5.1 The field of p-adic numbers

Definition 5.1. The field of *p-adic numbers* $\mathbb{Q}_p$ is the fraction field of $\mathbb{Z}_p$.

As a fraction field, the elements of $\mathbb{Q}_p$ are by definition all pairs $(a, b) \in \mathbb{Z}_p^2$, typically written as a/b, modulo the equivalence relation $a/b \sim c/d$ whenever $ad = bc$. But we can represent elements of $\mathbb{Q}_p$ more explicitly by extending our notion of a p-adic expansion to allow negative indices, with the proviso that only finitely many p-adic digits with negative indices are nonzero. If we view p-adic expansions in $\mathbb{Z}_p$ as formal power series in p, in $\mathbb{Q}_p$ we now have formal Laurent series in p.

Recall that every element of $\mathbb{Z}_p$ can be written in the form up^n, with $n \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}_p^\times$, and it follows that the elements of $\mathbb{Q}_p$ can all be written in the form up^n with $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. If $(b_0, b_1, b_2, \ldots)$ is the p-adic expansion of $u \in \mathbb{Z}_p^\times$, then the p-adic expansion of $p^n u$ is $(c_n, c_{n+1}, c_{n+2}, \ldots)$ with $c_{n+i} = b_i$ for all $i \geq 0$ and $c_{n-i} = 0$ for all $i < 0$ (this works for both positive and negative n).

We extend the p-adic valuation v_p to $\mathbb{Q}_p$ by defining $v_p(p^n) = n$ for any integer n; as with p-adic integers, the valuation of any p-adic number is just the index of the first nonzero digit in its p-adic expansion. We can then distinguish $\mathbb{Z}_p$ as the subset of $\mathbb{Q}_p$ with nonnegative valuations, and $\mathbb{Z}_p^\times$ as the subset with zero valuation. We have $\mathbb{Q} \subset \mathbb{Q}_p$, since $\mathbb{Z} \subset \mathbb{Z}_p$, and for any $x \in \mathbb{Q}_p$, either $x \in \mathbb{Z}_p$ or $x^{-1} \in \mathbb{Z}_p$. Note that analogous statement is not even close to being true for $\mathbb{Q}$ and $\mathbb{Z}$.

This construction applies more generally to the field of fractions of any discrete valuation ring, and a converse is true. Suppose we have a field k with a discrete valuation, which we recall is a function $v\colon k \to \mathbb{Z} \bigcup \{\infty\}$ that satisfies:

(1) $v(a) = \infty$ if and only if $a = 0$,

(2) $v(ab) = v(a) + v(b)$,

(3) $v(a + b) \geq \min(v(a), v(b))$.

The subset of k with nonnegative valuations is a discrete valuation ring R, called the *valuation ring of* k, and k is its fraction field. As with p-adic fields, the unit group of the valuation ring of k consists of those elements whose valuation is zero.

5.2 Absolute values

Having defined $\mathbb{Q}_p$ as the fraction field of $\mathbb{Z}_p$ and noting that it contains $\mathbb{Q}$, we now want to consider an alternative (but equivalent) approach that constructs $\mathbb{Q}_p$ directly from $\mathbb{Q}$. We can then obtain $\mathbb{Z}_p$ as the valuation ring of $\mathbb{Q}$.

Definition 5.2. Let k be a field. An *absolute value* on k is a function $\| \; \|\colon k \to \mathbb{R}_{\geq 0}$ with the following properties:

(1) $\|x\| = 0$ if and only if $x = 0$,

(2) $\|xy\| = \|x\| \cdot \|y\|$,

(3) $\|x + y\| \leq \|x\| + \|y\|$.

Andrew V. Sutherland

The last property is known as the *triangle inequality*, and it is equivalent to

(3) $\|x - y\| \geq \|x\| - \|y\|$

(replace x by $x \pm y$ to derive one from the other). The stronger property

(3') $\|x + y\| \leq \max(\|x\|, \|y\|)$

is known as the *nonarchimedean triangle inequality* An absolute value that satisfies (3') is called *nonarchimedean*, and is otherwise called *archimedean*.

Absolute values are sometimes called "norms", but since number theorists use this term with a more specific meaning, we will stick with absolute value. Examples of absolute values are the usual absolute value $| \ |$ on $\mathbb{R}$ or $\mathbb{C}$, which is archimedean and the *trivial absolute value* for which $\|x\| = 1$ for all $x \in k^\times$, which is nonarchimedean. To obtain non-trivial examples of nonarchimedean absolute values, if k is any field with a discrete valuation v and c is any positive real number less than 1, then it is easy to check that $\|x\|_v := c^{v(x)}$ defines a nonarchimedean absolute value on k (where we interpret c^∞ as 0). Applying this to the p-adic valuation v_p on $\mathbb{Q}_p$ with $c = 1/p$ yields the p-adic absolute value $| \ |_p$ on $\mathbb{Q}_p$:

$$|x|_p = p^{-v_p(x)}.$$

We now prove some useful facts about absolute values.

Theorem 5.3. *Let k be a field with absolute value $\| \ \|$ and multiplicative identity 1_k.*

(a) $\|1_k\| = 1$.

(b) $\| - x\| = \|x\|$.

(c) $\| \ \|$ *is nonarchimedean if and only if* $\|n\| \leq 1$ *for all positive integers* $n \in k$.

Proof. For (a), note that $\|1_k\| = \|1_k\| \cdot \|1_k\|$ and $\|1_k\| \neq 0$ since $1_k \neq 0_k$. For (b), the positive real number $\| - 1_k\|$ satisfies $\| - 1_k\|^2 = \|(-1_k)^2\| = \|1_k\| = 1$, and therefore $\| - 1_k\| = 1$. We then have $\| - x\| = \|(-1_k)x\| = \| - 1_k\| \cdot \|x\| = 1 \cdot \|x\| = \|x\|$.

To prove (c), we first note that a positive integer $n \in k$ is simply the n-fold sum $1_k + \cdots + 1_k$. If $\| \ \|$ is nonarchimedean, then for any positive integer $n \in k$, repeated application of the nonarchimedean triangle inequality yields

$$\|n\| = \|1_k + \cdots + 1_k\| \leq \max(\|1_k\|, \ldots, \|1_k\|) = 1.$$

If $\| \ \|$ is instead archimedean, then we must have $\|x+y\| > \max(\|x\|, \|y\|)$ for some $x, y \in k^\times$. We can assume without loss of generality that $\|x\| \geq \|y\|$, and if we divide through by $\|y\|$ and replace x/y with x, we can assume $y = 1$. We then have $\|x\| \geq 1$ and

$$\|x + 1\| > \max(\|x\|, 1) = \|x\|.$$

If we divide both sides by $\|x\|$ and let $z = 1/x$ we then have $\|z\| \leq 1$ and $\|z + 1\| > 1$. Now suppose for the sake of contradiction that $\|n\| \leq 1$ for all integers $n \in k$. then

$$\|z + 1\|^n = \|(z + 1)^n\| = \left\| \sum_{i=0}^{n} \binom{n}{i} z^i \right\| \leq \sum_{i=0}^{n} \left\| \binom{n}{i} \right\| \|z\|^i \leq \sum_{i=0}^{n} \left\| \binom{n}{i} \right\| \leq n + 1.$$

But $\|z + 1\| > 1$, so the LHS increases exponentially with n while the RHS is linear in n, so for any sufficiently large n we obtain a contradiction. □

Corollary 5.4. *In a field k of positive characteristic p every absolute value $\| \ \|$ is nonarchimedean and is moreover trivial if k is finite.*

Proof. Every positive integer $n \in k$ lies in the prime field $\mathbb{F}_p \subseteq k$ and therefore satisfies $n^{p-1} = 1$. This means the positive real number $\|n\|$ is a root of unity and therefore equal to 1, so $\|n\| = 1$ for all positive integers $n \in k$ and $\| \ \|$ is therefore nonarchimedean, by part (c) of Theorem 5.3. If $k = \mathbb{F}_q$ is a finite field, then for every nonzero $x \in \mathbb{F}_q$ we have $x^{q-1} = 1$ and the same argument implies $\|x\| = 1$ for all $x \in \mathbb{F}_q^\times$. □

5.3 Absolute values on $\mathbb{Q}$

As with $\mathbb{Q}_p$, we can use the p-adic valuation v_p on $\mathbb{Q}$ to construct an absolute value. Note that we can define v_p without reference to $\mathbb{Z}_p$: for any integer $v_p(a)$, is the largest integer n for which $p^n|a$, and for any rational number a/b in lowest terms we define

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

This of course completely consistent with our definition of v_p on $\mathbb{Q}_p$. We then define the *p-adic absolute value* of a rational number x to be

$$|x|_p = p^{-v_p(x)},$$

with $|0|_p = p^{-\infty} = 0$, as above. Notice that rational numbers with *large* p-adic valuations have *small* p-adic absolute values. In p-adic terms, p^{100} is a very small number, and p^{1000} is even smaller. Indeed,

$$\lim_{n\to\infty} |p^n| = \lim_{n\to\infty} p^{-n} = 0.$$

We also have the usual archimedean absolute value on $\mathbb{Q}$, which we will denote by $| \ |_\infty$, for the sake of clarity. One way to remember this notation is to note that archimedean absolute values are unbounded on $\mathbb{Z}$ while nonarchimedean absolute values are not (this follows from the proof of Theorem 5.3).

We now wish to prove Ostrowski's theorem, which states that every nontrivial absolute value on $\mathbb{Q}$ is equivalent either to one of the nonarchimedean absolute values $| \ |_p$, or to $| \ |_\infty$. We first define what it means for two absolute values to be equivalent.

Definition 5.5. Two absolute values $\| \ \|$ and $\| \ \|'$ on a field k are said to be *equivalent* if there is a positive real number α such that

$$\|x\|' = \|x\|^\alpha$$

for all $x \in k$.

Note that two equivalent absolute values are either both archimedean or both nonarchimedean, by Theorem 5.3 part (c), since $c^\alpha \le 1$ if and only if $c \le 1$, for any $c, \alpha \in \mathbb{R}_{>0}$.

Theorem 5.6 (Ostrowski)**.** *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to some $| \ |_p$, where p is either a prime, or $p = \infty$.*

Proof. Let $\| \ \|$ be a nontrivial absolute value on $\mathbb{Q}$. If $\| \ \|$ is archimedean then $\|b\| > 1$ for some positive integer b. Let b be the smallest such integer and let α be the positive real number for which $\|b\| = b^\alpha$ (such an α exists because we necessarily have $b > 1$). Every other positive integer n can be written in base b as

$$n = n_0 + n_1 b + n_2 b^2 + \cdots + n_t b^t,$$

with integers $n_i \in [0, b-1]$ and $n_t \neq 0$. We then have

$$\begin{aligned}
\|n\| &\le \|n_0\| + \|n_1 b\| + \|n_2 b^2\| + \cdots + \|n_t b^t\| \\
&= \|n_0\| + \|n_1\| b^\alpha + \|n_2\| b^{2\alpha} + \cdots + \|n_t\| b^{t\alpha} \\
&\le 1 + b^\alpha + b^{2\alpha} + \cdots + b^{t\alpha} \\
&= \left(1 + b^{-\alpha} + b^{-2\alpha} + \cdots + b^{-t\alpha}\right) b^{t\alpha} \\
&\le c b^{t\alpha} \\
&\le c n^\alpha
\end{aligned}$$

where c is the sum of the geometric series $\sum_{i=0}^\infty (b^{-\alpha})^i$, which converges because $b^{-\alpha} < 1$. This holds for every positive integer n, so for any integer $N \ge 1$ we have

$$\|n\|^N = \|n^N\| \le c(n^N)^\alpha = c(n^{\alpha N})$$

and therefore $\|n\| \le c^{1/N} n^\alpha$. Taking the limit as $N \to \infty$ we obtain

$$\|n\| \le n^\alpha,$$

for every positive integer n. On the other hand, for any positive integer n we can choose an integer t so that $b^t \le n < b^{t+1}$. By the triangle inequality $\|b^{t+1}\| \le \|n\| + \|b^{t+1} - n\|$, so

$$\begin{aligned}
\|n\| &\ge \|b^{t+1}\| - \|b^{t+1} - n\| \\
&= b^{(t+1)\alpha} - \|b^{t+1} - n\| \\
&\ge b^{(t+1)\alpha} - (b^{t+1} - n)^\alpha \\
&\ge b^{(t+1)\alpha} - (b^{t+1} - b^t)^\alpha \\
&= b^{(t+1)\alpha}\left(1 - (1 - b^{-1})^\alpha\right) \\
&\ge d n^\alpha
\end{aligned}$$

for some real number $d > 0$ that does not depend on n. Thus $\|n\| \ge d n^\alpha$ holds for all positive integers n and, as before, by replacing n with n^N, taking Nth roots, and then taking the limit as $N \to \infty$, we deduce that

$$\|n\| \ge n^\alpha,$$

and therefore $\|n\| = n^\alpha = |n|_\infty^\alpha$ for all positive integers n. For any other positive integer m,

$$\begin{aligned}
\|n\| \cdot \|m/n\| &= \|m\| \\
\|m/n\| &= \|m\| / \|n\| = m^\alpha / n^\alpha = (m/n)^\alpha,
\end{aligned}$$

and therefore $\|x\| = x^\alpha = |x|_\infty^\alpha$ for every positive $x \in \mathbb{Q}$, and $\|-x\| = \|x\| = x^\alpha = |-x|_\infty^\alpha$, so $\|x\| = |x|_\infty^\alpha$ for all $x \in \mathbb{Q}$ (including 0).

We now suppose that $\|\ \|$ is nonarchimedean. If $\|b\| = 1$ for all positive integers b then the argument above proves that $\|x\| = 1$ for all nonzero $x \in \mathbb{Q}$, which is a contradiction since $\| \ \|$ is nontrivial. So let b be the least positive integer with $\|b\| < 1$. We must have $b > 1$, so b is divisible by a prime p. If $b \neq p$ then $\|b\| = \|p\|\|b/p\| = 1 \cdot 1 = 1$, which contradicts $\|b\| < 1$, so $b = p$ is prime.

We know prove by contradiction that p is the only prime with $\|p\| < 1$. If not then let $q \neq p$ be a prime with $\|q\| < 1$ and write $up + vq = 1$ for some integers u and v, both of which have absolute value at most 1, since $\| \ \|$ is nonarchimedean.[1] We then have

$$1 = \|1\| = \|up + vq\| \leq \max(\|up\|, \|vq\|) = \max(\|u\| \cdot \|p\|, \|v\| \cdot \|q\|) \leq \max(\|p\|, \|q\|) < 1,$$

which is a contradiction.

Now define the real number $\alpha > 0$ so that $\|p\| = p^{-\alpha} = |p|_p^\alpha$. Any positive integer n may be written as $n = p^{v_p(n)}r$ with $v_p(r) = 0$, and we then have

$$\|n\| = \|p^{v_p(n)}r\| = \|p^{v_p(n)}\| \cdot \|r\| = \|p\|^{v_p(n)} = |p|_p^{\alpha v_p(n)} = |n|_p^\alpha.$$

This then extends to all rational numbers, as argued above. □

[1] This is a simplification of the argument given in class, as pointed out by Ping Ngai Chung (Brian).