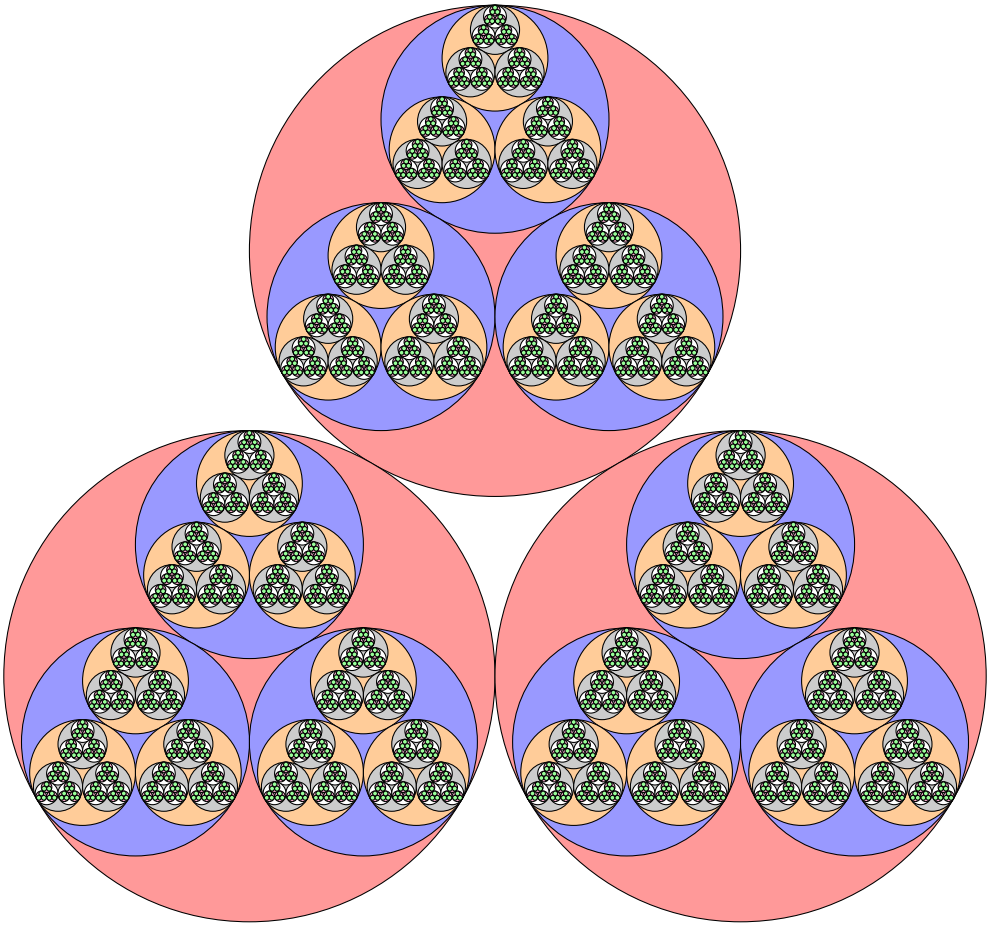
Introduction to the p-adic numbers

Ross Paterson
ross.paterson@bristol.ac.uk

February 2024



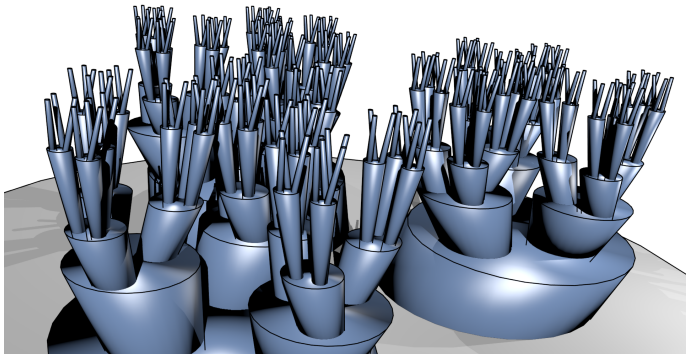
Introduction

The real numbers, $\mathbb{R}$, are a superset of the rational numbers, coming equipped with a natural notion of size, the usual absolute value $\|\cdot\|$, and are a very intuitive place to learn both analysis and algebra. Since they are so sensible, and we are so familiar with them, we spend much of our lives not even knowing what they are! We grow up thinking that 'real numbers' are just decimal expansions, and at some point we bump into the uncomfortable reality that this is not really a good definition since, for example, $0.9999... = 1$. Assuming that this is just a strange curiosity we continue to pretend that we know our friend $\mathbb{R}$, and it is only in our first course in real analysis that we learn that the real numbers are actually the 'completion' of $\mathbb{Q}$ with respect to the metric induced by $\|\cdot\|$. This involves a rather technical discussion about Cauchy sequences, which we eventually put to the back of our minds and go back to thinking in terms of decimal expansions.

In this language, the real numbers are just one in a zoo of completions! We have a whole family of other animals in this zoo: for each prime number p there is a completion $\mathbb{Q}_p$, which has a different notion of size and is known as the p-adic numbers. These other completions are strange beasts, often far easier to work with but sometimes very unintuitive. To give you some examples that we shall see in the course, consider the following.

- Say we want to know whether an infinite series $\sum_{n=1}^{\infty} a_n$ converges. Intuitively, we expect that if the size of the terms a_n is going to 0 as n goes to infinity then it should converge. In $\mathbb{R}$ this is not enough, the situation turns out to be somewhat delicate. However, in $\mathbb{Q}_p$, our intuition is correct: such a series converges if and only if the size of a_n goes to 0!
- Consider a disc of radius r in $\mathbb{R}$, then of course it should have a unique centre point. Such an intuitive claim is false in $\mathbb{Q}_p$: in fact, every element of a disc is a centre point. How odd!

This course is an introduction to these p-adic numbers, with the intention of packing your tool-kits with various p-adic spanners and wrenches. We shall survey them from various angles, without going to far in any one direction, so as to maximise on what you can concretely 'do' with them. Of course, this being quite a short course, there is far more to see than we show here! We have cherry-picked some useful and interesting results to prepare you to go forth and explore this exotic world in the future.



An approximation of the 3-adic numbers by Daniel Litt

Throughout these notes, p will *always* denote a prime number!

1 The Rational Numbers Through a p-adic Lens

We begin our p-adic safari by looking at the rational numbers through a different lens – a p-adic one. More precisely, we will consider a different notion of size on $\mathbb{Q}$ which depends on a fixed prime number p, and consider the properties therein.

1.1 p-adic valuation

Prime numbers are extremely self-obsessed, showing little interest in each other. For example, you may recall the Chinese Remainder Theorem, which can be understood as saying "the prime factors of an integer show no interest in each other".

In the p-adic world, which is of course ruled by it's vain namesake prime number p, value is given to an integer if the integer 'contains a lot of p'. In other words, integers which are divisible by higher powers of p are more valuable. This notion of value is made precise by the p-adic valuation.

Definition 1.1. The p-adic valuation on $\mathbb{Z}$ is the function

$$v_p : \mathbb{Z}\backslash\{0\} \to \mathbb{Z}$$

defined as follows. For each $n \in \mathbb{Z}\backslash\{0\}$, let $v_p(n)$ be the unique nonnegative integer such that

$$n = p^{v_p(n)} n'$$

where $n' \in \mathbb{Z}$ is coprime to p. We extend this to $\mathbb{Z}$ by writing $v_p(0) := \infty$.

We extend this definition to $\mathbb{Q}$ as follows: for every pair of nonzero integers $a, b \in \mathbb{Z}\backslash\{0\}$ we define

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

In the literature, v_p is sometimes denoted by ord_p instead. We've chosen the former notation, but you should keep this in mind when reading other sources.

Exercise 1.2. *Check that for every $x \in \mathbb{Q}$ the p-adic valuation is well defined. In other words, check that if $\frac{a}{b} = \frac{c}{d}$ then $v_p(a) - v_p(b) = v_p(c) - v_p(d)$. You should also check that for a nonzero rational number x, $v_p(x) \in \mathbb{Z}$ is the unique integer such that $x = p^{v_p(x)}\frac{a}{b}$ where $a, b \in \mathbb{Z}$ are coprime to p.*

This valuation function has some useful elementary properties, which we now observe.

Proposition 1.3. *The p-adic valuation satisfies the following properties for all $x, y \in \mathbb{Q}$.*

(a) $v_p(x) = \infty$ *if and only if* $x = 0$;

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

(c) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$, *with equality if* $v_p(x) \neq v_p(y)$.

Proof. (a) and (b) are clear, and left to the reader to verify as an exercise. For (c), write $x = p^{v_p(x)}\frac{a}{b}$ and $y = p^{v_p(y)}\frac{c}{d}$ for integers $a, b, c, d \in \mathbb{Z}$ which are coprime to p.

Now, if $v_p(x) = v_p(y)$ then we get

$$x + y = p^{v_p(x)} \left(\frac{ad + bc}{bd} \right),$$

and since $v_p(bd) = 0$, we see that $v_p(x + y) = v_p(x) + v_p(ad + bc) \geq v_p(x) = \min\{v_p(x), v_p(y)\}$. If $v_p(x) \neq v_p(y)$ then let us assume without loss of generality that $v_p(x) = \min\{v_p(x), v_p(y)\}$ is the smaller one. Then now we obtain

$$x + y = p^{v_p(x)} \frac{ad + p^{v_p(y) - v_p(x)}}{bd},$$

and since bd and ad are coprime to p, and $v_p(y) - v_p(x) \geq 1$, the numerator and denominator above are coprime to p and hence $v_p(x + y) = v_p(x)$. □

Example 1.4. *For $p = 3$, we have $v_3(9) = v_3(18) = v_3\left(\frac{765}{572}\right) = 2$. For every integer n, we can deduce that $v_3(n^3 - n) \geq 1$ by considering the possible congruence classes of n mod 3.*

Example 1.5. *We will see in the exercise class that for each positive integer $n \in \mathbb{Z}$,*

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

1.2 p-adic size

In the p-adic world, an integer $n \in \mathbb{Z}$ should be small if it takes a while to show up when we go looking for it modulo powers of p. Consider the following example.

Example 1.6. *Let $p = 3$, and consider $x = 18$. We cannot see anything modulo 3 since $x \equiv 0 \mod 3$, and similarly $x \equiv 0 \mod 9$. However, we do see something modulo $27 = 3^3$, since $18 \not\equiv 0 \mod 27$.*

This intuition leads us to define the "p-adic absolute value", which measures size in the p-adic world in an analogous way to how the 'usual' absolute value $\|\cdot\|$ measures size in the real world.

Definition 1.7. The p-adic absolute value of a rational number $x \in \mathbb{Q}$ is

$$|n|_p = \frac{1}{p^{v_p(n)}},$$

where for $n = 0$ we interpret $|0|_p = 1/p^{\infty}$ to be 0.

Example 1.8. $|p^n|_p = \frac{1}{p^n}$. *For $p = 3$, continuing Example 1.4, $|9|_3 = |18|_3 = \left|\frac{765}{572}\right|_3 = \frac{1}{9}$. Moreover, for every integer n we can bound $\left|n^3 - n\right|_3 \leq \frac{1}{3}$.*

Proposition 1.9. *The p-adic absolute value satisfies the following properties for all $x, y \in \mathbb{Q}$.*

1. $|x|_p = 0$ *if and only if* $x = 0$;
2. $|xy|_p = |x|_p |y|_p$;
3. *(ultrametric inequality)* $|x + y|_p \leq \max\left\{|x|_p, |y|_p\right\}$ *with equality if* $|x|_p \neq |y|_p$.

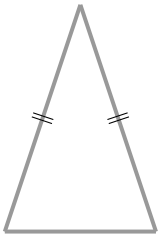
Proof. These follow immediately from the definition of the p-adic absolute value and the properties of the p-adic valuation in Proposition 1.3. □

Comparison 1.10

Note that the real absolute value $\|\cdot\|$ satisfies the first two properties above, but not the third. There is the triangle inequality:

$$\|x + y\| \leq \|x\| + \|y\|,$$

but this is far weaker than the third condition above. This has strange consequences for geometry in the p-adic world. Recall that an isosceles triangle is one for which two sides have the same length. Of course, in the real world, there are more kinds of triangles than this! However, in the p-adic world every triangle is isosceles (see exercise sheet 1).



Indeed, this notion of size lends itself to talking about sequences converging, in a p-adic sense, to a point.

Definition 1.11. Let a_n be a sequence of rational numbers. We say that a rational number a is the p-adic limit of the sequence a_n if $\lim_{n\to\infty} |a_n - a|_p = 0$. If such an a exists for the sequence a_n then we write

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

The correct way to interpret this limit is in the language of metric spaces. If we define the p-adic distance between $x, y \in \mathbb{Q}$ to be $d(x, y) := |x - y|_p$, then you can check with the properties of $|\cdot|_p$ above that this defines a metric on $\mathbb{Q}$. In this language, $\lim^{(p)}_{n\to\infty} a_n$ is the usual metric space limit of a_n (if it exists). We shall not make use of this perspective yet, but it is good to keep in mind.

Example 1.12. *The sequence $a_n = p^n$ satisfies $\lim^{(p)}_{n\to\infty} a_n = 0$.*

Example 1.13. *The sequence $a_n = \frac{1}{n}$ does not have a p-adic limit. Indeed, assume that there is a p-adic limit $a \in \mathbb{Q}$. Consider the subsequence $b_n := \frac{1}{p^n}$, so that $|b_n|_p = p^n$. For large enough n we have $p^n > |a|_p$, and so by Proposition 1.9 we have $|b_n - a|_p = |b_n|_p = p^n$, which does cannot go to 0 as $n \to \infty$. Hence the limit cannot exist.*

1.3 p-adic expansions

Given a rational number $x = \frac{a}{b}$, we can expand x as a power series in p, giving rise to the so-called p-adic expansion.

Definition 1.14. A p-adic digit is an element $a \in \{0, \ldots, p-1\}$. A p-adic expansion for a nonzero rational number $x \in \mathbb{Q}\backslash\{0\}$ is a sequence of p-adic digits $(a_k)_{k \geq v}$ such that

$$x = \lim_{N \to \infty}^{(p)} \sum_{k=v}^{N} a_k p^k,$$

and $a_v \neq 0$. We extend this definition to include $x = 0$ by taking the p-adic expansion of 0 to have $v = 0$ and $a_k = 0$ for all $k \geq 0$.

Comparison 1.15

The p-adic expansion is the p-adic analogue of the decimal expansion (e.g. $\frac{1}{3} = 0.333...$) for real numbers $\mathbb{R}$. Decimal expansions are thought of in this way as expressions

$$x = \lim_{N \to \infty} \sum_{k=v}^{N} r_k \left(\tfrac{1}{10}\right)^k,$$

where $r_k \in \{0, \ldots, 9\}$ are decimal digits.

Example 1.16. *Consider $p = 5$, and the number $x = 566$. Then we can check that a p-adic expansion is given by*

$$566 = 1 + 3 \cdot 5 + 2 \cdot 5^2 + 4 \cdot 5^3.$$

Example 1.17. *Consider $x = -1$, then how do we produce a p-adic expansion? Well, note that $|x|_p = 1$, and we would like to start approximating by partial sums. Note that $|x - (p-1)|_p = |-p|_p = 1/p$, so we'd like to choose $a_0 = (p-1)$. We now need to choose a_1, and note that $\left|x - (p^2-1)\right|_p = \left|-p^2\right|_p = 1/p^2$. Thinking of $p^2 - 1 = (p-1) + (p-1)p$ we see that we should choose $a_1 = (p-1)$ also. In fact, the same argument tells us that*

$$\left| x - \sum_{k=0}^{N} (p-1)p^k \right|_p = \left|p^{N+1}\right|_p = 1/p^N,$$

which goes to 0 as $N \to \infty$ and so

$$-1 = \lim_{N \to \infty}^{(p)} \sum_{k=0}^{N} (p-1)p^k.$$

We should check firstly that these p-adic expansions exist for every nonzero $x \in \mathbb{Q}$. How should we construct such an expansion? Firstly we note that finding a p-adic expansion for x is equivalent to finding one for $p^r x$ for any integer r, since multiplication by powers of p just shifts the digits of the expansion along:

$$p^r \cdot \left(\sum_{k=v}^{\infty} a_k p^k \right) = \sum_{k=v+r}^{\infty} a_{k-r} p^k.$$

Hence, in constructing the p-adic expansion, we can make a simplifying assumption that $v_p(x) \geq 0$ by multiplying x by an appropriate power of p. We want to find an expression of the form

$$x = a_0 + a_1 p + a_2 p^2 + \ldots. \tag{1}$$

Observe that, at least formally, if we could reduce x mod p then we would cut off everything after a_0 and we could define a_0 to be the unique p-adic digit such that $a_0 \equiv x \mod p$. We should make careful sense of this as we cannot reduce arbitrary elements of $\mathbb{Q}$ mod p – what would $1/6$ even mean mod 3? We begin by writing $x = p^v \frac{a}{b}$ for some pair of integers a, b coprime to p and $v = v_p(x) \geq 0$. If $v > 0$, then we shall set $a_0 = 0$. Else if $v = 0$ then since b is coprime to p, it is invertible mod p and so it makes sense to define a_0 to be the unique p-adic digit such that

$$a_0 \equiv ab^{-1} \mod p.$$

In particular, we then have $x - a_0 = \frac{a - a_0 b}{b}$. By construction, the numerator is $0 \mod p$ and the denominator is still coprime to p and so $v_p(x - a_0) \geq 1$ and we have found a sensible choice for a_0.

We now need to find a_1. In our proposed expression in (1), we note that

$$p^{-1}(x - a_0) = a_1 + a_2 p + \dots,$$

so $p^{-1}(x - a_0)$ has valuation at least 0 and a_1 can be determined by performing the same process as above replacing x with $p^{-1}(x - a_0)$. Iterating the process, we can calculate a_{N+1} from $p^{-N}\left(x - (a_0 + a_1 p + a_2 p^2 + \dots + a_N p^N)\right)$, which has valuation at least 0. In particular,

$$\left| x - \sum_{k=0}^{N} a_k p^k \right|_p \leq p^{-N},$$

so $x = \lim\limits_{N \to \infty}^{(p)} \sum_{k=0}^{N} a_k p^k$, and we have constructed a p-adic expansion for x.

Proposition 1.18. *For each $x \in \mathbb{Q}$ there is a unique p-adic expansion.*

Proof. Having provided a construction above, we are left to check that it is the only p-adic expansion. Let $x \in \mathbb{Q}$, and let $(a'_k)_{k \geq v}$ and $(a_k)_{k \geq v}$ be two different sequences of p-adic digits such that

$$x = \lim_{N \to \infty}^{(p)} \sum_{k=v}^{N} a'_k p^k = \lim_{N \to \infty}^{(p)} \sum_{k=v}^{N} a_k p^k.$$

Note that $a_k - a'_k \in \{-(p-1), \dots, (p-1)\}$ and so

$$|a_k - a'_k|_p = \begin{cases} 1 & \text{if } a_k \neq a'_k; \\ 0 & \text{if } a_k = a'_k. \end{cases}$$

Let $m \geq v$ be the first index where $a_m \neq a'_m$. Then for $N \geq m$, using the ultrametric inequality

$$\left| \sum_{k=v}^{N} a_k p^k - \sum_{k=v}^{N} a'_k p^k \right|_p = \left| \sum_{k=m}^{N} (a_k - a'_k) p^k \right|_p = p^{-m}.$$

On the other hand, choose $\varepsilon > 0$ such that $\varepsilon < p^{-m}$. Then since these p-adic expansions converge to x, for sufficiently large N we get

$$p^m = \left| \sum_{k=v}^{N} a_k p^k - \sum_{k=v}^{N} a'_k p^k \right|_p = \left| \sum_{k=v}^{N} a_k p^k - x + x - \sum_{k=v}^{N} a'_k p^k \right|_p \leq \max\left\{ \left| \sum_{k=v}^{N} a_k p^k - x \right|_p, \left| x - \sum_{k=v}^{N} a'_k p^k \right|_p \right\} \leq \varepsilon,$$

which is a contradiction. Thus we can only have at most one p-adic expansion. □

Comparison 1.19

The decimal expansion of a rational number is not unique, for example $0.999... = 1$, but the p-adic expansion is unique. This makes p-adic expansions quite special in comparison to their real analogue!

In fact a useful property of these expansions is that we can read off the p-adic valuation (and so the p-adic absolute value)!

Lemma 1.20. *Let $x \in \mathbb{Q}$ be a rational number and $\lim_{N\to\infty}{}^{(p)} \sum_{k=v}^{N} a_k p^k$ be the p-adic expansion of x. Then*

$$v_p(x) = v \qquad \text{and} \qquad |x|_p = p^{-v}.$$

Proof. By the ultrametric inequality, note that for every $N \geq v$

$$\left| \sum_{k=v}^{N} a_k p^k \right|_p = |a_v p^v|_p = p^{-v}.$$

If $p^{-v} \neq |x|_p$ then again by the ultrametric inequality

$$\left| x - \sum_{k=v}^{N} a_k p^k \right|_p = \max\left\{ p^{-v}, |x|_p \right\},$$

which does not depend on N and is bigger than 0. However since the definition of a p-adic expansion requires $\lim_{N\to\infty} \left| x - \sum_{k=v}^{N} a_k p^k \right|_p = 0$, we have reached a contradiction. The claim for the valuation follows immediately since $|x|_p = p^{-v_p(x)} = p^{-v}$ □

Since decimal expansions of rational numbers are (eventually) periodic, it is natural to hope that the same is true for the p-adic expansion. Whilst we've already seen plenty of situations where the p-adic world is different to the real one, this is a situation where both agree.

Lemma 1.21. *For all $x \in \mathbb{Q}$, the p-adic expansion is eventually periodic.*

Proof. See exercise sheet 1. □

2 The p-adic Numbers

2.1 Motivation: constructing the real numbers

In the previous section we introduced the p-adic expansion of a rational number $x \in \mathbb{Q}$, which is the p-adic analogue of the decimal expansion of a real number. Both types of expansion are eventually periodic for rational numbers. In the same way that the real numbers are somehow 'the rest of the decimal expansions', the p-adic numbers will be 'the rest of the p-adic expansions'.

We often think of real numbers as being given by sums (with respect to $\|\cdot\|$) of the form

$$\sum_{k=m}^{\infty} r_k(\tfrac{1}{10})^k,$$

where $r_k \in \{0, \ldots, 9\}$ are decimal digits and $m \in \mathbb{Z}$ is an integer. For example $\pi = 3.14159...$ can be written with $m = 0$, $r_0 = 3$, $r_1 = 1$, $r_2 = 4$, and so on. However one must be very careful with this, the reals are not just somehow the 'set of all decimal expansions' – some distinct decimal expansions represent the same real number, for example $0.999... = 1$ in $\mathbb{R}$.

How did we make this precise in real analysis? The answer: by using Cauchy sequences. Formally, the real numbers are *defined* to be the set of Cauchy sequences (with respect to $\|\cdot\|$) in $\mathbb{Q}$ modulo an equivalence relation: that two sequences $(x_n)_n, (y_n)_n$ are equal if $\lim_{n\to\infty} \|x_n - y_n\| = 0$. Decimal expansions provide a source of Cauchy sequences by partial sums:

$$\sum_{k=m}^{\infty} r_k(\tfrac{1}{10})^k \leftrightarrow \left(\sum_{k=m}^{m+n} r_k(\tfrac{1}{10})^k\right)_n,$$

and one shows that every Cauchy sequence is equivalent to one coming from a decimal expansion.

Example 2.1. *The elements* $0.999... \leftrightarrow (0,\ 0.9,\ 0.99,\ 0.999,\ \ldots)$ *and* $1.000... \leftrightarrow (1,\ 1,\ 1,\ 1,\ \ldots)$ *are equal in* $\mathbb{R}$ *– the difference between the* n*th terms has absolute value* $10^{-(n-1)}$*, which goes to* 0 *as* $n \to \infty$*.*

2.2 Defining $\mathbb{Q}_p$

The p-adic numbers will be the p-adic analogue of the story above: we want to make sense of all of the infinite sums

$$\sum_{k=v}^{\infty} a_k p^k,$$

where $a_k \in \{0, \ldots, p-1\}$ are p-adic digits and $m \in \mathbb{Z}$ is an integer. These sums will then be called 'p-adic numbers'. To make this rigorous, we take the same approach as with the real numbers above: our avatar for these infinite sums will be the sequence of partial sums

$$\sum_{k=v}^{\infty} a_k p^k \longleftrightarrow \left(\sum_{k=v}^{v+n} a_k p^k\right)_{n=0}^{\infty} = \left(a_v p^v,\ a_v p^v + a_{v+1}p^{v+1},\ \ldots,\ \sum_{k=v}^{v+n} a_k p^k,\ \ldots\right). \tag{2}$$

We will then define the p-adic numbers as the set of Cauchy sequences up to an equivalence relation. Recall the definition of a Cauchy sequence (with respect to our p-adic metric).

Definition 2.2. A sequence $(x_n)_{n=0}^{\infty}$ of rational numbers is Cauchy with respect to $|\cdot|_p$ if for every $\varepsilon > 0$ there exists an integer N such that for all $m, n \geq N$

$$|x_n - x_m|_p \leq \varepsilon.$$

Lemma 2.3. *Let $(a_k)_{k=v}^{\infty}$ be a sequence of p-adic digits. For each $n \geq 0$ let $s_n := \sum_{k=v}^{v+n} a_k p^k$. Then the sequence $(s_n)_n$ is a Cauchy sequence of rational numbers with respect to $|\cdot|_p$.*

Proof. For $\varepsilon > 0$, let $N > 0$ be an integer such that $p^{-(v+N)} \leq \varepsilon$. Then for $n \geq m \geq N$ we use the ultrametric inequality to obtain

$$|s_n - s_m|_p = \left| \sum_{k=v+m+1}^{v+n} a_k p^k \right|_p \leq p^{-(v+m)} \leq \varepsilon.$$

□

Definition 2.4. We denote the set of Cauchy sequences in $\mathbb{Q}$ with respect to $|\cdot|_p$ by

$$\mathscr{C}_p := \left\{ (x_n)_n \ : \ \begin{smallmatrix} (x_n)_n \text{ is a Cauchy sequence} \\ \text{with respect to } |\cdot|_p \end{smallmatrix} \right\}.$$

We define an equivalence relation $\sim_p$ on $\mathscr{C}_p$ by saying two sequences are equivalent if they are tending toward each other. Precisely: given two Cauchy sequences $(x_n), (x'_n) \in \mathscr{C}_p$,

$$(x_n) \sim_p (x'_n) \iff \lim_{n\to\infty} |x_n - x'_n|_p = 0$$

Example 2.5. *The constant sequence $(-1, -1, \dots)$ is equivalent to the sequence $(p^n - 1)_n$.*

Example 2.6. *The sequences $(n!)_n$ and (p^n) are both Cauchy and equivalent.*

Example 2.7. *Let $x \in \mathbb{Q}$ be a rational number, and let $\sum_{k=v}^{\infty} a_k p^k$ be its p-adic expansion. Then by definition of the p-adic expansion, the constant sequence $(x)_n$ is equivalent to the sequence of partial sums from the p-adic expansion, i.e.*

$$(x)_n \sim_p \left(\sum_{k=v}^{v+n} a_k p^k \right)_n$$

Definition 2.8. The set of p-adic numbers $\mathbb{Q}_p$ is the set of Cauchy sequences in $\mathbb{Q}$ (with respect to $|\cdot|_p$) modulo the equivalence relation $\sim_p$:

$$\mathbb{Q}_p := \mathscr{C}_p / \sim_p$$

In order for this new set $\mathbb{Q}_p$ to be analogous to the reals in some way, it had better contain our old friend $\mathbb{Q}$ – let us check this!

Lemma 2.9. *The map $\mathbb{Q} \to \mathbb{Q}_p$ given by sending each $x \in \mathbb{Q}$ to the equivalence class of the constant sequence $(x)_n$ is injective.*

Proof. If $x \neq y$ are two rational numbers then by Proposition 1.9 $\lim_{n\to\infty} |x - y|_p = |x - y|_p \neq 0$. □

Remark 2.10. In future, we will refer to $\mathbb{Q}$ as a subset of $\mathbb{Q}_p$, implicitly meaning via the identification between x and the equivalence class of the constant sequence $(x)_n$. In particular, we have distinguished elements $1, 0 \in \mathbb{Q}_p$ coming from the numbers $1, 0 \in \mathbb{Q}$.

2.3 Operations on $\mathbb{Q}_p$

Our next objective is now extend to the addition, multiplication, and p-adic absolute value from $\mathbb{Q}$ to $\mathbb{Q}_p$.

Definition 2.11. We add and multiply Cauchy sequences as follows: for $(x_n)_n, (y_n)_n \in \mathscr{C}_p$,

$$(x_n)_n + (y_n)_n := (x_n + y_n)_n,$$
$$(x_n)_n \cdot (y_n)_n := (x_n y_n)_n.$$

Exercise 2.12. *Let $(x_n)_n, (y_n)_n \in \mathscr{C}_p$ be two Cauchy sequences. Check that their product and sum really are both Cauchy sequences, i.e. both $(x_n)_n + (y_n)_n$ and $(x_n)_n \cdot (y_n)_n$ are in $\mathscr{C}_p$.*

Example 2.13. *If $x, y \in \mathbb{Q}$ are identified with their constant sequences $(x)_n, (y)_n \in \mathscr{C}_p$ then addition and multiplication for x, y are the same in $\mathbb{Q}$ as in $\mathscr{C}_p$. If you are familiar with rings, then the highbrow view on this is that $\mathscr{C}_p$ is a ring with respect to our operations above and $\mathbb{Q} \to \mathscr{C}_p$ is an injective ring homomorphism.*

We also extend the p-adic absolute value on $\mathbb{Q}$ to an absolute value on $\mathscr{C}_p$, to give us a notion of size for these sequences. Recall that we are thinking of a Cauchy sequence $(x_n)_n$ as representing its own limit, and so notions like size should really be limits of the sizes of the entries in the sequence, as follows.

Definition 2.14. The absolute value and valuation of a Cauchy sequence $x = (x_n)_n \in \mathscr{C}_p$ are

$$|x|_p := \lim_{n\to\infty} |x_n|_p, \quad \text{and}$$
$$v_p(x) := \lim_{n\to\infty} v_p(x_n)$$

where on the right hand side the expressions $|x_n|_p$ and $v_p(x_n)$ are the p-adic absolute value and valuation of the rational number x_n.

Example 2.15. *For $x \in \mathbb{Q}$, the absolute value and valuation of the corresponding constant sequence $(x)_n$ are just the p-adic valuation and p-adic absolute value of x.*

Example 2.16. *The absolute values of both $(n!)_n$ and $(p^n)_n$ are zero, the absolute value of $(1 + p^n)_n$ is 1.*

We should investigate the sequence of absolute values of the entries of our sequence to be sure that this is well defined! First, we shall need the use of a convenient lemma.

Lemma 2.17. *Let $x, y \in \mathbb{Q}$, then*

$$\left\| |x|_p - |y|_p \right\| \leq |x - y|_p .$$

Proof. Note that the triangle inequality gives

$$|x|_p = \left\| |x|_p - |y|_p + |y|_p \right\| \leq \left\| |x|_p - |y|_p \right\| + |y|_p ,$$

Similarly, swapping x and y we obtain

$$|y|_p \leq \left\| |y|_p - |x|_p \right\| + |x|_p = \left\| |x|_p - |y|_p \right\| + |x|_p .$$

In particular, since $\|-z\| = \|z\|$, the claim holds. □

Lemma 2.18. *Let $x = (x_n)_n \in \mathscr{C}_p$ be a Cauchy sequence. Then the sequence $\left(|x_n|_p\right)_n$ either converges to 0 or is eventually constant. In particular $|x|_p \in \mathbb{R}_{>0}$ and $v_p(x) \in \mathbb{Z} \cup \{\infty\}$ always exist and satisfy*

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

Proof. Recall that $|\cdot|_p$ on $\mathbb{Q}$ is defined by $|x|_p = p^{-v_p(x)}$. In particular, the second claim follows from the first, and so we must only prove the first claim about the sequence of absolute values.

We begin by claiming that the sequence $\left(|x_n|_p\right)_n$ is a Cauchy sequence with respect to $\|\cdot\|$, so converges to a limit in $\mathbb{R}$. Indeed, $(x_n)_n$ is Cauchy with respect to $|\cdot|_p$, so for $\varepsilon > 0$ we choose N so that for all $n, m \geq N$ we have $|x_n - x_m|_p \leq \varepsilon$. Now, using Lemma 2.17, for $m, n \geq N$ we have

$$\left\| |x_n|_p - |x_m|_p \right\| \leq |x_n - x_m|_p \leq \varepsilon,$$

as required.

Let $A := \lim_{n\to\infty} |x_n|_p \in \mathbb{R}$ and assume that $A \neq 0$ (so that we should show that $|x_n|_p$ is constant for large n). Then there exists an $N > 0$ such that for all $n \geq N$,

$$|x_n|_p > \frac{A}{2}.$$

Moreover, possibly making N larger, since $(x_n)_n$ is Cauchy we can ensure that for all $n, m \geq N$,

$$|x_n - x_m|_p < \frac{A}{2}.$$

We draw these two inequalities together using the ultrametric inequality (which is an equality by the sharpness of the bounds above) to obtain that for all $n, m \geq N$

$$\begin{aligned} |x_n|_p &= |x_n - x_m + x_m|_p \\ &= \max\left\{ |x_n - x_m|_p + |x_m|_p \right\} \\ &= |x_m|_p , \end{aligned}$$

as required. □

Now that we have these operations on the level of Cauchy sequences, we would like to make them operations on $\mathbb{Q}_p$ – and we should definitely check that this makes sense! We encapsulate everything we need as a theorem below.

Theorem 2.19. *$\mathbb{Q}_p$ has well defined addition and multiplication operations induced by the operations on representatives in $\mathscr{C}_p$*

$$(x_n)_n + (y_n)_n = (x_n + y_n)_n \qquad \text{and} \qquad (x_n)_n \cdot (y_n)_n = (x_n y_n)_n.$$

Moreover, each $x \in \mathbb{Q}_p$ has a well defined absolute value and valuation induced by the absolute value and valuation on a representative $(x_n) \in \mathscr{C}_p$

$$|x|_p := \lim_{n\to\infty} |x_n|_p, \quad \text{and} \quad v_p(x) := \lim_{n\to\infty} v_p(x_n),$$

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

If $x \in \mathbb{Q} \subseteq \mathbb{Q}_p$ then both the absolute value and valuation agree with the p-adic absolute value and valuation from Definitions 1.1 and 1.7

Proof. Let $(x_n)_n, (y_n)_n, (x'_n)_n, (y'_n)_n \in \mathscr{C}_p$ be Cauchy sequences with $(x_n)_n \sim_p (x'_n)_n$ and $(y_n)_n \sim_p (y'_n)$.

Addition: We must show that $(x_n + y_n)_n \sim_p (x'_n + y'_n)$. Taking differences,

$$|x_n + y_n - x'_n - y'_n|_p \leq \max\left\{|x_n - x'_n|_p, |y_n - y'_n|_p\right\},$$

so since the right hand side tends to 0 as $n \to \infty$, as does the left as required.

Multiplication: We must show that $(x_n y_n)_n \sim_p (x'_n y'_n)$. We have

$$\begin{aligned} |x_n y_n - x'_n y'_n|_p &= |(x_n - x'_n)y_n - x'_n(y'_n - y_n)|_p \\ &\leq \max\left\{|(x_n - x'_n)y_n|_p, |x'_n(y'_n - y_n)|_p\right\} \end{aligned}$$

Now, by Lemma 2.18, we know that there is a positive real number C such that for sufficiently large n $|y_n|_p, |x'_n|_p \leq C$, so

$$|x_n y_n - x'_n y'_n|_p \leq \max\left\{|(x_n - x'_n)y_n|_p, |x'_n(y'_n - y_n)|_p\right\} \leq C \cdot \max\left\{|x_n - x'_n|_p, |y'_n - y_n|_p\right\},$$

so again: since the right hand side tends to 0 as $n \to \infty$ so too does the left.

Absolute value: We must show that the absolute values of two equivalent sequences are the same, i.e. that $|(x_n)_n|_p = |(x'_n)_n|_p$. By Lemma 2.17 we know

$$\left|\,|x_n|_p - |x'_n|_p\,\right| \leq |x_n - x'_n|_p,$$

and so since the right hand side tends to 0 as $n \to \infty$ we have

$$|(x_n)_n|_p = \lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |x'_n|_p = |(x'_n)_n|_p,$$

as required.

Valuation: We must show that the valuations of two equivalent sequences are the same, i.e. that $v_p((x_n)_n) = v_p((x'_n)_n)$. By Lemma 2.18 and the claim for absolute values above we know that

$$p^{-v_p\left((x_n)_n\right)} = |(x_n)_n|_p = |(x'_n)_n|_p = p^{-v_p\left((x'_n)_n\right)}.$$

Hence $v_p((x_n)_n) = v_p((x'_n)_n)$. □

Excellent – we now have addition, multiplication, absolute value and valuation on $\mathbb{Q}_p$! We conclude by noting an important property: much like in $\mathbb{R}$, we can also divide in $\mathbb{Q}_p$.

Proposition 2.20. *Let $x \in \mathbb{Q}_p \setminus \{0\}$. Then there is an element $y \in \mathbb{Q}_p$ such that $xy = 1$.*

Proof. Let $(x_n)_n \in \mathscr{C}_p$ be a representative for x. Then as $x \neq 0$ we know that $\lim_{n\to\infty} |x_n|_p \neq 0$ and so by Lemma 2.18 there exists $N \geq 0$ such that for all $n \geq N$ the value of $|x_n|_p$ is the same (and not zero!). In particular, for all $n \geq N$ we at least have $x_n \neq 0$, and so has an inverse $1/x_n \in \mathbb{Q}$.

Consider the sequence $(y_n)_n$ defined by

$$y_n = \begin{cases} 1 & \text{if } n < N, \\ \frac{1}{x_n} & \text{if } n \geq N. \end{cases}$$

We then claim that the class of this sequence, $y = (y_n)_n \in \mathbb{Q}_p$, satisfies $xy = 1$. In other words, $(x_n y_n) \sim_p (1)_n$. Noting that

$$x_n y_n - 1 = \begin{cases} x_n & \text{if } n < N \\ 0 & \text{if } n \geq N. \end{cases}$$

In particular we get, $\lim_n \to \infty |x_n y_n - 1|_p = 0$ and so the claim holds. □

We summarise what we have shown now below.

Corollary 2.21. *The following are groups:*

- *$\mathbb{Q}_p$ with the addition operation $+$;*
- *$\mathbb{Q}_p^\times := \mathbb{Q}_p \setminus \{0\}$ with the multiplication operation $\cdot$.*

Proof. In both cases we have a binary operation which is associative by construction since it is given by the usual addition or multiplication on $\mathbb{Q}$ (which is associative) element-wise on Cauchy sequences. Thus we need only check the existence of identity elements and inverses. For addition, $0 \in \mathbb{Q}_p$ which is represented by the constant sequence $(0, 0, \dots)$ is the identity element, and for $x \in \mathbb{Q}_p$ represented by $(x_n)_n$ we define the (additive) inverse $-x \in \mathbb{Q}_p$ to be the class represented by $(-x_n)_n$. For multiplication, $1 \in \mathbb{Q}_p$ which is represented by the constant sequence $(1, 1, \dots)$ is the identity element and for $x \in \mathbb{Q}_p^\times$ there exists an inverse by Proposition 2.20. □

Remark 2.22. If you are familiar with this language, the above addition and multiplication endow $\mathbb{Q}_p$ with the structure of a field.

2.4 p-adic expansions

We will now interpret elements of $\mathbb{Q}_p$ more concretely, as p-adic expansions. This is in analogy to recovering decimal expansions from the Cauchy sequence definition of the real numbers. We begin by showing that for $(x_n)_n \in \mathscr{C}_p$, the p-adic expansions begin to converge as $n \to \infty$. More accurately, for each fixed precision M, if we go far enough along the sequence then the first M digits of the p-adic expansions become constant. This will allow us to define a p-adic expansion to which the sequence is approaching.

Lemma 2.23. *Let $(x_n)_n \in \mathscr{C}_p$, and let $x_n = \lim\limits_{N\to\infty}{}^{(p)} \sum_{k=v}^{N} a_{n,k}p^k$ be their p-adic expansions. Then for every $M \geq v$ there exists $T \geq 0$ such that for all $n, m \geq T$ and $v \leq k \leq M$,*

$$a_{n,k} = a_{m,k}.$$

Proof. Since the sequence is Cauchy, choose $T \geq 0$ such that for all $n, m \geq T$ we have $|x_n - x_m|_p \leq p^{-(M+1)}$. Assume that $a_{n,k} \neq a_{m,k}$ for some $v \leq k \leq M$. Then for all $N \geq M$, by the ultrametric inequality

$$\left|x_n - x_m - \sum_{k=v}^{N}(a_{n,k} - a_{m,k})p^k\right|_p = \max\left\{|x_n - x_m|_p, \left|\sum_{k=v}^{N}(a_{n,k} - a_{m,k})p^k\right|_p\right\} \geq p^{-M}.$$

In particular, as $N \to \infty$ this cannot go to 0. However, since we are using the p-adic expansions of x_n and x_m, if N is sufficiently large then we have

$$\begin{aligned}\left|x_n - x_m - \sum_{k=v}^{N}(a_{n,k} - a_{m,k})p^k\right|_p &\leq \max\left\{\left|x_n - \sum_{k=v}^{N} a_{n,k}p^k\right|_p, \left|x_m - \sum_{k=v}^{N} a_{m,k}p^k\right|_p\right\} \\ &< p^{-M},\end{aligned}$$

a contradiction. □

We then have the necessary tools to bring our discussion of p-adic numbers back to where it began – p-adic expansions. Indeed, we can approximate each $x \in \mathbb{Q}_p \setminus \{0\}$ by p-adic expansions which tend toward x.

Definition 2.24. A p-adic expansion is an expression $\sum_{k=v}^{\infty} a_k p^k$, where $(a_k)_{k\geq v}$ is a sequence of p-adic digits. Such an expression is a p-adic expansion for $x \in \mathbb{Q}_p$ if it converges to x, i.e.

$$\lim_{N\to\infty}\left|x - \sum_{k=v}^{N} a_k p^k\right|_p = 0.$$

We have p-adic expansions of rational numbers. Identifying rational numbers with their constant sequences, we obtain that these are an identical object here, and so will finally drop the notation $\lim\limits_{N\to\infty}{}^{(p)}$ since we are now working in $\mathbb{Q}_p$ where $\|\cdot\|$ is not defined and so there is only one available limit to us – the p-adic one.

At the start of this section, we showed that these expansions already give rise to a natural Cauchy sequence, to which we now show they converge.

Lemma 2.25. *p-adic expansions always converge to some $x \in \mathbb{Q}_p$.*

Proof. Let $\sum_{k=v}^{\infty} a_k p^k$ be a p-adic expansion, then consider the sequence of partial sums $\left(\sum_{k=v}^{v+n} a_k p^k\right)_n$. This is Cauchy by Lemma 2.3, so let $x \in \mathbb{Q}_p$ be the element represented by this sequence. For $N \geq 0$, using the ultrametric inequality,

$$\left| x - \sum_{k=v}^{N} a_k p^k \right|_p = \lim_{n\to\infty} \left| \sum_{k=v}^{v+n} a_k p^k - \sum_{k=v}^{N} a_k p^k \right|_p = \lim_{n\to\infty} \left| \sum_{k=N}^{n} a_k p^k \right|_p \leq p^{-N}.$$

Hence as $N \to \infty$, the sum converges to x. □

Now that we know that p-adic expansions are all elements of $\mathbb{Q}_p$, it remains to check that all elements of $\mathbb{Q}_p$ are given by a p-adic expansion. In fact, as for the p-adic expansions of rational numbers, these expansions are *unique* so that every $x \in \mathbb{Q}_p$ can be uniquely identified with one p-adic expansion.

Theorem 2.26. *For every $x \in \mathbb{Q}_p^\times$, there is a unique p-adic expansion $\sum_{k=v}^{\infty} a_k p^k$ which converges to x and has $a_v \neq 0$. For $x = 0$ the only p-adic expansion which converges to x is the trivial expansion with $a_k = 0$ for all k.*

Proof. For $x = 0$ this follows from uniqueness of the p-adic expansions of rational numbers, so we reduce to the case $x \in \mathbb{Q}_p^\times$. To see existence, we use Lemma 2.23. Indeed, let $(x_n)_n \in \mathscr{C}_p$ be a representative for x, and write $x_n = \sum_{k=v}^{\infty} a_{n,k} p^k$. Then let $v := v_p(x)$, and $a_k := \lim_{n\to\infty} a_{n,k}$, which exists by Lemma 2.23 since the sequences $(a_{n,k})_n$ are eventually constant as $n \to \infty$. We check that this is a p-adic expansion which converges to our x: for each $N \geq 0$

$$\left| x - \sum_{k=v}^{N} a_k p^k \right|_p = \lim_{n\to\infty} \left| x_n - \sum_{k=v}^{N} a_k p^k \right|_p = \lim_{n\to\infty} \left| \sum_{k=N}^{\infty} a_{n,k} p^k \right|_p \leq p^{-N}.$$

Taking the limit as $N \to \infty$ shows that this converges.

The proof of uniqueness is almost identical to the uniqueness for p-adic expansions of rational numbers in Proposition 1.18, and we leave it as an exercise to the reader. □

2.5 Working with the p-adic expansion

Now that we have p-adic expansions, we shall endeavour to distance ourselves from thinking about $\mathbb{Q}_p$ in terms of Cauchy sequences and instead work with $\mathbb{Q}_p$ in terms of these p-adic power series. There are a number of advantages to this, not least in the far simpler description of $\mathbb{Q}_p$ as this collection of formal power series in p:

$$\mathbb{Q}_p = \left\{ \sum_{k=v}^{\infty} a_k p^k \ : \ a_k \in \{0, \ldots, p-1\}, \ v \in \mathbb{Z} \right\}.$$

Of course, to labour the point a little, a power series corresponds to a Cauchy sequence (which is formally the element that the power series represents) via

$$\sum_{k=v}^{\infty} a_k p^k \longleftrightarrow \left(\sum_{k=v}^{v+n} a_k p^k \right)_n.$$

Our addition and multiplication of Cauchy sequences then just convert into addition and multiplication of power series. In other words, we can perform our arithmetic in $\mathbb{Q}_p$ with the p-adic expansions in a similar fashion to how it is done for decimal expansions in $\mathbb{R}$: working from the first term and making our way along the series.

Example 2.27. *Let's take $p = 5$ and consider the sum of, for example,*

$$\alpha = \sum_{k=-2}^{\infty} a_k 5^k = 5^{-2} + 5^{-1} + 3 \cdot 5^0 + 5^2 + 4 \cdot 5^3 + \cdots$$

and

$$\beta = \sum_{k=-1}^{\infty} b_k 5^k = 5^{-1} + 3 \cdot 5^0 + 5^1 + 3 \cdot 5^3 + \cdots .$$

Say that $\alpha + \beta = \sum_{k=-2}^{\infty} c_k 5^k$, then let us determine the first few c_k. Firstly, $c_{-2} = 1$, then summing the $k = -2$ digits gives $c_{-1} = 1 + 1 = 2$. When we reach the $k = 0$ we get $a_0 + b_0 = 3 + 3 = 1 + 1 \cdot 5$, and so we set $c_0 = 1$ and carry the extra digit over to the next k. For $k = 1$ we have $1 + a_1 + b_1 = 2$ and so $c_1 = 2$, with nothing to carry forward to $k = 2$. Continuing in this way we obtain

$$\sum_{k=-2}^{\infty} c_k p^k = 5^{-2} + 2 \cdot 5^{-1} + 5^0 + 2 \cdot 5^1 + 5^2 + 2 \cdot 5^3 + \ldots .$$

We can quite easily determine absolute values and valuations from these power series.

Lemma 2.28. *Let $x = \sum_{k=v}^{\infty} a_k p^k \in \mathbb{Q}_p$. Then*

$$v_p(x) = \begin{cases} \min\{k \ : \ a_k \neq 0\} & \text{if } x \neq 0, \\ \infty & \text{if } x = 0, \end{cases}$$
$$|x|_p = p^{-v_p(x)},$$

where, as always, we take $p^{-\infty} := 0$.

Proof. The claim for $|x|_p$ is just a restatement of part of Theorem 2.19, placed here for the readers convenience. For v_p we note that if $x = 0$ then the claim is immediate by definition. Else, by Lemma 1.20, the absolute values of the partial sum of the first n terms (once it is nonzero) is

$$v_p\left(\sum_{k=v}^{v+n} a_k\right) = \min\{k \ : \ a_k \neq 0\},$$

and so since $v_p(x) = \lim_{n\to\infty} v_p\left(\sum_{k=v}^{v+n} a_k\right)$, the claim holds. □

In fact it becomes much easier in this language to process the proofs of various results. For a start, let us verify that $|\cdot|_p$ and $v_p(\cdot)$ have the same properties on $\mathbb{Q}_p$ as on $\mathbb{Q}$. We now focus a little on the absolute value, whose properties over $\mathbb{Q}$ extend quite nicely to $\mathbb{Q}_p$ and will endow $\mathbb{Q}_p$ with the structure of a metric space.

Proposition 2.29. *For $x, y \in \mathbb{Q}_p$:*

(a) $v_p(x) = \infty$ *if and only if* $x = 0$*;*

(b) $v_p(xy) = v_p(x) + v_p(y)$*;*

(c) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$*, with equality if* $v_p(x) \neq v_p(y)$*.*

Consequently,

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

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

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

The last of these is called the ultrametric inequality.

Proof. By Lemma 2.28 we know $|\cdot|_p = p^{-v_p(\cdot)}$, and so the identities for $|\cdot|_p$ follow from those for $v_p(\cdot)$. Hence we only need to prove the $v_p(\cdot)$ identities. Firstly, (a) follows immediately from Lemma 2.28. Now consider the p-adic expansions $x = \sum_{k=v_p(x)}^{\infty} a_k p^k$ and $y = \sum_{k=v_p(y)}^{\infty} b_k p^k$. To prove (b) we multiply these together we obtain

$$\left(\sum_{k=v_p(x)}^{\infty} a_k p^k\right)\left(\sum_{k=v_p(y)}^{\infty} b_k p^k\right) = a_v b_w p^{v_p(x)+v_p(y)} + (\text{higher order terms}).$$

Since $p \nmid a_v b_w$, we thus have that this lower term above has a nonzero associate p-adic digit and so $v_p(xy) = v_p(x) + v_p(y)$. Finally, for (c), let $v = \min\{v_p(x), v_p(y)\}$ and extend the sequences of digits b_k or a_k by setting $b_k = 0$ or $a_k = 0$ for any k for which they were not yet defined. Then

$$v_p(x+y) = v_p\left(\sum_{k=v}^{\infty} a_k p^k + \sum_{k=v}^{\infty} b_k p^k\right) = v_p\left((a_v + b_v)p^v + (\text{higher order terms})\right).$$

It is clear immediately that $v_p(x+y) \geq v$. If $v_p(x) \neq v_p(y)$, then precisely one of a_v or b_v is nonzero, and so $a_v + b_v \not\equiv 0 \mod p$ and the expression $(a_v + b_v)$ in front of p^v above is already a nonzero p-adic digit. Hence $v_p(x+y) = v$. □

3 Some p-adic Analysis

We shall now consider some elementary analytic properties of $\mathbb{Q}_p$. We will begin by discussing convergence of sequences and series in $\mathbb{Q}_p$, before discussing power series. This will turn out to be far simpler than in real analysis!

From this point on, our sequences will be of elements in $\mathbb{Q}_p$, i.e. $(\alpha_n)_n$ where each $\alpha_n \in \mathbb{Q}_p$. This may require some mental separation from the previous section, since earlier we *defined* $\mathbb{Q}_p$ in terms of Cauchy sequences $(x_n)_n$ where $x_n \in \mathbb{Q}$, and so $(\alpha_n)_n$ is really (secretly) a sequence of sequences! Of course, we are doing our utmost to only think of $\mathbb{Q}_p$ as 'formal power series in p' via the p-adic expansion, but we must always remember the truth. Indeed, sometimes it is useful!

We will purposefully change our notation in this section to ease the mental transition: $(\alpha_n)_n$ will be used to refer to sequences of elements of $\mathbb{Q}_p$.

3.1 $\mathbb{Q}_p$ as a metric space

Let us now make formal what we mean when we talk about $\mathbb{Q}_p$ as a metric space. The metric on $\mathbb{Q}_p$ is the function $d_p(x, y) = |x - y|_p$. It is a worthwhile exercise to verify for yourself that this really is a metric, i.e. that it satisfies the metric space axioms. We leave this as an exercise, and suggest the reader make use of Proposition 2.29. Recall the following definitions from your metric space knowledge.

Definition 3.1. A sequence $(\alpha_n)_n$ of p-adic numbers is Cauchy if for every $\varepsilon > 0$ there exists an integer N such that for all $m, n > N$ we have

$$|\alpha_n - \alpha_m|_p < \varepsilon.$$

Note that a convergence sequence has to be Cauchy, a classical fact from the metric spaces course which is worth checking for yourself if you have forgotten! Ultimately it is our goal to show that conversely every Cauchy sequence converges in $\mathbb{Q}_p$. To make this precise we recall the idea of convergence here.

Definition 3.2. Let $(\alpha_n)_n$ be a sequence of p-adic numbers. Then we say $\lim_{n\to\infty} \alpha_n$ exists and is equal to some $\alpha \in \mathbb{Q}_p$ if for every $\varepsilon > 0$ there exists an integer N such that for all $n \geq N$

$$|\alpha - \alpha_n|_p < \varepsilon$$

Note that we already know that Cauchy sequences of elements in $\mathbb{Q} \subseteq \mathbb{Q}_p$ will converge to an element of $\mathbb{Q}_p$: namely the equivalence class of that Cauchy sequence! So what remains is to show that Cauchy sequences which are not all rational numbers still converge in $\mathbb{Q}_p$.

Theorem 3.3. *Let $(\alpha_n)_{n\geq 0}$ be a Cauchy sequence of elements of $\mathbb{Q}_p$. Then $\lim_{n\to\infty} \alpha_n$ exists in $\mathbb{Q}_p$.*

Proof. Our proof will proceed by constructing a Cauchy sequence $(x_n)_n \in \mathscr{C}_p$ of rational numbers such that that its equivalence class $\alpha \in \mathbb{Q}_p$ is the limit of the α_n. Note that if $(x_n)_n \in \mathscr{C}_p$ is a Cauchy sequence of rational numbers, then in $\mathbb{Q}_p$ we have $\lim_{n\to\infty} x_n$ exists and is the equivalence class of $(x_n)_n$.

Let $\alpha_n = \sum_{k=v_p(\alpha_n)}^{\infty} a_{n,k}p^k$ be the p-adic expansion of each element in our sequence. Let us define, for each $n \geq 0$, the element

$$x_n := \sum_{k=v_p(\alpha_n)}^{n} a_{n,k}p^k,$$

to be the terms up to the nth the p-adic expansion of α_n. Note that by definition $|\alpha_n - x_n|_p \leq p^{-n}$.
Claim: $(x_n)_n$ is a Cauchy sequence of rational numbers.
Proof: Clearly each $x_n \in \mathbb{Q}$, since it is a finite sum of rational numbers. Let $\varepsilon > 0$, and choose $N > 0$ such for all $n, m \geq N$ we have $|\alpha_n - \alpha_m|_p < \varepsilon$. Enlarging N, which preserves the previous property, we may assume that also $p^{-N} < \varepsilon$. Then for all $n, m \geq N$, using the ultrametric inequality we have

$$\begin{aligned} |x_n - x_m|_p &= |x_n - \alpha_n + \alpha_n - \alpha_m + \alpha_m - x_m|_p \\ &\leq \max\left\{|x_n - \alpha_n|_p, |\alpha_n - \alpha_m|_p, |\alpha_m - x_m|_p\right\} \\ &\leq \max\left\{p^{-n}, \varepsilon, p^{-m}\right\} \\ &< \varepsilon. \end{aligned}$$

so $(x_n)_n$ is a Cauchy sequence. □

Now that we have this Cauchy sequence, we show that its limit is precisely that of our sequence $(\alpha_n)_n$. Let $\alpha \in \mathbb{Q}_p$ be the equivalence class of $(x_n)_n$, let $\varepsilon > 0$. Choose $N > 0$ such that for all $n \geq N$ we have $|x_n - \alpha|_p < \varepsilon$. Possibly enlarging N, we additionally assume that $p^{-N} < \varepsilon$. Then, similarly to in the proof of the claim, we have for all $n \geq N$

$$|\alpha_n - \alpha|_p \leq \max\left\{|\alpha_n - x_n|_p, |x_n - \alpha|_p\right\} < \varepsilon.$$

Hence $\lim_{n\to\infty} \alpha_n$ exists and is equal to α. □

Comparison 3.4

You may recall from your metric spaces course that this property is known as *completeness*. In those words, our theorem says that $\mathbb{Q}_p$ is a *complete* metric space. Similarly, in real analysis $\mathbb{R}$ is complete with respect to the usual metric where the distance between x and y is $\|x - y\|$.

3.2 Sequences and series in $\mathbb{Q}_p$

We begin by asking: when is a sequence $(\alpha_n)_n$ of elements $\alpha_n \in \mathbb{Q}_p$ convergent in $\mathbb{Q}_p$? In the real numbers this is a delicate question, however in $\mathbb{Q}_p$ it is far easier! Indeed, in the definition of Cauchy we need only check the situation where $m = n + 1$.

Lemma 3.5. *A sequence $(\alpha_n)_n$ of p-adic numbers is Cauchy if and only if* $\lim_{n\to\infty}(\alpha_{n+1} - \alpha_n) = 0$.

Proof. If $(\alpha_n)_n$ is Cauchy then for every $\varepsilon > 0$ we can find $N > 0$ such that for all $n, m \geq N$ we have $|\alpha_m - \alpha_n|_p < \varepsilon$. In particular, when $m = n + 1$ we have for all $n \geq N$ that $|\alpha_{n+1} - \alpha_n|_p < \varepsilon$, and so by definition $\lim_{n\to\infty} |\alpha_{n+1} - \alpha_n|_p = 0$.

Conversely, let $\varepsilon > 0$. Then since $\lim_{n\to\infty} |\alpha_{n+1} - \alpha_n|_p = 0$, we choose $N > 0$ such that for all $n \geq N$ we have $|\alpha_{n+1} - \alpha_n|_p < \varepsilon$. Now let $m, n \geq N$, and assume that $m > n$. The ultrametric inequality shows

$$\begin{aligned} |\alpha_m - \alpha_n|_p &= |\alpha_m - \alpha_{m-1} + \alpha_{m-1} - \cdots - \alpha_{n+1} + \alpha_{n+1} - \alpha_n|_p \\ &\leq \max\left\{ |\alpha_{n+k+1} - \alpha_{n+k}|_p \ : \ 0 \leq k \leq m-n-1 \right\}. \end{aligned}$$

By our assumption, all of the $|\alpha_{n+k+1} - \alpha_{n+k}|_p < \varepsilon$ and so $|\alpha_m - \alpha_n|_p < \varepsilon$. □

Comparison 3.6

Our use of the ultrametric inequality was very much necessary here – this claim is not true in $\mathbb{R}$! For example: if $a_n = \sqrt{n}$ then clearly this sequence is not Cauchy in the real numbers since $a_n \to \infty$ as $n \to \infty$. However,

$$a_{n+1} - a_n = \sqrt{n+1} - \sqrt{n} = \frac{1}{\sqrt{n+1} + \sqrt{n}} \leq \frac{1}{2\sqrt{n}}$$

which goes to 0 as $n \to \infty$.

This lemma makes much of our p-adic analysis more pleasant than real analysis! Let us now consider infinite series $\sum_{n=1}^{\infty} \alpha_n$, when do these converge? Intuitively we expect that we at least need the $\alpha_n \to 0$ as $n \to \infty$ since we cannot keep adding large things to our sum and expect it to stop growing! In real analysis we learned that this was not sufficient to ensure convergence, and the situation was somewhat delicate. However, in the p-adic world this intuitive expectation is not just necessary but sufficient for convergence!

Proposition 3.7. *Let $(\alpha_n)_{n=0}^{\infty}$ be a sequence of p-adic numbers. Then the sum $\sum_{n=0}^{\infty} \alpha_n := \lim_{N\to\infty} \sum_{n=0}^{N} \alpha_n$ converges in $\mathbb{Q}_p$ if and only if $\lim_{n\to\infty} \alpha_n = 0$.*

Proof. Let $s_N := \sum_{n=0}^{N-1} \alpha_n$ be the Nth partial sum. Then by Theorem 3.3 the sequence $(s_n)_{n\geq 0}$ converges if and only if it is Cauchy, which by Lemma 3.5 is equivalent to $0 = \lim_{n\to\infty}(s_{n+1} - s_n)$. Since $\alpha_n = s_{n+1} - s_n$, the result is holds. □

Example 3.8. *The series $\sum_{n=1}^{\infty} np^n$ converges, since $|np^n|_p \leq p^{-n} \to 0$ as $n \to \infty$.*

Example 3.9. *The series $\sum_{n=1}^{\infty} n!$ converges since we have seen in the exercise sheets that $v_p(n!) \geq \left\lfloor \frac{n}{p} \right\rfloor$, so*

$$|n!|_p \leq p^{-\lfloor n/p \rfloor} \leq p^{1-(n/p)}.$$

Again, this tends to 0 as $n \to \infty$ so the series converges.

Example 3.10. *The series $\sum_{n=1}^{\infty} n$ does not converge in $\mathbb{Q}_p$. Indeed, the sequence $\alpha_n = n$ does not tend to 0 since there is the subsequence $\beta_n = np + 1$ which always has absolute value $|\beta_n|_p = 1$. Similarly, $\sum_{n=1}^{\infty} \frac{1}{n}$ does not converge.*

3.3 Power series on $\mathbb{Q}_p$ (non-examinable)

A familiar concept from calculus is that of a power series: an infinite series $F(X) = \sum \alpha_n X^n$ in one variable X. In real analysis we study these and their radii of convergence – the locus of X on which $F(X)$ converges. This provides an interesting family of functions with useful properties. Similarly we can consider power series over $\mathbb{Q}_p$, and study where these functions are well defined. Since the convergence of series is markedly simpler in $\mathbb{Q}_p$, it will come as no surprise that these behave very well!

Before discussing the radius of convergence, we will need to remember the notion of a limit superior (denoted lim sup) of a sequence of real numbers. If you do not remember, see Definition A.1!

Definition 3.11. Let $F(X) = \sum_{n=0}^{\infty} \alpha_n X^n$ where $\alpha_n \in \mathbb{Q}_p$, be a power series over the p-adic numbers. The radius of convergence of F is defined to be

$$r := \frac{1}{\limsup_{n\to\infty} |\alpha_n|_p^{1/n}}.$$

The radius of convergence, much like in real analysis, does what it says on the tin: the power series converges inside of its radius of convergence and diverges outside of it.

Proposition 3.12. *Let $F(X) = \sum_{n=0}^{\infty} \alpha_n X^n$, where $\alpha_n \in \mathbb{Q}_p$, be a power series over the p-adic numbers, and let r denote its radius of convergence. Then the following hold for $x \in \mathbb{Q}_p$:*

- *$F(x)$ converges when $|x|_p < r$; and*
- *$F(x)$ diverges when $|x|_p > r$; and*
- *if there is an $x_0 \in \mathbb{Q}_p$ with $|x_0|_p = r$ such that $F(x_0)$ converges (resp. diverges) then in fact $F(x)$ converges (resp. diverges) for all $x \in \mathbb{Q}_p$ with $|x|_p = r$.*

Proof (non-examinable). Let us write $\alpha^+ := \limsup_{n\to\infty} |\alpha_n|_p^{1/n}$, so that $r := 1/\alpha^+$, and by the definition of limsup we know the following.

(i) For every $\varepsilon > 0$ there exists an integer N such that for all $n > N$ we have $|\alpha_n|_p^{1/n} < \alpha^+ + \varepsilon$.

(ii) For every $\varepsilon > 0$ and every integer N there exists an integer $n > N$ with $|\alpha_n|_p^{1/n} > \alpha^+ - \varepsilon$.

Case $|x|_p < 1/\alpha^+$: In this setting, by Proposition 3.7 we must show that $|\alpha_n x^n|_p \to 0$ as $n \to \infty$. We make the following claim

Claim: *There exist constants $\delta, N > 0$ such that for all $n \geq N$ we have $|\alpha_n|_p^{1/n} |x|_p \leq (1-\delta)$.*
If the claim holds then as $n \to \infty$ we have

$$|\alpha_n x^n|_p = \left(|\alpha_n|_p^{1/n} |x|_p\right)^n \leq (1-\delta)^n \to 0.$$

Hence it remains in this case to prove the claim.
Proof of claim: Since $|x|_p < 1/\alpha^+$ then there exists $\gamma > 0$ such that have $|x|_p \leq (1-\gamma)/\alpha^+$. By (i) (with $\varepsilon = \gamma\alpha^+$) we can choose $N \in \mathbb{Z}$ such that for $n > N$ we have $|\alpha_n|_p^{1/n} < \alpha^+(1+\gamma)$. Putting this together, we obtain

$$|\alpha_n|_p^{1/n} |x|_p < (1-\gamma^2).$$

Hence setting $\delta = \gamma^2$ we obtain the claim. □

Case $|x|_p > 1/\alpha^+$**:** In this setting, by Proposition 3.7 we must show that $|\alpha_n x^n|_p \not\to 0$ as $n \to \infty$. We make the following claim.

Claim: *There exists a constant δ such that there are infinitely many $n > 0$ with $|\alpha_n|_p^{1/n} |x|_p \geq (1+\delta)$.* If the claim holds then for infinitely many n we have $|\alpha_n x^n|_p \geq (1+\delta)^n > 1$ and so $|\alpha_n x^n|_p \not\to 0$ as $n \to \infty$. Hence it remains to prove the claim.

Proof of claim: Since $|x|_p > 1/\alpha^+$ there exists $\gamma > 0$ such that $|x|_p \geq (1+\gamma)/\alpha^+$. By (ii) we know that for every $\varepsilon > 0$ there are infinitely many n such that $|\alpha_n|_p^{1/n} > \alpha^+(1-\varepsilon)$. Combining these estimates we obtain that for every $\varepsilon > 0$ there are infinitely many n such that

$$|\alpha_n|_p^{1/n} |x|_p > (1+\gamma)(1-\varepsilon).$$

Choosing ε to be very small, we obtain $(1+\gamma)(1-\varepsilon) > 1$, and so there exists such a δ.

Case: $|x|_p = 1/\alpha^+$ By Proposition 3.7 the series converges for such x if and only if

$$\lim_{n\to\infty} |a_n x^n|_p = \lim_{n\to\infty} |a_n|_p (1/\alpha^+)^n = 0.$$

Clearly, this condition holds for one x if and only if it holds for all such x. □

Example 3.13. *Consider the power series $f(X) = \sum_{n=1}^{\infty} (-1)^n X^n$. Since $|-1|_p^{1/n} = 1$ we have radius of convergence equal to 1. Hence $f(X)$ converges when $|x|_p < 1$. Moreover, if we take $x_0 = -1$ then we have for all n that*

$$|(-1)^n x_0^n|_p = 1,$$

so $f(x_0)$ diverges by Proposition 3.7. Thus by Proposition 3.12 the power series $f(X)$ diverges for all x with $|x|_p \geq 1$.

Example 3.14. *The (p-adic) logarithm on $\mathbb{Q}_p$ is defined by the power series*

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

The radius of convergence is 1, since we have a bound

$$\left| \frac{(-1)^{n+1}}{n} \right|_p^{1/n} = p^{v_p(n)/n} \leq 1$$

where this inequality is an equality infinitely often (for example, whenever $n = kp+1$ for some integer k).

4 Algebra over $\mathbb{Q}_p$

We will now consider the p-adic numbers as algebraists, giving a precise notion of reduction modulo powers of p (where this can be defined!) and solving polynomial equations in $\mathbb{Q}_p$. The former of these will be a useful tool in studying the latter.

In number theory more broadly, it is a fundamental goal to understand the rational number solutions to polynomial equations. For example, Fermat's last theorem (famously proved by Andrew Wiles in 1995) postulates that if $n \geq 3$ then the only solutions (x, y, z) to the polynomial equation

$$x^n + y^n = z^n,$$

are the ones where $x = 0$, $y = 0$, or $z = 0$.

There are many situations where we'd like to show that there are just no solutions. One thing we can do is check whether there are solutions over $\mathbb{Q}_p$, which will turn out to be easier to do, and if there are none then this rules out the possibility of having any over $\mathbb{Q}$

Comparison 4.1

Consider the equation $x^2 + 1 = 0$. We can see that this does not have a solution $x \in \mathbb{Q}$ because it does not even have one in $\mathbb{R}$! In this section we shall find analogues of this in the p-adic world.

4.1 The p-adic integers

We now introduce an important subspace of $\mathbb{Q}_p$: the p-adic integers $\mathbb{Z}_p$. These are to $\mathbb{Q}_p$, what the usual integers ($\mathbb{Z}$) are to $\mathbb{Q}$.

Definition 4.2. The p-adic integers are the unit disc in $\mathbb{Q}_p$:

$$\mathbb{Z}_p := \left\{ x \in \mathbb{Q}_p \ : \ |x|_p \leq 1 \right\}.$$

The reader may, quite rightly, be wondering: why are we calling these 'integers'? Well, if we think of $\mathbb{Z}$ as the rational numbers whose denominator is 1 then $\mathbb{Z}_p$ is the p-centric version of this where we only care about whether there is a p in the denominator. In fact, by Lemma 2.28 we could equivalently define $\mathbb{Z}_p$ as the set p-adic numbers whose p-adic expansion starts on or after 0.

$$\mathbb{Z}_p := \left\{ \sum_{k=0}^{\infty} a_k p^k \in \mathbb{Q}_p \ : \ a_k \in \{0, \ldots, p-1\} \ \forall k \geq 0 \right\},$$

since $|x|_p = p^{-v_p(x)} \leq 1$ is equivalent to $v_p(x) \geq 0$ and $v_p(x)$ is the index where the first nonzero p-adic digit of x occurs. We first observe, as an example, that $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Example 4.3. *Let $x \in \mathbb{Z}$ be an integer, then immediately $x \in \mathbb{Z}_p$ since $v_p(x) \geq 0$ for every p!*

The notation might lead you to expect that $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}$, but beware that this is false! For example, if p is an odd prime then $1/2 \in \mathbb{Z}_p$ since $v_p(1) = v_p(2) = 0$ so $|1/2|_p = p^0 = 1$, but $1/2 \notin \mathbb{Z}$. More generally, we can see from the definition of v_p that

$$\mathbb{Q} \cap \mathbb{Z}_p = \left\{ \frac{a}{b} \in \mathbb{Q} \ : \ p \nmid b \right\}.$$

Our operations on $\mathbb{Q}_p$ restrict to operations on $\mathbb{Z}_p$. That is, sums and products of p-adic integers are themselves p-adic integers.

Lemma 4.4. *The p-adic integers, $\mathbb{Z}_p$, form a subgroup of $(\mathbb{Q}_p, +)$ and moreover for every $x, y \in \mathbb{Z}_p$ we have $xy \in \mathbb{Z}_p$.*

Proof. To get that this is a subgroup, note that $|0|_p = 0 \leq 1$ and for $x, y \in \mathbb{Z}_p$ we have $|-x|_p = |x|_p \leq 1$ and $|x+y|_p \leq \max\left\{|x|_p, |y|_p\right\} \leq 1$ so $\mathbb{Z}_p$ is closed under inverses and sums and hence a subgroup. The second claim is immediate since $|xy|_p = |x|_p |y|_p \leq 1$. □

Remark 4.5. If you are familiar with the language, then $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.

Thinking back to when we discussed (and constructed) p-adic expansions, these are precisely the kind of numbers we expect to be able to 'reduce mod p' by just truncating the p-adic expansions. Indeed, this is not a hazy concept but a well defined one!

Proposition 4.6. *For every integer $r \geq 1$, there are well defined reduction mod p^r maps*

$$\begin{aligned} \bar{\cdot} : \mathbb{Z}_p &\to \mathbb{Z}/p^r\mathbb{Z} \\ x = \sum_{k=0}^{\infty} a_k p^k &\mapsto \overline{x} := \sum_{k=0}^{r-1} a_k p^k. \end{aligned}$$

Moreover, $\overline{x+y} \equiv \overline{x} + \overline{y}$ and $\overline{xy} = \overline{x}\,\overline{y}$. We often just write $x \equiv \overline{x} \mod p^r$ in the same way as we do for reduction of the integers mod p^r.

Proof. Since p-adic expansions are unique, this is well defined. Moreover, we can see that the operations are identical on either side. □

Remark 4.7. In particular, these reduction maps are homomorphisms of groups $(\mathbb{Z}_p, +) \to (\mathbb{Z}/p^k\mathbb{Z}, +)$. Indeed, if this is familiar to you, they are homomorphisms of rings.

Note that the kernels of these reduction maps are the natural thing: the multiples of p^r.

Lemma 4.8. *Let $r \geq 1$ be an integer. Then the kernel of the reduction map $\mathbb{Z}_p \to \mathbb{Z}/p^r\mathbb{Z}$ is*

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

Proof. If $v_p(x) \geq r$ then $x = p^r x'$ for some $x' \in \mathbb{Z}_p$. We then reduce and obtain

$$x \equiv p^r x' \equiv 0 \mod p^r.$$

Conversely, if $x \equiv 0 \mod p^r$, then by definition $x = 0 + \sum_{k=r}^{\infty} a_k p^k$, so $v_p(x) \geq r$. □

These reduction maps will turn out to be a great ally in solving polynomial equations! For a start, roots in $\mathbb{Z}_p$ reduce mod p^r to roots in $\mathbb{Z}/p^r\mathbb{Z}$, so if there are no roots in the latter then we certainly can't have any in the former. Let us see an example of this.

Example 4.9. *Let $f(X) = X^2 + 3$, we want to know if $f(X)$ has roots in $\mathbb{Q}_5$.*

Let us begin by asking a restricted question: does it have roots in $\mathbb{Z}_5$? Say that it does, so there is some $\alpha \in \mathbb{Z}_5$ such that $\alpha^2 + 3 = 0$. Reducing mod 5, we obtain that the reduction $\overline{\alpha} \in \mathbb{Z}/5\mathbb{Z}$ satisfies

$$\overline{\alpha}^2 \equiv 2 \mod 5.$$

However, we can quickly check that the squares modulo 5 are $0, 1$, and 4, so this $\overline{\alpha}$ (and hence this α) cannot exist. Thus f has no roots in $\mathbb{Z}_5$.

Now let us return to the bigger question: are there roots in $\mathbb{Q}_5$? Well let us assume that $\alpha \in \mathbb{Q}_5$ is a root. We have shown that α is not a 5-adic integer, so we must have $v_5(\alpha) < 0$. However, using the ultrametric inequality

$$v_5(\alpha^2 + 3) \geq \min\left\{v_5(\alpha^2), v_5(3)\right\} = \min\left\{2v_5(\alpha), 0\right\} = 2v_5(\alpha)$$

with equality if $2v_5(\alpha) \neq 0$, which is true by our assumption! However now we are in a spot of bother:

$$\infty = v_5(0) = v_5(\alpha^2 + 3) = 2v_5(\alpha),$$

which is a contradiction since we assumed that $v_5(\alpha) < 0$. Hence $f(X)$ has no roots in $\mathbb{Q}_5$.

There were two 'steps' in the example above: showing that the polynomial has no roots in $\mathbb{Z}_p$, and then showing that every $\mathbb{Q}_p$ root lies in $\mathbb{Z}_p$. A mathematician with a plan would probably prove the second step first, to reduce the set they need to search for roots in, and then perform the first step to show that there are no roots there. But we were out exploring and happened upon these facts by chance, so such planning could not have been done!

The second step in Example 4.9, showing that the roots in $\mathbb{Q}_p$ were actually in $\mathbb{Z}_p$ is also very general, as we will shortly show. Firstly, a useful definition.

Definition 4.10. A polynomial $f(X) = \alpha^d X^d + \alpha_{d-1}X^{d-1} \cdots + \alpha_0$ is said to be monic if the leading term has coefficient $\alpha_d = 1$.

Note that the roots of a non-monic polynomial of degree d, $f(X) = \alpha^d X^d + \alpha_{d-1}X^{d-1} \cdots + \alpha_0$ are the same as those of $\frac{1}{\alpha_d} f(X)$ which is a monic polynomial of degree d. So we can always work with monic polynomials if we wish.

Proposition 4.11. *Let $f(X) = X^d + \alpha_{d-1}X^{d-1} + \cdots + \alpha_0$ be a monic polynomial whose coefficients $\alpha_0, \ldots, \alpha_{d-1}$ are all in $\mathbb{Z}_p$. Assume that $\beta \in \mathbb{Q}_p$ is a root of f. Then $\beta \in \mathbb{Z}_p$.*

Proof. The proof proceeds similarly to the previous example. Let us assume for a contradiction that $v_p(\beta) < 0$ (equivalently, that $v_p(\beta) \leq -1$).

Firstly, $v_p(\beta^d) = dv_p(\beta)$.

Secondly,

$$v_p\left(\alpha_{d-1}\beta^{d-1} + \cdots + \alpha_0\right) \geq \min\left\{\alpha_i\beta^i \ : \ i \in \{0, \ldots, d-1\}\right\}.$$

Since each $\alpha_i \in \mathbb{Z}_p$ we have $v_p(\alpha_i\beta^i) = v_p(\alpha_i) + iv_p(\beta) \geq iv_p(\beta)$ and so the least that the min above can be is $(d-1)v_p(\beta)$.

Thirdly, since $v_p(\beta) < 0$, we have $dv_p(\beta) < (d-1)v_p(\beta)$ and so by the ultrametric inequality

$$\infty = v_p(0) = v_p\left(\beta^d + \left(\alpha_{d-1}\beta^{d-1} + \cdots + \alpha_0\right)\right) = dv_p(\beta),$$

so we have reached a contradiction. □

This idea of checking whether a polynomial has roots modulo p^k, which was the second step in Example 4.9, is in fact even stronger than it first appears. It is not just necessary but sufficient, in the sense of the lemma below.

Proposition 4.12. *Let $f(X)$ be a polynomial with coefficients in $\mathbb{Z}_p$. Let $y \in \mathbb{Z}_p$. Then $f(y) = 0$ if and only if $f(y) \equiv 0 \mod p^k$ for all $k \geq 1$.*

Proof. Clearly, if $f(y) = 0$ then it is zero modulo all powers of p. Conversely, recall that the kernel of the reduction mod p^k map is the set of integers $x \in \mathbb{Z}_p$ with $v_p(x) \geq k$. In particular, if $f(y) \equiv 0 \mod p^k$ then $v_p(f(y)) \geq k$. Since this holds for all k, we have $v_p(f(y)) = \infty$ and so $f(y) = 0$. □

Combining the steps we arrive at a useful theorem, which substantially generalises Example 4.9.

Theorem 4.13. *Let $f(X)$ be a monic polynomial with coefficients in $\mathbb{Z}_p$, and let $y \in \mathbb{Q}_p$. Then $f(y) = 0$ if and only if both $y \in \mathbb{Z}_p$ and $f(y) \equiv 0 \mod p^k$ for all $k \geq 1$.*

Proof. This is immediate from Propositions 4.11 and 4.12. □

Example 4.14. *If we are given a polynomial which has a coefficient in $\mathbb{Q}_p$ but not $\mathbb{Z}_p$ then what can we do? Well we can certainly re-arrange! Consider $f(X) = x^2 + \frac{1}{2}$ over $\mathbb{Q}_2$. The roots of f are the same as those of $4f$, so we can instead ask if $4f(x) = 4x^2 + 2$ has a root. But now we can perform the substitution $x := u/2$ to obtain the equation $g(u) = u^2 + 2$, and note that the roots of $g(u)$ are in bijection with those of f via $u \mapsto 2x$. Hence we can now check for roots by considering $g(u)$, which does satisfy our hypotheses above and so we can try to rule out roots by looking mod p.*

4.2 Solving Equations

We have so far seen that reduction modulo p (or its powers) can be used to rule out the existence of roots of polynomials, but what if the polynomial does have a root mod p? The p-adic numbers have a wonderful property: often we can go the other way! That is, given a nice enough root modulo p, we can lift it back to a root in $\mathbb{Z}_p$! Of course, this is not something we could do in $\mathbb{Q}$, as we see in the example below.

Example 4.15. *The polynomial $f(X) = X^2 - 2$ has no roots in $\mathbb{Q}$ but does have roots in $\mathbb{Z}_7 \subseteq \mathbb{Q}_7$, as we will see in the exercise class.*

The result which allows us to 'lift' roots modulo p to ones in $\mathbb{Z}_p$ is known as Hensel's lemma, and is an important and useful tool in p-adic algebra. The sorts of roots that we will be able to deal with are so-called simple roots.

Definition 4.16. Let $f(X)$ be a polynomial over $\mathbb{Q}_p$, and let $f'(X) = \frac{d}{dX} f(X)$ denote its derivative. Then we say that $y \in \mathbb{Q}_p$ is a *simple root* of f if both $f(y) = 0$ and $f'(y) \neq 0$.

Exercise 4.17. *One can alternatively characterise a simple root y as one which occurs with multiplicity 1 in $f(X)$, i.e. that $f(X) = (X-y)g(X)$ with $g(y) \neq 0$. Check that these two definitions are equivalent!*

Theorem 4.18 (Hensel's Lemma)**.** *Let $f(X)$ be a monic polynomial with coefficients in $\mathbb{Z}_p$. Assume that there exists $\alpha \in \mathbb{Z}_p$ such that*

- $|f(\alpha)|_p < 1$ *(equivalently, $f(\alpha) \equiv 0 \mod p$)*
- $|f'(\alpha)|_p = 1$ *(equivalently, $f'(\alpha) \not\equiv 0 \mod p$)*

Then there is a unique element $y \in \mathbb{Z}_p$ such that $f(y) = 0$ and $y \equiv \alpha \mod p$. Moreover, y is a simple root of f.

Proof of Hensel's lemma (Theorem 4.18). The proof proceeds via the so-called *Newton-Raphson algorithm*. Taking α as in the theorem statement, we define a sequence $(\alpha_k)_{k\geq 0}$ of p-adic numbers:

$$\begin{aligned} \alpha_0 &:= \alpha; \\ \alpha_{k+1} &:= \alpha_k - \frac{f(a_k)}{f'(a_k)} \qquad\qquad \forall k \geq 0. \end{aligned}$$

We will show that the sequence $(\alpha_k)_{k\geq 0}$ converges to a root of f, and the theorem will follow. To do this we will need a small lemma.

Lemma 4.19. *For all $k \geq 0$ we have $|f'(\alpha_k)|_p = 1$ and $|f(\alpha_k)|_p \leq \frac{1}{p^{2^k}}$.*

Assuming that Lemma 4.19 is true, then

$$|\alpha_{k+1} - \alpha_k|_p = \left|\frac{f(\alpha_k)}{f'(\alpha_k)}\right|_p \leq \frac{1}{p^{2^k}}. \tag{3}$$

Since this goes to 0 as $k \to \infty$, by Lemma 3.5 the sequence $(\alpha_k)_{k\geq 0}$ is Cauchy and so by Theorem 3.3 converges to an element $y = \lim_{k\to\infty} \alpha_k \in \mathbb{Q}_p$. We further claim that $y \in \mathbb{Z}_p$. Indeed, if not then $|y|_p > 1$ and by the ultrametric inequality we have for all k that $|y - \alpha_k|_p = |y|_p$. But by the definition of convergence this would mean that $1 < |y|_p < \varepsilon$ for all $\varepsilon > 0$, a contradiction. Thus we have $y \in \mathbb{Z}_p$. Also, by (3) we have $y \equiv \alpha_k \mod p^{2^k}$ for all k, and so

$$f(y) \equiv f(\alpha_k) \equiv 0 \mod p^{2^k},$$

so $f(y) \equiv 0 \mod p^r$ for all $r \geq 0$. Thus by Proposition 4.12 $f(y) = 0$.

The root y is unique and simple since, if it were not, then we would have $f(X) \equiv (X-\alpha)^2 g(X) \mod p$ for some polynomial $g(X)$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$. By the product rule we'd then have $f'(X) \equiv 2(X-\alpha)g(X) + (X-\alpha)^2 g'(X)$. In particular, $f'(\alpha) \equiv 0 \mod p$, which contradicts our initial hypotheses in the theorem statement.

Thus Hensel's lemma holds, so long as Lemma 4.19 is true. We now prove that this is indeed the case.

Proof of Lemma 4.19. We prove this by induction. For $k = 0$ this is simply the hypothesis of the theorem. Assuming then that it is true for $k \geq 0$, we proceed.

Firstly, by our inductive hypothesis $f(\alpha_k)/f'(\alpha_k) \equiv 0 \mod p$, so

$$\alpha_{k+1} = \alpha_k - \frac{f(\alpha_k)}{f'(\alpha_k)} \equiv \alpha_k \equiv \alpha \mod p.$$

Secondly, using this,

$$f'(\alpha_{k+1}) \equiv f'(\alpha) \not\equiv 0 \mod p.$$

In particular, since it is an integer, $|f'(\alpha_{k+1})|_p = 1$. Finally, we must show $f(\alpha_{k+1}) \equiv 0 \mod p^{2^{k+1}}$. We take the Taylor expansion (defined in the usual way) of $f(X)$ about the point α_k, so that

$$f(X) = f(\alpha_k) + (X - \alpha_k)f'(\alpha_k) + (X - \alpha_k)^2 G(X),$$

for some polynomial $G(X)$ over $\mathbb{Z}_p$. Setting $X = \alpha_{k+1}$ we see

$$\begin{aligned} f(\alpha_{k+1}) &= f(\alpha_k) + (\alpha_{k+1} - \alpha_k)f'(\alpha_k) + (\alpha_{k+1} - \alpha_k)^2 G(\alpha_{k+1}) \\ &= f(\alpha_k) + \left(-\frac{f(\alpha_k)}{f'(\alpha_k)}\right) f'(\alpha_k) + \left(-\frac{f(\alpha_k)}{f'(\alpha_k)}\right)^2 G(\alpha_{k+1}) \\ &= \left(\frac{f(\alpha_k)}{f'(\alpha_k)}\right)^2 G(\alpha_{k+1}). \end{aligned}$$

Hence $v_p\left(f(\alpha_{k+1})\right) = v_p\left(\left(\frac{f(\alpha_k)}{f'(\alpha_k)}\right)^2 G(\alpha_{k+1})\right) \geq 2v_p\left(f(\alpha_k)\right) \geq 2 \cdot 2^k = 2^{k+1}$, so the claim follows. □

□

Example 4.20. *Hensel's lemma shows that $f(X) = X^2 - 2$ has roots in $\mathbb{Z}_7$. Indeed, the derivative is $f'(X) = 2X$, so if $\alpha = 3$ then we have*

$$\begin{aligned} f(\alpha) &\equiv 0 \mod 7 \\ f'(\alpha) &= 6 \not\equiv 0 \mod 7. \end{aligned}$$

Hensel's lemma shows that there is a unique $\beta \in \mathbb{Z}_p$ with $f(\beta) = 0$ and $\beta \equiv 3 \mod 7$.

Corollary 4.21. *Assume p is an odd prime number. Then $\mathbb{Q}_p$ contains a root of unity of order $p-1$, i.e. there is an element $\zeta \in \mathbb{Q}_p$ such that $\zeta^k \neq 1$ for all $1 \leq k \leq p-2$ and $\zeta^{p-1} = 1$.*

Proof. Recall that $\mathbb{Z}/p\mathbb{Z}^\times$ is a cyclic group of order $p-1$. Let $n \in \{1, \ldots, p-1\}$ be such that $n \mod p$ generates $\mathbb{Z}/p\mathbb{Z}^\times$ (i.e. a primitive element).

Note that if $f(X) := X^{p-1} - 1$ then $f(n) \equiv 0 \mod p$, and moreover $f'(n) = (p-1)n \neq 0$ so by Hensel's lemma there is an element $\zeta \in \mathbb{Z}_p$ with $\zeta^{p-1} = 1$ and $\zeta \equiv n \mod p$. Since n reduces to a generator of $\mathbb{Z}/p\mathbb{Z}^\times$, $n^k \not\equiv 1 \mod p$ for all $1 \leq k \leq p-2$. In particular, for such k, $\zeta^k \equiv n^k \not\equiv 1 \mod p$, so $\zeta^k \neq 1$. □

Comparison 4.22

Corollary 4.21 shows that $\mathbb{Q}_p$ has $(p-1)$th roots of unity! This is markedly different from the real numbers where the only roots of unity are ± 1!

4.3 Irreducibility

So far we have considered how to determine how many roots a polynomial has. On the opposite side of the spectrum, there is the notion of irreducibility: that a polynomial does not factor into any smaller pieces, even non-linear ones!

Definition 4.23. Say a polynomial is irreducible if it cannot be written as a product of two polynomials of degree at least 1.

Example 4.24. *The polynomial $X^4 + 3X^2 + 2$ has no roots over $\mathbb{Q}$, but it is not irreducible. Indeed, $X^4 + 3X^2 + 2 = (X^2 + 1)(X^2 + 2)$, and we know that neither of these factors has a root over $\mathbb{R}$ (let alone $\mathbb{Q}$!).*

Example 4.25. *The polynomial $f(X) = X^3 - 2$ is irreducible over $\mathbb{Q}$. Indeed, if it were to factor as $f = gh$ then since $\deg(g), \deg(h) \geq 1$ and $\deg(g) + \deg(h) = \deg(f) = 3$, one of g or h must have degree 1. However, 2 is not the cube of any rational number. Note that we can prove that p-adically: if $2 = \alpha^3$ then in $\mathbb{Q}_2$ we would have $1 = v_2(2) = v_2(\alpha^3) = 3v_2(\alpha)$, but $v_2(\alpha) \in \mathbb{Z}$ and 1 is not an integer multiple of 3.*

As we have done in the past with questions about polynomials, we can reduce the question of irreducibility to an integral one. This is a classical result of Gauss, which says that if a (monic) polynomial with coefficients in $\mathbb{Z}_p$ factors into two non-constant polynomials, then these new polynomials can be taken to be in $\mathbb{Z}_p$.

Lemma 4.26 (Gauss' lemma)**.** *Let $f(X)$ be a monic polynomial with coefficients in $\mathbb{Z}_p$, and say $f(X) = g(X)h(X)$ where g and h are monic polynomials with coefficients in $\mathbb{Q}_p$ of degree at least 1. Then both g and h have all coefficients in $\mathbb{Z}_p$.*

Proof. Let $r, s \in \mathbb{Z}$ be the smallest integers such that $p^r g(X)$ and $p^s h(X)$ have $\mathbb{Z}_p$ coefficients. Note that since g, h are monic, we must have $r, s \geq 0$. Moreover, since r and s are minimal we must have that $p^r g$ and $p^s h$ are non-zero mod h and so $p^{r+s} hg = p^{r+s} f$ is nonzero mod p. But f was already nonzero mod p, so we must have $r + s = 0$. Hence $r = s = 0$.

□

An extremely useful tool in p-adic algebra is Eisenstein's criterion, which sometimes gives us a way to determine that a polynomial is irreducible simply from examining the coefficients.

Theorem 4.27 (Eisenstein's Criterion)**.** *Suppose that $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ is a monic polynomial with coefficients in $\mathbb{Z}_p$. If*

- *$|a_k|_p \leq 1/p$ for all k, and*
- *$|a_0|_p = 1/p$,*

then $f(x)$ is irreducible over $\mathbb{Q}_p$.

Proof. Say, for a contradiction, that f is not irreducible, so $f(X) = g(X)h(X)$ where g, h both have degree at least 1. Write

$$\begin{aligned} g(X) &= X^r + g_{r-1}X^{r-1} \cdots + g_0; \\ h(X) &= X^s + h_{s-1}X^{s-1} \cdots + h_0; \\ f(X) &= X^{r+s} + a_{r+s-1}X^{r+s-1} \cdots + a_0. \end{aligned}$$

By Lemma 4.26 both g and h have all $\mathbb{Z}_p$ coefficients. In particular we can reduce f, g and h modulo p to obtain

$$f(X) \equiv g(X)h(X) \mod p.$$

The assumptions in the theorem statement force $f(X) \equiv X^{r+s} \mod p$. Hence we must have that $g(X) \equiv X^r \mod p$ and $h(X) \equiv X^s \mod p$. In particular, we must have $g_0 \equiv h_0 \equiv 0 \mod p$, so $|g_0|_p, |h_0|_p \leq 1/p$. But then since $a_0 = h_0 g_0$, we must have $|a_0|_p \leq 1/p^2$, a contradiction. □

This provides us with an easy test to see whether a polynomial is irreducible!

Example 4.28. *Consider the polynomial $X^5 + 124625X^3 + 105$ over $\mathbb{Q}_5$. Then since $150 = 5 \times 21$ it follows that $|105|_p = 1/5$, and moreover $5 \mid 124625$ so $|124625|_p \leq 1/5$. Hence the polynomial is irreducible.*

Example 4.29. *Consider the polynomial $f(X) = X^2 + X + 1$ over $\mathbb{Q}_3$. Then we do not immediately see how to apply Eisenstein's criterion. However, note that $f(X)$ factors if and only if $f(X+1)$ factors, and for this latter we have $f(X+1) = X^2 + 3X + 3$ which now satisfies Eisenstein's criterion and so is irreducible.*

In fact, Eisenstein's criterion allows us to show more about roots of unity in $\mathbb{Q}_p$ – there are no non-trivial pth roots of unity.

Corollary 4.30. *Assume that p is an odd prime number. If $\alpha \in \mathbb{Q}_p$ satisfies $\alpha^p = 1$ then $\alpha = 1$.*

Proof. Factor $f(X) = X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + 1)$. If $\alpha \neq 1$ then it must be a root of the other factor, $\Phi(X) = X^{p-1} + X^{p-2} + \cdots + 1$, so let us examine that factor. Note that, in $\mathbb{Z}/p\mathbb{Z}$ we can perform

$$f(X+1) \equiv (X+1)^p - 1 = X^p + 1 - 1 = X^p,$$

In particular, since $\Phi(X+1)$ is a factor of $f(X+1)$, we must have $\Phi(X+1) \equiv X^{p-1} \mod p$. In particular, if $\Phi(X+1) = X^{p-1} + \sum_{k=0}^{p-2} \alpha_k X^k$, we have $|\alpha_k|_p \leq 1/p$. Moreover, looking at the constant term we get from

$$\Phi(X+1) = (X+1)^{p-1} + (X+1)^{p-2} + \cdots + 1,$$

we get $a_0 = p$ and so $|a_0|_p = 1/p$. In particular $\Phi(X+1)$ satisfies Eisenstein's criterion so is irreducible, so $\Phi(X)$ is also irreducible and hence if α is a root of $X^p - 1$ then it must be a root of the factor $X - 1$ so $\alpha = 1$. □

Comparison 4.31

This is the opposite of the situation for $(p-1)th$ roots of unity, of which $\mathbb{Q}_p$ has plenty. There is a sense in which this mimics the status of -1 not being a square in $\mathbb{R}$, though the analogy is hard to describe with the technology currently available.

5 Topological Properties of $\mathbb{Q}_p$

We shall now move to study $\mathbb{Q}_p$ from a topological perspective, i.e. as a metric space. The open (and closed) sets determine the structure of such a space, and so we start there and observe some interesting (and odd!) properties of $\mathbb{Q}_p$. We will then move to look at continuous functions on $\mathbb{Q}_p$. This study will conclude by defining and looking into properties of the 'Mahler expansion' of a continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$.

5.1 Open and closed balls

Let us recall the definitions of open and closed balls from the metric spaces course, in our setting.

Definition 5.1. The open ball of radius $r > 0$ centred at a point $\alpha \in \mathbb{Q}_p$ is the set

$$B_r(\alpha) := \left\{ y \in \mathbb{Q}_p \ : \ |\alpha - y|_p < r \right\}.$$

The closed ball of radius $r > 0$ centred at a point $\alpha \in \mathbb{Q}_p$ is the set

$$\overline{B_r(\alpha)} := \left\{ y \in \mathbb{Q}_p \ : \ |\alpha - y|_p \leq r \right\}.$$

More generally, a subset $U \subseteq \mathbb{Q}_p$ is an open set if for every $\alpha \in U$ there exists a radius $r > 0$ such that

$$B_r(\alpha) \subseteq U.$$

To make ideas more concrete, let us consider the open ball of radius 1 centred at 0,

$$B_1(0) = \left\{ y \in \mathbb{Q}_p \ : \ |y|_p < 1 \right\}.$$

Firstly, this is immediately a subset of $\mathbb{Z}_p$. Moreover, since $|y|_p = p^{-v_p(y)}$, this set can be characterised in many ways:

$$\begin{aligned} B_1(0) &= \left\{ y \in \mathbb{Q}_p \ : \ |y|_p \leq 1/p \right\} = \overline{B_{1/p}(0)} \\ &= \{ y \in \mathbb{Q}_p \ : \ v_p(y) \geq 1 \} \\ &= \left\{ y \in \mathbb{Z}_p \ : \ \text{the p-adic expansion of } y \text{ is of the form } \sum_{k=1}^{\infty} a_k p^k \right\} \\ &= \{ y \in \mathbb{Z}_p \ : \ y \equiv 0 \mod p \}. \end{aligned}$$

Note that we were able to translate the < 1 into $\leq 1/p$ because the values of $|\cdot|_p$ are always powers of p, so if they are less than $1 = p^0$ then they cannot be more than p^{-1}. Inspired by this observation, we note that closed sets are surprisingly redundant in $\mathbb{Q}_p$.

Lemma 5.2. *A subset $S \subseteq \mathbb{Q}_p$ is an open ball if and only if it is a closed ball.*

Proof. If $S = B_r(\alpha)$ for some $r > 0$ and $\alpha \in \mathbb{Q}_p$, then let $N \in \mathbb{Z}$ be the smallest integer such that $p^N < r$. Then since $|\cdot|_p$ takes values in powers of p, we obtain

$$B_r(\alpha) = \left\{ y \in \mathbb{Q}_p \ : \ |\alpha - y|_p < r \right\} = \left\{ y \in \mathbb{Q}_p \ : \ |\alpha - y|_p \leq p^N \right\} = \overline{B_{p^N}(\alpha)}.$$

Conversely, if $S = \overline{B_r(\alpha)}$ then choose $M \in \mathbb{Z}$ to be the smallest integer such that $p^M > r$. We similarly obtain

$$\overline{B_r(\alpha)} = \left\{ y \in \mathbb{Q}_p \ : \ |\alpha - y|_p \leq r \right\} = \left\{ y \in \mathbb{Q}_p \ : \ |\alpha - y|_p < p^M \right\} = \overline{B_{p^M}(\alpha)}$$

□

Comparison 5.3

In the real numbers, the ball of radius $r > 0$ around $x \in \mathbb{R}$ is the open interval $(x - r, x + r) \subseteq \mathbb{R}$. Similarly, the closed ball with the same parameters is the closed interval $[x-r, x+r] \subseteq \mathbb{R}$. Lemma 5.2 is a first indication that $\mathbb{Q}_p$ has very different topological behaviour to $\mathbb{R}$ – in the latter, closed balls are *never* equal to open balls!

If the fact that closed balls are the same thing as open balls can be categorised as odd, then the next fact is downright absurd!

Lemma 5.4. *Every element of an open ball is a centre-point of that ball. That is, if $r > 0$ is a real number, $\alpha \in \mathbb{Q}_p$ and $\beta \in B_r(\alpha)$ then*

$$B_r(\beta) = B_r(\alpha).$$

Proof. Note that for every $y \in \mathbb{Q}_p$ the ultrametric inequality shows

$$|\beta - y|_p = |(\beta - \alpha) + (\alpha - y)|_p \leq \max\left\{ |\alpha - \beta|_p , |\alpha - y|_p \right\}.$$

Note that since $\beta \in B_r(\alpha)$ we must have $|\alpha - \beta|_p < r$. Hence if $y \in B_r(\alpha)$ then $|\alpha - y|_p < r$, and so by the inequality above $|\beta - y|_p < r$. Hence $B_r(\alpha) \subseteq B_r(\beta)$. Note now that $\alpha \in B_r(\beta)$ and so by the same argument we must have $B_r(\beta) \subseteq B_r(\alpha)$, so equality. □

Comparison 5.5

It is needless to say this is completely ridiculous from the perspective of the real numbers. The open interval $(x - r, x + r) \subseteq \mathbb{R}$ has one centre-point, the point x, which is in the middle of the interval. The reason for this behaviour is the strength of the ultrametric inequality, which is far more powerful than the triangle inequality. We shall need to substantially change our metric space intuition from how we think of $\mathbb{R}$ in order to understand $\mathbb{Q}_p$!

More generally we will be interested in looking at subspaces $X \subseteq \mathbb{Q}_p$, in particular the case $X = \mathbb{Z}_p$ will be important. In this setting remember that all of our definitions simply descent to X in the natural way. We shall only recall the definition of open balls, since closed balls are analogous (and by Lemma 5.2 are a little redundant in the p-adic world).

Definition 5.6. Let $X \subseteq \mathbb{Q}_p$. Then the open ball of radius $r > 0$ in X centred at a point $\alpha \in X$ is the intersection

$$B_r^X(\alpha) := B_r(\alpha) \cap X.$$

5.2 Continuous functions

A central concept in the study of metric spaces is the collection of continuous functions on the space.

Definition 5.7. Let $X \subseteq \mathbb{Q}_p$. Then a function $f : X \to \mathbb{Q}_p$ is said to be continuous at a point $\alpha \in X$ if for every $\varepsilon > 0$ there exists $\delta > 0$ such that

$$|\beta - \alpha|_p < \delta \implies |f(\beta) - f(\alpha)|_p < \varepsilon.$$

We simply say that f is continuous if it is continuous at every $\alpha \in X$.

Recall that colloquially this is saying that we are continuous at a point $\alpha \in X$ if every ball we put around $f(\alpha)$ contains the image of a small ball around α. Formally: for every $\varepsilon > 0$ there exists $\delta > 0$ such that

$$\beta \in B_\delta^X(\alpha) \implies f(\beta) \in B_\varepsilon(f(\alpha)).$$

Example 5.8. *The identity function $f : X \to \mathbb{Q}_p$ sending $\alpha \in X$ to $f(\alpha) = \alpha$ is continuous, since we can choose $\delta = \varepsilon$.*

Example 5.9. $\mathbf{a_0} : \mathbb{Z}_p \to \mathbb{Q}_p$ *be the function given by $\mathbf{a_0}(\alpha) = a_0$ where $\alpha = \sum_{k=0}^{\infty} a_k p^k$ is the p-adic expansion of α. Then this function is continuous. Indeed, before we even think about ε, consider $\delta = 1$:*

$$\begin{aligned} B_1^{\mathbb{Z}_p}(\alpha) &= \left\{\beta \in \mathbb{Z}_p \ : \ |\beta - \alpha|_p < 1\right\} \\ &= \{\beta \in \mathbb{Z}_p \ : \ \beta - \alpha \equiv 0 \mod p\} \\ &= \{\beta \in \mathbb{Z}_p \ : \ \beta \equiv \alpha \mod p\} \\ &= \{\beta \in \mathbb{Z}_p \ : \ \mathbf{a_0}(\beta) = \mathbf{a_0}(\alpha)\}. \end{aligned}$$

Hence, for every $\varepsilon > 0$ we can choose $\delta = 1$ so that $\beta \in B_1(\alpha)$ immediately implies $\mathbf{a_0}(\beta) = \mathbf{a_0}(\alpha) \in B_\varepsilon(\mathbf{a_0}(\alpha))$.

Lemma 5.10. *Sums and products of continuous functions are continuous functions. That is, if $X \subseteq \mathbb{Q}_p$ and $f, g : X \to \mathbb{Q}_p$ are continuous, then $f + g$ and fg are both continuous also.*

Proof. See the exercise sheets. □

An important consequence of the above is that polynomials define continuous maps.

Lemma 5.11. *Polynomials define continuous functions from $\mathbb{Q}_p$ to $\mathbb{Q}_p$.*

Proof. Firstly, the identity function $x \mapsto x$ is continuous. By Lemma 5.10 we know that products of continuous functions are continuous, so applying this repeatedly we then obtain that $x \mapsto x^n$ is continuous for every x and every integer $n > 0$. Moreover, for $a \in \mathbb{Q}_p$ the constant function $x \mapsto a$ is also clearly continuous, and so again the product $x \mapsto ax^n$ is continuous. Since polynomial functions are sums of such functions, the result follows from the fact that sums of continuous functions are also continuous by Lemma 5.10. □

5.3 Locally constant functions

In Example 5.9, we saw that the function $\mathbf{a_0}$ was continuous by showing that it was constant on open balls of radius 1 around each point. This 'locally constant' behaviour is actually very common in the p-adic world, so we shall investigate!

Definition 5.12. Let $X \subseteq \mathbb{Q}_p$, and $f : X \to \mathbb{Q}_p$ be a function. Then f is locally constant if there is a ball around every point such that f is constant in that ball. Precisely: for every $\alpha \in X$ there exists $\delta > 0$ such that f is constant $B_\delta^X(\alpha)$.

Comparison 5.13

In the real numbers, every locally constant function is just constant, as otherwise we would have sharp jumps between two different balls with different constant values. However, in the p-adics we do have locally constant functions which are not constant, as we have already observed in Example 5.9. This is really a consequence of the disconnectedness of the balls in $\mathbb{Q}_p$, and we shall see some shadows of this in the exercise class.

As we saw in the example, locally constant functions are always continuous.

Lemma 5.14. *Let $X \subseteq \mathbb{Q}_p$, and let $f : X \to \mathbb{Q}_p$ be a locally constant function. Then f is continuous.*

Proof. Let $\alpha \in X$ and $\varepsilon > 0$. Since f is locally constant, choose $\delta > 0$ so that f is constant on $B_\delta^X(\alpha)$, then for $\beta \in B_\delta^X(\alpha)$

$$|f(\alpha) - f(\beta)|_p = 0 < \varepsilon.$$

□

Despite the fact that locally constant functions do not need to be constant, they cannot freely take as many values as they like. Their image is quite constrained!

Lemma 5.15. *Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be a locally constant function. Then the image of f is a finite set.*

5.4 Mahler Expansions

In the p-adic world, since factorials tend to 0 quickly, binomial coefficients are very useful. Indeed, we extend the usual binomial coefficients to functions on $\mathbb{Z}_p$ as follows.

Definition 5.16. For each $n \geq 0$ we define the extended binomial coefficient $\binom{\cdot}{n}$ to be the function

$$\binom{\cdot}{n} : \mathbb{Z}_p \to \mathbb{Q}_p$$
$$\alpha \mapsto \binom{\alpha}{n} := \frac{\alpha(\alpha-1)\dots(\alpha-(n-1))}{n!}.$$

Note that for each positive integer x the extended binomial coefficient is the usual binomial coefficient

$$\binom{x}{n} = \frac{x!}{n!(x-n)!}.$$

Example 5.17. *Note that* $\binom{-1}{n} = (-1)^n$.

The binomial coefficients are polynomials, and so by Lemma 5.11 are already continuous functions. In spite of their small denominators, they even map $\mathbb{Z}_p$ to $\mathbb{Z}_p$!

Lemma 5.18. *For every $n \geq 0$, and every $\alpha \in \mathbb{Z}_p$, we have*

$$\binom{\alpha}{n} \in \mathbb{Z}_p.$$

Proof. The proof is very similar to our computation of $v_p(n!)$ in Example 1.5, see the exercise sheet. □

These coefficients turn out to play an important role in the space of continuous $\mathbb{Q}_p$-valued functions on $\mathbb{Z}_p$. Their role is much like that of $e^{2\pi iz}$ in real and complex analysis, as they provide a sort-of basis for the continuous functions. That is, every continuous function $\mathbb{Z}_p \to \mathbb{Q}_p$ can be uniquely expressed as a sum of binomial coefficients. This is a result due to Mahler.

Theorem 5.19 (Mahler Expansion)**.** *Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be a continuous function. Then there is a unique sequence $(\alpha_n)_n$ in $\mathbb{Q}_p$ such that*

$$\sum_{n=0}^{\infty} \alpha_n \binom{x}{n}$$

converges to $f(x)$ for every $x \in \mathbb{Z}_p$. We call this the Mahler expansion of f.

Unfortunately, we do not have the time in this course to prove this result. We therefore assert it without proof, and instead focus on more practical questions – like how to compute it! For this we will require the difference operator, which you should think of as a form of 'discrete differentiation'.

Definition 5.20. Let $\mathcal{C}(\mathbb{Z}_p) := \{f : \mathbb{Z}_p \to \mathbb{Q}_p \ : \ f \text{ is continuous}\}$. Then the difference operator Δ is the map

$$\begin{aligned} \Delta : \mathcal{C}(\mathbb{Z}_p) &\to \mathcal{C}(\mathbb{Z}_p) \\ (\Delta f)(x) &:= f(x+1) - f(x). \end{aligned}$$

The difference operator is intimately linked to the Mahler expansion, and will be our primary inroad to compute Mahler expansions. Let us observe what this operator does to the Mahler expansion.

Lemma 5.21. *Let $f \in \mathcal{C}(\mathbb{Z}_p)$, and let $f(x) = \sum_{n=0}^{\infty} \alpha_n \binom{x}{n}$ be the Mahler expansion of f. Then the Mahler expansion of Δf is given by*

$$\Delta f(x) = \sum_{n=0}^{\infty} \alpha_{n+1} \binom{x}{n}.$$

Proof (non-examinable). By Pascal's triangle, we have

$$\binom{x+1}{n} = \binom{x}{n} + \binom{x}{n-1},$$

where we take $\binom{\cdot}{-1} := 0$. Thus,

$$\begin{aligned} \Delta f(x) &= f(x+1) - f(x) \\ &= \sum_{n=0}^{\infty} \alpha_n \left(\binom{x+1}{n} - \binom{x}{n} \right) \\ &= \sum_{n=1}^{\infty} \alpha_n \binom{x}{n-1} \\ &= \sum_{n=0}^{\infty} \alpha_{n+1} \binom{x}{n} \end{aligned}$$

□

Corollary 5.22. *Let $f \in \mathcal{C}(\mathbb{Z}_p)$, and let $f(x) = \sum_{n=0}^{\infty} \alpha_n \binom{x}{n}$ be the Mahler expansion of f. Then the coefficients are given by*

$$\alpha_n = (\Delta^n f)(0),$$

where $\Delta^n f = \underbrace{\Delta \dots \Delta}_{n} f$ is the function obtained by applying Δ n-times to f.

Proof. Note that $\alpha_0 = f(0)$. Repeatedly applying Δ to f we obtain by Lemma 5.21 that

$$\Delta^n f(0) = \sum_{m=0}^{\infty} \alpha_{m+n} \binom{0}{m} = \alpha_n.$$

□

Comparison 5.23

A good way to think of Δ as a 'discrete' version of differentiation. Indeed, then the fact that the Mahler expansion is given by

$$f(x) = \sum_{n=0}^{\infty} (\Delta^n f)(0) \binom{x}{n},$$

mimics the classical Maclaurin expansion (the Taylor expansion at $x = 0$) from the real world,

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

where $f^{(n)}$ is the nth derivative of the function f. An important thing to note is that this comparison is not perfect: Maclaurin expansions only exist for differentiable functions (not all continuous functions on $\mathbb{R}$) whereas Mahler expansions are for all continuous functions $\mathbb{Z}_p \to \mathbb{Q}_p$. A better real-world expansion to compare to is the *fourier expansion* of a continuous function $f : [a, b] \to \mathbb{R}$, which you may see if you are familiar with this.

Example 5.24. *Let us compute one of these Mahler expansions in a concrete situation. We'll take $p = 11$ and $f(x) = x^3$. In order to express $f(x) = \sum_{n=0}^{\infty} \alpha_n \binom{x}{n}$ we directly compute*

$$\begin{aligned}
&\Delta^0 f(x) = f(x) = x^3 \\
&\Delta^1 f(x) = f(x+1) - f(x) = 3x^2 + 3x + 1 \\
&\Delta^2 f(x) = \big(3(x+1)^2 + 3(x+1) + 1\big) - \big(3x^2 + 3x + 1\big) = 6x + 6 \\
&\Delta^3 f(x) = 6 \\
&\Delta^n f(x) = 0 \qquad\qquad n \geq 4.
\end{aligned}$$

Hence, evaluating these at 0, we get $x^3 = \binom{x}{1} + 6\binom{x}{2} + 6\binom{x}{3}$. Indeed, from this example it seems quite clear that for a general polynomial $f(x)$, once $n > \deg(f)$ we must have $\alpha_n = 0$ (see the example sheets).

Our method of determining the Mahler expansion of a continuous function f will be to compute $\Delta^n f(0)$ for each n. For a fixed n (say $n = 2$), this is easy to do directly. To do this for all n is also not usually too hard, and typically relies on some combinatorial trickery. We conclude this section by thinking about $\mathbb{Z}_p$-powers of elements in $\mathbb{Z}_p$, much like taking $\mathbb{R}$-powers in $\mathbb{R}$. We shall see more of this in the exercise sheets.

Example 5.25. *For each positive integer x we have $3^x = (1+2)^x = \sum_{n=0}^{\infty} \binom{x}{n} 2^n$. We can extend this to a function on $\mathbb{Z}_2$ now by defining for each $\alpha \in \mathbb{Z}_2$*

$$3^\alpha := \sum_{n=0}^{\infty} 2^n \binom{\alpha}{n}.$$

Note that this sum clearly converges for all $\alpha \in \mathbb{Z}_2$ since by Lemma 5.18 we have

$$\left| 2^n \binom{x}{n} \right|_2 \leq 2^{-n},$$

which goes to 0 as $n \to \infty$ and by Proposition 3.7 this proves that the sum converges.

Epilogue (non-examinable)

We are now at the end of our introduction to the p-adic numbers. We have touched on several facets of the p-adic world, looking at results from algebraic, analytic, and topological angles. Throughout the course we have compared $\mathbb{Q}_p$ with the trusty old real numbers $\mathbb{R}$, and hopefully you have seen that in fact this exotic and sometimes unintuitive p-adic world can also be much nicer. This begs the question: where to next? What other completions are there of $\mathbb{Q}$ besides $\mathbb{Q}_p$ and $\mathbb{R}$? The answer to this question is: nowhere, we have seen every completion that there is! A theorem of Ostrowski shows that every nontrivial completion of $\mathbb{Q}$ is either $\mathbb{Q}_p$ for some prime number p or the real numbers.

Whilst we may have met all of the completions, this course has only been a small taste of the p-adic universe that awaits an intrepid adventurer – and there is so much more that we do not have the time to see! The p-adic numbers are a fundamental concept in number theory, but have touched various other worlds also. For example, there is a beautiful theorem of Monsky (1970) which says that it is not possible to dissect a square into an odd number of triangles of equal area. The proof of this result uses the 2-adic numbers.

In number theory, the p-adic numbers are very useful. If f is a polynomial in n variables with coefficients in $\mathbb{Q}$ then we wish to determine whether there are rational numbers $a_1, \ldots, a_n \in \mathbb{Q}$ with

$$f(a_1, \ldots, a_n) = 0. \tag{4}$$

As we have discussed in the course, it is a necessary criterion that such a solution exists in $\mathbb{Q}_p$ for every prime number p and also in $\mathbb{R}$. This may lead us to hope that the converse statement is true:

if (4) has solutions in $\mathbb{Q}_p$ for every p and in $\mathbb{R}$, then there is a solution in $\mathbb{Q}$.

This statement is known as *the Hasse principle*, and it does not always hold! Below are examples.

- The Hasse principle holds when f is a homogeneous polynomial of degree 2 with coefficients in $\mathbb{Q}$, for example $f(x_1, \ldots, x_6) = x_1^2 + 2x_2^2 + 500x_6^2$. This is the Hasse–Minkowski theorem.
- The Hasse principle fails if $f(x, y, z) = 3x^3 + 4y^3 + 5z^3$, an example due to Selmer (1951). Similarly, it is false if $f(x) = (x^2 - 2)(x^2 + 7)(x^2 - 14)$ – for this one it is a worthwhile revision exercise to check that (4) has solutions in $\mathbb{Q}_p$ for every p, and it is clear that $x = \sqrt{2}$ is a solution in $\mathbb{R}$. But it clearly has no solutions in $\mathbb{Q}$ since none of $2, -7, 34$ are rational squares.

Classifying when the Hasse principle holds or does not hold is a large open problem in number theory, and a subject of very active research.

Even when we know that there are solutions, it is often very hard to know if we have written down all of them! For example the 'cursed curve' is given by the equation

$$y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z - 32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 = 0,$$

which had been a famously difficult equation to study until 2017 when Balakrishnan–Dogra–Müller–Tuitman–Vonk determined the solutions in $\mathbb{Q}$. Their work uses the p-adic numbers fundamentally.

For future reading on p-adic numbers, you should know that $\mathbb{Q}_p$ is an example of a local field, and books often discuss them in that context. Some excellent books which read further in this world are listed below – go forth, and explore!

References

[1] J. W. S. Cassels, *Local Fields*, Cambridge University Press, 1986.

[2] F. Gouvêa, *p-adic Numbers*, Springer-Verlag, 1997

[3] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer New York, NY,

[4] K. Mahler, *Introduction to p-adic numbers and Valuation Theory*, Cambridge University Press, 1981

[5] J. Neukirch, *Algebraic Number Theory* Chapter II, Springer Berlin, 1999

A Definitions from the past

Real Analysis

Definition A.1. Let $(r_n)_n$ be a sequence of real numbers, and $r \in \mathbb{R}$. Then we say that r is the limit superior of the sequence $(r_n)_n$ if the following holds.

- For every $\varepsilon > 0$ there exists an integer N such that for all $n > N$ we have $r_n < r + \varepsilon$.
- For every $\varepsilon > 0$ and every integer N there exists an integer $n > N$ with $r_n > r - \varepsilon$.

We write $r = \limsup_{n\to\infty} r_n$ if this holds. If no such r exists then we write $\limsup_{n\to\infty} r_n = \infty$. Moreover, if $\lim_{n\to\infty} r_n$ exists, then it is equal to the limit superior:

$$\lim_{n\to\infty} r_n = \limsup_{n\to\infty} r_n.$$

Metric Spaces

Definition A.2. A metric d on a set S is a function $d : S \times S \to \mathbb{R}$ such that for all $x, y, z \in S$ the following hold:

- (triviality) $d(x, x) = 0$;
- (positivity) if $x \neq y$ then $d(x, y) > 0$;
- (symmetry) $d(x, y) = d(y, x)$;
- (triangle inequality) $d(x, z) \leq d(x, y) + d(y, z)$.