# Hensel's lemma, valuations, and $p$-adic numbers

Jordan Bell
jordan.bell@gmail.com
Department of Mathematics, University of Toronto

November 2, 2014

## 1 Hensel's lemma

Let $p$ be prime and $f(x) \in \mathbb{Z}[x]$.[1] Suppose that $0 \leq a_0 < p$, satisfies

$$f(a_0) \equiv 0 \pmod p$$

and

$$f'(a_0) \not\equiv 0 \pmod p.$$

Using the power series expansion

$$f(a_0 + h) = f(a_0) + f'(a_0)h + \frac{f''(a_0)}{2}h^2 + \cdots,$$

for any $y \in \mathbb{Z}$ we have

$$f(a_0 + py) = f(a_0) + f'(a_0)py + \frac{f''(a_0)}{2}p^2y^2 + \cdots$$

so

$$\frac{f(a_0 + py)}{p} = \frac{f(a_0)}{p} + f'(a_0)y + \frac{f''(a_0)}{2}py^2 + \cdots.$$

Because $f(a_0) \equiv 0 \pmod p$, each term on the right-hand side is an integer. Then, $f(a_0 + py) \equiv 0 \pmod{p^2}$ is equivalent to

$$\frac{f(a_0)}{p} + f'(a_0)y + \frac{f''(a_0)}{2}py^2 + \cdots \equiv 0 \pmod p,$$

i.e.,

$$f'(a_0)y \equiv -\frac{f(a_0)}{p} \pmod p.$$

Because $f'(a_0) \not\equiv 0 \pmod p$, there is a unique $y \pmod p$ that solves the above congruence, so there is a unique $y \pmod p$ that solves $f(a_0+py) \equiv 0 \pmod{p^2}$. This $y$ is

$$y \equiv -\frac{f(a_0)}{p}(f'(a_0))^{-1} \pmod p.$$

[1] Hua Loo Keng, *Introduction to Number Theory*, Chapter 15, "$p$-adic numbers".

Let $0 \le a_1 < p$ be $a_1 \equiv y \pmod p$.

Suppose that

$$x = a_0 + a_1 p + a_2 p^2 + \cdots + a_{l-2} p^{l-2}, \qquad 0 \le a_j < p,$$

satisfies

$$f(x) \equiv 0 \pmod{p^{l-1}}$$

and

$$f'(x) \not\equiv 0 \pmod p.$$

Using the power series expansion

$$f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2}h^2 + \cdots,$$

for any $y \in \mathbb{Z}$ we have

$$f(x + p^{l-1}y) = f(x) + f'(x)p^{l-1}y + \frac{f''(x)}{2}p^{2l-2}y^2 + \cdots,$$

i.e.

$$\frac{f(x+p^{l-1}y)}{p^{l-1}} = \frac{f(x)}{p^{l-1}} + f'(x)y + \frac{f''(x)}{2}p^{l-1}y^2 + \cdots.$$

Because $f(x) \equiv 0 \pmod{p^{l-1}}$, each term on the right-hand side is an integer. Then, $f(x+p^{l-1}y) \equiv 0 \pmod{p^l}$ is equivalent to

$$\frac{f(x)}{p^{l-1}} + f'(x)y + \frac{f''(x)}{2}p^{l-1}y^2 + \cdots \equiv 0 \pmod p,$$

i.e.,

$$f'(x)y \equiv -\frac{f(x)}{p^{l-1}} \pmod p.$$

Because $f'(x) \not\equiv 0 \pmod p$, there is a unique $y \pmod p$ that solves the above congruence, so there is a unique $y \pmod p$ that solves $f(x+p^{l-1}y) \equiv 0 \pmod{p^l}$. This $y$ is

$$y \equiv -\frac{f(x)}{p^{l-1}}(f'(x))^{-1} \pmod p.$$

Let $0 \le a_{l-1} < p$ be $a_{l-1} \equiv y \pmod p$.

We have thus inductively defined a sequence $a_0, a_1, a_2, \ldots$, with $0 \le a_j < p$, such that for any $l$,

$$f(a_0 + a_1 p + \cdots + a_{l-1}p^{l-1}) \equiv 0 \pmod{p^l}.$$

We wish to make sense of the infinite expression

$$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

Calling this $x$, it ought to be the case that $f(x) \equiv 0 \pmod p$, $f(x) \equiv 0 \pmod{p^2}$, $f(x) \equiv 0 \pmod{p^3}$, etc.

**Example 1.** Take $p = 3$ and $f(x) = x^2 - 7$, $f'(x) = 2x$. The two conditions $f(x) \equiv 0 \pmod p$ and $f'(x) \not\equiv 0 \pmod p$ are satisfied both by $a_0 = 1$ and $a_0 = 2$. Take $a_0 = 1$. Then

$$a_1 \equiv -\frac{f(1)}{3}(f'(1))^{-1} \equiv -\frac{-6}{3}(2)^{-1} \equiv 1 \pmod 3.$$

So $a_1 = 1$. Then,

$$a_2 \equiv -\frac{f(1+1\cdot 3)}{3^2}(f'(1+1\cdot 3))^{-1} \equiv -\frac{9}{9}(8)^{-1} \equiv -2 \equiv 1 \pmod 3.$$

So $a_2 = 1$. Then,

$$a_3 \equiv -\frac{f(1+1\cdot 3+1\cdot 3^2)}{3^3}(f'(1+1\cdot 3+1\cdot 3^2))^{-1} \equiv -6\cdot 2 \equiv 0 \pmod 3.$$

So, $a_3 = 0$. Then,

$$a_4 \equiv -\frac{f(1+1\cdot 3+1\cdot 3^2+0\cdot 3^3)}{3^4}(f'(1+1\cdot 3+1\cdot 3^2+0\cdot 3^3))^{-1} \equiv -2\cdot 2 \equiv 2 \pmod 3.$$

So, $a_4 = 2$, etc.

# 2 Absolute values on fields

If $K$ is a field, an **absolute value on** $K$ is a map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that $|x| = 0$ if and only if $x = 0$, $|xy| = |x||y|$, and $|x+y| \leq |x| + |y|$. The **trivial absolute value on** $K$ is $|0| = 0$ and $|x| = 1$ for all nonzero $x \in K$.

If $|\cdot|$ is an absolute value on $K$, then $d(x,y) = |x-y|$ is a metric on $K$. The trivial absolute value yields the discrete metric. Two absolute values $|\cdot|_1, |\cdot|_2$ on $K$ are said to be **equivalent** if they induce the same topology on $K$.

The following theorem characterizes equivalent absolute values.[2]

**Theorem 2.** *Two nontrivial absolute values $|\cdot|_1, |\cdot|_2$ are equivalent if and only if there is some real $s > 0$ such that*

$$|x|_1 = |x|_2^s, \qquad x \in K.$$

*Proof.* Suppose that $s > 0$ and that $|x|_1 = |x|_2^s$ for all $x \in K$. Then

$$\begin{aligned} B_{d_1}(x,r) &= \{y \in K : |y-x|_1 < r\} \\ &= \{y \in K : |y-x|_2^s < r\} \\ &= \{y \in K : |y-x|_2 < r^{1/s}\} \\ &= B_{d_2}(x, r^{1/s}). \end{aligned}$$

[2] *Absolute values, valuations and completion*, `https://www.math.ethz.ch/education/bachelor/seminars/fs2008/algebra/Crivelli.pdf`

Since the collection of open balls for $d_1$ is equal to the collection of open balls for $d_2$, the absolute values $|\cdot|_1, |\cdot|_2$ induce the same topology on $K$.

Suppose that $|\cdot|_1, |\cdot|_2$ are equivalent. If $|x|_1 < 1$ then $d_1(x^n, 0) = |x^n|_1 = |x|_1^n \to 0$ as $n \to \infty$. Thus $x^n \to 0$ in $d_1$ and hence, because the topologies induced by $|\cdot|_1$ and $|\cdot|_2$ are equal, $x^n \to 0$ in $d_2$, i.e. $|x|_2^n = |x^n|_2 = d_2(x^n, 0) \to 0$. Therefore $|x|_2 < 1$. Thus, $|x|_1 < 1$ if and only if $|x|_2 < 1$.

Let $y \in K$ such that $|y|_1 > 1$ (there is such an element because $|\cdot|_1$ is nontrivial and $|y^{-1}|_1 = |y|_1^{-1}$) and let $x \in K$ with $|x|_1 \neq 0, 1$. There is some nonzero $\alpha \in \mathbb{R}$ such that $|x|_1 = |y|_1^{\alpha}$. Let $\frac{m_i}{n_i} \in \mathbb{Q}$ all be greater than $\alpha$ and converge to $\alpha$. Then, because $|y|_1 > 1$, we have $|x|_1 = |y|_1^{\alpha} < |y|_1^{\frac{m_i}{n_i}}$, hence $|x|_1^{n_i} < |y|_1^{m_i}$, hence $\frac{|x^{n_i}|_1}{|y^{m_i}|_1} < 1$, hence

$$\left| \frac{x^{n_i}}{y^{m_i}} \right|_1 < 1.$$

Because $|\cdot|_1$ and $|\cdot|_2$ are equivalent,

$$\frac{|x|_2^{n_i}}{|y|_2^{m_i}} = \left| \frac{x^{n_i}}{y^{m_i}} \right|_2 < 1,$$

so $|x|_2 < |y|_2^{\frac{m_i}{n_i}}$. Taking $i \to \infty$ gives

$$|x|_2 \leq |y|_2^{\alpha}.$$

Similarly, we check that

$$|x|_2 \geq |y|_2^{\alpha}.$$

Therefore,

$$|x|_2 = |y|_2^{\alpha}.$$

Using this and $|x|_1 = |y|_1^{\alpha}$, we have

$$\log |x|_1 = \alpha \log |y|_1, \qquad \log |x|_2 = \alpha \log |y|_2,$$

and so, as $\alpha \neq 0$,

$$\frac{\log |x|_1}{\log |x|_2} = \frac{\log |y|_1}{\log |y|_2}.$$

This is true for any $x \in K$ with $|x|_1 \neq 0, 1$. We define $s \in \mathbb{R}$ to be this common value. The fact that $|y|_1 > 1$ implies, because $|\cdot|_1$ and $|\cdot|_2$ are equivalent, that $|y|_2 > 1$, and so $s > 0$.

Now take $x \in K$. If $x = 0$ then $|x|_1 = 0 = 0^s = |x|_2^s$. Because $|\cdot|_1$ and $|\cdot|_2$ are equivalent, $|x|_2 > 1$ implies that $|x|_1 > 1$ and $|x|_2 < 1$ implies that $|x|_1 < 1$, so if $|x|_1 = 1$ then $|x|_2 = 1$ and hence $|x|_1 = 1 = 1^s = |x|_2^s$. If $|x|_1 \neq 0, 1$, then the above shows that

$$\frac{\log |x|_1}{\log |x|_2} = s,$$

i.e., $|x|_1 = |x|_2^s$, proving the claim. $\square$

An absolute value $|\cdot| : K \to \mathbb{R}_{\geq 0}$ is said to be **non-Archimedean** if

$$|x+y| \leq \max\{|x|, |y|\}, \qquad x, y \in K.$$

An absolute value is called **Archimedean** if it is not non-Archimedean. For example, the absolute value on the field $\mathbb{R}$ is Archimedean, since, for example, $|1+1| = 2 > \max\{|1|, |1|\} = 1$.

**Lemma 3.** *If $|\cdot|$ is a non-Archimedean absolute value on a field $K$ and $|x| \neq |y|$, then*

$$|x+y| = \max\{|x|, |y|\}.$$

# 3 Valuations

A **valuation** on a field $K$ is a function $v : K \to \mathbb{R} \cup \{\infty\}$ satisfying $v(x) = \infty$ if and only if $x = 0$, $v(xy) = v(x) + v(y)$, and

$$v(x+y) \geq \min\{v(x), v(y)\}.$$

The **trivial valuation** is $v(x) = 0$ for $x \neq 0$ and $v(0) = \infty$.

**Lemma 4.** *Let $v$ be a valuation on a field $K$. If $v(x) \neq v(y)$, then $v(x+y) = \min\{v(x), v(y)\}$.*

*Proof.* Take $v(y) < v(x) \leq \infty$. For $x = 0$,

$$v(x+y) = v(y) = \min\{\infty, v(y)\} = \min\{v(x), v(y)\}.$$

For $x \neq 0$, assume by contradiction that $\min\{v(x+y), v(x)\} = v(x)$. Then, since $v(-x) = v(-1 \cdot x) = v(-1) + v(x) = v(x)$,

$$v(x) > v(y) = v(x+y-x) \geq \min\{v(x+y), v(x)\} = v(x),$$

a contradiction. Hence $\min\{v(x+y), v(x)\} = v(x+y)$. Then

$$\begin{aligned} v(y) &= v(x+y-x) \\ &\geq \min\{v(x+y), v(x)\} \\ &= v(x+y) \\ &\geq \min\{v(x), v(y)\} \\ &= v(y). \end{aligned}$$

Hence $v(x+y) = v(y) = \min\{v(x), v(y)\}$, completing the proof. □

**Theorem 5.** *Let $K$ be a field. If $|\cdot|$ is a non-Archimedean absolute value on $K$ and $s > 0$, then $v_s : K \to \mathbb{R} \cup \{\infty\}$ defined by $v_s(x) = -s \log |x|$ for $x \neq 0$ and $v_s(0) = \infty$ is a valuation on $K$.*

*If $v$ is a valuation on $K$ and $q > 1$, then the function $|\cdot|_q : K \to \mathbb{R}_{\geq 0}$ defined by $|x|_q = q^{-v(x)}$ for $x \neq 0$ and $|0|_q = 0$ is a non-Archimedean absolute value on $K$.*

*Proof.* Suppose that $|\cdot|$ is a non-Archimedean absolute value on $K$ and that $s > 0$. Let $x, y \in K$. If either is 0, then it is immediate that $v_s(xy) = \infty = v_s(x) + v_s(y)$. If neither is 0, then

$$v_s(xy) = -s \log |xy| = -s \log(|x||y|) = -s \log |x| - s \log |y| = v_s(x) + v_s(y).$$

Now, if both $x, y$ are 0 then

$$v_s(x + y) = v_s(0) = \infty = \min\{\infty, \infty\} = \min\{v_s(x), v_s(y)\}.$$

If $x = 0$ and $y \neq 0$ then

$$v_s(x + y) = v_s(y) = -s \log |y| = \min\{-s \log |y|, \infty\} = \min\{v_s(y), v_s(x)\}.$$

If neither $x, y$ is 0 but $x = -y$, then

$$v_s(x + y) = v_s(0) = \infty \geq \min\{v_s(x), v_s(y)\}.$$

Finally, if neither $x, y$ is 0 and $x \neq -y$, then, because $|\cdot|$ is non-Archimedean,

$$\begin{aligned} v_s(x + y) &= -s \log |x + y| \\ &\geq -s \log(\max\{|x|, |y|\}) \\ &= \min\{-s \log |x|, -s \log |y|\} \\ &= \min\{v_s(x), v_s(y)\}. \end{aligned}$$

Thus $v_s$ is a valuation on $K$.

Suppose that $v$ is a valuation on $K$ and that $q > 1$. If $x, y$ are nonzero, then

$$|xy|_q = q^{-v(xy)} = q^{-v(x)-v(y)} = q^{-v(x)} q^{-v(y)} = |x|_q |y|_q.$$

Let $x, y \in K$. To show that $|x + y|_q \leq |x|_q + |y|_q$, it suffices to show that $|x + y|_q \leq \max\{|x|_q, |y|_q\}$; proving this will establish that $|\cdot|_q$ is an absolute value and furthermore that $|\cdot|_q$ is non-Archimedean. If $x, y$ are both 0, then $|x + y|_q = |0|_q = 0 = \max\{0, 0\} = \max\{|x|_q, |y|_q\}$. If $x = 0$ and $y \neq 0$, then $|x + y|_q = |y|_q = q^{-v(y)} = \max\{q^{-v(y)}, 0\} = \max\{|y|_q, |x|_q\}$. If neither $x, y$ is 0 but $x = -y$, then

$$|x + y|_q = |0|_q = 0 \leq \max\{|x|_q, |y|_q\}.$$

Finally, if neither $x, y$ is 0 and $x \neq -y$, then

$$\begin{aligned} |x + y|_q &= q^{-v(x+y)} \\ &\leq q^{-\min\{v(x), v(y)\}} \\ &= \max\{q^{-v(x)}, q^{-v(y)}\} \\ &= \max\{|x|_q, |y|_q\}. \end{aligned}$$

$\square$

Two valuations $v_1, v_2$ on a field $K$ are said to be **equivalent** if there is some real $s > 0$ such that

$$v_1 = sv_2.$$

A valuation $v$ on a field $K$ is said to be **discrete** if there is some real $s > 0$ such that

$$v(K^*) = s\mathbb{Z}.$$

A valuation is said to be **normalized** if

$$v(K^*) = \mathbb{Z}.$$

# 4 Valuation rings

**Theorem 6.** *If $K$ is a field and $v$ is a nontrivial valuation on $K$, then*

$$\mathcal{O}_v = \{x \in K : v(x) \geq 0\}$$

*is a maximal proper subring of $K$, and for all $x \neq 0$, $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$. The set*

$$\{x \in K : v(x) = 0\}$$

*is the group of invertible elements of $\mathcal{O}_v$, and the set*

$$\mathfrak{p}_v = \{x \in K : v(x) > 0\}$$

*is the unique maximal ideal of $\mathcal{O}_v$.*

*Proof.* It is immediate that $0, 1 \in \mathcal{O}_v$. For $x \in \mathcal{O}_v$, $v(-x) = v(x) \geq 0$, so $-x \in \mathcal{O}_v$. For $x, y \in \mathcal{O}_v$, $v(xy) = v(x) + v(y) \geq 0$, so $xy \in \mathcal{O}_v$. And $v(x+y) \geq \min\{v(x), v(y)\} \geq 0$, so $x + y \in \mathcal{O}_v$. Thus $\mathcal{O}_v$ is a subring of $K$. For nonzero $x \in K$, if $v(x) \geq 0$ then $x \in \mathcal{O}_v$, and if $v(x) < 0$ then $v(x^{-1}) = -v(x) > 0$, so $x^{-1} \in \mathcal{O}_v$.

Since $v$ is nontrivial, there is some $x \in K$ with $v(x) \neq 0, \infty$. If $x \in \mathcal{O}_v$ then $v(x) > 0$ and so $v(x^{-1}) = -v(x) < 0$, giving $x^{-1} \notin \mathcal{O}_v$. Hence $\mathcal{O}_v \neq K$, showing that $\mathcal{O}_v$ is a proper subring of $K$.

To show that $\mathcal{O}_v$ is a maximal proper subring, it suffices to show that if $z \in K \setminus \mathcal{O}_v$ then $\mathcal{O}_v[z] = K$, i.e., that the smallest ring containing $\mathcal{O}_v$ and $z$ is $K$. As $z \notin \mathcal{O}_v$, $v(z) < 0$. Let $y \in K$. For any positive integer $j$ we have $v(yz^{-j}) = v(y) - jv(z)$, and because $v(z) < 0$, there is some $j = j(y)$ such that $v(yz^{-j}) > 0$. For this $j$, $yz^{-j} \in \mathcal{O}_v$. Hence $y \in \mathcal{O}_v[z]$, and so $\mathcal{O}_v[z] = K$, showing that $\mathcal{O}_v$ is a maximal proper subring.

Suppose that $x \in \mathcal{O}_v$ and $x^{-1} \in \mathcal{O}_v$. If $v(x) > 0$, then $v(x^{-1} = -v(x) < 0$, contradicting that $x^{-1} \in \mathcal{O}_v$. Hence $v(x) = 0$. If $v(x) = 0$, then, as $x^{-1} \in K$, $v(x^{-1}) = -v(x) = 0$, so $x^{-1} \in \mathcal{O}_v$, hence $x$ is an element of $\mathcal{O}_v$ whose inverse is in $\mathcal{O}_v$.

Let $x, y \in \mathfrak{p}_v$. Then, since $v(x) > 0$ and $v(y) > 0$,

$$v(x - y) \geq \min\{v(x), v(-y)\} = \min\{v(x), v(y)\} > 0,$$

showing that $x - y \in \mathfrak{p}_v$, and thus that $\mathfrak{p}_v$ is an additive subgroup of $\mathcal{O}_v$. Let $x \in \mathfrak{p}_v$ and $z \in \mathcal{O}_v$. Then, since $v(z) \geq 0$ and $v(x) > 0$,

$$v(zx) = v(z) + v(x) \geq v(x) > 0,$$

showing that $zx \in \mathfrak{p}_v$. Therefore $\mathfrak{p}_v$ is an ideal in the ring $\mathcal{O}_v$. Since $v(1) = 0$, $1 \notin \mathfrak{p}_v$, so $\mathfrak{p}_v$ is a proper ideal.

The fact that $\mathfrak{p}_v$ is maximal follows from it being the set of noninvertible elements of $\mathcal{O}_v$. Suppose that $B$ is a maximal ideal $B$ of $\mathcal{O}_v$. Because $B$ is a proper ideal it contains no invertible elements, and hence is contained in $\mathfrak{p}_v$, the set of noninvertible elements of $\mathcal{O}_v$. Since $B$ is maximal, it must be that $B = \mathfrak{p}_v$. Therefore, any maximal ideal of $\mathcal{O}_v$ is $\mathfrak{p}_v$, showing that $\mathfrak{p}_v$ is the unique maximal ideal of $\mathcal{O}_v$. □

The above ring $\mathcal{O}_v$ is called the **valuation ring**. Generally, a ring that has a unique maximal ideal is called a **local ring**, and thus the above theorem shows that the valuation ring is a local ring. We call the quotient $\mathcal{O}_v/\mathfrak{p}_v$ the **residue field of** $\mathcal{O}_v$.

**Lemma 7.** *If $v$ is a normalized valuation on a field $K$ then for all nonzero $x \in K$ and $t \in \mathfrak{p}_v$, $v(t) = 1$, there is some $u \in \mathcal{O}_v^*$ such that*

$$x = ut^n, \qquad n = v(x).$$

*Proof.* Since $x \neq 0$, $v(x) = n \in \mathbb{Z}$. Hence $v(xt^{-n}) = v(x) - nv(t) = v(x) - n = 0$, and therefore $u = xt^{-n} \in \mathcal{O}^*$. Then $x = ut^n$, completing the proof. □

**Theorem 8.** *If $v$ is a normalized valuation on a field $K$, then $\mathcal{O}_v$ is a principal ideal domain. If $A$ is a nonzero ideal of $\mathcal{O}_v$, then there is some $t \in \mathfrak{p}$, $v(t) = 1$ and $n \geq 0$ such that*

$$A = t^n\mathcal{O}_v = \{x \in K : v(x) \geq n\} = \mathfrak{p}_v^n,$$

*and*

$$\mathfrak{p}_v^n/\mathfrak{p}_v^{n+1} \cong \mathcal{O}_v/\mathfrak{p}_v,$$

*as $\mathcal{O}_v/\mathfrak{p}_v$-linear vector spaces.*

*Proof.* Let $A \neq \{0\}$ be an ideal of $\mathcal{O}_v$. For any $y \in A$, $v(y) \geq 0$, and we take $x \in A$ such that

$$v(x) = \min\{v(y) : y \in A\}. \tag{1}$$

Since $v(K^*) = \mathbb{Z}$, there is some $t \in K$ with $v(t) = 1$, and because $v(t) > 0$, $t \in \mathfrak{p}_v$. By Lemma 7, there is some $u \in \mathcal{O}^*$ such that $x = ut^n$, $n = v(x)$. For any $z \in \mathcal{O}$, $xz \in A$ and so $t^n z \in A$. Thus $t^n\mathcal{O}_v \subset A$. On the other hand, let $y \in A$. Then also by Lemma 7 there is some $w \in \mathcal{O}_v^*$ such that $y = wt^m$,

$m = v(y)$. By (1), $m = v(y) \geq v(x) = n$, so $v(t^{m-n}) = (m-n)v(t) = m-n \geq 0$ so $t^{m-n} \in \mathcal{O}_v$, giving

$$y = wt^m = t^n(wt^{m-n}) \in t^n\mathcal{O}_v.$$

Therefore $A \subset t^n\mathcal{O}_v$, and so $A = t^n\mathcal{O}_v$. That is, $A$ is the principal ideal generated by $t^n$, which shows that $\mathcal{O}_v$ is a principal ideal domain.

Let $t \in \mathfrak{p}_v$ with $v(t) = 1$, and define $\phi : \mathfrak{p}_v^n \to \mathcal{O}_v/\mathfrak{p}_v$ by $v(at^n) = a + \mathfrak{p}$, for $a \in \mathcal{O}_v$. □

**Lemma 9.** *If $v_1, v_2$ are discrete valuations on a field $K$ such that $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$, then $v_1$ and $v_2$ are equivalent.*

# 5 $p$-adic valuations

Fix a prime number $p$. For nonzero $a \in \mathbb{Q}$, there are unique integers $n, r, s$ satisfying

$$a = \frac{r}{s}p^n,$$

where $r, s$ are coprime, $s > 0$, and $p \nmid rs$. We define $v_p(a) = n$. Furthermore, we define $v_p(0) = \infty$.

**Theorem 10.** *$v_p : \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$ is a normalized valuation.*

*Proof.* For nonzero $a, b \in \mathbb{Q}$, write

$$a = \frac{r_1}{s_1}p^m, \qquad b = \frac{r_2}{s_2}p^n,$$

where $\gcd(r_1, s_1) = \gcd(r_2, s_2) = 1$, $s_1, s_2 > 0$, and $p \nmid r_1s_1, p \nmid r_2s_2$. Then,

$$ab = \frac{r_1r_2}{s_1s_2}p^{m+n},$$

where $p \nmid r_1s_1r_2s_2$; the fraction $\frac{r_1r_2}{s_1s_2}$ need not be in lowest terms. So $v_p(ab) = m + n = v_p(a) + v_p(n)$.

Suppose that $v_p(a) \leq v_p(b)$. Then

$$a + b = \frac{r_1}{s_1}p^m + \frac{r_2}{s_2}p^n = \left(\frac{r_1}{s_1} + \frac{r_2}{s_2}p^{n-m}\right)p^m = \frac{r_1s_2 + r_2s_1p^{n-m}}{s_1s_2}p^m.$$

Since $p \nmid s_1$ and $p \nmid s_2$, then

$$v_p(a+b) \geq m = v_p(a) = \min\{v_p(a), v_p(b)\}.$$

□

We call $v_p$ the **$p$-adic valuation**. The valuation ring of $\mathbb{Q}$ corresponding to $v_p$ is

$$\mathcal{O}_p = \{x \in \mathbb{Q} : v_p(x) \geq 0\},$$

in other words, those rational numbers such that in lowest terms, $p$ does not divide their denominator. For example, $\frac{11}{169}, -\frac{9}{35} \in \mathcal{O}_3$, and $\frac{5}{3} \notin \mathcal{O}_3$. By Theorem 6, the group of units of the valuation ring $\mathcal{O}_p$ is

$$\mathcal{O}_p^* = \{x \in \mathbb{Q} : v_p(x) = 0\},$$

in other words, those rational numbers such that in lowest terms, $p$ divides neither their numerator nor their denominator. As well by Theorem 6, $\mathcal{O}_p$ is a local ring whose unique maximal ideal is

$$\mathfrak{p}_p = \{x \in \mathbb{Q} : v_p(x) > 0\},$$

in other words, those rational numbers such that in lowest terms, $p$ divides their numerator and does not divide their denominator. We see that $p \in \mathfrak{p}_p$ and $v_p(p) = 1$, so the nonzero ideals of $\mathcal{O}_p$ are of the form

$$p^n \mathcal{O}_p.$$

**Lemma 11.** *$\mathcal{O}_p/\mathfrak{p}_p \cong \mathbb{Z}/p\mathbb{Z}$.*

# 6 $p$-adic absolute values and metrics

We define $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ by $|a|_p = p^{-v_p(n)}$ for $a \neq 0$ and $|0|_p = 0$. This is a non-Archimedean absolute value on $\mathbb{Q}$, which we call the **$p$-adic absolute value**.

**Example 12.** For $p = 3$ and $a = -\frac{57}{10}$, we have $n = 1, r = -19, s = 10$. Thus $\left|-\frac{57}{10}\right|_3 = 3^{-1}$.

For $p = 5$ and $a = \frac{28}{75}$, we have $n = -2, r = 28, s = 3$. Thus $\left|\frac{28}{75}\right|_5 = 5^2$.

We define $d_p(x, y) = |x - y|_p$. The sequences $x_l = a_0 + a_1 p + a_2 p^2 + \cdots + a_{l-1} p^{l-1}$ constructed when applying Hensel's lemma satisfy, for $m < n$,

$$x_n - x_m = a_m p^m + a_{m+1} p^{m+1} + \cdots + a_{n-1} p^{n-1} \equiv 0 \pmod{p^m},$$

so

$$|x_n - x_m|_p \leq p^{-m},$$

and

$$f(x_n) \equiv 0 \pmod{p^n},$$

so

$$|f(x_n)|_p \leq p^{-n}.$$

Thus, $x_n$ is a Cauchy sequence in the $p$-adic metric $d_p(x, y) = |x - y|_p$, and $f(x_n) \to 0$ as $n \to \infty$.

**Lemma 13.** *If $x_n$ and $y_n$ are Cauchy sequences in $(\mathbb{Q}, d_p)$, then $x_n + y_n$ and $x_n \cdot y_n$ are Cauchy sequences in $(\mathbb{Q}, d_p)$.*

*Proof.* The claim follows from

$$|x_n + y_n - (x_m + y_m)|_p \leq |x_n - x_m|_p + |y_n - y_m|_p$$

and

$$\begin{aligned} |x_n \cdot y_n - x_m \cdot y_m|_p &= |x_n \cdot y_n - x_m \cdot y_n + x_m \cdot y_n - x_m \cdot y_m|_p \\ &\leq |x_n - x_m|_p |y_n|_p + |x_m|_p |y_n - y_m|_p, \end{aligned}$$

and the fact that $x_n, y_n$ being Cauchy implies that $|x_n|_p, |y_n|_p$ are bounded. □

# 7 Completions of metric spaces

If $(X, d)$ is a metric space, a **completion** of $X$ is a complete metric space $(Y, \rho)$ and an isometry $i : X \to Y$ such that for every metric space $(Z, r)$ and isometry $j : X \to Z$, there is a unique isometry $J : Y \to Z$ such that $J \circ i = j$. It is a fact that any metric space has a completion, and that if $(Y_1, \rho_1)$ and $(Y_2, \rho_2)$ are completions then there is a unique isometric isomorphism $f : Y_1 \to Y_2$.

For $p$ prime, let $(\mathbb{Q}_p, d_p)$ be the completion of $(\mathbb{Q}, d_p)$. Elements of $\mathbb{Q}_p$ are called **$p$-adic numbers**. For $x, y \in \mathbb{Q}_p$, there are Cauchy sequences $x_n, y_n$ in $(\mathbb{Q}, d_p)$ such that $x_n \to x$ and $y_n \to y$ in $(\mathbb{Q}_p, d_p)$. We define addition and multiplication on the set $\mathbb{Q}_p$ by

$$x + y = \lim(x_n + y_n), \qquad x \cdot y = \lim(x_n \cdot y_n);$$

that these limits exists follows from Lemma 13. If $x \in \mathbb{Q}_p$, $x \neq 0$, then there is a sequence $x_n \in \mathbb{Q}$, each term of which is $\neq 0$, such that $x_n \to x$ in $(\mathbb{Q}_p, d_p)$. Then $x_n^{-1}$ is a Cauchy sequence in $(\mathbb{Q}, d_p)$ hence converges to some $y \in \mathbb{Q}_p$ which satisfies $x \cdot y = 1$. Therefore $\mathbb{Q}_p$ is a field.

We define $v_p : \mathbb{Q}_p \to \mathbb{R} \cup \{\infty\}$

$$v_p(x) = \lim v_p(x_n), \qquad x_n \to x.$$

One proves that $v_p$ is a normalized valuation on the field $\mathbb{Q}_p$.[3] We then define $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_{\geq 0}$ by $|x|_p = p^{-v_p(x)}$ for $x \neq 0$ and $|0|_p = \infty$.

# 8 The exponential function

**Lemma 14.** *For $a_1, \ldots, a_r \in \mathbb{Q}_p$,*

$$|a_1 + \cdots + a_r|_p \leq \max\{|a_1|, \ldots, |a_r|\}.$$

[3] cf. Paul Garrett, *Classical definitions of $\mathbb{Z}_p$ and $\mathbb{A}$*, http://www.math.umn.edu/~garrett/m/mfms/notes/05_compare_classical.pdf

**Lemma 15.** *A sequence $a_i \in \mathbb{Q}_p$ is Cauchy if and only if $a_{i+1} - a_i \to 0$ as $i \to \infty$.*

*Proof.* Assume that $a_{i+1} - a_i \to 0$ and let $\epsilon > 0$. Then there is some $i_0$ such that $i \geq i_0$ implies $|a_{i+1} - a_i|_p < \epsilon$. For $i_0 \leq i < j$,

$$\begin{aligned} |a_j - a_i|_p &= |a_j - a_{j-1} + a_{j-1} + \cdots - a_{i+1} + a_{i+1} - a_i|_p \\ &= |(a_j - a_{j-1}) + \cdots + (a_{i+1} - a_i)|_p \\ &\leq \max\{|a_j - a_{j-1}|, \ldots, |a_{i+1} - a_i|\} \\ &< \epsilon. \end{aligned}$$

□

The above shows that if $a_i \to 0$ in $(\mathbb{Q}_p, d_p)$ then the series $\sum a_i$ converges in $(\mathbb{Q}_p, d_p)$.

**Lemma 16** (Exponential power series)**.** *If $v_p(x) > \frac{1}{p-1}$, then*

$$\sum_{n=0}^{\infty} \frac{x^n}{n!}$$

*converges in $(\mathbb{Q}_p, d_p)$.*

*Proof.*

$$v_p(n!) = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right] \leq \sum_{j=1}^{\infty} \frac{n}{p^j} = \frac{1}{np} \frac{1}{1 - \frac{1}{p}} = \frac{n}{p-1}.$$

Then

$$v_p\left(\frac{x^n}{n!}\right) = n v_p(x) - v_p(n!) \geq n v_p(x) - \frac{n}{p-1} = n\left(v_p(x) - \frac{1}{p-1}\right).$$

As $n \to \infty$ this tends to $+\infty$, hence

$$\left|\frac{x^n}{n!}\right|_p = p^{-v_p\left(\frac{x^n}{n!}\right)} \to 0,$$

and thus the series $\sum_{n=0}^{\infty} \frac{x^n}{n!}$ converges. □

**Lemma 17** (Logarithm power series)**.** *If $v_p(x) > 0$, then*

$$\sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

*converges in $(\mathbb{Q}_p, d_p)$.*

*Proof.* For $n$ a positive integer we have $v_p(n) \leq \log_p n$. Then,

$$v_p\left(\frac{x^n}{n}\right) = n v_p(x) - v_p(n) \geq n v_p(x) - \log_p n.$$

If $v_p(x) > 0$ then this tends to $+\infty$ as $n \to \infty$. □

## 9 Topology

We define $\mathbb{Z}_p$ to be the valuation ring of $\mathbb{Q}_p$. Elements of $\mathbb{Z}_p$ are called **$p$-adic integers**. For $x \in \mathbb{Q}_p$ and real $r > 0$, write

$$\overline{B}_p(r, x) = \{y \in \mathbb{Q}_p : |x - y|_p \leq r\} = \{y \in \mathbb{Q}_p : v_p(x - y) \geq -\log_p r\}.$$

In particular,

$$\overline{B}_p(0, 1) = \mathbb{Z}_p.$$

Because $v_p$ is discrete, there is some $\epsilon > 0$ such that

$$\{y \in \mathbb{Q}_p : |x - y|_p \leq r\} = \{y \in \mathbb{Q}_p : |x - y|_p < r + \epsilon\}.$$

This shows that $\overline{B}_p(x, r)$ is open in the topology induced by $v_p$, and thus is both closed and open. It follows that $\mathbb{Q}_p$ is **totally disconnected**.[4]

**Theorem 18.** *$\mathbb{Z}_p$ is totally bounded.*

The fact that $\mathbb{Z}_p$ is a totally bounded subset of a complete metric space implies that $\mathbb{Z}_p$ is compact. Then because

$$\overline{B}_d(0, p^k) = \{y \in \mathbb{Q}_p : |y|_p \leq p^k\} = \{y \in \mathbb{Q}_p : |p^k y|_p \leq 1\} = p^{-k}\mathbb{Z}_p$$

and translation is a homeomorphism, any closed ball in $\mathbb{Q}_p$ is compact. Therefore $\mathbb{Q}_p$ is locally compact.

$\mathbb{Q}_p$ is a locally compact abelian group under addition, and we take Haar measure on it satisfying $\mu(\mathbb{Z}_p) = 1$. One can explicitly calculate the characters on $\mathbb{Q}_p$.[5]

[4] Gerald B. Folland, *A Course in Abstract Harmonic Analysis*, pp. 34–36.

[5] Gerald B. Folland, *A Course in Abstract Harmonic Analysis*, pp. 91–93, 104. Cf. Keith Conrad, *The character group of* **Q**, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/characterQ.pdf`