Teoría de números, Universidad del Valle

Los aprendices de Weierstrass

Estuardo Menéndez-18072

UVG
UNIVERSIDAD DEL VALLE DE GUATEMALA

November 25, 2021

Contents

Introducción: La analogía de Hensel

- $\mathbb{Z}$ y $\mathbb{C}[X]$
- $\mathbb{Q}$ y $\mathbb{C}(X)$
- Series de Taylor para polinomios (centrados en algún α)
- ¿Podemos hacer lo mismo para $\mathbb{Z}$?

Introducción: Un ejemplo simple

Recordemos primero como escribir en base "n".

$$298 = 1 \times 3^5 + 0 \times 3^4 + 2 \times 3^3 + 0 \times 3^2 + 0 \times 3^1 + 1 \times 3^0 = 102001_3$$

Los elementos de $\mathbb{C}[X]$ y $\mathbb{Z}$ se pueden expresar así. Pero los elementos de $\mathbb{C}(X)$ también se pueden expresar como series de Taylor por medio de elementos "primos" (series infinitas de ellos, de hecho). Esto significa que:

$$f(x) = \frac{P(x)}{Q(x)} = \sum_{i>n_0} a_{n_0}(X-\alpha)^{n_0}$$

Donde α es complejo y n_0 es algún entero (puede ser negativo). Aquí los términos $(X-\alpha)$ son primos de $\mathbb{C}[X]$.

Introducción: Un ejemplo simple

Veamos un caso fácil, $f(x) = \frac{X}{X-1}$. Si se hace $\alpha = 0$ se tiene:

$$\frac{X}{X-1} = -X - X^2 - X^3 - \dots$$

Para $\alpha = 1$ se tiene:

$$\frac{X}{X-1} = (X-1)^{-1} + 1$$

Finalmente, para $\alpha = 2$ se tiene:

$$\frac{X}{X-1} = 2 - (X-2) + (X-2)^2 - (X-2)^3 + \dots$$

¿Podemos hacer lo mismo para $\mathbb{Q}$?

Introducción: ya no es tan simple

Empecemos por medio de un ejemplo relativamente simple. Tómese $1/2$ y $p = 5$. Haciendo uso del algoritmo de división de euclides se tiene $\frac{1}{2} = 5 \times \frac{-1}{2} + 3$. Con esto en mente, el primer "término" (de menor grado) en base 5 es 3. Ahora se repite el proceso para $-1/2$.

$$\frac{-1}{2} = 5 \times \frac{-1}{2} + 2$$

El segundo término es 2. El problema ahora (o la particularidad) es que volvimos a obtener $-1/2$. Para expresar la fracción en términos de 5 escribimos:

$$\frac{1}{2} = 3 + 2 \times 5 + 2 \times 5^2 + 2 \times 5^3 + \cdots = \ldots 22223_5$$

Nótese que, si multiplicamos este número por 2 en base 5 el 3 del comienzo queda como 11_5, que le "presta" a su término de la izquierda, el cual se convierte en 10_5. Este proceso se repite infinitamente para obtener $1 = \ldots 0001$

Introducción: ya no es tan simple

Con esta idea, la noción de expandir fracciones en términos primos no es rara. Siguiendo la analogía de Hensel se dice lo siguiente:

$$x = \frac{a}{b} = \sum_{i \geq n_0} a_{n_0} p^{n_0} = a_{n_0} p^{n_0} + a_{n_0+1} p^{n_0+1} + \dots$$

A estas series de Lauret normalmente se les refiere como "de cola finita". Nosotros las llamaremos *expansión p-ádica*. La analogía de Hensel va aún más alla; el conjunto de todas las expansiones p-ádicas forman un campo (análogo a como $\mathbb{C}((X-\alpha))$ lo es también). A dicho campo le llamaremos de ahora en adelante $\mathbb{Q}_p$, *el campo de números p-ádicos*. Finalmente, cabe mencionar que este campo es más grande que $\mathbb{Q}$ (no se demostrará).

Nociones preliminares

Definición

Sea p un primo. Se dice que la secuencia α_n tal que $1 \leq \alpha_n \leq p^n - 1$ es coherente si para cada n se tiene que:

$$\alpha_{n+1} \equiv \alpha_n (\mod p^n)$$

Estas series son algo que se estará usando detras de escenas mucho en los teoremas que se verán. También son sumamente convenientes a la hora de hacer levantamientos de soluciones de congruencias cuadráticas módulo p^n.

Nociones preliminares

Definición

Una funcion $|\ |: \mathbb{k} \to \mathbb{R}^+$ sobre un campo $\mathbb{k}$ es un valor absoluto si se cumple lo siguiente:

1. $|x| = 0$ ssi $x = 0$
2. $|xy| = |x||y|$ para todo $x, y \in \mathbb{k}$
3. $|x + y| \leq |x| + |y|$ para todo $x, y \in \mathbb{k}$
   Adicional a esto, se dice que el valor absoluto es no arquimediano si se cumple:
4. $|x + y| \leq \max\{|x|, |y|\}$ para todo $x, y \in \mathbb{k}$

Definición

Fíjese un primo p en $\mathbb{Z}$. La valuación p-ádica sobre $\mathbb{Z}$ es una función:

$$v_p : \mathbb{Z} - \{0\} \to \mathbb{R}$$

Definida de la siguiente manera: para cada entero $n \in \mathbb{Z} - \{0\}$ sea $v_p(n)$ el *único* entero que cumple con la condición:

$$n = p^{v_p(n)} n', \qquad p \nmid n'$$

Con este concepto, se puede extender esta idea a los racionales, donde $x = \frac{a}{b} \in \mathbb{Q}^\times$ es evaluado como:

$$v_p(x) = v_p(a) - v_p(b)$$

Por convención, tambien se dice que $v_p(0) = +\infty$ dado que 0 puede ser divido por p infinitamente

Con esto en mente, se define el valor absoluto p-ádico como:

Definición: valor absoluto p-ádico

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

Donde, una vez más, se extiende el concepto a todos los racionales haciendo $|0|_p = 0$

Con esta definición se puede notar que el valor absoluto p-ádico es un valor absoluto no arquimediano en los racionales. Adicional a esto, se observará que el valor absoluto de un número entero es siempre menor que 1.

Manos a la obra: topología

Lema

Sea $|\ |$ un valor absoluto en un campo $\mathbb{k}$ y definase la función de distancia $d(x, y) = |x - y|$. Entonces $|\ |$ es no arquimediano si y solo si:

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

Para cualquier $x, y, z \in \mathbb{k}$

A esta desigualdad se le llama *desigualdad de ultramétrica* y las métricas que cumplen dicha desigualdad se le llaman ultramétricas. En general, para cualquier par de elementos de $\mathbb{k}$ tales que $|x| \neq |y|$ se cumple que $|x + y| = \max\{|x, |y|\}$.

Manos a la obra: topología

A continuación se muestran algunas propieades de la topología generada por una métrica no arquimediana:

Propiedades

Para un campo $\mathbb{k}$ con un valor absoluto no arquimediano.

1. si $b \in B(a,r)$, entonces $B(a,r) = B(b,r)$. En otras palabras, todos los elementos de una bola son los centros de dicha bola.
2. El conjunto $B(a,r)$ es tanto abierto como cerrado. Esto significa que la frontera de la bola está vacia.
3. Si $a, b \in \mathbb{k}$ y $s, r \in \mathbb{R}^+$ entonces $B(a,r) \cap B(b,s) \neq \emptyset$ ssi $B(a,r) \subset B(b,s)$ o $B(b,s) \subset B(a,r)$. En otras palabras, en otras palabras, dos bolas son disjuntas o están contenidas entre sí.

Propiedad

En un campo $\mathbb{k}$ con un valor absoluto no arquimediano, las componentes conexas de cualquier punto $x \in \mathbb{k}$ es el conjunto $\{x\}$ que contiene únicamente a dicho punto.

Como se vió en la clase de topología, esto implica que cualquier espacio con un valor absoluto no arquimediano es totalmente disconexo.

Esta nueva información es sumamente importante para comprender el comportamiento de los números p-ádicos ya que ahora es posible buscar conjuntos totalmente disconexos para visualizar de mejor manera el comportamiento de dichos números. Un teorema importante sobre esta teoría es que los enteros p -adicos (los cuales definiremos formalmente pronto) son homeomorfos al conjunto de Cantor. Antes de atacar este concepto totalmente, es necesario definir formalmente los números p– ádicos. Para esto se mencionaran primero propiedades algebraicas que se usarán para la construcción necesaria.

El álgebra es mi amiga

Hay muchos conceptos algebráicos que trabajan tras bambalinas. No se mencionarán todos ya que no es necesario comprenderlos todos para llegar al resultado que queremos demostrar. Por ahora nos quedaremos con la siguiente propiedad:

Lema

Considérese los racionales $\mathbb{Q}$ bajo el valor absoluto $|\ |_p$. Entonces:

1. El conjunto $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b\}$ es un subanillo y se le llama *anillo de valuación asociado de* $|\ |_p$.
2. El conjunto $p\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b \text{ y } p|a\}$ es un ideal del anillo de valuación asociado y es llamado *ideal de valuación de* $|\ |_p$.
3. El cociente $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{F}_p$ se le llama campo de residuos (es el campo de p elementos).

Construcción de $\mathbb{Q}_p$

Primero notemos que el campo $\mathbb{Q}$ no es completo respecto a ningún valor absoluto no trivial. Con esto en mente, se tomará el conjunto de todas las sucesiones de Cauchy de elementos de $\mathbb{Q}$ con respecto al valor absoluto $|\ |_p$, llamado $\mathcal{C}$. Este tiene dos propiedades importantes. La primera es que es un anillo (y no campo). La segunda es que hay varios elementos que convergen al mismo valor $x \in \mathbb{Q}$.

Se construye el conjunto $\mathcal{N} \subset \mathcal{C}$, el conjunto de todas las sucesiones de Cauchy que convergen a 0. Este es un ideal maximal de $\mathcal{C}$ El cociente de estos generará un campo, que tendrá las propiedades que queremos que tenga $\mathbb{Q}_p$. Esta idea se resume con la siguiente definición

Construcción de $\mathbb{Q}_p$

Definición

Los números p–ádicos se definen como el cociente del anillo C y su ideal maximal $\mathcal{N}$:

$$\mathbb{Q}_p = C/\mathcal{N}$$

Propiedad

La imagen de $\mathbb{Q}$ bajo el mapeo de inclusión

$$\mathbb{Q} \to \mathbb{Q}_p$$

es un subconjunto denso de $\mathbb{Q}_p$

Los enteros p–ádicos

Con el concepto anterior bien definido, es posible empezar a visualizar de mejor manera $\mathbb{Q}_p$. Se definen los enteros p–ádicos $\mathbb{Z}_p$ como:

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

Con esto en mente se tiene la siguiente propiedad:

Propiedad

El anillo $\mathbb{Z}_p$ tiene un ideal maximal definido como $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$. Además:

1. $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$
2. La inclusión $\mathbb{Z} \to \mathbb{Z}_p$ tiene imagen densa
3. Para cualquier elemento $x \in \mathbb{Z}_p$ existe una única sucesión de Cauchy (α_n) que converge a x que cumple con:
   - $\alpha_n \in \mathbb{Z}$ satisface $0 \leq \alpha_n \leq p^n - 1$
   - $\alpha_n \equiv \alpha_{n-1} (\mod p^{n-1})$

Algunas propiedades importantes

- $\mathbb{Z}$ es denso en $\mathbb{Z}_p$
- $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$
- $\mathbb{Q}_p$ es un espacio topológico totalmente disconexo y Hausdorff.
- $\mathbb{Z}_p$ es compacto y $\mathbb{Q}_p$ es localmente compacto
- Los elementos invertibles de $\mathbb{Z}_p$ se les llama unidades p–ádicas y se denotan por $\mathbb{Z}_p^\times$

Conjunto de Cantor

Dada la compacidad y la total disconexidad del conjunto, es solo natural pensar que los p–ádicos tienen alguna relación importante o interesante con el conjunto de Cantor. En efecto:

Teorema

$\mathbb{Z}_p$ con el la norma 2-ádica es homeomorfo al conjunto de Cantor con $r = 1/3$ con la topología heredada por $\mathbb{R}$

Adicional a esto:

Propiedad

$\mathbb{Z}_2$ es homeomorfo a $\mathbb{Z}_p$ para cualquier primo p

Esta propiedad es sumamente importante a la hora de analizar los p–ádicos bajo la perspectiva de la topología. Esta idea, sin embargo, aún no provee una visualización del conjunto. A continuación se presenta una visualización más clara.

Referencias Y Agradecimientos

Se agradece especialmente a Roice Nelson, de la Universidad de Austin, quien compartió su programa para recrear la operación de suma de manera visual en los números p–ádicos.

Referencias:

- Gouvêa, F. (2021). *p-adic numbers, an introduction*. Tercera edición. Springer
- Robert, A. (2007). *A course on p-adic Analysis*. Springer.