An Introduction to p-adic Numbers and p-adic Analysis

A. J. Baker

[12/08/2007]

Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland.

E-mail address: a.baker@maths.gla.ac.uk

URL: http://www.maths.gla.ac.uk/∼ajb

Contents

Introduction

These notes were written for a final year undergraduate course taught at Manchester University in 1988/9 and also taught in later years by Dr M. McCrudden. I rewrote them in 2000 to make them available to interested graduate students. The approach taken is very down to earth and makes few assumptions beyond standard undergraduate analysis and algebra. Because of this the course was as self contained as possible, covering basic number theory and analytic ideas which would probably be familiar to more advanced readers. The problem sets are based on those for produced for the course.

I would like to thank Javier Diaz-Vargas and Jeremy Scofield for pointing out numerous errors.

CHAPTER 1

Congruences and modular equations

Let $n \in \mathbb{Z}$ (we will usually have $n > 0$). We define the binary relation $\underset{n}{\equiv}$ by

DEFINITION 1.1. If $x, y \in \mathbb{Z}$, then $x \underset{n}{\equiv} y$ if and only if $n \mid (x - y)$. This is often also written $x \equiv y \pmod{n}$ or $x \equiv y \ (n)$.

Notice that when $n = 0$, $x \underset{n}{\equiv} y$ if and only if $x = y$, so in that case $\underset{0}{\equiv}$ is really just equality.

PROPOSITION 1.2. *The relation* $\underset{n}{\equiv}$ *is an equivalence relation on* $\mathbb{Z}$.

PROOF. Let $x, y, z \in \mathbb{Z}$. Clearly $\underset{n}{\equiv}$ is reflexive since $n \mid (x - x) = 0$. It is symmetric since if $n \mid (x - y)$ then $x - y = kn$ for some $k \in \mathbb{Z}$, hence $y - x = (-k)n$ and so $n \mid (y - x)$. For transitivity, suppose that $n \mid (x - y)$ and $n \mid (y - z)$; then since $x - z = (x - y) + (y - z)$ we have $n \mid (x - z)$. □

If $n > 0$, we denote the equivalence class of $x \in \mathbb{Z}$ by $[x]_n$ or just $[x]$ if n is understood; it is also common to use $\overline{x}$ for this if the value of n is clear from the context. From the definition,

$$[x]_n = \{y \in \mathbb{Z} : y \underset{n}{\equiv} x\} = \{y \in \mathbb{Z} : y = x + kn \text{ for some } k \in \mathbb{Z}\},$$

and there are exactly $|n|$ such *residue classes*, namely

$$[0]_n, [1]_n, \ldots, [n-1]_n.$$

Of course we can replace these representatives by any others as required.

DEFINITION 1.3. The set of all *residue classes of* $\mathbb{Z}$ *modulo* n is

$$\mathbb{Z}/n = \{[x]_n : x = 0, 1, \ldots, n-1\}.$$

If $n = 0$ we interpret $\mathbb{Z}/0$ as $\mathbb{Z}$.

Consider the function

$$\pi_n \colon \mathbb{Z} \longrightarrow \mathbb{Z}/n; \quad \pi_n(x) = [x]_n.$$

This is onto and also satisfies

$$\pi_n^{-1}(\alpha) = \{x \in \mathbb{Z} : x \in \alpha\}.$$

We can define *addition* $\underset{n}{+}$ and *multiplication* $\underset{n}{\times}$ on $\mathbb{Z}/n$ by the formulæ

$$[x]_n \underset{n}{+} [y]_n = [x + y]_n, \quad [x]_n \underset{n}{\times} [y]_n = [xy]_n,$$

which are easily seen to be well defined, *i.e.*, they do not depend on the choice of representatives x, y. The straightforward proof of our next result is left to the reader.

PROPOSITION 1.4. *The set $\mathbb{Z}/n$ with the operations $+_n$ and $\times_n$ is a commutative ring and the function $\pi_n\colon \mathbb{Z} \longrightarrow \mathbb{Z}/n$ is a ring homomorphism which is surjective (onto) and has kernel*

$$\ker \pi_n = [0]_n = \{x \in \mathbb{Z} : x \underset{n}{\equiv} 0\}.$$

Now let us consider the structure of the ring $\mathbb{Z}/n$. The *zero* is $\overline{0} = [0]_n$ and the *unity* is $\overline{1} = [1]_n$. We may also ask about *units* and *zero divisors*. In the following, let R be a commutative ring with unity 1 (which we assume is not equal to 0).

DEFINITION 1.5. An element $u \in R$ is a *unit* if there exists a $v \in R$ satisfying

$$uv = vu = 1.$$

Such a v is necessarily unique and is called the *inverse* of u and is usually denoted u^{-1}.

DEFINITION 1.6. $z \in R$ is a *zero divisor* if there exists at least one $w \in R$ with $w \neq 0$ and $zw = 0$. There may be lots of such w for each zero divisor z.

Notice that in any ring 0 is always a zero divisor since $1 \cdot 0 = 0 = 0 \cdot 1$.

EXAMPLE 1.7. Let $n = 6$; then $\mathbb{Z}/6 = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$. The units are $\overline{1}, \overline{5}$ with $\overline{1}^{-1} = \overline{1}$ and $\overline{5}^{-1} = \overline{5}$ since $5^2 = 25 \underset{6}{\equiv} 1$. The zero divisors are $\overline{0}, \overline{2}, \overline{3}, \overline{4}$ since $\overline{2} \underset{6}{\times} \overline{3} = \overline{0}$.

In this example notice that the zero divisors all have a factor in common with 6; this is true for all $\mathbb{Z}/n$ (see below). It is also true that for any ring, a zero divisor cannot be a unit (why?) and a unit cannot be a zero divisor.

Recall that if $a, b \in \mathbb{Z}$ then the *greatest common divisor* (gcd) or *highest common factor* (hcf) of a and b is the largest positive integer dividing both a and b. We often write $\gcd(a, b)$ for this. When $a = 0 = b$ we have $\gcd(0, 0) = 0$.

THEOREM 1.8. *Let $n > 0$. Then $\mathbb{Z}/n$ is a disjoint union*

$$\mathbb{Z}/n = \{\text{units}\} \cup \{\text{zero divisors}\}$$

where {units} *is the set of units in $\mathbb{Z}/n$ and* {zero divisors} *the set of zero divisors. Furthermore,*

(a) *$\overline{z}$ is a zero divisor if and only if $\gcd(z, n) > 1$;*
(b) *$\overline{u}$ is a unit if and only if $\gcd(u, n) = 1$.*

PROOF. If $h = \gcd(x, n) > 1$ we have $x = x_0 h$ and $n = n_0 h$, so

$$n_0 x \underset{n}{\equiv} 0.$$

Hence $\overline{x}$ is a zero divisor in $\mathbb{Z}/n$.

Let us prove (b). First we suppose that $\overline{u}$ is a unit; let $\overline{v} = \overline{u}^{-1}$. Suppose that $\gcd(u, n) > 1$. Then $uv \underset{n}{\equiv} 1$ and so for some integer k,

$$uv - 1 = kn.$$

But then $\gcd(u, n) \mid 1$, which is absurd. So $\gcd(u, n) = 1$. Conversely, if $\gcd(u, n) = 1$ we must demonstrate that $\overline{u}$ is a unit. To do this we will need to make use of the *Euclidean Algorithm*.

RECOLLECTION 1.9. [Euclidean Property of the integers] Let $a, b \in \mathbb{Z}$ with $b \neq 0$; then there exist unique $q, r \in \mathbb{Z}$ for which $a = qb + r$ with $0 \leqslant r < |b|$.

From this we can deduce

THEOREM 1.10 (The Euclidean Algorithm). *Let $a, b \in \mathbb{Z}$ then there are unique sequences of integers q_i, r_i satisfying*

$$\begin{aligned} a &= q_1 b + r_1 \\ r_0 = b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ 0 \neq r_{N-1} &= q_{N+1} r_N \end{aligned}$$

where we have $0 \leqslant r_i < r_{i-1}$ for each i. Furthermore, we have $r_N = \gcd(a, b)$ and then by back substitution for suitable $s, t \in \mathbb{Z}$ we can write

$$r_N = sa + tb.$$

EXAMPLE 1.11. If $a = 6, b = 5$, then $r_0 = 5$ and we have

$$\begin{aligned} 6 &= 1 \cdot 5 + 1, && \text{so } q_1 = 1, r_1 = 1, \\ 5 &= 5 \cdot 1, && \text{so } q_2 = 5, r_2 = 0. \end{aligned}$$

Therefore we have $\gcd(6, 5) = 1$ and we can write $1 = 1 \cdot 6 + (-1) \cdot 5$.

Now we return to the proof of Theorem 1.8. Using the Euclidean Algorithm, we can write $su + tn = 1$ for suitable $s, t \in \mathbb{Z}$. But then $su \underset{n}{\equiv} 1$ and $\overline{s} = \overline{u}^{-1}$, so $\overline{u}$ is indeed a unit in $\mathbb{Z}/n$. These proves part (b). But we also have part (a) as well since a zero divisor $\overline{z}$ cannot be a unit, hence has to have $\gcd(z, n) > 1$. □

Theorem 1.8 allows us to determine the number of units and zero divisors in $\mathbb{Z}/n$. We already have $|\mathbb{Z}/n| = n$.

DEFINITION 1.12. $(\mathbb{Z}/n)^\times$ is the set of units in $\mathbb{Z}/n$. $(\mathbb{Z}/n)^\times$ becomes an abelian group under the multiplication $\underset{n}{\times}$.

Let $\varphi(n) = |(\mathbb{Z}/n)^\times|$ = order of $(\mathbb{Z}/n)^\times$. By Theorem 1.8, this number equals the number of integers $0, 1, 2, \ldots, n-1$ which have no factor in common with n. The function φ is known as the *Euler φ-function.*

EXAMPLE 1.13. $n = 6$: $|\mathbb{Z}/6| = 6$ and the units are $\overline{1}, \overline{5}$, hence $\varphi(6) = 2$.

EXAMPLE 1.14. $n = 12$: $|\mathbb{Z}/12| = 12$ and the units are $\overline{1}, \overline{5}, \overline{7}, \overline{11}$, hence $\varphi(12) = 4$.

In general $\varphi(n)$ is quite a complicated function of n, however in the case where $n = p$, a prime number, the answer is more straightforward.

EXAMPLE 1.15. Let p be a prime (*i.e.*, $p = 2, 3, 5, 7, 11, \ldots$). Then the only non-trivial factor of p is p itself-so $\varphi(p) = p - 1$. We can say more: consider a power of p, say p^r with $r > 0$. Then the integers in the list $0, 1, 2, \ldots, p^r - 1$ which have a factor in common with p^r are precisely those of the form kp for $0 \leqslant k \leqslant p^{r-1} - 1$, hence there are p^{r-1} of these. So we have $\varphi(p^r) = p^{r-1}(p - 1)$.

EXAMPLE 1.16. When $p = 2$, we have the groups $(\mathbb{Z}/2)^\times = \{\overline{1}\}$, $\left(\mathbb{Z}/2^2\right)^\times = \{\overline{1}, \overline{3}\} \cong \mathbb{Z}/2$, $\left(\mathbb{Z}/2^3\right)^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, and in general

$$\left(\mathbb{Z}/2^{r+1}\right)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{r-1}$$

for any $r \geqslant 1$. Here the first summand is $\{\overline{\pm 1}\}$ and the second can be taken to be $\left\langle \overline{3} \right\rangle$.

Now for a general n we have

$$n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$$

where for each i, p_i is a prime with

$$2 \leqslant p_1 < p_2 < \cdots < p_s$$

and $r_i \geqslant 1$. Then the numbers p_i, r_i are uniquely determined by n. We can break down $\mathbb{Z}/n$ into copies of $\mathbb{Z}/p_i^{r_i}$, each of which is simpler to understand.

THEOREM 1.17. *There is a unique isomorphism of rings*

$$\Phi \colon \mathbb{Z}/n \cong \mathbb{Z}/p_1^{r_1} \times \mathbb{Z}/p_2^{r_2} \times \cdots \times \mathbb{Z}/p_s^{r_s}$$

and an isomorphism of groups

$$\Phi^\times \colon (\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p_1^{r_1})^\times \times (\mathbb{Z}/p_2^{r_2})^\times \times \cdots \times (\mathbb{Z}/p_s^{r_s})^\times.$$

Thus we have

$$\varphi(n) = \varphi(p_1^{r_1})\varphi(p_2^{r_2}) \cdots \varphi(p_s^{r_s}).$$

PROOF. Let $a, b > 0$ be *coprime* (*i.e.*, $\gcd(a, b) = 1$). We will show that there is an isomorphism of rings

$$\Psi \colon \mathbb{Z}/ab \cong \mathbb{Z}/a \times \mathbb{Z}/b.$$

By Theorem 1.10, there are $u, v \in \mathbb{Z}$ such that $ua + vb = 1$. It is easily checked that

$$\gcd(a, v) = 1 = \gcd(b, u).$$

Define a function

$$\Psi \colon \mathbb{Z}/ab \longrightarrow \mathbb{Z}/a \times \mathbb{Z}/b; \quad \Psi([x]_{ab}) = \left([x]_a, [x]_b\right).$$

This is easily seen to be a ring homomorphism. Notice that

$$|\mathbb{Z}/ab| = ab = |\mathbb{Z}/a||\mathbb{Z}/b| = |\mathbb{Z}/a \times \mathbb{Z}/b|$$

and so to show that Ψ is an isomorphism, it suffices to show that it is *onto*.

Let $([y]_a, [z]_b) \in \mathbb{Z}/a \times \mathbb{Z}/b$. We must find an $x \in \mathbb{Z}$ such that $\Psi([x]_{ab}) = ([y]_a, [z]_b)$. Now set $x = vby + uaz$; then

$$x = (1 - ua)y + uaz \underset{a}{\equiv} y,$$
$$x = vby + (1 - vb)z \underset{b}{\equiv} z,$$

hence we have $\Psi([x]_{ab}) = ([y]_a, [z]_b)$ as required.

To prove the result for general n we proceed by induction upon s. □

EXAMPLE 1.18. Consider the case $n = 120$. Then $120 = 8 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$ and so the Theorem predicts that

$$\mathbb{Z}/120 \cong \mathbb{Z}/8 \times \mathbb{Z}/3 \times \mathbb{Z}/5.$$

We will verify this. First write $120 = 24 \cdot 5$. Then $\gcd(24, 5) = 1$ since

$$24 = 4 \cdot 5 + 4 \implies 4 = 24 - 4 \cdot 5 \quad \text{and} \quad 5 = 4 + 1 \implies 1 = 5 - 4,$$

hence

$$1 = 5 \cdot 5 - 24.$$

Therefore we can take $a = 24, b = 5, u = -1, v = 5$ in the proof of the Theorem. Thus we have a ring isomorphism

$$\Psi_1 \colon \mathbb{Z}/120 \longrightarrow \mathbb{Z}/24 \times \mathbb{Z}/5; \quad \Psi_1([25y - 24z]_{120}) = ([y]_{24}, [z]_5),$$

as constructed in the proof above. Next we have to repeat this procedure for the ring $\mathbb{Z}/24$. Here we have

$$8 = 2 \cdot 3 + 2 \implies 2 = 8 - 2 \cdot 3 \quad \text{and} \quad 3 = 2 + 1 \implies 1 = 3 - 2,$$

so

$$\gcd(8, 3) = 1 = (-8) + 3 \cdot 3.$$

Hence there is an isomorphism of rings

$$\Psi_2 \colon \mathbb{Z}/24 \longrightarrow \mathbb{Z}/8 \times \mathbb{Z}/3; \quad \Psi_2([9x - 8y]_{24}) = ([x]_8, [y]_3),$$

and we can of course combine these two isomorphisms to obtain a third, namely

$$\Psi \colon \mathbb{Z}/120 \longrightarrow \mathbb{Z}/8 \times \mathbb{Z}/3 \times \mathbb{Z}/5; \quad \Psi([25(9x - 8y) - 24z]_{120}) = ([x]_8, [y]_3, [z]_5),$$

as required. Notice that we have

$$\Psi^{-1}([1]_8, [1]_3, [1]_5) = [1]_{120},$$

which is *always* the case with this procedure.

We now move on to consider the subject of equations over $\mathbb{Z}/n$. Consider the following example.

EXAMPLE 1.19. Let $a, b \in \mathbb{Z}$ with $n > 0$. Then

$$ax \underset{n}{\equiv} b \tag{1.1}$$

is a *linear modular equation* or *linear congruence over* $\mathbb{Z}$. We are interested in finding *all* solutions of Equation (1.1) in $\mathbb{Z}$, not just one solution.

If $u \in \mathbb{Z}$ has the property that $au \underset{n}{\equiv} b$ then u is a solution; but then the integers of form $u + kn,\ k \in \mathbb{Z}$ are also solutions. Notice that there are an infinite number of these. But each such solution gives the same congruence class $[u + kn]_n = [u]_n$. We can equally well consider

$$[a]_n X = [b]_n \tag{1.2}$$

as a linear equation over $\mathbb{Z}/n$. This time we look for all solutions of Equation (1.2) in $\mathbb{Z}/n$ and as $\mathbb{Z}/n$ is itself finite, there are only a finite number of these. As we remarked above, any integer solution u of (1.1) gives rise to solution $[u]_n$ of (1.2); in fact many solutions of (1.1) give the *same* solution of (1.2). Conversely, a solution $[v]_n$ of (1.2) generates the set

$$[v]_n = \{v + kn : k \in \mathbb{Z}\}$$

of solutions of (1.1), so there is in fact an equivalence of these two problems.

Now let us attempt to solve (1.2), *i.e.*, try to find all solutions in $\mathbb{Z}/n$. There are two cases:

(1) the element $[a]_n \in \mathbb{Z}/n$ is a unit;
(2) the element $[a]_n \in \mathbb{Z}/n$ is a zero divisor.

In case (1), let $[c]_n = [a]_n^{-1}$ be the inverse of $[a]_n$. Then we can multiply (1.2) by $[c]_n$ to obtain

$$X = [bc]_n$$

which has exactly the same solutions as (1.2) (why?). Moreover, there is exactly one such solution namely $[bc]_n$! So we have completely solved equation (1.2) and found that $X = [bc]_n$ is the unique solution in $\mathbb{Z}/n$.

What does this say about solving (1.1)? There are certainly infinitely many solutions, namely the integers of form $bc + kn,\ k \in \mathbb{Z}$. But any given solution u must satisfy $[u]_n = [bc]_n$ in $\mathbb{Z}/n$, hence $u \underset{n}{\equiv} bc$ and so u is of this form. So the solutions of (1.1) are precisely the integers this form.

So in case (1) of (1.2) we have exactly one solution in $\mathbb{Z}/n$,

$$X = [a]_n^{-1}[b]_n$$

and (1.1) has all integers of the form $cb + kn$ as its solutions.

In case (2) there may be solutions of (1.2) or none at all. For example, the equation

$$nx \underset{n}{\equiv} 1,$$

can only have a solution in $\mathbb{Z}$ if $n = 1$. There is also the possibility of multiple solutions in $\mathbb{Z}/n$, as is shown by the example

$$2x \underset{12}{\equiv} 4.$$

By inspection, this is seen to have solutions $\overline{2}, \overline{8}$. Notice that this congruence can also be solved by reducing it to

$$x \underset{6}{\equiv} 2,$$

since if $2(x-2) \underset{12}{\equiv} 0$ then $x - 2 \underset{6}{\equiv} 0$, which is an example of case (1) again.

So if $[a]_n$ is not a unit, uniqueness is also lost as well as the guarantee of *any* solutions.

We can more generally consider a system of linear equations

$$a_1 x \underset{n_1}{\equiv} b_1, \quad a_2 x \underset{n_2}{\equiv} b_2, \quad \ldots \quad , a_k x \underset{n_k}{\equiv} b_k,$$

where we are now trying to find all integers $x \in \mathbb{Z}$ which simultaneously satisfy these congruences. The main result on this situation is the following.

THEOREM 1.20 (The Chinese Remainder Theorem). *Let $n_1, n_2, \ldots, n_k$ be a sequence of coprime integers, $a_1, a_2, \ldots, a_k$ a sequence of integers satisfying $\gcd(a_i, n_i) = 1$ and $b_1, b_2, \ldots, b_k$ be sequence of integers. Then the system of simultaneous linear congruences equations*

$$a_1 x \underset{n_1}{\equiv} b_1, \quad a_2 x \underset{n_2}{\equiv} b_2, \quad \ldots \quad , a_k x \underset{n_k}{\equiv} b_k,$$

has an infinite number of solutions $x \in \mathbb{Z}$ which form a unique congruence class

$$[x]_{n_1 n_2 \cdots n_k} \in \mathbb{Z}/n_1 n_2 \cdots n_k.$$

PROOF. The proof uses the isomorphism

$$\mathbb{Z}/ab \cong \mathbb{Z}/a \times \mathbb{Z}/b$$

for $\gcd(a, b) = 1$ as proved in the proof of Theorem 1.17, together with an induction on k. □

EXAMPLE 1.21. Consider the system

$$3x \underset{2}{\equiv} 5, \quad 2x \underset{3}{\equiv} 6, \quad 7x \underset{5}{\equiv} 1.$$

Since $8 \underset{5}{\equiv} 3$, this system is equivalent to

$$x \underset{2}{\equiv} 1, \quad x \underset{3}{\equiv} 0, \quad x \underset{5}{\equiv} 3.$$

Solving the first two equations in $\mathbb{Z}/6$, we obtain the unique solution $x \underset{6}{\equiv} 3$. Solving the simultaneous pair of congruences

$$x \underset{6}{\equiv} 3, \quad x \underset{5}{\equiv} 3,$$

we obtain the unique solution $x \underset{30}{\equiv} 3$ in $\mathbb{Z}/30$.

Theorem 1.17 is often used to solve polynomial equations modulo n, by first splitting n into a product of prime powers, say $n = p_1^{r_1} p_2^{r_2} \cdots p_d^{r_d}$, and then solving modulo $p_k^{r_k}$ for each k.

THEOREM 1.22. *Let $n = p_1^{r_1} p_2^{r_2} \cdots p_d^{r_d}$, where the p_k's are distinct primes with each $r_k \geqslant 1$. Let $f(X) \in \mathbb{Z}[X]$ be a polynomial with integer coefficients. Then the equation*

$$f(x) \underset{n}{\equiv} 0$$

has a solution if and only if the equations

$$f(x_1) \underset{p_1^{r_1}}{\equiv} 0, \quad f(x_2) \underset{p_2^{r_2}}{\equiv} 0, \quad \dots \quad , f(x_d) \underset{p_d^{r_d}}{\equiv} 0,$$

all have solutions. Moreover, each sequence of solutions in $\mathbb{Z}/p_k^{r_k}$ *of the latter gives rise to a unique solution* $x \in \mathbb{Z}/n$ *of* $f(x) \underset{n}{\equiv} 0$ *satisfying*

$$x \underset{p_k^{r_k}}{\equiv} x_k \quad \forall k.$$

EXAMPLE 1.23. Solve $x^2 - 1 \underset{24}{\equiv} 0$.

We have $24 = 8 \cdot 3$, so we will try to solve the pair of congruences equations

$$x_1^2 - 1 \underset{8}{\equiv} 0, \quad x_2^2 - 1 \underset{3}{\equiv} 0,$$

with $x_1 \in \mathbb{Z}/8, x_2 \in \mathbb{Z}/3$. Now clearly the solutions of the first equation are $x_1 \underset{8}{\equiv} 1, 3, 5, 7$; for the second we get $x_2 \underset{3}{\equiv} 1, 2$. Combining these using Theorem 1.17, we obtain

$$x \underset{24}{\equiv} 1, 5, 7, 11, 13, 17, 19, 23.$$

The moral of this is that we only need worry about $\mathbb{Z}/p^r$ where p is a prime. We now consider this case in detail.

Firstly, we will study the case $r = 1$. Now $\mathbb{Z}/p$ is a *field*, *i.e.*, every non-zero element has an inverse (it's a good exercise to prove this yourself if you've forgotten this result). Then we have

PROPOSITION 1.24. *Let* K *be a field, and* $f(X) \in K[X]$ *be a polynomial with coefficients in* K*. Then for* $\alpha \in K$*,*

$$f(\alpha) = 0 \quad \Longleftrightarrow \quad f(X) = (X - \alpha)g(X) \quad \textit{for some } g(X) \in K[X].$$

PROOF. This is a standard result in basic ring theory. □

COROLLARY 1.25. *Let* K *be a field and let* $f(X) \in K[X]$ *with* $\deg f = d > 0$*. Then* $f(X)$ *has at most* d *distinct roots in* K*.*

As a particular case, consider the field $\mathbb{Z}/p$, where p is a prime, and the polynomials

$$X^p - X, \; X^{p-1} - \overline{1} \in \mathbb{Z}/p[X].$$

THEOREM 1.26 (Fermat's Little Theorem). *For any* $\overline{a} \in \mathbb{Z}/p$*, either* $\overline{a} = \overline{0}$ *or* $(\overline{a})^{p-1} = \overline{1}$ *(so in the latter case* $\overline{a}$ *is a* $(p-1)$ *st root of 1). Hence,*

$$X^p - X = X(X - \overline{1})(X - \overline{2}) \cdots (X - \overline{p-1}).$$

COROLLARY 1.27 (Wilson's Theorem). *For any prime* p *we have*

$$(p-1)! \equiv -1 \pmod{p}.$$

We also have the more subtle

THEOREM 1.28 (Gauss's Primitive Root Theorem). *For any prime* p*, the group* $(\mathbb{Z}/p)^\times$ *is cyclic of order* $p - 1$*. Hence there is an element* $\overline{a} \in \mathbb{Z}/p$ *of order* $p - 1$*.*

The proof of this uses for example the structure theorem for finitely generated abelian groups. A generator of $(\mathbb{Z}/p)^\times$ is called a *primitive root modulo p* and there are exactly $\varphi(p-1)$ of these in $(\mathbb{Z}/p)^\times$.

EXAMPLE 1.29. Take $p = 7$. Then $\varphi(6) = \varphi(2)\varphi(3) = 2$, so there are two primitive roots modulo 7. We have

$$2^3 \underset{7}{\equiv} 1, \quad 3^2 \underset{7}{\equiv} 2, \quad 3^6 \underset{7}{\equiv} 1,$$

hence $\overline{3}$ is one primitive root, the other must be $\overline{3^5} = \overline{5}$.

One advantage of working with a field K is that all of basic linear algebra works just as well over K. For instance, we can solve systems of simultaneous linear equations in the usual way by Gaussian elimination.

EXAMPLE 1.30. Take $p = 11$ and solve the system of simultaneous equations

$$\begin{aligned} 3x + 2y - 3z &\underset{11}{\equiv} 1, \\ 2x \qquad + \quad z &\underset{11}{\equiv} 0, \end{aligned}$$

i.e., find all solutions with $x, y, z \in \mathbb{Z}/11$.

Here we can multiply the first equation by $\overline{3}^{-1} = \overline{4}$, obtaining

$$\begin{aligned} x + 8y - 1z &\underset{11}{\equiv} 4, \\ 2x \qquad + \quad z &\underset{11}{\equiv} 0, \end{aligned}$$

and then subtract twice this from the second to obtain

$$\begin{aligned} x + 8y - 1z &\underset{11}{\equiv} 4, \\ 6y + 3z &\underset{11}{\equiv} 3, \end{aligned}$$

and we know that the rank of this system is 2. The general solution is

$$x \underset{11}{\equiv} 5t, \quad y \underset{11}{\equiv} 5t + 6, \quad z \underset{11}{\equiv} t,$$

for $t \in \mathbb{Z}$.

Now consider a polynomial $f(X) \in \mathbb{Z}[X]$, say

$$f(X) = \sum_{k=0}^{d} a_k X^k.$$

Suppose we want to solve the equation

$$f(x) \underset{p^r}{\equiv} 0$$

for some $r \geqslant 1$ and let's assume that we already have a solution $x_1 \in \mathbb{Z}$ which works modulo p, *i.e.*, we have

$$f(x_1) \underset{p}{\equiv} 0.$$

Can we find an integer x_2 such that

$$f(x_2) \underset{p^2}{\equiv} 0$$

and $x_2 \underset{p}{\equiv} x_1$? More generally we would like to find an integer x_r such that

$$f(x_r) \underset{p^r}{\equiv} 0$$

and $x_r \underset{p}{\equiv} x_1$? Such an x_r is called a *lift* of x_1 modulo p^r.

EXAMPLE 1.31. Take $p = 5$ and $f(X) = X^2+1$. Then there are two distinct roots modulo 5, namely $\overline{2}, \overline{3}$. Let's try to find a root modulo 25 and agreeing with 2 modulo 5. Try $2+5t$ where $t = 0, 1, \ldots, 4$. Then we need

$$(2+5t)^2 + 1 \underset{25}{\equiv} 0,$$

or equivalently

$$20t + 5 \underset{25}{\equiv} 0,$$

which has the solution

$$t \underset{5}{\equiv} 1.$$

Similarly, we have $t \underset{5}{\equiv} 3$ as a lift of 3.

EXAMPLE 1.32. Obtain lifts of $2, 3$ modulo 625.

The next result is the simplest version of what is usually referred to as *Hensel's Lemma*. In various guises this is an important result whose proof is inspired by the proof of *Newton's Method* from Numerical Analysis.

THEOREM 1.33 (Hensel's Lemma: first version). *Let $f(X) = \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X]$ and suppose that $x \in \mathbb{Z}$ is a root of f modulo p^s (with $s \geqslant 1$) and that $f'(x)$ is a unit modulo p. Then there is a unique root $\overline{x'} \in \mathbb{Z}/p^{s+1}$ of f modulo p^{s+1} satisfying $x' \underset{p^s}{\equiv} x$; moreover, x' is given by the formula*

$$x' \underset{p^{s+1}}{\equiv} x - uf(x),$$

where $u \in \mathbb{Z}$ satisfies $uf'(x) \underset{p}{\equiv} 1$, i.e., u is an inverse for $f'(x)$ modulo p.

PROOF. We have

$$f(x) \underset{p^s}{\equiv} 0, \quad f'(x) \underset{p}{\not\equiv} 0,$$

so there is such a $u \in \mathbb{Z}$. Now consider the polynomial $f(x + Tp^s) \in \mathbb{Z}[T]$. Then

$$f(x + Tp^s) \equiv f(x) + f'(x)Tp^s + \cdots \pmod{(Tp^s)^2}$$

by the usual version of Taylor's expansion for a polynomial over $\mathbb{Z}$. Hence, for any $t \in \mathbb{Z}$,

$$f(x + tp^s) \equiv f(x) + f'(x)tp^s + \cdots \pmod{p^{2s}}.$$

An easy calculation now shows that

$$f(x + tp^s) \underset{p^{s+1}}{\equiv} 0 \quad \Longleftrightarrow \quad t \underset{p}{\equiv} -uf(x)/p^s. \qquad \square$$

EXAMPLE 1.34. Let p be an *odd* prime and let $f(X) = X^{p-1} - 1$. Then Gauss's Primitive Root Theorem 1.28, we have exactly $p-1$ distinct $(p-1)$ st roots of 1 modulo p; let $\alpha = \overline{a} \in \mathbb{Z}/p$ be any one of these. Then $f'(X) \underset{p}{\equiv} -X^{p-2}$ and so $f'(\alpha) \neq 0$ and we can apply Theorem 1.33. Hence there is a unique lift of a modulo p^2, say a_2, agreeing with $a_1 = a$ modulo p. So the reduction function

$$\rho_1 \colon \left(\mathbb{Z}/p^2\right)^\times \longrightarrow (\mathbb{Z}/p)^\times; \quad \rho_1(\overline{b}) = \overline{b}$$

must be a group homomorphism which is onto. So for each such $\alpha_1 = \alpha$, there is a unique element $\alpha_2 \in \mathbb{Z}/p^2$ satisfying $\alpha_2^{p-1} = 1$ and therefore the group $\left(\mathbb{Z}/p^2\right)^\times$ contains a unique cyclic subgroup of order $p-1$ which ρ_1 maps isomorphically to $(\mathbb{Z}/p)^\times$. As we earlier showed that $|\mathbb{Z}/p^2|$ has order $(p-1)p$, this means that there is an isomorphism of groups

$$\left(\mathbb{Z}/p^2\right)^\times \cong (\mathbb{Z}/p)^\times \times \mathbb{Z}/p,$$

by standard results on abelian groups.

We can repeat this process to construct a unique sequence of integers $a_1, a_2, \ldots$ satisfying $a_k \underset{p^k}{\equiv} a_{k+1}$ and $a_k^{p-1} \underset{p^k}{\equiv} 1$. We can also deduce that the reduction homomorphisms

$$\rho_k \colon \left(\mathbb{Z}/p^{k+1}\right)^\times \longrightarrow \left(\mathbb{Z}/p^k\right)^\times$$

are all onto and there are isomorphisms

$$\left(\mathbb{Z}/p^{k+1}\right)^\times \cong (\mathbb{Z}/p)^\times \times \mathbb{Z}/p^k.$$

The case $p = 2$ is similar only this time we only have a single root of $X^{2-1} - 1$ modulo 2 and obtain the isomorphisms

$$(\mathbb{Z}/2)^\times = 0, \qquad (\mathbb{Z}/4)^\times \cong \mathbb{Z}/2, \qquad (\mathbb{Z}/2^s)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{s-2} \quad \text{if } s \geqslant 2.$$

It is also possible to do examples involving multivariable systems of simultaneous equations using a more general version of Hensel's Lemma.

THEOREM 1.35 (Hensel's Lemma: many variables and functions). *Let*

$$f_j(X_1, X_2, \ldots, X_n) \in \mathbb{Z}[X_1, X_2, \ldots, X_n]$$

for $1 \leqslant j \leqslant m$ be a collection of polynomials and set $\mathbf{f} = (f_j)$. Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ be a solution of $\mathbf{f}$ modulo p^k. Suppose that the $m \times n$ derivative matrix

$$D\mathbf{f}(\mathbf{a}) = \left(\frac{\partial f_j}{\partial X_i}(\mathbf{a})\right)$$

has full rank when considered as a matrix defined over $\mathbb{Z}/p$. Then there is a solution $\mathbf{a}' = (a_1', \ldots, a_n') \in \mathbb{Z}^n$ of $\mathbf{f}$ modulo p^{k+1} satisfying $\mathbf{a}' \underset{p^k}{\equiv} \mathbf{a}$.

EXAMPLE 1.36. For each of the values $k = 1, 2, 3$, solve the simultaneous system

$$f(X, Y, Z) = 3X^2 + Y \underset{2^k}{\equiv} 1,$$
$$g(X, Y, Z) = XY + YZ \underset{2^k}{\equiv} 0.$$

Finally we state a version of Hensel's Lemma that applies under slightly more general conditions than the above and will be of importance later.

THEOREM 1.37 (Hensel's Lemma: General Version). *Let $f(X) \in \mathbb{Z}[X]$, $r \geqslant 1$ and $a \in \mathbb{Z}$, satisfy the equations*

(a) $$f(a) \underset{p^{2r-1}}{\equiv} 0,$$

(b) $$f'(a) \not\underset{p^r}{\equiv} 0.$$

Then there exists $a' \in \mathbb{Z}$ such that

$$f(a') \underset{p^{2r+1}}{\equiv} 0 \quad \textit{and} \quad a' \underset{p^r}{\equiv} a.$$

CHAPTER 2

The p-adic norm and the p-adic numbers

Let R be a ring with unity $1 = 1_R$.

DEFINITION 2.1. A function

$$N\colon R \longrightarrow \mathbb{R}^+ = \{r \in \mathbb{R} : r \geqslant 0\}$$

is called a *norm* on R if the following are true.

(Na) $N(x) = 0$ if and only if $x = 0$.
(Nb) $N(xy) = N(x)N(y) \quad \forall x, y \in R$.
(Nc) $N(x + y) \leqslant N(x) + N(y) \quad \forall x, y \in R$.

Condition (Nc) is called *the triangle inequality*.

N is called a *seminorm* if (Na) and (Nb) are replaced by the following conditions. The reader is warned that the terminology of norms and seminorms varies somewhat between algebra and analysis.

(Na′) $N(1) = 1$.
(Nb′) $N(xy) \leqslant N(x)N(y) \quad \forall x, y \in R$.

A (semi)norm N is called *non-Archimedean* if (Nc) can be replaced by the stronger statement, *the ultrametric inequality*:

(Nd) $N(x + y) \leqslant \max\{N(x), N(y)\} \quad \forall x, y \in R$.

If (Nd) is not true then the norm N is said to be *Archimedean*.

Exercise: Show that for a non-Archimedean norm N, (Nd) can be strengthened to

(Nd′) $N(x + y) \leqslant \max\{N(x), N(y)\} \quad \forall x, y \in R$ with equality if $N(x) \neq N(y)$.

EXAMPLE 2.2. (i) Let $R \subseteq \mathbb{C}$ be a subring of the complex numbers $\mathbb{C}$. Then setting $N(x) = |x|$, the usual absolute value, gives a norm on R. In particular, this applies to the cases $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. This norm is Archimedean because of the inequality

$$|1 + 1| = 2 > |1| = 1.$$

(ii) Let $I = [0, 1]$ be the unit interval and let

$$C(I) = \{f\colon I \longrightarrow \mathbb{R} : f \text{ continuous}\}.$$

Then the function $|f|(x) = |f(x)|$ is continuous for any $f \in C(I)$ and hence by basic analysis,

$$\exists x_f \in I \quad \text{such that} \quad |f|(x_f) = \sup\{|f|(x) : x \in I\}.$$

Hence we can define a function

$$N\colon C(I) \longrightarrow \mathbb{R}^+; \quad N(f) = |f|(x_f),$$

which turns out to be an Archimedean seminorm on $C(I)$, usually called the *supremum seminorm*. This works upon replacing I by any compact set $X \subseteq \mathbb{C}$.

Consider the case of $R = \mathbb{Q}$, the ring of rational numbers a/b, where $a, b \in \mathbb{Z}$ and $b \neq 0$. Suppose that $p \geqslant 2$ is a prime number.

DEFINITION 2.3. If $0 \neq x \in \mathbb{Z}$, the *p-adic ordinal* (or *valuation*) of x is

$$\operatorname{ord}_p x = \max\{r : p^r | x\} \geqslant 0.$$

For $a/b \in \mathbb{Q}$, the *p-adic ordinal* of a/b

$$\operatorname{ord}_p \frac{a}{b} = \operatorname{ord}_p a - \operatorname{ord}_p b.$$

Notice that in all cases, ord_p gives an integer and that for a rational a/b, the value of $\operatorname{ord}_p a/b$ is well defined, *i.e.*, if $a/b = a'/b'$ then

$$\operatorname{ord}_p a - \operatorname{ord}_p b = \operatorname{ord}_p a' - \operatorname{ord}_p b'.$$

We also introduce the convention that $\operatorname{ord}_p 0 = \infty$.

PROPOSITION 2.4. *If $x, y \in \mathbb{Q}$, the ord_p has the following properties:*

(a) $\operatorname{ord}_p x = \infty$ *if and only if* $x = 0$*;*
(b) $\operatorname{ord}_p(xy) = \operatorname{ord}_p x + \operatorname{ord}_p y$*;*
(c) $\operatorname{ord}_p(x + y) \geqslant \min\{\operatorname{ord}_p x, \operatorname{ord}_p y\}$ *with equality if* $\operatorname{ord}_p x \neq \operatorname{ord}_p y$.

PROOF. (a) and (b) are easy and left to the reader; we will therefore only prove (c). Let x, y be non-zero rational numbers. Write $x = p^r \dfrac{a}{b}$ and $y = p^s \dfrac{c}{d}$, where $a, b, c, d \in \mathbb{Z}$ with $p \nmid a, b, c, d$ and $r, s \in \mathbb{Z}$. Now if $r = s$, we have

$$\begin{aligned} x + y &= p^r \left(\frac{a}{b} + \frac{c}{d}\right) \\ &= p^r \frac{(ad + bc)}{bd} \end{aligned}$$

which gives $\operatorname{ord}_p(x + y) \geqslant r$ since $p \nmid bd$.

Now suppose that $r \neq s$, say $s > r$. Then

$$\begin{aligned} x + y &= p^r \left(\frac{a}{b} + p^{s-r}\frac{c}{d}\right) \\ &= p^r \frac{(ad + p^{s-r}bc)}{bd}. \end{aligned}$$

Notice that as $s - r > 0$ and $p \nmid ad$, then

$$\operatorname{ord}_p(x + y) = r = \min\{\operatorname{ord}_p x, \operatorname{ord}_p y\}.$$

The argument for the case where at least one of the terms is 0 is left as an exercise. □

DEFINITION 2.5. For $x \in \mathbb{Q}$, let *the p-adic norm* of x be given by

$$|x|_p = \begin{cases} p^{-\operatorname{ord}_p x} & \text{if } x \neq 0, \\ p^{-\infty} = 0 & \text{if } x = 0. \end{cases}$$

PROPOSITION 2.6. *The function* $|\ |_p \colon \mathbb{Q} \longrightarrow \mathbb{R}^+$ *has the properties*

(a) $|x|_p = 0$ *if and only if* $x = 0$*;*

(b) $|xy|_p = |x|_p|y|_p$*;*

(c) $|x + y|_p \leqslant \max\{|x|_p, |y|_p\}$ *with equality if* $|x|_p \neq |y|_p$.

Hence, $|\ |_p$ *is a non-Archimedean norm on* $\mathbb{Q}$.

PROOF. This follows easily from Proposition 2.4. □

Now consider a general norm N on a ring R.

DEFINITION 2.7. The *distance* between $x, y \in R$ with respect to N is

$$\mathrm{d}_N(x, y) = N(x - y) \in \mathbb{R}^+.$$

It easily follows from the properties of a norm that

(Da) $\mathrm{d}_N(x, y) = 0$ if and only if $x = y$;

(Db) $\mathrm{d}_N(x, y) = \mathrm{d}_N(y, x) \quad \forall x, y \in R$;

(Dc) $\mathrm{d}_N(x, y) \leqslant \mathrm{d}_N(x, z) + \mathrm{d}_N(z, y)$ if $z \in R$ is a third element.

Moreover, if N is non-Archimedean, then the second property is replaced by

(Dd) $\mathrm{d}_N(x, y) \leqslant \max\{\mathrm{d}_N(x, z), \mathrm{d}_N(z, y)\}$ with equality if $\mathrm{d}_N(x, z) \neq \mathrm{d}_N(z, y)$.

PROPOSITION 2.8 (The Isosceles Triangle Principle). *Let N be a non-Archimedean norm on a ring R. Let $x, y, z \in R$ be such that $\mathrm{d}_N(x, y) \neq \mathrm{d}_N(z, y)$. Then*

$$\mathrm{d}_N(x, y) = \max\{\mathrm{d}_N(x, z), \mathrm{d}_N(z, y)\}.$$

Hence, every triangle is isosceles in the non-Archimedean world.

PROOF. Use (Dd) above. □

Now let $(a_n)_{n \geqslant 1}$ be a sequence of elements of R, a ring with norm N.

DEFINITION 2.9. The sequence (a_n) *tends to the limit* $a \in R$ *with respect to* N if

$$\forall \varepsilon > 0 \ \exists M \in \mathbb{N} \quad \text{such that} \quad n > M \Longrightarrow N(a - a_n) = \mathrm{d}_N(a, a_n) < \varepsilon.$$

We use the notation

$$\lim_{n \to \infty}{}^{(N)} a_n = a$$

which is reminiscent of the notation in Analysis and also keeps the norm in mind.

DEFINITION 2.10. The sequence (a_n) is *Cauchy with respect to* N if

$$\forall \varepsilon > 0 \exists M \in \mathbb{N} \quad \text{such that} \quad m, n > M \Longrightarrow N(a_m - a_n) = \mathrm{d}_N(a_m, a_n) < \varepsilon.$$

PROPOSITION 2.11. *If* $\lim\limits_{n\to\infty}^{(N)} a_n$ *exists, then* (a_n) *is Cauchy with respect to* N.

PROOF. Let $a = \lim\limits_{n\to\infty}^{(N)} a_n$. Then we can find a M_1 such that

$$n > M_1 \Longrightarrow N(a - a_n) < \frac{\varepsilon}{2}.$$

If $m, n > M_1$, then $N(a-a_m) < \varepsilon/2$ and $N(a-a_n) < \varepsilon/2$, hence by making use of the inequality from (Nc) we obtain

$$\begin{aligned} N(a_m - a_n) &= N\left((a_m - a) + (a - a_n)\right) \\ &\leqslant N(a_m - a) + N(a - a_n) \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

□

Exercise: Show that in the case where N is non-Archimedean, the inequality

$$N(a_m - a_n) < \frac{\varepsilon}{2}$$

holds in this proof.

Consider the case of $R = \mathbb{Q}$, the rational numbers, with the p-adic norm $|\ |_p$.

EXAMPLE 2.12. Take the sequence $a_n = 1 + p + p^2 + \cdots + p^{n-1}$. Then we have

$$\begin{aligned} |a_{n+k} - a_n|_p &= \left|p^n + p^{n+1} + \cdots + p^{n+k-1}\right|_p \\ &= \left|p^n(1 + p + p^2 \cdots + p^{k-1})\right|_p \\ &= \frac{1}{p^n}. \end{aligned}$$

For each $\varepsilon > 0$, we can choose an M for which $p^M \geqslant 1/\varepsilon$, so if $n > M$ we have

$$|a_{n+k} - a_n|_p < \frac{1}{p^M} \leqslant \varepsilon.$$

This shows that (a_n) is Cauchy.

In fact, this sequence has a limit with respect to $|\ |_p$. Take $a = 1/(1-p) \in \mathbb{Q}$; then we have $a_n = (p^n - 1)/(p - 1)$, hence

$$\left|a_n - \frac{1}{(1-p)}\right|_p = \left|\frac{p^n}{(p-1)}\right|_p = \frac{1}{p^n}.$$

So for $\varepsilon > 0$, we have

$$\left|a_n - \frac{1}{(1-p)}\right|_p < \varepsilon$$

whenever $n > M$ (as above).

From now on we will write $\lim\limits_{n\to\infty}^{(p)}$ in place of $\lim\limits_{n\to\infty}^{(N)}$. So in the last example, we have

$$\lim_{n\to\infty}^{(p)}(1 + p + \cdots + p^{n-1}) = \frac{1}{(1-p)}.$$

Again consider a general norm N on a ring R.

DEFINITION 2.13. A sequence (a_n) is called a *null sequence* if

$$\lim_{n\to\infty}^{(N)} a_n = 0.$$

Of course this assumes the limit exists! This is easily seen to be equivalent to the the fact that in the real numbers with the usual norm $|\ |$,

$$\lim_{n\longrightarrow\infty} N(a_n) = 0.$$

EXAMPLE 2.14. In the ring $\mathbb{Q}$ together with p-adic norm $|\ |_p$, we have $a_n = p^n$. Then

$$|p^n|_p = \frac{1}{p^n} \longrightarrow 0 \quad \text{as } n \longrightarrow \infty$$

so $\lim_{n\to\infty}^{(p)} a_n = 0$. Hence this sequence is null with respect to the p-adic norm.

EXAMPLE 2.15. Use the same norm as in Example 2.14 with $a_n = (1+p)^{p^n} - 1$. Then for $n = 1$,

$$\begin{aligned} |a_1|_p &= |(1+p)^p - 1|_p \\ &= \left| \binom{p}{1} p + \cdots + \binom{p}{p-1} p^{p-1} + p^p \right|_p \\ &= \frac{1}{p^2}, \end{aligned}$$

since for $1 \leqslant k \leqslant p-1$,

$$\operatorname{ord}_p \binom{p}{k} = 1.$$

Hence $|a_1|_p = 1/p^2$.

For general n, we proceed by induction upon n, and show that

$$|a_n|_p = \frac{1}{p^{n+1}}.$$

Hence we see that as $n \longrightarrow \infty$, $|a_n|_p \longrightarrow 0$, so this sequence is null with respect to the p-adic norm $|\ |_p$.

EXAMPLE 2.16. $R = \mathbb{Q}$, $N = |\ |$, the usual norm. Consider the sequence (a_n) whose n-th term is the decimal expansion of $\sqrt{2}$ up to the n-th decimal place, *i.e.*, $a_1 = 1.4$, $a_2 = 1.41$, $a_3 = 1.414$, etc. Then it is well known that $\sqrt{2}$ is not a *rational* number although it is real, but (a_n) is a Cauchy sequence.

The last example shows that there may be holes in a normed ring, *i.e.*, limits of Cauchy sequences need not exist. The real numbers can be thought of as the rational numbers with all the missing limits put in. We will develop this idea next.

Let R be a ring with a norm N. Define the following two sets:

$$\begin{aligned} \mathrm{CS}(R,N) &= \text{the set of Cauchy sequences in } R \text{ with respect to } N, \\ \mathrm{Null}(R,N) &= \text{the set of null sequences in } R \text{ with respect to } N. \end{aligned}$$

So the elements of $\mathrm{CS}(R,N)$ are Cauchy sequences (a_n) in R, and the elements of $\mathrm{Null}(R,N)$ are null sequences (a_n). Notice that

$$\mathrm{Null}(R,N) \subseteq \mathrm{CS}(R,N).$$

We can add and multiply the elements of $\mathrm{CS}(R,N)$, using the formulae

$$(a_n)+(b_n)=(a_n+b_n), \quad (a_n)\times(b_n)=(a_nb_n),$$

since it is easily checked that these binary operations are functions of the form

$$+,\times\colon \mathrm{CS}(R,N)\times\mathrm{CS}(R,N)\longrightarrow \mathrm{CS}(R,N).$$

Claim: The elements $0_{\mathrm{CS}}=(0), 1_{\mathrm{CS}}=(1_R)$ together with these operations turn $\mathrm{CS}(R,N)$ into a ring (commutative if R is) with zero 0_{CS} and unity 1_{CS}. Moreover, the subset $\mathrm{Null}(R,N)$ is a two sided ideal of $\mathrm{CS}(R,N)$, since if $(a_n)\in\mathrm{CS}(R,N)$ and $(b_n)\in\mathrm{Null}(R,N)$, then

$$(a_nb_n),(b_na_n)\in\mathrm{Null}(R,N)$$

as can be seen by calculating $\lim\limits_{n\to\infty}^{(N)} a_nb_n$ and $\lim\limits_{n\to\infty}^{(N)} b_na_n$.

We can then define the *quotient ring* $\mathrm{CS}(R,N)/\mathrm{Null}(R,N)$; this is called the *completion of R with respect to the norm N*, and is denoted $\widehat{R}_N$ or just $\hat{R}$ if the norm is clear. We write $\{a_n\}$ for the coset of the Cauchy sequence (a_n). The zero and unity are of course $\{0_R\}$ and $\{1_R\}$ respectively. The norm N can be extended to $\widehat{R}_N$ as the following important result shows.

THEOREM 2.17. *The ring $\widehat{R}_N$ has sum $+$ and product $\times$ given by*

$$\{a_n\}+\{b_n\}=\{a_n+b_n\}, \quad \{a_n\}\times\{b_n\}=\{a_nb_n\},$$

and is commutative if R is. Moreover, there is a unique norm $\hat{N}$ on $\widehat{R}_N$ which satisfies $\hat{N}(\{a\})=N(a)$ for a constant Cauchy sequence $(a_n)=(a)$ with $a\in R$; this norm is defined by

$$\hat{N}(\{c_n\})=\lim_{n\longrightarrow\infty} N(c_n)$$

as a limit in the real numbers $\mathbb{R}$. Finally, $\hat{N}$ is non-Archimedean if and only if N is.

PROOF. We will first verify that $\hat{N}$ is a norm. Let $\{a_n\}\in\hat{R}$. We should check that the definition of $\hat{N}(\{a_n\})$ makes sense. For each $\varepsilon>0$, we have an M such that whenever $m,n>M$ then $N(a_m,a_n)<\varepsilon$. To proceed further we need to use an inequality.
Claim:

$$|N(x)-N(y)|\leqslant N(x-y) \quad \text{for all } x,y\in R.$$

PROOF. By (Nc),

$$N(x)=N\left((x-y)+y\right)\leqslant N(x-y)+N(y)$$

implying

$$N(x)-N(y)\leqslant N(x-y).$$

Similarly,

$$N(y)-N(x)\leqslant N(y-x).$$

Since $N(-z) = N(z)$ for all $z \in R$ (why?), we have

$$|N(x) - N(y)| \leqslant N(x - y). \qquad \square$$

This result tells us that for $\varepsilon > 0$, there is an M for which whenever $m, n > M$ we have

$$|N(a_m) - N(a_n)| < \varepsilon,$$

which shows that the sequence of real numbers $(N(a_n))$ is a Cauchy sequence with respect to the usual norm $|\ |$. By basic Analysis, we know it has a limit, say

$$\ell = \lim_{n\to\infty} N(a_n).$$

Hence, there is an M' such that $M' < n$ implies that

$$|\ell - N(a_n)| < \varepsilon.$$

So we have shown that $\hat{N}(\{a_n\}) = \ell$ is defined.

We have

$$\begin{aligned} \hat{N}(\{a_n\}) = 0 \quad &\iff \quad \lim_{n\to\infty} N(a_n) = 0 \\ &\iff \quad (a_n) \quad \text{is a null sequence} \\ &\iff \quad \{a_n\} = 0, \end{aligned}$$

proving (Na). Also, given $\{a_n\}$ and $\{b_n\}$, we have

$$\begin{aligned} \hat{N}(\{a_n\}\{b_n\}) = \hat{N}(\{a_n b_n\}) &= \lim_{n\to\infty} N(a_n b_n) \\ &= \lim_{n\to\infty} N(a_n) N(b_n) \\ &= \lim_{n\to\infty} N(a_n) \lim_{n\to\infty} N(b_n) \\ &= \hat{N}(\{a_n\})\hat{N}(\{b_n\}), \end{aligned}$$

which proves (Nb). Finally,

$$\begin{aligned} \hat{N}(\{a_n\} + \{b_n\}) &= \lim_{n\to\infty} N(a_n + b_n) \\ &\leqslant \lim_{n\to\infty} (N(a_n) + N(b_n)) \\ &= \lim_{n\to\infty} N(a_n) + \lim_{n\to\infty} N(b_n) \\ &= \hat{N}(\{a_n\}) + \hat{N}(\{b_n\}), \end{aligned}$$

which gives (Nc). Thus $\hat{N}$ is certainly a norm. We still have to show that if N is non-Archimedean then so is $\hat{N}$. We will use the following important Lemma.

LEMMA 2.18. *Let R be a ring with a non-Archimedean norm N. Suppose that (a_n) is a Cauchy sequence and that $b \in R$ has the property that $b \neq \lim^{(N)}_{n\to\infty} a_n$. Then there is an M such that for all $m, n > M$,*

$$N(a_m - b) = N(a_n - b),$$

so the sequence of real numbers $(N(a_n - b))$ is eventually constant. In particular, if (a_n) is not a null sequence, then the sequence $(N(a_n))$ is eventually constant.

PROOF. Notice that

$$|N(a_m - b) - N(a_n - b)| \leqslant N(a_m - a_n),$$

so $(N(a_n - b))$ is Cauchy in $\mathbb{R}$. Let $\ell = \lim_{n\to\infty} N(a_n - b)$; notice also that $\ell > 0$. Hence there exists an M_1 such that $n > M_1$ implies

$$N(a_n - b) > \frac{\ell}{2}.$$

Also, there exists an M_2 such that $m, n > M_2$ implies

$$N(a_m - a_n) < \frac{\ell}{2},$$

since (a_n) is Cauchy with respect to N. Now take $M = \max\{M_1, M_2\}$ and consider $m, n > M$. Then

$$\begin{aligned} N(a_m - b) &= N\left((a_n - b) + (a_m - a_n)\right) \\ &= \max\{N(a_n - b), N(a_m - a_n)\} \\ &= N(a_n - b) \end{aligned}$$

since $N(a_n - b) > \ell/2$ and $N(a_m - a_n) < \ell/2$. □

Let us return to the proof of Theorem 2.17. Let $\{a_n\}$, $\{b_n\}$ have the property that

$$\hat{N}(\{a_m\}) \neq \hat{N}(\{b_m\});$$

furthermore, we can assume that neither of these is $\{0\}$, since otherwise the inequality in (Nd) is trivial to verify. By the Lemma with $b = 0$ we can find integers M', M'' such that

$$n > M' \implies N(a_n) = \hat{N}(\{a_n\})$$

and

$$n > M' \implies N(b_n) = \hat{N}(\{b_n\}).$$

Thus for $n > \max\{M', M''\}$, we have

$$\begin{aligned} N(a_n + b_n) &= \max\{N(a_n), N(b_n)\} \\ &= \max\{\hat{N}(\{a_n\}), \hat{N}(\{b_n\})\}. \end{aligned}$$

This proves (Nd) for $\hat{N}$ and completes the proof of Theorem 2.17. □

DEFINITION 2.19. A ring with norm N is *complete with respect to the norm* N if every Cauchy sequence has a limit in R with respect to N.

EXAMPLE 2.20. The ring of real numbers (resp. complex numbers) is complete with respect to the usual norm $|\ |$.

DEFINITION 2.21. Let R be a ring with norm N, and let $X \subseteq R$; then X is *dense* in R if every element of R is a limit (with respect to N) of elements of X.

THEOREM 2.22. *Let R be a ring with norm N. Then $\hat{R}$ is complete with respect to $\hat{N}$. Moreover, R can be identified with a dense subring of $\hat{R}$.*

PROOF. First observe that for $a \in R$, the constant sequence $(a_n) = (a)$ is Cauchy and so we obtain the element $\{a\}$ in $\hat{R}$; this allows us to embed R as a subring of $\hat{R}$ (it is necessary to verify that the inclusion $R \hookrightarrow \hat{R}$ preserves sums and products). We will identify R with its image without further comment; thus we will often use $a \in R$ to denote the element $\{a\} \in \hat{R}$. It is easy to verify that if (a_n) is a Cauchy sequence in R with respect to N, then (a_n) is also a Cauchy sequence in $\hat{R}$ with respect to $\hat{N}$. Of course it may not have a limit in R, but it *always* has a limit in $\hat{R}$, namely the element $\{a_n\}$ by definition of $\hat{R}$.

Now suppose that (α_n) is Cauchy sequence in $\hat{R}$ with respect to the norm $\hat{N}$. Then we must show that there is an element $\alpha \in \hat{R}$ for which

$$\lim_{n\to\infty}^{(\hat{N})} \alpha_n = \alpha. \tag{2.1}$$

Notice that each α_m is in fact the equivalence class of a Cauchy sequence (a_{mn}) in R with respect to the norm N, hence if we consider each a_{mn} as an element of $\hat{R}$ as above, we can write

$$\alpha_m = \lim_{n\to\infty}^{(\hat{N})} a_{mn}. \tag{2.2}$$

We need to construct a Cauchy sequence (c_n) in R with respect to N such that

$$\{c_n\} = \lim_{m\to\infty}^{(\hat{N})} \alpha_m.$$

Then $\alpha = \{c_n\}$ is the required limit of (α_n).

Now for each m, by Equation (2.2) there is an M_m such that whenever $n > M_m$,

$$\hat{N}(\alpha_m - a_{mn}) < \frac{1}{m}.$$

For each m we now choose an integer $k(m) > M_m$; we can even assume that these integers are strictly increasing, hence

$$k(1) < k(2) < \cdots < k(m) < \cdots .$$

We define our sequence (c_n) by setting $c_n = a_{n\,k(n)}$. We must show it has the required properties.

LEMMA 2.23. *(c_n) is Cauchy with respect to N and hence $\hat{N}$.*

PROOF. Let $\varepsilon > 0$. As (α_n) is Cauchy there is an M' such that if $n_1, n_2 > M'$ then

$$\hat{N}(\alpha_{n_1} - \alpha_{n_2}) < \frac{\varepsilon}{3}.$$

Thus

$$\begin{aligned}\hat{N}(c_{n_1} - c_{n_2}) &= \hat{N}\left((a_{n_1\,k(n_1)} - \alpha_{n_1}) + (\alpha_{n_1} - \alpha_{n_2}) + (\alpha_{n_2} - a_{n_2\,k(n_2)})\right) \\ &\leqslant \hat{N}(a_{n_1\,k(n_1)} - \alpha_{n_1}) + \hat{N}(\alpha_{n_1} - \alpha_{n_2}) + \hat{N}(\alpha_{n_2} - a_{n_2\,k(n_2)}).\end{aligned}$$

If we now choose $M = \max\{M', 3/\varepsilon\}$, then for $n_1, n_2 > M$, we have

$$\hat{N}(c_{n_1} - c_{n_2}) < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon,$$

and so the sequence (c_n) is indeed Cauchy. □

LEMMA 2.24. $\lim\limits_{m\to\infty}^{(\hat{N})}\alpha_m = \{c_n\}$.

PROOF. Let $\varepsilon > 0$. Then denoting $\{c_n\}$ by γ we have

$$\begin{aligned}\hat{N}(\gamma - \alpha_m) &= \hat{N}\left((\gamma - a_{m\,k(m)}) + (a_{m\,k(m)} - \alpha_m)\right)\\ &\leqslant \hat{N}(\gamma - a_{m\,k(m)}) + \hat{N}(a_{m\,k(m)} - \alpha_m)\\ &= \lim_{n\to\infty} N(a_{n\,k(n)} - a_{m\,k(m)}) + \hat{N}(a_{m\,k(m)} - \alpha_m).\end{aligned}$$

Next choose M'' so that $M'' \geqslant 2/\varepsilon$ and whenever $n_1, n_2 > M''$ then

$$N(a_{n_1\,k(n_1)} - a_{n_2\,k(n_2)}) < \frac{\varepsilon}{2}.$$

So for $m, n > M''$ we have

$$N(a_{m\,k(m)} - a_{n\,k(n)}) + \hat{N}(a_{m\,k(m)} - \alpha_m) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Hence we see that

$$\hat{N}(\gamma - \alpha_m) < \varepsilon \quad \forall m > M''. \qquad \square$$

Lemmas 2.23 and 2.24 complete the proof of Theorem 2.22. $\square$

We will now focus attention upon the case of $R = \mathbb{Q}$ equipped with the p-adic norm $N = |\ |_p$ for a prime p.

DEFINITION 2.25. The ring of *p-adic numbers* is the completion $\hat{\mathbb{Q}}$ of $\mathbb{Q}$ with respect to $N = |\ |_p$; we will denote it $\mathbb{Q}_p$. The norm on $\mathbb{Q}_p$ will be denoted $|\ |_p$.

DEFINITION 2.26. The unit disc about $0 \in \mathbb{Q}_p$ is the set of *p-adic integers*,

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leqslant 1\}.$$

PROPOSITION 2.27. *The set of p-adic integers $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. Every element of $\mathbb{Z}_p$ is the limit of a sequence of (non-negative) integers and conversely, every Cauchy sequence in $\mathbb{Q}$ consisting of integers has a limit in $\mathbb{Z}_p$.*

PROOF. Let $\alpha, \beta \in \mathbb{Z}_p$. Then

$$|\alpha + \beta|_p \leqslant \max\{|\alpha|_p, |\beta|_p\} \leqslant 1$$

and hence $\alpha + \beta \in \mathbb{Z}_p$. Similarly, $\alpha\beta \in \mathbb{Z}_p$ by (Nb). Thus $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.

From the definition of $\mathbb{Q}_p$, we have that if $\alpha \in \mathbb{Z}_p$, then $\alpha = \{a_n\}$ with $a_n \in \mathbb{Q}$ and the sequence (a_n) being Cauchy. By Lemma 2.18, we know that for some M, if $n > M$ then $|a_n|_p = c$ for some constant $c \in \mathbb{Q}$. But then we have $|\alpha|_p = c$ and so $c \leqslant 1$. So without loss of generality, we can assume that $|a_n|_p \leqslant 1$ for all n. Now write $a_n = r_n/s_n$ with $r_n, s_n \in \mathbb{Z}$ and $r_n, s_n \neq 0$. Then we can assume $s_n \not\equiv_p 0$ as $\operatorname{ord}_p r_n - \operatorname{ord}_p s_n \geqslant 0$. But this means that for each m we can solve the equation $s_n x \underset{p^m}{\equiv} 1$ in $\mathbb{Z}$ (see Chapter 1), so let $u_{nm} \in \mathbb{Z}$ satisfy $s_n u_{nm} \underset{p^m}{\equiv} 1$. We can even assume that $1 \leqslant u_{nm} \leqslant p^m - 1$ by adding on multiples of p^m if necessary. Thus for each m we have

$$|s_n u_{nm} - 1|_p \leqslant \frac{1}{p^m}.$$

Then find for each m,

$$\left|\frac{r_n}{s_n} - r_n u_{nm}\right|_p = \left|\frac{r_n(1 - s_n u_{nm})}{s_n}\right|_p \leqslant \frac{1}{p^m}.$$

Now for each m, there is an k_m for which

$$|\alpha - a_{k_m}|_p < \frac{1}{p^m},$$

therefore

$$\begin{aligned}\left|\alpha - r_{k_m} u_{k_m\,(m+1)}\right|_p &= \left|(\alpha - a_{k_m}) + (a_{k_m} - r_{k_m} u_{k_m\,(m+1)})\right|_p \\ &\leqslant \max\{|\alpha - a_{k_m}|_p, \left|a_{k_m} - r_{k_m} u_{k_m\,(m+1)}\right|_p\} \\ &< \frac{1}{p^m}.\end{aligned}$$

Hence

$$\lim_{n\to\infty}{}^{(p)}(\alpha - r_{k_n} u_{k_n\,(n+1)}) = 0,$$

showing that α is a limit of non-negative integers as required. □

Now we will describe the elements of $\mathbb{Q}_p$ explicitly, using the *p-adic digit expansion*. We will begin with elements of $\mathbb{Z}_p$. So suppose that $\alpha \in \mathbb{Z}_p$. By Proposition 2.27 we know that there is an integer α_0 satisfying the conditions

$$|\alpha_0 - \alpha|_p < 1, \quad 0 \leqslant \alpha_0 \leqslant (p-1).$$

The p-adic integer $\alpha - \alpha_0$ has norm $\leqslant 1/p$ and so the p-adic number $(\alpha - \alpha_0)/p$ is in $\mathbb{Z}_p$. Repeating the last step, we obtain an integer α_1 satisfying

$$|\alpha - (\alpha_0 + \alpha_1 p)|_p < \frac{1}{p}, \quad 0 \leqslant \alpha_1 \leqslant (p-1).$$

Again repeating this, we find a sequence of integers α_n for which

$$|\alpha - (\alpha_0 + \alpha_1 p + \cdots + \alpha_n p^n))|_p < \frac{1}{p^n}, \quad 0 \leqslant \alpha_n \leqslant (p-1).$$

The sequence (β_n) for which

$$\beta_n = \alpha_0 + \alpha_1 p + \cdots + \alpha_n p^n$$

is Cauchy with respect to $|\ |_p$. Moreover its limit is α since

$$|\alpha - \beta_n|_p < \frac{1}{p^n}.$$

So we have an expansion

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$$

reminiscent of the decimal expansion of a real number but with possibly infinitely many positive powers of p. This is the (*standard*) *p-adic expansion* of $\alpha \in \mathbb{Z}_p$ and the α_n are known as the (*standard*) *p-adic digits*. It has one subtle difference from the decimal expansion of a real number, namely it is *unique*. To see this, suppose that

$$\alpha = \alpha'_0 + \alpha'_1 p + \alpha'_2 p^2 + \cdots$$

is a second such expansion with the properties of the first. Let d be the first integer for which $\alpha_d \neq \alpha'_d$. Then we can assume without loss of generality that $\alpha_d < \alpha'_d$ and hence $1 \leqslant \alpha'_d - \alpha_d \leqslant (p-1)$. If

$$\beta'_n = \alpha'_0 + \alpha'_1 p + \cdots + \alpha'_n p^n,$$

then

$$\beta'_d - \beta_d = (\alpha'_d - \alpha_d)p^d,$$

hence

$$\left|\beta'_d - \beta_d\right|_p = \frac{1}{p^d}.$$

Notice that

$$\begin{aligned}\left|\beta'_d - \beta_d\right|_p &= \left|(\beta'_d - \alpha) + (\alpha - \beta_d)\right|_p \\ &\leqslant \max\{\left|\beta'_d - \alpha\right|_p, |\alpha - \beta_d|_p\} \\ &< \frac{1}{p^d},\end{aligned}$$

which clearly contradicts the last equality. So no such d can exist and there is only one such expansion.

Now let $\alpha \in \mathbb{Q}_p$ be any p-adic number. If $|\alpha|_p \leqslant 1$, we have already seen how to find its p-adic expansion. If $|\alpha|_p > 1$, suppose $|\alpha|_p = p^k$ with $k > 0$. Consider $\beta = p^k\alpha$, which has $|\beta|_p = 1$; this has a p-adic expansion

$$\beta = \beta_0 + \beta_1 p + \beta_2 p^2 + \cdots$$

as above. Then

$$\alpha = \frac{\beta_0}{p^k} + \frac{\beta_1}{p^{k-1}} + \cdots + \frac{\beta_{k-1}}{p} + \beta_k + \beta_{k+1}p + \cdots + \beta_{k+r}p^r + \cdots$$

with $0 \leqslant \beta_n \leqslant (p-1)$ for each n.

Our discussion has established the following important result.

THEOREM 2.28. *Every p-adic number $\alpha \in \mathbb{Q}_p$ has a unique p-adic expansion*

$$\alpha = \alpha_{-r}p^{-r} + \alpha_{1-r}p^{1-r} + \alpha_{2-r}p^{2-r} + \cdots + \alpha_{-1}p^{-1} + \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$$

with $\alpha_n \in \mathbb{Z}$ and $0 \leqslant \alpha_n \leqslant (p-1)$. Furthermore, $\alpha \in \mathbb{Z}_p$ if and only if $\alpha_{-r} = 0$ whenever $r > 0$.

We can do arithmetic in $\mathbb{Q}_p$ in similar fashion to the way it is done in $\mathbb{R}$ with decimal expansions.

EXAMPLE 2.29. Find

$$(1/3 + 2 + 2\cdot 3 + 0\cdot 3^2 + 2\cdot 3^3 + \cdots) + (2/3^2 + 0/3 + 1 + 2\cdot 3 + 1\cdot 3^2 + 1\cdot 3^3 + \cdots).$$

The idea is start at the left and work towards the right. Thus if the answer is

$$\alpha = a_{-2}/3^2 + a_{-1}/3 + a_0 + a_1 3 + \cdots,$$

then

$$a_{-2} = 2, \quad a_{-1} = 1, \quad a_0 = 2 + 1 = 0 + 1\cdot 3 \underset{3}{\equiv} 0,$$

and so

$$a_1 = 2 + 2 + 1 = 2 + 1 \cdot 3 \underset{3}{\equiv} 2$$

where the 1 is carried from the 3^0 term. Continuing we get

$$a_2 = 0 + 1 + 1 = 2, \quad a_3 = 2 + 1 = 0 + 1 \cdot 3 \underset{3}{\equiv} 0,$$

and so we get

$$\alpha = 2/3^2 + 1/3 + 0 + 2 \cdot 3 + 2 \cdot 3^2 + 0 \cdot 3^3 + \cdots$$

as the sum to within a term of 3-adic norm smaller than $1/3^3$.

Notice that the p-adic expansion of a p-adic number is unique, whereas the decimal expansion of a real need not be. For example

$$0.999 \cdots = 1.000 \cdots = 1.$$

We end this section with another fact about completions.

THEOREM 2.30. *Let R be field with norm N. Then $\hat{R}$ is a field. In particular, $\mathbb{Q}_p$ is a field.*

PROOF. Let $\{a_n\}$ be an element of $\hat{R}$, not equal to $\{0\}$. Then $\hat{N}(\{a_n\}) \neq 0$. Put

$$\ell = \hat{N}(\{a_n\}) = \lim_{n \to \infty} N(a_n) > 0.$$

Then there is an M such that $n > M$ implies that $N(a_n) > \ell/2$ (why?), so for such an n we have $a_n \neq 0$. So eventually a_n has an inverse in R. Now define the sequence (b_n) in R by $b_n = 1$ if $n \leqslant M$ and $b_n = a_n^{-1}$ if $n > M$. Thus this sequence is Cauchy and

$$\lim_{n \to \infty}^{(N)} a_n b_n = 1,$$

which implies that

$$\{a_n\}\{b_n\} = \{1\}.$$

Thus $\{a_n\}$ has inverse $\{b_n\}$ in $\hat{R}$. □

CHAPTER 3

Some elementary p-adic analysis

In this chapter we will investigate elementary p-adic analysis, including concepts such as convergence of sequences and series, continuity and other topics familiar from elementary real analysis, but now in the context of the p-adic numbers $\mathbb{Q}_p$ with the p-adic norm $|\ |_p$.

Let $\alpha = \{a_n\} \in \mathbb{Q}_p$. From Chapter 2 we know that for some M,

$$|\alpha|_p = \frac{1}{p^{\operatorname{ord}_p a_M}},$$

which is an integral power of p. So for $t \in \mathbb{Z}$, an inequality of form

$$|\alpha|_p < \frac{1}{p^t}$$

is equivalent to

$$|\alpha|_p \leqslant \frac{1}{p^{t+1}}.$$

Let (α_n) be a sequence in $\mathbb{Q}_p$.

PROPOSITION 3.1. *(α_n) is a Cauchy sequence in $\mathbb{Q}_p$ if and only if $(\alpha_{n+1} - \alpha_n)$ is a null sequence.*

PROOF. See Problem set 3. □

Next we will now consider *series* in $\mathbb{Q}_p$. Suppose that (α_n) is a sequence in $\mathbb{Q}_p$. For each n we can consider the *n-th partial sum of the series* $\sum \alpha_n$,

$$s_n = \alpha_1 + \alpha_2 + \cdots + \alpha_n.$$

DEFINITION 3.2. If the sequence (s_n) in $\mathbb{Q}_p$ has a limit

$$S = \lim_{n\to\infty}{}^{(p)} s_n$$

we say that the series $\sum \alpha_n$ *converges to the limit S* and write

$$\sum_{n=1}^{\infty} \alpha_n = S.$$

S is called the *sum of the series* $\sum \alpha_n$. If the series has no limit we say that it *diverges*.

EXAMPLE 3.3. Taking $\alpha_n = np^n$ we have

$$s_m = \sum_{n=1}^{m} np^n$$

and

$$s_{n+1} - s_n = (n+1)p^{n+1}.$$

This has norm

$$\left|(n+1)p^{n+1}\right|_p = |n+1|_p \left|p^{n+1}\right|_p \leqslant \frac{1}{p^{n+1}},$$

which clearly tends to 0 as $n \longrightarrow \infty$ in the real numbers. By Proposition 3.1, (s_n) is a Cauchy sequence and therefore it has a limit in $\mathbb{Q}_p$.

In *real* analysis, there are series which converge but are not *absolutely* convergent. For example, the series $\sum(-1)^n/n$ converges to $-\ln 2$ but $\sum 1/n$ diverges. Our next result shows that this cannot happen in $\mathbb{Q}_p$.

PROPOSITION 3.4. *The series $\sum \alpha_n$ in $\mathbb{Q}_p$ converges if and only if (α_n) is a null sequence.*

PROOF. If $\sum \alpha_n$ converges then by Proposition 3.1 the sequence of partial sums (s_n) is Cauchy since

$$s_{n+1} - s_n = \alpha_n$$

is a null sequence. Conversely, if (α_n) is null, then by Proposition 3.1 we see that the sequence (s_n) is Cauchy and hence converges. □

So to check convergence of a series $\sum \alpha_n$ in $\mathbb{Q}_p$ it suffices to investigate whether

$$\lim_{n\to\infty}{}^{(p)} \alpha_n = 0.$$

This means that convergence of series in $\mathbb{Q}_p$ is generally far easier to deal with than convergence of series in the real or complex numbers.

EXAMPLE 3.5. The series $\sum p^n$ converges since in $\mathbb{R}$ we have

$$|p^n|_p = \frac{1}{p^n} \longrightarrow 0.$$

In fact,

$$\sum p^n = \lim_{m\to\infty}{}^{(p)} \sum_{n=0}^{m} p^n = \frac{1}{(1-p)}.$$

EXAMPLE 3.6. The series $\sum 1/n$ diverges in $\mathbb{Q}_p$ since for example the subsequence

$$\beta_n = \frac{1}{np+1}$$

of the sequence $(1/n)$ has $|\beta_n|_p = 1$ for every n.

As a particular type of series we can consider *power series* (in one variable x). Let $x \in \mathbb{Q}_p$ and let (α_n) be a sequence. Then we have the series $\sum \alpha_n x^n$. As in real analysis, we can investigate for which values of x this converges or diverges.

EXAMPLE 3.7. Take $\alpha_n = 1$ for all n. Then

$$\lim_{n\to\infty}{}^{(p)} x^n \begin{cases} = 0 & \text{if } |x|_p < 1, \\ \geqslant 1 & \text{otherwise.} \end{cases}$$

So this series converges if and only if $|x|_p < 1$. Of course, in $\mathbb{R}$ the series $\sum x^n$ converges if $|x| < 1$, diverges if $|x| > 1$, diverges to $+\infty$ if $x = 1$ and oscillates through the values 0 and -1 if $x = -1$.

EXAMPLE 3.8. For the series $\sum nx^n$, we have

$$|nx^n|_p = |n|_p |x^n|_p \leqslant |x|_p{}^n$$

which tends to 0 in $\mathbb{R}$ if $|x|_p < 1$. So this series certainly converges for every such x.

Just as in real analysis, we can define a notion of *radius of convergence* for a power series in $\mathbb{Q}_p$. For technical reasons, we will have to proceed with care to obtain a suitable definition. We first need to recall from real analysis the idea of the *limit superior* (lim sup) of a sequence of real numbers.

DEFINITION 3.9. A real number ℓ is the *limit superior* of the sequence of real numbers (a_n) if the following conditions are satisfied:
(LS1) For real number $\varepsilon_1 > 0$,

$$\exists M_1 \in \mathbb{N} \quad \text{such that} \quad n > M_1 \Longrightarrow \ell + \varepsilon_1 > a_n.$$

(LS2) For real number $\varepsilon_2 > 0$ and natural number M_2,

$$\exists m > M_2 \quad \text{such that} \quad a_m > \ell - \varepsilon_2.$$

We write

$$\ell = \limsup_n a_n$$

if such a real number exists. If no such ℓ exists, we write

$$\limsup_n a_n = \infty.$$

It is a standard fact that if the sequence (a_n) converges then $\limsup a_n$ exists and

$$\limsup_n a_n = \lim_{n\longrightarrow\infty} a_n.$$

In practise, this gives a useful method of computing $\limsup a_n$ in many cases.

Now consider a power series $\sum \alpha_n x^n$ where $\alpha_n \in \mathbb{Q}_p$. Then we can define the *radius of convergence* of $\sum \alpha_n x^n$ by the formula

$$r = \frac{1}{\limsup |\alpha_n|_p{}^{1/n}}. \tag{3.1}$$

PROPOSITION 3.10. *The series $\sum \alpha_n x^n$ converges if $|x|_p < r$ and diverges if $|x|_p > r$, where r is the radius of convergence. If for some x_0 with $|x_0|_p = r$ the series $\sum \alpha_n x_0^n$ converges (or diverges) then $\sum \alpha_n x^n$ converges (or diverges) for all $x \in \mathbb{Q}_p$ with $|x|_p = r$.*

PROOF. This is proved using Proposition 3.4. First notice that if $|x|_p < r$, then

$$|\alpha_n x^n|_p = |\alpha_n|_p |x|_p{}^n \longrightarrow 0$$

as $n \longrightarrow \infty$. Similarly, if $|x_0|_p > r$, then

$$|\alpha_n x^n|_p = |\alpha_n|_p |x|_p{}^n \not\longrightarrow 0$$

as $n \longrightarrow \infty$. Finally, if there is such an x_0, then

$$|\alpha_n x_0^n|_p = |\alpha_n|_p |x_0|_p{}^n \longrightarrow 0$$

as $n \longrightarrow \infty$ and so for every x with $|x|_p = r$ we have

$$|\alpha_n x^n|_p = |\alpha_n x_0^n|_p \longrightarrow 0.$$

□

CHAPTER 4

The topology of $\mathbb{Q}_p$

We will now discuss continuous functions on $\mathbb{Q}_p$ and related topics. We begin by introducing some basic topological notions.

Let $\alpha \in \mathbb{Q}_p$ and $\delta > 0$ be a real number.

DEFINITION 4.1. The *open disc centred at α of radius δ* is

$$\mathrm{D}(\alpha;\delta) = \{\gamma \in \mathbb{Q}_p : |\gamma - \alpha|_p < \delta\}.$$

The *closed disc centred at α of radius δ* is

$$\overline{\mathrm{D}(\alpha;\delta)} = \{\gamma \in \mathbb{Q}_p : |\gamma - \alpha|_p \leqslant \delta\}.$$

Clearly

$$\mathrm{D}(\alpha;\delta) \subseteq \overline{\mathrm{D}(\alpha;\delta)}.$$

Such a notion is familiar in the real or complex numbers; however, here there is an odd twist.

PROPOSITION 4.2. *Let $\beta \in D(\alpha;\delta)$. Then*

$$D(\beta;\delta) = D(\alpha;\delta).$$

Hence every element of $D(\alpha;\delta)$ is a centre. Similarly, if $\beta' \in \overline{D(\alpha;\delta)}$, then

$$\overline{D(\beta';\delta)} = \overline{D(\alpha;\delta)}.$$

PROOF. This is a consequence of the fact that the p-adic norm is non-Archimedean. Let $\gamma \in \mathrm{D}(\alpha;\delta)$; then

$$\begin{aligned} |\gamma - \beta|_p &= |(\gamma - \alpha) + (\alpha - \beta)|_p \\ &\leqslant \max\{|\gamma - \alpha|_p, |\alpha - \beta|_p\} \\ &< \delta. \end{aligned}$$

Thus $\mathrm{D}(\alpha;\delta) \subseteq \mathrm{D}(\beta;\delta)$. Similarly we can show that $\mathrm{D}(\beta;\delta) \subseteq \mathrm{D}(\alpha;\delta)$ and therefore these two sets are equal. A similar argument deals with the case of closed discs. □

Let $X \subseteq \mathbb{Q}_p$ (for example, $X = \mathbb{Z}_p$).

DEFINITION 4.3. The set

$$\mathrm{D}_X(\alpha;\delta) = \mathrm{D}(\alpha;\delta) \cap X$$

is the *open ball of radius δ in X centred at α*. Similarly,

$$\overline{\mathrm{D}_X(\alpha;\delta)} = \overline{\mathrm{D}(\alpha;\delta)} \cap X$$

is the *closed ball in X of radius δ centred at α*.

We will now define a continuous function. Let $f\colon X \longrightarrow \mathbb{Q}_p$ be a function.

Definition 4.4. We say that f is *continuous at $\alpha \in X$* if

$$\forall \varepsilon > 0 \exists \delta > 0 \quad \text{such that} \quad \gamma \in \mathrm{D}_X(\alpha;\delta) \Longrightarrow f(\gamma) \in \mathrm{D}(f(\alpha);\varepsilon).$$

If f is continuous at every point in X then we say that it is *continuous on X*.

Example 4.5. Let $f(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_d x^d$ with $\gamma_k \in \mathbb{Q}_p$ be a polynomial function. Then as in real analysis, this function is continuous at every point. To see this, we can either use the old proof with $|\ |_p$ in place of $|\ |$, or the following p-adic version.

Let us show that f is continuous at α. Then

$$|f(x) - f(\alpha)|_p = |x-\alpha|_p \left| \sum_{n=1}^{d} \gamma_n (x^{n-1} + \alpha x^{n-2} + \cdots + \alpha^{n-1}) \right|_p .$$

If we also assume that $|x|_p < |\alpha|_p$, then

$$\begin{aligned} |f(x) - f(\alpha)|_p &\leqslant |x-\alpha|_p \max\{|\alpha^{n-1}\gamma_n|_p : 1 \leqslant n \leqslant d\} \\ &\leqslant |x-\alpha|_p B, \end{aligned}$$

say, for some suitably large $B \in \mathbb{R}$ (in fact it needs to be at least as big as all the numbers $|\alpha^{n-1}\gamma_n|_p$ with $1 \leqslant n \leqslant d$). But if $\varepsilon > 0$ (and without loss of generality, $\varepsilon < |\alpha|_p$) we can take $\delta = \varepsilon/B$. If $|x-\alpha|_p < \delta$, we now have

$$|f(x) - f(\alpha)|_p < \varepsilon.$$

Example 4.6. Let the power series $\sum \alpha_n x^n$ have radius of convergence $r > 0$. Then the function $f\colon \mathrm{D}(0;r) \longrightarrow \mathbb{Q}_p$ for which

$$f(x) = \sum_{n=1}^{\infty} \alpha_n x^n$$

is continuous by a similar proof to the last one.

It is also the case that sums and products of continuous functions are continuous as in real analysis.

What makes p-adic analysis radically different from real analysis is the existence of non-trivial *locally constant functions* which we now discuss. First recall the following from real analysis.

Recollection 4.7. Let $f\colon (a,b) \longrightarrow \mathbb{R}$ be a continuous function. Suppose that for every $x \in (a,b)$ there is a $t > 0$ such that $(x-t, x+t) \subseteq (a,b)$ and f is constant on $(x-t, x+t)$, *i.e.*, f is *locally constant*. Then f is constant on (a,b).

We can think of (a,b) as a disc of radius $(b-a)/2$ and centred at $(a+b)/2$. This suggests the following definition in $\mathbb{Q}_p$.

Definition 4.8. Let $f\colon X \longrightarrow \mathbb{Q}_p$ be a function where $X \subseteq \mathbb{Q}_p$. Then f is *locally constant on* X if for every $\alpha \in X$, there is a real number $\delta_\alpha > 0$ such that f is constant on the open disc $\mathrm{D}_X(\alpha; \delta_\alpha)$.

This remark implies that there are no interesting examples of locally constant functions on open intervals in $\mathbb{R}$; however, that is false in $\mathbb{Q}_p$.

Example 4.9. Let $X = \mathbb{Z}_p$, the p-adic integers. From Theorem 2.28, we know that for $\alpha \in \mathbb{Z}_p$, there is a p-adic expansion

$$\alpha = \alpha_0 + \alpha_1 p + \cdots + \alpha_n p^n + \cdots,$$

where $\alpha_n \in \mathbb{Z}$ and $0 \leqslant \alpha_n \leqslant (p-1)$. Consider the functions

$$f_n\colon \mathbb{Z}_p \longrightarrow \mathbb{Z}_p; \quad f_n(\alpha) = \alpha_n,$$

which are defined for all $n \geqslant 0$. We claim these are locally constant. To see this, notice that f_n is unchanged if we replace α by any β with $|\beta - \alpha|_p < 1/p^n$; hence f_n is locally constant.

We can extend this example to functions $f_n\colon \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ for $n \in \mathbb{Z}$ since for any $\alpha \in \mathbb{Q}_p$ we have an expansion

$$\alpha = \alpha_{-r} p^{-r} + \cdots + \alpha_0 + \alpha_1 p + \cdots + \alpha_n p^n + \cdots$$

and we can set $f_n(\alpha) = \alpha_n$ in all cases; these are still locally constant functions on $\mathbb{Q}_p$.

One important fact about such functions is that they are continuous.

Proposition 4.10. *Let $f\colon X \longrightarrow \mathbb{Q}_p$ be locally constant on X. Then f is continuous on X.*

Proof. Given $\alpha \in X$ and $\varepsilon > 0$, we take $\delta = \delta_\alpha$ and then f is constant on $\mathrm{D}_X(\alpha; \delta_\alpha)$. □

This result is also true in $\mathbb{R}$.

Example 4.11. Let us consider the set $Y = \mathrm{D}(0;1) \subseteq \mathbb{Z}_p$. Then we define the *characteristic function of* Y by

$$\chi_Y\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p; \quad \chi_Y(\alpha) = \begin{cases} 1 & \text{if } \alpha \in Y, \\ 0 & \text{if } \alpha \notin Y. \end{cases}$$

This is clearly locally constant on $\mathbb{Z}_p$ since it is constant on each of the open discs $\mathrm{D}(k;1)$ with $0 \leqslant k \leqslant (p-1)$ and these exhaust the elements of $\mathbb{Z}_p$. This can be repeated for any such open ball $\mathrm{D}(\alpha;\delta)$ with $\delta > 0$.

Another example is provided by the *Teichmüller functions*. These will require some work to define. We will define a sequence of functions with the properties stated in the next result.

Proposition 4.12. *There is a unique sequence of locally constant, hence continuous, functions $\omega_n\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$, satisfying*

(T1) $$\omega_n(\alpha)^p = \omega_n(\alpha) \quad \text{for } n \geqslant 0,$$

(T2) $$\alpha = \sum_{n=0}^{\infty} \omega_n(\alpha) p^n.$$

PROOF. First we define the *Teichmüller character* $\omega\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ which will be equal to ω_0. Let $\alpha \in \mathbb{Z}_p$; then the sequence (α^{p^n}) is a sequence of p-adic integers and we claim it has a limit. To see this, we will show that it is Cauchy and use the fact that $\mathbb{Q}_p$ is complete.

By Theorem 2.28, α has a unique p-adic expansion

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$$

with $\alpha_k \in \mathbb{Z}$ and $0 \leqslant \alpha_k \leqslant (p-1)$. In particular,

$$|\alpha - \alpha_0|_p < 1.$$

By Fermat's Little Theorem 1.26, in $\mathbb{Z}$ we have

$$\alpha_0^p \underset{p}{\equiv} \alpha_0,$$

hence $|\alpha_0^p - \alpha_0|_p < 1$. Making use of the fact that $\left|\alpha^k \alpha_0^{p-1-k}\right|_p \leqslant 1$ together with the triangle inequality, we obtain

$$\begin{aligned} |\alpha^p - \alpha_0^p|_p &= \left|(\alpha - \alpha_0)(\alpha^{p-1} + \alpha^{p-2}\alpha_0 + \cdots + \alpha_0^{p-1})\right|_p \\ &\leqslant |\alpha - \alpha_0|_p < 1. \end{aligned}$$

Thus we have

$$\begin{aligned} |\alpha^p - \alpha|_p &= |(\alpha^p - \alpha_0^p) + (\alpha_0^p - \alpha_0) + (\alpha_0 - \alpha)|_p \\ &\leqslant \max\{|\alpha^p - \alpha_0^p|_p, |\alpha_0^p - \alpha_0|_p, |\alpha_0 - \alpha|_p\} \\ &< 1. \end{aligned}$$

We will show by induction upon $n \geqslant 0$ that

$$\left|\alpha^{p^{n+1}} - \alpha^{p^n}\right|_p < \frac{1}{p^n}. \tag{4.1}$$

Clearly this is true for $n = 0$ by the above. Suppose true for n. Then

$$\alpha^{p^{n+1}} = \alpha^{p^n} + \beta,$$

where $|\beta|_p < 1/p^n$. Raising to the power p gives

$$\begin{aligned} \alpha^{p^{n+2}} &= (\alpha^{p^n} + \beta)^p \\ &= \alpha^{p^{n+1}} + p\alpha^{p^n(p-1)}\beta + \cdots + \binom{p}{k}\alpha^{p^n k}\beta^{p-k} + \cdots + \beta^p, \end{aligned}$$

where all of the terms except the first in the last line have $|\ |_p$ less than $1/p^{n+1}$. Applying the p-adic norm gives the desired result for $n+1$.

Now consider α^{p^n}. Then

$$\begin{aligned} \alpha^{p^n} &= (\alpha^{p^n} - \alpha^{p^{n-1}}) + (\alpha^{p^{n-1}} - \alpha^{p^{n-2}}) + \cdots + (\alpha^p - \alpha) + \alpha \\ &= \alpha + \sum_{k=0}^{n-1} (\alpha^{p^{k+1}} - \alpha^{p^k}). \end{aligned}$$

Clearly the difference $\alpha^{p^{n+1}} - \alpha^{p^n}$ is a null sequence and by Proposition 3.1 the sequence (α^{p^n}) is Cauchy as desired.

Now we define the *Teichmüller function* or *character*,

$$\omega\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p; \quad \omega(\alpha) = \lim_{n\to\infty}^{(p)} \alpha^{p^n}.$$

This function satisfies

$$|\alpha - \omega(\alpha)|_p < 1, \quad \omega(\alpha)^p = \omega(\alpha).$$

The inequality follows from Equation (4.1), while the equation follows from the fact that

$$\begin{aligned}\left(\lim_{n\to\infty}^{(p)} \alpha^{p^n}\right)^p &= \lim_{n\to\infty}^{(p)} (\alpha^{p^n})^p \\ &= \lim_{n\to\infty}^{(p)} (\alpha^{p^{n+1}}).\end{aligned}$$

We now set $\omega_0(\alpha) = \omega(\alpha)$ and define the ω_n by recursion using

$$\omega_{n+1}(\alpha) = \omega\left(\frac{\alpha - (\omega_0(\alpha) + \omega_1(\alpha)p + \cdots + \omega_n(\alpha)p^n)}{p^{n+1}}\right). \qquad \square$$

For $\alpha \in \mathbb{Z}_p$, the expansion

$$\alpha = \omega_0(\alpha) + \omega_1(\alpha)p + \cdots + \omega_n p^n + \cdots$$

is called the *Teichmüller expansion* of α and the $\omega_n(\alpha)$ are called the *Teichmüller digits* of α. This expansion is often used in place of the other p-adic expansion. One reason is that the function ω is multiplicative. We sum up the properties of ω in the next proposition.

PROPOSITION 4.13. *The function $\omega\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ is locally constant and satisfies the conditions*

$$\begin{aligned}&\omega(\alpha\beta) = \omega(\alpha)\omega(\beta), \\ &|\omega(\alpha+\beta) - \omega(\alpha) - \omega(\beta)|_p < 1.\end{aligned}$$

Moreover, the image of this function consists of exactly p elements of $\mathbb{Z}_p$, namely the p distinct roots of the polynomial $X^p - X$.

PROOF. The multiplicative part follows from the definition, while the additive result is an easy exercise with the ultrametric inequality. For the image of ω, we remark that the distinct numbers in the list $0, 1, 2, \ldots, p-1$ satisfy

$$|r - s|_p = 1.$$

If $r \neq s$, then

$$|\omega(r) - \omega(s)|_p = 1.$$

Hence, the image of the function ω has at least p distinct elements, all of which are roots in $\mathbb{Q}_p$ of $X^p - X$. As $\mathbb{Q}_p$ is a field, there are not more than p of these roots. So this polynomial factors as

$$X^p - X = X(X - \omega(1))(X - \omega(2)) \cdots (X - \omega(p-1))$$

and the p roots are the only elements in the image of ω. $\square$

EXAMPLE 4.14. For the prime $p = 2$, the roots of $X^2 - X$ are 0,1. In fact, the Teichmüller expansion is just the p-adic expansion discussed in Chapter 2.

EXAMPLE 4.15. For the prime $p = 3$, the roots of $X^3 - X$ are $0, \pm 1$. So we replace the use of 2 in the p-adic expansion by that of -1. Let us consider an example.

Setting $\alpha = 1/5$, we have $5 \underset{3}{\equiv} -1$ and so $\omega(5) = -1$ since

$$|5 - (-1)|_3 < 1.$$

Hence $\omega(1/5) = -1$ too, so $\omega_0(1/5) = -1$. Now consider

$$\frac{(1/5) - (-1)}{3} = \frac{6}{15} = \frac{2}{5},$$

and notice that $2 \underset{3}{\equiv} -1$, hence $\omega_1(1/5) = \omega(2/5) = 1$. Next consider

$$\frac{(2/5) - 1}{3} = \frac{-3}{15} = \frac{-1}{5},$$

giving $\omega_2(1/5) = \omega(-1/5) = 1$. Thus

$$\frac{1}{5} = (-1) + 1 \cdot 3 + 1 \cdot 3^2 + \cdots$$

where we have stopped at the term in 3^2 and ignored terms of 3-norm less than $1/3^2$.

EXAMPLE 4.16. If $p = 5$, there are three roots of $X^5 - X$ in $\mathbb{Z}$, namely $0, \pm 1$ and two more in $\mathbb{Z}_5$ but not in $\mathbb{Z}$. On the other hand, $(\mathbb{Z}/5)^\times = \langle \overline{2} \rangle$ as a group. Thus, we can take $\omega(2) = \gamma$ say, to be generator of the group of $(5 - 1) = 4$-th roots of 1 in $\mathbb{Z}_5$. So the roots of $X^5 - X$ in $\mathbb{Z}_5$ are

$$\omega(0) = 0,\ \omega(1) = 1,\ \omega(2) = \gamma,\ \omega(3) = \gamma^3,\ \omega(4) = \gamma^2.$$

Suppose that we wish to find the Teichmüller expansion of 3 up to the term in 5^2. Then we first need to find an integer which approximates γ to within a 5-norm of less than $1/5^2$. So let us try to find an element of $\mathbb{Z}/5^3$ which agrees with 2 modulo 5 and is a root of $X^4 \underset{5^3}{\equiv} 1$. We can use Hensel's Lemma to do this.

We have a root of $X^4 - 1$ modulo 5, namely 2. Set $f(X) = X^4 - 1$ and note that $f'(X) = 4X^3$. Now $f'(2) \underset{5}{\equiv} 4 \cdot 8 \underset{5}{\equiv} 2$ and we can take $u = 3$. Then $x = 2 - 3f(2) = -43 \underset{25}{\equiv} 7$ is a root of $f(X)$ modulo 25. Repeating this we obtain

$$7 - 3f(7) = 7 - 75 = -68 \underset{125}{\equiv} 57$$

which is a root of the polynomial modulo 125. We now proceed as before.

This method always works and relies upon Hensel's Lemma (see Chapter 1 and Problem Set 3).

THEOREM 4.17 (Hensel's Lemma). *Let $f(X) \in \mathbb{Z}_p[X]$ be a polynomial and let $\alpha \in \mathbb{Z}_p$ be a p-adic number for which*

$$|f(\alpha)|_p < 1, \quad \left|f'(\alpha)\right|_p = 1.$$

Define a sequence in $\mathbb{Q}_p$ by setting $\alpha_0 = \alpha$ and in general

$$\alpha_{n+1} = \alpha_n - (f'(\alpha))^{-1} f(\alpha_n).$$

Then each α_n is in $\mathbb{Z}_p$ and moreover

$$|f(\alpha_n)|_p < \frac{1}{p^n}.$$

Hence the sequence (α_n) is Cauchy with respect to $|\ |_p$ and

$$f(\lim_{n\to\infty}{}^{(p)}\alpha_n) = 0.$$

The proof is left to the reader who should look at Hensel's Lemma in Chapter 1 and Problem Set 3.

EXAMPLE 4.18. Let $f(X) = X^{p-1} - 1$. Then from our earlier discussion of ω we know that there are $(p-1)$ roots of 1 in $\mathbb{Z}_p$. Suppose that we have an α such that $|\alpha - \gamma|_p < 1$ for one of these roots γ. By an easy norm calculation, $|f(\alpha)|_p < 1$. So we can take the sequence defined in Theorem 4.17 which converges to a root of $f(X)$, *i.e.*, a $(p-1)$-st root of 1 in $\mathbb{Z}_p$.

We now prove another general fact about locally constant functions on $\mathbb{Z}_p$.

THEOREM 4.19. *Let $f\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ be locally constant. Then the image of f,*

$$\operatorname{im} f = f(\mathbb{Z}_p) = \{f(\alpha) : \alpha \in \mathbb{Z}_p\},$$

is a finite set.

PROOF. For each $\alpha \in \mathbb{Z}_p$ there is a real number $\delta_\alpha > 0$ for which f is constant on the open disc $\mathrm{D}(\alpha; \delta_\alpha)$. We can assume without loss of generality that

$$\delta_\alpha = \frac{1}{p^{d_\alpha}}$$

with $d_\alpha \geqslant 0$ an integer. Now for each α there is an integer n_α such that

$$|\alpha - n_\alpha|_p < \frac{1}{p^{d_\alpha}}$$

and so $f(n_\alpha) = f(\alpha)$. By Proposition 4.2 we also have

$$\mathrm{D}\left(\alpha; 1/p^{d_\alpha}\right) = \mathrm{D}\left(n_\alpha; 1/p^{d_\alpha}\right).$$

In fact we can assume that n_α satisfies

$$0 \leqslant n_\alpha \leqslant p^{d_\alpha+1} - 1,$$

since adding a multiple of $p^{d_\alpha+1}$ to n_α does not change the open disc $\mathrm{D}\left(n_\alpha; 1/p^{d_\alpha}\right)$.

Now

$$\mathbb{Z}_p = \bigcup_{k=0}^{\infty} \mathrm{D}\left(k; 1/p^{d_k}\right)$$

and f is constant on each of these open discs. But also

$$\mathbb{Z}_p = \bigcup_{k=0}^{p^{d_0+1}-1} \mathrm{D}\left(k; 1/p^{d_0}\right).$$

Now take

$$\overline{d} = \max\{d_k : 0 \leqslant k \leqslant p^{d_0+1} - 1\}$$

and observe that for each k in the range $0 \leqslant k \leqslant p^{d_0+1}-1$, f is locally constant on the disc $\mathrm{D}\left(k; 1/p^{\overline{d}}\right)$. Hence

$$\mathbb{Z}_p = \bigcup_{k=0}^{p^{\overline{d}}-1} \mathrm{D}\left(k; 1/p^{\overline{d}}\right),$$

where f is constant on each of these discs. Since there is only a finite number of these discs, the image of f is the finite set

$$f(\mathbb{Z}_p) = \{f(k) : 0 \leqslant k \leqslant p^{\overline{d}} - 1\}. \qquad \square$$

A similar argument establishes a closely related result.

THEOREM 4.20 (The Compactness of $\mathbb{Z}_p$). *Let $A \subseteq \mathbb{Z}_p$ and for each $\alpha \in A$ let $\delta_\alpha > 0$. If*

$$\mathbb{Z}_p = \bigcup_{\alpha \in A} D\left(\alpha; 1/p^{\delta_\alpha}\right),$$

then there is finite subset $A' \subseteq A$ such that

$$\mathbb{Z}_p = \bigcup_{\alpha \in A'} D\left(\alpha; 1/p^{\delta_\alpha}\right).$$

A similar result holds for each of the closed discs $\overline{D(\beta; t)}$ where $t \geqslant 0$ is a real number.

We leave the proof as an exercise. In fact these two results are *equivalent* in the sense that each one implies the other (this is left as an exercise for the reader).

The next result is a direct consequence.

THEOREM 4.21 (The Sequential Compactness of $\mathbb{Z}_p$). *Let (α_n) be a sequence in $\mathbb{Z}_p$. Then there is a convergent subsequence of (α_n),* i.e., *a sequence (β_n) where $\beta_n = \alpha_{s(n)}$ with $s : \mathbb{N} \longrightarrow \mathbb{N}$ a strictly increasing sequence and which converges. A similar result holds for each of the closed discs $\overline{D(\beta; t)}$ where $t \geqslant 0$ is a real number.*

PROOF. We have

$$\mathbb{Z}_p = \bigcup_{k=1}^{p} \mathrm{D}(k; 1).$$

Hence, for one of the numbers $1 \leqslant k \leqslant p$, say a_1, the disc $\mathrm{D}(a_1; 1)$ has $\alpha_n \in \mathrm{D}(a_1; 1)$ for infinitely many values of n. Then

$$\mathrm{D}(a_1; 1) = \bigcup_{k=1}^{p^2} \mathrm{D}(k; 1/p)$$

and again for one of the numbers $1 \leqslant k \leqslant p^2$, say a_2, we have $\alpha_n \in \mathrm{D}(a_2; 1/p)$ for infinitely many values of n. Continuing in this way we have a sequence of natural numbers a_n for which $\mathrm{D}\left(a_n; 1/p^{n-1}\right)$ contains α_m for infinitely many values of m. Moreover, for each n,

$$\mathrm{D}\left(a_n; 1/p^{n-1}\right) \subseteq \mathrm{D}\left(a_n; 1/p^n\right).$$

Now for each $n \geqslant 1$, choose $s(n)$ so that $\alpha_{s(n)} \in \mathrm{D}\left(a_n; 1/p^{n-1}\right)$. We can even assume that $s(n) < s(n+1)$ for all n. Hence we have a subsequence (β_n) with $\beta_n = \alpha_{s(n)}$ which we must still show has limit. But notice that

$$|\beta_{n+1} - \beta_n|_p < \frac{1}{p^n},$$

since both of these are in $\mathrm{D}\left(a_{n+1}; 1/p^n\right)$. Hence the sequence (β_n) is null and so it has a limit in $\mathbb{Z}_p$. □

Recall the notion of uniform continuity:

Definition 4.22. Let $f\colon X \longrightarrow \mathbb{Q}_p$ be a function. Then f is *uniformly continuous on* X if

$$\forall \varepsilon > 0 \exists \delta > 0 \text{ such that } \forall \alpha, \beta \in X, \text{ with } |\alpha - \beta|_p < \delta \text{ then } |f(\alpha) - f(\beta)|_p < \varepsilon.$$

Clearly if f is uniformly continuous on X then it is continuous on X. In real or complex analysis, a continuous function on a compact domain is uniformly continuous. This is true p-adically too.

Theorem 4.23. *Let $t > 0$, $\alpha \in \mathbb{Q}_p$ and $f\colon \overline{D(\alpha; t)} \longrightarrow \mathbb{Q}_p$ be a continuous function. Then f is uniformly continuous.*

The proof is a direct translation of that in real or complex analysis.

Similarly, we also have the notion of boundedness.

Definition 4.24. Let $f\colon X \longrightarrow \mathbb{Q}_p$ be a function. Then f is *bounded on* X if

$$\exists b \in \mathbb{R} \text{ such that } \forall x \in X, \ |f(x)|_p \leqslant b.$$

Again we are familiar with the fact that a continuous function defined on a compact set is bounded.

Theorem 4.25. *Let $f\colon \overline{D(\alpha; t)} \longrightarrow \mathbb{Q}_p$ be a continuous function. Then f is bounded,* i.e.*, there is a $b \in \mathbb{R}$ such that for all $\alpha \in \overline{D(\alpha; t)}$, $|f(\alpha)|_p \leqslant b$.*

Again the proof is a modified version of that in classical analysis.

Now let us consider the case of a continuous function $f\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$. By Theorem 4.20, $\mathbb{Z}_p$ is compact, so by Theorem 4.25 f is bounded. Then the set

$$B_f = \{b \in \mathbb{R} : \forall \alpha \in \mathbb{Z}_p, \quad |f(\alpha)|_p \leqslant b\}$$

is non-empty. Clearly $B_f \subseteq \mathbb{R}^+$, the set of non-negative real numbers. As B_f is bounded below by 0, this set has an *infimum*, $\inf B_f \geqslant 0$. An easy argument now shows that

$$\sup\{|f(\alpha)|_p : \alpha \in \mathbb{Z}_p\} = \inf B_f.$$

We will write b_f for this common value.

Theorem 4.26. *Let $f\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ be a continuous function. Then there is an $\alpha_0 \in \mathbb{Z}_p$ such that $b_f = |f(\alpha_0)|_p$.*

PROOF. For all $\alpha \in \mathbb{Z}_p$ we have $|f(\alpha)|_p \leqslant b_f$. By definition of supremum, we know that for any $\varepsilon > 0$, there is a $\alpha \in \mathbb{Z}_p$ such that

$$|f(\alpha)|_p > b_f - \varepsilon.$$

For each n, take an $\alpha_n \in \mathbb{Z}_p$ such that

$$|f(\alpha_n)|_p > b_f - \frac{1}{n}$$

and consider the sequence (α_n) in $\mathbb{Z}_p$. By Theorem 4.21, there is a convergent subsequence $(\beta_n) = (\alpha_{s(n)})$ of (α_n), where we can assume that $s(n) < s(n+1)$. Let $\alpha' = \lim\limits_{n\to\infty}^{(p)} \alpha_{s(n)}$. Then for each n we have

$$b_f \geqslant \left|f(\alpha_{s(n)})\right|_p > b_f - \frac{1}{s(n)}$$

and so $\left|f(\alpha_{s(n)})\right|_p \to b_f$ as $n \to \infty$. Since

$$\lim_{n\to\infty} \left| \left|f(\alpha')\right|_p - \left|f(\alpha_{s(n)})\right|_p \right| \leqslant \lim_{n\to\infty} \left|f(\alpha' - \alpha_{s(n)})\right|_p = 0,$$

by a result used in the proof of Theorem 2.17), we have $b_f = |f(\alpha')|_p$. □

DEFINITION 4.27. Let $f\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ be continuous. The *supremum seminorm* of f is

$$\|f\|_p = b_f.$$

Consider the set of all continuous functions $\mathbb{Z}_p \longrightarrow \mathbb{Q}_p$,

$$C(\mathbb{Z}_p) = \{f\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p : f \text{ continuous}\}.$$

This is a ring with the operations of pointwise addition and multiplication, and with the constant functions $0, 1$ as zero and unity. The function $\| \|_p\colon C(\mathbb{Z}_p) \longrightarrow \mathbb{R}^+$ is in fact a non-Archimedean norm on $C(\mathbb{Z}_p)$.

THEOREM 4.28. *$C(\mathbb{Z}_p)$ is a ring with non-Archimedean seminorm $\| \|_p$. Moreover, $C(\mathbb{Z}_p)$ is complete with respect to this seminorm.*

We do not give the proof, but leave at least the first part as an exercise for the reader.

Now recall the notion of the *Fourier expansion* of a continuous function $f\colon [a, b] \longrightarrow \mathbb{R}$; this is a convergent series of the form

$$a_0 + \sum_{n=1}^{\infty} \left(a_n \cos \frac{2pix}{n} + \sin \frac{2\pi x}{n} \right)$$

which converges uniformly to $f(x)$. In p-adic analysis there is an analogous expansion of a continuous function using the binomial coefficient functions

$$C_n(x) = \binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}.$$

We recall that these are continuous functions $C_n\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ which actually map $\mathbb{Z}_p$ into itself (see Problem Set 4).

THEOREM 4.29. *Let $f \in C(\mathbb{Z}_p)$. Then there is a unique null sequence (α_n) in $\mathbb{Q}_p$ such that the series*

$$\sum_{n=0}^{\infty} \alpha_n C_n(x)$$

converges to $f(x)$ for every $x \in \mathbb{Z}_p$. Moreover, this convergence is uniform in the sense that the sequence of functions

$$\sum_{m=0}^{n} \alpha_m C_m \in C(\mathbb{Z}_p)$$

is a Cauchy sequence converging to f with respect to $\| \ \|_p$.

The expansion in this result is called the *Mahler expansion of f* and the coefficients α_n are the *Mahler coefficients* of f. We need to understand how to determine these coefficients.

Consider the following sequence of functions $f^{[n]} \colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$:

$$\begin{aligned} f^{[0]}(x) &= f(x) \\ f^{[1]}(x) &= f^{[0]}(x+1) - f^{[0]}(x) \\ f^{[2]}(x) &= f^{[1]}(x+1) - f^{[1]}(x) \\ &\vdots \\ f^{[n+1]}(x) &= f^{[n]}(x+1) - f^{[n]}(x) \\ &\vdots \end{aligned}$$

$f^{[n]}$ is called the n-th *difference function* of f.

PROPOSITION 4.30. *The Mahler coefficients are given by*

$$\alpha_n = f^{[n]}(0) \quad (n \geqslant 0).$$

PROOF. (Sketch) Consider

$$f(0) = \sum \alpha_n C_n(0) = \alpha_0.$$

Now by *Pascal's Triangle*,

$$C_n(x+1) - C_n(x) = C_{n-1}(x).$$

Then

$$\begin{aligned} f^{[1]}(x) &= f^{[0]}(x+1) - f^{[0]}(x) \\ &= \sum_{n=0}^{\infty} \alpha_{n+1} C_n(x) \end{aligned}$$

and repeating this we obtain

$$\begin{aligned} f^{[m+1]}(x) &= f^{[m]}(x+1) - f^{[m]}(x) \\ &= \sum_{n=0}^{\infty} \alpha_{n+m} C_n(x). \end{aligned}$$

Thus we have the desired formula

$$f^{[m]}(0) = \alpha_m. \qquad \square$$

The main part of the proof of Theorem 4.29 is concerned with proving that $\alpha_n \to 0$ and we will not give it here.

The functions C_n have the property that

$$\|C_n\|_p = 1. \tag{4.2}$$

To see this, note that if $\alpha \in \mathbb{Z}_p$, we already have $|C_n(\alpha)|_p \leqslant 1$. Taking $\alpha = n$, we get $C_n(n) = 1$, and the result follows. Of course this means that the series $\sum \alpha_n C_n(\alpha)$ converges for all $\alpha \in \mathbb{Z}_p$ if and only if $\alpha_n \to 0$.

EXAMPLE 4.31. Consider the case of $p = 3$ and the function $f(x) = x^3$. Then

$$\begin{aligned}
f^{[0]}(x) &= x^3, & f^{[0]}(0) &= 0,\\
f^{[1]}(x) &= 3x^2 + 3x + 1, & f^{[1]}(0) &= 1,\\
f^{[2]}(x) &= 6x + 3, & f^{[2]}(0) &= 3,\\
f^{[3]}(x) &= 6, & f^{[3]}(0) &= 6,\\
f^{[4]}(x) &= 0, & f^{[4]}(0) &= 0,
\end{aligned}$$

and for $n > 3$,

$$f^{[n]}(x) = 0, \qquad f^{[n]}(0) = 0.$$

So we have

$$x^3 = C_1(x) + 3C_2(x) + 6C_3(x).$$

In fact, for any polynomial function of degree d, the Mahler expansion is trivial beyond the term in C_d.

The following formula for these a_n can be proved by induction on n.

$$f^{[n]}(0) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(n-k). \tag{4.3}$$

EXAMPLE 4.32. Take $p = 2$ and the continuous function $f\colon \mathbb{Z}_2 \longrightarrow \mathbb{Q}_2$ given by

$$f(n) = (-1)^n \quad \text{if } n \in \mathbb{Z}.$$

Then

$$f^{[0]}(0) = 1, \quad f^{[1]}(0) = 0, \quad f^{[2]}(0) = -1,$$

and in general

$$f^{[n]}(0) = (-1)^n \sum_{k=0}^{n} \binom{n}{k} = (-2)^n.$$

Therefore

$$f(x) = \sum_{n=0}^{\infty} (-2)^n C_n(x).$$

Of course, this is just the binomial series for $(1-2)^x$ in $\mathbb{Q}_2$.

This ends our discussion of elementary p-adic analysis. We have not touched many important topics such as differentiability, integration and so on. For these I suggest you look at Koblitz [**4**]. I particularly recommend his discussion of the Γ-function and integration and the ζ-function.

The world of p-adic analysis is in many ways very similar to that of classical real analysis, but it is also startlingly different at times. I hope you have enjoyed this sampler. We will now move on to consider something more like the complex numbers in the p-adic context.

CHAPTER 5

p-adic algebraic number theory

In this section we will discuss a complete normed field $\mathbb{C}_p$ which contains $\mathbb{Q}_p$ as a subfield and has the property that every polynomial $f(X) \in \mathbb{C}_p[X]$ has a root in $\mathbb{C}_p$; furthermore the norm $|\ |_p$ restricts to the usual norm on $\mathbb{Q}_p$ and is non-Archimedean. In fact, $\mathbb{C}_p$ is the smallest such normed field, in the sense that any other one with these properties contains $\mathbb{C}_p$ as a subfield. We begin by considering roots of polynomials over $\mathbb{Q}_p$.

Let $f(X) \in \mathbb{Q}_p[X]$. Then in general f need not have any roots in $\mathbb{Q}_p$.

EXAMPLE 5.1. For a prime p, consider the polynomial $X^2 - p$. If $\alpha \in \mathbb{Q}_p$ were a root then we would have $\alpha^2 = p$ and so $|\alpha|_p^{\,2} = 1/p$. But we know that the norm of a p-adic number has to have the form $1/p^k$ with $k \in \mathbb{Z}$, so since $|\alpha|_p = p^{-1/2}$ this would give a contradiction.

We will not prove the next result, the interested reader should consult [**4**].

THEOREM 5.2. *There exists a field $\mathbb{Q}_p^{\mathrm{alg}}$ containing $\mathbb{Q}_p$ as a subfield and having the following properties:*

(a) *every $\alpha \in \mathbb{Q}_p^{\mathrm{alg}}$ is algebraic over $\mathbb{Q}_p$;*
(b) *every polynomial $f(X) \in \mathbb{Q}_p^{\mathrm{alg}}[X]$ has a root in $\mathbb{Q}_p^{\mathrm{alg}}$.*

Moreover, the norm $|\ |_p$ on $\mathbb{Q}_p$ extends to a unique non-Archimedean norm N on $\mathbb{Q}_p^{\mathrm{alg}}$ satisfying

$$N(\alpha) = |\alpha|_p$$

whenever $\alpha \in \mathbb{Q}_p$. This extension is given by

$$N(\alpha) = \left|\min_{\mathbb{Q}_p,\alpha}(0)\right|_p^{\,1/d},$$

where $d = \deg_{\mathbb{Q}_p}(\alpha) = \deg \min_{\mathbb{Q}_p,\alpha}(X)$ is the degree of the minimal polynomial of α over $\mathbb{Q}_p$.

The *minimal polynomial* $\min_{\mathbb{Q}_p,\alpha}(X)$ of α over $\mathbb{Q}_p$ is the monic polynomial in $\mathbb{Q}_p[X]$ of smallest positive degree having α as a root and is always irreducible. We will denote by $|\ |_p$ the norm on $\mathbb{Q}_p^{\mathrm{alg}}$ given in Theorem 5.2, *i.e.*,

$$|\alpha|_p = \left|\min_{\mathbb{Q}_p,\alpha}(0)\right|_p^{\,1/d}.$$

Let us look at some elements of $\mathbb{Q}_p^{\mathrm{alg}}$. Many examples can be found using the next two results.

THEOREM 5.3. *Let $r = a/b$ be a positive rational number where a, b are coprime. Then the polynomial $X^b - p^a \in \mathbb{Q}_p[X]$ is irreducible over $\mathbb{Q}_p$ and each of its roots $\alpha \in \mathbb{Q}_p^{\mathrm{alg}}$ has norm $|\alpha|_p = p^{-a/b}$.*

PROOF. This is a special case of [**5**, VIII theorem 16]. □

COROLLARY 5.4. *If $r = a/b$ is not an integer, then none of the roots of $X^b - p^a$ in $\mathbb{Q}_p^{\text{alg}}$ are in $\mathbb{Q}_p$.*

PROOF. We have $|\alpha|_p = p^{-a/b}$ which is not an integral power of p. But from Chapter 2 we know that all elements of $\mathbb{Q}_p$ have norms which are integral powers of p, hence $\alpha \notin \mathbb{Q}_p$. □

The *Eisenstein test* of the next result provides an important criterion for finding irreducible polynomials over $\mathbb{Q}_p$.

THEOREM 5.5 (The Eisenstein test). *Suppose that the polynomial*

$$f(X) = X^d + \alpha_{d-1}X^{d-1} + \cdots + \alpha_1 X + \alpha_0 \in \mathbb{Z}_p[X]$$

satisfies the conditions

- $|\alpha_k|_p < 1$ *for each k in the range $0 \leqslant k \leqslant d-1$,*
- $|\alpha_0|_p = 1/p$.

Then $f(X)$ is irreducible over $\mathbb{Q}_p$.

The proof can be found in many books or courses on basic ring theory.

EXAMPLE 5.6. Consider the polynomial

$$f_1(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Notice that

$$X^p - 1 = (X-1)f_1(X)$$

and so $f_1(X)$ is the polynomial whose roots are all the primitive p-th roots of 1. Now consider the polynomial $g_1(X) = f_1(X+1)$. Then

$$\begin{aligned} Xg_1(X) &= (X+1)^p - 1 \\ &= X^p + \sum_{k=1}^{p-1} \binom{p}{k} X^k \end{aligned}$$

and so

$$g_1(X) = X^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} X^{k-1}.$$

Each of the binomial coefficients $\binom{p}{k}$ for $1 \leqslant k \leqslant p-1$ is divisible by p; also $\binom{p}{1} = p$, hence it is not divisible by p^2. By the Eisenstein test, $g_1(X)$ is irreducible over $\mathbb{Q}_p$ and an easy argument also shows that $f_1(X)$ is irreducible. Thus the primitive roots of 1 in $\mathbb{Q}_p^{\text{alg}}$ are roots of the irreducible polynomial $f_1(X)$ and have degree $(p-1)$ over $\mathbb{Q}_p$. If ζ_p is a root of $f_1(X)$, then $|\zeta_p|_p = 1$. The remaining roots are of the form ζ_p^r with $1 \leqslant r \leqslant p-1$.

The roots of $g_1(X)$ have the form $\zeta_p^r - 1$ for $1 \leqslant r \leqslant p-1$ and $g_1(0) = p$, so

$$\left|\zeta_p^r - 1\right|_p = p^{-1/(p-1)}.$$

This example can be generalised as follows.

THEOREM 5.7. *Let $d \geqslant 1$. Then the polynomial*

$$f_d(X) = f_1(X^{p^{d-1}})$$

is irreducible over $\mathbb{Q}_p$ and its roots are the primitive p^d-th roots of 1 in $\mathbb{Q}_p^{\mathrm{alg}}$. If ζ_{p^d} is such a primitive root, any other has the form $\zeta_{p^d}^k$ where $1 \leqslant k \leqslant p^d - 1$ and k is not divisible by p. Moreover, we have

$$\left|\zeta_{p^d}\right|_p = 1,$$
$$\left|\zeta_{p^d} - 1\right|_p = p^{-(p-1)p^{d-1}}.$$

PROOF. This is proved by applying the Eisenstein test to the polynomial

$$g_d(X) = f_d(X + 1),$$

which satisfies the conditions required and has $g_d(0) = p$. □

COROLLARY 5.8. *If p is an odd prime, then 1 is the only p-th power root of 1 in $\mathbb{Q}_p$.*
If $p = 2$, the only square roots of 1 in $\mathbb{Q}_2$ are ± 1.

The proof is immediate.

What about other roots of 1? We already know that there all the $(p-1)$-st roots of 1 are in $\mathbb{Q}_p$; let us consider the d-th roots of 1 for any $d > 1$ not divisible by p. We begin by considering the case where d has the form $d = p^r - 1$.

PROPOSITION 5.9. *For each $r \geqslant 1$, a primitive $(p^r - 1)$-st root of 1, ζ say, has degree r over $\mathbb{Q}_p$ and has minimal polynomial*

$$\min_{\mathbb{Q}_p,\zeta}(X) = \prod_{0 \leqslant t \leqslant r-1} (X - \zeta^{p^t}).$$

Moreover, $|\zeta|_p = |\zeta - 1|_p = 1$.

The proof is omitted.

Now suppose that d is any natural number not divisible by p and ξ is any d-th root of 1. Then for some m we have

$$p^m \underset{d}{\equiv} 1;$$

we denote the smallest such m greater than 0 by m_d. Then for any primitive $(p^{m_d} - 1)$-th root of 1, $\zeta_{p^{m_d}-1}$ say, we can take

$$\xi = \zeta_{p^{m_d}-1}^{t(p^{m_d}-1)/m_d},$$

where t is an integer coprime to $(p^{m_d} - 1)/m_d$. This uses the fact that the group of roots of $X^n - 1$ in $\mathbb{Q}_p^{\mathrm{alg}}$ is always cyclic by a result from the basic theory of fields. From this it is possible to deduce

PROPOSITION 5.10. *Let $d > 0$ be a natural number not divisible by p. Then any primitive d-th root of 1, ξ, has degree over $\mathbb{Q}_p$ dividing m_d. Furthermore,*

$$|\xi|_p = 1, \quad |\xi - 1|_p = 1.$$

COROLLARY 5.11. *$\xi \in \mathbb{Q}_p$ if and only if $m_d = 1$.*

The proofs can be found in [**4**]. A complete statement is contained in

THEOREM 5.12. *Let $\xi \in \mathbb{Q}_p^{\text{alg}}$ be a primitive d-th root of 1. Let $d = d_0 p^t$ where d_0 is not divisible by p. Then $\xi \in \mathbb{Q}_p$ if and only if one of the following conditions holds:*

- *p is odd, $t = 0$ and $m_d = 1$,*
- *$p = 2$ and $d = 2$.*

DEFINITION 5.13. Let $\alpha \in \mathbb{Q}_p^{\text{alg}}$. Then α is *ramified* if $|\alpha|_p$ is not an integral power of p, otherwise it is *unramified*. Let $e(\alpha)$ be the smallest positive natural number such that $\alpha^{e(\alpha)}$ is unramified; then $e(\alpha)$ is called the *ramification degree* of α.

EXAMPLE 5.14. Let π be a square root of p. Earlier we saw that $|\pi|_p = p^{-1/2}$, hence π is ramified. In fact we have $e(\alpha) = 2$.

This example generalises in an obvious way to roots of the polynomials $X^b - p^a$ of Theorem 5.3.

Now we can consider $\mathbb{Q}_p^{\text{alg}}$ together with the norm $|\ |_p$ in the light of Chapter 2. It is reasonable to ask if every Cauchy sequence in $\mathbb{Q}_p^{\text{alg}}$ has a limit with respect to $|\ |_p$.

PROPOSITION 5.15. *There are Cauchy sequences in $\mathbb{Q}_p^{\text{alg}}$ with respect to $|\ |_p$ which do not have limits. Hence, $\mathbb{Q}_p^{\text{alg}}$ is not complete with respect to the norm $|\ |_p$.*

For an example of such a Cauchy sequence, see [**4**].

We can form the completion of $\mathbb{Q}_p^{\text{alg}}$ and its associated norm which are denoted

$$\mathbb{C}_p = \widehat{\mathbb{Q}_p^{\text{alg}}}_{|\ |_p}, \quad |\ |_p.$$

PROPOSITION 5.16. *If $0 \neq \alpha \in \mathbb{C}_p$, then*

$$|\alpha|_p = \frac{1}{p^t},$$

where $t \in \mathbb{Q}$.

PROOF. We know this is true for $\alpha \in \mathbb{Q}_p^{\text{alg}}$. By results of Chapter 2, if

$$\alpha = \lim_{n\to\infty}{}^{(p)} \alpha_n$$

with $\alpha_n \in \mathbb{Q}_p^{\text{alg}}$, then for sufficiently large n,

$$|\alpha|_p = |\alpha_n|_p. \qquad \square$$

Next we can reasonably ask whether an analogue of the *Fundamental Theorem of Algebra* holds in $\mathbb{C}_p$.

THEOREM 5.17. *$\mathbb{C}_p$ is algebraically closed in the sense that every non-zero polynomial $f(X) \in \mathbb{C}_p[X]$ has a root in $\mathbb{C}_p$. By construction, $\mathbb{C}_p$ is complete with respect to the norm $|\ |_p$.*

Again, we refer to [**4**] for a proof. Of course we have now obtained a complete normed field containing $\mathbb{Q}_p$ which is algebraically closed and this is the p-adic analogue of the complex numbers. It is helpful to compare the chains of fields

$$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}, \quad \mathbb{Q} \subseteq \mathbb{Q}_p \subseteq \mathbb{Q}_p^{\text{alg}} \subseteq \mathbb{C}_p,$$

which are the sequences of fields we need to construct in order to reach the fields $\mathbb{C}$ and $\mathbb{C}_p$ in the real and p-adic worlds. This field $\mathbb{C}_p$ is the home of p-adic analysis proper and plays an important rôle in Number Theory and increasingly in other parts of Mathematics. We will confine ourselves to a few simple observations on $\mathbb{C}_p$.

Consider a power series $\sum \alpha_n x^n$ where $\alpha_n \in \mathbb{C}_p$. Then we can define the radius of convergence exactly as in Chapter 3, using the formula

$$r = \frac{1}{\limsup |\alpha_n|_p^{\,1/n}}.$$

PROPOSITION 5.18. *The series $\sum \alpha_n x^n$ converges if $|x|_p < r$ and diverges if $|x|_p > r$, where r is the radius of convergence. If for some x_0 with $|x_0|_p = r$ the series $\sum \alpha_n x_0^n$ converges (or diverges) then $\sum \alpha_n x^n$ converges (or diverges) for all x with $|x|_p = r$.*

The proof is the same as that in Chapter 3.

EXAMPLE 5.19. Consider the logarithmic series

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

discussed in Chapter 3. We showed that $r = 1$ for this example. Consider what happens when $x = \zeta_p$, a primitive root of 1 as above. Then $|\zeta_p - 1|_p = p^{1/(p-1)}$, so $\log_p(\zeta_p)$ is defined. Now by the multiplicative formula for this series,

$$\log_p((\zeta_p)^p) = p \log_p(\zeta_p),$$

and hence

$$p \log_p(\zeta_p) = \log_p(1) = 0.$$

Thus $\log_p(\zeta_p) = 0$. Similarly, for any primitive p^n-th root of 1, ζ_{p^n} say, we have that $\log_p(\zeta_{p^n})$ is defined and is 0.

EXAMPLE 5.20. Consider the exponential series

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

In Chapter 3, the radius of convergence was shown to be $p^{-1/(p-1)}$. Suppose $\alpha \in \mathbb{C}_p$ with $|\alpha|_p = p^{-1/(p-1)}$. Then

$$\left|\frac{\alpha^n}{n!}\right|_p = p^{\text{ord}_p\, n/(p-1)}.$$

By considering the terms of the form $\alpha^{p^n}/(p^n!)$, we obtain

$$\left|\frac{\alpha^{p^n}}{p^n!}\right|_p = p^{n/(p-1)}$$

which diverges to $+\infty$ as $n \to \infty$. So the series $\sum \alpha^n/n!$ diverges whenever $|\alpha|_p = p^{-1/(p-1)}$.

In $\mathbb{C}_p$ we have the unit disc

$$\mathcal{O}_p = \{\alpha \in \mathbb{C}_p : |\alpha|_p \leqslant 1\}.$$

PROPOSITION 5.21. *The subset $\mathcal{O}_p \subseteq \mathbb{C}_p$ is a subring of $\mathbb{C}_p$.*

The proof uses the ultrametric inequality and is essentially the same as that for $\mathbb{Z}_p \subseteq \mathbb{Q}_p$.

We end with yet another version of *Hensel's Lemma*, this time adapted to use in $\mathbb{C}_p$.

THEOREM 5.22 (Hensel's Lemma: $\mathbb{C}_p$ version). *Let $f(X) \in \mathcal{O}_p[X]$. Suppose that $\alpha \in \mathcal{O}_p$ and $d \geqslant 0$ is a natural number satisfying the two conditions*

$$|f(\alpha)|_p \leqslant \frac{1}{p^{2d+1}}, \quad |f'(\alpha)|_p = \frac{1}{p^d}.$$

Setting $\alpha_1 = \alpha - f(\alpha)f'(\alpha)^{-1}$, we have

$$|f(\alpha_1)|_p \leqslant \frac{1}{p^{2d+3}}.$$

The proof is left as an exercise. This result generalises our earlier versions of Hensel's Lemma.

Bibliography

[1] G. Bachman, Introduction to p-adic numbers and valuation theory, Academic Press, 1964.

[2] J. W. S. Cassels, Local Fields, Cambridge University Press, 1986.

[3] F. Q. Gouvêa, p-adic Numbers: An Introduction, 2nd edition, Springer (1997).

[4] N. Koblitz, p-adic numbers, p-adic analysis and zeta functions, second edition, Springer-Verlag, 1984.

[5] S. Lang, Algebra, Addison-Wesley (1965).

[6] K. Mahler, Introduction to p-adic numbers and their functions, second edition, Cambridge University Press, 1981.

[7] A. M. Robert, A course in p-adic analysis, Springer-Verlag, 2000.

Problems

Problem Set 1

1-1. For each of the following values $n = 19, 27, 60$, in the ring $\mathbb{Z}/n$ find
(i) all the zero divisors,
(ii) all the units and their inverses.

1-2. Let $f(X) = X^2 - 2 \in \mathbb{Z}[X]$. For each of the primes $p = 2, 3, 7$, determine whether or not there is a root of $f(X)$:

$$\text{(i)} \mod p, \quad \text{(ii)} \mod p^2, \quad \text{(iii)} \mod p^3, \quad \text{(iv)} \mod p^4.$$

Can you say anything more?

1-3. Solve the following system of simultaneous linear equations over $\mathbb{Z}/n$ for each of the values $n = 2, 9, 10$:

$$\begin{array}{rcrcrcl} 3x & + & 2y & - & 11z & \underset{n}{\equiv} & 1 \\ 7x & & & + & 2z & \underset{n}{\equiv} & 12 \\ & - & 8y & + & z & \underset{n}{\equiv} & 2 \end{array}$$

1-4. Find a generator for the cyclic group of units $(\mathbb{Z}/n)^\times$ in each of the following rings:

$$\text{(i) } \mathbb{Z}/23, \quad \text{(ii) } \mathbb{Z}/27, \quad \text{(iii) } \mathbb{Z}/10.$$

1-5. (a) For a prime p, $n \geqslant 1$ and $x \underset{p}{\equiv} 0$, consider

$$s_n = 1 + x + x^2 + \cdots + x^{n-1} \in \mathbb{Z}.$$

What element of $\mathbb{Z}/p^n$ does s_n represent?
(b) Let p be an *odd* prime. Let $n \geqslant 0$, $x \underset{p}{\equiv} 0$ and a be an integer such that $2a \underset{p^n}{\equiv} 1$. Show that

$$r_n = 1 + \sum_{1 \leqslant k \leqslant n-1} \binom{2k}{k} (a^2 x)^k$$

satisfies the equation

$$(r_n)^2 (1 - x) \underset{p^n}{\equiv} 1.$$

For $p = 2$, show that this equation holds if $x \underset{8}{\equiv} 0$.

Problem Set 2

2-1. Use Hensel's Lemma to solve each of the following equations:

(i) $$X^2 + 6 \underset{625}{\equiv} 0;$$

(ii) $$X^2 + X + 8 \underset{2401}{\equiv} 0.$$

N.B. $2401 = 7^4$.

2-2. Determine each of the following numbers:

$$\mathrm{ord}_3\, 54,\ \mathrm{ord}_5(-0.0625),\ \mathrm{ord}_7(-700/197),\ |-128/7|_2,\ |-13.23|_3,\ |9!|_3.$$

2-3. Let p be a prime and $n > 0$.
(a) Show that $\mathrm{ord}_p((p^n)!) = 1 + p + \cdots + p^{n-1}$.
(b) When $0 \leqslant a \leqslant p-1$, show that

$$\mathrm{ord}_p(ap^n!) = a(1 + p + \cdots + p^{n-1}).$$

(c) Let $r = r_0 + r_1 p + \cdots + r_d p^d$, where $0 \leqslant r_k \leqslant p-1$ for each k, and set $\alpha_p(r) = \sum_{0 \leqslant i \leqslant d} r_i$. Show that

$$\mathrm{ord}_p(r!) = \frac{r - \alpha_p(r)}{p-1}.$$

Use this to determine $|r!|_p$.

2-4. (a) Show that for $0 \neq x \in \mathbb{Q}$,

$$\prod_p |x|_p = \frac{1}{|x|},$$

where the product is taken over all primes $p = 2, 3, 5, \ldots$.
(b) If $x \in \mathbb{Q}$ and $|x|_p \leqslant 1$ for every prime p, show that $x \in \mathbb{Z}$.

2-5. Let p be a prime and $x \in \mathbb{Q}$. Consider the sequence e_n where

$$e_n = \sum_{0 \leqslant i \leqslant n} \frac{x^i}{i!}.$$

Show that e_n is a Cauchy sequence with respect to $|\ |_p$ if (A) $p > 2$ and $|x|_p < 1$, or (B) $p = 2$ and $|x|_2 < 1/2$. In either case, does this sequence have a limit in $\mathbb{Q}$?

Problem Set 3

3-1. Let F be any field and let $R = F[X]$ be the ring of polynomials over F on the variable X. Define an integer valued function

$$\mathrm{ord}_X f(X) = \max\{r : f(X) = X^r g(X) \text{ for some } g(X) \in F[X]\},$$

and set $\mathrm{ord}_X 0 = \infty$. Then define

$$N(f(X)) = e^{-\mathrm{ord}_X f(x)}.$$

Prove that ord_X satisfies the conditions of Proposition 2.4 with ord_X in place of ord_p. Hence deduce that N satisfies the conditions required to be a non-Archimedean norm on R.

3-2. Which of the following are Cauchy sequences with respect to the p-adic norm $|\ |_p$ where p is a given prime?
(a) $n!$, (b) $1/n!$, (c) x^n (this depends on x), (d) a^{p^n} (this depends on a), (e) n^s for $s \in \mathbb{Z}$ (this depends on s).

In each case which is a Cauchy sequence find the limit if it is a rational number.

3-3. Let $f(X) \in \mathbb{Z}[X]$ and let p be a prime. Suppose that $a_0 \in \mathbb{Z}$ is a root of $f(X)$ modulo p (*i.e.*, $f(a_0) \underset{p}{\equiv} 0$). Suppose also that $f'(a_0)$ is not congruent to 0 mod p. Show that the sequence (a_n) defined by

$$a_{n+1} = a_n - uf(a_n),$$

where $u \in \mathbb{Z}$ satisfies $uf'(a_0) \underset{p}{\equiv} 1$, is a Cauchy sequence with respect to $|\ |_p$ converging to root of f in $\mathbb{Q}_p$.

3-4. Let p be a prime with $p \underset{4}{\equiv} 1$.
(a) Let $c \in \mathbb{Z}$ be a primitive $(p-1)$-st root of 1 modulo p. By considering powers of c, show that there is a root of $X^2 + 1$ modulo p.
(b) Use Question 3-3 to construct a Cauchy sequence (a_n) in $\mathbb{Q}$ with respect to $|\ |_p$ such that

$$\left|a_n^2 + 1\right|_p < \frac{1}{p^n}.$$

(c) Deduce that there is a square root α of -1 in $\mathbb{Q}_5$.
(d) For $p = 5$ find $\alpha_1 \in \mathbb{Q}$ so that

$$|\alpha_1^2 + 1|_5 < \frac{1}{3125}.$$

3-5. Let R be a ring equipped with a non-Archimedean norm N. Show that a sequence (a_n) is Cauchy with respect to N if and only if $(a_{n+1} - a_n)$ is a null sequence. Show that this is false if N is Archimedean.

3-6. Determine each of the following 5-adic numbers to within an error of norm at most $1/625$:

$$\alpha = (3/5 + 2 + 4 \times 5 + 0 \times 25 + 2 \times 125 + \cdots) - (4/5 + 3 \times 25 + 3 \times 125 + \cdots),$$
$$\beta = (1/25 + 2/5 + 3 + 4 \times 5 + 2 \times 25 + 2 \times 125 + \cdots) \times (3 + 2 \times 5 + 3 \times 125 \cdots),$$
$$\gamma = \frac{(5 + 2 \times 25 + 125 + \cdots)}{(3 + 2 \times 25 + 4 \times 125 + \cdots)}.$$

Problem Set 4

4-1. Discuss the convergence of the following series in $\mathbb{Q}_p$:

$$\sum n!; \quad \sum \frac{1}{n!}; \quad \sum \frac{2^{2n} - 1}{2^n - 1} \quad \text{for } p = 2; \quad \sum \binom{p^{n+1}}{p^n}.$$

4-2. Find the radius of convergence of each of the following power series over $\mathbb{Q}_p$:

$$\sum \frac{X^n}{n!}; \quad \sum p^n X^n; \quad \sum \frac{X^{p^n}}{p^n}; \quad \sum n^k X^n \quad \text{with } 0 \leqslant k \in \mathbb{Z} \text{ fixed}; \quad \sum n! X^n; \quad \sum \frac{X^n}{n}.$$

4-3. Prove that in $\mathbb{Q}_3$,

$$\sum_{n=1}^{\infty} \frac{3^{2n}(-1)^n}{4^{2n} n} = 2 \sum_{n=1}^{\infty} \frac{3^{2n}}{4^n n}.$$

4-4. For $n \geqslant 1$, let

$$C_n(X) = \frac{X(X-1)\cdots(X-n+1)}{n!}$$

and $C_0(X) = 1$; in particular, for a natural number x,

$$C_n(x) = \binom{x}{n}.$$

(a) Show that if $x \in \mathbb{Z}$ then $C_n(x) \in \mathbb{Z}$.

(b) Show that if $x \in \mathbb{Z}_p$ then $C_n(x) \in \mathbb{Z}_p$.

(c) If $\alpha_n \in \mathbb{Q}_p$, show that the series

$$\sum_{n=0}^{\infty} \alpha_n C_n(x),$$

converges for all $x \in \mathbb{Z}_p$ if and only if

$$\lim_{n \to \infty} \alpha_n = 0.$$

(d) For $x \in \mathbb{Z}$, determine $\sum_{n=0}^{\infty} C_n(x) p^n$.

Problem Set 5

5-1. (a) Let $\sum \alpha_n$ be a series in $\mathbb{Q}_p$. Prove that the p-adic Ratio Test is valid, *i.e.*, $\sum \alpha_n$ converges if

$$\lambda = \lim_{n \longrightarrow \infty} \left| \frac{\alpha_{n+1}}{\alpha_n} \right|_p$$

exists and $\lambda < 1$.

(b) If $\sum \gamma_n X^n$ is a power series in $\mathbb{Q}_p$, deduce that the p-adic Ratio Test for Power Series is valid, *i.e.*, if

$$\lambda = \lim_{n \longrightarrow \infty} \left| \frac{\gamma_n}{\gamma_{n+1}} \right|_p$$

exists then $\sum \gamma_n X^n$ converges if $|x|_p < \lambda$ and diverges if $|x|_p > \lambda$.

Use these tests to determine the radii of convergence of the following series.

$$\sum \binom{p^{n+1}}{p}^n X^n; \quad \sum n! X^n; \quad \sum p^n X^n; \quad \sum \frac{X^n}{p^n}; \quad \sum \binom{pn}{n} X^n.$$

5-2. Prove **Pascal's Triangle**, *i.e.*, the identity

$$\binom{X+1}{n} = \binom{X}{n} + \binom{X}{n-1}.$$

holds for each natural number $n \geqslant 1$.

Let $f(X) = c_0 + c_1 X + \cdots + c_d X^d$ be a polynomial. Show that there are numbers $a_0, a_1, \ldots, a_d$ with each a $\mathbb{Z}$ linear combination of the c_n, such that

$$f(X) = a_0 + a_1 \binom{X}{1} + \cdots + a_d \binom{X}{d}.$$

Show also that these a_n can be determined using the sequence of polynomials

$$f^{[n]}(X) = f^{[n-1]}(X+1) - f^{[n-1]}(X),$$

where $f^{[0]}(X) = f(X)$ and $a_n = f^{[n]}(0)$.

5-3. For $n \geqslant 0$, let $\omega_n \colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ denote the n-th Teichmüller function. So for $x \in \mathbb{Z}_p$ we have $x = \omega_0 + \omega_1 p + \cdots + \omega_n p^n + \cdots$ and $\omega_n(x)^p = \omega_n(x)$ for each n.

For $x, y \in \mathbb{Z}_p$, verify the inequalities

$$\left|\omega_1(x) - \left(\frac{x - x^p}{p}\right)\right|_p < 1, \quad |\omega_0(x+y) - \omega_0(x) - \omega_0(y)|_p < 1,$$

$$\left|\omega_1(x+y) - \left(\omega_1(x) + \omega_1(y) - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} \omega_0(x)^k \omega_0(y)^{p-k}\right)\right|_p < 1.$$

What can you say about $\omega_0(xy), \omega_1(xy)$? What about $\omega_n(x+y), \omega_n(xy)$ for $n > 1$?

5-4. Write out a proof that for real numbers a, b with $a < b$, a locally constant function $f \colon \mathbb{R} \longrightarrow \mathbb{R}$ is constant on (a, b). If your proof uses differentiability find one which doesn't, hence is more 'elementary'.

5-5. Let $f \colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ be a continuous function. Prove that f is bounded, *i.e.*, there is a positive $B \in \mathbb{R}$ such that for all $x \in \mathbb{Z}_p$, $|f(x)|_p < B$.

Problem Set 6

6-1. Calculate $\|f\|_p$ for each of the following functions $f \colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$:

$\binom{px}{n}$; $x^p - x$; $x(x+1)(x+2)\cdots(x+n-1)$ for $n > 0$ a natural number; x^n for $n \in \mathbb{Z}$.

6-2. For the prime $p = 3$ show that the function $f(x) = 1/(x^4 + 1)$ is defined on $\mathbb{Z}_3$. Determine the Mahler coefficients a_0, a_1, a_2, a_3, a_4 for f.

6-3. For the prime $p = 2$, find the Mahler expansion of the continuous function $f \colon \mathbb{Z}_2 \longrightarrow \mathbb{Q}_2$ which for an integer $t \in \mathbb{Z}$ is given by

$$f(t) = \begin{cases} \dfrac{t}{2} & \text{if } t \text{ is even,} \\ \dfrac{t-1}{2} & \text{if } t \text{ is odd.} \end{cases}$$

Hint: consider the Mahler expansion of $(-1)^x$ as a function of $x \in \mathbb{Z}_2$.

6-4. Determine the Mahler expansion of $f(x+1)$ in terms of that of $f(x)$ where $f\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ is a continuous function. Generalise this to $f(x+\alpha)$ where $\alpha \in \mathbb{Z}_p$.
Hint: find a formula for $\binom{x+y}{n}$ in terms of $\binom{x}{r}$ and $\binom{y}{s}$.

6-5. (a) Let $y \in \mathbb{Z}_p$ with $|y|_p < 1$. For any $x \in \mathbb{Z}_p$ show that if (x_n) is a sequence of integers converging to x in $\mathbb{Z}_p$, then $\lim\limits_{n\to\infty} (1+y)^{x_n}$ exists.
(b) Prove that the function

$$f(x) = \lim_{n\to\infty} (1+y)^{x_n}$$

is continuous on $\mathbb{Z}_p$. What is the Mahler expansion of f?

6-6. Find $|x|_3$ for each of the following elements x of $\mathbb{C}_p$:

$$\pm\sqrt{2},\ \sqrt[3]{2},\ \sqrt[3]{3},\ \sqrt[6]{1},\ \gamma - 1 \quad \text{where } \gamma^2 = -1.$$

6-7. Show that there is no root of the polynomial $X^4 - 2$ in any of the fields $\mathbb{Q}_p$ where $p = 2, 3, 5$. What about the polynomial $X^4 - 4$?