p-adic numbers

Petr Nižnanský

Department of Algebra
Faculty of Mathematics and Physics
Charles University in Prague

12. 4. 2013 / Spring School of Algebra

Definition

Let X be a set. The function $d\colon X \times X \to [0, \infty)$ is a *metric* on X if the following holds:

1. $d(x, y) = 0 \iff x = y$.
2. $d(x, y) = d(y, x)$.
3. $d(x, y) \leq d(x, z) + d(z, y)$ for all $z \in X$.

A set X together with metric d is called a *metric space*.

Definition

Let F be a field. The function $\|\ \|\colon F \to [0, \infty)$ is a *norm* on F if the following holds:

1. $\| x \| = 0 \iff x = 0$.
2. $\| x \cdot y \| = \| x \| \cdot \| y \|$.
3. $\| x + y \| \leq \| x \| + \| y \|$.

Definition

Let $p \in \mathbb{P}$ be any prime number ($\mathbb{P}$ is set of all prime numbers). The *p-adic valuation* (or *p-adic order*) is defined as $\nu_p \colon \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$

$$\nu_p(x) = \begin{cases} \max\{v \in \mathbb{N}_0 | p^v \text{ divides } x\} & \text{if } x \neq 0 \\ \infty & \text{if } x = 0. \end{cases}$$

We can naturally extend p-adic valuation on rational numbers $\mathbb{Q}$ as follows: let $x = a/b$ then $\nu_p(x) = \nu_p(a) - \nu_p(b)$.

Example

$\nu_3(5) = 0, \nu_2(12) = 2, \nu_5(1/5) = -1.$

Proposition

Let $|\ |_p$ be a map on $\mathbb{Q}$ as follows:

$$|x|_p = \begin{cases} (\frac{1}{p})^{\nu_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

Then $|\ |_p$ is a norm on $\mathbb{Q}$.

Proof.

Properties (1) and (2) are trivial and the triangular inequality is easy exercise :-) $\square$

Definition

The sequence $a_1, a_2, \ldots$ is *Cauchy* if

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall m, n > N \colon d(a_m, a_n) < \varepsilon.$$

Definition

Two metrics d_1 and d_2 on a set X are *equivalent* if a sequence is Cauchy with respect to d_1 if and only if it is Cauchy with respect to d_2 and two norms are *equivalent* if they induce equivalent metrics.

Proposition

Let $\| \ \|_1$ and $\| \ \|_2$ be two norms such that $\| \ \|_1 = \| \ \|_2^{\alpha}$ for some positive real α. Then they are equivalent.

Proof (sketch)

- let $a_1, a_2, \ldots$ be a Cauchy sequence with respect to $\| \ \|_1$
- for $\varepsilon > 0$ find $\overline{N}$ such that $\| a_m - a_n \|_1 < \varepsilon^{\alpha}$
- then for $\varepsilon > 0, \exists \overline{N} \in \mathbb{N}, \forall m, n > \overline{N}: \ \| a_m - a_n \|_1 = \| a_m - a_n \|_2^{\alpha} < \varepsilon^{\alpha}$
- similar to other side

Theorem (Ostrowski)

Every nontrivial norm $\| \ \|$ on $\mathbb{Q}$ is equivalent to $| \ |_p$ for some prime p or is equivalent to the absolute value $| \ |$.

Proof

Case (i): suppose there exists positive integer n such that $\| n \| > 1$.

- let n_0 be the least such n
- there exists α : $\| n_0 \| = n_0^{\alpha}$
- $n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s$

$$
\begin{aligned}
\| n \| &\leq \| a_0 \| + \| a_1 n_0 \| + \| a_2 n_0^2 \| + \cdots + \| a_s n_0^s \| \\
&= \| a_0 \| + \| a_1 \| n_0^{\alpha} + \| a_2 \| n_0^{2\alpha} + \cdots + \| a_s \| n_0^{s\alpha} \\
&\leq 1 + n_0^{\alpha} + n_0^{2\alpha} + \cdots + n_0^{s\alpha} \\
&= n_0^{s\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-s\alpha})
\end{aligned}
$$

$$
\begin{aligned}
&= n_0^{s\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \dots + n_0^{-s\alpha}) \\
&\leq n^{\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \dots + n_0^{-s\alpha}) \\
&\leq n^{\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \dots + n_0^{-s\alpha} + \dots) \\
&= n^{\alpha}\left(\sum_{i=0}^{\infty}(1/n_0^{\alpha})^i\right) = n^{\alpha} C
\end{aligned}
$$

- $\| n \| \leq n^{\alpha} C$, for some constant C
- $\| n^N \| \leq n^{\alpha N} C$
- $\| n \| \leq \sqrt[N]{C} n^{\alpha}$ for $N \to \infty$ we have $\| n \| \leq n^{\alpha}$

- $n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s$
- $n_0^{s+1} > n \geq n_0^s$
- $\| n_0^{s+1} \| = \| n + n_0^{s+1} - n \| \leq \| n \| + \| n_0^{s+1} - n \|$

$$\begin{aligned} \| n \| &\geq \| n_0^{s+1} \| - \| n_0^{s+1} - n \| \\ &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^\alpha \\ &= n_0^{(s+1)\alpha}(1 - (1 - 1/n_0)^\alpha) \\ &\geq n^\alpha K \end{aligned}$$

- same as before $\| n \| \geq \sqrt[N]{K} n^\alpha \implies \| n \| \geq n^\alpha$
- hence $\| n \| = n^\alpha$ for any positive integer
- from (2) we have $\| x \| = |x|^\alpha$ for any $x \in \mathbb{Q}$

Case (ii)

- suppose that $\| n \| \leq 1$ for all positive integers n
- let n_0 be the least such n that $\| n \| < 1$
- n_0 is prime, if $n_0 = n_1 \cdot n_2$ then $\| n_0 \| = \| n_1 \| \cdot \| n_2 \| = 1$
- denote $p = n_0$
- we claim $\| q \| = 1$ if q is prime not equal to p
- if not $\| q \| < 1$ and there exists N such that $\| q^N \| < 1/2$
- for p exists M such that $\| p^M \| < 1/2$
- $1 = \| 1 \| = \| mp^M + nq^N \| \leq \| m \| \| p^M \| + \| n \| \| q^N \| \leq \| p^M \| + \| q^N \| < 1/2 + 1/2 = 1$
- hence $\| q \| = 1$

- for any $a \in \mathbb{Q}$ we have $a = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r}$
- $\| a \| = \| p_1 \|^{b_1} \cdot \| p_2 \|^{b_2} \dots \| p_r \|^{b_r}$
- $\| a \| = \| p \|^{\nu_p(a)}$
- there exists ε such that $(1/p)^{\varepsilon} = \| p \|$
- hence $\| \ \|$ is equivalent to $| \ |_p$
- QED

Proposition

Let $a \in \mathbb{Q}$, and $a \neq 0$ then

$$|a| \prod_{p \in \mathbb{P}} |a|_p = 1.$$

Proof.

- let $a = \pm p_1^{\nu_{p_1}(a)} \cdot p_2^{\nu_{p_2}(a)} \dots p_k^{\nu_{p_k}(a)}$.
-

$$\begin{aligned} |a| \prod_{p \in \mathbb{P}} |a|_p = {} & p_1^{\nu_{p_1}(a)} \cdot p_2^{\nu_{p_2}(a)} \dots p_k^{\nu_{p_k}(a)} \\ & \cdot (1/p_1)^{\nu_{p_1}(a)} \cdot (1/p_2)^{\nu_{p_2}(a)} \dots (1/p_k)^{\nu_{p_k}(a)} \\ = {} & 1 \end{aligned}$$

$\square$

Thank you for your attention.