INTRODUCCIÓN A LOS NÚMEROS p-ÁDICOS

BENJAMÍN MACÍAS QUEZADA

RESUMEN. Los números p-ádicos son un campo resultante de completar $\mathbb{Q}$ respecto a una métrica distinta a la usual. Su importancia reside en que codifican información aritmética, por lo que resultan una potente herramienta para el estudio de la teoría de números. En esta charla presentaremos una introducción elemental, prestando atención a su construcción y propiedades básicas. Basado en [Gou20], §1– §3.

ÍNDICE

1. ANALOGÍA DE HENSEL

La definición de los números p-ádicos fue motivada principalmente por el deseo de aplicar ideas sobre series de potencias a la teoría de números. Hensel y Kronecker notaron similitudes entre $\mathbb{Z}$ junto a su campo de fracciones $\mathbb{Q}$, y $\mathbb{C}[x]$ junto a su campo de fracciones $\mathbb{C}(x)$, y exploraron hasta dónde llegaban. Esta comparación es lo que se conoce como la *Analogía de Hensel*:

1. - $\mathbb{C}[x]$ es un UFD: todo $P(x) \in \mathbb{C}[x]$ se escribe como producto de irreducibles $P(x) = a\prod_{i=1}^{s}(x-\alpha_i)$ de forma única para algunos $\alpha_i, a \in \mathbb{C}$.
   - Por otro lado, $\mathbb{Z}$ también lo es: todo $n \in \mathbb{Z}$ se escribe como producto de irreducibles $n = \pm\prod_{i=1}^{r} p_i$ de forma única para algunos p_i primos.
2. - Dado $\alpha \in \mathbb{C}$, todo $P \in \mathbb{C}[x]$ tiene una expansión de Taylor cerca de α, dada por $\sum_{i=0}^{n} a_i(x-\alpha)^i$.
   - Por otro lado, dada p un número primo, todo $n \in \mathbb{Z}$ tiene una expansión en base p, dada por $n = \sum_{i=0}^{n} a_i p^i$.
3. - Dado $\alpha \in \mathbb{C}$, todo $f \in \mathbb{C}(x)$ tiene una expansión de Laurent cerca de α, dada por $f(x) = \sum_{i\geq n_0} a_i(x-\alpha)^i$.
   - También, dado p número primo, todo $x \in \mathbb{Q}$ tiene una expansión en base p, dada por $\sum_{i\geq n_0} a_i p^i$. Para computarla, escribimos $x = \frac{a}{b}$, expresamos a y b como polinomios en p, y dividimos formalmente.

Date: 27 de mayo de 2022.

Por tanto, nuestro problema es formalizar este espacio de las expansiones de racionales en base p, y una vez hecho esto, estudiar sus propiedades.

2. 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.

Definición 2.1. Un *valor absoluto* en un campo k es una función $|\cdot|\colon k \to \mathbb{R}_{\geq 0}$ que para todos $x, y \in k$ cumple

(A1) $|x| = 0$ si y solo si $x = 0$,

(A2) $|xy| = |x||y|$,

(A3) $|x + y| \leq |x| + |y|$.

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

(A4) $|x + y| \leq \max\{|x|, |y|\}$.

El espacio métrico inducido por un valor absoluto no-arquimediano se llama *espacio ultramétrico*.

Observación. La desigualdad triangular fuerte implica la usual: tanto $|x|$ como $|y|$ son no-negativos, por lo que $\max\{|x|, |y|\} \leq |x| + |y|$.

Ejemplo 2.2. En todo campo se puede definir un valor absoluto trivial

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

También, el valor absoluto usual en $\mathbb{Q}$ es un valor absoluto.

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.

Definición 2.3. Sea p un número primo. La *valuación*[1] *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 $\nu_p(0) := \infty$.

Ejemplo 2.4. $\nu_2(60) = \nu_2(2^2 \cdot 3 \cdot 5) = 2$.

Definición 2.5. Sea p un número primo. Definimos la función $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}$ como

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

Lema 2.6. *Para cada p número primo, $|\cdot|_p$ es un valor absoluto no-arquimediano en $\mathbb{Q}$.*

[1] El nombre de "valuación" se debe a que ν_p es una valuación discreta en $\mathbb{Q}$ (cf. [AM18], p. 94).

Demostración. (A1) y (A2) son directos. Basta probar (A4). 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 máx $\left\{ |x|_p, |y|_p \right\} = |x|_p$. 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. □

Definición 2.7. El valor absoluto descrito en el lema anterior se llamará el *valor absoluto p-ádico.*

Observación. Es importante 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: ahora conocemos todos los valores absolutos en $\mathbb{Q}$, módulo ser equivalentes, en el sentido de la siguiente definición:

Definición 2.8. Dos métricas d_1, d_2 en un conjunto X son *equivalentes* si cada secuencia Cauchy respecto a d_1 también lo es respecto a d_2, y viceversa. Dos valores absolutos son *equivalentes* si inducen métricas equivalentes.

Observación. Recordar que $|\cdot|_1$ es equivalente a $|\cdot|_2$ si y solo si existe $\alpha > 0$ tal que $|x|_1 \leq |x|_2^\alpha$ para todo $x \in k$. También, los valores absolutos p-ádicos tienen una caracterización útil: 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 $|\cdot|_p$.

Teorema 2.9 (Ostrowski). *Todo valor absoluto no-trivial en $\mathbb{Q}$ es equivalente o al valor absoluto usual, o a un valor absoluto p-ádico.*

Demostración. La idea es notar que la imagen de $\mathbb{N}$ bajo un valor absoluto tiene dos posibilidades disjuntas: o existen tipos 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 prueba que no hay más casos.

1. Si existe algún natural con valor absoluto mayor a 1, tomemos n_0 el menor de tales números, y escribamos $|n_0| = n_0^\alpha$. Escribimos un $n \in \mathbb{N}$ en base n_0 como $n = \sum_{i=0}^{s} \left| a_i n_0^i \right|$, y acotamos:

$$\begin{aligned}|n| \leq \sum_{i=0}^{s} \left|a_i n_0^i\right| &\leq \sum_{i=0}^{s} |a_i| n_0^{\alpha i} \\ &\leq \sum_{i=0}^{s} n_0^{\alpha i} \\ &= n_0^{\alpha s} \sum_{i=0}^{s} \left(\frac{1}{n_0^{\alpha}}\right)^i \\ &= n_0^{\alpha s} \frac{n_0^{\alpha}}{n_0^{\alpha} - 1} \\ &\leq C n^{\alpha},\end{aligned}$$

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 $D n^{\alpha} \leq |n|$. 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 $|n| = C^{\nu_p(n)}$. □

3. Construcción y propiedades

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 3.1. *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 3.2. *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 3.3. *$(\mathbb{Q}, |\cdot|_p)$ 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 campo 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 campo, llamado la *compleción de k respecto a d*. El valor absoluto se extiende al cociente, el cual induce una estructura de espacio métrico completo.

Definición 3.4. La completación de $\mathbb{Q}$ respecto a $|\cdot|_p$ se llama el campo de los *números p-ádicos*, y se denota $\mathbb{Q}_p$.

Ejemplo 3.5. 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

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

Ejemplo 3.6. $\sum_{n=1}^{\infty} n!$ converge en $\mathbb{Q}_p$: a medida que n crece, hay más apariciones de p entre los factores de $n!$. Se sigue que $|n!|_p \to 0$.

Ejemplo 3.7. $\sum_{n=1}^{\infty} n \cdot n! =$ -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

[AM18] Michael Francis Atiyah and Ian G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley series in mathematics, CRC Press, Taylor Francis Group, Boca Raton London New York, 2018.

[Gou20] Fernando Q. Gouvêa, *p-adic numbers: an introduction*, third edition ed., Universitext, Springer, Cham, Switzerland, 2020.