proof of Ostrowski's valuation theorem

Canonical name	ProofOfOstrowskisValuationTheorem
Date of creation	2013-03-22 17:58:26
Last modified on	2013-03-22 17:58:26
Owner	rm50 (10146)
Last modified by	rm50 (10146)
Numerical id	4
Author	rm50 (10146)
Entry type	Proof
Classification	msc 13A18

This article proves Ostrowski's theorem on valuations of $\mathbb{Q}$, which states:

Theorem 1. *(Ostrowski) Over $\mathbb{Q}$, every nontrivial absolute value is equivalent either to $|\cdot|_p$ for some prime p, or to the usual absolute value $|\cdot|_\infty$.*

We start with an estimation lemma:

Lemma 2. *If $m, n > 1$ are integers and $|\cdot|$ any nontrivial absolute value on $\mathbb{Q}$, then $|m| \leq \max(1, |n|)^{\log m/\log n}$.*

Proof. Write $m = a_0 + a_1 n + \cdots + a_r n^r$ for $a_i \in \mathbb{Z}, 0 \leq a_i \leq n-1$, and with $a_r \neq 0$. Then clearly

$$|a_i| = \left|\underbrace{1 + \cdots + 1}_{a_i}\right| \leq a_i \, |1| = a_i \leq n$$

by the triangle inequality; also, $r < \frac{\log m}{\log n}$.

Thus

$$\begin{aligned} |m| = |a_0 + a_1 n + \cdots + a_r n^r| &\leq (r+1) n \max(1, |n|)^r \\ &\leq \left(1 + \frac{\log m}{\log n}\right) n \max(1, |n|)^{\log m/\log n} \end{aligned}$$

Replace m by m^t for t a positive integer, and take t^{th} roots of the resulting inequality, to get

$$|m| \leq \left(1 + t\frac{\log m}{\log n}\right)^{1/t} n^{1/t} \max(1, |n|)^{\log m/\log n}$$

Now let $t \to \infty$; the first two factors each approach 1, and the lemma follows.

Proof of Ostrowski's theorem:

First assume that for every $n > 1$ we have $|n| > 1$. Then by the lemma, $|m| \leq |n|^{\log m/\log n}$, so that for every m, n we have

$$|m|^{1/\log m} \leq |n|^{1/\log n}$$

Since this holds for every $m, n > 0$, after reversing the roles of m, n, we see that in fact equality holds, so that for every m, $|m|^{1/\log m} = c$ and $|m| = c^{\log m}$ for some constant c; this absolute value is obviously equivalent to $|m|_\infty = e^{\log m}$.

If instead, for some $n > 1$ we have $|n| < 1$, then by the lemma, for every m, $|m| \leq 1$. Thus the absolute value is nonarchimedean. Define $A = \{x \in \mathbb{Q} \ \mid \ |x| \leq 1\}$ and let $\mathfrak{m} \subset A$ be the (unique) maximal ideal defined by $\mathfrak{m} = \{x \in \mathbb{Q} \ \mid \ |x| < 1\}$. Then $\mathbb{Z} \subset A$ since $|m| \leq 1$ for every m, and $\mathfrak{m} \cap \mathbb{Z}$ is nonzero since otherwise the valuation would be trivial (we would have $|m| = 1$ for every m). Thus $\mathfrak{m} \cap \mathbb{Z}$ is prime since $\mathfrak{m}$ is, so is equal to (p) for some rational prime p. Now, if $p \nmid a$ for an integer a, then $|a|$ cannot be strictly less than 1 (else it would be in (p)), so $|a| = 1$ and $a \in A^\star$. But given any $x \in \mathbb{Q}$, we can write $x = \frac{ap^t}{b}$ with a, b prime to p, so that

$$|x| = \frac{|a| \cdot |p|^t}{|b|} = |p|^t$$

so that the valuation is obviously equivalent to the p-adic valuation.