2

p-adic numbers

Most of the familiar properties of the ordinary absolute value on the real or complex fields are consequences of the following three:

(i) $|r| \geq 0$, with equality precisely for $r = 0$.
(ii) $|rs| = |r||s|$.
(iii) $|r + s| \leq |r| + |s|$.

A real-valued function $|.|$ on a field k is said to be a *valuation* if it satisfies (i), (ii) (iii). Since $(-1)^2 = 1$, properties (i)-(iii) imply that $|-1| = 1$, $|-r| = |r|$ (all r).

The rational field $\mathbf{Q}$ has other valuations than the absolute value. Let p be a fixed prime. Any rational $r \neq 0$ can be put in the shape

$$r = p^{\rho}u/v, \ \rho \in \mathbf{Z}, \ u, \ v \in \mathbf{Z}, \ p \nmid u, \ p \nmid v.$$

We define

$$|r|_p = p^{-\rho}$$

and

$$|0|_p = 0.$$

This definition clearly satisfies (i), (ii) above. Let

$$s = p^{\sigma}m/n \qquad m, \ n \in \mathbf{Z}, \ p \nmid m, \ p \nmid n,$$

so

$$|s|_p = p^{-\sigma},$$

where without loss of generality

$$\sigma \geq \rho, \text{ i.e. } |s|_p \leq |r|_p.$$

Then

$$r + s = p^{\rho}(un + p^{\sigma-\rho}mv)/vn.$$

Here $p \nmid vn$. The numerator $un + p^{\sigma-\rho}mv$ is an integer, but, at least for for $\rho = \sigma$, it may be divisible by p. Hence

$$|r + s|_p \leq p^{-\rho},$$

that is

(iii*) $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

Clearly (iii*) implies (iii), so $|\ |_p$ is a valuation. We call it the *p-adic valuation*. The inequality (iii*) is called the *ultrametric inequality*, since (iii), the *triangle inequality*, expresses the fact that $|r - s|$ is a metric. A valuation which satisfies the ultrametric inequality is said to be *non-archimedean*.

We can transfer familiar terminology from the ordinary absolute value to the p-adic case. For example, we say that a sequence $\{a_n\}$, $n = 1, 2, \ldots$ is a *fundamental sequence* if for any $\varepsilon > 0$ there is an $n_0\ (\varepsilon)$ such that

$$|a_m - a_n|_p < \varepsilon \qquad \text{whenever} \qquad m, n \geq n_0\ (\varepsilon).$$

The sequence $\{a_n\}$ *converges* to b if

$$|a_n - b|_p < \varepsilon \qquad (\text{all } n \geq n_0\ (\varepsilon)).$$

For example let

$$p = 5$$

and consider the sequence

$$\{a_n\}: \quad 3, \quad 33, \quad 333, \quad 3333, \quad \ldots .$$

Then

$$a_m \equiv a_n \qquad \bmod 5^n \qquad (m \geq n)$$

i.e.

$$|a_m - a_n|_5 \leq 5^{-n} \qquad (m \geq n).$$

Hence $\{a_n\}$ is a fundamental sequence. Indeed it is a convergent sequence, since

$$3a_n = 99\ldots99 \equiv -1(5^n),$$

i.e.

$$|3a_n + 1|_5 \leq 5^{-n}$$

and so

$$a_n \ \to -1/3$$

5-adically.

As the above example shows, the main difficulties with the p-adic valuation are psychological: something is p-adically small if it is divisible by a high power of p. Not every p-adic fundamental sequence is convergent. Let us take $p = 5$ again. Then we construct a sequence of $a_n \in \mathbf{Z}$ such that

$$a_n^2 + 1 \equiv 0 \ (5^n)$$

and

$$a_{n+1} \equiv a_n \ (5^n).$$

We start with $a_1 = 2$. Suppose that we already have a_n for some n and put $a_{n+1} = a_n + b5^n$, where $b \in \mathbf{Z}$ is to be determined. We require

$$(a_n + b5^n)^2 + 1 \equiv 0 \ (5^{n+1}),$$

that is

$$2a_n b + c \equiv 0 \ (5), \qquad (*)$$

where we already have

$$c = (a_n^2 + 1)/5^n \in \mathbf{Z}.$$

Clearly $5 \nmid a_n$ and so we can solve the congruence $(*)$ for the unknown b.

The sequence $\{a_n\}$ just constructed is a 5-adic fundamental sequence since

$$|a_m - a_n|_5 \leq 5^{-n} \qquad (m \geq n).$$

Suppose, if possible, that a_n tends 5-adically to some $e \in \mathbf{Q}$. Then

$$a_n^2 + 1 \to e^2 + 1.$$

On the other hand, by our construction,

$$a_n^2 + 1 \to 0.$$

Hence $e^2 + 1 = 0$; a contradiction.

Just as the real numbers are constructed by completing the rationals with respect to the ordinary absolute value, so the rationals can be completed with respect to $|\ |_p$ to give the field $\mathbf{Q}_p$ of *p-adic numbers*. In fact the process can be simplified because $|\ |_p$ is non-archimedean. For the reader who is unfamiliar with this way of constructing the reals, we sketch a construction of $\mathbf{Q}_p$ at the end of this section.

We say that a field K is *complete* with respect to a valuation $|.|$ if every fundamental sequence is convergent. A field K with valuation $||.||$ is said to be the *completion* of the field k with valuation $|.|$ if there is an injection

$$\lambda : k \to K$$

which preserves the valuation:

$$||\lambda a|| = |a| \qquad (a \in k)$$

and such that

(i) K is complete with respect to $||.||$

(ii) K is the closure of λk with respect to the topology induced by $||.||$ (K is not "too large").

The completion always exists and is unique (up to a unique isomorphism). We henceforth identify k with λk and $|.|$ with $||.||$, so regard k as a subfield of K.

We now discuss the structure of the p-adic field $\mathbf{Q}_p$ with its valuation $|\ |_p$.

We note that

$$|a+b|_p = |a|_p \qquad \text{if} \qquad |b|_p < |a|_p.$$

For by (iii*) $|a+b|_p \leq |a|_p$ and, since $a = (a+b)+(-b)$, we have a contradiction if $|a+b|_p < |a|_p$. It follows that the set of values taken by $|\ |_p$ on $\mathbf{Q}_p$ is precisely the same as the set for $\mathbf{Q}$. Indeed if $\alpha \in \mathbf{Q}_p$, $\alpha \neq 0$ then by (ii) of the definition of the completion, there is an $a \in \mathbf{Q}$ with $|a-\alpha|_p < |\alpha|_p$, so $|\alpha|_p = |a|_p$.

The set of $\alpha \in \mathbf{Q}_p$ with $|\alpha| \leq 1$ is called the set of *p-adic integers* $\mathbf{Z}_p$. Because $|\ |_p$ is non-archimedean, $\mathbf{Z}_p$ is a ring:

$$|\alpha|_p,\ |\beta|_p \leq 1 \Rightarrow |\alpha\beta|_p \leq 1,\ |\alpha+\beta|_p \leq 1.$$

A rational number b is in $\mathbf{Z}_p$ precisely when it has the form $b = u/v$, where $u, v \in \mathbf{Z}$, $p \nmid v$.

The numbers $\varepsilon \in \mathbf{Q}_p$ with $|\varepsilon| = 1$ are the *p-adic units*. From what was said about the values taken by $|.|_p$ on $\mathbf{Q}_p$, every $\beta \neq 0$ in $\mathbf{Q}_p$ is of the shape $\beta = p^n\varepsilon$, where $n \in \mathbf{Z}$ and ε is a unit. The units are just the elements ε of $\mathbf{Q}_p$ such that $\varepsilon \in \mathbf{Z}_p$, $\varepsilon^{-1} \in \mathbf{Z}_p$.

As we have already noted, elementary analysis continues to hold in $\mathbf{Q}_p$, but can be simpler; as the following lemma shows.

Lemma 1. *In $\mathbf{Q}_p$ the series $\sum_0^\infty \beta_n$ converges if and only if $\beta_n \to 0$.*

Proof. By saying that the sum converges, we mean, of course, that the partial sums $\sum_0^N$ tend to a limit.

That convergence implies $\beta_n \to 0$ is true even in real analysis. To

prove the opposite implication, we note that

$$|\sum_0^N - \sum_0^M|_p = |\sum_{M+1}^N \beta_n|_p$$
$$\leq \max_{M<n\leq N} |\beta_n|_p$$

by an obvious extension of the ultrametric inequality (iii*) to several summands. Hence $\left\{\sum_0^N \beta_n\right\}$ is a fundamental sequence, so tending to a limit by the completeness of $\mathbf{Q}_p$.

We are now in a position to give an explicit description of $\mathbf{Z}_p$. We write

$$\mathcal{A} = \{0, 1, \ldots, p-1\}.$$

Lemma 2. *The elements of $\mathbf{Z}_p$ are precisely the sums*

$$\alpha = \sum_0^\infty a_n p^n,$$

where

$$a_n \in \mathcal{A} \qquad (\text{all } n).$$

Proof. By the preceeding lemma, the infinite sum converges, and its value is clearly in $\mathbf{Z}_p$.

Now let $\alpha \in \mathbf{Z}_p$ be given. There is a $b \in \mathbf{Q}$ such that $|b - \alpha|_p < 1$, and it is easy to prove that there is precisely one $a_0 \in \mathcal{A}$ such that $|a_0 - b|_p < 1$. Then

$$\alpha = a_0 + p\alpha_1$$

where $|\alpha_1| \leq 1$, i.e. $\alpha_1 \in \mathbf{Z}_p$. Proceeding inductively, we get

$$\alpha = a_0 + a_1 p + \ldots + a_N p^N + \alpha_N p^{N+1}$$

with $\alpha_N \in \mathbf{Z}_p$.

For the final result we must distinguish between $p = 2$ and $p \neq 2$.

Lemma 3 ($p \neq 2$). *Let $\alpha \in \mathbf{Q}_p$ be a unit. A necessary and sufficient condition that $\alpha = \beta^2$ for some $\beta \in \mathbf{Q}_p$ in that there is some $\gamma \in \mathbf{Q}_p$ with*

$$|\alpha - \gamma^2|_p < 1.$$

Proof. Necessity is obvious. We have already in effect given a proof in the special case $p = 5$, $\alpha = -1$. That in the general case is similar: one

constructs inductively $\beta_1 = \gamma, \beta_2, \beta_3, \ldots$ such that

$$|\beta_n^2 - \alpha| \leq p^{-n}$$

$$|\beta_{n+1} - \beta_n| \leq p^{-n}$$

If we already have β_n, we take $\beta_{n+1} = \beta_n + \delta$, so

$$\beta_{n+1}^2 = \beta_n^2 + 2\beta_n\delta + \delta^2$$

and it is enough to take

$$\delta = (\alpha - \beta_n^2)/2\beta_n.$$

This lemma ceases to hold for $p = 2$ (consider $\alpha = 5$, $\beta = 1$). We have

Lemma 4 ($p = 2$). *Let $\alpha \in \mathbf{Q}_2$ be a unit. A necessary and sufficient condition that $\alpha = \beta^2$ for some $\beta \in \mathbf{Q}_2$ is that $|\alpha - 1| \leq 2^{-3}$.*

Proof. Here again, the necessity is obvious. For sufficiency we construct a sequence $\beta_1 = 1, \beta_2, \beta_3, \ldots$ as in the previous proof. The details are left to the reader.

We conclude this section by the promised sketch of the construction of $\mathbf{Q}_p$.

Denote by $\mathfrak{F}$ the set of fundamental sequences $\{a_n\}$ for $|\ |_p$, where $a_n \in \mathbf{Q}$. Then $\mathfrak{F}$ is a ring under componentwise addition and multiplication.

$$\{a_n\} + \{b_n\} = \{a_n + b_n\} : \{a_n\}\{b_n\} = \{a_n b_n\}.$$

A sequence $\{a_n\}$ is a null sequence if $a_n \to 0$ (p-adically). The set $\mathfrak{N}$ of null-sequences is clearly an ideal in $\mathfrak{F}$.

Let $\{a_n\} \in \mathfrak{F}$ but $\{a_n\} \notin \mathfrak{N}$. Then it is easy to see that there is at least one N such that $|a_N - a_n| < |a_N|_p$ for all $n > N$. Then $|a_n|_p = |a_N|_p$ for all $n \geq N$. We write $|\{a_n\}|_p = |a_N|_p$. If $a_n \neq 0$ for all n, it is now **easy to deduce that** $\{a_n^{-1}\} \in \mathfrak{F}$.

We show that $\mathfrak{N}$ is a maximal ideal in $\mathfrak{F}$. For, if not, let $\mathfrak{M}$ be a strictly bigger ideal than $\mathfrak{N}$. It must contain an $\{a_n\} \notin \mathfrak{N}$. Then only finitely many of the a_n can be 0, and replacing them by (say) 1 merely adds an element of $\mathfrak{N}$. Hence we can suppose that $a_n \neq 0$ for all n. Then $\{a_n^{-1}\} \in \mathfrak{F}$, and so $\{a_n^{-1}\}\{a_n\} \in \mathfrak{M}$. Hence we should have $\mathfrak{M} = \mathfrak{F}$, a contradiction. We conclude that $\mathfrak{N}$ is maximal, and thus $\mathfrak{F}/\mathfrak{N}$ is a field.

The field $\mathbf{Q}$ is mapped into $\mathfrak{F}/\mathfrak{N}$ by

$$r \to \{r\} \in \mathfrak{F}.$$

The function $|\{a_n\}|$ on $\mathfrak{F}$ induces a function on $\mathfrak{F}/\mathfrak{N}$ which is easily seen to be a valuation and to coincide with $|\ |_p$ on the image of $\mathbf{Q}$.

Finally, it is not difficult to check that $\mathfrak{F}/\mathfrak{N}$ is itself complete by a diagonal argument on a sequence of elements of $\mathfrak{F}$.

§2. Exercises

1. For each of the sets of p, m, r given, either find an $x \in \mathbf{Z}$ such that

$$|r - x|_p \leq p^{-m},$$

or show that no such x exists.

(i) $p = 257$, $r = 1/2$, $m = 1$;
(ii) $p = 3$, $r = 7/8$, $m = 2$;
(iii) $p = 3$, $r = 7/8$, $m = 7$;
(iv) $p = 3$, $r = 5/6$, $m = 9$;
(v) $p = 5$, $r = 1/4$, $m = 4$.

2. Construct further examples along the lines of Exercise 1 until the whole business seems trivial.

3. For given p, m, r either find an $x \in \mathbf{Z}$ such that

$$|r - x^2|_p \leq p^{-m}$$

or show that no such x exists.

(i) $p = 5$, $r = -1$, $m = 4$;
(ii) $p = 5$, $r = 10$, $m = 3$;
(iii) $p = 13$, $r = -4$, $m = 3$;
(iv) $p = 2$, $r = -7$, $m = 6$;
(v) $p = 7$, $r = -14$, $m = 4$;
(vi) $p = 7$, $r = 6$, $m = 3$;
(vii) $p = 7$, $r = 1/2$, $m = 3$.

4. As Exercise 2.

5. Let $p > 0$ be prime, $p \equiv 2\ (3)$. For any integer a, $p \nmid a$, show that there is an $x \in \mathbf{Z}_p$ with $x^3 = a$.