Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Grado

Grado en Matemáticas

El cuerpo de los números p-ádicos. Propiedades algebraicas y topológicas.

Autora: Elena Dimitriadis Bermejo

Tutor: Jesús M. Domínguez Gómez

Índice general

Introducción

A lo largo de este trabajo vamos a estudiar las propiedades algebraicas y topológicas del cuerpo de los números p-ádicos. Introducidos explícitamente por primera vez por el matemático alemán Kurt Hensel en 1897, estos números surgieron de la analogía entre el anillo de los enteros $\mathbb{Z}$ junto con su cuerpo de fracciones $\mathbb{Q}$ y el de los polinomios $\mathbb{C}[X]$ con su cuerpo de fracciones $\mathbb{C}(X)$. En efecto, ambos son dominios de factorización única, los polinomios de la forma $(X-a)$ con $a \in \mathbb{C}$ haciendo el rol de los números primos en $\mathbb{Z}$. Ahora bien, esta comparación es algo más profunda de lo que parece a simple vista: por ejemplo, de la misma forma que fijando un $(X-a) \in \mathbb{C}[X]$ podemos escribir cualquier polinomio como una suma finita de potencias de $(X-a)$ multiplicadas por elementos de $\mathbb{C}$, en el caso de los enteros podríamos fijar un número primo p y escribir cualquier entero como suma finita de potencias de él, es decir, escribirlo en base p. Tomando entonces el cuerpo de fracciones de los polinomios, podríamos de nuevo escribir cualquier elemento de él como una serie de potencias de un $(X-a)$ (el desarrollo de Laurent), pero por un lado estas podrían tener potencias con exponentes negativos y por otro ya no serían necesariamente finitas, por lo que no tendrían un análogo claro en términos de números primos en $\mathbb{Z}$. Así, la idea de K. Hensel consistió en intentar utilizar la analogía vista previamente para construir un cuerpo en que existiesen todos los desarrollos en serie de potencias del primo p. [Gou93, págs. 5-6]

Esta manera de ver los números p-ádicos, aunque es interesante, y el estudio más pormenorizado de estos últimos saca a la luz más puntos de contacto entre ellos y el cuerpo $\mathbb{C}(X)$, no es en absoluto el camino que hemos elegido para enfocar el presente trabajo. En cambio, nos centraremos en el hecho de que el cuerpo $\mathbb{Q}_p$ de los números p-ádicos es una compleción de los racionales a partir de una norma diferente del valor absoluto usual, lo que nos da un punto de comparación importante con uno de los grandes sujetos de estudio del Grado de Matemáticas: el cuerpo $\mathbb{R}$ de los números reales. En un principio nuestro proyecto consistía en estudiar la topología de $\mathbb{Q}_p$ (con una pequeña digresión hacia el conjunto triádico de Cantor a fin de demostrar ciertas propiedades topológicas de $\mathbb{Z}_p$) y las propiedades algebraicas de $\mathbb{Q}_p$ y de su subanillo $\mathbb{Z}_p$, así como adentrarnos en las extensiones del cuerpo $\mathbb{Q}_p$, tanto finitas como infinitas, para llegar a su clausura algebraica y la compleción de esta. Finalmente, hemos tenido que dejar fuera este último apartado sobre las extensiones por falta de tiempo. Aunque nuestra

fuente de información principal ha sido el libro «p-adic Analysis Compared with Real», de Svetlana Katok [Kat07], hemos tomado también en muchos casos el punto de vista o los resultados de otros textos, principalmente «A Course in p-adic Analysis», de Alain M. Robert [Rob00]. Además, bastantes de los resultados que se presentan aquí estaban propuestos como ejercicios en la bibliografía original, y han sido desarrollados con el fin de ahondar y completar el trabajo expuesto. Para no sobrecargar de citas nuestro texto, hemos decidido mencionar al principio de cada capítulo el libro en que nos hemos basado de forma predominante y citar únicamente los resultados que hayamos tomado de otras fuentes.

A la hora de redactar hemos estructurado nuestro trabajo en seis capítulos. Así, tenemos un pequeño capítulo introductorio, en el que presentamos algunos resultados sobre los números reales que, aunque ampliamente conocidos, es útil recordar para tenerlos frescos a la hora de comparar con el caso de los números p-ádicos. En particular, nos centramos en la demostración de que $\mathbb{R}$ es una compleción de $\mathbb{Q}$ con la norma usual, definiendo para ello el concepto de compleción de un espacio métrico, y, por otra parte, de que cualquier número real puede expresarse como una serie de potencias de 10 de la forma

$$\sum_{i=k}^{\infty} a_i 10^{-i},$$

donde k es un entero y los coeficientes a_i son naturales entre 0 y 9.

A continuación, y antes de adentrarnos en el estudio de $\mathbb{Q}_p$, nos ocupamos de forma general de los cuerpos normados. Así, en el capítulo 2 introducimos las normas no arquimedianas, que serán muy importantes para los resultados posteriores puesto que la norma p-ádica $|\,.\,|_p$ es una norma no arquimediana, y damos algunos resultados básicos con respecto a ellas. También trabajamos un poco con el concepto de normas equivalentes, y finalmente damos un método general para crear la compleción de un cuerpo normado cualquiera a partir del conjunto de sus sucesiones de Cauchy. Esto nos permite por fin llegar a construir el objeto del que nos vamos a ocupar a lo largo de todo el resto del presente proyecto: el cuerpo de los números p-ádicos, $\mathbb{Q}_p$, que es una compleción de $\mathbb{Q}$ para la norma p-ádica.

Una vez que tenemos todos los útiles necesarios para nuestro objetivo, el capítulo 3 trata cuestiones básicas sobre $\mathbb{Q}_p$. Así, empezamos definiendo la norma p-ádica, y vemos que no sólo no es equivalente al valor absoluto usual, sino que toda norma no trivial sobre $\mathbb{Q}$ es equivalente a dicho valor absoluto, si es arquimediana, o a la norma p-ádica para un determinado primo p si no lo es (teorema de Ostrowski). Esto significa que al construir los cuerpos $\mathbb{Q}_p$ hemos agotado todas las posibilidades de compleciones del cuerpo normado $\mathbb{Q}$. A continuación explicitamos la construcción de $\mathbb{Q}_p$, y vemos que, de forma similar a lo que pasa con los números reales, podemos expresar cualquier número p-ádico

como una serie de potencias de p de la forma

$$\sum_{i=k}^{\infty} a_i p^i$$

donde k es un entero y los coeficientes a_i son naturales entre 0 y $p-1$, lo que llamamos el «desarrollo canónico» de un número p-ádico. Esta escritura nos permite definir el anillo de los enteros p-ádicos, $\mathbb{Z}_p$, como los números p-ádicos en cuyo desarrollo k es un natural. Una vez hecho esto sólo nos queda un apartado, en el que tratamos la relación entre las dos estructuras que acabamos de construir y el cuerpo de base, $\mathbb{Q}$. Ahí descubrimos que, al igual que en los números reales, un elemento de $\mathbb{Q}_p$ pertenece al subcuerpo $\mathbb{Q}$ si y sólo si su desarrollo canónico es periódico.

Ahora que conocemos más el cuerpo de los p-ádicos podemos tratar cuestiones algebraicas un poco más profundas. En el capítulo siguiente (capítulo 4) hablamos de raíces de polinomios con coeficientes en $\mathbb{Z}_p$, enunciando para ello el Lema de Hensel, que nos da unas condiciones suficientes para poder afirmar la existencia de raíces de un polinomio en $\mathbb{Z}_p[X]$. Este resultado, además de su utilidad directa, nos sirve para demostrar algunos otros resultados interesantes, como por ejemplo la condición necesaria y suficiente para la existencia de raíces cuadradas de enteros en el cuerpo $\mathbb{Q}_p$ si $p \neq 2$, o la caracterización del grupo cociente $\mathbb{Q}_p^*/\left(\mathbb{Q}_p^*\right)^2$, donde $\left(\mathbb{Q}_p^*\right)^2$ es el subgrupo formado por los cuadrados en $\mathbb{Q}_p^*$. Asimismo, de forma más indirecta nos permite hablar de las raíces de la unidad. Por último, cerramos el capítulo 4 con algunos resultados de Teoría de Anillos en $\mathbb{Z}_p$ (vemos, por ejemplo, que se trata de un anillo local). La mayoría de los resultados planteados en este apartado son ciertos en general para anillos de valoración discreta, pero al no conocer a fondo el lenguaje de estos damos demostraciones particulares para nuestro caso.

En el capítulo 5 damos un paso atrás respecto a nuestro sujeto de estudio y hablamos de los límites proyectivos en distintas estructuras (conjuntos, espacios topológicos y grupos). Estos resultados, aparte de su interés intrínseco, nos permitirán en el capítulo siguiente demostrar que los espacios $\mathbb{Z}_p$ son homeomorfos entre sí para todo p primo. Pero el principal objetivo se alcanza en el último apartado: en efecto, en él vemos que el anillo topológico $\mathbb{Z}_p$ con la topología derivada de la norma p-ádica es isomorfo (como anillo topológico) al límite proyectivo de los cuerpos $\mathbb{Z}/p^n\mathbb{Z}$ a los que dotamos de la topología discreta.

Y por último, cerramos el presente trabajo estudiando la topología de $\mathbb{Q}_p$ en el capítulo 6. Aquí descubrimos resultados como que las bolas abiertas de $\mathbb{Q}_p$ son también cerradas, o que forman un conjunto numerable. Aún así, durante la mayor parte del capítulo centramos nuestra atención en el conjunto triádico de Cantor, un subconjunto de la recta real homeomorfo a $\mathbb{Z}_2$. Una vez hecho esto, utilizamos los límites proyectivos para demostrar que dos espacios métricos compactos, perfectos y 0-dimensionales son siempre homeomorfos, lo cual

nos indica que en particular todos los espacios $\mathbb{Z}_p$ son homeomorfos entre sí. Y finalmente, acabamos con unas palabras sobre las representaciones de $\mathbb{Z}_p$ en $\mathbb{R}^n$. Tras ver que el conjunto de Cantor no es más que una representación unidimensional, damos alguna representación en dimensión superior.

Y, sin más dilación, les dejamos con el cuerpo del trabajo. Esperamos que les guste.

Capítulo 1

Preliminares: completitud de $\mathbb{R}$ y forma decimal.

En este capítulo vamos a recordar resultados muy básicos sobre el cuerpo de los reales $\mathbb{R}$. Para ello utilizaremos principalmente los apuntes de la asignatura de Cálculo Infinitesimal de Javier Sanz y los de Topología de C. Ana Núñez, así como «Numbers, Sets and Axioms» de A. G. Hamilton [Ham82, págs. 44-49]. Aunque se trata de resultados ya conocidos, nos servirán posteriormente al hacer comparaciones entre el caso real y el caso p-ádico.

1.1. $\mathbb{R}$ es compleción de $\mathbb{Q}$.

Definición 1.1.1. *Sea una sucesión $\{a_n\}_{n=0}^{\infty}$ en un espacio métrico (X,d). Se dice que $\{a_n\}_{n=0}^{\infty}$ es de Cauchy si para todo ϵ positivo existe un n_0 natural tal que para todo $n,m \geq n_0$, $d(a_n,a_m) < \epsilon$.*

Definición 1.1.2. *Sea una sucesión $\{a_n\}_{n=0}^{\infty}$ en un espacio métrico (X,d). Se dice que converge hacia a si para todo ϵ positivo existe n_0 natural tal que para todo $n > n_0$, $d(a_n,a) < \epsilon$. Una sucesión que converge se llama convergente.*

Definición 1.1.3. *Sea (X,d) un espacio métrico. Se dice que X es completo si en él toda sucesión de Cauchy es convergente.*

Definición 1.1.4. *Se dice que un espacio métrico X es una compleción de A si A es denso en X y X es completo.*

Teorema 1.1.5. *Sea (X,d) un espacio métrico completo, y A un subconjunto de X. Entonces A es completo si y sólo si es cerrado en X. En particular, la adherencia de A en X es una compleción de A.*

Demostración. Empecemos señalando que todo espacio métrico cumple el primer axioma de numerabilidad, y por lo tanto si $A \subset X$ métrico y $x \in X$,

$$x \in \bar{A} \Leftrightarrow \exists\ \{a_n\}_{n=0}^{\infty} \subset A \ / \ a_n \to x$$

Suponemos que A no es cerrado en X. Entonces $\exists\ x \in \bar{A}$ con $x \notin A$. Por tanto, $\exists\ \{a_n\}_{n=0}^{\infty} \subset A\ /\ a_n \to x \notin A$. La sucesión $\{a_n\}$ es convergente, luego de Cauchy. Pero $\{a_n\}$ no converge en A. Luego A no es completo.

Vamos con la segunda implicación. Sea A cerrado en X y $\{a_n\} \subset A$ una sucesión de Cauchy. En particular, $\{a_n\}$ es de Cauchy en X, que es completo. Por tanto, es convergente en X: existe un $x \in X$ límite de la sucesión. Esto significa que $x \in \bar{A}$. Por definición de cerrado, $A = \bar{A}$. Luego $\{a_n\}$ es convergente en A, y A es completo.

En cuanto a la última afirmación, es evidente: $\bar{A}$ es cerrado en X, luego, por lo anterior, completo, y A es denso en $\bar{A}$ por definición.

Q.E.D.

Ahora que tenemos definidos todos los conceptos necesarios, podemos proceder a ver que $\mathbb{R}$ es una compleción de $\mathbb{Q}$ para el valor absoluto usual. Nos limitaremos a demostrar que $\mathbb{R}$ es completo, sin hacer la demostración de la densidad.

Teorema 1.1.6. $\mathbb{Q}$ *es denso en* $\mathbb{R}$.

Teorema 1.1.7. $\mathbb{R}$ *con el valor absoluto usual es completo.*

Demostración. Sabemos que toda sucesión $\{a_n\}_{n=0}^{\infty}$ de Cauchy de números reales está acotada, y que $\limsup a_n$ y $\liminf a_n$ son finitos. Razonemos por reducción al absurdo.
Suponemos que $\exists\ \{a_n\}_{n=0}^{\infty}$ de Cauchy no convergente. Entonces $\liminf a_n < \limsup a_n$ y podemos definir $\epsilon = \frac{1}{3}(\limsup a_n - \liminf a_n)$. Por tanto, para todo $n_0 \in \mathbb{N}$ existen $n, m \geq n_0$ tales que $a_n < \liminf a_n + \epsilon$ y $a_m > \limsup a_n - \epsilon$. Luego $\forall n_0 \in \mathbb{N}\ \exists\ n, m \geq n_0 /\ \mid a_n - a_m \mid > 3\epsilon - 2\epsilon = \epsilon$, y la sucesión no es de Cauchy. Absurdo. En consecuencia, $\mathbb{R}$ es completo.

Q.E.D.

Corolario 1.1.8. $\mathbb{R}$ *es una compleción de* $\mathbb{Q}$.

Es posible definir el cuerpo de los números reales exclusivamente a partir de la forma decimal de los mismos, es decir, de $\sum_{i=k}^{\infty} a_i 10^{-i}$, pero esto hace la definición de las operaciones en $\mathbb{R}$ mucho más difícil. Aún así, nos gustaría poder utilizar dicha forma decimal, puesto que forma parte de nuestra intuición y es útil para ciertas demostraciones. En consecuencia, a continuación vamos a probar algunos resultados sobre ella.

1.2. Forma decimal de $\mathbb{R}$

Teorema 1.2.1. *Sea* $x = \sum_{i=k}^{\infty} a_i 10^{-i}$, *con* $k \in \mathbb{Z}$ *y* a_i *un natural entre* 0 *y* 9 *para todo* i. *Entonces* x *es un número real. Inversamente, si* x *es un real, existe una sucesión* $\{a_n\}_{n=k}^{\infty}$ *con* a_i *entre* 0 *y* 9 *para todo* i *tal que* $x = \sum_{i=k}^{\infty} a_i 10^{-i}$ *o* $x = -\sum_{i=k}^{\infty} a_i 10^{-i}$.

Demostración. La primera afirmación es bastante simple de demostrar. Por definición de serie,

$$\sum_{i=k}^{\infty} a_i 10^{-i} = \lim_{n\to\infty} \sum_{i=k}^{n} a_i 10^{-i}$$

Luego $x = \sum_{i=k}^{\infty} a_i 10^{-i}$ es el límite de una sucesión de números racionales, y por tanto reales. Está claro que $\left\{\sum_{i=k}^{n} a_i 10^{-i}\right\}$ es de Cauchy:

$$|\sum_{i=k}^{n} a_i 10^{-i} - \sum_{i=k}^{m} a_i 10^{-i}| < 10^{min(n,m)}$$

Como $\mathbb{R}$ es completo, $x \in \mathbb{R}$.

Vamos ahora con la segunda. Supongamos que $x > 0$ (en caso contrario, tomamos la forma decimal de $-x$ y la multiplicamos por -1). Entonces, por la propiedad arquimediana, $\exists\ r \in \mathbb{N}$ tal que $r > x$. Tomamos el mínimo natural que lo cumple, y definimos $n = r - 1$, que es el mayor entero menor o igual que x. Entonces podemos escribir $x = n + r_0$, con $r_0 \in [0, 1)$.
Ahora consideramos $10r_0$. Sabemos que $0 \leq 10r_0 < 10$. Con el mismo procedimiento que antes, tomamos como a_1 el mayor entero menor o igual a $10r_0$. Evidentemente, $a_i \in \{0, ..., 9\}$. Escribimos $10r_0 = a_i + r_1$ y obtenemos que $r_0 = a_1 10^{-1} + r_1 10^{-1}$, por tanto que $x = a + a_1 10^{-1} + r_1 10^{-1}$.
Iterando el proceso, obtenemos una sucesión $\left\{a + \sum_{i=1}^{n} a_i 10^{-i} + r_n 10^{-n}\right\}_{n=1}^{\infty}$ que converge hacia x. Por tanto, $x = a + \sum_{i=1}^{n} a_i 10^{-i}$.

Q.E.D.

Nota. *Obsérvese que en ningún momento se ha hablado de que dicha expresión decimal sea única. De hecho, es bien sabido que no lo es:* $1 = \sum_{i=1}^{n} 9 \cdot 10^{-i}$*, por ejemplo. Esto va a ser una diferencia notable con el caso p-ádico, en el que la forma de serie sí que cumple la unicidad.*

En cambio, la condición de pertenencia o no a $\mathbb{Q}$ de un elemento de la compleción es muy parecida en los casos real y p-ádico: tiene que ver con la periodicidad en su forma de serie. Para poder comparar más tarde, vamos a dar aquí el resultado en $\mathbb{R}$.

Teorema 1.2.2. *Un elemento de* $\mathbb{R}$ *es un número racional si y sólo si su expresión decimal es periódica.*

Demostración. Sea $x \in \mathbb{Q}$. Demostremos que su expresión decimal es periódica. Para ello partimos de la construcción del teorema anterior: si $x \in \mathbb{Q}$, r_0 también. Entonces existen $p, q \in \mathbb{N}$ con $(p, q) = 1$ y $q \neq 0$ tales que $r_0 = \frac{p}{q}$. Entonces

$$r_0 = \frac{p}{q} = a_1 10^{-1} + r_1 10^{-1} \Rightarrow q r_1 = 10p - a_1 q \Rightarrow 0 \leq r_1 = \frac{10p - a_1 q}{q} < 1$$

y $r_1 = \frac{p_1}{q}$ con $p_1 \in \mathbb{N}$, $0 \leq p_1 < q$.
De forma equivalente, $\forall n \in \mathbb{N},\ r_n = \frac{p_n}{q}$ con $p_n \in \mathbb{N}$, $0 \leq p_n < q$. Existe entonces

$i < j \in \mathbb{N}$ tales que $p_i = p_j$, y por tanto $r_i = r_j$. A partir de aquí el proceso será idéntico, y la expresión decimal se repetirá periódicamente (con un periodo de $j - i$ términos).

Sea $x = \sum_{i=k}^{\infty} a_i 10^{-i}$ periódico, con $r, s \in \mathbb{N}$ tales que a_{r+1}, ... a_s son los términos que se repiten. Entonces tenemos

$$x = \sum_{i=k}^{r} a_i 10^{-i} + \sum_{i=r+1}^{s} a_i 10^{-i} + \sum_{i=r+1}^{s} a_i 10^{-i-s} + \sum_{i=r+1}^{s} a_i 10^{-i-2s} + ... =$$

$$\sum_{i=k}^{r} a_i 10^{-i} + \sum_{i=r+1}^{s} a_i 10^{-i} + 10^{-s} \sum_{i=r+1}^{s} a_i 10^{-i} + 10^{-2s} \sum_{i=r+1}^{s} a_i 10^{-i} + ... =$$

$$\sum_{i=k}^{r} a_i 10^{-i} + (\sum_{i=r+1}^{s} a_i 10^{-i})(\sum_{i=0}^{\infty} 10^{-s \cdot i}) = \sum_{i=k}^{r} a_i 10^{-i} + (\sum_{i=r+1}^{s} a_i 10^{-i}) \frac{1}{1 - 10^{-s}},$$

por la fórmula de la suma de series geométricas. Luego $x \in \mathbb{Q}$.

Q.E.D.

Nota. *Es importante darse cuenta de que la elección aquí de la base 10 es circunstancial, propiciada por razones históricas, y que esta construcción podría hacerse con cualquier otro entero sin ninguna alteración de peso.*

Capítulo 2

Cuerpos normados.

En este capítulo vamos a utilizar principalmente «p-adic Analysis Compared with Real», de Svetlana Katok [Kat07, págs. 6-19], aunque para alguna de las demostraciones nos decantaremos por «A Course in p-adic Analysis», de Alain M. Robert, por una cuestión de preferencia personal. Utilizaremos la definición de cuerpo que dan Atiyah y MacDonald en su libro «Introduction to Commutative Algebra».

Definición 2.0.1. *Un cuerpo es un anillo $\mathbb{K}$ en el que $1 \neq 0$ y todo elemento no nulo es inversible respecto a la multiplicación (es una unidad).* [AM69, pág. 3]

Definición 2.0.2. *Sea $\mathbb{K}$ un cuerpo. Una norma (o valor absoluto) es una aplicación $\| \, . \, \|$ del cuerpo $\mathbb{K}$ a los reales positivos que cumple que*

1. $\| x \| = 0$ *si y sólo si* $x = 0$.
2. $\forall x, y \in \mathbb{K}, \ \| xy \| = \| x \| \cdot \| y \|$.
3. $\forall x, y \in \mathbb{K}, \ \| x + y \| \leq \| x \| + \| y \|$ *(desigualdad triangular).*

Nota. *Cuando se utiliza el término «valor absoluto» se suele usar la notación $| \, . \, |$ en lugar de la de $\| \, . \, \|$. En nuestro caso, seguiremos la notación del libro de Svetlana Katok, y por lo tanto denotaremos la norma genérica como $\| \, . \, \|$ aunque luego en el caso p-ádico escribamos $| \, . \, |_p$.*

Esta definición nos proporciona, de forma inmediata, una serie de propiedades básicas de la norma. Enunciamos algunas de ellas, aunque sin demostrarlas.

Propiedades 2.0.3. *Para todo $x, y \in \mathbb{K}$, la norma cumple:*

1. $\| x \| = \| -x \|$.
2. $\| x \pm y \| \geq | \, \| x \| - \| y \| \, |$.
3. *Para todo* $n \in \mathbb{N}$, $\| n \| \leq n$.

2.1. Normas no-arquimedianas.

Definición 2.1.1. *Sea $\| \cdot \|$ una norma sobre un cuerpo $\mathbb{K}$. Se dice que es no-arquimediana si cumple que $\forall x, y \in \mathbb{K}$, $\| x + y \| \leq max(\| x \|, \| y \|)$. Esta condición se llama desigualdad triangular fuerte. En ese caso, el espacio métrico derivado de esta norma se denomina ultramétrico.*

Teorema 2.1.2. *Estas afirmaciones son equivalentes:* [Rob00, págs. 82-83]

a) $\| \cdot \|$ es no-arquimediana.

b) Para todo $x \in \mathbb{K}$ con $\| x \| \leq 1$, $\| 1 + x \| \leq 1$.

c) Para todo $n \in \mathbb{Z}$, $\| n \| \leq 1$.

d) Para todo $x, y \in \mathbb{K}$ con $x \neq 0$, no existe un entero n tal que $\| nx \| > \| y \|$.

e) El conjunto $\{\| n \| \ / \ n \in \mathbb{Z}\}$ está acotado superiormente, es decir, $\sup\{\| n \|\} < \infty$

Demostración. Veamos $a) \Rightarrow c)$ por inducción.
La base de la inducción es inmediata: $\| 1 \| = 1 \leq 1$.
Sea $n \in \mathbb{N}$. Suponemos que $\| n - 1 \| \leq 1$. Como $\| n \| = \| (n-1) + 1 \| \leq$ máx$(\| n-1 \|, 1)$ gracias a la definición de norma no-arquimediana, por hipótesis de inducción tenemos que $\| n \| \leq 1$.
Como $\| x \| = \| -x \|$, $b)$ se cumple para todo entero.

Ataquemos ahora $c) \Rightarrow b)$. Suponiendo que sea cierto $c)$, sea $x \in \mathbb{K}$ con $\| x \| \leq 1$. Utilizando el binomio de Newton, la desigualdad triangular y la hipótesis, en ese orden, obtenemos que

$$\forall n \in \mathbb{N},\ \| 1 + x \|^n = \| (1+x)^n \| = \| \sum \binom{n}{i} x^i \| \leq \sum \| \binom{n}{i} x^i \| \leq \sum \| x \|^i.$$

Como $\| x \| \leq 1$, tenemos que

$$\| 1 + x \|^n \leq (n+1) \Rightarrow \| 1 + x \| \leq (n+1)^{-n}$$

Sabemos que $(n+1)^{-n} \to 1$ cuando $n \to \infty$, luego $\| 1 + a \| \leq 1$.

Una vez visto esto, la implicación $b) \Rightarrow a)$ es sencilla. Sean $x, y \in \mathbb{K}$. Podemos suponer sin pérdida de generalidad que $\| x \| \geq \| y \|$. Luego tenemos que $\| x + y \| = \| x(1 + \frac{y}{x}) \|$ con $\| \frac{y}{x} \| \leq 1$. Se cumplen las condiciones para aplicar $b)$. Entonces $\| x + y \| = \| x(1 + \frac{y}{x}) \| \leq \| x \| =$ máx$(\| x \|, \| y \|)$, y hemos acabado.

Veremos fácilmente que $\neg d) \Rightarrow \neg c) \Rightarrow \neg e) \Rightarrow \neg d)$.
Si $\forall x, y, \in \mathbb{K}, \exists\ n \in \mathbb{N} / \ \| nx \| > \| y \|$, tomamos $x, y \in \mathbb{K}$ con $\| y \| > \| x \|$. $\exists\ n / \ \| nx \| > \| y \|$, luego $\exists\ n \in \mathbb{N}$ con $\| n \| > \frac{\| y \|}{\| x \|} > 1$ y tenemos $\neg c)$.

Si $\exists\ n_0 \in \mathbb{N}$ con $\| n_0 \| > 1$, tenemos que $\| n_0 \|^k = \| n_0^k \| \to \infty$ si $k \to \infty$. Como $\left\{ \| n_0^k \| / k \in \mathbb{N} \right\} \subset \{ \| n \| / n \in \mathbb{Z} \}$, concluimos que $\infty = \sup \left\{ \| n_0^k \| / k \in \mathbb{N} \right\} \leq \sup \{ \| n \| / n \in \mathbb{Z} \}$. En consecuencia, $\sup \{ \| n \| / n \in \mathbb{Z} \} = \infty$.

Y por último, si $\sup \{ \| n \| / n \in \mathbb{Z} \} = \infty$, sean $x, y \in \mathbb{K}$. Entonces, por definición de supremo, existe un $n_0 \in \mathbb{N}$ tal que $\| n_0 \| > \frac{\|y\|}{\|x\|}$ y $\| nx \| > \| y \|$.

Q.E.D.

Proposición 2.1.3. *Sea* $(\mathbb{K}, \| \cdot \|)$ *un cuerpo normado en que la norma* $\| \cdot \|$ *es no-arquimediana. Si dos elementos* a, b *de* $\mathbb{K}$ *cumplen que* $\| b - a \| < \| a \|$, *entonces la norma de* b *es igual a la norma de* a.

Demostración. Primero, tenemos que

$$\| b \| = \| b - a + a \| \leq \text{máx}(\| b - a \|,\ \| a \|) = \| a \|$$

por hipótesis y porque la norma es no-arquimediana.
Por otro lado, como la norma es no-arquimediana, tenemos

$$\| a \| = \| a - b + b \| \leq \text{máx}(\| b - a \|,\ \| b \|)$$

Ahora bien, si $\| b - a \| \geq \| b \|$ la desigualdad anterior nos daría que $\| a \| \leq \| b - a \|$, falso por hipótesis. Luego necesariamente $\| b - a \| \leq \| b \|$, y por lo tanto $\| a \| \leq \| b \|$. En consecuencia, $\| b \| = \| a \|$ y hemos acabado.

Q.E.D.

Nota. *Si tomamos esta proposición con* $b = a + x$ *y* $a = a$, *tenemos que si* $\| a \| > \| x \|$, *entonces* $\| a + x \| = \| a \|$ *(«el mayor se impone»).*

2.2. Normas equivalentes.

Definición 2.2.1. *Sean* $\| \cdot \|_1$ *y* $\| \cdot \|_2$ *normas de un mismo cuerpo* $\mathbb{K}$ *y* d_1 *y* d_2 *las distancias que estas inducen. Se dice que* $\| \cdot \|_1$ *y* $\| \cdot \|_2$ *son equivalentes si toda sucesión de Cauchy respecto a* d_1 *también lo es respecto a* d_2 *y viceversa.*

Notación. *Si dos normas son equivalentes se escribe* $\| \cdot \|_1 \sim \| \cdot \|_2$.

Lema 2.2.2. *Sea* $x \in \mathbb{K}$: $\| x \| < 1$ *si y sólo si* $\lim_{n \to \infty} x^n = 0$.

Demostración. Sea $x \in \mathbb{K}$ tal que $\| x \| < 1$. Como $\| x \|^n = \| x^n \|$ y $\lim_{n \to \infty} a^n = 0$ si $a \in [0, 1)$,

$$\lim_{n \to \infty} \| x^n \| = \lim_{n \to \infty} \| x \|^n = 0$$

y por definición de convergencia ($\lim_{n \to \infty} \| x^n - 0 \| = 0$) concluimos que $\lim_{n \to \infty} x^n = 0$.
Sea $x \in \mathbb{K}$ tal que $\| x \| \geq 1$. Entonces tenemos que $\forall n \in \mathbb{N}$, $\| x^n \| \geq 1$, y 0 no puede ser límite de $\{x^n\}_{n=0}^{\infty}$, que de hecho puede incluso no tener límite en absoluto.

Q.E.D.

Proposición 2.2.3. *Sean* $\| \, . \, \|_1$ *y* $\| \, . \, \|_2$ *normas equivalentes y* $x \in \mathbb{K}$. *Entonces*

1. $\| x \|_1 < 1$ *si y sólo si* $\| x \|_2 < 1$
2. $\| x \|_1 > 1$ *si y sólo si* $\| x \|_2 > 1$
3. $\| x \|_1 = 1$ *si y sólo si* $\| x \|_2 = 1$.

Es decir, la relación de orden entre 1 *y la norma de* x *es la misma independientemente de cuál de las dos normas se elija.*

Demostración. Sea $x \in \mathbb{K}$ tal que $\| x \|_1 < 1$. Entonces, por el lema anterior,

$$\| x \|_1 < 1 \Leftrightarrow \lim_{n \to \infty} x^n = 0 \text{ respecto a } \| \, . \, \|_1$$

y, por definición de normas equivalentes, esto ocurre si y sólo si

$$\lim_{n \to \infty} x^n = 0 \text{ respecto a } \| \, . \, \|_2 \Leftrightarrow \| x \|_2 < 1$$

Ahora, sea $x \in \mathbb{K}$ tal que $\| x \|_1 > 1$. Entonces tenemos que $\| \frac{1}{x} \|_1 = \frac{1}{\|x\|_1} < 1$ y, por el apartado 1, $\| \frac{1}{x} \|_2 < 1$. Por tanto, $\| x \|_2 > 1$.

En cuanto a la igualdad, una vez demostrado lo anterior es casi inmediato por reducción al absurdo. Sea $x \in \mathbb{K}$ tal que $\| x \|_1 = 1$, y supongamos que $\| x \|_2 \neq 1$. Entonces podemos tener que $\| x \|_2 < 1$ y por el apartado 1 eso implica que $\| x \|_1 < 1$, o $\| x \|_2 > 1$, y por el apartado 2 eso implica que $\| x \|_1 > 1$. En ambos casos tenemos una contradicción.

Q.E.D.

Corolario 2.2.4. *Si dos normas* $\| \, . \, \|_1$ *y* $\| \, . \, \|_2$ *son equivalentes, entonces una de ellas es trivial si y sólo si la otra también lo es.*

Corolario 2.2.5. *Dos normas equivalentes son necesariamente ambas arquimedianas o ambas no-arquimedianas.*

Demostración. Por la proposición anterior, si $\| \, . \, \|_1 \sim \| \, . \, \|_2$, tenemos que para todo $n \in \mathbb{Z}$ $\| n \|_1 < 1$ si y sólo si $\| n \| < 1$. Por el teorema 2.1.2 b), eso implica que una de las normas es arquimediana si y sólo si la otra también lo es.

Q.E.D.

Teorema 2.2.6. *Sean* $\| \, . \, \|_1$ *y* $\| \, . \, \|_2$ *normas de un mismo cuerpo* $\mathbb{K}$. *Entonces estas normas son equivalentes si y sólo si existe un número real positivo* α *tal que para todo* $x \in \mathbb{K}$ *tenemos* $\| x \|_1 = \| x \|_2^{\alpha}$.

Demostración. Empecemos por la implicación inversa, porque es la más sencilla. Suponemos que $\{a_n\}_{n=0}^{\infty}$ es una sucesión de Cauchy respecto a $\| \, . \, \|_1$ y que

$$\exists \, \alpha \in \mathbb{R}^+ / \, \forall x \in \mathbb{K} \;\; \| x \|_1 = \| x \|_2^{\alpha}$$

Sea $\epsilon > 0$. Entonces por definición de sucesión de Cauchy $\exists\ n_0 \in \mathbb{N}$ tal que $\forall n, m \leq n_0,\ \| a_n - a_m \|_1 < \epsilon^\alpha$. Por hipótesis, $\| a_n - a_m \|_1 = \| a_n - a_m \|_2^\alpha < \epsilon^\alpha$ y $\| a_n - a_m \|_2 < \epsilon$. Luego $\{a_n\}_{n=0}^\infty$ es de Cauchy respecto a $\| \ . \ \|_2$. El argumento contrario es idéntico, luego las dos normas son equivalentes.

Sea $\| \ . \ \|_1 \sim \| \ . \ \|_2$. Si $\| \ . \ \|_1$ es la norma trivial, entonces por el corolario anterior $\| \ . \ \|_2$ también lo es, y la propiedad se cumple trivialmente para cualquier α.

Si $\| \ . \ \|_1$ no es trivial, existe un $a \in \mathbb{K}^*$ tal que $\| a \|_1 \neq 1$. Podemos suponer que de hecho $\| a \|_1 < 1$ (si no es el caso, tomamos a^{-1}), entonces, por la proposición anterior, $\| a \|_2 < 1$, porque las normas son equivalentes. Entonces definimos α como

$$\alpha = \frac{\log \| a \|_1}{\log \| a \|_2}$$

Como las dos normas son menores que uno, los logaritmos son ambos negativos, y $\alpha > 0$.

Vamos a comprobar que este α cumple las condiciones del teorema. Sea $x \in \mathbb{K}$ tal que $\| a \|_1 < 1$ y definamos los siguientes conjuntos:

$$S_1 = \left\{ r = \frac{m}{n} / \ m, n \in \mathbb{N}\ y\ \| x \|_1^r < \| a \|_1 \right\},\ S_2 = \left\{ r = \frac{m}{n} / \ m, n \in \mathbb{N}\ y\ \| x \|_2^r < \| a \|_2 \right\}$$

Sea $r \in S_1$. Entonces tenemos

$$\| x \|_1^r < \| a \|_1 \Rightarrow \| x \|_1^m < \| a \|_1^n \Rightarrow \| \frac{x^m}{a^n} \|_1 < 1$$

y, por la proposición anterior,

$$\| \frac{x^m}{a^n} \|_2 < 1 \Rightarrow \| x \|_2^m < \| a \|_2^n \Rightarrow \| x \|_2^r < \| a \|_2 \ .$$

La prueba en la otra dirección es completamente simétrica, y por tanto tenemos que $S_1 = S_2$. Tomando logaritmos, podemos escribir que

$$S_1 = \left\{ r \in \mathbb{Q}^+ / \ r > \frac{\log \| a \|_1}{\log \| x \|_1} \right\} = \left\{ r \in \mathbb{Q}^+ / \ r > \frac{\log \| a \|_2}{\log \| x \|_2} \right\} = S_2$$

Ahora bien, esas fracciones tienen que ser iguales, porque si no $\exists\ r \in S_1$ y $r \notin S_2$ o viceversa, y sabemos que $S_1 = S_2$. Luego

$$\frac{\log \| a \|_1}{\log \| x \|_1} = \frac{\log \| a \|_2}{\log \| x \|_2} \Rightarrow \frac{\log \| x \|_1}{\log \| x \|_2} = \frac{\log \| a \|_1}{\log \| a \|_2} = \alpha$$

y de ahí obtenemos la conclusión pedida:

$$\frac{\log \| x \|_1}{\log \| x \|_2} = \alpha \Rightarrow \log \| x \|_1 = \log \| x \|_2^\alpha \Rightarrow \| x \|_1 = \| x \|_2^\alpha \ .$$

Si $x \in \mathbb{K}$ con $\| x \|_1 > 1$, tenemos que $\| x \|_1 = \| x^{-1} \|_1^{-1}$, y por lo que acabamos de demostrar, $\| x^{-1} \|_1 = \| x^{-1} \|_2^\alpha$. Esto demuestra que $\| x \|_1 = \| x \|_2^\alpha$. Para el caso de $\| x \|_1 = 1$ es evidente por la proposición anterior.

Q.E.D.

Proposición 2.2.7. *Sea* $|\ .\ |$ *el valor absoluto usual de* $\mathbb{Q}$. *Una función que cumpla que* $\| x \| = | x |^{\alpha}\ \ \forall x \in \mathbb{Q}$ *con* $\alpha > 0$ *es una norma sobre* $\mathbb{Q}$ *si y sólo si* α *es menor que* 1. *En ese caso, es equivalente al valor absoluto usual.*

Demostración. Las dos primeras características de la norma se mantienen de forma evidente. Luego las restricciones tienen que venir de la desigualdad triangular.
Una de estas implicaciones es muy sencilla. Si $\alpha > 1$, $| 1 + 1 |^{\alpha} = 2^{\alpha} >$
$| 1 |^{\alpha} + | 1 |^{\alpha} = 2$, luego no es una norma, porque no cumple la desigualdad triangular.

Ahora veamos el caso en que sí que es una norma. Sean $\alpha \leq 1$, $x, y \in \mathbb{Q}$ y suponemos, sin pérdida de generalidad, que $| y | \leq | x |$. Así $\frac{|y|}{|x|} \leq 1$.

$$\| x + y \| = | x + y |^{\alpha} \leq (| x | + | y |)^{\alpha} = | x |^{\alpha} (1 + \frac{| y |}{| x |}) \leq | x |^{\alpha} (1 + \frac{| y |}{| x |})$$

$$\leq | x |^{\alpha} (1 + \frac{| y |^{\alpha}}{| x |^{\alpha}}) = | x |^{\alpha} + | y |^{\alpha} = \| x \| + \| y \| .$$

Luego si $\alpha \leq 1$, la función $\| \ .\ \| = | \ .\ |^{\alpha}$es una norma. Con el teorema anterior, el que esta norma es equivalente al valor absoluto usual es inmediato.

Q.E.D.

En el caso de las normas no-arquimedianas, el resultado es sorprendentemente sencillo de demostrar.

Proposición 2.2.8. *Sea* $\| \ .\ \|$ *una norma no-arquimediana. Entonces, para todo* α *positivo, la función* $\| \ .\ \|^{\alpha}$ *también lo es.*

Demostración. Igual que en el caso anterior, las dos primeras condiciones de la norma son evidentes. Vamos con la desigualdad triangular. Sean $x, y \in \mathbb{K}$, y suponemos sin pérdida de generalidad que $\| x \| \geq \| y \|$. Si $\alpha > 0$ se verifica que

$$\| x + y \|^{\alpha} \leq (\text{máx}(\| x \|, \| y \|))^{\alpha} = \| x \|^{\alpha} .$$

Ahora tenemos dos posibilidades: $\| x \|^{\alpha} \geq \| y \|^{\alpha}$, y entonces hemos acabado, porque $\| x \|^{\alpha} = \text{máx}(\| x \|^{\alpha}, \| y \|^{\alpha})$, o $\| x \|^{\alpha} \leq \| y \|^{\alpha}$, y entonces $\| x \|^{\alpha} \leq$ máx$(\| x \|^{\alpha}, \| y \|^{\alpha})$.
Luego la función cumple la desigualdad triangular fuerte, y es una norma no-arquimediana.

Q.E.D.

2.3. Construcción de la compleción de un cuerpo normado.

Empezaremos enunciando algunos resultados que, aunque ampliamente conocidos, emplearemos de forma crucial a continuación.

Definición 2.3.1. *Decimos que una sucesión $\{a_n\}_{n=0}^{\infty}$ es nula si su límite es 0, es decir, si para todo $\epsilon > 0$ existe un $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$, $\| a_n \| < \epsilon$.*

Propiedades 2.3.2. *Sea $\mathbb{K}$ un cuerpo normado. Tenemos las siguientes propiedades:*

1. *Sea $\{a_n\}_{n=0}^{\infty}$ una sucesión de Cauchy en $\mathbb{K}$. Dicha sucesión es acotada.*
2. *Sean $\{a_n\}_{n=0}^{\infty}$ y $\{b_n\}_{n=0}^{\infty}$ sucesiones de Cauchy en $\mathbb{K}$. Entonces $\{a_n \pm b_n\}_{n=0}^{\infty}$ y $\{a_n b_n\}_{n=0}^{\infty}$ también son de Cauchy.*
3. *Sea $\{a_n\}_{n=0}^{\infty}$ una sucesión de Cauchy en $\mathbb{K}$. Si tiene una subsucesión nula, entonces $\{a_n\}_{n=0}^{\infty}$ también es nula.*
4. *Sean $\{a_n\}_{n=0}^{\infty}$ y $\{b_n\}_{n=0}^{\infty}$ dos sucesiones nulas de $\mathbb{K}$. Entonces $\{a_n \pm b_n\}_{n=0}^{\infty}$ también lo es.*
5. *Sea $\{a_n\}_{n=0}^{\infty}$ una sucesión nula y $\{b_n\}_{n=0}^{\infty}$ una sucesión acotada en $\mathbb{K}$. Entonces $\{a_n b_n\}_{n=0}^{\infty}$ es nula.*
6. *Sea $\{a_n\}_{n=0}^{\infty}$ una sucesión de Cauchy no nula. Entonces existe un valor $c > 0$ y un natural $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$, $\| a_n \| > c$.*

Por fin tenemos todos los útiles necesarios para construir la compleción de cualquier cuerpo normado.

Sea $(\mathbb{K}, \| \ . \ \|)$ un cuerpo normado. Tomamos el conjunto de las sucesiones de Cauchy en $\mathbb{K}$, $\{\mathbb{K}\}$. Por 2.3.2, apartado 2, este conjunto tiene dos operaciones con las que forma un anillo conmutativo, con elemento neutro para la suma $\hat{0} = \{0\}_{n=0}^{\infty}$ y elemento neutro para el producto $\hat{1} = \{1\}_{n=0}^{\infty}$. Además, $\{\mathbb{K}\}$ contiene un subanillo isomorfo a $\mathbb{K}$, identificando $a \in \mathbb{K}$ con la sucesión $\hat{a} = \{a\}_{n=0}^{\infty}$, que es obviamente de Cauchy. Sin embargo, $\{\mathbb{K}\}$ no es un cuerpo, porque tiene divisores de cero: $\{1, 0, 0, 0, ...\} \cdot \{0, 1, 0, 0, ...\} = \hat{0}$.

Ahora bien, cojamos el subconjunto de $\{\mathbb{K}\}$ formado por todas las sucesiones nulas en $\mathbb{K}$, P. Por 2.3.2, apartado 1, todo elemento de $\{\mathbb{K}\}$ es acotado, y por tanto, por 2.3.2, apartados 4 y 5, P es un ideal de $\{\mathbb{K}\}$ y determina una relación de equivalencia en la que dos sucesiones son equivalentes si y sólo si su diferencia es una sucesión nula (es decir, si su diferencia está en P). Por tanto, podemos considerar el anillo cociente $\hat{\mathbb{K}} = \{\mathbb{K}\}/P$, formado por las clases de equivalencia de las sucesiones de Cauchy. Si $a, b \in \mathbb{K}$ y $a \neq b$, entonces $\hat{a} \neq \hat{b}$: $a \neq b \Rightarrow a - b \neq 0 \Rightarrow \hat{a} - \hat{b} = \widehat{a - b} \neq \hat{0}$. En consecuencia, podemos, a través del isomorfismo citado anteriormente, ver $\mathbb{K}$ como un subconjunto de $\hat{\mathbb{K}}$.

Notación. *Si $\{a_n\}_{n=0}^{\infty} \in \{\mathbb{K}\}$, escribimos $(\{a_n\})$ para denotar su clase de equivalencia en $\hat{\mathbb{K}}$.*

Teorema 2.3.3. *El anillo $\hat{\mathbb{K}}$ es un cuerpo.*

Demostración. Como P es un ideal del anillo $\mathbb{K}$, sabemos que $\hat{\mathbb{K}}$ es un anillo conmutativo con las operaciones $(\{a_n\})+(\{b_n\})=(\{a_n+b_n\})$ y $(\{a_n\})\cdot(\{b_n\})=(\{a_nb_n\})$. Por tanto, para demostrar que se trata de un cuerpo lo único que tenemos que hacer es ver que todo elemento no nulo tiene un inverso.

Sea $(\{a_n\})\in\hat{\mathbb{K}}$, con $(\{a_n\})\neq\hat{0}$. Por el apartado 6 de 2.3.2,

$$\exists\, c>0,\ n_0\in\mathbb{N}/\ \parallel a_n\parallel > c\ \forall n\geq n_0.$$

Ahora podemos definir otra sucesión como

$$a_n^*=\begin{cases}0\ si\ 1\leq n\leq n_0\\ \frac{1}{a_n}\ si\ n\geq n_0\end{cases}\quad .$$

Veamos que $\{a_n^*\}\in\{\mathbb{K}\}$, es decir, que $\{a_n^*\}_{n=0}^{\infty}$ es de Cauchy. Sea $\epsilon>0$. Entonces, como $(\{a_n\})\in\hat{\mathbb{K}}$, $\{a_n\}_{n=0}^{\infty}\in\mathbb{K}$ es de Cauchy y $\exists\ n_1/\ \forall n,m\geq n_1$ $\parallel a_n-a_m\parallel < c^2\epsilon$. Tomamos $n_2=\text{máx}(n_0,n_1)$. Entonces, si $n,m\geq n_2$,

$$0\leq\parallel a_n^*-a_m^*\parallel=\parallel\frac{1}{a_n}-\frac{1}{a_m}\parallel=\frac{\parallel a_n-a_m\parallel}{\parallel a_n\parallel\cdot\parallel a_m\parallel}<c^{-2}\parallel a_n-a_m\parallel<c^{-2}\cdot c^2\epsilon=\epsilon.$$

Luego tenemos que $\{a_n^*\}_{n=0}^{\infty}$ es de Cauchy. Con la definición que hemos dado de multiplicación, tenemos que $\{a_n\}\cdot\{a_n^*\}=\{0,...,0,1,1,...\}$, y por tanto, $(\{a_n\})\cdot(\{a_n^*\})=(\{0,0,...,0,1,1,...\})=(\hat{1})$. En resumen, $(\{a_n^*\})\in\hat{\mathbb{K}}$ es el inverso de $(\{a_n\})$, y $\hat{\mathbb{K}}$ es un cuerpo.

Q.E.D.

Definición 2.3.4. *Sea $A=(\{a_n\})\in\hat{\mathbb{K}}$. Definimos la norma de A en $\hat{\mathbb{K}}$ como*

$$\parallel A\parallel=\lim_{n\to\infty}\parallel a_n\parallel .$$

Proposición 2.3.5. *La función que acabamos de definir es una norma de $\hat{\mathbb{K}}$.*

Demostración. Lo primero es demostrar que la función está bien definida y no depende del representante elegido para A.
Tenemos, como propiedad de la norma en $\mathbb{K}$, que

$$0\leq|\parallel a_n\parallel-\parallel a_m\parallel|\leq\parallel a_n-a_m\parallel .$$

Como $\{a_n\}_{n=0}^{\infty}$ es de Cauchy en $\mathbb{K}$, esto implica que $\{\parallel a_n\parallel\}_{n=0}^{\infty}$ es de Cauchy en $\mathbb{R}$ respecto al valor absoluto usual. Como $\mathbb{R}$ es completo, eso nos indica que el límite de $\parallel a_n\parallel$, y, por tanto, la función que hemos definido, existe.
Sea $\{a_n'\}_{n=0}^{\infty}$ otro representante de A. Por la misma propiedad de antes, y la definición de la relación de equivalencia,

$$0\leq|\parallel a_n\parallel-\parallel a_n'\parallel|\leq\parallel a_n-a_n'\parallel\to 0,$$

y por tanto $\lim_{n\to\infty} |\| a_n \| - \| a'_n \|| = 0$, es decir, $\lim_{n\to\infty} \| a_n \| = \lim_{n\to\infty} \| a'_n \|$ y la función no depende del representante.

Una vez que sabemos que la función está correctamente definida, veamos que es una norma. Para ello tenemos que comprobar las tres condiciones de la definición de norma de 2.0.3.
1. Si $A = (\hat{0})$, entonces cualquier $\{a_n\}_{n=0}^{\infty}$ representante de A es una sucesión nula, y por tanto $\| A \| = \lim_{n\to\infty} \| a_n \| = 0$ por definición de sucesión nula. Por el contrario, si $A \neq (\hat{0})$, por 2.3.2, apartado 6, existen $c > 0$ y $n_0 \in \mathbb{N}$ tales que $\forall n \geq n_0 \ \| a_n \| > c > 0$ y $\| A \| \neq 0$.

Los apartados 2 y 3 se resuelven de forma evidente por las propiedades de la norma de $\mathbb{K}$ y de los límites. Sean $A = (\{a_n\}_{n=0}^{\infty})$ y $B = (\{b_n\}_{n=0}^{\infty})$ dos elementos de $\hat{\mathbb{K}}$.

2. $\| AB \| = \lim_{n\to\infty} \| a_n b_n \| = \lim_{n\to\infty} \| a_n \| \cdot \lim_{n\to\infty} \| b_n \| = \| A \| \cdot \| B \|$.

3. $\| A + B \| = \lim_{n\to\infty} \| a_n + b_n \| \leq \lim_{n\to\infty} \| a_n \| + \lim_{n\to\infty} \| b_n \| = \| A \| + \| B \|$.

Q.E.D.

Por tanto, ya sabemos que el objeto que hemos construido es un cuerpo normado que contiene al $\mathbb{K}$ de origen. Pero nuestro objetivo con esta maniobra era crear una compleción de $\mathbb{K}$, así que aún nos falta ver que, efectivamente, este cuerpo es una tal compleción.

Proposición 2.3.6. *Sea $\hat{\mathbb{K}}$ como lo hemos construido anteriormente. Entonces $\mathbb{K}$ es denso en $\hat{\mathbb{K}}$ y $\hat{\mathbb{K}}$ es completo respecto a la norma $\| \ . \ \|$, es decir, una compleción de $\mathbb{K}$.*

Demostración. Empezamos con la densidad. Sea $A = (\{a_n\}_{n=0}^{\infty}) \in \hat{\mathbb{K}}$. Para cada $n \in \mathbb{N}$ tomamos la sucesión constante $(\hat{a}_n) = (\{a_n\}_{m=0}^{\infty})$, que pertenece a $\mathbb{K}$ (o, para ser exactos, a su imagen como subconjunto de $\hat{\mathbb{K}}$ por el isomorfismo que hemos descrito antes). Entonces el elemento $A - (\hat{a}_n)$ tiene, por defnición de suma en $\hat{\mathbb{K}}$, un representante de la forma $\{a_m - a_n\}_{m=0}^{\infty}$, y obtenemos que

$$\lim_{m\to\infty} \| A - (\hat{a}_n) \| = \lim_{n,m\to\infty} \| a_m - a_n \| = 0.$$

Luego tenemos que $\{(\hat{a}_n)\}$ es una sucesión de $\mathbb{K}$ que tiende hacia A. Por tanto, $\mathbb{K}$ es denso en $\hat{\mathbb{K}}$.

Veamos ahora que $\hat{\mathbb{K}}$ es completo. Sea $\{A_n\}_{n=0}^{\infty}$ una sucesión de Cauchy de elementos de $\hat{\mathbb{K}}$. Como hemos demostrado que $\mathbb{K}$ es denso en $\hat{\mathbb{K}}$, para todo $n \in \mathbb{N}$ existe $\hat{a}_n \in \mathbb{K}$ tal que

$$\| A_n - (\hat{a}_n) \| < \frac{1}{n}.$$

La sucesión $\{A_n - \hat{a}_n\}_{n=0}^{\infty} \in \hat{\mathbb{K}}$ es una sucesión nula, y por tanto de Cauchy. Claramente, $\{(\hat{a}_n)\} = \{A_n\} - \{A_n - \hat{a}_n\}$, y, al ser resta de dos sucesiones de Cauchy, por 2.3.2, apartado 2, es de Cauchy en $\hat{\mathbb{K}}$. Pero todo elemento de $\{(\hat{a}_n)\}$ pertenece a $\mathbb{K}$, luego $\{(\hat{a}_n)\}$ es una sucesión de Cauchy en $\mathbb{K}$, y $A = (\{\hat{a}_n\}) \in \hat{\mathbb{K}}$. La relación entre A y $\{(\hat{a}_n)\}$ aquí es la misma que teníamos en la primera parte, cuando demostramos la densidad de $\mathbb{K}$ en $\hat{\mathbb{K}}$; en consecuencia, sabemos que $\{A - (\hat{a}_n)\}$ es una sucesión nula. Si combinamos esto con el hecho, mostrado anteriormente, de que $\{A_n - (\hat{a}_n)\}$ es nula, tenemos que

$$\{A - A_n\} = \{A - (\hat{a}_n)\} - \{A_n - (\hat{a}_n)\}$$

es una sucesión nula (por 2.3.2, apartado 4), y $\{A_n\}$ tiende hacia A.

Q.E.D.

Luego tenemos, dados un cuerpo y una norma, un método general para construir compleciones. Por fin estamos en condiciones de introducir el cuerpo $\mathbb{Q}_p$, nuestro principal objeto de estudio.

Capítulo 3

El cuerpo $\mathbb{Q}_p$.

En este capítulo utilizaremos principalmente el «p-adic Analysis Compared with Real», de Svetlana Katok [Kat07, págs. 19-33 y 43-46], con incursiones esporádicas en el punto de vista de «A Course in p-adic Analysis», de Alain M. Robert. En particular, el apartado 3.4 de este trabajo, «Operaciones en $\mathbb{Q}_p$», usa casi exclusivamente el contenido de este último. La demostración de que la norma p-ádica no es arquimediana proviene de «Introduction to p-adic Numbers and Valuation Theory», de George Bachman. Consideramos durante todo el capítulo que p es un entero primo positivo.

3.1. La norma $|\ .\ |_p$.

Cuando estudiamos los números reales, en el capítulo introductorio, vimos que el cuerpo de los números reales es una compleción de $\mathbb{Q}$ para el valor absoluto usual. Ahora bien, es fácil imaginar la existencia de otras normas para $\mathbb{Q}$ distintas a éste, y, gracias a la última sección del capítulo anterior, una vez definida dicha norma, podríamos fácilmente construir su compleción respecto a ella. Este será el proceso que sigamos para conseguir $\mathbb{Q}_p$.

Definición 3.1.1. *Sea $x \in \mathbb{Q}$. Llamamos «orden p-ádico de x» al valor*

$$\mathrm{ord}_p = \begin{cases} \textit{exponente de la mayor potencia de } p \textit{ que divide } x, \textit{ si } x \in \mathbb{Z} \\ \mathrm{ord}_p(a) - \mathrm{ord}_p(b), \textit{ si } x = \frac{a}{b},\ a, b \in \mathbb{Z},\ b \neq 0 \end{cases}$$

Definición 3.1.2. *Definimos la norma p-ádica como la función $|\ .\ |_p \colon \mathbb{Q} \to \mathbb{R}^+$ que cumple*

$$|\ x\ |_p = \begin{cases} p^{-\ \mathrm{ord}_p(x)}\ \forall x \in \mathbb{Q}^* \\ 0 \textit{ si } x = 0 \end{cases}$$

Nota. *Si $a, b \in \mathbb{N}$, entonces a es congruente con b módulo p^n si y sólo si $|\ a - b\ |_p \leq 1/p^n$.*

Notación. *Como es habitual, utilizaremos la notación (a, b) para denotar el máximo común divisor de a y b.*

Lema 3.1.3. *Un racional $x = a/b$ con $(a, b) = 1$ tiene norma p-ádica menor o igual que 1 si y sólo si $p \nmid b$.*

Demostración. La primera implicación la veremos por contrarrecíproco. Sea $x = a/b \in \mathbb{Q}$ con $(a, b) = 1$, $a \neq 0$ y $p \mid b$. Como $(a, b) = 1$, eso implica que $p \nmid a$. Por la definición de orden, tenemos que $\mathrm{ord}_p(a) = 0$ y $\mathrm{ord}_p(b) > 0$, y por tanto $\mathrm{ord}_p(x) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b) < 0$. Por la definición de norma eso significa que $\mid x \mid_p = p^{-\mathrm{ord}_p(x)} > 1$.

Para la implicación inversa, sea $x = a/b \in \mathbb{Q}$ con $p \nmid b$ y $(a, b) = 1$. El que $p \nmid b$ significa que $\mathrm{ord}_p(b) = 0$. Entonces $\mathrm{ord}_p(x) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b) \geq 0$. Por consiguiente, $\mid x \mid_p \leq 1$.

Q.E.D.

Proposición 3.1.4. $\mid . \mid_p$ *es una norma no-arquimediana de* $\mathbb{Q}$. [Bac64, pág. 2-3]

Demostración. La primera condición de la norma es evidente por la definición, y la segunda es consecuencia de las propiedades de las potencias ($\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$). Veamos la desigualdad triangular.
Como lo que queremos ver es que la norma es no arquimediana, utilizaremos la condición equivalente b) del teorema 2.1.2. Sea $x = a/b$ con $\mid x \mid_p \leq 1$. Por el lema anterior, eso significa que si tomamos $(a, b) = 1$ tenemos $p \nmid b$.

$$1 + x = 1 + \frac{a}{b} = \frac{b + a}{b}$$

y $1+x$ también tiene un denominador que no es divisible por p. Luego $\mid 1+x \mid_p \leq 1$ y la norma es no arquimediana.

Q.E.D.

Corolario 3.1.5. *La norma p-ádica no es equivalente al valor absoluto usual.*

Nota. *Es fácil ver que si p_1 y p_2 son dos primos positivos distintos, las normas $\mid . \mid_{p_1}$ y $\mid . \mid_{p_2}$ tampoco son equivalentes, porque la sucesión $\{(p_1/p_2)^n\}_{n=0}^{\infty}$ es convergente con la primera norma pero no con la segunda. Así, hemos definido un número infinito de normas no equivalentes en $\mathbb{Q}$. Ahora bien, veremos a continuación que de hecho ¡estas son todas las normas no equivalentes que se pueden definir en $\mathbb{Q}$!*

Teorema 3.1.6 (Teorema de Ostrowski)**.** *Toda norma no trivial de $\mathbb{Q}$ es equivalente al valor absoluto usual si es arquimediana o a una norma p-ádica si no lo es.*

Demostración. Sea $\| . \|$ una norma no trivial de $\mathbb{Q}$. Queremos ver, por tanto, que $\exists\ \alpha > 0$ tal que $\| x \| = \mid x \mid^{\alpha}$ o $\| x \| = \mid x \mid_p^{\alpha}$ para todo $x \in \mathbb{Q}$. Lo primero

que debemos tener en cuenta es que nos basta con demostrarlo para todo entero positivo. En efecto, sabemos que $\| x \| = \| -x \|$ con cualquier norma, lo cual nos reduce a los positivos, y que todo número racional positivo se puede escribir como $x = a/b$ con $a, b \in \mathbb{N}$, luego

$$\| x \| = \frac{\| a \|}{\| b \|} = \frac{| a |^\alpha}{| b |^\alpha} = | x |^\alpha$$

e igual en el caso de la norma p-ádica.

Empecemos con el caso arquimediano. Por el teorema 2.1.2 sabemos que existe un $n \in \mathbb{N}$ tal que $\| n \| > 1$. Tomemos el natural más pequeño en el que esto se cumple y llamémoslo n_0. Como la función exponencial es sobreyectiva y $n_0^x > 1$ si $x > 0$, existe un α tal que $\| n_0 \| = n_0^\alpha$.
Ahora, si n es un número natural podemos escribirlo en base n_0 de la manera siguiente: existen $s \in \mathbb{N}$ y $0 \leq a_i < n_0 \ \forall i \in \{0, ..., s\}$ tales que $n = a_0 + ... + a_s n_0^s$ y $a_s \neq 0$. Por las propiedades de la norma, sabemos que

$$\| n \| \leq \| a_0 \| + \| a_1 n_0 \| + ... + \| a_s n_0^s \| = \| a_0 \| + \| a_1 \| \, n_0^\alpha ... + \| a_s \| \, n_0^{s\alpha}.$$

Hemos definido n_0 como el menor natural para el cual la norma es mayor que 1, luego tenemos que $\| a_i \| \leq 1$ por definición. Esto, junto con $n \geq n_0^s$, nos permite escribir las siguientes desigualdades:

$$\| n \| \leq 1 + n_0^\alpha + ... + n_0^{s\alpha} = n_0^{s\alpha}(n_0^{-s\alpha} + ... + 1) \leq n^\alpha (\sum_{i=0}^{s} n_0^{-i\alpha}) \leq n^\alpha (\sum_{i=0}^{\infty} n_0^{-i\alpha}).$$

La serie $\sum_{i=0}^{\infty} n_0^{-i\alpha}$ es convergente en $\mathbb{R}$ con el valor absoluto usual, luego $\sum_{i=0}^{\infty} n_0^{-i\alpha} = C \in \mathbb{R}^+$ independiente de n. Tenemos, por tanto, que

$$\| n \| \leq C n^\alpha = C \mid n \mid^\alpha,$$

y, como esta fórmula es cierta para todo $n \in \mathbb{N}$, que

$$\forall m \in \mathbb{N} \ \ \| n^m \| \leq C \mid n^m \mid^\alpha \Rightarrow \| n \| \leq \sqrt[m]{C} \mid n \mid^\alpha .$$

Haciendo tender m a infinito obtenemos la desigualdad

$$\| n \| \leq | n |^\alpha .$$

Si probamos la desigualdad contraria habremos acabado con el caso arquimediano.
Por la escritura en base n_0 sabemos que $n_0^{s+1} > n \geq n_0^s$ y

$$\| n_0^{s+1} \| = \| n + n_0^{s+1} - n \| \leq \| n \| + \| n_0^{s+1} - n \| \Rightarrow \| n \| \geq n_0^{(s+1)\alpha} - \| n_0^{s+1} - n \|$$

Gracias a la desigualdad que hemos demostrado en el apartado anterior tenemos que

$$\| n_0^{s+1} - n \| \leq | \| n_0^{s+1} \| - \| n \| | \leq n_0^{(s+1)\alpha} - n^\alpha \leq (n_0^{s+1} - n)^\alpha$$

y eso nos da la serie de desigualdades siguientes:

$$\| n \| \geq n_0^{(s+1)\alpha} - (n_0^{(s+1)} - n)^\alpha \geq n_0^{(s+1)\alpha} - (n_0^{(s+1)} - n_0^s)^\alpha$$
$$= n_0^{(s+1)\alpha} \left[1 - \left(1 - \frac{1}{n_0} \right)^\alpha \right] = n_0^{(s+1)\alpha} D \geq D n^\alpha.$$

La constante D es positiva y no depende de n, luego estamos en un caso equivalente al anterior. Tomamos n^m, escribimos la desigualdad, tomamos raíces m-ésimas y hacemos tender m a infinito. Esto nos da

$$\| n \| \geq | n |^\alpha$$

y hemos acabado. Tenemos que si $\| \, . \, \|$ es arquimediana, entonces es equivalente al valor absoluto usual.

Vamos ahora con el caso no arquimediano. Sea $\| \, . \, \|$ una norma no-arquimediana sobre $\mathbb{Q}$. Entonces por el teorema 2.1.2 sabemos que para todo entero n se da $\| n \| \leq 1$. Como esta norma no es trivial tiene que existir un $n_0 \in \mathbb{N}$ tal que $\| n_0 \| < 1$. Tomamos el más pequeño que lo cumple y lo llamamos p. Este p tiene que ser un número primo, porque si no tendríamos que $p = n_1 n_2$, con $n_1, n_2 < p$, y por definición de p $\| n_1 \| = 1$ y $\| n_2 \| = 1$, lo que nos daría $\| p \| = \| n_1 \| \cdot \| n_2 \| = 1$, lo que es falso. Tenemos, pues, que p es un número primo.
Por el mismo argumento que en el apartado arquimediano, existe un $\alpha > 0$ tal que $\| p \| = p^{-\alpha}$. Veamos que si $n \in \mathbb{N}$ no es divisible por p, tenemos que $\| n \| = 1$. Sea $n \in \mathbb{N}$ tal que $p \nmid n$. En ese caso podemos escribirlo como $n = pk + r$ con $0 < r < p$ y, por la definición de p, $\| r \| = 1$. En cambio, $\| pk \| = \| p \| \cdot \| k \| < 1$. Eso nos da que

$$\| n - r \| = \| pk \| < 1 = \| r \| \Rightarrow \| n \| = \| r \| = 1$$

por ser la norma no-arquimediana(«el mayor se impone»).
Una vez que tenemos esto, podemos escribir cualquier natural n como $n = p^l a$ siendo $a \in \mathbb{N}$ y $p \nmid a$. Entonces,

$$\| n \| = \| p^l \| \cdot \| a \| = \| p \|^l = (p^{-l})^\alpha = | n |_p^\alpha \, .$$

y hemos acabado. Tenemos que si $\| \, . \, \|$ es no arquimediana, entonces es equivalente a una norma p-ádica.

Q.E.D.

3.2. El cuerpo $\mathbb{Q}_p$.

Ahora que tenemos la norma, podemos finalmente definir el cuerpo de los números p-ádicos. El cuerpo de los números p-ádicos, $\mathbb{Q}_p$ es la compleción de $(\mathbb{Q}, | \, . \, |_p)$ con el método desarrollado en el capítulo anterior. Así, podemos ver $\mathbb{Q}_p$ como las clases de equivalencia de las sucesiones de Cauchy de $\mathbb{Q}$, y su norma es $| A |_p = \lim_{n \to \infty} | a_n |_p$ si $A \in \mathbb{Q}_p$.

Nota. *Aquí, nada más definir el cuerpo de los p-ádicos, encontramos la primera gran diferencia con el caso real: la norma sobre $\mathbb{Q}_p$ no es sobreyectiva. De hecho, el conjunto de valores posibles para la norma p-ádica es «discreto»; para ser exactos,* $| \mathbb{Q}_p |_p = \{p^n / \ n \in \mathbb{Z}\} \cup \{0\}$.

Tenemos, por tanto, un cuerpo distinto a $\mathbb{R}$ que se construye de manera análoga. Pero esto no es lo único que sabemos sobre el cuerpo de los reales: también conocemos una manera de escribirlos como series de potencias de 10. ¿Podemos hacer algo similar con los elementos de $\mathbb{Q}_p$? Efectivamente, podemos escribir los números p-ádicos como series de potencias, de p en esta ocasión.

Proposición 3.2.1. *Sea $x = \sum_{i=k}^{\infty} a_i p^i$, con $k \in \mathbb{Z}$ y a_i entre 0 y $p-1$ para todo $i \geq k$ entero. Entonces x es un número p-ádico.*

Demostración. Esta demostración es esencialmente idéntica al caso real: se trata de mostrar que x es el límite de una sucesión de Cauchy para la norma $| \ . \ |_p$. Como nuestro cuerpo $\mathbb{Q}_p$ es completo, tendremos que $x \in \mathbb{Q}_p$. Por definición de serie, sabemos que

$$\sum_{i=k}^{\infty} a_i p^i = \lim_{n \to \infty} \sum_{i=k}^{n} a_i p^i,$$

y en consecuencia que x es el límite de una sucesión de números racionales. Ésta sucesión es de Cauchy: sea $\epsilon > 0$, entonces $\exists \ n_0 \in \mathbb{N}$ tal que $p^{-n_0} < \epsilon$. Si $m, n \geq n_0 \geq k$, suponemos sin pérdida de generalidad que $m \geq n$ y obtenemos que

$$| \sum_{i=k}^{m} a_i p^i - \sum_{i=k}^{n} a_i p^i |_p = | \sum_{i=n+1}^{m} a_i p^i |_p \leq p^{-n+1} \leq p^{-n_0} < \epsilon$$

por la desigualdad triangular fuerte.
Tenemos, por tanto, que x es el límite de una sucesión de Cauchy de números racionales, y en consecuencia $x \in \mathbb{Q}_p$.

Q.E.D.

La otra implicación es un poco más compleja. Para ello necesitaremos este resultado previo:

Lema 3.2.2. *Sea x un número racional cuya norma p-ádica sea menor que 1. Entonces para todo i entero existe otro entero $\alpha \in \mathbb{Z}$ tal que* $| \alpha - x |_p \leq p^{-i}$ *y podemos escogerlo en el conjunto de los naturales entre 0 y $p^i - 1$.*

Demostración. Escribamos x como $x = a/b$ con $a, b \in \mathbb{Z}$ y $(a, b) = 1$. Como a y b son primos entre sí y $| \ a/b \ |_p \leq 1$, sabemos que $(p, b) = 1$, luego $(p^i, b) = 1$. Por la identidad de Bézout, existen $n, m \in \mathbb{Z}$ tales que $np^i + mb = 1$. Tomamos $\alpha = am$. Así,

$$| \ \alpha - x \ |_p = | \ am - a/b \ |_p = | \ a/b \ |_p \cdot | \ mb - 1 \ |_p = | \ x \ |_p | \ np^i \ |_p \leq | \ np^i \ |_p = | \ n \ |_p \cdot p^{-i} \leq p^{-i}.$$

La última desigualdad es cierta por 2.1.2
Ahora, como la norma es no-arquimediana, podemos sumar el múltiplo de p^i

que queramos a α para conseguir un entero en el intervalo que nos interesa sin que ello cambie el resultado. Sea $k \in \mathbb{Z}$:

$$| \alpha + kp^i - x |_p \leq \text{máx}(| \alpha - x |_p, | kp^i |_p) \leq p^{-i},$$

porque $| \alpha - x |_p \leq p^{-i}$ y $| kp^i |_p \leq p^{-i}$.

Q.E.D.

Teorema 3.2.3. *Para todo elemento A en $\mathbb{Q}_p$ con norma menor que 1, existe un único representante $\{d_n\}_{n=0}^{\infty}$ que cumpla las siguientes condiciones:*

1. $\forall n \in \mathbb{N}^*$, $d_n \in \mathbb{N}$ *y* $0 \leq d_n < p^n$.
2. $\forall n \in \mathbb{N}^*$, $d_n \equiv d_{n+1} \pmod{p^n}$.

En consecuencia, todo elemento de $\mathbb{Q}_p$ se puede escribir de la forma $\sum_{i=k}^{\infty} a_i p^i$, a la que llamaremos «desarrollo canónico».

Demostración. Sea $A \in \mathbb{Q}_p$ con $| A |_p \leq 1$ y sea $\{b_n\}_{n=0}^{\infty}$ una sucesión de Cauchy representante de A. Como $| A |_p \leq 1$ y $b_n \to A$, suprimiendo los primeros términos si es necesario podemos suponer sin pérdida de generalidad que $| b_n |_p \leq 1 \ \forall n \in \mathbb{N}$. Ahora bien, como la sucesión es de Cauchy, para todo $j \in \mathbb{N}$ existe un $n_j \in \mathbb{N}$ tal que si $n, m \geq n_j$,

$$| b_n - b_m |_p \leq p^{-j}, \tag{3.1}$$

y podemos forzar que $n_j \geq j$ tomando $n_j = \text{máx}(n_j, j)$.
Por el lema anterior, como la norma de todos los elementos de $\{b_n\}_{n=0}^{\infty}$ es menor que 1, para todo $j \in \mathbb{N}$ podemos calcular naturales d_j estrictamente más pequeños que p^j que cumplan

$$| d_j - b_j |_p \leq p^{-j}. \tag{3.2}$$

La sucesión que forman estos elementos cumple la primera condición del teorema. Veamos si cumple la segunda, es decir, si $d_n \equiv d_{n+1} \pmod{p^n}$.
Gracias a la desigualdad triangular fuerte y a las desigualdades (3.1) y (3.2), tenemos que

$$\begin{gathered} | d_{j+1} - d_j |_p = | (d_{j+1} - b_{n_{j+1}}) + (b_{n_{j+1}} - b_{n_j}) + (b_{n_j} - d_j) |_p \leq \\ \text{máx}(| d_{j+1} - b_{n_{j+1}} |_p, | b_{n_{j+1}} - b_{n_j} |_p, | b_{n_j} - d_j |_p) \leq \\ \text{máx}(p^{-(j+1)}, p^{-j}, p^{-j}) = p^{-j}, \end{gathered}$$

y por la nota del principio del capítulo, eso significa que $d_{j+1} \equiv d_j \pmod{p^j}$.
Luego la sucesión cumple las propiedades exigidas en el teorema. ¿Pero es un representante de A? Es decir, ¿es $\{d_n\}$ equivalente a $\{b_n\}$?
Sea $\epsilon > 0$. Entonces existe $j \in \mathbb{N}$ tal que $p^j \leq \epsilon$. Luego si $i \geq n_j$ con n_j definido como en (3.1),

$$| d_i - b_i |_p = | (d_i - d_j) + (d_j - b_{n_j}) + (b_{n_j} - b_i) |_p \leq$$

$$\text{máx}(\mid d_i - d_j \mid_p, \mid d_j - b_{n_j} \mid_p, \mid b_{n_j} - b_i \mid_p) \leq p^{-j} \leq \epsilon.$$

Luego la resta de $\{d_n\}$ y $\{b_n\}$ es una sucesión nula y son equivalentes.

Veamos ahora la unicidad. Sea $\{d'_n\}$ otra sucesión que cumpla las dos condiciones del teorema. Si es distinta de $\{d_n\}$, $\exists\ n_0 \in \mathbb{N}/\ d_{n_0} \neq d'_{n_0}$. Como tanto d_{n_0} como d'_{n_0} están entre 0 y p^{n_0}, eso significa que $d_{n_0} \not\equiv d'_{n_0} \pmod{p^{n_0}}$. Por la segunda condición del teorema, $\forall n \geq n_0$

$$d_n \equiv d_{n_0} \not\equiv d'_{n_0} \equiv d'_n \pmod{p^{n_0}}.$$

Pero por la primera nota del capítulo, eso significa que

$$\mid d_n - d'_n \mid_p > p^{n_0}\ \forall n \geq n_0,$$

y las dos sucesiones no son equivalentes. Por contrarrecíproco, tenemos unicidad.

Si escribimos los términos de la sucesión $\{d_n\}$ en base p, obtenemos algo de la forma $d_n = \sum_{i=0}^{n} a_i p^i$, y por la segunda condición del teorema $d_{n+1} = \sum_{i=0}^{n+1} a_i p^i$ siendo el a_i el mismo en los dos casos $\forall i \leq n$. Tenemos, por tanto, una sucesión formada por sumas parciales de la forma $d_n = \sum_{i=0}^{n} a_i p^i$. A es la serie

$$A = \sum_{i=0}^{\infty} a_i p^i.$$

En el caso de $x \in \mathbb{Q}_p$ con $\mid x \mid_p = p^k > 1$, con $k \in \mathbb{N}$, podemos multiplicarlo por p^k para conseguir un número de norma 1. Aplicamos el método anterior a este nuevo elemento, y obtenemos $p^k \cdot x = \sum_{i=0}^{\infty} a_i p^i$, y por tanto $x = \sum_{i=-k}^{\infty} a_i p^i$.

Q.E.D.

Notación. *Sea tenemos un elemento de $\mathbb{Q}_p$ de la forma $x = \sum_{i=-k}^{\infty} a_i p^i$. En alguna ocasión, cuando queramos poner en evidencia el parecido con $\mathbb{R}$, lo escribiremos también como $x = ...a_n...a_1 a_0.a_{-1}...a_{-k}$.*

Esta forma, además de ser muy útil en términos prácticos, nos proporciona una definición equivalente de la norma p-ádica.

Proposición 3.2.4. *Si $x \in \mathbb{Q}_p$ y k es el índice de su primer sumando no nulo, la norma de x es p^{-k}. Es decir, si $x = \sum_{i=k}^{\infty} a_i p^i$ es un elemento de $\mathbb{Q}_p$ con $k \in \mathbb{Z}$ y $a_k \neq 0$, entonces $\mid x \mid_p = p^{-k}$.*

Demostración. Sea $x = \sum_{i=k}^{\infty} a_i p^i \in \mathbb{Q}_p$ con $k \in \mathbb{Z}$ y $a_k \neq 0$. Hemos definido la norma p-ádica como $\mid x \mid_p = \lim_{n\to\infty} \mid \sum_{i=k}^{n} a_i p^i \mid_p$, y por la desigualdad triangular fuerte tenemos que

$$\mid \sum_{i=k}^{n} a_i p^i \mid_p \leq \text{máx}(\{\mid a_i p^i \mid_p\ /\ k \leq i \leq n\}) =$$

$$\text{máx}(\{p^{-i}/\ k \leq i \leq n\}) = p^{-k}\ \forall n \in \mathbb{N}.$$

Luego $\mid x \mid_p = \lim_{n\to\infty} \mid \sum_{i=k}^{n} a_i p^i \mid_p = p^{-k}$.

Q.E.D.

3.3. Los enteros p-ádicos $\mathbb{Z}_p$.

Definición 3.3.1. *Se dice que $x \in \mathbb{Q}_p$ es un entero p-ádico si su desarrollo canónico no contiene sumandos de índice negativo. El conjunto de los enteros p-ádicos se denota por $\mathbb{Z}_p$.*

Gracias a 3.2.4, la siguiente proposición es trivial.

Proposición 3.3.2. *Los enteros p-ádicos son aquellos elementos de $\mathbb{Q}_p$ cuya norma p-ádica es menor o igual que 1.*

Nota. *El anillo $\mathbb{Z}_p$ nos proporciona otra forma de construir el cuerpo de los números p-ádicos. Efectivamente, podríamos haber empezado definiendo los enteros como las series formales*

$$\sum_{i=0}^{\infty} a_i p^i \text{ con } a_i \in \{0, ..., p-1\}.$$

Una vez que sabemos que $\mathbb{Z}_p$ es un dominio de integridad, $\mathbb{Q}_p$ no es más que su cuerpo de fracciones. Definiendo la norma como en la proposición 3.2.4 hemos acabado. Este, de hecho, es el método que sigue el libro de Alain M. Robert [Rob00]. *La razón que nos ha hecho preferir el procedimiento de Svetlana Katok es simplemente que creemos que así es más claro el paralelismo con el cuerpo $\mathbb{R}$.*

Proposición 3.3.3. *Los números p-ádicos forman un conjunto no numerable.*

Demostración. Esta prueba es semejante a la de que los números reales no son numerables. Suponemos, por reducción al absurdo, que existe una biyección entre $\mathbb{Z}_p$ y los naturales. Así, podemos ordenar los enteros p-ádicos de la forma siguiente:

$$\begin{gathered} ...a_{n0}...a_{10}a_{00} = a_0 \\ ...a_{n1}...a_{11}a_{01} = a_1 \\ \vdots \\ ...a_{nn}...a_{1n}a_{0n} = a_n \\ \vdots \end{gathered}$$

Ahora tomamos un elemento $x = ...x_n...x_1x_0 \in \mathbb{Z}_p$ tal que $x_i \neq a_{ii}\ \forall i \in \mathbb{N}$. Este x es constructible, puesto que para cada índice tenemos $p-1$ posibilidades. Es evidente que x no puede pertenecer a la lista escrita anteriormente, y en consecuencia no puede haber una aplicación sobreyectiva de $\mathbb{N}$ en $\mathbb{Z}_p$.
Luego $\mathbb{Z}_p$ es no numerable.

Q.E.D.

Teorema 3.3.4. *El conjunto $\mathbb{Z}_p$ es secuencialmente compacto, es decir, toda sucesión en $\mathbb{Z}_p$ tiene una subsucesión convergente.*

Demostración. Sea $\{a_n\}_{n=0}^{\infty} \subset \mathbb{Z}_p$. Entonces, por definición, podemos escribir los términos como $a_n = \sum_{i=0}^{\infty} a_i p^i$. Como $a_{0n} \in \{0, ..., p-1\}$ para todo $n \in \mathbb{N}$, existe un $b_0 \in \{0, ..., p-1\}$ tal que $a_{0n} = b_0$ para un número infinito de elementos. Tomamos la subsucesión formada por los elementos cuyo primer término es b_0. Iterando el procesos sobre esta nueva sucesión, obtenemos una sucesión de subsucesiones de $\{a_n\}_{n=0}^{\infty}$ de esta forma,

$$\begin{array}{c} a_0^0, a_1^0, a_2^0, ... \\ a_0^1, a_1^1, a_2^1 ... \\ a_0^2, a_1^2, a_2^2, ... \\ \vdots \end{array}$$

y tales que $\left\{a_n^{j+1}\right\}_{n=0}^{\infty}$ es subsucesión de $\left\{a_n^j\right\}_{n=0}^{\infty}$ y todo elemento de $\left\{a_n^j\right\}_{n=0}^{\infty}$ empieza por $b_j b_{j-1} ... b_0$ para todo $j \in \mathbb{N}$.
La subsucesión $\{a_n^n\}_{n=0}^{\infty}$ es aún una subsucesión de $\{a_n\}_{n=0}^{\infty}$, y converge trivialmente hacia $...b_n...b_2 b_1 b_0$. Luego toda sucesión de enteros p-ádicos contiene una subsucesión convergente.

Q.E.D.

Corolario 3.3.5. *Los enteros p-ádicos, $\mathbb{Z}_p$, forman un espacio métrico completo.*

Demostración. Sabemos que en un espacio métrico ser secuencialmente compacto es equivalente a ser compacto. Por tanto, $\mathbb{Z}_p$ es un compacto, y como $\mathbb{Q}_p$ es de Hausdorff (de nuevo, por ser un espacio métrico) eso implica que es cerrado en $\mathbb{Q}_p$. Hemos demostrado en 1.1.5 que todo conjunto cerrado en un completo es completo. Luego $\mathbb{Z}_p$ es completo.

Q.E.D.

Corolario 3.3.6. *Toda sucesión acotada de $\mathbb{Q}_p$ tiene una subsucesión convergente.*

Demostración. Sea $\{a_n\}_{n=0}^{\infty}$ una sucesión de $\mathbb{Q}_p$ acotada. Entonces $\exists\ m \in \mathbb{Z}$ tal que $\mid a_n \mid_p \leq p^m\ \forall n \in \mathbb{N}$. Por la proposición 3.2.4, eso significa que para todo $n \in \mathbb{N}$ podemos escribir $a_n = \sum_{i=-m}^{\infty} a_i p^i$. Luego $p^m a_n \in \mathbb{Z}_p\ \forall n \in \mathbb{N}$, que por el teorema anterior tiene una subsucesión $\{p^m a_{i_n}\}_{n=0}^{\infty}$ convergente. Si a es su límite, $\{a_{i_n}\}_{n=0}^{\infty}$ es una subsucesión convergente de $\{a_n\}_{n=0}^{\infty}$ y su límite es ap^{-m}.

Q.E.D.

Nota. *Es importante tener en cuenta que la condición de la acotación es necesaria en el caso de $\mathbb{Q}_p$. En efecto, la sucesión $\{p^{-n}\}_{n=0}^{\infty}$ es no acotada* ($\mid p^{-n} \mid_p = p^n\ \forall n \in \mathbb{N}$), *y no tiene ninguna subsucesión convergente, porque* $\lim_{n\to\infty} p^{-n} = +\infty$.

3.4. Desarrollo canónico y operaciones en $\mathbb{Q}_p$

La definición de $\mathbb{Q}_p$ como cuerpo de fracciones de $\mathbb{Z}_p$ nos da inmediatamente una manera de definir las operaciones del cuerpo aplicando la definición de las operaciones en series. Es decir, si $a = \sum_{i=k}^{\infty} a_i p^i$, $b = \sum_{i=h}^{\infty} b_i p^i$ y $k \leq h$,

$$a \pm b = \sum_{i=k}^{\infty} a_i p^i \pm \sum_{i=h}^{\infty} b_i p^i = \sum_{i=k}^{\infty} (a_i \pm b_i) p^i,$$

escribiendo $b_i = 0$ para todo $k \leq i < h$. En el caso de la multiplicación,

$$ab = \sum_{i=k+h}^{\infty} u_i p^i \text{ con } u_i = \sum_{i+j=n} a_i b_j.$$

Ahora bien, estos procesos nos dan series que no están necesariamente en forma canónica, porque algunos de sus términos pueden no ser de la forma $u_i p^i$ con $u_i \in \{0, ..., p-1\}$. Podríamos aplicar de nuevo la construcción de la demostración del teorema 3.2.3, pero existe un algoritmo mucho más simple. Veamos primero el caso de la suma.

Tomamos, como en el caso anterior, $b_i = 0$ para todo $k \leq i < h$, con lo que obtenemos dos series de la forma $a = \sum_{i=k}^{\infty} a_i p^i$ y $b = \sum_{i=k}^{\infty} b_i p^i$. El primer término de la suma es $a_k + b_k$ si $a_k + b_k < p$ y $a_k + b_k - p$ en caso contrario. En la segunda situación sumamos 1 a la siguiente suma y repetimos el proceso. En otras palabras, calculamos de derecha a izquierda, y si la suma de los términos es mayor que p, «nos llevamos» 1. Para ilustrar este método, calculamos el desarrollo canónico de -1. Sabemos que $1 + (-1) = 0$, y que $1 = 1 + \sum_{i=1}^{\infty} 0 p^i$ y $0 = \sum_{i=0}^{\infty} 0 p^i$. Tomamos $-1 = \sum_{i=0}^{\infty} a_i p^i$ con $a_i \in \{0, ..., p-1\}$. Entonces la única manera de que $1 + a_0 \in \{0, p\}$ es tener $a_0 = p - 1$ y «llevarnos» 1. Así, $0 + a_1 + 1 \in \{0, p\}$ implica que $a_1 = p - 1$ y «nos llevamos» 1. Iterando el proceso llegamos a que $-1 = \sum_{i=0}^{\infty} (p-1) p^i$.

De forma más general, para $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ definamos $\sigma(a) = \sum_{i=0}^{\infty} (p - 1 - a_i) p^i$. Entonces tenemos que $a + \sigma(a) + 1 = 0$ o, equivalentemente, $-a = \sigma(a) + 1 \in \mathbb{Z}_p$. [Rob00, págs. 2-3]

Ahora vamos a ver el caso de la multiplicación. Aquí, como en el de la suma, el algoritmo no es más que una generalización de la multiplicación de enteros en base p. Con la notación anterior, calculamos u_{k+h}. Si $u_{k+h} < p$, el primer término de la multiplicación es ese; en caso contrario, dicho primer término es un $c_{k+h} \equiv u_{k+h} \pmod{p}$ con $0 \leq u_{k+h} < p$ y sumamos el cociente entero de u_{k+h}/p al término siguiente. Iteramos el proceso.

Hemos visto hace un momento que $-1 = \sum_{i=0}^{\infty} (p-1) p^i$. Entonces tenemos

que

$$-1 = (p-1)\sum_{i=0}^{\infty} p^i \Rightarrow \frac{-1}{p-1} = \frac{1}{1-p} = \sum_{i=0}^{\infty} p^i,$$

luego $1/1-p \in \mathbb{Z}_p$ y $1-p$ es invertible en $\mathbb{Z}_p$. En cambio, $p \in \mathbb{Z}_p$ no es inversible: en efecto, $1/p = p^{-1} \notin \mathbb{Z}_p$, y el inverso es único.
Tenemos que algunos elementos de $\mathbb{Z}_p$ son inversibles y otros no, y en consecuencia, que $\mathbb{Z}_p$ no es un cuerpo. ¿Qué podemos decir de los elementos inversibles de $\mathbb{Z}_p$?

Definición 3.4.1. *Como es habitual, el conjunto de los elementos invertibles de $\mathbb{Z}_p$ se denota por $\mathbb{Z}_p^*$ y sus elementos se llaman unidades p-ádicas.*

Proposición 3.4.2. *Las unidades p-ádicas son exactamente aquellos elementos de $\mathbb{Z}_p$ cuyo desarrollo canónico tiene su primer coeficiente no nulo. Es decir, $\mathbb{Z}_p^* = \{\sum_{i=0}^{\infty} a_i p^i / \ a_0 \neq 0\}$.* [Rob00, pág. 5]

Demostración. En realidad, esta demostración no es más que una adaptación al caso p-ádico del resultado que dice que si A es un anillo, entonces un elemento a de $A[[X]]$, anillo de series formales, es inversible en $A[[X]]$ si y sólo si su término «independiente» es inversible en A. [AM69, pág. 11]

Sea $a \in \mathbb{Z}_p^*$. Entonces $\exists\ a^{-1} \in \mathbb{Z}_p$ tal que $a \cdot a^{-1} = 1$. Si suponemos que $a = \sum_{i=0}^{\infty} a_i p^i$ con $a_0 = 0$, y tomamos $a^{-1} = \sum_{i=0}^{\infty} b_i p^i$, por el algoritmo dado anteriormente tenemos que $0 = a_0 \cdot b_0 \equiv 1 \pmod{p}$. Imposible. Luego $a_0 \neq 0$.

Ahora tenemos que demostrar que todo elemento con $a_0 \neq 0$ es invertible en $\mathbb{Z}_p$. Sea $a = \sum_{i=0}^{\infty} a_i p^i$ con $a_0 \neq 0$. Escribimos $a = a_0 + \alpha p$ con $\alpha \in \mathbb{Z}_p$. Sabemos que $0 < a_0 < p$.. Sea $b_0 \in \mathbb{Z}$ tal que $0 < b_0 < p$ $a_0 b_0 \equiv 1 \pmod{p}$. Podemos escribir $a_0 b_0 = 1 + kp$ con $k \in \mathbb{Z}$. Por lo tanto, tenemos que

$$a \cdot b_0 = (a_0 + \alpha p) b_0 = 1 + kp + b_0 \alpha p = 1 + hp$$

con $h \in \mathbb{Z}_p$. Por lo tanto, es suficiente con ver que los elementos de la forma $1 + hp$ son inversibles, porque entonces tenemos que

$$ab_0 = 1 + hp \Rightarrow ab_0(1+hp)^{-1} = 1 \Rightarrow a^{-1} = b_0(1+hp)^{-1}.$$

Pero ya hemos visto que $(1-p) \in \mathbb{Z}_p^*$. Así, tenemos $(1+hp)^{-1} = 1 + (-hp) + (-hp)^2 + (-hp)^3 + ...$, que podemos escribir como un número p-ádico a través del algoritmo anterior. Luego a es invertible.

Q.E.D.

Corolario 3.4.3. *Por la proposición 3.2.4, tenemos que $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p / \ | \ x \ |_p = 1\}$.*

Proposición 3.4.4. *Sea $x \in \mathbb{Q}_p$. Entonces existe un entero n y una unidad p-ádica $u \in \mathbb{Z}_p^*$ tales que $x = p^n u$. En particular, si $| \ x \ |_p = p^{-k}$, entonces $n = k$ y $u = p^{-k} x$.*

Demostración. Sea $x \in \mathbb{Q}_p$ tal que $\mid x \mid_p = p^{-k}$. Escribamos entonces $x = p^k p^{-k} x$. Como sabemos que $\mid p^{-k} \mid_p = p^k$, tenemos que $\mid p^{-k}x \mid_p = p^k p^{-k} = 1$ y por tanto $p^{-k}x \in \mathbb{Z}_p^*$. Hemos terminado.

Q.E.D.

3.5. Relación entre $\mathbb{Q}$, $\mathbb{Z}_p$ y $\mathbb{Q}_p$.

El desarrollo canónico será la representación de los números p-ádicos que utilizaremos principalmente en un futuro, pero a la vez nos plantea un problema: ¿Cómo distinguir los elementos pertenecientes al subcuerpo de los racionales? ¿O al subanillo de los enteros? Es evidente que $\mathbb{Z} \subset \mathbb{Z}_p$, y que el desarrollo canónico de los números enteros no es más que su escritura en base p. Pero gracias a 3.2.4 sabemos que $\exists\, x \in \mathbb{Z}_p$ tales que $x \notin \mathbb{Z}$, sin ir más lejos $\frac{1}{1-p}$. ¿Existen racionales entre esos elementos de $\mathbb{Z}_p \setminus \mathbb{Z}$?

Proposición 3.5.1. *Sea $x = a/b \in \mathbb{Q}$ un número racional con $a, b \in \mathbb{Z}$, $b \neq 0$ y $(a, b) = 1$. Entonces*

1. *El número x es un entero p-ádico si y sólo si p no divide b, es decir, $\mathbb{Q} \cap \mathbb{Z}_p = \{x = a/b \in \mathbb{Q} /\ p \nmid b\}$.*
2. *El número x es una unidad p-ádica si y sólo si p no divide ab, es decir, $\mathbb{Q} \cap \mathbb{Z}_p^* = \{x = a/b \in \mathbb{Q} /\ p \nmid ab\}$.*

Demostración. 1. En el lema 3.1.3 hemos visto que $\{x = a/b \in \mathbb{Q} /\ p \nmid b\} = \{x \in \mathbb{Q} \text{ tal que } \mid x \mid_p \leq 1\}$. Como ya hemos visto que los enteros p-ádicos son exactamente los elementos de $\mathbb{Q}_p$ que tienen norma menor o igual que 1, hemos demostrado lo que queríamos.

2. Como p es un número primo, sabemos que $p \nmid ab \Leftrightarrow p \nmid a$ y $p \nmid b$.
Empecemos viendo que $\mathbb{Q} \cap \mathbb{Z}_p^* \subset \{x = a/b \in \mathbb{Q} /\ p \nmid ab\}$. Sea $x = a/b \in \mathbb{Q}$ con $(a, b) = 1$ y tal que $p \mid ab$. Por tanto, $p \mid a$ o $p \mid b$. Si $p \mid b$, por el primer apartado tenemos que $x \notin \mathbb{Z}_p$, y por tanto $x \notin \mathbb{Z}_p^*$. Si, en cambio, $p \mid a$, como $(a, b) = 1$, tenemos que $\mathrm{ord}_p(a) > 0$ y $\mathrm{ord}_p(b) = 0$. Entonces $\mathrm{ord}_p(x) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b) > 0$ y $\mid x \mid_p \neq 1$. Luego $x \notin \mathbb{Z}_p^*$.

La otra inclusión es directa. Sea $x = a/b \in \mathbb{Q}$ tal que $p \nmid ab$, luego $p \nmid a$ y $p \nmid b$. Tenemos que $\mathrm{ord}_p(a) = 0$ y $\mathrm{ord}_p(b) = 0$, y por tanto $\mid x \mid_p = p^0 = 1$. Con la descripción de $\mathbb{Z}_p^*$ que hemos dado en el apartado anterior, concluimos que $x \in \mathbb{Z}_p^*$ y hemos acabado.

Q.E.D.

Proposición 3.5.2. *El desarrollo canónico de un número p-ádico a es finito (es decir, $a_i = 0$ para todo i a partir de un cierto $n \in \mathbb{Z}$) si y sólo si a es un racional no negativo cuyo denominador es una potencia de p.*

Demostración. Sea $x \in \mathbb{Q}_p$ tal que su desarrollo p-ádico es finito, es decir, que existe un $m \in \mathbb{Z}$ tal que $x = \sum_{i=k}^{m} a_i p^i$. Entonces si $k \geq 0$ esa suma es un número

natural escrito en base p, y por tanto un racional no negativo con denominador una potencia de p (exponente 0). Si, en cambio, $k < 0$, entonces tenemos que $p^{-k}x = \sum_{i=0}^{m-k} a_i p^i \in \mathbb{N}$ y x es un número racional no negativo con denominador $p^{-k} \in \mathbb{N}$. Hemos acabado esta implicación.

Para la implicación contraria, sea $a = n/p^k \in \mathbb{Q}^+$ con $n, k \in \mathbb{N}$. Escribimos n en base p: $n = a_0 + ... + a_s p^s$. Entonces tenemos que

$$a = \frac{\sum_{i=0}^{s} a_i p^i}{p^k} = \sum_{i=-k}^{s-k} a_i p^i$$

que es su desarrollo canónico por la unicidad de este. Hemos terminado.

Q.E.D.

Teorema 3.5.3. *Sea $x = ...a_n...a_0.a_{-1}...a_{-k}$ el desarrollo canónico de un número p-ádico. Entonces x es racional si y sólo si su desarrollo es periódico.* [Rob00, págs. 39-40]

Demostración. Sea $x = \sum_{i=k}^{\infty} a_i p^i$ un número p-ádico con desarrollo periódico. Restando un entero y multiplicando por $\mid x \mid_p$ si es necesario podemos suponer que $x \in \mathbb{Z}_p$ y que el desarrollo es de la forma

$$x = a_0 + ... + a_n p^n + a_0 p^{n+1} + ... + a_n p^{2n} ...$$

$$= a_0 + a_1 p + ... + a_n p^n + (a_0 + a_1 p + ... + a_n p^n) p^n + ...$$

El «periodo», $a_0 + ... + a_n p^n$, es un entero en base p. Podemos, por tanto, escribir

$$x = (a_0 + ... + a_n p^n)(1 + p^n + ... + p^{kn} + ...) = \frac{a_0 + ... + a_n p^n}{1 - p^n}$$

que es un número racional.

Ahora bien, la otra implicación no es tan simple. Sea $x = a/b \in \mathbb{Q}$ y tomemos su desarrollo canónico $x = \sum_{i=k}^{\infty} x_i p^i$. Con el mismo método de antes, podemos suponer, sin pérdida de generalidad, que $x \in \mathbb{Z}_p$ (es decir, que $x = \sum_{i=0}^{\infty} x_i p^i$), e incluso que $x > 0$. Tomamos las expresiones de a y b en base p, $a = \sum_{i=0}^{n} a_i p^i$ y $b = \sum_{i=0}^{k} b_i p^i$. Entonces podemos escribir

$$x = \frac{a}{b} \Rightarrow \sum_{i=0}^{k} b_i p^i \sum_{i=0}^{\infty} x_i p^i = \sum_{i=0}^{n} a_i p^i$$

y esto nos da las ecuaciones de congruencias siguientes:

$$b_0 x_j + b_1 x_{j-1} + ... + b_j x_0 + r_j \equiv a_j \pmod{p} \ \forall j \leq \text{máx}(n, k)$$

$$b_0 x_j + ... + b_k x_{j-k} + r_j \equiv 0 \pmod{p} \ \forall j > \text{máx}(n, k),$$

$$r_0 = 0$$

$$pr_{j+1} = b_0x_j + b_1x_{j-1} + ... + b_jx_0 + r_j - a_j \ \forall 0 < j \leq \text{máx}(n,k)$$

$$pr_{j+1} = b_0x_j + ... + b_kx_{j-k} + r_j \ \forall j > \text{máx}(n,k).$$

Teniendo en cuenta que los b_i y los a_i son conocidos, podemos calcular de manera iterativa los valores de x_i como los representantes de la solución de las ecuaciones que cumplen que $0 \leq x_i < p$. Como el número de valores enteros entre 0 y $p-1$ es finito, en algún momento alcanzaremos un resultado ya encontrado y obtendremos un periodo.
Luego todo número racional tiene un desarrollo canónico periódico.

Q.E.D.

Nota. *Después de varios resultados contradiciendo nuestra experiencia en el caso real, he aquí uno importante que le es completamente análogo: hemos visto en el capítulo introductorio que un número real es racional si y sólo si su expresión decimal es periódica.*

Proposición 3.5.4. *Si $x \in \mathbb{Q}$, existe un entero k no nulo tal que $p^kx \in \mathbb{Z}_p$ y su desarrollo canónico es de la forma ...aaab con a y b enteros en base p con el mismo número de dígitos. Entonces $x > 0$ si y sólo si $a > b$.*

Demostración. Sea $x \in \mathbb{Q} \subset \mathbb{Q}_p$. Entonces por la proposición 3.4.4 sabemos que $\exists\ k \in \mathbb{Z}$ y $u \in \mathbb{Z}_p^*$ tales que $x = p^ku$ y por consiguiente que $p^{-k}x = u \in \mathbb{Z}_p$. Ahora, como $p^{-k}x$ es un racional tenemos que su desarrollo canónico es periódico. Denominamos n el número de cifras anteriores al periodo y t el número de cifras del periodo. Si definimos $d = \text{mcm}(n,t)$ podemos tomar $b =$ los primeros d términos del desarrollo y $a =$ los d siguientes. Como hemos cogido un múltiplo del periodo, efectivamente $p^{-k}x = ...aaaab$, y con un método semejante al del teorema anterior podemos ver que

$$p^{-k}x = b + a(p^d + p^{2d} + p^{3d} + ...) = b + a\frac{p^d}{1-p^d}.$$

Entonces

$$x > 0 \Leftrightarrow b + a\frac{p^d}{1-p^d} > 0 \Leftrightarrow b > a\frac{p^d}{p^d-1} > a.$$

Q.E.D.

Gracias al teorema de Ostrowski, que demostramos en el primer apartado de este capítulo, sabemos que el cuerpo de los reales, $\mathbb{R}$, y los cuerpos de los números p-ádicos, $\mathbb{Q}_p$, son las únicas compleciones (acordes a normas no triviales) no equivalentes de $\mathbb{Q}$. Esto nos hace preguntarnos qué relación hay exactamente entre las distintas normas de $\mathbb{Q}$.

Notación. *Con el interés de simplificar la escritura de estos resultados, denotaremos el valor absoluto usual por $|\ .\ |_\infty$ $(p = \infty)$ y el cuerpo de los números reales por $\mathbb{Q}_\infty$.*

Proposición 3.5.5 (Fórmula del producto)**.** *Para todo $x \in \mathbb{Q}^*$ el producto de su valor en todas las normas p-ádicas (incluyendo el «primo infinito» que acabamos de escribir) es* 1*. Es decir,*

$$\prod_{p \leq \infty} \mid x \mid_p = 1.$$

Demostración. Sabemos que $\parallel x \parallel = \parallel -x \parallel$ con cualquier norma, así que, al igual que en la demostración del teorema de Ostrowski, podemos reducirnos a los racionales positivos. Además, $\prod_{p \leq \infty} \mid n \mid_p = 1$ para cualquier natural, entonces también es cierto para todo racional. Por tanto, podemos restringir la prueba a los naturales no nulos.
Sea $n \in \mathbb{N} \setminus \{0\}$. Haciendo la descomposición en factores primos, obtenemos que $n = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_s^{a_s}$ con $s \in \mathbb{N}$ y $a_i \in \mathbb{N}$ para todo $i \in \{1, ..., s\}$. Luego tenemos que $\mid n \mid_p = 1$ si $p \neq p_i \ \forall i \in \{1, ..., s\}$, $\mid n \mid_{p_i} = p_i^{-a_i}$ y $\mid n \mid_\infty = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_s^{a_s}$. Una vez aquí el resultado es trivial.

Q.E.D.

Nota. *Esta fórmula nos permite, si conocemos el valor de todas las normas de un elemento menos una, calcular fácilmente el valor de la que falta.*

Y para acabar este capítulo, un comentario sobre las raíces de los polinomios con coeficientes racionales. Es evidente que si un polinomio $P(X) \in \mathbb{Q}[X]$ tiene una raíz en $\mathbb{Q}$ entonces tiene una raíz en $\mathbb{Q}_p$ para todo $p \leq \infty$. Esto significa que si existe un p tal que $P(X)$ no tiene ninguna raíz en $\mathbb{Q}_p$ entonces dicho polinomio no tiene ninguna raíz racional. Ahora bien, ¿es cierta la implicación contraria? Es decir, ¿es cierto que si un polinomio tiene raíces en todos los cuerpos $\mathbb{Q}_p$ y en $\mathbb{R}$ entonces tiene una raíz en $\mathbb{Q}$? Desgraciadamente, no es el caso. Aún así, existen ciertos contextos interesantes en los que sí que se cumple esta implicación. Uno de ellos es el de las raíces cuadradas.

Proposición 3.5.6. *Un número racional $x \in \mathbb{Q}$ es un cuadrado en $\mathbb{Q}$ (es decir, tiene una raíz cuadrada en $\mathbb{Q}$) si y sólo si es un cuadrado en $\mathbb{Q}_p$ para todo primo $p \leq \infty$.*

Demostración. Es evidente que si un número racional es un cuadrado en $\mathbb{Q}$, entonces también lo es en $\mathbb{Q}_p$ para todo primo $p \leq \infty$, ya que $\mathbb{Q} \subset \mathbb{Q}_p$ para todo p.

Para la otra implicación, sea $x \in \mathbb{Q}^*$. Entonces podemos escribirlo como $x = \pm \prod_{p \ primo} p^{\mathrm{ord}(p)}$ y será un cuadrado en $\mathbb{Q}$ si y sólo si es positivo y $\mathrm{ord}_p(x)$ es par para todo p. Ahora bien, como vimos en 3.4.4, podemos escribir x en $\mathbb{Q}_p$ como $x = p^{\mathrm{ord}_p(x)} u$ con $u \in \mathbb{Z}_p^*$, y entonces que x sea un cuadrado implica que $\mathrm{ord}_p(x)$ sea par. Añadiendo a esto que un número es un cuadrado en $\mathbb{R}$ si y sólo si es positivo, tenemos las condiciones que necesitábamos. Así pues, si un número racional es un cuadrado en $\mathbb{Q}_p$ para todo $p \leq \infty$ entonces es un cuadrado en $\mathbb{Q}$.

Q.E.D.

Capítulo 4

Propiedades algebraicas de $\mathbb{Q}_p$.

En este capítulo vamos de nuevo a basarnos en el trabajo de Svetlana Katok en «p-adic Analysis Compared with Real» [Kat07, págs. 33-43] al tiempo que no olvidamos el aporte que pueden hacer las demostraciones de «A Course in p-adic Analysis», de Alain M. Robert. En el apartado 4.4, «Propiedades algebraicas de $\mathbb{Z}_p$» utilizaremos ciertos resultados de «Introduction to Commutative Algebra», de Atiyah y MacDonald. Al igual que en el capítulo anterior, suponemos que p es un número primo positivo salvo que se diga lo contrario.

4.1. Raíces de los polinomios p-ádicos.

Después de haber hablado de métodos para saber si un polinomio con coeficientes racionales tiene raíces en $\mathbb{Q}$, es razonable preguntarse sobre los polinomios con coeficientes p-ádicos. Empecemos con un ejemplo sencillo de cálculo: ¿$\sqrt{6}$ pertenece a $\mathbb{Q}_5$? O lo que es lo mismo, ¿existe una sucesión de elementos $\{a_n\}_{n=k}^{\infty}$ con $k \in \mathbb{Z}$ y $0 \leq a_n < 5$ $\forall n \geq k$ tal que $\left(\sum_{i=k}^{\infty} a_i 5^i\right)^2 = 6$? Escribiendo 6 en su desarrollo canónico tenemos

$$\left(a_0 + a_1 5 + a_2 5^2 + ...\right)^2 = 1 + 1 \cdot 5.$$

Vayamos por partes. Siguiendo el algoritmo que hemos descrito en el capítulo anterior para la multiplicación, obtenemos que $a_0^2 \equiv 1 \pmod 5$. Teniendo en cuenta que $0 \leq a_0 < 5$, esto nos da dos posibilidades: $a_0 = 1$ o $a_0 = 4$. Elegimos el caso $a_0 = 1$ porque las operaciones son más sencillas, pero el procedimiento sería el mismo en el otro. Ahora tenemos que $2a_0a_1 + r_0 \equiv 1 \pmod 5$. Como hemos asumido que $a_0 = 1$, entonces $r_0 = 0$ y tenemos

$$2a_1 \equiv 1 \pmod 5 \Rightarrow a_1 = 3,\ r_1 = 1.$$

El siguiente paso sería determinar a_2: $2a_0a_2 + a_1^2 + r_1 \equiv 0 \pmod 5$ y eso nos da

$$2a_2 + 3^2 + 1 = 2a_2 + 10 \equiv 2a_2 \equiv 0 \pmod 5 \Rightarrow a_2 = 0,\ r_2 = 0.$$

Como podemos ver, una vez elegido un valor para a_0 el resto de los sumandos está determinado de manera unívoca por el algoritmo, dándonos los dos valores de $\sqrt{6}$ o, equivalentemente, las dos raíces de $P(X) = X^2 - 6 \in \mathbb{Q}_5[X]$. Sin embargo, no es difícil ver que existen elementos de $\mathbb{Q}_5$ que no tienen raíz cuadrada en el cuerpo: 2, por ejemplo. Podríamos continuar intentando encontrar un método general para saber si un elemento tiene raíz cuadrada o no, pero existe un resultado mucho más potente que nos asegura la existencia de soluciones para un polinomio cualquiera con coeficientes en $\mathbb{Z}_p$.

Notación. *Como es habitual, denotaremos a veces por $\mathbb{F}_p$ el cuerpo finito de p elementos.*

Notación. *Ampliando la equivalencia que explicitamos para los números naturales en la primera nota del capítulo 3, decimos que $a \in \mathbb{Z}_p$ es congruente con $b \in \mathbb{Z}_p$ módulo p^n y lo denotaremos por $a \equiv b \pmod{p^n}$ si se cumple que $\mid a - b \mid_p \leq p^{-n}$. Es decir, decimos que $a \equiv b \pmod{p^n}$ si tenemos que $a - b = \sum_{i=n}^{\infty} a_i p^i$.*

Nota. *Es importante darse cuenta de que se trata simplemente de una notación: a y b no pertenecen necesariamente a $\mathbb{Z}$, y en consecuencia la congruencia no tiene por qué estar definida.*

Teorema 4.1.1 (Lema de Hensel)**.** *Sea $P(X) \in \mathbb{Z}_p[X]$ un polinomio con coeficientes en los enteros p-ádicos. Si existe un entero p-ádico $a_0^* \in \mathbb{Z}_p$ tal que $P(a_0^*) \equiv 0 \pmod p$ y $P'(a_0^*) \not\equiv 0 \pmod p$, con $P'(X)$ el polinomio derivado de $P(X)$, entonces existe un único entero p-ádico a que sea raíz de $P(X)$ y cumpla que $a \equiv a_0^* \pmod p$.*

Demostración. Para esta demostración vamos a usar una especie de «forma p-ádica del método de Newton». Así, probaremos el resultado por recurrencia, siendo el elemento que encontramos en el paso k no una raíz del polinomio, sino únicamente una raíz módulo p^{k+1}. Obtendremos la raíz al hacer el paso al límite. Sea $P(X) = c_0 + ... + c_s X^s$.

Vamos a demostrar por inducción el siguiente resultado: para todo $n \in \mathbb{N}$ existe un entero p-ádico de la forma $a_n = \sum_{i=0}^{n} b_i p^i$ tal que

$$P(a_n) \equiv 0 \left(\mathrm{mod}\, p^{n+1}\right) \text{ y } a_n \equiv a_0^* \left(\mathrm{mod}\, p\right).$$

La base de la inducción es fácil: si tomamos $a_0 = a_0^*$ las propiedades se cumplen de forma automática.
Sea $n - 1 \in \mathbb{N}$. Por hipótesis de inducción existe un entero p-ádico $a_{n-1} = \sum_{i=0}^{n-1} b_i p^i$ que cumple las propiedades citadas anteriormente. Veamos si existe un entero p-ádico que las cumple para n.
Tomamos $a_n = a_{n-1} + x_n p^n$ en el que $x_n \in \mathbb{N}$ es un valor desconocido que

cumple que $0 \leq x_n < p$. Es evidente que $a_n \equiv a_0^* \,(\mathrm{mod}\, p)$. Escribimos el valor de $P(X)$ en ese punto, módulo p^{n+1}.

$$P(a_n) = P(a_{n-1}+x_n p^n) = \sum_{i=0}^{s} c_i (a_{n-1}+x_n p^n)^i = c_0 + \sum_{i=1}^{s} c_i \sum_{j=0}^{i} \binom{i}{j} a_{n-1}^j (x_n p^n)^{i-j}$$

$$= c_0 + \sum_{i=1}^{s} c_i (a_{n-1}^i + i a_{n-1}^{i-1} x_n p^n + p^{2n} C) \equiv P(a_{n-1}) + x_n p^n P'(a_{n-1}) \left(\mathrm{mod}\, p^{n+1}\right).$$

Por la hipótesis de inducción tenemos que $P(a_{n-1}) \equiv 0 \,(\mathrm{mod}\, p^n)$, lo cual significa que $P(a_{n-1}) = p^n \xi$ con $\xi \in \mathbb{Z}_p$, es decir, $P(a_{n-1}) \equiv \alpha_n p^n \left(\mathrm{mod}\, p^{n+1}\right)$ con $0 \leq \alpha_n < p$. Con estos datos, para que $P(a_n) \equiv 0 \left(\mathrm{mod}\, p^{n+1}\right)$ necesitamos que se cumpla lo siguiente:

$$P(a_n) \equiv \alpha_n p^n + x_n p^n P'(a_{n-1}) \equiv 0 \left(\mathrm{mod}\, p^{n+1}\right) \Rightarrow \alpha_n + x_n P'(a_{n-1}) \equiv 0 \,(\mathrm{mod}\, p),$$

lo cual es una ecuación que tiene una única solución si $P'(a_{n-1}) \not\equiv 0 \,(\mathrm{mod}\, p)$. Pero por hipótesis de inducción $a_{n-1} \equiv a_0^* \,(\mathrm{mod}\, p)$, y $P'(a_0^*) \not\equiv 0 \,(\mathrm{mod}\, p)$, luego tenemos nuestra solución. Es el elemento $x_n \in \{1, ..., p-1\}$ tal que

$$x_n \equiv \frac{-\alpha_n}{P'(a_{n-1})} \,(\mathrm{mod}\, p).$$

Tenemos, pues, una sucesión de elementos de $\mathbb{Z}_p$ tal que $P(a_n) \equiv 0 \left(\mathrm{mod}\, p^{n+1}\right)$ para todo n, es decir, tal que $\mid P(a_n) \mid_p \leq p^{-n}$. Si tomamos $a = \lim_{n\to\infty} a_n$ tenemos el valor requerido.
En cuanto a la unicidad, el método de obtención de la sucesión $\{a_n\}_{n=0}^{\infty}$ nos da la unicidad de sus elementos, y éstos la unicidad de a.

Q.E.D.

En la formulación que hemos dado de este teorema la condición $P'(a_0^*) \not\equiv 0 \,(\mathrm{mod}\, p)$ es esencial para el buen funcionamiento del resultado, pero existen otras formulaciones alternativas con condiciones más débiles. Vamos a enunciar otra versión más fuerte tomada del libro de Robert [Rob00]. Utilizaremos este resultado en el apartado siguiente.

Teorema 4.1.2 (Versión alternativa del Lema de Hensel)**.** *Sea $P(X) \in \mathbb{Z}_p[X]$ un polinomio con coeficientes en los enteros p-ádicos. Si existe un $a_0^* \in \mathbb{Z}_p$ tal que $\mid P(a_0^*) \mid_p < \mid P'(a_0^*) \mid_p^2$, entonces existe una raíz $a \in \mathbb{Z}_p$ de $P(X)$ tal que*

$$\mid a - a_0^* \mid_p = \mid \frac{P(a_0^*)}{P'(a_0^*)} \mid_p < \mid P'(a_0^*) \mid_p .$$

Además, a es la única raíz de $P(X)$ que pertenece a la bola abierta de centro a_0 y radio $\mid P'(a_0) \mid_p$. [Rob00, págs. 80-82]

Nota. *Es sencillo darse cuenta de que esta segunda versión del Lema de Hensel engloba la primera. En efecto, las condiciones de la primera versión escritas con la notación de las normas significan que* $\mid P(a_0^*) \mid_p \leq p^{-1}$ *y que* $\mid P'(a_0^*) \mid_p > p^{-1}$*, es decir, que* $\mid P'(a_0^*) \mid_p = 1$*, porque* $a_0^* \in \mathbb{Z}_p$*. Tenemos por tanto que* $\mid P(a_0^*) \mid_p \leq p^{-1} < 1^2 = \mid P'(a_0^*) \mid_p^2$ *y se cumplen las condiciones de la segunda versión.*

Tanto el ejemplo como la demostración de la primera versión del Lema de Hensel apuntan hacia una relación muy estrecha entre el anillo $\mathbb{Z}_p$ y los cuerpos finitos $\mathbb{Z}/p^n\mathbb{Z}$. Aunque estudiaremos dicha relación en profundidad en el capítulo siguiente, adelantamos aquí un par de resultados relacionados con las congruencias.

Definición 4.1.3. *Sea* $P(X) \in \mathbb{Z}[X]$ *un polinomio con coeficientes enteros y* k *un entero positivo. Diremos que* $a \in \mathbb{Z}$ *es una raíz entera de* $P(X)$ *módulo* p^k *si se cumple que* $P(a) \equiv 0 \pmod{p^k}$

Teorema 4.1.4. *Sea* $P(X) \in \mathbb{Z}[X]$ *un polinomio con coeficientes enteros. Entonces* $P(X)$ *tiene una raíz en* $\mathbb{Z}_p$ *si y sólo si tiene una raíz entera módulo* p^k *para todo* k *natural positivo.*

Demostración. Suponemos que existe una raíz a de $P(X)$ en los enteros p-ádicos, es decir, $\exists\, a \in \mathbb{Z}_p$ tal que $P(a) = 0$. Por la construcción del desarrollo canónico de a (teorema 3.2.3) sabemos que existe una sucesión $\{a_n\}_{n=0}^{\infty}$ de números enteros tal que $0 \leq a_n < p^n$ y $a \equiv a_n \pmod{p^n}$. Por lo tanto, para todo $n \in \mathbb{N}$ tenemos $a_n \in \mathbb{Z}$ y $a - a_n = \sum_{i=n}^{\infty} a_i p^i$. Entonces $\mid P(a_n) \mid_p = \mid P(a) - P(a_n) \mid_p \leq p^{-n}$, y como $a_n \in \mathbb{N}$ para todo $n \in \mathbb{N}$, eso significa que tenemos una raíz entera módulo p^n para todo natural, y hemos demostrado la primera implicación.

Veamos la implicación inversa. Suponemos que para todo entero $n > 0$ existe un $a_n \in \mathbb{Z}$ que es raíz de $P(X)$ módulo p^n. Estos elementos forman una sucesión $\{a_n\}_{n=0}^{\infty}$ en $\mathbb{Z}$. Hemos visto anteriormente que todo entero pertenece al anillo de los enteros p-ádicos. Ahora bien, también sabemos que $\mathbb{Z}_p$ es secuencialmente compacto, luego $\{a_n\}_{n=0}^{\infty}$ tiene una subsucesión convergente $\{a_{n_i}\}_{i=0}^{\infty}$. Llamamos $a = \lim_{i\to\infty} a_{n_i}$ y demostraremos que este a es una raíz del polinomio. Como un polinomio es una función continua, tenemos que $P(a) = P(\lim_{i\to\infty} a_{n_i}) = \lim_{i\to\infty} P(a_{n_i})$. Por otro lado, tenemos que $P(a_{n_i}) \equiv 0 \pmod{p^{n_i}}$, y si combinamos ambas cosas obtenemos que $\mid P(a_{n_i}) \mid_p \leq p^{n_i} \to 0$, es decir, que $P(a) = 0$ y a es una raíz de $P(X)$.

Q.E.D.

Nota. *Este resultado combinado con la primera versión del Lema de Hensel nos da una manera relativamente simple de determinar la existencia o no de una raíz*
p-ádica de un polinomio con coeficientes enteros. En un primer tiempo, comprobamos si $P(X)$ *tiene raíces enteras módulo* p*. Si no es el caso, entonces por el teorema que acabamos de demostrar el polinomio no puede tener una raíz en* $\mathbb{Z}_p$*. Ahora, si* $P(X)$ *tiene una raíz módulo* p*, calculamos si este valor es una*

raíz de la derivada módulo p. Si no lo es, entonces por el Lema de Hensel existe una raíz perteneciente a $\mathbb{Z}_p$.

Definición 4.1.5. *Suponemos que* $a \in \mathbb{Z}$ *no es divisible por p. Entonces decimos que a es un residuo cuadrático módulo p si la ecuación* $x^2 = a$ *tiene una solución en* $\mathbb{F}_p^*$*, o, equivalentemente, si* $x^2 \equiv a \,(\mathrm{mod}\, p)$ *tiene una solución en el conjunto* $\{1, ..., p-1\}$.

Proposición 4.1.6. *Sea* $a \in \mathbb{Z}$ *un entero no divisible por p. Entonces, si* $p \neq 2$*, tenemos que a tiene una raíz cuadrada en* $\mathbb{Z}_p$ *si y sólo si es un residuo cuadrático módulo p.*

Demostración. Lo primero de todo, definimos el polinomio $P(X) = X^2 - a \in \mathbb{Z}_p[X]$.

Sea $a \in \mathbb{Z}$ un residuo cuadrático. Demostrar que a tiene una raíz cuadrada en $\mathbb{Z}_p$ es lo mismo que ver que $P(X)$ tiene una raíz en $\mathbb{Z}_p$. Para ello utilizaremos el Lema de Hensel en su versión débil. Tenemos, por tanto, que $P'(X) = 2X$. Como a es un residuo cuadrático módulo p, sabemos que existe un $x \in \{1, ..., p-1\}$ tal que $a \equiv x^2 \,(\mathrm{mod}\, p)$. Tenemos, por consiguiente, que

$$P(x) \equiv 0 \,(\mathrm{mod}\, p) \text{ y } P'(x) = 2x \not\equiv 0 \,(\mathrm{mod}\, p)\,,$$

esto último porque $x \neq 0$ y $(x, p) = 1$. Por el Lema de Hensel, el polinomio $P(X) = X^2 - a$ tiene una raíz en $\mathbb{Z}_p$ y a tiene una raíz cuadrada en $\mathbb{Z}_p$.

La implicación contraria es una aplicación directa del teorema anterior. Si $a \in \mathbb{Z}$ no es un residuo cuadrático, por definición $P(X)$ no tiene ninguna raíz entera módulo p, y tampoco en $\mathbb{Z}_p$.

Q.E.D.

Nota. *No está de más destacar que, aunque la condición de* $p \neq 2$ *es necesaria para el buen funcionamiento de la primera implicación, no afecta en absoluto a la segunda. Por tanto, si* $p = 2$*, se cumple también que si* $a \in \mathbb{Z}$ *no es un residuo cuadrático entonces no tiene raíz cuadrada en* $\mathbb{Z}_p$.

Aunque en principio el resultado que hemos demostrado nos da la existencia y la inexistencia de raíces cuadradas únicamente en $\mathbb{Z}_p$, podemos demostrar que en realidad esto es todo lo que necesitamos.

Proposición 4.1.7. *Sean* $a \in \mathbb{Z}_p$ *un entero p-ádico y* $m \in \mathbb{N}^*$ *un entero positivo. Entonces a tiene una raíz m-ésima en* $\mathbb{Q}_p$ *si y sólo si la tiene en* $\mathbb{Z}_p$.

Demostración. Una de las dos implicaciones es inmediata: sabemos que $\mathbb{Z}_p \subset \mathbb{Q}_p$, y por tanto si a tiene una raíz en $\mathbb{Z}_p$ también la tiene en $\mathbb{Q}_p$.
Veamos la otra. Sea $a \in \mathbb{Z}_p$ tal que existe $x \in \mathbb{Q}_p$ tal que $x^m = a$. El que $a \in \mathbb{Z}_p$ significa que $\mid a \mid_p \leq 1$. Por lo tanto, tenemos que $\mid x^m \mid_p = \mid x \mid_p^m = \mid a \mid_p \leq 1$, y en consecuencia $\mid x \mid_p \leq \sqrt[m]{1} = 1$. Por definición de los enteros p-ádicos, esto es equivalente a que $x \in \mathbb{Z}_p$. Hemos acabado.

Q.E.D.

Así, con este sencillo método podemos saber si la raíz cuadrada de cualquier número entero pertenece a $\mathbb{Q}_p$. Por ejemplo, $\sqrt{-1}$ está en $\mathbb{Z}_5$, y por tanto en $\mathbb{Q}_5$, porque $-1 = 4 - 5 \equiv 2^2 \pmod 5$. En cambio, no es difícil ver, aunque no se pueda aplicar la proposición, que $\sqrt{p} \notin \mathbb{Q}_p$ para todo p primo. En efecto, si suponemos que existe $p = \left(\sum_{i=0}^{\infty} a_i p^i\right)^2 = x$, aplicando el mismo método que hemos utilizado al principio del capítulo para encontrar $\sqrt{6}$, tenemos que $a_0^2 \equiv 0 \pmod p$, y por tanto $a_0 = 0$, porque $p \nmid a_0$. Pero entonces el término de orden más pequeño de x es $(a_1 p)^2 \equiv 0 \left(\mathrm{mod}\, p^2\right)$ y no tenemos ningún término en p. Luego no existe ningún entero p-ádico tal que $x^2 = p$. Y como hemos probado que si un entero p-ádico no tiene raíz en $\mathbb{Z}_p$ tampoco la tiene en $\mathbb{Q}_p$, $\sqrt{p}$ no puede pertenecer a $\mathbb{Q}_p$.

4.2. Consecuencias del Lema de Hensel.

El Lema de Hensel, incluso en su versión más débil, es un resultado con algunas consecuencias realmente interesantes. Sea $(\mathbb{Q}_p^*)^2$ el conjunto de los elementos de $\mathbb{Q}_p^*$ que tienen una raíz cuadrada en $\mathbb{Q}_p^*$, es decir, $(\mathbb{Q}_p^*)^2 = \left\{a^2 /\ a \in \mathbb{Q}_p^*\right\}$. Entonces, a guisa de ejemplo de consecuencia de dicho lema, vamos a tratar el grupo cociente $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$.

Lema 4.2.1. *Si $p \neq 2$, una unidad p-ádica $u \in \mathbb{Z}_p^*$ es un cuadrado en $\mathbb{Z}_p$ si y sólo si el primer coeficiente de su desarrollo canónico es un residuo cuadrático módulo p.*

Demostración. Sea $p \neq 2$ y $u \in \mathbb{Z}_p^*$ con $u = \sum_{i=0}^{\infty} a_i p^i$.

Suponemos que u es un cuadrado en $\mathbb{Z}_p$. Entonces existe $x \in \mathbb{Z}_p$ con $x^2 = u$, y escribimos $x = \sum_{i=0}^{\infty} c_i p^i$. Calculando coeficientes como al principio del capítulo, tenemos que $a_0 \equiv c_0^2 \pmod p$.
Si $c_0 = 0$, entonces $c_0^2 = 0 \equiv a_0 \pmod p$. Esto no es posible, porque $u \in \mathbb{Z}_p^*$, y por tanto $a_0 \neq 0$.
Si $c_0 \neq 0$, entonces por la construcción del desarrollo canónico tenemos que $0 < c_0 < p$ y la congruencia $y^2 \equiv a_0 \pmod p$ tiene una solución. Luego a_0 es un residuo cuadrático de u.

Veamos la otra implicación. Suponemos que a_0 es un residuo cuadrático módulo p, es decir, que existe $a \in \{1, ..., p\}$ tal que $a^2 \equiv a_0 \pmod p$. Definimos el polinomio $P(X) = X^2 - u \in \mathbb{Q}_p[X]$. Si este polinomio tiene una raíz en $\mathbb{Z}_p$ hemos acabado. Para ello, vamos a intentar aplicar el Lema de Hensel (en la versión de 4.1.1) tomando $a_0^* = a$.

$$P(a) = a^2 - u = a^2 - a_0 - p\sum_{i=0}^{\infty} a_{i+1} p^i \Rightarrow P(a) \equiv a^2 - a_0 \equiv 0 \pmod p$$

$$P'(X) = 2X \Rightarrow P'(a) = 2a \not\equiv 0 \pmod p \text{ si } p \neq 2, \text{ porque } p \nmid a.$$

Luego podemos aplicar el Lema de Hensel: existe un $b \in \mathbb{Z}_p$ raíz del polinomio $P(X) = X^2 - u$, que es una raíz cuadrada en $\mathbb{Z}_p$ de u. Hemos acabado.

Q.E.D.

Teorema 4.2.2. *Si $p \neq 2$ entonces el grupo $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ es isomorfo al grupo de Klein, es decir, a $\mathbb{F}_2 \times \mathbb{F}_2$.* [Rob00, pág. 50]

Demostración. Sea $p \neq 2$. Si $x \in \mathbb{Q}_p^*$, entonces por la proposición 3.4.4 sabemos que existe $u \in \mathbb{Z}_p^*$ y $k \in \mathbb{Z}$ tales que $x = p^k u$. Por lo tanto, x es un cuadrado en $\mathbb{Q}_p$ si y sólo si u es un cuadrado en $\mathbb{Z}_p$ y k es par. Ahora bien, hemos visto en el lema anterior que $u \in \mathbb{Z}_p^*$ es un cuadrado en $\mathbb{Z}_p$ si y sólo si el primer coeficiente de su desarrollo canónico es un residuo cuadrático módulo p, es decir, $u = \sum_{i=0}^{\infty} a_i p^i$ y $\exists\ a \in \mathbb{F}_p^*$ tal que $a^2 = a_0$, considerando $a_0 \in \mathbb{F}_p^*$. Pero esto lo podemos expresar también diciendo que $u \in \mathbb{Z}_p^*$ es un cuadrado en $\mathbb{Z}_p$ si y sólo si $a_0 \in (\mathbb{F}_p^*)^2 = \left\{x^2 /\ x \in \mathbb{F}_p^*\right\}$.
Tomamos el homomorfismo sobreyectivo siguiente:

$$\begin{aligned} \Phi : \mathbb{Q}_p &\longrightarrow \frac{(p)}{(p)^2} \times \frac{\mathbb{F}_p^*}{(\mathbb{F}_p^*)^2} \\ x = p^n u &\longmapsto ([p^n], [a_0]) \end{aligned}$$

donde (p) es el ideal de $\mathbb{Z}$ generado por p. Por el primer teorema de isomorfía,

$$\frac{\mathbb{Q}_p^*}{\ker \Phi} \simeq \frac{(p)}{(p)^2} \times \frac{\mathbb{F}_p^*}{(\mathbb{F}_p^*)^2}$$

y $\ker \Phi = \left\{p^n u /\ n \text{ par y } c_0 \in (\mathbb{F}_p^*)^2\right\} = (\mathbb{Q}_p)^2$. Luego tenemos que

$$\frac{\mathbb{Q}_p^*}{(\mathbb{Q}_p^*)^2} \simeq \frac{(p)}{(p)^2} \times \frac{\mathbb{F}_p^*}{(\mathbb{F}_p^*)^2} \simeq \mathbb{F}_2 \times \mathbb{F}_2$$

y hemos acabado.

Q.E.D.

Ahora bien, este resultado no nos sirve para el caso de $p = 2$, porque el polinomio que utilizamos para demostrar el lema tiene derivada nula módulo 2, y por tanto no podemos aplicar el Lema de Hensel en su versión más débil. Aquí es donde veremos la utilidad de la versión alternativa del teorema.

Lema 4.2.3. *Si $p = 2$, entonces una unidad p-ádica $u \in \mathbb{Z}_p^*$ es un cuadrado en $\mathbb{Z}_p$ si y sólo si $u \equiv 1 \pmod 8$.*

Demostración. Tomamos $p = 2$. Sea $u \in \mathbb{Z}_2^*$ una unidad 2-ádica y $\sum_{i=0}^{\infty} u_i p^i$ su desarrollo canónico. Entonces, por definición de unidad p-ádica, sabemos que $0 < u_0 < 2$ y, en consecuencia, $u = 1 + 2a$, con $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$.
Suponemos ahora que u es un cuadrado en $\mathbb{Z}_2$, es decir, $\exists\ x = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_2$ tal que $x^2 = u$. Por tanto, tenemos que $b_0^2 + 2b_0b_1 \cdot 2 + (2b_0b_2 + b_1^2)2^2 + \ldots = 1 + 2a$. Esto nos permite obtener los siguientes coeficientes de x:

$$b_0^2 \equiv 1 \pmod 2 \Rightarrow b_0 = 1 \Rightarrow a_0 \equiv 2b_1 = 2b_1 \pmod 2 \Rightarrow a_0 = 0$$

$$\text{Si } b_1 = 0,\ a_1 \equiv 2b_0b_2 + b_1^2 = 2b_2 = 2b_2 \,(\mathrm{mod}\, 2) \Rightarrow a_1 = 0$$

$$\text{Si } b_1 = 1,\ a_2 \equiv 2b_0b_2 + b_1^2 + 1 = 2(b_2+1) = 2(b_2+1) \,(\mathrm{mod}\, 2) \Rightarrow a_1 = 0$$

Luego en todos los casos tenemos que $u = 1 + 8b$ con $b \in \mathbb{Z}_p$, y por tanto que $u \equiv 1 \,(\mathrm{mod}\, 8)$.

Es en la implicación inversa donde utilizaremos la versión fuerte del Lema de Hensel. Así, sea $u \in \mathbb{Z}_2^*$ una unidad 2-ádica tal que $u \equiv 1 \,(\mathrm{mod}\, 8)$. Definimos el polinomio $P(X) = X^2 - u$ y tomamos $1 \in \mathbb{Z}_2$. Entonces tenemos las siguientes desigualdades:

$$\mid P(1) \mid_p = \mid 1^2 - u \mid_p = \mid 1 - u \mid_p \leq \frac{1}{2^3} \text{ por la definición de } u \equiv 1 \left(\mathrm{mod}\, 2^3\right)$$

$$P'(X) = 2X \Rightarrow P'(1) = 2 \Rightarrow \mid P'(1) \mid_2 = \mid 2 \mid_2 = \frac{1}{2} \Rightarrow \mid P'(1) \mid_2^2 = \frac{1}{2^2}$$

Luego tenemos que

$$\mid P(1) \mid_2 \leq \frac{1}{2^3} < \frac{1}{2^2} = \mid P'(1) \mid_2^2$$

y cumplimos la condición del teorema 4.1.2. Por lo tanto, tenemos que $\exists\, x \in \mathbb{Z}_2$ tal que $P(x) = 0$, y $x^2 = u$. Hemos acabado.

Q.E.D.

Teorema 4.2.4. *Si $p = 2$ entonces el grupo $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ es isomorfo a $(\mathbb{F}_2)^3$.* [Rob00, págs. 50-51]

Demostración. Empezamos de la misma manera que en el caso $p \neq 2$. Sea $x \in \mathbb{Q}_2^*$. Por la proposición 3.4.4 tenemos que $\exists\, n \in \mathbb{Z}$ y $u \in \mathbb{Z}_2^*$ tales que $x = 2^n u$, y por lo tanto x es un cuadrado en $\mathbb{Q}_2$ si y sólo si n es par y u es un cuadrado en $\mathbb{Z}_2$. Entonces, por el mismo razonamiento que en el teorema anterior, tenemos que

$$\frac{\mathbb{Q}_2^*}{\left(\mathbb{Q}_2^*\right)^2} \simeq \frac{(2)}{(2)^2} \times \frac{\mathbb{Z}_2^*}{\left(\mathbb{Z}_2^*\right)^2}.$$

Por lo tanto, lo que nos falta por ver es a qué anillo es isomorfo $\mathbb{Z}_2^*/(\mathbb{Z}_2^*)^2$.
Sabemos (enunciado en la prueba del lema anterior) que si $u \in \mathbb{Z}_2^*$, entonces $u = 1 + 2a$ con $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_2$. Luego podemos escribir $\mathbb{Z}_2^* = 1 + 2\mathbb{Z}_2$.
Si dividimos $\mathbb{Z}_2$ en los casos $a_0 = 0$ y $a_0 = 1$ obtenemos que $\mathbb{Z}_2^* = (1 + 2\mathbb{Z}_2) \cup (1 + 4\mathbb{Z}_2)$. Con la fórmula que hemos dado en el apartado de «Operaciones en $\mathbb{Q}_p$» para calcular los opuestos de los enteros en su desarrollo canónico tenemos que $-4 = \sum_{i=2}^{\infty} 1 \cdot 2^i$, y eso nos da que $-1 - 4 = 1 + 2$ en $\mathbb{Q}_2$. Por lo tanto, podemos escribir $\mathbb{Z}_2^* = (-1 - 4\mathbb{Z}_2) \cup (1 + 4\mathbb{Z}_2)$, lo que nos permite asegurar que

$$\mathbb{Z}_2^* \simeq \{1, -1\} \times (1 + 4\mathbb{Z}_2) \simeq \mathbb{F}_2 \times (1 + 4\mathbb{Z}_2).$$

Por el lema anterior, $u \in \mathbb{Z}_2^*$ es un cuadrado si y sólo si $u \in (1 + 8\mathbb{Z}_2)$, y tenemos

$$\frac{\mathbb{Z}_2^*}{\left(\mathbb{Z}_2^*\right)^2} \simeq \mathbb{F}_2 \times \frac{1 + 4\mathbb{Z}_2}{1 + 8\mathbb{Z}_2} \simeq \mathbb{F}_2 \times \frac{4\mathbb{Z}_2}{8\mathbb{Z}_2} \simeq \mathbb{F}_2 \times \mathbb{F}_2.$$

Esto nos da

$$\frac{\mathbb{Q}_2^*}{(\mathbb{Q}_2^*)^2} \simeq \frac{(2)}{(2)^2} \times \frac{\mathbb{Z}_2^*}{(\mathbb{Z}_2^*)^2} \simeq \mathbb{F}_2 \times \mathbb{F}_2 \times \frac{1+4\mathbb{Z}_2}{1+8\mathbb{Z}_2} \simeq (\mathbb{F}_2)^3 .$$

Tenemos el resultado que buscábamos.

Q.E.D.

4.3. Raíces de la unidad.

En el apartado anterior hemos usado el Lema de Hensel para ver qué elementos de $\mathbb{Q}_p$ tienen raíz cuadrada. Ahora, otra cuestión que podemos plantear gracias a este teorema sería la de qué raíces de la unidad pertenecen a $\mathbb{Q}_p$, aunque en este caso la relación es menos estrecha. Sea m un entero positivo. Recordemos que una raíz m-ésima de la unidad es un elemento $x \in \mathbb{Q}_p$ tal que $x^m = 1$. Se dice que una raíz m-ésima es primitiva si $x^n \neq 1$ para todo $0 < n < m$.

Proposición 4.3.1. *Las raíces de la unidad son unidades p-ádicas.* [Rob00, pág. 51]

Demostración. Sea $x \in \mathbb{Q}_p$ una raíz m-ésima de la unidad. Entonces sabemos que $x^m = 1$, luego $\mathrm{ord}_p(x^m) = m \cdot \mathrm{ord}_p(x) = \mathrm{ord}_p(1) = 0$, y por tanto $\mathrm{ord}_p(x) = 0$, porque $m \neq 0$. Esto demuestra que x es una unidad p-ádica.

Q.E.D.

Proposición 4.3.2. *Para todo entero positivo m que no sea múltiplo de p, existe una raíz m-ésima de la unidad si y sólo si m divide a $p-1$. En ese caso, el conjunto de las raíces m-ésimas está contenido en el de las raíces $(p-1)$-ésimas de la unidad, y estas últimas forman un subgrupo cíclico de $\mathbb{Z}_p^*$ de orden $(p-1)$.*

Demostración. Supongamos que $m \mid p-1$. Entonces tenemos que $p-1 = km$ con $k \in \mathbb{N}$. Si α es una raíz $(p-1)$-ésima de la unidad, $\alpha^{p-1} = 1$ y $(\alpha^k)^m = \alpha^{km} = \alpha^{p-1} = 1$. Luego si existe α raíz $(p-1)$-ésima de la unidad existe una raíz m-ésima de la unidad, α^k.
Definimos el polinomio $P(X) = X^{p-1} - 1 \in \mathbb{Z}[X]$. Evidentemente, cualquier raíz del polinomio $P(X)$ es una raíz $(p-1)$-ésima de la unidad. Tomamos $x_0 \in \mathbb{N}$ tal que $0 < x_0 < p$. El grupo multiplicativo $\mathbb{F}_p^*$ tiene $p-1$ elementos, lo que significa que el orden de $[x_0]$ como elemento de $\mathbb{F}_p^*$ es un divisor de $p-1$. Por lo tanto, $P(x_0) \equiv 0 \,(\mathrm{mod}\, p)$. Por otro lado, como $p \nmid x_0^{p-2}$, $P'(x_0) \not\equiv 0 \,(\mathrm{mod}\, p)$ y se cumplen las condiciones del Lema de Hensel en la versión de 4.1.1, tenemos $(p-1)$ raíces $(p-1)$-ésimas cuyos desarrollos canónicos tienen como primer coeficiente $1, 2, ..., p-1$ respectivamente, y por tanto existen raíces m-ésimas de la unidad.

Supongamos, recíprocamente, que $\alpha \in \mathbb{Q}_p$ es una raíz m-ésima de la unidad.

Por 4.1.7, sabemos que $\alpha \in \mathbb{Z}_p$. Sea α_0 el primer coeficiente de su desarrollo canónico. Entonces sabemos que $\alpha_0^m \equiv 1 \,(\mathrm{mod}\, p)$, y, como el orden de todo elemento de $\mathbb{F}_p^*$ es un divisor de $p-1$, tenemos que $m \mid p-1$. Luego, podemos escribir de nuevo $p-1 = km$, y $\alpha^{p-1} = \alpha^{km} = 1^k = 1$. Así pues, toda raíz m-ésima es una raíz $(p-1)$-ésima.

Como el polinomio $P(X) = X^{p-1} - 1$ tiene como máximo $p-1$ raíces en $\mathbb{Q}_p$, estas son las que hemos encontrado, porque son todas distintas. Por tanto, el conjunto formado por las raíces $(p-1)$-ésimas de la unidad tiene $(p-1)$ elementos. Ahora bien, el grupo de las raíces k-ésimas de la unidad en un cuerpo es siempre cíclico [Coh03, pág. 218], luego tenemos que el conjunto de las raíces $(p-1)$-ésimas de la unidad forman un grupo cíclico de $\mathbb{Z}_p^*$ con $(p-1)$ elementos y hemos acabado.

Q.E.D.

Estas raíces $(p-1)$-ésimas de la unidad tienen una relación muy estrecha con la función signo que definimos a continuación.

Definición 4.3.3. *Sea $x \in \mathbb{Z}_p$ un entero p-ádico. Entonces llamamos «signo» a la función* $\mathrm{sgn}_p(x) = \lim_{n\to\infty} x^{p^n}$.

Para demostrar que esta función está bien definida, así como algunas otras propiedades, necesitamos de un lema previo.

Lema 4.3.4. *Sea $x \in \mathbb{Z}_p$ tal que el primer coeficiente de su desarrollo canónico sea x_0. Entonces* $\mid x^p - x_0^p \mid_p \leq p^{-1} \mid x - x_0 \mid_p$.

Demostración. Sea $x = \sum_{i=0}^{\infty} x_i p^i$ nuestro entero p-ádico. Entonces lo podemos escribir como $x = x_0 + \alpha$, con $\alpha = x - x_0 = \sum_{i=1}^{\infty} x_i p^i$, y por tanto $\mid \alpha \mid_p \leq p^{-1}$. Entonces tenemos las siguientes igualdades:

$$x^p - x_0^p = (x_0+\alpha)^p - x_0^p = \sum_{i=0}^{p} \binom{p}{i} x_0^{p-i}\alpha^i - x_0^p = \sum_{i=1}^{p} \binom{p}{i} x_0^{p-i}\alpha^i =$$

$$\alpha\left(\binom{p}{1}x_0^{p-1} + \binom{p}{2}x_0^{p-2}\alpha + ... + \binom{p}{p}\alpha^{p-1}\right) =$$

$$(x-x_0)\left(\binom{p}{1}x_0^{p-1} + \binom{p}{2}x_0^{p-2}\alpha + ... + \binom{p}{p}\alpha^{p-1}\right).$$

Como $\binom{p}{i} \in \mathbb{N}$, por el teorema 2.1.2 tenemos que $\mid \binom{p}{i} \mid_p \leq 1$. Al aplicar esta desigualdad junto con $\mid x_0 \mid_p = 1$ y que $\mid \alpha \mid_p \leq p^{-1}$ a los sumandos de la fórmula anterior obtenemos que $\mid \binom{p}{i} x_0^{p-i}\alpha^{i-1} \mid_p \leq p^{-1}$ para todo $1 \leq i < p$. Por la desigualdad triangular fuerte,

$$\mid x^p - x_0^p \mid_p = \mid (x-x_0)\left(\binom{p}{1}x_0^{p-1} + \binom{p}{2}x_0^{p-2}\alpha + ... + \binom{p}{p}\alpha^{p-1}\right) \mid_p$$

$$\leq \mid x - x_0 \mid_p \max(p^{-1}, ..., p^{-1}) = p^{-1} \mid x - x_0 \mid_p .$$

Hemos acabado.

Q.E.D.

Teorema 4.3.5. *Para todo $x \in \mathbb{Z}_p$, existe $\lim_{n\to\infty} x^{p^n}$. Además, la función «signo» cumple las siguientes propiedades:*

1. $\mathrm{sgn}_p(x)$ *depende únicamente del primer término del desarrollo canónico de x, que llamaremos x_0.*

2. $\mathrm{sgn}_p(xy) = \mathrm{sgn}_p(x) \cdot \mathrm{sgn}_p(y)$ *con $x, y \in \mathbb{Z}_p$.*

3. $\mathrm{sgn}_p(x) = 0$ *si $x_0 = 0$ y $\mathrm{sgn}_p(x)$ es una raíz $(p-1)$-ésima de la unidad si $x_0 \neq 0$.*

Demostración. Demostraremos la existencia del límite y la propiedad 1) de forma simultánea. Para ello, tomemos $x_0 \in \{1, ..., p-1\}$. Empezaremos mostrando que la sucesión $\left\{x_0^{p^n}\right\}_{n=0}^{\infty}$ es convergente. Recordamos el Teorema de Euler, que nos dice que si a y n son naturales primos entre sí, entonces $a^{\phi(n)} \equiv 1 \,(\mathrm{mod}\, n)$, donde ϕ es la función de Euler: $\phi(n)$ es el número de naturales menores que n primos con él. Este teorema nos da la siguiente congruencia:

$$x_0^{\phi(p^n)} \equiv 1 \,(\mathrm{mod}\, p^n)\,.$$

Como p es primo, sabemos que $\phi(p^n) = p^n - p^{n-1}$ y por lo tanto,

$$x_0^{p^n - p^{p-1}} \equiv 1 \,(\mathrm{mod}\, p^n) \Rightarrow x_0^{p^n} \equiv x_0^{p^{n-1}} \,(\mathrm{mod}\, p^n) \Rightarrow |\, x_0^{p^n} - x_0^{p^{n-1}} \,|_p \leq p^{-n}.$$

Por lo tanto, la sucesión $\left\{x_0^{p^n}\right\}_{n=0}^{\infty}$ es de Cauchy, y por completitud de $\mathbb{Z}_p$ converge hacia un $\mathrm{sgn}_p(x_0) = \lim_{n\to\infty} x_0^{p^n} \in \mathbb{Z}_p$. Como el límite en 0 es trivial ($\mathrm{sgn}_p(0) = 0$), tenemos que $\mathrm{sgn}_p(x_0)$ existe para todo $x_0 \in \{0, 1, ..., p-1\}$.

Veamos que de hecho existe $\mathrm{sgn}_p(x)$ para todo $x \in \mathbb{Z}_p$, y que está determinado por el primer término de su desarrollo canónico. Aplicando el lema anterior, tenemos que

$$|\, x^{p^n} - x_0^{p^n} \,|_p \leq p^{-1} \,|\, x^{p^{n-1}} - x_0^{p^{n-1}} \,|_p \leq ... \leq p^{-n} \,|\, x - x_0 \,|_p \longrightarrow 0.$$

Esto significa que $\lim_{n\to\infty} x^{p^n}$ existe y es igual a $\mathrm{sgn}_p(x_0) = \lim_{n\to\infty} x_0^{p^n}$. Por tanto, la función está bien definida en todo $\mathbb{Z}_p$ y se cumple la propiedad 1) del teorema.

La propiedad 2) es cierta por las propiedades de los límites.

Sólo nos falta ver la tercera propiedad, es decir, que si $x_0 \in \{1, ..., p-1\}$, entonces $\mathrm{sgn}_p(x_0)$ es una raíz $(p-1)$-ésima de la unidad. Para ello tenemos que

utilizar el Pequeño Teorema de Fermat, que no es más que el Teorema de Euler para $p = n$. Aplicando la segunda propiedad del teorema,

$$\mathrm{sgn}_p(x_0^{p-1}) = \mathrm{sgn}_p^{p-1}(x_0) = \mathrm{sgn}_p(1) = 1.$$

En consecuencia, los valores de $\mathrm{sgn}_p(x)$ son raíces del polinomio $P(X) = X^p - X$. Este polinomio tiene como máximo p raíces en $\mathbb{Q}_p$, que son $0 = \mathrm{sgn}_p(x)$ si $x_0 = 0$, y las raíces $(p-1)$-ésimas de la unidad. Esto demuestra la tercera propiedad y hemos terminado.

Q.E.D.

4.4. Otras propiedades algebraicas de $\mathbb{Z}_p$.

Para acabar el capítulo, veamos ahora algunas otras propiedades algebraicas de $\mathbb{Z}_p$. Somos conscientes de que algunos de los resultados enunciados aquí son ciertos en general para todo anillo de valoración discreta (ver [AM69, págs. 94-95]) y por tanto para $\mathbb{Z}_p$, pero al no estar familiarizados con el lenguaje de estos daremos demostraciones particulares para el caso p-ádico.

Nota. *El anillo $\mathbb{Z}_p$ es un dominio de integridad. Este resultado es evidente por la misma razón que lo es en el caso de $\mathbb{Z}$: están contenidos en sendos cuerpos ($\mathbb{Z} \subset \mathbb{Q}$ y $\mathbb{Z}_p \subset \mathbb{Q}_p$), los cuales por definición no pueden contener divisores de cero.*

Proposición 4.4.1. *El anillo $\mathbb{Z}_p$ es local, es decir, tiene un único ideal maximal. Este es $p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^*$.* [AM69, pág. 4]

Demostración. Cualquier ideal propio de $\mathbb{Z}_p$ está contenido en $p\mathbb{Z}_p$, porque un ideal propio de un anillo no puede contener unidades, y $p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^*$. Entonces si podemos ver que $p\mathbb{Z}_p$ es un ideal tendremos que es el único ideal maximal, y por tanto $\mathbb{Z}_p$ será un anillo local.

Sean $a, b \in \mathbb{Z}_p$. Entonces $pa, pb \in p\mathbb{Z}_p$. Como $\mathbb{Z}_p$ es un anillo, tenemos que $pa + pb = p(a+b) \in p\mathbb{Z}_p$ y $a \cdot pb = p(ab) \in p\mathbb{Z}_p$. Por lo tanto, $p\mathbb{Z}_p$ es cerrado para la suma y el producto, y $p\mathbb{Z}_p$ es un ideal. El anillo $\mathbb{Z}_p$ es local.

Q.E.D.

Proposición 4.4.2. *El anillo $\mathbb{Z}_p$ es un dominio de ideales principales. En concreto, sus ideales son $\{0\}$ y $p^k\mathbb{Z}_p$ con $k \in \mathbb{N}$.*

Demostración. Sea $I \neq \{0\}$ un ideal de $\mathbb{Z}_p$. Entonces vamos a ver que existe un $k \in \mathbb{N}$ tal que $I = p^k\mathbb{Z}_p$. Como la norma p-ádica toma un conjunto discreto de valores sobre $\mathbb{Z}_p$, existe $p^{-k} = \max\{|\, x \,|_p \,/\, x \in I\}$, y tal que $k \in \mathbb{N}$ (porque $I \subset \mathbb{Z}_p$). Tomamos un elemento $a \in I$ tal que $|\, a \,|_p = p^{-k}$. Entonces tenemos que $a = p^k u$ con $u \in \mathbb{Z}_p^*$ y, por la definición de ideal, $a \cdot u^{-1} = p^k u \cdot u^{-1} = p^k \in I$. Eso nos da que $p^k\mathbb{Z}_p \subset I$.

La inclusión contraria se prueba de la manera siguiente: sea $b \in I$. Entonces $\mid b \mid_p = p^{-j} \leq p^{-k}$, y tenemos las igualdades

$$b = p^j v = p^k p^{j-k} v \in p^k \mathbb{Z}_p, \text{ porque } p^{j-k} v \in \mathbb{Z}_p \text{ si } v \in \mathbb{Z}_p^* \text{ y } j \geq k.$$

Eso nos da que $I \subset p^k \mathbb{Z}_p$, y por tanto $I = p^k \mathbb{Z}_p$ y hemos acabado.

Q.E.D.

Proposición 4.4.3. *Para todo $n \in \mathbb{N}$, el anillo $\mathbb{Z}_p/p^n\mathbb{Z}_p$ es isomorfo a $\mathbb{Z}/p^n\mathbb{Z}$.* [Rob00, págs. 33-34]

Demostración. Antes de empezar, recordemos que dos elementos $x, y \in \mathbb{Z}_p$ pertenecen a la misma clase de equivalencia en $\mathbb{Z}_p/p^n\mathbb{Z}_p$ si y sólo si $x - y \in p^n\mathbb{Z}_p$. Eso quiere decir que $[x] = \left[\sum_{i=0}^{\infty} a_i p^i\right]$ e $[y] = \left[\sum_{i=0}^{\infty} b_i p^i\right]$ son iguales como elementos de $\mathbb{Z}_p/p^n\mathbb{Z}_p$ si y sólo si tenemos que $a_i = b_i \ \forall i < n$. Por tanto, podemos tomar como representantes de las clases de $\mathbb{Z}_p/p^n\mathbb{Z}_p$ los elementos de $\mathbb{Z}_p$ de la forma $\sum_{i=0}^{n-1} a_i p^i$. Esto nos da un isomorfismo de forma inmediata:

$$\begin{aligned} \mathbb{Z}_p/p^n\mathbb{Z}_p &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ \sum_{i=0}^{n-1} a_i p^i &\longmapsto \sum_{i=0}^{n-1} a_i p^i \end{aligned}$$

Esta función es evidentemente biyectiva, y no tenemos más que aplicar las descripciones que hicimos de las operaciones en $\mathbb{Z}_p$ para comprobar que se trata realmente de un homomorfismo.

Q.E.D.

Capítulo 5

Otra construcción de $\mathbb{Z}_p$: límites proyectivos.

A lo largo de este capítulo abandonaremos el punto de vista del libro de Svetlana Katok para centrarnos, durante un tiempo, en la visión de «A Course in p-adic Analysis», de Alain M. Robert [Rob00, págs. 26-34]. En el apartado 5.2 de este trabajo, «Límites proyectivos en espacios topológicos», utilizaremos también como apoyo el libro «General Topology», de Stephen Willard. De nuevo, suponemos que p es un primo positivo salvo que se diga lo contrario.

5.1. Límites proyectivos.

A lo largo de este trabajo hemos visto que los enteros p-ádicos se pueden definir de dos maneras distintas: como los elementos de $\mathbb{Q}_p$ con norma menor o igual que 1, y como series formales (téngase en mente el desarrollo canónico). Llegados a este punto vamos a considerar en una tercera opción: la de los límites proyectivos. Si tomamos $x = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$, podemos definir una función ϕ_n de $\mathbb{Z}_p$ en $\mathbb{Z}/p^n\mathbb{Z}$ tal que $\phi_n(x) = \sum_{i=0}^{n-1} a_i p^i$ para todo $n \in \mathbb{N}$. Entonces tendríamos que $\lim_{n\to\infty} \phi_n(x) = x$, en un cierto sentido. Nuestro objetivo en esta sección, pues, será formalizar esta noción de tal manera que podamos decir, de manera precisa, que $\mathbb{Z}/p^n\mathbb{Z}$ tiende hacia $\mathbb{Z}_p$. Para ello vamos a utilizar un concepto restringido del límite proyectivo. En efecto, aunque estos se pueden definir para sistemas no numerables a través de conjuntos parcialmente ordenados (ver [Gou12, pág. 64]), el caso numerable cubre todas nuestras necesidades.

Definición 5.1.1. *Llamamos sistema proyectivo o sistema inverso (de conjuntos y aplicaciones) a una sucesión $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ en la que los E_n son conjuntos y las ϕ_n son aplicaciones de E_{n+1} en E_n. Dichas aplicaciones suelen llamarse funciones de transición.*

Definición 5.1.2. *Sea $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ un sistema proyectivo. Entonces se dice que un conjunto E junto con las aplicaciones $\xi_n : E \to E_n$ es un límite*

proyectivo o límite inverso de $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ *si cumple que:*

1. *Para todo natural* $n \in \mathbb{N}$, $\xi_n = \phi_n \circ \xi_{n+1}$. *(condición de compatibilidad)*

2. *Para cualquier otro conjunto* X *y aplicaciones* $f_n : X \to E_n$ *con la condición de compatibilidad* $f_n = \phi_n \circ f_{n+1}$, *existe una única función* $f : X \to E$ *tal que* $f_n = \xi_n \circ f$ *para todo* $n \in \mathbb{N}$. *(propiedad universal)*

Notación. *Por abuso de notación, en muchas ocasiones omitiremos las funciones y llamaremos «límite proyectivo» al conjunto* E, *al que denotaremos por* $E = \lim_{\leftarrow} E_n$. *El sistema completo se puede representar como*

$$E_0 \leftarrow \ldots \leftarrow E_n \leftarrow \ldots \varprojlim E_n = E.$$

Es evidente que si E es límite proyectivo de un sistema proyectivo $\{(E_n, \phi_n)\}_{n=0}^{\infty}$, entonces lo es también de $\{(E_n, \phi_n)\}_{n=k}^{\infty}$ para todo $k \in \mathbb{N}$, teniendo en cuenta el abuso de notación explicado anteriormente: el conjunto es el mismo, pero eliminaríamos las funciones ξ_n con $n < k$. Por otro lado, si E junto con las funciones ξ_n con $n \geq k$ es el límite proyectivo del sistema $\{(E_n, \phi_n)\}_{n=k}^{\infty}$, entonces también lo es de $\{(E_n, \phi_n)\}_{n=0}^{\infty}$, definiendo ξ_{n-1} con $n \leq k$ por recurrencia de la forma siguiente: $\xi_{n-1} = \phi_{n-1} \circ \xi_n$. Podemos decir, entonces, que los límites proyectivos no dependen de los primeros términos de los sistemas inversos correspondientes.

Pero por ahora estamos hablado de una estructura abstracta que no es seguro que exista. Vamos, pues, a demostrar que para todo sistema inverso de conjuntos, el límite existe y es único (salvo biyección).

Teorema 5.1.3. *Para todo sistema proyectivo* $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ *existe un límite proyectivo contenido en el producto de los conjuntos* E_n *donde las funciones asociadas son las restricciones de las proyecciones. Además, este límite es único salvo biyección.*

Demostración. Empecemos por probar la **existencia**.
Para ello, definimos el conjunto siguiente,

$$E = \left\{ (x_n) \in \prod_{n \geq 0} E_n / \ \phi_n(x_{n+1}) = x_n \ \forall n \in \mathbb{N} \right\} \subset \prod_{n \geq 0} E_n$$

formado por las sucesiones «coherentes» respecto a ϕ_n. Llamamos π_n a las proyecciones de $\prod_{n \geq 0} E_n$ en E_n. Entonces, por la definición del conjunto E tenemos que si $x = (x_n) \in E$, entonces

$$\phi_n(\pi_{n+1}(x)) = \phi_n(x_{n+1}) = x_n = \pi_n(x)$$

y las restricciones a E de las proyecciones satisfacen la condición de compatibilidad. Veamos si se cumple la propiedad universal.
Sea X un conjunto junto con aplicaciones $f_n : X \to E_n$ que cumplen que

$f_n = \phi_n \circ f_{n+1}$. Veamos que hay una única factorización de ellas a través de E. Podemos definir la función siguiente:

$$\begin{aligned} f : X &\longrightarrow \prod_{n\geq 0} E_n \\ y &\longmapsto (f_n(y)) \end{aligned}$$

El hecho de que las aplicaciones f_n cumplan la condición de compatibilidad nos indica que la imagen de esta función está contenida en E. Entonces sin más que restringir el conjunto de llegada de f tenemos una función $f : X \to E$ que cumple que $f_n = (\pi_n \restriction_E) \circ f$. Esta descomposición nos da la unicidad de la factorización, pues $f_n = (\pi_n \restriction_E) \circ f = (\pi_n \restriction_E) \circ f'$ implica que $f = f'$. Por lo tanto, el conjunto E junto con las funciones $\pi_n \restriction_E$ forman un límite proyectivo de $\{(E_n, \phi_n)\}_{n=0}^{\infty}$.

Sólo nos queda ver la **unicidad**.
Sean E junto con las funciones $\xi_n : E \to E_n$ y E' junto con $\xi'_n : E' \to E_n$ dos límites proyectivos de un mismo sistema proyetivo. Entonces ambos tienen la propiedad universal, y por tanto existen $f : E \to E'$ y $f' : E' \to E$ únicas tales que $\xi_n = \xi'_n \circ f$ y $\xi'_n = \xi_n \circ f'$. Combinando estas dos igualdades obtenemos que

$$\xi_n = \xi'_n \circ f = (\xi_n \circ f') \circ f = \xi_n \circ (f' \circ f) : E \to E_n$$

y por tanto la función $f' \circ f$ es una factorización de la función identidad en E. Pero como hemos dicho que en un límite proyectivo la factorización es única, $f' \circ f = \mathrm{Id}_E$. Con un razonamiento absolutamente simétrico vemos que $f \circ f' = \mathrm{Id}'_E$, y tenemos una biyección entre E y E'. Así pues, el límite es único salvo biyección y hemos acabado.

Q.E.D.

Nota. *La construcción que acabamos de hacer, según la cual* $\lim_{\leftarrow} E_n = \left\{(x_n) \in \prod_{n\geq 0} E_n / \ \phi_n(x_{n+1}) = x_n \ \forall n \in \mathbb{N}\right\}$ *será la que utilizaremos habitualmente.*

Corolario 5.1.4. *Si las funciones de transición de un sistema inverso* $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ *son sobreyectivas y los conjuntos son todos no vacíos entonces las funciones* $\xi_n : E \to E_n$ *también son sobreyectivas, y en particular el límite proyectivo no es vacío.*

Demostración. Sean $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ un sistema proyectivo en el que ϕ_n es sobreyectiva para todo $n \in \mathbb{N}$ y sea $E = \lim_{\leftarrow} E_n$ su límite proyectivo. Para demostrar que las funciones ξ_n son sobreyectivas nos basta con ver que, fijado $n \in \mathbb{N}$, para todo elemento $x_n \in E_n$ existe una sucesión $(x_n)_{k=0}^{\infty}$ coherente respecto a ϕ_n (por el teorema anterior, en E).
Entonces los valores de la sucesión para $i \leq n$ existen siempre: se calculan por recurrencia de forma que $x_{i-1} = \phi_{i-1}(x_i)$. En cambio, para buscar los valores tales que $i > n$ tenemos que elegir un elemento perteneciente a $\phi_i^{-1}(x_i)$. Si las

funciones de transición del sistema no fueran sobreyectivas, este conjunto podría ser vacío. Pero como hemos supuesto que lo son, y $E_n \neq \emptyset$, $\phi_i^{-1}(x_i) \neq \emptyset$ y existe la sucesión coherente que buscamos.

Dado un $x_n \in E_n$, que siempre existe porque hemos supuesto que los conjuntos E_n son todos no vacíos, tenemos una forma de encontrar un elemento de E, que es por tanto no vacío. Hemos terminado.

Q.E.D.

5.2. Límites proyectivos de espacios topológicos.

En la sección anterior hemos definido los límites proyectivos de conjuntos, pero una de las cuestiones más interesantes de estos límites es que se adaptan con facilidad a estructuras más complejas. Para las necesidades de este trabajo nos centraremos en el caso de los espacios topológicos y los grupos abelianos. En toda esta sección suponemos que los espacios tratados son de Hausdorff.

Definición 5.2.1. *Sea $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ un sistema proyectivo formado por espacios topológicos y aplicaciones continuas entre ellos. Llamamos límite proyectivo (en espacios topológicos) del sistema anterior a un espacio topológico E junto con una sucesión de aplicaciones continuas $\xi_n : E \to E_n$ que satisfacen la condición de compatibilidad y la propiedad universal en espacios topológicos.*

Proposición 5.2.2. *Para todo sistema proyectivo de espacios topológicos $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ existe un límite proyectivo en (la categoría de los) espacios topológicos y es único salvo homeomorfismo.*

Demostración. Tomamos la construcción de límite proyectivo que hemos visto en el teorema anterior. Por tanto, si $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ es un sistema proyectivo formado por espacios topológicos y funciones continuas, tenemos que su límite proyectivo es el subconjunto $E = \{(x_n) \,/\, \phi_n(x_{n+1}) = x_n \ \forall n \in \mathbb{N}\}$ del producto de los espacios topológicos E_n, y las funciones asociadas a él son las restricciones a E de las proyecciones. Dotamos a E de la topología de subespacio del espacio producto. Entonces las proyecciones son funciones continuas, y la restricción de una función continua sigue siéndolo.
Sea E junto con las aplicaciones ξ_n el límite proyectivo y X junto con las aplicaciones f_n otra sucesión con funciones continuas y la condición de compatibilidad. Entonces tenemos una función f tal que, para todo $n \in \mathbb{N}$, $f_n = \xi_n \circ f$. Sabemos que una función $g : A \to \prod X_n$ es continua si y sólo si lo son todas sus proyecciones. Pero las proyecciones de f son $f_n = \pi_n \circ f$, que son continuas. Luego f es continua. Tenemos por tanto que E es un límite proyectivo de espacios topológicos.

En la demostración de unicidad que hemos hecho para conjuntos, tomábamos dos límites inversos junto con las funciones dadas por la propiedad universal, y veíamos que eran inversas la una de la otra. Como dichas aplicaciones en límites

proyectivos de espacios topológicos son continuas, tenemos un homeomorfismo. El límite es único salvo homeomorfismo y hemos acabado.

Q.E.D.

Proposición 5.2.3. *El límite proyectivo de espacios topológicos* $E = \lim_{\leftarrow} E_n$ *es un cerrado en* $\prod E_n$.

Demostración. Sea $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ un sistema proyectivo topológico y $E = \lim_{\leftarrow} E_n$ su límite proyectivo. Entonces sabemos que $E = \{(x_n) \in \prod E_n / \phi_n(x_{n+1}) = x_n \forall n \in \mathbb{N}\}$, o, equivalentemente, que $E = \bigcap_{n\in\mathbb{N}} \{x \in \prod E_n /\ \pi_n(x) = \phi_n \circ \pi_{n+1}(x)\}$. Ahora bien, hemos supuesto al principio del apartado que todos los espacios que trataríamos serían de Hausdorff. Si los E_n son todos de Hausdorff, al ser todas las funciones implicadas continuas, tenemos que $\{x \in \prod E_n /\ \pi_n(x) = \phi_n \circ \pi_{n+1}(x)\}$ es cerrado para todo $n \in \mathbb{N}$, y por tanto E es cerrado en $\prod E_n$.

Q.E.D.

Proposición 5.2.4. *El límite proyectivo de espacios topológicos compactos no vacíos* $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ *es compacto y no vacío.* [Wil68, pág. 212]

Demostración. Hemos visto en la proposición anterior que E es un cerrado de $\prod_{n\in\mathbb{N}} E_n$ que, por el teorema de Tychonoff, es compacto. Luego E es compacto. Para concluir que E es no vacío basta con observar que

$$E = \bigcap_{n\in\mathbb{N}} \left\{ x \in \prod_{n\in\mathbb{N}} E_n /\ \pi_n(x) = \phi_n \circ \pi_{n+1}(x) \right\} = \bigcap_{n\in\mathbb{N}} Y_n,$$

donde $Y_n = \bigcap_{i\leq n} \{x \in \prod E_i /\ \pi_i(x) = \phi_i \circ \pi_{i+1}(x)\}$, y ver que los Y_n constituyen una sucesión de cerrados encajados.

Q.E.D.

Corolario 5.2.5. *En particular, todo límite proyectivo de espacios finitos no vacíos es compacto y no vacío.*

En el caso de la topología producto tenemos que el conjunto formado por $\pi_\alpha^{-1}(U_\alpha)$, con π_α la proyección en X_α y U_α un abierto de X_α, es una subbase de abiertos de la topología. Vamos a ver que en el de los límites proyectivos el resultado es todavía mejor: este conjunto forma una base de abiertos.

Proposición 5.2.6. *Sea* E *junto con las aplicaciones* $\xi_n : E \to E_n$ *el límite proyectivo de un sistema inverso* $\{(E_n, \phi_n)\}_{n=0}^{\infty}$. *Entonces los conjuntos* $\xi_n^{-1}(U_n)$, *con* U_n *abiertos de* E_n, *forman una base de abiertos de* E.

Demostración. Como E es homeomorfo a un subespacio del espacio producto, sabemos que una base de E está formada por abiertos de la forma $E \cap \left(\prod_{n\in\mathbb{N}} U_n\right)$, donde todos salvo un número finito de los U_n son el espacio total, y el resto son abiertos de sus espacios respectivos. Podemos escribir estos de la forma $U = \left(\prod_{i\leq n} U_i \times \prod_{j>n} E_j\right) \cap E$, donde quizás alguno de los U_i sea E_i. Ahora bien, si $x = (x_n) \in E$ y $x_1 \in U_1$, $x_0 \in U_0$, entonces $\xi_1(x) \in U_1 \cap \phi_0^{-1}(U_0)$.

Puesto que ϕ_0 es una función continua, $\phi_0^{-1}(U_0)$ es un abierto, y tenemos un abierto $V_1 = U_1 \cap \phi_0^{-1}(U_0)$ tal que $x \in \xi_1^{-1}(V_1)$. En un número finito de pasos hemos llegado a un abierto $V_n \subset E_n$ tal que $U = \left(\prod_{i\leq n} U_i \times \prod_{j>n} E_j\right) \cap E = \xi_n^{-1}(V_n)$, y el conjunto de las imágenes inversas $\xi_n^{-1}(V_n)$ forman una base del límite inverso.

Q.E.D.

Corolario 5.2.7. *El límite proyectivo de* $\left\{\left(\prod_{i\leq n} E_i, \phi_n\right)\right\}_{n=0}^{\infty}$, *donde* ϕ_n *es la función que envía* $(x_0, ..., x_{n+1})$ *en* $(x_0, ..., x_n)$, *es homeomorfo al producto* $\prod_{n\in\mathbb{N}} E_n$.

Demostración. La proyecciones $\pi_n : \prod_{i\in\mathbb{N}} E_i \to \prod_{i\leq n} E_i$ que envían (x_i) en $(x_0, ..., x_n)$ son funciones continuas que cumplen que $\pi_n = \phi_n \circ \pi_{n+1}$, por lo que la propiedad universal del límite proyectivo nos dice que existe una función $f : \prod_{n\in\mathbb{N}} E_n \to \lim_{\leftarrow} E_n$ continua. Esta función además es biyectiva y abierta, por la definición de los abiertos en ambos espacios. Luego f es un homeomorfismo entre ellos.

Q.E.D.

Notación. *Llamamos «abierto-cerrados» a aquellos subconjuntos de un espacio topológico que son simultáneamente abiertos y cerrados.*

Definición 5.2.8. *Se dice que un espacio topológico* X *es* 0*-dimensional si todo punto* $x \in X$ *tiene un sistema fundamental de entornos formado por abierto-cerrados.* [Wil68, pág. 210]

Definición 5.2.9. *Sea* $\mathcal{U}_1, \mathcal{U}_2, ..., \mathcal{U}_n, ...$ *una sucesión de particiones de un espacio topológico* X *tales que cada una refina la anterior, es decir, que si* $n \in \mathbb{N}$, *para todo* $U_i \in \mathcal{U}_{n+1}$ *existe un* $V_j \in \mathcal{U}_n$ *tal que* $U_i \subset V_j$. *Entonces llamamos sistema derivado al sistema proyectivo* $\{(\mathcal{U}_n, \phi_n)\}_{n=0}^{\infty}$ *en el que* $\mathcal{U}_n$ *tiene la topología discreta y las aplicaciones* ϕ_n *son aquellas que envían cada elemento de* $\mathcal{U}_{n+1}$ *en el único elemento de* $\mathcal{U}_n$ *que lo contiene.* [Wil68, pág. 213]

$$\mathcal{U}_0 \xleftarrow{\phi_0} \dots \xleftarrow{\phi_{n-1}} \mathcal{U}_n \xleftarrow{\phi_n} \dots \lim_{\leftarrow} \mathcal{U}_n$$

Teorema 5.2.10. *Sea* X *un espacio métrico compacto y* 0*-dimensional. Entonces tenemos que:* [Wil68, pág. 213-214]

1. Para todo $n \in \mathbb{N}$, existe un recubrimiento finito $\mathcal{U}_n$ de X formado por abierto-cerrados disjuntos de diámetro estrictamente menor que $1/2^n$ y cada $\mathcal{U}_n$ refina al recubrimiento anterior.

2. Si X_∞ es el límite proyectivo del sistema derivado definido en el apartado 1, entonces X es homeomorfo a X_∞.

Demostración. 1. Tenemos que X es 0-dimensional, luego todo punto tiene un sistema fundamental de entornos abierto-cerrados. Como X es un espacio métrico, para todo $x \in X$ consideramos la bola abierta $B(x, 1/2^2)$, de diámetro

< 1. Existe un U_x entorno abierto-cerrado de x tal que $x \in U_x \subset B(x, 1/2^2)$, que tiene diámetro estrictamente menor que 1. Esto nos da un recubrimiento de X por abierto-cerrados de diámetro < 1, y como X es compacto existe un subrecubrimiento finito, $\mathcal{U}_0 = \{U_0, ..., U_k\}$. Definimos entonces los conjuntos disjuntos

$$U_0' = U_0, \quad U_1' = U_1 \setminus U_0, \dots U_j' = U_j \setminus \left(\bigcup_{i<j} U_i \right) \ \forall 0 \leq j \leq k,$$

que son abierto-cerrados por ser todos los U_j abierto-cerrados. Entonces $\mathcal{U}_0' = \{U_0', ..., U_k'\}$ es la partición que buscamos.
Suponemos que existe un recubrimiento finito $\mathcal{U}_n$ de X por abierto-cerrados disjuntos de diámetro $< 1/2^n$. Sea $U_k \in \mathcal{U}_n$ uno de los abierto-cerrados de este. Como U_k es cerrado en X, que es compacto, U_k es un subespacio compacto. Seguimos el método anterior para encontrar abierto-cerrados que formen un recubrimiento de U_k. El espacio X es métrico, luego para todo $x \in U_k$ existe una bola abierta $B(x, 1/2^{n+2})$ y, por ser 0-dimensional, existe un entorno abierto-cerrado de x, V_x, contenido en $B(x, 1/2^{n+2})$. Estos entornos nos dan un recubrimiento por abiertos de U_k. Por ser U_k compacto, existe un subrecubrimiento finito, que llamaremos $\mathcal{V}_{n+1} = \{V_0, ..., V_m\}$, formado por abierto-cerrados de diámetro estrictamente menor que $1/2^{n+1}$. Como puede que no sean disjuntos, definimos

$$V_j' = V_j \setminus \bigcup_{i<j} V_i \ \forall \ 0 \leq i \leq m,$$

que son abierto-cerrados disjuntos de diámetro $< 1/2^{n+1}$. Haciendo este proceso con todos los abiertos de $\mathcal{U}_n$ obtenemos una partición de X por abierto-cerrados de diámetro $< 1/2^{n+1}$ que refina $\mathcal{U}_n$ y hemos acabado.

2. Tomamos el sistema derivado que forman los $\mathcal{U}_n$ del apartado anterior. Como los $\mathcal{U}_n$ tienen todos la topología discreta, son de Hausdorff y X_∞ es un espacio de Hausdorff. Para todo $n \in \mathbb{N}$, definimos las aplicaciones $\psi_n : X \to \mathcal{U}_n$ de forma que $\psi_n(x)$ es el abierto perteneciente a $\mathcal{U}_n$ que contiene a x. Como se trata de un recubrimiento, esta imagen existe siempre, y como los conjuntos son disjuntos, es única; la aplicación está bien definida para todo $n \in \mathbb{N}$ y es suprayectiva. Además, por la definición de los $\mathcal{U}_n$, estas aplicaciones son continuas. Tenemos que $\psi_n = \phi_n \circ \psi_{n+1}$. En efecto,

$$\phi_n \circ \psi_{n+1}(x) = \phi_n(\text{elemento de } \mathcal{U}_{n+1} \text{ que contiene a } x) =$$

$$\text{elemento de } \mathcal{U}_n \text{ que contiene al elemento de } \mathcal{U}_{n+1} \text{ que contiene a } x =$$

$$\text{elemento de } \mathcal{U}_n \text{ que contiene a } x = \psi_n(x)$$

El espacio topológico X con las aplicaciones ψ_n tiene la condición de compatibilidad. Luego, por la propiedad universal de X_∞, existe una aplicación $\psi : X \to X_\infty$ continua que cumple que $\psi_n = \phi_n \circ \psi$. Como las aplicaciones

ϕ_n son sobreyectivas, por 5.1.4 ψ_n también es sobreyectiva para todo $n \in \mathbb{N}$, y por lo tanto ψ es suprayectiva. Como sabemos que X es compacto y X_∞ es de Hausdorff, si ψ es inyectiva será un homeomorfismo.
Supongamos que no lo es. Entonces existen $x, y \in X$ tales que $y \neq x$ y $\psi(x) = \psi(y)$. Entonces, como tenemos que $\psi_n = \phi_n \circ \psi$, eso significa que $\psi_n(x) = \phi_n \circ \psi(x) = \phi_n \circ \psi(y) = \psi_n(y)$ para todo $n \in \mathbb{N}$. Ahora bien, estando en un espacio métrico tenemos que si $x \neq y$, entonces $\| x - y \| = \epsilon > 0$. Existe $n \in \mathbb{N}$ tal que $1/2^n < \epsilon$. Pero eso significa que $\psi_n(x) \neq \psi_n(y)$, porque los elementos de $\mathcal{U}_n$ son de diámetro $1/2^n < \epsilon$, y por tanto x e y no pueden pertenecer al mismo abierto de $\mathcal{U}_n$. En consecuencia, ψ es una función continua y biyectiva de un compacto en un Hausdorff, luego un homeomorfismo. Los espacios X y X_∞ son homeomorfos.

Q.E.D.

Nota. *Es quizás interesante recordar aquí que el producto infinito de espacios con la topología discreta no tiene la topología discreta. Por lo tanto, aunque tomemos los $\mathcal{U}_n$ con dicha topología, el límite proyectivo tendrá otra topología más complicada.*

5.3. Límites proyectivos de grupos abelianos.

Definición 5.3.1. *Sea $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ un sistema proyectivo en el que todos los conjuntos E_n son grupos abelianos y todas las funciones de transición son homomorfismos de grupos. Llamamos límite proyectivo de grupos abelianos a un grupo abeliano E junto con una sucesión de homomorfismos de grupos $\xi_n : E \to E_n$ que satisfacen la condición de compatibilidad y la propiedad universal para grupos abelianos.*

Proposición 5.3.2. *Para todo sistema proyectivo de grupos abelianos $\{(E_n, \phi_n)\}_{n=0}^{\infty}$ existe un límite proyectivo en (la categoría de) grupos y es único salvo isomorfismos. Además, si todos los grupos son no vacíos el límite es no vacío.*

Demostración. De nuevo, utilizaremos la construcción de límite proyectivo de conjuntos como subconjunto E del producto $\prod_{n\in\mathbb{N}} E_n$. Se prueba sin dificultad que E es subgrupo del grupo producto con la operación definida componente a componente, es decir, $(x_0, x_1, ..., x_n, ...) + (y_0, y_1, ..., y_n, ...) = (x_0 + y_0, ..., x_n + y_n, ...)$, y las restricciones a E de las proyecciones son homomorfismos de grupos. Al igual que en el caso de los límites de espacios topológicos, la unicidad se prueba a partir de la propiedad universal: como en este caso está dada por homomorfismos, tenemos una isomorfía. En cuanto a ser no vacío, si e_n es el elemento neutro para la operación del grupo E_n, en cualquier homomorfismo tenemos que $\phi_n(e_{n+1}) = e_n$. Por tanto, el elemento $(e_0, e_1, ..., e_n, ...) \in E$ sean cuales sean los grupos del sistema proyectivo.

Q.E.D.

Proposición 5.3.3. *Sea $\{(G_n, \phi_n)\}_{n=0}^{\infty}$ un sistema proyectivo de grupos abelianos y $G = \lim_{\leftarrow} G_n$ junto con las aplicaciones ξ_n su límite proyectivo. Entonces*

la intersección de los núcleos de los ξ_n se reduce al elemento neutro y G es isomorfo al límite inverso $\lim_{\leftarrow}(G/\ker\xi_n)$.

Demostración. Llamemos G' al subgrupo de G de la forma $\bigcap \ker\xi_n$, y tomemos la inclusión $f : G' \to G$ que envía cada elemento de $G' \subset G$ en sí mismo. Entonces tenemos de forma evidente las funciones $f_n = \xi_n \restriction_{G'} = \xi_n \circ f$, que se pueden factorizar como $f_n = \xi_n \circ f = \phi_n \circ \xi_{n+1} \circ f = \phi_n \circ f_{n+1}$ y nos dan un grupo y una sucesión de funciones con la condición de compatibilidad. Entonces por la propiedad universal de los límites proyectivos existe un único homomorfismo h tal que $f_n = \xi_n \circ h \ \forall n \in \mathbb{N}$, que en nuestro caso será f. Pero las funciones f_n tienen la factorización trivial $g(x) = e \ \forall x \in G'$, luego por unicidad $f = g$. Como f es la inclusión de G' en G, eso significa que $G' = \bigcap \ker\xi_n = \{e\}$.

Veamos ahora que G es isomorfo a $\lim_{\leftarrow}(G/\ker\xi_n)$. Los conjuntos $\ker\xi_n$ forman una sucesión decreciente de grupos. En efecto, si $x \in \ker\xi_{n+1}$, entonces, como sabemos que $\xi_n = \phi_n \circ \xi_{n+1}$, tenemos que $\xi_n(x) = \phi_n \circ \xi_{n+1}(x) = \phi_n(e_{n+1}) = e_n$, por ser ϕ_n un homomorfismo. Esto nos da la sucesión decreciente $\ker\xi_0 \supset \ker\xi_1 \supset ... \supset \ker\xi_n \supset ....$ La sucesión $G/\ker\xi_n$ junto con las funciones $\psi_n : G/\ker\xi_{n+1} \to G/\ker\xi_n$ tales que $\psi_n([x]_{\ker\xi_{n+1}}) = [x]_{\ker\xi_n}$ forman un sistema inverso, y tienen un límite proyectivo $\lim_{\leftarrow}(G/\ker\xi_n)$.
Como las aplicaciones cociente $h_n : G \to G/\ker\xi_n$ siempre cumplen la condición de compatibilidad, obtenemos un homomorfismo $h : G \to \lim_{\leftarrow}(G/\ker\xi_n)$, y por el primer teorema de isomorfía tenemos que $G/\ker h \simeq \lim_{\leftarrow}(G/\ker\xi_n)$. Ahora bien, gracias al resultado que acabamos de demostrar no es difícil ver que

$$\ker h = h^{-1}\left(\bigcap \ker\xi_n\right) = \bigcap \ker h_n = \bigcap \ker\xi_n = \{e\}\,.$$

Luego G es isomorfo a $\lim_{\leftarrow}(G/\ker\xi_n)$ y hemos acabado.

Q.E.D.

Podríamos seguir así hablando de anillos, de módulos... o mezclando estructuras, como grupos topológicos. En realidad, para los objetivos del presente trabajo necesitaríamos definir el límite proyectivo en anillos, pero el método es muy semejante. Por lo tanto, vamos a abandonar aquí las disquisiciones generales y a volver a centrarnos en los números p-ádicos.

5.4. $\mathbb{Z}_p$ como límite proyectivo.

Retomaremos, pues, los comentarios hechos al principio del capítulo, adaptándolos a la luz de nuestros nuevos conocimientos. Consideramos la sucesión de ideales $\{p^n\mathbb{Z}\}_{n=0}^{\infty}$ de $\mathbb{Z}$. Puesto que $p^{n+1}\mathbb{Z} \subset p^n\mathbb{Z}$, la identidad $i : \mathbb{Z} \to \mathbb{Z}$ induce, por paso al cociente, el siguiente homomorfismo de anillos:

$$\begin{aligned} \phi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ [x]_{n+1} &\longmapsto [x]_n \end{aligned}$$

Tenemos por tanto un sistema inverso formado por los anillos $\mathbb{Z}/p^n\mathbb{Z}$ y los homomorfismos ϕ_n. Si ahora dotamos de la topología discreta a estos conjuntos, tenemos un sistema inverso de anillos topológicos. Entonces existe un límite proyectivo $\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$, que es un anillo topológico.

Teorema 5.4.1. *Los anillos topológicos $\mathbb{Z}_p$ y $L = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$ son isomorfos. En concreto, el isomorfismo de anillos topológicos es el siguiente:*

$$\Phi : \mathbb{Z}_p \longrightarrow \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$$
$$\sum_{i=0}^{\infty} a_i p^i \longmapsto \left(\sum_{i=0}^{n-1} a_i p^i \right)_{n=1}^{\infty}$$

Demostración. Con nuestra definición de ϕ_n, los elementos n-ésimo y m-ésimo de la sucesión coherente respecto a ellas serían $x_n = \sum_{i=0}^{n-1} a_i p^i$, $x_m = \sum_{i=0}^{m-1} b_i p^i$ tales que si $n \leq m$ entonces $a_i = b_i \ \forall i \leq n$. Esto significa que podrían verse como el representante que calculamos en el teorema 3.2.3. Esta función es evidentemente un homomorfismo de anillos con las definiciones que hicimos de las operaciones en $\mathbb{Z}_p$ (que, recordemos, estaban basadas en las operaciones en series formales) y podemos definir facilmente su inversa de forma que si $\Phi^{-1}((x_n)) = \sum_{i=0}^{\infty} a_i p^i$, entonces

$$a_0 = x_1, \quad a_n = \frac{x_{n+1} - x_n}{p^n},$$

que es también un homomorfismo.

Tenemos por tanto un isomorfismo de anillos entre $\mathbb{Z}_p$ y el límite proyectivo $\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$. Veamos ahora que esta función es un homeomorfismo. Podemos definir funciones $f_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ de la forma $f_n(\sum_{i=0}^{\infty} a_i p^i) = \sum_{i=0}^{n-1} a_i p^i$, que cumplen que $f_n = \phi_n \circ f_{n+1}$, y es evidente que se pueden factorizar como $f_n = (\pi_n \restriction_L) \circ \Phi$. Por la unicidad que nos proporciona la propiedad universal de los límites proyectivos, Φ es la factorización, que hemos demostrado en 5.2.2 que es una función continua. Estamos ante una función continua de un compacto en un espacio de Hausdorff, porque $\mathbb{Z}_p$ es compacto y los $\mathbb{Z}/p^n\mathbb{Z}$ son todos discretos, luego de Hausdorff, lo que implica que su límite proyectivo también lo es. Luego Φ es un homeomorfismo y tenemos un isomorfismo de anillos topológicos. Q.E.D.

Nota. *Una de las consecuencias de la representación de $\mathbb{Z}_p$ como el límite proyectivo de $\mathbb{Z}/p^n\mathbb{Z}$ es que pone de manifiesto que podemos escoger cualquier conjunto de representantes de $\mathbb{Z}/p\mathbb{Z}$ como coeficientes del desarrollo canónico de un elemento de $\mathbb{Z}_p$. Es decir, si S es un conjunto de representantes de $\mathbb{Z}/p\mathbb{Z}$, el número $\sum_{i=0}^{\infty} a_i p^i$ con $a_i \in S$ es un entero p-ádico, aunque $S \neq \{0, ..., p-1\}$. En la práctica siempre se eligen conjuntos que contengan al 0, para permitir la existencia de desarrollos finitos. Aún así, como nos hace notar el libro de Alain M. Robert, en los casos en que p es impar puede ser interesante utilizar $\left\{-\frac{p-1}{2}, ..., 0, ..., \frac{p-1}{2}\right\}$.*

Capítulo 6

Topología de $\mathbb{Q}_p$.

Tras la pequeña digresión que ha supuesoto el capítulo anterior volveremos a nuestra fuente principal, «p-adic Analysis Compared with Real», de Svetlana Katok [Kat07, págs. 53-74]. En el apartado de «Representaciones de $\mathbb{Z}_p$ en $\mathbb{R}^n$» nos inspiraremos en la manera de expresarse de «A Course in p-adic Analysis», de Alain M. Robert. La demostración de que todos los espacios métricos compactos, perfectos y 0-dimensionales son homeomorfos entre sí está adaptada de un resultado de «General Topology», de Stephen Willard.

6.1. Propiedades topológicas de $\mathbb{Q}_p$.

Una vez que tenemos la norma $|\ .\ |_p$, definir la topología es simple: es aquella que tiene como base de abiertos las bolas abiertas $B(a,r) = \{x \in \mathbb{Q}_p / \ \mid x-a \mid_p < r\}$, con $a \in \mathbb{Q}_p$ y $r > 0$. Recordamos que la norma p-ádica no toma todos los valores no negativos de $\mathbb{R}$, sino solamente aquellos que pertenecen al conjunto $\left\{p^k / \ k \in \mathbb{Z}\right\} \cup \{0\}$, así que podríamos definir la base únicamente con los conjuntos $B(a,p^k)$.

Notación. *Denotamos por $\bar{B}(a,r)$ la bola cerrada de centro $a \in \mathbb{Q}_p$ y radio $r > 0$, es decir, $\bar{B}(a,r) = \{x \in \mathbb{Q}_p / \ \mid x-a \mid_p \leq r\}$.*

Nota. *Es inmediato ver que el conjunto de los enteros p-ádicos se corresponde con la bola cerrada de centro 0 y radio 1 y que las unidades p-ádicas forman la esfera unidad, es decir, $\mathbb{Z}_p = \bar{B}(0,1)$ y $\mathbb{Z}_p^* = S(0,1)$.*

Proposición 6.1.1. *Las bolas abiertas de $\mathbb{Q}_p$ son también bolas cerradas, y recíprocamente. En particular, $\mathbb{Q}_p$ es 0-dimensional.*

Demostración. Recordemos que se dice que un espacio X es 0-dimensional cuando cada punto $x \in X$ tiene un sistema fundamental de entornos formado por abierto-cerrados. Sea $\bar{B}(a,r)$ la bola cerrada de centro $a \in \mathbb{Q}_p$ y radio $r > 0$. Entonces existe un cierto $k \in \mathbb{Z}$ entero tal que $p^k \leq r < p^{k+1}$, y tenemos las

siguientes igualdades:

$$\bar{B}(a,r) = \{x \in \mathbb{Q}_p / \ \mid x-a \mid_p \leq r\} = \left\{x \in \mathbb{Q}_p / \ \mid x-a \mid_p < p^{k+1}\right\} = B(a,p^{k+1}).$$

Hemos acabado.

Q.E.D.

Nota. *Es interesante resaltar que una consecuencia de este resultado es que siempre que el radio sea positivo todo lo que digamos a partir de aquí sobre las bolas abiertas servirá también para las cerradas, y viceversa.*

Corolario 6.1.2. *La frontera de una bola abierta es vacía.*

Demostración. Recordamos que la frontera de un conjunto U en un espacio topológico X se define como $Fr(U) = \overline{U} \cap \left(\overline{X \setminus U}\right)$. Ahora bien, como $B(a,r)$ es un abierto, $\mathbb{Q}_p \setminus B(a,r)$ es un cerrado, y por tanto coincide con su adherencia. Por otra parte, como hemos visto que $B(a,r)$ es un cerrado, coincide también con su adherencia. En consecuencia, $Fr\left(B(a,r)\right) = \overline{B(a,r)} \cap \left(\overline{\mathbb{Q}_p \setminus B(a,r)}\right) = B(a,r) \cap (\mathbb{Q}_p \setminus B(a,r)) = \emptyset$. Así, la frontera es vacía y hemos acabado.

Q.E.D.

Proposición 6.1.3. *Todo punto de una bola abierta en $\mathbb{Q}_p$ es su centro. Es decir, si $b \in B(a,r)$ con $a \in \mathbb{Q}_p$ y $r > 0$, entonces $B(a,r) = B(b,r)$.*

Demostración. Sea $a \in \mathbb{Q}_p$, $r > 0$ y $b \in B(a,r)$. Sea $x \in B(a,r)$. Entonces tenemos que $\mid a-b \mid_p < r$ y que $\mid a-x \mid_p < r$. Por la desigualdad triangular fuerte,

$$\mid b-x \mid_p = \mid b-a+a-x \mid_p \leq \text{máx}(\mid b-a \mid_p + \mid a-x \mid_p) < \text{máx}(r,r) = r,$$

y obtenemos que $B(a,r) \subset B(b,r)$. Tenemos la otra inclusión por simetría.

Q.E.D.

Proposición 6.1.4. *Dos bolas abiertas en $\mathbb{Q}_p$ tienen una intersección no vacía si y sólo si una está incluida en la otra.*

Demostración. Sean $a, b \in \mathbb{Q}_p$ y $r, s > 0$. Consideramos entonces las bolas abiertas $B(a,r)$ y $B(b,s)$. Si una está incluida en la otra, la intersección es trivialmente no vacía.
Veamos la implicación contraria. Para ello, supongamos que $s \leq r$ y que $y \in B(a,r) \cap B(b,s)$. Entonces por la proposición anterior tenemos que $B(a,r) = B(y,r)$ y que $B(b,s) = B(y,s)$. Pero $B(y,s) \subset B(y,r)$, porque $s \leq r$. En el caso en que $s > r$ el razonamiento sería idéntico.

Q.E.D.

Proposición 6.1.5. *La esfera $S(a,r)$ con $a \in \mathbb{Q}_p$ y $r > 0$ es un conjunto abierto.*

Demostración. Sea $x \in S(a,r)$ y $\epsilon < r$. Para ver que $S(a,r)$ es abierto vamos a ver que $B(x,\epsilon) \subset S(a,r)$. Sea $y \in B(x,\epsilon)$. En consecuencia,
$\mid x-y \mid_p = \mid (x-a)-(y-a) \mid_p < \epsilon < r = \mid x-a \mid_p$, y por la regla de «el mayor se impone», $\mid y-a \mid_p = \mid x-a \mid_p = r$, lo que significa que $B(x,\epsilon) \subset S(a,r) = \{x/ \mid x-a \mid_p = r\}$. Así pues, la esfera es un conjunto abierto.

Q.E.D.

Como $\mathbb{Q}$, que es numerable, es denso en $\mathbb{Q}_p$ (por ser este último su complección), sabemos que el espacio de los números p-ádicos es separable, y, por ser un espacio métrico, cumple el segundo axioma de numerabilidad. Pero en este caso tenemos un resultado más potente aún: no es que podamos encontrar una base de $\mathbb{Q}_p$ que sea numerable, es que el conjunto de todas las bolas abiertas de $\mathbb{Q}_p$ lo es.

Proposición 6.1.6. *El conjunto de todas las bolas abiertas $B(a,r)$ con $a \in \mathbb{Q}_p$ y $r > 0$ es numerable.*

Demostración. Nos basta con considerar los radios que son potencias de p. Así, sean $a \in \mathbb{Q}_p$ y $k \in \mathbb{Z}$ y escribamos el desarrollo canónico de a, centro de la bola $B(a,p^{-k})$, $a = \sum_{i=-m}^{\infty} a_i p^i$. Tomamos el número racional $a_0 = \sum_{i=-m}^{k} a_i p^i$. Entonces,

$$\mid a - a_0 \mid_p = \mid \sum_{i=k+1}^{\infty} a_i p^i \mid_p < p^{-k},$$

lo que significa que $a_0 \in B(a,p^{-k})$. Hemos visto que esto implica que $B(a_0,p^{-k}) = B(a,p^{-k})$. Así, existe una aplicación sobreyectiva, definida por

$$\begin{aligned} \mathbb{Q} \times \mathbb{Z} &\longrightarrow \{B(a,r)/\ a \in \mathbb{Q}_p,\ r > 0\} \\ (a_0,k) &\longmapsto B(a_0,p^k) \end{aligned}$$

Puesto que $\mathbb{Q} \times \mathbb{Z}$ es un conjunto numerable, concluimos que el conjunto de las bolas abiertas $B(a,r)$ es numerable y hemos acabado.

Q.E.D.

A lo largo de este trabajo hemos demostrado algunos resultados topológicos (o métricos) sobre $\mathbb{Q}_p$ y $\mathbb{Z}_p$ cuando los hemos necesitado. Aunque no los demostraremos de nuevo, los volvemos a enunciar aquí en aras de un mejor orden.

Proposición 6.1.7. *El espacio $\mathbb{Z}_p$ es compacto, y $\mathbb{Q}_p$ es localmente compacto, pues sus bolas son conjuntos compactos.*

Proposición 6.1.8. *El espacio métrico $\mathbb{Z}_p$ es completo.*

En el capítulo 3, en el apartado «Consecuencias del Lema de Hensel», hemos hablado algo del subconjunto de $\mathbb{Q}_p^*$ formado por sus cuadrados, $\left(\mathbb{Q}_p^*\right)^2$. Aquí tenemos otro resultado en relación a dicho subconjunto.

Proposición 6.1.9. *El subgrupo $\left(\mathbb{Q}_p^*\right)^2$ de $\mathbb{Q}_p^*$ es un abierto en $\mathbb{Q}_p^*$.*

Demostración. Recordamos lo que habíamos dicho en ese apartado: un elemento $x \neq 0$ es un cuadrado de $\mathbb{Q}_p$ si y sólo si existen $k \in \mathbb{Z}$ y $u \in \mathbb{Z}_p^*$ tales que $x = p^{2k}u^2$. Veamos entonces que como $x \in \left(\mathbb{Q}_p^*\right)^2$ es de la forma $x = p^{2k}u^2$, la bola abierta $B(x, p^{-2k})$ está contenida en $\left(\mathbb{Q}_p^*\right)^2$. Sea $y \in \mathbb{Q}_p^*$ tal que $y \in B(x, p^{-2k})$. Entonces se cumple que

$$\mid y - x \mid_p < p^{-2k} = \mid x \mid_p = \mid p^{2k} \mid_p \cdot \mid u^2 \mid_p = p^{-2k}.$$

Por la regla de «el mayor se impone», tenemos que $\mid y \mid_p = \mid x \mid_p = p^{-2k}$, y por lo tanto podemos escribir y como $y = p^{2k}v$ con $v \in \mathbb{Z}_p^*$. Nos encontramos por tanto con que $\mid x - y \mid_p = p^{-2k} \mid v - u^2 \mid_p < p^{-2k}$, lo que equivale a decir que $\mid v - u^2 \mid_p < 1$. Eso significa que u^2 y v tienen su primer coeficiente idéntico. Sabesmos que el que una unidad p-ádica sea un cuadrado o no depende sólo del primer coeficiente de su desarrollo canónico, luego como u^2 es un cuadrado, v también lo es. Esto significa que $y \in \left(\mathbb{Q}_p^*\right)^2$, y $B(x, p^{-2k}) \subset \left(\mathbb{Q}_p^*\right)^2$. Por lo tanto, el subgrupo de los cuadrados de $\mathbb{Q}_p^*$ es un abierto de $\mathbb{Q}_p$.

Q.E.D.

Definición 6.1.10. *Se dice que un espacio topológico X es totalmente desconectado si sus únicos subconjuntos conexos son el conjunto vacío y los puntos.*

Proposición 6.1.11. *El espacio $\mathbb{Q}_p$ es totalmente desconectado.*

Demostración. Sea $A \subset \mathbb{Q}_p$ un subconjunto de $\mathbb{Q}_p$ tal que A no es vacío y no está reducido a un punto. Entonces, si tomamos $a, b \in A$ con $a \neq b$, como $\mathbb{Q}_p$ es un espacio métrico (luego de Hausdorff), existe una bola $B(a, r)$ tal que $b \notin B(a, r)$. Entonces, por ser la bola $B(a, r)$ un cerrado en $\mathbb{Q}_p$, tenemos que $A \cap B(a, r)$ es un cerrado en A que no es vacío y no es el total. Luego A no es conexo.
Como el conjunto vacío y los unipuntuales son siempre conexos, hemos acabado.

Q.E.D.

6.2. El conjunto de Cantor.

En este apartado vamos a tratar el conjunto de Cantor, un subconjunto de la recta real con propiedades muy interesantes. Aunque en un principio puede parecer algo desconectado de lo anterior, es un instrumento bastante potente para demostrar propiedades topológicas de $\mathbb{Z}_p$, pues, como veremos hacia el final, es homeomorfo a este último. Como tenemos una cantidad considerable de resultados sobre él, dividiremos este apartado en dos subapartados.

6.2.1. Construcción y características topológicas.

Consideramos la recta real, $\mathbb{R}$, con la topología derivada del valor absoluto usual. Entonces construimos los siguientes subconjuntos:

$$C_0 = [0, 1], C_1 = \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right]$$

$$C_2 = \left[0, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, 1\right], etc.$$

Como podemos ver, cada uno de los conjuntos C_n está formado por la unión de 2^n intervalos cerrados, cada uno de los cuales se forma quitando el tercio central abierto a cada uno de los intervalos del conjunto C_{n-1}. Denominaremos I_{n_i} con $0 \leq i \leq n$ los intervalos que forman C_n. Estos intervalos tienen todos longitud 3^{-n}, y es evidente que tenemos las inclusiones $C_0 \supset C_1 \supset C_2 \supset ... \supset C_n \supset ....$ Como todos los C_n están formados por un número finito de intervalos cerrados de $\mathbb{R}$, son compactos, y podemos definir el conjunto

$$C = \bigcap_{n \in \mathbb{N}} C_n$$

con la seguridad de que C será cerrado (compacto, para más detalles) y no vacío. Este conjunto C se llama el conjunto triádico de Cantor.

Definición 6.2.1. *El conjunto C formado por la intersección infinita de los conjuntos C_n definidos anteriormente es denominado conjunto triádico de Cantor.*

Es evidente que los extremos de los intervalos que forman C_n pertenecen todos a C. Ahora, si escribimos los números del intervalo $[0, 1]$ en base 3, todos los elementos que pueden acabar en una sucesión infinita de 2 pueden acabar también en una sucesión infinita de 0. En particular, los extremos de los intervalos que forman los C_n tienen todos dos representaciones distintas: por ejemplo,

$$\frac{1}{3} = 0{,}1 = 0{,}0\hat{2}, \quad \frac{2}{9} = 0{,}02 = 0{,}01\hat{2}, \quad \frac{2}{27} = 0{,}001\hat{2} = 0{,}002.$$

Podemos siempre elegir una representación de forma que no contenga el dígito 1. De hecho, si hacemos esto tenemos una descripción alternativa del conjunto de Cantor.

Teorema 6.2.2. *El conjunto de Cantor está formado exactamente por los elementos de $[0, 1]$ cuya escritura en base 3 sólo tiene como dígitos 0 y 2.*

Demostración. Sea $x \in C \subset \mathbb{R}$. Entonces x se puede escribir en base 3 de forma que $x = 0.x_1x_2...x_n...$, con $x_i \in \{0, 1, 2\}$ para todo $i \in \mathbb{N}$. Ahora bien, como $x \in C = \bigcap C_n$ tenemos que $x \in C_n$ para todo $n \in \mathbb{N}$. No es difícil ver que si $a = 0.a_1a_2...a_n... \in C_n$ entonces la n-ésima cifra de su escritura en base 3 está en el conjunto $\{0, 2\}$. El único caso problemático podría ser el de los extremos de los intervalos, pero para estos ya hemos elegido la representación que no contiene el dígito 1. Como $x \in C_n$ para todo $n \in \mathbb{N}$, entonces para todo natural n la n-ésima componente de su escritura en base 3 no es un 1, y se puede escribir utilizando únicamente los dígitos 0 y 2 en base 3.

La inclusión contraria sigue más o menos la misma idea. Sea $x = 0.x_1...x_n... \in [0, 1]$ tal que su escritura en base 3 no contiene el dígito 1. Si $x_1 = 0$, entonces

$x \in I_{1_0}$, mientras que si $x_1 = 2$ tenemos que $x \in I_{1_1}$. En ambos casos $x \in C_1$. Supongamos que se cumple que $x \in C_j$ para todo $j \leq n$. Entonces existe un $I_{n_i} \subset C_n$ tal que $x \in I_{n_i}$. Si $x_{n+1} = 0$, entonces x pertenece al primer tercio de I_{n_i}, que está contenido en C_{n+1}; si, en cambio, $x_{n+1} = 2$, x pertenece al tercer tercio de I_{n_i}, que también está en C_{n+1}. Tenemos por tanto que $x \in C_{n+1}$, y por inducción $x \in C_n \ \forall n \in \mathbb{N}$. Por la definición de C, $x \in C$ y hemos acabado.
Q.E.D.

Nota. *Aquí empezamos a vislumbrar alguna característica que ya habíamos señalado en el caso de los enteros p-ádicos. En efecto, en C, como en $\mathbb{Q}_p$, tenemos un conjunto de números con un desarrollo único en forma de serie, a diferencia de los elementos de $\mathbb{R}$, que podían tener dos expresiones.*

Definición 6.2.3. *Se dice que un espacio topológico X es perfecto si no tiene puntos aislados.*

Proposición 6.2.4. *El conjunto C de Cantor es perfecto.*

Demostración. Para ver que C es perfecto, es decir, que no tiene puntos aislados, vamos a probar que cualquier entorno de un punto x de C contiene otros puntos de C.
Sea $x \in C$ e I un intervalo abierto de $\mathbb{R}$. Como $x \in C = \bigcap C_n$ sabemos que $x \in C_n \ \forall n \in \mathbb{N}$. Llamamos I_n al intervalo cerrado de C_n que contiene a x. Entonces, por ser I abierto, tenemos que existe un $n \in \mathbb{N}$ tal que $I_n \subset I$. Sea $x_n \in I_n$ un extremo del intervalo que cumpla que $x \neq x_n$. Sabemos que $x_n \in C$, y como $x_n \in I_n \subset I$, tenemos un punto distinto de x que pertenece a I, que es entorno de x. Por lo tanto, x no es un punto aislado, y hemos acabado. En consecuencia, el conjunto de Cantor es perfecto.
Q.E.D.

Hemos visto que para construir el conjunto de Cantor $C = \bigcap C_n$ obtenemos C_n quitando el tercio central abierto a cada uno de los intervalos de C_{n-1}. Ahora bien, ¿por qué tercios? En principio podríamos haber eliminado la parte que hubiésemos considerado conveniente, y, en efecto, si hubiésemos dividido cada intervalo en $2p-1$ partes y hubiésemos retirado la segunda parte de cada dos, con el mismo procedimiento hubiésemos conseguido un conjunto tal que su expresión en base $2p-1$ sólo tiene dígitos pares. Estos conjuntos, con unas demostraciones semejantes a las que hemos hecho aquí, resultan ser también perfectos. Los denotaremos por C^p.

6.2.2. Homeomorfía.

Vamos ahora a ver que, efectivamente, tenemos un homeomorfismo entre $\mathbb{Z}_p$ y este.

Teorema 6.2.5. *El espacio de los enteros p-ádicos, $\mathbb{Z}_p$, es homeomorfo al conjunto C^p.*

Demostración. Lo primero de todo, construimos la función que queremos que sea nuestro homeomorfismo, ψ.

$$\begin{aligned} \psi : \mathbb{Z}_p &\longrightarrow C^p \\ \sum_{i=0}^{\infty} a_i p^i &\longmapsto \sum_{i=0}^{\infty} \frac{2a_i}{(2p-1)^{i+1}} \end{aligned}$$

Gracias a la unicidad de la representación tanto de los elementos de $\mathbb{Z}_p$ como de los de C^p, tenemos que esta función es una biyección. De hecho, su inversa sería de la forma

$$\psi^{-1} : \sum_{i=0}^{\infty} a_i (2p-1)^{-(i+1)} \longmapsto \sum_{i=0}^{\infty} \frac{a_i}{2} p^i.$$

Sólo nos queda por ver la continuidad.
Sea $n \in \mathbb{N}$ y sean $x_1, x_2 \in C^p$ tales que $\mid x_1 - x_2 \mid < 1/(2p-1)^n$. Entonces, si dividimos $I = [0,1]$ en subintervalos de longitud $1/(2p-1)^n$, x_1 y x_2 pertenecen al mismo subintervalo o a subintervalos adyacentes. Ahora bien, por la construcción de C_n^p no pueden existir dos intervalos adyacentes de longitud $1/(2p-1)^n$ de forma que ambos tengan puntos en común con C_n^p. Por lo tanto, x_1 y x_2 pertenecen al mismo subintervalo, y los primeros n dígitos de su escritura en base $2p-1$ coinciden. Recíprocamente, si los n primeros dígitos de dicha escritura coinciden, entonces pertenecen necesariamente al mismo subintervalo de C_n^p, y tenemos que $\mid x_1 - x_2 \mid < 1/(2p-1)^n$.
Por otra parte, sabemos que los primeros n dígitos del desarrollo canónico de dos enteros p-ádicos $x_1, x_2 \in \mathbb{Z}_p$ coinciden si y sólo si se cumple que $\mid x_1 - x_p \mid_p < p^{-n}$.
Sea $\epsilon > 0$. Entonces $\exists\ n \in \mathbb{N}$ tal que $\epsilon > (2p-1)^{-n}$. Tomamos $\delta = p^{-n}$. Tenemos que si $x_1, x_2 \in \mathbb{Z}_p$ cumplen que $\mid x_1 - x_2 \mid_p < \delta = p^{-n}$, los primeros n coeficientes del desarrollo canónico de x_1 y de x_2 coinciden. Por la definición de ψ que hemos hecho, eso quiere decir que los primeros n términos de la escritura en base $2p-1$ de $\psi(x_1)$ y $\psi(x_2)$ coinciden, y hemos visto que entonces $\mid x_1 - x_2 \mid < (2p-1)^{-n} < \epsilon$. Por lo tanto, la función ψ es continua.
Tenemos una función continua de un espacio compacto en uno de Hausdorff. Luego la función que hemos definido es un homeomorfismo y $\mathbb{Z}_p$ es homeomorfo a C^p para todo p primo.

Q.E.D.

Nota. *Este resultado nos dice que todos los resultados de topología que hemos demostrado para los enteros p-ádicos son ciertos para los conjuntos C^p, y viceversa. En particular, tanto C^p como $\mathbb{Z}_p$ son espacios métricos compactos, 0-dimensionales, totalmente desconectados y perfectos, así como no numerables.*

Corolario 6.2.6. *El conjunto de los enteros 2-ádicos, $\mathbb{Z}_2$, es homeomorfo al conjunto de Cantor.*

Hemos visto que cada uno de los espacios $\mathbb{Z}_p$ es homeomorfo a un C^p, un conjunto del tipo del de Cantor. Veremos después que todos los espacios métricos

que sean compactos, 0-dimensionales y perfectos son homeomorfos entre sí. Por esto, no vamos a seguir trabajando con los conjuntos C^p, sino que vamos a centrarnos en el conjunto de Cantor, pues toda propiedad topológica pasará después por homeomorfismo.

Corolario 6.2.7. *El conjunto de Cantor tiene interior vacío, es decir, no contiene ningún intervalo abierto no vacío.*

Demostración. Acabamos de ver que el conjunto de Cantor es totalmente desconectado. Eso significa que sus únicos conexos son el vacío y los conjuntos unipuntales. Ahora bien, los intervalos abiertos de la recta real son conjuntos conexos, y si no son vacíos entonces tampoco son unipuntuales. Por tanto, el conjunto de Cantor no contiene ningún intervalo abierto y no vacío, y en consecuencia tiene interior vacío.

Q.E.D.

El homeomorfismo entre C y $\mathbb{Z}_2$ tiene una interesante consecuencia: en efecto, nos permite definir una función continua y suprayectiva de $I = [0,1]$ en I^2. La imagen de esta función se denomina «curva de Peano», y se construye habitualmente de forma recursiva. Para llegar hasta ella tendremos que demostrar algunos resultados en los que construiremos las funciones que utilizaremos posteriormente.

Proposición 6.2.8. *Sea $\phi_p : \mathbb{Q}_p \to \mathbb{R}$ una función que envía un número p-ádico a un número real en base p de forma que $\phi_p(...a_1a_0.a_{-1}...a_{-k}) = a_{-k}...a_{-1}.a_0....$ La función ϕ_p es continua y sobreyectiva, pero no biyectiva. Además, la imagen de $\mathbb{Z}_p$ es el intervalo $I = [0,1]$.*

Demostración. Antes de empezar vamos a escribir los elementos de $\mathbb{Q}_p$ y sus imágenes en forma de serie. Así, tenemos que

$$\phi_p\left(\sum_{i=-k}^{\infty} a_i p^i\right) = \sum_{i=k}^{-\infty} a_{-i} p^i.$$

Ver que ϕ_p es sobreyectiva es fácil: sea $x = \sum_{i=k}^{-\infty} a_i p^i \in \mathbb{R}$ un número real en base p, es decir, $a_i \in \{0, ..., p-1\}$ $\forall i$. Tomamos el número p-ádico $y = \sum_{i=-k}^{\infty} a_{-i} p^i \in \mathbb{Q}_p$. Tenemos que

$$\phi_p(y) = \sum_{i=k}^{-\infty} a_{-(-i)} p^i = \sum_{i=k}^{-\infty} a_i p^i.$$

Comprobar que no es biyectiva consiste en ver que no es inyectiva. Para ello, sea $x = 0.(p-1)(p-1)... \in \mathbb{R}$ en base p. Sabemos que entonces $x = 1$. Al mismo tiempo, $...(p-1)(p-1) = -1 \in \mathbb{Q}_p$, y por tanto tenemos que $\phi_p(-1) = \phi_p(...(p-1)(p-1)) = 0.(p-1)(p-1)... = 1 = x = \phi_p(p^{-1})$. Pero $-1 \neq p^{-1}$, y la función no es inyectiva.

Veamos la continuidad. Lo primero de todo, tenemos que para todo $\epsilon > 0$ existe un $n \in \mathbb{Z}$ tal que $\epsilon > p^{-n}$. Eso significa que para todo $x \in \mathbb{R}$ se cumple que $B(x, p^{-n}) \subset B(x, \epsilon)$, y las bolas de centro x y radio p^{-n} $\forall n \in \mathbb{Z}$ forman un sistema fundamental de entornos del punto.
Sean $x \in \mathbb{R}$ y $n \in \mathbb{Z}$. Tomamos la bola $B(x, p^n) = \{y \in \mathbb{R}/ \ \mid x - y \mid < p^n\} = \left\{y \in \mathbb{R}/ \ \mid x - y \mid = \sum_{i=n-1}^{-\infty} a_i p^i\right\}$. Entonces su imagen inversa es

$$\phi_p^{-1}\left(B(x, p^n)\right) = \{z \in \mathbb{Q}_p/ \ \mid \phi_p(z) - x \mid < p^n\} =$$

$$\left\{z \in \mathbb{Q}_p/ \ \mid z - \phi_p^{-1}(x) \mid_p = \phi_p^{-1}\left(\sum_{i=n-1}^{-\infty} a_i p^i\right)\right\} =$$

$$\left\{z \in \mathbb{Q}_p/ \ \mid z - \phi_p^{-1}(x) \mid_p = \sum_{i=-n+1}^{\infty} a_i p^i\right\} =$$

$$\left\{z \in \mathbb{Q}_p/ \ \mid z - \phi_p^{-1}(x) \mid_p < p^n\right\} = B(\phi_p^{-1}(x), p^n),$$

y es un entorno del punto $\phi_p^{-1}(x)$. Así pues, la función ϕ_p es continua.

Por último, comprobemos que $\phi_p(\mathbb{Z}_p) = [0, 1]$. Sea $x = ...a_k...a_0 \in \mathbb{Z}_p$. Entonces $\phi_p(x) = 0.a_0...a_k... \in [0, 1]$. Para la contención contraria, sea $x = 0.a_0...a_k... \in [0, 1]$. Si escribimos $y = ...a_k...a_0$, que es un entero p-ádico por definición, entonces $\phi_p(y) = x$. Tenemos que $\phi_p(\mathbb{Z}_p) = [0, 1]$.

Q.E.D.

Para demostrar el siguiente resultado haremos uso de la hipótesis del continuo: no existe ningún conjunto cuyo cardinal sea no numerable y estrictamente menor que el de $\mathbb{R}$.

Corolario 6.2.9. *El conjunto $\mathbb{Q}_p$ tiene el mismo cardinal que los números reales.*

Demostración. Acabamos de demostrar que existe una función sobreyectiva de $\mathbb{Q}_p$ en el conjunto $\mathbb{R}$. Por tanto, tenemos que el cardinal del cuerpo de los números p-ádicos es menor o igual que el de los reales. Ahora bien, ya hemos visto en la proposición 3.3.3 que los enteros p-ádicos, $\mathbb{Z}_p$, no son numerables, y como forman un subconjunto de $\mathbb{Q}_p$, este último tampoco lo es. Por la hipótesis del continuo, eso significa que $\mathbb{Q}_p$ tiene el mismo cardinal que $\mathbb{R}$ y hemos acabado.

Q.E.D.

Proposición 6.2.10. *La función $f : C \to C^2$ dada por $f(0.a_1a_2a_3a_4...) = (0.a_1a_3..., \ 0.a_2a_4...)$ es un homeomorfismo entre C y C^2.*

Demostración. La demostración del homeomorfismo aquí es semejante a la del caso de C^p y $\mathbb{Z}_p$. Sea $f : C \to C^2$ tal que $f(0.a_1a_2a_3a_4...) = (0.a_1a_3..., 0.a_2a_4...)$. Entonces tenemos que las componentes de f son de la forma $f_1(0.a_1a_2a_3...) = 0.a_1a_3...$ y $f_2(0.a_1a_2a_3...) = 0.a_2a_4...$. La biyectividad es evidente.
Sea $\epsilon > 0$. Entonces existe un natural $n \in \mathbb{N}$ tal que $\epsilon > 3^{-n}$. Sean $x, y \in$

C tal que $\mid x - y \mid < 3^{-2n}$. Entonces, por el razonamiento que hicimos en el teorema 6.2.5, sabemos que los primeros $2n$ términos de x e y coinciden. Por lo tanto, los primeros n términos de $f_i(x)$ y de $f_i(y)$ coinciden, para $i \in \{1, 2\}$. Luego tenemos que para $i \in \{1, 2\}$, $\mid f_i(x) - f_i(y) \mid < 3^{-n} < \epsilon$. Tenemos por consiguiente que todas las componentes de f son continuas, y en consecuencia, f es continua.
Así, hemos conseguido una biyección f continua de un espacio compacto en uno de Hausdorff, y la función f es un homeomorfismo.

Q.E.D.

Estamos por fin en condiciones de construir la curva de Peano.

Teorema 6.2.11. *Existe una función continua y sobreyectiva entre el intervalo cerrado unidad $I = [0, 1]$ y su cuadrado, I^2.*

Demostración. Sea $g : C \to I$ la composición de la función $\phi_2 \restriction_{\mathbb{Z}_2} : \mathbb{Z}_2 \to I$ de la proposición 6.2.8 con el homeomorfismo de 6.2.5 $\psi : C \to \mathbb{Z}_2$, y tomamos la función $f : C \to C^2$ tal y como la hemos definido en la proposición 6.2.10. Como g es la composición de una función sobreyectiva y continua con un homeomorfismo, también es continua y sobreyectiva. La función $g \times g : C^2 \to I^2$ es, por tanto, sobreyectiva y continua. Sea $h = (g \times g) \circ f$ una aplicación de C en I^2 que vuelve a ser sobreyectiva y continua. Sean $h_1, h_2 : C \to I$ las componentes de h. Ahora bien, como C es cerrado en I, e $I \subset \mathbb{R}$ es un espacio normal (porque es métrico), por el Teorema de Extensión de Tietze tenemos que para cada una de las componentes existe una función $\hat{h}_i : I \to I$ continua tal que $\hat{h}_i \restriction_C = h_i$. Como h_i era sobreyectiva, $\hat{h}_i$ también lo es para $i \in \{1, 2\}$. Así obtenemos una función $\hat{h} = (\hat{h}_1, \hat{h}_2)$ continua y sobreyectiva de I en I^2 y hemos acabado.

Q.E.D.

Lema 6.2.12. *Sea U un abierto-cerrado no vacío de un espacio 0-dimensional, perfecto y de Hausdorff. Entonces para todo $n \in \mathbb{N}$ existen abierto-cerrados disjuntos $U_1, ..., U_n$ tales que $U = U_1 \cup U_2 \cup ... \cup U_n$.* [Wil68, pág. 216]

Demostración. Para demostrar este resultado nos basta con comprobar que se cumple para $n = 2$, pues el resto pueden demostrarse fácilmente por inducción. Como U es un abierto no vacío en un espacio perfecto, por definición de perfecto no puede ser un conjunto unipuntual. Tomamos $x, y \in U$ distintos. Entonces como el espacio es 0-dimensional y de Hausdorff tenemos que existe un abierto-cerrado V tal que $x \in V$, $y \notin V$. Tomamos $U_1 = U \cap V$ y $U_2 = U \setminus V$. Como V es abierto-cerrado, U_1 y U_2 también lo son, $U = U_1 \cup U_2$ y son disjuntos por construcción.

Q.E.D.

Teorema 6.2.13. *Dos espacios métricos perfectos, compactos y 0-dimensionales son siempre homeomorfos.* [Wil68, págs. 216-217]

Demostración. Sean X, Y dos espacios métricos perfectos, compactos y 0-dimensionales. Por el apartado 1. del teorema 5.2.10 tenemos dos sucesiones de

particiones finitas de X e Y formadas por abierto-cerrados de diámetro $< 1/2^n$, $(\mathcal{U}_n)$ y $(\mathcal{V}_n)$. Denotamos por X_∞ junto con las aplicaciones $\{\xi_n\}_{n=0}^\infty$ el límite proyectivo del sistema derivado $\{(\mathcal{U}_n, f_n)\}_{n=0}^\infty$ y por Y_∞ junto con las aplicaciones $\{\chi_n\}_{n=0}^\infty$ al límite proyectivo del sistema derivado $\{(\mathcal{V}_n, g_n)\}_{n=0}^\infty$. Podemos suponer sin pérdida de generalidad (aplicando el lema anterior si es necesario) que, para todo $n \in \mathbb{N}$, $\mathcal{U}_n$ y $\mathcal{V}_n$ tienen el mismo número de elementos.
Por la construcción que hicimos de los conjuntos $\mathcal{U}_n$ en el teorema 5.2.10, sabemos que cada elemento de $\mathcal{U}_j$ es unión de elementos de $\mathcal{U}_{j+1}$, y equivalentemente en el caso de $\mathcal{V}_j$. Denotamos los elementos de $\mathcal{U}_j$ por $U_{j,k}$ y los de $\mathcal{V}_j$ por $V_{j,k}$. Aplicando de nuevo el lema anterior podemos, salvo reordenación y sin pérdida de generalidad, afirmar que

$$U_{j,k} \subset U_{j+1,l} \Leftrightarrow V_{j,k} \subset V_{j+1,l}, \text{ es decir, } f_j(U_{j+1,l}) = U_{j,k} \Leftrightarrow g_j(V_{j+1,l}) = V_{j,k}.$$

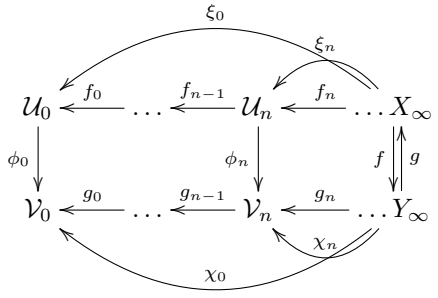
Ahora, podemos construir las aplicaciones $\phi_n : \mathcal{U}_n \to \mathcal{V}_n$ de forma que $\phi_n(U_{n,j}) = V_{n,j}$. Son biyectivas, continuas y abiertas, pues la topología de $\mathcal{U}_n$ y de $\mathcal{V}_n$ es en ambos casos la discreta. Tenemos por tanto que las funciones ϕ_n son homeomorfismos. Podemos componer estas aplicaciones con las aplicaciones propias de los límites proyectivos, y tendremos $\phi_n \circ \xi_n : X_\infty \to \mathcal{V}_n$ y $\phi_n^{-1} \circ \chi_n : Y_\infty \to \mathcal{V}_n$ continuas. Ahora bien, con la equivalencia que hemos dado antes tenemos que si $x \in X_\infty$, $\xi_n(x) = U_{n,j}$ y $\xi_{n+1}(x) = U_{n+1,k}$, entonces

$$g_n \circ (\phi_{n+1} \circ \xi_{n+1})(x) = g_n(V_{n+1,k}) = V_{n,j} = \phi_n(U_{n,j}) = \phi_n \circ \xi_n(x)$$

y X_∞ con las aplicaciones $\{\phi_n \circ \xi_n\}_{n=0}^\infty$ tienen la condición de compatibilidad respecto a $\{(\mathcal{V}_n, g_n)\}_{n=0}^\infty$. Con un razonamiento simétrico obtenemos que Y_∞ junto con las aplicaciones $\{\phi_n^{-1} \circ \chi_n\}_{n=0}^\infty$ tiene la condición de compatibilidad respecto a $\{(\mathcal{U}_n, f_n)\}_{n=0}^\infty$. Existen por tanto $f : X_\infty \to Y_\infty$ y $g : Y_\infty \to X_\infty$ continuas tales que $\phi_n \circ \xi_n = \chi_n \circ f$ y $\phi_n^{-1} \circ \chi_n = \xi_n \circ g$. Esta última igualdad nos da que $\chi_n = \phi_n \circ \xi_n \circ g$, y sustituyendo en la otra igualdad obtenemos que

$$\phi_n \circ \xi_n = \phi_n \circ \xi_n \circ g \circ f \Rightarrow g \circ f = \mathrm{Id}_{Y_\infty}.$$

De forma equivalente vemos que $f \circ g = \mathrm{Id}_{X_\infty}$. Tenemos por lo tanto que X_∞ e Y_∞ son homeomorfos.



Pero por el apartado 2. del teorema 5.2.10 sabemos que X es homeomorfo a

X_∞ e Y es homeomorfo a Y_∞. Por la transitividad de la homeomorfía, X es homeomorfo a Y y hemos acabado.

Q.E.D.

Corolario 6.2.14. *Los espacios topológicos $\mathbb{Z}_{p_1}$ y $\mathbb{Z}_{p_2}$ son homeomorfos.*

Corolario 6.2.15. *El espacio $\mathbb{Z}_2$ es el único espacio métrico perfecto, compacto y 0-dimensional, salvo homeomorfismo.*

6.3. Representaciones de $\mathbb{Z}_p$ en $\mathbb{R}^n$.

Para terminar, vamos a tratar un poco las representaciones de $\mathbb{Z}_p$ en $\mathbb{R}^n$. Evidentemente, los conjuntos C^p que hemos desarrollado en los apartados anteriores forman parte de las representaciones unidimensionales de $\mathbb{Z}_p$. Tenemos por tanto toda una familia de representaciones unidimensionales. Veamos qué pasa en dimensión superior. Sea $\nu : S = \{0, 1, ..., p-1\} \to \mathbb{R}^n$ una función inyectiva del espacio dicreto S en $\mathbb{R}^n$. Denotaremos $\Sigma = \nu(S)$. Entonces podemos definir la función $\psi_{\nu,b} : \mathbb{Z}_p \to \mathbb{R}^n$ como

$$\psi_{\nu,b}\left(\sum_{i=0}^{\infty} a_i p^i\right) = \alpha \sum_{i=0}^{\infty} \frac{\nu(a_i)}{b^{i+1}},$$

donde $\alpha = b - 1$. Separando el «término independiente» del desarrollo canónico de un entero p-ádico y sacando factor común a p en el resto de términos, vemos que $\mathbb{Z}_p = \coprod_{a_0 \in S} (a_0 + p\mathbb{Z}_p)$, es decir, que $\mathbb{Z}_p$ es la unión disjunta de los conjuntos de la forma $a_0 + p\mathbb{Z}_p$ donde $a_0 \in S$. Tenemos que

$$\psi_{\nu,b}(\mathbb{Z}_p) = \bigcup_{a_0 \in S} \left(\alpha \frac{\nu(a_0)}{b} + \frac{1}{b}\psi_{\nu,b}(\mathbb{Z}_p)\right) = \bigcup_{v \in \Sigma} \left(\alpha \frac{v}{b} + \frac{1}{b}\psi_{\nu,b}(\mathbb{Z}_p)\right),$$

y para valores suficientemente grandes de b, el conjunto imagen de $\psi_{\nu,b}$ estará formado por una unión disjunta de conjuntos. Así, podemos construir estos modelos de forma iterativa. En efecto, denotemos ahora la envolvente convexa de Σ por $\hat{\Sigma}$. Recordamos que la envolvente convexa de un conjunto $C = \{p_0, ..., p_n\}$ de puntos es el conjunto $\left\{\sum_{i \le n} \lambda_i p_i / \ \lambda_i \ge 0, \ \sum_{i \le n} \lambda_i = 1\right\}$. Tenemos que

$$\psi_{\nu,b}\left(\sum_{i=0}^{\infty} a_i p^i\right) = \alpha \sum_{n=0}^{\infty} \frac{\nu(a_i)}{b^{i+1}} = \sum_{i=0}^{p-1} \lambda_i \nu(a_i),$$

agrupando todos los coeficientes que están multiplicando al mismo $\nu(a_i)$. Entonces la imagen de $\sum_{i=0}^{\infty} a_i p^i$ está en $\hat{\Sigma}$ si y sólo si la suma de estos coeficientes vale 1.

$$\sum_{i=0}^{p-1} \lambda_i = \alpha \sum_{i=0}^{\infty} \frac{1}{b^{i+1}} = \frac{\alpha}{b-1} = \frac{b-1}{b-1} = 1,$$

por nuestra elección de la constante α y por la fórmula de las series geométricas. Por lo tanto, $\psi_{\nu,b}(\mathbb{Z}_p)$ está contenido en $\hat{\Sigma} = K_0$.
Hemos visto que $\psi_{\nu,b}(\mathbb{Z}_p) \subset K_0$. Ahora bien, habíamos probado anteriormente que $\psi_{\nu,b}(\mathbb{Z}_p) = \bigcup_{v\in\Sigma} (\alpha(v/b) + (1/b)\psi_{\nu,b}(\mathbb{Z}_p))$. Si juntamos estas dos fórmulas obtenemos que

$$\psi_{\nu,b}(\mathbb{Z}_p) = \bigcup_{v\in\Sigma} \left(\alpha\frac{v}{b} + \frac{1}{b}\psi_{\nu,b}(\mathbb{Z}_p)\right) \subset \bigcup_{v\in\Sigma} \left(\alpha\frac{v}{b} + \frac{1}{b}K_0\right) = K_1.$$

Iterando este proceso, tenemos que

$$K_n = \bigcup_{v\in\Sigma} \left(\alpha\frac{v}{b} + \frac{1}{b}K_{n-1}\right) \ \forall n \geq 1,\ K_0 = \hat{\Sigma},$$

y $\psi_{\nu,b}(\mathbb{Z}_p) \subset K_n$ para todo $n \in \mathbb{N}$. De forma análoga a lo que pasaba en el caso de los conjuntos C^p, podemos representar la imagen de $\mathbb{Z}_p$ por esta función como una intersección de los compactos K_n. [Rob00, págs. 12-13] Veamos unos ejemplos.

Ejemplo 6.3.1. *Tomemos $p = 3$ y la función $\psi_{\nu,b}$ con llegada en $\mathbb{R}^2$. La función ν es tal que $\nu(0) = 0$, $\nu(1) = (1,0) = e_1$ y $\nu(2) = (1/2, \sqrt{3}/2) = e_2$. Por el razonamiento que hemos seguido anteriormente, $\psi_{\nu,b}(\mathbb{Z}_p)$ está contenida en la envolvente convexa de $\{0, e_1, e_2\}$, que es un triángulo equilátero. Si $b > 2$ entonces la función es inyectiva. Por otra parte, si tenemos que $b = 2$, la figura es conexa, y forma el llamado «triángulo de Sierpinski».*

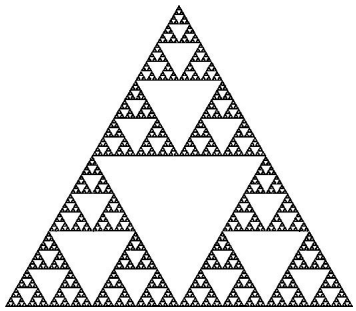


Figura 6.1: Triángulo de Sierpinski, $b = 2$

Ejemplo 6.3.2. *Generalicemos ahora esta construcción para $p > 3$. Tomamos $e_0, ..., e_{p-1}$ de forma que $e_0 = 0$ y el resto los e_i son los vértices de un polígono regular de $p-1$ lados y definimos la función $\nu(i) = e_i\ \forall i \in \{0, ..., p-1\}$. Entonces, si tomamos $\alpha = b - 1$, la imagen de la función $\psi_{\nu,b}$ en $\mathbb{Z}_p$ está contenida en dicho polígono regular.*

Bibliografía

[AM69] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969.

[Bac64] George Bachman. *Introduction to p-Adic Numbers and Valuation Theory*. Academic Press Inc., 1964.

[Coh03] P. M. Cohn. *Groups, Rings and Fields*. Springer, 2003.

[Gou93] F. Q. Gouvêa. *p-adic Numbers: an Introduction*. Springer-Verlag, 1993.

[Gou12] F. Q. Gouvêa. *A Guide to Groups, Rings and Fields*. The Mathematical Association of America, 2012.

[Ham82] A. G. Hamilton. *Numbers, Sets and Axioms*. Cambidge University Press, 1982.

[Kat07] S. Katok. *p-adic Analysis Compared with Real*. American Mathematical Society, 2007.

[Rob00] A. M. Robert. *A Course in p-adic Analysis*. Springer, 2000.

[Wil68] S. Willard. *General Topology*. Addison-Wesley Publishing Company, 1968.