6 p-Adic Number Field and Arithmetic

It is well-known that the rational number field $\mathbb{Q}$ is not complete with respect to the ordinary absolute value. Therefore, by Theorem 4.8, it admits a unique completion which is the real number field $\mathbb{R}$. Now, the same question applies to $\mathbb{Q}$ with respect to $|\cdot|_p$. It can be proved, for example in [8], that $\mathbb{Q}$ is still not complete with respect to $|\cdot|_p$. Again, it admits a unique completion $\mathbb{Q}_p$, which is called the p-adic number field. In this section, we will concentrate on $\mathbb{Q}_p$ and investigate its new and odd properties both in algebraic and topological situation. Furthermore, we will do some arithmetic like the classical case.

First, we summarize some fundamental properties without proof obtained from the previous sections.

Theorem 6.1 *Let p be a prime number. Then there exists unique complete valuated field $\mathbb{Q}_p$ whose valuation is also denoted by $|\cdot|_p$ which extends $|\cdot|_p$ on $\mathbb{Q}$.*

Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. From the proof of Theorem 5.2, we know that each element $x \in \mathbb{Q}_p$ is represented by a Cauchy sequence $\{a_n\}$ in $\mathbb{Q}$ with respect to $|\cdot|_p$, and

$$|x|_p = \lim_{n\to\infty} |a_n|_p .$$

Therefore, the value group of $|\mathbb{Q}_p^*| = \{p^n | n \in \mathbb{Z}\}$ which is also discrete by Theorem 3.6. In particular, $\mathbb{Q}$ and $\mathbb{Q}_p$ have the same value group with respect to $|\cdot|_p$.

The valuation ring of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$, i.e.

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p | \, |x|_p \leq 1\},$$

its maximal ideal is

$$P = \{x \in \mathbb{Q}_p | \, |x|_p < 1\},$$

and its group of units is

$$U = \{x \in \mathbb{Q}_p | \, |x|_p = 1\}.$$

Elements in $\mathbb{Q}_p$ and $\mathbb{Z}_p$ are called p-adic numbers and p-adic integers, respectively.

As we mentioned above, $\mathbb{Q}$ and $\mathbb{Q}_p$ have the same value group with respect to $|\cdot|_p$, all the topological properties proved in section 3 hold also for $\mathbb{Q}_p$. We will use them without mentioning.

Now, we come to another point. In elementary school, we all know that every real number x has essentially unique decimal representation, namely,

$$\begin{aligned} x &= a_{-n}\cdots a_{-1}a_0.a_1a_2\cdots \\ &= \sum_{j=-n}^{\infty} a_j 10^{-j}, \end{aligned}$$

where $0 \le a_j \le 9$ are digits. We will prove a well-known similar result in the p-adic case. The proof below is taken from [6]. First, we deal with the case of p-adic integers.

Lemma 6.2 *Let $x \in \mathbb{Q}$ and $|x|_p \le 1$. Then, for each $i \in \mathbb{N}$, there exists a unique $\alpha \in \{0, 1, 2, \ldots, p^i - 1\}$ such that*

$$|\alpha - x|_p \le p^{-i}.$$

Proof. Write $x = \frac{a}{b}$, $a, b \in \mathbb{Z}$ and $(a, b) = 1$. Since $|x|_p \le 1$, $(p, b) = 1$, hence, $(p^i, b) = 1$. Choose $m, n \in \mathbb{Z}$ such that $mb + np^i = 1$. Set $\beta = am$. Then

$$\begin{aligned} |\beta - x|_p &= |am - x|_p \\ &= \left| am - \frac{a}{b} \right|_p \\ &= \left| \frac{a}{b} \right|_p |mb - 1|_p \\ &\le |mb - 1|_p \\ &= \left| np^i \right|_p \\ &\le p^{-i}. \end{aligned}$$

If $\beta \in \{0, 1, 2, \ldots, p^i - 1\}$, then we choose $\alpha = \beta$. Now, assume that $\beta \notin \{0, 1, 2, \ldots, p^i - 1\}$. We divide the proof into two cases:

(1) $\beta > 0$. Write $\beta = a_0 + a_1 p + \cdots + a_t p^t$ in the base p, where $0 \le a_j \le p-1$, for all $0 \le j \le t$. Then $t \ge i$. Let

$$\alpha = a_0 + a_1 p + \cdots + a_{i-1} p^{i-1}.$$

Then $\alpha \in \{0, 1, 2, \ldots, p^i - 1\}$ and

$$\begin{aligned} |\,\alpha - x\,|_p &= |\,\alpha - \beta + \beta - x\,|_p \\ &\le \max\{|\,\alpha - \beta\,|_p, |\,\beta - x\,|_p\} \\ &\le p^{-i}. \end{aligned}$$

(2) $\beta < 0$. In this case, as above, $\beta = -(a_0 + a_1 p + \cdots + a_t p^t)$, where a_j and t are as in (i). Then $\beta + p^{t+1} > 0$ and

$$\begin{aligned} \left|\,\beta + p^{t+1} - x\,\right|_p &\le \max\{|\,\beta - x\,|_p, \left|\,p^{t+1}\,\right|_p\} \\ &\le \max\{p^{-i}, p^{-(t+1)}\} \\ &\le p^{-i} \text{ since } t \ge i. \end{aligned}$$

Apply the argument as in (1) to get an $\alpha \in \{0, 1, 2, \ldots, p^i - 1\}$ such that

$$|\,\alpha - x\,|_p \le p^{-i}.$$

Finally, to show that such α is unique. If α' is another such one satisfying

$$\left|\,\alpha^{'} - x\,\right|_p \le p^{-i}.$$

Then

$$\begin{aligned} |\,\alpha - \alpha'\,|_p &= \left|\,\alpha - x + x - \alpha^{'}\,\right|_p \\ &\le \max\{|\,\alpha - x\,|_p, \left|\,\alpha^{'} - x\,\right|_p\} \\ &\le p^{-i}, \end{aligned}$$

which is impossible since the highest power in α and $\alpha^{'}$ is at most $i-1$. Therefore, $\alpha = \alpha^{'}$. ❑

Theorem 6.3 *Let $x \in \mathbb{Z}_p$. Then x has a unique representation by Cauchy sequence $\{x_i\}$ in $\mathbb{Q}$ such that*

(i) $x_i \in \mathbb{Z}$, $0 \le x_i \le p^i - 1$ *for* $i = 1, 2, \ldots$

(ii) $x_i \equiv x_{i+1} (\mathrm{mod}\ p^i)$ *for* $i = 1, 2, \ldots$

Proof. Let $\{y_i\}$ be a Cauchy sequence in $\mathbb{Q}$ which represents x. For each $j \in \mathbb{N}$, there exists $N_j \in \mathbb{N}$ such that, for all $i, i' \ge N_j$, we have

$$| y_i - y_{i'} |_p \le p^{-j}$$

Obviously, we may take $\{N_j\}$ to be strictly increasing so that $N_j \ge j$. Note that if $i \ge N_j$, then, for all $i' \ge N_j$,

$$\begin{aligned} | y_i |_p &= | y_i - y_{i'} + y_{i'} |_p \\ &\le \max\{ | y_i - y_{i'} |_p , | y_{i'} |_p \} \\ &\le \max\{ p^{-j}, | y_{i'} |_p \} \end{aligned}$$

and, since, $\lim_{i' \to \infty} | y_{i'} |_p = | x |_p \le 1$, we have $| y_i |_p \le 1$. In particular,

$$\left| y_{N_j} \right|_p \le 1.$$

By Lemma 6.2, there exists integer x_j, $0 \le x_j \le p^j - 1$ such that

$$\left| x_j - y_{N_j} \right|_p \le \frac{1}{p^j}$$

which is true for all $j = 1, 2, \ldots$.

Claim 1. $x_j \equiv x_{j+1} (\mathrm{mod}\ p^j)$ for all $j = 1, 2, \ldots$.

$$\begin{aligned} | x_{j+1} - x_j |_p &= \left| x_{j+1} - y_{N_{j+1}} + y_{N_{j+1}} - y_{N_j} + y_{N_j} - x_j \right|_p \\ &\le \max\{ \left| x_{j+1} - y_{N_{j+1}} \right|_p , \left| y_{N_{j+1}} - y_{N_j} \right|_p , \left| y_{N_j} - x_j \right|_p \} \\ &\le \max\{ p^{-(j+1)}, p^{-j}, p^{-j} \} \\ &= p^{-j}. \end{aligned}$$

Therefore, $x_j \equiv x_{j+1} (\mathrm{mod}\ p^j)$.

Claim 2. $\{y_j\}$ and $\{x_j\}$ are equivalent Cauchy sequences in $\mathbb{Q}$. In particular, x is represented by $\{x_j\}$. For all $i \geq N_j$,

$$\begin{aligned} |\, x_i - y_i \,|_p &= \left|\, x_i - x_j + x_j - y_{N_j} + y_{N_j} - y_i \,\right|_p \\ &\leq \max\{|\, x_i - x_j \,|_p, \left|\, x_j - y_{N_j} \,\right|_p, \left|\, y_{N_j} - y_i \,\right|_p\} \\ &\leq \max\{p^{-j}, p^{-j}, p^{-j}\} \\ &= p^{-j}, \end{aligned}$$

which implies that $\lim_{i\to\infty} |\, x_i - y_i \,|_p = 0$, i.e. $\{x_i\}$ and $\{y_i\}$ are equivalent. Therefore, we have proved the existence of sequence satisfies (i) and (ii).

Finally, if $\{x_i^{'}\}$ is another such sequence representing x and $\{x_i^{'}\} \neq \{x_i\}$, say $x_j^{'} \neq x_j$, then $x_j^{'} \not\equiv x_j (\mathrm{mod}\ p^j)$ since $0 \leq x_j^{'}, x_j \leq p^j - 1$. It follows from (ii) that, for all $i > j$,

$$x_i^{'} \equiv x_j^{'} \not\equiv x_j \equiv x_i (\mathrm{mod}\ p^j),$$

which means that

$$\left|\, x_i^{'} - x_i \,\right|_p > p^{-j}$$

for all $i \geq j$. Hence $\{x_i\}$ and $\{x_i^{'}\}$ are not equivalent. This shows that $\{x_i\}$ is a unique such sequence. ❑

In order to deal with all $x \in \mathbb{Q}_p$, we need another simple lemma.

Lemma 6.4 *Let $x \in \mathbb{Q}_p$. Then there exists a unique $u \in U$, where U is the group of units in $\mathbb{Z}_p$, such that*

$$x = up^{\mathrm{ord}_p\, x}.$$

Proof. We know that $|\, x \,|_p = p^{-\mathrm{ord}_p\, x}$ which implies that

$$\left|\, xp^{-\mathrm{ord}_p\, x} \,\right|_p = 1.$$

Set

$$u = xp^{-\mathrm{ord}_p\, x}.$$

Then $|\, u \,|_p = 1$, i.e., $u \in U$, and

$$x = up^{\mathrm{ord}_p\, x}.$$

The uniqueness of u is obvious from the expression of u. ❑

Combine Lemma 6.4 and Theorem 6.3, we have

Corollary 6.5 *If $x \in \mathbb{Q}$ with $|\, x \,|_p > 1$, then $xp^{-\mathrm{ord}_p\, x}$ has a unique representation by Cauchy sequence $\{x_n\}$ in $\mathbb{Q}$ satisfying (i) and(ii) in Theorem 6.3.*

Definition 6.6 *The sequence $\{x_n\}$ representing an element $x \in \mathbb{Z}_p$ satisfying Theorem 6.3 is called the canonical p-adic representation of x.*

Now, given $x \in \mathbb{Z}_p$, x has a canonical p-adic representation $\{x_n\}$. Since $x_n \in \mathbb{Z}$ and satisfies (i) and (ii) in Theorem 6.3, we may write, for all $n = 1, 2, \ldots$,

$$x_n = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$$

and

$$x_{n+1} = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} + a_n p^n,$$

where $a_i \in \{0, 1, 2, \ldots, p-1\}$ for all $0 \le i \le n$, called the p-adic digits. Note that

$$\lim_{n\to\infty} x_n = x \text{ with respect to } |\cdot|_p$$

implies that the p-adic series (see section 7) $\sum_{n=0}^{\infty} a_n p^n$ converges to x, i.e.

$$x = \sum_{n=0}^{\infty} a_n p^n.$$

As usual, we may write

$$x = \cdots a_2 a_1 a_0$$

For $x \in \mathbb{Q}_p$ with $|\, x \,|_p > 1$, by Corollary 6.5, $xp^{-\mathrm{ord}_p\, x}$ has a canonical representation, say,

$$xp^{-\mathrm{ord}_p\, x} = \sum_{n=0}^{\infty} a_n p^n.$$

Since $|\, x \,|_p > 1$, $\mathrm{ord}_p\, x < 0$, write $-m = \mathrm{ord}_p\, x$, $m \in \mathbb{N}$, we have

$$x = \sum_{n=0}^{\infty} a_n p^{n-m}.$$

We may write

$$\begin{aligned} x &= \sum_{n=-m}^{\infty} b_n p^n, \\ &= \cdots b_2 b_1 b_0 . b_{-1} \cdots b_{-m} \end{aligned}$$

where $b_j's$ are also p-adic digits. Such expression is also called the canonical p-adic representation of x.

Remark.

(1) Every p-adic number admits a canonical p-adic representation.

(2) The sequence in (2) of Example 3.5, indeed, converge to a number in $\mathbb{Q}_p$.

From the above results, we have the following consequences.

Corollary 6.7 *We have*

(i) *Let $x \in \mathbb{Z}_p$ and $x = \sum_{n=j}^{\infty} a_n p^n$ be the canonical p-adic representation of x. Then $|\, x \,|_p = p^{-j}$.*

(ii) *The ring of p-adic integers $\mathbb{Z}_p = \{\sum_{n=0}^{\infty} a_n p^n | 0 \le a_n \le p-1 \ for \ \ all \ n = 1, 2, \ldots\}$.*

(iii) *The group of units in $\mathbb{Z}_p$ is $U = \{\sum_{n=0}^{\infty} a_n p^n | a_0 \neq 0\}$.*

In the remaining of this section, we will see how to find the canonical p-adic representation of a p-adic number and to operate the usual "carrying" and "borrowing" in the p-adic case.

Example 6.8 *Canonical p-adic representation of some p-adic numbers:*

(1)

$$1 = \sum_{n=0}^{\infty} a_n p^n, \text{ where } a_0 = 1 \text{ and } a_n = 0 \text{ for all } n \geq 1$$
$$= \cdots 0001$$

(2)

$$-1 = \sum_{n=0}^{\infty} a_n p^n, \text{ where } a_n = p-1 \text{ for all } n = 0, 1, 2, \cdots$$
$$= \cdots (p-1)(p-1)(p-1)$$

In fact, from $(-1) + 1 = 0$ *to get* $a_0 = a_1 = a_2 = \cdots = p - 1$.

(3) $\frac{1}{4} = \sum_{n=0}^{\infty} a_n p^n$ *with* $p = 5$. *To find* a_n:

$$\frac{1}{4} \equiv a_0 (\text{mod } 5);\ 1 \equiv 4a_0 (\text{mod } 5);\ a_0 = 4$$

$$\frac{1}{4} \equiv a_0 + a_1 p (\text{mod } 5^2);\ \frac{1}{4} - 4 \equiv 5a_1 (\text{mod } p^2);\ \frac{-15}{4} \equiv 5a_1 (\text{mod } p^2)$$

$$-\frac{3}{4} \equiv a_1 (\text{mod } 5);\ -3 \equiv 4a_1 (\text{mod } 5);\ 2 \equiv 4a_1 (\text{mod } 5)$$

$$1 \equiv 2a_1 (\text{mod } 5);\ a_1 = 3.$$

Continuing this way, we obtain

$$\frac{1}{4} = \cdots 333334$$

(4) $-3 = \sum_{n=0}^{\infty} a_n p^n$ *with* $p = 7$. *To find* a_n:

$$-3 \equiv a_0 (\text{mod } 7);\ a_0 = 4.$$

$$-3 \equiv 4 + a_1 p (\text{mod } 7^2);\ -7 \equiv 7a_1 (\text{mod } 7^2);\ -1 \equiv a_1 (\text{mod } 7);\ a_1 = 6.$$

$$-3 \equiv 4 + 6p + a_2 p^2 (\text{mod } 7^3);\ -3 \equiv 4 + 42 + 49a_2 (\text{mod } 7^3);$$

$$-49 \equiv 49a_2 (\text{mod } 7^3);\ -1 \equiv a_2 (\text{mod } 7);\ a_2 = 6$$

$$-3 \equiv 4 + 6p + 6p^2 + a_3 p^3 (\text{mod } 7^4);\ -343 \equiv 7^3 a_3 (\text{mod } 7^4);$$

$$-1 \equiv a_3 (\text{mod } 7);\ a_3 = 6.$$

Continuing this way, we get

$$-3 = \cdots 66664.$$

(5) $\frac{3}{7} = \sum_{n=0}^{\infty} a_n p^n$ *with* $p = 2$. *To find* a_n*:*

$$\frac{3}{7} \equiv a_0 (\text{mod } 2);\ 3 \equiv 7a_0 (\text{mod } 2);\ a_0 = 1.$$

$$\frac{3}{7} \equiv 1 + a_1 p (\text{mod } 2^2);\ -\frac{4}{7} \equiv 2a_1 (\text{mod } 2^2);\ -4 \equiv 14a_1 (\text{mod } 2^2);\ -2 \equiv 7a_1 (\text{mod } 2);\ a_1 = 0.$$

$$\frac{3}{7} = 1 + 0p + a_2 p^2 (\text{mod } 2^3);\ -\frac{4}{7} \equiv 4a_1 (\text{mod } 2^3);\ -\frac{1}{7} \equiv a_2 (\text{mod } 2);\ -1 \equiv 7a_2 (\text{mod } 2);\ a_2 = 1.$$

$$\frac{3}{7} = 1 + 0p + p^2 + a_3 p^3 (\text{mod } 2^4);\ -\frac{32}{7} \equiv 8a_3 (\text{mod } 2^4);\ -\frac{4}{7} \equiv a_3 (\text{mod } 2);\ -4 \equiv 7 (\text{mod } 2);\ a_3 = 0.$$

Continuing this way, we obtain that

$$\frac{3}{7} = \cdots 010101.$$

Example 6.9 *Using carrying and borrowing, we can evaluate the following sum, difference, product and division of p-adic numbers.*

(1) $p = 2$

$$\cdots 100101001 + \cdots 011011011 = \cdots 000000100.$$

(2) $p = 5$

$$(\cdots 134134134) - (\cdots 222222222) = \cdots 411411412.$$

(3) $p = 3$

$$(\cdots 122122122) \times (\cdots 121212121) = \cdots 112221002.$$

(4) $p = 5$

$$(\cdots 121212) \div (\cdots 343434) = \cdots 124124.$$