Los números p-ádicos: Principales propiedades

Trabajo Fin de Grado
Grado en Matemáticas

Maider Sada Allo

Trabajo dirigido por
Federico Berlai
Javier Gutiérrez García

Leioa, 17 de junio de 2020

Índice general

1. Recordatorio **1**
- 1.1. Espacios métricos y espacios topológicos 1
  - 1.1.1. Espacios métricos 1
  - 1.1.2. Espacios topológicos cero-dimensionales y conexidad . 3
  - 1.1.3. Compacidad en espacios topológicos y métricos 4
- 1.2. Normas 6
- 1.3. Valuaciones 7
- 1.4. Normas y valuaciones p-ádicas 8

2. Espacios ultramétricos **11**
- 2.1. Definición y propiedades principales 11
- 2.2. Normas no arquimedianas y valuaciones 14

3. Sucesiones de Cauchy y completaciones **17**
- 3.1. Sucesiones de Cauchy 17
- 3.2. Completación: Definición y propiedades 18
- 3.3. Completación: Construcción 21

4. Equivalencias de normas y el Teorema de Ostrowski **27**
- 4.1. Equivalencias de normas 27
- 4.2. Teorema de Ostrowski 31

5. Los números y enteros p-ádicos **35**
- 5.1. Definición de los enteros p-ádicos 35
- 5.2. Las expansiones p-ádicas 38
- 5.3. Propiedades topológicas de $\mathbb{Q}_p$ y $\mathbb{Z}_p$ 40

A. Ejercicios **43**
- Recordatorio 43
- Espacios ultramétricos 45
- Sucesiones de Cauchy y completaciones 50
- Equivalencias de normas y el Teorema de Ostrowski 51

B. Visualización de la norma p-ádica en los números enteros **55**

Introducción

Los números p-ádicos fueron introducidos por primera vez por el matemático alemán Kurt Hensel en 1897 en un artículo que exploraba las analogías entre $\mathbb{Z}$ y $\mathbb{Q}$ con $\mathbb{C}[X]$ y $\mathbb{C}(X)$. Tanto $\mathbb{Z}$ como $\mathbb{C}[X]$ son dominios de factorización única, de manera que los números primos juegan un papel análogo a los de los polinomios primos $X - \alpha$ para $\alpha \in \mathbb{C}$.

Otro ejemplo de esta analogía es la siguiente: si $p(X) \in \mathbb{C}[X]$, para cada $\alpha \in \mathbb{C}$ existe $n \in \mathbb{N}$ tal que

$$p(X) = \sum_{i=0}^{n} \alpha_i (X - \alpha)^i, \quad \text{para ciertos } \alpha_i \in \mathbb{C},$$

y si $a \in \mathbb{Z}$, para cada primo p existe $n \in \mathbb{N}$ tal que

$$a = \sum_{i=0}^{n} a_i p^i, \quad \text{para ciertos } a_i \in \{0, \ldots, p-1\}.$$

Por último, si tomamos las potencias negativas de $X - \alpha$, para $f(X) \in \mathbb{C}(X)$ podemos calcular su desarrollo de Laurent de la siguiente forma:

$$f(x) = \sum_{i=m}^{\infty} \alpha_i (X - \alpha)^i, \quad m \in \mathbb{Z}, \alpha_m \neq 0, \alpha_i \in \mathbb{C}.$$

De forma análoga para cualquier $x \in \mathbb{Q}$ tenemos la siguiente expresión:

$$x = \sum_{i=m}^{\infty} a_i p^i, \quad m \in \mathbb{Z}, a_m \neq 0, a_i \in \{0, \ldots, p-1\}.$$

En el caso de los racionales, la convergencia de estas series nos puede dar problemas porque, los últimos términos de la serie son los más grandes. Para solucionar ésto se define una nueva norma para la que estas series sean sucesiones de Cauchy, que será la norma p-ádica y la denotaremos como $\|\cdot\|_p$. A partir de esta norma se definen los números p-ádicos de tal modo que toda sucesión en $\mathbb{Q}$ converja respecto de $\|\cdot\|_p$ si y solo si es de Cauchy para $\|\cdot\|_p$. Así las series definidas convergen en este nuevo cuerpo para todo $n \in \mathbb{Z}$ y para todo $a_i \in \frac{\mathbb{Z}}{p\mathbb{Z}}$.

En este trabajo intentamos presentar una base sólida del concepto de los números p-ádicos. Para ello definimos la norma p-ádica y tomamos los números p-ádicos como la complementación de $\mathbb{Q}$ respecto de esta norma. También trabajamos con las principales propiedades del espacio métrico que forma $\mathbb{Q}$ respecto de la norma p-ádica y del cuerpo de los números p-ádicos.

A la hora de redactarlo hemos tomado como base los apuntes "Introducción a los números p-ádicos" [1] y hemos ido complementándolos con el resto de documentos de la bibliografía.

Este trabajo está estructurado en cinco capítulos y dos apéndices cuyo contenido resumido es el siguiente:

En el primer capítulo hemos incluido la teoría necesaria sobre espacios topológicos, métricos y normados para poder desarrollar el resto de trabajo correctamente. También definimos los conceptos de valuación y norma p-ádica para un primo p que denotaremos por v_p y $\|\cdot\|_p$ respectivamente.

En el segundo capítulo definimos el concepto de espacio ultramétrico y trabajamos con sus propiedades. Es interesante desarrollar esta teoría ya que $(\mathbb{Q}, \|\cdot\|_p)$ es un espacio ultramétrico y nos da pistas sobre cómo se comporta esta norma.

En el tercer capítulo trabajamos con sucesiones de Cauchy y completaciones. Además de dar una definición matemática de las completaciones y trabajar con las principales propiedades tratamos de dar una expresión para cualquier anillo normado $(R, \|\cdot\|)$.

En el cuarto capítulo definimos las equivalencias de normas y probamos el Teorema de Ostrowski. También definimos los números p-ádicos, que denotamos $\mathbb{Q}_p$, como la completación de $\mathbb{Q}$ respecto de la norma p-ádica y deducimos que las únicas completaciones no triviales de $\mathbb{Q}$ son $\mathbb{R}$ y $\mathbb{Q}_p$ para algún primo p.

Finalmente, en el quinto capítulo definimos los enteros p-ádicos y trabajamos con diferentes propiedades algebráicas y topológicas de los enteros y números p-ádicos. También demostramos que todo $x \in \mathbb{Q}_p \setminus \{0\}$ se puede escribir de forma única como la siguiente serie convergente:

$$x = \sum_{i=m}^{\infty} a_i p^i \quad m \in \mathbb{Z}, a_m \neq 0, a_i \in \{0, \dots, p-1\}.$$

En el primer apéndice hemos enunciado y resuelto diferentes ejercicios y problemas de los capítulos anteriores. Finalmente en el segundo apéndice hemos trabajado con la visualización de la norma p-ádica para los números enteros.

Capítulo 1

Recordatorio: Espacios métricos, espacios topológicos, normas y valuaciones

En este capítulo veremos algunas definiciones, proposiciones y teoremas ya trabajados durante el grado y que vamos a necesitar para poder desarrollar la teoría de los siguientes capítulos. Hay algunas nociones que no hemos definido en este apartado porque las entenderemos como básicas para cualquier persona con conocimientos mínimos de Topología.

1.1. Espacios métricos y espacios topológicos

1.1.1. Espacios métricos

Definición 1.1.1. Sea X un conjunto dotado de una aplicación $d: X \times X \to \mathbb{R}^+$ que cumple las siguientes propiedades para todo $x, y, z \in X$:

(M1) $d(x,y) = 0 \iff x = y$.

(M2) $d(x,y) = d(y,x)$ (Simetría).

(M3) $d(x,z) \leq d(x,y) + d(y,z)$ (Desigualdad triangular).

El par (X, d) es un *espacio métrico* y d la distancia de éste.

Definición 1.1.2. Sean (X, d) un espacio métrico, $x_0 \in X$ y $r > 0$, podemos definir los siguientes conjuntos:

- *Bola abierta* centrada en x_0 y de radio r:

$$B(x_0, r) := \{x \in X \mid d(x, x_0) < r\}.$$

- *Bola cerrada* centrada en x_0 y de radio r:

$$\overline{B}(x_0, r) := \{x \in X \mid d(x, x_0) \leq r\}.$$

- *Esfera* centrada en x_0 y de radio r:

$$S(x_0, r) := \{x \in X \mid d(x, x_0) = r\}.$$

Definición 1.1.3. Sea A un subconjunto de un espacio métrico (X, d). El *diámetro* de A es el siguiente:

$$\text{diám}(A) := \sup\{d(x, y) \mid x, y \in A\}.$$

Proposición 1.1.4. *En un espacio métrico (X, d) el conjunto*

$$\beta = \{B(x_0, r) \mid x_0 \in X,\ r > 0\}$$

es una base de abiertos de un espacio topológico. A este espacio lo denominamos espacio topológico inducido por d y denotamos con (X, τ_d).

El espacio (X, τ_d) es Hausdorff, y $\overline{B}(x_0, r)$ es un conjunto cerrado para todo $x_0 \in X$ y $r > 0$.

Proposición 1.1.5. *Para un espacio métrico (X, d), la función*

$$d\colon (X \times X, \tau_{Tych}) \to (\mathbb{R}^+, \tau_u)$$

es continua en el espacio topológico producto del espacio topológico que induce la métrica d.

Demostración. Una base de abiertos de $(\mathbb{R}^+, \tau_u)$ es la que componen los siguientes conjuntos:

- $U = (a, b)$ tal que $0 \leq a < b$
- $U = [0, b)$ tal que $0 < b$

En el primer caso, la imagen inversa por d es un abierto de $X \times X$.

$$A_1 = d^{-1}((a, b)) = \{(x, y) \in X \times X \mid d(x, y) \in (a, b)\}$$

Sea $(x, y) \in A_1$. Tomemos $r_1 = \text{mín}\{b - d(x, y), d(x, y) - a\} > 0$. Entonces, veamos como $B\big(x, \frac{r_1}{2}\big) \times B\big(y, \frac{r_1}{2}\big) \subseteq A_1$. Sea $(z, t) \in B\big(x, \frac{r_1}{2}\big) \times B\big(y, \frac{r_1}{2}\big) \subseteq A_1$, entonces,

$$d(z, t) \leq d(z, x) + d(x, y) + d(y, t) < \frac{r_1}{2} + d(x, y) + \frac{r_1}{2} \leq b$$

Además,

$$d(x,y) \leq d(x,z) + d(z,t) + d(t,y) < r_1 + d(z,t) \implies d(z,t) > d(x,y) - r_1 \geq a$$

Por lo que $d(z,t) \in (a,b)$ y $(z,t) \in A_1$.

En el segundo caso para ver que $A_2 = d^{-1}([0,b))$ tomemos $(x,y) \in A_2$. Si $d(x,y) \neq 0$, entonces, existe $d^{-1}((0,b))$ un entorno abierto que lo contiene. Si $d(x,y) = 0$, entonces, $x = y$. Por lo que si tomamos $r_2 < b$ y $B\big(x, \frac{r_1}{2}\big) \times B\big(x, \frac{r_1}{2}\big)$ vamos a demostrar que $B\big(x, \frac{r_1}{2}\big) \times B\big(x, \frac{r_1}{2}\big) \subseteq A_2$. Sea $(z,t) \in B\big(x, \frac{r_1}{2}\big) \times B\big(x, \frac{r_1}{2}\big)$, entonces,

$$d(z,t) \leq d(z,x) + d(x,t) = r_2 < b$$

Por lo que $(x,z) \in A_2$. En consecuencia, A_2 es abierto y d es una función continua. □

1.1.2. Espacios topológicos cero-dimensionales y conexidad

Definición 1.1.6. Un espacio topológico (X,τ) que tiene una base de abiertos que también son cerrados es un espacio topológico *cero-dimensional.*

Definición 1.1.7. Un espacio topológico (X,τ) es *disconexo* si y sólo si existen $U, V \in \tau$ dos conjuntos abiertos no vacíos tales que $U \cap V = \varnothing$ y $X = U \cup V$. En el caso contrario es un espacio *conexo.*

Definición 1.1.8. Sean (X,τ) un espacio topológico y $D \subseteq X$. Si para todo par de abiertos $U, V \in \tau$ tal que $U \cap V \cap D = \varnothing$ y $D \subseteq U \cup V$ se cumple que $D \subseteq U$ o $D \subseteq V$, entonces D es un *conjunto conexo.*

Definición 1.1.9. Sea $x \in X$ un elemento de un espacio topológico (X,τ). Su *componente conexa*, que denotamos por $C(x)$, es el maximal de los conjuntos conexos que contienen a x.

Definición 1.1.10. Un espacio topológico (X,τ) es *totalmente disconexo* si para cada $x \in X$ la componente conexa de x es $\{x\}$.

Proposición 1.1.11. *Todo espacio topológico cero-dimensional y T_1 es totalmente disconexo.*

Demostración. Por reducción al absurdo, supongamos que siendo X un espacio cero-dimensional, la componente conexa $C(x)$ de un cierto $x \in X$, no es $\{x\}$. Tomemos β la base de abiertos que cumple que todos sus elementos son cerrados.

Como $C(x) \neq \{x\}$, existe $y \in C(x)$ tal que $y \neq x$. Por lo tanto, al ser X un espacio T_1 tenemos que, para la base de abiertos ya definida, existen dos abiertos $U, V \in \beta$ de modo que x e y están contenidos en uno solo de los abiertos pero no en el mismo.

Como U es cerrado, $X \setminus U$ es abierto. Por lo tanto, existen U y $X \setminus U$ abiertos, donde su intersección es nula y $C(x)$ está contenido en su union, pero $C(x)$ no está contenido en ninguno de los dos. Por lo que $C(x)$ es disconexo lo cual es absurdo ya que es la componente conexa de x. □

1.1.3. Compacidad en espacios topológicos y métricos

Definición 1.1.12. Sean (X, τ) un espacio topológico y $(a_n)_{n\in\mathbb{N}}$ una sucesión de elementos de X. Se dice que a es el *límite* de $(a_n)_{n\in\mathbb{N}}$, si y sólo si para todo abierto U que contiene a x, existe $n_0 \in \mathbb{N}$ tal que para todo $n > n_0$ se cumple que $a_n \in U$. La notación es la siguiente:

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

En este caso, se dice que $(a_n)_{n\in\mathbb{N}}$ es *convergente* en X, o que $(a_n)_{n\in\mathbb{N}}$ *converge* a a.

Proposición 1.1.13. *Sea (X, d) un espacio métrico y $A \subseteq X$. $x \in \overline{A}$ si y solo si existe una sucesión $(x_n)_{n\in\mathbb{N}}$ en A que converge a x. Además, si x es un punto de acomulación existe una sucesión de elementos de A que son diferentes de dos en dos.*

Definición 1.1.14. Sea (X, τ) un espacio topológico. Un subconjunto $A \subseteq X$ es

- *compacto* si todo recubrimiento abierto de A admite un subrecubrimiento finito.

- *localmente compacto* si para todo punto $x \in A$ existe un entorno (en A) compacto que lo contiene.

- *Compacto por punto límite* si cada subconjunto infinito de A tiene punto de acomulación en A.

- *secuencialmente compacto* si toda sucesión en A tiene una subsucesión convergente a un punto de A.

Si X es un espacio métrico, A es *totalmente acotado* si para todo $\varepsilon > 0$ existe un recubrimiento finito de A por bolas abiertas de radio ε.

Observación 1.1.15. Es fácil demostrar que un subespacio compacto es localmente compacto, totalmente acotado y compacto por punto límite. Pero las implicaciones contrarias no son ciertas. (Ver Ejercicio 2).

Proposición 1.1.16. *Todo subconjunto secuencialmente compacto de un espacio métrico (X, d) es totalmente acotado.*

Demostración. Por reducción al absurdo supongamos que siendo A secuencialmente compacto no es totalmente acotado. Entonces, existe $r > 0$ tal que A no admite un recubrimiento finito por bolas abiertas de radio r.

Tomamos $x_1 \in A$ cualquiera. Como $\{B(x_1, r)\}$ no puede ser un recubrimiento de A, existe $x_2 \in A$ tal que $d(x_1, x_2) \geq r$. Del mismo modo, como $\{B(x_1, r), B(x_2, r)\}$ no es un recubrimiento de A existe $x_3 \in A$ tal que $d(x_1, x_3) \geq r$ y $d(x_2, x_3) \geq r$. Si aplicamos esto de forma inductiva podemos definir la sucesión $(x_n)_{n\in\mathbb{N}}$ de elementos de A que cumple para todo $n \neq m$ $d(x_n, x_m) \geq r$.

Como A es secuencialmente compacto existe $(x_{n_k})_{k\in\mathbb{N}}$ una subsucesión convergente de $(x_n)_{n\in\mathbb{N}}$. Supongamos que el límite es $x \in A$. Entonces, existe $n_0 \in \mathbb{N}$ tal que para todo $k, m > n_0$ tenemos que $d(x_{n_k}, x) < \frac{r}{2}$ y $d(x_{n_m}, x) < \frac{r}{2}$. Por lo que,

$$d(x_{n_k}, x_{n_m}) \leq d(x_{n_k}, x) + d(x_{n_m}, x) < \tfrac{r}{2} + \tfrac{r}{2} = r$$

Lo cual es absurdo ya que $d(x_{n_k}, x_{n_m}) \geq r$. □

Lema 1.1.17 (**Lema de Lebesgue**). *Sea A un subconjunto secuencialmente compacto de un espacio métrico (X, d). Para todo recubrimiento abierto de A $\{U_i\}_{i\in I}$ existe $r > 0$ tal que para cada $x \in A$ existe $i \in I$ de modo que $B(x, r) \subseteq U_i$.*

Demostración. Por reducción al absurdo supongamos que para $\{U_i\}_{i\in I}$ no existe $r > 0$ que cumpla esa hipótesis. Entonces, para todo $n \in \mathbb{N}$ existe $x_n \in A$ tal que $B\big(x_n, \frac{1}{n}\big) \nsubseteq U_i$ para todo $i \in I$. Tomamos la sucesión $(x_n)_{n\in\mathbb{N}} \subseteq A$, como A es compacto por sucesiones existe $(x_{n_k})_{k\in\mathbb{N}}$ una subsucesión que converge a $x \in A$.

Como $\{U_i\}_{i\in I}$ es un recubrimiento abierto de A, existe $j \in I$ tal que $x \in U_j$. Como U_j es abierto existe $n_j \in \mathbb{N}$ tal que $B\big(x, \frac{2}{n_j}\big) \subseteq U_j$.

Como $(x_{n_k})_{k\in\mathbb{N}}$ converge a x, exite $n_0 \in \mathbb{N}$ tal que para todo $k > n_0$ $x_{n_k} \in B\big(x, \frac{1}{n_j}\big)$. Sin pérdida de generalidad podemos suponer que $n_k > n_j$. Tenemos que demostrar que $B\big(x_{n_k}, \frac{1}{n_k}\big) \subseteq B\big(x, \frac{2}{n_j}\big)$.

$$\begin{aligned} y \in B\Big(x_{n_k}, \frac{1}{n_k}\Big) &\implies d(x_{n_k}, y) < \frac{1}{n_k} \\ &\implies d(x, y) \leq d(x, x_{n_k}) + d(x_{n_k}, y) < \frac{1}{n_j} + \frac{1}{n_k} < \frac{2}{n_j} \\ &\implies y \in B\Big(x, \frac{2}{n_j}\Big) \end{aligned}$$

Por lo que $B\big(x_{n_k}, \frac{1}{n_k}\big) \subseteq U_j$ lo cual va en contra de la hipótesis. □

Teorema 1.1.18 (**Heine-Borel-Lebesgue**). *Un subconjunto de un espacio métrico es compacto si y solo si es secuencialmente compacto.*

Demostración. $\Rightarrow$) Sea (X, d) un espacio métrico y $A \subseteq X$ compacto. Tomemos $(a_n)_{n\in\mathbb{N}}$ una sucesión en A. Si $(a_n)_{n\in\mathbb{N}}$ tiene una cantidad finita de elementos diferentes, entonces existe un elemento a que se repite infinitas veces en la sucesión. Si tomamos la subsucesión creada por las repeticiones de este elemento, es una sucesión constante y en consecuencia convergente.

En el caso de que existan infinitos elementos diferentes, definimos B el subconjunto de los elementos de la sucesión. Como A es compacto, es compacto por punto límite y existe $x \in A$ un punto de acomulación de B, por lo que, por la Proposición 1.1.13, existe una sucesión $(b_n)_{n\in\mathbb{N}}$ de elementos de B que converge a x y que son diferentes de dos a dos. Por ello, $(b_n)_{n\in\mathbb{N}}$ es una subsucesión convergente de $(a_n)_{n\in\mathbb{N}}$.

$\Leftarrow$) Sea $\{U_i\}_{i\in I}$ un recubrimiento abierto de A, como A secuencialmente compacto entonces, por el Lema de Lebesgue existe $r > 0$ tal que para todo $x \in A$ se tiene que $B(x, r) \subseteq U_i$ para algún $i \in I$. Por otro lado, por la Proposición 1.1.16, se tiene que existe un recubrimiento finito de A por bolas de radio r. Para cada centro x de estas bolas tomamos $i_x \in I$ tal que $B(x, r) \subseteq U_{i_x}$. La familia que forman estos abiertos es un subrecubrimiento finito de $\{U_i\}_{i\in I}$. Por ello, A es compacto. $\square$

1.2. Normas

Definición 1.2.1. Sea R un anillo conmutativo. Una *norma* sobre R es una aplicación $\|\cdot\|: R \to \mathbb{R}^+$ que cumple las siguientes propiedades para todo $x, y \in R$:

(N1) $\|x\| = 0 \iff x = 0$.

(N2) $\|xy\| = \|x\|\|y\|$ (Multiplicidad).

(N3) $\|x + y\| \leq \|x\| + \|y\|$ (Desigualdad triangular).

Ejemplos 1.2.2. Los ejemplos más sencillos de una norma son los siguientes:

- El valor absoluto en $\mathbb{R}$. Tal que, para todo $x \in \mathbb{R}$

$$|x| := \begin{cases} x & \text{si } x \geq 0, \\ -x & \text{si } x < 0. \end{cases}$$

- La norma trivial sobre un anillo R. Para todo $x \in R$

$$\|x\| := \begin{cases} 0 & \text{si } x = 0, \\ 1 & \text{si } x \neq 0. \end{cases}$$

A partir de la desigualdad triangular, podemos deducir la siguiente desigualdad:

Proposición 1.2.3 (Desigualdad triangular inversa). *Sea $\|\cdot\|$ una norma sobre el anillo conmutativo R. Para todo $x, y \in R$ se cumple que*

$$\big|\|x\| - \|y\|\big| \leq \|x+y\|.$$

Demostración. Por la desigualdad triangular tenemos que

$$\|x\| = \|x+y-y\| \leq \|x+y\| + \|y\|.$$

Por lo que, $\|x\| - \|y\| \leq \|x+y\|$ y del mismo modo podemos demostrar que $\|y\| - \|x\| \leq \|x+y\|$. Por lo tanto

$$\big|\|x\| - \|y\|\big| = \max\{\|x\| - \|y\|, \|y\| - \|x\|\} \leq \|x+y\|. \quad \square$$

Proposición 1.2.4. *Todo anillo normado $(R, \|\cdot\|)$ es un dominio íntegro.*

Demostración. Sean $x, y \in R$ tal que $xy = 0$, tenemos lo siguiente:

$$\begin{aligned} xy = 0 &\iff \|x\|\|y\| = \|xy\| = 0 \iff \|x\| = 0 \text{ o } \|y\| = 0 \\ &\iff x = 0 \text{ o } y = 0. \end{aligned}$$

Por lo tanto, R es un dominio íntegro. $\square$

Como consecuencia de este resultado, vamos a poder trabajar con su cuerpo de fracciones $\mathbb{K}$.

Proposición 1.2.5. *Sean R un anillo conmutativo con norma $\|\cdot\|_R$ y $\mathbb{K}$ el cuerpo de fracciones de R. La aplicación $\|\cdot\|_{\mathbb{K}}$ con la siguiente definición es una norma sobre el cuerpo $\mathbb{K}$:*

$$\left\|\tfrac{x}{y}\right\|_{\mathbb{K}} := \tfrac{\|x\|_R}{\|y\|_R}, \qquad x, y \in R.$$

Proposición 1.2.6. *Toda norma $\|\cdot\|$ sobre un anillo conmutativo R define un espacio métrico $(R, \mathrm{d}_{\|\cdot\|})$ con la siguiente métrica.*

$$\begin{aligned} \mathrm{d}_{\|\cdot\|} \colon R \times R &\longrightarrow \mathbb{R}^+ \\ (x, y) &\longmapsto \mathrm{d}_{\|\cdot\|}(x, y) = \|x - y\|. \end{aligned}$$

Como $\mathrm{d}_{\|\cdot\|}$ es contínua bajo la topología inducida (ver Proposición 1.1.5), también $\|\cdot\|$ lo es.

1.3. Valuaciones

Definición 1.3.1. Sea R un anillo conmutativo. Una aplicación $v \colon R \longrightarrow \mathbb{Z} \cup \{\infty\}$ es una *valuación* si cumple las siguientes propiedades para todo $x, y, z \in R$:

(V1) $v(x) = \infty \iff x = 0$.

(V2) $v(xy) = v(x) + v(y)$.

(V3) $v(x + y) \geq \text{mín}\{v(x), v(y)\}$.

Proposición 1.3.2. *Si es posible definir una valuación v sobre un anillo conmutativo R, entonces, R es un dominio íntegro.*

Demostración. Sean $x, y \in R$ tal que $xy = 0$,

$$\begin{aligned} xy = 0 &\iff v(xy) = \infty \iff v(x) + v(y) = \infty \\ &\iff v(x) = \infty \text{ o } v(y) = \infty \iff x = 0 \text{ o } y = 0. \end{aligned}$$

Es decir, R es un dominio íntegro. □

Proposición 1.3.3. *Sean R un anillo conmutativo con valuación v_R y $\mathbb{K}$ su cuerpo de fracciones. La aplicación $v_{\mathbb{K}}$ con la siguiente definición es una valuación sobre el cuerpo $\mathbb{K}$:*

$$v_{\mathbb{K}}\big(\tfrac{x}{y}\big) := v_R(x) - v_R(y), \qquad x, y \in R.$$

Proposición 1.3.4. *Sean v una valuación sobre el anillo conmutativo R y $x, y \in R$ dos elementos cualquiera. Si $v(x) \neq v(y)$ se cumple que $v(x + y) = \text{mín}\{v(x), v(y)\}$.*

Proposición 1.3.5. *Sean R un anillo conmutativo con la valuación v, y $p \in \mathbb{N}$. La aplicación $\|\cdot\|_v$ con la siguiente definición es una norma:*

$$\|x\|_v := \begin{cases} 0 & \text{si } x = 0, \\ p^{-v(x)} & \text{si } x \neq 0. \end{cases}$$

1.4. Normas y valuaciones p-ádicas

Definición 1.4.1. Sean un número primo p y $n \in \mathbb{Z}$, definimos la *valuación p-ádica* del siguiente modo:

(1) $v_p(0) = \infty$ si $n = 0$, y

(2) $v_p(n) = k$ si $p^k \mid n$ pero $p^{k+1} \nmid n$.

Observaciones 1.4.2. (1) Para cualquier $n \in \mathbb{Z}$ y para cualquier primo p, $v_p(n) \geq 0$. Como para todo $n \in \mathbb{Z}$ $1 = p^0 \mid n$, su valuación p-ádica será mayor o igual a 0.

(2) Que k cumpla $p^k \mid n$ pero $p^{k+1} \nmid n$ es equivalente a que $n = p^k n'$ donde $p \nmid n'$.

Proposición 1.4.3. *La valuación p-ádica es una valuación sobre $\mathbb{Z}$ para todo número primo p.*

Demostración. Veamos cómo para todo número primo P la valuación p-ádica cumple las condiciones de la Definición 1.3.1.
(V1) La cumple por definición.

(V2) Sean $m, n \in \mathbb{Z}$. Si $v_p(n) = a$ y $v_p(m) = b$, vamos a distinguir dos casos: En el caso en el que m o n sean 0, podemos suponer sin pérdida de generalidad que $m = 0$. Entonces, $v_p(m) = \infty$ y $v_p(mn) = v_p(0) = \infty = v_p(m) + v_p(n)$.

En el caso de que $m, n \neq 0$, por la observación anterior, tenemos que $n = p^a n'$ y $m = p^b m'$ tal que $p \nmid n', m'$. Por lo que, $nm = p^{a+b} n' m'$ donde $p \nmid n'm'$, es decir, $v_p(nm) = a + b = v_p(n) + v_p(m)$.

(V3) Sean $m, n \in \mathbb{Z}$, vamos a separar en los dos mismos casos que en la demostración para (V2). Si $m = 0$, entonces, $v_p(m+n)_p = v_p(n) = \text{mín}\{v_p(m), v_p(n)\}$.

En el caso de que $m, n \neq 0$, tomando las referencias de la demostración de (V2), tenemos $n + m = p^a n' + p^b m'$. Sin pérdida de generalidad supongamos que $a \leq b$, entonces, $n + m = p^a(n' + p^{b-a} m')$. Por lo que

$$\begin{aligned} v_p(n+m) &= v_p(p^a(n' + p^{b-a}m') = v_p(p^a) + v_p(n' + p^{b-a}m') \\ &= a + v_p(n' + p^{b-a}m') \geq a = \text{mín}\{v_p(n), v_p(m)\} \end{aligned}$$

Ya que $v_p(n' + p^{b-a}m') \geq 0$ por la Observación 1.4.2. $\square$

Observación 1.4.4. Como caso particular de la Proposición 1.3.3, podemos definir la valuación p-ádica sobre $\mathbb{Q}$ de la siguiente forma:

$$v_p(x) = v_p\left(\tfrac{m}{n}\right) := v_p(m) - v_p(n), \qquad m, n \in \mathbb{Z}.$$

Además esta expresión no dependerá de los números m y n con los que se representa a x. Veámoslo.

Sean m_1, n_1, m_2, n_2 tal que $x = \frac{m_1}{n_1} = \frac{m_2}{n_2}$, entonces $m_1 n_2 = m_2 n_1$, luego

$$v_p(m_1) + v_p(n_2) = v_p(m_1 n_2) = v_p(m_2 n_1) = v_p(m_2) + v_p(n_1),$$

es decir,

$$v_p(m_1) - v_p(n_1) = v_p(m_2) - v_p(n_2) \iff v_p\left(\tfrac{m_1}{n_1}\right) = v_p\left(\tfrac{m_2}{n_2}\right).$$

Gracias a esto, vamos a poder asumir sin pérdida de generalidad que m y n son primos entre sí.

Siguiendo lo que dice la Proposición 1.3.5 podemos generalizar la definición de norma p-ádica sobre $\mathbb{Q}$.

Definición 1.4.5. La norma p-ádica sobre $\mathbb{Q}$ para un número primo p es la siguiente:

$$\|x\|_p := \begin{cases} 0 & \text{si } x = 0, \\ p^{-v_p(x)} & \text{si } x \neq 0. \end{cases}$$

Observación 1.4.6. Partiendo de esta definición, vamos a ver qué supone que $\|x\|_p$ sea menor o igual que 1 cuando $x \neq 0$. Tomemos $x = \frac{m}{n}$ tal que m y n son primos entre sí y $m \neq 0$.

Si $p^{-v_p(x)} = \|x\|_p \leq 1$, aplicando los logaritmos de base p tenemos que $-v_p(x) \leq 0$, por lo que,

$$0 \leq v_p(x) = v_p\left(\tfrac{m}{n}\right) = v_p(m) - v_p(n).$$

De esta última expresión podemos deducir que p no divide a n, ya que si lo hiciese, tanto $v_p(m)$ como $v_p(n)$ serían mayores que 0, lo que implica que p divide a m y n. Lo cual va contra la hipótesis de que son primos entre sí.

Por otro lado, es claro que si tenemos $\frac{m}{n}$ tal que p no divide a n, entonces $v_p(n) = 0$, y en consecuencia $\|n\|_p = 1$. Por lo que, $\|\frac{m}{n}\|_p = \frac{\|m\|_p}{\|n\|_p} = \frac{\|m\|_p}{1} = p^{-v_p(m)}$ y como $m \neq 0$, $v_p(m) \in \mathbb{Z}$ y, en consecuencia, $\|m\|_p \leq 1$.

En conclusión tenemos que si m y n son primos entre sí y $m \neq 0$, $\|\frac{m}{n}\|_p \leq 1$ si y solo si p no divide a n. Además en este caso, $\|\frac{m}{n}\|_p = \|m\|_p$.

El conjunto de estos números los definiremos como *enteros sobre p*.

Definición 1.4.7. Sea p un primo, definimos los *enteros sobre p*:

$$\begin{aligned}\mathbb{Z}_{(p)} &= \{a \in \mathbb{Q} \mid \|a\|_p \leq 1\} \\ &= \{0\} \cup \left\{\tfrac{m}{n} \in \mathbb{Q} \mid m \text{ y } n \text{ son primos entre sí y } p \text{ no divide a } n\right\}.\end{aligned}$$

Observación 1.4.8. Es claro que $\mathbb{Z} \subseteq \mathbb{Z}_{(p)}$ para todo número primo p y también que si $\frac{m}{n}$ es entero sobre p para todo número primo p entonces necesariamente $n = 1$, luego se cumple lo siguiente:

$$\bigcap_{p \text{ primo}} \mathbb{Z}_{(p)} = \mathbb{Z}.$$

Capítulo 2

Espacios ultramétricos

2.1. Definición y propiedades principales

Definición 2.1.1. Un espacio métrico (X, d) en el que se cumple la siguiente propiedad para todo $x, y, z \in X$ es un *espacio ultramétrico*

(M3*) $d(x, z) \leq \max\{d(x, y), d(y, z)\}$ (Desigualdad ultramétrica).

Proposición 2.1.2. *Sean (X, d) un espacio ultramétrico y $x, y, z \in X$. Si $d(x, y) \neq d(y, z)$ entonces $d(x, z) = \max\{d(x, y), d(y, z)\}$.*

Demostración. Por reducción al absurdo, supongamos que siendo $d(x, y) \neq d(y, z)$ se cumple que $d(x, z) < \max\{d(x, y), d(y, z)\}$. Sin pérdida de generalidad tomemos $d(x, y) < d(y, z)$. Entonces,

$$d(x, z) < \max\{d(x, y), d(y, z)\} = d(y, z) \leq \max\{d(x, y), d(x, z)\}.$$

Si $\max\{d(x, y), d(x, z)\} = d(x, y)$, entonces llegamos a que $d(y, z) \leq d(x, y)$, lo cual es una contradicción. Si por el contrario $\max\{d(x, y), d(x, z)\} = d(x, z)$ llegamos a que $d(x, z) < d(x, z)$. Por lo que en los dos casos llegamos a una contradicción y $d(x, z) = \max\{d(x, y), d(y, z)\}$. $\square$

Lema 2.1.3. *En un espacio ultramétrico las esferas de radio finito son conjuntos abiertos y cerrados.*

Demostración. Sean (X, d) un espacio ultramétrico y $x_0 \in X$. Tomamos $x \in S(x_0, r)$ y $0 < \varepsilon < r$, para ver cómo $B(x_0, \varepsilon) \subseteq S(x_0, r)$.
Sea $y \in B(x, \varepsilon)$. Es claro que $d(x, y) < \varepsilon < r = d(x_0, x)$, luego por la proposición anterior,

$$d(x_0, y) = \max\{d(x_0, x), d(x, y)\} = r \implies y \in S(x_0, r).$$

Por lo que $B(x, \varepsilon) \subseteq S(x_0, r)$ y $S(x_0, r)$ es un conjunto abierto.

Por otro lado, $X \setminus S(x_0, r) = \{x \in X \mid x < r\} \cup \{x \in X \mid x > r\}$ al ser una unión de dos conjuntos abiertos, es abierto. Por lo tanto $S(x_0, r)$ es cerrado. $\square$

Teorema 2.1.4. *En un espacio ultramétrico* (X, d) *los conjuntos* $B(x_0, r)$ *y* $\overline{B}(x_0, r)$ *son abiertos y cerrados al mismo tiempo, para todo* $x_0 \in X$ *y* $r \geqslant 0$.

Demostración. Fijamos $x_0 \in X$ y $r > 0$, y consideramos la bola $B(x_0, r)$, que es abierta por definición. Para demostrar que es cerrada es suficiente ver que

$$X \setminus B(x_0, r) = \{x \in X \mid d(x, x_0) \geq r\} = S(x_0, r) \cup X \setminus B(x_0, r)$$

es abierto.

Sabemos que la esfera $S(x_0, r)$ es un conjunto abierto por el Lema 2.1.3, y $X \setminus \overline{B}(x_0, r)$ es abierto al ser el complementario del cerrado $\overline{B}(x_0, r)$. Entonces el conjunto $X \setminus B(x_0, r)$ es abierto.

De manera similar tenemos que $\overline{B}(x_0, r) = S(x_0, r) \cup B(x_0, r)$ es la unión de dos conjuntos abiertos, y por ello es abierto. □

Del Teorema 2.1.4 deducimos:

Corolario 2.1.5. *Si* (X, d) *es un espacio ultramétrico entonces* (X, τ_d) *es un espacio topológico cero-dimensional.*

Observación 2.1.6. En un espacio ultramétrico todas las bolas abiertas son cerradas y viceversa, pero esto no quiere decir que para cada $x_0 \in X$ y $r > 0$ la bola abierta centrada en x_0 y de radio r sea igual a la cerrada.

Por ejemplo, en el espacio ultramétrico $(\mathbb{Z}, \|\cdot\|_2)$, la bola abierta $B(0, 1) = 2\mathbb{Z}$ no es igual a la bola cerrada $\overline{B}(0, 1) = \mathbb{Z}$.

Observación 2.1.7. Como todas las bolas abiertas son cerradas y viceversa, a partir de ahora hablaremos de bolas de radio r y centradas en x_0. Normalmente utilizaremos las bolas abiertas, pero los razonamientos serían perfectamente válidos utilizando las bolas cerradas. Por otro lado, al conjunto de bolas abiertas o cerradas que se pueden generar en X lo llamaremos $\mathbb{B}_X$.

Proposición 2.1.8. *Sea* $B(x, r)$ *una bola abierta en un espacio ultramétrico* (X, d). *Todo punto de* $B(x, r)$ *es el centro de la bola, es decir,* $B(x, r) = B(y, r)$ *para todo* $y \in B(x, r)$. *Lo mismo se cumple para toda bola cerrada* $\overline{B}(x, r)$.

Demostración. Sea $y \in B(x, r)$ un elemento de una bola abierta, vamos a demostrar que $z \in B(x, r)$ si y sólo si $z \in B(y, r)$. Veámoslo. Como $d(y, x) < r$ se tiene que

$$\begin{aligned} z \in B(x, r) &\iff d(z, x) < r \iff d(z, y) \leq \max\{d(z, x), d(x, y)\} < r \\ &\iff z \in B(y, r). \end{aligned}$$

Análogamente, si $y \in \overline{B}(x, r)$ entonces

$$\begin{aligned} z \in \overline{B}(x, r) &\iff d(z, x) \leq r \iff d(z, y) \leq \max\{d(z, x), d(x, y)\} \leq r \\ &\iff z \in \overline{B}(y, r). \end{aligned}$$

□

Proposición 2.1.9. *Sea $B(x_0, r)$ una bola abierta en un espacio ultramétrico (X, d). Entonces se tiene que* $\text{diám}\,(B(x_0, r)) \leq r$*. De manera análoga,* $\text{diám}\,(\overline{B}(x_0, r)) \leq r$ *para toda bola cerrada $\overline{B}(x_0, r)$.*

Demostración. Sean $x, y \in B(x_0, r)$, entonces $x \in B(x_0, r) = B(y, r)$, luego $d(x, y) < r$. Por lo que $\sup\{d(x, y) \mid x, y \in B(x_0, r)\} \leq r$. Del mismo modo, si $x, y \in \overline{B}(x_0, r)$, entonces, $d(x, y) \leq r$ y en consecuencia,
$\sup\{d(x, y) \mid x, y \in B(x_0, r)\} \leq r$. □

Proposición 2.1.10. *Sean $B_1, B_2 \in \mathbb{B}_X$ dos bolas en un espacio ultramétrico (X, d). Se cumplen las siguientes propiedades:*

(1) *Si $B_1 \cap B_2 \neq \varnothing$ entonces $B_1 \subseteq B_2$ o $B_2 \subseteq B_1$.*

(2) *Si $B_1 \cap B_2 = \varnothing$ entonces $d(B_1, B_2) = d(x_1, x_2)$ para cualquier $x_1 \in B_1$ y $x_2 \in B_2$.*

Demostración. (1) Sean r y s los radios de B_1 y B_2 respectivamente, tomemos $z \in B_1 \cap B_2$. Por la Proposición 2.1.8, z es el centro de las dos bolas. En consecuencia, si $r \leq s$, entonces, $B_1 \subseteq B_2$, y analogamente si $r > s$, entonces, $B_2 \subseteq B_1$.

(2) Demostramos la proposición en el caso que B_1 y B_2 sean bolas abiertas. De manera análoga se comprueban los demás casos. Supongamos que $B_1 \cap B_2 = \varnothing$. Sean $x_1 \in B_1$ y $x_2 \in B_2$. Por la Proposición 2.1.8, para todo $y_1 \in B_1$ e $y_2 \in B_2$ tenemos que $B_1 = B(x_1, r) = B(y_1, r)$ y $B_2 = B(x_2, s) = B(y_2, s)$, y como $B_1 \cap B_2 = \varnothing$, tendremos que

$$d(x_1, y_1) < r < \text{mín}\{d(x_1, x_2), d(y_1, y_2)\}$$

y del mismo modo

$$d(x_2, y_2) < s < \text{mín}\{d(x_1, x_2), d(y_1, y_2)\}.$$

Por lo que, $d(x_1, x_2) \leq \text{máx}\{d(x_1, y_1), d(y_1, y_2), d(y_2, x_2)\} = d(y_1, y_2)$ y del mismo modo, $d(y_1, y_2) \leq \text{máx}\{d(y_1, x_1), d(x_1, x_2), d(x_2, y_2)\} = d(x_1, x_2)$. Así, $d(y_1, y_2) = d(x_1, x_2)$ y por tanto

$$d(B_1, B_2) = \text{ínf}\{d(y_1, y_2) \mid y_1 \in B_1,\ y_2 \in B_2\} = d(x_1, x_2). \qquad \square$$

Estas dos últimas proposiciones no sólo son propiedades de los espacios ultramétricos, son una caracterización de estos. Veámoslo en el siguiente teorema.

Teorema 2.1.11. *Sea (X, d) un espacio métrico, las siguientes condiciones son equivalentes:*

(1) *(X, d) es un espacio ultramétrico.*

(2) *Para cada* $B_1, B_2 \in \mathbb{B}_X$ *se tiene que si* $B_1 \cap B_2 \neq \varnothing$ *entonces* $B_1 \subseteq B_2$ *o* $B_2 \subseteq B_1$.

(3) *Para cada* $B \in \mathbb{B}_X$ *y para cada* $x \in B$, x *es el centro de* B.

Demostración. La Proposición 2.1.8 prueba la implicación (1) $\Rightarrow$ (3). Supongamos ahora que (3) se cumpla, y sean $B_1, B_2 \in \mathbb{B}_X$ dos bolas con intersección no vacía. Sea $z \in B_1 \cap B_2$, así que z es el centro de B_1 y de B_2. Comparando los radios de B_1 y de B_2 podemos entonces deducir que $B_1 \subseteq B_2$ o que $B_2 \subseteq B_1$. Eso es, (3) implica (2).

Para comprobar que (2) implica (1), sean $x, y, z \in X$, definimos las distancias $r = d(x, y)$ y $s = d(z, y)$, $\varepsilon > 0$ y las bolas $B_1 = B(x, r+\varepsilon)$ y $B_2 = B(z, s+\varepsilon)$. Por definición tenemos que $y \in B_1 \cap B_2 \neq \varnothing$. En consecuencia, por (2) se cumple $B_1 \subseteq B_2$ o $B_2 \subseteq B_1$. Sin pérdida de generalidad, supongamos que $B_1 \subseteq B_2$.

Tenemos que $x \in B_2$ y que $s \geq r$. Por ello, $d(x, z) \leq s + \varepsilon$ para todo $\varepsilon > 0$. Por lo que $d(x, y) \leq s = \text{máx}\{s, r\} = \text{máx}\{d(y, z), d(x, y)\}$. Por tanto, (X, d) es un espacio ultramétrico. □

Por último tenemos el siguiente resultado.

Proposición 2.1.12. *Todo espacio ultramétrico es totalmente disconexo.*

Demostración. Todo espacio ultramétrico es T_1, además como hemos visto en el Corolario 2.1.5 es cero-dimensional. Por lo que por la Proposición 1.1.11, será totalmente disconexo. □

2.2. Normas no arquimedianas y valuaciones

Definición 2.2.1. Una norma $\|\cdot\|\colon R \to \mathbb{R}^+$ sobre el anillo conmutativo R que para todo $x, y \in R$ cumple la siguiente propiedad, es una *norma no arquimediana.*

(N3*) $\|x + y\| \leq \text{máx}\{\|x\|, \|y\|\}$.

Proposición 2.2.2. *Sea* $\|\cdot\|\colon R \to \mathbb{R}^+$ *una norma no arquimediana. Para todo* $x, y \in R$ *donde* $\|x\| \neq \|y\|$ *se cumple*

$$\|x + y\| = \text{máx}\{\|x\|, \|y\|\}.$$

Demostración. Supongamos que siendo $\|x\| \neq \|y\|$ se cumple la desigualdad estricta $\|x + y\| < \text{máx}\{\|x\|, \|y\|\}$. Sin pérdida de generalidad suponemos que $\|y\| < \|x\|$. Entonces $\|x + y\| < \|x\|$, por lo que

$$\|x\| = \|x + y - y\| \leq \text{máx}\{\|x + y\|, \|y\|\} < \|x\|$$

lo cual es una contradicción. Por lo que $\|x + y\| = \text{máx}\{\|x\|, \|y\|\}$. □

Observación 2.2.3. La anterior proposición se puede generalizar a n elementos de manera inductiva.

Proposición 2.2.4. *Una norma $\|\cdot\|$ sobre un anillo conmutativo R es no arquimediana si y sólo si para todo $n \in \mathbb{N}$, $\|1n\| = \|1 + \cdots + 1\| \leq 1$.*

Demostración. $\Rightarrow$) Vamos a hacer esta demostración por inducción. Para $n = 1$, se cumple por lo que, si tomamos cualquier $n \in \mathbb{N}$ y suponemos que es cierto, entonces,

$$\|n + 1\| \leq \max\{\|n\|, 1\} = 1.$$

$\Leftarrow$) Sean $x, y \in R$, tenemos que

$$\begin{aligned}
\|x + y\|^n = \|(x + y)^n\| &= \left\| \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \right\| \\
&\leq \sum_{k=0}^{n} \left\| \binom{n}{k} x^k y^{n-k} \right\| \\
&= \sum_{k=0}^{n} \left\| \binom{n}{k} \right\| \|x\|^k \|y\|^{n-k} \\
&\leq \sum_{k=0}^{n} \|x\|^k \|y\|^{n-k} \leq (n + 1) \max\{\|x\|, \|y\|\}^n.
\end{aligned}$$

Por ello, para todo $n \in \mathbb{N}$

$$\|x + y\| \leq \sqrt[n]{n + 1} \max\{\|x\|, \|y\|\}.$$

Cuando n tiende a infinito, obtenemos la desigualdad que queremos demostrar. $\square$

Proposición 2.2.5. *Sea $\|\cdot\| \colon R \to \mathbb{R}^+$ una norma no arquimediana sobre el anillo conmutativo R. El espacio $(X, d_{\|\cdot\|})$ es un espacio ultramétrico, donde $d_{\|\cdot\|}$ es la distancia inducida por $\|\cdot\|$.*

Demostración. La distancia inducida a partir de $\|\cdot\|$ es la siguiente (ver Proposición 1.2.6):

$$\begin{aligned}
d_{\|\cdot\|} \colon R \times R &\longrightarrow \mathbb{R}^+ \\
(x, y) &\longmapsto d_{\|\cdot\|}(x, y) = \|x - y\|.
\end{aligned}$$

Por definición $d_{\|\cdot\|}$ es una métrica, por lo que solo nos queda ver que cumple la propiedad (M3*) de la Definición 2.1.1. Es claro que la propiedad (N3*) de la Definición 2.2.1 implica (M3*). $\square$

Proposición 2.2.6. *Si v es una valuación, entonces $\|\cdot\|_v$ dada por*

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

es una norma no arquimediana.
Del mismo modo, si $\|\cdot\|$ es una norma no arquimediana sobre un anillo conmutativo R, entonces, $v_{\|\cdot\|}$ dada por

$$v_{\|\cdot\|}(x) := \begin{cases} 0 & \text{si } x = 0, \\ -\log\|x\| & \text{si } x \neq 0, \end{cases}$$

es una valuación si y solo si $v_{\|\cdot\|}(R) \subseteq \mathbb{Z}$.

Demostración. (1) Veamos cómo una valuación v induce una norma no arquimediana. Por la Proposición 1.3.5 sabemos que (N1) y (N2) se cumplen, ahora veamos cómo se cumple (N3*). Si $x = 0$, $y = 0$ o $x + y = 0$ entonces se cumple trivialmente, luego supondremos que $x \neq 0$, $y \neq 0$ y $x + y \neq 0$. Tenemos que

$$\begin{aligned} \|x+y\|_v \leq p^{-v(x+y)} &\leq p^{-\min\{v(x),v(y)\}} \\ &= \max\{p^{-v(x)}, p^{-v(y)}\} = \max\{\|x\|, \|y\|\}. \end{aligned}$$

(2) Ahora veamos que siendo $\|\cdot\|$ una norma no arquimediana, cumple las siguientes propiedades:
(V1) es evidente.
(V2) Sean $x, y \in R$ tales que $x, y \neq 0$, entonces

$$v(xy) = -\log\|xy\| = -\log(\|x\|\|y\|) = -(\log\|x\| + \log\|y\|) = v(x) + v(y).$$

(V3) Sean $x, y \in R$ tales que $x, y, x + y \neq 0$, entonces

$$\begin{aligned} v(x+y) = -\log\|x+y\| &\geq -\log(\max\{\|x\|, \|y\|\}) \\ &= \min\{-\log\|x\|, -\log\|y\|\} = \min\{v(x), v(y)\}. \end{aligned}$$

Por lo que, como cumple las tres propiedades de la Definición 1.3.1, es una valuación si y solo si $v_p(R) \subseteq \mathbb{Z}$. □

Podemos entonces deducir que la norma p-ádica definida en la Definición 1.4.5 es una norma no arquimediana y que en consecuencia $(\mathbb{Q}, \|\cdot\|_p)$ y $(\mathbb{Z}, \|\cdot\|_p)$ son espacios ultramétricos.

Corolario 2.2.7. *Para todo número primo p la norma p-ádica $\|\cdot\|_p$ es una norma no arquimediana y el espacio $(\mathbb{Q}, d_p)$ es un espacio ultramétrico, donde $\|\cdot\|_p$ es*

$$\|x\|_p := \begin{cases} 0 & \text{si } x = 0, \\ p^{-v_p(x)} & \text{si } x \neq 0. \end{cases}$$

Capítulo 3

Sucesiones de Cauchy y completaciones

3.1. Sucesiones de Cauchy

Si tomamos la Definición 1.1.12 para un anillo normado $(R, \|\cdot\|)$ tenemos lo siguiente.

Definición 3.1.1. Sean $(R, \|\cdot\|)$ un anillo normado y $(a_n)_{n\in\mathbb{N}}$ una sucesión de elementos de R. Se dice que a es el *límite* de $(a_n)_{n\in\mathbb{N}}$, si y sólo si para todo $\varepsilon > 0$, existe $n_\varepsilon \in \mathbb{N}$ tal que para todo $n > n_\varepsilon$ se cumple

$$\|a - a_n\| < \varepsilon.$$

La notación es la siguiente:

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

En este caso, se dice que $(a_n)_{n\in\mathbb{N}}$ es *convergente* en R, o que $(a_n)_{n\in\mathbb{N}}$ *converge* a a.

Proposición 3.1.2. *Sean $(R, \|\cdot\|)$ un anillo normado y $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$ dos sucesiones convergentes de elementos de R. Se tiene que*

(1) $\left(\lim_{n\to\infty} a_n\right) \pm \left(\lim_{n\to\infty} b_n\right) = \lim_{n\to\infty}(a_n \pm b_n)$,

(2) $\left(\lim_{n\to\infty} a_n\right) \cdot \left(\lim_{n\to\infty} b_n\right) = \lim_{n\to\infty}(a_n \cdot b_n)$.

Demostración. (1) Sean $(a_n)_{n\in\mathbb{N}}$ y $(b_n)_{n\in\mathbb{N}}$, dos sucesiones que convergen respectivamente a a y b. Para todo $\varepsilon > 0$, existen $n_1, n_2 \in \mathbb{N}$ tales que para todo $n \in \mathbb{N}$ donde $n > n_1$ y $n > n_2$, se cumple lo siguiente,

$$\|a_n - a\| < \frac{\varepsilon}{2} \quad \text{y} \quad \|b_n - b\| < \frac{\varepsilon}{2}.$$

Si tomamos $n_0 = \text{máx}\{n_1, n_2\}$, entonces, para todo $n > n_0$

$$\|(a_n \pm b_n) - (a \pm b)\| = \|(a_n - a) \pm (b_n - b)\| \leq \|a_n - a\| + \|b_n - b\| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

(2) Sean $(a_n)_{n\in\mathbb{N}}$ y $(b_n)_{n\in\mathbb{N}}$, dos sucesiones que convergen respectivamente en a y b. Para todo $\varepsilon > 0$, tomemos $0 < \delta < \varepsilon$, entonces, existen n_3, n_4 tales que para todo $n > n_3$ y $n > n_4$

$$\|a_n - a\| < \frac{\varepsilon}{\frac{\delta}{\|a\|} + 2\|b\|} \quad \text{y} \quad \|b_n - b\| < \frac{\delta}{2\|a\|}.$$

Tomando $n_0' = \text{máx}\{n_3, n_4\}$ tenemos que para todo $n > n_0'$

$$\begin{aligned}
\|a_n b_n - ab\| &= \|a_n b_n - ab_n + ab_n - ab\| \leq \|a_n - a\|\|b_n\| + \|a\|\|b_n - b\| \\
&= \|a_n - a\|\|b_n - b + b\| + \|a\|\|b_n - b\| \\
&\leq \|a_n - a\|(\|b_n - b\| + \|b\|) + \|a\|\|b_n - b\| \\
&< \frac{\varepsilon}{\frac{\delta}{\|a\|} + 2\|b\|}\left(\frac{\delta}{2\|a\|} + \|b\|\right) + \|a\|\frac{\delta}{2\|a\|} = \frac{\varepsilon}{2} + \frac{\delta}{2} \\
&< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.
\end{aligned}$$

□

Definición 3.1.3. Una sucesión $(a_n)_{n\in\mathbb{N}}$ en un anillo normado $(R, \|\cdot\|)$ es una *sucesión de Cauchy* si y sólo si para todo $\varepsilon > 0$ existe $n_\varepsilon \in \mathbb{N}$ tal que para todo $n, m > n_\varepsilon$ se cumple

$$\|a_n - a_m\| < \varepsilon.$$

3.2. Completación: Definición y propiedades

Definición 3.2.1. Un anillo normado $(R, \|\cdot\|)$ en el que toda sucesión de Cauchy es convergente es un anillo *completo* respecto a la norma $\|\cdot\|$.

La siguiente proposición es del ámbito del cálculo real. Por ello no la demostraremos.

Proposición 3.2.2. $\mathbb{R}$ *es completo respecto a el valor absoluto.*

De el hecho que $\mathbb{R}$ sea completo respecto al valor absoluto se deduce lo siguiente:

Proposición 3.2.3. *Sean $(R, \|\cdot\|)$ un anillo normado y $(a_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy en R. La sucesión $(\|a_n\|)_{n\in\mathbb{N}}$ tiene límite en $(\mathbb{R}, |\cdot|)$.*

Demostración. Veamos cómo la sucesión $(\|a_n\|)_{n\in\mathbb{N}}$ es una sucesión de Cauchy en $\mathbb{R}$, y por lo tanto tiene límite. Sea $\varepsilon > 0$, como $(a_n)_{n\in\mathbb{N}}$ es de Cauchy, existe $n_\varepsilon \in \mathbb{N}$ tal que para todo $n > n_\varepsilon$ se cumple

$$\|a_m - a_n\| < \varepsilon.$$

Por la desigualdad triangular inversa

$$\big|\|a_m\| - \|a_n\|\big| < \|a_m - a_n\| < \varepsilon.$$

Como consecuencia $(\|a_n\|)_{n\in\mathbb{N}}$ es una sucesión de Cauchy en $\mathbb{R}$ y por ser $\mathbb{R}$ completo respecto a $|\cdot|$, $(\|a_n\|)_{n\in\mathbb{N}}$ es convergente. □

Una completación de un anillo normado $(R, \|\cdot\|)$ será otro anillo normado $\big(\widehat{R}, \|\cdot\|\big)$ donde $R \subseteq \widehat{R}$ y toda sucesión de Cauchy de $\widehat{R}$ tenga límite. Por ejemplo, $\mathbb{R}$ es la completación de $\mathbb{Q}$ respecto al valor absoluto.

Definamos de una manera matemática esta idea y veamos sus propiedades.

Definición 3.2.4. Sea $(R, \|\cdot\|)$ un anillo normado. Una *completación* $\widehat{R}$ de R respecto a $\|\cdot\|$ es un anillo que junto al homomorfismo de anillos:

$$\begin{aligned} i\colon R &\longrightarrow \widehat{R} \\ a &\longmapsto i(a) = \widehat{a}. \end{aligned}$$

cumple las siguientes propiedades:

(C1) Existe una norma en $\widehat{R}$, que se denota con $\|\cdot\|$, tal que $\|i(a)\| = \|a\|$. para todo $a \in R$.

(C2) $i(R)$ es *denso* en $\widehat{R}$, es decir, para todo $x \in \widehat{R}$, existe una sucesión $(a_n)_{n\in\mathbb{N}}$ en R cuyo límite en $\widehat{R}$ es x.

(C3) $\widehat{R}$ es *completo*, es decir, toda sucesión de Cauchy en $\widehat{R}$ tiene límite.

Proposición 3.2.5. *Sean $(R, \|\cdot\|)$ un anillo normado y $\widehat{R}$ su completación respecto a $\|\cdot\|$. El homomorfismo i es inyectivo.*

Demostración. Por (C1) tenemos que

$$\widehat{a} = 0 \iff \|\widehat{a}\| = 0 \iff \|a\| = 0 \iff a = 0.$$

Por lo que es un homomorfismo inyectivo. □

Lema 3.2.6. *Sean $(R, \|\cdot\|)$ un anillo normado, $\widehat{R}$ su completación respecto a $\|\cdot\|$ y $(a_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy en R. Tenemos que*

$$\Big\|\lim_{n\to\infty} \widehat{a_n}\Big\| := \lim_{n\to\infty} \|a_n\|.$$

Demostración. Como $(a_n)_{n\in\mathbb{N}}$ es de Cauchy, por la Proposición 3.2.3 es convergente en $\mathbb{R}$ y por (C3) $(\widehat{a_n})_{n\in\mathbb{N}}$ es convergente en $\widehat{R}$.

Además, por (C1) es claro que $\lim_{n\to\infty} \|a_n\| = \lim_{n\to\infty} \|\widehat{a_n}\|$. Como por la Proposición 1.2.6 $\|\cdot\|$ es continua en la topología que induce, se cumple que $\lim_{n\to\infty} \|\widehat{a_n}\| = \|\lim_{n\to\infty} \widehat{a_n}\|$. En consecuencia

$$\Big\|\lim_{n\to\infty} \widehat{a_n}\Big\| = \lim_{n\to\infty} \|a_n\|.$$

□

Teorema 3.2.7 (Unicidad). *Si existen $\widehat{R}$ y $\overline{R}$, dos complementaciones respecto a una misma norma de un anillo R, entonces existe un isomorfismo $f\colon \widehat{R} \to \overline{R}$ tal que $\|f(\widehat{a})\| = \|\overline{a}\|$ para todo $a \in R$.*

Demostración. Definamos los homomorfismos de las completaciones $\widehat{R}$ y $\overline{R}$.

$$i\colon R \longrightarrow \widehat{R}, \quad a \longmapsto \widehat{a}.$$

$$j\colon R \longrightarrow \overline{R}, \quad a \longmapsto \overline{a}.$$

Definamos f. Sea $x \in \widehat{R}$. Tenemos dos opciones:

Si $x \in i(R)$, entonces $x = \widehat{a}$ para algún $a \in R$ y $f(x) = f(\widehat{a}) = j(a) = \overline{a}$. En otro caso, por (C2) existe una sucesión $(a_n)_{n\in\mathbb{N}}$ de R tal que $x = \lim_{n\to\infty} \widehat{a_n}$. Como $(\widehat{a_n})_{n\in\mathbb{N}}$ es convergente en $\widehat{R}$, es una sucesión de Cauchy, y como $\|\widehat{a}\| = \|a\| = \|\overline{a}\|$, $(\overline{a_n})_{n\in\mathbb{N}}$ también lo será, ya que al ser i y j homomorfismos, si $a_n - a_m \in R$ se cumple lo siguiente

$$\|\widehat{a_n} - \widehat{a_m}\| = \|\widehat{a_n - a_m}\| = \|a_n - a_m\| = \|\overline{a_n - a_m}\| = \|\overline{a_n} - \overline{a_m}\|.$$

Y por (C3) $\overline{R}$ es completo, luego existe $f(x) := \lim_{n\to\infty} \overline{a_n}$.

Primero veamos como mantiene la norma. Si $x = \lim_{n\to\infty} \overline{a_n} \in \widehat{R}$, por el Lema 3.2.6 tenemos que

$$\|x\| = \left\|\lim_{n\to\infty} \widehat{a_n}\right\| = \lim_{n\to\infty} \|\widehat{a_n}\| = \lim_{n\to\infty} \|\overline{a_n}\| = \left\|\lim_{n\to\infty} \overline{a_n}\right\| = \|f(x)\|$$

Por ello, tenemos lo siguiente:

$$x = 0 \iff \|x\| = 0 \iff \|f(x)\| = 0 \iff f(x) = 0$$

De lo que deducimos que f está bien definida y además es inyectiva.

Veamos como f es un homomorfismo entre anillos:

Usando la Proposición 3.1.2 tenemos que para todo $a = \lim_{n\to\infty} \widehat{a_n}$, $b = \lim_{n\to\infty} \widehat{b_n} \in \widehat{R}$.

$$\begin{aligned}
f(a \pm b) &= f\left(\left(\lim_{n\to\infty} \widehat{a_n}\right) \pm \left(\lim_{n\to\infty} \widehat{b_n}\right)\right) = f\left(\lim_{n\to\infty} \left(\widehat{a_n} \pm \widehat{b_n}\right)\right) \\
&= f\left(\lim_{n\to\infty} \widehat{a_n \pm b_n}\right) = \lim_{n\to\infty} \overline{a_n \pm b_n} = \lim_{n\to\infty} (\overline{a_n} \pm \overline{b_n}) \\
&= \left(\lim_{n\to\infty} \overline{a_n}\right) \pm \left(\lim_{n\to\infty} \overline{b_n}\right) = f\left(\lim_{n\to\infty} \widehat{a_n}\right) \pm f\left(\lim_{n\to\infty} \widehat{b_n}\right) \\
&= f(a) + f(b).
\end{aligned}$$

Análogamente, $f(ab) = f(a)f(b)$.

Como $1 \in R$, $f(1) = f(\widehat{1}) = \overline{1} = 1$. Por lo que, queda demostrado que es un homomorfismo. Para demostrar que es un isomorfismo de anillos sólo nos queda demostrar que es sobreyectiva. Sea $y \in \overline{R}$. Como $\overline{R}$ es completo, $y = \lim_{n\to\infty} \overline{a_n}$ por alguna sucesión $(a_n)_{n\in\mathbb{N}}$ de R. Como $\widehat{R}$ es completo $\lim_{n\to\infty} \widehat{a_n} =: x \in \widehat{R}$ existe, y por definición tenemos que $f(x) = y$. Es decir, f es sobreyectiva. ∎

Proposición 3.2.8. *Sean $(R, \|\cdot\|)$ un anillo normado y $\widehat{R}$ su completación respecto a $\|\cdot\|$. La norma $\|\cdot\|$ es no arquimediana respecto a R si y sólo si la norma extendida tampoco lo es respecto a $\widehat{R}$.*

Demostración. ($\Rightarrow$) Sean $x, y \in \widehat{R}$ cualesquiera. Como R es denso en $\widehat{R}$ existen dos sucesiones $(a_n)_{n\in\mathbb{N}}$ y $(b_n)_{n\in\mathbb{N}}$ en R que convergen a x e y respectivamente. Por lo tanto, al ser $\|\cdot\|$ no arquimediana en R,

$$\begin{aligned}\|x+y\| &= \left\|\left(\lim_{n\to\infty} a_n\right) + \left(\lim_{n\to\infty} b_n\right)\right\| = \|\lim_{n\to\infty}(a_n+b_n)\| = \lim_{n\to\infty}\|a_n+b_n\| \\ &\le \lim_{n\to\infty}\max\{\|a_n\|,\|b_n\|\} = \max\{\lim_{n\to\infty}\|a_n\|, \lim_{n\to\infty}\|b_n\|\} \\ &= \max\{\|\lim_{n\to\infty} a_n\|, \|\lim_{n\to\infty} b_n\|\} = \max\{\|x\|,\|y\|\}.\end{aligned}$$

($\Leftarrow$) Como $i(R)$ es un subanillo de $\widehat{R}$, para todo $a, b \in R$,

$$\|a-b\| = \|\widehat{a-b}\| = \|\widehat{a}-\widehat{b}\| \le \max\{\|\widehat{a}\|,\|\widehat{b}\|\} = \max\{\|a\|,\|b\|\}. \quad \square$$

3.3. Completación: Construcción

Aunque en general sea suficiente con imaginarnos que la completación existe, vamos a dar una expresión de ésta.

Lema 3.3.1. *Sea R un anillo normado. El conjunto*

$$SC(R) = \{(a_n)_{n\in\mathbb{N}} \subseteq R \mid (a_n)_{n\in\mathbb{N}} \text{ es de Cauchy en } R\}$$

es un anillo conmutativo respecto a las siguientes operaciones

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n+b_n)_{n\in\mathbb{N}},$$

$$(a_n)_{n\in\mathbb{N}}(b_n)_{n\in\mathbb{N}} = (a_nb_n)_{n\in\mathbb{N}}.$$

Además, $0 = (0,0,\dots)$ y $1 = (1,1,\dots)$ son el elemento neutro y unitario respectivamente.

Demostración. Para empezar, veamos como las operaciones definidas son cerradas en $SC(R)$.

Sean $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$, dos sucesiones de Cauchy en R. Tenemos que para todo $\varepsilon > 0$ existen $n_1, n_2 \in \mathbb{N}$ tales que para todo $n, m > n_\varepsilon = \max\{n_1, n_2\}$ se cumple

$$\|a_n - a_m\| < \frac{\varepsilon}{2} \quad \text{y} \quad \|b_n - b_m\| < \frac{\varepsilon}{2}.$$

Por lo que, si tomamos la sucesión $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n+b_n)_{n\in\mathbb{N}}$,

$$\begin{aligned}\|(a_n+b_n)-(a_m+b_m)\| &= \|(a_n-a_m)+(b_n-b_m)\| \\ &\le \|a_n-a_m\| + \|b_n-b_m\| < \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon.\end{aligned}$$

En conclusión $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy y la suma es una operación cerrada.

Por otro lado, veamos como $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} \in SC(R)$. Por el Corolario 3.2.3 sabemos que, como $(a_n)_{n\in\mathbb{N}}$ y $(b_n)_{n\in\mathbb{N}}$ son sucesiones de Cauchy en R, las sucesiones $(\|a_n\|)_{n\in\mathbb{N}}$ y $(\|b_n\|)_{n\in\mathbb{N}}$ son convergentes en $\mathbb{R}$. Tomemos a y b los limites respectivos de $(\|a_n\|)_{n\in\mathbb{N}}$ y $(\|b_n\|)_{n\in\mathbb{N}}$. Sean $n_1, n_2 \in \mathbb{N}$ tales que para todo $n > n_1$ y $n' > n_2$ se cumple

$$\big|\|a_n\| - a\big| < 1 \quad \text{y} \quad \big|\|b_{n'}\| - b\big| < 1.$$

Tomemos $n_3, n_4 \in \mathbb{N}$ tales que para todo $n, m > n_3$ y $n', m' > n_4$ se cumple que

$$\|a_n - a_m\| < \frac{\varepsilon}{2(1+|b|)} \quad \text{y} \quad \|b_{n'} - b_{m'}\| < \frac{\varepsilon}{2(1+|a|)}.$$

Si definimos $n_\varepsilon = \max\{n_1, n_2, n_3, n_4\}$, entonces, para todo $n, m > n_\varepsilon$ se tiene que

$$\begin{aligned}
\|a_nb_n - a_mb_m\| &= \|a_nb_n - a_mb_n + a_mb_n - a_mb_m\| \\
&\leq \|b_n\|\|a_n - a_m\| + \|a_m\|\|b_n - b_m\| \\
&= \big|\|b_n\| - b + b\big|\|a_n - a_m\| + \big|\|a_m\| - a + a\big|\|b_n - b_m\| \\
&\leq \big(\big|\|b_n\| - b\big| + |b|\big)\|a_n - a_m\| + \big(\big|\|a_m\| - a\big| + |a|\big)\|b_n - b_m\| \\
&< (1+|b|)\frac{\varepsilon}{2(1+|b|)} + (1+|a|)\frac{\varepsilon}{2(1+|a|)} = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon
\end{aligned}$$

En consecuencia, $(a_n)_{n\in\mathbb{N}}(b_n)_{n\in\mathbb{N}} \in SC(R)$ y el producto es una operación cerrada.

Por otra parte, la suma de $SC(R)$ hereda de la suma de R la propiedad asociativa y conmutativa. También hereda el elemento neutro $(0, 0, \dots)$. Para cada sucesión de Cauchy $(a_n)_{n\in\mathbb{N}}$ es claro que $(-a_n)_{n\in\mathbb{N}} + (a_n)_{n\in\mathbb{N}} = (0, 0, \dots)$ y $(-a_n)_{n\in\mathbb{N}} = (-1, -1, \dots)_{n\in\mathbb{N}}(a_n)_{n\in\mathbb{N}}$ que por ser el producto cerrado es un elemento de $SC(R)$. Por lo tanto, $(SC(R), +)$ es un grupo abeliano.

Para que $(SC(R), +, \cdot)$ sea un anillo cunmutativo, nos queda por demostrar que el producto es asociativo y conmutativo y que la suma y el producto son asociativos. Es sencillo demostrar que estas propiedades se heredan de la suma y el producto del anillo conmutativo R. Además si el elemento neutro de R es 1, entonces, el elemento neutro de $SC(R)$ es $(1, 1, \dots)$. □

Lema 3.3.2. *La aplicación $i : R \to SC(R)$, $a \mapsto (a)_{n\in\mathbb{N}} = (a, a, \dots)$ es un homomorfismo inyectivo.*

Demostración. Veamos que es un homomorfismo de anillos,

- $i(a + b) = (a + b)_{n\in\mathbb{N}} = (a)_{n\in\mathbb{N}} + (b)_{n\in\mathbb{N}} = i(a) + i(b)$.

- $i(ab) = (ab)_{n\in\mathbb{N}} = (a)_{n\in\mathbb{N}}(b)_{n\in\mathbb{N}} = i(a)i(b)$.
- $i(1) = (1)_{n\in\mathbb{N}}$.

Por lo que efectivamente es un homomorfismo. Por otro lado, es claro que i es inyectiva. □

La norma $\|\cdot\|$ de R se puede extender a $SC(R)$ del siguiente modo:

$$\|(a_n)_{n\in\mathbb{N}}\| := \lim_{n\to\infty} \|a_n\|.$$

Según el Corolario 3.2.3 este límite existirá por ser $(a_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy. Aun así, para que esta expresión defina una norma sobre $SC(R)$ tiene que cumplir los axiomas de la definición 1.2.1. El axioma (N1) no lo cumple, ya que puede existir una sucesión $(a_n)_{n\in\mathbb{N}} \neq (0, 0, \dots)$ que cumple lo siguiente,

$$\lim_{n\to\infty} \|a_n\| = 0 \in \mathbb{R}.$$

En consecuencia, aunque la sucesión no sea el elemento nulo, tiene norma 0. Para resolver esto, vamos a considerar nulas todas las sucesiones que cumplan eso.

Definición 3.3.3. Una sucesión $(a_n)_{n\in\mathbb{N}}$ es *nula* si $\lim_{n\to\infty} \|a_n\| = 0$.

Lema 3.3.4. *Las sucesiones nulas en R forman un ideal $N(R)$ del anillo $SC(R)$.*

Demostración. Veamos cómo cumple las dos condiciones para ser ideal:

Sean $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in N(R)$, se tiene

$$0 \le \lim_{n\to\infty} \|a_n + b_n\| \le \lim_{n\to\infty} \|a_n\| + \|b_n\| = \lim_{n\to\infty} \|a_n\| + \lim_{n\to\infty} \|b_n\| = 0 + 0.$$

Luego $\lim_{n\to\infty} \|a_n + b_n\| = 0$ y por tanto $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} \in N(R)$.

Sean $(a_n)_{n\in\mathbb{N}} \in N(R)$ y $(b_n)_{n\in\mathbb{N}} \in SC(R)$, como por la Proposición 3.2.3 $(\|b_n\|)_{n\in\mathbb{N}}$ es convergente en $k \in R$,

$$0 \le \lim_{n\to\infty} \|a_n b_n\| = \lim_{n\to\infty} \|a_n\|\|b_n\| = \lim_{n\to\infty} \|a_n\| \lim_{n\to\infty} \|b_n\| = 0 \cdot k = 0.$$

Por lo que $(a_n)_{n\in\mathbb{N}}(b_n)_{n\in\mathbb{N}} \in N(R)$. □

Como es un ideal, podremos trabajar con el anillo $\frac{SC(R)}{N(R)}$ en el que podremos definir la norma anteriormente introducida sin ningún problema. Pero antes observemos como la extensión del homeomorfismo definido en el Lema 3.3.2 sigue siendo un homeomorfismo inyectivo.

Lema 3.3.5. *La aplicación $i\colon R \to \frac{SC(R)}{N(R)}$, $a \mapsto (a)_{n\in\mathbb{N}} + N(R)$ es un homeomorfismo inyectivo.*

Demostración. Es claro que i sigue cumpliendo las condiciones para ser un homeomorfismo, por lo que sólo demostraremos que es inyectiva. Sean $a, b \in R$. Si $i(a) = i(b)$ entonces $N(R) = i(a) - i(b) = (a)_{n\in\mathbb{N}} + N(R) - (b)_{n\in\mathbb{N}} + N(R) = (a-b)_{n\in\mathbb{N}} + N(R)$, y $(a-b)_{n\in\mathbb{N}} \in N(R)$, es decir, $a = b$. $\square$

Lema 3.3.6. *Toda norma sobre el anillo R se puede extender a la siguiente norma sobre $\frac{SC(R)}{N(R)}$:*

$$\|(a_n)_{n\in\mathbb{N}}\| = \lim_{n\to\infty} \|a_n\|.$$

Demostración. Antes de ver que cumple con los axiomas veamos como está bien definido. Si dos sucesiones $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in SC(R)$ cumplen que $(a_n)_{n\in\mathbb{N}} + N(R) = (b_n)_{n\in\mathbb{N}} + N(R)$, entonces

$$(a_n - b_n)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} - (b_n)_{n\in\mathbb{N}} \in N(R) \implies \lim_{n\to\infty} \|a_n - b_n\| = 0.$$

Además por la desigualdad triangular inversa, tenemos que

$$\big|\|a_n\| - \|b_n\|\big| \leq \|a_n - b_n\|.$$

Por lo que,

$$\big|\lim_{n\to\infty} \|a_n\| - \lim_{n\to\infty} \|b_n\|\big| = \lim_{n\to\infty} \|a_n - b_n\| = 0.$$

En consecuencia, $\|(a_n)_{n\in\mathbb{N}}\| = \lim_{n\to\infty} \|a_n\| = \lim_{n\to\infty} \|b_n\| = \|(b_n)_{n\in\mathbb{N}}\|$ y la función que hemos definido está bien definida. Ahora veamos como cumple los axiomas para ser una norma.

(N1) Por cómo hemos definido $N(R)$ es claro que $\|(a_n)_{n\in\mathbb{N}}\| = 0$ si y sólo si $(a_n)_{n\in\mathbb{N}} \in N(R)$.

(N2) Tenemos que

$$\begin{aligned}\|(a_n)_{n\in\mathbb{N}}(b_n)_{n\in\mathbb{N}}\| &= \|(a_nb_n)_{n\in\mathbb{N}}\| = \lim_{n\to\infty} \|a_nb_n\| = \lim_{n\to\infty} \|a_n\| \lim_{n\to\infty} \|b_n\| \\ &= \|(a_n)_{n\in\mathbb{N}}\|\|(b_n)_{n\in\mathbb{N}}\|.\end{aligned}$$

(N3) Concluyendo,

$$\begin{aligned}\|(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}}\| = \|(a_n + b_n)_{n\in\mathbb{N}}\| &= \lim_{n\to\infty} \|a_n + b_n\| \\ &\leq \lim_{n\to\infty} \|a_n\| + \|b_n\| = \lim_{n\to\infty} \|a_n\| + \lim_{n\to\infty} \|b_n\| \\ &= \|(a_n)_{n\in\mathbb{N}}\| + \|(b_n)_{n\in\mathbb{N}}\|.\end{aligned}$$ $\square$

Para demostrar que $\frac{SC(R)}{N(R)}$ es la completación de $i(R)$ tenemos que ver que se cumplen los axiomas (C2) y (C3) de la Definición 3.2.4.

Lema 3.3.7. *El subanillo $i(R) \subseteq \frac{SC(R)}{N(R)}$ es denso en $\frac{SC(R)}{N(R)}$.*

Demostración. Sea $(a_n)_{n\in\mathbb{N}} \in \frac{SC(R)}{N(R)}$ una sucesión de Cauchy en R, tenemos que encontrar una sucesión de elementos de $i(R)$ que converja en $(a_n)_{n\in\mathbb{N}}$.

Sea $m \in \mathbb{N}$ fijo, como $a_m \in R$ $\widehat{a_m} = (a_m, a_m, \dots) \in i(R)$. Definamos la sucesión $(\widehat{a_m})_{n\in\mathbb{N}}$ y veamos cómo converge a $(a_n)_{n\in\mathbb{N}}$.

$$\lim_{m\to\infty} \widehat{a_m} = (a_n)_{n\in\mathbb{N}} \iff \lim_{m\to\infty} \|\widehat{a_m} - (a_n)_{n\in\mathbb{N}}\| = 0.$$

Calculemos este límite.

$$\lim_{m\to\infty} \|\widehat{a_m} - (a_n)_{n\in\mathbb{N}}\| = \lim_{m\to\infty} \left(\lim_{n\to\infty} \|a_m - a_n\| \right),$$

que por ser $(a_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy es 0. □

Lema 3.3.8. *El anillo $\frac{SC(R)}{N(R)}$ es completo respecto a la norma $\|\cdot\|$.*

Demostración. Sea $(x_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy en $\frac{SC(R)}{N(R)}$. Para un $m \in \mathbb{N}$ fijo x_m es una clase de equivalencia y se puede representar con $\big((a_m)_n\big)_{n\in\mathbb{N}}$, una sucesión de Cauchy en R.

Como hemos visto en la demostración del Lema 3.3.7, $\big(\widehat{(a_m)_k}\big)_{k\in\mathbb{N}}$ converge en $\frac{SC(R)}{N(R)}$ a $x_m = \big((a_m)_n\big)_{n\in\mathbb{N}}$. En consecuencia, por la definición de límite, existe $k_m \in \mathbb{N}$ tal que para todo $k \geq k_m$, se cumple lo siguiente:

$$\|x_m - \widehat{(a_m)_k}\| < \tfrac{1}{m}.$$

Es claro que en estas circunstancias se cumple lo que:

$$k_1 < k_2 < \dots$$

Teniendo en cuenta esto, definamos la sucesión $(c_n)_{n\in\mathbb{N}}$ del siguiente modo:

$$c_n = (a_n)_{k_n}.$$

Veamos cómo $(c_n)_{n\in\mathbb{N}}$ es un elemento de $\frac{SC(R)}{N(R)}$. Sea $\varepsilon > 0$, por cómo está definida la sucesión, podemos tomar $m_1 \in \mathbb{N}$ tal que $\frac{1}{m_1} < \frac{\varepsilon}{3}$. Por lo que, para toda $n_1, n_2 > m_1$, se cumple lo siguiente:

$$\|x_{n_1} - \widehat{c_{n_1}}\| = \|x_{n_1} - \widehat{(a_{n_1})_{k_{n_1}}}\| < \tfrac{1}{n_1} < \tfrac{1}{m_1} < \tfrac{\varepsilon}{3}.$$

$$\|x_{n_2} - \widehat{c_{n_2}}\| = \|x_{n_2} - \widehat{(a_{n_2})_{k_{n_2}}}\| < \tfrac{1}{n_2} < \tfrac{1}{m_1} < \tfrac{\varepsilon}{3}.$$

Además, al ser $(x_m)_{m\in\mathbb{N}}$ una sucesión de Cauchy, existe $m_2 \in \mathbb{N}$ tal que, para todo $n_1, n_2 > m_2$, se tenemos lo siguiente:

$$\|x_{n_1} - x_{n_2}\| < \tfrac{\varepsilon}{3}.$$

Es claro que si tomamos $m = \text{máx}\{m_1, m_2\}$, para todo $n_1, n_2 > m$ se cumplen las tres desigualdades. Por ello tenemos lo siguiente:

$$\begin{aligned}
\|c_{n_1} - c_{n_2}\| = \|\widehat{c_{n_1} - c_{n_2}}\| = \|\widehat{c_{n_1}} - \widehat{c_{n_2}}\| &= \|\widehat{(a_{n_1})_{k_{n_1}}} - \widehat{(a_{n_2})_{k_{n_2}}}\| \\
&= \|\widehat{(a_{n_1})_{k_{n_1}}} - x_{n_1} + x_{n_1} - x_{n_2} + x_{n_2} - \widehat{(a_{n_2})_{k_{n_2}}}\| \\
&\leq \|\widehat{(a_{n_1})_{k_{n_1}}} - x_{n_1}\| + \|x_{n_1} - x_{n_2}\| + \|x_{n_2} - \widehat{(a_{n_2})_{k_{n_2}}}\| \\
&< \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon.
\end{aligned}$$

Por lo que $(c_n)_n$ es una sucesión de Cauchy sobre R y es un elemento de$\frac{SC(R)}{N(R)}$. Ahora veamos cómo $(c_n)_{n\in\mathbb{N}}$ es el límite de $(x_m)_{m\in\mathbb{N}}$. Sea $\varepsilon > 0$. Tomemos $m_0 \in \mathbb{N}$ tal que, $\frac{1}{m_0} < \frac{\varepsilon}{2}$. Entonces, para todo $m > m_0$ se tiene que

$$\|x_m - \widehat{(a_m)_{k_m}}\| < \tfrac{1}{m} < \tfrac{\varepsilon}{2}.$$

Por otro lado, como $(c_n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy, existe $N \in \mathbb{N}$ tal que para todo $m, n > N$ se cumple que:

$$\|c_n - c_m\| < \tfrac{\varepsilon}{2}.$$

Por lo tanto,

$$\|(c_n)_{n\in\mathbb{N}} - \widehat{(a_m)_{k_m}}\| = \|(c_n)_{n\in\mathbb{N}} - \widehat{c_m}\| = \lim_{n\to\infty} \|c_n - c_m\| < \tfrac{\varepsilon}{2}.$$

Si tomamos $m = \text{máx}\{m_1, N\}$, entonces

$$\begin{aligned}
\|(c_n)_{n\in\mathbb{N}} - x_m\| &= \|(c_n)_{n\in\mathbb{N}} - \widehat{(a_m)_{k_m}} + \widehat{(a_m)_{k_m}} - x_m\| \\
&\leq \|(c_n)_{n\in\mathbb{N}} - \widehat{(a_m)_{k_m}}\| + \|\widehat{(a_m)_{k_m}} - x_m\| \\
&< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon.
\end{aligned}$$

En consecuencia $(c_n)_{n\in\mathbb{N}}$ es el límite de $(x_m)_{m\in\mathbb{N}}$. □

Si resumimos todo lo visto hasta ahora tenemos el siguiente teorema.

Teorema 3.3.9. *Sea $(R, \|\cdot\|)$ un anillo. Su completación respecto a la norma $\|\cdot\|$ es el anillo $\frac{SC(R)}{N(R)}$ con norma*

$$\|(a_n)_{n\in\mathbb{N}}\| = \lim_{n\to\infty} \|a_n\|,$$

donde la inclusión de R en $\frac{SC(R)}{N(R)}$ es la función $a \mapsto (a, a, \dots)$.

Capítulo 4

Equivalencias de normas y el Teorema de Ostrowski

4.1. Equivalencias de normas

Definición 4.1.1. Sean X y τ_1, τ_2 dos topologías sobre X con bases de abiertos β_1 y β_2 respectivamente. τ_1 y τ_2 son *equivalentes* si todo $B_1 \in \beta_1$ es abierto en τ_2 y viceversa.

Definición 4.1.2. Sean R un anillo conmutativo y $\|\cdot\|_1, \|\cdot\|_2$ dos normas sobre éste. Se dice que las dos normas son topológicamente equivalentes si las bases de abiertos que éstas inducen son equivalentes, y se denota de la siguiente forma:

$$\|\cdot\|_1 \sim \|\cdot\|_2.$$

Proposición 4.1.3. *Dos normas $\|\cdot\|_1$ y $\|\cdot\|_2$ sobre un anillo conmutativo R son topológicamente equivalentes si y solo si para todo $x \in R$ y para todo $r > 0$ existen $r_1, r_2 > 0$ que cumplen lo siguiente:*

$$B_1(x, r_1) \subseteq B_2(x, r) \quad y \quad B_2(x, r_2) \subseteq B_1(x, r),$$

siendo $B_1(x, r)$ y $B_2(x, r)$ las bolas abiertas centradas en x y de radio r respecto a las normas $\|\cdot\|_1$ y $\|\cdot\|_2$ respectivamente.

Demostración. Sólo demostraremos la existencia de r_1 ya que la demostración de la existencia de r_2 es análoga.

Recordemos que las bases inducidas a partir de $\|\cdot\|_1$ y $\|\cdot\|_2$ son

$$\beta_1 = \{B_1(x, r) \mid x \in X,\ r > 0\} \text{ y } \beta_2 = \{B_2(x, r) \mid x \in X,\ r > 0\},$$

respectivamente. Si β_1 y β_2 son topológicamente equivalentes, toda bola abierta $B_2(x, r)$ respecto a $\|\cdot\|_2$ es abierta en τ_1. Por ello, como $x \in B_2(x, r)$ existen $y \in B_2(x, r_2)$ y $r_1' > 0$ tal que $x \in B_1(y, r_1') \subseteq B_2(x, r)$.

Definamos $r_1 := r_1' - d_1(x,y) > 0$, y comprobemos como $B_1(x,r_1) \subseteq B_2(x,r)$

$$d_1(z,y) \leq d_1(z,x) + d_1(x,y) < r_1 + d_1(x,y) = r_1'.$$

Por lo que $z \in B_1(y, r_1') \subseteq B_2(x,r)$ y $B_1(x,r_1) \subseteq B_2(x,r)$.

Por otro lado, supongamos que para todo $x \in R$ y todo $r > 0$ existen $r_1, r_2 > 0$ que cumplen

$$B_1(x,r_1) \subseteq B_2(x,r) \quad \text{y} \quad B_2(x,r_2) \subseteq B_1(x,r).$$

Para todo $y \in B_2(x,r)$, si tomamos $r_0 = r - d_2(x,y) > 0$ entonces, $B_2(y,r_0) \subseteq B_2(x,r)$. Por hipotesis, existe $r_1 > 0$ tal que $B_1(y,r_1) \subseteq B_2(y,r_0) \subseteq B_2(x,r)$ y, en consecuencia, $B_2(x,r)$ es abierto en τ_1. La demostración de que $B_1(x,r)$ es abierto en τ_2 es análoga. □

Proposición 4.1.4. *Si dos normas $\|\cdot\|_1$ y $\|\cdot\|_2$ sobre un anillo conmutativo R son equivalentes, entonces, una sucesión converge a un elemento en $(R, \|\cdot\|_1)$ si y solo si converge al mismo elemento en $(R, \|\cdot\|_2)$.*

Demostración. Supongamos que $\|\cdot\|_1 \sim \|\cdot\|_2$ y demostremos que si una sucesión $(a_n)_{n\in\mathbb{N}}$ de elementos de R converge al elemento $a \in R$ respecto a $\|\cdot\|_1$, entonces también lo hace respecto a $\|\cdot\|_2$.

Para todo $r > 0$, por la Proposición 4.1.3 existe $r_1 > 0$ tal que $B_1(a,r_1) \subseteq B_2(a,r)$. Como $(a_n)_{n\in\mathbb{N}}$ converge a a respecto a $\|\cdot\|_1$ existe $n_r \in \mathbb{N}$ tal que para todo $n > n_r$ tenemos que $a_n \in B_1(a,r_1) \subseteq B_2(a,r)$. Por lo que $(a_n)_{n\in\mathbb{N}}$ converge a a respecto a $\|\cdot\|_2$. □

Teorema 4.1.5 (Caracterización de equivalencia de normas). *Sea $\mathbb{K}$ un cuerpo y $\|\cdot\|_1$, $\|\cdot\|_2$ dos normas sobre éste. Las siguientes afirmaciones son equivalentes:*

(1) *$\|\cdot\|_1$ y $\|\cdot\|_2$ son topológicamente equivalentes.*

(2) *Para todo $x \in \mathbb{K}$, se cumple:*

$$\|x\|_1 < 1 \iff \|x\|_2 < 1.$$

(2') *Para todo $x \in \mathbb{K}$ se cumple:*

$$\begin{aligned} \|x\|_1 < 1 &\iff \|x\|_2 < 1, \\ \|x\|_1 = 1 &\iff \|x\|_2 = 1, \\ \|x\|_1 > 1 &\iff \|x\|_2 > 1. \end{aligned}$$

(3) *Existe $\alpha > 0$ tal que para todo $x \in \mathbb{K}$, $\|x\|_1 = \|x\|_2^{\alpha}$.*

(4) *Toda sucesión sobre $\mathbb{K}$ es de Cauchy respecto a $\|\cdot\|_1$ si y solo si es de Cauchy respecto a $\|\cdot\|_2$.*

Demostración. (1) $\Longrightarrow$ (2) Basta con demostrar que para todo $x \in \mathbb{K}$, si $\|x\|_1 < 1$, entonces, $\|x\|_2 < 1$ ya que la otra implicación es análoga.

Sea $x \in \mathbb{K}$ tal que $\|x\|_1 < 1$, entonces, la sucesión $(x^n)_{n\in\mathbb{N}}$ converge a 0 respecto a $\|\cdot\|_1$ y por ser $\|\cdot\|_2 \sim \|\cdot\|_1$ también en $\|\cdot\|_2$ (ver Proposición 4.1.4). Por lo que existe $n \in \mathbb{N}$ tal que $\|x\|_2^n = \|x^n\|_2 < 1$ lo que implica que $\|x\|_2 < 1$.

(2) $\Longrightarrow$ (2') Supongamos que se cumple (2) y tomemos un elemento $x \in \mathbb{K}$ tal que $\|x\|_1 > 1$. Entonces, $\|x^{-1}\|_1 = \|x\|_1^{-1} < 1$, por lo que $\|x^{-1}\|_2 < 1$ y $\|x\|_2 = \|x\|_2^{-1} > 1$. Del mismo modo, si tomamos $y \in \mathbb{K}$ tal que $\|y\|_2 > 1$ se demuestra que $\|y\|_1 > 1$. Deducimos entonces que $\|y\|_1 = 1$ si y solo si $\|y\|_2 = 1$.

(2') $\Longrightarrow$ (3) La condición (3) se cumple trivialmente para todo $x \in \mathbb{K}$ tal que $\|x\|_1 = 1$ y para $x = 0$. Tomemos $x_0 \in \mathbb{K}$ tal que $\|x_0\|_1 \neq 1, 0$. Podemos definir α para que cumpla $\|x_0\|_1 = \|x_0\|_2^\alpha$,

$$\alpha = \frac{\log \|x_0\|_1}{\log \|x_0\|_2}.$$

Sea $x \in \mathbb{K} \setminus 0$ tal que $\|x\|_1 \neq \|x_0\|_1$ y $\|x\| \neq 1$ (en el caso de que no exista se cumple la propiedad (3) trivialmente). Veamos cómo $\|x\|_1 = \|x\|_2^\alpha$ o lo que es igual,

$$0\frac{\log \|x\|_1}{\log \|x\|_2} = \alpha = \frac{\log \|x_0\|_1}{\log \|x_0\|_2} \iff \frac{\log \|x_0\|_1}{\log \|x\|_1} = \frac{\log \|x_0\|_2}{\log \|x\|_2}.$$

Vamos a demostrar esta última igualdad por reducción al absurdo. Supongamos que $\frac{\log \|x_0\|_1}{\log \|x\|_1} \neq \frac{\log \|x_0\|_2}{\log \|x\|_2}$. Sin pérdida de generalidad, supongamos que $\frac{\log \|x_0\|_1}{\log \|x\|_1} < \frac{\log \|x_0\|_2}{\log \|x\|_2}$, entonces, al ser números reales existe un número racional $\frac{m}{n}$ tal que

$$0 < \frac{\log \|x_0\|_1}{\log \|x\|_1} < \frac{m}{n} < \frac{\log \|x_0\|_2}{\log \|x\|_2}.$$

Esto se cumple si y solo si

$$n \log \|x_0\|_1 < m \log \|x\|_1, \qquad m \log \|x\|_2 < n \log \|x_0\|_2,$$

es decir si y solo si

$$\|x_0\|_1^n < \|x\|_1^m, \qquad \|x\|_2^m < \|x_0\|_2^n.$$

Por tanto $\left\|\frac{x_0^n}{x^m}\right\|_1 < 1$ y $1 < \left\|\frac{x_0^n}{x^m}\right\|_2$, lo cual contradice a la hipótesis (2'). En consecuencia $\|x\|_1 = \|x\|_2^\alpha$.

(3) $\Longrightarrow$ (1) Si existe $\alpha > 0$ tal que para todo $x \in \mathbb{K}$ se cumple que $\|x\|_1 = \|x\|_2^\alpha$, entonces para todo $r > 0$ veamos como $B_2(x, r) = B_1(x, r^\alpha)$. Tenemos que

$$\begin{aligned} x_0 \in B_2(x, r) &\iff \|x - x_0\|_2 < r \iff \|x - x_0\|_1 = \|x - x_0\|_2^\alpha < r^\alpha \\ &\iff x_0 \in B_1(x, r^\alpha). \end{aligned}$$

En consecuencia, por la Proposición 4.1.3, tenemos que $\|\cdot\|_1 \sim \|\cdot\|_2$.

(3) $\Longrightarrow$ (4) Vamos a demostrar que suponiendo (3), si una sucesión es de Cauchy respecto a $\|\cdot\|_1$, entonces, también lo es respecto a $\|\cdot\|_2$. Sea $(a_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy respecto a $\|\cdot\|_1$, entonces

$$\forall \varepsilon > 0\ \exists n_\varepsilon \in \mathbb{N}\ \forall n, m > n_\varepsilon \qquad \|a_n - a_m\|_2^\alpha = \|a_n - a_m\|_1 < \varepsilon^\alpha,$$

es decir $\|a_n - a_m\|_2 < \varepsilon$. En conclusión, $(a_n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy respecto a $\|\cdot\|_2$.

(4) $\Longrightarrow$ (2) Suponiendo que se cumple (4) vamos a demostrar que para todo $x \in \mathbb{K}$, si $\|x\|_1 < 1$, entonces, $\|x\|_2 < 1$. La implicación contraria se demuestra con una demostración análoga.

Sea $x \in \mathbb{K}$ tal que $\|x\|_1 < 1$, entonces, definamos la sucesión $(x^n)_{n\in\mathbb{N}}$. Para $n > m > 0$, desarrollamos $\|x^n - x^m\|_1$:

$$\|x^n - x^m\|_1 = \|x\|_1^m \|x^{n-m} - 1\|_1 \leq \|x\|_1^m \big(\|x\|_1^{n-m} + 1\big) \leq 2\|x\|_1^m.$$

Cuando m tiende a ∞ la expresión $2\|x\|_1^m$ tiende a 0. En consecuencia $(x^n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy respecto a $\|\cdot\|_1$ y por (4) también respecto a $\|\cdot\|_2$. Por lo que, $(x^n)_{n\in\mathbb{N}}$ tiene límite respecto a la norma $\|\cdot\|_2$. Distinguimos tres casos:

- Si $\|x\|_2 > 1$, entonces, $(x^n)_{n\in\mathbb{N}}$ es divergente por lo que llegamos a un absurdo.
- Si $\|x\|_2 = 1$, entonces, como es una sucesión de Cauchy respecto a $\|\cdot\|_2$, cuando n tiende a ∞, el valor $\|x^n - x^{n+1}\|_2 = \|x\|_2^n \|1 - x\|_2 = \|1 - x\|_2$ tiende a 0. Por lo que, $x = 1$, lo cual es absurdo por que $\|x\|_1 \neq 1$.
- $\|x\|_2 < 1$ que es lo que queríamos demostrar. □

Observación 4.1.6. Esto sólo ocurre para un cuerpo y no para un anillo. Por ejemplo si tomamos la norma trivial y el valor absoluto en $\mathbb{Z}$ (ver Ejemplos 1.2.2), entonces, las dos inducen la topología discreta, por lo que serán topológicamente equivalentes pero (2') y (3) no se cumplen.

Corolario 4.1.7. *Sean $\|\cdot\|_1$ y $\|\cdot\|_2$ dos normas topológicamente equivalentes sobre un cuerpo $\mathbb{K}$. Entonces, $\|\cdot\|_1$ será trivial si y solo si $\|\cdot\|_2$ lo es.*

Demostración. Tomemos $x \in \mathbb{K}$ no nulo, entonces, si $\|\cdot\|_1$ es trivial, $\|x\|_1 = 1$ y por la propiedad (2') del Teorema 4.1.5 esto ocurre si y solo si $\|x\|_2 = 1$ es decir, si y solo si $\|\cdot\|_2$ es trivial. □

Corolario 4.1.8. *Si $\|\cdot\|_1$ y $\|\cdot\|_2$ son dos normas topológicamente equivalentes sobre un cuerpo $\mathbb{K}$, o bien ambas son arquimedianas o bien ambas no lo son.*

Demostración. $\|\cdot\|_1$ es no arquimediana si y solo si $\|n\|_1 \leq 1$ para todo $n \in \mathbb{N}$ (Proposición 2.2.4) y como son normas topológicamente equivalentes, esto ocurre si y solo si $\|n\|_2 \leq 1$ para todo $n \in \mathbb{N}$, es decir si y solo si $\|\cdot\|_2$ es no arquimediana. □

Proposición 4.1.9. *Sean $\|\cdot\|_1$ y $\|\cdot\|_2$ dos normas sobre un cuerpo $\mathbb{K}$. Si son topológicamente equivalentes entonces, las completaciones respecto a ambas normas $\widehat{\mathbb{K}}_1$ y $\widehat{\mathbb{K}}_2$ son la misma.*

Demostración. Si $\|\cdot\|_1$ y $\|\cdot\|_2$ son topológicamente equivalentes entonces, para toda sucesión $(a_n)_{n\in\mathbb{N}}$ de $\mathbb{K}$, ésta es una sucesión de Cauchy respecto a la norma $\|\cdot\|_1$ si y solo si lo es respecto a $\|\cdot\|_2$.

Supongamos que las dos normas son topológicamente equivalentes. Como hemos visto en el Teorema 3.3.9, $\mathbb{K}_1$ y $\mathbb{K}_2$ cumplen lo siguiente:

$$\mathbb{K}_1 \cong \frac{SC_1(\mathbb{K})}{N_1(\mathbb{K})}, \qquad\qquad \mathbb{K}_2 \cong \frac{SC_2(\mathbb{K})}{N_2(\mathbb{K})}.$$

Por el Teorema 4.1.5 tenemos que las suceciones en $\mathbb{K}$ que son de Cauchy respecto a la norma $\|\cdot\|_1$ y los que lo son respecto a $\|\cdot\|_2$ son las mismas. Además, por la Proposición 4.1.4 una sucesión es nula respecto a $\|\cdot\|_1$ si y solo si lo es respecto a $\|\cdot\|_2$. Por ello, $\frac{SC_1(\mathbb{K})}{N_1(\mathbb{K})} = \frac{SC_2(\mathbb{K})}{N_2(\mathbb{K})}$ y en consecuencia, $\mathbb{K}_1 \cong \mathbb{K}_2$. □

4.2. Teorema de Ostrowski

En este apartado vamos a trabajar con las normas sobre $\mathbb{Q}$. Vamos a ver cuáles son todas las normas que podemos generar en este cuerpo salvo equivalencias.

Lema 4.2.1. *Toda norma arquimediana sobre $\mathbb{Q}$ es topológicamente equivalente al valor absoluto.*

Demostración. Sea $\|\cdot\|$ una norma arquimediana sobre $\mathbb{Q}$. El objetivo de esta demostración es encontrar $\alpha \in \mathbb{R}$ tal que $\|n\| = |n|^\alpha = n^\alpha$ para todo $n \in \mathbb{N}$ para luego extender esta igualdad a todo $x \in \mathbb{Q}$, demostrando que las dos normas son topológicamente equivalentes.

Como la norma $\|\cdot\|$ es arquimediana, existe $n \in \mathbb{N}$ tal que $\|n\| > 1$ (Proposición 2.2.4), por lo que el conjunto $A = \{n \in \mathbb{N} \mid \|n\| > 1\}$ será no vacío, luego tiene un mínimo. Llamemos a este elemento n_0 y tomemos $\alpha = \frac{\log\|n_0\|}{\log n_0} \in \mathbb{R}$ tal que $\|n_0\| = n_0^\alpha$. Como $\|n_0\| > 1$ se tiene que $\alpha > 0$.

Para todo $n \in \mathbb{N}$ expresando n en base n_0 obtenemos que existen $s \in \mathbb{N}$ y $a_i \in \{0, \dots, n_0 - 1\}$ para cada $i \in \{0, \dots, s\}$ tales que

$$n = a_0 + a_1 n_0 + \cdots + a_s n_0^s, \qquad a_s \neq 0. \tag{4.1}$$

Así,

$$\|n\| \leq \|a_0\| + \|a_1\|\|n_0\| + \cdots + \|a_s\|\|n_0\|^s.$$

Como para todo $i \in \{0, \ldots, s\}$, $a_i \in \{0, \ldots, n_0 - 1\}$, entonces, $\|a_i\| \leq 1$, por lo que,

$$\begin{aligned}\|n\| &\leq 1 + \|n_0\| + \cdots + \|n_0\|^s = 1 + n_0^{\alpha} + \cdots + n_0^{s\alpha} \\ &= n_0^{s\alpha}\big(1 + n_0^{-\alpha} + \cdots + n_0^{-s\alpha}\big) = n_0^{s\alpha}\sum_{k=0}^{s}\frac{1}{n_0^{k\alpha}} \leq n_0^{s\alpha}\sum_{k=0}^{\infty}\big(\tfrac{1}{n_0^{\alpha}}\big)^k.\end{aligned}$$

Como $n_0 > 1$, $\frac{1}{n_0^{\alpha}} < 1$ y la serie geométrica converge a $C = \frac{n_0^{\alpha}}{n_0^{\alpha}-1}$, una constante que no depende de $n \in \mathbb{N}$. En conclusión, $\|n\| \leq n_0^{s\alpha}C$. Por otro lado, por como hemos escrito n (ver Ecuación (4.1)) $n \geq n_0^s$, entonces,

$$\|n\| \leq n^{\alpha}C.$$

Del mismo modo, si consideramos n^N en vez de n tenemos el siguiente resultado

$$\|n\|^N \leq n^{\alpha N}C \implies \|n\| \leq n^{\alpha}\sqrt[N]{C}.$$

Cuando N tiende a infinito tenemos lo siguiente:

$$\|n\| \leq n^{\alpha}. \tag{4.2}$$

Ahora nos toca demostrar la desigualdad contraria. Para cada $n \in \mathbb{N}$ existe $s \in \mathbb{N}$ tal que

$$n_0^s \leq n \leq n_0^{s+1}$$

(ver Ecuación (4.1)), luego,

$$\|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leq \|n\| + \|n_0^{s+1} - n\|. \tag{4.3}$$

Por lo que, si usamos las desigualdades demostradas en las Ecuaciones (4.2) y (4.3),

$$\begin{aligned}\|n\| &\geq \|n_0\|^{s+1} - \|n_0^{s+1} - n\| \geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^{\alpha} \\ &= n_0^{(s+1)\alpha}\Big(1 - \big(1 - \tfrac{n}{n_0^{s+1}}\big)^{\alpha}\Big) \\ &\geq\ n_0^{(s+1)\alpha}\Big(1 - \big(1 - \tfrac{1}{n_0}\big)^{\alpha}\Big) \geq n^{\alpha}C',\end{aligned}$$

donde $C' = 1 - \big(1 - \frac{1}{n_0}\big)^{\alpha}$ es una constante que no depende de n. Si consideramos n^N en vez de n tenemos el siguiente resultado

$$\|n\| \geq \sqrt[N]{C'}n^{\alpha}.$$

Cuando N tiende a infinito tenemos lo siguiente:

$$\|n\| \geq n^{\alpha}.$$

Por lo que hemos demostrado que $\|n\| = |n|^{\alpha}$ para todo $n \in \mathbb{N}$.

Esta igualdad se extiende a $\mathbb{Z}$ por que $\|-n\| = \|n\| = |n|^{\alpha} = |-n|^{\alpha}$. También se puede extender a $\mathbb{Q}$ del siguiente modo: Sea

$$\left\|\frac{n}{m}\right\| = \frac{\|n\|}{\|m\|} = \frac{|n|^{\alpha}}{|m|^{\alpha}} = \left(\frac{|n|}{|m|}\right)^{\alpha} = \left|\frac{n}{m}\right|^{\alpha}.$$

para cada $\frac{n}{m} \in \mathbb{Q}$.

El Teorema 4.1.5 entonces nos asegura que la norma $\|\cdot\|$ es topológicamente equivalente al valor absoluto. □

Lema 4.2.2. *Sea $\|\cdot\|$ una norma no arquimediana y no trivial sobre $\mathbb{Q}$, entonces, existe un primo p tal que $\|\cdot\|$ es topológicamente equivalente a $\|\cdot\|_p$.*

Demostración. Como $\|\cdot\|$ es no arquimediana, por la Proposición 2.2.4 sabemos que $\|n\| \leq 1$ para todo $n \in \mathbb{N}$. Al ser $\|\cdot\|$ no trivial, existe $\frac{n}{m} \in \mathbb{Q}$ tal que $\left\|\frac{n}{m}\right\| \neq 1$. Por lo tanto $\|n\| < 1$ o $\|m\| < 1$, y en consecuencia el conjunto $A = \{n \in \mathbb{N} \mid \|n\| < 1\}$ no es vacío y existe p su mínimo.

Veamos que p es primo. Tomemos $n, m \in \mathbb{N}$ tal que que $p = nm$. Entonces, $\|p\| = \|n\|\|m\| < 1$ y como $\|n\|, \|m\| \leq 1$ la norma de uno de los dos es menor que 1. Sin pérdida de generalidad supongamos que $\|n\| < 1$, entonces, $n \in A$ y $n \leq p$. Como p es el mínimo de este conjunto $n = p$ y $m = 1$. Por ello p es primo.

Ahora veamos como para todo primo $q \neq p$ se tiene que $\|q\| = 1$. Como los dos números son primos entre sí existen $a, b \in \mathbb{N}$ tal que $1 = ap + bq$. Por lo que,

$$1 = \|1\| = \|ap + bq\| \leq \text{máx}\{\|a\|\|p\|, \|b\|\|q\|\}$$

Por ser $a, b, q \in \mathbb{N}$, se tiene que $\|a\|, \|b\|, \|q\| \leq 1$ (ver Proposición 2.2.4). Por tanto

$$1 \leq \text{máx}\{\|a\|\|p\|, \|b\|\|q\|\} \leq 1$$

Por lo que $\text{máx}\{\|a\|\|p\|, \|b\|\|q\|\} = 1$ y siendo $\|a\|\|p\| < 1$ esto solo puede ocurrir si $\|b\|\|q\| = 1$. Por ello, al ser $\|b\|$ y $\|q\|$ menores o iguales que 1 la única opción es que $\|b\| = \|q\| = 1$.

Sabiendo esto tomemos $n \in \mathbb{N}$. Si factorizamos n tenemos lo siguiente,

$$\begin{aligned} n = p_1^{v_{p_1}(n)} \cdot \dots \cdot p_s^{v_{p_s}(n)} &\implies \|n\| = \|p_1\|^{v_{p_1}(n)} \cdot \dots \cdot \|p_s\|^{v_{p_s}(n)} \\ &\implies \|n\| = \|p\|^{v_p(n)}. \end{aligned}$$

Por lo que, como $\|p\| < 1$,

$$\|n\| = \|p\|^{v_p(n)} < 1 \iff v_p(n) > 0 \iff \|n\|_p < 1.$$

En conclusión, $\|\cdot\| \sim \|\cdot\|_p$ por el Teorema 4.1.5. $\square$

Combinando el Corolario 4.1.7 con Lema 4.2.1 y Lema 4.2.2 obtenemos:

Teorema 4.2.3 (Teorema de Ostrowski)**.** *Salvo equivalencia, las únicas normas sobre $\mathbb{Q}$ son la trivial, el valor absoluto y las normas p-ádicas.*

Definimos los *números p-ádicos* $\mathbb{Q}_p$ como la completación de $\mathbb{Q}$ respecto a la norma p-ádica $\|\cdot\|_p$. Por otro lado, la completación respecto a el valor absoluto es $\mathbb{R}$ y respecto a la norma trivial $\mathbb{Q}$.

Corolario 4.2.4. *Las únicas completaciones no triviales de $\mathbb{Q}$ son $\mathbb{R}$ y $\mathbb{Q}_p$, para todo número primo p.*

Capítulo 5

Los números y enteros p-ádicos

Como hemos definido en la Sección 4.2, recordamos que los números p-ádicos son la completación de $\mathbb{Q}$ respecto a la norma $\| \cdot \|_p$. En las siguientes secciones vamos a definir los enteros p-ádicos y vamos a trabajar con diferentes propiedades de los números y los enteros p-ádicos.

5.1. Definición de los enteros p-ádicos

Definición 5.1.1. Para todo p primo, definimos *los enteros p-ádicos* como:

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid \|x\|_p \leq 1\}.$$

Proposición 5.1.2. *Los enteros p-ádicos satisfacen las siguientes propiedades:*

(1) *Son un subanillo de $\mathbb{Q}_p$.*

(2) *Su anillo de unidades es $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid \|x\|_p = 1\}$.*

(3) *Todo elemento $x \in \mathbb{Q}_p \setminus \{0\}$ se puede escribir como $x = p^{v_p(x)}u$, donde $u \in \mathbb{Z}_p^\times$.*

(4) *Es un* anillo local, *es decir tiene un único ideal maximal, que es el siguiente:*

$$\mathfrak{m} := \{x \in \mathbb{Z}_p \mid \|x\|_p < 1\} = p\mathbb{Z}_p.$$

(5) *Todo ideal no vacío en $\mathbb{Z}_p$ tiene la forma $\mathfrak{m}^n = p^n\mathbb{Z}_p$ para algún $n \in \mathbb{N} \cup \{0\}$. En consecuencia, $\mathbb{Z}_p$ es un dominio de ideales principales.*

Demostración. (1) Para ver que es un subanillo tomemos $x, y \in \mathbb{Z}_p$ cualesquiera. Tenemos lo siguiente:

$$\|x + y\|_p \leq \text{máx}\{\|x\|_p, \|y\|_p\} \leq 1 \implies x + y \in \mathbb{Z}_p,$$

y también

$$\|xy\|_p = \|x\|_p\|y\|_p \leq 1 \implies xy \in \mathbb{Z}_p.$$

Además, como $\|1\|_p = 1$ entonces, $1 \in \mathbb{Z}_p$. Por lo que, $\mathbb{Z}_p$ es un subanillo de $\mathbb{Q}_p$.

(2) Por un lado, si tomamos $u \in \mathbb{Z}_p^\times \subseteq \mathbb{Z}_p$, entonces, existe $u^{-1} \in \mathbb{Z}_p$. Por ello, $\|u\|_p \leq 1$ y $\|u^{-1}\|_p \leq 1$. Pero como $1 = \|1\|_p = \|uu^{-1}\|_p = \|u\|_p\|u^{-1}\|_p$, se tiene que cumplir que $\|u\|_p = \|u^{-1}\|_p = 1$.

Por otro lado, sea $u \in \mathbb{Z}_p$ tal que $\|u\|_p = 1$. Como $\mathbb{Q}_p$ es un cuerpo, existirá $u^{-1} \in \mathbb{Q}_p$ el elemento inverso de u. Ya que $\|u^{-1}\|_p = \|u\|_p^{-1} = 1$, tenemos que $u \in \mathbb{Z}_p^\times$.

(3) Sea $x \in \mathbb{Q}_p \setminus \{0\}$, si $v_p(x) = n$, entonces $\|x\|_p = p^{-n}$. Por lo que si tomamos $u = xp^{-n} \in \mathbb{Q}_p$, entonces

$$\|u\|_p = \|xp^{-n}\|_p = \|x\|_p\|p^{-n}\|_p = p^{-n}p^n = 1.$$

Por ello $u \in \mathbb{Z}_p^\times$ y es claro que $x = p^n u$.

(4) Primero, veamos como $\mathfrak{m}$ es un ideal. Sean $x, y \in \mathfrak{m}$, entonces,

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

por lo que $x + y \in \mathfrak{m}$. Por otro lado, sean $x \in \mathfrak{m}$, $y \in \mathbb{Z}_p$, entonces,

$$\|xy\|_p = \|x\|_p\|y\|_p \leq \|x\|_p < 1.$$

Por lo que $xy \in \mathfrak{m}$, y $\mathfrak{m}$ es un ideal.

Además, todo $x \in \mathfrak{m}$ cumple que $\|x\|_p = p^{-n} < 1$ con $n \in \mathbb{N}$. Como $n > 0$, entonces, $p \mid x$ y $x \in p\mathbb{Z}_p$. Además, $p \in \mathfrak{m}$. En conclusión $\mathfrak{m} = p\mathbb{Z}_p$.

Por último, si tenemos un ideal I de un anillo A, entonces si I contiene a una unidad de A, se tiene que $I = A$. Por lo que $\mathfrak{m} = \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$ es un ideal maximal y cumplirá que todo ideal no trivial de $\mathbb{Z}_p$ está contenido en el. En conclusión, es el único ideal maximal de $\mathbb{Z}_p$.

(5) Sea $\mathfrak{a}$ un ideal no vacío en $\mathbb{Z}_p$. Si $\mathfrak{a} = \mathbb{Z}_p$ se tiene que $\mathfrak{a} = p^0\mathbb{Z}_p$. En el caso de que $\mathfrak{a} \neq \mathbb{Z}_p$ entonces, definimos el conjunto $S = \{v_p(x) \mid x \in \mathfrak{a}\}$ con la valuación extendida definida en el Ejercicio 10:

$$v_p(x) := \begin{cases} 0 & \text{si } x = \infty, \\ -\log_p \|x\|_p & \text{si } x \neq 0, \end{cases}$$

Como $\mathfrak{a}$ es no vacío, entonces, S también lo es y además como $x \in \mathbb{Z}_p$ y no es una unidad ya que $\mathfrak{a} \neq \mathbb{Z}_p$, S es un subconjunto no vacío de $\mathbb{N}$ y existe su mínimo. Tomemos n_0 el mínimo de S y $x_0 \in \mathfrak{a}$ con $v_p(x_0) = n_0$. Veamos cómo $\mathfrak{a} = p^{n_0}\mathbb{Z}_p$.

Por la propiedad (3) de esta proposición se tiene que $x_0 = p^{n_0}y_0$ con $y_0 \in \mathbb{Z}_p^\times$. Por ello $p^{n_0} = x_0y_0^{-1}$ y $p^{n_0} \in \mathfrak{a}$. Es decir, $p^{n_0}\mathbb{Z}_p \subseteq \mathfrak{a}$.

Para demostrar la inclusión contraria tomemos $a \in \mathfrak{a}$. Como $n = v_p(a) \geq n_0$, se tiene que $a = p^n u$ con $u \in \mathbb{Z}_p^{\times}$. Por lo tanto, $a = p^{n_0} p^{n-n_0} u \in p^{n_0}\mathbb{Z}_p$. □

Observación 5.1.3. $\mathbb{Z}_p = \overline{B}(0,1)$ por lo que todos los ideales no vacíos de $\mathbb{Z}_p$, por la quinta parte de Proposición 5.1.2, son de la forma

$$p^n\overline{B}(0,1) = \{p^n x \mid \|x\|_p \leq 1\} = \left\{y \mid \|y\|_p \leq \frac{1}{p^n}\right\} = \overline{B}(0, p^{-n}).$$

Teorema 5.1.4. *Para todo número primo p se tiene que*

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

Demostración. Considerando los enteros sobre p ya definidos en la Definición 1.4.7 es fácil de demostrar que $\mathbb{Z}_{(p)}$ es un subanillo de los números p-ádicos y que $p^n\mathbb{Z}_{(p)} = \mathbb{Q} \cap p^n\mathbb{Z}_p$ es su ideal.

Definamos la siguiente función:

$$\begin{aligned} \varphi \colon \mathbb{Z}_{(p)} &\to \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p} \\ a &\mapsto a + p^n\mathbb{Z}_p \end{aligned}$$

Es un homeomorfismo de anillos porque es la composición de dos homeomorfismos: la inclusión $\mathbb{Z}_{(p)} \to \mathbb{Z}_p$ y la aplicación cociente $\mathbb{Z}_p \to \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}$.

El núcleo de la función es el siguiente:

$$\ker\varphi = \{a \in \mathbb{Z}_{(p)} \mid a \in p\mathbb{Z}_p\} = p^n\mathbb{Z}_{(p)}$$

Ahora veamos que es suprayectiva. Sea $x \in \mathbb{Z}_p$, como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, existe $(a_n)_{n\in\mathbb{N}}$ una sucesión de $\mathbb{Q}$ que converge en x. Por ello podemos tomar $a \in \mathbb{Q}$ un elemento de la sucesión $(a_n)_{n\in\mathbb{N}}$ tal que $\|x-a\|_p \leq \frac{1}{p^n}$. Por lo tanto, $v_p(x-a) \geq n$ y $x - a = p^n y \in p^n\mathbb{Z}_p$, donde $y \in \mathbb{Z}_p$, por lo que $x + p^n\mathbb{Z}_p = a + p^n\mathbb{Z}_p$. Además, $\|a\|_p = \|a - x + x\|_p = \text{máx}\{\|a-x\|_p, \|x\|_p\} \leq 1$ es decir, $a \in \mathbb{Z}_{(p)}$. En consecuencia, existe $a \in \mathbb{Z}_{(p)}$ tal que $\varphi(a) = a + p^n\mathbb{Z}_p = x + p^n\mathbb{Z}_p$.

En conclusión, por el primer teorema de isomorfismos para anillos,

$$\frac{\mathbb{Z}_{(p)}}{p^n\mathbb{Z}_{(p)}} \cong \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}.$$

Ahora definamos el siguiente homeomorfismo

$$\begin{aligned} \varsigma \colon \mathbb{Z}_{(p)} &\to \frac{\mathbb{Z}}{p^n\mathbb{Z}} \\ \frac{a}{b} &\mapsto ab^{-1} + p^n\mathbb{Z} \end{aligned}$$

Como $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ es un cuerpo y p no divide a b, esta aplicación está bien definida y ademas es un homeomorfismo de anillos ya que para todo $\frac{a}{b}, \frac{c}{d} \in \mathbb{Z}_{(p)}$

$$\begin{aligned}\varsigma\Big(\frac{a}{b}+\frac{c}{d}\Big) = \varsigma\Big(\frac{ad+cb}{bd}\Big) &= (ad+cb)b^{-1}d^{-1} + p^n\mathbb{Z} = ab^{-1} + cd^{-1} + p^n\mathbb{Z}\\ &= \varsigma\Big(\frac{a}{b}\Big) + \varsigma\Big(\frac{c}{d}\Big),\end{aligned}$$

que

$$\varsigma\Big(\frac{a}{b}\frac{c}{d}\Big) = acb^{-1}d^{-1} + p^n\mathbb{Z} = (ab^{-1})(cd^{-1}) + p^n\mathbb{Z} = \varsigma\Big(\frac{a}{b}\Big)\varsigma\Big(\frac{c}{d}\Big),$$

y que

$$\varsigma(1) = 1 + p^n\mathbb{Z}.$$

Por otro lado, $\ker\varsigma = \left\{\frac{a}{b} \in \mathbb{Z}_{(p)} \mid a \in p^n\mathbb{Z}\right\} = p^n\mathbb{Z}_{(p)}$, y ς es suprayectiva por que $\mathbb{Z} \subseteq \mathbb{Z}_{(p)}$. Por lo que,

$$\frac{\mathbb{Z}}{p^n\mathbb{Z}} \cong \frac{\mathbb{Z}_{(p)}}{p^n\mathbb{Z}_{(p)}} \cong \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}. \qquad \square$$

Observación 5.1.5. En concreto, para todo primo p se tiene que $\frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$. Como representantes de las coclases de $\frac{\mathbb{Z}_p}{p\mathbb{Z}_p}$ vamos a tomar $\{0, \dots, p-1\}$.

Teorema 5.1.6. *$\mathbb{Q}_p$ es el cuerpo de fracciones de $\mathbb{Z}_p$ para cada primo p.*

Demostración. Por la Proposición 5.1.2 tenemos que todo elemento $x \in \mathbb{Q}_p$ puede ser escrito como $x = p^n u$ con $n = v_p(x) \in \mathbb{Z}$ y $u \in \mathbb{Z}_p^\times$. Como para todo elemento $y \in \mathbb{Z}_p$ se cumple que $\|y\|_p \leq 1$ tenemos que $v_p(y) \geq 0$. Por ello, el cuerpo de fracciones de $\mathbb{Z}_p$ es el siguiente

$$\begin{aligned}\mathbb{K} &= \left\{\frac{p^{n_1}u_1}{p^{n_2}u_2} \mid u_1, u_2 \in \mathbb{Z}_p^\times,\ n_1, n_2 \in \mathbb{N}\cup\{0\}\right\} \cup \{0\}\\ &= \{p^m u \mid m = n_1 - n_2 \in \mathbb{Z},\ u = u_1u_2^{-1} \in \mathbb{Z}_p^\times\} \cup \{0\}\\ &= \mathbb{Q}_p.\end{aligned} \qquad \square$$

5.2. Las expansiones p-ádicas

Teorema 5.2.1. *Todo elemento $x \in \mathbb{Q}_p$ se puede escribir del siguiente modo*

$$x = a_m p^m + \cdots + a_0 + a_1 p + \cdots + a_n p^n + \dots,$$

con $m \in \mathbb{Z}$, $a_m \neq 0$ y $a_i \in \{0, \dots, p-1\}$ únicos. Además, en el caso de que $x \in \mathbb{Z}_p$, entonces $m \geq 0$.

Demostración. Lo vamos a demostrar para $x \in \mathbb{Z}_p$ y luego lo vamos a generalizar para cualquier elemento de $\mathbb{Q}_p$.

Por la Observación 5.1.5 tenemos que para todo $x \in \mathbb{Z}_p$ existe $a_0 \in \{0, \dots, p-1\}$ tal que $x + p\mathbb{Z}_p = a_0 + \mathbb{Z}_p$. Por ello existe $k_1 \in \mathbb{Z}_p$ tal que $x = a_0 + pk_1$. Del mismo modo, existen $a_1 \in \{0, \dots, p-1\}$ y $k_2 \in \mathbb{Z}_p$ tal que $k_1 = a_1 + pk_2$ y $x = a_0 + pa_1 + p^2k_2$ y si aplicamos esto de una manera inductiva, para todo $n \in \mathbb{N}$ tenemos lo siguiente:

$$x = a_0 + a_1p + \cdots + a_np^n + k_{n+1}p^{n+1},$$

con $a_i \in \{0, \dots, p-1\}$ y $k_{n+1} \in \mathbb{Z}_p$. Por ello, si tomamos la secuencia $(s_n)_{n\in\mathbb{N}}$ con $s_i = a_0 + \cdots + a_ip^i$, entonces $\|x - s_n\|_p = \|k_{n+1}p^{n+1}\|_p \leq p^{-n-1}$ tiende a cero por lo que $x = \lim_{n\to\infty} s_n$.

Ahora veamos cómo la sucesión $(a_n)_{n\in\mathbb{N}}$ es única. Tomamos $(a'_n)_{n\in\mathbb{N}}$ tal que $x = a'_0 + \cdots + a'_np^n + \dots$ y $a'_i \in \{0, \dots, p-1\}$, y sea $s'_n = a'_0 + \cdots + a'_np^n$. Como en el caso de s_n, vamos a demostrar que $\|x - s'_n\|_p = \|a'_{n+1}p^{n+1} + \dots\|_p \leq p^{-n-1}$. Al ser $(s'_n)_{n\in\mathbb{N}}$ convergente, existe $n_0 \in \mathbb{N}$ tal que para todo $m > n_0$, se tiene que $\|x - s'_m\|_p \leq p^{-n-1}$. Si $n > n_0$, entonces $\|x - s_m\|_p \leq p^{-n-1}$ se cumple por hipótesis y si $n_0 > n$, entonces

$$\|x - s'_n\| = \|x - s'_{n_0} + s'_{n_0} - s'_n\|_p \leq \max\{\|x - s'_{n_0}\|_p, \|s'_{n_0} - s'_n\|_p\} \leq p^{-n-1},$$

ya que

$$\|a'_{n+1}p^{n+1} + \dots a_{n_0}p^{n_0}\|_p \leq \max\{\|a'_{n+1}p^{n+1}\|_p, \dots, \|a_{n_0}p^{n_0}\|_p\} = p^{-n-1}.$$

Por reducción al absurdo supongamos que $(a_n)_{n\in\mathbb{N}} \neq (a'_n)_{n\in\mathbb{N}}$ y tomemos $N \in \mathbb{N}$ el primer elemento que cumple que $a_N \neq a'_N$. Entonces

$$\|s_N - s'_N\|_p = \|a_Np^N - a'_Np^N\|_p = \|(a_N - a'_N)\|_p\|p^N\|_p = 1p^{-N} = p^{-N}.$$

Pero por otro lado,

$$\begin{aligned}\|s_N - s'_N\|_p = \|s_N - x + x - s'_N\|_p &\leq \max\{\|x - s_N\|_p, \|x - s'_N\|_p\} \leq p^{-N-1}\\ &< p^{-N} = \|s_N - s'_N\|_p,\end{aligned}$$

lo cual es absurdo, por lo que $(a_n)_{n\in\mathbb{N}} = (a'_n)_{n\in\mathbb{N}}$ y

$$x = \sum_{n\geq m} a_np^n, \qquad a_i \in \{0, \dots, p-1\}, \quad m \geq 0, \quad a_m \neq 0 \tag{5.1}$$

donde los coeficientes a_i son únicos, para todo $x \in \mathbb{Z}_p$.

Consideramos entonces el caso $x \in \mathbb{Q}_p \setminus \mathbb{Z}_p$. Por el Teorema 5.1.2 existen $v_p(x) = -m < 0$ y $u \in \mathbb{Z}_p^\times$ tales que $x = up^{-m}$. Ya que $\|u\|_p = 1$, el elemento $u \in \mathbb{Z}_p^\times$ satisface la expresión de la Ecuación (5.1) con $m = 0$, y entonces en este caso

$$x = \sum_{n\geq -m} a_np^n, \qquad a_i \in \{0, \dots, p-1\}, \quad m \geq 0, \quad a_{-m} \neq 0,$$

donde los coeficientes a_i son únicos. □

Corolario 5.2.2. *$\mathbb{Z}_p$ es la completación de $\mathbb{Z}$ respecto a la norma p-ádica.*

Demostración. Para empezar, toda sucesión de Cauchy $(a_n)_{n\in\mathbb{N}}$ de $\mathbb{Z}_p$ es convergente en $\mathbb{Q}_p$ por ser $\mathbb{Q}_p$ completo. Pero además, para $x \in \mathbb{Q}_p$ tal que $x = \lim_{n\to\infty} a_n$, se cumple que $\|x\|_p = \lim_{n\to\infty} \|a_n\|_p \leq 1$ ya que $\|a_n\|_p \leq 1$. Por ello, $\mathbb{Z}_p$ es completo. Además, por el teorema anterior $\mathbb{Z}$ es denso en $\mathbb{Z}_p$, por lo que $\mathbb{Z}_p$ es la completación de $\mathbb{Z}$ respecto a la norma $\|\cdot\|_p$ □

Corolario 5.2.3. *Los números y enteros p-ádicos se pueden expresar de la siguiente forma:*

$$\mathbb{Q}_p = \Big\{ \sum_{i=m}^{\infty} a_i p^i \mid m \in \mathbb{Z}, a_m \neq 0, a_i \in \{0, \ldots, p-1\} \Big\}$$
$$\mathbb{Z}_p = \Big\{ \sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, \ldots, p-1\} \Big\}$$

5.3. Propiedades topológicas de $\mathbb{Q}_p$ y $\mathbb{Z}_p$

Hasta ahora hemos visto que $\mathbb{Q}_p$ es un espacio métrico respecto a la norma $\|\cdot\|_p$. Al ser esta norma no arquimediana se tiene que $\mathbb{Q}_p$ es un espacio últramétrico, y en consecuencia cero-dimensional y totalmente disconexo como visto en el Capítulo 1. Todas propiedades que $\mathbb{Z}_p$ hereda. Por otro lado, al ser $\mathbb{Q}_p$ y $\mathbb{Z}_p$ las completaciones de $\mathbb{Q}$ y $\mathbb{Z}$ respectivamente, los dos conjuntos son completos. Además $\mathbb{Q}$ es denso en $\mathbb{Q}_p$ y $\mathbb{Z}$ en $\mathbb{Z}_p$. Veamos otras propiedades topológicas que cumplen los números p-ádicos.

Proposición 5.3.1. *Todo subespacio cerrado A en un espacio métrico completo (X, d) es completo.*

Demostración. Sea $(x_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy en A, entonces, como X es completo, existe $x \in X$ el límite de $(x_n)_{n\in\mathbb{N}}$. Por la Proposición 1.1.13 $x \in \overline{A}$ por lo que concluimos que toda sucesión de Cauchy en A es convergente, eso es, que A es completo. □

Como hemos visto en el Teorema 2.1.4 las bolas en espacios ultramétricos son conjuntos abiertos y cerrados. Entonces:

Corolario 5.3.2. *Toda bola en un espacio ultramétrico completo es completa. En particular, toda bola en $\mathbb{Q}_p$ para un número primo p es completa.*

Lema 5.3.3. *Todo espacio métrico completo y totalmente acotado es secuencialmente compacto.*

Demostración. Sea $(x_n)_{n\in\mathbb{N}}$ una sucesión en X, tomemos $S = \bigcup_{n\in\mathbb{N}} x_n$. Si S es finito, entonces existe un elemento que se repite infinitas veces, por lo que $(x_n)_{n\in\mathbb{N}}$ tiene una subsucesión constante y en consecuencia convergente.

En el caso contrario tomemos $r_1 = \frac{1}{2}$. Como X es totalmente acotado existe un recubrimiento finito por bolas abiertas de radio r_1 del subconjunto S. Como S es infinito, dentro de dicho recubrimiento existe una bola B_1 que contiene infinitos elementos de S. Tomemos $x_{n_1} \in S_1 := B_1 \cap S$.

Del mismo modo, existe un recubrimiento finito por bolas abiertas de radio $r_2 = \frac{1}{2^2}$ del conjunto S_1. Una de estas bolas contiene infinitos elementos de S_1, llamemos a esta bola B_2 y tomemos $x_{n_2} \in S_2 := B_2 \cap S_1$, con $n_2 > n_1$.

Repitiendo esto de manera inductiva obtenemos $(x_{n_j})_{j\in\mathbb{N}} \subseteq (x_n)_{n\in\mathbb{N}}$. Para todo $\varepsilon > 0$ existe $n_\varepsilon \in \mathbb{N}$ con $r_{n_\varepsilon} = \frac{1}{2^{n_\varepsilon}} < \varepsilon$ tal que si $j, k > n_\varepsilon$ se tiene que $x_{n_j} \in B_{n_\varepsilon}$ y $x_{n_k} \in B_{n_\varepsilon}$. Entonces $d(x_{n_j}, x_{n_k}) < r_{n_\varepsilon} < \varepsilon$ y por lo tanto $(x_{n_j})_{j\in\mathbb{N}}$ es una sucesión de Cauchy. Siendo X completo, $(x_{n_j})_{j\in\mathbb{N}}$ es una sucesión convergente, y entonces X es secuencialmente compacto. □

Teorema 5.3.4. *Un espacio métrico, completo y totalmente acotado es compacto.*

Demostración. Sea (X, d) un espacio métrico, completo y totalmente acotado, entonces por la Proposición 5.3.3 es secuencialmente acotado. Al ser métrico, por el Teorema de Heine-Borel-Lebesgue tenemos que es un espacio topológico compacto. □

Teorema 5.3.5. *Toda bola de $\mathbb{Q}_p$ es compacta.*

Demostración. Por la Proposición 5.3.1 toda bola cerrada es completa.

Vamos a ver que toda bola cerrada $\overline{B}(x, r)$ cumple lo siguiente,

$$\overline{B}(x, r) = \bigcup_{i=0}^{p-1} B(x + ri, r)$$

Para demostrar esto vamos a ver cómo se cumple con $x = 0$ y $r = 1$. La generalización a cualquier punto y radio la tenemos en el Ejercicio 9. Por un lado, en claro que $B(i, 1) = i + B(0, 1) \subseteq \overline{B}(0, 1)$ para todo $i \in \{0, ..., p-1\}$ por ser $i \in \mathbb{Z}_p$. Por otro lado, sea $x \in \mathbb{Z}_p$, por la Observación 5.1.4 se tiene que existe $i \in \{0, ..., p-1\}$ tal que $x = i + py$ con $y \in \mathbb{Z}_p$, por lo que $\|x - i\|_p = \|py\|_p < 1$. Es decir, $x \in B(i, 1)$.

Por esto, se tiene que toda bola cerrada es totalmente acotada. Por el Teorema 5.3.4 se tiene que toda bola cerrada es compacta.

Como para toda bola abierta $B(x, r)$ existe $r_1 > 0$ tal que $B(x, r) = \overline{B}(x, r_1)$, todo lo dicho anteriormente se puede aplicar a cualquier bola abierta. □

Corolario 5.3.6. *$\mathbb{Z}_p$ es compacto y $\mathbb{Q}_p$ localmente compacto.*

Apéndice A

Ejercicios

Recordatorio: Espacios métricos, espacios topológicos, normas y valuaciones

Sea $A \subseteq \mathbb{R}$ y $x \in A$. Recordamos que x es un punto aislado de A si existe $\varepsilon > 0$ tal que $(r - \varepsilon, r + \varepsilon) \cap A = \{r\}$.

Ejercicio 1. Sea (X, d) un espacio métrico y $A = d(X \times X) \subseteq [0, +\infty)$. Probar que:

(1) Si 0 es un punto aislado de A , entonces (X, τ_d) es discreto.

(2) Si $r > 0$ es un punto aislado de A , entonces $B(x, r)$, $\overline{B}(x, r)$ y $S(x, r)$ son conjuntos abiertos y cerrados para todo $x \in X$.

(3) Si todo $r \in A \setminus \{0\}$ es aislado, entonces (X, τ_d) es cero-dimensional y por tanto totalmente disconexo.

Solución. (1) Si tomamos τ_A la topología inducida en A, el conjunto $[0, \varepsilon) \cap A$ es abierto en esta topología. Por lo que, al ser d una aplicación continua, (ver Proposición 1.1.5) el conjunto $d^{-1}([0, \varepsilon) \cap A)$ es abierto.

Supongamos que $[0, \varepsilon) \cup A = \{0\}$, y sea $x \in X$ cualquiera. Veamos que la intersección

$$d^{-1}([0, \varepsilon) \cap A) \cap \big(B(x, \varepsilon) \times B(x, \varepsilon)\big),$$

que por definición es abierta en $X \times X$, es $\{x\} \times \{x\}$.

Sea $(y, z) \in \big(B(x, \varepsilon) \times B(x, \varepsilon)\big) \cap d^{-1}([0, \varepsilon) \cap A)$. Por estar y en $B(x, \varepsilon)$, se cumple

$$d(x, y) < \varepsilon \implies d(x, y) \in [0, \varepsilon) \cap A = \{0\} \implies d(x, y) = 0 \implies x = y.$$

Por el mismo razonamiento $x = z$, por lo que

$$d^{-1}([0, \varepsilon) \cap A) \cap \big(B(x, \varepsilon) \times B(x, \varepsilon)\big) = \{x\} \times \{x\}.$$

Por lo que $\{x\} \times \{x\}$ es abierto en $X \times X$ y esto solo es posible si $\{x\}$ es abierto en X.

(2) Primero veamos cómo $S(x, r)$ es abierto. Vamos a ver que para todo $y \in S(x, r)$, la bola abierta $B(y, \varepsilon)$ es un subconjunto de $S(x, r)$.

Sea $z \in B(y, \varepsilon)$ veamos que $z \in S(x, r)$. Por un lado,

$$d(z, x) \leq d(z, y) + d(y, x) < r + \varepsilon$$

Por otro,

$$r = d(x, y) \leq d(z, x) + d(y, z) < d(z, x) + \varepsilon \implies r - \varepsilon < d(z, x)$$

Luego $d(x, z) \in (r - \varepsilon, r + \varepsilon) \cup A = \{r\}$, es decir, $d(x, z) = r$ y $z \in S(x, r)$.

Por lo que $S(x, r)$ será un conjunto abierto. Además es cerrado por definición ya que es la intersección de $X \setminus B(x, r)$ y $\overline{B}(x, r)$.

Por otro lado, como $S(x, r)$ es abierto, $X \setminus B(x, r) = \big(X \setminus \overline{B}(x, r)\big) \cup S(x, r)$ también es abierto, por lo que $B(x, r)$ es un conjunto cerrado, y $\overline{B}(x, r) = B(x, r) \cup S(x, r)$ por lo que es abierto también.

(3) Si todo $r \in A \setminus \{0\}$ es aislado, por el apartado anterior tenemos que para todo $r \in A \setminus \{0\}$, $B(x, r)$ es cerrado. Por lo que si tomamos $r_0 > 0$ cualquiera,

- Si $r_0 \in A$ entonces $B(x, r_0)$ es cerrado.
- Si $r_0 \notin A$ entonces $S(x, r_0) = \{y \in X \mid d(x, y) = r_0\} = \varnothing$ luego $B(x, r_0) = \overline{B}(x, r_0)$.

Es decir, todos los conjuntos de la base de abiertos son cerrados, por lo que X es cero-dimensional. $\square$

Ejercicio 2. Demostrar las siguientes implicaciones.

(1) Si A es un subespacio compacto de un espacio topológico (X, τ), entonces A es localmente compacto. Pero la implicación contraria es falsa.

(2) Si A es un subespacio compacto de un espacio topológico (X, τ), entonces A es un espacio compacto por punto límite. Pero la implicación contraria es falsa.

(3) Si A es un subespacio compacto de un espacio métrico (X, d), entonces es totalmente acotado. Pero la implicación contraria es falsa.

Solución. (1) Si A es compacto, entonces A es un entorno (en A) compacto de todo punto de A. Por ello, es localmente compacto. Por otro lado, $\mathbb{R}$ es localmente compacto por que para todo $x \in \mathbb{R}$ se tiene que $[x - 1, x + 1]$

es un entorno compacto de x pero no es compacto porque en $\mathbb{R}$ los únicos subespacios compactos son los cerrados y acotados.

(2) Veamos cómo si A es compacto entonces es compacto por punto límite. Por reducción al absurdo supongamos que A no es compacto por punto límite. Entonces, existe un subconjunto infinito $B \subseteq A$ que no tiene ningún punto de acomulación. Es decir, para todo $x \in A$ existe $U_x \in \tau$ un abierto que contiene a x tal que $U \cap A \subseteq \{x\}$. Tomemos $\{U_x\}_{x\in A}$ un recubrimiento abierto de A. Como A es compacto entonces existe el subrecubrimiento $\{U_1', \ldots, U_n'\}$. Como $B \subseteq A \subseteq \bigcup_{i=1}^{n} U_i'$ y B es infinito, existe $U_i' \in \{U_1', \ldots, U_n'\} \subseteq \{U_x\}_{x\in A}$ que contiene infinitos puntos de B, lo cual es absurdo por que por hipótesis cada abierto $U_{x_0} \in \{U_x\}_{x\in A}$ contiene como mucho un elemento de B.

Por otro lado, si tomamos la topología de Kolmogorov, el subespacio $(0, \infty)$ no es compacto ya que el recublimiento abierto $\left\{\left(\frac{1}{n}, \infty\right)\right\}_{n\in\mathbb{N}}$ no tiene ningín subrecubrimiento finito. Pero todo subconjunto infinito y por lo tanto no vacío tiene puntos de acomulación.

(3) Como es compacto si tomamos el recubrimiento abierto $\{B(x, \varepsilon)_{x\in A}\}$ para cualquier $\varepsilon > 0$ existe un subencubrimiento finito. Por otro lado, $(0, 1)$ es totalmente acotado pero no es compacto. □

Espacios ultramétricos

Ejercicio 3. Demuestre que todos los triángulos en un espacio ultramétrico son isósceles.

Solución. Sean $a, b, c \in X$ los vértices del triángulo, tenemos que demostrar que al menos dos vértices están a la misma distancia. Tomemos $d(a, b)$ y $d(a, c)$. Si $d(a, b) = d(a, c)$ hemos terminado, así que supongamos que $d(a, b) > d(a, c)$. De la Proposición 2.1.2 deducimos que

$$d(b, c) = \text{máx}\{d(a, b), d(a, c)\} = d(a, b). \quad \square$$

Ejercicio 4. Sean (X, d) un espacio ultramétrico, $\mathbb{B}_X$ el conjunto de las bolas de (X, d) y $A \subseteq X$ un subconjunto acotado, es decir un subconjunto para el que existe B una bola abierta tal que $A \subseteq B$. Demuestre que las siguientes expresiones son equivalentes:

(1) $A \in \mathbb{B}_X$.

(2) Para cualquier $a \in A$ se tiene que $x \in A$ si y sólo si $d(x, a) \leq \text{diám}\,(A)$ o $x \in A$ si y sólo si $d(x, a) < \text{diám}\,(A)$, es decir, $A = \overline{B}(a, \text{diám}\,(A))$ o $A = B(a, \text{diám}\,(A))$.

(3) $\mathbb{B}_A = \{B \in \mathbb{B}_X \mid B \subseteq A\}$, donde $\mathbb{B}_A$ es el conjunto de las bolas de $(A, d|_{A\times A})$.

Solución. En las demostraciones solo trabajaremos con bolas abiertas pero todas las demostraciones se pueden hacer usando bolas cerradas.

(1)⇒(3) Para empezar demostremos lo siguiente:

$$\mathbb{B}_A = \mathbf{B}_A := \{B \cap A \mid B \in \mathbb{B}_X \text{ y } B \cap A \neq \varnothing\}.$$

Sea $B_A(a,r) \in \mathbb{B}_A$, entonces tiene la siguiente forma:

$$\begin{aligned} B_A(a,r) &= \{x \in A \mid d_{A\times A}(x,a) < r\} = \{x \in A \mid d(x,a) < r\} \\ &= B(a,r) \cap A \in \mathbf{B}_A. \end{aligned}$$

Ahora, sea $B(x,r) \in \mathbb{B}_X$ tal que $B(x,r) \cap A \neq \varnothing$, y sea $a \in B(x,r) \cap A$. Al estar en un espacio ultramétrico $B(x,r) = B(a,r)$, y por lo tanto $B(x,r) \cap A = B_A(a,r) \in \mathbb{B}_A$. En consecuencia $\mathbb{B}_A = \{B \cap A \mid B \in \mathbb{B}_X \text{ y } B \cap A \neq \varnothing\}$.

Teniendo esto en cuenta, supongamos que $A \in \mathbb{B}_X$ y demostremos que

$$\{B \cap A \mid B \in \mathbb{B}_X \text{ y } B \cap A \neq \varnothing\} = \{B \in \mathbb{B}_X \mid B \subseteq A\}.$$

En primer lugar, es claro que para toda bola $B \in \mathbb{B}_X$ tal que $B \subseteq A$, $B \in \{B \cap A \mid B \in \mathbb{B}_X\}$. Tenemos que demostrar que $B \cap A \in \{B \in \mathbb{B}_X \mid B \subseteq A\}$ para todo $B \in \mathbb{B}_X$.

Sea $B \cap A \in \overline{B}_A$, como los dos conjuntos son bolas en X, tenemos dos opciones:

- $B \subseteq A \implies B \cap A = B \in \{B \in \mathbb{B}_X \mid B \subseteq A\}$.
- $A \subseteq B \implies B \cap A = A \in \{B \in \mathbb{B}_X \mid B \subseteq A\}$.

Por lo que hemos demostrado (3).

(3)⇒(1) Como A es acotado, existe $B \in \mathbb{B}_X$ tal que $A \subseteq B$. Por lo que $A = A \cap B \in \mathbb{B}_A = \{B \in \mathbb{B}_X \mid B \subseteq A\}$. Por lo que $A \in \mathbb{B}_X$.

(1)⇒(2) Sea $A = \overline{B}(a,r)$. Si $x \in A$ entonces $d(x,a) \leq \operatorname{diám}(A)$, y recíprocamente, si $d(x,a) \leq \operatorname{diám}(A)$, por la Proposición 2.1.9 tenemos que $\operatorname{diám}(A) \leq r$, luego $d(x,a) \leq r$, es decir, $x \in A$. Análogamente, si $A = B(a,r)$ para todo $x \in A$ se tiene que $d(a,x) < r$ y $d(a,x) \leq \operatorname{diám}(A) \leq r$ pero como $d(a,x) < r$ se tiene que cumplir que $d(a,x) < \operatorname{diám}(A)$. Recíprocamente, si $d(a,x) < \operatorname{diám}(A) \leq r$ entonces $x \in A$.

(2)⇒(1) Por (2) tenemos que $A = \overline{B}(a,r)$ o $A = B(a,r)$, siendo $r = \operatorname{diám}(A)$. □

Ejercicio 5. Sean (X,d) un espacio ultramétrico, $A \subseteq X$ un subconjunto acotado no vacío y $a \in A$, entonces $\overline{B}(a, \operatorname{diám}(A))$ es la bola más pequeña que contiene a A.

Solución. Primero, veamos cómo siendo $r = \text{diám}\,(A)$ y $a \in A$, entonces, $A \subseteq \overline{B}(a,r)$. Sea $x \in A$, entonces,

$$d(a,x) \leq r \implies x \in \overline{B}(a,r).$$

Ahora veremos cómo si tomamos $r_0 < r$, entonces $A \nsubseteq \overline{B}(a,r_0)$ para todo $a \in A$. Tomemos $a_0, a_1 \in A$ tales que $d(a_0,a_1) = r_1 > r_0$. Esto será posible ya que $r_0 < \sup_{\alpha,\beta\in A} d(\alpha,\beta)$. Separamos en dos casos:

- Si $a_0 \notin \overline{B}(a,r_0)$, entonces $A \nsubseteq \overline{B}(a,r_0)$.
- Si $a_0 \in \overline{B}(a,r_0)$, entonces $\overline{B}(a,r_0) = \overline{B}(a_0,r_0)$ por la Proposición 2.1.8. Como $d(a_0,a_1) = r_1 > r_0$, tenemos que $a_1 \notin \overline{B}(a,r_0)$. Por lo que $A \nsubseteq \overline{B}(a,r_0)$. □

Ejercicio 6. En el espacio ultramétrico $(\mathbb{Q}, \|\cdot\|_p)$

$$\overline{B}(0,1) = B(0,1) \cup B(1,1) \cup \cdots \cup B(p-1,1).$$

Solución. Para empezar, escribamos las expresiones de cada bola:

$$\begin{aligned}
\overline{B}(0,1) &= \{x \in \mathbb{Q} \mid \|x\|_p = p^{-v_p(x)} \leq 1\} = \{x \in \mathbb{Q} \mid v_p(x) \geq 0\}.\\
B(0,1) &= \{x \in \mathbb{Q} \mid \|x\|_p = p^{-v_p(x)} < 1\} = \{x \in \mathbb{Q} \mid v_p(x) > 0\}.\\
B(i,1) &= \{x \in \mathbb{Q} \mid \|x-i\|_p = p^{-v_p(x-i)} < 1\} = \{x \in \mathbb{Q} \mid v_p(x-i) > 0\}\\
&= \{x+i \in \mathbb{Q} \mid v_p(x) > 0\} = \{x+i \in \mathbb{Q} \mid x \in B(0,1)\}\\
&= B(0,1)+i.
\end{aligned}$$

Viendo esto, empecemos con la demostración.

$(\subseteq)$ Sea $\frac{m}{n} \in \mathbb{Q}$ tal que m y n son primos entre sí. Si $\frac{m}{n} \in \overline{B}(0,1)$, entonces, $p \nmid n$. Es decir, $n \not\equiv 0 \ (mod\ p)$, y por lo tanto podemos encontrar $i \in \{0,\ldots,p-1\}$ que cumpla $m \equiv ni \ (mod\ p)$. Por lo que,

$$\begin{aligned}
m \equiv ni \ (mod\ p) &\implies \exists k \in \mathbb{Z} \mid m = pk + in\\
&\implies \frac{m}{n} = \frac{pk}{n} + i \in B(0,1) + i = B(i,1).
\end{aligned}$$

Por lo que $\overline{B}(0,1) \subseteq \bigcup_{i=0}^{p-1} B(i,1)$.

$(\supseteq)$ Sea $i \in \{0,\ldots,p-1\}$, y veamos cómo $B(i,1) = B(0,1)+i \subseteq \overline{B}(0,1)$. Tomemos $x+i \in B(i,1)$ con $x \in B(0,1)$, entonces,

$$\|x+i\|_p \leq \text{máx}\{\|x\|_p, \|i\|_p\}.$$

Como $\|x\|_p < 1$ y $\|i\|_p = 0$ si $i = 0$, o $\|i\|_p = 1$ en otro caso, es claro que $\|x+i\|_p \leq 1$. Por lo que $x+i \in \overline{B}(0,1)$. □

Ejercicio 7. Definimos la función suelo $\lfloor\cdot\rfloor\colon \mathbb{R} \to \mathbb{Z}$ y la función techo $\lceil\cdot\rceil\colon \mathbb{R} \to \mathbb{Z}$ del la siguiente forma

$$\lfloor x\rfloor := \max\{n \in \mathbb{Z} \mid x \geq n\}, \qquad \lceil x\rceil := \min\{n \in \mathbb{Z} \mid x \leq n\}.$$

Sean el espacio ultramétrico $(\mathbb{Q}, \|\cdot\|_p)$, $x \in \mathbb{Q}$ y $r > 0$. Demuestre que se tiene lo siguiente:

$$B(a,r) = B\big(a, p^{\lceil \log_p r\rceil}\big), \qquad \overline{B}(a,r) = \overline{B}\big(a, p^{\lfloor \log_p (r)\rfloor}\big).$$

Concluir que para cada $n \in \mathbb{Z}$ se tiene que $B(a,p^n) = \overline{B}(a,p^{n-1})$ y $\overline{B}(a,p^n) = B(a,p^{n+1})$.

Solución. Escribamos la expresión para $B(a,r)$.

$$\begin{aligned} B(a,r) &= \{x \in \mathbb{Q} \mid \|x-a\|_p < r\} \\ &= \{0\} \cup \big\{x \in \mathbb{Q} \mid p^{-v_p(x-a)} < r\big\} \\ &= \cup\{x \in \mathbb{Q} \mid -v_p(x-a) < \log_p r\} \\ &= \{0\} \cup \{x \in \mathbb{Q} \mid v_p(x-a) > -\log_p r\}. \end{aligned}$$

Como $v_p(x-a) \in \mathbb{Z}$ para todo $x \in \mathbb{Q}$ y por la definición de la función suelo, tenemos que $v_p(x-a) > -\log_p r$ es equivalente a que $v_p(x-a) > \lfloor -\log_p r\rfloor$. Por ello,

$$\begin{aligned} B(a,r) &= \{0\} \cup \{x \in \mathbb{Q} \mid v_p(x-a) > \lfloor -\log_p r\rfloor\} \\ &= \{0\} \cup \{x \in \mathbb{Q} \mid -v_p(x-a) < -\lfloor -\log_p r\rfloor = \lceil \log_p r\rceil\} \\ &= \big\{x \in \mathbb{Q} \mid \|x-a\|_p = p^{-v_p(x-a)} < p^{\lceil \log_p r\rceil}\big\} \\ &= B\big(a, p^{\lceil \log_p r\rceil}\big). \end{aligned}$$

Por otro lado, se tiene que

$$\overline{B}(a,r) = \{x \in \mathbb{Q} \mid \|x-a\|_p \leq r\} = \{0\} \cup \{x \in \mathbb{Q} \mid v_p(x-a) \geq -\log_p r\}.$$

Ya que $v(x-a) \in \mathbb{Z}$ y por la definición de la función techo, tenemos que $v(x-a) \geq -\log_p r$ es equivalente a que $v_p(x-a) \geq \lceil -\log_p r\rceil$. Por ello,

$$\begin{aligned} \overline{B}(a,r) &= \{0\} \cup \{x \in \mathbb{Q} \mid v_p(x-a) \geq \lceil -\log_p r\rceil\} \\ &= \{0\} \cup \{x \in \mathbb{Q} \mid -v_p(x-a) \leq -\lceil -\log_p r\rceil = \lfloor \log_p r\rfloor\} \\ &= B\big(a, p^{\lfloor \log_p r\rfloor}\big). \end{aligned}$$

Por ello, cuando trabajamos con una bola de radio r podemos asumir sin pérdida de generalidad que $r = p^n$ para algun $n \in \mathbb{Z}$. Por ello, si tenemos las bolas $B(a,p^n)$ y $\overline{B}(a,p^n)$, como por la definición de la norma p-ádica sobre $\mathbb{Q}$ los valores posibles para la norma $\|\cdot\|_p$ son p^k con $k \in \mathbb{Z}$, tenemos lo siguiente.

$$\begin{aligned} B(a, p^n) &= \{x \in \mathbb{Q} \mid \|x-a\|_p < p^n\} \\ &= \{x \in \mathbb{Q} \mid \|x-a\|_p \leq p^{n-1}\} = \overline{B}(a, p^{n-1}). \end{aligned}$$

Del mismo modo $\overline{B}(a, p^n) = B(a, p^{n+1})$. □

Ejercicio 8. En el espacio ultramétrico $(\mathbb{Q}, \|\cdot\|_5)$ demuestre que $B(1,1) = B\left(1, \frac{1}{2}\right) = \overline{B}\left(1, \frac{1}{5}\right)$.

Solución. Por el Ejercicio 7 se tiene lo siguiente:

$$B\big(1, \tfrac{1}{2}\big) = B\big(1, 5^{\lceil \log_5(\frac{1}{2}) \rceil}\big) = B(1, 5^0) = B(1,1).$$

Por otro lado,

$$\overline{B}\big(1, \tfrac{1}{5}\big) = \overline{B}(1, 5^{-1}) = B(1, 5^{-1+1}) = B(1,1). \qquad \square$$

Ejercicio 9. En el espacio ultramétrico $(\mathbb{Q}, \|\cdot\|_p)$ demuestre que toda bola abierta es una unión disjunta de otras bolas abiertas.

Solución. Este ejercicio es una generalización de el Ejercicio 6. Basándonos en él vamos a demostrar lo siguiente:

$$\overline{B}(a, r) = \bigcup_{i=0}^{p-1} B(a + ri, r).$$

Empezamos demostrando lo siguiente. Sean $\|\cdot\|$ una norma sobre un cuerpo X, $a \in X$ y $r > 0$. Entonces, si existe $x \in X$ tal que $\|x\| = r$, se cumple lo siguiente

$$B(a, r) = xB\Big(\frac{a}{x}, 1\Big),$$

y lo mismo ocurre con esferas y bolas cerradas. Vamos a demostrarlo para las bolas abiertas, pero para esferas o bolas cerradas la demostración es análoga.

$$\begin{aligned} B(a, r) &= \{y \in X \mid \|y-a\| < r\} = \Big\{y \in X \mid \frac{\|y-a\|}{r} < 1\Big\} \\ &= \Big\{y \in X \mid \frac{\|y-a\|}{\|x\|} < 1\Big\} = \Big\{y \in X \mid \Big\|\frac{y-a}{x}\Big\| < 1\Big\} \\ &= \Big\{x \cdot y \in X \mid \Big\|y - \frac{a}{x}\Big\| < 1\Big\} = \Big\{x \cdot y \in X \mid y \in B\Big(\frac{a}{x}, 1\Big)\Big\} \\ &= x \cdot B\Big(\frac{a}{x}, 1\Big). \end{aligned}$$

Por el Ejercicio 7, podemos suponer sin pérdida de generalidad que para una bola $B(a, r)$ existe $n \in \mathbb{Z}$ tal que $r = p^n$.

Cuando $a = 0$ usando esto y el Ejercicio 6 con $x = p^{-n}$ tenemos lo siguiente:

$$\overline{B}(0,r) = p^{-n}\cdot\overline{B}(0,1) = p^{-n}\cdot\left(\bigcup_{i=0}^{p-1} B(i,1)\right) = \bigcup_{i=0}^{p-1} p^{-n}\cdot B(i,1) = \bigcup_{i=0}^{p-1} B(ir,r).$$

Si $a \neq 0$ tenemos lo siguiente:

$$\overline{B}(a,r) = a + \overline{B}(0,r) = a + \bigcup_{i=0}^{p-1} B(ir,r) = \bigcup_{i=0}^{p-1} a + B(ir,r) = \bigcup_{i=0}^{p-1} B(a+ir,r).$$

Solo nos queda ver que estas bolas son disjuntas. Por reducción al absurdo, supongamos que existen $x \in \overline{B}(a,r)$ e $i,j \in \{0,\ldots,p-1\}$, donde $i \neq j$, tales que $x \in B(a+ir,r)$ y $x \in B(a+jr,r)$. Entonces

$$\|x-a-ir\|_p < r \quad \text{y} \quad \|x-a-jr\|_p < r.$$

Por lo que

$$\begin{aligned} r = r\|i-j\|_p = \|ri-rj\|_p &= \|x-a-rj-(a+x-ri)\|_p \\ &\leq \text{máx}\{\|x-a-rj\|_p, \|x-a-ri\|_p\} < r, \end{aligned}$$

lo cual es absurdo. $\square$

Sucesiones de Cauchy y completaciones

En los ejercicios anteriores hemos utilizado que para cualquier elemento de $x \in \mathbb{Q}$, como $v_p(x) \in \mathbb{Z}$, se tiene que $\|x\|_p = p^n$ para algún $n \in \mathbb{Z}$. En el siguiente ejercicio vamos a probar que esto también es cierto para los elementos de $\mathbb{Q}_p$.

Ejercicio 10. Para todo $0 \neq x \in \mathbb{Q}_p$ se tiene que $\|x\|_p = p^n$ para algún $n \in \mathbb{Z}$. Para eso vamos a dar los siguientes pasos:

(1) Demostrar que toda sucesión $(a_n)_{n\in\mathbb{N}}$ sobre $\mathbb{Z}$ es de Cauchy respecto al valor absoluto si y sólo si es semiconstante. Concluir que $\mathbb{Z}$ es completo respecto al valor absoluto.

(2) Demostrar que la función $v_p\colon \mathbb{Q}_p \longrightarrow \mathbb{Z}\cup\{\infty\}$ dada por

$$x = \lim_{n\to\infty} x_n \longmapsto v_p(x) = \lim_{n\to\infty} v_p(x_n)$$

es una valuación.

(3) Concluir que la norma p-ádica toma valores en $\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}$.

Solución. (1) Por un lado, si una sucesión $(a_n)_{n\in\mathbb{N}}$ es semiconstante, entonces existe $N \in \mathbb{N}$ tal que $a_m = a_N$ para todo $m \geq N$. Por lo que para todo $\varepsilon > 0$ y para todo $m, n \geq N$ se tiene que $|a_n - a_m| = 0 < \varepsilon$, es decir, es una sucesión de Cauchy.

Por otro lado, si $(a_n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy, entonces existe $n_0 \in \mathbb{N}$ tal que para todo $n, m > n_0$ se da que $|a_n - a_m| < 1$. Como $a_n, a_m \in \mathbb{Z}$, entonces, $a_n - a_m \in \mathbb{Z}$ por lo que $|a_n - a_m| = 0$ y $a_n = a_m$. Si tomamos $N = n_0 + 1$, para todo $m \geq N$ se cumple que $a_m = a_N$.

Además, si $(a_n)_{n\in\mathbb{N}}$ es semiconstante, entonces $|a_n - a_N| = 0 < \varepsilon$ para todo $\varepsilon > 0$ y para todo $n > N$. Por lo que $(a_n)_{n\in\mathbb{N}}$ es convergente. En consecuencia, toda sucesión de $\mathbb{Z}$ que es de Cauchy respecto a el valor absoluto es convergente.

(2) Por la Proposición 3.2.6 si tomamos $x = \lim_{n\to\infty} x_n \in \mathbb{Q}_p$ entonces, $\|x\|_p = \lim_{n\to\infty} \|x_n\|_p$. Como $\|\cdot\|_p$ es no arquimediana en $\mathbb{Q}$, por la Proposición 3.2.8 también lo es respecto a $\mathbb{Q}_p$. Por ello, la siguiente función

$$v_p(x) := \begin{cases} 0 & \text{si } x = \infty, \\ -\log_p \|x\|_p & \text{si } x \neq 0, \end{cases}$$

es una valuación si y solo si $v_p(x) \in \mathbb{Z}$ para todo $x = \lim_{n\to\infty} x_n \in \mathbb{Q}_p$. Es claro que, por cómo hemos definido v_p, se cumple lo siguiente:

$$\begin{aligned} v_p(x) &= v_p\big(\lim_{n\to\infty} x_n\big) = -\log_p \big\|\lim_{n\to\infty} x_n\big\|_p = -\log_p \lim_{n\to\infty} \|x_n\|_p \\ &= \lim_{n\to\infty} \Big(-\log_p \|x_n\|_p\Big) = \lim_{n\to\infty} v_p(x_n) \end{aligned}$$

Como $v_p(x) \in \mathbb{R}$, la sucesión de números enteros $(v_p(x_n))_{n\in\mathbb{N}}$ es convergente en $\mathbb{R}$, por lo que es una sucesión de Cauchy. Por el apartado anterior es una sucesión convergente en $\mathbb{Z}$ y $v_p(x) \in \mathbb{Z}$. Entonces v_p es una valuación en $\mathbb{Q}_p$.

(3) Al igual que la valuación p-ádica se puede expresar usando la norma p-ádica se cumple lo contrario, es decir:

$$\|x\|_p := \begin{cases} 0 & \text{si } x = 0, \\ p^{-v_p(x)} & \text{si } x \neq 0, \end{cases}$$

Como $v_p(x) \in \mathbb{Z}$, la norma p-ádica toma valores en $\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}$. □

Equivalencias de normas y el Teorema de Ostrowski

Ejercicio 11. Demuestre que las normas $\|\cdot\|_p$ y $\|\cdot\|_q$ no son equivalentes para p y q, primos distintos.

Solución. Sean p y q dos primos distintos. $\|p\|_p = \frac{1}{p} \neq 1$ y $\|p\|_q = 1$. Por el Teorema 4.1.5, $\|\cdot\|_p$ y $\|\cdot\|_q$ no son topológicamente equivalentes. □

Ejercicio 12. Sea $\mathbb{K}$ un cuerpo y consideremos el anillo de polinomios $\mathbb{K}[X]$. Éste es un dominio de factorización única, y en ese sentido es un anillo parecido a $\mathbb{Z}$. Los polinomios irreducibles son análogos de los números primos. El cuerpo de fracciones correspondiente,

$$\mathbb{K}(X) = \left\{ \tfrac{f(X)}{g(X)} \mid f, g \in \mathbb{K}[X],\ g \neq 0 \right\},$$

es análogo a $\mathbb{Q}$.

Supongamos que $\|\cdot\|$ es una norma sobre $\mathbb{K}(X)$ tal que $\|\cdot\|$ es trivial sobre $\mathbb{K}$.

(1) Probar que $\|\cdot\|$ es necesariamente no arquimediana.

(2) Probar que $\|\cdot\|$ está definida por sus valores sobre $\mathbb{K}[X] \subseteq \mathbb{K}(X)$.

(3) Supongamos que $\|X\| > 1$. Probar que para todo $f \in \mathbb{K}[X]$ se cumple $\|f\| = \|X\|^{\deg(f)}$, así que la noma es equivalente a la norma $f \mapsto \rho^{-\deg(f)}$ para algún $0 < \rho < 1$.

(4) Supongamos que $\|X\| \leq 1$. Probar que $\|f\| \leq 1$ para todo $f \in \mathbb{K}[X]$. Además, si la norma no es trivial y $f_0 \neq 0$ es un polinomio mónico del mínimo grado posible tal que $\|f_0\| < 1$, probar que $f_0 = p$ es un polinomio irreducible y $\|q\| = 1$ si $q \neq p$ es otro polinomio mónico irreducible. Concluir que en este caso la norma es equivalente a $f \mapsto \rho^{v_p(f)}$, donde $\rho < 1$ y

$$v_p(f) \colon = \text{máx}\{k \mid p^k \text{ divide a } f\}.$$

Solución. (1) Para todo $n \in \mathbb{N}$ tenemos que $n \in \mathbb{K}$, de manera que, por hipótesis, $\|n\| = 1$. De la Proposición 2.2.4 deducimos que $\|\cdot\|$ es no arquimediana.

(2) Para cada elemento $z \in \mathbb{K}(X)$ existen $f, g \in \mathbb{K}[X]$ tales que $z(X) = \frac{f(X)}{g(X)}$. Por ello, $\|z(X)\| = \left\| \frac{f(X)}{g(X)} \right\| = \frac{\|f\|}{\|g\|}$. En conclusión, los valores de $\|\cdot\|$ en $\mathbb{K}(X)$ están dados por los valores que $\|\cdot\|$ toma en $\mathbb{K}[X]$.

(3) Sea $f(X) = a_0 + \cdots + a_n X^n \in \mathbb{K}[X]$ con $a_n \neq 0$, veamos como $\|a_i X^i\| \neq \|a_j X^j\|$ para todo $i, j \in \{0, \ldots, n\}$ con $i \neq j$:

$$\begin{aligned} \|a_i X^i\| = \|a_j X^j\| &\iff \|a_i\| \|X\|^i = \|a_j\| \|X\|^j \iff \|X\|^i = \|X\|^j \\ &\iff \|X\| = 1, \end{aligned}$$

contradiciendo la hipótesis que $\|X\| > 1$. Así si aplicamos la generalización de la Proposición 2.2.2 tenemos que

$$\begin{aligned} \|f(X)\| &= \text{máx}\{\|a_0\|, \|a_1 X\|, \ldots, \|a_n X^n\|\} = \text{máx}\{1, \|X\|, \ldots, \|X\|^n\} \\ &= \|X\|^n = \|X\|^{\deg(f)}. \end{aligned}$$

En conclusión $\|f\| = \rho^{-\deg(f)}$, donde $\rho = \|X\|^{-1}$.

(4) Sea $f(X) = a_0 + \cdots + a_n X^n \in \mathbb{K}[X]$ con $a_n \neq 0$. Si $\|X\| \leq 1$, entonces, $\|f(X)\| \leq \text{máx}\{\|a_0\|, \ldots, \|a_n X^n\|\} = \text{máx}\{1, \ldots, \|X\|^n\} \leq 1$.

Si además $\|\cdot\|$ no es trivial, existen $f, g \in \mathbb{K}[X] \setminus \{0\}$ tales que $\frac{\|f\|}{\|g\|} < 1$. Por ello, $\|f\| \neq \|g\|$ y al menos uno de los dos tiene norma diferente a 1. En consecuencia $S = \{f \in \mathbb{K}[X] \mid 0 < \|f\| < 1\}$ es un conjunto no vacío y, como las normas de estos elementos definen un subconjunto de $\mathbb{N}$ no vacío, entonces existe algún $f_0 \in S$ con grado mínimo.

Veamos que f_0 es un polinomio irreducible. Supongamos que $f_0 = gh$. Como $1 > \|f_0\| = \|g\|\|h\|$, tenemos que $\|g\| < 1$ o $\|h\| < 1$. Sin pérdida de generalidad, supongamos que $\|g\| < 1$. Entonces, $g \notin \mathbb{K}$ y $g \in S$. Como $\deg(f_0) = \deg(g) + \deg(h)$, $\deg(g) \leq \deg(f_0)$ y como f_0 es un elemento con grado mínimo de S, $\deg(g) = \deg(f_0)$ y en consecuencia $\deg(h) = 0$. Por lo que $h \in \mathbb{K}$ es una unidad y f_0 es un polinomio irreducible.

Como $\mathbb{K}$ es un cuerpo, $\mathbb{K}[X]$ es un dominio de ideales principales, por lo que para dos polinomios existe el máximo común divisor. Sea g un polinomio primo distinto a f_0, veamos que $\|g\| = 1$. Como los dos polinomios son primos, el máximo común divisor es 1, por lo que existen $a, b \in \mathbb{K}[X]$ tales que $1 = af_0 + bg$, así que

$$1 = \|1\| = \|af_0 + bg\| \leq \text{máx}\{\|a\|\|f_0\|, \|b\|\|g\|\}.$$

Como $\|a\| \leq 1$ y $\|f_0\| < 1$ tenemos que $\|b\|\|g\| = 1$, y esto sólo es posible si $\|b\| = \|g\| = 1$.

Sea $f \in \mathbb{K}[X]$. Como $\mathbb{K}[X]$ es un dominio de factorización única, existen polinomios primos $f_1, \ldots, f_n \in \mathbb{K}[X]$ y $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ tales que $f = f_0^{a_0} f_1^{a_1} \cdots f_n^{a_n}$. Por ello,

$$\begin{aligned}\|f\| &= \|f_0^{a_0} \cdot f_1^{a_1} \cdots f_n^{a_n}\| = \|f_0\|^{a_0} \|f_1\|^{a_1} \cdots \|f_n\|^{a_n} \\ &= \|f_0\|^{v_p(f)} \cdot 1 \cdots 1 = \|f_0\|^{v_p(f)}.\end{aligned}$$

Como $\|f_0\| < 1$, para todo $\rho < 1$ se cumple que

$$\|f\| = \|f_0\|^{v_p(f)} < 1 \iff \rho^{v_p(f)} < 1.$$

Por lo que, $\|\cdot\|$ es topológicamente equivalente a la norma definida por $f \mapsto \rho^{v_p(f)}$ por el Teorema 4.1.5. $\square$

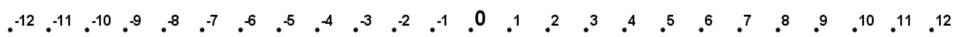
Apéndice B

Visualización de la norma p-ádica en los números enteros

A partir del artículo *Buissons et balais* [5] hemos intentado dar una visualización de $\mathbb{Z}$ que facilite la comprensión del funcionamiento de la norma p-ádica. Para esto hemos creado una aplicación interactiva, mediante el programa GeoGebra, accesible en
`https://www.geogebra.org/m/rdypsdkw`.

En este apartado intentamos describir esta visualización apoyándonos en imágenes capturadas desde la citada.

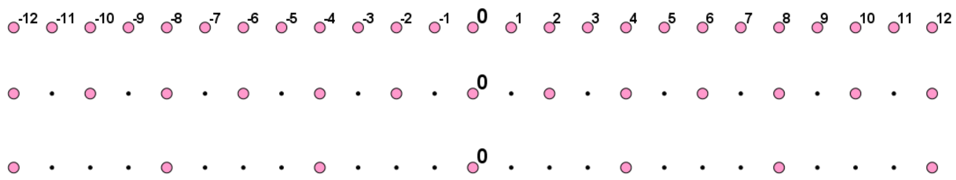
La manera usual en la que nos imaginamos los números enteros es colocándolos en una línea de la siguiente manera.



Este tipo de visualización es muy adecuada cuando trabajamos con el valor absoluto ya que coincide con nuestra idea intuitiva de distancia.

Sin embargo, cuando trabajamos con las normas p-ádicas esta representación no es útil. No se respetan visualmente las distancias teóricas de los números. Esto provoca, entre otras cosas, que las visualizaciones de las bolas no sean muy intuitivas y que, por ejemplo, cuando disminuimos el radio de una bola no da la sensación de que los elementos que quedan sean los más cercanos al centro.

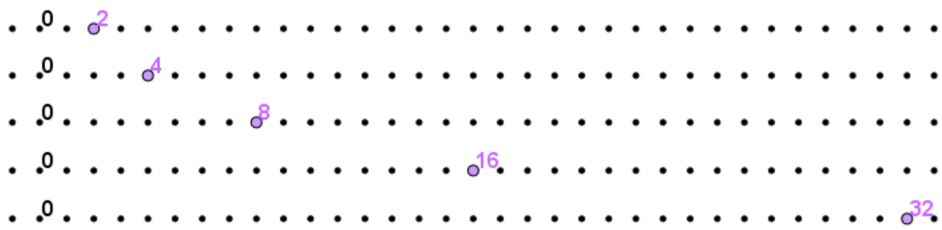
Ejemplo 1. Si tomamos $p = 2$ y las bolas abiertas centradas en 0 y de radio $2, 1$ y $\frac{1}{2}$ tenemos lo siguiente:



(La versión interactiva de esta imagen se encuentra en `https://www.geogebra.org/m/r57mn3cf`)

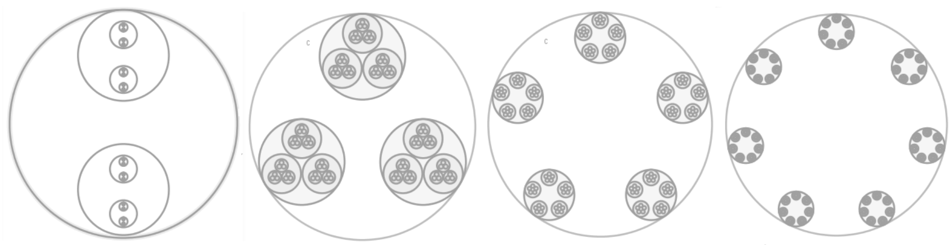
Tampoco nos permite visualizar el límite de una sucesión. Por ejemplo si tomamos la sucesión $(p^n)_{n\in\mathbb{N}}$ que bajo la norma p-ádica converge a 0 cuando trabajamos con la representación de la línea recta no da la sensación de que se "acerque" a 0 sino que da la sensación de que se "aleja".

Ejemplo 2. Si tomamos $p = 2$ y los cuatro primeros elementos de la sucesión $(p^n)_{n\in\mathbb{N}}$ tenemos lo siguiente:



(La versión interactiva de esta imagen se encuentra en `https://www.geogebra.org/m/r57mn3cf`)

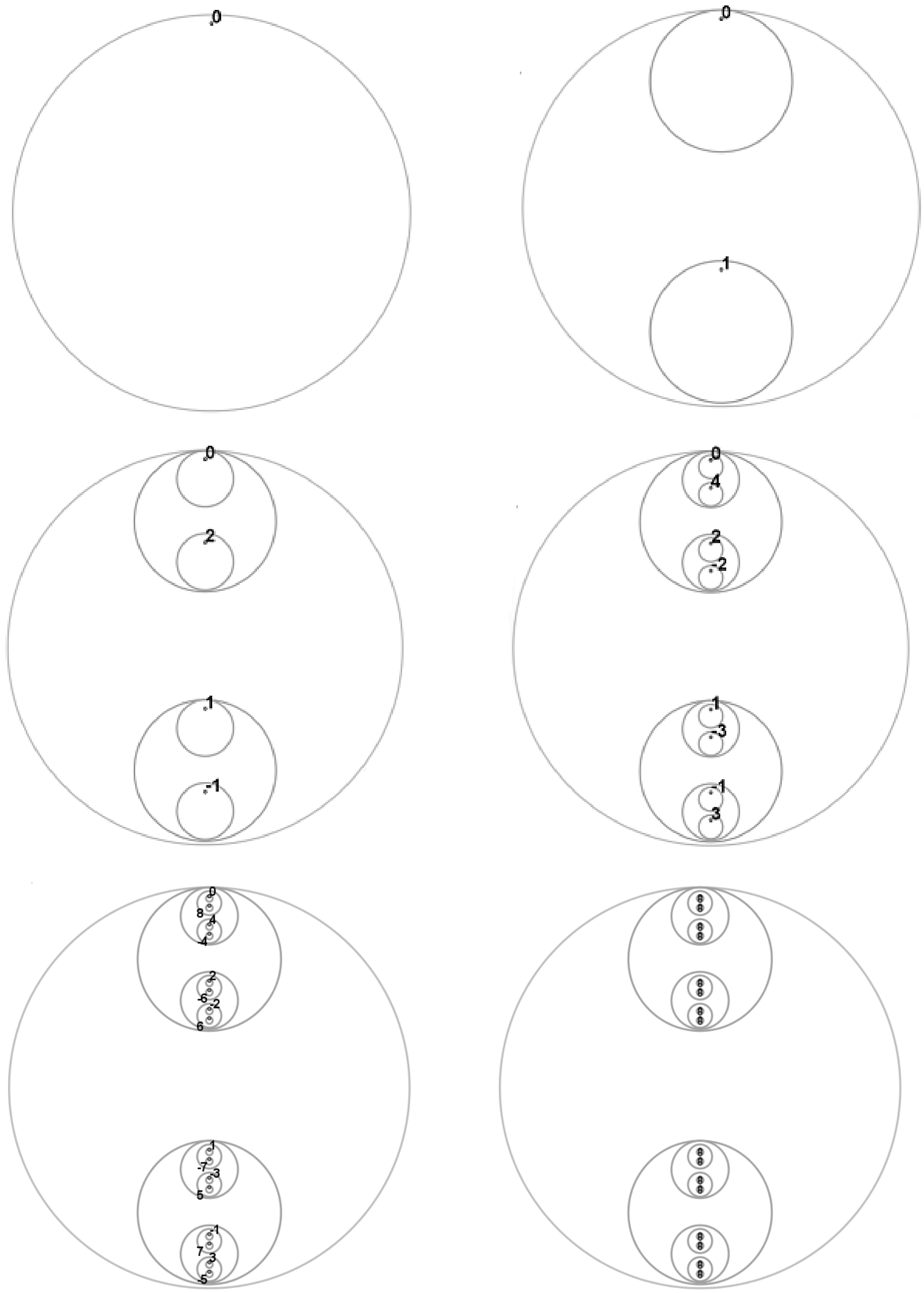
Para solucionar esto vamos a crear una nueva manera de visualizar los números enteros. Nos vamos a basar en que $\mathbb{Z} = \overline{B}(0,1)$ y en el Ejercicio 9. Según este ejercicio toda bola $B(a, p^n)$ es la unión disjunta de p bolas diferentes de radio p^{n-1}. Así la inclusión de las bolas puede ilustrarse del siguiente modo (para $p = 2, 3, 5, 7$):



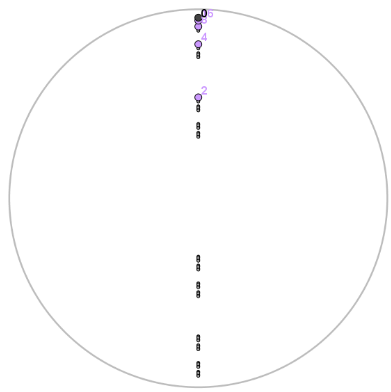
Cuando nos disponemos a ordenar los elementos de $\mathbb{Z}$ dentro de estas bolas vamos a hacerlo partiendo desde 0 e incluyendo de manera alternada los números positivos y negativos.

Ejemplo 3. Visualización con p=2.

La siguiente serie de imágenes ilustra el modo en el que se irían visualizando ordenada y sucesivamente los elementos de $\mathbb{Z}$ siguiendo el orden de $\{0, 1, -1, 2, -2, \dots\}$.

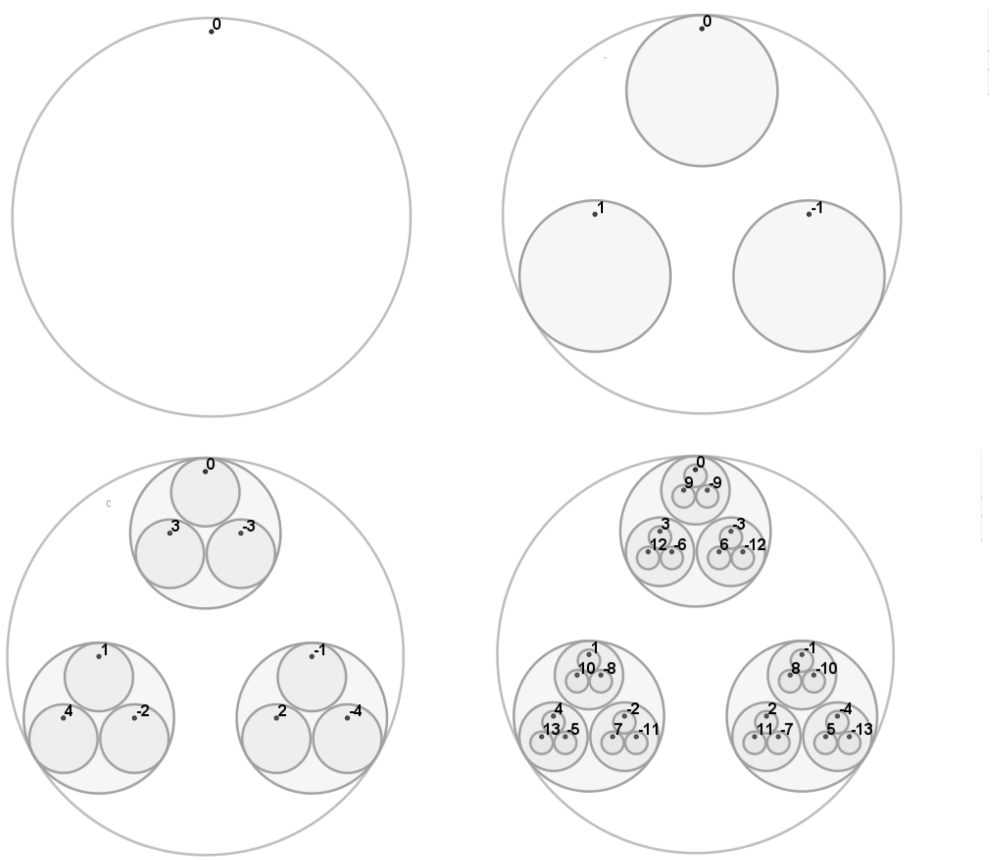


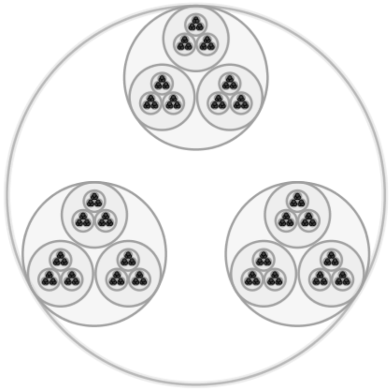
Podemos observar varias cosas. Para empezar, la distancia entre cualquier par de enteros x e y va a coincidir con el radio de la menor de las bolas cerradas que contienen a los dos números. De este modo se entiende mucho mejor el cumplimiento de la desigualdad ultramétrica definida en la Definición 2.1.1. También se puede observar que, entre otras cosas, se cumple el Ejercicio 7. Por último también resulta intuitiva la comprensión de que una sucesión converja a un elemento, por ejemplo $(2^n)_{n\in\mathbb{N}}$.



(La versión interactiva de esta imagen se encuentra en `https://www.geogebra.org/m/jfmvrpw8`)

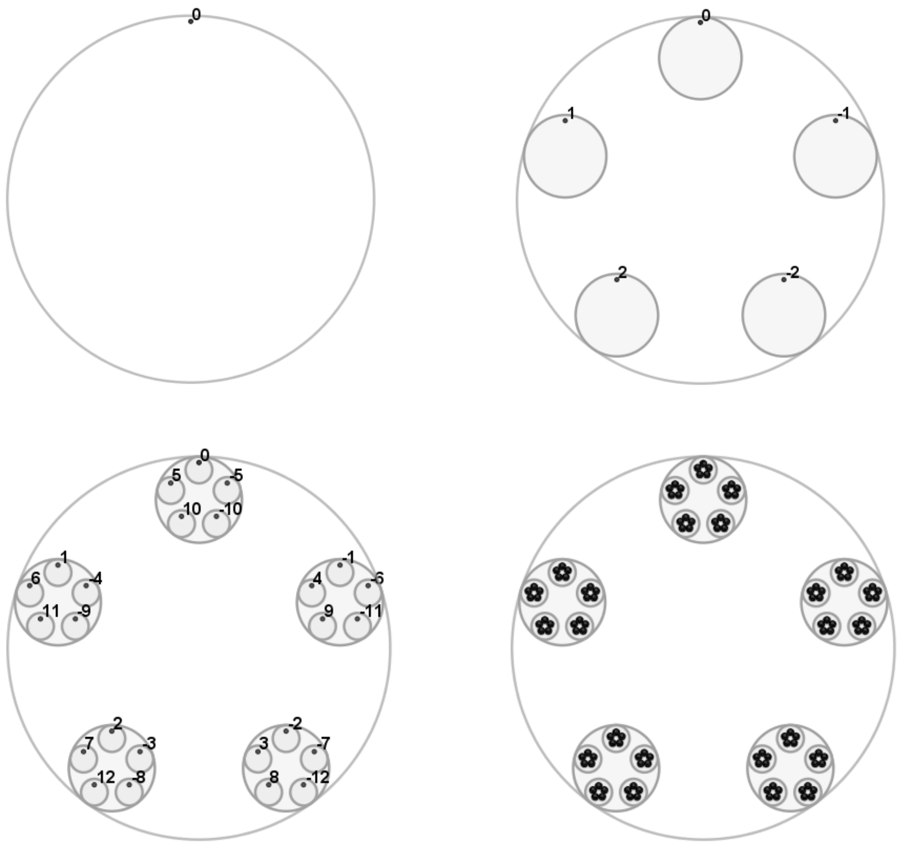
Ejemplo 4. Visualización con $p = 3$. Repitiendo la misma estrategia con el caso anterior, volvemos a obtener figuras de forma fractal.





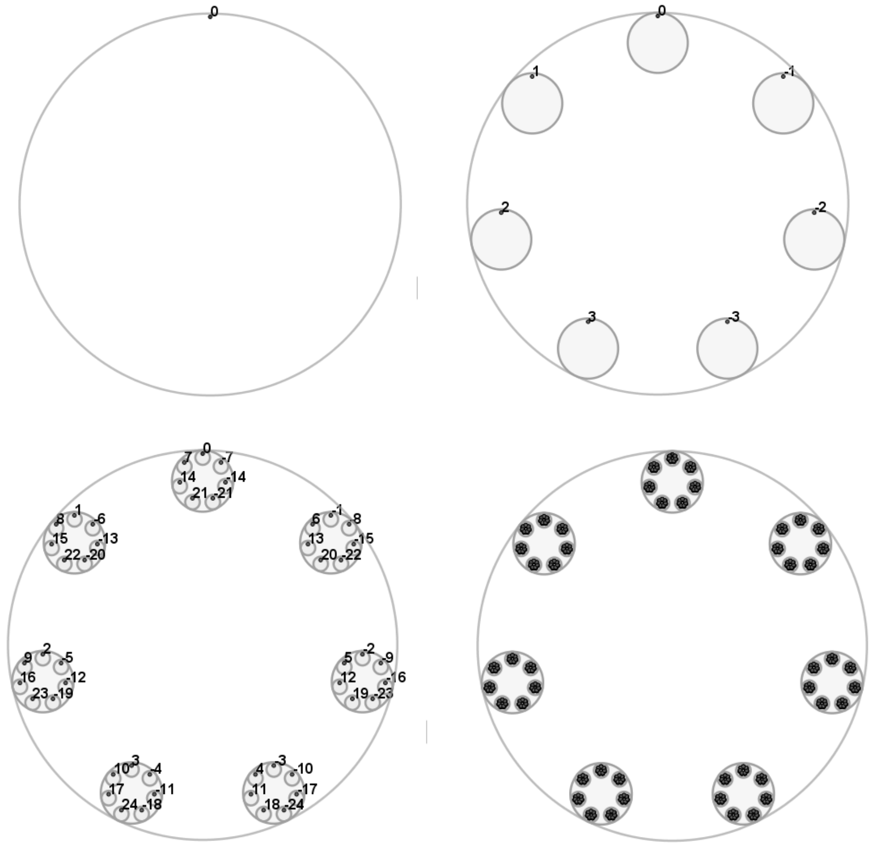
(La versión interactiva de esta imagen se encuentra en
`https://www.geogebra.org/m/dwp6msuj`)

Ejemplo 5. Visualización con $p = 5$.



(La versión interactiva de esta imagen se encuentra en
`https://www.geogebra.org/m/g9zdczgt`)

Ejemplo 6. Visualización con $p = 7$. Tenemos los siguientes resultados.



(La versión interactiva de esta imagen se encuentra en
`https://www.geogebra.org/m/frpvaxpr`)

Bibliografía

[1] Alexey Beshenov, *Introducción a los números p-ádicos*, Universidad de El salvador (2018).
http://cadadr.org/san-salvador/2018-04-numeros-p-adicos/numeros-p-adicos.pdf

[2] Gilles Bellot, *Introduction to p-adic numbers*, TU Dortmund University (2015).
https://bell0bytes.eu/content/images/mathematics/algnum/p-adic.pdf

[3] Pedro José Herrero Piñeyro, *Topología de Espacios Metricos*, OCW-Universidad de Murcia (2010).
https://www.um.es/web/innovacion/plataformas/ocw/listado-de-cursos/topologia-de-espacios-metricos/material-de-clase

[4] Oleksiy Dovgodhey, *Finite Ultrametric Balls*, Institute of Applied Mathematics and Mechanics of NASU (2019).
https://arxiv.org/abs/1810.03128

[5] Daniele Turchetti, *Buissons et balais*, Images des Mathématiques (2013).
https://images.math.cnrs.fr/Buissons-et-balais.html?lang=fr.

[6] Miguel Monsalve López ,*Una aplicación del análisis p-ádico*, La Gaceta de la RSME (2018).
http://gaceta.rsme.es/abrir.php?id=1435.