15
2ej

UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE CIENCIAS

"DESCOMPOSICION DE UN ANILLO G-ADICO"

T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C O

P R E S E N T A :

MIGUEL ANGEL JIMENEZ BELTRAN

México, D.F. 1994

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

CIUDAD UNIVERSITARIA

UNIVERSIDAD NACIONAL AVENTMA DE MEXICO

FACULTAD DE CIENCIAS
División de Estudios Profesionales
Exp. Núm. 55

M. EN C. VIRGINIA ABRIN BATULE
Jefe de la División de Estudios Profesionales
Universidad Nacional Autónoma de México.
P r e s e n t e .

Por medio de la presente, nos permitimos informar a Usted, que habiendo revisado el trabajo de tesis que realiz a el pasante
MIGUEL ANGEL JIMENEZ BELTRAN
con número de cuenta 8351581-9 con el título:
"Descomposición de un anillo g-ádico

Consideramos que reune los méritos necesarios para que pueda continuar el trámite de su Examen Profesional para obtener el título de - MATEMATICO .

GRADO NOMBRE Y APELLIDOS COMPLETOS	FIRMA
M. EN C. MARIO PINEDA RUELAS Director de Tesis	
DR. FELIPE ZALDIVAR CRUZ	
M. EN C. ALEJANDRO BRAVO MOJICA	
MAT. JULIO CESAR GUEVARA BRAVO Suplente	
M. EN C. PABLO MENDOZA ITURRALDE Suplente	

Ciudad Universitaria, D.F., a 21 de febrero de 199 4

Descomposición de un anillo g-ádico

Miguel Angel Jiménez Beltran

Junio de 1994

Una piedra en el camino
me enseño que mi destino
era rodar y rodar.
Después me dijo un arriero
que no hay que llegar primero
pero hay que saber llegar...

José Alfedo Jiménez S.

A mi gran José Alfedo Jiménez
como un ejemplo...
A mi Padre el Señor Teodoro Jiménez M.
a mi Madre la Señora Catalina Beltran de Jiménez
como agradecimiento...

A mis hermanos Luis Rey, Alejandra, Graciela y David
como complemento...

Al M. en C. Mario Pineda R. por sus consejos y enseñanzas
gracias...

Sería imposible nombrar a cada pesonaje que ha hecho presente su afecto, su comprensión, su apoyo. Es por eso que dedico está tesis a todas las personas que directamente conviven cada uno de mis días...

Contenido

Introducción

Kurt Hensel estudió matemáticas en Bonn y Berlín, fué discípulo de *Rudolf Lipschitz*, *Karl Weierstrass*, *Carl Borchardt*, *Gustav Kirchhoff*, *Herman von Helmholtz* y principalmente de *Leopold Kronecker*, obteniendo con él su doctorado. Al morir *Kronecker*, *Hensel* se dedica muchos años preparando la edición de sus artículos que ha coleccionado. Posteriormente en cooperación con *G. Llandsberg*, *Hensel* publica su primer y más importante libro *Theorie der algebraischen Funktionen* (1902). En 1901 siendo *Hensel* profesor de la Universidad de Marbur escribe otros dos libros también muy importantes, *Theorie der algebraischen Zahlen* y *Zahlentheorie*.

El trabajo científico de *Hensel* se basó principalmente en la Teoría aritmética de Campos de Números Algebraicos de *Kronecker*. El método de *Kronecker – Hensel* también aportó fundamentos de aritmética en Campos de funciones algebráicas, estos fundamentos se desarrollaron posteriormente en *Theorie der algebraischen Funktionen*. Aproximadamente en 1899, *Hensel* deduce el método de Weierstrass de series de potencias desarrollado para funciones algebráicas y con ello interpretá una teoría análoga de números algebraicos: los números p-ádicos.

Los números p-ádicos se considerarón como su gran descubrimiento. Considerando el método de series de potencias para funciones algebráicas, uno puede pensar que no existe su fundamento conceptual para su desarrollo, por el contrario *Hensel* aportó el estímulo decisivo para el incremento de nociones de álgebra abstracta que se requieren para ese fundamento: la teoría de campos valuados. En sus libros *Theorie der algebraischen Zahlen* y *Zahlentheorie*, *Hensel* desarrollo números p-ádicos en una teoría sistemática y dió una aplicación de gran interés -la clásica teoría de formas cuadráticas- además de una intersante extensión de su método p-ádico para la introducción del análisis p-ádico. Posteriormente los pupilos de *Hensel*, principalmente *Helmut Hasse* probaron de manera satisfactoria el método p-ádico para formas cuadráticas y en la teoría de álgebras sobre campos numericos, que se conoce actualmente como el principio local-global. El método de *Hensel* propició bastantes resultados interesantes en la teoría de números, que posteriormente fueron publicados en un gran número de articulos. Los primeros números p-ádicos que construyó se consideraron , en general, de poca relevancia, pero él vivió para ver su reconocimiento como un elemento matemático ampliamente generalizable.

En estas notas se proporciona una introducción elemental a la teoría de los números p-ádicos y analisis p-ádico. En muchos libros de álgebra y teoría de números, se tiene poca información al respecto, y no parece existir una buena introducción a los números p-ádicos desde el punto de vista del estilo del análisis elemental.

El objetivo principal de este trabajo es descomponer un anillo g-ádico como suma directa de campos p-ádicos.

En el capítulo uno se definen los números g-ádicos y se estudian las pseudo-valuaciones. Se finaliza con una construcción de la representación canónica de números racionales como números g-ádicos.

En el capítulo dos se construyen los anillos g-ádicos y los campos p-ádicos vía sucesiones de la misma manera que se construye $\mathbb{R}$ a partir de $\mathbb{Q}$.

En el capítulo tres probamos que $\mathbb{Q}_g$ no es un campo si g al menos tiene dos factores primos distintos. Tomando en cuenta que en $\mathbb{Q}$ se tienen definidas las pseudo-valuaciones $|\ |_g$ y las valuaciones $|\ |_p$, entonces sus completaciones son $\mathbb{Q}_g$ y $\mathbb{Q}_p$ respectivamente.

En el capítulo cuatro se estudia la aritmética de $\mathbb{Q}_g$ por medio de las series canónicas.

En el capítulo cinco se estudia la estructura de $\mathbb{Q}_g$ para el caso de $g \geq 2$ y se muestra que este anillo es la suma directa de campos p-ádicos.

Capítulo 1

Valor g-ádico de números racionales

En este capítulo estudiaremos la función g-ádica para números racionales, tomando en cuenta las propiedades de valuación o pseudo-valuación, así como la construcción de una representación para ellos denominada serie canónica.

Lema 1 *Sean $G, r, s \in \mathbf{Z}$ tales que $G \geq 2$, $s \geq 1$ y $(G, s) = 1$, entonces existe un único par de enteros A y R tal que*

$$\frac{r}{s} = A + \left(\frac{GR}{s}\right) \qquad 0 \leq A \leq G - 1$$

Demostración: Prueba de Existencia. Como $(G, s) = 1$ entonces existen $x, y \in \mathbf{Z}$ tal que $Gy + sx = 1$, multiplicamos por r

$$rGy + rsx = r$$

le sumamos $skG - skG$

$$rGy + rsx + skG - skG = r$$

factorizamos s y G

$$s(rx - kG) + G(ry + ks) = r$$

donde k es un entero tal que

$$0 \leq (rx - kG) \leq G - 1.$$

El entero k existe por el Principio de Arquímides. Sea $A = rx - kG$ y $R = ry + ks$, entonces

$$r = sA + GR$$

donde

$$0 \leq A \leq G - 1$$

Por lo tanto

$$\frac{r}{s} = A + \left(\frac{GR}{s}\right)$$

es la expresión buscada.

Prueba de Unicidad. Suponemos que existen A' y R' tal que $0 \leq A' \leq G - 1$ y $r/s = A' + (\frac{GR'}{s})$. Por el resultado anterior

$$\frac{r}{s} = A + \left(\frac{GR}{s}\right)$$

y

$$\frac{r}{s} = A' + \left(\frac{GR'}{s}\right)$$

igualando tenemos

$$sA' + GR' = sA + GR$$

así que

$$s(A - A') = G(R - R').$$

Pero $(G, s) = 1$ entonces $G \mid (A - A')$. Por otro lado $0 \leq A \leq G - 1$ y $0 \leq A' \leq G - 1$, de donde $-(G-1) \leq (A - A') \leq (G-1)$. De lo anterior se sigue que $A = A'$ y $R = R'$.

◇

Lema 2 *Sean r, s y $g \in \mathbb{Z}$ tales que $r \neq 0$; $s \geq 1$, $g \geq 2$ y $(r, s) = 1$ entonces, existe un único entero f y otro par R y S tal que*

$$g^f \frac{r}{s} = \frac{R}{S}$$

donde $g \nmid R$, $(R, S) = (g, S) = 1$

Demostración: Si $g \mid r$ entonces $r = gt = g^{-\phi} t_0$ donde $g^\phi \mid r$ y $g^{\phi+1} \nmid r$ (Teorema Fundamental de la Aritmética). Llamemos $R = g^{-\phi} r$; $S = s$ entonces

$$R = g^{-\phi} r = g^{-\phi}(g^\phi t_0) = (g^{-\phi} g^\phi) t_0 = t_0$$

donde $f = -\phi < 0$ entonces

$$\frac{R}{S} = g^{-\phi} \frac{r}{s} = g^{-\phi} \frac{r}{s}$$

además $g \nmid R$. Ahora supongamos que $g | R$; como $R = t_0$ entonces $g | t_0$, lo que quiere decir que $t_0 = g r_0$. Por lo tanto

$$r = g^\phi t_0 = g^\phi (g r_0) = g^{\phi+1} r_0$$

entonces $g^{\phi+1} \mid r$ con lo que llegamos a una contradicción y por tanto $g \nmid R$.

Si $(R, S) = d$ entonces $d \mid R$ y $d \mid S$ y como $R = g^{-\phi} r$ y $r = g^\phi t_0$ entonces $d \mid t_0$ lo que implica que $d \mid g^\phi t_0 = r$, en particular como $d \mid S$, $d \mid r$ y $S = s$, $d \mid s x_0 + r y_0 = 1$. Por lo tanto $d = 1$. Ahora si $(g, s) = d$ entonces $d \mid g$ y $d \mid S$, pero si $d \mid g$ y $g \mid r$ entonces $d \mid r$. Por lo tanto $d \mid S$ y $d \mid r$ y como $S = s$ entonces $d \mid s x_0 + r y_0 = 1$ entonces $d = 1$. Concluyendo tenemos que

$$\frac{r}{s} = g^{-f} \left(\frac{R}{S} \right)$$

donde $g \nmid R$ y $(R, S) = (g, S) = 1$

◇

Definición 1 *Si la notación es como en el Lema 2 y si $a = \frac{r}{s}$ de modo que $a \neq 0$ entonces ponemos*

$$|a|_g = g^f \qquad |0|_g = 0$$

la función así definida $|a|_g = g^f$ de a se llama valor g-ádico de a.

Observación 1 *$|\ |_g$ tiene la propiedad de ser una función par, es decir, $|-x|_g = |x|_g$ para $x \in \mathbb{Q}$.*

Definición 2 *Sea $a = \frac{r}{s} \in \mathbb{Q}$, a es un entero g-ádico si $|a|_g \leq 1$.*

Teorema 1 *La desigualdad $\left| \frac{r}{s} \right|_g \leq 1$ se satisface si y sólo si $(g, s) = 1$*

Demostración: Supongamos que $(g, s) = 1$. Haremos la prueba de esta implicación en dos casos:

CASO I.- Suponemos que $g | r$ y $g \nmid s$ entonces $r = g^t t$; $s = g^\alpha q$, entonces $\frac{r}{s} = \frac{g^t t}{g^\alpha q}$,o bien, $\frac{r}{s} = g^{t-\alpha} \frac{t}{q}$ si $(g, s) = 1$, la máxima potencia de g que divide a s es cero; entonces $\alpha = 0$ y $\frac{r}{s} = g^{t-0} \frac{t}{q} = g^t \frac{t}{s}$. Por el lema anterior y la definición

$$\left| \frac{r}{s} \right|_g = g^{-t} = \frac{1}{g^t} < 1$$

CASO II.- Suponemos que $g \nmid r$ y $g \nmid s$; la máxima potencia de g que divide a r y s es cero (para este caso l y α són cero) $\frac{r}{s} = \frac{g^0 r}{g^0 s} = g^0 \frac{r}{s}$. Por el lema anterior y la definición

$$\left|\frac{r}{s}\right|_g = 1.$$

Supongamos ahora que $\left|\frac{r}{s}\right|_g \leq 1$, nuevamente haremos la prueba en dos casos y en ambos suponemos que $(g, s) = 1$.

CASO I.- Si $g \mid r$ entonces $r = g^l t$ donde $l > 0$ y como $(g, s) = 1$ tenemos $\frac{r}{s} = g^l \frac{t}{s}$. Por el lema anterior

$$\left|\frac{r}{s}\right|_g = g^{-l} = \frac{1}{g^l} < 1.$$

CASO II .- Si $g \nmid r$ entonces la máxima potencia de g que divide a r es cero $\frac{r}{s} = g^0 \frac{r}{s}$, entonces $\left|\frac{r}{s}\right|_g = 1$.

Concluyendo de ambos casos obtenemos que:

$$(g, s) = 1 \iff \left|\frac{r}{s}\right|_g \leq 1$$

◇

Corolario 1 *Sea $a \in \mathbb{Q}$, entonces se cumple:*

i) $|a|_g = 1 \iff a = \frac{r}{s}; \quad g \nmid r; \quad (g, s) = 1$

ii) $|a|_g = g^l \iff |ag^l|_g = 1$

iii) Para cualquier $n \in \mathbb{Z}$ tenemos

$$|ag^n|_g = |a|_g g^{-n}$$

Demostración: *(i)* La afirmación se sigue al considerar $a = \frac{r}{s}$. Para *(ii)* si $|a|_g = g^l$, por el Lema anterior $a = g^{-l}(\frac{R}{S})$, si multiplicamos por g^l ambos lados tenemos

$$g^l a = g^l g^{-l} \left(\frac{R}{S}\right) = g^0 \left(\frac{R}{S}\right) = \frac{R}{S}$$

entonces

$$|ag^l|_g = 1.$$

De la definición se sigue que

$$g^l a = 1 \left(\frac{R}{S}\right) \iff a = g^{-l} \left(\frac{R}{S}\right)$$

y por lo tanto

$$|a|_g = g^l$$

Para *(iii)* la solución es obvia cuando $a = 0$. Si $n = 0$ estamos en el caso anterior. Excluyendo este caso, sea $|a|_g = g^l$ entonces $a = g^{-l}(\frac{R}{S})$ y multiplicando por g^n

$$g^n a = g^n g^{-l} \frac{R}{S} = g^{n-l} \frac{R}{S} \iff |ag^n|_g = g^{-n+l} \qquad \text{pero} \qquad |a|_g = g^l$$

entonces

$$|ag^n|_g = |a|_g g^{-n}.$$

◇

Definición 3 $|\ |_g$ *es* no-Arquimediana *si ocurre*

$$|a+b|_g \leq \max\{|a|_g, |b|_g\}$$

para todos $a, b \in \mathbb{Q}$ *y* Arquimediana *si*

$$|a+b|_g \leq |a|_g + |b|_g$$

Observación 2 *Notemos que no-Arquimediana implica Arquimediana pero no en sentido opuesto. El valor g-ádico es ejemplo de función no-Arquimediana y el valor absoluto en* $\mathbb{Q}$ *es un ejemplo de función Arquimediana.*

Teorema 2 *Sea* $a, b \in \mathbb{Q}$, *tal que* $a = \frac{r}{s} < b = \frac{p}{q}$, *entonces*

i) $|a|_g < |b|_g$ *si* $g|r \quad g \nmid p$

ii) $|a|_g > |b|_g$ *si* $g \nmid r \quad g|p$

iii) $|a|_g = |b|_g$ *si* $g \nmid r \quad y \quad g \nmid p$

Demostración: Supongamos que a y b son números g-ádicos definidos como en el Lema 2, es decir, $a = \frac{r}{s} = g^n \frac{R}{S}$ tal que $g \nmid R$ y $(g,S) = 1$, $b = \frac{p}{q} = g^m \frac{P}{Q}$ tal que $g \nmid P$ y $(g,Q) = 1$ $|a|_g = g^{-n} \leq 1$ y $|b|_g = g^{-m} \leq 1$.

i) Si $g|r$ y $g \nmid p$ tenemos

$$\frac{r}{s} = g^n \frac{R}{S} \implies \left|\frac{r}{s}\right|_g = g^{-n}$$

$$\frac{p}{q} = g^{-h} \frac{P}{Q} \implies \left|\frac{p}{q}\right|_g = g^h$$

entonces

$$|a|_g < |b|_g \quad si \quad g|r \quad g \nmid p$$

ii) Ahora si $g \nmid r$ y $g|p$ tenemos

$$\frac{r}{s} = g^{-i} \frac{r}{S} \implies \left|\frac{r}{s}\right|_g = g^i$$

$$\frac{p}{q} = g^m \frac{P}{Q} \implies \left|\frac{p}{q}\right|_g = g^{-m}$$

entonces

$$|a|_g > |b|_g \quad si \quad g \nmid r \quad g|p$$

iii) Consideremos el caso cuando $g \nmid r$, $g \nmid p$ y además $(g,s) = (g,q) = 1$

$$\frac{r}{s} = g^0 \frac{r}{s} \implies \left|\frac{r}{s}\right|_g = g^0 = 1$$

$$\frac{p}{q} = g^0 \frac{p}{q} \implies \left|\frac{p}{q}\right|_g = g^0 = 1$$

entonces

$$|a|_g = |b|_g \quad si \quad g \nmid r \quad g \nmid p$$

para este caso si s y q fueran divididas por g no podríamos determinar la desigualdad.

◇

Teorema 3 *Sean* a *y* $b \in \mathbb{Q}$ *y*

$$|a|_g = g^n \qquad |b|_g = g^m$$

entonces se cumple

$$|a \pm b|_g \leq \max\{|a|_g, |b|_g\}$$

Demostración: Sabemos que si $|a|_g = g^n$ y $|b|_g = g^m$ entonces $a = \frac{r}{s} = g^{-n}\frac{R}{S}$ con $g \nmid R$ y $(g,S) = 1$, $b = \frac{p}{q} = g^{-m}\frac{P}{Q}$ con $g \nmid P$ y $(g,Q) = 1$. La prueba es en dos casos.

CASO I.- Suponemos que $-n < -m$ (es decir, que existe un $r \in \mathbb{N}$ tal que $-n + r = -m$) entonces lo que hay que demostrar es $a + b = g^k\frac{L}{M}$ con $g \nmid L$ y $(g,M) = 1$. Entonces

$$\begin{aligned} a+b &= g^{-n}\frac{R}{S} + g^{-m}\frac{P}{Q} = g^{-n}\frac{R}{S} + g^{-n+r}\frac{P}{Q} \\ &= g^{-n}\left(\frac{R}{S} + g^r\frac{P}{Q}\right) = g^{-n}\left(\frac{RQ + g^rPS}{SQ}\right) \end{aligned}$$

Aseguramos que $(g, SQ) = 1$ y $g \nmid RQ + g^rPS$. Sea

$$k = -n \quad ; \quad L = (RQ + g^rPS) \quad ; \quad M = SQ$$

entonces

$$a + b = g^{-n}\left(\frac{RQ + g^rPS}{SQ}\right)$$

$$|a+b|_g = g^n = |a|_g$$

Si hubiéramos supuesto que $-m < -n$ entonces concluiríamos que

$$|a+b|_g = g^m = |b|_g$$

Por lo tanto

$$|a \pm b|_g = \max\{|a|_g, |b|_g\}.$$

CASO II.- Supongamos ahora que $-n = -m$, haciendo el mismo desarrollo tenemos

$$a + b = g^{-n}\left(\frac{RQ + PS}{SQ}\right)$$

donde $(g, SQ) = 1$ pero g puede dividir a $RQ + PS$.

Supongamos que $g \mid RQ + PS$ entonces $RQ + PS = g^rT$ y $r > 0$ donde $g \nmid T$ y $(g,T) = 1$ (si $r = 0$ estamos en el Caso I)

$$a + b = g^{-n}\left(\frac{RQ + PS}{SQ}\right) = g^{-n}\left(g^r\frac{T}{SQ}\right) = g^{-n+r}\frac{T}{SQ}$$

$$a + b = g^{-n+r}\frac{T}{SQ}$$

entonces

$$|a+b|_g = g^{n-r}$$

pero

$$n - r < n$$

entonces

$$g^{n-r} < g^n$$

Por lo tanto

$$|a+b|_g = g^{n-r} < g^n = |a|_g$$

o bien,

$$|a+b|_g = g^{m-r} < g^m = |b|_g$$

◇

Teorema 4 *Sean $a_1, a_2, a_3, \ldots a_n$ números racionales cualesquiera, entonces*

$$|a_1 + a_2 + a_3 + \ldots + a_n|_g \leq \max\{|a_1|_g, |a_2|_g, |a_3|_g, \ldots, |a_n|_g\}$$

Demostración: Inducción sobre n. Si $n = 2$ por el teorema anterior se sigue el resultado. Supongamos que el teorema es cierto para $\{a_1, a_2, \ldots, a_{n-1}\}$, es decir,

$$|a_1 + a_2 + \ldots + a_{n-1}|_g \leq \max\{|a_1|_g, |a_2|_g, \ldots, |a_{n-1}|_g\}$$

Tomemos ahora los $\{a_1, a_2, \ldots, a_{n-1}, a_n\}$. Sabemos que si $a_1+a_2+\cdots+a_{n-1} = \frac{h}{j} = g^{-s}\frac{H}{J}$ con $g \nmid H$ y $(g, J) = 1$ y $a_n = \frac{l}{m} = g^{-t}\frac{L}{M}$ con $g \nmid L$ y $(g, M) = 1$ hacemos $a_1+a_2+\cdots+a_{n-1}+a_n = \frac{h}{j} + \frac{l}{m} = g^{-s}\frac{H}{J} + g^{-t}\frac{L}{M} = g^{-(s+t)}\frac{HM + JL}{JM}$ a partir de aquí la prueba es análoga a la que se realizó en el Teorema 3, es decir, separando en dos casos y tomando en cuenta los exponentes de g.

Por lo tanto

$$|a_1 + a_2 + a_3 + \ldots + a_n|_g \leq \max\{|a_1|_g, |a_2|_g, |a_3|_g, \ldots, |a_n|_g\}$$

◇

Corolario 2 *Sea $|a|_g$ el valor g-ádico de a y $n \in \mathbf{N}$ entonces*

$$|na|_g \leq |a|_g$$

Demostración: Del teorema anterior sean $a_1 = a_2 = a_3 = \cdots = a_n$ entonces

$$|a_1 + a_2 + \ldots + a_n|_g \leq \max\{|a_1|_g, |a_2|_g, \ldots, |a_n|_g\}$$

$$|na_1|_g \leq \max\{|a_1|_g\}$$

Por lo tanto $|na|_g \leq |a|_g$

◇

Definición 4 *Sean $a, b \in \mathbf{Q}$ entonces $|\ |_g$ es* pseudo-valuación *si ocurre*

$$|ab|_g \leq |a|_g\,|b|_g$$

y valuación *si*

$$|ab|_g = |a|_g\,|b|_g$$

Teorema 5 *Sean a y $b \in \mathbf{Q}$ y*

$$|a|_g = g^n \quad , \quad |b|_g = g^m$$

entonces

$$|ab|_g \leq |a|_g\,|b|_g$$

Demostración: Sabemos que si $|a|_g = g^n$ y $|b|_g = g^m$ entonces $a = \frac{r}{s} = g^{-n}\frac{R}{S}$ tal que $g \nmid R$ y $(g, S) = 1$ y $b = \frac{p}{q} = g^{-m}\frac{P}{Q}$ tal que $g \nmid P$ y $(g, Q) = 1$. Para está demostración, como en anteriores, lo haremos en dos casos.

CASO I.- Hagamos el producto de a y b substituyendo su valor

$$ab = g^{-n}g^{-m}\frac{R}{S}\frac{P}{Q} = g^{-n-m}\frac{RP}{SQ},$$

entonces $(g, SQ) = 1$.

Supongamos que $g \nmid RP$, así

$$ab = g^{-(n+m)}\frac{RP}{SQ}$$

donde $g \nmid RP$ y $(g, SQ) = 1$. Por tanto

$$|ab|_g = g^{n+m} = g^n g^m = |a|_g\,|b|_g.$$

CASO II.- Para este caso suponemos que $g|RP$, es decir, $RP = g^t M$ puesto que lo demás es análogo

$$ab = g^{-n-m}\frac{RP}{SQ} = g^{-(n+m)}g^t\frac{M}{SQ} = g^{-(n+m)+t}\frac{M}{SQ}$$

donde t es la máxima potencia de g que divide a M, es decir, $g \nmid M$

$$\begin{aligned} |ab|_g &= g^{n+m-t} = g^n g^m g^{-t} \\ &= |a|_g\,|b|_g\,g^{-t} \\ &= |a|_g\,|b|_g\,\frac{1}{g^t} < |a|_g\,|b|_g \end{aligned}$$

Por lo tanto

$$|ab|_g < |a|_g\,|b|_g$$

◇

Corolario 3 *Si p es primo, entonces*

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

Demostración: Sabemos que si $|a|_p = p^n$ y $|b|_p = p^m$ entonces $a = \frac{r}{s} = p^{-n}\frac{R}{S}$ tal que $p \nmid R$ y $(p,S) = 1$ y $b = \frac{x}{q} = p^{-m}\frac{X}{Q}$ tal que $p \nmid X$ y $(p,Q) = 1$.

Tomemos el Caso I de la demostración anterior

$$ab = p^{-n}p^{-m}\frac{RX}{SQ} = p^{-n-m}\frac{RX}{SQ}$$

de aquí que $(p, SQ) = 1$ y además que $p \nmid RX$ entonces

$$|ab|_p = p^{n+m} = p^n p^m = |a|_p\,|b|_p$$

Por lo tanto

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

◇

Observación 3 *La función valor g-ádico $|\ |_g$ es una* pseudo-valuación no-Arquimediana.

Teorema 6 *Sea a un entero g-ádico y $n \in \mathbb{N}$, entonces existen únicos A_n y r_n tales que*

$$a = A_n + g^n\frac{r_n}{s} \qquad , \qquad 0 \le A_n \le g^n - 1$$

con

$$|a - A_n|_g \le g^{-n}$$

y

$$\left|\frac{r_n}{s}\right|_g \le 1$$

Demostración: Aplicamos el Lema 1 con $G = g^n$ para obtener que

$$a = A_n + g^n\frac{r_n}{s} \qquad 0 \le A_n \le g^n - 1$$

Si $g \nmid r_n$ entonces claramente $|a - A_n|_g = g^{-n}$. Ahora si $g|r_n$ entonces r_n es de la forma $r_n = g^m t$ con $(g,t) = 1$ y además $a - A_n = g^{n+m}\frac{t}{s}$. Por tanto

$$|a - A_n|_g \le g^{-(n+m)} < g^{-n}$$

Ahora $a = A_n + g^n \frac{r_n}{s}$, $\quad 0 \leq A_n \leq g^n - 1$ y

$$|g^{-n}(a - A_n)|_g = \left|\frac{r_n}{s}\right|_g$$

Usando (iii) del Corolario 1, $g^n |a - A_n|_g = \left|\frac{r_n}{s}\right|_g$, entonces $\left|\frac{r_n}{s}\right|_g = g^n |a - A_n|_g \leq g^n g^{-n} = 1$. Por lo tanto

$$\left|\frac{r_n}{s}\right|_g \leq 1$$

Para n fija $\quad a = A_n + g^n \frac{r_n}{s} = a_0 + a_1 g + a_2 g^2 + cdots + g^n \frac{r_n}{s}$, donde

$$\begin{aligned}
A_0 &= 0 \\
A_1 &= A_0 + a_0 \\
A_2 &= A_1 + a_1 g = a_0 + a_1 g \\
A_3 &= A_2 + a_2 g^2 = a_0 + a_1 g + a_2 g^2 \\
&\vdots \\
A_n &= A_{n-1} + a_{n-1} g^{n-1} = a_0 + a_1 g + a_2 g^2 + \ldots + a_{n-1} g^{n-1}
\end{aligned}$$

y $\quad 0 \leq a_{n-1} \leq g - 1$

◇

Teorema 7 *La representación de A_n es única.*

Demostración: Suponemos que existen A_n y A'_n tales que

$$\begin{aligned}
A_n &= a_0 + a_1 g + a_2 g^2 + \ldots + a_{n-1} g^{n-1} \\
A'_n &= a'_0 + a'_1 g + a'_2 g^2 + \ldots + a'_{n-1} g^{n-1}
\end{aligned}$$

igualamos A_n y A'_n y tenemos

$$\begin{aligned}
& a_0 + a_1 g + a_2 g^2 + \ldots + a_{n-1} g^{n-1} = a'_0 + a'_1 g + a'_2 g^2 + \ldots + a'_{n-1} g^{n-1} \\
0 &= (a_0 + a_1 g + a_2 g^2 + \ldots + a_{n-1} g^{n-1}) - (a'_0 + a'_1 g + a'_2 g^2 + \ldots + a'_{n-1} g^{n-1}) \\
0 &= a_0 + a_1 g + a_2 g^2 + \ldots + a_{n-1} g^{n-1} - a'_0 - a'_1 g - a'_2 g^2 - \ldots - a'_{n-1} g^{n-1} \\
0 &= (a_0 - a'_0) + (a_1 - a'_1) g + (a_2 - a'_2) g^2 + \ldots + (a_{n-1} - a'_{n-1}) g^{n-1}
\end{aligned}$$

Aplicamos el valor g-ádico y tomando el resultado del Teorema 3 tenemos

$$\begin{aligned}
|0|_g &= \left|(a_0 - a'_0) + (a_1 - a'_1) g + (a_2 - a'_2) g^2 + \ldots + (a_{n-1} - a'_{n-1}) g^{n-1}\right|_g \\
0 &= \left|(a_0 - a'_0) + (a_1 - a'_1) g + (a_2 - a'_2) g^2 + \ldots + (a_{n-1} - a'_{n-1}) g^{n-1}\right|_g \\
&\leq \max\{|(a_0 - a'_0)|_g, |(a_1 - a'_1) g|_g, |(a_2 - a'_2) g^2|_g, \ldots, |(a_{n-1} - a'_{n-1}) g^{n-1}|_g\}
\end{aligned}$$

como cada $(a_i - a'_i) g^i$ es distinto ; para $1 \leq i \leq n-1$, entonces

$$\max\{|(a_0 - a'_0)|_g, |(a_1 - a'_1) g|_g, |(a_2 - a'_2) g^2|_g, \ldots, |(a_{n-1} - a'_{n-1}) g^{n-1}|_g\} = 0$$

así $|(a_i - a'_i) g^i|_g = 0$ para $1 \leq i \leq n-1$ que implica $(a_i - a'_i) g^i = 0$ pero $g^i \neq 0$ entonces $(a_i - a'_i) = 0$ y de aquí $a_i = a'_i$ para $1 \leq i \leq n-1$ y llegamos a una contradicción porque habíamos supuesto que A_n y A'_n eran diferentes. Por lo tanto A_n es única.

◇

A continuación estudiaremos una representación para $a \in \mathbb{Q}$ donde $|a|_g > 1$.

Teorema 8 *Sea $a \in \mathbb{Q}$ tal que $|a|_g > 1$, entonces a se puede expresar como*

$$a = a_{-f}g^{-f} + a_{-f+1}g^{-f+1} + \ldots + a_0 + a_1 g + \ldots + g^n \frac{R_{f+n}}{S}$$

Demostración: Si $a = g^{-f}\dfrac{R}{S}$, entonces

$$a = g^{-f}\frac{R}{S} \Longrightarrow ag^f = \frac{R}{S}$$

Por el Corolario 1, $\left|\dfrac{R}{S}\right|_g = |ag^f|_g = 1$ entonces $\dfrac{R}{S}$ es un entero g-ádico. Para cada N por el Teorema 6 tenemos $a = A_n + g^n\dfrac{r_n}{s}$ entonces

$$\frac{R}{S} = b_0 + b_1 g + b_2 g^2 + \ldots + b_{N-1}g^{N-1} + g^N\left(\frac{R_N}{S}\right)$$

Regresando al Lema 2

$$\begin{aligned} a &= g^{-f}\frac{R}{S} = g^{-f}\left(b_0 + b_1 g + b_2 g^2 + \ldots + b_{N-1}g^{N-1} + g^N\left(\frac{R_N}{S}\right)\right) \\ &= b_0 g^{-f} + b_1 g^{-f+1} + b_2 g^{-f+2} + \ldots + b_{N-1}g^{-f+N-1} + g^{-f+N}\left(\frac{R_N}{S}\right). \end{aligned}$$

Sea $N = f + n$. Igualando término a término en las dos ultimas expresiones

$$a_k = b_{k+f} \qquad (k = -f, -f+1, \ldots, n-1)$$

entonces

$$\begin{aligned} b_0 &= b_{-f+0+f} = a_{-f+0} \\ b_1 &= b_{-f+1+f} = a_{-f+1} \\ b_2 &= b_{-f+2+f} = a_{-f+2} \\ &\vdots \\ b_{N-1} &= b_{-f+n-1+f} = a_{n-1} \end{aligned}$$

Por tanto nos queda

$$a = a_{-f}g^{-f} + a_{-f+1}g^{-f+1} + \ldots + a_0 + a_1 g + \ldots + g^n \frac{R_{f+n}}{S}$$

◇

Definición 5 *Sea $a \in \mathbb{Q}$ llamaremos expansión g-ádica a la representación de a dada por*

$$a = a_{-f}g^{-f} + a_{-f+1}g^{-f+1} + \ldots + a_0 + a_1 g + \ldots + g^n \frac{R_{f+n}}{S}$$

Convenio: Si a es un entero g-ádico, la expansión g-ádica de a la escribiremos

$$a = a_0, a_1 a_2 a_3 \ldots (g)$$

y si a no es entero g-ádico

$$a = a_{-f}a_{-f+1}\ldots a_0, a_1 a_2 \ldots (g)$$

Observación 4 *Si $|a|_g < 1$ entonces los primeros dígitos de la expansión son cero.*

Teorema 9 *Una expansión g-ádica representa un número racional si y sólo si es periódica.*

Demostación Primero vamos a suponer que la expansión es periódica y tiene la forma

$$a = a_{-f}a_{-f+1}\cdots a_0, a_1a_2\ldots a_{m-1}\overline{a_m a_{m+1}\cdots a_{m+p-1}}\ldots(g)$$

donde la barra se coloca sobre el período. Al término de la expansión después de n repeticiones del período obtenemos un número $a(n)$ el cual se dá explicitamente por

$$a(n) = \sum_{k=-f}^{m-1} a_k g^k + \sum_{k=m}^{m+np-1} a_k g^k$$

Por periodicidad tenemos

$$\sum_{k=m}^{m+np-1} a_k g^k = \sum_{k=m}^{m+p-1} a_k(g^k + g^{k+p} + g^{k+2p} + \cdots + g^{k+(n-1)p})$$

Usando la progresión geométrica

$$g^k + g^{k+p} + g^{k+2p} + \cdots + g^{k+(n-1)p} = \frac{(1-g^{np})}{(1-g^p)}g^k$$

obtenemos

$$a(n) = \sum_{k=-f}^{m-1} a_k g^k + \sum_{k=m}^{m+p-1} a_k \frac{g^k}{(1-g^p)}(1-g^{np})$$

de donde

$$a(n) - \left(\sum_{k=-f}^{m-1} a_k g^k + \sum_{k=m}^{m+p-1} a_k \frac{g^k}{(1-g^p)}(1-g^{np})\right) = 0$$

$$\left|a(n) - \left(\sum_{k=-f}^{m-1} a_k g^k + \sum_{k=m}^{m+p-1} a_k \frac{g^k}{(1-g^p)}\right)\right|_g = g^{-p-m} < g^{-np-m}$$

y por tanto

$$\left|a(n) - \left(\sum_{k=-f}^{m-1} a_k g^k + \sum_{k=m}^{m+r-1} a_k \frac{g^k}{(1-g^p)}\right)\right|_g \leq g^{-np-m}$$

y como n tiende a infinito, $a(n)$ se convierte en la expansión deseada, así encontramos que

$$a = \sum_{k=-f}^{m-1} a_k g^k + \sum_{k=m}^{m+p-1} a_k \frac{g^k}{(1-g^p)}$$

En segundo lugar, probaremos que la expansión p-ádica de un número racional es periódica. Basta considerar $a \in \mathbb{Q}$ tal que sea entero g-ádico, o sea, $(r,s) = (g,s) = 1$. Por el Teorema 6 existe para cualquier entero positivo n un par de enteros A_n, r_n tal que

$$a = \frac{r}{s} = A_n + g^n\frac{r_n}{s} \qquad 0 \leq A_n \leq g^n - 1$$

Por lo tanto

$$r_n = \frac{(r - A_n s)}{g^n}$$

y

$$\frac{(r-(g^n-1)s)}{g^n} \leq r_n \leq \frac{r}{g^n}.$$

Notemos que para n muy grande, $-s \leq r_n \leq 0$. Ahora con el dígito a_n y n reemplazando por $n+1$ obtenemos

$$a = A_n + g^n \frac{r_n}{s} = A_{n+1} + g^{n+1} \frac{r_{n+1}}{s} = A_n + a_n g^n + g^{n+1} \frac{r_{n+1}}{s}$$

Así para toda n

$$r_n = a_n s + g r_{n+1}$$

Sea j tal que $r_n = r_{n+j}$

$$\begin{aligned} r_n &= a_n s + g r_{n+1} \\ r_{n+j} &= a_{n+j} s + g r_{n+j+1} \\ a_n s + g r_{n+1} &= a_{n+j} s + g r_{n+j+1} \\ (a_n - a_{n+j}) s &= (r_{n+j+1} - r_{n+1}) g \end{aligned}$$

como $(g, s) = 1$ entonces $g | (a_n - a_{n+j})$ y además $0 \leq a_i \leq g-1$. Por lo tanto $a_n - a_{n+j} = 0$, y

$$a_n = a_{n+j} \quad ; \quad r_{n+1} = r_{n+j+1}$$

◇

Observación 5 *La representación g-ádica de un número racional esta determinada en forma única por los a_i, y si se conocen estos se conoce el número racional. No es necesario mostrar la unicidad de esta representación pues se hereda del teorema anterior.*

EJEMPLOS

1. Valor g-ádico de un racional

   i) $\left|\frac{54}{21}\right|_3 = 3^{-2}$

   $\frac{54}{21} = \frac{(3^3 \times 2)}{(3^1 \times 7)} = 3^{3-1} \frac{2}{7} = 3^2 \frac{2}{7}$

   ii) $\left|\frac{13}{24}\right|_6 = 6^1$

   $\frac{13}{24} = \frac{(6^0 \times 13)}{(6^1 \times 4)} = 6^{0-1} \frac{13}{4} = 6^{-1} \frac{13}{4}$

   iii) $\left|\frac{39}{8}\right|_5 = 5^0 = 1$

   $\frac{39}{8} = \frac{(5^0 \times 39)}{(5^0 \times 8)} = 5^{0-0} \frac{39}{8} = 5^0 \frac{39}{8}$

2. Expansión g-ádica de un número racional

   i) $\frac{r}{s} = \frac{58}{39}$; $g = 5$; $\left|\frac{58}{39}\right|_5 = 1$

$$\begin{aligned} \frac{58}{39} &= 2 + 5\left(\frac{-4}{39}\right) \\ -\frac{4}{39} &= 4 + 5\left(-\frac{32}{39}\right) \\ -\frac{32}{39} &= 2 + 5\left(-\frac{22}{39}\right) \\ -\frac{22}{39} &= 2 + 5\left(-\frac{20}{39}\right) \\ -\frac{20}{39} &= 0 + 5\left(-\frac{4}{39}\right) \\ -\frac{4}{39} &= 4 + 5\left(-\frac{32}{39}\right) \end{aligned}$$

$$\frac{58}{39} = 2,\overline{4220}(5)$$

ii) $\frac{c}{s} = \frac{97}{98}$; $g = 7$; $\left|\frac{97}{98}\right|_7 = 7^2 > 1$

$$\frac{97}{2} = 3 + 7\left(\frac{13}{2}\right)$$
$$\frac{13}{2} = 3 + 7\left(\frac{1}{2}\right)$$
$$\frac{1}{2} = 4 + 7\left(-\frac{1}{2}\right)$$
$$-\frac{1}{2} = 3 + 7\left(-\frac{1}{2}\right)$$
$$-\frac{1}{2} = 3 + 7\left(-\frac{1}{2}\right)$$

$$\frac{97}{98} = 7^2 \times \frac{97}{2} = 7^2 \times (3, \overline{343}(7))$$

3. Representación de una expansión g-ádica a un número racional

i) $\overline{4,20}(7)$

$$\sum_{k=0}^{3} a_k \frac{7^k}{(1-7^3)} = \frac{(4 + 2 \times 7 + 0 \times 7^2)}{(1-7^3)} = \frac{18}{-342} = \frac{-9}{171} = \frac{-1}{19}$$

$$\overline{4,20}(7) = \frac{-1}{19}$$

ii) $22\overline{1},(3)$

$$\sum_{k=-2}^{0} a_k \frac{3^k}{(1-3^1)} = \frac{(2 \times 3^{-2} + 2 \times 3^{-1} + 1 \times 3)}{(1-3^1)}$$
$$= \frac{\frac{33}{9}}{-2} = \frac{-33}{18} = \frac{-11}{6}$$

$$22\overline{1},(3) = \frac{-11}{6}$$

Capítulo 2

Valuaciones y pseudo-valuaciones

En el presente capítulo haremos un estudio sobre anillos o campos tomando en cuenta propiedades de sucesiones y límites que se tienen en el análisis real utilizando el valor g-ádico. Haremos una convención para utilizar pseudo-valuaciones o valuaciones Arquimedianas o no-Arquimedianas.

Definición 6 *Sea A un anillo conmutativo con unidad y $\omega : A \longrightarrow [0,\infty)$ una función. Si ω satisface*

i) $\omega(0) = 0, \quad \omega(a) > 0, \qquad a \neq 0 \in A$

ii) $\omega(a+b) \leq \omega(a) + \omega(b) \qquad a, b \in A$

iii) $\omega(a \cdot b) \leq \omega(a) \cdot \omega(b) \qquad a, b \in A$

entonces diremos que ω es una **pseudo-valuación Arquimediana.**

Si además ω satisface

$$\omega(a+b) \leq \max\{\omega(a), \omega(b)\} \qquad a, b \in A$$

entonces diremos que ω es **no-Arquimediana.** Si en *(iii)* ocurre que

$$\omega(a \cdot b) = \omega(a) \cdot \omega(b) \qquad a, b \in A$$

entonces diremos que ω es una **valuación.**

Lema 3 . *Si ω es* valuación *o* pseudo-valuación

$$\omega(a) = \omega(-a)$$

Demostración: Supongamos que ω es **Arquimediana,** entonces para $a \in A$

$$\omega(a) = \omega(0-a) \leq \omega(0) + \omega(-a) = \omega(-a) \qquad \omega(a) \leq \omega(-a)$$

Similarmente

$$\omega(-a) = \omega(0-a) \leq \omega(0) + \omega(a) = \omega(a) \qquad \omega(-a) \leq \omega(a)$$

Concluyendo

$$\omega(a) = \omega(-a)$$

Supongamos ahora que ω es *no − Arquimediana*, entonces

$$\omega(a) = \omega(0-a) \leq \max\{\omega(0), \omega(-a)\}$$

$$\omega(a) \leq \omega(-a)$$

Similarmente

$$\omega(-a) = \omega(0-a) \leq \max\{\omega(0), \omega(a)\} \qquad \omega(a) \leq \omega(-a)$$

Por lo tanto

$$\omega(a) = \omega(-a)$$

◇

Lema 4 *Sean $a, b \in A$ y ω una valuación, entonces*

$$|\omega(a) - \omega(b)| \leq \omega(a - b)$$

Demostración: Sea $a = b + (a - b)$, aplicando la valuación ω tenemos

$$\omega(a) = \omega(b + (a - b)) \leq \omega(b) + \omega(a - b)$$

entonces

$$\omega(a) - \omega(b) \leq \omega(a - b)$$

Similarmente para $b = a - (a - b)$ tenemos que

$$\omega(b) = \omega(a - (a - b)) \leq \omega(a) + \omega(a - b)$$

$$\omega(b) - \omega(a) \leq \omega(a - b)$$

pero

$$\omega(a) - \omega(b) \leq \omega(a - b)$$

entonces como

$$\omega(a) - \omega(b) \leq \omega(a - b)$$

y

$$\omega(b) - \omega(a) \leq \omega(a - b)$$

Por tanto

$$|\omega(a) - \omega(b)| \leq \omega(a - b).$$

◇

Definición 7 *i) Sea $\{a_n\}$ una sucesión en A. Decimos que $\{a_n\}$ es ω-acotada si existe $C > 0$ tal que $\omega(a_n) \leq C$ para todo $n \in \mathbb{N}$.*

ii) $\{a_n\}$ es una sucesión nula si

$$\lim_{n \to \infty} \omega(a_n) = 0$$

iii) $\{a_n\}$ es una sucesión fundamental si

$$\lim_{n,m \to \infty} \omega(a_n - a_m) = 0$$

Definición 8 *El ω-límite se definira como sigue:*
para todo $\epsilon > 0$ existe $\delta > 0$ tal que $\omega(a_n - a_m) < \epsilon$ para toda $m, n \geq \delta$.

Notemos que una sucesión nula se dice cuando tenemos ω-límite 0 y una sucesión fundamental se dice que es *ω – convergente.*

Teorema 10 . *Toda sucesión fundamental es acotada.*

Demostración: Sea ϵ y δ tal que para todo $\epsilon > 0$ existe δ tal que $\omega(a_n - a_m) < \epsilon$ para toda $m, n \geq \delta$ y sea $\delta_0 > \delta$, si $n \geq \delta_0$ entonces

$$0 \leq \omega(a_n) = \omega(a_{\delta_0} + (a_n - a_{\delta_0})) \leq \omega(a_{\delta_0}) + \omega(a_n - a_{\delta_0}) \leq \omega(a_{\delta_0}) + \epsilon = C_1$$

Ahora para todos los subíndices n tenemos

$$0 \leq \omega(a_n) \leq \max\{\omega(a_1), \omega(a_2), \ldots, \omega(a_{\delta_0 - 1}), C_1\} = C$$

Por tanto

$$\omega(a_n) \leq C \qquad \text{para todo } n \in \mathbb{N}$$

◇

Teorema 11 *Toda sucesión nula es fundamental.*

Demostración: Sean ϵ y δ y supongamos que $m, n > \delta$, entonces

$$0 \leq \omega(a_n - a_m) \leq \omega(a_m) + \omega(a_n) < \epsilon + \epsilon = 2\epsilon$$

Por tanto

$$\omega(a_n - a_m) < \epsilon \qquad \forall m, n > \delta.$$

◇

Teorema 12 . *Sea $\{a_n\}$ una sucesión fundamental y $\{n_1, n_2, \ldots\}$ una sucesión creciente de enteros positivos. Si la subsucesión*

$$\{a_{n_1}, a_{n_2}, a_{n_3}, \ldots\}$$

de $\{a_n\}$ es la sucesión nula, entonces $\{a_n\}$ es sucesión nula.

Demostración: Sean ϵ, δ, δ_1 y k un subíndice tal que $n_k \geq \max\{\delta_1, \delta\}$ y sea $m \geq \delta_1$ entonces

$$\omega(a_m) = \omega(a_{n_k} + (a_m - a_{n_k})) \leq \omega(a_{n_k}) + \omega(a_m - a_{n_k}) < \epsilon + \epsilon = 2\epsilon$$

entonces

$$\omega(a_m) < \epsilon \qquad \forall n_k \geq \max\{\delta, \delta_1\}$$

◇

Este teorema nos indica que para que una sucesión sea nula es suficiente que contenga una subsucesión nula.

Observación 6 *Notemos que una sucesión fundamental que no sea nula no puede contener una subsucesión que sea sucesión nula.*

Corolario 4 *Si $\{a_n\}$ es sucesión fundamental, pero no nula, entonces existen C y N tal que*

$$\omega(a_n) \geq C \qquad si \quad n \geq N$$

Demostración: Supongamos que no existen C, N tal que

$$\omega(a_n) \geq C \quad \text{si} \quad n \geq N$$

Es claro que:
Para toda $C > 0$ y para toda N existe $n \geq N$ tal que $\omega(a_n) < 0$.
En particular tenemos:
$1 > 0$ para toda N existe n_1 tal que $\omega(a_{n_1}) < 1$.
$\frac{1}{2} > 0$ para $N = n_1$ existe $n_2 > n_1$ tal que $\omega(a_{n_2}) < \frac{1}{2}$.
$\frac{1}{3} > 0$ existe $n_3 > n_2$ tal que $\omega(a_{n_3}) < \frac{1}{3}$.
De esta forma podemos suponer que existen enteros positivos $n_1 < n_2 < n_3 < \ldots < n_k < \ldots$ tal que $\omega(a_{n_k}) < \frac{1}{k}$.
Por lo tanto $\{a_{n_k}\}$ es una sucesión nula y así la sucesión $\{a_n\}$ es nula. Esto es una contradicción.

◇

Teorema 13 *Sean $\{a_n\}$, $\{b_n\}$ sucesiones fundamentales entonces lo son*

$$i) \quad \{a_n + b_n\} \qquad ; \qquad ii) \quad \{a_n b_n\}$$

Demostración: Para $\{a_n\} + \{b_n\} = \{a_n + b_n\}$
i) Como $\lim_{n,m\to\infty} \omega[(a_m + b_m) - (a_n + b_n)] = 0$ por ser sucesiones fundamentales entonces

$$\begin{aligned}
\lim_{n,m\to\infty} \omega[(a_m + b_m) - (a_n + b_n)] &= \lim_{n,m\to\infty} \omega(a_m + b_m - a_n - b_n) \\
&= \lim_{n,m\to\infty} \omega(a_m - a_n + b_m - b_n) \\
&= \lim_{n,m\to\infty} \omega((a_n - a_m) + (b_m - b_n)) \\
&= \lim_{n,m\to\infty} \omega(a_n - a_m) + \lim_{n,m\to\infty} \omega(b_m - b_n) \\
&= 0
\end{aligned}$$

Por tanto $\{a_n + b_n\}$ es sucesión fundamental.

ii) Sean C_1 y C_2 tal que $\omega\{a_n\} \leq C_1$ y $\omega\{b_n\} \leq C_2$ (Teorema 10) entonces

$$\{a_n\}\{b_n\} = \{a_n b_n\}$$

$$\begin{aligned}
\lim_{n,m\to\infty} \omega[\{a_m b_m\} - \{a_n b_n\}] &= \lim_{n,m\to\infty} \omega[\{(a_n - a_m)(b_n - b_m) + a_n(b_n - b_m) + b_n(a_n - a_m)\} \\
&\leq \lim_{n,m\to\infty} \omega[\{(a_n - a_m)(b_n - b_m)\} + \omega[a_n(b_n - b_m) + b_n(a_n - a_m)\} \\
&= \lim_{n,m\to\infty} \omega[\{(a_n - a_m)(b_n - b_m)\} + \lim_{n,m\to\infty} \omega[a_n(b_n - b_m) + b_n(a_n - a_m)] \\
&= \lim_{n,m\to\infty} \omega[\{(a_n - a_m)(b_n - b_m)\} + \lim_{n,m\to\infty} \omega(a_n(b_n - b_m)) \\
&\quad + \lim_{n,m\to\infty} \omega(b_n(a_n - a_m)) \\
&\leq \lim_{n,m\to\infty} \omega[\{(a_n - a_m)(b_n - b_m)\} + \lim_{n,m\to\infty} \omega(a_n) \lim_{n,m\to\infty} \omega(b_n - b_m) \\
&\quad + \lim_{n,m\to\infty} \omega(b_n) \lim_{n,m\to\infty} \omega(a_n - a_m) \\
&\leq \lim_{n,m\to\infty} \omega[\{(a_n - a_m)(b_n - b_m)\} + C_1 \lim_{n,m\to\infty} \omega(b_n - b_m) \\
&\quad + C_2 \lim_{n,m\to\infty} \omega(a_n - a_m) \\
&= 0
\end{aligned}$$

Por tanto $\{a_n b_n\}$ es sucesión fundamental.

◇

Teorema 14 *Si $\{a_n\}$ y $\{b_n\}$ son sucesiones nulas, lo son también $\{a_n + b_n\}$ y $\{a_n - b_n\}$. Si además $\{a_n\}$ es sucesión nula y $\{b_n\}$ es sucesión acotada entonces $\{a_n b_n\}$ es sucesión nula.*

Demostración: Dado que $\{a_n\}$ y $\{b_n\}$ son sucesiones nulas, de la definición tenemos

$$\begin{aligned}
0 &\leq \lim_{n\to\infty} \omega(a_n \pm b_n) \leq \lim_{n\to\infty} \omega(a_n) + \omega(b_n) \\
&\leq \lim_{n\to\infty} \omega(a_n) + \lim_{n,m\to\infty} \omega(b_n) = 0
\end{aligned}$$

Ahora para la tercera afirmación sabemos que $\omega(b_n) \leq C$ para toda n y como n tiende a infinito.

$$0 \leq \omega(a_n b_n) \leq \omega(a_n)\omega(b_n) \leq \omega(a_n)C = 0$$

Sea $A_\omega = \{\{a_n\} \mid \{a_n\}$ es sucesión fundamental en $A\}$ entonces con la suma y el producto de sucesiones, A_ω es un anillo conmutativo con uno, que no es un campo, pues, por ejemplo, la sucesión $\{1, 0, 0, \cdots\}$ es un divisor de cero.

Proposición 1 *Sea $\mathbf{P}$ el conjunto de sucesiones nulas y sea ω pseudo-valuación de A entonces $\mathbf{P}$ es un ideal de A_ω*

i) $\{0\} \in \mathbf{P}$

ii) $\{a_n\} + \{b_n\} \in \mathbf{P}$ cuando $\{a_n\}, \{b_n\} \in \mathbf{P}$

iii) Si $\{a_n\} \in A_\omega \;\; ; \;\; \{b_n\} \in \mathbf{P} \;\; \{a_n\}\{b_n\} \in \mathbf{P}$

Corolario 5 *Si ω es valuación entonces $\mathbf{P}$ es primo.*

Demostración: Supongamos que ω es valuación de A y consideremos dos elementos en A_ω que no sean sucesiones nulas, es decir, que no pertenezcan a P. Por el Colorario 4 existen cuatro enteros positivos C, C', N, N' tales que

$$\omega(a_n) \geq C \;\; n \geq N \;\; ; \;\; \omega(b_n) \geq C' \;\; n \geq N'$$

De aquí, si N^* es mayor que N, N' entonces

$$\omega(a_n) \geq C \quad \omega(b_n) \geq C' \quad n \geq N^*$$

como ω es una valuación obtenemos que

$$\omega(a_n b_n) \geq CC' \quad n \geq N^*$$

entonces $\{a_n\} \cdot \{b_n\} = \{a_n \cdot b_n\}$ no es una sucesión nula y no está en P. Por lo tanto un producto de sucesiones en $\bar{A}_\omega$ pertenece a P si al menos una de ellas pertenece a P. Por tanto P es primo.

◇

Definición 9 *Definimos la completación de A con respecto a ω como $\bar{A}_\omega = A_\omega/\mathbf{P}$. Es claro que $\bar{A}_\omega$ es un anillo conmutativo con unidad y si ω es una valuación entonces $\bar{A}\omega$ es un Dominio Entero.*

Teorema 15 *Si A es un campo y ω es valuación entonces $\bar{A}_\omega$ es un campo.*

Demostración: Es suficiente mostrar que P es un ideal máximo o, alternativamente, que cualquier elemento diferente de cero en $\bar{A}_\omega$ tiene inverso multiplicativo. Sea $\{a_n\} + \mathbf{P}$ una clase residual en A_ω con $\{a_n\} \notin \mathbf{P}$.

Definamos

$$a_n^* = \begin{cases} 0 & \text{si } 1 \leq n \leq N-1 \\ \frac{1}{a_n} & \text{si } n \geq N \end{cases}$$

donde la N es la del Corolario 4. Esta sucesión es fundamental no nula. Porque si $m, n \geq N$ como ω es valuación

$$0 \leq \omega(a_m^* - a_n^*) = \omega\left(\frac{1}{a_m} - \frac{1}{a_n}\right) = \frac{\omega(a_n - a_m)}{\omega(a_m)\omega(a_n)} = \frac{\omega(a_n - a_m)}{C^2}$$

donde la C es la del Corolario 4. Por lo tanto

$$\lim_{n,m\to\infty} \omega(a_m^* - a_n^*) = 0$$

Denotemos por A^{-1} la clase residual de $\{a_n^*\}$ entonces $A \cdot A^{-1} = \{1\}$ porque

$$\{a_n\} \cdot \{a_n^*\} = \{\overbrace{0, 0, \cdots, 0}^{N-1 \text{ ceros}}, 1, \cdots, 1\}$$

donde la sucesión fundamental de la derecha difiere de la identidad $\{1\}$ en la sucesión nula

$$\{\overbrace{-1, -1, \cdots, -1}^{N-1 \quad -1\text{'s}}, 0, \cdots\}.$$

Por tanto hemos probado que $\bar{A}_\omega$ es un campo.

◇

Definición 10 *Sea* A *una clase residual en $\bar{A}_\omega$ y $\{a_n\}$ una sucesión fundamental representante de* A *definiremos*

$$\mathbf{A} = \overset{\omega}{\lim_{n\to\infty}} (a_n)$$

En el caso que $\{a_n\}$ sea sucesión nula

$$\overset{\omega}{\lim_{n\to\infty}} (a_n) = (0) \subseteq \mathbf{P}$$

Si el representante $\{a_n\}$ converge a $a \in A$ entonces

$$\{a_n\} \equiv \{a\} \quad ; \quad \{a_n - a\} \in \mathbf{P}$$

y por tanto

$$\lim_{n\to\infty}\omega(a_n - a) = 0$$

$$(a) = \overset{\omega}{\lim_{n\to\infty}}(a_n) = \mathbf{A}$$

Como $\{a_n\}$ converge a $a \in A$ entonces claramente $\{a\} \in \mathbf{A}$ y $\mathbf{A} = (\{a\})$. Por lo tanto

$$\lim_{n\to\infty}\omega(a_n) = \omega(a)$$

Sea $\{b_n\} \in \mathbf{A}$ entonces $\{b\} \sim \{a_n\}$ y así $\{b_n - a\} \in \mathbf{P}$, es decir, $\lim_{n\to\infty}\omega(b_n - a) = 0$ y por lo anterior $\lim_{n\to\infty}\omega(b_n) = \omega(a) = \lim_{n\to\infty}\omega(a_n)$.

Por lo tanto si $\mathbf{A} = (\{a\})$ con $a \in A$ definimos

$$\omega(\mathbf{A}) = \lim_{n\to\infty}\omega(a_n)$$

con $\{a_n\} \in \mathbf{A}$. En seguida veremos el caso en que $\{a_n\}$ no converge en A. Si $\mathbf{A}$ en $\hat{A}_\omega$ entonces

$$\mathbf{A} = \{a_n\} + \mathbf{P} = \{\{a_n\} + \{b_n\} \mid \{b_n\} \in \mathbf{P}\}$$

Sean $\{a_n\}$ y $\{a'_n\}$ representantes de $\mathbf{A}$, mostraremos que

$$\lim_{n\to\infty}\omega(a_n + b_n) = \lim_{n\to\infty}\omega(a'_n + b_n)$$

Para ello se tomará el Lema 4, es decir,

$$|\omega(a) - \omega(b)| \leq \omega(a - b)$$

$$0 \leq \lim_{n\to\infty}|\omega(a_n + b_n) - \omega(a'_n + b_n)| \leq \lim_{n\to\infty}\omega(a_n + b_n - a'_n - b_n) = 0$$

de donde

$$\lim_{n\to\infty}\omega(a_n) = \lim_{n\to\infty}\omega(a'_n)$$

Por lo anterior la siguiente definición tiene sentido

Definición 11 *Si $\{a_n\}$ es una sucesión fundamental representante de $\mathbf{A}$*

$$\omega(\mathbf{A}) = \lim_{n\to\infty}\omega(a_n)$$

Teorema 16 *ω es una valuación o pseudo-valuación sobre $\hat{A}_\omega$*

Demostración: Sean $\mathbf{A}$ y $\mathbf{B}$ dos clases residuales representadas por sucesiones fundamentales $\{a_n\}$ y $\{b_n\}$ respectivamente. Si $\mathbf{A} = 0$ entonces $\{a_n\}$ es sucesión nula y por el Corolario 4 existen C y N tal que $\omega(a_n) \geq C$ para $n \geq N$ también $\omega(\mathbf{A}) \geq C > 0$. Por propiedades del límite real

$$\begin{aligned}\omega(\mathbf{A} \pm \mathbf{B}) &= \lim_{n\to\infty}\omega(a_n \pm b_n) \leq \lim_{n\to\infty}(\omega(a_n) + \omega(b_n)) \\ &= \lim_{n\to\infty}\omega(a_n) + \lim_{n\to\infty}\omega(b_n) \\ &= \omega(\mathbf{A}) + \omega(\mathbf{B})\end{aligned}$$

entonces $\omega(\mathbf{A} \pm \mathbf{B}) \leq \omega(\mathbf{A}) + \omega(\mathbf{B})$

De la misma manera

$$\begin{aligned}\omega(\mathbf{A} \cdot \mathbf{B}) &= \lim_{n\to\infty}\omega(a_n \cdot b_n) \leq \lim_{n\to\infty}(\omega(a_n) \cdot \omega(b_n)) \\ &= \lim_{n\to\infty}\omega(a_n) \cdot \lim_{n\to\infty}\omega(b_n) \\ &= \omega(\mathbf{A}) \cdot \omega(\mathbf{B})\end{aligned}$$

entonces $\omega(A \cdot B) \leq \omega(A) \cdot \omega(B)$. Con esto hemos demostrado que ω es una pseudo-valuación de $\bar{A}_\omega$. Si ω es valuación entonces en la última forma

$$\omega(A \cdot B) = \omega(A) \cdot \omega(B)$$

Por lo tanto $\omega(A)$ también es valuación sobre $\bar{A}_\omega$. Unicamente falta probar que ω es no-Arquimediana sobre $\bar{A}_\omega$, pero si ω es no-Arquimediana sobre A entonces

$$\begin{aligned} \omega(A \pm B) &= \lim_{n\to\infty} \omega(a_n + b_n) \leq \lim_{n\to\infty} (\max(\omega(a_n), \omega(b_n)) \\ &\leq \max(\lim_{n\to\infty} \omega(a_n), \lim_{n\to\infty} \omega(b_n)) \\ &= \max(\omega(A), \omega(B)) \end{aligned}$$

entonces $\omega(A \pm B) \leq \max(\omega(A), \omega(B))$, así que ω es también no-Arquimediana sobre $\bar{A}_\omega$.

◇

Teorema 17 *Si ω es valuación, entonces A es denso en $\bar{A}_\omega$.*

Demostración: Sea A en $\bar{A}_\omega$ $A = \overset{\omega}{\lim_{n\to\infty}}(a_n)$ tal que $\{a_n\}$ es un representante de A. Tomemos la clase residual $A' = (a)$ tal que $m \in \mathbb{N}$ donde la sucesión fundamental $\{a_m\} = \{a, a, \ldots, a\}$ tal que $a_m = a \,;\, a \in A$ para toda $m \in \mathbb{N}$ es su representante. Definimos $A - A' = A - a_m$ como el ω-limite.

$$A - a_m = \overset{\omega}{\lim_{n\to\infty}}(a_n - a_m) \qquad \text{para } m \in \mathbb{N}$$

tomando la definición anterior de $\omega(A)$

$$\omega(A - a_n) = \lim_{n\to\infty} \omega(a_n - a_m) \qquad \text{para } m \in \mathbb{N}$$

como $\{a_n\}$ es sucesión fundamental

$$\lim_{n\to\infty} \omega(A - a_m) = \lim_{n\to\infty} \omega(a_n - a_m) = 0$$

Cuando m es muy grande $\omega(A - a_m)$ es arbitrariamente pequeño
Por tanto A es denso sobre $\bar{A}_\omega$.

◇

Teorema 18 *Sea A un campo y ω una valuación de A, entonces $\bar{A}_\omega$ es completo.*

Demostración: Por construcción, la valuación ω esta definida en $\bar{A}_\omega$. Sea $\bar{\bar{A}}_\omega$ construido con la valuación ω en $\bar{A}_\omega$. Basta probar que $\bar{\bar{A}}_\omega = \bar{A}_\omega$. Sea $A \in \bar{\bar{A}}_\omega$ y $\{A_n\} \in A$. Sabemos que $\lim_{n\to\infty} \omega(A_n - A) = 0$ y $\lim_{n\to\infty} \omega(A_n - A_m) = 0$. Para $A_n \in \{A_n\}$ existe $a_n \in A$ tal que

$$\omega(A_n - a_n) < \frac{1}{n}$$

de esto, $\{A_n - a_n\}$ es sucesión nula y por tanto sucesión fundamental. La sucesión

$$\{a_n\} = \{A_n\} - \{A_n - a_n\}$$

también es fundamental en $\bar{A}_\omega$ y en efecto porque $a_n \in A$ tiene límite

$$A = \overset{\omega}{\lim_{n\to\infty}}(a_n)$$

Además $\{A - a_n\}$ y $\{A_n - a_n\}$ son sucesiones nulas en $\bar{A}_\omega$, su diferencia

$$\{A - A_n\} = \{A - a_n\} - \{A_n - a_n\}$$

también es sucesión nula. Entonces $\lim_{n\to\infty} \omega(A_n - A) = 0$. De esto la sucesión fundamental $\{A\} = \{A, A, \ldots\}$ tiene el mismo ω-límite en $\dot{A}_\omega$ que $\{A_n\}$ es decir,

$$A = \overset{\omega}{\lim_{n\to\infty}}(A_n)$$

con $A \in \dot{A}_\omega$. Pero A pertenece nuevamente a $\dot{A}_\omega$, así que $\dot{A}_\omega = \dot{A}_\omega$.

◇

Observación 7 *Si $A = Q$ y $\omega(a) = |a|$, $\dot{A}_\omega = R$, entonces R es la completación de Q con respecto a $|\ |$. De la misma manera la completación de Q con respecto a $|\ |_p$ y $|\ |_\infty$ es Q_p y Q_∞ respectivamente.*

Capítulo 3

Números g-ádicos y p-ádicos

Recordemos que si A es un campo y ω una valuación entonces $\hat{A}_\omega$ es un campo completo en el sentido usual. En $\mathbf{Q}$, por ejemplo, tenemos el valor absoluto $|\ |$, como valuación y la completez de $\mathbf{Q}$ con respecto a $|\ |$ es $\mathbf{R}$. Tomando en cuenta que en $\mathbf{Q}$ se tienen definidas las pseudo-valuaciones $|\ |_g$ y las valuaciones $|\ |_p$, entonces sus completaciones son $\mathbf{Q}_g$ y $\mathbf{Q}_p$ respectivamente. En este capítulo probaremos que $\mathbf{Q}_g$ no es un campo si g al menos tiene dos factores primos distintos.

Sean $A_1 + A_2 + A_3 + \cdots + A_n \in \hat{A}_\omega$ y ω una pseudo-valuación, definiremos

$$A_1 + A_2 + A_3 + \cdots = \sum_{n\geq 1} A_n$$

como una suma de series infinita, llamadas tambien ω-convergentes.

Definición 12 $\sum_{n\geq 1} A_n$ *es ω-convergente si $\{S_n\}$ es sucesión fundamental, donde* $S_n = \sum_{k=1}^{n} A_k$ *para* $n = 1,2,3,\ldots$

Teorema 19 $\sum_{n\geq 1} A_n$ *es ω-convergente si y sólo si*

$$\lim_{m,n\to\infty} \omega(A_{n+1} + A_{n+2} + \cdots + A_m) = 0$$

Demostración: Suponiendo que $\sum_{n\geq 1} A_n$ es ω-convergente entonces $\{S_n\}$ es sucesión fundamental

$$0 = \lim_{m,n\to\infty} \omega(S_m - S_n) = \lim_{m,n\to\infty} \omega(A_{n+1} + A_{n+2} + \cdots + A_m)$$

El regreso es inmediato pues si

$$\lim_{m,n\to\infty} \omega(A_{n+1} + A_{n+2} + \cdots + A_m) = 0$$

$$\lim_{m,n\to\infty} \omega(S_m - S_n) \longrightarrow \{S_n\}$$

es sucesión fundamental

◇

Notese que en la prueba anterior no se uso el hecho de que ω fuese Arquimediana o no-Arquimediana.

Corolario 6 $\sum_{n\geq 1} A_n$ *es ω-convergente si y sólo si*

$$\lim_{m\to\infty} \omega(A_m) = 0$$

Demostración: En el teorema anterior sea $m = n + 1$

◇

Corolario 7 *En $\mathbf{Q}_g$ y $\mathbf{Q}_p$ una serie $\sum_{n\geq 1} A_n$ es ω-convergente si y sólo si*

$$\lim_{m\to\infty} |A_n|_g = 0 \quad \acute{o} \quad \lim_{m\to\infty} |A_n|_p = 0$$

Teorema 20 *Sea A un anillo y ω pseudo-valuación no-Arquimediana si $\sum_{n=1}^{\infty} {A_n}^{\omega}$ existe y si $\sum_{n\geq 1} A'_n$ es una serie con los mismos términos, pero en diferente orden, entonces $\sum_{n=1}^{\infty} {A'_n}^{\omega}$ existe y es igual a $\sum_{n=1}^{\infty} {A_n}^{\omega}$.*

Demostración: Sea $\epsilon > 0$ y $N \in \mathbf{Z}$ tal que

$$\omega(A_n) < \epsilon \qquad \omega(A'_n) < \epsilon \qquad \text{para} \quad n > N$$

y además de la Definición 12 sabemos que

$$S = \lim_{n\to\infty}{}^{\omega} S_n = \sum_{n=1}^{\infty} {A'_n}^{\omega}$$

entonces

$$\omega\left(\sum_{n=1}^{\infty} {A_n}^{\omega} - \sum_{n=1}^{N} {A_n}^{\omega}\right) < \epsilon$$

$$\omega\left(\sum_{n=N+1}^{\infty} {A_n}^{\omega}\right) < \epsilon$$

Sean $S = \sum_{n=1}^{N} A_n$ y $S' = \sum_{n=1}^{N} A'_n$. Si $S_1 = \sum_{n=1}^{1} A_1$ es tal que $\omega(A_1) \geq \epsilon$ y $S'_1 = \sum_{n=1}^{1} A'_1$ tal que $\omega(A'_1) \geq \epsilon$ entonces $S_1 = S'_1$ y además $\omega(S_1 - S'_1) = 0 < \epsilon$. Por lo tanto $\omega(S_1 - S'_1) < \epsilon$ y $\omega(S - S_1) < \epsilon$.

◇

Corolario 8 *Los términos de una serie convergente en $\mathbf{Q}_g$ ó $\mathbf{Q}_p$ se pueden reordenar sin cambiar su convergencia.*

Corolario 9 *Existe una serie convergente $\sum_{n\geq 1} A_n$ en $\mathbf{Q}_g$ tal que la serie real $\sum_{n=1}^{\infty} |A_n|_g$ diverge.*

Demostración: Escojamos los términos consecutivos de las series

$$1; g, g - \text{veces repetido};\ g^2, g^2 - \text{veces repetido};\ g^3, g^3 - \text{veces repetido};\ \ldots$$

estos términos convergen a 0, y así la serie converge. Por otro lado

$$\sum_{n=1}^{\infty} |A_n|_g = 1 + g^{-1}\cdot g + g^{-2}\cdot g^2 + g^{-3}\cdot g^3 + \cdots \longrightarrow \infty$$

◇

Definición 13 *Denotaremos los límites g-ádico y p-ádico como:*

$$\lim^{g} \qquad y \qquad \lim^{p}$$

así la suma en $\mathbf{Q}_g$ y $\mathbf{Q}_p$ de $\sum_{n\geq 1} A_n$ será definida como

$$\sum_{n=1}^{\infty} A_n(g) \qquad y \qquad \sum_{n=1}^{\infty} A_n(p)$$

Teorema 21 *Sea $B \in \mathbf{Q}_g$ y $\{b_n\}$ un representante de la clase residual B, entoces B tiene una representación*

$$B = b_{-f}g^{-f} + b_{-f+1}g^{-f+1} + \cdots + b_0 + b_1 g + b_2 g^2 + \cdots (g)$$

llamada serie canónica, donde $0 \leq b_i \leq g-1$.

Demostración: Sea $B \in \mathbf{Q}_g$ y $\{b_n\}$ tal que

$$B = \lim_{n\to\infty}{}_g\, b_n$$

donde $b_n \in \mathbf{Q}_g$. Entonces

$$|B|_g = \lim_{n\to\infty} |b_n|_g$$

Si $B = 0$ entonces $\{b_n\}$ es sucesión nula. Por tanto es suficiente probar el resultado para $B \neq 0$. Sabemos que

$$|B|_g = g^f$$

para alguna $f \in \mathbf{Z}$. Como $\{b_n\}$ puede reemplazarse por cualquier subsucesión infinita sin cambiar su límite, entonces podemos suponer que $\{b_n\}$ satisface

$$|b_n|_g = g^f \qquad \text{para } n = 1, 2, \ldots$$

$$|b_n - b_m|_g \leq g^{-N} \qquad \text{si } m, n \geq N, \text{ para } N = 1, 2, \ldots$$

Por el Teorema 8

$$B = b_{n,-f}g^{-f} + b_{n,-f+1}g^{-f+1} + \cdots + b_{n,0} + b_{n,1}g + b_{n,2}g^2 + \cdots + b_{n,N-1}g^{N-1} + g^N \frac{R_{n,N}}{S_{n,N}}$$

donde los coeficientes $b_{n,-f}, b_{n,-f+1}, \ldots, b_{n,0}, b_{n,1}, b_{n,N-1}$ son dígitos $0, 1, 2, \ldots, g-1$. En particular $b_{n,-f} \neq 0$ y además $R_{n,N}$ y $S_{n,N}$ son enteros que satisfacen

$$(R_{n,N}, S_{n,N}) = (g, S_{n,N}) = 1$$

Existe una representación similar para b_m

$$b_m = b_{m,-f}g^{-f} + b_{m,-f+1}g^{-f+1} + \cdots + b_{m,0} + b_{m,1}g + b_{m,2}g^2 + \cdots b_{m,N-1}g^{N-1} + g^N \frac{R_{m,N}}{S_{m,N}}$$

De lo anterior se sigue que

$$b_m - b_n = \sum_{k=-f}^{N-1} (b_{m,k} - b_{n,k}) + g^N \left(\frac{R_{m,N}}{S_{m,N}} - \frac{R_{n,N}}{S_{n,N}} \right)$$

y

$$(g, S_{m,N}S_{n,N}) = 1$$

Sean $m, n \geq N$. En la expresión

$$|b_m - b_n|_g = \left| \sum_{k=-f}^{N-1} (b_{m,k} - b_{n,k}) g^k \right|_g \leq g^{-N}$$

Notemos que todos los términos de la forma $b_{m,k} - b_{n,k}$ satisfacen

$$|b_{m,k} - b_{n,k}|_g \leq g - 1$$

es decir, $-(g-1) \leq b_{m,k} - b_{n,k} \leq g - 1$, así que $g \mid (b_{m,k} - b_{n,k})$ si y sólo si $b_{m,k} = b_{n,k}$. Consideremos $\left|(b_{m,k} - b_{n,k})g^k\right|_g$ para $k = -f, -f+1, \ldots, N-1$. Por (iii) del Corolario 1

$$\left|(b_{m,k} - b_{n,k})g^k\right|_g = g^{-k}\left|(b_{m,k} - b_{n,k})\right|_g$$

pero $|(b_{m,k} - b_{n,k})|_g = 1$, así que $|(b_{m,k} - b_{n,k})g^k|_g = g^{-k}$ y puesto que $g^{-f}, g^{-f+1}, \ldots, g^{N-1}$ son diferentes dos a dos entonces por las propiedades de $|\ |_g$ se tiene que

$$\left|\sum_{k=-f}^{N-1}(b_{m,k} - b_{n,k})g^k\right|_g = \max\{|(b_{m,k} - b_{n,k})g^k|_g\}_{k=-f}^{N-1} = g^t \leq g^N$$

con lo que llegamos a una contradicción, a menos que ocurra

$$|b_{m,k} - b_{n,k}|_g = 0$$

Por tanto

$$b_{m,k} = b_{n,k} = b_k \qquad k = -f, -f+1, \cdots, N-1$$

Concluyendo tenemos que el número g-ádico B se puede escribir como

$$B = b_{-f}g^{-f} + b_{-f+1}g^{-f+1} + \cdots + b_0 + b_1 g + b_2 g^2 + \cdots (g)$$

◇

Tomando en cuenta los resultados que se obtuvieron con anterioridad para las series canónicas, es fácil mostrar que esta serie canónica de A es única y además que representa un número racional si y sólo si es periódica.

Definición 14 *Sea $B \in \mathbb{Q}_g$ tal que $|B|_g \leq 1$ entonces diremos que B es un entero g-ádico.*

Sean C y D enteros g-ádicos, entonces claramente

$$i)\,|C + D|_g \leq 1 \qquad ii)\,|C \cdot D|_g \leq 1$$

Sea $\mathbf{I}_g = \{B \in \mathbf{Q}_g \mid |B|_g \leq 1\}$, por (i) y (ii) $\mathbf{I}_g$ es un anillo conmutativo unitario, $\mathbf{I}_g$ el cual llamaremos el anillo de los enteros g-ádicos. Particularmente la serie canónica de un entero g-ádico ó p-ádico es de la forma $b_0 + b_1 g + b_2 g^2 + \cdots (g)$.

Notemos que todo entero racional es un entero g-ádico y p-ádico, así que $\mathbb{Z} \subset \mathbf{I}_g$ y $\mathbb{Z} \subset \mathbf{I}_p$. Supongamos que $|A|_g = g^f > 1$ donde $f \geq 1$, si definimos $R = g^f A$ y $S = g^f$ entonces $A = \dfrac{R}{S}$ donde claramente

$R, S \in \mathbf{I}_g(\mathbf{I}_p)$. En particular, $\mathbf{Q}_p$ es el campo de cocientes del dominio entero $\mathbf{I}_p$. Similarmente, $\mathbf{Q}_g$ se obtiene dividiendo adecuadamente los elementos de $\mathbf{I}_g$.

Capítulo 4

Aritmética en $\mathbf{Q}_g$

En lo que sigue aplicaremos en $\mathbf{Q}_g$ y en $\mathbf{Q}_p$ el uso de las series canónicas para efectuar operaciones aritméticas y llamaremos dígitos a los números que estan entre $0, 1, \ldots, g-1$. Como se vió en el capítulo 1, para $A \in \mathbf{Q}_g - \{0\}$ con $|A|_g = g^f$ se tiene

$$A = a_{-f}a_{-f+1}\cdots a_0, a_1a_2\cdots(g)$$

Si $A \in \mathbf{I}_g$ entonces

$$A = a_0, a_1a_2\cdots(g)$$

donde los a_i son dígitos. Recordemos que si $|A|_g < 1$, entonces uno o mas de los primeros dígitos son cero. El siguiente resultado nos garantiza que una serie no-canónica puede transformarse en una serie canónica.

Teoroma 22 *Sea $A \in \mathbf{Q}_g$ tal que*

$$A = u_{-f}g^{-f} + u_{-f+1}g^{-f+1} + \cdots + u_0 + u_1g + u_2g^2 + \cdots(g)$$

donde los $u_i \in \mathbf{Z}$. Entonces A se puede reducir a la forma

$$A = a_{-f}g^{-f} + a_{-f+1}g^{-f+1} + \cdots + a_0 + a_1g + a_2g^2 + \cdots(g)$$

donde los a_i son dígitos.

Demostración: Consideremos

$$u_ng^n = (u_n - gv_n)g^n + v_ng^{n+1} \qquad (i)$$

donde v_n se escoge de tal forma que $0 \leq (u_n - gv_n) \leq g-1$. Primero escogemos el entero v_{-f} tal que

$$u_{-f} - gv_{-f} = a_{-f}$$

por (i), a_{-f} es un dígito. Claramente tenemos

$$u_{-f}g^{-f} + u_{-f+1}g^{-f+1} = a_{-f}g^{-f} + (u_{-f+1} + v_{-f})g^{-f+1}. \qquad (ii)$$

En segundo lugar escojemos un entero v_{-f+1} de tal forma que

$$(u_{-f} + v_{-f}) - gv_{-f+1} = a_{-f+1}$$

y por (ii) tenemos que a_{-f+1} es un dígito y así obtenemos

$$(u_{-f+1} + v_{-f})g^{-f+1} + u_{-f+2}g^{-f+2} = a_{-f+1}g^{-f+1} + (u_{-f+2} + v_{-f+1})g^{-f+2}$$

En el i-ésimo paso hemos elegido el entero v_{-f+i} de tal forma que

$$(u_{-f+i} + v_{-f+(i-1)}) - gv_{-f+i} = a_{-f+i}$$

es un dígito y

$$(u_{-f+l}+v_{-f+(l-1)})g^{-f+l}+u_{-f+(l+1)}g^{-f+(l+1)}=a_{-f+l}g^{-f+l}+(u_{-f+(l+1)}+v_{-f+l})g^{-f+(l+1)}$$

Utilizando lo anterior obtenemos

$$\begin{aligned} A &= a_{-f}g^{-f}+a_{-f+1}g^{-f+1}+\cdots+a_0+a_1g+a_2g^2+\cdots(g) \\ &= u_{-f}g^{-f}+u_{-f+1}g^{-f+1}+\cdots+u_0+u_1g+u_2g^2+\cdots(g) \end{aligned}$$

◇

Sean $A, B \in \mathbb{Q}_g$ tal que $|A|_g = g^f$, $|A|_g \geq |B|_g$, con

$$A = a_{-f}g^{-f}+a_{-f+1}g^{-f+1}+\cdots+a_0+a_1g+a_2g^2+\cdots(g)$$

$$B = b_{-f}g^{-f}+b_{-f+1}g^{-f+1}+\cdots+b_0+b_1g+b_2g^2+\cdots(g)$$

donde a_i, b_i son dígitos. Definimos la suma $A+B$ como

$$\begin{aligned} A+B &= (a_{-f}+b_{-f})g^{-f}+(a_{-f+1}+b_{-f+1})g^{-f+1}+\cdots \\ &\quad +(a_0+b_0)+(a_1+b_1)g+(a_2+b_2)g^2+\cdots(g) \end{aligned}$$

Notemos que $A+B$ puede ser una serie no-cánonica, sin embargo, aplicando el Teorema 22 y definiendo

$$c_{-f}=(a_{-f}+b_{-f})\,;\, c_{-f+1}=(a_{-f+1}+b_{-f+1})\,;\ldots$$

llegamos a la serie canónica de $A+B$ y por tanto podemos suponer que

$$A+B=c_{-f}g^{-f}+c_{-f+1}g^{-f+1}+\cdots+c_0+c_1g+c_2g^2+\cdots(g)$$

donde los c_i son dígitos.

El producto $A \cdot B$ lo definimos como:

$$\begin{aligned} A\cdot B &= (a_{-f}\cdot b_{-f})g^{-f-\phi}+(a_{-f+1}\cdot b_\phi+a_{-f}\cdot b_{-\phi+1})g^{-f-\phi+1}+\cdots+ \\ &\quad +(a_{-f+2}\cdot b_{-\phi}+a_{-f+1}\cdot b_{-\phi+1}+a_{-f}\cdot b_{-\phi+2})g^{-f-\phi+2}+\cdots(g). \end{aligned}$$

Por el Teorema 22, podemos suponer que la serie canónica de $A\cdot B$ es de la forma

$$A\cdot B=e_{-\psi}g^{-\psi}+e_{-\psi+1}g^{-\psi+1}+\cdots+e_0+e_1g+e_2g^2+\cdots(g)$$

donde los e_i son dígitos. El elemento B es una unidad en $\mathbb{Q}_g$ si existe $C \in \mathbb{Q}_g$ tal que $BC=1$, C se llama el inverso multiplicativo de B y denotamos $C=B^{-1}$

Teorema 23 *Sea $B \in \mathbb{I}_g$ con*

$$B=b_0,b_1b_2\cdots(g),$$

entonces B es unidad en $\mathbb{Q}_g$ si y sólo si $(b_0,g)=1$.

Demostración: Supongamos que $B^{-1}=c_0,c_1c_2\cdots(g)$, entonces debe suceder

$$\begin{aligned} 1 &= B\cdot B^{-1}=(b_0c_0),(b_0c_1+b_1r_0)(b_0c_2+b_1c_1+b_2r_0) \\ &\quad (b_0c_3+b_1c_2+b_2c_1+b_3c_0)\cdots(g). \end{aligned}$$

Construiremos inductivamente los c_i. Puesto que $(b_0,g)=1$, entonces existe $c_0 \in \mathbb{Z}$ tal que $0 \leq c_0 \leq g-1$ y

$$b_0c_0=1+gd_1$$

donde d_1 es un entero positivo.

Para el i-ésimo paso construimos un dígito c_i tal que

$$b_ic_0+b_{i-1}c_1+\cdots+b_0c_i+d_i=gd_{i+1}$$

donde d_{i+1} es un entero positivo. Por tanto

$$\begin{aligned}(b_0,b_1b_2\cdots)(c_0,c_1c_2\cdots) &= (b_0c_0),(b_0c_1+b_1c_0)(b_0c_2+b_1c_1+b_2c_0)\\ &\quad (b_0c_3+b_1c_2+b_2c_1+b_3c_0)\cdots(g)\\ &= 1,000\cdots(g)\end{aligned}$$

y así $B^{-1}=c_0,c_1c_2\cdots$ Supongamos ahora que $B\in\mathbf{Q}_g$ tiene inverso, B^{-1}, entonces

$$\begin{aligned}1,000\cdots(g) &= B\cdot B^{-1}\\ &= (b_0c_0),(b_0c_1+b_1c_0)(b_0c_2+b_1c_1+b_2c_0)\\ &\quad (b_0c_3+b_1c_2+b_2c_1+b_3c_0)\cdots(g)\end{aligned}$$

esto implica que

$$b_0c_0\equiv 1 \mod(g)$$

Así que existe $t\in\mathbf{Z}$ tal que

$$b_0c_0+g(t)=1$$

Por tanto $(b_0,g)=1$.

Por último, definimos $\frac{A}{B}=AB^{-1}$ siempre que B tenga inverso. ◇

EJEMPLOS

Sean $a=\frac{3}{17}$ y $b=\frac{58}{39}\in\mathbf{Q}_5$. Por la Definición 1 del Capítulo 1 $\left|\frac{3}{17}\right|_5=1$ y $\left|\frac{58}{39}\right|_5=1$ y además

$$\frac{3}{17}=4,\overline{12102401323420433}\quad(5)\qquad \frac{58}{39}=2,\overline{4220}\quad(5)$$

entonces

$$a+b=6,543024013234204 33\quad(5)$$

Utilizando el Teorema 22 encontramos una expresión para $a+b$, para ello determinamos los u_i.

$a+b=6\times5^0+5\times5^1+4\times5^2+3\times5^3+0\times5^4+2\times5^5+4\times5^6+0\times5^7+1\times5^8+3\times5^9+2\times5^{10}+3\times5^{11}+4\times5^{12}+2\times5^{13}+0\times5^{14}+4\times5^{15}+3\times5^{16}+3\times5^{17}$

entonces $u_0=6$; $u_1=5$; $u_2=4$; $u_3=3$; $u_4=0$; $u_5=2$; $u_6=4$; $u_7=0$; $u_8=1$; $u_9=3$; $u_{10}=2$; $u_{11}=3$; $u_{12}=4$; $u_{13}=2$; $u_{14}=0$; $u_{15}=4$; $u_{16}=3$; $u_{17}=3$

$$\begin{array}{ll}0\le 6-5v_0\le 4 & 0\le(3+0)-5v_9\le 4\\ v_0=1\quad a_0=1 & v_9=0\quad a_9=3\\ 0\le(5+1)-5v_1\le 4 & 0\le(2+0)-5v_{10}\le 4\\ v_1=1\quad a_1=1 & v_{10}=0\quad a_{10}=2\\ 0\le(4+1)-5v_2\le 4 & 0\le(3+0)-5v_{11}\le 4\\ v_2=1\quad a_2=0 & v_{11}=0\quad a_{11}=3\\ 0\le(3+1)-5v_3\le 4 & 0\le(4+0)-5v_{12}\le 4\\ v_3=0\quad a_3=4 & v_{12}=0\quad a_{12}=4\\ 0\le(0+0)-5v_4\le 4 & 0\le(2+0)-5v_{13}\le 4\\ v_4=0\quad a_4=1 & v_{13}=0\quad a_{13}=2\\ 0\le(2+0)-5v_5\le 4 & 0\le(0+0)-5v_{14}\le 4\\ v_5=0\quad a_5=2 & v_{14}=0\quad a_{14}=0\\ 0\le(4+0)-5v_6\le 4 & 0\le(4+0)-5v_{15}\le 4\\ v_6=0\quad a_6=4 & v_{15}=0\quad a_{15}=4\\ 0\le(0+0)-5v_7\le 4 & 0\le(3+0)-5v_{16}\le 4\\ v_7=0\quad a_7=0 & v_{16}=0\quad a_{16}=3\\ 0\le(1+0)-5v_8\le 4 & 0\le(3+0)-5v_{17}\le 4\\ v_8=0\quad a_8=1 & v_{17}=0\quad a_{17}=3\end{array}$$

Por tanto

$$a+b=1,\overline{10412401323420433}\quad(5)$$

Con los mismos valores de a y b obtenemos que

$$a - b = 2.(-3)0(-1)02401323420433 \quad (5)$$

y nuevamente utilizando el Teorema 22 encontramos que:

$a - b = 2 \times 5^0 + (-3) \times 5^1 + 0 \times 5^2 + (-1) \times 5^3 + 0 \times 5^4 + 2 \times 5^5 + 4 \times 5^6 + 0 \times 5^7 + 1 \times 5^8 + 3 \times 5^9 + 2 \times 5^{10} + 3 \times 5^{11} + 4 \times 5^{12} + 2 \times 5^{13} + 0 \times 5^{14} + 4 \times 5^{15} + 3 \times 5^{16} + 3 \times 5^{17}$

entonces los u_i son $u_0 = 2$; $u_1 = -3$; $u_2 = 0$; $u_3 = -1$; $u_4 = 0$; $u_5 = 2$; $u_6 = 4$; $u_7 = 0$; $u_8 = 1$; $u_9 = 3$; $u_{10} = 2$; $u_{11} = 3$; $u_{12} = 4$; $u_{13} = 2$; $u_{14} = 0$; $u_{15} = 4$; $u_{16} = 3$; $u_{17} = 3$

$$\begin{array}{cc}
0 \le 2 - 5v_0 \le 4 & 0 \le (3+0) - 5v_9 \le 4 \\
v_0 = 0 \quad a_0 = 2 & v_9 = 0 \quad a_9 = 3 \\
0 \le (-3+0) - 5v_1 \le 4 & 0 \le (2+0) - 5v_{10} \le 4 \\
v_1 = -1 \quad a_1 = 2 & v_{10} = 0 \quad a_{10} = 2 \\
0 \le (0-1) - 5v_2 \le 4 & 0 \le (3+0) - 5v_{11} \le 4 \\
v_2 = -1 \quad a_2 = 4 & v_{11} = 0 \quad a_{11} = 3 \\
0 \le (-1-1) - 5v_3 \le 4 & 0 \le (4+0) - 5v_{12} \le 4 \\
v_3 = -1 \quad a_3 = 3 & v_{12} = 0 \quad a_{12} = 4 \\
0 \le (0-1) - 5v_4 \le 4 & 0 \le (2+0) - 5v_{13} \le 4 \\
v_4 = -1 \quad a_4 = 4 & v_{13} = 0 \quad a_{13} = 2 \\
0 \le (2-1) - 5v_5 \le 4 & 0 \le (0+0) - 5v_{14} \le 4 \\
v_5 = 0 \quad a_5 = 1 & v_{14} = 0 \quad a_{14} = 0 \\
0 \le (4+0) - 5v_6 \le 4 & 0 \le (4+0) - 5v_{15} \le 4 \\
v_6 = 0 \quad a_6 = 4 & v_{15} = 0 \quad a_{15} = 4 \\
0 \le (0+0) - 5v_7 \le 4 & 0 \le (3+0) - 5v_{16} \le 4 \\
v_7 = 0 \quad a_7 = 0 & v_{16} = 0 \quad a_{16} = 3 \\
0 \le (1+0) - 5v_8 \le 4 & 0 \le (3+0) - 5v_{17} \le 4 \\
v_8 = 0 \quad a_8 = 1 & v_{17} = 0 \quad a_{17} = 3
\end{array}$$

Retomando los valores encontrados para estos dígitos, tenemos que el número $a - b$ en forma canónica es

$$a - b = 2,\overline{2434140132342043 3} \quad (5)$$

Para el producto $a \cdot b$ tenemos

$$a \cdot b = 8,(18)(16)(20)(10)(10)(18)(20)(14)(18)(18)(22)(30)(30)(22)(20)(26)(26) \quad (5)$$

como en los casos anteriores, utilizando el Teorema 22 obtenemos la expresión

$a \cdot b = 8 \times 5^0 + (18) \times 5^1 + (16) \times 5^2 + (20) \times 5^3 + (10) \times 5^4 + (10) \times 5^5 + (18) \times 5^6 + (20) \times 5^7 + (14) \times 5^8 + (18) \times 5^9 + (18) \times 5^{10} + (22) \times 5^{11} + (30) \times 5^{12} + (30) \times 5^{13} + (22) \times 5^{14} + (20) \times 5^{15} + (26) \times 5^{16} + (26) \times 5^{17}$

entonces los u_i son $u_0 = 8$; $u_1 = 18$; $u_2 = 16$; $u_3 = 20$; $u_4 = 10$; $u_5 = 10$; $u_6 = 18$; $u_7 = 20$; $u_8 = 14$; $u_9 = 18$; $u_{10} = 18$; $u_{11} = 22$; $u_{12} = 30$; $u_{13} = 30$; $u_{14} = 22$; $u_{15} = 20$; $u_{16} = 26$; $u_{17} = 26$

$$0 \leq 8 - 5v_0 \leq 4 \qquad 0 \leq (18+3) - 5v_9 \leq 4$$
$$v_0 = 1 \quad a_0 = 3 \qquad v_9 = 4 \quad a_9 = 1$$
$$0 \leq (18+1) - 5v_1 \leq 4 \qquad 0 \leq (18+4) - 5v_{10} \leq 4$$
$$v_1 = 3 \quad a_1 = 4 \qquad v_{10} = 4 \quad a_{10} = 2$$
$$0 \leq (16+3) - 5v_2 \leq 4 \qquad 0 \leq (22+4) - 5v_{11} \leq 4$$
$$v_2 = 3 \quad a_2 = 4 \qquad v_{11} = 5 \quad a_{11} = 1$$
$$0 \leq (20+3) - 5v_3 \leq 4 \qquad 0 \leq (30+5) - 5v_{12} \leq 4$$
$$v_3 = 4 \quad a_3 = 3 \qquad v_{12} = 7 \quad a_{12} = 0$$
$$0 \leq (10+4) - 5v_4 \leq 4 \qquad 0 \leq (30+7) - 5v_{13} \leq 4$$
$$v_4 = 2 \quad a_4 = 4 \qquad v_{13} = 7 \quad a_{13} = 2$$
$$0 \leq (10+2) - 5v_5 \leq 4 \qquad 0 \leq (22+7) - 5v_{14} \leq 4$$
$$v_5 = 2 \quad a_5 = 2 \qquad v_{14} = 5 \quad a_{14} = 4$$
$$0 \leq (18+2) - 5v_6 \leq 4 \qquad 0 \leq (20+5) - 5v_{15} \leq 4$$
$$v_6 = 4 \quad a_6 = 0 \qquad v_{15} = 5 \quad a_{15} = 0$$
$$0 \leq (20+4) - 5v_7 \leq 4 \qquad 0 \leq (26+5) - 5v_{16} \leq 4$$
$$v_7 = 4 \quad a_7 = 4 \qquad v_{16} = 6 \quad a_{16} = 1$$
$$0 \leq (14+4) - 5v_8 \leq 4 \qquad 0 \leq (26+6) - 5v_{17} \leq 4$$
$$v_8 = 3 \quad a_8 = 3 \qquad v_{17} = 6 \quad a_{17} = 2$$

Nuevamente, con los valores encontrados tenemos

$$a \cdot b = 3, \overline{4434204312102402}12(5)$$

Para efectuar la división $\frac{a}{b}$ primero encontramos el inverso de b utilizando el Teorema 23. Como $b = \frac{46}{39} = 2, \overline{4220}\ (5)$, $b = 2 \times 5^0 + 4 \times 5^1 + 2 \times 5^2 + 2 \times 5^3 + 0 \times 5^4$ donde $a_0 = 2$; $a_1 = 4$; $a_2 = 2$; $a_3 = 2$; $a_4 = 0$. Puesto que $(2,5) = 1$

$$5(-1) + 2(3) = 1$$
$$d_1 = 1 \quad c_0 = 3$$
$$4(3) + 2c_1 + 1 = 5d_2$$
$$d_2 = 3 \quad c_1 = 1$$
$$2(3) + 4(1) + 2c_2 + 3 = 5d_3$$
$$d_3 = 3 \quad c_2 = 1$$
$$2(3) + 2(1) + 4(1) + 2c_3 + 3 = 5d_4$$
$$d_4 = 3 \quad c_3 = 0$$
$$0(3) + 2(1) + 2(1) + 4(0) + 2c_4 + 3 = 5d_5$$
$$d_5 = 3 \quad c_4 = 4$$

con esto hemos determinado los c_i y por tanto

$$b^{-1} = 3,1104 \quad (5)$$

Mostraremos ahora que el producto $b \cdot b^{-1} = 1$. En efecto:

$$b \cdot b^{-1} = 6, (14)(12)(12)(12)$$

utilizando el Teorema 22 encontramos la expresión b^{-1} en Q_5 y así $b \cdot b^{-1} = 6 \times 5^0 + 14 \times 5^1 + 12 \times 5^2 + 12 \times 5^3 + 12 \times 5^4$ entonces $u_0 = 6$; $u_1 = 14$; $u_2 = 12$; $u_3 = 12$; $u_4 = 12$

$$0 \leq 6 - 5v_0 \leq 4 \qquad 0 \leq (12+3) - 5v_3 \leq 4$$
$$v_0 = 1 \quad a_0 = 1 \qquad v_3 = 3 \quad a_3 = 0$$
$$0 \leq (14+1) - 5v_1 \leq 4 \qquad 0 \leq (12+3) - 5v_4 \leq 4$$
$$v_1 = 3 \quad a_1 = 0 \qquad v_4 = 3 \quad a_4 = 0$$
$$0 \leq (12+3) - 5v_2 \leq 4$$
$$v_2 = 3 \quad a_2 = 0$$

Por tanto

$$b \cdot b^{-1} = 1,0000 \quad (5)$$

Una vez encontrado el inverso de b obtenemos que

$$\frac{a}{b} = 12,(7)(11)(6)(19)(11)(22)(10)(7)(18)(26)(30)(21)(25)(14)(26)(29)(24) \quad (5)$$

pero utilizando el Teorema 22 encontramos una expresión para $\frac{a}{b}$,

$\frac{a}{b} = 12 \times 5^0 + 7 \times 5^1 + 11 \times 5^2 + 6 \times 5^3 + 19 \times 5^4 + 11 \times 5^5 + 22 \times 5^6 + 10 \times 5^7 + 7 \times 5^8 + 18 \times 5^9 + 26 \times 5^{10} + 30 \times 5^{11} + 21 \times 5^{12} + 25 \times 5^{13} + 14 \times 5^{14} + 26 \times 5^{15} + 29 \times 5^{16} + 24 \times 5^{17}$

entonces $u_0 = 12$; $u_1 = 7$; $u_2 = 11$; $u_3 = 6$; $u_4 = 19$; $u_5 = 11$; $u_6 = 22$; $u_7 = 10$; $u_8 = 7$; $u_9 = 18$; $u_{10} = 26$; $u_{11} = 30$; $u_{12} = 21$; $u_{13} = 25$; $u_{14} = 14$; $u_{15} = 26$; $u_{16} = 29$; $u_{17} = 24$

$$0 \leq 12 - 5v_0 \leq 4 \qquad 0 \leq (18+2) - 5v_9 \leq 4$$
$$v_0 = 2 \quad a_0 = 2 \qquad v_9 = 4 \quad a_9 = 0$$
$$0 \leq (7+2) - 5v_1 \leq 4 \qquad 0 \leq (26+4) - 5v_{10} \leq 4$$
$$v_1 = 1 \quad a_1 = 4 \qquad v_{10} = 6 \quad a_{10} = 0$$
$$0 \leq (11+1) - 5v_2 \leq 4 \qquad 0 \leq (30+6) - 5v_{11} \leq 4$$
$$v_2 = 2 \quad a_2 = 2 \qquad v_{11} = 7 \quad a_{11} = 1$$
$$0 \leq (6+2) - 5v_3 \leq 4 \qquad 0 \leq (21+7) - 5v_{12} \leq 4$$
$$v_3 = 1 \quad a_3 = 3 \qquad v_{12} = 5 \quad a_{12} = 3$$
$$0 \leq (19+1) - 5v_4 \leq 4 \qquad 0 \leq (25+5) - 5v_{13} \leq 4$$
$$v_4 = 4 \quad a_4 = 0 \qquad v_{13} = 6 \quad a_{13} = 0$$
$$0 \leq (11+4) - 5v_5 \leq 4 \qquad 0 \leq (14+6) - 5v_{14} \leq 4$$
$$v_5 = 3 \quad a_5 = 0 \qquad v_{14} = 4 \quad a_{14} = 0$$
$$0 \leq (22+3) - 5v_6 \leq 4 \qquad 0 \leq (26+4) - 5v_{15} \leq 4$$
$$v_6 = 5 \quad a_6 = 0 \qquad v_{15} = 6 \quad a_{15} = 0$$
$$0 \leq (10+5) - 5v_7 \leq 4 \qquad 0 \leq (29+6) - 5v_{16} \leq 4$$
$$v_7 = 3 \quad a_7 = 0 \qquad v_{16} = 7 \quad a_{16} = 0$$
$$0 \leq (7+3) - 5v_8 \leq 4 \qquad 0 \leq (24+7) - 5v_{17} \leq 4$$
$$v_8 = 2 \quad a_8 = 0 \qquad v_{17} = 6 \quad a_{17} = 1$$

Por tanto

$$\frac{a}{b} = 2,\overline{423000000013000001} \quad (5)$$

Capítulo 5

La descomposición de $\mathbf{Q}_g$

A continuación estudiaremos la estructura de $\mathbf{Q}_g$ para el caso de $g \geq 2$ y mostraremos que este anillo es la suma directa de campos p-ádicos. Recordemos que si A es un campo y ω valuación de A entonces $\hat{A}_\omega$ es un campo, en particular, $|\ |_p$ y $|\ |_{p^r}$ son valuaciones de Q entonces $\mathbf{Q}_p$ y $\mathbf{Q}_{p^r}$ son campos.

Sea $a = p^t \frac{a_0}{b_0}$ con $p \nmid a_0$ y $p \nmid b_0$. Por el algoritmo de la división $t = rt_0 + \alpha$ con $0 \leq \alpha < |r|$. Es claro que de lo anterior $|a|_p = p^{-t}$; $|a|_{p^r} = p_0^{-rt}$ y

$$-t \leq -rt_0 \qquad (i)$$

Por otro lado $\alpha < |r|$ implica que

$$0 \leq r - (1 + \alpha)$$

así que

$$r - 1 - t = r - 1 - rt_0 - \alpha = -rt_0 + r - (1 + \alpha) \geq -rt_0 \qquad (ii)$$

Juntando (i) y (ii) obtenemos

$$-t \leq -rt_0 \leq r - 1 - t$$

Por tanto

$$p^{-t} \leq p^{-rt_0} \leq p^{r-1} p^{-t}$$

así que

$$|a|_p \leq |a|_{p^r} \leq p^{r-1} |a|_p$$

Sea $\{a_n\}$ una sucesión nula en Q con respecto a $|\ |_p$, entonces

$$0 = \lim_{n \longrightarrow \infty} |a_n|_p \leq \lim_{n \longrightarrow \infty} |a_n|_{p^r} \leq \lim_{n \longrightarrow \infty} p^{r-1} |a_n|_p = p^{r-1} \lim_{n \longrightarrow \infty} |a_n|_p = 0$$

Por tanto

$$\lim_{n \longrightarrow \infty} |a_n|_{p^r} \longrightarrow 0$$

así que $\{a_n\}$ también es sucesión nula con respecto a $|\ |_{p^r}$. Usando un argumento similar es fácil ver que :

i) $|a|_g = 1 \Longleftrightarrow a = \frac{r}{s}$; $g \nmid r$; $(g, s) = 1$

ii) $\{a_n\}$ es una sucesión acotada con respecto a $|\ |_p$ si y sólo si $\{a_n\}$ es sucesión acotada con respecto a $|\ |_{p^r}$.

iii) $\{a_n\}$ es una sucesión fundamental con respecto a $|\ |_p$ si y sólo si $\{a_n\}$ es sucesión fundamental con respecto a $|\ |_{p^r}$.

Lema 5 *Para todo* $r \geq 2$ $\mathbf{Q}_p = \mathbf{Q}_{p^r}$.

Demostración: Puesto que $\mathbf{Q}_p$ y $\mathbf{Q}_{p^r}$ son completos entonces es suficiente probar una contención. Sea $A = \sum_{n=-f}^{\infty} A_n (p^r)^n \in \mathbf{Q}_{p^r}$ la serie canónica para A; aquí f es algún entero y los coeficientes A_n son tales que $0 \leq A_n \leq p^r - 1$. Para la base p éstos coeficientes se pueden escribir como

$$A_n = \sum_{k=0}^{N-1} a_{nr+k} p^k \qquad (n = -f, -f+1, \ldots) \qquad (i)$$

donde los nuevos coeficientes a_{nr+k} son tales que $0 \leq a_{nr+k} \leq p-1$. Por lo tanto A se puede expresar como el número p-ádico

$$A = \sum_{m=-fr}^{\infty} a_m p^m.$$

Para expresar un número p-ádico como p^r-ádico únicamente combinamos todos los términos $a_m p^m$ para los cuales $nr \leq m \leq nr + r - 1$ y después se utiliza (i).

◇

Nota: En el lenguaje de la topología de conjuntos se tiene que $|\ |_p$ y $|\ |_{p^r}$ definen topologías equivalentes en $\mathbf{Q}$. Este resultado se puede generalizar:

Corolario 10 $\mathbf{Q}_{p^{r_1}} = \mathbf{Q}_{p^{r'_1}}$.

Demostración: Sea $a \in \mathbf{Q}$ y $g = p_1^{r_1}$; $g' = p_1^{r'_1}$ con

$$|a|_g = g^{-t} \qquad |a|_{g'} = g'^{-t_1}$$

$$|a|_g = g^{-t} = p_1^{-r_1 t} \Longrightarrow a = p_1^{r_1 t} \frac{a_1}{b_1} \qquad p_1^{r_1} \nmid a_1 \ ; \ p_1^{r_1} \nmid b_1$$

también

$$|a|_{g'} = g'^{-t_1} = p_1^{-r'_1 t} \Longrightarrow a = p_1^{r'_1 t} \frac{a'_1}{b'_1} \qquad p_1^{r'_1} \nmid a'_1 \ ; \ p_1^{r'_1} \nmid b'_1$$

Usando el algoritmo de la división

$r_1 t = r' t_1 z + \alpha$ con $0 \leq \alpha < r'_1 t$, entonces $r'_1 t_1 z \leq r_1 t$, $-r_1 t \leq -r'_1 t_1 z$ y

$$p_1^{-r_1 t} \leq p_1^{-r'_1 t_1 z}$$

$$(p_1^{r_1})^{-t} \leq (p_1^{r'_1})^{t_1 z} = (p_1^{r'_1})^{-t_1} (p_1^{r'_1})^{t_1 (1-z)}$$

$$(p_1^{r_1})^{-t} \leq (p_1^{-r'_1})^{t_1} C$$

donde $C = (p_1^{r'_1})^{t_1(1-z)}$; $g^{-t} \leq (g')^{-t_1} C$. Entonces $|a|_g \leq C |a|_{g'}$ donde $C > 0$.

Sea $\{a_n\}$ una sucesión nula con la valuación $|\ |_{g'}$ entonces $\lim_{n\to\infty} |a_n|_{g'} = 0$ y

$$0 \leq \lim_{n\to\infty} |a_n|_g \leq C \lim_{n\to\infty} |a_n|_{g'} = 0.$$

Por tanto $\{a_n\}$ es sucesión nula con la valuación $|\ |_g$.

Si $\{a_n\}$ sucesión fundamental con $|\ |_{g'}$ entonces $\lim_{n\to\infty} |a_m - a_n|_{g'} = 0$ y

$$0 \leq \lim_{n\to\infty} |a_m - a_n|_g \leq C \lim_{n\to\infty} |a_m - a_n|_{g'} = 0$$

Por tanto $\{a_n\}$ es una sucesión fundamental con la valuación $|\ |_g$

Por último, si $\{a_n\}$ es una sucesión acotada con $|\ |_{g'}$, y $|a_n|_{g'} \leq M$ para alguna $M > 0$, entonces existe M' tal que

$$0 \leq |a_n|_g \leq C |a_n|_{g'} \leq CM = M'.$$

Por tanto $\{a_n\}$ es una sucesión acotada con $|\ |_g$. Con lo anterior tenemos que sucesiones acotadas, nulas y fundamentales con $|\ |_{g'}$ son también sucesiones acotadas, nulas y fundamentales con $|\ |_g$.

Sea $a \in \mathbf{Q}$ y $g = p_1^{r_1} p_2^{r_2}$; $g' = p_1^{r'_1} p_2^{r'_2}$ donde

$$|a|_g = g^{-t} \qquad |a|_{g'} = g^{-t_1}$$

entonces

$$|a|_g = g^{-t} = p_1^{-r_1 t} p_2^{-r_2 t} \Longrightarrow a = p_1^{r_1 t} p_2^{r_2 t} \frac{a_2}{b_2} \qquad p_1^{r_1 t} p_2^{r_2 t} \nmid a_2 \ ; \ p_1^{r_1} p_2^{r_2} \nmid b_2$$

y

$$|a|_g' = g^{-t_1} = p_1^{-r'_1 t} p_2^{-r'_2 t} \Longrightarrow a = p_1^{r'_1 t} p_2^{r'_2 t} \frac{a'_2}{b'_2} \qquad p_1^{r'_1 t} p_2^{r'_2 t} \nmid a'_2 \ ; \ p_1^{r'_1} p_2^{r'_2} \nmid b'_2.$$

Por el algoritmo de la división $r_1 t = r'_1 z_1 t_1 + \alpha_1$ con $0 \leq \alpha_1 < r'_1 t$ y $r_2 t = r'_2 z_2 t_1 + \alpha_2$ con $0 \leq \alpha_2 < r'_2 t$. Por lo tanto

$$-r_1 t \leq -r'_1 t_1 z_1 \ \text{ y } \ -r_2 t \leq -r'_2 t_1 z_2$$

$$p_1^{-r_1 t} \leq p_1^{-r'_1 t_1 z_1} \text{ y } p_2^{-r_2 t} \leq p_2^{-r'_2 t_1 z_2}$$

$$p_1^{-r_1 t} p_2^{-r_2 t} \leq p_1^{-r'_1 t_1 z_1} p_2^{-r'_2 t_1 z_2}$$

$$(p_1^{r_1} p_2^{r_2})^{-t} \leq (p_1^{r'_1} p_2^{r'_2})^{-t_1 z_1 z_2} = (p_1^{r'_1} p_2^{r'_2})^{-t_1} (p_1^{-r'_1} p_2^{r'_2})^{t_1 (1 - z_1 z_2)}$$

$$(p_1^{r_1} p_2^{r_2})^{-t} \leq (p_1^{-r'_1} p_2^{r'_2})^{-t_1} C$$

donde

$$C = (p_1^{r'_1} p_2^{r'_2})^{t_1 (1 - z_1 z_2)}$$

$$g^{-t} \leq (g')^{-t_1} C$$

$$|a|_g \leq C |a|_{g'}^{t_1} \quad \text{tal que } C > 0$$

Sea $\{a_n\}$ una sucesión nula con la valuación $|\ |_{g'}$, entonces $\lim_{n \to \infty} |a_n|_{g'} = 0$ y

$$0 \leq \lim_{n \to \infty} |a_n|_g \leq C \lim_{n \to \infty} |a_n|_{g'} = 0$$

Por tanto $\{a_n\}$ es una sucesión nula con la valuación $|\ |_g$. En general tenemos

i) $\{a_n\}$ es una sucesión acotada con $|\ |_{g'}$ si y sólo si $\{a_n\}$ es sucesión acotada con $|\ |_g$

ii) $\{a_n\}$ sucesión fundamental con $|\ |_{g'}$ si y sólo si $\{a_n\}$ es sucesión fundamental con $|\ |_g$.

Por medio de inducción veremos que este resultado se puede generalizar para el caso $g = p_1^{r_1} \ldots p_s^{r_s}$ y $g' = p_1^{r'_1} \ldots p_s^{r'_s}$

Teorema 24 *Sean* $g = p_1^{r_1} \ldots p_s^{r_s}$ y $g' = p_1^{r'_1} \ldots p_s^{r'_s}$ *entonces* $\mathbf{Q}_g = \mathbf{Q}_{g'}$.

Demostración: Sea $a \in \mathbf{Q}$, entonces

$$|a|_g = g^{-t} \quad a = p^{t_1 \frac{a_s}{b_s}} = p_1^{r_1 t} \ldots p_s^{r_s t} \frac{a_s}{b_s}$$

donde

$$p_1^{r_1} \ldots p_s^{r_s} \nmid a_s \ ; \ p_1^{r_1} \ldots p_s^{r_s} \nmid b_s$$

de forma análoga:

$$|a|_{g'} = g^{-t_1} \quad a = g^{t_1} \frac{a'_s}{b'_s} = p_1^{r'_1 t} \ldots p_s^{r'_s t} \frac{a_s}{b_s}$$

donde

$$p_1^{r'_1} \ldots p_s^{r'_s} \nmid a_s \, ; \, p_1^{r'_1} \ldots p_s^{r'_s} \nmid b_s$$

Por el algoritmo de la división

$$r_1 t = r_1' z_1 t_1 + a_1 \quad con \quad 0 \le a_1 < r_1' t$$
$$\vdots$$
$$r_s t = r_s' z_s t_1 + a_s \quad con \quad 0 \le a_s < r_s' t$$

entonces $-r_1 t \le -r_1' t_1 z_1 ; \ldots ; -r_s t \le -r_s' t_1 z_s$

$$p_1^{-r_1 t} \le p_1^{-r_1' t_1 z_1} \ldots \quad p_s^{-r_s t} \le p_s^{-r_s' t_1 z_s}$$

$$p_1^{-r_1 t} \ldots \quad p_s^{-r_s t} \le p_1^{-r_1' t_1 z_1} \ldots \quad p_s^{-r_s' t_1 z_s}$$

$$(p_1^{r_1'} \ldots p_s^{r_s'})^{-t} \le (p_1^{r_1'} \ldots p_s^{r_s'})^{-t_1 z_1 z_2 \ldots z_s} = (p_1^{r_1'} \ldots p_s^{r_s'})^{-t_1} (p_1^{-r_1'} \ldots p_s^{r_s'})^{t_1(1 - z_1 z_2 \ldots z_s)}$$

$$(p_1^{r_1'} \ldots p_s^{r_s'})^{-t} \le (p_1^{-r_1'} \ldots p_s^{r_s'})^{-t_1} C$$

donde

$$C = (p_1^{r_1'} \ldots p_s^{r_s'})^{t_1(1 - z_1 z_2 \ldots z_s)}$$
$$g^{-t} \le g^{-t_1} C$$

Por tanto

$$|a|_g \le C |a|_{g'} \quad \text{donde } C > 0$$

Concluyendo:

i) $\{a_n\}$ es una sucesión acotada con $|\ |_{g'}$ si y sólo si $\{a_n\}$ es sucesión acotada con $|\ |_g$

ii) $\{a_n\}$ es una sucesión nula con $|\ |_{g'}$ si y sólo si $\{a_n\}$ es sucesión nula con $|\ |_g$.

iii) $\{a_n\}$ es una sucesión fundamental con $|\ |_{g'}$ si y sólo si $\{a_n\}$ es sucesión fundamental con $|\ |_g$

así que $|\ |_g$ y $|\ |_{g'}$ definen la misma completación de $\mathbb{Q}$, es decir, $\mathbb{Q}_g = \mathbb{Q}_{g'}$.

Corolario 11 *Sea $a \in \mathbb{Q}$ y $g = p_1 \ldots p_s$; $g^* = p_1 \ldots p_{s-1}$, entonces las completaciones $\mathbb{Q}_g$ y $\mathbb{Q}_{g^*}$ son distintas.*

Demostración: Basta dar $\{a_n\}$ sucesión nula en $\mathbb{Q}_g$ que no sea sucesión nula en $\mathbb{Q}_{g^*}$. Sea $\{g^{*n} \mid n \in \mathbb{N}\}$ sucesión nula con $|\ |_{g^*}$, entonces

$$g^{*n} = g^* \frac{a}{b} \qquad |g^{*n}|_{g^*} = (g^*)^n = \frac{1}{(g^*)^n} \xrightarrow[n \to \infty]{} 0$$

$\{g^{*n}\}$ sucesión nula con $|\ |_{g^*}$. Pero no es sucesión nula con la valuación $|\ |_g$ para ello expresamos a g^* en términos de g

$$g^{*n} = g^n \frac{a}{b}$$

$$(g^*)^n = p_1^n \ldots p_{s-1}^n = (p_1^n \ldots p_{s-1}^n)(p_1 \ldots p_{s-1} p_s)^0 = g^0 \frac{a}{b}$$

donde $a = g^{*n}$ y $b = 1$

$$|g^{*n}|_g = 1 \qquad \text{para toda } n \in \mathbb{N}$$

y no es sucesión nula con $|\ |_g$. Por tanto las completaciones $\mathbb{Q}_g$ y $\mathbb{Q}_{g^*}$ son distintas. ◇

Sea $\{a_n\} \subset \mathbb{Q}$ sucesión fundamental con $|\ |_g$, entonces para $m, n \gg 0$

$$a_m - a_n = g^i \frac{m}{qs} = p_i^i \frac{m}{qs} \qquad \text{para } i = 1, 2, \ldots$$

de esta igualdad se sigue que $\{a_n\}$ es sucesión fundamental con $|\ |_g$.

Por otro lado si $\{a_n\}$ es sucesión fundamental con $|\ |_p$, donde $i = 1, 2, \ldots$ entonces para $m, n \gg 0$.

$a_m - a_n = p_i^j \frac{a_i}{b_i} \quad p_i \nmid a_i \quad p_i \nmid b_i \quad (i = 1, 2, \ldots)$ y $j \gg 1$

$$|a_m - a_n|_{p_i} = p_i^{-j_i} = \frac{1}{p_i^{-j_i}} \longrightarrow 0 \qquad (iii)$$

Pero

$$a_m - a_n = (p_1 p_2 \ldots p_s)^\alpha \frac{a}{b} = p_i (p_1 \ldots p_i^\wedge \ldots p_s) \frac{a}{b}$$

y la igualdad (*iii*) implica que $\alpha \gg 0$. Por tanto $\{a_n\}$ es sucesión fundamental con $|\ |_g$. Sea $A_i = \lim_{n \to \infty}^{p_i} a_n$ entonces hemos probado que existe $A = \lim_{n \to \infty}^{g} a_n$ si y sólo si existe $A = \lim_{n \to \infty}^{p_i} a_n$ para $\quad (i = 1, 2, \ldots)$.

Definición 15 *Si $A =< A_1, A_2, \ldots, A_s >$ entonces A_i se llama la i-ésima componente de A donde el número de componentes A_s es el mismo que el de g.*

Probemos ahora que la sucesión $\{A_1, A_2, \ldots A_s\}$ no depende de la sucesión que se tenga en cada entrada, sino que depende de la factorización de g.

Lema 6 *Las componentes A_i de A no dependen de la sucesión $\{a_n\}$.*

Demostración: Sea $\{a'_n\}$ sucesión fundamental distinta a $\{a_n\}$ y

$$A = \lim_{n \to \infty}^{g} a'_n$$

entonces $\{a_n - a'_n\}$ es sucesión nula. Para $n \gg 0 \quad a_n - a'_n = \frac{pq' - p'q}{qq'}$ donde $g \nmid pq' - p'q$ y $(g, qq') = 1$. Esto implica $pq' - p'q = g^\alpha h = p_1^\alpha p_2^\alpha \ldots p_s^\alpha h$ entonces $\{a_n - a'_n\}$ es sucesión nula con $|\ |_{p_1}, |\ |_{p_2}, \ldots, |\ |_{p_s}$ y así las sucesiones $\{a_n\}$ y $\{a'_n\}$ tienen los mismos p_i-límites. ◇

Si $A \in \mathbb{Q}_g$ se define como la suma de una serie infinita

$$A = \sum_{n=1}^{\infty} a_n(g)$$

las componentes A_i de A son las series

$$A_i = \sum_{n=1}^{\infty} a_n(p_i) \qquad (i = 1, 2, \ldots).$$

Supongamos que el número g-ádico A se dá por su serie canónica

$$A = \sum_{n=-f}^{\infty} a_n g^n(g).$$

Para encontrar el componente A_i de A escribimos $g = g^* p_i$ y tenemos

$$A_i = \sum_{n=-f}^{\infty} a_n g^{*n} p_i^n(p_i)$$

que no es la serie p_i-ádica de A_i. Usando el Teorema 21 determinamos dicha serie. De las reglas generales para suma, diferencia y producto de límites g-ádicos y p-ádicos se sigue que si tenemos $B \in \mathbb{Q}_g$ con componentes

$$B_1, B_2, \ldots, B_s$$

entonces

$$A+B=<A_1+B_1,A_2+B_2,\ldots,A_s+B_s>$$
$$A-B=<A_1-B_1,A_2-B_2,\ldots,A_s-B_s>$$
$$AB=<A_1B_1,A_2B_2,\ldots,A_sB_s>$$

Para escojer las componentes A_i de A de una manera arbitraria en los campos respectivos $\mathbb{Q}_{p_i}$ para $i=1,2,\ldots$ construiremos para cada subíndice i un número g-ádico E^i que tiene 1 en la i-ésima componente y 0 en lo demás. Hagamos

$$q_i=\frac{p_1p_2\ldots p_s}{p_i}=p_1p_2\ldots p_i^{\wedge}\ldots p_s \quad (i=1,2,\ldots)$$

$$e_n^i=\frac{q_i^n}{(p_i^n+q_i^n)} \qquad (i=1,\ldots,s \;\; ; \;\; n=1,2,\ldots)$$

entonces

$$1-e_n^i=\frac{p_i^n}{(p_i^n+q_i^n)}$$

Observación 8 *Como los primos $p_1,p_2,\ldots,p_s$ son distintos*

$$p_i \nmid (p_i^n+q_i^n)$$

y además

$$(g,p_i^n+q_i^n)=1$$

Lema 7 *Para $i,\lambda=1,\ldots,s$ la sucesión $\{e_n^i\}$ es nula para $i\neq\lambda$.*

Demostración: Si $i\neq\lambda$

$$\begin{aligned}e_n^i &= \frac{q_i^n}{(p_i^n+q_i^n)}\\ &= \frac{p_1^n,\ldots,p_{\lambda}^n,\ldots,p_{r-1}^n,p_{r+1}^n,\ldots,p_s^n}{(p_i^n+p_1^n,\ldots,p_{\lambda}^n,\ldots,p_{r-1}^n,p_{r+1}^n,\ldots,p_s^n)}\\ &= p_{\lambda}^n\left(\frac{p_1^n,\ldots,p_{\lambda}^n,\ldots,p_{r-1}^n,p_{r+1}^n,\ldots,p_s^n}{(p_i^n+p_1^n,\ldots,p_{\lambda}^n,\ldots,p_{r-1}^n,p_{r+1}^n,\ldots,p_s^n)}\right)\end{aligned}$$

$$|e_n^i|_{p_\lambda}=p_{\lambda}^{-n}=\frac{1}{p_{\lambda}^n}\underset{n\to\infty}{\longrightarrow}0$$

Si $i=\lambda$

$$\begin{aligned}e_n^i &= \frac{q_i^n}{(p_i^n+q_i^n)}\\ &= \frac{p_1^n,\ldots,p_{\lambda-1}^n,p_{\lambda+1},\ldots,p_s^n}{(p_{\lambda}^n+p_1^n,\ldots,p_{\lambda-1}^n,p_{\lambda+1},\ldots,p_s^n)}\\ &= p_{\lambda}^0\left(\frac{p_1^n,\ldots,p_{\lambda}^n,\ldots,p_{r-1}^n,p_{r+1}^n,\ldots,p_s^n}{(p_i^n+p_1^n,\ldots,p_{\lambda-1}^n,p_{\lambda+1},\ldots,p_s^n}\right)\end{aligned}$$

$$|e_n^i|_{p_\lambda}=p_{\lambda}^0=1$$

entonces tenemos que los límites p_λ-ádicos existen y son

$$\lim_{n\to\infty}{}^{p_\lambda} e_n^i=\delta_{i,\lambda}=\begin{cases}1 & \text{si } i=\lambda\\ 0 & \text{si } i\neq\lambda\end{cases}$$

también los límites g-ádicos existen y estan dados por

$$\lim_{n\to\infty}{}^{g} e_n^i=E^i$$

donde E^i tiene como componentes

$$E^i =< \delta_{1i}, \delta_{2i}, \ldots, \delta_{si} >$$

mas aún

$$E^i E^\lambda = \begin{cases} 1 & \text{si } i = \lambda \\ 0 & \text{si } i \neq \lambda \end{cases}$$

$$E^1 + E^2 + \ldots E^s =< 1, 1, \ldots, 1 >= 1$$

◇

Teorema 25 *Sea A_i un número p_i-ádico con $i = 1, 2, \ldots, s$ entonces existe un único $A \in \mathbf{Q}_g$ tal que*

$$A =< A_1, A_2, \ldots, A_s > .$$

Demostración: Para cada subíndice $i = 1, 2, \ldots, s$ denotemos por $\{a_n^i\} \subset \mathbf{Q}$ una sucesión fundamental p_i-ádica tal que

$$A_i = \lim_{n \to \infty}^{p_i} a_n^i$$

Para $i \neq \lambda$ la sucesión $\{a_n^i\}$ puede no tener limite p_λ-ádico y no estar acotada por $|\ |_{p_\lambda}$. Recordemos que la sucesión $\{e_n^i\}$ satisface

$$\lim_{n \to \infty}^{p_i} e_n^i = \begin{cases} 1 & \text{si } i = \lambda \\ 0 & \text{si } i \neq \lambda \end{cases}$$

escojamos una subsucesión $\{e_{m_n}^i\}$ de la sucesión $\{e_n^i\}$ tal que

$$\lim_{n \to \infty}^{p_\lambda} e_{m_n}^i = \begin{cases} 1 & \text{si } i = \lambda \\ 0 & \text{si } i \neq \lambda \end{cases}$$

entonces claramente

$$\lim_{n \to \infty}^{p_\lambda} a_n^i e_{m_n}^i = \begin{cases} A_i & \text{si } i = \lambda \\ 0 & \text{si } i \neq \lambda \end{cases}$$

Puesto que $\{a_n^i\}$ es sucesión fundamental entonces por el Teorema 19

$$\lim_{n \to \infty}^{g} a_n^i e_{m_n}^i =< 0, 0, \ldots, A_i, \ldots, 0 >$$

Sea $A = \{a_n\}$ definida por $\sum_{n=1}^{s} a_n^i e_{m_n}^i$ (i=1,2 ...), entonces

$$\begin{aligned} A &= \lim_{n \to \infty}^{g} a_n = \lim_{n \to \infty}^{g} \sum_{i=1}^{s} a_n^i e_{m_n}^i \\ &= \sum_{i=1}^{s} \lim_{n \to \infty}^{g} a_n^i e_{m_n}^i \\ &= \sum_{i=1}^{s} < 0, \ldots, A_i, \ldots, 0 > \\ &= < A_1, A_2, \ldots, A_s > \end{aligned}$$

Ahora sea $A' \in \mathbf{Q}_g$ tal que

$$A' =< A_1', A_2', \ldots, A_s' >$$

entonces

$$A - A' =< A_1 - A_1', A_2 - A_2', \ldots, A_s - A_s' >=< 0, \ldots, 0 >$$

lo que quiere decir que $A - A'$ esta representado por una sucesión nula en cada entrada, es decir, $A - A' = 0$ en $\mathbf{Q}_g$. Por tanto $A = A'$

◇

Corolario 12

$$Q_r = Q_{p_1} \oplus Q_{p_2} \oplus \cdots \oplus Q_{p_r}$$

COMENTARIO.- Si $r \geq 2$ entonces Q_r tiene divisores de cero diferentes de cero, a saber, sean a y $b \in Q_6$ donde

$$a = 2,10101 \quad (6) \qquad b = 3,12022 \quad (6)$$

efectuaremos el producto donde mostraremos que si $a, b \neq 0$ $a \cdot b = 0$

$$a \cdot b = 6,5555(11) \quad (6)$$

como se hizó anteriormente utilizaremos el Teorema 22 para la expresión de $a \cdot b$.

Sea $6 \times 6^0 + 5 \times 6^1 + 5 \times 6^2 + 5 \times 6^3 + 5 \times 6^4 + (11) \times 6^5$

entonces los u_i son $u_0 = 6$; $u_1 = 5$; $u_2 = 5$; $u_3 = 5$; $u_4 = 5$; $u_5 = 11$

$$\begin{array}{cc} 0 \leq 6 - 6v_0 \leq 5 & 0 \leq (5+1) - 6v_3 \leq 5 \\ v_0 = 1 \quad a_0 = 0 & v_3 = 1 \quad a_3 = 0 \\ 0 \leq (5+1) - 6v_1 \leq 5 & 0 \leq (5+1) - 6v_4 \leq 5 \\ v_1 = 1 \quad a_1 = 0 & v_4 = 1 \quad a_4 = 0 \\ 0 \leq (5+1) - 6v_2 \leq 5 & 0 \leq (11+1) - 6v_5 \leq 5 \\ v_2 = 1 \quad a_2 = 0 & v_5 = 2 \quad a_5 = 0 \end{array}$$

Tomaremos ahora los valores encontrados para estos dígitos, el número $a \cdot b$ en forma canónica queda

$$a \cdot b = 0,00000 \quad (6)$$

Por lo anterior Q_r no puede ser campo si $r \geq 2$

Bibliografía

[1]K. Mahler, *p-adic numbers and their functions*, Cambridge University Press, 2a ed. N. Y. 1980.

[2] G. Bachman, *Introduction to p-adic numbers and valuation theory*, Academic Press, 1a ed. N. Y. 1964.

[3] I. Niven, *Introducción a la Teoría de los Números*, Limusa, 2a ed. México. 1982.

[4] W. Rudin, *Principios de análisis matemático*, Ed. McGraw Hill, 3a edición, México 1986.