Introducción a los números p-ádicos

Alexey Beshenov (cadadr@gmail.com)

Universidad de El Salvador. Abril de 2018

Estos son mis apuntes para una serie de charlas con una introducción a los números p-ádicos que di para los estudiantes de la maestría en la Universidad de El Salvador. Otras fuentes recomendadas son [Kob1984] y [Kat2007]. Para más información sobre la topología de espacios métricos el lector puede consultar [Mun2000].

Índice

1 Recordatorio: espacios métricos

1.1. Definición. Un **espacio métrico** es un conjunto X dotado de una aplicación $d\colon X\times X\to\mathbb{R}_{\geq 0}$ (**distancia**) que satisface los siguientes axiomas.

M1) La distancia entre x e y es nula si y solamente si $x=y$:

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

para cualesquiera $x,y\in X$.

M2) La distancia es **simétrica**:

$$d(x,y)=d(y,x)$$

para cualesquiera $x,y\in X$.

M3) Se cumple la **desigualdad del triángulo**:

$$d(x,y)\leq d(x,z)+d(z,y)$$

para cualesquiera $x,y,z\in X$.

1.2. Definición. Sea (X,d) un espacio métrico. La **bola abierta** de radio $\epsilon>0$ centrada en $x_0\in X$ es el subconjunto

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

La **bola cerrada** correspondiente es el subconjunto

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

A todo espacio métrico (X,d) se puede asociar una topología.

1.3. Definición. Para un espacio métrico (X,d), la topología **inducida por la métrica** d es la topología que tiene como su base de conjuntos abiertos las bolas abiertas $B(x_0,\epsilon)$ para todo $x_0\in X$ y $\epsilon>0$.

Ejercicio 1.

1) Toda bola cerrada $\overline{B}(x_0,\epsilon)$ es cerrada en la topología de arriba.
2) La topología inducida por una métrica es Hausdorff (T2).

2 Normas

Nos va a interesar la situación cuando la métrica viene de una norma sobre un anillo conmutativo, o en particular un cuerpo.

2.1. Definición. Sea R un anillo conmutativo. Una **norma** sobre R es una aplicación $\|\cdot\|\colon R\to\mathbb{R}_{\geq 0}$ que satisface las siguientes propiedades.

N1) $\|x\|=0$ si y solamente si $x=0$.

N2) La norma es multiplicativa: $\|xy\|=\|x\|\cdot\|y\|$ para cualesquiera $x,y\in R$.

N3) Se cumple la **desigualdad del triángulo** $\|x+y\|\leq\|x\|+\|y\|$ para cualesquiera $x,y\in R$.

Se dice que $\|\cdot\|$ es una norma **no arquimediana**, si para cualesquiera $x,y\in R$ se cumple la **desigualdad ultramétrica**

N3*) $\|x+y\| \leq \max\{\|x\|, \|y\|\}$.

En el caso contrario, se dice que $\|\cdot\|$ es **arquimediana**.

Note que N2) implica que si $xy = 0$, entonces $x = 0$ o $y = 0$; es decir, según nuestra definición, el anillo conmutativo R no puede tener divisores de cero.

2.2. Ejemplo. Demuestre que para cualquier subanillo $R \subseteq \mathbb{C}$, el valor absoluto habitual

$$|x + y\sqrt{-1}| = \sqrt{x^2 + y^2}$$

es una norma arquimediana. ▲

Ejercicio 2. Demuestre que la multiplicatividad de la norma implica las siguientes propiedades:

1) $\|1\| = \|-1\| = 1$,
2) $\|-x\| = \|x\|$ para todo $x \in R$,
3) $\|x^n\| = \|x\|^n$ para todo $x \in R,\ n = 1, 2, 3, \ldots$,
4) $\|x^{-1}\| = \|x\|^{-1}$ para todo $x \in R^\times$.

2.3. Observación. *Si R es un anillo conmutativo con alguna norma $\|\cdot\|$, entonces la aplicación*

$$\begin{aligned} d\colon R \times R &\to \mathbb{R}_{\geq 0}, \\ (x, y) &\mapsto \|x - y\| \end{aligned}$$

*define una estructura de **espacio métrico** sobre R.*

Demostración. La propiedad M1) corresponde a N1) de 2.1. Luego, para M2), notamos que

$$\|x - y\| = \|-(x - y)\| = \|y - x\|.$$

En fin, M3) corresponde a N3):

$$\|x - y\| = \|(x - z) + (z - y)\| \leq \|x - z\| + \|z - y\|.$$

■

En particular, todo anillo conmutativo R con norma $\|\cdot\|$ lleva una topología inducida por $\|\cdot\|$. Cuando un anillo está equipado con una topología respecto a cual las operaciones son continuas, se dice que R es un **anillo topológico**. En particular, esto sucede cuando la topología está inducida por una norma.

Ejercicio 3. Deduzca de los axiomas de normas la **desigualdad del triángulo inversa**

$$\Big|\|x\| - \|y\|\Big| \leq \|x - y\|.$$

Note que esta significa que la norma $\|\cdot\|\colon R \to \mathbb{R}_{\geq 0}$ es una aplicación continua respecto a la topología habitual sobre $\mathbb{R}$ y la topología sobre R inducida por $\|\cdot\|$.

Ejercicio 4. Demuestre que si R es un anillo conmutativo con norma $\|\cdot\|$, entonces las operaciones

$$(x, y) \mapsto x + y, \quad (x, y) \mapsto x \cdot y, \quad x \mapsto -x$$

son continuas respecto a la topología inducida por $\|\cdot\|$. De la misma manera, para los elementos invertibles la operación $x \mapsto x^{-1}$ es continua. Note que todo esto es equivalente a demostrar que

1) para cualesquiera $x, y \in R$ y $\epsilon > 0$ existe $\delta > 0$ tal que

$$\|x' - x\| < \delta,\ \|y' - y\| < \delta \Longrightarrow \|(x' + y') - (x + y)\| < \epsilon;$$

2) para cualesquiera $x, y \in R$ y $\epsilon > 0$ existe $\delta > 0$ tal que

$$\|x' - x\| < \delta,\ \|y' - y\| < \delta \Longrightarrow \|x'y' - xy\| < \epsilon;$$

3) para todo $x \in R$ y $\epsilon > 0$ existe $\delta > 0$ tal que

$$\|x' - x\| < \delta \Longrightarrow \|(-x') - (-x)\| < \epsilon;$$

4) para todo $x \in R^\times$ y todo $\epsilon > 0$ existe $\delta > 0$ tal que

$$\|x' - x\| < \delta \Longrightarrow \|(x')^{-1} - x^{-1}\| < \epsilon.$$

2.4. Ejemplo. Para cualquier anillo conmutativo R tenemos la **norma trivial** definida por

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

Trivialmente, es no arquimediana. Más adelante vamos a ver ejemplos no triviales de normas no arquimedianas. ▲

2.5. Ejemplo. Sobre los cuerpos finitos $\mathbb{F}_q$ no hay normas no triviales. En efecto, el grupo de las unidades $\mathbb{F}_q^\times$ es cíclico de orden $q-1$, y por lo tanto para todo $a \neq 0$ en $\mathbb{F}_q$ tenemos $a^{q-1} = 1$. Luego, si $\|\cdot\|$ es una norma sobre $\mathbb{F}_q$, tenemos $\|a^{q-1}\| = \|a\|^{q-1} = 1$, así que $\|a\| = 1$. ▲

Ejercicio 5. Demuestre que si la norma $\|\cdot\|$ sobre R es trivial, entonces la topología inducida por $\|\cdot\|$ es discreta.

Ejercicio 6. Sea R un anillo conmutativo y sea $\|\cdot\|$ una norma sobre R. Demuestre que $\|\cdot\|$ se extiende de modo único a una norma sobre el cuerpo de fracciones $\mathrm{Frac}(R)$ mediante la fórmula

$$\left\| \frac{x}{y} \right\| = \frac{\|x\|}{\|y\|},$$

y si $\|\cdot\|$ es una norma no arquimediana, entonces su extensión a $\mathrm{Frac}(R)$ es no arquimediana.

Nos van a interesar las normas no arquimedianas (las que satisfacen $\|x + y\| \leq \max\{\|x\|, \|y\|\}$). Notemos que de los axiomas se sigue que si $\|x\| \neq \|y\|$, entonces $\|x + y\|$ es precisamente el máximo entre $\|x\|$ e $\|y\|$:

2.6. Observación. *Si $\|\cdot\|$ es una norma no arquimediana, entonces*

$$\|x + y\| = \max\{\|x\|, \|y\|\} \quad \textit{si } \|x\| \neq \|y\|.$$

Demostración. Supongamos que se cumple la desigualdad estricta

$$\|x + y\| < \max\{\|x\|, \|y\|\}.$$

Tenemos entonces

$$\|x\| = \|x + y - y\| \leq \max\{\|x + y\|, \|y\|\} = \|y\|$$

y

$$\|y\| = \|x + y - x\| \leq \max\{\|x + y\|, \|x\|\} = \|x\|,$$

así que $\|x\| = \|y\|$. ■

Por inducción se sigue que para las normas no arquimedianas

$$\|x_1 + \cdots + x_n\| \leq \max\{\|x_1\|, \ \ldots, \ \|x_n\|\},$$

y 2.6 implica que

$$\|x_1 + \cdots + x_n\| = \max\{\|x_1\|, \ \ldots, \ \|x_n\|\}$$

si entre $\|x_1\|, \ \ldots, \ \|x_n\|$ hay un valor que es estrictamente mayor que los otros.

He aquí una caracterización útil de normas no arquimedianas:

2.7. Observación. *Las siguientes condiciones son equivalentes:*

1) $\|\cdot\|$ *es una norma no arquimediana,*

2) *para todo* $n \in \mathbb{N}$ *se tiene*

$$\|\underbrace{1 + 1 + \cdots + 1}_{n}\| \leq 1.$$

Demostración. 1) $\Rightarrow$ 2) se demuestra por inducción. La base de inducción es $\|0\| = 0$ o $\|1\| = 1$. Luego, si $\|\cdot\|$ es no arquimediana, entonces

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

Para ver que 2) $\Rightarrow$ 1), consideremos

$$\|x + y\|^n = \|(x + y)^n\| = \left\| \sum_{0 \leq k \leq n} \binom{n}{k} x^k \, y^{n-k} \right\| \leq \sum_{0 \leq k \leq n} \left\| \binom{n}{k} \right\| \cdot \|x\|^k \cdot \|y\|^{n-k}.$$

Por nuestra hipótesis, $\left\|\binom{n}{k}\right\| \leq 1$, así que

$$\|x + y\|^n \leq \sum_{0 \leq k \leq n} \|x\|^k \cdot \|y\|^{n-k} \leq (n + 1) \max\{\|x\|, \|y\|\}^n.$$

Tomando las raíces n-ésimas, tenemos

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

que para $n \to +\infty$ nos da la desigualdad deseada. ■

2.8. Corolario.

1) *Si* R *es un subanillo de* S*, una norma* $\|\cdot\|$ *sobre* S *es no arquimediana si y solamente si su restricción a* R *es no arquimediana.*

2) *Si* R *es un anillo conmutativo de característica positiva, toda norma sobre* R *es no arquimediana.*

Demostración. 1) sigue de 2.7. En 2), si $\operatorname{char} R = n$, entonces $\mathbb{Z}/n\mathbb{Z} \subset R$. Si n no es primo, R tiene divisores de cero y por lo tanto no tiene ninguna norma. Si $n = p$, entonces la única norma sobre $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ es trivial, como hemos notado en 2.5. ■

3 Valuaciones

Las normas no arquimedianas normalmente surgen de valuaciones.

3.1. Definición. Una **valuación** sobre un anillo conmutativo R es una función

$$v\colon R \to \mathbb{Z} \cup \{+\infty\}$$

que satisface las siguientes propiedades:

V1) $v(x) = +\infty$ si y solamente si $x = 0$.

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

V3) La desigualdad ultramétrica $v(x+y) \geq \min\{v(x), v(y)\}$.

Note que en V2), si $xy = 0$, entonces $+\infty = v(x) + v(y)$, lo que quiere decir que $x = 0$ o $y = 0$. Esto significa que según nuestra definición, un anillo conmutativo con valuación es necesariamente un dominio de integridad.

Ejercicio 7. Demuestre que la propiedad V2) implica

1) $v(1) = v(-1) = 0$,

2) $v(-x) = v(x)$ para todo $x \in R$,

3) $v(x^n) = n\, v(x)$ para todo $x \in R,\ n = 1, 2, 3, \ldots$,

4) $v(x^{-1}) = -v(x)$ para todo $x \in R^\times$.

Ejercicio 8. Sea R un dominio de integridad y sea v una valuación sobre R. Entonces v se extiende de modo único a una valuación sobre el cuerpo de fracciones $\mathrm{Frac}(R)$ mediante la fórmula

$$v\left(\frac{x}{y}\right) = v(x) - v(y).$$

(Esto es similar al ejercicio 6.)

Ya conocemos bien un ejemplo de valuaciones.

3.2. Ejemplo. Sea R un dominio de integridad. Para el producto de dos polinomios $f, g \in R[X]$ se cumple

$$\deg(fg) = \deg f + \deg g.$$

Para que esta igualdad se cumpla en el caso cuando $f = 0$ es el polinomio nulo, se pone

$$\deg 0 := -\infty.$$

Para la suma de polinomios se tiene

$$\deg(f+g) \leq \max\{\deg f, \deg g\}.$$

Entonces,

$$v(f) := -\deg f$$

es una valuación sobre el anillo de polinomios. ▲

3.3. Ejemplo. De nuevo, sea R un dominio de integridad. Para un polinomio no nulo $f = \sum_{i\geq 0} a_i X^i \in R[X]$ definamos

$$v_X(f) := \min\{i \mid a_i \neq 0\}.$$

Si $f = 0$, pongamos

$$v_X(0) := +\infty.$$

Para el producto de dos polinomios $f = \sum_{i\geq 0} a_i X^i$ y $g = \sum_{j\geq 0} b_j X^j$ tenemos

$$fg = \sum_{k\geq 0} c_k X^k, \quad \text{donde } c_k = \sum_{i+j=k} a_i b_j.$$

Ahora si $v_X(f) = m$ y $v_X(g) = n$, se ve que $c_k = 0$ si $k < m+n$, mientras que $c_{m+n} = a_m b_n \neq 0$, puesto que $a_m \neq 0$ y $b_n \neq 0$. Entonces, podemos concluir que

$$v_X(fg) = v_X(f) + v_X(g).$$

Para la suma de dos polinomios, se ve que

$$v_X(f+g) \geq \min\{v_X(f), v_X(g)\}.$$

Entonces, lo que acabamos de definir es también una valuación sobre el anillo de polinomios. ▲

Ejercicio 9. Para toda valuación tenemos

$$v(x+y) = \min\{v(x), v(y)\} \quad \text{si } v(x) \neq v(y).$$

(Es similar a 2.6.)

3.4. Observación. *Si R es un anillo conmutativo con valuación v, fijemos un número real $0 < \rho \leq 1$. Entonces*

$$\|x\|_v := \rho^{v(x)}$$

define una norma no arquimediana sobre R.

(Si $\rho = 1$, se obtiene la norma trivial (2.4).)

Demostración. Tenemos $\|x\|_v = 0$ si y solamente si $v(x) = +\infty$, si y solamente si $x = 0$. Entonces, la propiedad V1) implica N1). Luego, V2) implica N2):

$$\|xy\|_v = \rho^{v(xy)} = \rho^{v(x)+v(y)} = \rho^{v(x)}\rho^{v(y)} = \|x\|_v \cdot \|y\|_v,$$

y V3) implica N3*): $\|x+y\|_v := \rho^{v(x+y)}$, donde $v(x+y) \geq \min\{v(x), v(y)\}$, y entonces

$$\|x+y\|_v \leq \max\{\|x\|_v, \|y\|_v\}.$$

■

4 Valuaciones y normas p-ádicas sobre $\mathbb{Q}$

Hemos desarrollado un poco de la teoría de normas y valuaciones, pero todavía no hemos visto muchos ejemplos, excepto 3.2 y 3.3. Ahora vamos a estudiar el ejemplo más importante para nosotros.

4.1. Definición. Fijemos un número primo $p = 2, 3, 5, 7, 11, 13, \ldots$ Para un número entero $n \in \mathbb{Z}$ su **valuación p-ádica** (u **orden p-ádico**) $v_p(n)$ es la potencia máxima de p que divide a n:

$$v_p(n) := \max\{k \mid p^k \mid n\}.$$

Para $n = 0$ se define

$$v_p(0) := +\infty.$$

En efecto $v_p(\cdot)$ es una valuación en el sentido de 3.1. Por la definición, tenemos $v_p(n) = +\infty$ si y solamente si $n = 0$. Luego, sean m, n dos enteros no nulos (si uno de ellos es nulo, las propiedades de valuaciones V2) y V3) son evidentes). Supongamos que las valuaciones p-ádicas correspondientes son $v_p(m) = k$ y $v_p(n) = \ell$; es decir, $m = p^k m'$, $n = p^\ell n'$, donde $p \nmid m'$, $p \nmid n'$. Luego, $mn = \ell^{k+\ell} m' n'$, donde $p \nmid m' n'$, entonces

$$v_p(mn) = v_p(m) + v_p(n).$$

Para la suma, sin pérdida de generalidad, supongamos que $k \le \ell$. Entonces $m + n = p^k (m' + p^{\ell-k} n')$, y

$$v_p(m+n) = v_p(p^k (m' + p^{\ell-k} n')) = v_p(p^k) + v_p(m' + p^{\ell-k} n') \ge v_p(p^k) = k = \min\{v_p(m), v_p(n)\}.$$

Así que v_p es una valuación sobre $\mathbb{Z}$. Como hemos visto en el ejercicio 8, v_p se extiende de modo único a una valuación sobre $\mathbb{Q}$ mediante la fórmula

$$v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n).$$

Para todo número $a \in \mathbb{Q}^\times$ se tiene la factorización en primos

$$a = \pm \prod_{p \text{ primo}} p^{v_p(a)}.$$

4.2. Ejemplo.

$$v_2(128) = v_2(2^7) = 7, \quad v_3(57) = v_3(3 \cdot 19) = 1, \quad v_7(10^{2018}) = 0, \quad v_3(9!) = v_3(2^7 \cdot 3^4 \cdot 5 \cdot 7) = 4,$$
$$v_2(128/7) = 7, \quad v_7(128/7) = -1, \quad v_2(-800/23) = v_2(-2^5 \cdot 5^2/23) = 5.$$

▲

La siguiente desigualdad es trivial, pero es útil en algunos casos.

4.3. Observación. *Para $n \ge 1$ tenemos*

$$v_p(n) \le \lfloor \log_p(n) \rfloor.$$

Ejercicio 10.

1) Demuestre que para los coeficientes binomiales se tiene

$$v_p\left(\binom{p}{n}\right) = 1 \quad \text{para todo } n = 1, 2, \ldots, p-1.$$

2) En general, demuestre que

$$v_p\left(\binom{p^k}{n}\right) = k - v_p(n) \quad \text{para todo } n = 1, 2, \ldots, p^k.$$

Sugerencia: calcule las valuaciones p-ádicas de ambos lados de la identidad

$$n!\binom{p^k}{n} = p^k (p^k - 1)(p^k - 2) \cdots (p^k - n + 1).$$

Note que $v_p(p^k - a) = v_p(a)$ para todo $a = 1, 2, \ldots, p^k - 1$ (véase el ejercicio 9).

He aquí un cálculo curioso de las valuaciones p-ádicas.

4.4. Observación (Fórmula de Legendre). *Para un número natural n,*

$$v_p(n!) = \sum_{i\geq 1} \lfloor n/p^i \rfloor = \frac{n - s_p(n)}{p-1},$$

donde $s_p(n) := \sum_i a_i$ denota la suma de sus dígitos en la base p:

$$n = a_0 + a_1\, p + a_2\, p^2 + \cdots + a_k\, p^k, \quad 0 \leq a_i < p.$$

4.5. Ejemplo. Un par de ejemplos específicos:

$$5 = 1 + 2^2,$$

y

$$v_2(5!) = 5 - 2 = 3 = v_2(2^3 \cdot 3 \cdot 5).$$

Otro ejemplo:

$$2018 = 2 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10},$$

y entonces

$$v_2(2018!) = 2018 - 7 = 2011.$$

▲

Demostración de 4.4. Entre los números $1, 2, \ldots, n$, precisamente $\lfloor n/p^i \rfloor$ son divisibles por p^i. Entre estos números, algunos pueden ser divisibles por potencias superiores de p. En total, tenemos

$$\lfloor n/p^i \rfloor - \lfloor n/p^{i+1} \rfloor$$

números de valuación p-ádica igual a i. Entonces,

$$v_p(n!) = (\lfloor n/p \rfloor - \lfloor n/p^2 \rfloor) + 2\,(\lfloor n/p^2 \rfloor - \lfloor n/p^3 \rfloor) + 3\,(\lfloor n/p^3 \rfloor - \lfloor n/p^4 \rfloor) + \cdots$$

(note que la suma es finita: $\lfloor n/p^i \rfloor = 0$ para $i \gg 0$). Simplificando esta expresión, tenemos

$$v_p(n!) = \sum_{i\geq 1} \lfloor n/p^i \rfloor.$$

Ahora para la expansión de n en la base p

$$n = a_0 + a_1\, p + a_2\, p^2 + \cdots + a_k\, p^k$$

notemos que

$$\lfloor n/p^j \rfloor = a_j + a_{j+1}\, p + a_{j+2}\, p^2 + \cdots + a_k\, p^{k-j}.$$

Luego,

$$\begin{aligned} v_p(n!) = \sum_{1\leq j\leq k} \lfloor n/p^j \rfloor &= \sum_{1\leq j\leq k} (a_j + a_{j+1}\, p + a_{j+2}\, p^2 + \cdots + a_k\, p^{k-j}) = \sum_{1\leq i\leq k} \sum_{1\leq j\leq i} a_i\, p^{i-j} \\ &= \sum_{1\leq i\leq k} a_i \sum_{0\leq \ell\leq i-1} p^\ell = \sum_{1\leq i\leq k} a_i \frac{p^i - 1}{p-1} = \frac{1}{p-1}\Big(\sum_{1\leq i\leq k} a_i\, p^i - \sum_{1\leq i\leq k} a_i\Big) \\ &= \frac{1}{p-1}\Big(\sum_{0\leq i\leq k} a_i\, p^i - \sum_{0\leq i\leq k} a_i\Big) = \frac{n - \sum_i a_i}{p-1}. \end{aligned}$$

■

Ejercicio 11. Demuestre que

$$v_p(p^k!) = \frac{p^k - 1}{p-1} = 1 + p + p^2 + \cdots + p^{k-1},$$
$$v_p((a\,p^k)!) = \frac{a\,p^k - a}{p-1} = a\,(1 + p + p^2 + \cdots + p^{k-1}) \quad \text{para } 0 \le a \le p-1.$$

Ejercicio 12. Demuestre la cota

$$v_p\left(\binom{m}{n}\right) \le \lfloor \log_p m \rfloor - v_p(n).$$

Sugerencia: la fórmula de Legendre nos dice que

$$v_p\left(\binom{m}{n}\right) = \sum_{i \ge 1} (\lfloor m/p^i \rfloor - \lfloor n/p^i \rfloor - \lfloor (m-n)/p^i \rfloor).$$

Note que cada término de esta suma es igual a 0 o 1, y es siempre igual a 0 para $k \le v_p(n)$ y para $k > \lfloor \log_p m \rfloor$.

Como hemos visto en 3.4, toda valuación $v(\cdot)$ define una norma no-arquimediana $\|\cdot\|_v := \rho^{v(\cdot)}$, donde $0 < \rho \le 1$ es algún parámetro fijo. Para la valuación p-ádica v_p normalmente se escoge $\rho = 1/p$.

4.6. Definición. Sea p un número primo. Para $a \in \mathbb{Q}$ la **norma p-ádica** es dada por

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

Por supuesto, se puede considerar $\rho^{-v_p(a)}$ para cualquier $0 < \rho < 1$, y la norma que se obtiene va a ser equivalente a $|\cdot|_p$ (en cierto sentido preciso que vamos a investigar más adelante).

Note que para $m, n \in \mathbb{Z}$, la relación $m \equiv n \pmod{p^k}$ significa precisamente que $|m-n|_p \le 1/p^k$: los números son cercanos en la métrica p-ádica $d(m,n) := |m-n|_p$ si son congruentes módulo una potencia alta de p.

Para un número racional $a \in \mathbb{Q}$ y un primo p, si tenemos $|a|_p \le 1$, esto quiere decir que $v_p(a) \ge 0$; en otras palabras, que p no aparece en el denominador de a. Así que

$$\{a \in \mathbb{Q} \mid |a|_p \le 1\} = \{m/n \mid p \nmid n\} = \mathbb{Z}_{(p)},$$

donde $\mathbb{Z}_{(p)}$ denota la **localización** de $\mathbb{Z}$ afuera del ideal primo $(p) \subset \mathbb{Z}$. Luego,

$$\bigcap_p \mathbb{Z}_{(p)} = \{a \in \mathbb{Q} \mid |a|_p \le 1 \text{ para todo } p\} = \mathbb{Z}.$$

Es un caso particular de la identidad

$$\bigcap_{\substack{\mathfrak{m} \subset R \\ \text{ideal maximal}}} R_{\mathfrak{m}} = R$$

que se cumple para cualquier dominio de integridad R.

La normalización $\rho = 1/p$ en la definición de la norma p-ádica se usa para que se cumpla la siguiente identidad importante.

Ejercicio 13 (Fórmula del producto)**.** Demuestre que para todo $a \in \mathbb{Q}^\times$ se cumple

$$\prod_p |a|_p = 1,$$

donde el producto es sobre todos los números primos y $p = \infty$ y $|a|_\infty := |a|$ denota el valor absoluto habitual (arquimediano). El producto tiene sentido, ya que para a fijo $|a|_p \ne 1$ (es decir, $v_p(a) \ne 0$) para un número finito de valores de p.

Ejercicio 14. Usando la fórmula del producto, demuestre que para todo $n = 1, 2, 3, 4, \ldots$ se cumple $|n|_p \geq 1/n$.

Veremos alguna aplicación de las normas p-ádicas.

4.7. Aplicación. El n-ésimo **número armónico** es la suma de los recíprocos de los primeros n enteros positivos:

$$H_n := \sum_{1 \leq k \leq n} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + + \frac{1}{n}.$$

He aquí los primeros de estos números:

$$H_1 = 1,\ H_2 = \frac{3}{2},\ H_3 = \frac{11}{6},\ H_4 = \frac{25}{12},\ H_5 = \frac{137}{60},\ H_6 = \frac{49}{20},\ H_7 = \frac{363}{140},\ H_8 = \frac{761}{280},\ H_9 = \frac{7129}{2520}.$$

Se ve que $H_n \notin \mathbb{Z}$ para $n > 1$. ¿Cómo podemos demostrarlo? Se ve que en los denominadores aparecen potencias de 2. Podemos separarlas para calcular las normas 2-ádicas correspondientes:

$$\begin{aligned}
H_2 &= 1 + \frac{1}{2} = \frac{3}{2}, \\
H_3 &= 1 + \frac{1}{2} + \frac{1}{3} = \frac{11}{2 \cdot 3}, \\
H_4 &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2^2} = \frac{25}{2^2 \cdot 3}, \\
H_5 &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2^2} + \frac{1}{5} = \frac{137}{2^2 \cdot 3 \cdot 5}, \\
H_6 &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2^2} + \frac{1}{5} + \frac{1}{2 \cdot 3} = \frac{49}{2^2 \cdot 5}, \\
H_7 &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2^2} + \frac{1}{5} + \frac{1}{2 \cdot 3} + \frac{1}{7} = \frac{363}{2^2 \cdot 5 \cdot 7}, \\
H_8 &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2^2} + \frac{1}{5} + \frac{1}{2 \cdot 3} + \frac{1}{7} + \frac{1}{2^3} = \frac{761}{2^3 \cdot 5 \cdot 7}, \\
H_9 &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{2^2} + \frac{1}{5} + \frac{1}{2 \cdot 3} + \frac{1}{7} + \frac{1}{2^3} + \frac{1}{3^2} = \frac{7129}{2^3 \cdot 3^2 \cdot 5 \cdot 7}.
\end{aligned} \tag{4.1}$$

Si $2^\ell \leq n < 2^{\ell+1}$, entonces para $k = 1, \ldots, n$ tenemos $|1/k|_2 \leq 2^\ell$. Además, el único término en la suma $\sum_{1 \leq k \leq n} 1/k$ con 2^ℓ en el denominador es $1/2^\ell$. Entonces, la desigualdad ultramétrica nos da la *igualdad*

$$\left| \sum_{1 \leq k \leq n} 1/k \right|_2 = \max_{1 \leq k \leq n} \{|1/k|_2\} = 2^\ell.$$

Esto demuestra que para $n > 1$ el número H_n tiene 2^ℓ en el denominador (donde $\ell = \lfloor \log_2 n \rfloor$) y por lo tanto no es entero.

Note que para los primos diferentes de 2 el mismo argumento no demuestra que $|H_n|_p \xrightarrow{n \to \infty} +\infty$ (es decir, $v_p(H_n) \xrightarrow{n \to \infty} -\infty$): la potencia máxima de p puede aparecer dos veces en los denominadores, como, por ejemplo, 3 en la suma (4.1).

n:	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$v_2(H_n)$:	−1	−1	−2	−2	−2	−2	−3	−3	−3	−3	−3	−3	−3	−3	−4	−4	−4
$v_3(H_n)$:	1	−1	−1	−1	0	1	0	−2	−2	−2	−2	−2	−2	−2	−2	−2	−1
$v_5(H_n)$:	0	0	2	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1
$v_7(H_n)$:	0	0	0	0	2	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1

4.8. Aplicación. El siguiente resultado es conocido como el **lema de Gauss** (*Disquisitiones Arithmeticae*, Artículo 42).
Si $f \in \mathbb{Z}[X]$ es un polinomio mónico con coeficientes enteros y $f(X) = g(X) \cdot h(X)$ para algunos polinomios mónicos $g(X), h(X) \in \mathbb{Q}[X]$, entonces los coeficientes de g y h son enteros.

He aquí la observación clave que dejo como un ejercicio.

Ejercicio 15. Sea k un cuerpo con norma no-arquimediana $\|\cdot\|$. Para un polinomio $g(X) = \sum_i a_i X^i \in k[X]$ definamos su **norma de Gauss** correspondiente como el máximo de las normas de sus coeficientes:

$$\|g(X)\| := \max_i \{\|a_i\|\}.$$

Demuestre que

$$\|g(X) \cdot h(X)\| = \|g(X)\| \cdot \|h(X)\|.$$

Ahora podemos volver al lema de Gauss. Si $f(X) = g(X) \cdot h(X)$, donde $f(X)$ es mónico y tiene coeficientes enteros, entonces para todo p

$$|g(X)|_p \cdot |h(X)|_p = |f(X)|_p = 1$$

—el coeficiente mayor de $f(X)$ es 1, y los coeficientes enteros tienen normas $|a_i|_p \leq 1$. Luego, si $g(X)$ y $h(X)$ son mónicos, entonces $|g(X)|_p \geq 1$ y $|h(X)|_p \geq 1$, y la última identidad nos da

$$|g(X)|_p = |h(X)|_p = 1.$$

Esto significa que p no aparece en los denominadores de los coeficientes de $g(X)$ y $h(X)$; es decir, $g(X), h(X) \in \mathbb{Z}_{(p)}[X]$. Aplicado para todo p, este argumento demuestra que $g(X)$ y $h(X)$ tienen coeficientes en

$$\bigcap_p \mathbb{Z}_{(p)} = \mathbb{Z}.$$

■

La demostración usa idea muy común: para ver que $x \in \mathbb{Z}$, se puede demostrar por separado que $x \in \mathbb{Z}_{(p)}$ para todo primo p.

5 Espacios ultramétricos

5.1. Definición. Si (X, d) es un espacio métrico donde en lugar de la desigualdad del triángulo se cumple la propiedad más fuerte

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

se dice que X es un **espacio ultramétrico**.

5.2. Observación. *Sea R es un anillo conmutativo con alguna norma no-arquimediana $\|\cdot\|$. La distancia*

$$d(x, y) := \|x - y\|$$

define una estructura de espacio ultramétrico.

Demostración. La propiedad N3*) corresponde a M3*). ■

5.3. Ejemplo. $\mathbb{Z}$ y $\mathbb{Q}$ son espacios ultramétricos respecto a la distancia p-ádica $d(a, b) := |a - b|_p$. ▲

Nuestra intuición para espacios métricos normalmente viene del ejemplo más común y geométrico, que es $\mathbb{R}^n$ con la distancia habitual inducida por el valor absoluto arquimediano $|\cdot|$. Si X es un espacio ultramétrico (en particular, un cuerpo con una norma no-arquimediana), muchas propiedades topológicas de X son bastante contraintuitivas. Dediquemos esta sección a las propiedades de espacios ultramétricos.

5.4. Observación. *En un espacio ultramétrico, todo punto de una bola abierta es su centro: si* $y_0 \in B(x_0, \epsilon)$, *entonces* $B(y_0, \epsilon) = B(x_0, \epsilon)$.

Demostración. Si $x, y_0 \in B(x_0, \epsilon)$, entonces

$$d(x, x_0) < \epsilon, \quad d(x_0, y_0) < \epsilon,$$

y luego

$$d(x, y_0) \leq \max\{d(x, x_0), d(x_0, y_0)\} < \epsilon.$$

Así que $B(x_0, \epsilon) \subseteq B(y_0, \epsilon)$. De la misma manera, $B(y_0, \epsilon) \subseteq B(x_0, \epsilon)$. ■

Otro resultado inesperado:

5.5. Observación. *En un espacio ultramétrico, la esfera de radio* $r > 0$

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

es un subconjunto abierto.

Demostración. Para $x \in S_r(x_0)$ y $\epsilon < r$ tenemos $B(x, \epsilon) \subset S_r(x_0)$. En efecto, si $y \in B(x, \epsilon)$, tenemos $d(y, x) < \epsilon < r$, y luego

$$d(y, x_0) \leq \max\{d(y, x), d(x, x_0)\} = r,$$

así que $y \in S_r(x_0)$. ■

5.6. Observación. *En un espacio ultramétrico,*

1) *las bolas abiertas* $B(x_0, \epsilon)$ *son conjuntos cerrados al mismo tiempo,*
2) *las bolas cerradas* $\overline{B}(x_0, \epsilon)$ *son conjuntos abiertos al mismo tiempo.*

(Note que *no* estamos diciendo que toda bola abierta $B(x_0, \epsilon)$ coincide con una bola cerrada $\overline{B}(x_0, \epsilon')$ para algún ϵ' y viceversa. Esto sucede cuando los valores de $d(\cdot, \cdot)$ son discretos, pero en general es falso.)

Demostración. En 1) necesitamos ver que

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

es un conjunto abierto. En efecto, es la union de la esfera

$$S_\epsilon(x_0) = \{x \in X \mid d(x, x_0) = \epsilon\},$$

que es abierta según 5.5, y el conjunto

$$X \setminus \overline{B}(x_0, \epsilon) = \{x \in X \mid d(x, x_0) > \epsilon\}$$

que es abierto según el ejercicio 1. De la misma manera en 2), tenemos

$$\overline{B}(x_0, \epsilon) = \{x \in X \mid d(x, x_0) \leq \epsilon\} = B(x_0, \epsilon) \cup S_\epsilon(x_0),$$

que es la unión de dos conjuntos abiertos. ■

En particular, en un espacio ultramétrico, $\overline{B}(x_0, \epsilon)$ *no es* la clausura de $B(x_0, \epsilon)$, ya que $B(x_0, \epsilon)$ es un conjunto cerrado.

Ejercicio 16. Recordemos que la **frontera** de un subespacio $A \subset X$ es dada por la intersección de la clausura de A con la clausura del complemento de A:

$$\operatorname{fr} A := \overline{A} \cap \overline{X \setminus A}.$$

Nuestra intuición para $\mathbb{R}^n$ diría que $\operatorname{fr} B(x_0, \epsilon) = S_\epsilon(x_0)$, pero es falso en un espacio ultramétrico. Demuestre que en este caso $\operatorname{fr} B(x_0, \epsilon) = \emptyset$.

Recordemos la noción de espacio conexo.

5.7. Definición. Se dice que un espacio topológico X es **inconexo** si $X = U \cup V$, para algunos subconjuntos abiertos no vacíos $U \subset X$ y $V \subset X$ tales que $U \cap V = \emptyset$. (Note que en este caso U y V son también cerrados.)

Si X no es **inconexo**, se dice que X es **conexo**.

Por ejemplo, $\mathbb{R}$ es conexo. Todo espacio ultramétrico es inconexo en el peor sentido posible.

5.8. Observación. *Todo espacio ultramétrico es* ***totalmente inconexo****: los únicos subespacios conexos de X son $\emptyset$ y $\{x\}$ para $x \in X$.*

Demostración. Esto sigue de la misma propiedad que las bolas abiertas son cerradas. Para $x \in X$, sea $A \subset X$ un subconjunto tal que $\{x\} \subsetneq A$. Tenemos $B(x, \epsilon) \cap A \neq A$ para algún $\epsilon > 0$. Luego, tenemos la unión disjunta

$$A = (B(x, \epsilon) \cap A) \cup ((X \setminus B(x, \epsilon)) \cap A),$$

donde $B(x, \epsilon)$ y $X \setminus B(x, \epsilon)$ son abiertos. ■

6 Límites y sucesiones de Cauchy

Recordemos algunas nociones de análisis. Voy a formular todo para un anillo conmutativo R dotado de una norma $\|\cdot\|$, arquimediana o no arquimediana.

6.1. Definición. Se dice que una sucesión $(a_n)_n$ de elementos de R tiene **límite** $a \in R$ respecto a $\|\cdot\|$ y se escribe

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

si para todo $\epsilon > 0$ existe N tal que

$$\|a - a_n\| < \epsilon \quad \text{para todo } n > N.$$

6.2. Ejemplo. Sea $a_n := 1 + p + p^2 + \cdots + p^n$. La sucesión $(a_n)_n$ tiene límite en $\mathbb{Q}$ respecto a la norma p-ádica:

$$\lim_{n \to \infty} a_n = \frac{1}{1-p}.$$

En efecto, esto sigue de

$$\left| a_n - \frac{1}{1-p} \right|_p = \left| \frac{(1-p)(1 + p + p^2 + \cdots + p^n) - 1}{1-p} \right|_p = \left| \frac{p^{n+1}}{p-1} \right|_p = |p^{n+1}|_p = \frac{1}{p^{n+1}}.$$

▲

Ejercicio 17. Demuestre que para la sucesión

$$a_n := 1 - p + p^2 - p^3 + \cdots + (-1)^n p^n$$

se tiene

$$\lim_{n \to \infty} a_n = \frac{1}{1+p}$$

respecto a la norma p-ádica.

Ejercicio 18. Supongamos que $\|\cdot\|$ es una norma no arquimediana sobre algún cuerpo. Como siempre, en análisis, la serie $\sum_{n\geq 0} a_n$ denota el límite de la sucesión de las sumas parciales $\sum_{0\leq n\leq k} a_n$.

1) Demuestre que la serie geométrica $\sum_{n\geq 0} x^n$ converge si y solamente si $\|x\| < 1$ y en este caso

$$\sum_{n\geq 0} x^n = \frac{1}{1-x}.$$

2) Calcule las series

$$1 - p + p^2 - p^3 + p^4 - p^5 + \cdots$$

y

$$1 + (p-1)\,p + p^2 + (p-1)\,p^3 + p^4 + (p-1)\,p^5 + \cdots$$

en $\mathbb{Q}$ respecto a la norma p-ádica.

6.3. Definición. Se dice que $(a_n)_n$ es una **sucesión de Cauchy** respecto a $\|\cdot\|$ si para todo $\epsilon > 0$ existe N tal que

$$\|a_m - a_n\| < \epsilon \quad \text{para cualesquiera } m, n > N.$$

6.4. Observación. *Si una sucesión $(a_n)_n$ tiene límite respecto a $\|\cdot\|$, entonces es una sucesión de Cauchy respecto a $\|\cdot\|$.*

Demostración. Si $\lim_{n\to\infty} a_n = a$, entonces para todo $\epsilon > 0$ existe N tal que

$$\|a - a_n\| < \epsilon/2 \quad \text{para todo } n > N.$$

Luego, por la desigualdad del triángulo, para cualesquiera $m, n > N$ tenemos

$$\|a_m - a_n\| = \|(a - a_n) - (a - a_m)\| \leq \|a - a_n\| + \|a - a_m\| \leq \epsilon.$$

■

6.5. Ejemplo. Para todo $a \in R$, tenemos la sucesión constante (a) definida por $a_n := a$ para todo $n \in \mathbb{N}$. Obviamente, es una sucesión de Cauchy. ▲

En nuestra notación "$\lim_{n\to\infty} a_n$" la norma es implícita. Por supuesto, una sucesión puede tener diferentes límites respecto a diferentes normas, o tener límite respecto a una norma y no tenerlo respecto a otra.

Ejercicio 19.

1) Demuestre que la sucesión $a_n = p^n$ no tiene límite respecto al valor absoluto habitual $|\cdot|$ sobre $\mathbb{Q}$, pero a_n tiende a 0 respecto a la norma p-ádica $|\cdot|_p$. Demuestre que no es de Cauchy respecto a $|\cdot|_q$ para $q \neq p$.

2) Demuestre que la sucesión $a_n := \frac{p^n}{p^n+1}$ tiene límites diferentes respecto a $|\cdot|_p$ y respecto al valor absoluto habitual $|\cdot|$.

3) Construya una sucesión de números enteros que converja a dos números diferentes respecto a $|\cdot|_p$ y $|\cdot|_q$ donde $p \neq q$ son dos primos fijos diferentes.

Los ejemplos de arriba son bastante tontos, pero algunos principiantes creen que, por ejemplo, si una sucesión $a_n \in \mathbb{Q}$ tiende a algún número racional respecto a $|\cdot|_p$ y respecto a otro número racional respecto a $|\cdot|$, entonces los dos límites coinciden. Como acabamos de ver, es totalmente falso.

Ejercicio 20. Demuestre que las siguientes sucesiones de números racionales no son de Cauchy respecto a ninguna de las normas p-ádicas $|\cdot|_p$:

1) 1, 1/10, 1/100, 1/1000, 1/10000, …;

2) 1, 1/2, 1/3, 1/4, 1/5, …;

3) $a_n := \sum_{0 \le i \le n} i$.

Ejercicio 21. Para la sucesión $a_n := \frac{n!}{n!+1}$, encuentre su límite respecto a todas las normas p-ádicas $|\cdot|_p$ y respecto al valor absoluto habitual $|\cdot|$.

6.6. Observación. *Si $(a_n)_n$ es una sucesión de Cauchy, entonces las normas $(\|a_n\|)_n$ forman una sucesión de Cauchy en $\mathbb{R}$; en particular, el límite $\lim_{n\to\infty} \|a_n\|$ existe.*

Demostración. Si $(a_n)_n$ es una sucesión de Cauchy, entonces para todo $\epsilon > 0$ existe N tal que

$$\|a_m - a_n\| < \epsilon \quad \text{para cualesquiera } m, n > N.$$

Luego, por la desigualdad del triángulo inversa,

$$\Big|\|a_m\| - \|a_n\|\Big| \le \|a_m - a_n\|.$$

■

7 Equivalencia de normas

Para simplificar la exposición, vamos a introducir la siguiente noción solamente para normas sobre cuerpos.

7.1. Definición. Se dice que dos normas $\|\cdot\|_1$ y $\|\cdot\|_2$ sobre un cuerpo F son **equivalentes** si se cumple una de las siguientes condiciones:

1) una sucesión en F es de Cauchy respecto a $\|\cdot\|_1$ si y solamente si es de Cauchy respecto a $\|\cdot\|_2$;

2) para todo $x \in F$ tenemos
$$\|x\|_1 < 1 \iff \|x\|_2 < 1;$$

2′) para todo $x \in F$ tenemos

$$\|x\|_1 < 1 \iff \|x\|_2 < 1, \tag{7.1}$$
$$\|x\|_1 > 1 \iff \|x\|_2 > 1, \tag{7.2}$$
$$\|x\|_1 = 1 \iff \|x\|_2 = 1; \tag{7.3}$$

3) existe algún $\alpha > 0$ tal que $\|x\|_1 = \|x\|_2^\alpha$ para todo $x \in F$;

4) $\|\cdot\|_1$ y $\|\cdot\|_2$ inducen la misma topología sobre F.

En general, para normas sobre *anillos*, las condiciones de arriba son diferentes. Por ejemplo, sobre $\mathbb{Z}$, podemos considerar la norma trivial (definida por $\|n\| = 1$ para todo $n \neq 0$) y el valor absoluto habitual $|\cdot|$. Luego, una sucesión $(a_n)_n$ es de Cauchy si y solamente si $a_n = a_m$ para $m, n \gg 0$, así que se cumple la condición 1). También se cumple 4): ambas normas inducen la topología discreta: $B(n,\epsilon) = \{n\}$ para $\epsilon < 1$ respecto a ambas normas. Sin embargo, 2), 2′), 3) no se cumplen.

También notemos que la condición 3) no significa que si $\|\cdot\|$ es una norma sobre F, entonces $\|\cdot\|^\alpha$ es también una norma para todo $\alpha > 0$. Por ejemplo, si $|\cdot|$ es el valor absoluto habitual sobre $\mathbb{Q}$, entonces $|\cdot|^2$ no es una norma: tenemos $|1+1|^2 > |1|^2 + |1|^2$, así que la desigualdad de triángulo no se cumple.

Ejercicio 22. Sea $|\cdot|$ el valor absoluto habitual sobre $\mathbb{Q}$. Encuentre para cuáles valores $\alpha > 0$ la función $x \mapsto |x|^\alpha$ es una norma sobre $\mathbb{Q}$.

Ahora demostremos que las condiciones 1), 2), 2′), 3), 4) son equivalentes.

Para la implicación 1) $\Rightarrow$ 2), supongamos que una sucesión es de Cauchy respecto a $\|\cdot\|_1$ si y solamente si lo es respecto a $\|\cdot\|_2$. Si tenemos $\|x\|_1 < 1$, entonces la sucesión $(x^n)_n$ es de Cauchy respecto a $\|\cdot\|_1$: tenemos

$$\|x^n\|_1 = \|x\|_1^n \xrightarrow{n\to\infty} 0.$$

Ahora si $\|x\|_2 > 1$, entonces

$$\|x^n\|_2 = \|x\|_2^n \xrightarrow{n\to\infty} \infty,$$

y $(a_n)_n$ no es de Cauchy respecto a $\|\cdot\|_2$. Si $\|x\|_2 = 1$, tenemos

$$\|x^{n+1} - x^n\|_2 = \|x-1\|_2 \cdot \|x\|_2^n = \|x-1\|_2.$$

Aquí $\|x-1\|_2 \neq 0$, ya que $x \neq 1$ por nuestra hipótesis $\|x\|_1 < 1$. Esto demuestra que $(x^n)_n$ no es una sucesión de Cauchy respecto a $\|\cdot\|_2$. Así que tenemos la implicación

$$\|x\|_1 < 1 \Longrightarrow \|x\|_2 < 1,$$

y de la misma manera,

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

Ahora notemos que 2) $\Leftrightarrow$ 2′). En efecto, (7.1) aplicado a x^{-1} implica (7.2), y luego (7.1) y (7.2) implican (7.3).

La implicación más complicada es 2′) $\Rightarrow$ 3). Supongamos que para $\|\cdot\|_1$ y $\|\cdot\|_2$ se cumple (7.1), (7.2), (7.3). Tenemos que ver que $\|\cdot\|_1 = \|\cdot\|_2^\alpha$ para algún $\alpha > 0$. Si $\|\cdot\|_1$ es una norma trivial, entonces según (7.2), $\|\cdot\|_2$ es también trivial, y funciona cualquier $\alpha > 0$. Ahora si $\|\cdot\|_1$ no es trivial, entonces existe algún $x_0 \in F$ tal que $\|x_0\|_1 \neq 1$. Tenemos

$$\|x_0\|_1 = \|x_0\|_2^\alpha, \quad \text{donde } \alpha = \frac{\log\|x_0\|_1}{\log\|x_0\|_2}.$$

Aquí $\alpha > 0$ porque por nuestra hipótesis 2), tenemos o bien $\|x_0\|_1 < 1$, $\|x_0\|_2 < 1$, o bien $\|x_0\|_1 > 1$, $\|x_0\|_2 > 1$, y por lo tanto $\log\|x_0\|_1$ y $\log\|x_0\|_2$ tienen el mismo signo. Necesitamos ver que

$$\|x\|_1 = \|x\|_2^\alpha \quad \text{para todo } x \in F.$$

Si $\|x\|_2 = 1$, entonces también $\|x\|_1 = 1$, y la relación se cumple. Va a ser suficiente analizar el caso cuando $\|x\|_1 < 1$ (y entonces $\|x\|_2 < 1$); si $\|x\|_1 > 1$ se puede considerar x^{-1}. Podemos escribir la relación de arriba como

$$\frac{\log\|x\|_1}{\log\|x\|_2} = \frac{\log\|x_0\|_1}{\log\|x_0\|_2} = \alpha \quad \text{para todo } x \in F,$$

o como

$$\frac{\log\|x_0\|_1}{\log\|x\|_1} = \frac{\log\|x_0\|_2}{\log\|x\|_2} \quad \text{para todo } x \in F.$$

Ahora, si $\frac{\log\|x_0\|_1}{\log\|x\|_1} < \frac{\log\|x_0\|_2}{\log\|x\|_2}$, entonces existe un número racional $\frac{m}{n}$ tal que

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

Luego,

$$\|x_0\|_1 < \|x\|_1^{m/n} \quad y \quad \|x\|_2^{m/n} < \|x_0\|_2.$$

Podemos escribir estas desigualdades como

$$\|x_0\|_1^n < \|x\|_1^m \quad y \quad \|x\|_2^m < \|x_0\|_2^n.$$

Esto nos da

$$\left\| \frac{x_0^n}{x^m} \right\|_1 = \frac{\|x_0\|_1^n}{\|x\|_1^m} < 1, \quad \left\| \frac{x_0^n}{x^m} \right\|_2 = \frac{\|x_0\|_2^n}{\|x\|_2^m} > 1,$$

lo que contradice 2). De la misma manera, podemos descartar el caso $\frac{\log\|x_0\|_1}{\log\|x\|_1} > \frac{\log\|x_0\|_2}{\log\|x\|_2}$.

La implicación 3) ⇒ 1) **es fácil**: si $\|\cdot\|_1 = \|\cdot\|_2^\alpha$ para algún $\alpha > 0$, entonces está claro que una sucesión es de Cauchy respecto a $\|\cdot\|_1$ si y solamente si es de Cauchy respecto a $\|\cdot\|_2$.

Claramente, tenemos 3) ⇒ 4): la condición 3) implica que las bolas abiertas correspondientes son las mismas.

En fin, 4) ⇒ 2). En efecto, para $x \in F$ tenemos $\|x\| < 1$ si y solamente si el límite

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

respecto a la norma $\|\cdot\|$. Si las topologías inducidas por $\|\cdot\|_1$ y $\|\cdot\|_2$ coinciden, entonces,

$$\|x\|_1 < 1 \iff \lim_{n\to\infty}{}^{\|\cdot\|_1}(x^n) = 0 \iff \lim_{n\to\infty}{}^{\|\cdot\|_2}(x^n) = 0 \iff \|x\|_2 < 1.$$

Esto termina la demostración de 1) ⇔ 2) ⇔ 3) ⇔ 4). ■

7.2. Observación. *Si $\|\cdot\|_1$ y $\|\cdot\|_2$ son dos normas equivalentes sobre un cuerpo F, entonces $\|\cdot\|_1$ es trivial si y solamente si $\|\cdot\|_2$ es trivial.*

Demostración. Evidente de la condición 2) de 7.1. ■

7.3. Observación. *Dos normas equivalentes $\|\cdot\|_1$ y $\|\cdot\|_2$ sobre un cuerpo son o bien ambas arquimedianas o bien ambas no arquimedianas.*

Demostración. Según 2.7, una norma es no-arquimediana si y solamente si $\|n\| \le 1$ para todo $n \in \mathbb{Z}$. Entonces, la condición 2) de 7.1 lo demuestra todo. ■

8 Teorema de Ostrowski: normas sobre $\mathbb{Q}$

Sobre $\mathbb{Q}$ tenemos la norma arquimediana $|\cdot|$, el valor absoluto habitual, y normas no arquimedianas $|\cdot|_p$ para diferentes primos p. Resulta que, salvo equivalencia, estas son todas las normas no triviales sobre $\mathbb{Q}$.

8.1. Teorema (Ostrowski[*]). *Toda norma sobre $\mathbb{Q}$ es equivalente a una de las siguientes:*

1) *la norma trivial (2.4);*
2) *el valor absoluto habitual arquimediano, que se denota por $|\cdot|_\infty$;*
3) *las normas no arquimedianas p-ádicas $|\cdot|_p$ para diferentes primos p (4.6).*

Recordemos que según el criterio 3) de 7.1, equivalencia de dos normas sobre un cuerpo quiere decir que $\|\cdot\|_1 = \|\cdot\|_2^\alpha$ para algún $\alpha > 0$. Note que $|\cdot|_p$ y $|\cdot|_q$ no son equivalentes para $p \ne q$. En efecto, en este caso tenemos $|p|_p = 1/p$ y $|p|_q = 1$, así que $|\cdot|_p \ne |\cdot|_q^\alpha$.

[*] Alexander Ostrowski (1893–1986), matemático de origen judío-ucraniano. Nació en Kiev, en ese tiempo parte del imperio ruso. Estudió en Alemania e hizo su tesis en Gotinga bajo dirección de Edmund Landau y Felix Klein. A partir de 1927 trabajo en la Universidad de Basilea.

Demostración. Sea $\|\cdot\|$ una norma sobre $\mathbb{Q}$. Dado que

$$\left\|\frac{m}{n}\right\| = \|m\| \cdot \|n\|^{-1}, \quad \|m\| = \|-m\|, \quad \|n\| = \|-n\|,$$

la norma está definida por sus valores $\|n\|$ en los enteros positivos $n = 1, 2, 3, \ldots$

Caso 1. Si para todo entero positivo n tenemos $\|n\| = 1$, la norma es trivial.

Caso 2. Supongamos que existe un entero positivo n tal que $\|n\| > 1$. Esto significa que la norma es arquimediana (véase 2.7), y vamos a ver que es equivalente a $|\cdot|_\infty$; es decir, que existe algún número $\alpha > 0$ tal que $\|n\| = n^\alpha$ para todo $n = 1, 2, 3, \ldots$

Sea n_0 el mínimo entero positivo tal que $\|n_0\| > 1$. Tenemos $\|n_0\| = n_0^\alpha$ para algún $\alpha > 0$. Todo entero positivo n puede ser escrito en la base n_0:

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s. \qquad (0 \le a_i < n_0,\ a_s \neq 0)$$

La desigualdad del triángulo nos da

$$\|n\| \le \|a_0\| + \|a_1 n_0\| + \|a_2 n_0^2\| + \cdots + \|a_s n_0^s\| = \|a_0\| + \|a_1\| \cdot n_0^\alpha + \|a_2\| \cdot n_0^{2\alpha} + \cdots + \|a_s\| \cdot n_0^{s\alpha}.$$

Ya que $a_i < n_0$ para todo i, tenemos $\|a_i\| \le 1$ por nuestra elección de n_0, así que

$$\|n\| \le 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{s\alpha} = n_0^{s\alpha}\,(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-s\alpha}) \le n_0^{s\alpha} \sum_{k\ge 0} \frac{1}{(n_0^\alpha)^k} \le n^\alpha \sum_{k\ge 0} \frac{1}{(n_0^\alpha)^k},$$

donde la última desigualdad sigue de $n \ge n_0^s$. Dado que $n_0^\alpha < 1$, la serie $\sum_{k\ge 0} \frac{1}{(n_0^\alpha)^k}$ converge a alguna constante C. Entonces, hemos demostrado que para todo entero positivo n se tiene

$$\|n\| \le C\, n^\alpha,$$

donde C no depende de n. En particular, podemos reemplazar n por n^N, donde N es algún número natural suficientemente grande. Tenemos la desigualdad

$$\|n\|^N \le C\, n^{N\alpha},$$

y tomando raíces N-ésimas,

$$\|n\| \le \sqrt[N]{C}\, n^\alpha.$$

Para $N \to \infty$, esto nos da

$$\|n\| \le n^\alpha.$$

Ahora, para la expansión de n en la base n_0, tenemos $n_0^{s+1} > n \ge n_0^s$, y por la desigualdad del triángulo,

$$\|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \le \|n\| + \|n_0^{s+1} - n\|,$$

de donde

$$\|n\| \ge \|n_0^{s+1}\| - \|n_0^{s+1} - n\| = \|n_0\|^{s+1} - \|n_0^{s+1} - n\| \ge n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^\alpha.$$

(usando la desigualdad $\|n_0^{s+1} - n\| \le (n_0^{s+1} - n)^\alpha$ que acabamos de demostrar). Ya que $n \ge n_0^s$, tenemos

$$\|n\| \ge n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^\alpha = n_0^{(s+1)\alpha}\left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) \ge C'\, n^\alpha,$$

donde C' es alguna constante que depende de n_0 y α y no depende de n. Por el mismo argumento de arriba, esto nos da la desigualdad

$$\|n\| \ge n^\alpha.$$

Podemos concluir que existe algún $\alpha > 0$ tal que para todo $n = 1, 2, 3, \ldots$

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

Esto significa que la norma es equivalente a $|\cdot|_{\infty}$.

Caso 3. Supongamos que $\|n\| \leq 1$ para todo entero positivo n, y existe algún n tal que $\|n\| < 1$. Esto significa que la norma es no-arquimediana y no es trivial, y nos gustaría ver que es equivalente a $|\cdot|_p$ para algún primo p. Sea n_0 el mínimo entero positivo tal que $\|n_0\| < 1$. Notemos que $n_0 = p$ tiene que ser primo: en efecto, si $n_0 = n_1 \cdot n_2$ para algunos $1 < n_1 < n$ y $1 < n_2 < n$, entonces $\|n_0\| = \|n_1\| \cdot \|n_2\|$, y $\|n_1\| < 1$ o $\|n_2\| < 1$, lo que contradice nuestra elección de n_0.

Ahora si q es otro primo diferente de p, tenemos $\|q\| = 1$. En efecto, si $\|q\| < 1$, entonces tenemos la relación de Bézout

$$1 = ap + bq$$

para algunos enteros a y b, y luego la desigualdad ultramétrica nos da una contradicción

$$1 = \|1\| \leq \max\{\|a\| \cdot \|p\|, \|b\| \cdot \|q\|\} < 1.$$

Entonces, $\|q\| = 1$ para todo primo $q \neq p$. Todo entero positivo n puede ser factorizado en números primos:

$$n = p_1^{v_{p_1}(n)} \cdot p_2^{v_{p_2}(n)} \cdots p_s^{v_{p_s}(n)},$$

y

$$\|n\| = \|p_1\|^{v_{p_1}(n)} \cdot \|p_2\|^{v_{p_2}(n)} \cdots \|p_s\|^{v_{p_s}(n)}.$$

Si $p_i \neq p$, el factor correspondiente es igual a 1. Entonces,

$$\|n\| = \|p\|^{v_p(s)},$$

donde $0 < \|p\| < 1$. Esta norma es equivalente a $|\cdot|_p$. ■

Ejercicio 23 (Teorema de Ostrowski para $k(X)$)**.** Ahora para un cuerpo k consideremos el anillo de polinomios $k[X]$. Este es un dominio de factorización única, y en tal sentido es parecido al anillo $\mathbb{Z}$. Los polinomios irreducibles son análogos de los números primos. El cuerpo de fracciones correspondiente

$$k(X) = \{f/g \mid f, g \in k[X],\ g \neq 0\}$$

es el cuerpo de funciones racionales y es un análogo de $\mathbb{Q}$.

Supongamos que $\|\cdot\|$ es una norma sobre $k(X)$ tal que $\|\cdot\|$ es trivial sobre k.

1) Note que bajo esta hipótesis, $\|\cdot\|$ es necesariamente no arquimediana (véase 2.8).

2) Note que $\|\cdot\|$ está definida por sus valores sobre $k[X] \subset k(X)$.

3) Supongamos que $\|X\| > 1$. Demuestre que para todo $f \in k[X]$ se cumple $\|f\| = \|X\|^{\deg f}$, así que la norma es equivalente a la norma $f \mapsto \rho^{-\deg f}$ para $0 < \rho < 1$ que viene de 3.2.

   (Use la desigualdad ultramétrica y la hipótesis que $\|\cdot\|$ es trivial sobre k.)

4) Supongamos que $\|X\| \leq 1$. Note que $\|f\| \leq 1$ para todo $f \in k[X]$ (de nuevo, use la desigualdad ultramétrica). Supongamos que la norma no es trivial y sea $f_0 \neq 0$ un polinomio mónico del mínimo grado posible tal que $\|f_0\| < 1$. Deduzca que $f_0 = p$ es un polinomio irreducible y $\|q\| = 1$ si $q \neq p$ es otro polinomio mónico irreducible. Concluya que la norma es equivalente a $f \mapsto \rho^{v_p(f)}$, donde

$$v_p(f) := \max\{k \mid p^k \mid f\}.$$

   (El argumento sería idéntico a la parte no arquimediana de nuestra demostración del teorema de Ostrowski.)

9 Completación respecto a una norma: definición

En esta sección vamos a revisar la construcción de la completación de un anillo R respecto a una norma $\|\cdot\|$. El lector debe conocer este material de los cursos de análisis real donde el mismo método se usa para construir los números reales $\mathbb{R}$. Note que por nuestra definición, una norma sobre R es una aplicación $R \to \mathbb{R}_{\geq 0}$, así que ya se asume que hemos construido $\mathbb{R}$ como la completación de $\mathbb{Q}$ respecto al valor absoluto arquimediano $|\cdot|$. En particular, vamos a usar que toda sucesión de Cauchy en $\mathbb{R}$ converge.

9.1. Definición. Sea R un anillo conmutativo dotado de una norma $\|\cdot\|$. La **completación** de R respecto a esta norma es un anillo $\widehat{R}$ junto con un homomorfismo de anillos

$$\begin{aligned} R &\to \widehat{R}, \\ a &\mapsto \widehat{a} := i(a) \end{aligned}$$

que satisface las siguientes propiedades.

1) La norma $\|\cdot\|$ se extiende a una norma sobre $\widehat{R}$, que vamos a denotar también por $\|\cdot\|$ por abuso de notación. Para cualquier $a \in R$ se tiene
$$\|\widehat{a}\| = \|a\|.$$
(En particular, $\widehat{a} = 0 \iff \|\widehat{a}\| = 0 \iff \|a\| = 0 \iff a = 0$, así que i es un homomorfismo inyectivo. Además, se nota que es automáticamente continuo respecto a las topologías inducidas por las normas sobre R y $\widehat{R}$.)

2) R es **denso** en $\widehat{R}$; es decir, todo elemento de $x \in \widehat{R}$ es el límite de alguna sucesión de elementos de R:
$$x = \lim_{n\to\infty} \widehat{a_n}.$$

3) $\widehat{R}$ es **completo**; es decir, toda sucesión de Cauchy en $\widehat{R}$ converge en $\widehat{R}$.

La construcción de $\widehat{R}$ requiere un poco de trabajo, pero de la definición de arriba se puede deducir que $\widehat{R}$ está definido de modo único.

9.2. Lema. *Para $x = \lim_{n\to\infty} \widehat{a_n} \in \widehat{R}$ la norma viene dada por*

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

Demostración. La norma $\|\cdot\| \colon \widehat{R} \to \mathbb{R}_{\geq 0}$ es continua respecto a la topología inducida por la misma norma y por lo tanto conmuta con límites. ∎

9.3. Lema. *Sean*

$$R \to \widehat{R}, \quad a \mapsto \widehat{a}$$

y

$$R \to \widetilde{R}, \quad a \mapsto \widetilde{a}$$

dos completaciones del mismo anillo respecto a la misma norma $\|\cdot\|$. Entonces el homomorfismo identidad $R \to R$ se extiende de modo único a un isomorfismo de anillos $\widehat{R} \xrightarrow{\cong} \widetilde{R}$ que preserva la norma ($\|f(x)\| = \|x\|$ para todo $x \in R$):

$$\begin{array}{ccc} R & \xrightarrow{\mathrm{id}} & R \\ \downarrow & & \downarrow \\ \widehat{R} & \overset{\exists! f}{\dashrightarrow}_{\cong} & \widetilde{R} \end{array}$$

Demostración. Gracias a la densidad, todo elemento $x \in \widehat{R}$ puede ser expresado como

$$x = \lim_{n\to\infty} \widehat{a_n} \tag{9.1}$$

para algunos $a_n \in R$. En particular, $(\widehat{a_n})_n$ es una sucesión de Cauchy en $\widehat{R}$, siendo una sucesión convergente. Luego, tenemos para todo n

$$\|\widehat{a_n}\| = \|a_n\| = \|\widetilde{a_n}\|,$$

así que $(\widetilde{a_n})_n$ es una sucesión de Cauchy en $\widetilde{R}$. Por nuestra hipótesis el anillo $\widetilde{R}$ es completo, y por lo tanto $(\widetilde{a_n})_n$ converge a algún elemento de $\widetilde{R}$. Ya que f debe preservar la norma, f debe ser una aplicación continua y preservar los límites. Para hacer conmutar el diagrama, f debe satisfacer

$$f(\widehat{a}) = \widetilde{a}$$

para todo $a \in R$. Entonces, la aplicación f debe ser dada por

$$f(x) = f\left(\lim_{n\to\infty} \widehat{a_n}\right) = \lim_{n\to\infty} f(\widehat{a_n}) = \lim_{n\to\infty} \widetilde{a_n}. \tag{9.2}$$

Veamos que que la fórmula (9.2) no depende de una expresión particular (9.1), sino de x. Supongamos que

$$\lim_{n\to\infty} \widehat{a_n} = \lim_{n\to\infty} \widehat{a'_n}$$

para algunos $a'_n \in R$. Entonces

$$\|\widetilde{a_n} - \widetilde{a'_n}\| = \|\widetilde{a_n - a'_n}\| = \|a_n - a'_n\| = \|\widehat{a_n - a'_n}\| = \|\widehat{a_n} - \widehat{a'_n}\| \xrightarrow{n\to\infty} 0$$

y la desigualdad del triángulo inversa

$$\left|\|\widetilde{a_n}\| - \|\widetilde{a'_n}\|\right| \leq \|\widetilde{a_n} - \widetilde{a'_n}\|$$

demuestra que

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

Luego, f preserva la norma gracias a 9.2:

$$\left\|\lim_{n\to\infty} \widehat{a_n}\right\| = \lim_{n\to\infty} \|a_n\| = \left\|\lim_{n\to\infty} \widetilde{a_n}\right\|.$$

En particular, f es automáticamente una aplicación inyectiva.

Veamos que f es un homomorfismo de anillos:

$$\begin{aligned} f\left(\lim_{n\to\infty} \widehat{a_n} \pm \lim_{n\to\infty} \widehat{b_n}\right) &= f\left(\lim_{n\to\infty} (\widehat{a_n} \pm \widehat{b_n})\right) = f\left(\lim_{n\to\infty} \widehat{a_n \pm b_n}\right) = \lim_{n\to\infty} \widetilde{a_n \pm b_n} \\ &= \lim_{n\to\infty} (\widetilde{a_n} \pm \widetilde{b_n}) = \lim_{n\to\infty} \widetilde{a_n} \pm \lim_{n\to\infty} \widetilde{b_n} = f\left(\lim_{n\to\infty} \widehat{a_n}\right) \pm f\left(\lim_{n\to\infty} \widehat{b_n}\right), \end{aligned}$$

donde hemos usado que las operaciones + y − son continuas y por ende conmutan con límites. De modo similar, se demuestra que

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

Por fin, si $1 \in R$ es la identidad del anillo, entonces $\widehat{1}$ es la identidad en $\widehat{R}$ y $\widetilde{1}$ es la identidad en $\widetilde{R}$. Por nuestra definición se tiene $f(\widehat{1}) = \widetilde{1}$ y en general $f(\widehat{a}) = \widetilde{a}$ para todo $a \in R$.

Nos queda ver que f es un isomorfismo. Ya sabemos que es una aplicación inyectiva y falta ver que es sobreyectiva. Gracias a la densidad de R en $\widetilde{R}$, todo elemento $y \in \widetilde{R}$ se expresa como

$$y = \lim_{n\to\infty} \widetilde{a_n}$$

para algunos $a_n \in R$. En particular, aquí $(\widetilde{a_n})_n$ es una sucesión de Cauchy en $\widetilde{R}$, pero esto implica que $(\widehat{a_n})_n$ es una sucesión de Cauchy en $\widehat{R}$ que converge, puesto que $\widehat{R}$ es completo, y

$$f\left(\lim_{n\to\infty} \widehat{a_n}\right) = \lim_{n\to\infty} \widetilde{a_n}.$$

■

9.4. Lema. *Si la norma $\|\cdot\|$ sobre R es arquimediana (resp. no arquimediana), entonces su extensión a $\widehat{R}$ es también arquimediana (resp. no arquimediana).*

Demostración. El homomorfismo $R \to \widehat{R}$ es una inyección, así que R puede ser identificado con un subanillo de $\widehat{R}$ con la misma norma. Luego, una norma será no arquimediana sobre $\widehat{R}$ si y solamente si es no arquimediana sobre R (véase 2.8). ■

9.5. Lema. *Si $R = F$ es un cuerpo, entonces $\widehat{F}$ es también un cuerpo.*

Demostración. Sea $x \in \widehat{R}$ un elemento no nulo. Gracias a la densidad,

$$x = \lim_{n\to\infty} \widehat{a_n},$$

donde $\widehat{a_n}$ es alguna sucesión de Cauchy en $\widehat{R}$, y por lo tanto a_n es una sucesión de Cauchy en R. Ya que x no es nulo,

$$\|x\| = \left\|\lim_{n\to\infty} \widehat{a_n}\right\| = \lim_{n\to\infty} \|a_n\| \neq 0.$$

Entonces, existen N y $C > 0$ tales que

$$\|a_n\| > C \quad \text{para todo } n > N.$$

En particular,

$$a_n \neq 0 \quad \text{para todo } n > N.$$

Definamos

$$b_n := \begin{cases} 1, & \text{si } n \leq N, \\ a_n^{-1}, & \text{si } n > N. \end{cases}$$

Ahora para $m, n > N$ tenemos

$$\|b_m - b_n\| = \left\|\frac{1}{a_m} - \frac{1}{a_n}\right\| = \left\|\frac{a_n - a_m}{a_m\, a_n}\right\| = \left\|\frac{1}{a_m\, a_n}\right\| \cdot \|a_n - a_m\| < \frac{1}{C^2} \cdot \|a_n - a_m\|.$$

Puesto que $(a_n)_n$ es una sucesión de Cauchy en R, de aquí se ve que $(b_n)_b$ lo es, y $(\widehat{b_n})_n$ es una sucesión de Cauchy en $\widehat{R}$. Sea

$$y := \lim_{n\to\infty} \widehat{b_n} \in \widehat{R}.$$

Este límite existe puesto que $\widehat{R}$ es un anillo completo. Luego,

$$x \cdot y = \lim_{n\to\infty} \widehat{a_n} \cdot \lim_{n\to\infty} \widehat{b_n} = \lim_{n\to\infty} \widehat{a_n}\,\widehat{b_n} = \lim_{n\to\infty} \widehat{a_n\, b_n}.$$

Pero $a_n\, b_n = 1$ (y por lo tanto $\widehat{a_n\, b_n} = \widehat{a_n}\,\widehat{b_n} = \widehat{1}$) para $n \gg 0$ y

$$x \cdot y = \lim_{n\to\infty} \widehat{1} = \widehat{1}.$$

■

10 Completación respecto a una norma: construcción

> Dios hizo los números enteros;
> el resto es obra del hombre.
>
> Leopold Kronecker

Ahora procedamos con la construcción de la completación. Escribí las pruebas de abajo solo para no dejar la impresión de que todo queda en el aire, pero no nos va a servir ninguna construcción particular. El lector puede aceptar la existencia de completación y pasar a la siguiente sección.

10.1. Lema. *El conjunto*

$$SC(R) := \{\textit{sucesiones de Cauchy en } R\}.$$

es un anillo conmutativo respecto a las operaciones

$$(a_n)_n + (b_n)_n := (a_n + b_n)_n,$$
$$(a_n)_n \cdot (b_n)_n := (a_n b_n)_n,$$

y el cero y la identidad en $SC(R)$ son las series constantes

$$\widehat{0} := (0,0,0,\ldots) \quad \text{y} \quad \widehat{1} := (1,1,1,\ldots).$$

Asociando a todo $a \in R$ la sucesión constante $(a) \in SC(R)$, se obtiene un homomorfismo inyectivo $R \hookrightarrow SC(R)$.

Demostración. Se ve fácilmente que las sumas y productos de sucesiones de Cauchy son también sucesiones de Cauchy (¡ejercicio para el lector!). El resto debe ser claro. ■

Podemos tratar de extender la norma $\|\cdot\|$ de R al anillo $SC(R)$ mediante la fórmula

$$\|(a_n)_n\| := \lim_{n\to\infty} \|a_n\|.$$

Este límite existe para toda sucesión de Cauchy (a_n), como hemos notado en 6.6. Sin embargo, esta fórmula no define una norma sobre $SC(R)$, ya que para una sucesión de Cauchy $(a_n) \neq (0,0,0,\ldots)$ el límite $\lim_{n\to\infty} \|a_n\|$ puede ser nulo, lo que contradice el axioma de normas N1). Para resolver este problema, podemos considerar las sucesiones de Cauchy módulo las sucesiones tales que $\lim_{n\to\infty} \|a_n\| = 0$.

10.2. Definición. Se dice que una sucesión $(a_n)_n$ es **nula** si $\lim_{n\to\infty} a_n = 0$.

Note que esto es equivalente a $\lim_{n\to\infty} \|a_n\| = 0$. Toda sucesión nula es una sucesión de Cauchy, puesto que esta tiene límite.

10.3. Ejemplo. La sucesión $(p^n)_n$ en $\mathbb{Q}$ es nula respecto a la norma p-ádica. ▲

10.4. Lema. *Las sucesiones nulas de elementos de R forman un ideal $N(R)$ en el anillo $SC(R)$.*

Demostración. Está claro que $\widehat{0} = (0,0,0,\ldots) \in N(R)$. Luego, si $(a_n)_n, (b_n)_n \in N(R)$ y $(c_n)_n \in SC(R)$, entonces $(a_n)_n \pm (b_n)_n := (a_n \pm b_n)_n \in N(R)$. En efecto, en este caso

$$\lim_{n\to\infty} \|a_n + b_n\| \leq \lim_{n\to\infty} (\|a_n\| + \|b_n\|) = \lim_{n\to\infty} \|a_n\| + \lim_{n\to\infty} \|b_n\| = 0.$$

Ahora si $(a_n)_n \in N(R)$ y $(c_n)_n \in SC(R)$, entonces

$$\lim_{n\to\infty} \|c_n a_n\| = \lim_{n\to\infty} (\|c_n\| \cdot \|a_n\|) = \lim_{n\to\infty} \|c_n\| \cdot \lim_{n\to\infty} \|a_n\| = 0,$$

así que $(c_n)_n \cdot (a_n)_n := (c_n a_n)_n \in N(R)$. ■

Ahora podemos pasar al anillo cociente $SC(R)/N(R)$.

10.5. Lema. *La fórmula*

$$\|(a_n)_n\| := \lim_{n\to\infty} \|a_n\|$$

define una norma sobre $SC(R)/N(R)$.

Demostración. Si tenemos $(a_n)_n \equiv (a'_n) \pmod{N(R)}$, esto quiere decir que

$$(a_n)_n - (a'_n)_n = (a_n - a'_n)_n \text{ es una sucesión nula;}$$

luego, la desigualdad del triángulo inversa nos da

$$\Big|\|a_n\| - \|a'_n\|\Big| \le \|a_n - a'_n\| \xrightarrow{n\to\infty} 0,$$

y podemos concluir que

$$\|(a_n)_n\| := \lim_{n\to\infty} \|a_n\| = \lim_{n\to\infty} \|a'_n\| =: \|(a'_n)_n\|.$$

Esto significa que la formula para $\|\cdot\|$ sobre $SC(R)/N(R)$ no depende de un representante particular de una clase de equivalencia módulo $N(R)$.

Verifiquemos ahora los axiomas de norma. Los axiomas N2) y N3) se cumplen gracias a los mismos axiomas para la norma $\|\cdot\|$ sobre R, mientras que N1) se cumple porque hemos tomado el cociente por las sucesiones de norma nula:

N1) $\|(a_n)_n\| := \lim_{n\to\infty} \|a_n\| = 0$ significa precisamente que la sucesión es nula; es decir, representa el elemento nulo en el anillo cociente $SC(R)/N(R)$;

N2) para los productos tenemos

$$\|(a_n)_n \cdot (b_n)_n\| = \|(a_n b_n)_n\| = \lim_{n\to\infty} \|a_n b_n\| = \lim_{n\to\infty} \|a_n\| \cdot \lim_{n\to\infty} \|a_n\| = \|(a_n)_n\| \cdot \|(b_n)_n\|;$$

N3) se cumple la desigualdad del triángulo:

$$\|(a_n)_n + (b_n)_n\| = \|(a_n + b_n)_n\| = \lim_{n\to\infty} \|a_n + b_n\| \le \lim_{n\to\infty} \|a_n\| + \lim_{n\to\infty} \|b_n\| = \|(a_n)_n\| + \|(b_n)_n\|.$$

■

El siguiente resultado sigue directamente de las definiciones.

10.6. Lema. *La inclusión de sucesiones constantes induce un homomorfismo de anillos*

$$\begin{aligned} R &\to SC(R)/N(R), \\ a &\mapsto \widehat{a} := (a, a, a, \ldots). \end{aligned}$$

Se cumple $\|\widehat{a}\| = \|a\|$ *para todo* $a \in R$.

Ahora $R \to SC(R)/N(R)$ es un homomorfismo inyectivo y continuo, así que R puede ser identificado con un subanillo topológico de $SC(R)/N(R)$.

10.7. Lema. *El subanillo* $R \subset SC(R)/N(R)$ *es* ***denso*** *en* $SC(R)/N(R)$*: todo elemento de* $SC(R)/N(R)$ *es el límite de alguna sucesión de elementos de* R.

Demostración. Por nuestra construcción, un elemento de $SC(R)$ está representado por una sucesión de Cauchy $(a_n)_n$, donde $a_n \in R$. Para todo m fijo podemos considerar la sucesión constante correspondiente

$$\widehat{a_m} := (a_m, a_m, a_m, \ldots).$$

Ahora $(\widehat{a_m})_m$ representa un elemento en $SC(R)/N(R)$ y $(\widehat{a_m})_m$ tiene $(a_n)_n$ como su límite:

$$\lim_{m\to\infty} \widehat{a_m} = (a_n)_n.$$

En efecto, $(a_n)_n - \widehat{a_m}$ es la sucesión representada por $(a_n - a_m)_n$, y luego, puesto que $(a_n)_n$ es una sucesión de Cauchy, tenemos

$$\lim_{m\to\infty} \|(a_n)_n - \widehat{a_m}\| = \lim_{m\to\infty}\lim_{n\to\infty} \|a_m - a_n\| = 0.$$

■

10.8. Lema. *$SC(R)/N(R)$ es un anillo completo respecto a la norma $\|\cdot\|$: toda sucesión de Cauchy $(x_m)_m$ en $SC(R)/N(R)$ converge a algún elemento de $SC(R)/N(R)$.*

Demostración (argumento diagonal). Si tenemos una sucesión (x_m) en $SC(R)/N(R)$, esto quiere decir que cada x_m es una clase de equivalencia representada por una sucesión de Cauchy en R. Gracias a la densidad sabemos que

$$x_m = \lim_{n\to\infty} \widehat{a_{mn}}$$

para algunos $a_{mn} \in R$. En particular, para todo m existe $k(m)$ tal que

$$\|x_m - \widehat{a_{mn}}\| < \frac{1}{m} \quad \text{para todo } n > k(m).$$

Si necesario, podemos reemplazar los $k(m)$ por números más grandes y suponer que

$$k(0) < k(1) < k(2) < \cdots$$

Consideremos

$$c_n := a_{n,k(n)}.$$

1) Veamos que $(c_n)_n$ es una sucesión de Cauchy en R y por lo tanto representa un elemento de $SC(R)/N(R)$. De hecho, por la desigualdad del triángulo,

$$\begin{aligned}\|c_{n_1} - c_{n_2}\| = \|a_{n_1,k(n_1)} - a_{n_2,k(n_2)}\| &= \|\widehat{a_{n_1,k(n_1)}} - \widehat{a_{n_2,k(n_2)}}\| \\ &= \|(\widehat{a_{n_1,k(n_1)}} - x_{n_1}) + (x_{n_1} - x_{n_2}) + (x_{n_2} - \widehat{a_{n_2,k(n_2)}})\| \\ &\le \|x_{n_1} - \widehat{a_{n_1,k(n_1)}}\| + \|x_{n_1} - x_{n_2}\| + \|x_{n_2} - \widehat{a_{n_2,k(n_2)}}\|.\end{aligned}$$

Ya que $(x_n)_n$ es una sucesión de Cauchy en $SC(R)/N(R)$, en particular, para todo $\epsilon > 0$ existe N tal que

$$\|x_{n_1} - x_{n_2}\| < \epsilon/3 \quad \text{para cualesquiera } n_1, n_2 > N.$$

Luego, por nuestra elección de $k(n)$, tenemos

$$\|x_{n_1} - \widehat{a_{n_1,k(n_1)}}\| < \epsilon/3 \quad \text{y} \quad \|x_{n_2} - \widehat{a_{n_2,k(n_2)}}\| < \epsilon/3 \quad \text{para cualesquiera } n_1, n_2 > 3/\epsilon.$$

Entonces,

$$\|c_{n_1} - c_{n_2}\| < \epsilon \quad \text{para cualesquiera } n_1, n_2 > \max\{N, 3/\epsilon\},$$

lo que demuestra que $(c_n)_n$ es una sucesión de Cauchy en R.

2) Veamos que $\lim_{m\to\infty} x_m = (c_n)_n$. Notemos que

$$\|(c_n)_n - x_m\| = \|((c_n)_n - \widehat{a_{m,k(m)}}) + (\widehat{a_{m,k(m)}} - x_m)\| \leq \|(c_n)_n - \widehat{a_{m,k(m)}}\| + \|x_m - \widehat{a_{m,k(m)}}\|.$$

Luego, para el primer término, tenemos

$$\|(c_n)_n - \widehat{a_{m,k(m)}}\| = \lim_{n\to\infty} \|c_n - c_m\|,$$

y, como acabamos de ver en la parte 1), existe N tal que

$$\|c_n - c_m\| < \frac{\epsilon}{2} \quad \text{para cualesquiera } m, n > N.$$

Para el segundo término, se cumple

$$\|x_m - \widehat{a_{m,k(m)}}\| < \frac{\epsilon}{2} \quad \text{para todo } m > 2/\epsilon.$$

Entonces,

$$\|(c_n)_n - x_m\| < \epsilon \quad \text{para todo } m > \text{máx}\{N, 2/\epsilon\},$$

lo que demuestra que $(c_n)_n$ es el límite de las sucesiones x_m.

■

Resumamos todo lo que hemos demostrado.

10.9. Teorema. *Sea R un anillo con norma $\|\cdot\|$. Entonces (salvo isomorfismo que preserva R y la norma) su completación viene dada por*

$$\widehat{R} = SC(R)/N(R),$$

junto con el homomorfismo natural $R \to \widehat{R}$ (la inclusión de las sucesiones constantes) y la norma definida por

$$\|(a_n)_n\| := \lim_{n\to\infty} \|a_n\|.$$

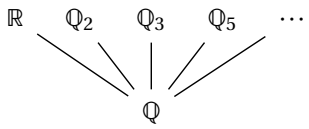
11 Los números p-ádicos $\mathbb{Q}_p$ y los enteros p-ádicos $\mathbb{Z}_p$

En la larga historia de las matemáticas, por "número" se entendía un número real, y no fue sino hasta relativamente hace poco que nos dimos cuenta de que existe el mundo de los números p-ádicos. Fue como si alguien que haya visto el cielo solamente de día se maraville ante el cielo nocturno. El firmamento matemático es ahora completamente distinto. En el cielo nocturno, $\mathbb{Q}_p$ emite "la luz del número primo p" cual una estrella que no podemos ver debido al sol $\mathbb{R}$, que emite "la luz de los números reales" durante el día. Así como hay incontables estrellas en el cielo nocturno, existe un $\mathbb{Q}_p$ para cada p; cada estrella es al sol como cada $\mathbb{Q}_p$ es a $\mathbb{R}$. De la misma forma en que los objetos del espacio se aprecian mejor de noche, hemos comenzado a explorar el profundo universo matemático a través de los números p-ádicos.

[KKS2000, §2.4]

11.1. Definición. El **cuerpo de los números p-ádicos** $\mathbb{Q}_p$ es la completación del cuerpo de los números reales $\mathbb{Q}$ respecto a la norma p-ádica $|\cdot|_p$.

Según el teorema de Ostrowski, todas las normas sobre $\mathbb{Q}$ salvo equivalencia son la norma trivial, la norma habitual arquimediana $|\cdot|$ y las normas p-ádicas $|\cdot|_p$ para todo primo p. De la caracterización de normas equivalentes (7.1) se ve que si $\|\cdot\|_1 \sim \|\cdot\|_2$, entonces $SC(R,\|\cdot\|_1) = SC(R,\|\cdot\|_2)$ y $N(R,\|\cdot\|_1) = N(R,\|\cdot\|_2)$, así que nuestra construcción de $\widehat{R} = SC(R)/N(R)$ nos dice que la completación respecto a normas equivalentes nos da el mismo resultado. Entonces, $\mathbb{Q}$ tiene las siguientes completaciones no triviales: $\mathbb{R}$ es la completación respecto a $|\cdot|$ y para cada primo p el cuerpo $\mathbb{Q}_p$ es la completación respecto a $|\cdot|_p$.



11.2. Comentario. Se puede demostrar que $\mathbb{R}$ y los $\mathbb{Q}_p$ para diferentes primos p nos son isomorfos como cuerpos abstractos. Normalmente esto se demuestra mediante el lema de Hensel, pero tal resultado haría parte de otro curso.

Según la teoría general, la norma p-ádica se extiende a una norma no arquimediana sobre $\mathbb{Q}_p$ que también vamos a denotar por $|\cdot|_p$. Específicamente, para $0 \in \mathbb{Q}_p$ tenemos

$$|0|_p = 0,$$

y si

$$x = \lim_{n\to\infty} a_n \in \mathbb{Q}_p^\times$$

para alguna sucesión de Cauchy $(a_n)_n$ en $\mathbb{Q}$, entonces

$$|x|_p := \lim_{n\to\infty} |a_n|_p = |a_m|_p \text{ para } m \gg 0$$

según el siguiente resultado.

11.3. Lema. *Sea R un anillo con una norma no arquimediana $\|\cdot\|$. Sea $(a_n)_n$ una sucesión de Cauchy no nula en R respecto a $\|\cdot\|$. Entonces existe N tal que*

$$\|a_m\| = \|a_n\| \quad \textit{para cualesquiera } m,n > N.$$

Demostración. Como vimos en 6.6, si $(a_n)_n$ es una sucesión de Cauchy, entonces $(\|a_n\|)_n$ es una sucesión de Cauchy en $\mathbb{R}$ y por lo tanto el límite $\lim_{n\to\infty}\|a_n\|$ existe. Es algún número positivo $C > 0$ (la sucesión no es nula por nuestra hipótesis). Entonces, existe N_1 tal que

$$\|a_n\| > C/2 \quad \text{para todo } n > N_1.$$

Y ya que $(a_n)_n$ es una sucesión de Cauchy, existe N_2 tal que

$$\|a_m - a_n\| < C/2 \quad \text{para cualesquiera } m,n > N_2.$$

Luego, para $N := \max\{N_1, N_2\}$ tenemos

$$\|a_n\| > \|a_m - a_n\| \quad \text{para cualesquiera } m,n > N,$$

y por lo tanto,

$$\|a_m\| = \|(a_m - a_n) + a_n\| = \max\{\|a_m - a_n\|, \|a_n\|\} = \|a_n\| \quad \text{para cualesquiera } m,n > N.$$

■

Podemos concluir que la norma $|\cdot|_p$ sobre $\mathbb{Q}_p^\times$ toma los mismos valores $\{1/p^n \mid n \in \mathbb{Z}\}$ que la norma p-ádica sobre $\mathbb{Q}^\times$.

11.4. Comentario.

1) El lema de arriba es falso si la norma es arquimediana: por ejemplo, los números

$$a_0 = 1,\ a_1 = 1{,}4,\ a_2 = 1{,}41,\ a_3 = 1{,}414,\ a_4 = 1{,}4142,\ a_5 = 1{,}41421,\ a_6 = 1{,}414213,\ \ldots$$

forman una sucesión de Cauchy en $\mathbb{Q}$ que converge a un número no nulo $\sqrt{2}$ en $\mathbb{R}$, pero sus valores absolutos no se estabilizan para $n \gg 0$.

2) La hipótesis de que la sucesión no sea nula es también importante: la sucesión $a_n = p^n$ es nula en $\mathbb{Q}$ respecto a la norma p-ádica $|\cdot|_p$, y en particular es una sucesión de Cauchy, pero los valores $|p^n|_p = 1/p^n$ no se estabilizan.

11.5. Teorema.

1) El conjunto

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

*es un subanillo de $\mathbb{Q}_p$. Este es el **anillo de los enteros p-ádicos**.*

2) El grupo de los elementos invertibles en $\mathbb{Z}_p$ viene dado por

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}.$$

3) Todo elemento $x \in \mathbb{Q}_p^\times$ puede ser escrito de modo único como up^n para algunos $u \in \mathbb{Z}_p^\times$ y $n \in \mathbb{Z}$.

4) $\mathbb{Q}_p$ es el cuerpo de fracciones de $\mathbb{Z}_p$.

*5) $\mathbb{Z}_p$ es un **anillo local**; es decir, tiene un único ideal maximal, a saber*

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

6) Todo ideal no nulo en $\mathbb{Z}_p$ es de la forma $\mathfrak{m}^n = p^n\mathbb{Z}_p$ para algún $n = 0, 1, 2, 3, \ldots$ En particular, $\mathbb{Z}_p$ es un dominio de ideales principales.

Demostración. Para 1) notamos que $|0|_p = 0 < 1$ y $|1|_p = 1$, y si tenemos $|x|_p \leq 1$ y $|y|_p \leq 1$, entonces

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

y

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

En 2), si $x, x^{-1} \in \mathbb{Z}_p$, entonces $|x|_p \leq 1$ y $|x^{-1}|_p \leq 1$. Sin embargo, $|x^{-1}|_p = |x|_p^{-1}$ así que $|x|_p = 1$. En la otra dirección, si $|x|_p = 1$, entonces $x \neq 0$ y x es invertible en $\mathbb{Q}_p$. Luego, $|x^{-1}|_p = |x|_p^{-1} = 1$ y $x^{-1} \in \mathbb{Z}_p$.

En 3) si $x \in \mathbb{Q}_p^\times$, entonces $|x|_p = 1/p^n$ para algún n. Luego, $|x\,p^{-n}|_p = 1$, así que $u := x\,p^{-n} \in \mathbb{Z}_p^\times$ y $x = up^n$.
Para ver que la expresión $x = up^n$ es única, supongamos que $up^n = vp^m$. Sin pérdida de generalidad $m \geq n$, y tenemos $v^{-1}u = p^{m-n} \in \mathbb{Z}_p^\times$, así que $m = n$, y por lo tanto $u = v$.

Luego, ya que todo elemento de $\mathbb{Z}_p$ puede ser escrito como up^n donde $u \in \mathbb{Z}_p^\times$ y $n \in \mathbb{N}$, y todo elemento de $\mathbb{Q}_p$ tiene la misma forma con $n \in \mathbb{Z}$, está claro que $\mathbb{Q}_p$ es el mínimo cuerpo que contiene $\mathbb{Z}_p$. Esto establece 4).

Para 5) primero notamos que $\mathfrak{m}$ es un ideal. Evidentemente, $0 \in \mathfrak{m}$, y si $x, y \in \mathfrak{m}$, entonces $|x \pm y|_p \leq \max\{|x|_p, |y|_p\} < 1$, así que $x \pm y \in \mathfrak{m}$. Por fin, si $z \in \mathbb{Z}_p$ y $x \in \mathfrak{m}$, entonces $|z \pm x|_p = |z|_p \cdot |x|_p < 1$.

Ahora comparando 1) y 2), notamos que todo elemento no invertible de $\mathbb{Z}_p$ pertenece a $\mathfrak{m}$, y por esto $\mathfrak{m}$ es el único ideal maximal. Luego, se ve que todo $x \in \mathfrak{m}$ se expresa como $x = up^n$ para algún $u \in \mathbb{Z}_p^\times$, así que $\mathfrak{m} = p\mathbb{Z}_p$.

Finalmente, en 6), si $\mathfrak{a} \subset \mathbb{Z}_p$ es un ideal no nulo, todo elemento no nulo $x \in \mathfrak{a}$ puede ser escrito como $x = up^n$ para $u \in \mathbb{Z}_p^\times$ y $n \in \mathbb{N}$. Sea x tal elemento con el valor mínimo de n. Tenemos $p^n = u^{-1}\, x \in p^n\mathbb{Z}_p$, así que $p^n\mathbb{Z}_p \subseteq \mathfrak{a}$. Luego, para cualquier otro elemento no nulo $y \in \mathfrak{a}$, tenemos $y = v\, p^m$, donde $m \geq n$ por nuestra elección de n, así que $y = v\, p^{m-n}\, p^n \in p^n\mathbb{Z}_p$. Esto demuestra la otra inclusión $\mathfrak{a} \subseteq p^n\mathbb{Z}_p$. ■

Sabiendo que los ideales no nulos de $\mathbb{Z}_p$ son de la forma $p^n\mathbb{Z}_p$ para $n = 0, 1, 2, \ldots$, sería interesante calcular los anillos cociente correspondientes $\mathbb{Z}_p / p^n\mathbb{Z}_p$.

11.6. Proposición. *Tenemos* $\mathbb{Z}_p / p^n\mathbb{Z}_p \cong \mathbb{Z} / p^n\mathbb{Z}$ *y en particular* $\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{F}_p$.

Demostración. Consideremos primero el subanillo

$$\mathbb{Z}_{(p)} := \left\{ \frac{m}{n} \in \mathbb{Q} \;\middle|\; p \nmid n \right\} = \{a \in \mathbb{Q} \mid |a|_p \leq 1\} \subset \mathbb{Z}_p.$$

Tenemos

$$p^n\mathbb{Z}_{(p)} = p^n\mathbb{Z}_p \cap \mathbb{Z}_{(p)}.$$

Consideremos el homomorfismo de anillos

$$\begin{aligned} f\colon \mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p &\twoheadrightarrow \mathbb{Z}_p / p^n\mathbb{Z}_p, \\ a &\longmapsto a + p^n\mathbb{Z}_p. \end{aligned}$$

El núcleo de este homomorfismo es

$$\ker f = \{a \in \mathbb{Z}_{(p)} \mid p^n \mid a\} = p^n\, \mathbb{Z}_{(p)}.$$

Además, f es sobreyectivo. En efecto, supongamos que $x \in \mathbb{Z}_p$; es decir, $|x|_p \leq 1$. Ya que $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, existe algún $a \in \mathbb{Q}$ tal que

$$|a - x|_p \leq 1/p^n,$$

y entonces $x \equiv a \pmod{p^n\mathbb{Z}_p}$. Tenemos

$$|a|_p = |a - x + x|_p \leq \max\{|a - x|_p, |x|_p\} \leq 1,$$

y por lo tanto $a \in \mathbb{Z}_{(p)}$. Gracias al teorema de isomorfía, podemos concluir que f induce un isomorfismo de anillos

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

Por último,

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

En efecto, dado que para $\frac{a}{b} \in \mathbb{Z}_{(p)}$ se cumple $p \nmid b$, la "reducción módulo p"

$$\begin{aligned} \mathbb{Z}_{(p)} &\to \mathbb{Z} / p^n\mathbb{Z}, \\ \frac{a}{b} &\mapsto a\, b^{-1} \end{aligned}$$

está bien definida, es sobreyectiva y su núcleo es igual a $p^n\, \mathbb{Z}_{(p)}$. ■

12 Las expansiones p-ádicas

Como siempre, una serie $\sum_{n\geq 0} a_n$ denota el límite de las sumas parciales $\lim_{n\to\infty} s_n$, donde $s_n := \sum_{0\leq i\leq n} a_n$. Primero notamos que en cualquier caso, arquimediano o no, una serie convergente debe cumplir $\|a_n\| \xrightarrow{n\to\infty} 0$. En efecto, la sucesión (s_n) debe ser de Cauchy, y en particular

$$\|a_n\| = \|s_n - s_{n-1}\| \xrightarrow{n\to\infty} 0.$$

Resulta que en el caso no arquimediano, esto es *suficiente* para concluir que la serie es convergente.

12.1. Lema (El criterio de convergencia de series no arquimedianas). *En un cuerpo completo no arquimediano una serie $\sum_{n\geq 0} a_n$ converge si y solamente si $\|a_n\| \xrightarrow{n\to\infty} 0$.*

Demostración. Usando la desigualdad ultramétrica, notamos que para cualesquiera $m > n$ las sumas parciales cumplen

$$\|s_m - s_n\| = \left\| \sum_{n+1\leq i\leq m} a_i \right\| \leq \max_{n+1\leq i\leq m} \{\|a_i\|\},$$

así que si $\|a_i\| \xrightarrow{i\to\infty} 0$, la sucesión (s_n) es de Cauchy. ■

12.2. Teorema (Expansiones p-ádicas).

1) *Todo elemento $x \in \mathbb{Z}_p$ puede ser representado de modo único por una serie*

$$x = a_0 + a_1\, p + a_2\, p^2 + a_3\, p^3 + a_4\, p^4 + \cdots$$

donde $0 \leq a_i \leq p-1$. Es decir, tenemos un límite p-ádico

$$x = \lim_{n\to\infty} x_n,$$

donde

$$x_n := a_0 + a_1\, p + \cdots + a_{n-1}\, p^{n-1} + a_n\, p^n.$$

2) *En general, todo elemento de $\mathbb{Q}_p$ puede ser representado de modo único por una serie*

$$x = a_{-m}\, p^{-m} + a_{-m+1}\, p^{-m+1} + \cdots + a_0 + a_1\, p + a_2\, p^2 + a_3\, p^3 + a_4\, p^4 + \cdots$$

para algún m.

Demostración. Sabemos que todo elemento de $\mathbb{Q}_p$ puede ser escrito como $x = up^n$ para algunos $u \in \mathbb{Z}_p^\times$ y $n \in \mathbb{Z}$, así que 1) implica 2).

Para demostrar 1), notamos primero que el límite $\lim_{n\to\infty} x_n$ existe en $\mathbb{Q}_p$. Esto se sigue del criterio 12.1, puesto que

$$|a_n\, p^n|_p \leq \frac{1}{p^n} \xrightarrow{n\to\infty} 0$$

(aquí $|a_i|_p = 0$ o 1). Además,

$$|x|_p = \lim_{n\to\infty} |x_n|_p \leq 1,$$

así que $x \in \mathbb{Z}_p$. Ahora veamos cómo a partir de $x \in \mathbb{Z}_p$ se pueden encontrar los coeficientes $0 \leq a_n \leq p-1$. Puesto que $\{0, 1, 2, \ldots, p-1\}$ son representantes de $\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{F}_p$, existe un único $0 \leq a_0 \leq p-1$ tal que $x = a_0 + y_1\, p$ para algún $y_1 \in \mathbb{Z}_p$. Luego,

$$|x - a_0|_p = |y_1|_p \cdot |p|_p \leq 1/p.$$

Sea $0 \leq a_1 \leq p-1$ el único elemento tal que $y_1 = a_1 + y_2\, p$ para algún $y_2 \in \mathbb{Z}_p$. Tenemos

$$x = a_0 + a_1\, p + y_2\, p^2$$

y

$$|x-(a_0+a_1\,p)|_p = |y_2|_p\cdot|p|_p^2 \le 1/p^2.$$

Continuando de este modo, por inducción se encuentran $0 \le a_i \le p-1$ tales que

$$|x-(a_0+a_1\,p+\cdots+a_{n-1}\,p^{n-1}+a_n\,p^n)|_p \le 1/p^{n+1}.$$

Entonces,

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

es una sucesión que tiene como su límite x. Si tenemos otra expansión diferente

$$x = a_0'+a_1'\,p+a_2'\,p^2+a_3'\,p^3+\cdots$$

con $0 \le a_i' \le p-1$, sea n el primer índice donde $a_n' \neq a_n$. Tenemos $a_n' \not\equiv a_n \pmod p$, así que $|a_n'-a_n|_p = 1$. Denotemos

$$x_n' := a_0'+a_1'\,p+\cdots+a_{n-1}'\,p^{n-1}+a_n'\,p^n.$$

Tenemos

$$|x_n'-x_n|_p = |(a_n'-a_n)\,p^n|_p = |a_n'-a_n|_p\cdot|p^n|_p = 1/p^n.$$

Sin embargo,

$$|x_n'-x_n|_p = |(x_n'-x)+(x-x_n)|_p \le \max\{|x_n'-x|_p, |x-x_n|_p\} \le 1/p^{n+1},$$

y hemos obtenido una contradicción. ■

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

Demostración. Gracias a las expansiones p-ádicas, sabemos que todo elemento de $\mathbb{Z}_p$ es un límite de una sucesión (a_n) donde $a_n \in \mathbb{Z}$. Ya que $\mathbb{Q}_p$ es completo, toda sucesión (x_n) con $x_n \in \mathbb{Z}_p$ converge a algún $x \in \mathbb{Q}_p$, pero $|x_n|_p \le 1$ implica que $|x|_p = \lim_{n\to\infty}|x_n|_p \le 1$. ■

Los enteros p-ádicos son literalmente series formales en p en el siguiente sentido.

12.4. Corolario. *Se tiene un isomorfismo $\mathbb{Z}_p \cong \mathbb{Z}[[X]]/(X-p)$, donde*

$$\mathbb{Z}[[X]] = \left\{ \sum_{n\ge 0} a_n\,X^n \;\middle|\; a_n \in \mathbb{Z} \right\}$$

es el anillo de las series formales con coeficientes enteros.

Demostración. La aplicación

$$\mathbb{Z}[[X]] \to \mathbb{Z}_p, \quad \sum_{n\ge 0} a_n\,X^n \mapsto \sum_{n\ge 0} a_n\,p^n$$

es un homomorfismo de anillos bien definido (evaluación de series en p). En efecto, notamos que para cualquier serie formal

$$f = \sum_{n\ge 0} a_n\,X^n \in \mathbb{Z}[[X]]$$

la serie

$$f(p) := \sum_{n\ge 0} a_n\,p^n$$

converge a un entero p-ádico. Esto se sigue del criterio 12.1:

$$|a_n\,p^n|_p = |a_n|_p\cdot|p^n|_p \le |p^n|_p = \frac{1}{p^n} \xrightarrow{n\to\infty} 0.$$

El homomorfismo de arriba es sobreyectivo porque todo entero p-ádico puede ser escrito como una suma $\sum_{n\geq 0} a_n\, p^n$ con $0 \leq a_n < p$. Para calcular el núcleo, asumamos que $f(p) = 0$ en $\mathbb{Z}_p$. En el anillo $\mathbb{Q}[\![X]\!]$ se tiene

$$g := (X-p)^{-1} f = (X-p)^{-1} \sum_{n\geq 0} a_n X^n = \Big(-\sum_{n\geq 0} p^{-n-1} X^n\Big) \cdot \Big(\sum_{n\geq 0} a_n X^n\Big) = \sum_{n\geq 0} b_n X^n,$$

donde

$$b_n = -\sum_{0\leq i\leq n} a_i\, p^{i-n-1}.$$

Notamos que

$$b_n = p^{-n-1} \underbrace{\sum_{i\geq 0} a_i\, p^i}_{=0} - \sum_{0\leq i\leq n} a_i\, p^{i-n-1} = \sum_{i\geq n+1} a_i\, p^{i-n-1},$$

de donde se ve que $b_n \in \mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}$. Podemos concluir que existe una serie de potencias $g \in \mathbb{Z}[\![X]\!]$ tal que $(X-p)\, g = f$. Esto demuestra que f pertenece al ideal generado por $X - p$. Viceversa, está claro que $X - p$ está en el núcleo de la evaluación en p. ■

El último resultado significa que para obtener los números p-ádicos, se puede primero construir $\mathbb{Z}_p$ y luego declarar que $\mathbb{Q}_p$ es el cuerpo de fracciones de $\mathbb{Z}_p$.

12.5. Ejemplo. Para un número natural n, su expansión p-ádica es la expresión de n en base p. Por ejemplo,

$$23 = 1 + 2 + 2^2 + 2^4.$$

▲

12.6. Ejemplo. La expansión p-ádica de -1 viene dada por

$$-1 = \sum_{n\geq 0} (p-1)\, p^n = (p-1) + (p-1)\, p + (p-1)\, p^2 + (p-1)\, p^3 + (p-1)\, p^4 + \cdots$$

Esto se sigue del hecho de que

$$\begin{aligned}
&-1 \equiv p - 1 \pmod{p},\\
&-1 \equiv p^2 - 1 = p - 1 + (p-1)\, p \pmod{p^2},\\
&-1 \equiv p^3 - 1 = p - 1 + (p-1)\, p + (p-1)\, p^2 \pmod{p^3},\\
&\quad \cdots
\end{aligned}$$

En efecto, usando la fórmula para la serie geométrica se obtiene

$$\sum_{n\geq 0} (p-1)\, p^n \equiv (p-1) \sum_{0\leq n\leq k-1} p^n \pmod{p^k} = (p-1)\, \frac{p^k - 1}{p-1} \equiv -1 \pmod{p^k}.$$

▲

12.7. Ejemplo. Sea p un primo impar. Entonces la expansión p-ádica de $\frac{1}{2} \in \mathbb{Z}_p$ viene dada por

$$\frac{1}{2} = \frac{p+1}{2} + \frac{p-1}{2}\, p + \frac{p-1}{2}\, p^2 + \frac{p-1}{2}\, p^3 + \frac{p-1}{2}\, p^4 + \cdots$$

En efecto, la serie geométrica nos da

$$\frac{p+1}{2} + \frac{p-1}{2} \sum_{n\geq 1} p^n = \frac{p+1}{2} + \frac{p-1}{2}\, \frac{p}{1-p} = \frac{p+1}{2} - \frac{p}{2} = \frac{1}{2}.$$

▲

El programa PARI/GP (http://pari.math.u-bordeaux.fr/) puede hacer cálculos con los números p-ádicos. Para especificar un número p-ádico, se puede escribir una serie en p truncada y luego poner `+ O (p^k)` para especificar que los términos a partir de $a_k\, p^k$ están omitidos:

```
1 + 2 + 2^3 + 2^5 + 2^7 + 2^9 + O(2^10)
```

Con estas expresiones se pueden hacer las operaciones aritméticas habituales; por ejemplo

```
? (1 + 2 + O(2^10)) * (1 + 2 + 2^3 + 2^5 + 2^7 + 2^9 + O(2^10))
% = 1 + O(2^10)
```

Para encontrar los primeros términos de la expansión p-ádica de un número racional, podemos escribirlo y poner después "`+ O (p^k)`":

```
? 1/2 + O (7^10)
% = 4 + 3*7 + 3*7^2 + 3*7^3 + 3*7^4 + 3*7^5 + 3*7^6 + 3*7^7 + 3*7^8 + 3*7^9 + O(7^10)
? 1/5 + O (3^10)
% = 2 + 3^2 + 2*3^3 + 3^4 + 3^6 + 2*3^7 + 3^8 + O(3^10)
? 1/5 + O (5^10)
% = 5^-1 + O(5^10)
? -1/5 + O (3^10)
% = 1 + 2*3 + 3^2 + 3^4 + 2*3^5 + 3^6 + 3^8 + 2*3^9 + O(3^10)
```

La función `valuation (x, p)` devuelve la valuación p-ádica de x, donde x es un número entero, racional o p-ádico:

```
? valuation (2018,2)
% = 1
? valuation (3/32,2)
% = -5
? valuation (3*7^4 + 3*7^5 + 3*7^6 + 3*7^7 + 3*7^8 + 3*7^9 + O(7^10), 7)
% = 4
```

En términos de las expansiones p-ádicas, la norma de $x = \sum_{-m\le n} a_n\, p^n \in \mathbb{Q}_p$ viene dada por

$$|x|_p = p^{-v_p(x)},$$

donde $v_p(x) = n$ es el primer índice en la serie con $a_n \neq 0$. Luego, tenemos

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\} = \{a_0 + a_1\, p + a_2\, p^2 + a_3\, p^3 + a_4\, p^4 + \cdots \mid a_0 \neq 0\}.$$

Todo ideal no nulo en $\mathbb{Z}_p$ es de la forma

$$p^n\, \mathbb{Z}_p = \{a_n\, p^n + a_{n+1}\, p^{n+1} + a_{n+2}\, p^{n+2} + a_{n+3}\, p^{n+3} + \cdots\}$$

para $n = 1, 2, 3, \ldots$

La biyección

$$\{0, 1, \ldots, p-1\}^{\mathbb{N}} \ni (a_0, a_1, a_2, a_3, \ldots) \longleftrightarrow a_0 + a_1\, p + a_2\, p^2 + a_3\, p^3 + \cdots \in \mathbb{Z}_p$$

demuestra que la cardinalidad de $\mathbb{Z}_p$ es $p^{\aleph_0} = 2^{\aleph_0}$, la cardinalidad del continuo. De la misma manera, $\mathbb{Q}_p$ tiene cardinalidad $2^{\aleph_0}$ (por ejemplo, podemos notar que en general, si R es un dominio de integridad, entonces hay inyecciones de conjuntos $R \hookrightarrow \mathrm{Frac}(R) \hookrightarrow R \times R$). En particular, $\mathbb{Q}_p$ y $\mathbb{Z}_p$ no son numerables.

Note que todo número real también puede ser escrito como una fracción decimal, por ejemplo $\pi = 3{,}1415926\ldots$ Sin embargo, estas expansiones no son únicas: tenemos $1{,}00000\ldots = 0{,}99999\ldots$, etc. Como acabamos de ver, en el caso no arquimediano las expansiones sí son únicas.

12.8. Advertencia. Aunque las expansiones p-ádicas permiten hacer cálculos específicos con los números p-ádicos, el lector no tiene por qué pensar en ellos como en sumas de la forma $\sum_n a_n\, p^n$, de la misma manera que uno raramente piensa en los números reales como en fracciones decimales infinitas.

Ejercicio 24.

1) Demuestre que si $x \in \mathbb{Z}_p$ tiene expansión p-ádica

$$x = \sum_{n\geq 0} a_n\, p^n = a_0 + a_1\, p + a_2\, p^2 + a_3\, p^3 + \cdots,$$

entonces

$$-x = (p - a_0) + \sum_{n\geq 1} (p - 1 - a_n)\, p^n = (p - a_0) + (p - 1 - a_1)\, p + (p - 1 - a_2)\, p^2 + (p - 1 - a_3)\, p^3 + \cdots$$

Note que, según esta fórmula, los números enteros negativos tienen expansión p-ádica infinita; por ejemplo, para $23 = 1 + 2 + 2^2 + 2^4$ tenemos

$$-23 = 1 + 2^3 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10} + \cdots \in \mathbb{Z}_2$$

2) Si la expansión p-ádica de $x \in \mathbb{Q}_p$ es dada por

$$x = \sum_{n\geq -m} a_n\, p^n = a_{-m}\, p^{-m} + a_{-m+1}\, p^{-m+1} + \cdots + a_0 + a_1\, p + a_2\, p^2 + \cdots,$$

demuestre que

$$-x = (p - a_{-m}) + \sum_{n\geq -m+1} (p - 1 - a_n)\, p^n = (p - a_{-m})\, p^{-m} + (p - 1 - a_{-m+1})\, p^{-m+1} + \cdots$$
$$+ (p - 1 - a_0) + (p - 1 - a_1)\, p + (p - 1 - a_2)\, p^2 + \cdots$$

Ejercicio 25.

1) Demuestre que un número p-ádico tiene expansión de la forma

$$x = a_0 + a_1\, p + a_2\, p^2 + \cdots + a_n\, p^n + 0 \cdot p^{n+1} + 0 \cdot p^{n+2} + \cdots$$

que termina en ceros si y solamente si x es un número natural $0, 1, 2, 3, \ldots$

2) Demuestre que un número p-ádico tiene expansión de la forma

$$x = a_{-m}\, p^{-m} + a_{-m+1}\, p^{-m+1} + \cdots + a_0 + a_1\, p + a_2\, p^2 + \cdots + a_n\, p^n + 0 \cdot p^{n+1} + 0 \cdot p^{n+2} + \cdots$$

que termina en ceros si y solamente si x es un número racional *no negativo* con denominador p^m para algún $m = 0, 1, 2, \ldots$

Recordemos que en $\mathbb{R}$ los números racionales son precisamente los números con expansión decimal eventualmente periódica; por ejemplo, $5/3 = 1{,}666666666\ldots$ El mismo resultado se cumple para $\mathbb{Q}_p$ y la expansión p-ádica.

Ejercicio 26. Supongamos que en la expansión p-adica $x = \sum_{-m\leq n} a_n\, p^n \in \mathbb{Q}_p$ los dígitos a_n son periódicos a partir de algún momento. Deduzca que $x \in \mathbb{Q}$.
(Use la serie geométrica.)

También es cierto que para todo número racional $x \in \mathbb{Q}$ los dígitos p-ádicos son periódicos a partir de algún momento, pero la prueba es un poco más técnica y no la doy como un ejercicio.

13 Topología sobre $\mathbb{Q}_p$ y $\mathbb{Z}_p$

Consideremos $\mathbb{Q}_p$ como un espacio métrico respecto a la norma p-ádica $d(x,y) = |x-y|_p$. Como todo espacio métrico, es de Hausdorff. Sin embargo, es un espacio ultramétrico, así que es totalmente inconexo y satisface otras propiedades exóticas. Además, $\mathbb{Q}_p$ tiene otras propiedades especiales que vienen del hecho de que los posibles valores de $|x|_p$ para $x \in \mathbb{Q}_p^\times$ son *discretos*: son de la forma $1/p^n$ para $n \in \mathbb{Z}$.

Por ejemplo, aparte de las bolas abiertas

$$B(x_0, \epsilon) := \{x \in \mathbb{Q}_p \mid |x - x_0|_p < \epsilon\}$$

que por la definición forman una base de la topología sobre $\mathbb{Q}_p$, podríamos considerar las bolas cerradas

$$\overline{B}(x_0, \epsilon) := \{x \in \mathbb{Q}_p \mid |x - x_0|_p \leq \epsilon\}.$$

Sin embargo,

$$B(x_0, 1/p^n) = \{x \in \mathbb{Q}_p \mid |x - x_0|_p < 1/p^n\} = \{x \in \mathbb{Q}_p \mid |x - x_0|_p \leq 1/p^{n+1}\} = \overline{B}(x_0, 1/p^{n+1}).$$

Recordemos brevemente algunas nociones de la topología general.

13.1. Definición.

- Un espacio métrico (X, d) es **secuencialmente compacto** si toda sucesión de puntos $x_n \in X$ contiene una subsucesión convergente respecto a la métrica d.
- Un espacio topológico X es **compacto** si todo recubrimiento abierto $X = \bigcup_{i \in I} U_i$ contiene un subrecubrimiento finito.
- Un espacio topológico X es **localmente compacto** si para todo punto $x \in X$ existe un subespacio compacto $C \subset X$ tal que C contiene un entorno abierto de x.
- Un espacio métrico (X, d) es **totalmente acotado** si para todo $\epsilon > 0$ existe un recubrimiento finito de X por bolas de radio ϵ.

Mencionemos algunos resultados relevantes (el lector puede consultar [Mun2000]).

- Todo subespacio cerrado $Z \subset X$ de un espacio métrico completo es también completo.

  (En efecto, si (x_n) es una sucesión de Cauchy en Z, esta converge a algún punto $x \in X$, entonces $x \in \overline{Z} = Z$, ya que Z es cerrado.)
- En un espacio de Hausdorff, todo subespacio compacto es cerrado [Mun2000, Theorem 26.3].
- Un espacio métrico X es secuencialmente compacto si y solamente si es compacto respecto a la topología inducida por la métrica [Mun2000, Theorem 28.2].
- Un espacio métrico es compacto si y solamente si es completo y totalmente acotado [Mun2000, Theorem 45.1].

  En particular, en un espacio métrico completo, un subespacio es compacto si y solamente si es cerrado y totalmente acotado. Es una generalización del **teorema de Heine–Borel** (que dice que todo subconjunto de $\mathbb{R}^n$ es compacto si y solamente si es cerrado y acotado; en $\mathbb{R}^n$ "acotado" implica "totalmente acotado").

13.2. Teorema. *$\mathbb{Z}_p$ es compacto y $\mathbb{Q}_p$ es localmente compacto.*

Primera demostración. Toda bola $B(x,\epsilon)$ en $\mathbb{Q}_p$ es cerrada y por lo tanto completa.

Además, toda bola $B(x,r)$ es totalmente acotada. Para simplificar el argumento, podemos suponer que $r = p$ (después se puede escalar las bolas que aparecen en la prueba) y que $x = 0$ (después se puede trasladar las bolas por x). Entonces, sin pérdida de generalidad, $B(x,r) = B(0,p) = \overline{B}(0,1) = \mathbb{Z}_p$. Necesitamos cubrir $\mathbb{Z}_p$ por las bolas de radio $0 < \epsilon < 1$. Sea $n \in \mathbb{N}$ un número tal que $1/p^n < \epsilon$. Luego,

$$p^n \mathbb{Z}_p = \overline{B}(0, 1/p^n) \subseteq B(0,\epsilon).$$

El cociente

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

es finito y la expresión

$$\mathbb{Z}_p = \bigcup_{x_0 \in \{0,1,\ldots,p^n-1\}} (x_0 + p^n \mathbb{Z}_p).$$

nos da un recubrimiento finito de $\mathbb{Z}_p$ por las bolas $x_0 + p^n \mathbb{Z}_p$.

Entonces, toda bola es compacta. Esto implica que $\mathbb{Z}_p$ es compacto y que $\mathbb{Q}_p$ es localmente compacto. ■

Segunda demostración. Podemos demostrar que $\mathbb{Z}_p$ es secuencialmente compacto. Sea $(x_n)_n$ una sucesión en $\mathbb{Z}_p$. Escribamos las expansiones p-ádicas correspondientes:

$$x_n = a_{n,0} + a_{n,1}\, p + a_{n,2}\, p^2 + a_{n,3}\, p^3 + \cdots$$

donde $a_{n,i}$ pertenecen al conjunto *finito* $\{0, 1, \ldots, p-1\}$. Entonces existe un número infinito de x_n con el mismo primer dígito $a_{n,0} = b_0$[*]; estos x_n forman una subsucesión $(x_n^{(0)})$. Por la misma razón, $(x_n^{(0)})$ contiene una subsucesión $(x_n^{(1)})$ donde todos los elementos tienen el mismo segundo dígito $a_{n,1} = b_1$, etcétera. De este modo se obtiene una cadena de subsucesiones

$$(x_n) \supset (x_n^{(0)}) \supset (x_n^{(1)}) \supset (x_n^{(2)}) \supset \cdots$$

donde todos los elementos de $x_n^{(k)}$ empiezan por

$$b_0 + b_1\, p + b_2\, p^2 + \cdots + b_k\, p^k$$

Podemos entonces tomar la "sucesión diagonal"

$$x_0^{(0)},\ x_1^{(1)},\ x_2^{(2)},\ x_3^{(3)},\ \ldots$$

que es una subsucesión de (x_n) y por la construcción converge a

$$b_0 + b_1\, p + b_2\, p^2 + b_3\, p^3 + \cdots$$

Para ver que $\mathbb{Q}_p$ es localmente compacto, notamos que para todo $x_0 \in \mathbb{Q}_p$ y $\epsilon > 0$ la bola

$$B(x,\epsilon) = \{x \in \mathbb{Q}_p \mid |x - x_0|_p < \epsilon\} = \{x \in \mathbb{Q}_p \mid |x - x_0|_p \leq 1/p^m\} \quad \text{para algún } m \in \mathbb{Z}$$

es compacta. De hecho, a toda sucesión $(x_n)_n$ en $B(x,\epsilon)$ corresponde una sucesión $(p^{-m} x_n)_n$ en $\mathbb{Z}_p$. Esta sucesión tiene una subsucesión que converge a algún $y \in \mathbb{Z}_p$ a la cual corresponde una subsucesión de $(x_n)_n$ que converge a algún $p^{-m}\, y \in B(x,\epsilon)$. ■

Para ver que $\mathbb{Q}_p$ no es secuencialmente compacto, podemos considerar, por ejemplo, la sucesión $x_n = p^{-n}$. Para $m \neq n$ se tiene

$$|p^{-m} - p^{-n}|_p = p^{\max\{m,n\}}.$$

Los puntos x_n cada vez están más lejos en la distancia inducida por $|\cdot|_p$, y entre ellos no se puede encontrar una subsucesión convergente.

[*] Esto es el **principio del palomar infinito**: si un número infinito de palomas se distribuyen en un número finito de palomares, entonces al menos habrá un palomar con un número infinito de palomas :-)

14 Series formales (ejercicios adicionales)

En esta sección vamos a revisar brevemente los cuerpos de series formales $\mathbb{F}_q((X))$ que son un análogo de los cuerpos $\mathbb{Q}_p$. Una diferencia fundamental es que los $\mathbb{Q}_p$ son cuerpos de característica 0, mientras que los $\mathbb{F}_q((X))$ son cuerpos de característica positiva. Los resultados de abajo pueden ser deducidos imitando nuestras pruebas para $\mathbb{Q}_p$. De hecho, hay una noción de **cuerpo local no arquimediano** que abarca $\mathbb{Q}_p$, $\mathbb{F}_q((X))$ y sus extensiones finitas.

Consideremos el cuerpo de funciones racionales con coeficientes en un cuerpo k:

$$k(X) = \{f/g \mid f, g \in k[X], g \neq 0\}$$

y la norma no arquimediana sobre $k(X)$ que corresponde a la valuación definida en 3.3:

$$v_X\left(\sum_{i\geq 0} a_i X^i\right) := \min\{i \mid a_i \neq 0\},$$

$$v_X(0) := +\infty, \quad v_X(f/g) := v_X(f) - v_X(g),$$

$$|f/g|_X := \rho^{v_X(f/g)},$$

donde $0 < \rho < 1$ es algún parámetro fijo.

Sea $k((X))$ la completación de $k(X)$ respecto a la norma $|\cdot|_X$.

Ejercicio 27. Demuestre que los posibles valores de $|\cdot|_X$ sobre $k((X))$ son 0 y ρ^n para $n \in \mathbb{Z}$.

Ejercicio 28. Establezca los siguientes análogos de las propiedades de 11.5.

1) Demuestre que
$$k[[X]] := \{\phi \in k((X)) \mid |\phi|_X \leq 1\}$$
es un subanillo de $k((X))$.

2) Demuestre que
$$k[[X]]^\times = \{\phi \in k[[X]] \mid |\phi|_X = 1\}.$$

3) Demuestre que todo elemento $\phi \in k((X))^\times$ puede ser escrito como uX^n, donde $u \in k[[X]]^\times$ y $n \in \mathbb{Z}$.

4) Demuestre que $k((X))$ es el cuerpo de fracciones de $k[[X]]$.

5) Demuestre que $k[[X]]$ es un anillo local: su único ideal maximal viene dado por
$$\mathfrak{m} = \{\phi \in k[[X]] \mid |\phi|_X < 1\} = X\,k[[X]].$$

6) Demuestre que todo ideal no nulo en $k[[X]]$ es de la forma $\mathfrak{m}^n = X^n\,k[[X]]$ para $n = 0, 1, 2, 3, \ldots$

7) Demuestre que
$$k[[X]]/X^n k[[X]] \cong k[X]/X^n k[X].$$

Ejercicio 29. Demuestre que los elementos de $k[[X]]$ y $k((X))$ son series en X.

1) Todo elemento $\phi \in k[[X]]$ puede ser representado de modo único por una serie
$$\phi = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + a_4 X^4 + \cdots$$
donde $a_i \in k$.

2) En general, todo elemento $\phi \in k((X))$ puede ser representado de modo único por una serie

$$\phi = a_{-m} X^{-m} + a_{-m+1} X^{-m+1} + \cdots + a_0 + a_1 X + a_2 X^2 + a_3 X^3 + a_4 X^4 + \cdots$$

El anillo $k[[X]]$ se denomina el **anillo de series formales** en la variable X con coeficientes en k, y el cuerpo $k((X))$ se denomina el **cuerpo de series de Laurent** en la variable X con coeficientes en k.

Ejercicio 30. Si $k = \mathbb{F}_q$ es un cuerpo finito, demuestre que $\mathbb{F}_q[[X]]$ es compacto y $\mathbb{F}_q((X))$ es localmente compacto.

PARI/GP puede hacer cálculos con series formales (con coeficientes en $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}, \mathbb{F}_q$, etc.):

```
? 1/(1+X) + O (X^10)
% = 1 - X + X^2 - X^3 + X^4 - X^5 + X^6 - X^7 + X^8 - X^9 + O(X^10)
? (1 + X + 1/2*X^2 + 1/6*X^3 + 1/24*X^4 + 1/120*X^5 + 1/720*X^6 + O (X^7))^3
% = 1 + 3*X + 9/2*X^2 + 9/2*X^3 + 27/8*X^4 + 81/40*X^5 + 81/80*X^6 + O(X^7)
? valuation ((X + 1/2*X^2 + 1/6*X^3 + O (X^4))^5, X)
% = 5
? 1/(1-X-X^2) + O (X^10)
% = 1 + X + 2*X^2 + 3*X^3 + 5*X^4 + 8*X^5 + 13*X^6 + 21*X^7 + 34*X^8 + 55*X^9
+ O(X^10)
```

Referencias

[Kat2007] Svetlana Katok, *p-adic analysis compared with real*, Student Mathematical Library, vol. 37, American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA, 2007. MR2298943
http://dx.doi.org/10.1090/stml/037

[KKS2000] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito, *Number theory 1: Fermat's dream*, Translations of Mathematical Monographs, vol. 186, American Mathematical Society, Providence, RI, 2000, Translated from the 1996 Japanese original by Masato Kuwata, Iwanami Series in Modern Mathematics. MR1728620

[Kob1984] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR754003
http://dx.doi.org/10.1007/978-1-4612-1112-9

[Mun2000] James R. Munkres, *Topology*, second ed., Pearson, 2000.