Explicit construction of the p-adic numbers

Jordan Bell

March 17, 2016

1 $\mathbb{Z}_p$

Let p be prime, let $N_p = \{0, \ldots, p-1\}$, and let $\mathbb{Z}_p$ be the set of maps $x : \mathbb{Z} \to N_p$ such that $x(k) = 0$ for all $k < 0$.

1.1 Addition

For $x, y \in \mathbb{Z}_p$, we define $x + y \in \mathbb{Z}_p$ by induction. Define

$$(x+y)(0) \equiv x(0) + y(0) \pmod p, \qquad (x+y)(0) \in N_p.$$

Assume for $k \geq 0$ that there is some $A_k \in \mathbb{Z}$ such that

$$\sum_{j=0}^{k} (x+y)(j)p^j = A_k p^{k+1} + \sum_{j=0}^{k} (x(j)+y(j))p^j.$$

Define

$$(x+y)(k+1) \equiv -A_k + x(k+1) + y(k+1) \pmod p, \qquad (x+y)(k+1) \in N_p,$$

and then define $A_{k+1} \in \mathbb{Z}$ by

$$(x+y)(k+1) = A_{k+1}p - A_k + x(k+1) + y(k+1).$$

Then

$$\begin{aligned}
\sum_{j=0}^{k+1} (x+y)(j)p^j &= (x+y)(k+1)p^{k+1} + \sum_{j=0}^{k} (x+y)(j)p^j \\
&= A_{k+1}p^{k+2} - A_k p^{k+1} + (x(k+1) + y(k+1))p^{k+1} \\
&+ A_k p^{k+1} + \sum_{j=0}^{k} (x(j)+y(j))p^j \\
&= A_{k+1}p^{k+2} + \sum_{j=0}^{k+1} (x(j)+y(j))p^j.
\end{aligned}$$

Thus, for each $k \geq 0$, $(x+y)(k) \in N_p$ and

$$\sum_{j=0}^{k}(x+y)(j)p^j \equiv \sum_{j=0}^{k}(x(j)+y(j))p^j \pmod{p^{k+1}}. \tag{1}$$

It is immediate that $x+y = y+x$.

Lemma 1. *If $x, y \in \mathbb{Z}_p$ and for each $k \geq 0$,*

$$\sum_{j=0}^{k} x(j)p^j \equiv \sum_{j=0}^{k} y(j)p^j \pmod{p^{k+1}},$$

then $x = y$.

Proof. Suppose by contradiction that $x \neq y$. Now, $x(0) \equiv y(0) \pmod{p}$ and $x(0), y(0) \in N_p$ so $x(0) = y(0)$. As $x \neq y$, there is a minimal $k \geq 0$ such that $x(k+1) \neq y(k+1)$. On the one hand,

$$\sum_{j=0}^{k+1} x(j)p^j = x(k+1)p^{k+1} + \sum_{j=0}^{k} y(j)p^j,$$

and on the other hand,

$$\sum_{j=0}^{k+1} x(j)p^j \equiv \sum_{j=0}^{k+1} y(j)p^j \pmod{p^{k+2}}.$$

Then there is some B such that

$$x(k+1)p^{k+1} = Cp^{k+2} + y(k+1)p^{k+1}.$$

so $x(k+1) - y(k+1) = Bp$. But $-p+1 \leq x(k+1) - y(k+1) \leq p-1$, so $B = 0$ and hence $x(k+1) = y(k+1)$, a contradiction and thus $x = y$. $\square$

Therefore, if $t \in \mathbb{Z}_p$ satisfies, for all $k \geq 0$,

$$\sum_{j=0}^{k} t(j)p^j \equiv \sum_{j=0}^{k}(x(j)+y(j))p^j \pmod{p^{k+1}}.$$

then $t = x+y$. Now let $x, y, z \in \mathbb{Z}_p$. For $k \geq 0$,

$$\begin{aligned}
\sum_{j=0}^{k}(x+(y+z))(j)p^j &\equiv \sum_{j=0}^{k}(x(j)+(y+z)(j))p^j \pmod{p^{k+1}} \\
&= \sum_{j=0}^{k}(x(j)+y(j)+z(j))p^j \pmod{p^{k+1}} \\
&\equiv \sum_{j=0}^{k}((x+y)(j)+z(j))p^j \pmod{p^{k+1}},
\end{aligned}$$

which shows that $x + (y + z) = (x + y) + z$.

Define $t \in \mathbb{Z}_p$ by $t(k) = 0$ for all $k \geq 0$. It is immediate that for $x \in \mathbb{Z}_p$, $x + t = x$, $t + x = x$. If $x \neq 0$, let $m \geq 0$ be minimal such that $x(m) \neq 0$, and define $y \in \mathbb{Z}_p$ by

$$y(k) = \begin{cases} 0 & 0 \leq k < m \\ p - x(m) & k = m \\ p - 1 - x(k) & k > m. \end{cases}$$

This makes sense because $1 \leq x(m) \leq p-1$. Then $x(k)+y(k) = 0$ for $0 \leq k < m$, $x(m) + y(m) = p$, and $x(k) + y(k) = p - 1$ for $k > m$. For $k > m$,

$$\begin{aligned} \sum_{j=0}^{k} (x(j) + y(j))p^j &= p \cdot p^m + \sum_{j=m+1}^{k} (p-1)p^j \\ &= p^{m+1} + (p-1) \cdot \frac{p^{k+1} - p^{m+1}}{p-1} \\ &= p^{k+1}, \end{aligned}$$

so

$$\sum_{j=0}^{k} (x(j) + y(j))p^j \equiv \sum_{j=0}^{k} 0 \cdot p^j \pmod{p^{k+1}},$$

and it follows that $x + y = 0$, $y + x = 0$, namely $y = -x$.

We have established that $(\mathbb{Z}_p, +)$ is an abelian group whose identity is $k \mapsto 0$, $k \geq 0$.

Lemma 2. *For $x \in \mathbb{Z}_p$ and $m \geq 1$,*

$$(p^m x)(k) = \begin{cases} 0 & 0 \leq k < m \\ x(k-m) & k \geq m. \end{cases}$$

Proof. For $x \in \mathbb{Z}_p$ and $m \geq 1$ define $y(j) = 0$ for $0 \leq j < m$ and $y(j) = x(j-m)$

for $j \geq m$. By (1), for $k \geq m$,

$$\begin{aligned}
\sum_{j=0}^{k} (p^m x)(j) p^j &\equiv \sum_{j=0}^{k} p^m x(j) p^j \pmod{p^{k+1}} \\
&\equiv \sum_{j=0}^{k} x(j) p^{j+m} \pmod{p^{k+1}} \\
&\equiv \sum_{j=m}^{m+k} x(j-m) p^j \pmod{p^{k+1}} \\
&\equiv \sum_{j=m}^{k} x(j-m) p^j \pmod{p^{k+1}} \\
&\equiv \sum_{j=0}^{k} y(j) p^j \pmod{p^{k+1}}.
\end{aligned}$$

□

The following lemma shows that if $x(k) = 0$ for $k < m$ then it makes sense to talk about $p^{-m}x \in \mathbb{Z}_p$. That is, if $x(k) = 0$ for $k < m$ then there is a unique $y \in \mathbb{Z}_p$ such that $p^m y = x$. (For comparison, it is false that for any $z \in \mathbb{C}$ there is a unique $z^{1/2} \in \mathbb{C}$, or that for any $n \in \mathbb{Z}$ there is a unique $p^{-1}n \in \mathbb{Z}$.)

Lemma 3. *Let $x \in \mathbb{Z}_p$ with $x(0) = 0$. If $y \in \mathbb{Z}_p$ and $py = x$ then $y(k) = x(k+1)$ for $k \geq 0$.*

Proof. By Lemma 2, $(py)(0) = 0$ and $(py)(k) = y(k-1)$ for $k \geq 1$, and as $py = x$ this means $x(0) = 0$ and $x(k) = y(k-1)$ for $k \geq 1$, i.e. $x(k+1) = y(k)$ for $k \geq 0$. □

1.2 Multiplication

For $x, y \in \mathbb{Z}_p$, we define $xy \in \mathbb{Z}_p$ by induction. Define

$$(xy)(0) \equiv x(0)y(0) \pmod{p}, \qquad (xy)(0) \in N_p.$$

Assume for $k \geq 0$ that there is some $A_k \in \mathbb{Z}$ such that

$$\sum_{j=0}^{k} (xy)(j) p^j = A_k p^{k+1} + \left(\sum_{j=0}^{k} x(j) p^j \right) \left(\sum_{j=0}^{k} y(j) p^j \right).$$

There is some $B \in \mathbb{Z}$ such that

$$\left(\sum_{j=0}^{k+1} x(j)p^j\right)\left(\sum_{j=0}^{k+1} y(j)p^j\right)$$

$$=\left(x(k+1)p^{k+1}+\sum_{j=0}^{k} x(j)p^j\right)\left(y(k+1)p^{k+1}+\sum_{j=0}^{k} y(j)p^j\right)$$

$$=Bp^{k+2}+x(k+1)y(0)p^{k+1}+x(0)y(k+1)p^{k+1}+\left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k} y(j)p^j\right).$$

Hence

$$\left(\sum_{j=0}^{k+1} x(j)p^j\right)\left(\sum_{j=0}^{k+1} y(j)p^j\right)=Bp^{k+2}+x(k+1)y(0)p^{k+1}+x(0)y(k+1)p^{k+1}$$
$$+\sum_{j=0}^{k}(xy)(j)p^j-A_kp^{k+1}.$$

Now define

$$(xy)(k+1)\equiv x(k+1)y(0)+x(0)y(k+1)-A_k \pmod p, \qquad (xy)(k+1)\in N_p,$$

and let $C \in \mathbb{Z}$ such that

$$(xy)(k+1)=Cp+x(k+1)y(0)+x(0)y(k+1)-A_k,$$

whence, taking $A_{k+1}=B-C$,

$$\begin{aligned}\left(\sum_{j=0}^{k+1} x(j)p^j\right)\left(\sum_{j=0}^{k+1} y(j)p^j\right)&=Bp^{k+2}+(xy)(k+1)p^{k+1}-Cp^{k+2}+A_kp^{k+1}\\&\quad+\sum_{j=0}^{k}(xy)(j)p^j-A_kp^{k+1}\\&=A_{k+1}p^{k+2}+\sum_{j=0}^{k+1}(xy)(j)p^j.\end{aligned}$$

Thus, for each $k\geq 0$, $(xy)(k)\in N_p$ and

$$\sum_{j=0}^{k}(xy)(j)p^j\equiv\left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k} y(j)p^j\right) \pmod{p^{k+1}}. \tag{2}$$

It is immediate that $xy=yz$.

For $t \in \mathbb{Z}_p$, if for each $k \geq 0$,

$$\sum_{j=0}^{k} t(j)p^j \equiv \left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k} y(j)p^j\right) \pmod{p^{k+1}}.$$

then $t = xy$. Now let $x, y, z \in \mathbb{Z}_p$. For $k \geq 0$,

$$\begin{aligned}
\sum_{j=0}^{k}(x(yz))(j)p^j &\equiv \left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k}(yz)(j)p^j\right) \pmod{p^{k+1}} \\
&\equiv \left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k} y(j)p^j\right)\left(\sum_{j=0}^{k} z(j)p^j\right) \pmod{p^{k+1}} \\
&\equiv \left(\sum_{j=0}^{k}(xy)(j)p^j\right)\left(\sum_{j=0}^{k} z(j)p^j\right) \pmod{p^{k+1}} \\
&\equiv \sum_{j=0}^{k}((xy)z)(j)p^j \pmod{p^{k+1}},
\end{aligned}$$

which shows that $x(yz) = (xy)z$.

Define $u \in \mathbb{Z}_p$ by $u(0) = 1$, $u(k) = 0$ for $k \geq 1$. It is apparent that for $x \in \mathbb{Z}_p$, $xu = x$ and $ux = x$.

1.3 Ring

For $x, y, z \in \mathbb{Z}_p$ and for $k \geq 0$, using (1) and (2),

$$\begin{aligned}
\sum_{j=0}^{k} (x(y+z))(j)p^j &\equiv \left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k} (y+z)(j)p^j\right) \pmod{p^{k+1}} \\
&\equiv \left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k} (y(j)+z(j))p^j\right) \pmod{p^{k+1}} \\
&\equiv \left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k} y(j)p^j\right) \\
&+ \left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k} z(j)p^j\right) \pmod{p^{k+1}} \\
&\equiv \sum_{j=0}^{k} (xy)(j)p^j + \sum_{j=0}^{k} (xz)(j)p^j \pmod{p^{k+1}} \\
&\equiv \sum_{j=0}^{k} (xy+xz)(j)p^j \pmod{p^{k+1}},
\end{aligned}$$

which shows that $x(y+z) = xy + xz$. Therefore $\mathbb{Z}_p$ is a commutative ring with unity $0 \mapsto 1$, $k \mapsto 0$ for $k \geq 1$.

1.4 Integral domain

Let $\mathbb{Z}_p^*$ be the set of those $x \in \mathbb{Z}_p$ for which there is some $y \in \mathbb{Z}_p$ such that $xy = 1$, namely the set of invertible elements of $\mathbb{Z}_p$.

Lemma 4. *Let $x \in \mathbb{Z}_p$. $x \in \mathbb{Z}_p^*$ if and only if $x(0) \neq 0$.*

Proof. If $x(0) = 0$ and $y \in \mathbb{Z}_p$ then $(xy)(0) \equiv x(0)y(0) \equiv 0 \pmod{p}$ while $1(0) \equiv 1 \pmod{p}$, so $xy \neq 1$ and therefore $x \notin \mathbb{Z}_p^*$.

If $x(0) \neq 0$, we define $y \in \mathbb{Z}_p$ by induction. As $x(0) \neq 0$, it makes sense to define

$$y(0)x(0) \equiv 1 \pmod{p}, \qquad y(0) \in N_p.$$

We use (2) and the fact that $1(0) = 1$, $1(k) = 0$ for $k \geq 1$. Suppose for $k \geq 0$ that there is some $A_k \in \mathbb{Z}$ such that

$$\left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k} y(j)p^j\right) = A_k p^{k+1} + 1.$$

Because $x(0) \neq 0$, it makes sense to define

$$y(k+1)x(0) + x(k+1)y(0) \equiv -A_k \pmod{p}.$$

Then

$$\begin{aligned}\left(\sum_{j=0}^{k+1} x(j)p^j\right)\left(\sum_{j=0}^{k+1} y(j)p^j\right) &\equiv x(k+1)y(0)p^{k+1} + y(k+1)x(0)p^{k+1}\\ &\left(\sum_{j=0}^{k} x(j)p^j\right)\left(\sum_{j=0}^{k} y(j)p^j\right) \pmod{p^{k+2}}\\ &\equiv -A_k p^{k+1} + A_k p^{k+1} + 1 \pmod{p^{k+2}}\\ &\equiv 1 \pmod{p^{k+2}}.\end{aligned}$$

This shows that $xy = 1$, thus $x \in \mathbb{Z}_p^*$ and $y = x^{-1}$. $\square$

Theorem 5. *$\mathbb{Z}_p$ is an integral domain.*

Proof. Let $x, y \in \mathbb{Z}_p$ be nonzero. Let $m \geq 0$ be minimal such that $x(m) \neq 0$ and let $n \geq 0$ be minimal such that $y(n) \neq 0$. Then $(p^{-m}x)(0) \neq 0$ and $(p^{-n}y)(0) \neq 0$, and using $p^{-m-n}(xy) = p^{-m}x \cdot p^{-n}y$,

$$\begin{aligned}(xy)(m+n) &\equiv (p^{-m-n}(xy))(0) \pmod{p}\\ &\equiv (p^{-m}x)(0)\cdot(p^{-n}y)(0) \pmod{p}\\ &\not\equiv 0 \pmod{p},\end{aligned}$$

thus $xy \neq 0$. $\square$

1.5 p-adic valuation

For $x \in \mathbb{Z}_p$, let

$$v_p(x) = \inf\{k \geq 0 : x(k) \neq 0\}.$$

$x(k) = 0$ for $0 \leq k < v_p(x)$. $v_p(x) = \infty$ if and only if $x = 0$.

Lemma 6. *For $x, y \in \mathbb{Z}_p$,*

$$v_p(xy) = v_p(x) + v_p(y)$$

and

$$v_p(x+y) \geq \min(v_p(x), v_p(y)).$$

Lemma 4 says that for $x \in \mathbb{Z}_p$, $x \in \mathbb{Z}_p^*$ if and only if $x(0) \neq 0$. In other words,

$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : v_p(x) = 0\} = \{x \in \mathbb{Z}_p : |x|_p = 1\}.$$

For $n \geq 1$, define $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ by

$$\pi_n(x) = \sum_{k=0}^{n-1} x(k)p^k + p^n\mathbb{Z}.$$

It is apparent that π_n is onto.

Lemma 7. *$\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ is a ring homomorphism, and*

$$\ker \pi_n = \{x \in \mathbb{Z}_p : v_p(x) \geq n\} = p^n\mathbb{Z}_p.$$

Proof. Let $x, y \in \mathbb{Z}_p$. By (1),

$$\sum_{k=0}^{n-1}(x+y)(k)p^k + p^n\mathbb{Z} = \sum_{k=0}^{n-1} x(k)p^k + \sum_{k=0}^{n-1} y(k)p^k + p^n\mathbb{Z},$$

i.e.

$$\pi_n(x+y) = \pi_n(x) + \pi_n(y).$$

By (2),

$$\sum_{k=0}^{n-1}(xy)(k)p^k + p^n\mathbb{Z} = \left(\sum_{k=0}^{n-1} x(k)p^k + p^n\mathbb{Z}\right)\left(\sum_{k=0}^{n-1} y(k)p^k + p^n\mathbb{Z}\right),$$

i.e.

$$\pi_n(xy) = \pi_n(x)\pi_n(y).$$

For $1 \in \mathbb{Z}_p$, $1(0) = 1$, $1(k) = 0$ for $k \geq 1$, so

$$\pi_n(1) = 1 + p^n\mathbb{Z},$$

which is the unity of $\mathbb{Z}/p^n\mathbb{Z}$. Therefore π_n is a ring homomorphism.

$\pi_n(x) = 0$ means

$$\sum_{k=0}^{n-1} x(k)p^k \in p^n\mathbb{Z}.$$

But $0 \leq \sum_{k=0}^{n-1} x(k)p^k < \sum_{k=0}^{n-1}(p-1)p^k = p^n - 1$, so $\pi_n(x) = 0$ if and only if $x(k) = 0$ for $0 \leq k \leq n-1$. □

Then for $n \geq 1$,

$$\begin{aligned}\mathbb{Z}_p &= \bigcup_{j=0}^{p^n-1}(j + p^n\mathbb{Z}_p)\\ &= \bigcup_{j=0}^{p^n-1}\{x \in \mathbb{Z}_p : v_p(x-j) \geq n\}\\ &= \bigcup_{j=0}^{p^n-1}\{x \in \mathbb{Z}_p : |x-j|_p \leq p^{-n}\}\\ &= \bigcup_{j=0}^{p^n-1}\{x \in \mathbb{Z}_p : |x-j|_p < p^{-n+1}\}.\end{aligned}$$

Because $\mathbb{Z}/p\mathbb{Z}$ is a field and $\pi_1 : \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ is an onto ring homomorphism,

$$\ker \pi_1 = p\mathbb{Z}_p$$

is a maximal ideal in $\mathbb{Z}_p$.

Theorem 8. *If I is an ideal in $\mathbb{Z}_p$ and $I \neq \{0\}$, then there is some $n \geq 0$ such that $I = p^n \mathbb{Z}_p$.*

Proof. There is some $a \in I$ with minimal $v_p(a) \geq 0$, and as $I \neq \{0\}$, $v_p(a) \neq \infty$. Then $(p^{-v_p(a)}a)(0) = a(v_p(a)) \neq 0$, so by Lemma 4, $p^{-v_p(a)}a \in \mathbb{Z}_p^*$. Hence there is some $u \in \mathbb{Z}_p^*$ such that $p^{-v_p(a)}a = u$, i.e. $p^{v_p(a)} = u^{-1}a$. But I is an ideal and $a \in I$, so $p^{v_p(a)} \in I$, which shows that $p^{v_p(a)}\mathbb{Z}_p \subset I$. Let $x \in I$, $x \neq 0$. Then there is some $v \in \mathbb{Z}_p^*$ such that $p^{-v_p(x)}x = v$, i.e. $x = p^{v_p(x)}v$. Because $v_p(a)$ is minimal, $v_p(x) \geq v_p(a)$ and so

$$x = p^{v_p(x)}v = p^{v_p(a)} \cdot p^{v_p(x)-v_p(a)} \in p^{v_p(a)}\mathbb{Z}_p.$$

Therefore $I = p^{v_p(a)}\mathbb{Z}_p$. □

2 Q_p

Let $\mathbb{Q}_p$ be the set of maps $x : \mathbb{Z} \to N_p$ such that for some $m \in \mathbb{Z}$, $x(k) = 0$ for all $k < m$. For $x \in \mathbb{Q}_p$ define

$$v_p(x) = \inf\{k \in \mathbb{Z} : x(k) \neq 0\}.$$

$x(k) = 0$ for $k < v_p(x)$, $k \in \mathbb{Z}$. $v_p(x) = \infty$ if and only if $x = 0$.

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}.$$

For $m \in \mathbb{Z}$ and $x \in \mathbb{Q}_p$, define

$$(T_m x)(k) = x(k+m), \qquad k \in \mathbb{Z}.$$

For $x \in \mathbb{Q}_p$ with $x(k) = 0$ for $k < m$, if $k < 0$ then $k + m < m$ and so

$$(T_m x)(k) = x(k+m) = 0,$$

which means that $T_m x \in \mathbb{Z}_p$. For $x, y \in \mathbb{Q}_p$ with $x(k) = 0$ and $y(k) = 0$ for $k < m$, $T_m x, T_m y \in \mathbb{Z}_p$ and $T_m x + T_m y \in \mathbb{Z}_p$. Define

$$x + y = T_{-m}(T_m x + T_m y) \in \mathbb{Q}_p.$$

Check that this makes sense. Likewise, $T_m x \cdot T_m y \in \mathbb{Z}_p$, and define

$$xy = T_{-m}(T_m x \cdot T_m y) \in \mathbb{Q}_p.$$

Check that this makes sense. Check that $\mathbb{Q}_p$ is a commutative ring with additive identity $k \mapsto 0$ for $k \in \mathbb{Z}$. and unity $0 \mapsto 1$, $k \mapsto 0$ for $k \neq 0$. Finally,[1]

$$T_m x = p^{-m}x.$$

Theorem 9. *$\mathbb{Q}_p$ is a field, of characteristic 0.*

[1]For a ring R with $x \in R$, $px = \sum_{k=1}^{p} x$. It does not make sense to talk about px before we have $x + y$, and it is nonsense to talk about $p^{-m}x$ for $x \in \mathbb{Q}_p$ before have defined addition on $\mathbb{Q}_p$. This is why I defined T_m rather than initially using $x \mapsto p^{-m}x$; it is incorrect and a sloppy habit to use properties of an object before showing that it exists.

3 Metric

For $x \in \mathbb{Q}_p$ define

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

$|x|_p = 0$ if and only if $x = 0$. For $x, y \in \mathbb{Q}_p$ define

$$d_p(x, y) = |x - y|_p.$$

d_p is an **ultrametric**:

$$d_p(x, z) \le \max(d_p(x, y), d_p(y, z)).$$

Theorem 10. *$\mathbb{Q}_p$ is a topological field.*

Proof. For $(x, y), (u, v) \in \mathbb{Q}_p \times \mathbb{Q}_p$ let

$$\rho((x, y), (u, v)) = \max(d_p(x, u), d_p(y, v)).$$

$d_p(x+y, u+v) = |(x-u)+(y-v)|_p = \max(|x-u|_p, |y-v|_p) = \rho((x, y), (u, v))$, which shows that $(x, y) \mapsto x + y$ is continuous $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$. And

$$d_p(-x, -y) = |-x-y|_p = |-1|_p|x+y|_p = |x+y|_p = d_p(x, y),$$

which shows that $x \mapsto -x$ is continuous $\mathbb{Q}_p \to \mathbb{Q}_p$. For $\rho((x, y), (u, v)) \le \delta$, $|x - u|_p \le \delta$ so $|u|_p \le |x|_p + \delta$ and

$$\begin{aligned} d_p(xy, uv) &= |xy - uv|_p \\ &= |xy - uy + uy - uv|_p \\ &= \max(|xy - uy|_p, |uy - uv|_p) \\ &= \max(|y|_p|x - u|_p, |u|_p|y - v|_p) \\ &\le \max(|y|_p\delta, (|x|_p + \delta)\delta), \end{aligned}$$

which shows that $(x, y) \mapsto xy$ is continuous $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$. Finally, for $x, y \ne 0$,

$$d_p(x^{-1}, y^{-1}) = |x^{-1} - y^{-1}|_p = |xy|_p^{-1}|y - x|_p,$$

which shows that $x \mapsto x^{-1}$ is continuous $\mathbb{Q}_p \setminus \{0\} \to \mathbb{Q}_p \setminus \{0\}$. $\square$

For $x \in \mathbb{Q}_p$ and $r > 0$, write

$$B_{<r}(x) = \{y \in \mathbb{Q}_p : |y - x|_p < r\}, \quad B_{\le r}(x) = \{y \in \mathbb{Q}_p : |y - x|_p < r\}.$$

Thus, for $x \in \mathbb{Q}_p$ and $n \ge 0$,

$$x + p^n\mathbb{Z} = B_{\le p^{-n}}(x).$$

Lemma 11. *For $x \in \mathbb{Q}_p$,*

$$\{x + p^n\mathbb{Z}_p : n \ge 0\}$$

is a local base at x.

Proof. For $\epsilon > 0$, let $p^{-n} < \epsilon$, $n \geq 0$, namely $n > \frac{1}{\log p} \log \frac{1}{\epsilon}$. For this n,

$$x + p^n \mathbb{Z}_p = B_{\leq p^{-n}}(x) \subset B_{<\epsilon}(x).$$

□

Theorem 12. *$\mathbb{Z}_p$ is a compact subspace of $\mathbb{Q}_p$.*

Proof. Let $x_n \in \mathbb{Z}_p$ be a sequence. Because $x_n(0) \in N_p$, $n \geq 0$, there is some $a(0) \in N_p$ and an infinite subset I_0 of $\{n \geq 0\}$ such that $x_n(0) = a(0)$ for $n \in I_0$. Suppose by induction that for some $N \geq 0$ there are $a(0), \ldots, a(N) \in N_p$ and an infinite set $I_N \subset \{n \geq 0\}$ such that

$$x_n(k) = a(k), \qquad 0 \leq k \leq N, \quad n \in I_N.$$

But for each $x \in I_N$, $x_n(N+1)$ belongs to the finite set N_p, and because I_N is infinite there is some $a(N+1) \in N_p$ and an infinite set $I_{N+1} \subset I_N$ such that $x_n(N+1) = a(N+1)$ for $n \in I_{N+1}$. We have thus defined $a \in \mathbb{Z}_p$.

Let $\alpha_0 \in I_0$, and by induction let $\alpha_n > \alpha_{n-1}$, $\alpha_n \in I_n$; in particular as $\alpha_0 \geq 0$ we have $\alpha_n \geq n$. Then for any $n \geq 0$, $x_{\alpha_n}(k) = a(k)$ for $0 \leq k \leq n$. Take $\epsilon > 0$ and let $p^{-m-1} < \epsilon$. For $n \geq m$,

$$|x_{\alpha_n} - a|_p \leq p^{-n-1} \leq p^{-m-1} < \epsilon,$$

which shows that the sequence x_{α_n} tends to a. This means that $\mathbb{Z}_p$ is sequentially compact and therefore compact. □

For $x, y \in \mathbb{Q}_p$,

$$d_p(px, py) = |px - py|_p = |p|_p |x - y|_p = p^{-1} |x - y|_p,$$

which shows that $x \mapsto px$ is continuous $\mathbb{Q}_p \to \mathbb{Q}_p$. Therefore, the fact that $\mathbb{Z}_p$ is compact implies that for $n \geq 0$, $p^n \mathbb{Z}_p$ is compact. Then by Lemma 11 we get the following.

Theorem 13. *$\mathbb{Q}_p$ is locally compact.*

Theorem 14. *$\mathbb{Q}_p$ is a complete metric space.*

A topological space X is **zero-dimensional** if there is a base for its topology each element of which is clopen. In a Hausdorff space, a compact set is closed, and because the sets $p^n \mathbb{Z}_p$ are compact, $n \geq 0$, from Lemma 11 we get the following.

Lemma 15. *$\mathbb{Q}_p$ is zero-dimensional.*

It is a fact that if a Hausdorff space is zero-dimensional then it is **totally disconnected**, so by the above, $\mathbb{Q}_p$ is totally disconnected.

4 p-adic fractional part

For $x \in \mathbb{Q}_p$, let

$$[x]_p = \sum_{k \geq 0} x(k) p^k \in \mathbb{Z}_p$$

and

$$\{x\}_p = \sum_{k<0} x(k) p^k \in \mathbb{Z}[1/p] \subset \mathbb{Q}.$$

We call $\{x\}_p$ the **p-adic fractional part of** x. Then

$$x = [x]_p + \{x\}_p \in \mathbb{Q}_p.$$

Furthermore, as $x(k) \to 0$ as $k \to -\infty$,

$$0 \leq \{x\}_p < \sum_{k<0} (p-1) p^k = (p-1) \sum_{k=1}^{\infty} p^{-k} = 1,$$

therefore for $x \in \mathbb{Q}_p$,

$$\{x\}_p \in [0,1) \cap \mathbb{Z}[1/p].$$

Define the **Prüfer p-group**

$$\mathbb{Z}(p^\infty) = \{e^{2\pi i m p^{-n}} : m, n \geq 0\}.$$

We assign the Prüfer p-group the discrete topology.

Define $\psi_p : \mathbb{Q}_p \to S^1$ by

$$\psi_p(x) = e^{2\pi i \{x\}_p}.$$

We prove that this is a homomorphism from the locally compact group $\mathbb{Q}_p$ whose image is the Prüfer p-group and whose kernel is $\mathbb{Z}_p$.[2]

Theorem 16. *$\psi_p : \mathbb{Q}_p \to S^1$ is a homomorphism of locally compact groups. $\psi_p(\mathbb{Q}_p) = \mathbb{Z}(p^\infty)$, and $\ker \psi_p = \mathbb{Z}_p$.*

Proof. For $x, y \in \mathbb{Q}_p$,

$$\begin{aligned} \{x+y\}_p - \{x\}_p - \{y\}_p &= x + y - [x+y]_p - x + [x]_p - y + [y]_p \\ &= [x]_p + [y]_p - [x+y]_p \in \mathbb{Z}_p. \end{aligned}$$

Check that $\mathbb{Z}[1/p] \cap \mathbb{Z}_p = \mathbb{Z}$. It then follows that

$$\{x+y\}_p - \{x\}_p - \{y\}_p \in \mathbb{Z},$$

therefore $e^{2\pi i (\{x+y\}_p - \{x\}_p - \{y\}_p)} = 1$, i.e.

$$\psi_p(x+y) = e^{2\pi i \{x+y\}_p} = e^{2\pi i \{x\}_p} e^{2\pi i \{y\}_p} = \psi_p(x)\psi_p(y), \qquad x, y \in \mathbb{Q}_p,$$

[2] Alain M. Robert, *A Course in p-adic Analysis*, p. 42, Proposition 5.4.

namely ψ_p is a homomorphism.

$\psi_p(x) = 1$ if and only if $e^{2\pi i\{x\}_p} = 1$ if and only if $\{x\}_p \in \mathbb{Z}$. But $\{x\}_p \in [0,1)$, so $\psi_p(x) = 1$ if and only if $\{x\}_p = 0$, hence $\psi_p(x) = 1$ if and only if $x \in \mathbb{Z}_p$, namely

$$\ker \psi_p = \mathbb{Z}_p.$$

Let $x \in \mathbb{Q}_p$. As $\{x\}_p \in \mathbb{Z}[1/p]$, there is some $n \geq 0$ such that $p^n\{x\}_p \in \mathbb{Z}$, so $\psi_p(x)^{p^n} = 1$, which means that $\psi_p(x) \in \mathbb{Z}[p^\infty]$. Let $e^{2\pi imp^{-n}} \in \mathbb{Z}[p^\infty]$, $n, m \geq 0$. But $p^{-n} \in \mathbb{Q}_p$ and, whether or not $n > 0$,

$$\psi_p(p^{-n}) = e^{2\pi i\{p^{-n}\}_p} = e^{2\pi ip^{-n}},$$

and $mp^{-n} \in \mathbb{Q}_p$, and using that ψ_p is a homomorphism,

$$\psi_p(mp^{-n}) = \psi_p(p^{-n})^m = e^{2\pi imp^{-n}}.$$

This shows that $\psi_p(\mathbb{Q}_p) = \mathbb{Z}[p^\infty]$.

Finally, let $x \in \mathbb{Q}_p$. For $y \in B_{\leq 1}(x) = x + \mathbb{Z}_p$, so there is some $w \in \mathbb{Z}_p$ such that $y = x + w$. But $\psi_p(x + w) = \psi_p(x)\psi_p(w) = \psi_p(x)$, so

$$|\psi_p(y) - \psi_p(x)| = |\psi_p(x) - \psi_p(x)| = 0,$$

showing that ψ_p is continuous at x. $\square$

Because $\mathbb{Z}[p^\infty]$ is discrete, it is immediate that ψ_p is an open map. The **first isomorphism theorem for topological groups** states that if G and H are locally compact groups, $f : G \to H$ is a homomorphism of topological groups that is onto and open, then $G/\ker f$ and H are isomorphic as topological groups. Therefore the quotient group $\mathbb{Q}_p/\mathbb{Z}_p$ and the Prüfer group $\mathbb{Z}[p^\infty]$ are isomorphic as topological groups.