Introducción a los números p-ádicos

Benjamín Macías Quezada

27 de mayo de 2022

Resumen

Esta es una versión escrita de una charla para el Seminario de Teoría de Números de la PUC. Revisaremos la construcción de los números p-ádicos, un cuerpo resultante de completar $\mathbb{Q}$ respecto a una métrica distinta a la usual, demostraremos el Teorema de Ostrowski que clasifica los valores absolutos en $\mathbb{Q}$, y revisaremos un par de ejemplos que evidencian el contraste de estos cuerpos con su contraparte arquimediana. Basado en [Gou20, Chs. 1–3]

1. Valores absolutos

Veremos la construcción clásica de los números p-ádicos. Estos vienen de completar $\mathbb{Q}$ respecto a un valor absoluto distinto al usual. La primera idea clave es abstraer la noción de valor absoluto. Un *valor absoluto* en un cuerpo k es una función $|\cdot|\colon k \to \mathbb{R}_{\geq 0}$ que para todos $x, y \in k$ cumple que:

1. $|x| = 0$ si y solo si $x = 0$.
2. $|xy| = |x||y|$.
3. $|x + y| \leq |x| + |y|$.

Además decimos que el valor absoluto es *no-arquimediano* de cumplir la *desigualdad triangular fuerte*,

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

Notemos que la desigualdad triangular fuerte implica la usual: tanto $|x|$ como $|y|$ son no-negativos, por lo que $\text{máx}\{|x|, |y|\} \leq |x| + |y|$. Los ejemplos más cercanos son los siguientes:

1. En $\mathbb{Q}$ (y en cualquier cuerpo) se puede definir un *valor absoluto trivial* dado por

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

2. El valor absoluto usual en $\mathbb{Q}$.

Una pregunta natural es si es que existen más valores absolutos en $\mathbb{Q}$. La respuesta es positiva, y ahora procedemos a construir una familia de estos. La idea es que, fijado un primo p, los números "pequeños" son aquellos divisibles por potencias altas de p.

En efecto, fijemos p un número primo. La *valuación p-ádica* en $\mathbb{Z}$ es la función ν_p que asigna a cada $n \in \mathbb{Z} - \{0\}$ la mayor potencia de p que aparece en la descomposición en factores primos de n. Esta función se extiende a $\mathbb{Q} - \{0\}$ notando que todo $x \in \mathbb{Q} - \{0\}$ se puede escribir como $x = p^{\nu_p(x)} x_0$, donde $x_0 \in \mathbb{Q}$ es coprimo con p. Finalmente, es conveniente definir $\nu_p(0) := \infty$. Con esto, definimos la función $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}$ como

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

y se tendrá que:

Proposición 1.1. *Para cada p número primo, $|\cdot|_p$ es un valor absoluto no-arquimediano en $\mathbb{Q}$.*

Demostración. Probemos la desigualdad triangular fuerte. Sean $x, y \in \mathbb{Q}$. En primer lugar, supongamos que $\nu_p(x) \neq \nu_p(y)$, y en particular, que $\nu_p(x) < \nu_p(y)$—de modo que $\max\left\{|x|_p, |y|_p\right\} = |x|_p$. Se sigue que

$$\begin{aligned} x + y &= p^{\nu_p(x)} x_1 + p^{\nu_p(y)} y_1 \\ &= p^{\nu_p(x)} (x_1 + p^{\nu_p(y)-\nu_p(x)} y_1), \end{aligned}$$

y por tanto, se tendrá $|x+y|_p \leq |x|_p$. En el caso de que $\nu_p(x) = \nu_p(y)$, el resultado es directo. $\square$

El valor absoluto descrito en la Proposición se llamará el *valor absoluto p-ádico*. Notar que todo número natural tiene valor absoluto p-ádico menor o igual a 1.

Después estudiaremos propiedades de estos valores absolutos. De momento, nos preguntamos nuevamente si existen aún más valores absolutos en $\mathbb{Q}$. Ahora la respuesta es negativa: conocemos todos los valores absolutos en $\mathbb{Q}$, módulo ser *equivalentes*, en el sentido que inducen métricas equivalentes (recordar que dos métricas d_1, d_2 son *equivalentes* si cada secuencia Cauchy respecto a d_1 también lo es respecto a d_2, y viceversa). El siguiente resultado de Alexander Ostrowski hace explícita la clasificación:

Teorema 1.2. ([Ost16]) *Todo valor absoluto no-trivial en $\mathbb{Q}$ es equivalente o al valor absoluto usual, o a un valor absoluto p-ádico.*

Demostración. Utilizaremos libremente los dos resultados siguientes:

1. $|\cdot|_1$ es equivalente a $|\cdot|_2$ si y solo si existe $\alpha > 0$ tal que $|x|_1 \leq |x|_2^\alpha$ para todo $x \in k$.
2. Dada una constante $c \in (0,1)$, el valor absoluto

$$|x| := \begin{cases} c^{\nu_p(x)} & x \neq 0 \\ 0 & x = 0, \end{cases}$$

   es equivalente a $|\cdot|_p$.

Prosigamos a la demostración del teorema. La idea es notar que la imagen de $\mathbb{N}$ bajo un valor absoluto tiene dos posibilidades disjuntas: o existen elementos que tienen valor absoluto mayor a 1 (como es el caso del valor absoluto usual), o todos tienen valor absoluto menor o igual a 1 (como en el caso de los valores absolutos p-ádicos). La demostración consiste en probar que no hay más (clases de) valores absolutos aparte del usual o alguno p-ádico.

1. Si existe algún natural con valor absoluto mayor a 1, verifiquemos que el valor absoluto resulta equivalente al usual. Para ello, tomemos n_0 el menor de tales números, y escribamos $|n_0| = n_0^\alpha$ para algún $\alpha > 0$. Escribimos un $n \in \mathbb{N}$ en base n_0 (es decir, $a_i < n_0$) como $n = \sum_{i=0}^s \left|a_i n_0^i\right|$, y acotamos:

$$\begin{aligned} |n| \leq \sum_{i=0}^s \left|a_i n_0^i\right| &\leq \sum_{i=0}^s |a_i| n_0^{\alpha i} \\ &\leq \sum_{i=0}^s n_0^{\alpha i} && \text{pues } |a_i| \leq |n_0 - 1| < 1 \\ &= n_0^{\alpha s} \sum_{i=0}^s \left(\frac{1}{n_0^\alpha}\right)^i \\ &= n_0^\alpha \underbrace{n_0^{\alpha(s-1)} \frac{n_0^\alpha}{n_0^\alpha - 1}}_{=:C} && \text{suma geométrica} \\ &\leq C n^\alpha, \end{aligned}$$

de lo que $\left|n^N\right| \leq C n^{N\alpha}$, y por tanto $|n| \leq \sqrt[N]{C} n^\alpha$. Tomando $N \to \infty$, concluimos que $|n| \leq n^\alpha = |n|_\infty^\alpha$. Para la otra desigualdad, acotamos nuevamente:

$$\begin{aligned} \left|n_0^{s+1}\right| &= \left|n + n_0^{s+1} - n\right| \\ &\leq |n| + \left|n_0^{s+1} - n\right| \end{aligned}$$

$$\begin{aligned} \implies |n| &\geq \left|n_0^{s+1}\right| - \left|n_0^{s+1} - n\right| \\ &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^\alpha \\ &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^\alpha \\ &\geq n_0^{(s+1)\alpha}\left(1 - (1 - \frac{1}{n_0})^\alpha\right) \end{aligned}$$

Sea $C_1 := \left(1 - (1 - \frac{1}{n_0})^\alpha\right)$, y el tomar $C_1 < D < C_1 \frac{C_1 n_0^{(s+1)\alpha}}{n^\alpha}$ nos da la cota $Dn^\alpha \leq |n|$. Argumentando análogo a lo anterior, obtenemos que $n^\alpha \leq n$. Por tanto, en este caso $|\cdot| = |\cdot|_\infty$.

2. Si para todo natural tiene valor absoluto menor o igual a 1, consideremos n_0 el menor natural de valor absoluto menor a 1. En primer lugar, n_0 debe ser un número primo, porque si no $|n_0| = |a||b| \leq 1$, lo que contradice la minimalidad de n_0. Llamémoslo p. Sea q otro número primo. Si $|q| < 1$, se tendrá que existen M, N tales que $\left|q^N\right|, \left|p^M\right| < \frac{1}{2}$. Como son coprimos, hay una combinación $\mathbb{Z}$-lineal tal que $ap^M + bq^N = 1$. Se sigue que

$$\begin{aligned} 1 &= \left|ap^M + bq^N\right| \\ &\leq |a|\left|p^M\right| + |b||q^n| \\ &\leq 1/2 + 1/2 \\ &= 1, \end{aligned}$$

lo que es contradictorio. Por tanto, debe ser que $|q| = 1$. Sea $C := |p|$, de lo que $|n| = C^{\nu_p(n)}$. □

2. Construcción

Veamos algunas propiedades de $(\mathbb{Q}, |\cdot|_p)$. La primera desafía nuestra intuición, pues este tipo de sucesiones divergen con la métrica usual, pero esto no ocurre con las métrica p-ádicas:

Lema 2.1. *En $(\mathbb{Q}, |\cdot|_p)$, la sucesión $(p^n)_{n\in\mathbb{N}}$ converge a 0.*

Demostración. Para $n \in \mathbb{N}$, se tiene que $|p^n|_p = p^{-n} = \frac{1}{p^n}$. Tomando $n \to \infty$, el resultado es claro. □

Otro resultado no-intuitivo: usualmente, las cuyos términos sucesivos se van acercando son Cauchy, pero al converso no es necesariamente cierto. Con las métricas no-arquimedianas esto *siempre* es cierto.

Lema 2.2. *En un espacio ultramétrico $(k, |\cdot|)$, una sucesión $(x_n)_{x\in\mathbb{N}}$ es Cauchy si y solo si $|x_n - x_{n+1}| \to 0$.*

Demostración. Dados $m, n \in \mathbb{N}$, escribimos $m = n + r$, de lo que

$$\begin{aligned} |x_m - x_n| &= |x_{n+r} - x_{n+r-1} + \cdots + x_{n+1} - x_n| \\ &\leq \max\{|x_{n+1} - x_{n+r-1}|, \ldots, |x_{n+1} - x_n|\}. \end{aligned}$$

Concluimos haciendo $n \to \infty$. □

Al estudiar la construcción de $\mathbb{R}$ desde $\mathbb{Q}$ el problema que se intenta arreglar es que $\mathbb{Q}$ no es completo respecto a la métrica usual, y por eso tomamos su compleción. Nos podemos hacer la misma pregunta respecto a métricas no-arquimedianas, y la respuesta es la misma:

Lema 2.3. $(\mathbb{Q}, |\cdot|_p)$ *no es un espacio métrico completo.*

Demostración. Trataremos el caso $p \neq 2$. Sea $a \in \mathbb{Z}$ un residuo cuadrático módulo p coprimo a p, que no sea un cuadrado de $\mathbb{Q}$. Sea x_0 alguna solución de $x^2 \equiv a \pmod{p}$, y para $n > 0$, sea x_n de modo que $x_n \equiv x_{n-1} \pmod{p^n}$ y $x_n^2 \equiv a \pmod{p^{n+1}}$. Se tiene que $|x_{n+1} - x_n| = \left|\lambda p^{n+1}\right| \leq p^{-(n+1)}$, tomando $n \to \infty$ tenemos que $(x_n)_{n\in\mathbb{N}}$ es Cauchy. Sin embargo, no converge en $\mathbb{Q}$, pues

$$\left|x_n^2 - a\right| = \left|\mu p^{n+1}\right| \leq p^{-(n+1)},$$

que de converger, nos indica que lo hace a un cuadrado de $\mathbb{Q}$, pero a no lo es. □

De acá, podemos seguir el procedimiento estándar para completar $\mathbb{Q}$ respecto a una métrica p-ádica:

1. Sea k un cuerpo con valor absoluto $|\cdot|$ que induce una métrica d. El conjunto R de todas las secuencias Cauchy es un anillo conmutativo con unidad respecto a las operaciones obvias.

2. Queremos identificar dos sucesiones como equivalentes si convergen al mismo límite. Esto es equivalente a cocientar por el ideal $\mathfrak{m}$ consistente de las secuencias Cauchy que convergen a 0.

3. El ideal $\mathfrak{m}$ resulta ser maximal, por lo que $R/\mathfrak{m}$ es un cuerpo, llamado la *compleción de k respecto a d*. El valor absoluto se extiende al cociente, el cual induce una estructura de espacio métrico completo.

La completación de $\mathbb{Q}$ respecto a $|\cdot|_p$ se llama el cuerpo de los *números p-ádicos*, y se denota $\mathbb{Q}_p$.

3. Algunas propiedades

En $\mathbb{R}$, es sabido que si una serie converge entonces su cola se va a 0. En $\mathbb{Q}_p$ la afirmación recíproca también es cierta:

Ejemplo 3.1. Una serie $\sum_{n=1}^{\infty} c_n$, con $c_n \in \mathbb{Q}_p$ converge si y solo si $|c_n| \to 0$. En efecto, dado $S_j := \sum_{n=1}^{j} c_n$, se tiene que

$$\begin{aligned}|S_m - S_n|_p &= |c_{n+1} + \ldots + c_m|_p \\ &\leq \text{máx}\left\{|c_{n+1}|, \ldots, |c_m|_p\right\} \to 0.\end{aligned}$$

En $\mathbb{R}$, la serie de $n!$ diverge. En $\mathbb{Q}_p$ de hecho converge:

Ejemplo 3.2. $\sum_{n=1}^{\infty} n!$ converge en $\mathbb{Q}_p$: a medida que n crece, hay más apariciones de p entre los factores de $n!$. Se sigue que $|n!|_p \to 0$.

Un último ejemplo que contrasta con el mundo arquimediano:

Ejemplo 3.3. $\sum_{n=1}^{\infty} n \cdot n! =$ -1 en $\mathbb{Q}_p$: se tiene que $S_N := \sum_{n=1}^{N} n \cdot n! = (N+1)! - 1$, de lo que $S_N \to -1$.

Referencias

[Gou20] Fernando Q. Gouvêa, *p-adic Numbers: An iIntroduction*, third edition ed., Universitext, Springer, Cham, Switzerland, 2020.

[Ost16] Alexander Ostrowski, *Über einige Lösungen der Funktionalgleichung $\phi(x) \cdot \phi(y) = \phi(xy)$*, Acta Mathematica **41** (1916), no. 1, 271–284.