Chapter 2
Some Arithmetic and Analysis in $\mathbb{Q}_p$; Derivatives in Ultrametric Analysis

Abstract In this chapter, we discuss some arithmetic and analysis in the p-adic field. We also introduce the concepts of differentiability and derivatives in ultrametric analysis and briefly indicate how ultrametric calculus is different from our usual calculus.

Keywords Valuation ring · Residue class field · Canonical expansion · Differentiability · Derivatives

We need the following results in the sequel.

Theorem 2.1 *Let $|\cdot|$ be an ultrametric valuation of K. Then the set $V \subseteq K$ of all elements a such that $|a| \leq 1$ is a ring with identity. The set $P \subseteq V$ of all elements a such that $|a| < 1$ is the unique maximal ideal of V and P is also a prime ideal.*

Proof If $a, b \in V$, then $|ab| = |a||b| \leq 1$ and so $ab \in V$. Again,

$$|a - b| \leq \max(|a|, |b|) \leq 1,$$

so that $a - b \in V$. Thus V is a ring. Also $1 \in V$. Now, if $a, b \in P$,

$$|a + b| \leq \max(|a|, |b|) < 1,$$

and so $a + b \in P$. If $a \in P$, $b \in V$, then

$$|ba| = |b||a| < 1,$$

so $ba \in P$. Thus P is an ideal of V. Further, if $a \in V$ and if $a \notin P$, then $|a| = 1$. Now,

$$1 = |1| = |a.a^{-1}| = |a||a^{-1}|,$$

so that $|a^{-1}| = 1$. It now follows that P is the unique maximal ideal of V. Since $1 \in V$, P is also a prime ideal, completing the proof. □

P.N. Natarajan, *An Introduction to Ultrametric Summability Theory*,
Forum for Interdisciplinary Mathematics 2, DOI 10.1007/978-81-322-2559-1_2

The ring V is called the "valuation ring" associated with the ultrametric valuation $|\cdot|$. The field V/P is called the associated "residue class field".

Theorem 2.2 *If $|\cdot|$ is an ultrametric valuation of K and $\hat{K}$ is the completion of K, then $|K| = |\hat{K}|$, where $|K|$ is the image of K in $\mathbb{R}$ under the valuation $|\cdot|$ and $|\hat{K}|$ is the image of $\hat{K}$ in $\mathbb{R}$ under the extended valuation (for the notion of extended valuation, see [1]), which we denote by $|\cdot|$ again.*

Proof Let $\alpha \in \hat{K}$. If $\alpha = 0$, $|\alpha| = 0$. So let $\alpha \neq 0$. Since K is dense in $\hat{K}$, there exists a sequence $\{a_n\}$ in K such that $\lim_{n\to\infty} a_n = \alpha$. Now, since $|\cdot|$ is an ultrametric valuation,

$$|a_n| = |\alpha + (a_n - \alpha)| = \max(|\alpha|, |a_n - \alpha|) = |\alpha|,$$

for sufficiently large n, since $|\alpha| \neq 0$, $|a_n - \alpha|$ can be made arbitrarily small for sufficiently large n. Thus $|\hat{K}| \subseteq |K|$. The reverse inclusion is trivial. This proves the theorem. □

Theorem 2.3 *Any $\alpha \in \mathbb{Q}_p$ can be written as*

$$\alpha = \sum_{j=n}^{\infty} a_j p^j, \tag{2.1}$$

where $a_j \in \mathbb{Z}$, $j = n, n+1, \ldots$ and n is such that $|\alpha|_p = |p|_p^n$.

Proof Let $\alpha \in Q_p$, $\alpha \neq 0$. In view of Theorem 2.2,

$$|\mathbb{Q}_p|_p = |\mathbb{Q}|_p = \{|p|_p^n, n = 0, \pm 1, \pm 2, \ldots\}$$

so that

$$|\alpha|_p = |p|_p^n \text{ for some } n \in \mathbb{Z}. \tag{2.2}$$

Let $\beta = \frac{\alpha}{p^n}$ so that $|\beta|_p = 1$. Let V, P respectively denote the valuation ring of $|\cdot|_p$ on $\mathbb{Q}$ and the unique maximal ideal of V; let $\hat{V}$, $\hat{P}$ respectively denote the valuation ring of $|\cdot|_p$ on $\mathbb{Q}_p$ and the unique maximal ideal of $\hat{V}$. Now, $\beta \in \hat{V}$ and so $\beta = \lim_{k\to\infty} c_k$, $c_k \in \mathbb{Q}$, $k = 0, 1, 2, \ldots$. There exists a positive integer N (depending on n) such that $|\beta - c_k|_p < 1$, $k \geq N$. In particular, $|\beta - c_N|_p < 1$. Consequently,

$$|c_N|_p = |\beta + (c_N - \beta)|_p = \max(|\beta|_p, |c_N - \beta|_p) = 1,$$

since $|\cdot|_p$ is an ultrametric valuation. Since $c_N \in \mathbb{Q}$ and $|c_N|_p = 1$, $c_N \in V$. Let us write $c_N = b_n$. $|\beta - b_n|_p = |\beta - c_N|_p < 1$ and so $\beta - b_n \in \hat{P}$. Thus $\beta + \hat{P} = b_n + \hat{P}$. Since $|b_n|_p = 1$, $b_n \in \mathbb{Q}$, $b_n = \frac{e_n}{d_n}$, $e_n, d_n \in \mathbb{Z}$, e_n, d_n are prime to p. Thus there exist integers x, y such that

$$xd_n + yp = 1,$$

$$i.e., xd_n \equiv 1(mod\ p).$$

Then,

$$\begin{aligned} b_n - e_n x &= \frac{e_n}{d_n} - e_n x \\ &= e_n\left(\frac{1}{d_n} - x\right) \\ &= \frac{e_n(1 - d_n x)}{d_n} \\ &\equiv 0(mod\ p) \end{aligned}$$

so that $|b_n - e_n x|_p < 1$. Thus $b_n - e_n x \in P$ and so $b_n - e_n x \in \hat{P}$. Let $a_n = e_n x$. Then $a_n \in \mathbb{Z}$ and $|b_n - a_n|_p < 1$, i.e., $b_n - a_n \in \hat{P}$ and so $b_n + \hat{P} = a_n + \hat{P}$. Already $\beta + \hat{P} = b_n + \hat{P}$ so that $\beta + \hat{P} = a_n + \hat{P}$. Thus $\beta - a_n \in \hat{P}$ and so $|\beta - a_n|_p < 1$. We note that $|a_n|_p = |(a_n - \beta) + \beta|_p = \max(|a_n - \beta|_p, |\beta|_p) = 1$. We now have

$$\begin{aligned} \alpha = \beta p^n &= a_n p^n + (\beta - a_n) p^n \\ &= a_n p^n + \gamma_1, \end{aligned}$$

where $\gamma_1 = (\beta - a_n) p^n$.

$$|\gamma_1|_p = |(\beta - a_n) p^n|_p = |\beta - a_n|_p |p|_p^n < |p|_p^n.$$

So

$$|\gamma_1|_p = |p|_p^m, \quad \text{where } m > n, \tag{2.3}$$

which is similar to (2.2). Treating γ_1 like α and continuing the process, after k steps, we get

$$\alpha = a_n p^n + a_{n+1} p^{n+1} + \cdots + a_{n+k-1} p^{n+k-1} + \gamma_k,$$

where $a_i \in \mathbb{Z}$, $i = n, n+1, \ldots, n+k-1$, $|a_i|_p = 1$ or 0 and

$$|\gamma_k|_p < |p|_p^{n+k} \to 0, k \to \infty,$$

since $|p|_p < 1$. This completes the proof of the theorem. □

The integer coefficients of (2.1) are only unique modulo p. So if we agree to choose the a_i's such that $0 \le a_i \le p - 1$, then (2.1) is called the "canonical representation or expansion" of α.

We shall illustrate the above with an example. We shall find the canonical expansion of $\frac{3}{8}$ in $\mathbb{Q}_5$. We shall follow the notation used in Theorem 2.3. Since $\left|\frac{3}{8}\right|_5 = |5|_5^0 = 1$, we see that $n = 0$. A solution of

$$8x \equiv 1(mod\ 5)$$

is $x = 2$. Since $3 \cdot 2 \equiv 1(mod\ 5)$, $a_0 = 1$. Now,

$$\gamma_1 = \left(\frac{3}{8} - 1\right) 5^0 = -\frac{5}{8}.$$

We repeat the above procedure for γ_1. $|\gamma_1|_5 = \left|-\frac{5}{8}\right|_5 = |5|_5^1$. Now, $-\frac{5}{8} \cdot \frac{1}{5} = -\frac{1}{8}$. Again, a solution of

$$8x \equiv 1(mod\ 5)$$

is $x = 2 \cdot (-1) \cdot 2 \equiv 3(mod\ 5)$ so that $a_1 = 3$. Next,

$$\gamma_2 = \left(-\frac{1}{8} - 3\right) 5 = \left(-\frac{25}{8}\right) 5$$

and so $|\gamma_2|_5 = |5|_5^3$, which implies that $a_2 = 0$. Since $\frac{\gamma_2}{5^3} = -\frac{1}{8}$, proceeding as above, we see that $a_3 = 3$. Continuing in this manner, we see that

$$a_4 = a_6 = a_8 = \cdots = 0 \text{ and } a_5 = a_7 = a_9 = \cdots = 3.$$

We now follow the notation as under:

The expansion of $\alpha \in \mathbb{Q}_p$, say,

$$\alpha = \frac{a_{-\gamma}}{p^\gamma} + \frac{a_{-\gamma+1}}{p^{\gamma-1}} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots$$

is, for convenience, written as

$$\alpha = a_{-\gamma} a_{-\gamma+1} \ldots a_0, a_1 a_2 \ldots (p). \tag{2.4}$$

We now write the canonical expansion of $\frac{3}{8}$ in $\mathbb{Q}_5$ as

$$\frac{3}{8} = 1, 30\ 30\ 30 \ldots (5),$$

or, in a shorter form as

$$\frac{3}{8} = 1, \overline{30} \ldots (5),$$

where the bar above denotes periodic repetition.

If $\alpha \in \mathbb{Q}_p$ has an expansion of the form

$$\alpha = a_0, a_1 a_2 \ldots (p),$$

then α is called a p-adic integer. Note that α is a p-adic integer if and only if $|\alpha|_p = |p|_p^n$ with $n \geq 0$, i.e., if and only if $\alpha \in \hat{V}$, the valuation ring of $|\cdot|_p$ on $\mathbb{Q}_p$.

We shall now illustrate the arithmetic operations in $\mathbb{Q}_p$, using the notation introduced in (2.4).

Addition

(1) In $\mathbb{Q}_7$, add the following

$$\begin{array}{r} \ 1\ 1\ 1\quad 1\ 1\quad 1 \\ 4\,5\,2,\,1\,3\,7\,6\,1\,2 \\ +\quad 3\,7,\,5\,2\,1\,3\,1\,5\,2 \\ \hline 4\,1\,3,\,0\,6\,1\,3\,3\,0\,3 \end{array}$$

(2) In $\mathbb{Q}_5$,

$$\begin{array}{r} 1,\,3\,0\,3\,0\,3\,0\ldots \quad \left(=\frac{3}{8}\right) \\ +\,1\,0,\,0\,0\,0\,0\,0\,0\ldots \quad \left(=\frac{1}{5}\right) \\ \hline 1\,1,\,3\,0\,3\,0\,3\,0\ldots \end{array}$$

Subtraction

(1) In $\mathbb{Q}_7$,

$$\begin{array}{r} 5\,6,\,3\,5\,2\,4 \\ -\quad 1,\,2\,4\,0\,3 \\ \hline 5\,5,\,1\,1\,2\,1 \end{array}$$

(2) In $\mathbb{Q}_5$,

$$\begin{array}{r} \ 7\ 5\ 3\quad 5\,6 \\ 2\,2\,1,\,4\,3\,0\,2\,1 \\ -\,1\,3\,4,\,2\,3\,1\,4\,2\,2 \\ \hline 1\,4\,1,\,1\,0\,4\,2\,3\,2\,4\,4\ldots \end{array}$$

Multiplication

In $\mathbb{Q}_7$,

$$\begin{array}{r} 1\,2,\,3\,1\,4 \\ \times\quad 1,\,2\,0\,3 \\ \hline 1\,2,\,3\,1\,4 \\ \,2,\,4\,6\,2\,1\,1 \\ \qquad 3\,6\,2\,4\,5\,1 \\ \hline 1\,4,\,0\,4\,6\,4\,5\,5\,1 \end{array}$$

Division

In $\mathbb{Q}_5$, divide 32,13 by 43,12

$$
\begin{array}{l}
43,\ 12\ )\ 3\ \ 2,\ \ 1\ \ 3\ (\ 2,\ \overline{0\,2\,4\,4\,2\,0} \\
\quad\ 3\,2,\,3\,4 \\
\quad\overline{\quad\ 3\,3\,4\,4\ldots} \\
\quad\ 3\,2\,3\,4 \\
\quad\overline{\quad\ 1\,1\,0\ \ 4\ \ 4\ldots} \\
\quad\ 1\,0\,2\ \ 4\ \ 1 \\
\quad\overline{\quad\ 1\,3\ \ 4\ \ 2\ \ 4\ \ 4\ldots} \\
\quad\ 1\,0\ \ 2\ \ 4\ \ 1 \\
\quad\overline{\quad\ 3\ \ 2\ \ 3\ \ 2\ \ 4\ \ 4\ \ \ldots} \\
\quad\ 3\ \ 2\ \ 3\ \ 4 \\
\quad\overline{\qquad\qquad\ 3\ \ 3\ \ 4\ \ 4\ \ \ \ldots}
\end{array}
$$

In $\mathbb{R}$, we write a given number as a decimal expansion. Its analogue in $\mathbb{Q}_p$ is the canonical expansion. We recall that in $\mathbb{R}$, a number is rational if and only if its decimal expansion is periodic. We have an analogue in $\mathbb{Q}_p$. We state the result (for proof, one can refer to [1]).

Theorem 2.4 *An element $\alpha \in \mathbb{Q}_p$ is rational if and only if its canonical expansion*

$$\alpha = \sum_{j=n}^{\infty} a_j p^j, \quad 0 \le a_j \le p-1,$$

when n is such that $|\alpha|_p = |p|_p^n$, is periodic.

Example 2.1 Find the rational number represented by the canonical expansion $1, \overline{30}$ in $\mathbb{Q}_5$.

$$
\begin{aligned}
1, \overline{30} &= 1 + 3.5^1 + 0.5^2 + 3.5^3 + 0.5^4 + \cdots \\
&= 1 + 3[5^1 + 5^3 + \cdots] \\
&= 1 + 3 \cdot \frac{5}{1-5^2}, \quad \text{since } |5^2|_5 = |5|_5^2 < 1 \\
&= 1 - \frac{15}{24} \\
&= 1 - \frac{5}{8} \\
&= \frac{3}{8}.
\end{aligned}
$$

Exercise 2.1 Find the canonical expansion of

(i) $\frac{1}{5}$ in $\mathbb{Q}_3$; (ii) $\frac{1}{3}$ in $\mathbb{Q}_2$; (iii) $-\frac{5}{7}$ in $\mathbb{Q}_5$.

Exercise 2.2 In $\mathbb{Q}_5$, find

(i) $\begin{array}{r} 1\,2\,3,\,4\,1\,2 \\ +\,4\,2\,1,\,0\,3\,2 \end{array}$;

(ii) $\begin{array}{r} 1\,2\,4,\,1\,3\,1 \\ -\,3\,2\,1,\,2\,2\,1 \end{array}$;

(iii) $\begin{array}{r} (3\;\;4,\;1\;2\;1) \\ \times\,(0,\;\;2\;\;1\;0\;3) \end{array}$;

(iv) $(1\;3\;1,\;2) \div (2,\;4\;2)$

Exercise 2.3 In $\mathbb{Q}_3$, find the rational number whose canonical expansion is $2, \overline{0121}$.

As in the classical set up, in $\mathbb{Q}_p$ too, we have the "exponential" and "logarithmic" series respectively defined by

$$E(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \text{ and } L(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^n}{n},$$

which converge for all $x \in \mathbb{Q}_p$ with $|x|_p < 1$. These series have properties which are very similar to their classical counterparts, say, for instance,

$E(x+y) = E(x)E(y)$; $L((1+x)(1+y)) = L(1+x) + L(1+y)$;
$L(E(x)) = x$; $E(L(1+x)) = 1+x$.

In $\mathbb{Q}_p$, we have Binomial series too (for details, refer to [1]).

Though not relevant to the present monograph, it is worth noting that the concept of derivative and its properties have been studied in ultrametric analysis (see [2]). With regard to derivatives, we need the following definition.

Definition 2.1 If U is any subset of an ultrametric field K without isolated points and $f : U \to K$, we say that f is differentiable at $x \in U$ if

$$\lim_{y \to 0} \frac{f(x+y) - f(x)}{y} \text{ exists.} \tag{2.5}$$

Whenever the limit (2.5) exists, it is called the derivative of f at x, denoted by $f'(x)$.

It is immediate from the above definition that the characteristic function (K-valued) χ_U of any clopen set (i.e., any set which is both open and closed) is differentiable everywhere with $\chi'_U = 0$ everywhere. This shows that there are nonconstant functions whose derivatives are 0 everywhere contrary to the classical situation. There

exist (1-1) functions too whose derivatives are 0 everywhere. If the characteristic of K is 2 (We recall that any valuation of such a field is ultrametric, in view of Exercise 1.1) and $f : K \to K$ is defined by $f(x) = x^2$, $x \in K$, then f is (1-1) (since $f(x) = f(y) \Rightarrow x^2 = y^2 \Rightarrow x = y$, using the fact that the characteristic of K is 2) and

$$f'(a) = \lim_{x \to a} \frac{x^2 - a^2}{x - a} = \lim_{x \to a} (x + a) = 2a = 0,$$

at any $a \in K$. We can also give examples of functions which are continuous everywhere but not differentiable anywhere. For instance, let U denote the closed unit disc in $\mathbb{Q}_p$. Let $f : U \to \mathbb{Q}_p$ defined by $f\left(\sum_n a_n p^n\right) = \sum_n a_n p^{2n}$, $0 \leq a_n \leq p - 1$. Then f is continuous everywhere but not differentiable anywhere (see [3]). In classical analysis, functions which have antiderivatives do not have jump discontinuities and they are pointwise limits of continuous functions. However, both these conditions are not sufficient for the functions to have an antiderivative. Unlike the classical case in which sufficient conditions are not known, the situation in the ultrametric case is simpler: If U is a subset of K without isolated points, then $f : U \to K$ has an antiderivative if and only if f is the pointwise limit of continuous functions ([4], p. 283).

References

1. Bachman, G.: Introduction to p-adic Numbers and Valuation Theory. Academic Press, New York (1964)
2. Schikhof, W.H.: Ultrametric Calculus. Cambridge University Press, Cambridge (1984)
3. Narici, L., Beckenstein, E.: Strange terrain—non-archimedean spaces. Amer. Math. Monthly **88**, 667–676 (1981)
4. Van Rooij, A.C.M.: Non-archimedean Functional Analysis. Marcel Dekker, New York (1978)

http://www.springer.com/978-81-322-2558-4

An Introduction to Ultrametric Summability Theory

Natarajan, P.

2015, XIII, 159 p., Hardcover
ISBN: 978-81-322-2558-4