Resource F

p-adic numbers

F.1 Valuations

Definition F.1 *A valuation on a field k is a map*

$$x \mapsto \|x\| : k \to \mathbb{R}$$

such that

i) $\|x\| \geq 0$ *and* $\|x\| = 0 \iff x = 0$*;*

ii) $\|xy\| = \|x\|\|y\|$*;*

iii) $\|x + y\| \leq \|x\| + \|y\|$.

The valuation is said to be non-archimedean *if it satisfies the stronger relation*

iii') $\|x + y\| \leq \max(\|x\|, \|y\|)$*;*

otherwise it is said to be archimedean.

F.2 The p-adic valuation on $\mathbb{Q}$

The absolute value $|x|$ defines a valuation on $\mathbb{Q}$. Surprisingly perhaps, there are other valuations on $\mathbb{Q}$ just as worthy of study.

Definition F.2 *Let p be a prime. If $x \in \mathbb{Q}$, $x \neq 0$, then we can write*

$$x = \frac{m}{n} p^e$$

where $p \nmid m, n$. The p-adic value of x is given by

$$\|x\|_p = p^{-e}.$$

Also, $\|0)_p\| = 0$.

For example, $\| -2/3\|_3 = 3$, $\|36/7\|_p = 3^{-2}$.

Note that integers are quite small in the p-adic valuation:

$$x \in \mathbb{Z} \Longrightarrow \|x\|_p \leq 1.$$

High powers of p are very small:

$$p^n \to 0 \text{ as } n \to \infty.$$

Proposition F.1 *$\|x\|_p$ defines a non-archimedean valuation on $\mathbb{Q}$*

To emphasize the analogy between the p-adic valuation and the familiar valuation $|x|$ we sometimes write

$$\|x\|_\infty = |x| \text{ and } |x| = \|x\|_\infty.$$

F.3 p-adic numbers

The reals $\mathbb{R}$ can be constructed by *completing* the rationals $\mathbb{Q}$ with respect to the valuation $|x|$. In this construction each Cauchy sequence

$$\{x_i \in \mathbb{Q} : |x_i - x_j| \to 0 \text{ as } i, j \to \infty\}$$

defines a real number, with 2 sequences defining the same number if $|x_i - y_i| \to 0$.

(There are 2 very different ways of constructing $\mathbb{R}$ from $\mathbb{Q}$: by completing $\mathbb{Q}$, as above; or alternatively, by the use of *Dedekind sections*. In this each real number corresponds to a partition of $\mathbb{Q}$ into 2 subsets L, R where

$$l \in L,\ r \in R \Longrightarrow l < r.$$

The construction by completion is much more general, since it applies to any metric space; while the alternative construction uses the fact that $\mathbb{Q}$ is an *ordered* field. John Conway, in *On Numbers and Games,* has generalized Dedekind sections to give an extraordinary construction of rationals, reals and infinite and infinitesimal numbers, starting 'from nothing', by defining a number recursively as two sets L, R of numbers where

$$l \in L,\ r \in R \Longrightarrow l < r.$$

Knuth has given a popular account of Conway numbers in the small book *Surreal Numbers.*)

We can complete $\mathbb{Q}$ with respect to the p-adic valuation in the same way. The resulting field is called *the field of p-adic numbers*, and is denoted by $\mathbb{Q}_p$. We can identify $x \in \mathbb{Q}$ with the Cauchy sequence $(x, x, x, \dots)$. Thus

$$\mathbb{Q} \subset \mathbb{Q}_p.$$

To bring out the parallel with the reals, we sometimes write

$$\mathbb{R} = \mathbb{Q}_\infty.$$

The numbers $x \in \mathbb{Q}_p$ with $\|x\|_p \leq 1$ are called *p-adic integers*. The p-adic integers form a ring, denoted by $\mathbb{Z}_p$. For if $x, y \in \mathbb{Z}_p$ then by property (3) above,

$$\|x + y\|_p \leq \max(\|x\|_p, \|y\|_p) \leq 1,$$

and so $x + y \in \mathbb{Z}_p$. Similarly, by property (1),

$$\|xy\|_p = \|x\|_p \|y\|_p \leq 1,$$

and so $xy \in \mathbb{Z}_p$.

Evidently

$$\mathbb{Z} \subset \mathbb{Z}_p.$$

More generally,

$$x = \frac{m}{n} \in \mathbb{Z}_p$$

if $p \nmid n$. (We sometimes say that a rational number x of this form is *p-integral*.) In other words,

$$\mathbb{Q} \cap \mathbb{Z}_p = \{\frac{m}{n} : p \nmid n\}.$$

Evidently the p-integral numbers form a sub-ring of $\mathbb{Q}$.

Concretely, each element $x \in \mathbb{Z}_p$ is uniquely expressible in the form

$$x = c_0 + c_1 p + c_2 p^2 + \cdots \quad (0 \leq c_i < p).$$

More generally, each element $x \in \mathbb{Q}_p$ is uniquely expressible in the form

$$x = c_{-i} p^{-i} + c_{-i+1} p^{-i+1} + \cdots + c_0 + c_1 p + \cdots \quad (0 \leq c_i < p).$$

We can think of this as the p-adic analogue of the decimal expansion of a real number $x \in \mathbb{R}$.

Suppose for example $p = 3$. Let us express $1/2 \in \mathbb{Q}_3$ in standard form. The first step is to determine if

$$\frac{1}{2} \equiv 0, 1 \text{ or } 2 \bmod 3.$$

In fact $2^2 \equiv 1 \bmod 3$; and so

$$\frac{1}{2} \equiv 2 \bmod 3.$$

Next

$$\frac{1}{3}\left(\frac{1}{2} - 2\right) = -\frac{1}{2} \equiv 1 \bmod 3$$

ie

$$\frac{1}{2} - 2 \equiv 1 \cdot 3 \bmod 3^2.$$

Thus

$$\frac{1}{2} \equiv 2 + 1 \cdot 3 \bmod 3^2$$

For the next step,

$$\frac{1}{3}\left(-\frac{1}{2} - 1\right) = -\frac{1}{2} \equiv 1 \bmod 3$$

giving

$$\frac{1}{2} \equiv 2 + 1 \cdot 3 + 1 \cdot 3^2 \bmod 3^3$$

It is clear that this pattern will be repeated indefinitely. Thus

$$\frac{1}{2} = 2 + 3 + 3^2 + 3^3 + \cdots .$$

To check this,

$$\begin{aligned} 2 + 3 + 3^2 + \cdots &= 1 + (1 + 3 + 3^2 + \cdots) \\ &= 1 + \frac{1}{1-3} \\ &= 1 - \frac{1}{2} \\ &= \frac{1}{2}. \end{aligned}$$

As another illustration, let us expand $3/5 \in \mathbb{Q}_7$. We have

$$\begin{aligned} \frac{3}{5} &\equiv 2 \bmod 7 \\ \frac{1}{7}\left(\frac{3}{5} - 2\right) = -\frac{1}{5} &\equiv 4 \bmod 7 \\ \frac{1}{7}\left(-\frac{1}{5} - 4\right) = -\frac{3}{5} &\equiv 5 \bmod 7 \\ \frac{1}{7}\left(-\frac{3}{5} - 5\right) = -\frac{4}{5} &\equiv 2 \bmod 7 \\ \frac{1}{7}\left(-\frac{4}{5} - 2\right) = -\frac{2}{5} &\equiv 1 \bmod 7 \\ \frac{1}{7}\left(-\frac{2}{5} - 1\right) = -\frac{1}{5} &\equiv 4 \bmod 7 \end{aligned}$$

We have entered a loop; and so (in $\mathbb{Q}_7$)

$$\frac{3}{5} = 2 + 4 \cdot 7 + 5 \cdot 7^2 + 2 \cdot 7^3 + 1 \cdot 7^4 + 4 \cdot 7^5 + 5 \cdot 7^6 + \cdots$$

Checking,

$$\begin{aligned} 1 + \left(1 + 4 \cdot 7 + 5 \cdot 7^2 + 2 \cdot 7\right) \frac{1}{1 - 7^4} &= 1 - \frac{960}{2400} \\ &= 1 - \frac{2}{5} \\ &= \frac{3}{5}. \end{aligned}$$

It is not difficult to see that a number $x \in \mathbb{Q}_p$ has a recurring p-adic expansion if and only if it is rational (as is true of decimals).

Let $x \in \mathbb{Z}_p$. Suppose $\|x\|_p = 1$. Then

$$x = c + yp,$$

where $0 < c < p$ and $y \in \mathbb{Z}_p$. Suppose first that $c = 1$, ie

$$x = 1 + yp.$$

Then x is invertible in $\mathbb{Z}_p$, with

$$x^{-1} = 1 - yp + y^2p^2 - y^3p^3 + \cdots .$$

Even if $c \neq 1$ we can find d such that

$$dc \equiv 1 \bmod p.$$

Then

$$dx \equiv dc \equiv 1 \bmod p,$$

say

$$dx = 1 + py,$$

and so x is again invertible in $\mathbb{Z}_p$, with

$$x^{-1} = d\left(1 - yp + y^2p^2 - \cdots\right).$$

Thus the elements $x \in \mathbb{Z}_p$ with $\|x\|_p = 1$ are all *units* in $\mathbb{Z}_p$, ie they have inverses in $\mathbb{Z}_p$; and all such units are of this form. These units form the multiplicative group

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : \|x\|_p = 1\}.$$

Exercises 6 p-adic numbers

In exercises 1–5 express the given number in standard p-adic form.

** 1. $1/2$ in $\mathbb{Q}_5$.

** 2. -2 in $\mathbb{Q}_3$.

** 3. $1/2$ in $\mathbb{Q}_5$.

** 4. $1/6$ in $\mathbb{Q}_2$.

** 5. 6 in $\mathbb{Q}_2$.

In exercises 6–10 give the first 5 terms in standard 2-adic form for the given number or numbers.

*** 6. $\sqrt{3}$.

*** 7. $\sqrt{5}$.

** 8. $\sqrt{9}$.

*** 9. $7^{1/3}$.

*** 10. The solutions of $x^3 - x + 1 = 0$ in $\mathbb{Q}_2$.

** 11. Show that the standard p-adic form of a positive integer is finite.

*** 12. Show that the standard p-adic form of a rational number is recurring.

** 13. Show that in a p-adic equation

$$x_1 + \cdots + x_n = 0 \qquad (x_1, \ldots, x_n \in \mathbb{Q}_p)$$

no term can dominate, ie at least two of the x_i must attain $\max \|x_i\|_p$. Show that if

$$x_1 + x_2 + \cdots + x_n = 0$$

in $\mathbb{Q}_p$ then at least two of the x_i have maximal p-adic value. ("No term dominates")

*** 14. Show that a series $\sum a_n$ converges in $\mathbb{Q}_p$ if and only if $a_n \to 0$.

*** 15. [Hensel's Lemma] Suppose $f(x) \in \mathbb{Z}[x]$, and suppose $f(a) \equiv 0$ for some $a \in \mathbb{Z}$. Show that if $f'(a) \not\equiv 0 \bmod p$ then there is a unique $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv 0 \bmod p$ and $f(\alpha) = 0$.

*** 16. If the standard form for $\alpha \in \mathbb{Z}_p$ is $\alpha = \sum a_n p^n$, find the standard form for $-\alpha$.

**** 17. Show that the only valuations of $\mathbb{Q}$ are the absolute valuation and the p-adic valuations.

*** 18. Show that if p is an odd prime then $\exp x = \sum_{n\geq 0} x^n/n!$ converges in $\mathbb{Q}_p$ for $\|x\|_p < 1$.
What is the corresponding result for $p = 2$?

*** 19. Show that if p is an odd prime then $\log(1 + x) = \sum_{n\geq 1}(-1)^n x^n/n$ converges in $\mathbb{Q}_p$ for $\|x\|_p < 1$
What is the corresponding result for $p = 2$?

*** 20. Given $r, s \in \mathbb{Q}$, find a sequence $a_n \in \mathbb{Q}$ such that $a_n \to r$ in $\mathbb{R}$ while $a_n \to s$ in $\mathbb{Q}_2$.