Completions of $\mathbb{Q}$

September 4, 2016

1 From $\mathbb{Q}$ to $\mathbb{Q}_p$, the field of p-adic numbers

Let us define what a valuation is. Let F be a field. A *valuation* over F is a function $\mathcal{V}(\cdot)$ such that:

1. $\mathcal{V}(\cdot) : F \mapsto \mathbb{R}_+$, where $\mathbb{R}_+$ is the set of positive real numbers,
2. For $a, b \in F$, $\mathcal{V}(a \cdot b) = |a| \cdot |b|$, and
3. For $a, b \in F$, $\mathcal{V}(a + b) \leq \mathcal{V}(a) + \mathcal{V}(b)$.
4. $\mathcal{V}(a) = 0$ iff $a = 0$.

It is easy to see that the above definition captures the key properties of the absolute value definition for rational numbers. Armed with this abstraction, we investigate if there are other valuations over $\mathbb{Q}$ besides the absolute value.

Let $\mathcal{V}(\cdot)$ be any valuation over $\mathbb{Q}$. Our first observation is:

Lemma 1.1. $\mathcal{V}(1) = \mathcal{V}(-1) = 1$.

Proof. We have, $\mathcal{V}(1) = \mathcal{V}(1) * \mathcal{V}(1)$, which gives $\mathcal{V}(1) = 1$ since $\mathcal{V}(1) \neq 0$. Similar proof for $\mathcal{V}(-1) = 1$. □

Next, we observe that:

Lemma 1.2. $\mathcal{V}(a) = |a|^\alpha$ *is a valuation for any* $\alpha \in \mathbb{R}_+$.

Proof. Properties 1, 2, and 4 are straightforward. For 3, we need to show that:

$$|a + b|^\alpha \leq |a|^\alpha + |b|^\alpha .$$

This follows from the fact that $\alpha > 0$. □

The valuations identified above are essentially the same as the absolute valuation. To enumerate all possible valuations, we consider the behavior of the valuation function on $\mathbb{Z}_+$, the set of positive integers. Since valuation is multiplicative, its values over $\mathbb{Q}$ are fixed by values over $\mathbb{Z}_+$. We distinguish two cases.

Case 1: $\mathcal{V}(n) > 1$ for some $n \in \mathbb{Z}_+$

In this case, let m be the smallest positive integer with $\mathcal{V}(m) > 1$. Then there exists $\alpha \in \mathbb{R}_+$ such that $\mathcal{V}(m) = m^\alpha$.

Lemma 1.3. *For every $n \in \mathbb{Z}_+$, $\mathcal{V}(n) = n^\alpha$.*

Proof. Let n be any positive integer. Let $m^k \leq n < m^{k+1}$ for some $k \geq 0$. Write n in base-m representation:

$$n = \sum_{i=0}^{k} a_i m^i,$$

with $|a_i| < m$. Then,

$$\mathcal{V}(n) = \mathcal{V}(\sum_{i=0}^{k} a_i m^i) \leq \sum_{i=0}^{k} \mathcal{V}(a_i)\mathcal{V}(m)^i \leq \sum_{i=0}^{k} m^{i\alpha} < \frac{m^{(k+1)\alpha}}{m^\alpha - 1} \leq \frac{m^\alpha}{m^\alpha - 1} \cdot n^\alpha,$$

since $\mathcal{V}(a_i) \leq 1$ and $n \geq m^k$. We also have:

$$m^{k+1} \leq n + (m-1)m^k,$$

which gives

$$m^{(k+1)\alpha} = \mathcal{V}(m^{k+1}) \leq \mathcal{V}(n) + \mathcal{V}(m^k) = \mathcal{V}(n) + m^{k\alpha}.$$

Since $n < m^{k+1}$, we get:

$$\mathcal{V}(n) \geq m^{(k+1)\alpha}(1 - \frac{1}{m^\alpha}) > \frac{m^\alpha - 1}{m^\alpha} \cdot n^\alpha.$$

Therefore,

$$\frac{1}{c} \cdot n^\alpha < \mathcal{V}(n) \leq c \cdot n^\alpha,$$

for $c = \frac{m^\alpha}{m^\alpha - 1} > 1$.

Using the above inequality for n^ℓ, we get:

$$\frac{1}{c} \cdot n^{\ell\alpha} < \mathcal{V}(n^\ell) \leq c \cdot n^{\ell\alpha},$$

which gives

$$\frac{1}{c^{1/\ell}} \cdot n^\alpha < \mathcal{V}(n) \leq c^{1/\ell} \cdot n^\alpha.$$

When $\ell \mapsto \infty$, $c^{1/\ell} \mapsto 1$, and so taking the limit, we get

$$\mathcal{V}(n) = n^\alpha.$$

□

Corollary 1.4. *For $a \in \mathbb{Q}$, let $|a| = \frac{m}{n}$, $m, n \in \mathbb{Z}_+$. Then,*

$$\mathcal{V}(a) = \frac{m^\alpha}{n^\alpha} = |a|^\alpha .$$

These valuations have already been identified.

Case 2: $\mathcal{V}(n) \leq 1$ for all $n \in \mathbb{Z}_+$

Let p be the smallest positive integer for which $\mathcal{V}(m) < 1$.

Lemma 1.5. *p is a prime number.*

Proof. If $p = m_1 \cdot m_2$, $m_1, m_2 < p$, then $\mathcal{V}(p) = \mathcal{V}(m_1) \cdot \mathcal{V}(m_2) = 1$. A contradiction. □

Lemma 1.6. *For every prime $q \neq p$, $\mathcal{V}(q) = 1$.*

Proof. Suppose $\mathcal{V}(q) < 1$ for some $q \neq p$. Choose a power ℓ such that both $\mathcal{V}(q^\ell), \mathcal{V}(p^\ell) < \frac{1}{2}$. Since p and q are relatively prime, there exist integers a and b such that $a \cdot p^\ell + b \cdot q^\ell = 1$. Then,

$$1 = \mathcal{V}(1) = \mathcal{V}(a) \cdot \mathcal{V}(p^\ell) + \mathcal{V}(b) \cdot \mathcal{V}(q^\ell) < \frac{1}{2} + \frac{1}{2} = 1.$$

A contradiction. □

Let $\beta = \mathcal{V}(p)$. Then, the following is immediate from the above two:

Corollary 1.7. *For any $n \in \mathbb{Z}_+$, $\mathcal{V}(n) = \beta^k$ where p^k is the largest power of p that divides n.*

For $a \in \mathbb{Q}$, let $|a| = \frac{m}{n}$, $m, n \in \mathbb{Z}_+$. Let $\mathrm{ord}_p(a) = k_m - k_n$ where k_m and k_n are the largest powers of p dividing m and n respectively.

Corollary 1.8. *For $a \in \mathbb{Q}$,*

$$\mathcal{V}(a) = \beta^{\mathrm{ord}_p(a)}.$$

It is easy to verify that the above definition satisfies all the properties of a valuation:

Lemma 1.9. *The function as defined in Corollary 1.8 is a valuation for any β, $0 < \beta < 1$.*

Proof. Properties 1, 2, and 4 are obvious. For 3, we need to show that:

$$\beta^{\mathrm{ord}_p(a+b)} \leq \beta^{\mathrm{ord}_p(a)} + \beta^{\mathrm{ord}_p(b)}.$$

It follows from the observation that $\mathrm{ord}_p(a+b) \geq \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}$. In fact, we have

$$\beta^{\mathrm{ord}_p(a+b)} \leq \max\{\beta^{\mathrm{ord}_p(a)}, \beta^{\mathrm{ord}_p(b)}\}.$$

□

The above valuations are very different from the absolute value valuations, and hold for every $0 < \beta < 1$. We will use a special value of $\beta = \frac{1}{p}$ to define the *p-adic* valuation.

Definition 1.10. For any prime number p, define $|\, a \,|_p = \frac{1}{p^{\mathrm{ord}_p(a)}}$, for $a \in \mathbb{Q}$ to be the *p-adic valuation.*

Completion of $\mathbb{Q}$ with respect to p-adic valuation gives us a different field $\mathbb{Q}_p$, the field of *p-adic numbers*. We investigate this field in the next section. We end this section by making an interesting observation.

Let us denote, by $|\cdot|_\infty$ the usual absolute value (i.e., valuation defined in the previous section with $\alpha = 1$). Let P be the union of the set of all prime numbers and ∞.

Theorem 1.11. *For any $a \in \mathbb{Q}$,*

$$\prod_{q \in P} |a|_q = 1.$$

Proof. Let $|a| = \prod_{i=1}^{k} p_i^{e_i}$ for distinct primes p_i and $e_i \in \mathbb{Z}$. Then, $|a|_{p_i} = \frac{1}{p_i^{e_i}}$, and for any prime $p \notin \{p_1, p_2, \ldots, p_k\}$, $|a|_p = 1$. And $|a|_\infty = |a| = \prod_{i=1}^{k} p_i^{e_i}$. Multiplying all valuations, we get 1. □

Above theorem explains the reason for the choices made for α and β. It is a special case of similar theorem for a large class of fields containing $\mathbb{Q}$.

2 The Field $\mathbb{Q}_p$

Now that we have discovered new ways of extending $\mathbb{Q}$, let us develop an understanding of the field $\mathbb{Q}_p$. First, let us see what do Cauchy sequences look like.

By definition, $s = (a_0, a_1, a_2, \ldots)$ is a Cauchy sequence if for every rational number $\epsilon > 0$, there exists an $m > 0$ such that for all $n \geq m$: $|a_n - a_m|_p < \epsilon$. Given that the p-adic valuation equals $\frac{1}{p^\ell}$ for $\ell \in \mathbb{Z}$, we can rephrase the above condition as: for every $\ell \in \mathbb{Z}_+$, there exists an $m > 0$ such that for all $n \geq m$: $|a_n - a_m|_p < \frac{1}{p^\ell}$. In other words, the difference $a_n - a_m$ is divisible by p^ℓ, and therefore, $a_n - a_m = 0 \pmod{p^\ell}$ for all $n \geq m$.

A Cauchy sequence s converging to 0 would therefore satisfy: for all $\ell \in \mathbb{Z}_+$, there exists an $m \geq 0$ such that for all $n \geq m$, $a_n = 0 \pmod{p^\ell}$. In particular, the following sequence converges to zero:

$$(1, p, p^2, p^3, \ldots, p^\ell, \ldots).$$

Under the standard valuation, this sequence of numbers diverges and so does not form a Cauchy sequence!

Above example shows that the numbers in $\mathbb{Q}_p$ are very different from numbers in $\mathbb{R}$. Of course, all rational numbers are in $\mathbb{Q}_p$. What are the Cauchy sequences corresponding to rational numbers? In general, how does one view the numbers of $\mathbb{Q}_p$? We now describe it. Let R_p be the ring of Cauchy sequences under p-adic valuation, and I_p the ideal of Cauchy sequences converging to 0 (as defined in the previous section). Then $\mathbb{Q}_p = R_p/I_p$. A number of $\mathbb{Q}_p$ corresponds to an equivalence class of Cauchy sequences converging to the same value. Each such class has a *canonical* sequence:

Definition 2.1. A *canonical sequence* is a Cauchy sequence in R_p of the form

$$(r_0 \cdot p^t, r_0 \cdot p^t + r_1 \cdot p^{t+1}, \ldots, \sum_{i=0}^{\ell} r_i \cdot p^{t+i}, \ldots)$$

with $t \in \mathbb{Z}$, $\ell \geq t$, and $0 \leq r_i < p$. Notice that t can be negative here. It is succinctly written as

$$(t; r_0, r_1, r_2, \ldots).$$

We will show that every number in $\mathbb{Q}_p$ can be uniquely represented as a canonical sequence. Before we do that, let us see some examples of such representations:

- Number 1 is represented by canonical sequence $(1, 1, 1, \ldots)$, or $(0; 1, 0, 0, \ldots)$ in succinct form.
- Number -1 is represented by canonical sequence $(p-1, (p-1)+(p-1)\cdot p = p^2-1, p^3-1, \ldots)$ or $(0; p-1, p-1, p-1, \ldots)$ in succinct form.
- For $m \in \mathbb{Z}_+$, write m in base p:

  $$m = a_0 + a_1 \cdot p + \cdots + a_k \cdot p^k,$$

  for $0 \leq a_i < p$. The canonical sequence of m is $(a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots, \sum_{i=0}^{k} a_i p^i = m, m, m, \ldots)$, or $(0; a_0, a_1, a_2, \ldots, a_k, 0, 0, \ldots)$ in succinct form.

We now identify an alternative way of expressing rational numbers.

Lemma 2.2. *Let $\frac{m}{n} \in \mathbb{Q}$ with $gcd(n, m) = 1$ and n not a multiple of p. There exists a sequence of numbers a_0, a_1, a_2, ..., with $0 \leq a_i < p$ such that for every $\ell > 0$:*

$$\frac{m}{n} = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_\ell \cdot p^\ell \ (mod\ p^{\ell+1}).$$

Proof. Follows by induction. Define $a_0 = \frac{m}{n} \pmod p$ which exists since p does not divide n. Now assume that a_0, a_1, ..., $a_{\ell-1}$ are defined such that $\sum_{i=0}^{\ell-1} a_i p^i = \frac{m}{n} \pmod{p^\ell}$. Then

$$a_\ell = \frac{1}{p^\ell} \cdot \left(\frac{m}{n} - \sum_{i=0}^{\ell-1} a_i p^i \right) \pmod p.$$

□

Above lemma immediately gives is canonical sequences for rational numbers.

- For $m, n \in \mathbb{Z}_+$, n not a multiple of p, the canonical sequence of $\frac{m}{n}$ is $(a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots)$, or $(0; a_0, a_1, a_2, \ldots)$ in succinct form with a_0, a_1, a_2 ... as per the Lemma 2.2.
- For $m, n \in \mathbb{Z}_+$, $n = p^t \cdot n'$, n' and m not a multiple of p, if the succinct sequence of $\frac{m}{n'}$ is $(0; a_0, a_1, a_2, \ldots)$, then the succinct sequence of $\frac{m}{n}$ is $(-t, a_0, a_1, a_2, \ldots)$.

Theorem 2.3. *Every number in $\mathbb{Q}_p$ is uniquely represented by a canonical sequence.*

Proof. A canonical sequence is Cauchy: $\sum_{i=-t}^{n} r_i \cdot p^i - \sum_{i=-t}^{\ell} r_i \cdot p^i = \sum_{\ell+1}^{n} r_i \cdot p^i$ and so the p-adic valuation of the difference is $< \frac{1}{p^\ell}$ for all $\ell \in \mathbb{Z}_+$ and $n \geq \ell$.

Let $s = (a_0, a_1, \ldots)$ be any Cauchy sequence. We show that there exists a canonical sequence converging to the same number as s. In other words, we show that their difference converges to 0. By the discussion above, we have that for every $\ell \in \mathbb{Z}_+$, there exists an $m_\ell > 0$ such that for all $n \geq m_\ell$, $a_n - a_{m_\ell} = 0 \pmod{p^\ell}$. Without loss of generality, we can assume that $m_1 < m_2 < m_3 < \cdots$. Hence, $m_\ell \geq \ell$.

Let

$$a_{m_1} = \frac{r_0}{p^t} + \frac{r_1}{p^{t-1}} + \cdots + r_t \pmod p,$$

as per the Lemma 2.2. Since $a_n - a_{m_1} = 0 \pmod p$ for $n \geq m_1$, it follows that

$$a_n = \frac{r_0}{p^t} + \frac{r_1}{p^{t-1}} + \cdots + r_t \pmod p.$$

So

$$a_{m_2} = \frac{r_0}{p^t} + \frac{r_1}{p^{t-1}} + \cdots + r_t + r_{t+1}p \pmod{p^2},$$

and continuing inductively, we get

$$a_{m_\ell} = \frac{r_0}{p^t} + \frac{r_1}{p^{t-1}} + \cdots + r_t + r_{t+\ell-1}p^{\ell-1} \pmod{p^\ell}.$$

Consider canonical sequence $s_c = (\ldots, \sum_{i=-t}^{\ell} r_{t+i}p^i, \ldots)$ (in succinct form $(-t, r_0, r_1, r_2, \ldots)$). The sequence $s - s_c$ converges to 0: for any $n \geq m_\ell$, $a_n - \sum_{i=-t}^{n-t} r_{t+i}p^i = 0 \pmod{p^\ell}$ since $m_\ell \geq \ell$.

It is straightforward to show that difference of two distinct canonical sequences does not converge to zero. Hence, s_c is the unique canonical sequence representing the number.

□

Therefore, a number a in $\mathbb{Q}_p$ is the sum $\sum_{i \geq -t} r_i p^i$ for $t \geq 0$. Except for rational numbers with denominator being a power of p, this sum is infinite. In the usual valuation, it does not converge, however, in p-adic valuation, $|a|_p = p^t$.

The is a natural ring associated with $\mathbb{Q}_p$: the set of numbers a with $|a|_p \leq 1$. Equivalently, $a = \sum_{i \geq 0} r_i p^i$. It is straightforward to show that it is a ring. This ring is denoted by $\mathbb{Z}_p$. This is duplication of notation; we have used $\mathbb{Z}_p$ to denote ring of residues modulo p earlier. To resolve it, ring of integers modulo p is often written as $\mathbb{Z}/p\mathbb{Z}$.

Numbers in $\mathbb{Z}_p$ are called *p-adic integers*. This ring is very different from $\mathbb{Z}$. Let

$$(p) = \{a \in \mathbb{Z}_p \mid a = \sum_{i \geq 1} r_i p^i\}.$$

(p) is clearly an ideal of $\mathbb{Z}_p$.

Theorem 2.4. *Ideal (p) is the only maximal ideal of $\mathbb{Z}_p$. Any proper ideal of $\mathbb{Z}_p$ is of the form $(p)^k$ for some $k \geq 1$.*

Proof. Let I be a proper ideal of $\mathbb{Z}_p$. We first show that if $a \in I$, $a \neq 0$ and $a \in (p)^k \backslash (p)^{k+1}$ then $(p)^k \subseteq I$. Let $a = r_k p^k + r_{k+1}p^{k+1} + \cdots$, $r_k \neq 0$. Let $b = r_k + r_{k+1}p + \cdots$, $b \in \mathbb{Z}_p$. Define $c = u_0 + u_1 p + u_2 p^2 + \cdots \in \mathbb{Z}_p$ inductively as follows: $u_0 r_k = 1 \pmod p$, and $u_\ell = -\frac{1}{r_k} \sum_{i=0}^{\ell-1} u_i r_{k+\ell-i} \pmod{p^{\ell+1}}$. It is easy to see that $b \cdot c = 1$. Therefore, $p^k \in I$, and hence $(p)^k \subseteq I$.

The above argument also shows that every element of $\mathbb{Z}_p \backslash (p)$ is a unit, and therefore, cannot be in a proper ideal. Hence, $I \subseteq (p)$. This proves that (p) is the only maximal ideal of $\mathbb{Z}_p$.

Now suppose $I \subseteq (p)^k$, $a \in I$, and $a \in (p) \backslash (p)^{k+1}$. The argument above shows that $(p)^k \subseteq I$ and hence $I = (p)^k$. □

Rings with a unique maximal ideal are called *local rings*. These rings capture "local" properties. For example, ring $\mathbb{Z}_p$ is used to study prime number p. The finite field F_p is also present there: $F_p \equiv \mathbb{Z}_p/(p)$.