Una Breve Introducción a los Números p-ádicos

Seminario de Teoría de Números

Luciano Sciaraffia R.

Pontificia Universidad Católica de Chile

14 de agosto de 2018

Valores absolutos

Definición

Un valor absoluto en un cuerpo K es una función

$$|\cdot| : K \to \mathbb{R}$$

que satisface las condiciones:

1. $|x| = 0$ *si y sólo si* $x = 0$;
2. $|xy| = |x||y|$ *para todo* $x, y \in K$;
3. $|x + y| \leq |x| + |y|$ *para todo* $x, y \in K$.

Valores absolutos

Definición

Un valor absoluto en un cuerpo K es una función

$$|\cdot| : K \to \mathbb{R}$$

que satisface las condiciones:

1. $|x| = 0$ *si y sólo si* $x = 0$;
2. $|xy| = |x||y|$ *para todo* $x, y \in K$;
3. $|x + y| \leq |x| + |y|$ *para todo* $x, y \in K$.

Decimos que el valor absoluto es no arquimediano si además satisface

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

en caso contrario, es arquimediano.

Valores absolutos

- $\mathbb{R}$ con el valor absoluto usual:

$$|x| = \begin{cases} |x| = x & \text{si } x \geq 0, \\ |x| = -x & \text{si } x \leq 0. \end{cases}$$

- Un cuerpo K con el valor absoluto trivial:

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

- $\mathbb{Q}$ con el valor absoluto p-ádico:

$$|x|_p = p^{-n}\,, \quad \text{si } x = p^n \frac{a}{b}\,,\ (p,a) = (p,b) = 1.$$

Valores absolutos

Consideremos la función $v : K[x] \to \mathbb{R}$, $v = -\deg$. Podemos extenderla a $K(x)$ mediante

$$v\left(\frac{f(x)}{g(x)}\right) = v(f(x)) - v(g(x)) \, .$$

La función v satisface:

- $v(fg) = v(f) + v(g)$;
- $v(f+g) \geq \min\{v(f), v(g)\}$.

Esto nos da un valor absoluto no arquimediano $|f(x)| = e^{-v(f)}$.

Curiosidades del caso no arquimediano

- Todo triángulo es isósceles.

Curiosidades del caso no arquimediano

- Todo triángulo es isósceles.
- Todo elemento de una bola es su centro.

Curiosidades del caso no arquimediano

- Todo triángulo es isósceles.
- Todo elemento de una bola es su centro.
- (Sueño del estudiante de cálculo) Si el cuerpo K es completo respecto a $|\cdot|$, entonces

$$\sum_{n=1}^{\infty} x_n \quad \text{converge si y sólo si} \quad \lim_{n\to\infty} x_n = 0\ ;$$

$$\{x_n\}_{n=1}^{\infty} \quad \text{converge si y sólo si} \quad \lim_{n\to\infty} |x_{n+1} - x_n| = 0\ .$$

Valores absolutos en $\mathbb{Q}$

Definición

Dos valores absolutos $|\cdot|_1$, $|\cdot|_2$ *en un cuerpo* K *son equivalentes si existe un* $\alpha > 0$ *tal que*

$$|x|_1 = |x|_2^{\alpha} .$$

Valores absolutos en $\mathbb{Q}$

Definición

Dos valores absolutos $|\cdot|_1$, $|\cdot|_2$ en un cuerpo K son equivalentes si existe un $\alpha > 0$ tal que

$$|x|_1 = |x|_2^{\alpha} .$$

Teorema (Ostrowski)

Todo valor absoluto no trivial en $\mathbb{Q}$ es quivalente al valor absoluto usual o a algún valor absoluto p-ádico.

Valores absolutos en $\mathbb{Q}$

Definición

Dos valores absolutos $|\cdot|_1$, $|\cdot|_2$ en un cuerpo K son equivalentes si existe un $\alpha > 0$ tal que

$$|x|_1 = |x|_2^{\alpha} .$$

Teorema (Ostrowski)

Todo valor absoluto no trivial en $\mathbb{Q}$ es quivalente al valor absoluto usual o a algún valor absoluto p-ádico.

Demostración

Idea: En el caso arquimediano, escogemos n_0 el menor entero tal que $|n| > 1$ y tomamos $\alpha > 0$ tal que $|n_0| = n_0^{\alpha}$. En el caso no arquimediano, escogemos el menor n_0 tal que $|n| < 1$, entonces $n_0 = p$ es primo, $|\cdot|$ es equivalente a $|\cdot|_p$.

Completaciones

Teorema

Sea K un cuerpo con valor absoluto $|\cdot|$. Luego, existe un cuerpo $\hat{K}$ extendiendo K tal que:

1. *$|\cdot|$ se extiende a un valor absoluto en $\hat{K}$, también denotado $|\cdot|$, tal que $\hat{K}$ es completo respecto a $|\cdot|$.*
2. *K es denso en $\hat{K}$.*

Esta extensión es única, salvo por isomorfismo que preserva el valor absoluto, y $\hat{K}$ se llama la completación de K.

Completaciones

Teorema

Sea K un cuerpo con valor absoluto $|\cdot|$. Luego, existe un cuerpo $\hat{K}$ extendiendo K tal que:

1. *$|\cdot|$ se extiende a un valor absoluto en $\hat{K}$, también denotado $|\cdot|$, tal que $\hat{K}$ es completo respecto a $|\cdot|$.*
2. *K es denso en $\hat{K}$.*

Esta extensión es única, salvo por isomorfismo que preserva el valor absoluto, y $\hat{K}$ se llama la completación de K.

Demostración

Idea: Sea C el conjunto de sucesiones de Cauchy de K, y N el conjunto de sucesiones que convergen a 0. C es un anillo con las operaciones definidas punto a punto y N un ideal maximal. Entonces $\hat{K} = C/N$.

Números p-ádicos

Definición

Sea p un número primo.

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

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

Números p-ádicos

Lema

Para cada $x \in \mathbb{Z}_p$ y cada $n \geq 1$ existe un único $x_n \in \mathbb{Z}$, $0 \leq x_n < p^n$, tal que

$$x \equiv x_n \mod p^n .$$

Números p-ádicos

Lema

Para cada $x \in \mathbb{Z}_p$ y cada $n \geq 1$ existe un único $x_n \in \mathbb{Z}$, $0 \leq x_n < p^n$, tal que

$$x \equiv x_n \mod p^n .$$

Teorema

Todo elemento $x \in \mathbb{Z}_p$ puede expresarse de manera única como serie

$$\sum_{n=0}^{\infty} x_n p^n ,$$

con $0 \leq x_n < p$. Recíprocamente, toda serie tal pertenece a $\mathbb{Z}_p$.

Números p-ádicos

Lema

Las unidades de $\mathbb{Z}_p$ son

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

Todo elemento $x \in \mathbb{Z}_p$ puede escribirse de modo único como $x = p^n u$, donde $u \in \mathbb{Z}_p^\times$.

Números p-ádicos

Lema

Las unidades de $\mathbb{Z}_p$ son

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

Todo elemento $x \in \mathbb{Z}_p$ puede escribirse de modo único como $x = p^n u$, donde $u \in \mathbb{Z}_p^\times$.

Corolario

Todo elemento $x \in \mathbb{Q}_p$ puede expresarse de manera única como serie

$$\sum_{n=n_0}^{\infty} x_n p^n ,$$

con $0 \leq x_n < p$, $n_0 \in \mathbb{Z}$. Recíprocamente, toda serie tal pertenece a $\mathbb{Q}_p$.

Construcción alternativa

Lema

- *Los ideales no nulos de* $\mathbb{Z}_p$ *son* $p^n\mathbb{Z}_p$, $n \geq 0$.
- $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

Construcción alternativa

Lema

- *Los ideales no nulos de* $\mathbb{Z}_p$ *son* $p^n\mathbb{Z}_p$, $n \geq 0$.
- $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

Teorema

Existe una inclusión

$$\mathbb{Z}_p \hookrightarrow \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \,,$$

la cual identifica a $\mathbb{Z}_p$ *con el subanillo de las sucesiones* $\{x_n\}_{n=1}^{\infty}$ *tales que* $x_{n+1} \equiv x_n \mod p^n$.

Construcción alternativa

Tomando los homomorfismos $\psi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$ de reducción mod p^{n-1}, tenemos la secuencia

$$\cdots \to \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z} \to \cdots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \,.$$

Entonces, $\mathbb{Z}_p$ es el límite proyectivo

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} \,.$$

Construcción alternativa

Tomando los homomorfismos $\psi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$ de reducción mod p^{n-1}, tenemos la secuencia

$$\cdots \to \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z} \to \cdots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \,.$$

Entonces, $\mathbb{Z}_p$ es el límite proyectivo

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} \,.$$

Esto es, el anillo con la siguiente propiedad universal: existen únicas proyecciones $\pi_n : \varprojlim \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ tales que para cualquier anillo R y homomorfismos $\phi_n : R \to \mathbb{Z}/p^n\mathbb{Z}$ tales que $\phi_{n-1} = \psi_n \circ \phi_n$, existe un único homomorfismo $\phi : R \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ tal que $\phi_n = \pi_n \circ \phi$.

Lema de Hensel

Teorema (Hensel)

Sea $f(x) \in \mathbb{Z}_p[x]$. Supongamos que existe $\alpha_0 \in \mathbb{Z}_p$ tal que

$$f(\alpha_0) \equiv 0 \mod p\,, \quad f'(\alpha_0) \not\equiv 0 \mod p\,.$$

Luego, existe $\alpha \in \mathbb{Z}_p$ tal que

$$f(\alpha) = 0\,, \qquad \alpha \equiv \alpha_0 \mod p\,.$$

Lema de Hensel

Teorema (Hensel)

Sea $f(x) \in \mathbb{Z}_p[x]$. Supongamos que existe $\alpha_0 \in \mathbb{Z}_p$ tal que

$$f(\alpha_0) \equiv 0 \mod p\,, \quad f'(\alpha_0) \not\equiv 0 \mod p\,.$$

Luego, existe $\alpha \in \mathbb{Z}_p$ tal que

$$f(\alpha) = 0\,, \qquad \alpha \equiv \alpha_0 \mod p\,.$$

Demostración

Idea: construir una sucesión $\{\alpha_n\}_{n=0}^{\infty}$ tal que

$$f(\alpha_n) \equiv 0 \mod p^n\,, \qquad \alpha_{n+1} \equiv \alpha_n \mod p^n\,.$$

Lema de Hensel

Demostración

La segunda condición arriba entrega

$$f(\alpha_{n+1}) = f(\alpha_n + bp^n) \equiv f(\alpha_n) + bp^n \cdot f'(\alpha_n) \mod p^{n+1} .$$

Despejando $b \equiv -\frac{f(\alpha_n)/p^n}{f'(\alpha_n)}$ *de la primera condición, obtenemos*

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)} .$$

La sucesión $\{\alpha_n\}_{n=0}^{\infty}$ *es de Cauchy y* $\lim_{n\to\infty} \alpha_n = \alpha$ *satisface* $f(\alpha) = 0$.

Aplicaciones

Teorema (Cuadrados en $\mathbb{Q}_p$, $p > 2$)

Sea $p > 2$ un primo. Luego, $x \in \mathbb{Q}_p$, $x = p^n u$, con $n \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$, es un cuadrado si y sólo si n es par y $u \mod p$ es un cuadrado en $\mathbb{Z}/p\mathbb{Z}$.

Aplicaciones

Teorema (Cuadrados en $\mathbb{Q}_p$, $p > 2$)

Sea $p > 2$ un primo. Luego, $x \in \mathbb{Q}_p$, $x = p^n u$, con $n \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$, es un cuadrado si y sólo si n es par y $u \mod p$ es un cuadrado en $\mathbb{Z}/p\mathbb{Z}$.

Teorema (Hasse-Minkowski)

Una forma cuadrática sobre $\mathbb{Q}$,

$$f(x_1, \ldots, x_n) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j \ , \qquad a_{ij} \in \mathbb{Q} \ ,$$

representa 0 si y sólo si representa a 0 sobre $\mathbb{R}$ y $\mathbb{Q}_p$ para todo primo p.

Referencias


Herivelto Borges, Eduardo Tengan.

Álgebra Comutativa em quatro Movimentos.


Otto Endler.

Valuation Theory.


Jan-Hendrik Evertse.

p-adic Numbers.


Fernando Q. Gouvêa.

p-adic Numbers, An Introduction.


Alexey N. Parshin, Igor R. Shafarevich.

Number Theory I, Encyclopaedia of Mathematical Sciences.