CHAPTER 1

Ostrowski's Theorem

The field of real numbers $\mathbb{R}$ is constructed from the field of the rational numbers by completion of the metric space $(\mathbb{Q}, d_\infty)$ for d_∞ the distance induced by the usual (archimedean) absolute value

$$d_\infty(x,y) = |x-y|_\infty,\ \ |x|_\infty := \max(x,-x).$$

This absolute value is one way to measure the size (or complexity) of the rational numbers, but there are many others.

DEFINITION 1.1. *An* absolute value *(or* valuation*) on $\mathbb{Q}$ is a map*

$$|\cdot| : \mathbb{Q} \to \mathbb{R}_{\geqslant 0}$$

satisfying

- *(non-degeneracy) $|x| = 0 \Leftrightarrow x = 0$,*
- *(multiplicativity) $|xy| = |x||y|$; in particular for every $x \in \mathbb{Q}$, $|-x| = |x|$.*
- *(triangle inequality) $|x+y| \leqslant |x| + |y|$.*

Examples of absolute values include the usual *archimedean* absolute value $|\cdot|_\infty$; another example is the *trivial* absolute value

$$|x|_0 = |x|_\infty^0 = \delta_{x\neq 0}.$$

By the non-degeneracy and multiplicativity, one sees that $|1| = 1$. If $|.|$ is an absolute value, then so is $|.|^a$ for any $a \in]0,1]$. This fact prompts the following definition:

DEFINITION 1.2. *Two absolute values $|.|_1$, $|.|_2$ are said to be* equivalent *if there exists $a > 0$ such that $|.|_2 = |.|_1^a$.*

This defines an equivalence relation and the equivalence class of the trivial absolute value is reduced to itself.

DEFINITION 1.3. *A* place *of $\mathbb{Q}$ is an equivalence class of non-trivial absolute values. The set of places of $\mathbb{Q}$ is denoted $\mathcal{V}_\mathbb{Q}$.*

THEOREM 1.1 (Ostrowski). *The set $\mathcal{V}_\mathbb{Q}$ is in bijection with*

$$\mathcal{P} \cup \{\infty\},$$

where $\mathcal{P} = \{2,3,5,7,\cdots\}$ denotes the set of prime numbers. A representative for each place is given by

- *The archimedean absolute value $|.|_\infty$*
- *For p a prime number, $|x|_p = p^{-v_p(x)}$ where $v_p(x)$ denote the p-adic valuation*

$$v_p(x) = \sup\{k \in \mathbb{Z},\ \exists a,b \in \mathbb{Z},\ (b,p) = 1,\ p^{-k}x = \frac{a}{b}\} \in \mathbb{Z} \cup \{+\infty\}$$
$$= \begin{cases} +\infty & \text{if } x = 0, \\ k & \text{if } x = p^k a/b \text{ for some nonzero } a,b \in \mathbb{Z} \text{ with } p \nmid a, p \nmid b. \end{cases}$$

Proof. Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. Since $|.|$ is multiplicative and satisfies $|1| = 1$, it suffices to determine $|m|$ for each $m \in \mathbb{N}_{>1}$.

We begin by establishing, for each $m, m' > 1$, a relationship between $|m'|$ and $|m|$. For each $n \geqslant 1$, we have

$$|m'| = |(m')^n|^{1/n}.$$

We decompose m'^n in base m as the sum

$$m'^n = \sum_{k=0}^{K} r_k m^k \quad \text{for some } 0 \leqslant r_k < m,$$

where $K \leqslant 1 + \frac{\log(m'^n)}{\log m} = 1 + \frac{n \log m'}{\log m}$. Let $R = \max\{|r|,\ r = 0, \ldots, m-1\}$, which is an upper bound for the absolute values of the coefficients appearing in this sum. By the triangle inequality, we have

$$|m'| \leqslant R^{1/n}(1+K)^{1/n} \max(1, |m|)^{K/n} \leqslant R^{1/n}(2 + \frac{n \log m'}{\log m})^{1/n} \max(1, |m|)^{1/n + \frac{\log m'}{\log m}}.$$

Letting $n \to +\infty$, it follows that

$$|m'| \leqslant \max(1, |m|)^{\frac{\log m'}{\log m}}.$$

Suppose now that $|m'| > 1$ for some $m' \in \mathbb{Z}$. Since $|m'| \leqslant 1$ for $m' \in \{-1, 0, 1\}$ and $|m'| = |-m'|$, we may and shall assume that $m' > 1$. The above inequality implies that for every $m > 1$, one has $|m| > 1$. Reversing the roles of m and m', we deduce that

$$|m'| = |m|^{\frac{\log m'}{\log m}}.$$

In other words, the function $m \mapsto |m|^{1/\log m}$ is constant. Let us write the value it takes as e^a, which is > 1 by our supposition. Then

$$|m| = |m|_\infty^a$$

for each $m > 1$. By the reduction noted above, it follows that $|.|$ is equivalent to $|.|_\infty$.

It remains to consider the case that every $m \in \mathbb{Z}$ satisfies $|m| \leqslant 1$. In that case, we observe that for $a, b \in \mathbb{Q}$ and $n \geqslant 1$, one has

$$|a+b| = |(a+b)^n|^{1/n} \leqslant (\sum_{k=0}^{n} |C_n^k||a|^k|b|^{n-k})^{1/n} \leqslant (n+1)^{1/n} \max(|a|^n, |b|'n)^{1/n}.$$

Letting $n \to +\infty$, we obtain

$$|a+b| \leqslant \max(|a|, |b|). \tag{0.1}$$

Since $|.|$ is non-trivial, there exists $m > 1$ such that $|m| < 1$. We choose such an m of minimal size with respect to the usual archimedean absolute value. If m factors as $m = ln$ with $l, n > 1$, then $|ln| = |l||n| < 1$, so that either $|l|$ or $|n|$ is < 1, contradicting minimality. Therefore $m = p$ is a prime.

With p as above, consider any other value of $m \in \mathbb{Z}$ satisfying $|m| < 1$. We wish to show that p divides m. By division with remainder, we may write $m = kp + r$ for some integers k, r with $0 \leqslant r < p$. Suppose $r \neq 0$. Our earlier assumption ($|r| \leqslant 1$) and the minimality of p imply that $|r| = 1$. By (0.1) and the inequality $|k||p| \leqslant |p| < 1$, we deduce

$$1 = |r| \leqslant \max(|k||p|, |m|) < 1.$$

Therefore $r = 0$, i.e., p divides m. In summary,

$$\{m \in \mathbb{Z},\ |m| < 1\} = p\mathbb{Z},$$

or put another way,

$$|m| = 1 \text{ if and only if } (m,p) = 1.$$

We may factor a general $m \neq 0, \pm 1$ as

$$m = ap^{v_p(m)},\ (a,p) = 1$$

where

$$v_p(m) = \max\{k \in \mathbb{N},\ p^k | m\}$$

is the p-adic valuation of m. Then

$$|m| = |a||p|^{v_p(m)} = |m|_p^{-\frac{\log |p|}{\log p}}.$$

Observe that this identity remain valid for $m = 0, \pm 1$ since $v_p(0) = \infty$, $v_p(\pm 1) = 0$.

It remains to verify that $|.|_p$ is indeed an absolute value. This is a consequence of the following easily verified properties of the p-adic valuation v_p:

- $v_p(x) = +\infty \Leftrightarrow x = 0$,
- $v_p(xy) = v_p(x) + v_p(y)$,
- $v_p(x + y) \geqslant \inf(v_p(x), v_p(y))$.

□

The valuation $|\cdot|_p$ is called the *normalized* p-adic valuation, or simply "the p-adic valuation." Its called equivalence class is called the *p-adic place*; any valuation in this class will be called "p-adic." Observe that the set of p-adic valuations is precisely

$$\{|\cdot|_p^a,\ a \in \mathbb{R}_{>0}\}.$$

As we have seen from the proof, the absolute values in the class of $|.|_p$ satisfy the

(Ultrametric inequality). *For all $x, y \in \mathbb{Q}$*

$$|x + y| \leqslant \max(|x|, |y|).$$

This is stronger than the triangle inequality. It may also be seen to follow from the third property of the p-adic valuation $v_p(.)$.

Definition 1.4. *The absolute values equivalent to $|.|_\infty$ are called archimedean and the corresponding place is called archimedean or infinite while those equivalent to some $|\cdot|_p$ are called non-archimedean and the corresponding place non-archimedean or finite.*