Teorema de Ostrowski

Prof. Dr. Plamen Emilov Kochloukov

10 de março de 2016

Definição. Seja $f : K \to \mathbb{R}_+ \cup \infty$ uma função, em que K é um corpo qualquer, satisfazendo:

(i) $f(x) = 0$ se e somente se $x = 0$.

(ii) $f(xy) = f(x)f(y)$.

(iii) $f(x + y) \leq f(x) + f(y)$.

Denominamos f um **valor absoluto** para K, ou uma norma para K.

Proposição. *Seja f um valor absoluto para K. Então:*

(a) $f(1) = f(-1) = 1$.

(b) $f(n) \leq n$, *para todo* $n = 1 + 1 + \cdots + 1 \in K$, *em que* $n < charK$.

Demonstração. (a) Da condição (ii) da definição, temos $f(1) = f(1^2) = f(1)f(1)$, e daí, $f(1) = 0$ ou $f(1) = 1$. Mas sabe-se que $f(1) \neq 0$ por (i).

Agora, $f(-1)f(-1) = f((-1)(-1)) = f(1) = 1$, e daí, $f(-1) = 1$ ou $f(-1) = -1$. Mas, sabe-se que $f(-1) > 0$.

(b) Do item (iii) da definição, segue que

$$f(n) = f(1 + 1 + \cdots + 1) \leq f(1) + f(1) + \cdots + f(1) = n.$$

□

Exemplo. *São normas no conjunto dos números racionais $\mathbb{Q}$:*

(1) $|\cdot|$, *valor absoluto usual.*

(2) $|\cdot|^\alpha$, *norma usual com potência* α, *em que* $0 \leq \alpha \leq 1$. *Quando* $\alpha = 0$, *a notação* $|\cdot|^\alpha$ *denota a norma trivial, isto é:*

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

(3) Seja $p \in \mathbb{N}$ um número primo. Para cada $\frac{m}{n} \in \mathbb{Z}$, escreva $\frac{m}{n} = p^t \frac{a}{b}$, em que p não divide a e nem b. Então, define-se $\left|\frac{m}{n}\right|_p = p^{-t}$, denominado a ***norma p-ádica*** *em $\mathbb{Q}$.*

(4) $|\cdot|_p^\alpha$, com $\alpha \geq 0$.

Deve-se mencionar que se f é uma norma em $\mathbb{Q}$, então o conhecimento de f em $\mathbb{N}$ completamente define a norma sobre $\mathbb{Q}$. De fato:

- Para cada $n \in \mathbb{N}$, temos que $f(-n) = f(-1)f(n) = f(n)$, e daí, conhece-se f em $\mathbb{Z}$;
- Dado $z \in \mathbb{Z}$, temos $1 = f(1) = f(zz^{-1}) = f(z)f(z^{-1})$, e daí, $f(z^{-1}) = f(z)^{-1}$, e conhece-se $f(z^{-1})$ para todo $z \in \mathbb{Z}$;
- Por fim, dado $p/q \in \mathbb{Q}$, temos que $f(p/q) = f(p)f(q^{-1}) = f(p)f(q)^{-1}$, e isso prova a afirmação.

Teorema (Ostrowski)**.** *As normas apresentadas em (2) e (4) do exemplo anterior são todas normas possíveis em $\mathbb{Q}$.*

Demonstração. **Caso 1:** Existe $n \in \mathbb{N}$ com $f(n) < 1$.

Seja n o menor positivo com essa propriedade. Temos $n > 1$, pois $f(1) = 1$.

Por condição (ii) da definição de valor absoluto, necesssariamente n deve ser primo, $n = p$.

Seja $b \in \mathbb{N}$, e escreva $b = b_0 + b_1 p + \cdots + b_k p^k$, com $0 \leq b_i \leq p-1$, para cada $i = 0, 1, 2, \cdots, k$ e $b_k \neq 0$. Temos $f(b) \leq f(b_0) + \cdots + f(b_k) \leq (k+1)(p-1)$. Mas $k \leq \frac{\log b}{\log p}$. Daí

$$f(b)^n = f(b^n) \leq \left(n\frac{\log b}{\log p} + 1\right)(p-1).$$

Tomando o limite $n \to \infty$, $f(b) \leq 1$, para todo $b \in \mathbb{Z}$.

Seja $b \in \mathbb{N}$ tal que p não divide b. Então $(p^n, b^n) = 1$, para todo $n \in \mathbb{N}$, e daí, existem $x_n, y_n \in \mathbb{Z}$ tais que $x_n p^n + y_n b^n = 1$. Segue que

$$1 = f(1) \leq f(x_n p^n) + f(y_n b^n) \leq f(p)^n + f(b^n), \forall n \in \mathbb{N},$$

e isso implica necessariamente $f(b) = 1$.

Como consequência, $f = |\cdot|_p^\alpha$, e então, f é do tipo (4).

Caso 2: $f(n) \geq 1$, para todo $n \in \mathbb{N}$. Sejam $a, b \in \mathbb{N}$, $a, b \geq 2$, e escreva

$$b = b_0 + b_1 a + \cdots + b_k a^k, 0 \leq b_i < a, i = 1, 2, \cdots, k, b_k \neq 0.$$

Temos

$$f(b) \leq (a-1)(1+f(a)+\cdots+f(a)^k) \leq (a-1)(k+1)f(a)^k \leq (a-1)\left(1 + \frac{\log b}{\log a}\right) f(a)^{\frac{\log b}{\log a}}.$$

Daí

$$f(b)^n = f(b^n) \leq (a-1)\left(1 + n\frac{\log b}{\log a}\right) f(a)^{n\frac{\log b}{\log a}}.$$

Fazendo $n \to \infty$, segue que $f(b) \leq f(a)^{\frac{\log b}{\log a}}$.

Da mesma forma, temos $f(a) \leq f(b)^{\frac{\log a}{\log a}}$, e daí $f(a)^{\frac{1}{\log a}} = f(b)^{\frac{1}{\log b}}$, para todo $a, b \in \mathbb{N}$, $a, b \geq 2$.

Escrevendo $f(2) = 2^{\alpha}$ (necessariamente $0 \leq \alpha \leq 1$), segue que $f(n) = n^{\alpha}$, para todo $n \in \mathbb{N}$, e esse é exatamente o caso (2). □

Valoração. Seja K um corpo, um mapa $v : K \to \mathbb{R} \cup \{\infty\}$ é denominado valoração se:

(i) $v(xy) = v(x) + v(y), \forall x, y \in K$,

(ii) $v(x) = \infty$ se e somente se $x = 0$,

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

Algumas propriedades:

1. Sejam v valoração em K e $c \in \mathbb{R}$, $c > 1$. Então o mapa

$$f : x \in K \mapsto c^{-v(x)} \in \mathbb{R}$$

é valor absoluto.

2. Os valores absolutos definidos no item 1 satisfazem a denominada **desigualdade ultramétrica** (ou seja, a norma é não-arquimediana). (Vale a recíproca desta afirmação!)

Definição. Denomina-se $\operatorname{Im} v$ o grupo da valoração de v e o anel da valoração é definido por $\{x \in K | v(x) \geq 0\}$.

Exercícios:

1. Quais os valores absolutos em K, se K for finito?

2. Qual seria uma valoração p-ádica em $\mathbb{Q}$ (isto é, uma valoração que origina as normas p-ádicas)?

Spoiler (soluções):

1. Se K é finito, então para cada $x \in K$ não nulo, existe uma potência $x^t = 1$ com $t \geq 1$, e daí, necessariamente a única norma possível em K é a trivial.

2. Dados $m, n \in \mathbb{Z}$, escreva $\frac{m}{n} = p^k \frac{a}{b}$, com p não dividindo nem a e nem b. Então, definindo $v_p\left(\frac{m}{n}\right) = k$, obtém-se uma valoração que define uma norma p-ádica em $\mathbb{Q}$.

Aplicações e discussões. Um dos resultados clássicos e conhecidos do passado da teoria de anéis associativos é o seguinte: dado uma álgebra associativa A de dimensão finita sobre um corpo algebricamente fechado C, existe um ideal nilpotenten $N \subset A$ (o ideal contendo todos os ideais nil de A) tal que $A/N \simeq \oplus M_{n_i}(C)$.

Mais tarde, essa teoria foi estendida para um contexto mais geral, em que substitui-se o termo "álgebra" para anel, e substitui a condição de "dimensão finita" para uma condição de cadeias finitas de ideais, e obtém-se que todo anel R satisfazendo tais condições admite um ideal J tal que R/J é a soma direta de anéis de matrizes sobre anéis de divisão (Teorema conhecido hoje pelo nome de Wedderburn e Artin).

Antes disso, na tentativa de estudar o que seria um "anel simples" (por exemplo, $A/N \simeq \oplus M_{n_i}(C)$ na notação acima, ou seja, uma álgebra quebra como soma de anéis de matrizes - neste caso, anéis de matrizes seriam, em algum sentido, os objetos mais simples), chega-se ao conceito de anéis primitivos. Jacobson define o conceito de **anel primitivo** de forma dependente de módulos à direita. Poderíamos, da mesma forma, definir o conceito de primitividade utilizando-se módulos à esquerda, obtendo assim o conceito de **primitivo à esquerda**.

Uma questão natural que ficou em aberto por um tempo é se as duas noções são equivalentes, ou seja, se primitividade à direita (isto é, o conceito original de primitividade) coincide com o conceito de primitivo à esquerda.

Bergman, em 1964, obteve uma solução negativa a esse problema: apresentou um exemplo de um anel primitivo à direita, mas não primitivo à esquerda. Para essa construção, utilizou-se fortemente o conceito de valoração. Assim, obtém-se também aplicações da teoria de valoração em anéis não-comutativos.