UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA
Departamento de Ciências Exatas

Resolvendo equações em corpos p-ádicos

Maurício de Araujo Ferreira

VII Bienal da SBM - UFAL

02 a 06 de novembro de 2014

Valor absoluto em corpos

Definição

Seja K um corpo. Dizemos que uma aplicação

$$|\cdot| : K \longrightarrow \mathbb{R},$$

é um valor absoluto em K se satisfaz as seguintes condições:

(i) $|x| \geq 0$ *e* $|x| = 0$ *se, e somente se,* $x = 0$;

(ii) $|xy| = |x||y|$ *para todos os* $x, y \in K$;

(iii) $|x + y| \leq |x| + |y|$ *para todos os* $x, y \in K$.

Valor absoluto em corpos

Definição

Seja K um corpo. Dizemos que uma aplicação

$$|\cdot| : K \longrightarrow \mathbb{R},$$

é um valor absoluto em K se satisfaz as seguintes condições:

(i) $|x| \geq 0$ *e* $|x| = 0$ *se, e somente se,* $x = 0$;

(ii) $|xy| = |x||y|$ *para todos os* $x, y \in K$;

(iii) $|x + y| \leq |x| + |y|$ *para todos os* $x, y \in K$.

Exemplo

Valor absoluto trivial em K: $|x| = \begin{cases} 1, & \text{se } x \neq 0; \\ 0, & \text{se } x = 0. \end{cases}$

Exemplo

Valor absoluto usual no corpo dos números reais $\mathbb{R}$*:*

$$|x| = \begin{cases} x, & \text{se } x \geq 0; \\ -x, & \text{se } x < 0. \end{cases}$$

Exemplo

Valor absoluto usual no corpo dos números complexos $\mathbb{C}$*:*

$$|a + bi| = \sqrt{a^2 + b^2}$$

Definição

Um valor absoluto $|\cdot|$ em um corpo K é dito não-arquimediano se satizfaz a seguinte propriedade para todos $x, y \in K$

$$|x+y| \leq \max\{|x|, |y|\}. \tag{1}$$

Nota

Note que (1) implica a desigualdade triangular.

Definição

Um valor absoluto $|\cdot|$ em um corpo K é dito não-arquimediano se satizfaz a seguinte propriedade para todos $x, y \in K$

$$|x + y| \leq \max\{|x|, |y|\}. \tag{1}$$

Nota

Note que (1) implica a desigualdade triangular.

Proposição

Um valor absoluto $|\cdot|$ em um corpo K é não-arquimediano se e somente se $\{n \cdot 1 \mid n \in \mathbb{N}\}$ é limitado em K.

Definição

Um valor absoluto $|\cdot|$ em um corpo K é dito não-arquimediano se satizfaz a seguinte propriedade para todos $x, y \in K$

$$|x + y| \leq \max\{|x|, |y|\}. \tag{1}$$

Nota

Note que (1) implica a desigualdade triangular.

Proposição

Um valor absoluto $|\cdot|$ em um corpo K é não-arquimediano se e somente se $\{n \cdot 1 \mid n \in \mathbb{N}\}$ é limitado em K.

$|n \cdot 1| = |1 + 1 + \ldots + 1| \leq \max\{|1|\} = 1.$

Seja p um número natural primo qualquer. Se x é um número racional diferente de zero, então podemos escrever x de maneira única da seguinte forma:

$$x = p^{\alpha}\frac{a}{b}, \text{ com } \frac{a}{b} \in \mathbb{Q} \setminus \{0\},\ p \nmid ab \text{ e } \alpha \in \mathbb{Z}.$$

Para qualquer $x \in \mathbb{Q}$, definimos:

$$|x|_p = \begin{cases} 0, & \text{se } x = 0; \\ e^{-\alpha}, & \text{se } x \neq 0. \end{cases}$$

A aplicação $|\cdot|_p$ é um valor absoluto não-arquimediano em $\mathbb{Q}$, que é chamado de valor absoluto p-ádico.

Verificação:
Sejam $x = p^{\alpha}\frac{a}{b}$ e $y = p^{\beta}\frac{c}{d}$ racionais diferentes de zero.

(ii) $|xy|_p = |p^{\alpha+\beta}\frac{ac}{bd}|_p = e^{-\alpha-\beta} = e^{-\alpha}\cdot e^{-\beta} = |x|_p \cdot |y|_p$.

(iii) Suponhamos que $|x|_p \leq |y|_p$, isto é, $\alpha \geq \beta$.

$$|x+y|_p = |\frac{p^{\beta}(p^{\alpha-\beta}ad+bc)}{bd}|_p = e^{-\beta-k},$$

onde k é maior potência de p que divide $p^{\alpha-\beta}ad+bc$. Segue que

$$|x+y|_p \leq e^{-\beta} = |y|_p = \max\{|x|_p, |y|_p\}.$$

Proposição

Seja K um corpo e $|\cdot|$ um valor absoluto em K. Considere a aplicação:

$$\begin{aligned} d: \quad K \times K &\longmapsto \mathbb{R}; \\ (x,y) &\longmapsto d(x,y) := |x-y|. \end{aligned}$$

A aplicação d tem as seguintes propriedades para x, y e $z \in K$:

(i) $d(x,y) \geq 0$, *e* $d(x,y) = 0$ *se e somente se,* $x = y$;

(ii) $d(x,y) = d(y,x)$;

(iii) $d(x,z) \leq d(x,y) + d(y,z)$. *(Desigualdade triangular)*

Portanto, o valor absoluto induz uma métrica no corpo.

Definição

Dois valores absolutos são ditos equivalentes se as respectivas métricas induzidas são equivalentes.

Definição

Dois valores absolutos são ditos equivalentes se as respectivas métricas induzidas são equivalentes.

Proposição

Se p e q são primos distintos, então os valores absolutos p-ádicos $|\cdot|_p$ e $|\cdot|_q$ não são equivalentes.

Definição

Dois valores absolutos são ditos equivalentes se as respectivas métricas induzidas são equivalentes.

Proposição

Se p e q são primos distintos, então os valores absolutos p-ádicos $|\cdot|_p$ e $|\cdot|_q$ não são equivalentes.

$|\frac{p}{q^n}|_p = e^{-1}$ e $|\frac{p}{q^n}|_q = e^n \Rightarrow B^p(0,1) \nsubseteq B_q(0,r)$.

Definição

Dois valores absolutos são ditos equivalentes se as respectivas métricas induzidas são equivalentes.

Proposição

Se p e q são primos distintos, então os valores absolutos p-ádicos $|\cdot|_p$ e $|\cdot|_q$ não são equivalentes.

$|\frac{p}{q^n}|_p = e^{-1}$ e $|\frac{p}{q^n}|_q = e^n \Rightarrow B^p(0,1) \nsubseteq B_q(0,r)$.

Teorema (Ostrowski, 1916)

Todo valor absoluto não trivial em $\mathbb{Q}$ é equivalente ao valor absoluto usual ou ao valor absoluto p-ádico para algum primo p.

Completamento

Seja (M, d) um espaço métrico e (x_n) uma sequência em M.

Definição

Dizemos que (x_n) *converge para* $a \in M$ *se* $\lim d(x_n, a) = 0$.
Denotamos por $(x_n) \to a$.

Completamento

Seja (M, d) um espaço métrico e (x_n) uma sequência em M.

Definição

Dizemos que (x_n) converge para $a \in M$ se $\lim d(x_n, a) = 0$.
Denotamos por $(x_n) \to a$.

Definição

Dizemos que (x_n) é uma sequência de Cauchy se dado $\varepsilon > 0$, existe $N > 0$ tal que se $n, m > N$, então $d(x_n, x_m) < \varepsilon$.

Completamento

Seja (M, d) um espaço métrico e (x_n) uma sequência em M.

Definição

Dizemos que (x_n) converge para $a \in M$ se $\lim d(x_n, a) = 0$.
Denotamos por $(x_n) \to a$.

Definição

Dizemos que (x_n) é uma sequência de Cauchy se dado $\varepsilon > 0$, existe $N > 0$ tal que se $n, m > N$, então $d(x_n, x_m) < \varepsilon$.

Definição

(M, d) é dito completo quando toda sequência de Cauchy é convergente.

Definição

O completamento de $\mathbb{Q}$ com respeito ao valor absoluto p-ádico é o corpo de números p-ádicos, que denotamos por $\mathbb{Q}_p$.

Definição

O completamento de $\mathbb{Q}$ com respeito ao valor absoluto p-ádico é o corpo de números p-ádicos, que denotamos por $\mathbb{Q}_p$.

Proposição

Seja $(K, |\cdot|)$ um corpo completo não-arquimediano e seja (a_n) uma sequência em K. Então a série $\sum a_n$ converge se e somente se $(a_n) \to 0$.

Definição

O completamento de $\mathbb{Q}$ com respeito ao valor absoluto p-ádico é o corpo de números p-ádicos, que denotamos por $\mathbb{Q}_p$.

Proposição

Seja $(K, |\cdot|)$ um corpo completo não-arquimediano e seja (a_n) uma sequência em K. Então a série $\sum a_n$ converge se e somente se $(a_n) \to 0$.

$|s_m - s_n| = |a_m + \ldots + a_{n+1}| \leq \max\{|a_n|\} \to 0.$

Definição

O completamento de $\mathbb{Q}$ com respeito ao valor absoluto p-ádico é o corpo de números p-ádicos, que denotamos por $\mathbb{Q}_p$.

Proposição

Seja $(K, |\cdot|)$ um corpo completo não-arquimediano e seja (a_n) uma sequência em K. Então a série $\sum a_n$ converge se e somente se $(a_n) \to 0$.

$|s_m - s_n| = |a_m + \ldots + a_{n+1}| \leq \max\{|a_n|\} \to 0.$

Proposição

Todo $x \in \mathbb{Q}_p^\times$ se escreve de maneira única da forma $\sum_{i=k}^{\infty} a_i p^i$, onde $k = -\ln |x|_p$ e $0 \leq a_i < p$.

Valorização

Seja K um corpo com um valor absoluto $|\cdot|$ e seja ∞ um símbolo tal que $\infty > \gamma$, e $\infty = \infty + \infty = \infty + \gamma = \gamma + \infty$ para todo $\gamma \in \mathbb{R}$. A aplicação $v : K \to \mathbb{R} \cup \{\infty\}$, definida por

$$v(x) = \begin{cases} -\ln|x|, & \text{se } x \neq 0; \\ \infty, & \text{se } x = 0, \end{cases}$$

satisfaz para todo $x, y \in K$:

(i) $v(x) = \infty$ se e somente se $x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

(iii) $v(x + y) \geq \min(v(x), v(y))$.

Valorização

Seja K um corpo com um valor absoluto $|\cdot|$ e seja ∞ um símbolo tal que $\infty > \gamma$, e $\infty = \infty + \infty = \infty + \gamma = \gamma + \infty$ para todo $\gamma \in \mathbb{R}$.
A aplicação $v : K \to \mathbb{R} \cup \{\infty\}$, definida por

$$v(x) = \begin{cases} -\ln|x|, & \text{se } x \neq 0; \\ \infty, & \text{se } x = 0, \end{cases}$$

satisfaz para todo $x, y \in K$:

(i) $v(x) = \infty$ se e somente se $x = 0$;
(ii) $v(xy) = v(x) + v(y)$;
(iii) $v(x + y) \geq \min(v(x), v(y))$.

Um aplicação $v : K \to \mathbb{R} \cup \{\infty\}$ satisfazendo (i), (ii) e (iii) acima é dita uma valorização.
Se v é uma valorização em K então $|x| = e^{-v(x)}$ define um valor absoluto em K.

Anel de valorização e corpo de resíduos

Seja K um corpo com uma valorização v. Então

$$V = \{x \in F \mid v(x) \geq 0\} \text{ é um subanel de } K,$$

que é chamado de anel de valorização e

$$M = \{x \in F \mid v(x) > 0\} \text{ é um ideal maximal de } V.$$

O anel quociente $\overline{F} = V/M$ é chamado de corpo de resíduos.

Anel de valorização e corpo de resíduos

Seja K um corpo com uma valorização v. Então

$$V = \{x \in F \mid v(x) \geq 0\} \text{ é um subanel de } K,$$

que é chamado de anel de valorização e

$$M = \{x \in F \mid v(x) > 0\} \text{ é um ideal maximal de } V.$$

O anel quociente $\overline{F} = V/M$ é chamado de corpo de resíduos.

No caso em que $K = \mathbb{Q}$ ou $\mathbb{Q}_p$ e v é valorização p-ádica, temos que o corpo de resíduos V_p/M_p é o corpo finito com p elementos $\mathbb{F}_p$.

Lema de Hensel

Teorema

Seja $(K, v, V, M, \overline{K})$ um corpo valorizado completo. Seja $f \in V[X]$ e $a_0 \in V$ tal que

$$v(f(a_0)) > 2v(f'(a_0)).$$

Então existe $a \in V$ tal que $f(a) = 0$ e $\overline{a} = \overline{a_0}$ em $\overline{K}$.

Lema de Hensel

Teorema

Seja $(K, v, V, M, \overline{K})$ um corpo valorizado completo. Seja $f \in V[X]$ e $a_0 \in V$ tal que

$$v(f(a_0)) > 2v(f'(a_0)).$$

Então existe $a \in V$ tal que $f(a) = 0$ e $\overline{a} = \overline{a_0}$ em $\overline{K}$.

Corolário

Seja $(K, v, V, M, \overline{K})$ um corpo valorizado completo. Seja $f \in V[X]$. Suponhamos que $\overline{f}$ tem uma raíz simples $\overline{a_0} \in \overline{K}$. Então existe $a \in V$ tal que $f(a) = 0$ e $\overline{a} = \overline{a_0}$.

Exemplo

Resolver a equação $X^2 + 1 = 0$ *em* $\mathbb{Q}_5$.

Exemplo

Resolver a equação $X^2 + 1 = 0$ *em* $\mathbb{Q}_5$.

Note que $g(X) = X^2 + 1 \in V_5[X]$.

Projetamos $\overline{g}(X) = X^2 + \overline{1} \in \mathbb{F}_5[X]$.

Como $\overline{2} \in \mathbb{F}_5$ é raíz simples de $\overline{g}$, então pelo Lema de Hensel, existe $a \in V_5$ tal que $g(a) = 0$ e $\overline{a} = \overline{2}$

Exemplo

Resolver a equação $X^2 + 1 = 0$ *em* $\mathbb{Q}_5$.

Note que $g(X) = X^2 + 1 \in V_5[X]$.

Projetamos $\overline{g}(X) = X^2 + \overline{1} \in \mathbb{F}_5[X]$.

Como $\overline{2} \in \mathbb{F}_5$ é raíz simples de $\overline{g}$, então pelo Lema de Hensel, existe $a \in V_5$ tal que $g(a) = 0$ e $\overline{a} = \overline{2}$

$$a = 2 + a_1 5 + a_2 5^2 + a_3 5^3 + \ldots$$

Princípio local-global de Hasse

Teorema

Seja $f(X_1, \ldots, X_n) = a_1X_1^2 + \ldots + a_nX_n^2$ uma forma quadrática com coeficientes em $\mathbb{Q}$. Então $f(X_1, \ldots, X_n) = 0$ tem solução não trivial em $\mathbb{Q}$ se e somente se $f(X_1, \ldots, X_n) = 0$ tem solução não trivial em $\mathbb{R}$ e em $\mathbb{Q}_p$ para cada primo p.

Exemplo

$$f(X_1, X_2, X_3) = 5X_1^2 + 7X_2^2 - 13X_3^2 = 0.$$

Exemplo

$f(X_1, X_2, X_3) = 5X_1^2 + 7X_2^2 - 13X_3^2 = 0.$

- $\mathbb{R}$,

$$(X_1, X_2, X_3) = \left(1, 0, \sqrt{\frac{5}{13}}\right).$$

Exemplo

$f(X_1, X_2, X_3) = 5X_1^2 + 7X_2^2 - 13X_3^2 = 0.$

- $\mathbb{R}$,

$$(X_1, X_2, X_3) = \left(1, 0, \sqrt{\frac{5}{13}}\right).$$

- $\mathbb{Q}_5$,
  Em $\mathbb{F}_5$, temos

$$\overline{f} = \overline{7}X_2^2 - \overline{13}X_3^2 = \overline{2}X_2^2 + \overline{2}X_3^2,$$

que tem solução $X_2 = \overline{2}$, $X_3 = \overline{1}$. Considere o polinômio

$$g(X) = 7X^2 - 13 \in V_5[X].$$

Como $\overline{2}$ é raíz simples de $\overline{g}$, então pelo Lema de Hensel, existe $a \in V_5$ tal que $g(a) = 0$ e $\overline{a} = \overline{2}$. Segue que

$$f(0, a, 1) = 7a^2 - 13 = 0.$$

- $\mathbb{Q}_7$,
  Em $\mathbb{F}_7$, temos

$$\overline{f} = \overline{5}X_1^2 - \overline{13}X_3^2 = \overline{5}X_1^2 + X_3^2,$$

que tem solução $X_2 = \overline{2}$, $X_3 = \overline{1}$. Considere o polinômio

$$g(X) = 5X^2 - 13 \in V_7[X].$$

Como $\overline{2}$ é raíz simples de $\overline{g}$, então pelo Lema de Hensel, existe $a \in V_7$ tal que $g(a) = 0$ e $\overline{a} = \overline{2}$. Segue que

$$f(a, 0, 1) = 5a^2 - 13 = 0.$$

- $\mathbb{Q}_{13}$,
  Em $\mathbb{F}_{13}$, temos
  $$\overline{f} = \overline{5}X_1^2 + \overline{7}X_2^2,$$
  que tem solução $X_2 = \overline{3}$, $X_3 = \overline{1}$. Considere o polinômio
  $$g(X) = 5X^2 + 7 \in V_{13}[X].$$
  Como $\overline{3}$ é raíz simples de $\overline{g}$, então pelo Lema de Hensel, existe $a \in V_{13}$ tal que $g(a) = 0$ e $\overline{a} = \overline{3}$. Segue que
  $$f(a, 1, 0) = 5a^2 + 7 = 0.$$

- $\mathbb{Q}_2$,
  Considere o polinômio

$$g(X) = 5X^2 - 13 \in V_2[X].$$

Note que $g(1) = -8$, logo $v_2(g(1)) = 3$.
Por outro lado, $g'(1) = 10$, logo $v_2(g'(1)) = 1$.
Como $v_2(g(1)) > 2v_2(g'(1))$, segue pelo Lema de Hensel que existe $a \in V_2$ tal que $g(a) = 0$ e $\overline{a} = \overline{1}$. Segue que

$$f(a, 0, 1) = 5a^2 - 13 = 0.$$

- $\mathbb{Q}_p$, $p \neq 2, 5, 7, 13$.

- $\mathbb{Q}_p$, $p \neq 2, 5, 7, 13$.

Lema

Seja $f(X_1, \ldots, X_n) = a_1 X_1^2 + \ldots + a_n X_n^2$ uma forma quadrática com coeficientes em um corpo finito $\mathbb{F}_q$. Se $n \geq 3$, então $f(X_1, \ldots, X_n) = 0$ tem solução não trivial em $\mathbb{F}_q$.

- $\mathbb{Q}_p$, $p \neq 2, 5, 7, 13$.

Lema

Seja $f(X_1, \ldots, X_n) = a_1X_1^2 + \ldots + a_nX_n^2$ uma forma quadrática com coeficientes em um corpo finito $\mathbb{F}_q$. Se $n \geq 3$, então $f(X_1, \ldots, X_n) = 0$ tem solução não trivial em $\mathbb{F}_q$.

Em $\mathbb{F}_p$ a equação

$$\overline{5}X_1^2 + \overline{7}X_2^2 - \overline{13}X_3^2 = 0$$

tem solução não trivial, digamos $(\overline{a}, \overline{b}, \overline{c})$. Suponhamos que $\overline{a} \neq 0$, isto é, p não divide a. Considere o polinômio

$$g(X) = 5X^2 + 7b^2 - 13c^2 \in V_p[X].$$

Note que $g(a) \in M_p$, isto é, $v_p(g(a)) > 0$. Por outro lado, $g'(a) = 10a$, o que implica $v_p(g'(a)) = 0$.

Como $v_p(g(a)) > 2v_p(g'(a))$, segue pelo Lema de Hensel que existe $\alpha \in V_p$ tal que $g(a) = 0$ e $\overline{\alpha} = \overline{a}$.
Segue que

$$f(\alpha, b, c) = 5\alpha^2 + 7b^2 - 13c^2 = 0.$$

Como $v_p(g(a)) > 2v_p(g'(a))$, segue pelo Lema de Hensel que existe $\alpha \in V_p$ tal que $g(a) = 0$ e $\overline{\alpha} = \overline{a}$.
Segue que

$$f(\alpha, b, c) = 5\alpha^2 + 7b^2 - 13c^2 = 0.$$

Portanto, como a equação

$$5X_1^2 + 7X_2^2 - 13X_3^2 = 0$$

tem solução não trivial em $\mathbb{R}$ e em $\mathbb{Q}_p$ para todo primo p, esta tem solução não trivial em $\mathbb{Q}$.


Bachman, G. *Introduction to p-Adic Numbers and Valuation Theory*. Academic Press, New York, 1964.


Engler, A. J.; Prestel, A. *Valued fields.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.


Gouvêa, F. Q. *Primeiros Passos P-ádicos*. Rio de Janeiro: IMPA, 1989.


Serre, J-P, *A Course in Arithmetic.* Springer Monographs in Mathematics. Springer-Verlag, 3ed. 1996.

Obrigado!