum a_n X^n \in K[[X]]$ y $\alpha \in K$ con $c = |\alpha|$. Entonces como $\sum a_n \alpha^n$ converge, la secuencia $(a_n \alpha_n)$ tiende a cero, por tanto $\lim_n |a_n|c^n = 0$. □

Observación 8.3.3 El anterior contenido de conjunto puede ser estricto. De hecho, si $K = \mathbb{C}_p$ y $c = \pi$, tomemos $(q_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ creciente tal que $\lim_n q_n = \pi$ y $(a_n) \subset \mathbb{C}_p$ tal que $v_p(a_n) = nq_n$ para todo $n \in \mathbb{N}$. Entonces

$$\limsup \sqrt[n]{|a_n|} = \limsup p^{-q_n} = p^{-\pi},$$

por lo cual $f(X) = \sum a_n X^n \in K[[X]]$ es convergente en $\mathcal{D}(\pi) = \mathcal{D}[\pi]$. Sin embargo,

$$|a_n|p^{n\pi} = p^{n(\pi - q_n)} \geq 1, \qquad \text{para todo } n \in \mathbb{N}.$$

La siguiente proposición es inmediata de la definición y la proposición 4.4.12.

Proposición 8.3.4 *Sea $c > 0$ y $f(X) \in \mathfrak{A}_c$. Si $\alpha \in \mathcal{D}[c]$ se tiene entonces $|f(\alpha)| \leq \|f(X)\|_c$.*

Proposición 8.3.5 *El conjunto $\mathfrak{A}_c$ es un subanillo de $K[[X]]$.*

Demostración.- Sean $f(X) = \sum_i a_i X^i$ y $g(X) = \sum_j b_j X^j$ en $\mathfrak{A}_c$ no nulos. Dado $\epsilon > 0$, tomemos $I, J \in \mathbb{N}$ tales que

$$|a_i|c^i < \epsilon/\|g(X)\|_c \text{ y } |b_j|c^j < \epsilon/\|f(X)\|_c \quad \text{siempre que } i \geq I, \ \ j \geq J.$$

Si $i \geq I$ o $j \geq J$ entonces $|a_i||b_j|c^{i+j} < \epsilon$; por lo cual para todo $k \geq I + J$ ocurre que

$$|\sum_{i+j=k} a_i b_j|c^k \leq \max_{i+j=k}\{|a_i||b_j|c^k\} \leq \epsilon,$$

pues si $i < I$ entonces $j > J$. □

Observación 8.3.6 Durante esta sección denotaremos por P_m al conjunto P_m de los polinomios de grado a lo más m, para cada $m \geq 0$ entero.

No es dificíl ver que $\mathfrak{A}_c$ posee estructura de K-espacio vectorial con las operaciones de suma de series formales y producto por un elemento de K (heredadas del anillo $K[[X]]$); como también que $\|\cdot\|_c$ es una norma sobre $\mathfrak{A}_c$. Así también, los subconjuntos $K[X]$ y P_m seran K-subespacioa vectoriales de $\mathfrak{A}_c$. Todavia podemos decir algo más acerca de estos subespacios vectoriales.

Lema 8.3.7 *Dado $c > 0$, se tiene que*

- *El espacio $(\mathfrak{A}_c, \|\cdot\|_c)$ es de Banach.*
- *El subespacio $P_m \subset K[X]$ de los es cerrado bajo $\|\cdot\|_c$, para todo $m \geq 0$.*
- *El subespacio $K[X]$ es denso $\mathfrak{A}_c$.*

Demostración.- Veamos que $\mathfrak{A}_c$ es completo bajo esta norma. Dado $(f_j(X))_{j\in\mathbb{N}} \subset \mathfrak{A}_c$ de Cauchy, denotemos $f_j(X) = \sum_n a_{j,n}X^n$, para todo $j \in \mathbb{N}$. Entonces, dado $n \geq 0$ entero y $\epsilon > 0$, existe $j_0 \in \mathbb{N}$ tal que $j \geq j_0$ implica que $\|f_j(X) - f_{j+1}(X)\|_c < \epsilon c^n$. Por lo tanto,

$$|a_{j+1,n} - a_{j,n}| < \epsilon, \quad \text{siempre que } j \geq j_0;$$

así concluimos que $(a_{j,n})_{j\in\mathbb{N}} \in K$ es de Cauchy, para todo $n \geq 0$. Puesto que K es completo, para cada $n \geq 0$, existe $\lim_j a_{j,n}$, que denotamos por a_n. Definamos $f(X) = \sum_n a_n X^n \in K[[X]]$ y verifiquemos que $f(X) \in \mathfrak{A}_c$. Dado $\epsilon > 0$ existe $l \in \mathbb{N}$ tal que

$$\|f_j(X) - f_k(X)\|_c < \epsilon/2, \quad \text{siempre que } j, k \geq l;$$

esto es

$$|a_{j,n} - a_n|c^n < \epsilon/2 \quad \text{para todo } n \geq 0, j \geq l. \tag{8.1}$$

Tomando $N \in \mathbb{N}$ tal que $n \geq N$ implique $|a_{l,n}|c^n < \epsilon/2$, tendremos que $n \geq N$ implica

$$|a_n|c^n \leq |a_{l,n} - a_n|c^n + |a_{l,n}|c^n < \epsilon/2 + \epsilon/2 = \epsilon;$$

como $\epsilon > 0$ fue arbitrario, esto significa que $\lim_n |a_n|c^n = 0$. Luego, la desigualdad (8.1) se traduce a

$$\|f_j(X) - f(X)\|_c \leq \epsilon/2 \quad \text{siempre que } j \geq l;$$

lo cual nos indica que $f_j(X)$ converge a $f(X)$ en la norma $\|\cdot\|_c$.

Ahora, supongamos que $(f_j(X)) \subset P_m$ es una sucesión convergente. Entonces $(f_j(X))_{j\in\mathbb{N}}$ es una sucesión de Cauchy en $\mathfrak{A}_c$. Escribamos $f_j(X) = \sum_n a_{j,n}X^n$, para todo $j \in \mathbb{N}$. Vemos que estamos en bajo las mismas hipótesis de las cuales partimos al inicio de la demostración el primer ítem, entonces concluimos que existe

$$a_n = \lim_{j\to\infty} a_{j,n}, \qquad \text{para todo } n \in \mathbb{N}$$

y $\lim_{j\to\infty} f_j(X) = \sum_n a_n X^n$. Dado $n > m$, se tiene que $a_{j,n} = 0$, para todo $j \in \mathbb{N}$; por tanto $\sum a_n X^n$ tienen términos de orden a lo más m.

Finalmente, veamos que $K[X]$ es un denso $\mathfrak{A}_c$, tomemos $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathfrak{A}_c$ y demostremos que podemos obtener $g(X) \in K[X]$ tan cerca como nos deseesemos. Dado $\epsilon > 0$, existe $N \in \mathbb{N}$, tal que $|a_n|c^n < \epsilon$, para todo $n \geq N$. Entonces, definiendo $g(X) = \sum_{n=0}^{N} a_n X^n \in K[X]$ tendremos que

$$\|f(X) - g(X)\|_c = \text{máx}\{|a_n|c^n \ ; \ n > N\} < \epsilon.$$

□

Definición 8.3.8 Dado $f(X) = \sum_n a_n X^n \in K[[X]]$, diremos que $f(X)$ *alcanza* $\|\cdot\|$ *en* N si $|a_N|c^N = \|f(X)\|_c$.

Vemos que $\|\cdot\|_c$ en $\mathfrak{A}_c$ es una función que extiende el valor absoluto que definimos en el segundo ítem de los ejemplos 4.2.7 (el cual estaba definido sobre $K[X]$). Veamos como repercute el hecho que $K[X]$ sea denso en $\mathfrak{A}_c$.

Proposición 8.3.9 *La norma* $\|\cdot\|_c$ *es un valor absoluto no arquimediano sobre* $\mathfrak{A}_c$.

Demostración.- Es de verificación inmediata que $\|\cdot\|_c$ cumple las propiedades que definen a un valor absoluto no arquimediano excepto que respeta el producto (referente de la definición 4.2.1), la cual procedemos a demostrar. Para $f(X), g(x) \in \mathfrak{A}_c$ cualesquiera se tiene

$$\|f(X)g(X)\|_c \leq \|f(X)\|_c\|g(X)\|_c;$$

lo cual resulta del hecho que $|\cdot|$ es no arquimediano. Con el fin de probar la desigualdad recíproca, tomemos $(f_j(X)), (g_j(X)) \subset K[X]$ tales que $\lim_j f_j(X) = f(X)$ y $\lim_j g_j(X) = g(X)$. Entonces, aplicando la desigualdad triangular que cumple $\|\cdot\|_c$ como norma y lo antes mostrado tenemos que

$$\|f(X)g(X) - f_j(X)g_j(X)\|_c \leq \|f(X)\|_c\|g(X) - g_j(X)\|_c + \|g_j(X)\|_c\|f(X) - f_j(X)\|_c;$$

y como $(\|g_j(X)\|) \subset \mathbb{R}$ esta acotada (porque es sucesión convergente a $\|g(X)\|_c$), concluimos que $(f_j(X)g_j(X))_{j\in\mathbb{N}}$ converge a $f(X)g(X)$ respecto a $\|\cdot\|_c$. Entonces

$$\|f(X)g(X)\|_c = \|\lim_j f_j(X) \lim_j g_j(X)\|_c = \|\lim_j f_j(X)g_j(X)\|_c;$$

y, como acabamos de mencionar, puesto que $\|\cdot\|_c$ extiende a un valor absoluto en $K[X]$, tendremos que

$$\|f(X)g(X)\|_c = \lim_j \|f_j(X)\|_c\|g_j(X)\|_c = \|f(X)\|_c\|g(X)\|_c;$$

lo demuestra que $\|\cdot\|_c$ respeta el producto en $\mathfrak{A}_c$. □

Observación 8.3.10 Dado $f(X) = \sum_n a_n X^n \in \mathfrak{A}_c$, se tiene que $\lim_n |a_n|c^n = 0$; por lo cual existe $N \in \mathbb{N}$ tal que $n \geq N$ implica $|a_n|c^n < \|f(X)\|_c$. Por lo tanto, existe una cantidad finita de índices n_0 tales que $|a_{n_0}|c^{n_0} = \|f(X)\|_c$.

El siguiente proposición nos muestra algunas relaciones entre la estructura de serie de potencias y este valor absoluto no arquimediano, el enunciado hace uso de la observación previa.

Proposición 8.3.11 *Sean $f(X) \in \mathfrak{A}_c$ y $g(X) \in K[X]$.*

1. *Si $g(X)$ alcanza $\|\cdot\|_c$ en* grad $g(X)$ *e I es último índice donde $f(X)$ alcanza $\|\cdot\|_c$, entonces $f(X)g(X)$ alcanza $\|\cdot\|_c$ en* grad $g(X) + I$.

2. *Si $f(X) \in \mathfrak{A}_c$ alcanza $\|f(X)\|_c$ en N y* grad $g(X) < N$, *entonces*

$$\text{máx}\{\|f(X)\|_c, \|g(X)\|_c\} = \|f(X) + g(X)\|_c.$$

Demostración.-

1. Sean $g(X) = b_0 + b_1X + \cdots + b_NX^N$ tal que $|b_N|_p c^N = \|g(X)\|_c$, $f(X) = \sum_n d_nX^n \in \mathfrak{A}_c$ e $I = \text{máx}\{i\ ;\ |d_i|c^i = \|f(X)\|_c\}$. Si $i > I$, ocurria que $|d_i| < |d_I|c^{I-i}$; luego, para n tal que $i + n = I + N$ sucede que

$$|b_nd_i| < |b_n||d_I|c^{I-i} \leq |b_N|c^{N-n}|d_I|c^{I-i} = |b_N||d_I|.$$

En consecuencia,

$$|\sum_{i+n=I+N} b_nd_i|c^{N+I} = \max_{i+n=I+N}\{|b_nd_i|\}c^{N+I} = |b_N||d_I|c^{N+I} = \|g(X)\|_c\|f(X)\|_c,$$

de esta forma $f(X)g(X)$ al alcanza $\|f(X)g(X)\|_c$ en $N + I$.

2. Sea $f(X) = \sum d_n X^n$ tal que alcanza $\|f(X)\|_c$ en N y $g(X) = b_0 + b_1 X + \cdots + b_t X^t \in K[X]$ con $t < N$. Entonces el coeficiente N-ésimo de $f(X) + g(X)$ es el mismo que $f(X)$, por lo cual

$$\|f(X) + g(X)\|_c \geq |d_N| c^N = \|f(X)\|_c;$$

luego

$$\|g(X)\|_c \leq \max\{\|f(X) + g(X)\|_c, \|f(X)\|_c\} \leq \|f(X) + g(X)\|_c.$$

En resumen,

$$\max\{\|g(X)\|_c, \|f(X)\|_c\} \leq \|f(X) + g(X)\|_c,$$

y como $\|\cdot\|_c$ es no arquimediano, deducimos que esta desigualdad es en realidad una igualdad.

□

Una importante consecuencia de esta proposición es el siguiente lema, el cual muestra la relación entre el valor absoluto $\|\cdot\|_c$ respecto al algoritmo euclideano de la división en $K[X]$, siempre que el divisor sea el adecuado.

Lema 8.3.12 *Sea $g(X) \in K[X]$ no nulo que alcanza $\|\cdot\|_c$ en $N = \operatorname{grad} g(X)$. Si $f(X), q(X), r(X) \in K[X]$ cumplen que*

$$f(X) = q(X)g(X) + r(X) \qquad \text{con } r(X) = 0 \text{ o } \operatorname{grad} r(X) < \operatorname{grad} g(X),$$

entonces $\|f(X)\| = \max\{\|g(X)\|_c \|q(X)\|_c, \|r(X)\|_c\}$.

Demostración.- Esta claro que la dicha igualdad se verifica para el caso que $q(X)$ o $r(X)$ sean nulos, por lo cual asumiremos que ambos son distintos de 0. Por el primer ítem de la proposición anterior $g(X)q(X)$ alcanza en un índice mayor o igual a N; por tanto el segundo ítem nos conduce al resultado enunciado. □

Nuevamente utilizaremos la densidad de $K[X]$ en $\mathfrak{A}_c$ para extender resultados del anillo de polinomios a $\mathfrak{A}_c$.

Lema 8.3.13 *Sea $g(X) \in K[X]$ alcanza $\|g(x)\|_c$ en $\operatorname{grad} g(X)$. Para cada $f(X) \in \mathfrak{A}_c$ existen únicos $q(X) \in \mathfrak{A}_c$ y $r(X) \in K[X]$ de grado menor a $g(X)$ tales que*

$$f(X) = q(X)g(X) + r(X) \quad y \quad \|f(X)\|_c = \max\{\|q(X)\|_c \|g(X)\|_c, \|r(X)\|_c\}.$$

Demostración.- Tomemos $(f_j(X))_{j\in\mathbb{N}} \subset K[X]$ que sea convergente a $f(X)$ respecto a $\|\cdot\|_c$ Para cada $j \in \mathbb{N}$, por el algoritmo Euclideano de la división en $K[X]$ y el lema anterior existe únicos $q_j(X), r_j(X) \in K[X]$ con grad $r_j(X) <$ grad $g(X)$ tales que

$$f_j(X) = q_j(X)g(X) + r_j(X) \quad \text{y} \quad \|f_j(X)\|_c = \text{máx}\{\|q_j(X)\|_c\|g(X)\|_c, \|r_j(X)\|_c\}.$$

De esta forma obtenemos dos sucesiones en $K[X]$, veamos que estas son de Cauchy. De hecho, para cada $j \in \mathbb{N}$ se tiene que

$$f_{j+1}(X) - f_j(X) = (q_{j+1}(X) - q_j(X))g(X) + (r_{j+1}(X) - r_j(X)),$$

y como $r_{j+1}(X)$ y $r_j(X)$ son ambos de grado menor a grad $g(X)$, tendremos que $r_{j+1}(X) - r_j(X)$ también posee grado menor a grad $g(X)$. Por la unicidad del cociente y el residuo en el algoritmo de la división euclideana, concluimos que $q_{j+1}(X) - q_j(X)$ y $r_{j+1}(X) - r_j(X)$ son el cociente y el residuo de la divisón de $f_{j+1}(X) - f_j(X)$ por $g(X)$. Entonces, en virtud del lema previo, sucede que

$$\|q_{j+1}(X) - q_j(X)\|_c \leq \|g(X)\|_c^{-1}\|f_{j+1}(X) - f_j(X)\|_c$$

y

$$\|r_{j+1}(X) - r_j(X)\|_c\} \leq \|f_{j+1}(X) - f_j(X)\|_c$$

para todo $j \in \mathbb{N}$. Como $(f_j(X))$ es convergente, esta sucesión será de Cauchy, y por tanto $\lim_j(f_{j+1}(X) - f_j(X)) = 0$; por lo que concluimos con ayuda de estas dos últimas desigualdades que $(q_j(X))$ y $(r_j(X))$ son de Cauchy. Como $\mathfrak{A}_c$ es completo dichas sucesiones convergeran a $q(X)$ y $r(X)$ en $\mathfrak{A}_c$ respectivamente. Más aun, porque $(r_j(X))$ fue una sucesión de polinomios de grado menor a grad $g(X)$ (y este subespacio es cerrado en $\mathfrak{A}_c$), tendremos que $r(X)$ es también un polinomio de grado a lo más grad $g(X) - 1$. Luego

$$\|f(X)\|_c = \lim_j \|f_j(X)\|_c = \text{máx}\{\lim_j \|q_j(X)\|_c\|g(X)\|_c, \lim_j \|r_j(X)\|_c\},$$

esto es $\|f(X)\|_c = \text{máx}\{\|q(X)\|_c\|g(X)\|_c, \|r(X)\|_c\}$. Finalmente verifiquemos la unicidad de este "cociente" y " residuo". Supongamos que $q_0(X) \in \mathfrak{A}_c$ y $r_0(X) \in K[X]$ satisfacen las hipótesis del lema, entonces

$$(q(X) - q_0(X))g(X) = (r_0(X) - r(X)).$$

Si $q(X)$ fuese distinto de $q_0(X)$, por la proposición 8.3.11, ocurriria que $(q(X) - q_0(X))g(X)$ alcanza $\|(q(X) - q_0(X))g(X)\|$ en índice mayor o igual a N, lo cual no sucede en la serie $r_0(X) - r(x)$. Por lo tanto, $q(X)$ y $q_0(X)$ son iguales, y en consecuencia $r(X)$ y $r_0(X)$ son iguales. □

Observación 8.3.14 Sea $g(X) \in K[X]$ como en el enunciado del lema previo, entonces $g(X)$ sólo posee ceros en $\mathcal{D}[c]$. De hecho, si existiese $\alpha \in K$ con $|\alpha| = t > c$ y $g(\alpha) = 0$, entonces

$$|b_N||\alpha|^N = |-b_{N-1}\alpha^{N-1} - \cdots - b_0| \leq \max\{|b_k\alpha^k| \; ; \; k = 0, 1, \ldots, N-1\} = |b_{k_0}||\alpha|^{n_0},$$

para algún $k_0 \in \{0, 1, \ldots, N-1\}$. Entonces

$$|b_N|t^{N-k_0} \leq |b_{k_0}| \quad \text{y} \quad |b_N|c^{N-k_0} < |b_{k_0}|,$$

por lo tanto $\|g(X)\|_c < |b_{k_0}|c^{k_0}$, lo que es una absurdo.

A continuación presentamos el resultado principal de la sección, el nos muestra un tipo de factorización en $\mathfrak{A}_c$ y como veremos despues esta factorización nos permite separar los ceros de una serie en $\mathfrak{A}_c$ en el disco cerrado $\mathcal{D}[c]$.

Teorema 8.3.15 (Teorema p–ádico de Preparación de Weierstrass) *Sean* $f(X) = \sum_n a_n X^n \in \mathfrak{A}_c$ *y* $N = \max\{n \; ; \; |a_n|c^n = \|f(X)\|_c\}$. *Entonces, existen* $h(X) = \sum d_n X^n \in 1 + XK[[X]]$ *y* $g(X) = \sum b_n X^n \in K[X]$ *de grado* N. *Se cumple que*

1. $f(X) = g(X)h(X)$.
2. *El polinomio* $g(X)$ *alcanza* $\|\cdot\|$ *en* N.
3. $\|f(X) - g(X)\|_c < \|f(X)\|_c$.
4. *La serie* $h(X)$ *pertenece a* $\mathfrak{A}_c$.
5. $\|h(X) - 1\|_c < 1$.

Demostración.- Construiremos $g(X)$ y $h(X)$ como límites de dos sucesiones adecuadas; para empezar, tomemos que $g_0(X) = a_0 + a_1X + \cdots + a_NX^N \in K[X]$. Si $g(X) = f(X)$, entonces $g_0(X)$ y $h(X) = 1$ satisfacerian el teorema, por lo cual supondremos que $g_0(X) \neq f(X)$. Entonces,

$$\|f(X) - g_0(X)\|_c = \|\sum_{n \geq N+1} a_n X^n\|_c < |a_N|c^N,$$

por lo tanto $\delta = \|f(X) - g_0(X)\|_c / \|f(X)\| < 1$. Definamos el conjunto $\mathcal{B}$ de los pares $(g(X), h(x)) \in \mathcal{P}_N \times \mathfrak{A}_x$ tales que

i) $\|f(X) - g(X)\|_c \leq \delta\|f(X)\|$ y $\|h(X) - 1\|_c \leq \delta$.

ii) $\|f(X) - g(X)h(X)\|_c \leq \delta\|f(X)\|_c$.

recordamos que $\mathcal{P}_N$ es el conjunto de polinomios de grado a lo más N. El conjunto $\mathcal{B}$ es no vacío porque $(g_0(X), 1)$ le pertenece, procedamos a construir una función $G : \mathcal{B} \to \mathcal{B}$ con la intención de crear una sucesión en este conjunto por inducción.

En primer lugar, si $(g(X), h(X)) \in \mathcal{B}$, entonces $g(X) = b_0 + b_1 + \cdots + b_N X^N$ es un polinomio de grado N que satisface

$$\|g(X)\|_c = \max\{\|f(X) - g(X)\|_c, \|f(X)\|_c\} = \|f(X)\|_c.$$

Además,

$$|a_N - b_N|c^N \leq \|f(X) - q(X)\|_c < \|f(X)\|_c = |a_N|c^N,$$

por lo tanto

$$|b_N|pc^N = |a_N|c^N = \|f(X)\|_c = \|g(X)\|_c,$$

lo cual nos dice que $g(X)$ es un polinomio que puede ser utilizado en el lema previo. Tomemos los únicos $q(X) \in \mathfrak{A}_c$ y $r(X) \in K[X]$ de grado menor a N tales que

$$f(X) - g(X)h(X) = q(X)g(X) + r(X) \quad \text{y} \quad \|f(X) - g(X)h(X)\|_c = \max\{\|q(X)g(X)\|_c, \|r(X)\|_c\}.$$

Deducimos que

$$\|q(X)\|_c \leq \|f(X) - g(X)h(X)\|_c / \|g(X)\|_c = \|f(X) - g(X)h(X)\|_c / \|f(X)\|_c \tag{8.2}$$

en particular $\|q(X)\|_c \leq \delta$. Así también

$$\|r(X)\|_c \leq \|f(X) - g(X)h(X)\|_c, \tag{8.3}$$

y por tanto $\|r(X)\|_c \leq \delta\|f(X)\|_c$. En consecuencia, definiendo $\widetilde{g}(X) = g(X) + r(X)$ y $\widetilde{h}(X) = h(X) + q(X)$, tendremos que

$$\|f(X) - \widetilde{g}(X)\|_c \leq \max\{\|f(X) - g(X)\|_c, \|r(X)\|_c\} \leq \delta\|f(X)\|_c,$$

así también

$$\|\widetilde{h}(X) - 1\|_c \leq \max\{\|h(X) - 1\|_c, \|q(X)\|_c\} \leq \delta.$$

Además

$$f(X) - \widetilde{g}(X)\widetilde{h}(X) = r(X) - r(X)h(X) - r(X)q(X),$$

por tanto $\|f(X) - \widetilde{g}(X)\widetilde{h}(X)\|_c \leq \|r(X)\|_c \max\{\|1 - h(X)\|_c, \|q(X)\|_c\}$ y

$$\|f(X) - \widetilde{g}(X)\widetilde{h}(X)\|_c \leq \delta\|f(X) - g(X)h(X)\|; \tag{8.4}$$

en particular, $\|f(X) - \widetilde{g}(X)\widetilde{h}(X)\|_c \leq \delta\|f(X)\|_c$. Estas últimas desigualdades nos dicen que $(\widetilde{g}(X), \widetilde{h}(X)) \in \mathcal{B}$, dada la unicidad de los anteriores $q(X)$ y $r(X)$ podemos definir $G : \mathcal{B} \to \mathcal{B}$ por $G(g(X), h(X)) = (\widetilde{g}(X), \widetilde{h}(X))$. Luego, por inducción, existen $(g_n(X)) \in P_N$ y $(h_n(X)) \in \mathfrak{A}_c$ tales que

- $(g_1(X), h_1(X)) = (g_0(X), 1)$.
- $(g_{n+1}(X), h_{n+1}(X)) = G(g_n(X), h_n(X))$, para todo $n \in \mathbb{N}$.

Partiendo de que $\|f(X) - g_1(X) \cdot h_1(X)\|_c \leq \delta\|f(X)\|_c$ y por medio de la desigualdad (8.4) e inducción sobre $n \in \mathbb{N}$, obtenemos que

$$\|f(X) - g_n(X)h_n(X)\|_c \leq \delta^n\|f(X)\|_c \tag{8.5}$$

En consecuencia, por las desigualdades (8.2) y (8.3) (que tratan acerca de lo que añade G a $h_n(X)$ y $g_n(X)$) **chequear si esta aclaracion no ofende al lector**, para cada $n \in \mathbb{N}$ se tiene

$$\|h_{n+1}(X) - h_n(X)\|_c \leq \delta^n \quad \text{y} \quad \|g_{n+1}(X) - g_n(X)\|_c \leq \delta^n\|f(X)\|_c \tag{8.6}$$

Las desigualdades (8.5) y (8.6) nos conllevan a que $(g_n(X)) \subset \mathcal{P}_N$ y $(h_n(X)) \subset \mathfrak{A}_c$ son de Cauchy, por lo tanto convergen a $l(X) \in P_N$ y $t(X) \in \mathfrak{A}_c$. Asi tenemos que

$$\|t(X) - 1\|_c = \lim_{n\to\infty} \|h_n(X) - 1\|_c \leq \delta :$$

por lo tanto, escribiendo $t(X) = \sum d'_n X^n$, tendremos que

$$|d'_0 - 1| \leq \|t(X) - 1\|_c \leq \delta < 1,$$

lo cual implica que $|d'_0| = |1| = 1$. Definimos $h(X) = (d'_0)^{-1}t(X) \in 1 + XK[X]$ y $g(X) = d'_0 l(X)$, entonces $g(X) \in \mathcal{P}_N$ y $h(X) \in \mathfrak{A}_c$. Además,

$$\|f(X) - g(X)h(X)\|_c = \|f(X) - l(X)t(X)\| = \lim_{n\to\infty} \|f(X) - g_j(X)h_j(X)\|_c = 0;$$

por tanto el primer ítem del enunciado es cierto. Así también

$$\|h(X) - 1\|_c = \|\sum_{n\geq 1}(d'_0)^{-1}d'_n X^n\|_c = \|\sum_{n\geq 1} d'_n X^n\|_c = \|t(X) - 1\|_c < 1;$$

y el quinto ítem esta verificado. Lo que trae como consecuencia que

$$\|f(X)\|_c = \|g(X)h(X)\|_c = 1 \cdot \|g(X)\|_c = \|g(X)\|_c,$$

lo cual, a su vez nos conduce a

$$\|f(X) - g(X)\|_c = \|g(X)\|_c\|h(X) - 1\|_c < \|f(X)\|_c,$$

que es el tercer ítem. Y finalmente, como en el comienzo de esta demostración, esta desigualdad y que $g(X)$ tiene a lo más grado N, nos conlleva a que $g(X)$ alcanza $\|\cdot\|_c$ en N. □

Observaciones 8.3.16 Asumiendo las notaciones y resultados del teorema anterior, podemos deducir lo siguiente:

- Nótese que $\|h(X) - 1\|_c < 1$ implica que $h(X) \in 1 + XK[[X]]$.
- El hecho que $\|h(X) - 1\|_c < 1$ y $h \in \mathfrak{P}$, implica que $h(X)$ no posee ceros en $\mathcal{D}[c]$. De hecho, si $h(X) = \sum d_n X^n$ y tuviese un cero $\alpha \in \mathcal{D}[c]$, entonces $|\sum d_n \alpha^n - 1| = |1| = 1$ lo que contradice que la proposición 8.3.4.
- Por una observación anterior, el polinomio obtenido $g(X)$ sólo posee raíces en el disco $\mathcal{D}[c]$. Por lo tanto, este teorema logra "separar"todos los ceros de $f(X)$ contenidos en $\mathcal{D}[c]$ en el polinomio $g(X)$.
- Más aun, si $K = \mathbb{C}_p$, entonces el polinomio $g(X)$ puede ser descompuesto en $\mathbb{C}_p[X]$. En consecuencia, la serie $f(X)$ posee exactamente N ceros (contando multiplicidades) en el disco $\mathcal{D}[c]$ y todos son ceros de $g(X)$.

El segunda observación también puede ser consecuencia del siguiente lema, el cual nos muestra que las caracteristicas de la serie formal $h(X)$ obtenidas en el teorema anterior son muy utiles.

Lema 8.3.17 *Sea $h(X) \in \mathfrak{A}_c$ y $\|h(X) - 1\|_c < 1$, entonces $h^{-1}(X) \in \mathfrak{A}_c$ y satiface $\|h^{-1}(X) - 1\|_c < 1$.*

Demostración.- Por la demostración de la proposición 7.3.2 existe $h^{-1}(X) = \sum t_n X^n \in K[[X]]$ y satisface las ecuaciones (que lo definen recursivamente)

$$t_0 = 1 \quad \text{y} \quad t_n = -\sum_{k=0}^{n-1} t_k d_{n-k}, \qquad \text{para todo } n \in \mathbb{N}.$$

Puesto que $t_0 = d_0$ y $t_1 = -d_1$, tiene lugar planter la siguiente afirmación.

Afirmación : *Para cada $n \geq 1$*

$$|t_n| \leq \text{máx}\{|d_{i_1}| \cdots |d_{i_n}| \; ; \; i_j \in \mathbb{N}_0, i_1 + \cdots + i_n = n\}.$$

Para el caso $n = 1$ ya cierto esta afirmación. Supongamos que es cierto para todo $1 \leq k < n$. Entonces,

$$|t_n| = |-\sum_{k=0}^{n-1} t_k d_{n-k}| \leq \text{máx}\{|t_k||d_{n-k}| \; ; \; k = 0, 1, \ldots, n-1\}.$$

Por la hipótesis de inducción, cuando $k \geq 1$ vemos que

$$|t_k||d_{n-k}| \leq \text{máx}\{|d_{i_1}| \cdots |d_{i_k}||d_{n-k}| \; ; \; i_j \in \mathbb{N}_0, i_1 + \cdots + i_k = k\} \tag{8.7}$$

pero cada producto de arriba es tal que

$$|d_{i_1}| \cdots |d_{i_k}||d_{n-k}| = |d_{j_1}| \cdots |d_{j_{n-1}}||d_{j_n}|$$

donde $j_l = i_l$, para $l = 1, \ldots, k$, $j_{k+1} = n - k$ y $j_l = 0$ para $l = k+2, \ldots, n$. Entonces en (8.7) tendremos que

$$|t_k||d_{n-k}| \leq \text{máx}\{|d_{j_1}| \cdots |d_{j_n}| \; ; \; j_l \in \mathbb{N}_0, j_1 + \cdots + j_n = n\},$$

por lo tanto $|t_k|$ cumple también la afirmación. Como $|t_0||d_n| = |d_{j_1}| \cdots |d_{j_{n-1}}||d_{j_n}|$ con $j_1 = n$ y $j_2 = \cdots = j_n = 0$, concluimos la afirmación por inducción sobre n.

Por esta afirmación tendremos que

$$\begin{aligned} |t_n|c^n &< \text{máx}\{|d_{i_1}| \cdots |d_{i_n}| \; ; \; i_j \in \mathbb{N}_0, i_1 + \cdots + i_n = n\}c^n \\ &= \text{máx}\{|d_{i_1}|c^{i_1} \cdots |d_{i_n}|c^{i_n} \; ; \; i_j \in \mathbb{N}_0, i_1 + \cdots + i_n = n\}; \end{aligned}$$

por lo tanto concluimos $|t_n|c^n < 1$, para todo $n \geq 1$.

Dado $\epsilon > 0$ demostraremos que para n suficientemente grande $|t_n|c^n < \epsilon$. Como $\alpha = \text{máx}\{|d_n|c^n \; , \; n \geq 1\} = \|h(X) - 1\|_c < 1$, existe $M \in \mathbb{N}$ tal que $m \geq M$ implica $\alpha^m < \epsilon$. Así también, existe $N \in \mathbb{N}$ tal que $|d_n|c^n < \epsilon$, para todo $n \geq N$. Tomemos $n \geq NM$ e índices $i_1, \ldots, i_n \geq 0$ enteros tal que $i_1 + \cdots + i_n = n$. Si algún i_{j_0} es mayor que N, entonces

$$(|d_{i_1}| \cdots |d_{i_n}|)c^n = (|d_{i_1}|c^{i_1}) \cdots (|d_{i_n}|c^{i_n}) \leq |d_{i_{j_0}}|c^{i_{j_0}} < \epsilon.$$

Si todos los índices son a lo más N, denotemos a todos lo no nulos por $j_1, j_2, \ldots, j_r$; entonces

$$n = i_1 + \cdots + i_n = j_1 + j_2 + \cdots + j_r \leq rN,$$

y $r \geq n/N \geq M$, por lo tanto

$$(|d_{i_1}| \cdots |d_{i_n}|)c^n = (|d_{j_1}|c^{j_1}) \cdots (|d_{j_r}|_p c^{j_r}) \leq \alpha^r < \epsilon.$$

Por la afirmación, concluimos que $|t_n|c^n < \epsilon$, siempre que $n \geq NM$. Por lo tanto $\lim_{n\to\infty} |t_n|c^n = 0$ y $h^{-1}(X) \in \mathfrak{A}_c$. Además, como vimos que $|t_n|c^n < 1$ para $n \in \mathbb{N}$, se obtiene que $\|h(X) - 1\|_c$. □ Uniendo este lema y el teorema anterior conseguimos un resultado clave para el siguiente capítulo.

Corolario 8.3.18 *Sean $c > 0$ y $f(X) \in \mathfrak{A}_c$. Entonces existen $g(X) \in K[X]$ y $h(X) \in \mathfrak{A}_c$ con coeficiente independiente igual a 1, tales que $h(X)f(X) = g(X)$.*

8.4. Propiedades de series en $\mathbb{Z}_p$

En esta sección denotaremos por $\mathfrak{P}_X$ y $\mathfrak{P}_X^0$ los ideales de valuación de ω_X en $\mathbb{Z}_p[[X]]$ y $\mathbb{Q}_p[[X]]$, respectivamente. El siguiente lema, debido a Dwork, nos brinda condiciones suficientes y necesarias para que una serie formal en $\mathbb{Q}_p$ deba o no poseer coeficientes en $\mathbb{Z}_p$, este será un muy util test más adelante.

Lema 8.4.1 (Dwork) *Dado $F(X) \in 1 + \mathfrak{P}_X^0$, tendremos que*

$$F(X) \in 1 + \mathfrak{P}_X \quad \textit{si y sólo si} \quad \frac{F(X^p)}{(F(X))^p} \in 1 + p\mathfrak{P}_X.$$

Demostración.- Escribamos $F(X) = \sum_u a_u X^u$, donde el coeficiente independiente a_0 es 1. Supongamos que $a_u \in \mathbb{Z}_p$, para todo $u \in \mathfrak{N}$. Dado $d \in \mathbb{N}$, tomemos

$$F_d(X) = 1 + \sum_{0<|u|\leq d} a_u X^u = 1 + \sum_{j=1}^{l_d} a_{u_j} X^{u_j} \in \mathbb{Z}_p[X],$$

esto significa que $F_d(X)$ es el polinomio en n variables formado por los monomios de grado menor o igual a d, y que hemos enumerado los multiíndices no nulos. No es dificil verificar, por inducción, que en un anillo A se cumple que

$$(\sum_{k=1}^{m} c_k)^p = \sum_{k=1}^{m} c_k^p + \sum_{k=2}^{m} p c_k G_k(c_1, \ldots, c_m),$$

donde cada $G_k(Y_1, \ldots, Y_m) \in A[Y_1, \ldots, Y_m]$, para cada $k = 2, \ldots, m$. Entonces, realizando los reemplazos respectivos, obtendremos d_l polinomios $G_j(Y_1, \ldots, Y_{l_d}) \in \mathbb{Z}_p[Y_1, \ldots, Y_{l_d}]$ tales que

$$(F_d(X))^p = 1 + \sum_{j=1}^{l_d} a_{u_j}^p X^{pu_j} + p \sum_{j=1}^{l_d} a_{u_j} X^{u_j} G_j(a_{u_1} X^{u_1}, \ldots, a_{u_{l_d}} X^{u_{l_d}});$$

nótese que aquí estamos obviando la variable en donde se evaluo el sumando 1 (por ello los polinomios sólo poseen l_d variables en lugar de $l_d + 1$). Completando coeficientes tendremos que

$$(F_d(X))^p = F_d(X^p) + \sum_{j=1}^{l_d} (a_{u_j}^p - a_{u_j}) X^{pu_j} + p \sum_{j=1}^{l_d} a_{u_j} X^{u_j} G_j(a_{u_1} X^{u_1}, \ldots, a_{u_{l_d}} X^{u_{l_d}}).$$

La primera sumatoria presenta monomios de grado mayor o igual a 1, además poseen coeficientes en $\mathbb{Z}_p$ que son divisibles por p (por la proposición 5.1.13); por lo tanto esta sumatoria pertenece a $p\mathfrak{P}$. Así también, como cada u_j posee peso mayor o igual a 1, tendremos que la segunda sumatoria también pertenece a $p\mathfrak{P}_X$. Por tanto

$$(F_d(X))^p = F_d(X^p) + pH_d(X), \qquad \text{para algún } H_d(X) \in \mathfrak{P}_X.$$

Como $(F_d(X)^p)_{d\in\mathbb{N}}, (F_d(X^p))_{d\in\mathbb{N}} \subset \mathbb{Z}_p[[X]]$ son convergentes, también lo sera $(H_d(X))_{d\in\mathbb{N}} \subset \mathfrak{P}_X$ a algún $H(X) \in \mathfrak{P}_X$ (pues $\mathfrak{P}$ es cerrado, por la proposición 4.3.4). Tomando límite cuando d tiende a ∞, obtendremos que $(F(X))^p = F(X^p) + pH(X)$. Puesto que $F(X) \in 1 + \mathfrak{P}_X$, esta serie poseerá inversa $T(X) \in \mathbb{Z}_p[[X]]$, luego

$$\frac{F(X^p)}{(F(X))^p} = 1 - pH(X)(T(X))^p \in 1 + p\mathfrak{P}_X.$$

Recíprocamente, supongamos que existe $G(X) \in \mathfrak{P}_X$ tal que

$$F(X^p) = (F(X))^p(1 + pG(X)) \tag{8.8}$$

y escribamos $G(X) = \sum_v b_v X^v$, entonces $b_0 = 0$. Como $a_u \in \mathbb{Z}_p$ para todo $u \in U$ con $|u| = 0$ (pues es el único u es 0), tendremos el paso inicial del proceso de inducción que nos proponemos realizar, esto es, realizaremos inducción sobre el peso d de los multiindices. Asumamos que para todo $|u| < d$ se cumple que $a_u \in \mathbb{Z}_p$; nuestro objetivo sera demostrar que todo multiindice de peso d es un entero $p-$ádico. Fijemos $w \in \mathfrak{N}$ tal que $|w| = d$ y denotemos $F(X)^p = \sum_u \alpha_u X^u$ con

$$\alpha_u = \sum_{u_1+\cdots+u_p=u} a_{u_1} \cdots a_{u_p}, \qquad \text{para todo } u \in \mathcal{U}.$$

Tomemos a_w igual a $a_{w/p}$ cuando $p \nmid w$, o igual a 0 en caso contrario; entonces comparando el coeficiente $w-$ésimo de los extremos de (8.8), tendremos que

$$a_w = \alpha_w + p \sum_{\substack{u+v=w \\ u\neq w}} \alpha_u b_v, \tag{8.9}$$

Notemos que

$$\alpha_w = a_w^p + \sum_{\substack{u_1+\cdots+u_p=w \\ u_i\neq u_j}} a_{u_1} \cdots a_{u_p}$$

Ahora, cada sumando $a_{u_1} \cdots a_{u_p}$ se repite un número de veces igual al número de distintas reordenaciones de una n-ada $(u_1, \ldots, u_p)$. Por lo tanto, si un sumando $a_{u_1} \cdots a_{u_n}$ posee como multiindices distintos a $u_{i_1}, u_{i_2}, \ldots, u_{i_r}$ y estos multiindices se repiten $k_1, \ldots, k_r$ veces, respectivamente (en particular $k_1 + \cdots + k_r = p$). Entonces obtendremos que $a_{u_1} \cdots a_{u_n}$ se repetirá exactamente $\dfrac{p!}{k_1! \cdots k_2!}$ veces. Así por ejemplo, el sumando $a_w a_0 \cdots a_0$ se repite $\frac{p!}{1!(p-1)!} = p$ veces, y se obtiene pa_w dentro de la sumatoria. Más aún, los sumandos restantes $a_{u_1} a_{u_2} \cdots a_{u_p}$ poseen multindices distintos a w, pues las unicas n-adas que poseen a w son $(w, 0, \ldots, 0)$ y sus posibles reordenaciones, que ya fueron contabilizadas. Entonces, entre estos multiindices existen al menos dos distintos de 0 (y distintos de w), por decir u_j y u_k; luego, dado $i \in \{1, 2, \ldots, p\}$, si eligimos $l \in \{j, k\} \setminus \{i\}$ verificamos que

$$|u_i| < |u_i| + |u_l| \leq |u_1| + |u_2| + \cdots + |u_p| = |w|.$$

En consecuencia, estos sumandos sólo poseen multiindices de peso menor a $|w| = d$, entonces $a_{u_1} \cdots a_{u_p} \in \mathbb{Z}_p$. Además, puesto que entre sumandos poseen multiindices que se repiten menos que p veces (pues el caso $k_i = p$, ya esta catalogado en $a_{w/p}^p$), tendremos que el número de veces que se repiten ($\frac{p!}{k_1! \cdots k_r!}$) es multiplo de p, pues los factoriales $k_i!$ no seran divisibles por p. Así concluimos que

$$\alpha_w = a_w^p + p a_w + \sum_{\lambda \in \Lambda} p n_\lambda \beta_\lambda, \qquad \text{con } \beta_\lambda \in \mathbb{Z}_p, n_\lambda \in \mathbb{N};$$

donde Λ es un conjunto finito de multiindices. Finalmente, observando que los sumandos $\alpha_u b_v$ en (8.8) cumplen que $v \neq 0$, por tanto $|v| > 0$ y $|u| < |w|$. En estos sumandos, α_u es producto y suma de a_{u_j}, con $|u_j| \leq |u|$; y como $|u| < d$, por hipótesis de inducción, tendremos que cada a_{u_j} pertenece $\mathbb{Z}_p$, por lo tanto $\alpha_u \in \mathbb{Z}_p$. Entonces

$$a_w = a_w^p + p a_w + p \sum_{\lambda \in \Lambda} n_\lambda \beta_\lambda + p \sum_{u+v=w} \alpha_u b_v,$$

y por lo tanto $p a_w \in p\mathbb{Z}_p$ (pues $p \mid (a_{w/p} - a_{w/p}^p)$), esto significa $a_w \in \mathbb{Z}_p$; con lo cual concluimos el proceso de inducción. □

8.5. La serie binomial $p-$ádica.

Como vimos en una anterior sección, existe una relación entre las series formales $B(X,Y)$, $\exp(X)$ y $\log(1+Y)$; ahora nos proponemos explotarla evaluandolas con valores en $\mathbb{C}_p$.

Dado $a \in \mathbb{C}_p$, denotamos $B_a(Y) = B(a,Y) \in \mathbb{Q}[[Y]]$ a la *serie binomial de exponente a*. La razon de este nombre proviene de su relación con el binomio de Newton.

Proposición 8.5.1

1. *Dados $f(X), g(X) \in \mathbb{Q}[X]$ y $l \in \mathbb{N}$, se tiene que*

$$B\big(f(t), Y^l\big) B\big(g(t), Y^l\big) = B\big(p(t) + g(t), Y^l\big); \qquad \text{para todo } t \in \mathbb{C}_p.$$

2. *Si $a \in \mathfrak{D}_p$, entonces $B_a(Y)$ converge en $\mathcal{D}(p^{\frac{-1}{p-1}})$.*

3. *Más aun, si $a \in \mathbb{Z}_p$ entonces $B_a(Y) \in \mathbb{Z}_p[[Y]]$, y en consecuencia converge en $\mathcal{D}(1)$.*

4. *Si $(a_m) \subset \mathbb{Z}_p$ converge a $\alpha \in \mathbb{Z}_p$, entonces $\big(B(a_m, \lambda)\big)_{m \in \mathbb{N}}$ converge a $B(\alpha, \lambda)$, para todo $\lambda \in \mathcal{D}[p^{-1/(p-1)}]$.*

Demostración.

1. Dado $t \in \mathbb{C}_p$, aplicando el corolario 7.5.7 y la función evaluación de coeficientes $\mathcal{E}_t$ de series en $\mathbb{Q}[X][[Y]]$ (y sus propiedades como homomorfismo expuestas en el lema 7.4.10) tendremos que

$$\begin{aligned}\mathcal{E}_t(B(f(X),Y^p))\mathcal{E}_t(B(g(X),Y^p)) &= \mathcal{E}_t(B(f(X),Y^p)B(g(X),Y^p)) \\ &= \mathcal{E}_t(B(f(X)+g(X),Y^p)).\end{aligned}$$

En virtud de la proposición 7.4.11 concluimos este ítem.

2. Dado $n \in \mathbb{N}$, tenemos que

$$\left|\binom{a}{n}\right|_p = \left|\frac{a(a-1)\cdots(a-n+1)}{n!}\right|_p \leq \frac{1}{|n!|_p},$$

pues $a, a-1, \ldots, a-n+1 \in \mathfrak{D}_p$. Puesto que $v_p(n!) < n/(p-1)$ (por el lema 5.1.2), tendremos que

$$\sqrt[n]{\left|\binom{a}{n}\right|_p} \leq \sqrt[n]{\frac{1}{|n!|_p}} \leq p^{1/(p-1)}, \text{ para todo } n \in \mathbb{N},$$

luego $\limsup \sqrt[n]{|\binom{a}{n}|_p} \leq p^{1/p-1}$ y concluimos que $\mathcal{R}_{B_a(Y)} \geq p^{\frac{-1}{p-1}}$.

3. Dado $n \in \mathbb{N}$, debemos de verificar que $\binom{a}{n} \in \mathbb{Z}_p$, para este fin tomemos que $(a_m) \subset \mathbb{Z}$ que converja a a. Puesto que $\binom{X}{n}$ es un polinomio, este define una función continua en $\mathbb{Z}_p$, por lo cual $\lim_n \binom{a_m}{n} = \binom{a}{n}$. Como cada $\binom{a_m}{n}$ es un número entero (en particular pertenece a $\mathbb{Z}_p$) y $\mathbb{Z}_p$ es completo, tendremos que $\binom{a}{n} \in \mathbb{Z}_p$.

4. Dado $m, n \geq 1$, tenemos que

$$\left|\binom{a_m}{n}\lambda^n - \binom{\alpha}{n}\lambda^n\right|_p \leq \left|\prod_{i=0}^{n-1}(a_m - i) - \prod_{i=0}^{n-1}(\alpha - i)\right|_p \frac{|\lambda|_p^n}{|n!|_p} \leq \left|\prod_{i=0}^{n-1}(a_m - i) - \prod_{i=0}^{n-1}(\alpha - i)\right|_p p^{-s(n)},$$

donde $s(n)$ es la suma de digitos de la representación en base p de n (por el lema 5.1.2). Sumando y restando términos de la forma $y(y-1)\cdots(y-j)(x-(j+1))\cdots(x-(n+1))$, para luego utilizar la desigualdad no arquimediana, obtendriamos que

$$\begin{aligned}\left|\binom{a_m}{n}\lambda^n - \binom{\alpha}{n}\lambda^n\right|_p \leq\ & \max\{|(a_m-\alpha)(a_m-1)\cdots(a_m-(n-1))|_p, \cdots \\ & , |\alpha(\alpha-1)\cdots(\alpha-(n-2))(a_m-\alpha)|_p\}.\end{aligned}$$

Puesto que cada a_m pertenece a $\mathbb{Z}_p$, conluimos que $|\binom{a_m}{n}\lambda^n - \binom{\alpha}{n}\lambda^n|_p \leq |a_m - \alpha|)p$, para todo $n \geq 1$. Luego, por la proposición 4.4.12 concluimos que $|B(a_m,\lambda) - B(\alpha,\lambda)|_p \leq |a_m - \alpha|_p$, para todo $m \in \mathbb{N}$; con esta desigualdad terminamos esta demostración.

□

Ahora, veremos el mayor aporte de este serie $p-$ádica a nuestro trabajo, la construcción de la siguiente serie. Definimos $F(X,Y) \in \mathbb{Q}[[X,Y]]$ como

$$F(X,Y) = B(X,Y)\prod_{i=1}^{\infty} B\Big(\frac{X^{p^i} - X^{p^{i-1}}}{p^i}, Y^{p^i}\Big),$$

esta serie existe en $\mathbb{Q}[[X,Y]]$. De hecho, dado $i \in \mathbb{N}$ se tiene

$$\begin{aligned}
\omega_{(X,Y)}\Big(B\big(\frac{X^{p^i} - X^{p^{i-1}}}{p^i}, Y^{p^i}\big) - 1\Big) &= \omega_{(X,Y)}\Big(\sum_{n=1}^{\infty}\binom{\frac{X^{p^i}-X^{p^{i-1}}}{p^i}}{n} Y^{np^i}\Big) \\
&\geq \omega_{(X,Y)}\Big(\big(\frac{X^{p^i} - X^{p^{i-1}}}{p^i}\big)Y^{p^i}\Big) \\
&= p^i + p^{i-1},
\end{aligned}$$

de lo cual se deduce que

$$\lim_{i\to\infty}\Big|B\big(\frac{X^{p^i} - X^{p^{i-1}}}{p^i}, Y^{p^i}\big) - 1\Big|_{X,Y} = 0,$$

y la productoria converge en virtud de la propiedad de la proposición 7.3.1. La siguiente propiedad será crucial para encontrar una región de convergencia adecuada a nuestros futuros fines.

Lema 8.5.2 *La serie formal* $F(X,Y) \in \mathbb{Z}_p[[X,Y]]$.

Demostración.- En primer lugar, por el lema 7.2.5 tenemos que

$$\begin{aligned}
F(X^p, Y^p) &= F(X,Y) \circ (X^p, Y^p) \\
&= B(X,Y) \circ (X^p, Y^p)\Big(\prod_{i=1}^{\infty} B\big(\frac{X^{p^i} - X^{p^{i-1}}}{p^i}, Y^{p^i}\big)\Big) \circ (X^p, Y^p) \\
&= B(X^p, Y^p)\prod_{i=1}^{\infty} B\Big(\frac{X^{p^{i+1}} - X^{p^i}}{p^i}, Y^{p^{i+1}}\Big);
\end{aligned}$$

y por el corolario 7.5.7 obtenemos

$$\begin{aligned}
F(X,Y)^p &= B(X,Y)^p\prod_{i=1}^{\infty} B\Big(\frac{X^{p^i} - X^{p^{i-1}}}{p^i}, Y^{p^i}\Big)^p \\
&= B(pX,Y)\prod_{i=1}^{\infty} B\Big(\frac{X^{p^i} - X^{p^{i-1}}}{p^{i-1}}, Y^{p^i}\Big)
\end{aligned}$$

Por lo tanto

$$\frac{F(X^p,Y^p)}{(F(X,Y))^p} = \frac{B(X^p,Y^p)}{B(pX,Y)B(X^p - X, Y^p)} = \frac{B(X^p,Y^p)}{B(pX,Y)B(X^p,Y^p)B(-X,Y^p)} = \frac{B(X,Y^p)}{B(pX,Y)},$$

puesto que $B(-X,Y^p)=B(-X,Y^p)^{-1}$. Nuevamente, por el corolario 7.5.7 tenemos que

$$B(pX,Y)=\exp(pX\log(1+Y))=\exp(X\log((1+Y)^p)),$$

entonces

$$\frac{F(X^p,Y^p)}{(F(X,Y))^p}=\frac{\exp\big(X\log(1+Y^p)\big)}{\exp\big(X\log((1+Y)^p)\big)}=\exp\Big(X\big(\log(1+Y^p)-\log((1+Y)^p)\big)\Big).$$

Si escribimos $(1+Y)^p=1+YT(Y)$ dónde $T(Y)\in\mathbb{Q}[Y]$, entonces existira $\big(1+YT(Y)\big)^{-1}=(1+Y)^{-p}=1+YR(Y)$ con $R(Y)\in\mathbb{Q}[[Y]]$. Luego, tendremos que $-\log\big((1+Y)^p\big)=-\log\big(1+YT(Y)\big)=\log\big(1+YR(Y)\big)$, por lo tanto

$$\frac{F(X^p,Y^p)}{(F(X,Y))^p}=\exp\Big(X\log\big((1+Y^p)(1+YR(Y))\big)\Big).$$

Como $1+Y\in\mathbb{Z}_p[[Y]]$, por el lema 8.4.1 tendremos que la serie formal $(1+Y^p)(1+YR(Y))\in 1+pY\mathbb{Z}_p[[Y]]$; así que la reescribimos como $1+pYG(Y)$ con $G(Y)\in\mathbb{Z}_p[[Y]]$. Luego,

$$\frac{F(X^p,X^p)}{F(X,Y)^p}=\exp\Big(X\log\big(1+pYG(Y)\big)\Big)=B\big(X,pYG(Y)\big),$$

así obtenemos

$$\frac{F(X^p,X^p)}{F(X,Y)^p}=\sum_{n=0}^{\infty}\binom{X}{n}\big(pYG(Y)\big)^n=\sum_{n=0}^{\infty}\frac{p^n}{n!}X(X-1)\cdots(X-n+1)Y^nG(Y)^n.$$

Como $v_p(n!)<n/(p-1)\leq n=v_p(p^n)$ (en virtud del lema 5.1.2), tendremos que $v_p(p^n/n!)>0$, para todo $n\in\mathbb{N}$. Por lo tanto, la anterior serie formal pertenece a $1+pX\mathbb{Z}_p[[X,Y]]+pY\mathbb{Z}_p[[X,Y]]$. □

A continuación encontraremos una region de convergencia para esta serie, primero veamos que tipo de serie es $F(X,Y)$. Dado $i\in\mathbb{N}$, tendremos que

$$\omega_Y\Big(B\big(\frac{X^{p^i}-X^{p^{i-1}}}{p^i},Y^{p^i}\big)-1\Big)\geq\omega_Y\Big(\big(\frac{X^{p^i}-X^{p^{i-1}}}{p^i}\big)Y^{p^i}\Big)=p^i.$$

Por lo tanto, la productoria que define a $F(X,Y)$ en $\mathbb{Q}[[X,Y]]$ también converge respecto al valor absoluto $Y-$ádico a una serie $F_0(X,Y)\in\mathbb{Q}_p[X][[Y]]$, la cual coincidirá con $F(X,Y)$, en virtud del corolario 7.4.6. Escribamos $F(X,Y)=\sum_{n=0}^{\infty}a_n(X)Y^n$, donde $a_n(X)\in\mathbb{Z}_p[[X]]$, para cada $n\in\mathbb{N}_0$. Dado $n\in\mathbb{N}_0$, por las observaciones 7.1.9, existirá $k\in\mathbb{N}$ suficientemente grande tal que $a_n(X)$ y coincide con el coeficiente de Y^n en $B(X,Y)\prod_{i=1}^{k}B(\frac{X^{p^i}-X^{p^{i-1}}}{p^i},Y)$. Esto nos da

$$a_n(X)=\sum_{j_0+pj_1+\cdots+p^kj_k=n}\binom{X}{j_0}\binom{\frac{X^p-X}{p}}{j_1}\cdots\binom{\frac{X^{p^2}-X^p}{p^2}}{j_2}\binom{\frac{X^{p^k}-X^{p^{k-1}}}{p^k}}{j_k},$$

pues los términos Y^j con posibles coeficientes no nulos en $B(\frac{X^{p^i}-X^{p^{i-1}}}{p^i}, Y)$ son aquellos que $p^i \mid j$. No es dificil ver que si grad $f(X) = n \geq 1$, entonces

$$\text{grad} \binom{f(X)}{i} = i\text{grad } f(X), \qquad \text{para todo } i \geq 0 \quad \text{entero.}$$

De ahi que cada sumando de la sumatoria de arriba tiene grado $i_0 + p_1 i_1 + \cdots + p^k i_k$, que es igual a m; por lo tanto $a_m(X)$ es un polinomio de grado a lo más n. Ahora, si para cada $n \in \mathbb{N}_0$ escribimos $a_n(X) = \sum_{m=0}^{\infty} a_{m,n} X^m \in \mathbb{Z}_p[[X]]$, obtendremos que $a_{m,n} = 0$ siempre que $m > n$. Entonces, en virtud de la proposición 7.4.3, tendremos que

$$F(X,Y) = \sum_{n=0}^{\infty} (\sum_{m=0}^{\infty} a_{m,n} X^m) Y^n = \sum_{m=0}^{\infty} (\sum_{n=m}^{\infty} a_{m,n} Y^n) X^m.$$

Las siguientes proposiciones culminan este análisis y nos dan la region de convergencia enunciada lineas arriba.

Proposición 8.5.3 *La serie formal $F(X,Y)$ converge en $\mathcal{D}[1] \times \mathcal{D}(1)$.*

Demostración.- Tomemos $\alpha, \beta \in \mathbb{C}_p$ con $|\alpha|_p \leq 1$ y $|\beta|_p = c < 1$. Dado ϵ, tomemos y $N \in \mathbb{N}$ tal que $c^N < \epsilon$ y $F = \{(m,n)\ ;\ m \leq N, n \leq N\}$. Entonces, si $(m,n) \notin F$ ocurria alguno de los siguientes casos

- Si $m > n$ entonces $a_{m,n} = 0$.
- Si $m \leq n$ entonces $n > N$, pues en caso contrario $(m,n) \in F$. Luego $|a_{m,n}\alpha^m\beta^n|_p \leq r^n < r^N$.

Entonces ambos casos implican que $|a_{m,n}\alpha^m\beta^n|_p < \epsilon$, para todo $(m,n) \notin F$; concluimos que $F(\alpha,\beta)$ existe. □

Proposición 8.5.4 *Si $r > 0$ y $\beta \in \mathbb{C}_p$ con $v_p(\beta) \geq r$, entonces*

1. *Dado $m \in \mathbb{N}_0$, la serie $a_m(\beta) = \sum_{n=m}^{\infty} a_{m,n}\beta^n$ existe.*
2. *Dado $m \in \mathbb{N}_0$, para cada $v_p(a_m(\beta)) > mr$.*
3. *$F(X,\beta) \in \mathbb{Z}_p[[X]]$ es convergente en $\mathcal{D}(p^r)$.*

Demostración.- Fijemos $m \geq 0$; por el lema previo, tenemos que $a_{m,n} \in \mathbb{Z}_p$, para todo $n \geq 0$. En consecuencia, la serie $\sum_{n=m}^{\infty} a_{m,n} Y^n$ converge en $\mathcal{D}(1)$ (por el corolario 8.1.8). Como $|\beta|_p < 1$, tendremos que existe $a_m(\beta) = \sum_{n=m}^{\infty} a_{m,n}\beta^n$. Más aun, como

$$v_p(a_m(\beta)) \geq \min\{v_p(a_{m,m}\beta^m), v_p(\beta^{m+1} \sum_{n>m} a_{m,n}\beta^{n-m-1})\}.$$

Entonces

$$v_p\big(a_m(\beta)\big) \geq \min\{mv_p(\beta)+0,(m+1)v_p(\beta)+0\} = mv_p(\beta) > mr,$$

que no es mas que el segundo ítem. Ahora tomando límite inferior en esta última desigualdad, obtendremos que

$$\liminf \frac{v_p(a_m(\beta))}{m} \geq r.$$

De ahí que el radio de convergencia de $F(X,\beta)$ es mayor o igual a r, y que $\mathcal{D}(p^r)$ es una region de convergencia. □

El siguiente paso será verificar la principal relación que cumple la serie $F(X,Y)$ respecto a los representantes de Teichmüller en $\mathbb{C}_p$.

Lema 8.5.5 *Sea $t \in \mathbb{C}_p$ tal que $t = t^{p^s}$. Entonces*

$$F(t,Y)F(t^p,Y)\cdots F(t^{p^s-1},Y) = B(t+t^p+\cdots+t^{p^s},Y).$$

Demostración.- Puesto que la función evaluación $\mathcal{E}_t : \mathbb{Q}[X][[Y]] \to \mathbb{Q}[X][[Y]]$ definida por $\mathcal{E}_t(\sum p_n(x)Y^n) = \sum p_n(t)Y^n$ es un homomorfismo continuo de anillos, para cada $j \in \mathbb{N}$ ocurrira que

$$\begin{aligned}\mathcal{E}_{t^{p^j}}\big(F(X,Y)\big) &= \mathcal{E}_{t^{p^j}}\big(B(X,Y)\big)\mathcal{E}_{t^{p^j}}\Big(\prod_{i=1}^{\infty} B(X^{p^i}-X^{p^{i-1}}/p, Y^{p^i})\Big)\\ &= \mathcal{E}_{t^{p^j}}\big(B(X,Y)\big)\prod_{i=1}^{\infty}\mathcal{E}_{t^{p^j}}\big(B(X^{p^i}-X^{p^{i-1}}/p, Y^{p^i})\big).\end{aligned}$$

Luego por la proposición 7.4.11 tendremos que

$$F(t^{p^j},Y) = B(t^{p^j},Y)\prod_{i=1}^{\infty} B\Big(\frac{(t^{p^j})^{p^i}-(t^{p^j})^{p^{i-1}}}{p^i}, Y^{p^i}\Big), \qquad \text{para cada} j \in \mathbb{N}.$$

Por lo tanto, el primer miembro de la ecuación del enunciado queda expresado como

$$\prod_{j=0}^{s-1}\left(B(t^{p^j},Y)\prod_{i=1}^{\infty} B\Big(\frac{(t^{p^j})^{p^i}-(t^{p^j})^{p^{i-1}}}{p^i}, Y^{p^i}\Big)\right),$$

entonces aplicando el primer ítem de la proposición 8.5.1, y que el límite respecta el producto obtendremos que

$$F(t,Y)F(t^p,Y)\cdots F(t^{p^s-1},Y) = B\Big(\sum_{j=0}^{s-1} t^{p^j},Y\Big)\prod_{i=1}^{\infty}\left(\prod_{j=0}^{s-1} B\Big(\frac{t^{p^{j+i}}-t^{p^{j+i-1}}}{p^i}, Y^{p^i}\Big)\right).$$

Nuevamente, utilizando el primer ítem de la proposición 8.5.1 tendremos que el factor $i-$ésimo de la productoria de arriba es

$$B\Big(\sum_{j=0}^{s-1}((t^{p^{i+j}}-t^{p^{i+j-1}})/p^i), Y^{p^i}\Big) = B\Big(((t^{p^s})^{p^{i-1}}-t^{p^{i-1}})/p^i, Y^{p^i}\Big) = B(0,Y^{p^i}) = 1.$$

Por lo tanto, se cumple la igualdad formal enunciada. □

8.6. Operadores lineales en $\mathbb{C}_p[[X]]$

En esta sección extenderemos las nociones de Traza y Determinante que se tienen para operadores lineales en espacios de dimensión finita hacia el $\mathbb{C}_p$–espacio vectorial $\mathbb{C}_p[[X_1,\ldots,X_n]]$, que simplemente denotaremos por $\mathbb{C}_p[[X]]$. Este espacio vectorial, como sabemos, es infinito dimensional, lo cual nos restringe la posibilidad de establecer estas definiciones de modo habitual. Sin embargo, como este $\mathbb{C}_p$–espacio vectorial posee una base de Schauder (por la proposición 7.1.10),podremos extender estas nociones a cierta familia de operadores lineales, la cual sera muy importante para el desarrollo del siguiente capítulo.

Definición 8.6.1 Sean $q \in \mathbb{N}$ y $G(X) \in \mathbb{C}_p[[X]]$ definimos

1. La función $\widetilde{G} : \mathbb{C}_p \to \mathbb{C}_p$ por $\widetilde{G}(f(X)) = G(X) \cdot f(X)$.
2. La serie formal $G_q(X) = G(X^q)$.
3. La función $T_q : \mathbb{C}_p[[X]] \to \mathbb{C}_p[[X]]$ por $T_q(\sum a_u X^u) = \sum a_{qu} X^u$.
4. La función $\Psi_{q,G(X)} = T_q \circ \widetilde{G}$.

Observaciones 8.6.2 Durante esta sección utilizaremos algunas otras notaciones.

- Salvo mencionemos otro orden en particular (como el lexicografico), dados $u = (u_1,\ldots,u_n)$, $v = (v_1,\ldots,v_n) \in \mathfrak{N}$, diremos que u es *menor que* (respectivamente *mayor que*) v, que denotaremos por $u \leq v$ (respectivamente $u \geq v$), cuando $u_i \leq v_i$ (respectivamente $u_i \geq v_i$), para $i = 1, 2, \ldots, n$. Nótese que esta es una relación de orden parcial, pero no es un orden total.
- Dado $r \geq 0$, el conjunto de los multiindices de peso menor o igual a r sera denotado por $\mathfrak{N}_r$.
- La familia de subconjuntos de X con m elementos sera denotado por $\mathscr{P}_m(X)$.
- El conjunto de permutaciones de Y es denotado por $\mathcal{S}(Y)$.
- Dado $U \subset \mathfrak{N}$ finito, $|U|$ denotará a $\sum_{u\in U} |u|$.

Ejemplos 8.6.3

1. Si $n = 1$ y $q = 2$ entonces
$$T_q\Big(\sum_k \frac{1}{k} X^k\Big) = \sum_k \frac{1}{2k} X^k.$$

2. Dado $u \in \mathfrak{N}$ y $G(X) = \sum b_v X^v \in \mathbb{C}_p[[X]]$ tendremos que

$$\Psi_{q,G(X)}(X^u) = \sum_{qw \geq u} b_{qw-u} X^w.$$

De hecho

$$\Psi_{q,G(X)}(X^u) = T_q(\sum_v b_v X^{v+u}) = T_q(\sum_{v \geq u} b_{v-u} X^v) = \sum_{qw \geq u} b_{qw-u} X^w.$$

Enunciemos las propiedades básicas que cumplen estos operadores.

Proposición 8.6.4 *Dado $q \in \mathfrak{N}$ y $G(X) \in \mathbb{C}_p[[X]]$, tenemos que $\widetilde{G}, T_q, \Psi_{q,G(X)}$ son operadores $\mathbb{C}_p-$lineales que son continuos respecto a la métrica inducida por $|\cdot|_X$. Además satisfacen la relación*

$$\widetilde{G} \circ T_q = T_q \circ \widetilde{G_q} = \Psi_{q,G_q(X)}.$$

Demostración.- Es claro que $\widetilde{G}$ y T_q son $\mathbb{C}_p-$operadores lineales sobre $\mathbb{C}_p[[X]]$, y por lo tanto $\Psi_{q,G(X)}$ es $\mathbb{C}_p$-lineal. Es claro que $\widetilde{G}$ será continua, puesto que el producto fijando un factor define una función continua respecto a un valor absoluto dado (ver la proposición 4.3.5). Ahora verificaremos que T_q es continua, para esto demostraremos cierta desigualdad. Dado $f(X) = \sum a_u X^u \in \mathbb{C}_p[[X]]$, tenemos que

$$\begin{aligned} \omega_X(T_q(f(X))) &= \text{mín}\{|u| \ , \ a_{qu} \neq 0 \ , u \in \mathfrak{N}\} \\ &= 1/q \, \text{mín}\{|qu| \ , \ a_{qu} \neq 0 \ , u \in \mathfrak{N}\} \ \geq \ (1/q)\omega_X(f(X)). \end{aligned}$$

Entonces, dado $f_1(X), f_2(X) \in \mathbb{C}_p[[X]]$, se cumple que

$$|T_q(f_1(X)) - T_q(f_2(X))|_X = |T_q(f_1(X) - f_2(X))|_X \leq |f_1(X) - f_2(X)|_X^{1/q};$$

por esta desigualdad concluimos la continuidad de T_q respecto a $|\cdot|_X$; en consecuencia, $\Psi_{q,G(X)}$ también es continua. Ahora, si bien utilizando la linealidad y continuidad de estos operadores podemos demostrar la relación enunciada tan sólo verificandola en la base $\{X^u \ , u \in \mathfrak{N}\}$ de $\mathbb{C}_p[[X]]$ (para luego utilizar la densidad de $\mathbb{C}_p[X]$ en $\mathbb{C}_p[[X]]$); optaremos por ejemplizar la mecanica de los calculos mostrando esta relación de forma directa. Escribamos $G(X) = \sum b_v X^v$, entonces para cada $f(X) = \sum a_u X^u \in \mathbb{C}_p[[X]]$, se tiene

$$\widetilde{G} \circ T_q(f(X)) = \widetilde{G}(\sum_u a_{qu} X^u) = \sum_w (\sum_{u+v=w} a_{qu} b_v) X^w.$$

Por otra parte

$$T_q \circ \widetilde{G_q}(f(X)) = T_q(\sum_w (\sum_{u+qv=w} a_u b_v) X^w) = \sum_w (\sum_{u+qv=qw} a_u b_v) X^w;$$

el que hecho que $u + qv = qw$ implica que $q \mid u$ (pues esto es lo que ocurre componente a componente), luego u es de la forma qu' para algún $u' \in \mathfrak{N}$. Por lo tanto

$$T_q \circ \widetilde{G_q}(f(X)) = \sum_w \Big(\sum_{qu'+qv=qw} a_{qu'} b_v \Big) X^w = \sum_w \Big(\sum_{u'+v=w} a_{qu'} b_v \Big) X^w = \widetilde{G} \circ T_q\big(f(X)\big),$$

para cualquier $f(X) \in \mathbb{C}_p[[X]]$.

Corolario 8.6.5 *Dado $q, s \in \mathbb{N}$ y $G(X) \in \mathbb{C}_p[[X]]$ tenemos que*

$$\Psi^s_{q,G(X)} = \Psi_{q^s, G(X)G_q(X)\cdots G_{q^{s-1}}(X)}.$$

Demostración.- Verifiquemos esta ecuación por inducción sobre s. Vemos que es cierta en el caso $s = 1$, asumiendo que cierta para algún $s \in \mathbb{N}$, verifiquemosla para $s + 1$. Tenemos que

$$\Psi^{s+1}_{q,G(X)} = \Psi_{q,G(X)} \circ \Psi^s_{q,G(X)} = \Psi_{q,G(X)} \circ \Psi_{q^s, G(X)G_q(X)\cdots G_{q^{s-1}}(X)};$$

luego, escribiendo $H(X) = G(X)G_q(X)\cdots G_{q^s}(X)$, tendremos

$$\Psi^{s+1}_{q,G(X)} = T_q \circ \widetilde{G} \circ T_{q^s} \circ \widetilde{H}(X) = T_q \circ T_{q^s} \circ \widetilde{G_{q^s}} \circ \widetilde{H}(X) = T_{q^{s+1}} \circ \widetilde{G_{q^s}} \circ \widetilde{H}(X).$$

Por lo tanto $\Psi^{s+1}_{q,G(X)} = \Psi_{q^s, G_{q^{s+1}}G(X)G_q(X)\cdots G_{q^s}(X)}$, y queda demostrado el corolario.

Observación 8.6.6 Puesto que $|\cdot|_X$ no es norma para $\mathbb{C}_p[[X]]$ como $\mathbb{C}_p$-espacio vectorial, ocurre que los operadores del tipo T_q no son continuos en el sentido comun. Más aun la última desigualdad utilizada en la demostración nos muestra que no es necesariamente una función Lipschitz como sí lo son los operadores continuos respecto a una norma.

Las principales propiedades de los operadores del tipo $\Psi_{q,G(X)}$ se estableceran cuando $G(X)$ pertenezca al siguiente conjunto por definir.

Definición 8.6.7 En el anillo $\mathbb{C}_p[[X_1, \ldots, X_n]]$, definimos el conjunto

$$\mathfrak{R}^n_p = \{ \sum_u a_u X^u \; ; \; \exists\, c > 0 \,,\; v_p(a_u) \geq c|u| \,, \forall\, u \in \mathfrak{N} \}.$$

Un ejemplo de este tipo de serie formal se vio en la proposición 8.5.4. Mostremos algunas cualidades propias de este conjunto.

Proposición 8.6.8

- *Sean $u \in \mathfrak{N}$ no nulo y $\alpha \in \mathfrak{D}_p$. Si $f(T)$ pertenece a $\mathfrak{R}^1_p$, entonces $f(\alpha X^u)$ pertenece $\mathfrak{R}^n_p$.*
- *El conjunto $\mathfrak{R}^n_p$ es cerrado bajo el producto de $\mathbb{C}_p[[X_1, \ldots, X_n]]$.*

- *Si* $G(X) \in \mathfrak{R}_p^n$ *entonces también* $G_q(X)$.
- *Si* $G(X) \in \mathfrak{R}_p^n$ *entonces* $G(X)$ *converge en* $\mathfrak{D}_p^n$.

Demostración.-

- Supongamos que $f(T) = \sum_n a_n T^n \in \mathbb{C}_p[[T]]$ y que exista $c > 0$ que cumpla $v_p(a_n) \geq cn$, para todo $n \geq 0$. Entonces

$$f(\alpha X^u) = \sum_{n=0}^{\infty} a_n (\alpha X^u)^n = \sum_{v \in \mathfrak{N}} b_v X^v,$$

donde b_v es $a_n \alpha^n$, cuando v es de la forma nu (con $n \geq 0$ entero); y 0, en otro caso. Luego, tomando $d = c/|u|$ tendremos que

$$v_p(\beta_v) = n v_p(\alpha) + v_p(a_n) \geq nc + 0 = d|v|,$$

en caso $v = nu$ con $n \geq 0$; esta desigualdad será trivialmente cierto en el otro caso. Por lo tanto, $f(\alpha X^u) \in \mathfrak{R}_p^n$.

- Sean $f(X) = \sum a_u X^u, g(X) = \sum b_v X^v \in \mathbb{C}_p[[X]]$ y $c, d > 0$ tales que

$$v_p(a_u) \geq c|u| \quad \text{y} \quad v_p(b_v) \geq d|v|\,, \qquad \text{para todo } u, v \in \mathfrak{N}.$$

Tomando $h(X) = f(X)g(X) = \sum c_w X^w$, tendremos que para cada $w \in \mathfrak{N}$ se cumple que

$$v_p(c_w) \geq \min_{u+v=w} \{v_p(a_u b_v)\} \geq \min_{u+v=w} \{c|u|+d|v|\} \geq \min_{u+v=w} \big\{\min\{c,d\}(|u|+|v|)\big\} = \min\{c,d\}|w|.$$

- Si $G(X) = \sum_u a_u X^u \in \mathbb{R}_p^n$, entonces $G_q(X) = \sum_v b_v X^v$ con $b_v = a_{v/q}$ cuando $q \mid v$, y 0 cuando no. Luego, si $c > 0$ es tal que $v_p(a_u) \geq c|u|$ para todo $u \in \mathfrak{N}$, entonces tomando $d = c/q > 0$ tendremos que $b_v \geq d|v|$, para todo $v \in \mathfrak{N}$.
- Sean $G(X) = \sum a_u X^u \in \mathfrak{R}_p^n$ con $c > 0$ tal que $|a_u|_p \geq p^{-c|u|}$, para todo $u \in \mathfrak{N}$. Dado $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathfrak{D}_p^n$ y $\epsilon > 0$, basta tomar $r > 0$ tal que $p^{-cr} < \epsilon$ y $F_0 = \mathfrak{N}_r$ para obtener que todo $u = (u_1, \ldots, u_n) \notin F_0$ cumple que

$$|a_u \alpha^u|_p = |a_u \alpha_1^{u_1} \cdots \alpha_n^{u_n}|_p \leq |a_u| \leq p^{-c|u|} < \epsilon;$$

por lo cual concluimos que existe $G(\alpha) \in \mathbb{C}_p$.

□

Observación 8.6.9 Por resto de la sección obviaremos el superindice n de la notación $\mathfrak{R}_p^n$, pues tan sólo trabajaremos con series de n variables.

Procederemos a establecer una versión de representación n matricial en $\mathbb{C}_p[[X]]$ que se tiene en espacios de dimensión finita, partiendo del hecho que $\{X^u\ ,\ u \in \mathfrak{N}\}$ es una base de Schauder sobre $\mathbb{C}_p[[X]]$; así también estableceremos la noción de Traza para operadores lineales en $\mathbb{C}_p[[X]]$.

Definición 8.6.10 Sea L un operador lineal en $\mathbb{C}_p[[X]]$.

- Si se tiene
$$L(X^u) = \sum_{v\in\mathfrak{N}} a_{u,v}X^v\ , \quad \text{para cada } u \in \mathfrak{N};$$
entonces denominaremos a $\{a_{u,v}\}_{u,v\in\mathfrak{N}}$, por *la representación (canonica) matricial* de L en $\mathbb{C}_p[[X]]$, lo cual denotaremos por $[[a_{u,v}]]_{u,v}$.
- Definimos *la Traza de* L, si existe, como la serie
$$\mathrm{TR}(L) = \sum_{u\in\mathfrak{N}} a_{u,u} \in \mathbb{C}_p.$$

El siguiente lema ejemplizara este concepto y la importancia de la de los operadores del tipo $\Psi_{q,G(X)}$.

Lema 8.6.11 *Sean $q, s \in \mathbb{N}$ con $q \geq 2$ y $G(X) \in \mathfrak{R}_p$. Si $\Psi = \Psi_{q,G(X)}$ entonces existe $\mathrm{TR}(\Psi^s)$, más aun se cumple*
$$(q^s-1)^n \mathrm{TR}(\Psi^s) = \sum_{w\in(\mathcal{U}_p^{q^s-1})^n} G(w)G(w^q)\cdots G(w^{q^{s-1}}),$$
donde $\mathcal{U}_p^{q^s-1}$ denota al conjunto de raíces q^s-1-esimas de la unidad en $\mathbb{C}_p$.

Demostración.- Empecemos por comprobar el lema para el caso $s = 1$. Por lo mencionado en los ejemplos 8.6.3, si $G(X) = \sum b_v X^v$ entonces la representación matricial $[[a_{u,v}]]_{u,v}$ de Ψ es dada por $a_{u,v} = b_{qv-u}$, para cada $u, v \in \mathfrak{N}$. Entonces
$$\mathrm{TR}(\Psi) = \sum_{u\in\mathfrak{N}} a_{u,u} = \sum_{u\in\mathfrak{N}} b_{(q-1)u}$$
existe en $\mathbb{C}_p$, en virtud del cuarto ítem de la última proposición y del segítem ítem de la proposición 4.4.12 aplicados a $G(1)$ y el subconjunto de multiindices $\{(q-1)u\ ;\ u \in \mathfrak{N}\}$, respectivamente. Dado $m \in \mathbb{N}$, por el lema 3.12.3 se tiene que
$$\sum_{w\in\mathcal{U}_p^{q-1}} w^m = \begin{cases} q-1 & ;\ \text{si } q-1 \mid m \\ 0 & ;\ \text{si } q-1 \nmid m \end{cases},$$

para todo $m \in \mathbb{N}$. De lo cual, en la notación de series de potencias en varias variables, para cada $u = (u_1, \ldots, u_n) \in \mathfrak{N}$, deducimos que

$$\sum_{w \in (\mathfrak{U}_p^{q-1})^n} w^u = \sum_{w \in (\mathfrak{U}_p^{q-1})^n} w_1^{u_1} \cdots w_n^{u_n} = \prod_{i=1}^{n} \Big(\sum_{w_i \in \mathfrak{U}_p^{q-1}} w_i^{u_i} \Big) = \begin{cases} (q-1)^n & ; \text{ si } q-1 \mid u \\ 0 & ; \text{ si } q-1 \nmid u \end{cases}$$

Luego, como $G(w)$ existe para todo $w \in (\mathfrak{U}_p^{q-1})^n$, podemos utilizar el lema 4.4.14 y obtener que

$$\sum_{w \in (\mathfrak{U}_p^{q-1})^n} G(w) = \sum_{w \in (\mathfrak{U}_p^{q-1})^n} \Big(\sum_{u \in \mathfrak{N}} b_u w^u \Big) = \sum_{w \in (\mathfrak{U}_p^{q-1})^n} \Big(\lim_{d \to \infty} \sum_{|u| \le d} b_u w^u \Big) = \lim_{d \to \infty} \sum_{|u| \le d} \Big(\sum_{w \in (\mathfrak{U}_p^{q-1})^n} b_u w^u \Big).$$

Puesto que

$$\sum_{|u| \le d} \Big(\sum_{w \in (\mathfrak{U}_p^{q-1})^n} b_u w^u \Big) = \sum_{\substack{|u| \le d \\ (q-1) \mid u}} (b_u (q-1)^n) = \sum_{|u'| \le d/q} (q-1)^n b_{(q-1)u'},$$

nuevamente, por el lema 4.4.14 concluimos que

$$\sum_{w \in (\mathfrak{U}_p^{q-1})^n} G(w) = \lim_{d \to \infty} \sum_{|u'| \le d/q} (q-1)^n b_{(q-1)u'} = \sum_{u' \in \mathfrak{N}} b_{(q-1)u'} (q-1)^n;$$

queda así demostrado el lema para el caso $s = 1$. En el caso general, basta renombrar q y $G(X)$, por q^s y $G(X)G_q(X) \cdots G_{q^s}(X)$ (respectivamente), y utilizar el corolario 8.6.5 en el caso que acabamos de demostrar. Nótese que esto es posible porque $\mathfrak{N}_p^n$ es cerrado bajo el producto y la operación $G(X) \to G_q(X)$, como mencionamos en la proposición 8.6.8. □

En lo siguiente desarrollaremos una versión del polinomio conjugado característico de una $K-$operador lineal en el $\mathbb{C}_p$-espacio infinito dimensional $\mathbb{C}_p[[X]]$, el cual estaba asociado a una representación matricial A de un $K-$operador lineal sobre un espacio de dimensión finita. Utilizaremos la representación matricial canonica del operador en cuestión mediante calculos sucesivos en algunas de sus submatrices finitas.

Sea L un $\mathbb{C}_p$-operador lineal de $\mathbb{C}_p[[X]]$ y $A = [[a_{u,v}]]$ su representación matricial canonica. Dado $r \in \mathbb{N}$, tomemos $s(r) = \#\mathfrak{N}_r$ y $A_r = [a_{u,v}]_{|u|,|v| \le r} \in \mathbb{C}_p^{s(r) \times s(r)}$ la matriz formada con las respectivas entradas de A de multiindices de peso a lo mas r, aquí los multiindices u y v ordenan las entradas dentro de la matriz A_r en cierta forma (más adelante veremos que esta elección sera no sera trascedental). Entonces el polinomio característico conjugado de A_r sería

$$\det(I - A_r T) = \sum_{m=0}^{s(r)} \beta_m^r T^m \in 1 + X\mathbb{C}_p[X],$$

donde

$$\beta_0^r 1 \quad \text{y} \quad = \beta_m^r = (-1)^m \sum_{U \subset \mathscr{P}_m(\mathfrak{N}_r)} \sum_{\sigma \in \mathcal{S}(U)} (-1)^{\mathrm{sig}(\sigma)} \prod_{u \in U} a_{u,\sigma(u)}, \qquad \text{para todo } m \ge 1.$$

La intención de extender este objeto para el operador L sobre todo $\mathbb{C}_p[[X]]$ nos induce a evaluar la sumatoria sobre todo $\mathscr{P}_m(\mathfrak{N})$. Esto nos producira una suma infinita, pero como los índices de sus sumandos son numerables (pues $\{(U,\sigma)\ ;\ U \in \mathscr{P}_m(\mathfrak{N})\ ,\ \sigma \in \mathcal{S}(U)\}$ admite una aplicación inyectiva hacia $\mathfrak{N}^{r+1}$), será posible considerar este objeto resultante dentro de nuestras nociones de serie, y establecer si existe o no en $\mathbb{C}_p$.

Definición 8.6.12 Sea L un $\mathbb{C}_p$-operador lineal de $\mathbb{C}_p[[X]]$ y $A = [[a_{u,v}]]$ su representación matricial canonica. Definimos la *serie característica conjugada*

$$\det(I - AT) = \sum_{m=0}^{\infty} \beta_m T^m \in \mathbb{C}_p[[T]],$$

por

$$\beta_0 = 1 \qquad \text{y} \qquad \beta_m = (-1)^m \sum_{(U,\sigma)} (-1)^{\mathrm{sig}(\sigma)} \prod_{u \in U} a_{u,\sigma(u)}, \qquad \text{para todo } m \geq 1$$

donde (U,σ) recorre todo subconjunto $U \in \mathscr{P}_m(\mathfrak{N})$ y toda permutación $\sigma \in \mathcal{S}(U)$, siempre que existe cada coeficiente β_m.

Observación 8.6.13 Con las notaciones del análisis previo a esta definición, tenemos que

$$\beta_m = \lim_{r \to \infty} \beta_m^r, \qquad \text{para todo } m \geq 0.$$

En efecto, esto sería una aplicación directa del lema 4.4.14 a la familia $\{(U,\sigma)\ ,\ U \in \mathscr{P}_m(\mathfrak{N}_r)\ ,\ \sigma \in \mathcal{S}(U)\}_{r \geq 1}$.

Lema 8.6.14 *Sean $q \geq 2$, $G(X) \in \mathfrak{R}_p[[X]]$ y $A = [[a_{u,v}]]$ la representación canonica de $\Psi_{q,G(X)}$. Entonces existe* $\det(I - AT)$ *en $\mathbb{C}_p[[T]]$, más aun converge en $\mathbb{C}_p$.*

Demostración.- Si $G(X) = \sum b_u X^u$, tendremos que $a_{u,v} = b_{qv-u}$ para todo $u, v \in \mathfrak{N}$ (asumiendo $b_{qv-u} = 0$, cuando no ocurre $qv \geq u$). Sea $c > 0$ de modo que indica que $G(X) \in \mathfrak{R}_p$ y fijemos $m \geq 1$ entero. Dado (U,σ) con $U \in \mathscr{P}_m(\mathfrak{N}_r)$ y $\sigma \in \mathcal{S}(U)$ tendremos que

$$v_p(\prod_{u \in U} a_{u,\sigma(u)}) = \sum_{u \in U} v_p(b_{q\sigma(u)-u}) \geq c \sum_{u \in U} |q\sigma(u) - u|,$$

nótese que esta desigualdad se verifica aun en el caso que $q\sigma(u)$ no sea mayor o igual a u (pues en ese caso $a_{u,\sigma(u)}$ es nulo). Puesto que el peso es una restricción de la norma suma en $\mathbb{R}^n$, obtenemos que

$$v_p(\prod_{u \in U} a_{u,\sigma(u)}) \geq c(\sum_{u \in U} |q\sigma(u)| - \sum_{u \in U} |u|) = c(q \sum_{u \in U} |\sigma(u)| - \sum_{u \in U} |u|) = c(q-1)|U| \qquad (8.10)$$

Ahora, dado $\epsilon > 0$ tomemos $r_0 \in \mathbb{N}$ tal que $p^{-c(q-1)r_0} < \epsilon$ y

$$\mathcal{F}_m^{r_0} = \{(U, \sigma)\ ,\ U \in \mathscr{P}_m(\mathfrak{N})\ ,\ |U| \leq r_0\ ,\ \sigma \in \mathcal{S}(U)\};$$

nótese que este último conjunto es finito desde todo $(U, \sigma) \in \mathcal{F}_m^{r_0}$ cumple que $U \subset \mathfrak{N}_{r_0}$. Como todo (U, σ) no que pertenezca a $\mathcal{F}_m^{r_0}$ satisface que

$$|\prod_{u \in U} a_{u,\sigma(u)}|_p \leq p^{-c(q-1)|U|} < p^{-c(q-1)r_0} < \epsilon,$$

por la proposición 4.4.11 concluimos que existe $\beta_m \in \mathbb{C}_p$.

Ahora mostremos que $\sum_m \beta_m T^m$ posee radio de convergencia infinito, para esto buscaremos obtener que $v_p(\beta_m)/m$ tiende a $+\infty$ (lo cual es suficiente en virtud del lema 8.1.7). Por la desigualdad 8.10 y el primer ítem de la proposición 4.4.12 deducimos que

$$v_p(\beta_m) \geq \min\{c(q-1)|U|, U \in \mathscr{P}_m(\mathfrak{N}), \sigma \in U\} = q(c-1)\min\{|U|, U \in \mathscr{P}_m(\mathfrak{N})\}.$$

Entonces, encontrando una sucesión $(\chi_m)_{m \in \mathbb{N}} \subset \mathbb{R}$ tal que

$$\min\{|U|, U \in \mathscr{P}_m(\mathfrak{N})\} \geq \chi_m \qquad \text{y} \qquad \lim_{m \to \infty} \chi_m/m = +\infty,$$

concluiremos la prueba de este lema.

Definamos $\mathcal{A}_i = \{u \in \mathfrak{N}\ ,\ |u| = i\}$ y $\alpha_i = \#\mathcal{A}_i$, para cada $i \geq 0$ entero. Entonces, dado $U \in \mathscr{P}_m(\mathfrak{N})$ se tiene que

$$|U| = \sum_{u \in U} |u| = \sum_{i=0}^{\infty} \sum_{u \in U \cap \mathcal{A}_i} |u| = \sum_{i=1}^{\infty} i\#(U \cap \mathcal{A}_i),$$

donde este serie es, en realidad, finita y cierta (pues $\mathfrak{N} = \cup_{i=0}^{\infty} \mathcal{A}_i$). Esto nos ayuda a encontrar una cota inferior para $|U|$ sujeto a $U \in \mathscr{P}_m(\mathfrak{N})$, pues, intuitivamente, el menor valor posible seria cuando U posea mayor cantidad posible de sus elementos en los subconjuntos $\mathcal{A}_i$ donde i sea el menor posible; de hecho, esto es cierto. Dado $m \in \mathbb{N}$, definamos $r(m)$ y $s(m)$ por la ecuación

$$m = \sum_{i=0}^{s(m)} \alpha_i + r(m)\ ,\quad \text{sujeta a } 0 \leq r(m) < \alpha_{s(m)+1};$$

esto significa que $s(m)$ es el mayor entero no negativo s tal que $m \geq \sum_{i=0}^{s} \alpha_i$, y que $r(m)$ es el " resto"; nótese que todo esto es posible porque cada $\mathcal{A}_i$ es no vacío. Para cada $m \geq 1$ entero, definimos

$$\chi_m = \sum_{i=0}^{s(m)} i\alpha_i + (s(m)+1)r(m) \in \mathbb{R};$$

planteamos la siguiente

Afirmación : *Para cada* $m \in \mathbb{N}$: $\quad \min\{|U| \, ; \, U \in \mathscr{P}_m(\mathfrak{N})\} \geq \chi_m$.

En efecto, fijemos $U \in \mathscr{P}_m(\mathfrak{N})$. Dado $i \geq 0$, denotando $\mu_i = \#(U \cap \mathcal{A}_i)$ tendremos que $\mu_i \leq \alpha_i$. Como $m = \#U = \sum_{i \geq 0} \mu_i$ tendremos que

$$\sum_{i=s(m)+1}^{\infty} \mu_i = m - \sum_{i=0}^{s(m)} \mu_i = \sum_{i=0}^{s(m)} \alpha_i + r(m) - \sum_{i=0}^{s(m)} \mu_i = \sum_{i=0}^{s(m)} (\alpha_i - \mu_i) + r(m),$$

por esta igualdad y la finitud de μ_i no nulos

$$\begin{aligned} \sum_{i=s(m)+1}^{\infty} i\mu_i &\geq \sum_{i=s(m)+1}^{\infty} (s(m)+1)\mu_i \\ &= \sum_{i=0}^{s(m)} (s(m)+1)(\alpha_i - \mu_i) + r(m)(s(m)+1) \\ &\geq \sum_{i=0}^{s(m)} i(\alpha_i - \mu_i) + r(m)(s(m)+1); \end{aligned}$$

por lo tanto

$$|U| = \sum_{i=0}^{\infty} i\mu_i \geq \sum_{i=0}^{\infty} i\alpha_i + r(m)(s(m)+1) = \chi_m.$$

Finalmente demostremos que $\lim_m \chi_m/m = +\infty$: Dado $M \in \mathbb{N}$, encontremos algún $m_0 \in \mathbb{N}$ tal que $\chi_m/m \geq M$, para todo $m \geq m_0$. Reemplazando la definición de χ_m y la descomposición de m en α_i, $s(m)$ y $r(m)$ obtenemos que nuestro objetivo equivale a que

$$\sum_{i=0}^{s(m)} (i - M)\alpha_i + (s(m) + 1 - M)r(m) \geq 0$$

sea cierto para cada $m \geq m_0$. Note que

- Para todo $i \geq 0$, se tiene que $\alpha_{i+1} \geq \alpha_i$. En efecto, $(u_1, u_2, \ldots, u_n) \in \mathcal{A}_i$, el multiindice $(u_1 + 1, u_2, \ldots, u_n) \in \mathcal{A}_{i+1}$, así $\mathcal{A}_{i+1}$ contiene una cantidad de elementos de por lo menos α_i.

- Si $m_1 \geq m_2$ entonces $s(m_1) \geq s(m_2)$. De hecho, esto cierto porque

$$\sum_{i=0}^{s(m_2)} \alpha_i \leq m_1 \quad \text{y} \quad s(m_1) = \max\{s \geq 0 \, ; \, \sum_{i=0}^{s} \alpha_i \leq m_1\}.$$

Con esto presente, para cada $M \geq 0$ entero, tomamos

$$N = M + \sum_{i=0}^{M} (M - i)\alpha_i \quad \text{y} \quad m_0 = \alpha_0 + \alpha_1 + \cdots \alpha_N.$$

Entonces, todo $m \geq m_0$ cumple que $s(m) \geq s(m_0) = N \geq M$, y en consecuencia

$$\begin{aligned}\sum_{i=0}^{s(m)}(i-M)\alpha_i + \big(s(m)+1-M\big)r(m) &\geq \sum_{i=M+1}^{s(m)}(i-M)\alpha_i - \sum_{i=0}^{M}(M-i)\alpha_i \\ &\geq \Big(\big(s(m)-(M+1)\big)+1\Big)\cdot 1 - \sum_{i=0}^{M}(M-i)\alpha_i \\ &= s(m)-N \geq 0.\end{aligned}$$

□

Observaciones 8.6.15

- Es conocido el valor de cada α_i. De hecho, en un primer curso de calculo de probabilidad se demuestra que es igual a $\binom{i+n-1}{i}$ (vea por ejemplo [8, páginas 48,49 y 50]).
- Cabe decir que en realidad χ_m es el minimo que acota segun la anterior definición, pues llega a ser el cardinal de un subconjunto U_m que es exactamente la unión de $\mathcal{A}_0, \ldots, \mathcal{A}_{s(m)}$ y de un subconjunto de $\mathcal{A}_{s(m)+1}$ de cardinal $r(m)$.

La extensión del siguiente lema en el ambito infinito dimensional de $\mathbb{C}_p[[X]]$ es el resultado más importante de esta sección, y uno de los mas trascendentes en esta monografía.

Lema 8.6.16 *Sea $A = [a_{i,j}] \in \mathbb{C}_p^{n\times n}$, entonces*

$$\det(I - AT) = \exp\Big(-\sum_{s=1}^{\infty} \mathrm{TR}(A^s)\frac{T^s}{s}\Big).$$

Demostración.- Supongamos que la matriz A es triangular superior. Entonces $I - AT \in \mathbb{C}_p[T]^{n\times n}$ también será triangular superior, por lo tanto $\det(I - AT)$ es el producto de los elementos de su diagonal, que es $\prod_{i=1}^{n}(1 - a_{i,i}T)$. Por otro lado, si para cada $s \in \mathbb{N}$ denotamos $A^s = [a_{i,j}^{(s)}]$ tendremos que $a_{i,i}^{(s)} = a_{i,i}^s$, para $i = 1, 2, \ldots, n$. Luego,

$$\exp\Big(-\sum_{s=1}^{\infty}\mathrm{TR}(A^s)T^s/s\Big) = \exp\Big(-\sum_{s=1}^{\infty}\sum_{i=1}^{n}a_{i,i}^s T^s/s\Big) = \prod_{i=1}^{n}\exp\Big(-\sum_{s=1}^{\infty}a_{i,i}^s T^s/s\Big),$$

a lo que aplicando las propiedades del log y exp nos da

$$\exp\Big(-\sum_{s=1}^{\infty}\mathrm{Tr}(A^s)T^s/s\Big) = \prod_{i=1}^{n}\exp\Big(\log\big(1+(-a_{i,i})T\big)\Big) = \prod_{i=1}^{n}(1 - a_{i,i}T);$$

de esta forma queda demostrado el caso de las matrices triangulares superiores. En el caso general, como $\mathbb{C}_p$ es algebraicamente cerrado, por el teorema 3.10.9 existe $C \in \mathbb{C}_p^{n\times n}$ inversible tal que $C^{-1}AC$ es triangular superior. Observando que

$$\det(I - AT) = \det(C^{-1})\det(I - AT)\det(C) = \det\big(C^{-1}(I - AT)C\big) = \det\big(I - (C^{-1}AC)T\big)$$

y

$$\exp\Big(-\sum_{s=1}^{\infty}\mathrm{Tr}\big((C^{-1}AC)^s\big)T^s/s\Big)=\exp\big(-\sum_{s=1}^{\infty}\mathrm{Tr}(A^s)T^s/s\big),$$

concluimos que el lema. □

Observación 8.6.17 Veamos una equivalencia de la ecuación de este lema. Dado $m \geq 0$ entero, sea $\pi_m : K[[T]] \to K$ la proyección en el $m-$ésimo coeficiente. Entonces, la ecuación mencionada equivale a

$$\beta_m = \pi_m\big(\det(I-AT)\big) = \pi_m\Big(\exp\big(-\sum_{s=1}^{\infty}\mathrm{Tr}(A^s)\frac{T^s}{s}\big)\Big),$$

para todo $m \geq 0$. Puesto que ambas series formales tienen coeficientes independientes iguales a 1, gracias al lema 7.5.4 esto equivale a

$$\beta_m = (-1)^m\sum_{k=1}^{m}\sum_{i_1+\cdots+i_k=m}\frac{1}{k!}\frac{\mathrm{Tr}(A^{i_1})\cdots\mathrm{Tr}(A^{i_k})}{i_1\cdots i_k}. \qquad \text{para cada } m \geq 1.$$

Recuerde que en este caso finito dimensional, β_m será nulo cuando $m > k$.

Teorema 8.6.18 *Sean $q \geq 2$, $G(X) \in \mathfrak{R}_p$, $\Psi = \Psi_{q,G(X)}$ y $A = [a_{u,v}]$ la representación canonica de Ψ en $\mathbb{C}_p[[X]]$. Entonces*

$$\det(I-AT) = \exp\big(-\sum_{s=1}^{\infty}\mathrm{Tr}(\Psi^s)\frac{T^s}{s}\big).$$

Demostración.- Por el mismo razonamiento que en la observación previa y el lema 7.5.4, escribiendo $\sum_m \beta_m T^m = \det(I-AT)$, llegamos a que este teorema equivale a

$$\beta_m = (-1)^m\sum_{k=1}^{m}\sum_{i_1+\cdots+i_k=m}\frac{1}{k!}\frac{\mathrm{Tr}(\Psi^{i_1})\cdots\mathrm{Tr}(\Psi^{i_k})}{i_1\cdots i_k}, \qquad \text{para cada } m \geq 1. \tag{8.11}$$

Como mencionamos en la observación 8.6.13, se cumple que

$$\lim_{r\to\infty}\beta_m^r = \beta_m \quad \text{para cada } m \geq 0,$$

donde β_m^r es el coeficiente m-ésimo del polinomio característico conjugado de la matriz $A_r = [a_{u,v}]_{|u|,|v|\leq r} \in \mathbb{C}_p^{s(r)\times s(r)}$ en algún orden establecido en $\mathfrak{N}_r$. Como β_m^r satisfacen las ecuaciones de la observación anterior (respecto a la matriz A_r), y en las ecuaciones 8.11 tan sólo aparecen un número finito de términos del tipo $\mathrm{Tr}(\Psi^s)$, deducimos que es suficiente demostrar

$$\lim_{r\to\infty}\mathrm{Tr}(A_r^s) = \mathrm{Tr}(\Psi^s), \qquad \text{para cada } s \in \mathbb{N}.$$

De hecho, el caso $s = 1$ se verifica de manera inmediata por medio de la proposición 4.4.14 y la familia $\{\mathfrak{N}_r\}_{r\in\mathbb{N}}$, pues al existir $\mathrm{TR}(\Psi)$ ocurre que

$$\mathrm{TR}(\Psi) = \sum_{u\in\mathfrak{N}} a_{u,u} = \lim_{r\to\infty} \sum_{u\in\mathfrak{N}_r} a_{u,u} = \lim_{r\to\infty} \mathrm{TR}(A_r),$$

pues la traza de cada A_r es la suma de los elementos de la diagonal que son de la forma $a_{u,u}$ con $|u| \leq r$; de este modo el siguiente analísis se resume al caso $s \geq 2$. Sean $u_1, u_2, \ldots, u_{s(r)} \in \mathfrak{N}_r$ en el orden en el cual estos multiindices definen a las entradas de la matriz de A_r. Denotemos $A_r^s = [a_{u_i,u_j}^{(s)}]$, entonces la entrada de la fila $i-$ésima y j-columna será

$$a_{u_i,u_j}^{(s)} = \sum_{k_1,\ldots,k_{s-1}=1}^{s(r)} a_{u_i,u_{k_1}} a_{u_{k_1},u_{k_2}} \cdots a_{u_{k_{s-1}},u_j};$$

como estos multiindices u_{k_j} recorren todos los posibles elementos de $\mathfrak{N}_r$, tendremos que

$$a_{u_i,u_j}^{(s)} = \sum_{v_1,\ldots,v_{s-1}\in\mathfrak{N}_r} a_{u_i,v_1} a_{v_1,v_2} \cdots a_{v_{s-1},u_j}.$$

Asi obtenemos que

$$\mathrm{TR}(A_r^s) = \sum_{i=1}^{s(r)} \sum_{v_1,\ldots,v_{s-1}\in\mathfrak{N}_r} a_{u_i,v_1} \cdots a_{v_{s-1},u_i};$$

nuevamente, porque u recorre todos los posibles multiindices de $\mathfrak{N}_r$ y reemplanzando los valores de $a_{u,v}$ en relación a $G(X) = \sum_u b_u X^u$, concluimos que

$$\mathrm{TR}(A_r^s) = \sum_{u\in\mathfrak{N}_r} \sum_{v_1,\ldots,v_{s-1}\in\mathfrak{N}_r} b_{qv_1-u} \cdots b_{qu-v_{s-1}}, \tag{8.12}$$

para todo $r \in \mathbb{N}$; nótese que este valor independe del orden el cual fueron ordenados los multiindices de peso no mayor a r. Por otro lado, tomando $H(X) = G(X)G_q(X)\cdots G_{q^s}(X) = \sum_u c_u X^u$ tendremos que $H(X) \in \mathfrak{R}_p$, $\Psi^s = \Psi_{q^s,H(X)}$ y $\mathrm{TR}(\Psi^s)$ esta dado por

$$\mathrm{TR}(\Psi^s) = \sum_{u\in\mathfrak{N}} c_{(q^s-1)u} = \sum_{u\in\mathfrak{N}} \sum_{v_0+qv_1\cdots+q^{s-1}v_{s-1}=(q^s-1)u} b_{v_0} b_{v_1} \cdots b_{v_{s-1}};$$

los multiindices $q^i v_i$ que aparecen, son los unicos posibles exponentes de monomios X^u que poseen coeficientes posiblemente no nulos, los cuales son b_{v_i}, respectivamente. Como $\mathrm{TR}(\Psi^s)$ existe, aplicando la proposición 4.4.14 a la familia $\{\mathfrak{N}_r\}_{r\in\mathbb{N}}$ obtenemos que

$$\mathrm{TR}(\Psi^s) = \lim_{r\to\infty} \sum_{u\in\mathfrak{N}_r} \sum_{v_0+qv_1\cdots+q^{s-1}v_{s-1}=(q^s-1)u} b_{v_0} b_{v_1} \cdots b_{v_{s-1}}. \tag{8.13}$$

Con nuestro objetivo en mente, las ecuaciones (8.12) y (8.13) nos inducen a definir y comparar a los conjuntos

$$\mathcal{A}_u = \{(qw_1 - u, qw_2 - w_1, \ldots, qu - w_{s-1}) \in \mathfrak{N}^s \ ; \ w_1, \ldots, w_{s-1} \in \mathfrak{N}\}$$

y

$$\mathcal{B}_u = \{(v_0, \ldots, v_{s-1}) \in \mathfrak{N}\,;\; v_0 + qv_1 + \cdots + q^{s-1}v_{s-1} = (q^s - 1)u\},$$

para cada $u \in \mathfrak{N}$.

Afirmación : *Para todo* $u \in \mathfrak{N}$: $\mathcal{A}_u = \mathcal{B}_u$.

Dado $u \in \mathfrak{N}$, es claro que $\mathcal{A}_u \subset \mathcal{B}_u$; veamos que el contenido recíprocotambién sucede. Sea $(v_0, v_1, \ldots, v_{s-1}) \in \mathcal{B}_u$, deducimos que

$$v_0 = (q^s - 1)u - \sum_{i=1}^{s-1} q^i v_i = q(\underbrace{q^{s-1}u - \sum_{i=1}^{s-1} q^{i-1}v_i}_{w_1}) - u$$

con $w_1 \in \mathfrak{N}$, pues de lo contrario v_0 tendria componente negativas. Denotando $u = w_0$, supongamos que

$$v_i = qw_{i+1} - w_i \qquad \text{con } w_i \in \mathfrak{N}$$

para $i = 0, 1, \ldots, t$ (con $t \leq s-2$). Entonces,

$$(qw_1 - w_0) + q(qw_2 - w_1) + \cdots + q^t(qw_{t+1} - w_t) + \sum_{i=t+1}^{s-1} q^i v_i = (q^s - 1)u;$$

luego

$$q^{t+1}w_{t+1} - u + q^{t+1}v_{t+1} + \sum_{i=t+2}^{s-1} q^i v_i = q^s u - u,$$

y

$$v_{t+1} = qw_{t+2} - w_{t+1} \qquad \text{donde} \quad w_{t+2} = q^{s-t-2}u - \sum_{i=t+2}^{s-1} q^{i-1}v_i \in \mathfrak{N};$$

así obtenemos un proceso constructivo por el cual verificamos que existen $w_0, w_1, \ldots, w_s \in \mathfrak{N}$ tales que $w_0 = w_s = u$ $v_i = qw_{i+1} - w_i$, para cada $i = 0, 1, \ldots, s-1$; nótese que $w_s = u$ resulta directamente del paso $i = s-1$. Por lo tanto $(v_0, v_1, \ldots, v_{s-1}) \in \mathcal{A}_u$.

Ahora, dado $r \in \mathbb{N}$ definamos

$$\mathcal{A}_u^r = \{(qw_1 - u, \ldots, qu - w_{s-1}) \in \mathfrak{N}^s; w_1, \ldots, w_{s-1} \in \mathfrak{N}_r\}.$$

Vemos que todo $(v_0, \ldots, v_{s-1}) \in \mathcal{A}_u \setminus \mathcal{A}_u^r$ es de la forma $(qw_1 - u, \cdots, qu - w_{s-1})$ con algún $w_i \notin \mathfrak{N}_r$. Más aun, si $c > 0$ es tal que garantiza que $G(X) \in \mathfrak{N}_p$, tendremos que

$$\begin{aligned} v_p(b_{v_0}b_{v_1}\cdots b_{v_{s-1}}) &= v_p(b_{qw_1-u}) + \cdots + v_p(b_{qu-w_{s-1}}) \\ &\geq c(|qw_1 - u| + \cdots + |qu - w_{s-1}|) \\ &\geq c\big((q|w_1| - |u|) + \cdots + (q|u| - |w_{s-1}|)\big) \\ &= c(q-1)(|u| + |w_1|\cdots|w_{s-1}|) \\ &\geq c(q-1)r. \end{aligned}$$

Por otra parte, como la diferencia de la suma parcial que aparece en (8.13) con $\mathrm{TR}(A_r^s)$ es

$$\begin{aligned}\epsilon_r &= \sum_{u\in\mathfrak{N}_r}\sum_{(v_0,v_1,\cdots,v_{s-1})\in\mathcal{B}_u} b_{v_0}b_{v_1}\cdots b_{v_{s-1}} - \sum_{u\in\mathfrak{N}_r}\sum_{(v_0,\ldots,v_{s-1})\in\mathcal{A}_u^r} b_{v_0}b_{v_1}\cdots b_{v_{s-1}}\\ &= \sum_{u\in\mathfrak{N}_r}\sum_{(v_0,\ldots,v_{s-1})\in\mathcal{A}_u\setminus\mathcal{A}_u^r} b_{v_0}b_{v_1}\cdots b_{v_{s-1}},\end{aligned}$$

obtendremos que

$$|\epsilon_r|_p \le \max_{(v_0,v_1,\cdots,v_{s-1}} \{|b_{v_0}b_{v_1}\cdots b_{v_{s-1}}|_p\} \le p^{c(q-1)r}.$$

De esta desigualdad deducimos que

$$\lim_{r\to\infty}\Big(\sum_{u\in\mathfrak{N}_r}\sum_{(v_0,\ldots,v_{s-1})\in\mathcal{B}_u} b_{v_0}b_{v_1}\cdots b_{v_{s-1}} - \mathrm{TR}(A_r^s)\Big) = 0$$

y que $\lim_{r\to\infty}\mathrm{TR}(A_r^s) = \mathrm{TR}(\Psi)$, con lo cual concluimos el teorema.

Capítulo 9

El Teorema de Dwork

Un gran topico en Teoría de Números son las Ecuaciones Diofanticas. Este tipo de ecuaciones puede ser reducidas a una ecuación modular. Puesto que $\mathbb{Z}/\mathbb{Z}_p$ es un cuerpo, la ecuación inicial nos conlleva a una ecuación polinomial en cuerpos finitos. Estudiaremos el número de soluciones de este último tipo de ecuaciones a partir de una serie formal que derivamos de éstas.

9.1. Hipersuperficies afines y su función zeta

Definición 9.1.1 Sean K un cuerpo y $n \in \mathbb{N}$. Definimos

1. *El espacio afín n dimensional* $\mathbb{A}_K^n$ como K^n.

2. Para cada $f(X) \in K[X_1, \ldots, X_n]$ y L extensión de K, *la hipersuperficie afín* determinada por $f(X)$ en L como

$$\mathcal{H}_{f(X)}(L) = \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{A}_L^n \; ; \; f(\alpha_1, \ldots, \alpha_n) = 0\}.$$

   La dimensión de $\mathcal{H}_{f(X)}(L)$ es $n-1$.

3. El conjunto $\mathcal{H}'_{f(X)}(L) = \{(\alpha_1, \ldots, \alpha_n) \in \mathcal{H}_{f(X)} \; ; \alpha_i \neq 0, \forall i \}$.

Observación 9.1.2 En el caso que $n = 2$, las hipersuperfices afines son conocidas como *curvas afines.*

Nuestro estudio se restringirá al caso en que K sea un cuerpo finito y las extensiones L de K sean extensiones finitas de éste, por tanto también estos seran cuerpos finitos. Fijamos un polinomio $f(X) \in K[X_1, \ldots, X_n]$, entonces estaremos en la posibilidad de calcular el cardinal

de su hipersuperficie afín $\mathcal{H}_{f(X)}(L)$. Puesto que se tratan de cuerpos finitos veremos la independencia de este cardinal con respecto de la extensión tomada, siempre que sea del mismo grado sobre K.

Lema 9.1.3 *Sean K_q y $\bar{K}_q$ cuerpos de q elementos y $\sigma : K_q \to \bar{K}_q$ un isomorfismo. Dados $n \in \mathbb{N}$ y $f(x) \in K_q[X_1, \ldots, X_n]$, si K_{q^s} y $\bar{K}_{q^s}$ son cuerpos de q^s que contienen a K_q y $\bar{K}_q$ (respectivamente), entonces*

$$\#\mathcal{H}_{f(X)}(K_{q^s}) = \#\mathcal{H}_{\sigma f(X)}(\bar{K}_{q^s}) \qquad y \qquad \#\mathcal{H}'_{f(X)}(K_{q^s}) = \#\mathcal{H}'_{\sigma f(X)}(\bar{K}_{q^s}).$$

Demostración.- En virtud de la proposición 3.11.1 y del teorema 3.11.6, los cuerpos K_{q^s} y $\bar{K}_{q^s}$ son cuerpos de descomposición de $X^{q^s} - X \in K_q[X]$ sobre K_q y $X^{q^s} - X \in \bar{K}_q[X]$ sobre $\bar{K}_q$, respectivamente; por tanto, existe un isomorfismo $\tau : K_{q^s} \to \bar{K}_{q^s}$ que extiende a σ (por el teorema 3.6.10). Definamos $\eta : K_{q^s}^n \to \bar{K}_{q^s}^n$ por

$$\eta(\alpha_1, \ldots, \alpha_n) = \big(\tau(\alpha_1), \ldots, \tau(\alpha_n)\big),$$

entonces η sera una biyección. Para cada $(\alpha_1, \ldots, \alpha_n) \in \mathcal{H}_{f(X)}(K_{q^s})$ se cumple

$$\sigma f\big(\eta(\alpha_1, \ldots, \alpha_n)\big) = \tau f\big(\tau(\alpha_1), \ldots, \tau(\alpha_n)\big) = \tau\big(f(\alpha_1, \ldots, \alpha_n)\big) = 0,$$

por tanto $\eta\big(\mathcal{H}_{f(X)}(K_{q^s})\big) \subset \mathcal{H}_{\sigma f(X)}(\bar{K}_{q^s})$. De manera análoga, como $\eta^{-1}(\beta_1, \ldots, \beta_n) = \big(\tau^{-1}(\beta_1), \ldots, \tau^{-1}(\beta_n)\big)$ y τ^{-1} es una extensión de σ^{-1} deducimos que

$$\eta^{-1}\big(\mathcal{H}_{\sigma f(X)}(\bar{K}_{q^s})\big) \subset \mathcal{H}_{\sigma^{-1}\sigma f(X)}(K_{q^s}).$$

Por lo tanto $\mathcal{H}_{\sigma f(X)}(\bar{K}_{q^s}) \subset \eta\big(\mathcal{H}_{f(X)}(K_{q^s})\big)$, entonces concluimos la igualdad de estos conjuntos. Luego, puesto que η es inyectiva se concluye la primera igualdad del enunciado. Puesto que τ es un isomorfismo, dado $\alpha \in K_{q^s}^n$ tendremos que $\eta(\alpha)$ tendrá alguna componente no nula si y sólo si (α) lo tuviesé; por lo tanto concluimos que $\eta\big(\mathcal{H}'_{f(X)}(K_{q^s})\big) = \mathcal{H}'_{\sigma f(X)}(\bar{K}_{q^s})$, y por la inyectividad de η concluimos la segunda igualdad □

En base a este lema la siguiente definición es buena.

Definición 9.1.4 Sean $\mathbb{F}_q$ un cuerpo finito de q elementos y $f(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$. Elijamos una familia $\{\mathbb{F}_{q^s}\}_{s\in\mathbb{N}}$ de extensiones de $\mathbb{F}_q$, donde $\#\mathbb{F}_{q^s}$ es un cuerpo de q^s elementos, para cada $s \in \mathbb{N}$.

1. Dado $s \in \mathbb{N}$, definimos $N_s = \#\mathcal{H}_{f(X)}(\mathbb{F}_{q^s})$. La *función zeta de la hipersuperficie afín generada por $f(X)$ sobre $\mathbb{F}_q$* es determinaba por

$$\mathcal{Z}(\mathcal{H}_f/\mathbb{F}_q; T) = \exp \circ \Big(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}\Big).$$

2. Dado $s \in \mathbb{N}$, definimos $N'_s = \#\mathcal{H}_{f(X)}(\mathbb{F}_{q^s})$, y la serie formal $\mathscr{Z}'(\mathcal{H}_f/\mathbb{F}_q;T) = \exp\circ(\sum_{s=1}^{\infty} N_s\frac{T^s}{s})$.

Observaciones 9.1.5

- Por el teorema 3.11.7, tenemos que las extensiones tomadas en la anterior definición son todas las extensiones finitas de dicho cuerpo $\mathbb{F}_q$, más aun son las únicas dentro de una clausura algebraica de K.

- Sean $\mathbb{F}_q, \bar{\mathbb{F}}_q$ cuerpos de q elementos y $f(X) \in \mathbb{F}_q[X]$. Si σ es un isomorfismo entre estos cuerpos, entonces $\mathscr{Z}(\mathcal{H}_f/\mathbb{F}_q;T) = \mathscr{Z}(\mathcal{H}_{\sigma f}/\bar{\mathbb{F}}_q;T)$ y $\mathscr{Z}'(\mathcal{H}_f/\mathbb{F}_q;T) = \mathscr{Z}'(\mathcal{H}_{\sigma f}/\bar{\mathbb{F}}_q;T)$; de hecho, esto es consecuencia inmediata del lema previo.

Ejemplos 9.1.6 Asumamos las notaciones de la definición previa.

- Si $f(X) = X^n + g(X_1, X_2, \cdots, X_{n-1}) \in \mathbb{F}_q[X_1, \ldots, X_n]$. Entonces, podremos ver que

  $$\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) = \{(\alpha_1, \ldots, \alpha_{n-1}, g(\alpha_1, \ldots, \alpha_{n-1}) \ , \ (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_{q^s}^{n-1}\}, \quad \text{para todo } s \in \mathbb{N}.$$

  Por lo tanto, $N_s = \#\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) = q^{s(n-1)}$, para todo $s \in \mathbb{N}$

  $$\mathscr{Z}(\mathcal{H}_{f(X)}/\mathbb{F}_q;T) = \exp(\sum_{s=1}^{\infty} q^{s(n-1)}\frac{T^s}{s}) = (1-q^{n-1}T)^{-1}.$$

- Si $f(X_1, X_2) = X_1X_2 \in F_q[X_1, X_2]$. Entonces

  $$\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) = \{0\} \times \mathbb{F}_{q^s} \cup (\mathbb{F}_{q^s} \times \{0\} \setminus \{(0,0)\}), \qquad \text{para todo } s \in \mathbb{N}.$$

  Asi es como concluimos que

  $$\mathscr{Z}(\mathcal{H}_{f(X)}/\mathbb{F}_q;T) = \exp(\sum_{s=1}^{\infty}(2q^s-1)\frac{T^s}{s}) = \exp(\sum_{s=1}^{\infty} q^s\frac{T^s}{s})^2\exp(\sum_{s=1}^{\infty} q^s\frac{T^s}{s})^{-1} = \frac{1-T}{(1-qT)^2}.$$

En un inicio, el estudio de las funciones zeta se profundizó para ciertos tipos de curvas en el espacio proyectivo de $\mathbb{F}_q$ (vea por ejemplo [16, capítulo 3]). Luego, se conjeturo la validez de muchos de estos resultados para variades proyectivas, siendo pieza clave para la demostración de la primera de estas el siguiente lema.

Teorema 9.1.7 (Dwork) *Toda función zeta de una hipersuperficie es una función racional en $\mathbb{Q}$, es decir es cociente de dos polinomios con coeficientes en $\mathbb{Q}$.*

Podemos generalizar un tanto la definición de hipersuperficie afín manteniendo el teorema de Dwork cierto.

Definición 9.1.8 Sea K un cuerpo y $f_1(X), \ldots, f_m(X) \in K[X_1, \ldots X_n]$ y L extensión de K, *el conjunto algebraico* determinado por $f_1(X)$ en L como

$$\mathcal{H}_{f_1(X),\ldots,f_m(X)}(L) = \{(\alpha_1, \ldots, \alpha_n) \in L^n \; ; \; f_1(\alpha_1, \ldots, \alpha_n) = \cdots = f_m(\alpha_1, \ldots, \alpha_n) = 0\}.$$

La dimensión de $\mathcal{H}_{f_1(X),\ldots,f_m(X)}(L)$ es $n-1$.

Observación 9.1.9 Se cumple

$$\mathcal{H}_{f_1(X),\ldots,f_m(X)}(L) = \mathcal{H}_{f_1(X)}(L) \cap \cdots \cap \mathcal{H}_{f_m(X)}(L).$$

Es claro que se puede formular y demostrar un resultado similar al lema 9.1.3 para el caso en que L y K sean cuerpos finitos, el cual nos asegure la concretitud de la siguiente definición.

Definición 9.1.10 Sean $\mathbb{F}_q$ un cuerpo finito de q elementos y $f_1(X), \ldots, f_m(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$. Dado $s \in \mathbb{N}$, definimos $N_s = \#\mathcal{H}_{f_1(X),\ldots,f_m(X)}(\mathbb{F}_{q^s})$, donde $\mathbb{F}_{q^s}$ es un cuerpo de q^s elementos que contiene a $\mathbb{F}_q$. La *función zeta* del conjunto algebraico determinado por $f_1(X), \ldots, f_m(X)$ sobre $\mathbb{F}_q$ es dado por

$$\mathcal{Z}(\mathcal{H}_{f_1(X),\ldots,f_m(X)}/\mathbb{F}_q; T) = \exp \circ (\sum_{s=1}^{\infty} N_s T^s).$$

Proposición 9.1.11 *La función zeta de un conjunto algebraico* $\mathcal{H}_{f_1(X),\ldots,f_m(X)}$ *es una función racional con coeficientes en* $\mathbb{Q}$.

Demostración.- Realizaremos esta prueba por inducción sobre m, el números de hipersuperficies que definen al conjunto algebraico. Empecemos por notar que esta proposición es cierta cuando $m = 1$, supongamos que es cierto para toda cantidad de polinomios menor a m. Dado $s \in \mathbb{N}$, es clara la siguiente relación entre hipersuperficies afines:

$$\mathcal{H}_{f_1(X)\cdots f_m(X)}(\mathbb{F}_{q^s}) = \mathcal{H}_{f_1(X)}(\mathbb{F}_{q^s}) \cup \cdots \cup \mathcal{H}_{f_m(X)}(\mathbb{F}_{q^s});$$

lo cual nos implica que

$$\#\mathcal{H}_{f_1(X)\cdots f_m(X)}(\mathbb{F}_{q^s}) = \sum_{k=1}^{m} (-1)^{k+1} \sum_{1 \le i_1 < \cdots < i_k \le m} \#\big(\mathcal{H}_{f_{i_1}(X)}(\mathbb{F}_{q^s}) \cap \cdots \cap \mathcal{H}_{f_{i_k}(X)}(\mathbb{F}_{q^s})\big),$$

para todo $s \in \mathbb{N}$. Luego, tomando en cuenta la observación 9.1.9 y las propiedades de la serie exponencial, deducimos que

$$\mathcal{Z}(\mathcal{H}_{f_1(X)\cdots f_m(X)}/\mathbb{F}_q; T) = \prod_{k=1}^{m} \Big(\prod_{1 \le i_1 < \cdots < i_k \le m} \mathcal{Z}(\mathcal{H}_{f_{i_1}(X),\ldots,f_{i_k}(X)}/\mathbb{F}_q; T) \Big)^{(-1)^{k+1}};$$

por lo tanto

$$\mathscr{Z}(\mathcal{H}_{f_1(X),\ldots,f_m(X)}/\mathbb{F}_q;T) = \mathscr{Z}(\mathcal{H}_{f_1(X)\cdots f_m(X)}/\mathbb{F}_q;T)^{(-1)^{m+1}} \times \prod_{k=1}^{m-1}\Big(\prod_{1\le i_1<\cdots<i_k\le m}\mathscr{Z}(\mathcal{H}_{f_{i_1}(X),\ldots,f_{i_k}(X)}/\mathbb{F}_q;T)\Big)^{(-1)^{m+k+1}}.$$

De este modo, hemos expresado a $\mathscr{Z}(\mathcal{H}_{f_1(X),\ldots,f_m(X)}/\mathbb{F}_q;T)$ como el producto de funciones zeta de conjuntos algebraicos (o inversas de estas funciones), cada uno de estos conjuntos algebraicos es generado por un número de polinomios menor a m. Luego, la serie formal $\mathscr{Z}(\mathcal{H}_{f_1(X),\ldots,f_m(X)}/\mathbb{F}_q;T)$ es una función racional con coeficientes en $\mathbb{Q}$. □

9.2. Propiedades basicas de $\mathscr{Z}(\mathcal{H}_f/\mathbb{F}_q;T)$

Los siguientes lemas describen las primeras caracteristicas que podemos deducir estas series formales.

Lema 9.2.1 *La serie formal $\mathscr{Z}(\mathcal{H}_f;/\mathbb{F}_q,T)$ tiene coeficientes enteros.*

Demostración.- Ahora haremos del uso lema 9.1.3, fijemos una clausura algebraica Ω sobre $\mathbb{F}_q$ y, para cada $s \ge 1$, escojamos por $\mathbb{F}_{q^s}$ al único cuerpo contenido en Ω con q^s elementos.

Sea K una extensión finita de $\mathbb{F}_q$ y $P = (\alpha_1,\ldots,\alpha_n) \in \mathcal{H}_f(K)$, tomemos $s_0 = \text{mín}\{s \in \mathbb{N}\ ;\ P \in \mathcal{H}_f(\mathbb{F}_{q^s})$. Dado $\sigma \in G(\mathbb{F}_{q^{s_0}}/\mathbb{F}_q)$, definamos $\sigma(P) = \big(\sigma(\alpha_1),\ldots,\sigma(\alpha_n)\big)$. Como vimos en el teorema 3.11.6, el grupo de Galois de $\mathbb{F}_{q^{s_0}}/\mathbb{F}_q$ tendra s_0 elementos, a los cuales denotamos por $\sigma_1 = \text{id}, \sigma_2, \ldots, \sigma_{s_0}$. Por lo tanto tendremos s_0 puntos de la forma $\sigma_i(P)$; denotemos por P_i a $\sigma_i(P)$, para cada $i = 1, 2, \ldots, s_0$.

Afirmación 1: *Para $1 \le i < j \le s_0$, se tiene que $P_i \ne P_j$.*

De hecho, si $\sigma_i(\alpha_k) = \sigma_j(\alpha_k)$ para cada $k \in \{1,2,\ldots,n\}$, entonces $x_k = \sigma_l(\alpha_k)$ con $\sigma_l = \sigma_i^{-1}\sigma_j \ne \text{id}$. Lo cual significará que α_k pertenece a $\mathcal{F}(\sigma_l)$, el subcuerpo fijado por σ_l, para todo k; por tanto $P \in \mathcal{H}_{f(X)}\big(\mathcal{F}(\sigma_l)\big)$. Como $\sigma_l \ne \text{id}$, tendremos que $\mathcal{F}(\sigma_l)$ esta contenido propiamente en $\mathbb{F}_{q^{s_0}}$ (por el lema 3.11.9), de modo que $\mathcal{F}(\sigma_l) = \mathbb{F}_{q^{\bar{s}}}$ con $\bar{s} < s_0$, contradiciendo la minimalidad s_0.

Ahora denotemos por

$$\mathcal{P}(s) = \{P \in \mathcal{H}_f(\mathbb{F}_{q^s})\ ;\ P \notin \mathcal{H}_f(\mathbb{F}_{q^r})\ ,\ r < s\} \quad \text{y} \quad \mathcal{R}(s) = \#\mathcal{P}(s).$$

Afirmación 2: *Para $s \in \mathbb{N}$: s divide a $\mathcal{R}(s)$*

En $\mathcal{P}(s)$ podemos definir la relación $\sim$ como $P \sim Q$ si y sólo si $Q = \sigma(P)$ para algún $\sigma(Q) \in G(\mathbb{F}_{q^s}/\mathbb{F}_q)$.Es claro que esta relación es de equivalencia (porque $G(\mathbb{F}_{q^s}/\mathbb{F}_q)$ es un

grupo), más aun la clase de cada elemento tiene exactamente s elementos por la afirmación anterior; lo cual es cierto pues $\sigma(P) \in \mathcal{P}(s)$, para todo $P \in \mathcal{P}(s), \sigma \in G(\mathbb{F}_{q^s}/\mathbb{F}_q)$. En efecto, como $\mathbb{F}_{q^s}$ es normal sobre $\mathbb{F}_q$ tendremos que $\sigma(P) \in \mathbb{F}_{q^s}^n$ (por la proposición 3.7.9), luego $s \geq \bar{t} = \text{mín}\{t\ ;\ \sigma(P) \in \mathcal{H}_{f(X)}(\mathbb{F}_{q^t})\}$. Un razonamiento analogo muestra que $P = \sigma^{-1}(\sigma(P)) \in \mathcal{H}_{f(X)}(\mathbb{F}_{q^{\bar{t}}})$; por lo tanto $\bar{t} = s$ y $\sigma(P) \in \mathcal{P}(s)$. Luego, $\mathcal{P}(s)$ será particionada por las clases de equivalencia de sus elementos, como cada clase tiene exactamente s elementos concluimos lo afirmado.

Afirmación 3: *Dado* $s \in \mathbb{N}$: $\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) = \biguplus_{d|s} \mathcal{P}(d)$.

En efecto, dado $P \in \mathcal{P}(d)$ con $d \mid s$, se tiene que P es un cero de $f(X)$ contenido en $\mathbb{F}_{q^d}^n$. Por el teorema 3.11.7 acontece que $P \in \mathbb{F}_{q^s}^n$ y $P \in \mathcal{H}_{f(X)}(\mathbb{F}_{q^s})$. Recíprocamente, dado $P \in \mathcal{H}_{f(X)}(\mathbb{F}_{q^s})$, tomemos $d = \text{mín}\{t\ ;\ P \in \mathcal{H}_{f(X)}(\mathbb{F}_{q^t})\}$. Escribiendo $P = (\alpha_1, \ldots, \alpha_n)$, tenemos que $\mathbb{F}_q(\alpha_1, \ldots, \alpha_n)$ es un cuerpo de q^t elementos para algún $t \geq 1$; luego, por la unicidad de extensiones finitas dentro de Ω tenemos que $\mathbb{F}_{q^t} = \mathbb{F}_q(\alpha_1, \ldots, \alpha_n)$. Así pues $P \in \mathcal{H}_{f(X)}(\mathbb{F}_{q^t})$ y $t \geq d$. Por otra parte, como $\mathbb{F}_q(\alpha_1, \ldots, \alpha_n) \subset \mathbb{F}_{q^d}$ tendremos que $t \leq d$; por lo tanto, $t = d$ y $\mathbb{F}_{q^d} = \mathbb{F}_q(\alpha_1, \ldots, \alpha_n)$. Como $\mathbb{F}_q(\alpha_1, \ldots, \alpha_n) \subset \mathbb{F}_{q^s}$, nuevamente, por el teorema 3.11.7 concluimos d divide a s.

Esta afirmación nos permite deducir que

$$N_s = \sum_{d|s} \mathcal{R}(s), \quad \text{para todo } s \in \mathbb{N};$$

en consecuencia,

$$\sum_{s=1}^{\infty} \frac{N_s}{s} T^s = \sum_{s=1}^{\infty} \sum_{d \cdot r = s} \frac{\mathcal{R}(s)}{dr} (T^d)^r = \sum_{s=1}^{\infty} \sum_{(d,r) \in \mathcal{A}(s)} \frac{\mathcal{R}(s)}{dr} (T^d)^r, \tag{9.1}$$

donde $\mathcal{A}(s) = \{(d, r) \in \mathbb{N}^2\ ;\ d \cdot r = s\}$.

Ahora, para cada $m \in \mathbb{N}$ definamos los conjuntos $\mathcal{N}_m = \{(d, r) \in \mathbb{N}^2\ ;\ d \leq m\}$, los cuales seran numerables; más aun permitirá que las series

$$Z_m(T) = \sum_{(d,r) \in \mathcal{N}_m} \frac{\mathcal{R}(d)}{dr} (T^d)^r$$

sean convergentes en $(\mathbb{Q}[[T]], |\cdot|_T)$. De hecho, para cada $m \in \mathbb{N}$ y $\epsilon > 0$ tomamos $r_0 \in \mathbb{N}$ tal que $e^{-r_0} < \epsilon$ y $F_0 = \{(d, r)\ ;\ r \leq r_0\ ,\ d \leq m\}$, que es finito. Entonces, $(d, r) \in \mathcal{N}_m \setminus F_0$ implica que $|\frac{\mathcal{R}(d)}{dr}(T^d)^r|_T < e^{-dr_0} < \epsilon$; con esto y la proposición 4.4.11 podemos deducir la convergencia de $Z_m(T)$. Vea que $\mathcal{N}_m$ es particionado por las dos siguientes familias $\{\mathcal{A}_s\}_{s \in \mathbb{N}}$ y $\{\mathcal{B}_d\}_{d \leq m}$ definidas por :

$$\mathcal{A}_m(s) = \{(d, r) \in \mathbb{N}^2\ ;\ d \cdot r = s\} \quad \text{y} \quad \mathcal{B}_d = \{(d', r) \in \mathbb{N}^2\ ;\ d' = d\}.$$

En virtud del lema 4.4. 15, estas particiones nos permiten representar a $Z_m(T)$ como

$$\sum_{d=1}^{m}\sum_{r=1}^{\infty}\frac{\mathcal{R}(d)}{dr}(T^d)^r \quad \text{y} \quad \sum_{s=1}^{\infty}\sum_{(d,r)\in\mathcal{A}_m(s)}\frac{\mathcal{R}(d)}{dr}(T^d)^r.$$

Observando que $\mathcal{A}_m(s)=\mathcal{A}(s)$ cuando $s\leq m$, la igualdad (9. 1) nos permite concluir que

$$\sum_{s=1}^{\infty}\frac{N_s}{s}T^s-\sum_{d=1}^{m}\sum_{r=1}^{\infty}\frac{\mathcal{R}(d)}{dr}(T^d)^r=\sum_{s=m+1}^{\infty}\sum_{(d,r)\in\mathcal{A}(s)\setminus\mathcal{A}_m(s)}\frac{\mathcal{R}(d)}{dr}(T^d)^r,$$

para todo $m\in\mathbb{N}$. Como

$$\Big|\sum_{(d,r)\in\mathcal{A}(s)\setminus\mathcal{A}_m(s)}\frac{\mathcal{R}(d)}{dr}(T^d)^r\Big|_T\leq \text{máx}\{\Big|\frac{\mathcal{R}(d)}{dr}(T^d)^r\Big|_T;\ (d,r)\in\mathcal{A}(s)\}=e^{-s},$$

para todo $s\geq m+1$, por la proposición 4.4. 12 tenemos que

$$\Big|\sum_{s=1}^{\infty}\frac{N_s}{s}T^s-\sum_{d=1}^{m}\sum_{r=1}^{\infty}\frac{\mathcal{R}(d)}{dr}(T^d)^r\Big|_T\leq e^{-s};$$

por lo tanto $(Z_m(T))_{m\in\mathbb{N}}$ converge a $\sum N_sT^s/s$ en $(\mathbb{Q}[[T]],|\cdot|_T)$. Luego,

$$\exp\Big(\sum_{s=1}^{\infty}\frac{N_s}{s}T^s\Big)=\exp\Big(\sum_{d=1}^{\infty}\sum_{r=1}^{\infty}\frac{\mathcal{R}(d)}{dr}(T^d)^r\Big)=\prod_{d=1}^{\infty}\exp\Big(\frac{\mathcal{R}(d)}{d}\sum_{r=1}^{\infty}\frac{(T^d)^r}{r}\Big),$$

donde la última igualdad se logra gracias a la propiedad de la serie formal $\exp(T)$ con respecto a la suma y la continuidad de la composición mostrada en la proposición 7. 2 5. Más aun, puesto que cada factor $\mathcal{R}(d)/d$ es un entero (por la afirmación 2), podemos aplicar las propiedades de $\exp(T)$ y obtener que

$$\mathcal{Z}(\mathcal{H}_{f(X)},\mathbb{F}_q;T)=\prod_{d=1}^{\infty}\exp\Big(\sum_{r=1}^{\infty}\frac{(T^d)^r}{r}\Big)^{\frac{\mathcal{R}(d)}{d}}.$$

Finalmente, por la proposición 7. 5. 12 tendremos que

$$\mathcal{Z}(\mathcal{H}_{f(X)},\mathbb{F}_q;T)=\prod_{d=1}^{\infty}\exp\big(\log(1-T^d)\big)=\prod_{d=1}^{\infty}\Big(\sum_{r=0}^{\infty}(T^d)^r\Big),$$

de esta forma hemos demostrado que $\mathcal{Z}(\mathcal{H}_{f(X)},\mathbb{F}_q;T)$ es el límite de una secuencia en $(\mathbb{Z}[[T]],|\cdot|_T)$, como este conjunto es cerrado en $(\mathbb{Q}[[T]],|\cdot|_T)$ concluimos el lema. □

El siguiente lema nos brinda una estimación muy sencilla acerca del tamaño de los coeficientes de una función zeta.

Lema 9.2.2 *Si representamos* $\mathcal{Z}(\mathcal{H}_{f(X)},\mathbb{F}_q;T)=\sum_{s=1}^{\infty}a_sT^s$, *entonces* $|a_s|_\infty\leq q^{sn}$, *para todo* $s\geq 0$; *donde* $|\cdot|_\infty$ *es el valor absoluto tradicional en* $\mathbb{Q}$.

Demostración.- Empezamos por observar que el lema ya es cierto para $s = 0$. Para cada $s \in \mathbb{N}$ ocurre que

$$N_s = \#\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \leq \#\mathbb{F}_{q^s}^n = q^{sn}.$$

Por el lema 7.5.4, vemos que el a_s es menor que el coeficiente s-ésimo de $\exp(\sum q^{sn}T^s/s)$, para cada $s \geq 1$. Pero

$$\exp(\sum_{s=1}^{\infty} \frac{q^{sn}T^s}{s}) = (1 - q^nT)^{-1} = \sum_{s=1}^{\infty} q^{ns}T^s;$$

por lo tanto $a_s \leq q^{sn}$, para todo $s \in \mathbb{N}$. □

Observación 9.2.3 Estas dos últimas demostraciones coinciden en un hecho: los coeficientes de la función zeta de una hipersuperficie son racionales positivos.

9.3. Caracteres en $\mathbb{C}_p$ y un levantamiento analítico

Ahora estableceremos un concepto que será una herramienta primordial para contabilizar los elementos de cada hipersuperficie $\mathcal{H}_f(\mathbb{F}_{q^s})$.

Definición 9.3.1 Sean G un grupo y $\psi : G \to \mathbb{C}_p^\times$, diremos que ψ es C_p-caracter, si ψ es un homomorfismo de grupos (hacia el grupo multiplicativo $\mathbb{C}_p^\times$). Además, diremos que ψ es no trivial si es un homomorfismo no trivial.

Observación 9.3.2 Si G es un grupo de orden $n \in \mathbb{N}$, entonces $\psi(g)$ es una raíz n-ésima en $\mathbb{C}$. De hecho, por Lagrange tendremos

$$\psi(g)^n = \psi(g^n) = \varphi(1) = 1, \qquad \text{para todo } g \in G.$$

Este hecho nos motiva a realizar la siguiente construcción.

Fijemos una raíz primitiva $p-$ésima $\epsilon \in \mathbb{C}_p$ durante este capítulo. Definiendo $\varphi : \mathbb{Z} \to \mathbb{C}_p^\times$ por $\varphi(n) = \epsilon^n$, obtendremos un $\mathbb{C}_p-$caracter; más aun, se cumple

$$\varphi(n) = \varphi(m), \quad \text{siempre que } m \equiv n \text{ mód } p \tag{9.2}$$

Procedamos a extender este $\mathbb{C}_p-$caracter sobre $\mathbb{Z}_p$. Puesto que la serie binomial extiende al binomio de Newton tendremos que

$$\varphi(n) = \epsilon^n = (1 + \lambda)^n = B(n, \lambda) \quad \text{para cada } n \in \mathbb{N};$$

donde $\lambda = \epsilon - 1$. Como hemos visto en el lema 6.4.14, el valor absoluto p-ádico de λ es $p^{1/(1-p)}$, por tanto $B(a, Y)$ converge en λ, para todo $a \in \mathbb{Z}_p$ (por el segundo ítem de la proposición

8.5.1). De este modo es admisible extender el $\mathbb{C}_p$-caracter φ por $B(\cdot,\lambda)$ en $\mathbb{Z}_p$; verifiquemos que todavia φ será un $\mathbb{C}_p-$caracter: Dado $\alpha\in\mathbb{Z}_p$, denotemos su expasión $p-$ádica por $\sum_{i\geq 0}a_ip^i$, entonces, en virtud del cuarto ítem de la proposición 8.5.1, tendremos que

$$\varphi(\alpha)=B(\sum_{i=0}^{\infty}a_ip^i,\lambda)=\lim_{n\to\infty}B(\sum_{i=0}^{n}a_ip^i,\lambda),$$

entonces por la propiedad 9.2 tendremos que $\varphi(\alpha)=\lim_{n\to\infty}\varphi(a_0)=\varphi(a_0)$. Por lo tanto,

$$\varphi(\alpha)=\varphi(a),\quad \text{siempre que } \alpha\equiv a \text{ mód } p; \tag{9.3}$$

puesto que en estas condiciones $a\equiv a_0$ mód p.

Ahora, dados $\alpha,\beta\in\mathbb{Z}_p$, elijamos $a,b\in\mathbb{Z}$ tales que $\alpha\equiv a(\text{mód } p)$ y $\beta\equiv b(\text{mód } p)$, entonces

$$\alpha+\beta\equiv a+b(\text{mód } p)\quad \text{y}\quad \varphi(\alpha+\beta)=\varphi(a+b)=\varphi(a)\varphi(b)=\varphi(\alpha)\varphi(\beta);$$

por lo tanto φ es un $\mathbb{C}_p$-caracter de $\mathbb{Z}_p$. En consecuencia, la propiedad 9.3 es generalizada inmediatamente en

$$\varphi(\alpha)=\varphi(\beta),\qquad \text{cuando } \alpha\equiv\beta \text{ mód } p. \tag{9.4}$$

Aunque esta extensión es ciertamente trivial, nos concedera el más importante "ingrediente $p-$ádico" para la demostración del Teorema de Dwork.

Sea $\zeta:\mathcal{R}_p\to\mathcal{T}_p$ la biyección mencionada en el lema 6.6.6. Dado $r\in\mathbb{N}$, sean $\widetilde{\mathbb{k}}_r$ el subcuerpo de p^r elementos contenido en $\mathcal{R}_p$ y $\mathcal{Z}_r$ el conjunto de ceros de $X^{p^r}-X$ en $\mathbb{C}_p$. Como hemos visto en el lema 6.6.6, ocurria que $\zeta(\widetilde{\mathbb{k}}_r)=\mathcal{Z}_r$. Puesto que $\mathcal{Z}_r$ esta contenido en el anillo de valuación de $\mathcal{L}_r$ (la extensión no ramificada de grado r), tendremos que $T_{\mathcal{L}_r/\mathbb{Q}_p}(\zeta(\mathbb{k}_r))\subset\mathbb{Z}_p$, en virtud de la proposición 6.3.14. Por lo tanto, podemos definir $\psi_0:\widetilde{\mathbb{k}}_r\to\mathbb{C}_p$ por

$$\psi_0(A)=\varphi\big(T_{\mathcal{L}_r/\mathbb{Q}_p}(\zeta(A))\big),\qquad \text{para todo } A\in\widetilde{\mathbb{k}}_r;$$

veamos ψ_0 que es un $\mathbb{C}_p-$caracter. De hecho, dados $A,B\in\widetilde{\mathbb{k}}_r$, en virtud del corolario 6.4.10 se cumple que $T_{\mathcal{L}_r/\mathbb{Q}_p}\big(\zeta(A+B)\big)=\sum_{k=0}^{r-1}\zeta(A+B)^{p^k}$; luego

$$T_{\mathcal{L}_r/\mathbb{Q}_p}\big(\zeta(A+B)\big)\equiv\sum_{k=0}^{r-1}\big(\zeta(A)+\zeta(B)\big)^{p^k}\equiv\sum_{k=0}^{r-1}\big(\zeta(A)+\zeta(B)\big)^{p^k}\ \text{mód } \mathfrak{d}_p.$$

Por lo tanto $T_{\mathcal{L}_r/\mathbb{Q}_p}\big(\zeta(A+B)\big)\equiv T_{\mathcal{L}_r/\mathbb{Q}_p}\big(\zeta(A)\big)+T_{\mathcal{L}_r/\mathbb{Q}_p}\big(\zeta(B)\big)$ mód $\mathfrak{d}_p$. Como éstos elementos son enteros p-ádicos, en virtud de la propiedad 9.4 concluimos que

$$\psi_0(A+B)=\varphi(T_{\mathcal{L}_r/\mathbb{Q}_p}(\zeta(A))+T_{\mathcal{L}_r/\mathbb{F}_p}(\zeta(B)))=\varphi(T_{\mathcal{L}_r/\mathbb{F}_p}(\zeta(A)))\varphi(T_{\mathcal{L}_r/\mathbb{F}_p}(\zeta(B)))=\psi_0(A)\psi_0(B).$$

El último paso en todo este análisis será reformular la definición de ψ_0 sobre $\widetilde{\mathbb{k}}_r$, para esto utilizaremos las propiedades de la serie formal $F(X,Y)$ que fueron indicadas en el lema 8.5.5.

Lema 9.3.3 *Sean $\epsilon \in \mathbb{C}_p$ una raíz $p-$ésima de la unidad distinta de 1 y $\lambda = \epsilon - 1$. Entonces, $\Theta(X) = F(X,\lambda) = \sum a_m X^m \in \mathbb{C}_p$ es una serie formal bien definida que satisface*

1. *Para $m \geq 0$, $v_p(a_m) \geq m(p-1)^{-1}$. En particular, $\Theta(X)$ converge en $\mathcal{D}(p^{1/(p-1)})$.*

2. *Dado $r \in \mathbb{N}$, sea $\widetilde{\mathbb{k}}_r$ el subcuerpo de $\mathfrak{K}_p$ que posee p^r elementos. Entonces, la función $\psi : \widetilde{\mathbb{k}}_r \to \mathbb{C}_p$ definida por*

$$\psi(A) = \Theta\big(\zeta(A)\big)\Theta\big(\zeta(A)^p\big)\cdots\Theta\big(\zeta(A)^{p^{r-1}}\big),$$

es un $\mathbb{C}_p$-caracter no trivial sobre $\widetilde{\mathbb{k}}_r$, donde $\zeta : \mathfrak{K}_p \to \mathcal{T}_p$ es la función mencionada en el lema 6.6.6.

Demostración.- Como $v_p(\lambda) = (p-1)^{-1}$, el primer item es consecuencia directa de la proposición 8.5.4; luego la función ψ esta bien definida, pues $\mathcal{T}_p \subset \mathfrak{D}_p$. Utilizaremos el lema 8.5.5 junto con nuestro análisis previo para concluir que $\psi = \psi_0$.

Dado $A \in \mathbb{k}_r$, denotemos $t = \zeta(A)$, entonces $(t,\lambda) \in \mathcal{D}[1] \times \mathcal{D}(1)$. Por tanto, $F(X,Y)$ converge en (t^{p^j},λ), para cada $j \geq 0$ (por la proposición 8.5.3). Luego, dado $j \geq 0$, por la proposición 8.2.4 tendremos que

$$F(t^{p^j},\lambda) = \sum_{m=0}^{\infty}\Big(\sum_{n=0}^{\infty} a_{m,n}\lambda^n\Big)(t^{p^j})^m = \sum_{n=0}^{\infty}\Big(\sum_{m=0}^{\infty} a_{m,n}(t^{p^j})^m\Big)\lambda^n.$$

Tomando en cuenta que $F(X,Y) \in K[X][[Y]]$ y denotando por $H_j(Y) = F(t^{p^j},Y)$ tendremos que

$$\Theta(t^{p^j}) = \sum_{m=0}^{\infty} a_m(t^{p^j})^m = H_j(\lambda) \qquad \text{para cada } j \geq 0.$$

Entonces

$$\Theta(t)\Theta(t^p)\cdots\Theta(t^{p^{s-1}}) = H_0(\lambda)H_1(\lambda)\cdots H_{s-1}(\lambda).$$

Puesto que el segundo miembro de esta igualdad es el valor de $H_0(Y)H_1(Y)\cdots H_{s-1}(Y)$ en λ (por la proposición 8.2.3), en virtud del lema 8.5.5 concluimos que

$$\Theta\big(\zeta(A)\big)\Theta\big(\zeta(A)^p\big)\cdots\Theta\big(\zeta(A)^{p^{s-1}}\big) = B\big(\zeta(A)+\zeta(A)^p+\cdots+\zeta(A)^{p^{s-1}},\lambda\big); \qquad (9.5)$$

de este modo $\psi = \psi_0$ y ψ es un $\mathbb{C}_p$-caracter.

Finalmente, mostraremos que ψ no es trivial. Puesto que $T_{\mathbb{k}_r/\mathbb{F}_p}$ es sobreyectiva (por el lema 3.11.10), existe $A_0 \in \mathbb{k}_r$ tal que $T_{\mathbb{k}_r/\mathbb{F}_p}(A_0) = 1 + \mathfrak{d}_p$. Luego, en virtud del lema 6.6.6 tendremos que

$$1 + \mathfrak{d}_p = T_{\widetilde{\mathbb{k}}_f/\mathbb{F}_p}(A_0) = T_{\mathcal{L}_f/\mathbb{Q}_p}\big(\zeta(A_0)\big) + \mathfrak{d}_p,$$

en consecuencia $\psi(A_0) = \varphi\big(\zeta(A_0)\big) = \varphi(1) = \epsilon \neq 1$; por lo tanto ψ es no trivial. □

Observaciones 9.3.4

- Note que en caso $r = 1$, tenemos $\psi(A) = \Theta\big(\zeta(A)\big)$, para todo $A \in \widetilde{\mathbb{k}_1}$. Por tanto $\Theta(0) = \Theta\big(\zeta(0)\big) = \psi(\mathfrak{d}_p) = 1$. Esto nos indica que el término independiente de $\Theta(X)$ es 1.

- Vemos que resultado importante de esta demostración es la ecuación 9.5. La propiedad de la serie binomial con respecto al producto (primer ítem de la proposición 8.5.1) nos sugiere tomar simplemente $\Theta(X) = B(X, \lambda)$, veamos que esto es imposible en general. Si $t = \zeta(A)$ con $A \in \mathfrak{K}_p \setminus \mathbb{F}_p$, entonces $t + \mathfrak{d}_p \neq n + \mathfrak{d}_p$, para todo $n \in \mathbb{Z}$; en particular $|t - n|_p = 1$ para todo $n \in \mathbb{Z}$. Luego, para $n \geq 1$

$$\left|\binom{t}{n}\lambda^n\right|_p = \left|t\prod_{m=1}^{n-1}\frac{t-m}{m}\lambda^n\right|_p = \left|\frac{\lambda^n}{n!}\right|_p = p^{\frac{s(n)}{p-1}},$$

donde $s(n)$ es la suma de los digitos del numeral de n en base p. Por lo tanto $\left|\binom{t}{p^m}\lambda^{p^m}\right|_p = p^{1/(p-1)}$, para todo $m \in \mathbb{N}$; de este modo $B(t, \lambda)$ no existirá en $\mathbb{C}_p$.

El hecho que un $\mathbb{C}_p-$ caracter sea no trivial repercute en un tipo de extensión del lema 3.12.3.

Lema 9.3.5 *Sea φ un $\mathbb{C}_p$-caracter no trivial de un grupo finito G, entonces*

$$\sum_{g\in G}\varphi(g) = 0.$$

Demostración.- Puesto que $\varphi(G)$ es un subgrupo finito de $\mathbb{C}_p^\times$, éste posee un generador ζ_0 de orden $m \neq 1$. Por ser G un grupo y φ un homomorfismo, dado $\zeta \in \mathrm{im}(\varphi)$ se tiene que

$$\varphi^{-1}(\zeta) = \varphi^{-1}(g)\mathrm{Nu}(\varphi),$$

para todo $g \in \varphi^{-1}(\zeta)$. Luego, si $\zeta = \varphi(g_0)$ con $g_0 \in G$ entonces

$$G = \biguplus_{\zeta\in \mathrm{im}\,(\varphi)} \varphi^{-1}(\zeta) = \biguplus_{k=1}^{m} \varphi^{-1}(\zeta^k) = \biguplus_{k=1}^{m} g_0^k\mathrm{Nu}(\varphi),$$

por lo tanto

$$\sum_{g\in G}\varphi(g) = \sum_{k=1}^{m}\sum_{g\in \mathrm{Nu}(\varphi)}\varphi(g_0^k g) = \sum_{k=1}^{m}\sum_{g\in \mathrm{Nu}(\varphi)}\zeta_0^k\cdot 1 = \#\mathrm{Nu}(\varphi)\sum_{k=1}^{m}\zeta_0^k = 0,$$

en virtud del lema 3.12.3. □

Corolario 9.3.6 *Dado $r \in \mathbb{N}$, el caracter ψ establecido en el lema 9.3.3 satisface*

$$\sum_{\alpha_0 \in \widetilde{\mathbf{k}}_r^\times} \psi(\alpha_0 u) = \begin{cases} p^r - 1 & , \ si\ u = 0 \\ -1 & , \ si\ u \neq 0 \end{cases} \qquad \text{para todo } u \in \widetilde{\mathbf{k}}_r.$$

Demostración.- En el caso que u sea 0, el corolario se verifica inmediatamente. En caso contrario, tenemos que el producto por u, genera una permutación en los elementos del grupo multiplicativo $\widetilde{\mathbf{k}}_r \times$, por lo tanto

$$\sum_{\alpha_0 \in \mathbf{k}_r^\times} \psi(\alpha_0 u) = \sum_{\beta_0 \in \mathbf{k}_r^\times} \psi(\beta_0) = -\psi(\mathfrak{K}_p) = -1.$$

□

9.4. La demostración del teorema de Dwork

Empecemos por establecer el siguiente teorema, el cual puede ser entendido como una primera aproximación la tesis del teorema de Dwork desde un punto de vista analítico.

Teorema 9.4.1 *Toda función zeta $\mathcal{Z}(\mathcal{H}_{f(X)}, \mathbb{F}_q; T)$ define una función meromorfa p-ádica.*

Para demostrar este teorema empezaremos por verificar que este se cumple para la serie formal $\mathcal{Z}'(\mathcal{H}_{f(X)}, \mathbb{F}_q; T)$.

Lema 9.4.2 *Dados $\mathbb{F}_q$ un cuerpo finito y $f(X) \in \mathbb{F}_q[X_1, \ldots, X_n]$, la serie formal $\mathcal{Z}'(\mathcal{H}_{f(X)}, \mathbb{F}_q; T)$ define una función meromorfa $p-$ádica en $\mathbb{C}_p$.*

Demostración.- Supongamos que $q = p^r$ con $r \in \mathbb{N}$. Demostraremos este hecho en el caso que $\mathbb{F}_q = \widetilde{\mathbf{k}}_r$ y $\mathbb{F}_{q^s} = \widetilde{\mathbf{k}}_{sr}$, para todo $s \in \mathbb{N}$; todos estos cuerpos estan contenidos en $\mathfrak{K}_p$. Fijemos una raíz de p-ésima de la unidad $\epsilon \in \mathbb{C}_p$. Dado $s \in \mathbb{N}$, tomemos el $\mathbb{C}_p$-caracter ψ en $\mathbb{F}_{q^s}$ mencionado en el lema 9.3.3. Dados $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^s}^\times$, en virtud del corolario 9.3.6 se cumple que

$$\sum_{\alpha_0 \in \mathbb{F}_{q^s}} \psi\big(\alpha_0 f(\alpha_1, \ldots, \alpha_n)\big) = \begin{cases} q^s - 1 & , \ \text{si } (\alpha_1, \ldots, \alpha_n) \in \mathcal{H}'_{f(X)}(\mathbb{F}_{q^s}) \\ -1 & , \ \text{si } (\alpha_1, \ldots, \alpha_n) \notin \mathcal{H}'_{f(X)}(\mathbb{F}_{q^s}) \end{cases}$$

En consecuencia, sumando sobre todos las n-adas en $(\mathbb{F}_{q^s}^\times)^n$, obtenemos

$$\begin{aligned} \sum_{\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^s}^\times} \sum_{\alpha_0 \in \mathbb{F}_{q^s}} \psi\big(\alpha_0 f(\alpha_1, \ldots, \alpha_n)\big) &= (q^s - 1)\#\mathcal{H}'_{f(X)}(\mathbb{F}_{q^s}) + (-1)\#\big((\mathbb{F}_{q^s}^\times)^n \setminus \mathcal{H}'_{f(X)}(\mathbb{F}_{q^s})\big) \\ &= (q^s - 1)N'_s - \big((q^s - 1)^n - N'_s\big); \end{aligned}$$

por lo tanto

$$\sum_{\alpha_0,\alpha_1,\ldots,\alpha_n\in\mathbb{F}_{q^s}^{\times}} \psi\big(\alpha_0 f(\alpha_1,\ldots,\alpha_n)\big) = q^s N_s' - (q^s-1)^n. \tag{9.6}$$

Escribamos al polinomio $X_0 f(X_1,\ldots,X_n) \in \mathbb{F}_q[X_0,\ldots,X_n]$ como $\sum_u \beta_u X^u$, nótese que este polinomio no tiene término independiente. Luego, para $\alpha_0,\alpha_1,\ldots\alpha_n \in \mathbb{F}_{q^s}^{\times}$ se tiene que

$$\begin{aligned}\psi\big(\alpha_0 f(\alpha_1,\ldots,\alpha_n)\big) &= \psi\Big(\sum_u \beta_u \alpha_0^{u_0}\alpha_1^{u_1}\cdots\alpha_n^{u_n}\Big)\\ &= \prod_u \psi(\beta_u\alpha_0^{u_0}\alpha_1^{u_1}\cdots\alpha_n^{u_n}).\end{aligned}$$

Utilizando la función ζ del lema 6.6.6 y la serie analítica $\Theta(T)$ del lema 9.3.3, podemos expresar cada factor la siguiente forma

$$\begin{aligned}\psi(\beta_u\alpha_0^{u_0}\cdots\alpha_n^{u_n}) &= \prod_{i=0}^{rs-1}\Theta\big(\zeta(\beta_u\alpha_0^{u_0}\cdots\alpha_n^{u_n})^{p^i}\big)\\ &= \prod_{i=0}^{rs-1}\Theta\big((\zeta(\beta_u)\zeta(\alpha_0)^{u_0}\cdots\zeta(\alpha_n)^{u_n})^{p^i}\big)\\ &= \prod_{k=0}^{r-1}\prod_{j=0}^{s-1}\Theta\big((\zeta(\beta_u)^{p^{jr}})^{p^k}(\zeta(\alpha_0)^{u_0}\cdots\zeta(\alpha_n)^{u_n})^{p^{k+rj}}\big)\\ &= \prod_{k=0}^{r-1}\prod_{j=0}^{s-1}\Theta\big(\zeta(\beta_u)^{p^k}(\zeta(\alpha_0)^{u_0p^k}\cdots\zeta(\alpha_n)^{u_np^k})^{p^{rj}}\big),\end{aligned}$$

siendo esta última igualdad cierta porque $\zeta(\beta_u)$ es una raíz del polinomio $X^{p^r}-X \in \mathbb{Q}_p[X]$ (pues $\beta_u \in \mathbb{F}_{p^r}$). Como el índice u_0 de cada multindice u es igual a 1, podemos definir la serie formal

$$G_u(X) = \prod_{k=0}^{r-1}\Theta\big(\zeta(\beta_u)^{p^k}X_0^{p^ku_0}\cdots X_n^{p^ku_n}\big) \in \mathbb{C}_p[[X_0,X_1,\ldots,X_n]];$$

nótese que en el caso $\zeta(\beta_u)=0$, simplemente cada factor será 1 y $G_u(X)=1$. Gracias al lema 8.2.5, $G_u(X)$ converge en $(\zeta(\alpha_0)^{q^j},\zeta(\alpha_1)^{q^j},\ldots,\zeta(\alpha_n)^{q^j})$, para $j=0,1,\ldots,s-1$; más aun, la igualdad de arriba se transforma en

$$\psi(\beta_u\alpha_0^{u_0}\cdots\alpha_n^{u_n}) = \prod_{j=0}^{s-1}G_u(\zeta(\alpha_0)^{q^j},\zeta(\alpha_1)^{q^j},\ldots,\zeta(\alpha_n)^{q^j}).$$

Por lo tanto, para $\alpha_0,\alpha_1,\ldots,\alpha_n \in \mathbb{F}_{q^s}^{\times}$ se tendrá que

$$\begin{aligned}\psi\big(\alpha_0 f(\alpha_1,\ldots,\alpha_n)\big) &= \prod_u\prod_{j=0}^{s-1}G_u\big(\zeta(\alpha_0)^{q^j},\zeta(\alpha_1)^{q^j},\ldots,\zeta(\alpha_n)^{q^j}\big),\\ &= \prod_{j=0}^{s-1}G\big(\zeta(\alpha_0)^{q^j},\zeta(\alpha_1)^{q^j},\ldots,\zeta(\alpha_n)^{q^j}\big),\end{aligned}$$

donde $G(X) = \prod_u G_u(X) \in \mathbb{C}_p[[X]]$. Luego, la ecuación 9.6 se transforma en

$$\sum_{\alpha_0,\alpha_1,\ldots,\alpha_n \in \mathbb{F}_{q^s}^\times} \prod_{j=0}^{s-1} G\big(\zeta(\alpha_0)^{q^j}, \zeta(\alpha_1)^{q^j}, \ldots, \zeta(\alpha_n)^{q^j}\big) = q^s N_s' - (q^s-1)^n.$$

Como $\zeta(\mathbb{F}_{q^s}^\times) = \mathfrak{U}_p^{q^s-1}$ (por el lema 6.6.6), tendremos que

$$\sum_{w \in (\mathfrak{U}_p^{q^s-1})^{n+1}} \prod_{j=0}^{s-1} G(w^{p^{jr}}) = q^s N_s' - (q^s-1)^n;$$

veamos que podemos utilizar el lema 8.6.11 del capítulo anterior. De hecho, la primera propiedad de la serie formal $\Theta(X)$ enunciada en el lema 9.3.3 nos indica que $\Theta(X) \in \mathfrak{R}_p^1$. Por tanto, cada serie formal $G_u(X)$ también pertenece $\mathfrak{R}_p^n$, en consecuencia $G(X) \in \mathfrak{R}_p^n$ (por el lema 8.6.8). Luego, en virtud del lema 8.6.11, el operador lineal $\Psi = \Psi_{q,G(X)}$ satisface

$$(q^s-1)^{n+1}\mathrm{TR}(\Psi^s) = q^s N_s' - (q^s-1)^n;$$

lo cual se convierte en

$$N_s' = \sum_{j=0}^{n}(-1)^j\binom{n}{j}q^{s(n-j-1)} + \sum_{j=0}^{n+1}(-1)^j\binom{n+1}{j}q^{s(n-j)}\mathrm{TR}(\Psi^s). \tag{9.7}$$

Como Ψ sólo depende de q y $G(X)$, y este último de $\epsilon \in \mathfrak{U}_p^p$ y $f(X)$, concluimos que la ecuación 9.7 es valida para todo $s \in \mathbb{N}$. Luego, multiplicando por el monomio T^s/s y sumando sobre todo $s \in \mathbb{N}$ obtenemos que

$$\sum_{s=1}^{\infty} N_s' \frac{T^s}{s} = \sum_{j=0}^{n}(-1)^j\binom{n}{j}\Big(\sum_{s=1}^{\infty} q^{s(n-j-1)}\frac{T^s}{s}\Big) + \sum_{j=0}^{n+1}(-1)^j\binom{n+1}{j}\Big(\sum_{s=1}^{\infty} q^{s(n-j)}\mathrm{TR}(\Psi^s)\frac{T^s}{s}\Big);$$

componiendo con $\exp(X)$ y aplicando su propiedad respecto al producto, se consigue

$$\mathscr{Z}'(\mathcal{H}_{f(X)}, \mathbb{F}_q; T) = \prod_{j=0}^{n}\exp\Big(\sum_{s=1}^{\infty} q^{s(n-j-1)}\frac{T^s}{s}\Big)^{(-1)^j\binom{n}{j}} \cdot \prod_{j=0}^{n+1}\exp\Big(-\sum_{s=1}^{\infty} q^{s(n-j)}\mathrm{TR}(\Psi^s)\frac{T^s}{s}\Big)^{(-1)^{j+1}\binom{n+1}{j}}$$

Por otro lado, como $G(X) \in \mathfrak{R}_p^n$, tendremos que la representación matricial canonica A de Ψ cumple que $D(T) = \det(1 - AT) \in \mathbb{C}_p[[T]]$ posee radio de convergencia infinito y $D(T) = \exp(-\sum_{s=1}^{\infty} q^s \frac{T^s}{s})$, en virtud del lema 8.6.14 y el teorema 8.6.18. Utilizando la proposición 7.5.12 y realizando los intercambios respectivos concluimos que

$$\mathscr{Z}'(\mathcal{H}_{f(X)}, \mathbb{F}_q; T) = \prod_{j=0}^{n}(1 + q^{n-j-1}T)^{(-1)^j\binom{n}{j}} \prod_{j=0}^{n+1} D(q^{n-j}T)^{(-1)^{j+1}\binom{n+1}{j}};$$

por lo tanto $\mathscr{Z}'(\mathcal{H}_{f(X)}, \mathbb{F}_q; T)$ es el producto de potencias (positivas y negativas) de series formales con radio de convergencia infinito, y en consecuencia define una función meromorfa p-ádica. □

Demostración del teorema.- Procedamos a demostrar el lema por inducción sobre n (la dimensión de $\mathbb{F}_q^n$).

Empecemos en el caso $n = 1$. Dado $s \in \mathbb{N}$ tenemos que $\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) = \mathcal{H}'_{f(X)}(\mathbb{F}_{q^s}) \uplus (\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \cap \{0\})$. Como

$$\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \cap \{0\} = \begin{cases} \{0\} & , \text{ si } f(0) = 0 \\ \emptyset & , \text{ si } f(0) \neq 0 \end{cases},$$

vemos que $\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \cap \{0\} = \mathcal{H}_{f(X)}(\mathbb{F}_q) \cap \{0\}$, para todo $s \in \mathbb{N}$. Por lo tanto, denotando $\delta = \#\big(\mathcal{H}_{f(X)}(\mathbb{F}_q) \cap \{0\}\big)$ tendremos que

$$Y(T) = \exp\Big(\sum_{s=1}^{\infty} \#(\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \cap \{0\}) \frac{T^s}{s}\Big) = \exp\Big(\sum_{s=1}^{\infty} \delta \frac{T^s}{s}\Big) = \begin{cases} (1-T)^{-1} & , \text{ si } \delta = 1 \\ 1 & , \text{ si } \delta = 0 \end{cases},$$

luego, $Y(T)$ define una función meromorfa p-ádica. Puesto que $\mathscr{Z}'(\mathcal{H}_{f(X)}, \mathbb{F}_q; T) = \mathscr{Z}'(\mathcal{H}_{f(X)}, \mathbb{F}_q; T)\, Y(T)$, concluimos que el teorema es cierto para el caso $n = 1$.

Supongamos que el teorema es cierto para toda hipersuperficie afin en $\mathbb{F}_q^k$ con $k = 1, 2, \ldots, n$. Fijemos $s \in \mathbb{N}$. Notamos que

$$\begin{aligned} \mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \setminus \mathcal{H}'_{f(X)}(\mathbb{F}_{q^s}) &= \bigcup_{i=1}^{n} \{(\alpha_1, \ldots, \alpha_n) \in \mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \,;\, \alpha_i = 0\} \\ &= \bigcup_{i=1}^{n} \big(\mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \cap \mathcal{H}_{X_i}(\mathbb{F}_{q^s})\big) \end{aligned}$$

Tomemos $A_i^s = \mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \cap \mathcal{H}_{X_i}(\mathbb{F}_{q^s})$, para $i = 1, 2, \ldots, n$. Entonces

$$N_s - N'_s = \#\Big(\bigcup_{i=1}^{n} A_i^s\Big) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leq i_1 < \cdots < i_k \leq n} \#(A_{i_1}^s \cap \cdots \cap A_{i_k}^s);$$

esta última sumatoria se cumple para cualquier colección de finita de conjuntos (la cual es no dificil de demostrar por inducción sobre la cantidad de conjuntos). Para cada colección $1 \leq i_1 < \cdots < i_k \leq n$ se tiene que

$$\begin{aligned} A_{i_1}^s \cap \cdots \cap A_{i_k}^s &= \mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \cap \big(\mathcal{H}_{X_{i_1}}(\mathbb{F}_{q^s}) \cap \cdots \cap \mathcal{H}_{X_{i_k}}(\mathbb{F}_{q^s})\big) \\ &= \{(\alpha_1, \ldots, \alpha_n) \in \mathcal{H}_{f(X)}(\mathbb{F}_{q^s}) \,;\, \alpha_{i_1} = \cdots = \alpha_{i_k} = 0\}. \end{aligned}$$

Definamos $g_{i_1,\ldots,i_k}(X) \in \mathbb{F}_q[X_1, \ldots, X_{i_1-1}, X_{i_1+1}, \cdots, X_{i_k-1}, X_{i_k+1}, \cdots, X_n]$ como el polinomio que resulta de evaluar que resulta de evaluar $X_{i_1} = \cdots = X_{i_k} = 0$, noteśe que en el caso que $k = n$, el polinomio resultante es en realidad un elemento de $\mathbb{F}_q$. Luego, la función $\psi_{i_1,\ldots,i_k} : A_{i_1}^s \cap \cdots \cap A_{i_k}^s \to \mathcal{H}_{g_{i_1,\ldots,i_k}(X)}(\mathbb{F}_{q^s})$ que obvia las entradas $i_1, \ldots, i_k$ de los elementos

$(\alpha_1,\ldots,\alpha_n)$ es una biyección, para $1 \leq i_1 < \cdots < i_k \leq n$ con $k < n$. En el caso $k = n$, tendremos que

$$A^s_{i_1} \cap \cdots \cap A^s_{i_k} = \begin{cases} \{(0,\ldots,0)\} & ; \text{ si } f(0,\ldots,0) = 0 \\ \emptyset & ; \text{ si } f(0,\ldots,0) \neq 0 \end{cases};$$

de este modo $\#(A^s_{i_1} \cap \cdots \cap A^s_{i_k}) = \delta \subset \{0,1\}$, donde δ no depende de $s \in \mathbb{N}$.

Entonces, para cada $s \in \mathbb{N}$ obtenemos que

$$N_s - N'_s = \sum_{k=1}^{n-1}(-1)^{k+1}\Big(\sum_{1\leq i_1<\cdots<i_k\leq n} \#\mathcal{H}_{g_{i_1,\ldots,i_k}(X)}(\mathbb{F}_{q^s}))\Big) + (-1)^{n+1}\delta.$$

Multiplicando esta ecuación por el monomio T^s/s, sumando sobre $n \in \mathbb{N}$ y aplicando las propiedades de la exponencial concluimos que

$$\exp(\sum(N_s - N'_s)\frac{T^s}{s}) = \prod_{k=1}^{n-1}\Big(\big(\prod_{1\leq i_1<\cdots<i_k\leq n} \mathcal{Z}(\mathcal{H}_{g_{i_1,\ldots,i_k}(X)}, \mathbb{F}_q; T)\big)^{(-1)^{k+1}}\Big)\ell(T)^{(-1)^{n+1}},$$

donde $\ell(T) = \exp(-\delta\sum_{s=1}^{\infty} T^s/s)$, la cual definirá una función meroforma p-ádica. Luego, la hipótesis de inducción nos asegura que $Y(T) = \exp\big(\sum(N_s - N'_s)T^s/s\big) \in \mathbb{Q}[[T]]$ define una función meroforma p-ádica, lo cual nos permite concluir el teorema. □

Observación 9.4.3 En esta demostración hemos separado el caso de evaluar a $f(X)$ en $(0,\ldots,0)$, pues el conjunto $\mathcal{H}_{f(X)} \cap \{(0,\ldots,0)\}$ no puede ser visto como una hipersuperficie afin. Sin embargo, este conjunto podria ser vistoa como una hipersuperficie " 0-dimensional". El caso $k < n$ es dieferente, pues obtendemos polinomios de a lo más $n-k$ variables en en un espacio afín de dimensión exactamente $n-k$.

Comenzemos la demostración del teorema de Dwork denotando a $\mathcal{Z}(\mathcal{H}_{f(X)}, \mathbb{F}_q; T)$ por $Z(T)$. Por lo que acabamos de demostrar existen series formales $f(T), g(T) \in \mathbb{C}_p[[T]]$ tales que $g(T)Z(T) = f(T)$. Puesto que $Z(T) \in 1 + T\mathbb{C}_p[[T]]$, tendremos que $\omega_T\big(g(T)\big) = \omega_T\big(f(T)\big)$, por lo cual, si es necesario dividir entre una potencia de T, podemos suponer que $f(T)$ y $g(T)$ poseen coeficiente independiente no nulo. Más aun, como $Z(T)$ posee coeficiente independiente igual a 1, también podemos asumir que $f(T), g(T) \in 1 + T\mathbb{C}_p[[T]]$.

Tomando $R = q^{2n}$, tenemos que $R \in |\mathbb{C}_p^{\times}|_p$ y, en consecuencia, entonces $g(T) \in \mathfrak{A}_R$ (pues $g(T)$ converge en $\mathcal{D}[R]$). Luego, por el corolario 8.3.18 existirán $h(T) \in \mathbb{C}_p[T]$ y $l(T) \in \mathfrak{A}_R$ con coeficiente independiente igual a 1, tales que $l(T)g(T) = h(T)$; observamos que $h(T)$ tiene coeficiente independiente igual a 1.

Definamos $F(T) = l(T)f(T) \in 1 + T\mathbb{C}_p[[T]]$ que pertenecerá a $\mathfrak{A}_R$ (porque este conjunto es un anillo), entonces

$$F(T) = l(T)\big(g(T)Z(T)\big) = \big(l(T)g(T)\big)Z(T) = h(T)Z(T).$$

Escribamos $Z(T) = \sum a_s T^s$, $F(T) = \sum b_s T^s$ y $h(T) = \sum_{s=0}^{e} c_s T^s$, con $a_0 = b_0 = c_0 = 1$. Como $F(T) \in \mathfrak{A}_R$, existe $S \in \mathbb{N}$ tal que

$$s \geq S \quad \text{implica} \quad |b_s|_p < R^{-s}.$$

Tomemos $m = 2e + 1$ y, como en el lema 7.3.6, definamos las matrices $A_{s,m} = [a_{s+i+j}]_{0 \leq i,j \leq m}$ y $D_{s,m} = \det(A_{s,m})$ respecto a $Z(T)$, para todo $s \geq 0$ entero.

Comparando la igualdad de $F(T)$ y $h(T)Z(T)$ tenemos que

$$b_{j+e} = a_{j+e} + c_1 a_{j+e-1} + \cdots + c_e a_j \qquad \text{, para todo } j \geq 0.$$

Retomemos nuestra notación para las filas de $A_{s,m}$, expresando la i-ésima fila por $A_{s,m}^{(i)}$. Dado $s \geq 0$, tendremos que

$$[b_{s+j+e}, b_{s+j+e+1}, \ldots, b_{s+j+e+m}] = A_{s,m}^{(j+e)} - c_1 A_{s,m}^{(j+e-1)} - \cdots - c_e A_{s,m}^{(j)},$$

para $j = 0, 1, \ldots, m - e$. Realizando la operación elemental de sumarle la combinación lineal $-c_1 A_{s,m}^{(m-1)} - \cdots - c_e A_{s,m}^{(m-e)}$ a la última fila $A_{s,m}^{(m)}$, tendremos una matriz con el mismo determinante y con las mismas m primeras filas que A, pero con la última fila igual a $[b_{s+m}, b_{s+m+1}, \ldots, b_{s+2m}]$. Puesto que no han sido alteradas las anteriores filas a la m–ésima, podemos repertir el proceso para la $m-1$-ésima con sus e anteriores filas. Repitiendo estas operaciones elementales en este orden, lograremos obtener una matriz $B_{s,m} = [d_{i,j}]$ con determinante $D_{s,m}$ de la forma

$$B_{s,m} = \begin{pmatrix} & A_{s,m}^{(0)} & \\ & \vdots & \\ & A_{s,m}^{(e-1)} & \\ b_{s+e} & \cdots & b_{s+e+m} \\ & \vdots & \\ b_{s+m} & \cdots & b_{s+2m} \end{pmatrix}$$

Denotemos $M = \{0, 1, \ldots, m\}$. Puesto que $Z(T) \in \mathbb{Z}[[T]]$, se tiene que $|a_j|_p \leq 1$, para todo $j \geq 0$. En consecuencia, para todo $s \geq S$ se cumple que

$$\begin{aligned} |\det(B_{s,m})|_p &\leq \max_{\sigma \in \mathcal{S}_{m+1}(M)} \{|d_{0\sigma(0)} \cdots d_{m\sigma(m)}|_p\} \\ &= \max_{\sigma \in \mathcal{S}_{m+1}(M)} \{|a_{s+0+\sigma(0)}| \cdots |a_{s+e-1+\sigma(e-1)}|_p |b_{s+e+\sigma(e)}|_p \cdots |b_{s+m+\sigma(m)}|_p\} \\ &< \max_{\sigma \in \mathcal{S}_{m+1}(M)} \{R^{-(s+e+\sigma(e))} \ldots R^{-(s+m+\sigma(m))}\} \\ &\leq R^{-(s+e)} \ldots R^{-(s+m)}, \end{aligned}$$

puesto que $R > 1$; por lo tanto $|D_{s,m}|_p \leq R^{-s(m+1-e)}$. Reemplazando el valor de R, tendremos que

$$|D_{s,m}|_p \leq q^{-2ns(m+1-e)} = q^{-ns(m+3)}, \qquad \text{para todo } s \geq S. \tag{9.8}$$

Por otro lado, utilizando el valor absoluto tradicional $|\cdot|_\infty$ sobre $\mathbb{Q}$ y el lema 9.2.2 tendremos que

$$\begin{aligned} |\det(A_{s,m})|_\infty &\leq \sum_{\sigma \in \mathcal{S}_{m+1}(M)} |a_{s+0+\sigma(0)}|_\infty \cdots |a_{s+m+\sigma(m)}|_\infty \\ &< \sum_{\sigma \in \mathcal{S}_{m+1}(M)} q^{(s+0+\sigma(0))n} \ldots q^{(s+m+\sigma(m))n} \\ &\leq \sum_{\sigma \in \mathcal{S}_{m+1}(M)} q^{(s+2m)n} \ldots q^{(s+2m)n}, \end{aligned}$$

por lo tanto

$$|D_{s,m}|_\infty \leq (m+1)!\, q^{(m+1)(s+2m)n}, \text{ para todo } s \geq 0. \tag{9.9}$$

Luego, por las desigualdades (9.8) y (9.9), para $s \geq S$ se tiene que

$$|D_{s,m}|_\infty |D_{s,m}|_p \leq (m+1)!\, q^{(m+1)2mn} q^{(m+1)sn} q^{-(m+3)ns} = \frac{(m+1)! q^{(m+1)2mn}}{q^{2sn}}$$

Tomando $S_1 \in \mathbb{N}$ tal que $(m+1)!\, q^{(m+1)2mn} < q^{2S_1 n}$, para $s \geq \max\{S, S_1\}$ tendremos que $|D_{s,m}|_\infty |D_{s,m}|_p < 1$. Observando que todo entero $n \in \mathbb{Z}$ no nulo cumple que $|n|_p |n|_\infty \geq 1$; en consecuencia, $D_{s,m}$ debe de ser nulo (por el lema 5.1.6). Luego, por el lema 7.3.6 concluimos que $Z(T) \in \mathbb{Q}[[T]]$ es en realidad el cociente de polinomios en $\mathbb{Z}[T]$.

Bibliografía

[1] Cohen, H. "Number Theory, Volumen I: Tools and Diophantine Equations", New York: Springer, 2007.

[2] Niven, I. y Zuckerman, H., "Introducción a la teoría de los números", Limusa: Mexico,1969.

[3] Garcia, A. y Lequain, Y., "Elementos de lgebra", Projeto Euclides: IMPA, 2002.

[4] Mc Carthy, P. "Algebraic Extensions of Fields". U.S.A.: Blaisdell Publising Company, 1966.

[5] Herstein, I.N. "Topics in Algebra". Chicago: Blaisdell Publising Company, 1964.

[6] Lang, S. " Algebra". Madrid: Aguilar S.A., 1977 .

[7] Bromwich, "Introduction to the theory of Infinite Series". New York: Chelsea Publising Company, 1991.

[8] Cesar de Oliveira A., Pitombeira e Carvalho J., Pinto Carvalho PFernandez P., " Análise Combinatória e Probabilidad". Rio de Janeiro: SERGAC, 1991.

[9] Koblitz, N., " P-adic Numbers, p-adic analysis and zeta-functions". U.S.A.: Springer-Verlag, 1984.

[10] Neukirch, J., " Algebraic Number Theory ". Berlin: Springer-Verlag, 1999.

[11] Chavez, C., " Algebra Lineal ". Perú. Moshera, 2004.

[12] Robert, E., "An Introduction to Banach Space Theory".New York: Springer-Verlag, 1998

[13] Morandi, P."Fields and Galois Theory". U.S.A.: Springer-Verlag, 1996.

[14] Editores Choung, N., Egorov, Y. Khrennikov, A. Meyer,Y. y Mumford, D. "Harmonic, wavelet and p-adic analysis". Singapur: World Scientific Publishing, 2007.

[15] Vladimirov, V., Volovich, I. y Zelenov, E. "P-adic Analysis and Mathematical Physics". Singapur: World Scientific Publishing, 1994.

[16] Stepanov, S.A "Arithmetic of algebraic curves". U.S.A.: Plenum Publising corporation, 1995.

[17] Alain M., "A Course in p-adic Analysis". U.S.A.: Springer, 2000.