NÚMEROS p-ÁDICOS

GASTÓN ANDRÉS GARCÍA

RESUMEN. Éste es un curso introductorio al cuerpo de los número p-ádicos, donde p es un número primo. Al igual que se obtienen los números reales de los números racionales, estos cuerpos se obtienen completando el cuerpo de los racionales con respecto a una determinada métrica, la métrica p-ádica.

Basándonos en los desarrollos s-ádicos de los enteros, s cualquier número natural, comenzaremos estudiando la aritmética en los enteros con respecto a los desarrollos s-ádicos, para así definir de una forma más pragmática y rudimentaria, pero intuitiva, el anillo de números racionales s-ádicos. Este anillo resulta un cuerpo si y sólo si s es primo.

Finalmente, daremos la definición usual basada en la completación con respecto a una métrica y veremos que coincide con la dada anteriormente.

ÍNDICE

INTRODUCCIÓN

Estas notas corresponden a un curso dictado en el IV Encuentro Nacional de Álgebra (elENA IV) desarrollado en La Falda durante la semana del 4 al 9 de agosto de 2008. Puesto que el mismo es de carácter introductorio a la teoría de números p-ádicos, he tratado de acentuar primero algunos aspectos en la aritmética de estos cuerpos, y luego dar la definición concreta de los mismos usando completaciones.

Apoyado parcialmente por CONICET, FONCyT-ANPCyT, Secyt (UNC), Agencia Córdoba Ciencia y elENA.

Como es sabido, el cuerpo de los números racionales $\mathbb{Q}$ no es un cuerpo completo. Es decir, existen sucesiones de Cauchy de números racionales que pueden no converger a un número racional. Para *completar* estos agujeros, se completa $\mathbb{Q}$ a $\mathbb{R}$ usando el valor absoluto $|\cdot|$. Este proceso se denomina completación de $\mathbb{Q}$ con respecto a $|\cdot|$. El cuerpo de los números p-ádicos $\mathbb{Q}_p$ se obtiene a partir del cuerpo de los números racionales por completación con respecto a otro valor absoluto o norma, la norma p-ádica. Esta aplicación, similar en varios aspectos al valor absoluto usual, posee varias propiedades importantes, aunque sin embargo, algunas de ellas contrastan con nuestra intuición sobre la distancia.

Los números p-ádicos fueron introducidos por Hensel, aparentemente a partir de una analogía con el cuerpo de funciones racionales $\mathbb{C}(X)$. La idea es que dada una función racional

$$f(X) = \frac{P(X)}{Q(X)} \qquad \text{con } P,\ Q \in \mathbb{C}[X],$$

y dado $\alpha \in \mathbb{C}$ es siempre posible expandir f con una serie de Laurent en torno a α, es decir:

$$f(X) = \sum_{n_0}^{\infty} a_n (X-\alpha)^n.$$

La serie así obtenida refleja el comportamiento de la función $f(X)$ cuando X se aproxima a α, esto es "localmente en α". La primera observación que debemos hacer es que los cuerpos $\mathbb{C}(X)$ y $\mathbb{Q}$ tienen muchas propiedades semejantes. Cada uno de ellos es un cuerpo de fracciones de un dominio de ideales principales en el cual todos los ideales primos no nulos son maximales. Es esto lo que le sugiere a Hensel una contrucción análoga y así percibe que los elementos $(x-\alpha)$ son exactamente los primos del anillo $\mathbb{C}(X)$. La versión para $\mathbb{Q}$ entonces debería estar referida a los primos $p \in \mathbb{Z}$.

Fijemos entonces un primo $p \in \mathbb{Z}$. El análogo al desarrollo de un polinomio en potencias de $(x-\alpha)$ es el desarrollo de un entero positivo n en potencias de p, esto es:

$$n = n_0 + n_1 p + n_2 p^2 + ... + n_k p^k, \tag{0.1}$$

con $0 \leq n_i < p$ para todo $i = 1, \ldots, k$. Esta última condición puede parecer no tener analogía en el caso del anillo $\mathbb{C}[X]$. Sin embargo, el cociente de $\mathbb{C}[X]$ por el ideal generado por $(x-\alpha)$ es isomorfo a $\mathbb{C}$, y las constantes son un sistema de representantes. De la misma forma los números entre 0 y $p-1$ son representantes de los elementos del cociente de $\mathbb{Z}$ por el ideal $p\mathbb{Z}$ generado por p.

La expresión (0.1) se se denomina "expansión de n en base p", o el desarrollo p-ádico de n y como veremos más adelante, siempre existe. Vale notar, que como en el caso de los polinomios, ésta es una expansión finita.

Ahora bien, a todo número racional x lo podemos escribir como un cociente entre dos números enteros $x = a/b$. Dicho cociente, corresponde ser el análogo al caso de la función $f(X)$ como cociente de dos polinomios en $\mathbb{C}[X]$. Así, operando análogamente al caso de los polinomios, podemos obtener una serie de Laurent en potencias de p. El único caso que hay que notar es que la suma de dos coeficientes de la expansión puede ser mayor que p, y debe entonces ser escrito nuevamente. La serie obtenida

$$x = \frac{a}{b} = \sum_{n_0}^{\infty} a_n p^n,$$

refleja "localmente en p ", las propiedades del numero racional $x = a/b$.

Se puede ver que el conjunto de todas las series formales de Laurent en p forma un cuerpo que contiene al cuerpo de los números racionales pero es estrictamente mayor respecto a la inclusión. Este cuerpo se llama el cuerpo de los números p-ádicos, y es denotado por $\mathbb{Q}_p$.

Para tener una definición formal, debemos tener una topología en $\mathbb{Q}$, en la cual la sucesión $\{p^n\}_{n\in\mathbb{N}}$ tienda a cero cuando $n \to \infty$, para que así las series de potencias en p^n puedan tener la posibilidad de converger. Esta topología viene dada por una norma, la norma p-ádica y $\mathbb{Q}_p$ resulta ser la completación con respecto a esta norma.

Es un hecho que todo elemento x de $\mathbb{Q}_p$ admite una expresión canónica, la cual permite escribir a x en un sistema similar al sistema decimal, el sistema de desarrollos p-ádicos. Por tal motivo, comenzaremos este curso recordando los desarrollos s-ádicos para los números enteros.

Finalmente, aparte del interés matemático en sí mismo como en el análsis p-ádico, los cuerpos de los números p-ádicos tienen aplicaciones en otras ramas de la matemática. Por ejemplo, resulta que los mismos son de particular interés e importancia en la teoría algebraica de números y en la geometría algebraica. Además, la noción de completación con respecto a una norma o valuación se utiliza, entre otras aplicaciones, en la teoría de representaciones modulares de grupos, es decir, representaciones de grupos sobre cuerpos de característica positiva.

Agradecimientos

Quisiera agradecer a los organizadores de este encuentro por haberme dado la posibilidad de dictar este curso. Quisiera también agradecerle a L. Aburto por haberme acercado sus notas preliminares, a P. Román, S. Simondi y P. Tirao por haber intercambiado conmigo ideas sobre el contenido de este curso, y especialmente a L. Cagliero, por su siempre buena disposición a discutir sobre matemática; este curso se basa esencialmente en las discusiones y charlas que he mantenido con él.

1. Preliminares

Comenzaremos recordando algunas definiciones y conceptos básicos. De aquí en más, $\mathbb{N}$ denotará los números naturales, $\mathbb{Z}$ los enteros, $\mathbb{Q}$ los racionales, $\mathbb{R}$ los reales y $\mathbb{C}$ los complejos.

1.1. Congruencias en $\mathbb{Z}$.

Sean $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$

Definición 1.1. Diremos que a *es congruente* a b módulos m, en símbolos

$$a \equiv b \mod m,$$

si m divide a $b - a$.

Ejemplo 1.2. (a) $1 \equiv 15 \mod 2$, pues $2|15 - 1$.
(b) $25 \equiv 7 \mod 9$, pues $9|7 - 25 = -18$.

En la siguiente proposición resumimos algunas propiedades básicas.

Proposición 1.3.
(a) $\forall\ a \in \mathbb{Z}$, $a \equiv a \mod m$.
(b) $\forall\ a, b \in \mathbb{Z}$, $a \equiv b \mod m \Leftrightarrow b \equiv a \mod m$.
(c) $\forall\ a, b, c \in \mathbb{Z}$, $a \equiv b \mod m$ *y* $b \equiv c \mod m$ *entonces* $a \equiv c \mod m$.
(d) $\forall\ a, b, c \in \mathbb{Z}$, $a \equiv b \mod m \Leftrightarrow a + c \equiv b + c \mod m$.
(e) $\forall\ a, b, c \in \mathbb{Z}$, $a \equiv b \mod m \Leftrightarrow a + m.c \equiv b \mod m$.
(f) $\forall\ a, b, c \in \mathbb{Z}$, $a \equiv b \mod m \Leftrightarrow a.c \equiv b.c \mod m$.
(g) $\forall\ a \in \mathbb{Z}$, $a \equiv 0 \mod m \Leftrightarrow m|a$.
(h) $\forall\ a, b \in \mathbb{Z}$, $a \equiv b \mod m$ *si y sólo si* a *y* b *tienen el mismo resto al dividir por* m. *En particular, todo número es congruente a su resto de la división por* m.

Demostración. Los ítems $(a), \ldots, (g)$ quedan como ejercicio. Probaremos sólo (h).

Por el algoritmo de división podemos escribir

$$\begin{aligned} a &= mh + r_a, \qquad 0 \leq r_a < m, \\ b &= mk + r_b, \qquad 0 \leq r_b < m. \end{aligned}$$

Supongamos que $r_a \leq r_b$. Entonces $b - a = m(k-h) + (r_b - r_a)$ con $0 \leq r_b - r_a < m$. Luego, por la unicidad del algoritmo de división se sigue que $r_b - r_a$ es el resto de la división de $b - a$ por m. Por lo tanto

$$a \equiv b \mod m \Leftrightarrow m | b - a \Leftrightarrow r_b = r_a.$$

□

Observación 1.4. Sea $m \in \mathbb{Z}$. Se define en $\mathbb{Z}$ la relación $a \sim b$ si y sólo si $a \equiv b \mod m$. Las propiedades $(a), (b)$ y (c) dicen que la relación es de equivalencia. Como tal, determina una partición de $\mathbb{Z}$ en clases de equivalencia. Por ejemplo, si $m = 5$, las clases de equivalencia son

$$\begin{aligned} \bar{0} &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\ \bar{1} &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\ \bar{2} &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\ \bar{3} &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\ \bar{4} &= \{\ldots, -6, -1, 4, 9, 14, \ldots\} \end{aligned}$$

Notar que dos enteros cualesquiera están en la misma clase de equivalencia si y sólo si tienen el mismo resto al dividir por m.

1.1.1. Los anillos $\mathbb{Z}/m\mathbb{Z}$. En esta subsección recordamos la definición de los conjuntos $\mathbb{Z}/m\mathbb{Z}$ junto con sus operaciones básicas. Dado $m \in \mathbb{Z}$ definimos

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\},$$

es decir, el conjunto dado por las clases de equivalencia módulo m, que está en biyección con el conjunto dado por los posibles restos de la división por m. Por ejemplo, si $m = 5$,

$$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}.$$

Notar que este conjunto consta de un representante por cada clase de equivalencia dada por la congruencia módulo m.

Usando las propiedades de congruencia, podemos definir las operaciones dos operaciones binarias:

$$\begin{aligned} + : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z}, \\ (\bar{a}, \bar{b}) &\mapsto \overline{a+b} \end{aligned} \qquad \begin{aligned} \cdot : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z}. \\ (\bar{a}, \bar{b}) &\mapsto \overline{a \cdot b} \end{aligned}$$

Ambas operaciones son cerradas, conmutativas, asociativas, cumplen la propiedad distributiva y tienen elementos neutros, $\bar{0}$ para la suma y $\bar{1}$ para el producto. Además, siempre existe un elemento opuesto con respecto a la suma $-\bar{a} = \overline{m-a}$.

Usualmente, si no hay peligro de confusión, se denota por abuso de notación $\{0, \ldots, m-1\}$ a los elementos de $\mathbb{Z}/m\mathbb{Z}$.

Ejemplo 1.5. Las siguientes son las tablas de la suma y el producto para $\mathbb{Z}/6\mathbb{Z}$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Notar que la ecuación $x^2 = 1$ tiene las soluciones $x = 1$ y $x = 4$; pero la ecuación $x^2 = 2$ no tiene soluciones en $\mathbb{Z}/6\mathbb{Z}$.

Ejercicios.

1. Probar las propiedades $(a), \ldots, (g)$ de la Proposición 1.3.
2. Probar que
   - a) Para todo $m \in \mathbb{Z}$, las operaciones suma y producto están bien definidas en $\mathbb{Z}/m\mathbb{Z}$, es decri, no dependen de la elección del representante.
   - b) Ambas operaciones son conmutativas, asociativas y cumplen la propiedad distributiva.
   - c) $\bar{0}$ es el elemento neutro para la suma y $\bar{1}$ para el producto.
   - d) Para todo $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$, $-\bar{a} = \overline{m - a}$ es el elemento opuesto con respecto a la suma, es decir $\bar{a} + (-\bar{a}) = 0$ en $\mathbb{Z}/m\mathbb{Z}$.
3. Calcular las tablas de la suma y el producto para $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ y $\mathbb{Z}/5\mathbb{Z}$. ¿Qué elementos tienen inverso multiplicativo?
4. ¿ Tiene la ecuación $x^2 = 2$ solución en $\mathbb{Z}/3\mathbb{Z}$ y en $\mathbb{Z}/4\mathbb{Z}$?

1.2. Anillos y cuerpos. En esta subsección recordamos brevemente las definiciones de anillo y cuerpo, junto con algunos ejemplos.

Definición 1.6. Un *anillo con unidad* R es un conjunto munido de dos operaciones binarias

$$+ : R \times R \to R, \qquad \cdot : R \times R \to R,$$

denominadas suma y producto, que satisfacen los siguientes axiomas:

- $(r1)$ $\forall\ a, b \in R,\ a + b = b + a$ (conmutatividad de la suma).
- $(r2)$ $\forall\ a, b, c \in R,\ a + (b + c) = (a + b) + c$ (asociatividad de la suma).
- $(r3)$ Existe $0 \in R$ tal que $\forall\ a \in R,\ a + 0 = 0 + a = a$ (elemento neutro para la suma).
- $(r4)$ $\forall\ a \in R$, existe $b \in R$ tal que $a + b = b + a = 0$. Al elemento b se lo llama inverso aditivo de a y se lo denota usualmente por $-a$ (inverso aditivo).
- $(r5)$ $\forall\ a, b, c \in R,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociatividad del producto).
- $(r6)$ Existe $1 \in R$ tal que $\forall\ a \in R,\ a \cdot 1 = 1 \cdot a = a$ (elemento neutro para el producto).
- $(r7)$ $\forall\ a, b, c \in A, a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$ (propiedad distributiva de $\cdot$ respecto de $+$).

Si el producto $\cdot$ es conmutativo, diremos que R *es un anillo conmutativo.*

Ejemplo 1.7. (a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos con las operaciones usuales, pero $\mathbb{N}$ no es un anillo.

(b) Para todo $m \in \mathbb{Z}$, el conjunto $\mathbb{Z}/m\mathbb{Z}$ es un anillo con las operaciones definidas anteriormente.

(c) El conjunto de las matrices $M_n(\mathbb{R})$ de tamaño $n \times n$ con las operaciones usuales es un anillo, donde el elemento neutro para el producto está dado por la matríz identidad.

Definición 1.8. El conjunto de unidades $\mathcal{U}(R)$ de un anillo R es el conjunto formado por los elementos con inverso multiplicativo en el anillo, esto es

$$\mathcal{U}(R) := \{a \in R |\ \exists\ b \in R :\ a \cdot b = b \cdot a = 1\}$$

Por ejemplo, $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$ y $\mathcal{U}(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$.

Recordamos ahora la definición de ideal de un anillo conmutativo. Existen también nociones de ideales a izquierda, a derecha y biláteros en anillos que no son conmutativos que aquí no daremos, pues sólo trabajaremos con anillos conmutativos.

Definición 1.9. Un *ideal* de un anillo conmutativo R es un subconjunto I de R tal que

(*i*) $x + y \in I$, para todo $x, y \in I$,
(*ii*) $r \cdot x \in I$ para todo $r \in R$ y $x \in I$.

Claramente, los subconjuntos $\{0\}$ y R de un anillo R son ideales de R. A estos ideales se los llama *triviales*. Es también claro que si un ideal contiene a la unidad, entonces dicho ideal debe ser R.

Diremos que un ideal I es *maximal* si I es no trivial y si J es otro ideal de R tal que $I \subseteq J$, entonces $I = J$ o $J = R$. Esto es, un ideal maximal no está contenido en ningún ideal que no sea trivial.

Ejemplo 1.10. Para todo $m \in \mathbb{Z}$, el conjunto $m\mathbb{Z}$ de múltiplos de m es un ideal de $\mathbb{Z}$ que resulta maximal si y sólo si m es primo – ver Ejercicio 8.

Sea R un anillo conmutativo e I un ideal de R. Dado $x \in R$, denotamos por $x+I$ al conjunto dado por $\{x + a |\ a \in I\}$. Claramente, $x + I = y + I$ si y sólo si $x - y \in I$. Así, se define el conjunto cociente R/I como

$$R/I = \{x + I | x \in R\}.$$

R/I resulta un anillo conmutativo con las operaciones definidas por

$$(x + I) + (y + I) = (x + y) + I \quad \text{y} \quad (x + I) \cdot (y + I) = (x \cdot y) + I, \tag{1.1}$$

donde el elemento neutro para la suma es $I = 0 + I$, el elemento neutro para el producto es $1 + I$ y el inverso aditivo de $x + I$ es $-x + I$. Es decir, se puede probar que estas operaciones están bien definidas y dotan a R/I de una estructura de anillo conmutativo – ver Ejercicio 11. Usualmente se denota $\bar{x} = x + I$, cuando es claro sobre qué ideal se toma el cociente.

Definición 1.11. Un *cuerpo* $\Bbbk$ es un anillo conmutativo tal que $\forall\ a \in \Bbbk$, existe $b \in \Bbbk$ tal que $a \cdot b = b \cdot a = 1$. Al elemento b se lo llama inverso multiplicativo de a y se lo denota usualmente por a^{-1}.

Ejemplo 1.12. (*a*) $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos con las operaciones usuales, pero $\mathbb{N}$, $\mathbb{Z}$ y $M_n(\mathbb{R})$ no lo son.

(*b*) Un anillo conmutativo es un cuerpo si todos sus elementos no nulos son unidades, *i.e.* $\mathcal{U}(R) = R \setminus \{0\}$. En particular, $\mathcal{U}(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$, $\mathcal{U}(\mathbb{R}) = \mathbb{R} \setminus \{0\}$ y $\mathcal{U}(\mathbb{C}) = \mathbb{C} \setminus \{0\}$.

(*c*) Si R es un anillo conmutativo e I es un ideal maximal, entonces, R/I es un cuerpo. Recíprocamente, si I es un ideal no trivial y R/I es un cuerpo, entonces I es maximal – ver Ejercicio 11.

Ejercicios.

1. Probar que con las operaciones definidas en la subsección anterior $\mathbb{Z}/m\mathbb{Z}$ es un anillo conmutativo para todo $m \in \mathbb{Z}$.
2. Probar que $M_n(\mathbb{R})$ es un anillo. ¿Por qué no es un cuerpo?
3. Probar que $\mathbb{Z}/m\mathbb{Z}$ es un cuerpo si y sólo si m es un número primo. En ese caso, se lo denota $\mathbb{F}_m$.
4. Sea $\Bbbk$ un cuerpo. La *característica* de $\Bbbk$, denotada $\operatorname{car}\Bbbk$, es el menor entero positivo n tal que $\underbrace{1+\cdots+1}_{n-veces} = 0$. Si tal entero no existe, decimos que $\operatorname{car}\Bbbk = 0$.
   a) Probar que $\operatorname{car}\mathbb{R} = \operatorname{car}\mathbb{Q} = \operatorname{car}\mathbb{C} = 0$.
   b) Dado un número primo p, calcular $\operatorname{car}\mathbb{F}_p$.
   c) Sea $\Bbbk$ un cuerpo, entonces $\operatorname{car} k = 0$ o $\operatorname{car} k = p$, p un número primo.
5. Probar que $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$.
6. Probar que $\mathcal{U}(\mathbb{Z}/m\mathbb{Z}) = \{a \in \mathbb{Z}/m\mathbb{Z} |\ (a, m) = 1\}$
7. Calcular $\mathcal{U}(M_n(\mathbb{R}))$.
8. Probar que para todo $m \in \mathbb{Z}$, el conjunto $m\mathbb{Z}$ de múltiplos de m es un ideal de $\mathbb{Z}$. Más aún, este ideal resulta maximal si y sólo si m es primo. Esto establece una correspondencia entre números primos e ideales maximales de $\mathbb{Z}$.
9. Sea R un anillo conmutativo e I, J dos ideales de R. Probar que los conjuntos
$$I + J = \{x + y |\ x \in I,\ y \in J\},$$
$$I \cdot J = \{x \cdot y |\ x \in I,\ y \in J\},$$
$$I \cap J = \{x |\ x \in I,\ x \in J\},$$
son ideales de R.
10. Probar que todo elemento no nulo de un anillo conmutativo R está contenido en un ideal maximal (Ayuda: usar el Lema de Zorn).
11. Sea R un anillo e I un ideal de R.
    a) Probar que la relación $x \sim y \Leftrightarrow x - y \in I$ define una relación de equivalencia en R, cuyas clases de equivalencia son exactamente los conjuntos $\bar{x} = x + I$. En particular, el conjunto R/I es el cociente de R por esta relación de equivalencia.
    b) Probar que las operaciones definidas en (1.1), están bien definidas y hacen del conjunto R/I un anillo conmutativo.
    c) Probar que R/I es un cuerpo si y sólo si I es maximal.

2. Desarrollos s-ádicos

Usualmente escribimos los números racionales en sistema decimal, es decir, en cifras cuyos dígitos van del 0 al 9:

$$10; 1235; 3,1416; 928,$$

y desde pequeños aprendimos a operar con ellos. Los métodos para operar con los números racionales se basan en el hecho que éstos se expresan en forma decimal, esto es

$$10 = 1 \cdot 10$$
$$1235 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 5$$
$$3,1416 = 3 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + 6 \cdot 10^{-3}$$
$$928 = 9 \cdot 10^2 + 2 \cdot 10 + 8$$

Así, $3,1416 \times 10 = 31,416$ se puede ver como

$$(3 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + 6 \cdot 10^{-3}) \cdot 10 = 3 \cdot 10 + 1 \cdot 10^0 + 4 \cdot 10^{-1} + 6 \cdot 10^{-2} = 31,416.$$

Además de con 10, esto puede hacerse con cualquier número natural s. La idea es expresar cualquier número racional q como una expresión polinómica en s, que quizás involucre potencias negativas, cuyos coeficientes sean números naturales mayores o iguales a 0 y menores a s. A este desarrollo se lo denomina *desarrollo s-ádico* de q. Por ejemplo,

$$2351 = 3 \cdot 5^4 + 3 \cdot 5^3 + 4 \cdot 5^2 + 0 \cdot 5 + 1,$$

es el desarrollo 5-ádico de 2351. Para encontrar los desarrollos s-ádicos de un número entero m se utiliza el algoritmo de división de la siguiente manera: primero se divide m por s. Luego, al cociente de dicha división se lo divide por s y así sucesivamente hasta llegar a un cociente que sea menor que s. La sucesión (en orden inverso) dada por los restos de las sucesivas divisiones son los coeficientes de la expresión en potencias de s. Por ejemplo,

$$\begin{array}{rl|l|l|l|l}
2351 & 5 & & & & \\
\cline{2-2}
35 & 470 & 5 & & & \\
\cline{2-3}
01 & 20 & 94 & 5 & & \\
\cline{2-4}
\underline{1} & \underline{0} & 44 & 18 & 5 & \\
\cline{3-5}
 & & \underline{4} & \underline{3} & \underline{3} &
\end{array}$$

Los sucesivos restos, en orden inverso, dieron 3 3 4 0 1, quienes son exactamente los coeficientes de la expresión dada anteriormente. Veamos por qué sucede esto. Utilizando el algoritmo de división escribimos en cada paso al dividendo como la suma del cociente por el divisor más el resto:

$$\begin{aligned}
2351 &= 470 \cdot 5 + 1 = (94 \cdot 5 + 0) \cdot 5 + 1 = 94 \cdot 5^2 + 0 \cdot 5 + 1 = (18 \cdot 5 + 4) \cdot 5^2 + 0 \cdot 5 + 1 \\
&= 18 \cdot 5^3 + 4 \cdot 5^2 + 0 \cdot 5 + 1 = (3 \cdot 5 + 3)5^3 + 4 \cdot 5^2 + 0 \cdot 5 + 1 \\
&= 3 \cdot 5^4 + 3 \cdot 5^3 + 4 \cdot 5^2 + 0 \cdot 5 + 1
\end{aligned}$$

Escribimos entonces $2351 = (2351)_{10} = (33401)_5$ para especificar sobre qué base está escrito el desarrollo s-ádico. Aunque resulte redundante escribir $2351 = (2351)_{10}$, lo haremos cuando querramos acentuar la base del desarrollo. Así,

$$\begin{aligned}
2351 &= (2351)_{10} = (100100101111)_2 \\
37 &= (37)_{10} = (201)_6 \\
1024 &= (1024)_{10} = (714)_{12}
\end{aligned}$$

Teorema 2.1. *Sea $s \in \mathbb{N},\ s > 1$. Para todo $n \in \mathbb{N}$ existe una expresión polinomial en s, llamado el desarrollo s-ádico de n, del tipo siguiente*

$$n = \sum_{i=0}^{t} a_i s^i = a_t s^t + \cdots + a_1 s + a_0,$$

donde $a_i \in \mathbb{Z},\ 0 \leq a_i < s$. Dicho desarrollo es único, en el siguiente sentido: si

$$\sum_{i=0}^{t} a_i s^i = \sum_{j=0}^{h} b_j s^j, \qquad 0 \leq i, j < s,\ a_t \neq 0 \neq b_h,$$

entonces $t = h$ y $a_i = b_i$ para todo $1 \leq i \leq t = h$. En tal caso decimos que $(a_t a_{t-1} \cdots a_1 a_0)_s$ es el desarrollo de n en base s.

Demostración. Probaremos el teorema por inducción global. Si $n = 1$, el desarrollo s-ádico de 1 es $1.s^0$ y el teorema es cierto. Supongamos que el teorema ha sido probado para todos los enteros positivos menores que un cierto entero positivo k y probemos que el teorema es cierto para k.

Por el algoritmo de división tenemos que

$$k = s \cdot q + r, \qquad 0 \leq r < s.$$

Más aún, podemos suponer que $s < k$ pues si $k \leq s$, entonces su desarrollo s-ádico es

$$\begin{aligned} k &= 0 \cdot s + k, \quad \text{si } k < s, \\ k &= 1 \cdot s + 0, \quad \text{si } k = s. \end{aligned}$$

Luego, de suponer que $s < k$ se sigue que $0 < q$. Por lo tanto, como $1 < s$ tenemos que

$$q < q \cdot s \leq q \cdot s + r = k.$$

Por otro lado, por hipótesis inductiva, el teorema vale para q, es decir, existe una expresión polinomial en s tal que

$$q = \sum_{i=0}^{t} a_i s^i = a_t s^t + \cdots + a_1 s + a_0, \quad 0 \leq a_i < s$$

Así,

$$\begin{aligned} k = q \cdot s + r &= \left(\sum_{i=0}^{t} a_i s^i \right) \cdot s + r = (a_t s^t + \cdots + a_1 s + a_0) \cdot s + r \\ &= a_t s^{t+1} + \cdots + a_1 s^2 + a_0 s + r, \end{aligned}$$

que es un desarrollo s-ádico de k, lo que prueba la primera parte del teorema.

Veamos la unicidad. Supongamos que existen dos desarrollos s-ádicos

$$\sum_{i=0}^{t} a_i s^i = \sum_{j=0}^{h} b_j s^j, \qquad 0 \leq i, j < s, \ a_t \neq 0 \neq b_h.$$

Entonces

$$a_0 + \left(\sum_{i=1}^{t} a_i s^{i-1} \right) \cdot s = b_0 + \left(\sum_{j=1}^{h} b_j s^{j-1} \right) \cdot s.$$

Como $0 \leq a_0, b_0 < s$, de la unicidad en el algoritmo de división se sigue que

$$a_0 = b_0 \qquad \text{y} \qquad \sum_{i=1}^{t} a_i s^{i-1} = \sum_{j=1}^{h} b_j s^{j-1}.$$

Aplicando la hipótesis inductiva en el término de la derecha, resulta que $t = h$ y $a_i = b_i$ para todo $1 \leq i \leq h = t$, y el teorema queda demostrado. □

Observación 2.2. La escritura decimal que estamos acostumbrados a usar en los números enteros no es ni más ni menos que el desarrollo 10-ádico.

2.1. Operaciones con desarrollos s-ádicos. Las operaciones, suma, resta, multiplicación y división, se realizan de manera muy similar a las operaciones en desarrollo decimal o 10-ádico. En esta sección discutiremos cómo se realizan estas operaciones en otras bases.

2.1.1. Suma. Calculemos la siguiente suma: $(4412)_5 + (301)_5$. Para comprender la regla, escribamos primero los desarrollos como expresiones polinómicas y realicemos la suma

$$\begin{aligned}(4412)_5 &= 4\cdot 5^3 + 4\cdot 5^2 + 1\cdot 5 + 2\\ (301)_5 &= \underline{\qquad 3\cdot 5^2 + 0\cdot 5 + 1}\\ &\qquad 4\cdot 5^3 + 7\cdot 5^2 + 1\cdot 5 + 3\end{aligned}$$

El resultado obtenido es $4\cdot 5^3 + 7\cdot 5^2 + 1\cdot 5 + 3$, que no es un desarrollo s-ádico pues hay un coeficiente que es mayor que 5. Sin embargo, $7 = 5+2$, luego $7\cdot 5^2 = (5+2)\cdot 5^2 = 1\cdot 5^3 + 2\cdot 5^2$ y así

$$\begin{aligned}4\cdot 5^3 + 7\cdot 5^2 + 1\cdot 5 + 3 &= 4\cdot 5^3 + 1\cdot 5^3 + 2\cdot 5^2 + 1\cdot 5 + 3\\ &= 5\cdot 5^3 + 2\cdot 5^2 + 1\cdot 5 + 3\\ &= 1\cdot 5^4 + 0\cdot 5^3 + 2\cdot 5^2 + 1\cdot 5 + 3\end{aligned}$$

Luego, $(4412)_5 + (301)_5 = (10213)_5$. Claramente, la suma se realiza de forma análoga a la que estamos acostumbrados. Sumamos las cifras correspondientes y cada vez que superamos s, en este caso 5, debemos sumar 1 a la cifra siguiente, es decir, utilizando congruencias y "llevandose unidades". Para realizar las operaciones, no especificaremos la base sobre la cual estamos trabajando para no entorpecer la notación.

$$\begin{array}{rcccc} & {\scriptstyle +1} & 4^{+1} & 4 & 1\ 2\\ + & & 3 & 0 & \underline{1}\\ & 1 & 0 & 2 & 1\ 3\end{array}$$

Calculemos ahora la suma $(345)_6 + (523)_6 + (1155)_6$:

$$\begin{array}{rcccc} & {\scriptstyle +1} & 3^{+2} & 4^{+2} & 5\\ & & 5 & 2 & 3\\ + & 1 & 1 & 5 & \underline{5}\\ & 2 & 5 & 1 & 1\end{array}$$

Así $(345)_6 + (523)_6 + (1155)_6 = (2511)_6$.

2.1.2. Orden en desarrollos s-ádicos. Sabemos que en los enteros existe un orden. ¿Cómo se refleja este orden en los desarrollos s-ádicos?

Sean $a = (a_t a_{t-1}\cdots a_1 a_0)_s$ y $b = (b_h b_{h-1}\cdots b_1 b_0)_s$ dos números naturales expresados en base s y supongamos que $a \neq b$. Luego, $a = a_t s^t + a_{t-1}s^{t-1} + \cdots + a_1 s + a_0$, $b = b_h s^h + b_{h-1}s^{h-1} + \cdots + b_1 s + b_0$ y por el orden en los naturales tenemos que $a < b$ si y sólo si

$$\begin{aligned}a_t s^t + a_{t-1}s^{t-1} + \cdots + a_1 s + a_0 &< b_h s^h + b_{h-1}s^{h-1} + \cdots + b_1 s + b_0\\ &\Leftrightarrow t < h \text{ o } t = h \text{ y } a_m < b_m,\end{aligned}$$

donde $m = \max\{1 \leq i \leq t = h |\ a_i \neq b_i\}$; tal m existe pues estamos suponiendo que $a \neq b$. Esto se refleja en el desarrollo en base s como el orden lexicográfico (o el orden del diccionario):

$$(a_t a_{t-1}\cdots a_1 a_0)_s < (b_h b_{h-1}\cdots b_1 b_0)_s \Leftrightarrow t < h \text{ o } t = h \text{ y } a_m < b_m,$$

donde $m = \max\{1 \leq i \leq t = h |\ a_i \neq b_i\}$. Por ejemplo, $(2020)_3 > (121)_3$, $(201)_3 > (121)_3$ y $(210)_3 > (200)_3 > (21)_6$.

2.1.3. Resta. Como el conjunto de los números enteros no negativos no es un anillo, primero describiremos la operación de la resta utilizando el orden dado en la subsección anterior, de manera tal de asegurarnos que el resultado sea un número entero. Consideremos primero un ejemplo: tomemos $60 = (2020)_3$ y $16 = (121)_3$. Claramente, $60 - 16 = 44$ y $44 = (1122)_3$. Pues bien,

$$\begin{aligned} (2020)_3 &= 2\cdot 3^3 + 0\cdot 3^2 + 2\cdot 3 + 0 \\ -\quad (121)_3 &= \underline{\qquad\quad 1\cdot 3^2 + 2\cdot 3 + 1} \\ &\qquad 2\cdot 3^3 - 1\cdot 3^2 + 0\cdot 3 - 1 \end{aligned}$$

Al igual que para la suma, el resultado obtenido no es un desarrollo 3-ádico. Para lograrlo, debemos operar de la siguiente manera:

$$\begin{aligned} 2\cdot 3^3 - 1\cdot 3^2 + 0\cdot 3 - 1 &= 1\cdot 3^3 + 3\cdot 3^2 - 1\cdot 3^2 + 0\cdot 3 - 1 \\ &= 1\cdot 3^3 + 2\cdot 3^2 + 1\cdot 3^2 - 1\cdot 3^2 + 0\cdot 3 - 1 \\ &= 1\cdot 3^3 + 2\cdot 3^2 - 1\cdot 3^2 + 3\cdot 3^1 + 0\cdot 3 - 1 \\ &= 1\cdot 3^3 + 2\cdot 3^2 - 1\cdot 3^2 + 2\cdot 3 + 1\cdot 3 - 1 \\ &= 1\cdot 3^3 + 1\cdot 3^2 + 2\cdot 3 + 3 - 1 \\ &= 1\cdot 3^3 + 1\cdot 3^2 + 2\cdot 3 + 2. \end{aligned}$$

Luego, la resta se realiza de forma análoga a la que estamos acostumbrados: restando las cifras correspondientes y cada vez que debamos restar una cifra mayor a una quedanes menor, debemos tomar prestado de la cifra anterior s unidades, en este caso 3, y debemos restar 1 a la cifra siguiente, es decir, utilizando congruencias y "sustrayendo unidades":

$$\begin{array}{rcccc} & 2 & 0 & 2^{-1} & {}^{+3}0 \\ - & & 1 & 2 & 1 \\ \hline & & & & 2 \end{array} \rightsquigarrow - \begin{array}{cccc} 2 & 0 & 1 & {}^{+3}0 \\ & 1 & 2 & 1 \\ \hline & & & 2 \end{array} \rightsquigarrow - \begin{array}{cccc} 2^{-1} & {}^{+3}0^{-1} & {}^{+3}1 & {}^{+3}0 \\ & 1 & 2 & 1 \\ \hline 1 & 1 & 2 & 2 \end{array}$$

Calculemos ahora $(20341)_5 - (2340)_5$ y $(3216)_7 - (426)_7$:

$$\begin{array}{rcccc} & 2^{-1} & {}^{+5}0^{-1} & {}^{+5}3^{-1} & {}^{+5}0 \quad 1 \\ - & & 2 & 3 & 4 \quad 0 \\ \hline & 1 & 2 & 4 & 1 \quad 1 \end{array}$$

Así $(20341)_5 - (2340)_5 = (12411)_5$; y

$$\begin{array}{rcccc} & 3^{-1} & {}^{+7}2^{-1} & {}^{+7}1 & 6 \\ - & & 4 & 2 & 6 \\ \hline & 2 & 4 & 6 & 0 \end{array}$$

lo que implica que $(3216)_7 - (426)_7 = (2460)_7$.

2.1.4. Producto. Al igual que para la suma y la resta, calculemos en un ejemplo el producto usando los desarrollos como expresiones polinómicas y aplicando la ley distributiva. Veamos cuánto es $(121)_3 \times (2020)_3$:

$$\begin{aligned} (121)_3 \times (2020)_3 &= (1\cdot 3^2 + 2\cdot 3 + 1) \times (2\cdot 3^3 + 0\cdot 3^2 + 2\cdot 3 + 0) \\ &= 2\cdot 3^5 + 4\cdot 3^4 + 2\cdot 3^3 + 2\cdot 3^3 + 4\cdot 3^2 + 2\cdot 3 \\ &= 2\cdot 3^5 + 4\cdot 3^4 + 4\cdot 3^3 + 4\cdot 3^2 + 2\cdot 3. \end{aligned}$$

Para escribir el resultado en base 3, debemos reducir la expresión $2\cdot 3^5+4\cdot 3^4+4\cdot 3^3+4\cdot 3^2+2\cdot 3$ a un desarrollo 3-ádico. Para ello, procedemos como antes

$$\begin{aligned}2\cdot 3^5+4\cdot 3^4+4\cdot 3^3+4\cdot 3^2+2\cdot 3 &= 2\cdot 3^5+(3+1)\cdot 3^4+(3+1)\cdot 3^3+(3+1)\cdot 3^2+2\cdot 3\\ &= 2\cdot 3^5+3^5+1\cdot 3^4+3^4+1\cdot 3^3+3^3+1\cdot 3^2+2\cdot 3\\ &= 3\cdot 3^5+2\cdot 3^4+2\cdot 3^3+1\cdot 3^2+2\cdot 3\\ &= 1\cdot 3^6+0\cdot 3^5+2\cdot 3^4+2\cdot 3^3+1\cdot 3^2+2\cdot 3.\end{aligned}$$

Así, $(121)_3\times(2020)_3=(1022120)_3$ y claramente la multiplicación se realiza de forma muy similar a la que estamos acostumbrados, salvo que luego de multiplicar las cifras, debemos sumar usando congruencia módulo s, que en este caso es 3. Veamos el esquema:

$$\begin{array}{cccccccc}
 & & & & 2 & 0 & 2 & 0\\
 & & & \times & & 1 & 2 & 1\\
\hline
 & & & & {}^{+1}2 & 0 & 2 & 0\\
 & & & {}^{+1}4 & 0 & 4 & 0 & \\
 & & {}^{+1}2 & 0 & 2 & 0 & & \\
\hline
1 & 0 & 2 & 2 & 1 & 2 & 0 &
\end{array}$$

Calculemos otros ejemplos, $(234)_5\times(1001)_5$ y $(210)_6\times(341)_6$:

$$\begin{array}{cccccc}
 & 1 & 0 & 0 & 1 & \\
\times & & 2 & 3 & 4 & \\
\hline
 & 4 & 0 & 0 & 4 & \\
3 & 0 & 0 & 3 & & \\
2 & 0 & 0 & 2 & & \\
\hline
2 & 3 & 4 & 2 & 3 & 4
\end{array}
\qquad\qquad
\begin{array}{cccccc}
 & & 2 & 1 & 0 & \\
\times & & 3 & 4 & 1 & \\
\hline
 & & 2 & 1 & 0 & \\
 & {}^{+1}8 & 4 & 0 & & \\
{}^{+2}6 & 3 & 0 & & & \\
\hline
1 & 2 & 0 & 0 & 1 & 0
\end{array}$$

Luego, $(234)_5\times(1001)_5=(234234)_5$ y $(210)_6\times(341)_6=(120010)_6$.

Ejercicios.

1. Escribir 1024 en base 2, 3, 4 y 5.
2. Escribir en base 10 los siguientes números:
   a) $(11110)_3;(100002)_3$.
   b) $(170)_8;(21)_8$.
   c) $(1\,10)_{11};(1\,8\,5)_{11}$.
3. Calcular:
   a) $(1212)_3+(102)_3+(22)_3;(220)_3-(102)_3;(111)_3\times(21)_3;(12001)_3\times(12)_3$.
   b) $(150)_6+(21)_6+(234)_6-(123)_6;\ (234)_6-\times(123)_6$.
   c) $(1212)_3+(21)_6-(1101)_2;\ (231)_5\times(11)_3$.
4. Probar que mediante pesas de 1, 3, 9, 27, 81, ... unidades es posible pesar, y en forma **unívoca**, cualquier cuerpo cuyo peso sea un número entero de unidades, siempre que sea posible utilizar ambos platillos para colocar pesas.
5. Probar que los desarrollos s-ádicos pueden efectuarse para valores $s<0$.

   Ayuda: Desarrollar en base $-s$ y notar que si $0\le t<|s|$, entonces $-t=(|s|-t)+s$. Por ejemplo, en base -5 :

$$17=2+3\cdot 5=2+(-3)\cdot(-5)=2+2\cdot(-5)+1\cdot(-5)^2=(122)_{-5}.$$

6. *a*) Escribir en el sistema binario negativo (base -2) los siguientes números dados en el sistema decimal: $-10,\ -9, \ldots,\ -1,\ 1,\ 2, \ldots,\ 9,\ 10$.
   b) Dado $a = (323414)_5$, expresar a y $-a$ en base -5.

3. Anillo de números racionales s-ádicos

Hasta aquí hemos visto que todo número entero positivo admite un desarrollo s-ádico, $s \in \mathbb{N}$, y como tal posee una escritura en base s que denotamos como una sucesión de números a_i tales que $0 \leq a_i < s$. ¿Admiten los números enteros negativos una escritura similar? Veamos,

$$\begin{aligned} -1 &= (s-1) - s \\ &= (s-1) + [(s-1) - s] \cdot s = (s-1) + (s-1)s - s^2 \\ &= (s-1) + (s-1)s + [(s-1) - s] \cdot s = (s-1) + (s-1)s + (s-1)s^2 - s^3 \\ &= (s-1) + (s-1)s + (s-1)s^2 + [(s-1) - s] \cdot s^3 \\ &= (s-1) + (s-1)s + (s-1)s^2 + (s-1)s^3 - s^4 \end{aligned}$$

Si aceptamos escibir formalmente infinitos sumandos, siguiendo con el procedimiento anterior tendríamos que

$$-1 = (s-1) + (s-1)s + (s-1)s^2 + (s-1)s^3 + (s-1)s^4 + (s-1)s^5 + \cdots$$

Por lo tanto, podemos definir

$$-1 = (\ldots(s-1)(s-1)(s-1)(s-1))_s$$

como escritura s-ádica de -1. Análogamente, $-s = (\ldots(s-1)(s-1)(s-1)0)_s$.

Ejemplo 3.1. (*a*) Escribamos -2 en base 3. Sabemos que $-2 \equiv 1 \mod 3$ y que $-2 = 1 - 3$. Como $-3 = (\ldots, 2, 2, 2, 2, 0)_3$ tenemos que

$$-2 = (1)_3 + (\ldots, 2, 2, 2, 2, 0)_3 = (\ldots, 2, 2, 2, 2, 1)_3$$

(*b*) Escribamos ahora -12 en base 7. Sabemos que $-12 \equiv 2 \mod 7$ y que

$$\begin{aligned} -12 &= -(1 \cdot 7 + 5) = -5 - 7 = 2 - 7 - 7 \\ &= (2)_7 + (\ldots, 6, 6, 6, 6, 0)_7 + (\ldots, 6, 6, 6, 6, 0)_7 \\ &= (\ldots, 6, 6, 6, 6, 2)_7 + (\ldots, 6, 6, 6, 6, 0)_7 \end{aligned}$$

El cálculo de la suma en este caso lo podemos realizar al igual que en el caso de finitas cifras, salvo que ahora debemos determinar quiénes serán los coeficientes, que son infinitos

$$\begin{array}{cccccccc} & \ldots & {}^{+1}6 & {}^{+1}6 & {}^{+1}6 & 6 & 2 \\ + & \ldots & 6 & 6 & 6 & 6 & 0 \\ \hline & \ldots & 6 & 6 & 6 & 5 & 2 \end{array}$$

Es claro que salvo las dos primeras cifras, todas las demás cifras son 6. Así $-12 = (\ldots, 6, 6, 6, 5, 2)_7$. Observar que $12 = 1 \cdot 7 + 5$ y que $5 = 6 - 1,\ 2 = 7 - 5$.

La última observación hecha en el ejemplo anterior, vale en general.

Lema 3.2. *Si $(a_t a_{t-1} \ldots a_1 a_0)_s$ es el desarrollo en base s de un número entero positivo a, entonces el desarrollo de $-a$ está dado por*

$$(\ldots(s-1)(s-1)[(s-1) - a_t][(s-1) - a_{t-1}] \ldots [(s-1) - a_1](s - a_0))_s.$$

Demostración. Para demostrarlo basta ver que con esta definición vale que $a + (-a) = 0$. □

Ejemplo 3.3. (*a*) Escribamos -2873 en base 7. Como $2873 = (11243)_7$, por el lema anterior tenemos que

$$-2873 = (\ldots 6\,6\,6\,(6-1)\,(6-1)\,(6-2)\,(6-4)\,(7-3))_7 = (\ldots 6\,6\,6\,5\,5\,4\,2\,4)_7$$

(*b*) Notar que si $-m = (\ldots (s-1)\,(s-1)\,m_t\,\ldots m_0)_7$ entonces

$$-m \cdot 7^n = (\ldots (s-1)\,(s-1)\,m_t\,\ldots m_0\,\underbrace{0\ldots 0}_{n-veces})_7.$$

Como consecuencia de este lema tenemos que los números enteros negativos están representados por sucesiones infinitas tales que sólo un número finito de cifras es distinta de $s-1$ y éstas están al principio de la sucesión.

Consideremos ahora el conjunto de todas las sucesiones cuyos coeficientes cumple que son enteros no negativos menores que s:

$$\mathbb{Z}_s = \{(\ldots a_3a_2a_1a_0) |\ 0 \leq a_i < s\}.$$

A este conjunto se lo denomina el anillo de enteros s-ádicos. Luego, por construcción tenemos que

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Z}_s,$$

donde los números naturales están representados en $\mathbb{Z}_s$ como las sucesiones que tienen sólo finitas cifras no nulas. Más aún, las inclusiones son propias pues una sucesión que no se estabiliza en $(s-1)$ o en 0 no representa un número entero.

Como el mismo nombre lo dice, $\mathbb{Z}_s$ es un anillo conmutativo con las operaciones definidas como en la sección anterior. Sin embargo, resulta muy engorroso demostrarlo y lo dejamos como ejercicio para el lector interesado – ver [1, pág. 37]. En los ejercicios correspondientes a esta sección se podrán verificar algunos de los axiomas.

Recordemos que las unidades en un anillo son los elementos que tienen un inverso con respecto al producto. ¿Cuáles son las unidades en $\mathbb{Z}_s$? Sea $a = (\ldots a_2a_1a_0)$. Veamos qué condiciones debe cumplir a para tener inverso multiplicativo. Buscamos $b = (\ldots b_2b_1b_0)$ tal que $a \cdot b = b \cdot a = 1 = (\ldots 001)$. Entonces

			$\ldots$	b_3	b_2	b_1	b_0
$\times$			$\ldots$	a_3	a_2	a_1	a_0
			$\ldots$	b_0a_3	b_0a_2	b_0a_1	b_0a_0
		$\ldots$	b_1a_3	b_1a_2	b_1a_1	b_1a_0	
	$\ldots$	b_2a_3	b_2a_2	b_2a_1	b_2a_0		
	$\vdots$	$\vdots$	$\vdots$	$\vdots$			
				$\ldots$	$(b_0a_2 + b_1a_1 + b_2a_0)$	$(b_0a_1 + b_1a_0)$	b_0a_0

donde el resultado no está escrito en base s, pues primero debemos reducir la expresión. Por lo pronto, tenemos que para que se cumpla $a \cdot b = 1$, debemos tener que $b_0a_0 \equiv 1 \mod s$. Es decir, a_0 debe ser una unidad en $\mathbb{Z}/s\mathbb{Z}$ y esto sucede si y sólo si a_0 es coprimo con s, *i.e.* $(a_0, s) = 1$. Si a_0 cumple esta condición, entonces b_0 queda completamente determinado por el inverso multiplicativo de a_0.

Ahora bien, si $(a_0, s) = 1$ entonces existe $q_0 \in \mathbb{Z}$ tal que $b_0a_0 = q_0 \cdot s + 1$. Según el algoritmo de la suma que describimos en la subsección anterior, para realizar la suma en la segunda cifra debemos sumar q_0 a $b_0a_1 + b_1a_0$ y luego reducir módulo s. Como buscamos $a \cdot b = (\ldots 0001)$, debemos tener

$$b_0a_1 + b_1a_0 + q_0 \equiv 0 \mod s.$$

Por lo tanto, $b_1a_0 \equiv -b_0a_1 - q_0 \mod s$ y como a_0 es inversible en $\mathbb{Z}/s\mathbb{Z}$ con inversa b_0, multiplicando a ambos miembros por b_0 tenemos que

$$b_1 \equiv -b_0^2a_1 - b_0q_0 \mod s. \tag{3.1}$$

Puesto que $0 \leq b_1 < s$, la ecuación (3.1) determina b_1. Para hallar b_2 procedemos de la misma forma. Si $b_0a_1 + b_1a_0 + q_0 \equiv 0 \mod s$, entonces existe $q_1 \in \mathbb{Z}$ tal que $b_0a_1 + b_1a_0 + q_0 = q_1 \cdot s$. Usando nuevamente el algoritmo de la suma en la tercera cifra, debemos tener que

$$b_0a_2 + b_1a_1 + b_2a_0 + q_1 \equiv 0 \mod s.$$

Por lo tanto, $b_2a_0 \equiv -b_0a_2 - b_1a_1 - q_1 \mod s$ y multiplicando a ambos miembros por b_0 obtenemos

$$b_2 \equiv -b_0^2a_2 - b_0b_1a_1 - b_0q_1 \mod s. \tag{3.2}$$

Puesto que $0 \leq b_2 < s$, la ecuación (3.2) determina b_2. Siguiendo este método recursivamente podemos determinar de manera unívoca un elemento b que es el inverso multiplicativo de a, siempre y cuando a_0 sea coprimo con s. Por lo tanto, hemos probado lo siguiente:

Lema 3.4. $\mathcal{U}(\mathbb{Z}_s) = \{(\ldots a_3a_2a_1a_0) \in \mathbb{Z}_s |\ (a_0, s) = 1\}$.

Observación 3.5. Para todo s, los elementos no nulos en $\mathbb{Z}_s$ que comienzan con cifras nulas no tienen inversos. Más aún, si s es primo, éstos son los únicos elementos no nulos no inversibles.

Ejemplo 3.6. Veamos cómo funciona en un ejemplo fácil, calculemos el inverso de $(\ldots 0005)_6$. Por el párrafo anterior, debemos buscar primero el inverso de 5 en $\mathbb{Z}/6\mathbb{Z}$ que existe pues 5 es comprimo con 6. Como $5 \cdot 5 = 25 \equiv 1 \mod 6$, tenemos que $b_0 = 5$. Además, $25 = 6 \cdot 4 + 1$ lo que implica que $q_0 = 4$. Luego, siguiendo la ecuación (3.1) debemos buscar b_1 tal que

$$\begin{aligned} b_1 &\equiv -b_0^2a_1 - b_0q_0 \mod s \\ &\equiv -5^2 \cdot 0 - 5 \cdot 4 \mod 6 \\ &\equiv -20 \mod 6 \\ &\equiv -2 \mod 6 \\ &\equiv 4 \mod 6 \end{aligned}$$

Así, $b_1 = 4$. Además $b_0a_1 + b_1a_0 + q_0 = 5 \cdot 0 + 4 \cdot 5 + 4 = 24 = 4 \cdot 6 = q_1 \cdot s$, de donde se sigue que $q_1 = 4$. Por la ecuación (3.2) debemos buscar b_2 tal que $b_2 \equiv -b_0^2a_2 - b_0b_1a_1 - b_0q_1 \mod s$. Entonces

$$\begin{aligned} b_2 &\equiv -b_0^2a_2 - b_0b_1a_1 - b_0q_1 \mod s \\ &\equiv -5^2 \cdot 0 - 5 \cdot 0 \cdot 3 - 5 \cdot 4 \mod 6 \\ &\equiv -20 \mod 6 \\ &\equiv -2 \mod 6 \\ &\equiv 4 \mod 6 \end{aligned}$$

Luego, $b_2 = 4$. Además $b_0a_2 + b_1a_1 + b_2a_0 + q_1 = 5 \cdot 0 + 4 \cdot 0 + 4 \cdot 5 + 4 = 24 = 4 \cdot 6 = q_2 \cdot s$, de donde se sigue que $q_2 = 4$. Ahora debemos buscar b_3 tal que

$$b_0a_3 + b_1a_2 + b_2a_1 + b_3a_0 + q_2 \equiv 0 \mod s.$$

Entonces, operando en ambos miembros y multiplicando por b_0 tenemos que

$$b_3 \equiv -b_0^2a_3 - b_0b_1a_2 - b_0b_2a_1 - b_0q_2 \mod s,$$

lo que en nuestro caso da

$$\begin{aligned} b_3 &\equiv -5^2 \cdot 0 - 5 \cdot 4 \cdot 0 - 5 \cdot 4 \cdot 0 - 5 \cdot 4 \mod 6 \\ &\equiv -20 \mod 6 \\ &\equiv -2 \mod 6 \\ &\equiv 4 \mod 6 \end{aligned}$$

Luego, $b_3 = 4$. Claramente, de las cuentas se observa que $b_n = 4$ para todo $n \geq 2$, puesto que $a_j = 0$ para todo $j \geq 1$. En efecto, siempre tendremos que

$$\begin{aligned} b_n &\equiv -b_0^2a_n - b_0b_1a_{n-1} - \ldots - b_0b_{n-2}a_2 - b_0b_{n-1}a_1 - b_0q_n \mod 6, \\ &\equiv -b_0q_n \mod 6, \\ &\equiv -5 \cdot q_n \mod 6, \end{aligned}$$

donde q_n es tal que

$$b_0a_{n-1} + b_1a_{n-2} + \ldots + b_{n-2}a_1 + b_{n-1}a_0 + q_{n-1} = b_{n-1} \cdot 5 + q_{n-1} = q_n \cdot 6.$$

Usando inducción en $n \geq 2$ se ve que $b_n = 4$ y $q_n = 4$ para todo $n \geq 2$. En conclusión, $(5)_6^{-1} = (\ldots 44445)_6$.

Puesto que no todo elemento en $\mathbb{Z}_s$ tiene inverso, para construir un cuerpo que contenga a $\mathbb{Z}_s$ debemos introducir los inversos de los elementos no nulos. La extensión de los números enteros a los números racionales se ve reflejada en el desarrollo decimal con la introducción de decimales

$$\frac{1}{10} = 0,01; \qquad \frac{1}{3} = 0,3333\ldots$$

Así, como el inverso de $s \in \mathbb{Q}$ es $\frac{1}{s} = s^{-1}$, debemos antes que nada, introducir los inversos de las potencias de s. Para ello usaremos la misma notación de los decimales, pero sólo admitiendo finitas cifras después de la coma, así

$$(0,1)_s = 1 \cdot s^{-1}; \qquad (0,01)_s = 1 \cdot s^{-2}; \qquad (24,131)_5 = 2 \cdot 5^1 + 4 + 1 \cdot 5^{-1} + 3 \cdot 5^{-2} + 1 \cdot 5^{-3}$$

Observación 3.7. En $\mathbb{Q}$ la escritura en base 10 admite infinitas cifras a la derecha, luego de la coma. Aquí tomamos la convención opuesta, admitimos infinitas cifras a la izquierda y sólo finitas a la derecha, luego de la coma. La ventaja radica en el hecho que podemos seguir operando con las operaciones definidas en las secciones anteriores.

El conjunto

$$\mathbb{Q}_s = \{(\ldots a_2a_1a_0, a_{-1}a_{-2}\ldots a_{-t} |\ 0 \leq a_i < s,\ a_{-t} \neq 0\}$$

se denomina el *anillo de los números racionales s-ádicos*. Es claro que, para obtener $\mathbb{Q}_s$ basta agregarle a $\mathbb{Z}_s$ sucesiones con finitos decimales. Así,

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Z}_s \subset \mathbb{Q}_s.$$

Al igual que antes, este conjunto resulta ser un anillo conmutativo. La demostración es análoga a la demostración que $\mathbb{Z}_s$ es un anillo, por tal motivo la obviaremos.

Lema 3.8. *Todo entero s-ádico cuya primera cifra no nula es coprima con s tiene inverso en $\mathbb{Q}_s$. En particular, $\mathbb{Q}_s$ es un cuerpo si y sólo si s es primo.*

Demostración. Sea $a = (\dots a_{t+1}a_t \underbrace{0\dots0}_{t-veces})_s$ tal que $(a_t, s) = 1$. Entonces

$$s^{-t}a = (0, \underbrace{0\dots0}_{(t-1)-veces} 1)_s \cdot (\dots a_{t+1}a_t \underbrace{0\dots0}_{t-veces})_s = (\dots a_{t+2}a_{t+1}a_t)_s.$$

Denotemos $\bar{a} = (\dots a_{t+2}a_{t+1}a_t)_s$. Como $(a_t, s) = 1$, del Lema 3.4 se sigue que $\bar{a}$ tiene un inverso multiplicativo en $\mathbb{Z}_s$. Si $b = (\dots b_2b_1b_0)_s$ es tal inverso, entonces $1 = b\bar{a} = bs^{-t}a$, lo que implica que $bs^{-t} = (\dots b_{t+1}b_t, b_{t-1}\dots b_1b_0)_s$ es el inverso de a.

Sabemos que para todo $s \in \mathbb{N}$, $\mathbb{Q}_s$ es un anillo conmutativo. Si s es primo, entonces todo número entero a_i tal que $0 \leq a_i < s$ es coprimo con s. Por lo tanto, todo $a \in \mathbb{Q}_s$ no nulo es inversible, lo que implica que $\mathbb{Q}_s$ es un cuerpo. Recíprocamente, si $\mathbb{Q}_s$ es un cuerpo, entonces todo elemento no nulo tiene inverso multiplicativo, lo que implica que todo número entero a_i tal que $0 \leq a_i < s$ es coprimo con s, de donde se sigue que s es primo. □

Definición 3.9. Si p es un número primo, entonces $\mathbb{Q}_p$ se denomina el *cuerpo de los números p-ádicos.*

Observación 3.10. Por construcción sabemos que $\mathbb{Z} \subseteq \mathbb{Q}_p$ para todo p primo. Como $\mathbb{Q}_p$ es un cuerpo, se sigue que $\mathbb{Q} \subseteq \mathbb{Q}_p$ para todo p. En efecto, en general si $\Bbbk$ es un cuerpo que contiene a $\mathbb{Z}$, entonces $\Bbbk$ contiene una copia de $\mathbb{Q}$: sea $a \in \mathbb{Z}$ tal que $a \neq 0$. Como $\Bbbk$ es un cuerpo, existe $a^{-1} \in \Bbbk$ tal que $aa^{-1} = a^{-1}a = 1$. Así podemos definir un homomorfismo de cuerpos – ver ejercicio 6,

$$f : \mathbb{Q} \to \Bbbk, \qquad \frac{a}{b} \mapsto ab^{-1},$$

que resulta ser inyectivo, pues si $ab^{-1} = cd^{-1}$ en $\Bbbk$, entonces $ad = cb$ en $\Bbbk$ y por lo tanto en $\mathbb{Z}$. Pero esto implica que $a/b = c/d$ y consecuentemente f es inyectiva.

Para finalizar esta sección, mostraremos un algoritmo basado en el algoritmo de división de polinomios, que nos permite escribir a los números racionales en $\mathbb{Q}_p$.

Notar que hay racionales que ya podemos escribir en base p. Por ejemplo,

$$\frac{2}{27} = \frac{2}{3^3} = (2,001)_3, \qquad \frac{25}{49} = \frac{3\cdot 7 + 4}{7^2} = \frac{3}{7} + \frac{4}{7^2} = (0,3)_7 + (0,04)_7 = (0,34)_7$$

Dado que admitimos infinitas cifras a la izquierda, para realizar una división, pondremos al divisor a la izquierda y al dividivendo a la derecha, con el orden inverso. Por ejemplo, si queremos dividir $b = (\dots b_2b_1b_0)_p$ por $a = (\dots a_2a_1a_0)_p$ escribimos

$$\underline{\dots a_2a_1a_0}| \quad b_0b_1b_2\dots$$

Ahora bien, para escribir a/b en base p, procederemos a dividir a por b de acuerdo a este algoritmo, que explicaremos en un ejemplo.

Ejemplo 3.11. (a) Escribir $\frac{1}{2}$ en base 3.

Para resolverlo, escribimos primero ambos números en base 3: $1 = (\dots 0001)_3$, $2 = (\dots 0002)_3$ y luego

$$\begin{array}{rl} \underline{\dots 002}| & \underline{1}00\dots \end{array}$$

Para encontrar el cociente, debemos hallar un número a tal que $2 \times a \equiv 1 \mod 3$. Este número es 2. Como $2 \times 2 = 4 = (\dots 0011)_3$ tenemos

$$\begin{array}{rl} \underline{\dots 002}| & 100\dots \\ 2 & 110\dots \end{array}$$

El siguiente paso es realizar la resta $(\dots 001)_3 - (\dots 011)_3$. Como $(\dots 011)_3$ es mayor que $(\dots 001)_3$ debemos pedir prestado una "unidad" a la cifra de al lado, así

$$\begin{array}{rlllll} \underline{\dots 002}| & 1 & 0^{+3} & 2 & 2 & \dots \\ 2 & 1 & 1 & 0 & 0 & \dots \\ 0 & \underline{2} & & 2 & 2 & \dots \end{array}$$

Ahora, el siguiente número es claramente 1, pues siempre tomamos como referencia las primeras cifras del dividendo y del divisor

$$\begin{array}{rlllllll} \underline{\dots 002}| & 1 & 0^{+3} & 2 & 2 & 2 & 2 & \dots \\ 12 & 1 & 1 & 0 & 0 & \dots & & \\ 0 & 2 & & 2 & 2 & 2 & 2 & \dots \\ & 2 & & 0 & 0 & 0 & 0 & \dots \\ & 0 & & \underline{2} & 2 & 2 & 2 & \dots \end{array}$$

Siguiendo la división de esta manera, tenemos que el cociente es $(\dots 1112)_3$ y por lo tanto, ésta es la escritura de $\frac{1}{2}$ en base 3.

(b) Escribir $\frac{7}{11}$ en base 3. Al igual que antes, debemos escribir primero $7 = 3 \cdot 2 + 1 = (\dots 0021)_3$ y $11 = 3 \cdot 3 + 2 = (\dots 00102)_3$. Luego, la primera cifra del cociente es claramente 2, y como $(\dots 002)_3 \times (\dots 00102)_3 = (\dots 00211)_3$ tenemos que

$$\begin{array}{rllllll} \underline{\dots 00102}| & 1 & 2 & 0 & 0 & 0 & \dots \\ 2 & 1 & 1 & 2 & 0 & 0 & \dots \end{array}$$

Restando y procediendo de la misma manera tenemos

$$\begin{array}{rlllllllll} \underline{\dots 00102}| & \underline{1} & 2 & 0^{+3} & 2 & 2 & 2 & 2 & 2 & 2 & \dots \\ 1102202 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ & 0 & \underline{1} & 1 & 2 & 2 & 2 & 2 & 2 & 2 & \dots \\ & & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & \dots \\ & & 0 & \underline{0} & \underline{0} & \underline{2} & 2 & 2 & 2 & 2 & \dots \\ & & & & & 2 & 0 & 1 & 0 & 0 & \dots \\ & & & & & 0 & \underline{2} & 1 & 2 & 2 & \dots \\ & & & & & & 2 & 0 & 1 & 0 & \dots \\ & & & & & & 0 & \underline{1} & 1 & 2 & \dots \end{array}$$

Siguiendo de esta manera, se pueder ver que

$$\frac{7}{11} = (\dots 0\ 2\ 1\ 1\ 0\ 2\ 1\ 1\ 0\ 2\ 1\ 1\ 1\ 0\ 0\ 2\ 2)_3.$$

Notar que a partir de la cuarta cifra se repite el período 0211.

Observación 3.12. (a) Al igual que en el desarrollo decimal, en el que los números racionales se identifican con los números reales cuyos decimales poseen períodos, en $\mathbb{Q}_p$ los racionales son aquellos números que tienen períodos en sus desarrollos en base p – ver [1, Teo. II.2.2].

(b) Notar que este algoritmo sirve para hallar los desarrollos en base s para cualquier racional en $\mathbb{Q}_s$, sin importar que s sea primo, siempre y cuando la primera cifra del denominador sea coprima con s.

Ejercicios.

1. Considere el anillo de enteros s-ádicos $\mathbb{Z}_s$.
   a) Probar que $(\dots 000)_s$ es el neutro para la suma y que $(\dots 001)_s$ es el neutro para el producto.
   b) El inverso aditivo de un elemento $(\dots a_2a_1a_0)_s$ está dado por la sucesión
   $$(\dots[(s-1)-a_2][(s-1)-a_1](s-a_0))_s.$$
   Si $\alpha = (\dots a_2a_1a_0, a_{-1}a_{-2}\dots a_{-m})_p \in \mathbb{Q}_p$ ¿Cuál es su inverso aditivo?
2. Calcular $(11)_2^{-1}$, $(2)_3^{-1}$, $(3)_4^{-1}$.
3. Probar que $\alpha = (\dots a_2a_1a_0, a_{-1}a_{-2}\dots a_{-m})_p \in \mathbb{Q}_s$ tiene finitas cifras, *i.e.* $a_i = 0$ para todo i mayor o igual a un cierto $N \in \mathbb{N}$, si y sólo si $\alpha \in \mathbb{Q}$ es positivo y su denominador es una potencia de p.
4. Probar que $\alpha = (\dots a_2a_1a_0, a_{-1}a_{-2}\dots a_{-m})_p \in \mathbb{Q}_s$ tiene cifras que se repiten, *i.e.* $a_i = a_{i+r}$ para algún $r \in \mathbb{N}$ y para todo i mayor o igual a un cierto $N \in \mathbb{N}$, si y sólo si $\alpha \in \mathbb{Q}$.
5. Probar que $\operatorname{car}\mathbb{Q}_p = 0$.
6. Sean $\Bbbk$ y $\Bbbk'$ dos cuerpos. Un homomorfismo de cuerpos es una aplicación $f : \Bbbk \to \Bbbk'$ tal que
   (*i*) $f(1) = 1,\ f(0) = 0$,
   (*ii*) $f(a+b) = f(a) + f(b)$ para todo $a, b \in \Bbbk$,
   (*iii*) $f(ab) = f(a)f(b)$ para todo $a, b \in \Bbbk$.
   Probar que siempre se tiene que $f(a^{-1}) = f(a)^{-1}$ para todo $a \in \Bbbk$ no nulo.
7. Si $f : \mathbb{Q} \to \Bbbk$ es un morfismo de cuerpos, entonces $f(a) = a \cdot 1$ para todo $a \in \mathbb{Z}$.
8. Verificar que las divisiones en el ejemplo 3.11 están bien hechas, es decir, ver que $(\dots 1112)_3 \times (\dots 0002)_3 = 1$ y que $(\dots 2011\ 0211\ 1022)_3 \times (\dots 00102)_3 = (\dots 0021)_3$.
9. Escribir
   a) $\frac{1}{4}$, $\frac{1}{9}$ $\frac{5}{12}$ en base 3.
   b) $\frac{20}{3}$, $\frac{25}{11}$ $\frac{5}{12}$ en base 5.
   c) $\frac{1}{5}$ en base 6. Comparar con el ejemplo 3.6.
10. ¿Cuáles de los siguientes números 11-ádicos tiene raíces cuadradas en $\mathbb{Q}_{11}$?

(*i*) 5	(*ii*) 7	(*iii*) -7
(*iv*) $5 + 3\cdot 11 + 9\cdot 11^2 + 1\cdot 11^3$	(*v*) $3\cdot 11^{-2} + 6\cdot 11^{-1} + 3 + 7\cdot 11^2$	
(*vi*) $3\cdot 11^{-1} + 6 + 3\cdot 11 + 7\cdot 11^3$	(*vii*) $1\cdot 11^7$	
(*viii*) $7 - 6\cdot 11^2$	(*ix*) $5\cdot 11^{-2} + \sum_{n=0}^{\infty} n\cdot 11^n$.	

11. ¿Para qué $p = 2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19$ tiene -1 una raíz cuadrada en $\mathbb{Q}_p$?
12. Sea p un número primo impar y supongamos que $\alpha \in \mathbb{Z}_p$. Describir un método que decida cuándo α tiene una raíz cuadrada en $\mathbb{Q}_p$. Probar que existen cuatro números $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{Q}_p$ tales que para todo elemento no nulo $\alpha \in \mathbb{Q}_p$, exactamente uno de los números $\alpha\alpha_1, \alpha\alpha_2, \alpha\alpha_3, \alpha\alpha_4$ tiene una raíz cuadrada. En el caso que reemplazamos p por ∞ y $\mathbb{Q}_p$ por $\mathbb{R}$, existen dos números, por ejemplo ± 1.

4. Cuerpo de números p-ádicos

Con lo hecho hasta aquí, hemos encontrado infinitos cuerpos $\mathbb{Q}_p$, uno para cada número primo, que contienen a $\mathbb{Q}$. En esta sección definiremos más rigurosamente dichos cuerpos y probaremos que admiten una representación como la dada en el capítulo anterior.

4.1. Distancias y normas. En esta sección recordamos la definición de distancia, o métrica, y norma para aplicarla a la construcción de los números p-ádicos.

Definición 4.1. Sea X un conjunto no vacío. Una *métrica* o *distancia* sobre X es una función $d : X \times X \to \mathbb{R}_{\geq 0}$ tal que para todo $x, y \in X$ se cumple

($d1$) $d(x, y) = 0 \Leftrightarrow x = y$.
($d2$) $d(x, y) = d(y, x)$.
($d3$) $d(x, y) \leq d(x, z) + d(z, y)$ para todo $z \in X$ (desigualdad triangular).

A un par (X, d) con X un conjunto no vacío y d una métrica en X, se lo denomina *espacio métrico*. En lo que sigue, sólo consideraremos $X = \mathbb{Q}$ con diferentes métricas.

Ejemplo 4.2. $(\mathbb{Q}, |\cdot|)$ es un espacio métrico, donde $d(x, y) = |y - x|$ es el valor absoluto. Ésta es la distancia usual en $\mathbb{Q}$.

Ahora recordamos la definición de norma sobre un cuerpo.

Definición 4.3. Una *norma* $\|\cdot\|$ sobre un cuerpo $\Bbbk$ es una aplicación $\|\cdot\| : \Bbbk \to \mathbb{R}_{\geq 0}$ tal que para todo $x, y \in \Bbbk$ se tiene

($n1$) $\|x\| = 0 \Leftrightarrow x = 0$.
($n2$) $\|x \cdot y\| = \|x\|\|y\|$.
($n3$) $\|x + y\| \leq \|x\| + \|y\|$ (desigualdad triangular).

Ejemplo 4.4. Si tomamos $\Bbbk = \mathbb{Q}$, es fácil ver que el valor absoluto $|\cdot|$ es una norma en $\mathbb{Q}$.

Diremos que una distancia d está inducida por una norma $\|\cdot\|$ si

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

En lo que sigue, definiremos otras normas sobre $\mathbb{Q}$ que darán lugar a otras nociones de distancia. Éstas van a satisfacer las propiedades $(d1), (d2), (d3)$ pero van a diferir bastante de las nociones intuitivas de la distancia inducida por el valor absoluto. Todas estas normas cumplen una relación más fuerte que la propiedad $(n3)$, la desigualdad triangular. Este hecho nos lleva a la definición básica del análisis p-ádico.

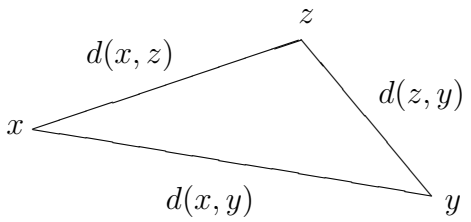
Definición 4.5. Una norma se dice *no arquimedeana* si para todo $x, y \in \Bbbk$ se tiene que

$$\|x + y\| \leq \max\,(\|x\|, \|y\|).$$

Una métrica en un conjunto X se dice no arquimedeana si $d(x, y) \leq \max\,(d(x, z), d(z, y))$ para todo $x, y, z \in X$. En particular, una métrica sobre un cuerpo $\Bbbk$ es no arquimedeana si está inducida por una norma no arquimedeana.

Decimos que una métrica es *trivial* si $\|0\| = 0$ y $\|x\| = 1$, para todo $x \neq 0$.

Observación 4.6. Nuestra intuición sobre distancia está basada en la métrica inducida por el valor absoluto. Por tal motivo, algunas propiedades de las métricas no arquimedeanas pueden parecer algo extrañas al principio. Por ejemplo, la propiedad $(d3)$ se conoce como la desigualdad triangular puesto que, en el caso del cuerpo de los números complejos con la distancia usual (ver ejercicio 3 de esta sección), dice que en el plano complejo, la suma entre dos lados de un triángulo es mayor que el tercer lado.



Veamos qué sucede con una norma no arquimedeana sobre un cuerpo. Por simplicidad, supongamos que $z = 0$. Entonces la desigualdad triangular para una norma no arquimedeana se lee como $\|x - y\| \leq \max(\|x\|, \|y\|)$. Supongamos primero que los lados x e y tienen distinta longitud, *i.e.* $\|x\| < \|y\|$. Luego, el tercer lado $x - y$ tiene longitud

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

Pero

$$\|y\| = \|x - (x - y)\| \leq \max\{\|x\|, \|x - y\|\}.$$

Como $\|y\| > \|x\|$, debe ser que $\|y\| \leq \|x - y\|$ y por lo tanto tenemos que $\|x - y\| = \|y\|$. En conclusión, si tenemos dos lados de un triángulo que no tienen la misma longitud, el más largo debe tener la misma longitud que el tercer lado. Por ende,

Todo triángulo en un espacio métrico con una métrica no arquimedeana es isósceles

Ejercicios.

1. Probar que el valor absoluto $|\cdot|$ es una norma no-arquimedeana sobre $\mathbb{Q}$ y la distancia usual sobre $\mathbb{Q}$ es la inducida por la norma.
2. Probar que la función $d : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}_{\geq 0}$ definida por
$$d(x, y) = \begin{cases} 0 & \text{si } x = y \\ 1 & \text{si } x \neq y \end{cases}$$
es una métrica en $\mathbb{Q}$. Esta métrica se denomina la métrica trivial.
3. Se define la siguiente aplicación sobre números complejos
$$\|\cdot\| : \mathbb{C} \times \mathbb{C} \to \mathbb{R}_{\geq 0}, \qquad \|z\| = \sqrt{x^2 + y^2}$$
donde $z = x + iy$ es la escritura de un número complejo como parte real más parte imaginaria. Probar que $\|\cdot\|$ es una norma en $\mathbb{C}$. Si restringimos esta norma a $\mathbb{Q}$, ¿Cuál es la norma inducida?
4. Probar que si $\|\cdot\|$ es cualquier norma sobre un cuerpo $\Bbbk$, entonces $\|-1\| = \|1\| = 1$. Probar que si $\|\cdot\|$ es no arquimedeana, entonces para todo entero n, $\|n\| \leq 1$ (aquí n es el resultado de sumar n-veces 1 en el cuerpo).

4.2. Orden p-ádico y métricas sobre $\mathbb{Q}$. En esta sección definiremos métricas sobre $\mathbb{Q}$, una para cada número primo. Como se verá más adelante – ver Teorema 4.14, toda métrica no trivial sobre $\mathbb{Q}$ es equivalente a una de éstas. Denotaremos por $\mathcal{P}$ al conjunto de los números primos. Comenzaremos por definir el orden p-ádico.

Sea $m \in \mathbb{Z}$ y $p \in \mathcal{P}$. Por $\nu_p(m)$ denotaremos la máxima potencia de p que divide a m, es decir, el mayor n tal que $m \equiv 0 \mod p^n$. Entonces, si $m \neq 0$,

$$0 \leq \nu_p(m), \qquad p^a | m \Rightarrow a \leq \nu_p(m), \qquad p^{\nu_p(m)} | m. \tag{4.1}$$

Además es claro que $p|m \Leftrightarrow \nu_p(m) > 0$.

Definición 4.7. $\nu_p(m)$ se denomina el orden p-ádico o el orden de m con respecto a p. Definimos también $\nu_p(0) = \infty$.

Ejemplo 4.8. $\nu_5(40) = 1$ y $\nu_2(40) = 3$, pues $40 = 5 \cdot 2^3$. Análogamente $\nu_2(81) = 0$, $\nu_3(81) = 4$ y $\nu_5(100) = 2$.

Observación 4.9. Del Teorema Fundamental de la Aritmética se sigue que $\forall\ m \in \mathbb{Z}$, $m = \varepsilon p_1^{\nu_{p_1}(m)} \cdot p_2^{\nu_{p_2}(m)} \cdots p_t^{\nu_{p_t}(m)}$, donde $\varepsilon = \pm 1$. En efecto, sabemos que todo número entero m se escribe de manera única como potencias de primos distintos $m = \varepsilon p_1^{n_1} \cdot p_2^{n_2} \cdots p_t^{n_t}$. Claramente, la mayor potencia de p_i que divide a m es n_i, para todo $1 \leq i \leq t$. Así, $n_i = \nu_{p_i}(m)$ para todo $1 \leq i \leq t$.

Como $\nu_p(m) = 0$ si $p \nmid m$, podemos escribir

$$m = \prod_{p \in \mathcal{P}} p^{\nu_p(m)}.$$

En el siguiente lema resumimos algunas propiedades del orden. En la lista de ejercicios al final de esta sección el lector puede encontrar algunas propiedades más.

Lema 4.10. *Para todo $m, n \in \mathbb{Z}$ se tiene*

(*i*) $\nu_p(m \cdot n) = \nu_p(m) + \nu_p(n)$,
(*ii*) $\nu_p(m + n) \geq \min\{\nu_p(m), \nu_p(n)\}$,
(*iii*) *Si* $\nu_p(m) \neq \nu_p(n)$, *entonces* $\nu_p(m + n) = \min\{\nu_p(m), \nu_p(n)\}$.

Demostración. (*i*) Por la Observación 4.9 podemos escribir $m = \prod_{p \in \mathcal{P}} p^{\nu_p(m)}$ y $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$. Así,

$$m \cdot n = \prod_{p \in \mathcal{P}} p^{\nu_p(m) + \nu_p(n)} = \prod_{p \in \mathcal{P}} p^{\nu_p(m \cdot n)},$$

lo que implica por el Teorema Fundamental de la Aritmética que $\nu_p(m \cdot n) = \nu_p(m) + \nu_p(n)$.

(*ii*) Sabemos que $p^{\nu_p(m)} | m$ y $p^{\nu_p(n)} | n$. Si $t_p = \min\{\nu_p(m), \nu_p(n)\}$, entonces $p^{t_p} | p^{\nu_p(m)}$, $p^{t_p} | p^{\nu_p(n)}$ y por ende $p^{t_p} | m$ y $p^{t_p} | n$. Consecuentemente $p^{t_p} | m + n$, de donde se sigue que $\nu_p(m + n) \geq \min\{\nu_p(m), \nu_p(n)\}$ por (4.1).

(*iii*) Supongamos que $\nu_p(m) \neq \nu_p(n)$ y que $t_p = \nu_p(n)$. Por (*ii*) sabemos que $\nu_p(m + n) \geq t_p$. Luego, debemos probar la otra desigualdad. Si $p^s | m + n$, con $\nu_p(n) \leq s \leq \nu_p(m)$, entonces $p^s | m$ y por lo tanto $p^s | n$. Esto sucede si y sólo si $s \leq \nu_p(n)$, lo que prueba que $s = \nu_p(n)$. □

Ahora extendemos el orden p-ádico para los números racionales. Para $x = a/b \in \mathbb{Q}$, $(a, b) = 1$, definimos

$$\nu_p(x) = \nu_p(a) - \nu_p(b).$$

Por ejemplo, $\nu_3(\frac{2}{9}) = -2$, $\nu_5(\frac{3}{7}) = 0$ y $\nu_7(\frac{14}{5}) = 1$.

Observación 4.11. Notar que esta definición del orden sobre $\mathbb{Q}$ no depende de la escritura de x, pues si $x = \frac{ac}{bc}$ entonces $\nu_p(\frac{ac}{bc}) = \nu_p(ac) - \nu_p(bc) = \nu_p(a) - \nu_p(b)$, por el Lema 4.10 (*i*).

Más aún, definimos ahora para todo $p \in \mathcal{P}$ la aplicación $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ dada por

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

Denotaremos de aquí en más $|\cdot|_\infty$ al valor absoluto usual. Cabe aclarar que ésta es sólo una convención que adoptamos y no implica una relación directa entre $|\cdot|_\infty$ y $|\cdot|_p$.

Proposición 4.12. *Para todo $p \in \mathcal{P}$, $|\cdot|_p$ es una norma no arquimedeana sobre $\mathbb{Q}$.*

Demostración. Para ver que $|\cdot|_p$ es una norma, debemos ver que se verifican las propiedades $(n1), (n2)$ y $(n3)$ de la Definición 4.3.

Sea $x \in \mathbb{Q}$. Claramente por definición $|x|_p \neq 0$ si y sólo si $x \neq 0$. Luego, $|\cdot|_p$ verifica $(n1)$. Sea $y \in \mathbb{Q}$. Si $x = 0$ o $y = 0$, entonces $|xy|_p = 0 = |x|_p|y|_p$. Si $x \neq 0 \neq y$, entonces por el Lema 4.10 (i) tenemos que

$$|xy|_p = p^{-\nu_p(xy)} = p^{-\nu_p(x)-\nu_p(y)} = p^{-\nu_p(x)} \cdot p^{-\nu_p(y)} = |x|_p|y|_p,$$

lo que implica que se cumple $(n2)$.

Probemos ahora $(n3)$. Si $x = 0$ o $y = 0$ o si $x+y = 0$, la propiedad $(n3)$ se verifica trivialmente. Por lo tanto, podemos suponer que $x, y, x + y$ son no nulos. Escribamos $x = a/b$, $y = c/d$ tales que $(a, b) = 1 = (c, d)$. Entonces $x + y = (ad + bc)/bd$ y $\nu_p(x + y) = \nu_p(ad + bc) - \nu_p(b) - \nu_p(d)$. Luego, del Lema 4.10 (ii) se sigue que

$$\begin{aligned} \nu_p(x+y) &\geq \min\{\nu_p(ad), \nu_p(bc)\} - \nu_p(b) - \nu_p(d) \\ &= \min\{\nu_p(a) + \nu_p(d), \nu_p(b) + \nu_p(c)\} - \nu_p(b) - \nu_p(d) \\ &= \min\{\nu_p(a) - \nu_p(b), \nu_p(c) - \nu_p(d)\} \\ &= \min\{\nu_p(x), \nu_p(y)\} \end{aligned}$$

Por lo tanto, $|x + y|_p = p^{-\nu_p(x+y)} \leq p^{-\min\{\nu_p(x),\nu_p(y)\}} = \max\{p^{-\nu_p(x)}, p^{-\nu_p(y)}\} = \max\{|x|_p, |y|_p\}$, y esto es menor o igual que $|x|_p + |y|_p$. En particular, hemos probado que la norma es no arquimedeana. □

4.2.1. Equivalencias de normas y el Teorema de Ostrowski.

Definición 4.13. Sea (X, d) un espacio métrico. Una sucesión $\{a_n\}_{n\in\mathbb{N}} = (a_1, a_2, a_3, \ldots)$ se dice una *sucesión de Cauchy* si para todo $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $d(a_n, a_m) < \varepsilon$ para todo $n, m \geq n_0$.

Diremos que dos métricas d_1, d_2 sobre un conjunto X son *equivalentes* si una sucesión $\{a_n\}_{n\in\mathbb{N}}$ es de Cauchy con d_1 si y sólo si $\{a_n\}_{n\in\mathbb{N}}$ es de Cauchy con d_2. Diremos que dos normas son equivalentes si las métricas que inducen son equivalentes.

En la definición de $|\cdot|_p$ podríamos haber escrito $\rho^{\nu_p(x)}$ con $\rho \in (0, 1)$ en lugar de $(1/p)^{\nu_p(x)}$. De haberlo hecho, hubiéramos obtenido una norma no arquimedeana equivalente – ver Ejercicios 7 y 8. La razón por la cual se toma $\rho = 1/p$ está relacionada con la fórmula dada por el Ejercicio 11.

Teorema 4.14. (Ostrowski) *Toda norma no trivial $\|\cdot\|$ sobre $\mathbb{Q}$ es equivalente a $|\cdot|_p$ para algún primo p o $p = \infty$.*

Demostración. Caso 1: Supongamos que existe un entero positivo n tal que $\|n\| > 1$. Sea n_0 el menor de tales n. Como $\|n_0\| > 1$, existe un número real positivo α tal que $\|n_0\| = n_0^\alpha$. Sea n cualquier número entero positivo y

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s, \text{ donde } 0 \leq a_i < n_0 \text{ y } a_s \neq 0,$$

su desarrollo n_0-ádico. Entonces

$$\begin{aligned} \|n\| &\leq \|a_0\| + \|a_1 n_0\| + \|a_2 n_0^2\| + \cdots + \|a_s n_0^s\| \\ &= \|a_0\| + \|a_1\| n_0^{\alpha} + \|a_2\| n_0^{2\alpha} + \cdots + \|a_s\| n_0^{s\alpha}. \end{aligned}$$

Como para todo $1 \leq i \leq s$ vale que $a_i < n_0$, por nuestra elección de n_0 tenemos que $\|a_i\| \leq 1$ y por lo tanto

$$\begin{aligned} \|n\| &\leq 1 + n_0^{\alpha} + n_0^{2\alpha} + \cdots + n_0^{s\alpha} \\ &= n_0^{s\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-s\alpha}) \\ &\leq n^{\alpha} \left(\sum_{i=0}^{\infty} (1/n_0^{\alpha})^i \right), \end{aligned}$$

pues $n \geq n_0^s$. La expresión entre pareréntesis es una serie convergente, y por lo tanto es una constante finita a la cual llamaremos C. Luego,

$$\|n\| \leq C n^s \qquad \text{para todo } n \in \mathbb{N}.$$

Ahora tomemos cualquier entero positivo n y cualquier entero positivo N suficientemente grande y reemplacemos n^N en lugar de n en la desigualdad anterior:

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

Tomando raíces N-ésimas obtenemos

$$\|n\| \leq C^{1/N} n^{\alpha}.$$

Haciendo tender $N \to \infty$ para un n fijo se sigue que $\|n\| \leq n^{\alpha}$.

Probemos ahora la desigualdad hacia el otro lado. Si escribimos n en base n_0 como antes, tenemos que $n_0^{s+1} > n \geq n_0^s$. Como $\|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leq \|n\| + \|n_0^{s+1} - n\|$ se sigue que

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

puesto que $\|n_0^{s+1}\| = n_0^{\alpha(s+1)}$ y por la primera parte de la prueba $\|n_0^{s+1} - n\| \leq (n_0^{s+1} - n)^{\alpha}$. Como $n \geq n_0^s$, tenemos que

$$\begin{aligned} \|n\| &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^{\alpha} \\ &= n_0^{(s+1)\alpha} \left[1 - \left(1 - \frac{1}{n_0} \right)^{\alpha} \right] \\ &\geq C' n^{\alpha}, \end{aligned}$$

para una cierta constante C' que puede depender de n_0 y de α pero no de n. Como antes, usamos la desigualdad anterior para n^N en lugar de n y tomamos raíces N-ésimas obteniendo $\|n\| \geq (C')^{1/n} n^{\alpha}$. Haciendo tender nuevamente $N \to \infty$ tenemos que $\|n\| \geq n^{\alpha}$.

En conclusión, hemos probado que $\|n\| = n^{\alpha}$ para todo $n \in \mathbb{N}$. De aquí se deduce que esta igualdad vale para cualquier $x \in \mathbb{Q}$. En efecto, si $x = a/b \in \mathbb{Q}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, y $a = \varepsilon |a|$, $\varepsilon = \pm 1$, entonces

$$\left\|\frac{a}{b}\right\| = \|a\|\left\|\frac{1}{b}\right\| = \|a\|\|b^{-1}\| = \|a\|\|b\|^{-1} = \|\varepsilon|a|\|\|b\|^{-1} = \|\varepsilon\||a|^{\alpha}b^{-\alpha} = |a|^{\alpha}b^{-\alpha},$$

pues la igualdad vale para para todo número natural. Luego, por el Ejercicio 10 tenemos que $\|\cdot\|$ es equivalente al valor absoluto $|\cdot|$ en $\mathbb{Q}$.

Caso 2: Supongamos que $\|n\| \leq 1$ para todos los enteros positivos n y sea n_0 el menor de tales n tal que $\|n_0\| < 1$. Dicho número existe pues estamos suponiendo que la norma es no trivial. Más aún, tal número debe ser primo, pues de lo contrario, $n_0 = n_1 n_2$, con $1 < n_1, n_2 < n_0$ y debe ser $\|n_1\| = \|n_2\| = 1$ por nuestra elección de n_0. Esto implicaría que $\|n_0\| = \|n_1 n_2\| = \|n_1\|\|n_2\| = 1$, lo cual contradice la elección de n_0. Denotemos $p = n_0$ a este número primo.

Sea q un número primo distinto de p. Entonces $\|q\| = 1$. En efecto, supongamos que existe $q \neq p$ tal que $\|q\| < 1$. Entonces existe $N \in \mathbb{N}$ tal que $\|q^N\| = \|q\|^N < 1/2$. Además, como $\|p\| < 1$, existe $M \in \mathbb{N}$ tal que $\|p^M\| = \|p\|^M < 1/2$. Como p^M y q^N son coprimos, existen números enteros n y m tales que $1 = mp^M + nq^N$. Pero entonces por $(n1)$ y $(n2)$ tenemos que

$$1 = \|1\| = \|mp^M + nq^N\| \leq \|mp^M\| + \|nq^N\| = \|m\|\|p^M\| + \|n\|\|q^N\| = \|m\|\|p\|^M + \|n\|\|q\|^N.$$

Pero por hipótesis tenemos que $\|m\|, \|n\| \leq 1$, lo que implica

$$1 = \|p\|^M + \|q\|^N < \frac{1}{2} + \frac{1}{2} = 1,$$

una contradicción. Por lo tanto, $\|q\| = 1$.

Consideremos ahora cualquier número entero positivo a. Por el Teorema Fundamental de la Aritmética, sabemos que a se factoriza como $a = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, donde $p_i \in \mathcal{P}$ son todos distintos. Así, por $(n2)$ tenemos que $\|a\| = \|p_1\|^{b_1}\|p_2\|^{b_2} \cdots \|p_r\|^{b_r}$. Pero este producto es igual a 1 a menos que exista $1 \leq i \leq r$ tal que $p_i = p$. La potencia correspondiente sería en este caso $b_i = \nu_p(a)$. Por lo tanto, si tomamos $\rho = \|p\| < 1$, tenemos que

$$\|a\| = \rho^{\nu_p(a)}.$$

Al igual que antes, la propiedad $(n2)$ de la definición de norma implica que esta igualdad vale para todo $x \in \mathbb{Q}$ en lugar de a. Finalmente, por el Ejercicio 8 tenemos que esta norma es equivalente a $|\cdot|_p$, lo que termina de probar el teorema. □

4.3. Completación de $\mathbb{Q}$. Como todos sabemos, hay una gran ventaja, tanto en álgebra como en análisis, en pasar del cuerpo de los racionales $\mathbb{Q}$ al cuerpo de los números reales $\mathbb{R}$. Uno de los grandes problemas al trabajar con $\mathbb{Q}$ es que no toda sucesión de Cauchy con el valor absoluto $|\cdot|$ es convergente en $\mathbb{Q}$, es decir, una sucesión de Cauchy puede no converger a un número racional. Estos agujeros en $\mathbb{Q}$ son llenados por el proceso de completación que da como resultado $\mathbb{R}$. Si consideramos a $\mathbb{Q}$ con la norma p-ádica, con p un número primo, resulta que $\mathbb{Q}$ tampoco es completo con esta norma. Su completación da lugar al cuerpo $\mathbb{Q}_p$ de números p-ádicos.

Uno de los métodos conocidos para *completar* espacios es el método de Cantor, el cual utilizaremos más adelante. Primero necesitamos algunas definiciones.

Definición 4.15. Sea $\Bbbk$ un cuerpo y $\|\cdot\|$ una norma en $\Bbbk$. Decimos que una sucesión $\{a_n\}_{n\in\mathbb{N}}$ es *convergente* a un elemento $a \in \Bbbk$ si para todo número real $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que $\|a_n - a\| < \varepsilon$ para todo $n \geq N$. En términos de la distancia d inducida por la norma esto se traduce en $d(a_n, a) \to 0$ cuando $n \to \infty$.

Ejemplo 4.16. Si $\Bbbk = \mathbb{Q}$ y $\|\cdot\| = |\cdot|$, entonces la sucesión dada por $a_n = 1/n$ converge a 0, pero la sucesión dada por $b_n = (1 + 1/n)^n$ es una sucesión de Cauchy que converge al número real e, que no es racional.

Definición 4.17. Un cuerpo $\Bbbk$ se dice *completo* con respecto a una norma $\|\cdot\|$ si toda sucesión de Cauchy en $\Bbbk$ es convergente con respecto a la norma $\|\cdot\|$.

Ejemplo 4.18. Como es sabido, o por el ejemplo anterior, $\mathbb{Q}$ no es completo con respecto al valor absoluto, mientras que $\mathbb{R}$ y $\mathbb{C}$ son completos con sus valores absolutos usuales.

Comenzaremos ahora a construir completaciones de $\mathbb{Q}$ con distintas normas. En general, dado un cuerpo $\Bbbk$ con una norma $\|\cdot\|$, se puede construir un cuerpo completo $\widehat{\Bbbk}$, llamado la completación de $\Bbbk$, que contiene un cuerpo $\widetilde{\Bbbk}$ isomorfo a $\Bbbk$ y tal que $\widetilde{\Bbbk}$ es denso en $\widehat{\Bbbk}$. Más aún, $\widehat{\Bbbk}$ es único salvo isomorfismo isométrico, es decir, si $\Bbbk'$ es otro cuerpo que es una completación de $\Bbbk$, no sólo resulta que los cuerpos son isomorfos, sino que también el isomorfismo preserva distancias. En ese caso, decimos que estos dos cuerpos son *congruentes*.

Sea $\Bbbk$ un cuerpo con una norma $\|\cdot\|$ y sean $\{a_n\}$ y $\{b_n\}$ dos sucesiones de Cauchy de $\Bbbk$ con respecto a $\|\cdot\|$. Se define la suma y el producto entre sucesiones de Cauchy por la suma y el producto término a término, esto es,

$$\{a_n\} + \{b_n\} = \{a_n + b_n\} \text{ y } \{a_n\} \cdot \{b_n\} = \{a_n b_n\}.$$

Veamos ahora que el conjunto de sucesiones de Cauchy es cerrado con respecto a estas operaciones. Claramente, $\{a_n + b_n\}_{n\in\mathbb{N}}$ es una sucesión de Cauchy pues $\{a_n\}_{n\in\mathbb{N}}$ y $\{b_n\}_{n\in\mathbb{N}}$ son de Cauchy y

$$\|a_n + b_n - (a_m + b_m)\| \leq \|a_n - a_m\| + \|b_n - b_m\|,$$

por la desigualdad triangular. Por otro lado, como toda sucesión de Cauchy es acotada, se deduce que la sucesión $\{a_n b_n\}_{n\in\mathbb{N}}$ también es de Cauchy. En efecto,

$$\begin{aligned}
\|a_n b_n - a_m b_m\| &= \|a_n b_n - a_n b_m + a_n b_m - a_m b_m\| \\
&= \|a_n(b_n - b_m) + b_m(a_n - a_m)\| \\
&\leq \|a_n\|\|b_n - b_m\| + \|b_m\|\|a_n - a_m\| \\
&\leq K\|b_n - b_m\| + K'\|a_n - a_m\|,
\end{aligned}$$

donde $\|a_n\| \leq K$ para todo $n \in \mathbb{N}$ y $\|b_n\| \leq K'$ para todo $n \in \mathbb{N}$. Esto implica que si dos sucesiones $\{a_n\}$ y $\{b_n\}$ son de Cauchy, entonces su producto también.

Además, si $\{a_n\}$ es una sucesión de Cauchy, entonces la sucesión $-\{a_n\} = \{-a_n\}$ definida por el inverso aditivo en cada coordenada, es una sucesión de Cauchy. De aquí se sigue que el conjunto A de sucesiones de Cauchy de $\Bbbk$ con respecto a estas dos operaciones es un anillo, cuya unidad está dada por la sucesión $\{u_n\}$, $u_n = 1$ para todo $n \in \mathbb{N}$, que al ser constante es claramente de Cauchy – ver Ejercicio 16.

Definición 4.19. Una sucesión $\{a_n\}$ se dice una *sucesión nula* con respecto a una norma $\|\cdot\|$ si para todo número real $\varepsilon > 0$, existe un número natural N tal que $\|a_n\| < \varepsilon$ para todo $n \geq N$. En otras palabras, una sucesión se llama nula con respecto a $\|\cdot\|$, si es convergente a 0 con respecto a $\|\cdot\|$.

Claramente, una sucesión nula con respecto a $\|\cdot\|$ es una sucesión de Cauchy en $\Bbbk$ con respecto a $\|\cdot\|$.

En lo que sigue, consideramos un cuerpo $\Bbbk$ con una norma $\|\cdot\|$. En general diremos que una sucesión es nula, sin referirnos a la norma, si es claro a qué norma nos referimos.

Sean $\{a_n\}$ y $\{b_n\}$ dos sucesiones nulas. Entonces, la sucesión dada por $\{a_n\}+\{b_n\}$ es también una sucesión nula, pues por la desigualdad triangular tenemos que

$$\|a_n + b_n\| \leq \|a_n\| + \|b_n\|.$$

Más aún, si $\{c_n\}$ es una sucesión de Cauchy y $\{a_n\}$ es una sucesión nula, entonces la sucesión $\{a_n c_n\}$ dada por el producto de ambas es una sucesión nula, ya que toda sucesión de Cauchy es acotada y

$$\|a_n c_n\| = \|a_n\|\|c_n\| \leq \|a_n\| K,$$

donde $c_n \leq K$ para todo $n \in \mathbb{N}$. Por lo tanto, hemos probado que el conjunto M de sucesiones nulas es un ideal del anillo A. Más aún, mostraremos en lo que sigue que este ideal es un ideal maximal de A y por ende, el cociente A/M es un cuerpo.

Notar primero que si una sucesión $\{a_n\}$ de Cauchy es no nula, entonces existe un número real $\varepsilon > 0$ y $N \in \mathbb{N}$ tal que

$$\|a_n\| \geq \varepsilon, \qquad \forall\ n > N.$$

Puesto que de lo contrario, para todo $\varepsilon > 0$ y $N \in \mathbb{N}$ existe $n > N$ tal que $\|a_n\| < \varepsilon$. Pero por ser $\{a_n\}$ de Cauchy tenemos que existe un entero N_0 tal que $\|a_n - a_m\| < \varepsilon$ para todo $n, m > N_0$, y consecuentemente

$$\|a_m\| \leq \|a_n\| + \|a_m - a_n\| < 2\varepsilon,$$

para todo $\varepsilon > 0$, siempre que $m > N_0$, lo cual implica que $\{a_n\}$ es una suesión nula, una contradicción.

Ahora bién, sea $\{a_n\}$ una sucesión de Cauchy no nula y sean ε y N como más arriba. Definimos entonces la sucesión $\{b_n\}$ por

$$b_n = \begin{cases} 0 & \text{para} \quad n \leq N \\ \frac{1}{a_n} & \text{para} \quad n > N. \end{cases} \tag{4.2}$$

Esta sucesión resulta ser una sucesión de Cauchy, pues si $n, m > N$ entonces

$$\|b_n - b_m\| = \left\| \frac{1}{a_n} - \frac{1}{a_m} \right\| = \left\| \frac{a_m - a_n}{a_n a_m} \right\| \leq \frac{\|a_m - a_n\|}{\varepsilon^2}.$$

Como $\{a_n\}$ es una sucesión de Cauchy, para todo número real $\varepsilon' > 0$, existe $N_0 \in \mathbb{N}$ tal que $\|a_m - a_n\| < \varepsilon'\varepsilon^2$, para todo $n, m \geq N_0$. Esto implica que

$$\|b_n - b_m\| \leq \frac{\|a_m - a_n\|}{\varepsilon^2} < \varepsilon',$$

para todo $n, m \geq N_0$ y consecuentemente $\{b_n\}$ es de Cauchy. Notar que con esta definición vale que

$$\{a_n\} \cdot \{b_n\} = (\underbrace{0, \ldots 0}_{N-veces}, 1, 1 \ldots) = (1, 1, \ldots) - (\underbrace{1, \ldots 1}_{N-veces}, 0, 0 \ldots). \tag{4.3}$$

Veamos ahora que el ideal M es maximal. Claramente M es no trivial, pues es no nulo y no contiene a la sucesión constantemente 1. Sea I un ideal de A que contiene propiamente a M.

Entonces, existe una sucesión $\{a_n\} \in I$ que es no nula, es decir $\{a_n\} \notin M$. Sea $\{b_n\}$ la sucesión de Cauchy correspondiente construida en (4.2). Como I es un ideal, tenemos que $\{a_n\}\{b_n\} \in I$, pero esto implica por (4.3) que $(1, 1, \ldots) - (\underbrace{1, \ldots 1}_{N-veces}, 0, 0 \ldots) \in I$. Como $(\underbrace{1, \ldots 1}_{N-veces}, 0, 0 \ldots)$ es una sucesión nula y $M \subseteq I$, se sigue que $(1, 1, \ldots) \in I$, lo que implica que $I = A$ y consecuentemente M es maximal.

Definimos entonces

$$\widehat{k} = A/M,$$

el cociente de A por el ideal maximal M. Por el ejercicio 11, $\widehat{k}$ es un cuerpo.

Sea ahora $a \in \Bbbk$, por $\{a\}$ denotamos la sucesión constante igual a a, que obviamente es de Cauchy. Con esto en mente definimos la aplicación

$$f : \Bbbk \to \widehat{\Bbbk} \tag{4.4}$$

dada por $f(a) = \{a\} + M$, para todo $a \in \Bbbk$. Esta aplicación resulta ser claramente un morfismo de cuerpos que es inyectivo, pues si $f(a) = 0$, esto implica que $0 = \{a\} + M$ y por lo tanto $\{a\} \in M$ es una sucesión nula, pero esto sucede si y sólo si $a = 0$. Así, si definimos

$$\widetilde{\Bbbk} = \{\{a\} + M |\ a \in \Bbbk\},$$

por lo probado anteriormente, resulta que $\Bbbk \simeq \widetilde{\Bbbk}$. Por lo tanto, identificamos a $\Bbbk$ con $\widetilde{\Bbbk}$.

Teorema 4.20. *Dado un cuerpo $\Bbbk$ con una norma $\|\cdot\|$, existe un cuerpo $\widehat{\Bbbk}$, único salvo congruencia, llamado la completación de $\Bbbk$, tal que $\widehat{\Bbbk}$ es completo con respecto a la norma inducida por la norma $\|\cdot\|$ y $\Bbbk$ es denso en $\widehat{\Bbbk}$.*

Demostración. La construcción del cuerpo $\widehat{k}$ fue dada anteriormente. Lo que resta probar es que la norma de $\Bbbk$ induce una norma en $\widehat{\Bbbk}$, el morfismo f en (4.4) respeta la norma, k es denso en $\widehat{\Bbbk}$ y $\widehat{\Bbbk}$ es completo con la norma inducida.

Sea $\{a_n\} + M \in \widehat{\Bbbk}$. Entonces, la sucesión de números reales dada por $\{\|a_n\|\}$ es una sucesión de Cauchy en $\mathbb{R}$, pues $\{a_n\}$ es una sucesión de Cauchy en $\Bbbk$ y de la desigualdad triangular se deduce que

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

Como $\mathbb{R}$ es completo con respecto a $|\cdot|$, la sucesión $\{\|a_n\|\}$ tiene límite en $\mathbb{R}$. Definimos entonces la norma en $\widehat{\Bbbk}$ como

$$\|\{a_n\} + M\| = \lim_{n\to\infty} \|a_n\|.$$

Esta norma está bien definida: sea $\{b_n\} \in A$ tal que $\{a_n\} + M = \{b_n\} + M$. Entonces $\{a_n - b_n\} = \{a_n\} - \{b_n\} \in M$. Usando nuevamente la desigualdad triangular, tenemos que

$$|\|a_n\| - \|b_n\|| \leq \|a_n - b_n\| \to 0,$$

esto es, $\lim_{n\to\infty} \|a_n\| = \lim_{n\to\infty} \|b_n\|$, y la norma resulta bien definida.

Demostremos ahora que el morfismo f en (4.4) respeta la norma, es decir, $\|f(a)\| = \|a\|$ para todo $a \in \Bbbk$. Pero $\|f(a)\| = \|\{a\} + M\| = \lim_{n\to\infty} \|a\| = \|a\|$. En particular, el morfismo f induce un isomorfismo isométrico entre $\Bbbk$ y su imagen por f.

Veamos ahora que $\Bbbk = \widetilde{\Bbbk}$ es denso en $\widehat{\Bbbk}$, esto es, para todo elemento $\{a_n\} + M \in \widehat{\Bbbk}$, y todo número real $\varepsilon > 0$, existe $b \in \Bbbk$ tal que $\|(\{a_n\} + M) - (\{b\} + M)\| < \varepsilon$. Sea $\varepsilon > 0$. Como $\{a_n\}$ es una sucesión de Cauchy en $\Bbbk$, existe $N \in \mathbb{N}$ tal que $\|a_n - a_m\| < \varepsilon$ para todo $n, m \geq N$. Tomemos entonces la sucesión constante dada por $\{a_m\}$, $m \geq N$ y su respectivo elemento $\{a_m\} + M$ en $\widetilde{\Bbbk} \subseteq \widehat{\Bbbk}$. Entonces

$$\|(\{a_n\} + M) - (\{a_m\} + M)\| = \lim_{n\to\infty} \|a_n - a_m\| \leq \varepsilon.$$

Finalmente probemos que $\widehat{\Bbbk}$ es completo con la norma inducida. Sea $\{\{a_n\} + M\}_{n\in\mathbb{N}}$ una sucesión de Cauchy en $\widetilde{\Bbbk}$, esto es, $\{a_n\}$ es una sucesión constante con valor a_n,

$$\{a_n\} + M = (a_n, a_n, a_n, \dots) + M.$$

Como $\|\{a_n\} + M\| = \|f(a_n)\| = \|a_n\|$, tenemos que la sucesión $(a_1, a_2, a_3, \dots)$ es una sucesión de Cauchy en $\Bbbk$. Por lo tanto, esta sucesión determina un elemento en $\widehat{\Bbbk}$, a saber $(a_1, a_2, a_3, \dots) + M$, que resulta ser el límite de la sucesión $\{\{a_n\} + M\}_{n\in\mathbb{N}}$ en $\widehat{k}$. En efecto,

$$\lim_{n\to\infty} \|[(a_1, a_2, a_3, \dots) + M] - [(a_n, a_n, a_n, \dots) + M]\| = \lim_{n\to\infty} \left(\lim_{m\to\infty} \|a_m - a_n\| \right) = 0$$

Sea $\{\alpha_n\}_{n\in\mathbb{N}} = \{(\{a_k\} + M)_n\}_{n\in\mathbb{N}}$ una sucesión de Cauchy arbitraria en $\widehat{\Bbbk}$, esto es, para cada $n \in \mathbb{N}$, el elemento $(\{a_k\} + M)_n$ consta de una sucesión de Cauchy $\{a_k\}$ de $\Bbbk$. Como $\widetilde{\Bbbk} = \Bbbk$ es denso en $\widehat{\Bbbk}$, existe una sucesión de elementos $\beta_1, \beta_2, \beta_3, \dots$ en $\widetilde{\Bbbk}$, con $\beta_k = (b_k, b_k, \cdots) + M$ y $b_k \in \Bbbk$ tales que

$$\|\alpha_n - \beta_n\| < \frac{1}{n}.$$

Como

$$\|\beta_n - \beta_m\| \leq \|\beta_n - \alpha_n\| + \|\alpha_n - \alpha_m\| + \|\alpha_m - \beta_m\|,$$

tenemos que $\{\beta_n\}_{n\in\mathbb{N}}$ es una sucesión de Cauchy en $\widetilde{\Bbbk}$. Por lo visto anteriormente, esta sucesión tiene un límite en $\widehat{\Bbbk}$ dado por $\beta = (b_1, b_2, b_3, \dots) + M$. Pero entonces

$$\|\alpha_n - \beta\| \leq \|\alpha_n - \beta_n\| + \|\beta_n - \beta\|,$$

lo que implica que $\lim_{n\to\infty} \alpha_n = \beta$ y consecuentemente $\widehat{\Bbbk}$ es completo. Con esto finaliza la prueba. □

Observación 4.21. Hablando de forma poco precisa, podríamos resumir el proceso de completación de la siguiente manera: a cada sucesión de Cauchy que no tiene un límite en $\Bbbk$ se le asocia un elemento *ideal* y a sucesiones de Cauchy equivalentes, le asociamos el mismo elemento ideal. Estos elementos, junto con los del cuerpo $\Bbbk$ forman la completación de $\Bbbk$.

Definición 4.22. La completación del cuerpo de los números racionales $\mathbb{Q}$ con respecto a la norma p-ádica se denomina el *cuerpo de los números p-ádicos* y se denota por $\mathbb{Q}_p$. Denotaremos también por $|\cdot|_p$ a la extensión de la norma de $\mathbb{Q}$ a $\mathbb{Q}_p$.

Definimos además

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p |\ |\alpha|_p \leq 1\}.$$

A un elemento de $\mathbb{Z}_p$ se lo llama *entero p-ádico*. Se puede ver fácilmente – Ejercicio 17 – que $\mathbb{Z}_p$ es un anillo con las operaciones definidas para $\mathbb{Q}_p$, esto es, $\mathbb{Z}_p$ es un subanillo de $\mathbb{Q}_p$.

Esta construcción abstracta nos da la oportunidad de comparar la construcción p-ádica con la construccón de los números reales y ver que el procedimiento es esencialmente el mismo. Sin embargo, el siguiente teorema nos ayuda a olvidarnos pronto de las sucesiones de Cauchy para pensar en términos más concretos, como en los capítulos anteriores de estas notas.

Teorema 4.23. *Toda clase de equivalencia $\alpha \in \mathbb{Z}_p$ tiene exactamente una sucesión de Cauchy $\{a_n\}$ que la representa que cumple que*

(*i*) $0 \leq a_n < p^n$ *para* $n \geq 1$,
(*ii*) $a_n \equiv a_{n+1} \mod p^n$ *para* $n \geq 1$.

Demostración. [4, Teo. I.2]. □

¿Qué se puede decir si un número p-ádico α no satisface que $|\alpha|_p \leq 1$? Sea $\alpha \in \mathbb{Q}_p$ y supongamos que $|\alpha|_p = p^m$, $m \geq 1$. Entonces el número p-ádico $\alpha' = p^m\alpha$ satisface que $|\alpha|_p \leq 1$. Por lo tanto, α' se puede representar por una sucesión de Cauchy $\{a'_n\}$ como en el teorema anterior y por ende α se puede representar por la sucesión de Cauchy dada por $\{a_n\}$ donde $a_n = p^m a'_n$ para todo $n \in \mathbb{N}$.

Ahora bien, conviene escribir todos los números enteros a'_n de la sucesión de Cauchy en desarrollo p-ádico:

$$a'_n = b_{n-1}p^{n-1} + \cdots + b_2p^2 + b_1p + b_0,$$

donde los $0 \leq b_i < p$, para todo $1 \leq i \leq n-1$, *i.e.* los b_i son los dígitos de a'_n en la base p. La condición (*ii*) del teorema dice exactamente que

$$a'_{n+1} = b_np^n + b_{n-1}p^{n-1} + \cdots + b_2p^2 + b_1p + b_0,$$

donde los dígitos b_i, $0 \leq i \leq n-1$ son los mismos que los dígitos de a'_n en la base p. Luego, podemos pensar a α como un número, escrito en base p que se extiende infinitamente hacia la izquierda, esto es, agregamos un nuevo dígito cada vez que pasamos de a'_n a a'_{n+1}.

Nuestro número p-ádico original α se puede pensar como un número escrito en base p que tiene *finitos decimales*, que se corresponden con las potencias negativas de p, pero que tiene infinitos términos hacia la izquierda.

$$\alpha = \cdots + b_{m+2}p^2 + b_{m+1}p + b_m + \frac{b_{m-1}}{p} + \cdots + \frac{b_1}{p^{m-1}} + \frac{b_0}{p^m}. \tag{4.5}$$

La expresión a la derecha de la igualdad es una manera distinta de escribir los términos de la sucesión $\{a_n\}$, donde $a_n = b_0p^{-m} + b_1p^{-m+1} + \cdots + b_{n-1}p^{n-1-m}$. En particular, ésta es una forma de pensar a todos los términos de la sucesión $\{a_n\}$ de una sola vez. En lo que sigue, veremos que la igualdad (4.5) es de hecho una igualdad real y concreta. Para ello, debemos estudiar la convergencia de series para $|\cdot|_p$, la norma p-ádica.

Sea $\{\alpha_n\}_{n\in\mathbb{N}}$ cualquier sucesión de números p-ádicos tal que $|\alpha_n|_p \to 0$ cuando $n \to \infty$ y consideremos

$$S_N = \alpha_1 + \alpha_2 + \cdots + \alpha_N,$$

la suma parcial. Entonces la sucesión dada por las sumas parciales $\{S_n\}_{n\in\mathbb{N}}$ es una sucesión de Cauchy en $\mathbb{Q}_p$. En efecto, dado un número real $\varepsilon > 0$, sabemos que existe $N_0 \in \mathbb{N}$ tal que $|\alpha_n|_p < \varepsilon$ si $n \geq N_0$. Pero si tomamos $N_0 \leq N < M$, entonces

$$|S_M - S_N|_p = |\alpha_M + \cdots \alpha_{N+1}|_p \leq \text{máx}\{|\alpha_M|_p, \cdots, |\alpha_{N+1}|_p\} < \varepsilon,$$

lo que implica que la sucesión es de Cauchy. Como $\mathbb{Q}_p$ es completo, existe un límite en $\mathbb{Q}_p$ que denotamos por $\sum_{n=1}^{\infty} \alpha_n$. Así, hemos probado que toda serie de números p-ádicos cuyos término general tienda a cero, es una serie convergente, es decir, la sucesión de sumas parciales es una sucesión convergente. Por lo tanto,

Una serie de números p-ádicos es convergente si y sólo si su término general tiende a cero.

En particular, comprobar la convergencia de una serie de números p-ádicos es mucho más fácil que comprobar la convergencia de una serie de números reales. Notar que aquí no tenemos nada similar a la serie armónica $a_n = 1/n$, que es una serie divergente en $\mathbb{R}$. La diferencia radica en el hecho que la norma p-ádica es no arquimedeana y el valor absoluto no.

Ahora bien, tomando una sucesión $\{b_n\}_{n=-m}^{\infty}$ de número p-ádicos tales que para todo $n \geq -m$ vale que $b_n \in \mathbb{Z}$, y $0 \leq b_n < p$, (i.e, b_n está representado por una sucesión de Cauchy de términos constantes iguales a $b_n \in \mathbb{Z}$ para todo $n \geq -m$), tenemos que la serie dada por el desarrollo p-ádico

$$\cdots + b_{m+2}p^2 + b_{m+1}p + b_m + \frac{b_{m-1}}{p} + \cdots + \frac{b_1}{p^{m-1}} + \frac{b_0}{p^m},$$

es una serie convergente en $\mathbb{Q}_p$ cuyo límite es por definición $\sum_{n=-m}^{\infty} b_n$. Recíprocamente, hemos visto que todo número p-ádico admite tal escritura. Luego, hemos probado el siguiente teorema:

Teorema 4.24. *Todo número p-ádico α se puede escribir de forma única*

$$\alpha = \sum_{-m}^{\infty} a_j p^j,$$

donde $a_j \in \mathbb{Z}, 0 \leq a_j < p$ y $p^m = \|\alpha\|_p$. A esta expresión se la denomina la expresión canónica o la expansión de α.

Demostración. Para otra demostración ver [1, II.2.1]. □

Observación 4.25. En la Sección 3, dado p un número primo hemos denominado al conjunto

$$\mathbb{Q}_p = \{(\ldots a_2 a_1 a_0, a_{-1} a_{-2} \ldots a_{-m} |\ 0 \leq a_i < p,\ a_{-m} \neq 0\}$$

el cuerpo de los números p-ádicos. Claramente, este conjunto coincide con el conjunto

$$\left\{ \sum_{i=-m}^{\infty} a_i p^i |\ m \in \mathbb{Z},\ 0 \leq a_i < p \right\},$$

de las series formales de Laurent en potencias de p cuyos coeficientes cumplen la condición $0 \leq a_i < p$, pues es simplemente escribir la serie en base p. El hecho que ambos conjuntos coinciden está dado por el teorema anterior. Así, dicho teorema nos permite representar concretamente los números p-ádicos y trabajar con ellos sin tener que pensar en clases de equivalencia de sucesiones de Cauchy.

Notar que la unicidad no se tiene en el caso de los números reales, pues en $\mathbb{R}$, las expresiones decimales $0,999999\ldots$ y 1 representan el mismo número real, mientras que si escribimos en base p a una expansión p-ádica, la forma de escribirla es única. Nuevamente, esto es una consecuencia directa del hecho que la norma es no arquimedeana.

4.3.1. Algunos resultados interesantes. Para finalizar damos algunos resultados importantes, sin su demostración, pero junto con sus referencias, para el lector interesado. Puesto que este curso es solamente introductorio, le recomendamos fuertemente a aquella persona que tenga cierto interés en el tema, que lea las referencias dadas y que busque algunas otras sobre este fascinante tema.

El primero de los resultados es un teorema que prueba la Observación 3.12 (a).

Teorema 4.26. *Un elemento $\alpha \in \mathbb{Q}_p$ es racional si y sólo si su expansión*

$$\alpha = \sum_{n}^{\infty} a_j p^j, \qquad 0 \leq a_j < p, \quad n = \nu_p(a),$$

es periódica.

Demostración. Ver [1, Teo. II.2.2]. □

El siguiente teorema muestra que todos los cuerpos que hemos construido anteriormente son no isomorfos entre sí. Para demostrarlo, hay que trabajar con ecuaciones sobre estos cuerpos, ya que la idea de la prueba radica en el hecho que la ecuación $x^2 - p$ tiene solución en $\mathbb{Q}_q$ y no en $\mathbb{Q}_p$, siendo p, q primos distintos.

Teorema 4.27. *Si p, q son dos primos distintos, entonces los cuerpos $\mathbb{Q}_p$ y $\mathbb{Q}_q$ son no isomorfos.*

Demostración. Ver [1, Teo. V.4.5]. □

Ejercicios.

1. Evaluar

(i)	$\nu_3(54)$	(ii)	$\nu_2(128)$	(iii)	$\nu_3(57)$
(iv)	$\nu_7(-700/197)$	(v)	$\nu_2(128/7)$	(vi)	$\nu_3(7/9)$
(vii)	$\nu_5(0{,}0625)$	$(viii)$	$\nu_3(10^9)$	(ix)	$\nu_3(-13{,}23)$
(x)	$\nu_7(-13{,}23)$	(xi)	$\nu_5(-13{,}23)$	(xii)	$\nu_{11}(-13{,}23)$
$(xiii)$	$\nu_{13}(-26/169)$	(xiv)	$\nu_{103}(-1/309)$	(xv)	$\nu_3(9!)$

2. Probar que $\nu_p((p^n)!) = 1 + p + p^2 + \cdots + p^{n-1}$.
3. Si $0 \leq a \leq p-1$, probar que $\nu_p((ap^n)!) = a(1 + p + p^2 + \cdots + p^{n-1})$.
4. Con la noción de orden, probar que se puede enunciar la siguiente condición de divisibilidad
$$m|n \Leftrightarrow \forall\ p \text{ primo}, \ \nu_p(m) \leq \nu_p(n).$$
5. Sean $m, n \in \mathbb{Z}$ y denotemos por (m, n) y $[m, n]$ al máximo común divisor y al mínimo común múltiplo de m y n. Probar que
$$(m, n) = \prod_{p \in \mathcal{P}} p^{t_p}, \qquad t_p = \text{mín}\{\nu_p(m), \nu_p(n)\},$$
$$[m, n] = \prod_{p \in \mathcal{P}} p^{r_p}, \qquad r_p = \text{máx}\{\nu_p(m), \nu_p(n)\}.$$
6. Probar que dos normas $\|\cdot\|_1$ y $\|\cdot\|_2$ sobre un cuerpo $\Bbbk$ son equivalentes si para algún $0 \neq a \in \Bbbk$, $\|a\|_1 < 1$ si y sólo si $\|a\|_2 < 1$.
7. Sean $\|\cdot\|_1$ y $\|\cdot\|_2$ dos normas sobre un cuerpo $\Bbbk$. Probar que $\|\cdot\|_1$ es equivalente a $\|\cdot\|_2$ si y sólo si existe un número real positivo α tal que $\|x\|_1 = \|x\|_2^{\alpha}$ para todo $x \in \Bbbk$.

8. Probar que, si $0 < \rho < 1$, entonces la función sobre $\mathbb{Q}$ definida por
$$|x|_{\rho,p} = \begin{cases} \rho^{\nu_p(x)} & \text{si } x \neq 0, \\ 0 & \text{si } x = 0. \end{cases}$$
es una norma no arquimedeana. Probar usando el ejercicio anterior que esta norma es equivalente a $|\cdot|_p$. ¿Qué sucede si $\rho = 1$? ¿y si $\rho > 1$?
9. Probar que $\|\cdot\|_{p_1}$ no es equivalente a $\|\cdot\|_{p_2}$ si p_1 y p_2 son primos distintos.
10. Para $x \in \mathbb{Q}$ se define $\|x\| = |x|^\alpha$ para un número real positivo fijo α, donde $|\cdot|$ es el valor absoluto usual. Probar que $\|\cdot\|$ es una norma si y sólo si $\alpha \leq 1$ y en tal caso, $\|\cdot\|$ es equivalente a $|\cdot|$.
11. Sea x un número racional no nulo. Probar que el producto sobre todos los primos, *incluyendo* ∞ de todas las normas $|x|_p$ es 1. En símbolos,
$$\prod_{p \in \mathcal{P} \cup \infty} |x|_p = 1.$$
Notar que el producto está bien definido pues sólo un número finito de factores es distinto de 1.
12. Evaluar la distancia p-ádica $\|a - b\|_p$ entre dos números a, b donde

(i)	$a = 1, b = 26, p = 5$	(ii)	$a = 1, b = 26, p = \infty$
(iii)	$a = 1, b = 26, p = 3$	(iv)	$a = 1, b = 244, p = 3$
(v)	$a = 1/9, b = -1/16, p = 5$	(vi)	$a = 1, b = 244, p = 5$
(vii)	$a = 1, b = 243, p = 3$	$(viii)$	$a = 1, b = 183, p = 13$
(ix)	$a = 1, b = 183, p =$	(x)	$a = 1, b = 183, p = 2$
(xi)	$a = 1, b = 183, p = \infty$	(xii)	$a = 9!, b = 0, p = 3$
$(xiii)$	$a = (9!)^2/3^9, b = 0, p = 3$	(xiv)	$a = 2^{2^N}/2^N, b = 0, p = 2$

13. Probar que para cualquier $p \neq \infty$, cualquier sucesión de número enteros tiene una subsucesión de Cauchy con respecto a $|\cdot|_p$.
14. Probar que si $x \in \mathbb{Q}$ y $|x|_p \leq 1$ para todo $p \in \mathcal{P}$, entonces $x \in \mathbb{Z}$.
15. Sea $\Bbbk$ un cuerpo y $\|\cdot\|$ una norma en $\Bbbk$. Probar que toda sucesión de Cauchy en $\Bbbk$ con respecto a $\|\cdot\|$ es acotada.
16. Sea $\Bbbk$ un cuerpo y $\|\cdot\|$ una norma en $\Bbbk$. Probar que el conjunto A de las sucesiones de Cauchy en $\Bbbk$ con respecto a $\|\cdot\|$ es un anillo con las operaciones definidas en la Subsección 4.3.
17. Probar que $\mathbb{Z}_p$ es un subanillo de $\mathbb{Q}_p$.

Referencias

[1] G. Bachman, *Introduction to p-adic numbers and valuation theory*, Academic Press, New York-London, ix+173 pp (1964).

[2] A. I. Borevich y I. R. Shafarevich, *Number theory*, Pure and Applied Mathematics, Vol. **20**, Academic Press, New York-London, x+435 pp (1966).

[3] E. Gentile, *Notas de Álgebra I*, Eudeba (1988).

[4] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Second edition, Graduate Texts in Mathematics, **58**, Springer-Verlag, New York, xii+150 pp (1984).

[5] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, No. **7**, Springer-Verlag, New York-Heidelberg, viii+115 pp (1973).

FaMAF-CIEM (CONICET), Universidad Nacional de Córdoba, Medina Allende s/n, Ciudad Universitaria, 5000 Córdoba

E-mail address: ggarcia@mate.uncor.edu