1
Valuations

PART 1: VALUATIONS

1. Valuations

The absolute value function on the field of the real numbers $\mathbb{R}$ or the field of the complex numbers $\mathbb{C}$ has the following fundamental properties. For all elements x and y we have

(i) $|x| \geqslant 0$, $|x| = 0$ if and only if $x = 0$
(ii) $|x + y| \leqslant |x| + |y|$ (the *triangle inequality*)
(iii) $|xy| = |x|\,|y|$

In this book we shall be concerned with the following generalization.

DEFINITION 1.1. Let K be a field. A *valuation* on K is a map $|\ |: K \to \mathbb{R}$ satisfying the rules (i), (ii), (iii), for all $x, y \in K$. The pair $(K, |\ |)$ is a *valued field*. Often we will write simply K instead of $(K, |\ |)$.

There are many examples of valued fields other than subfields of $\mathbb{C}$ with the ordinary absolute value function. The most important one is the field of the p-adic numbers, which we shall introduce in Section 4. An obvious example is the *trivial valuation* that can be defined on any field by setting

$$|x|: = \begin{cases} 0 \text{ if } x = 0 \\ 1 \text{ if } x \neq 0 \end{cases}$$

Let $(K, |\ |)$ be a valued field. The map $(x, y) \mapsto |x - y|$ is easily seen to be a metric on K which, in turn, yields a topology on K in the usual way (a set $U \subset K$ is called open if for each $a \in U$ there is $\delta > 0$ such that $\{ x \in K: |x - a| < \delta \} \subset U$. Then the union of arbitrarily many open sets is open, the intersection of finitely many open sets is open). The above metric and topology are said to be *induced* by the valuation $|\ |$.

**Exercise* 1.A. Let 1_K denote the unit element of a valued field $(K, |\ |)$. Show that $|1_K| = 1$, $|-x| = |x|$ $(x \in K)$, $|x^{-1}| = |x|^{-1}$ $(x \in K, x \neq 0)$, $|x - y| \geqslant ||x| - |y||$ $(x, y \in K)$.

Exercise 1.B. The topology induced by a valuation $|\ |$ on a field K makes K into a *topological field*. That is, prove the following.
(i) Addition $(x, y) \mapsto x + y$ and multiplication $(x, y) \mapsto xy$ are continuous maps $K \times K \to K$. (Here $K \times K$ carries the product topology.)
(ii) The maps $x \mapsto -x$ $(x \in K)$ and $x \mapsto x^{-1}$ $(x \in K, x \neq 0)$ are continuous.

Exercise 1.C. Show that the trivial valuation on a field K induces the discrete topology on K (i.e. each subset of K is open).

Before starting with the actual calculus in Chapter 2 we first develop the necessary theory on valued fields, study the basic examples and consider some important metrical aspects. Those who want to reach the main subject as quickly as possible may skip over the hard proofs of Sections 14–18. Also observe that Appendixes A.1, A.9 and A.10 logically belong to Chapter 1.

2. The strong triangle inequality

In this book we shall mainly be interested in valued fields $(K, |\ |)$ whose valuation satisfies the *strong triangle inequality*

$$|x+y| \leqslant \max(|x|, |y|) \qquad (x, y \in K)$$

rather than the general, weaker, form

$$|x+y| \leqslant |x| + |y| \qquad (x, y \in K)$$

Such a field is constructed in Example 2.1 below. Although it is not itself going to play a central role in the sequel, it is quite easy to understand and illustrative for what follows.

For a nonzero polynomial $f \in \mathbb{R}[X]$ given by

$$f = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \qquad (a_0, \ldots, a_n \in \mathbb{R}, a_n \neq 0)$$

we set $d(f) := n$ (the *degree* of f). Let $d(f) := -\infty$ if f is the zero polynomial. Then we have the following rules for d.

$$\left.\begin{aligned} d(f+g) &\leqslant \max(d(f), d(g)) \\ d(fg) &= d(f) + d(g) \end{aligned}\right\} \quad (f, g \in \mathbb{R}[X])$$

Let ρ be any real number, greater than 1. For $f \in \mathbb{R}[X]$ put

$$|f| := \begin{cases} 0 \text{ if } f = 0 \\ \rho^{d(f)} \text{ if } f \neq 0 \end{cases}$$

Then the above rules for d now look as follows.

$$\left.\begin{aligned} |f+g| &\leqslant \max(|f|, |g|) \\ |fg| &= |f|\,|g| \end{aligned}\right\} \quad (f, g \in \mathbb{R}[X])$$

Also we have trivially

$$|f| \geqslant 0;\ |f| = 0 \text{ if and only } f = 0 \qquad (f \in \mathbb{R}[X])$$

So, forgetting for a moment that $\mathbb{R}[X]$ is not a field, we see that $|\ |$ behaves like a valuation. The strong triangle inequality here simply expresses the fact that *if two polynomials each have a degree $\leqslant n$ then so has their sum.*

We now extend $|\ |$ to the field $\mathbb{R}(X)$ of rational functions.

EXAMPLE 2.1. (A valued field) *Let $\rho > 1$. For $f \in \mathbb{R}[X]$ put*

$$|f| := \begin{cases} 0 \text{ if } f = 0 \\ \rho^{d(f)} \text{ if } f \neq 0 \end{cases}$$

For $s \in \mathbb{R}(X)$ set

$$|s| := |f|\,|g|^{-1} \quad (s = fg^{-1}; f, g \in \mathbb{R}[X], g \neq 0)$$

Then $|\ |$ is a valuation on $\mathbb{R}(X)$ satisfying the strong triangle inequality

$$|s + t| \leqslant \max(|s|, |t|) \qquad (s, t \in \mathbb{R}(X))$$

Remarks.

1. The above construction yields infinitely many valuations on $\mathbb{R}(X)$, one for each $\rho > 1$. See, however, Section 9.
2. The constant polynomials form a subfield of $\mathbb{R}(X)$, isomorphic to $\mathbb{R}$. If a is such a constant polynomial then

$$|a| = \begin{cases} 1 \text{ if } a \neq 0 \\ 0 \text{ if } a = 0 \end{cases}$$

so that $|\ |$ does not induce the ordinary absolute value on $\mathbb{R}$, but the trivial valuation.
3. In the above example we may without harm replace $\mathbb{R}$ by an arbitrary field K. It follows that there are non-trivial examples of valued fields of characteristic $p \neq 0$!

**Exercise* 2.A. Show that the definition of $|\ |$ given in Example 2.1 is meaningful and that $(\mathbb{R}(X), |\ |)$ is indeed a valued field. More generally, prove the following. Let D be an integral domain and let $|\ |$ be a map of D into $\mathbb{R}$ satisfying the conditions (i), (ii), (iii) (see Section 1) for a valuation. Then $|\ |$ can uniquely be extended to a valuation on the quotient field of D. If $|\ |$ satisfies the strong triangle inequality then so does the extension.

Exercise 2.B. Let σ: $\mathbb{R}(X) \to \mathbb{R}(X)$ be the automorphism of $\mathbb{R}(X)$ sending X into X^{-1}. Then, with $|\ |$ as in Example 2.1, set $|s|_1 := |\sigma(s)|\ (s \in \mathbb{R}(X))$. Show that $|\ |_1$ is also a valuation on $\mathbb{R}(X)$ and that

$$|f|_1 = \rho^{-k} \qquad (f \in \mathbb{R}[X], f = a_k X^k + a_{k+1} X^{k+1} + \ldots + a_n X^n, a_k \neq 0)$$

*Exercise 2.C. Let $|\ |$ be a valuation on a field K satisfying the strong triangle inequality. Let $x_1, x_2, \ldots, x_n \in K$, where $n \in \mathbb{N}$. Show that $|x_1 + x_2 + \ldots + x_n| \leq \max(|x_1|, |x_2|, \ldots, |x_n|)$.

3. The p-adic integers

In Sections 3 and 4 we shall construct the valued field $\mathbb{Q}_p$ of the p-adic numbers. This field, whose valuation satisfies the strong triangle inequality, is the fundamental example throughout this book. In this section we make a start by defining the subring $\{x: |x| \leq 1\}$ of this field.

In the decimal system we denote nonnegative integers by expressions such as 1028 $(8 + 2\cdot 10 + 0\cdot 10^2 + 1\cdot 10^3)$. When we write down a sequence $a_n\, a_{n-1} \ldots a_0$ we mean $a_0 + a_1\, 10 + \ldots + a_n\, 10^n$. Here each a_i is one of the symbols 0, 1, ..., 9. Of course we may also write this as an infinite sequence

$$\ldots a_{n+2}\, a_{n+1}\, a_n \ldots a_0$$

where $a_i = 0$ for $i > n$. Further, instead of 10, we can choose any number $\in \{2, 3, \ldots\}$ as a base. These simple observations lead to the following.

DEFINITION 3.1. For any $n \in \{2, 3, \ldots\}$, let $\mathbb{Z}_n$ be the set of *all* infinite sequences

$$\ldots a_m\, a_{m-1} \ldots a_1\, a_0$$

where each a_m is one of the elements $0, 1, \ldots, n-1$. The elements of $\mathbb{Z}_n$ are *n-adic integers*. The sequences with $a_m = 0$ for sufficiently large m can be identified with the nonnegative integers. Thus we may write

$$\mathbb{N} \subset \mathbb{Z}_n$$

Remarks.
1. The elements of $\mathbb{Z}_n \setminus \{0, 1, 2, \ldots\}$ are sequences

$$\ldots . a_2\, a_1\, a_0$$

for which $a_m \neq 0$ for infinitely many m. One may be tempted to think of these elements as being 'infinitely large' or 'supernatural' numbers. However, in the sequel we shall see that, according to a quite natural point of view, these elements are limits of sequences of natural numbers.
2. One may wonder why the elements of $\mathbb{Z}_n$ are called n-adic *integers* rather than n-adic natural numbers. For this, see Proposition 3.2.

We can define a natural addition and multiplication in $\mathbb{Z}_n$ that extend the operations on $\mathbb{N}$. The following examples (in $\mathbb{Z}_{10}$) will make this clear.

```
. . . .8427159
. . . .5478563
-------------- +
. . . .3905722
```

```
    . . . .27159
    . . . .78563
---------------- X
    . . . .81477
  . . . .62954
. . . .35795
  . . . .17272
    . . . .90113
. . . . . . . . .
        .
      .
    .
  .
----------------
    . . . .92517
```

The ideas suggested in the above examples ('treat the elements of $\mathbb{Z}_n$ as ordinary integers') can of course be sharpened to correct definitions of addition and multiplication in $\mathbb{Z}_n$. (Let $x = \ldots . a_2\, a_1\, a_0$ and $y = \ldots . b_2\, b_1\, b_0$ be elements of $\mathbb{Z}_n$. Then $x + y = \ldots . c_2\, c_1\, c_0$, where the c_i are determined by

(i) $c_i \in \{0, 1, \ldots, n-1\}$ for each i
(ii) for each $m \in \{0, 1, 2, \ldots\}$

$$\sum_{i=0}^{m} c_i n^i \equiv \sum_{i=0}^{m} (a_i + b_i) n^i \qquad (\mathrm{mod}\ n^{m+1})$$

Similarly, $xy = \ldots . d_2\, d_1\, d_0$, where the d_i are determined by
(i) $d_i \in \{0, 1, \ldots, n-1\}$ for each i
(ii) for each $m \in \{0, 1, 2, \ldots\}$

$$\sum_{i=0}^{m} d_i n^i \equiv \left(\sum_{i=0}^{m} a_i n^i \right) \left(\sum_{i=0}^{m} b_i n^i \right) \qquad (\mathrm{mod}\ n^{m+1})$$

So, what we do is nothing but elementary school arithmetic.) Notice that in the second example we 'add' infinitely many elements of $\mathbb{Z}_{10}$. The 'sum' is well defined since every column has only finitely many (nonzero) entries. (See the preamble to Definition 3.4.)

A surprising fact is that one can subtract every element of $\mathbb{Z}_n$ from every other element of $\mathbb{Z}_n$. For example in $\mathbb{Z}_{10}$ we have

```
. . . .8427159
. . . .5478563
-------------- -
. . . .2948596
```

```
. . . .5478563
. . . .8427159
-------------- -
. . . .7051404
```

Subtracting familiar numbers we may obtain a non-familiar result. For example, in $\mathbb{Z}_{10}$ we have $3-5 = \ldots.999998$. The same subtraction in $\mathbb{Z}_5$ yields $\ldots.444443$ as an answer. The following proposition is not hard to prove.

PROPOSITION 3.2. *With the above addition and multiplication, $\mathbb{Z}_n$ is a commutative ring with $0 := \ldots.000000$ as a zero element and $1 := \ldots.000001$ as a unit. $\mathbb{Z}$ can be identified with a subring of $\mathbb{Z}_n$.*

Remark. Let $\ldots.a_2\,a_1\,a_0$ and $\ldots.b_2\,b_1\,b_0$ be elements of $\mathbb{Z}_n$. Suppose we want to know, for a certain m, the last $m+1$ digits $c_m, c_{m-1}, \ldots, c_0$ of their product (sum) $\ldots.c_2\,c_1\,c_0$. Then we only need to compute the product (sum) $d_k\,d_{k-1}\ldots d_0$ of the nonnegative integers $a_m\,a_{m-1}\ldots a_0$ and $b_m\,b_{m-1}\ldots b_0$ in the ordinary way and we get $c_0 = d_0, \ldots, c_m = d_m$.

Exercise 3.A. (Extension of the ordering to $\mathbb{Z}_n$) Let $x = \ldots.a_2\,a_1\,a_0$ and $y = \ldots.b_2\,b_1\,b_0$ be elements of $\mathbb{Z}_n$. Consider the following two definitions (*) and (**).
(*) $x >_1 y$ if there is an $m \in \{0,1,2,\ldots\}$ for which $a_m > b_m$ and $a_j = b_j$ for $j > m$.
(**) $x >_2 y$ if there is an $m \in \{0,1,2,\ldots\}$ for which $a_m > b_m$ and $a_j \geqslant b_j$ for $j > m$.
Show that (*) and (**) define partial orderings $>_1$ and $>_2$ on $\mathbb{Z}_n$ extending the natural ordering on $\mathbb{N}$ and that $>_1 \neq >_2$. Prove, however, that in general $x >_1 y$ does not imply $x+1 >_1 y+1$ and that $x >_2 y$ does not imply $x+1 >_2 y+1$.

Division in $\mathbb{Z}_n$ is less simple. For example, in $\mathbb{Z}_{10}$ we can find nonzero elements x and y for which $xy = 0$, as suggested below.

```
    ....10112
    ....03125
    ---------- X
    ....50560
   ....20224
  ....10112
 ....30336
....00000
      .
     .
    .
-------------
    ....00000
```

(The reader is asked to show that one can indeed fill in the dots in such a way as to obtain the zero sequence.) Thus, $\mathbb{Z}_{10}$ is not an integral domain and there is no way to extend $\mathbb{Z}_{10}$ to a field. The situation becomes better if n is a prime number.

PROPOSITION 3.3. *Let p be a prime number. Then $\mathbb{Z}_p$ is an integral domain. An element $\ldots a_2 a_1 a_0$ of $\mathbb{Z}_p$ has an inverse in $\mathbb{Z}_p$ if and only if $a_0 \neq 0$.*

Proof. As $\ldots a_2a_1a_00 = p(\ldots a_2a_1a_0)$, $\ldots a_2a_1a_000 = p^2(\ldots a_2a_1a_0)$, etc. it suffices to show the second statement. If $a_0 = 0$ then the product of $\ldots a_0$ and any element of $\mathbb{Z}_p$ ends with a 0, so certainly $\ldots a_2a_1a_0$ has no inverse. Suppose $a_0 \neq 0$. We prove inductively that we can find $x_0, x_1, \ldots \in \{0,1,\ldots,p-1\}$ such that the product of $\ldots x_2x_1x_0$ and $\ldots a_2a_1a_0$ equals $\ldots 001$. By looking at the 'long multiplication'

$$
\begin{array}{r}
\ldots a_2 a_1 a_0 \\
\ldots x_2 x_1 x_0 \\
\hline \times \\
\ldots \\
\ldots \\
\ldots \\
\hline \\
\ldots 0\,0\,1
\end{array}
$$

we see that we have to sole the following congruences.

$$x_0 a_0 \equiv 1 \pmod{p}$$
$$x_0 a_1 + x_1 a_0 + p^{-1}(a_0 x_0 - 1) \equiv 0 \pmod{p}, \text{ etc.}$$

The essential point is that for each $n \in \mathbb{N}$ it is required that

$$x_{n+1} a_0 \equiv c_{n+1} \pmod{p}$$

where c_{n+1} depends only on $x_0, x_1, \ldots, x_n$. Whatever c_{n+1} is, we always can solve this congruence since $a_0 \not\equiv 0 \pmod{p}$ and $\mathbb{Z}/p\mathbb{Z}$ is a field.

Exercise 3.B. Describe how at the p-adic elementary school one would carry out a division $(\ldots b_2b_1b_0) \div (\ldots a_2a_1a_0)$ in $\mathbb{Z}_p$. (Assume that $a_0 \neq 0$.)

Exercise 3.C. Let $n \in \{2,3,4,\ldots\}$. Show that an element $\ldots a_2a_1a_0$ of $\mathbb{Z}_n$ has an inverse if and only if the greatest common divisor of a_0 and n equals 1.

We proceed to investigate $\mathbb{Z}_p$ where p is a prime number. In particular we want to introduce a 'valuation' on $\mathbb{Z}_p$ (that can be extended to a valuation

on the quotient field of $\mathbb{Z}_p$, see Section 4). Let us return to the first example of a multiplication we have given for $\mathbb{Z}_{10}$. We mentioned there that the final 'addition' succeeds since every column contains only finitely many digits. More generally, if we are given a sequence $x_1, x_2, \ldots$ where $x_i \in \mathbb{Z}_p$ for every i we can formally define $\sum_{i=1}^{\infty} x_i$ if, from a certain i_0 on, the last digit of x_i is always 0, from a certain i_1 on the last two digits of x_i are 00, etc. If we want to consider $\sum_{i=1}^{\infty} x_i$ as the 'limit' of $\sum_{i=1}^{n} x_i$ for $n \to \infty$ it is intuitively clear that the x_i must 'tend to zero'. So we come to the somewhat unusual conclusion that an element of $\mathbb{Z}_p$ must be called 'small' if it ends in many zeros. This implies that an element of $\mathbb{N}$ is 'small' in the sense of $\mathbb{Z}_p$ if it is divisible by a large power of p. Thus, the sequence $1, p, p^2, \ldots$ will tend to zero in $\mathbb{Z}_p$! We formalize this as follows.

DEFINITION 3.4. Let p be a prime number and let $\ldots a_2 a_1 a_0$ be an element of $\mathbb{Z}_p$. The *order* of $\ldots a_2 a_1 a_0$ is the smallest m for which $a_m \neq 0$. More precisely,

$$\operatorname{ord}_p(\ldots a_2 a_1 a_0) := \begin{cases} \infty \text{ if } a_i = 0 \text{ for all } i \\ \min\{s : a_s \neq 0\} \text{ otherwise} \end{cases}$$

We set

$$|\ldots a_2 a_1 a_0|_p := \begin{cases} 0 \text{ if } a_i = 0 \text{ for all } i \\ p^{-\operatorname{ord}_p(\ldots a_2 a_1 a_0)} \text{ otherwise} \end{cases}$$

The function $|\ |_p$ is the *p-adic valuation* on $\mathbb{Z}_p$.

PROPOSITION 3.5. *Let p be a prime number and let $x, y \in \mathbb{Z}_p$.*
(i) $|x|_p \geqslant 0$; $|x|_p = 0$ *if and only if* $x = 0$.
(ii) $|x + y|_p \leqslant \max(|x|_p, |y|_p)$ (*the strong triangle inequality*).
(iii) $|xy|_p = |x|_p\, |y|_p$.

The easy proof is left to the reader. The strong triangle inequality for $|\ |_p$ reflects the fact that *if*, for some $s \in \{0,1,2,\ldots\}$, *two integers are divisible by p^s then so is their sum*. Observe that the set of values of $|\ |_p$ equals $\{0, 1, p^{-1}, p^{-2}, \ldots\}$.

Exercise 3.D. (Other valuations on $\mathbb{Z}_p$) Let $\rho \in \mathbb{R}$, $\rho > 1$. Define

$$|\ldots a_2 a_1 a_0|'_p := \begin{cases} 0 \text{ if } a_i = 0 \text{ for all } i \\ \rho^{-\operatorname{ord}_p(\ldots a_2 a_1 a_0)} \text{ otherwise} \end{cases}$$

Show that the properties (i), (ii), (iii) of Proposition 3.5 hold for $|\ |'_p$ in place of $|\ |_p$. Compare Remark 1 following Example 2.1 and Exercise 9.A.

Exercise 3.E. Find the '5-adic representation' $\ldots a_2 a_1 a_0$ ($a_i \in \{0,1,2,3,4,\}$) of the numbers 15, -1 and -3. The numbers 2,3,4 have inverses in $\mathbb{Z}_5$. Find their 5-adic representations.

Exercise 3.F. Let p be an odd prime. Show that $2^{-1} = \ldots a_2 a_1 a_0$ in $\mathbb{Z}_p$ where $a_0 = \frac{1}{2}(p+1)$ and $a_i = \frac{1}{2}(p-1)$ for $i \geqslant 1$.

Exercise 3.G. (On $\sqrt{-1}$) Show that the equation $x^2 + 1 = 0$ has no solutions in $\mathbb{Z}_3$ but has two solutions in $\mathbb{Z}_5$.

Exercise 3.H. Compute $\operatorname{ord}_p(p^n!)$ and $|p^n!|_p$ (p prime, $n \in \mathbb{N}$).

**Exercise* 3.I. (Basic facts on $\mathbb{Z}_p$. See the frontispiece for a 'picture' of $\mathbb{Z}_7$) Let p be a prime number. Prove the following.
(i) An element x of $\mathbb{Z}_p$ has an inverse in $\mathbb{Z}_p$ if and only if $|x|_p = 1$.
(ii) If x is a nonzero element of $\mathbb{Z}_p$ then $x = p^{\operatorname{ord}_p(x)} y$ where $y \in \mathbb{Z}_p$, $|y|_p = 1$.
(iii) Set

$$p\mathbb{Z}_p := \{py : y \in \mathbb{Z}_p\}$$

Then $p\mathbb{Z}_p$ is a maximal ideal of $\mathbb{Z}_p$ and $\mathbb{Z}_p/p\mathbb{Z}_p$ is a field of p elements. The additive cosets

$$p\mathbb{Z}_p,\ 1+p\mathbb{Z}_p,\ \ldots,\ p-1+p\mathbb{Z}_p$$

form a partition of $\mathbb{Z}_p$. For each $j \in \{0,1,2,\ldots,p-1\}$ we have

$$j+p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x-j|_p < 1\} = \{x \in \mathbb{Z}_p : |x-j|_p \leqslant p^{-1}\}$$

(iv) Let $p^n\mathbb{Z}_p := \{p^n y : y \in \mathbb{Z}_p\}$ ($n \in \mathbb{N}$). The cosets $p^n\mathbb{Z}_p$, $1+p^n\mathbb{Z}_p$, $\ldots$, $p^n-1+p\mathbb{Z}_p$ form a partition of $\mathbb{Z}_p$. For each $j \in \{0,1,\ldots,p^n-1\}$ we have $j+p^n\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x-j|_p < p^{-n+1}\} = \{x \in \mathbb{Z}_p : |x-j|_p \leqslant p^{-n}\}$.

Exercise 3.J. (Valuation on $\mathbb{Z}_n$) Let $n \in \{2, 3, 4, \ldots\}$ be not a prime number. Define an 'n-adic valuation' $|\ |_n$ on $\mathbb{Z}_n$ in the spirit of Definition 3.4. Are the properties (i), (ii), (iii) of Proposition 3.5 true for p replaced by n and $x, y \in \mathbb{Z}_n$?

Exercise 3.K. (Some p-adic numerical analysis) Let p be a prime number, let $a \in \mathbb{Z}$, $|a|_p = 1$. We shall describe a method to approximate the inverse a^{-1} of a in $\mathbb{Z}_p$ by means of integers which is more efficient than the one that follows from the proof of Proposition 3.3.
(i) Choose $x_0 \in \mathbb{Z}$ such that $|1-x_0 a|_p < 1$. The formula $1-x_{n+1}a = (1-x_n a)^2$, i.e. $x_{n+1} = x_n(2-x_n a)$ defines a sequence $x_0, x_1, \ldots$ of integers. Show that $|x_n - a^{-1}|_p \leqslant p^{-2^n}$ ($n \in \mathbb{N}$). In other words, if

$$x_n = \ldots s_2 s_1 s_0,\ a^{-1} = \ldots a_2 a_1 a_0$$

then $a_j = s_j$ for $0 \leqslant j < 2^n$. Observe that this method is quadratic and that we do not have to worry about rounding errors as x_n gives us the exact values of a_j $(0 \leqslant j < 2^n)$.
(ii) Choose $p = 5$, $a = 23$ (twenty-three) and use (i) to find an integer s for which $|a^{-1} - s|_p \leqslant p^{-8}$.

4. The p-adic numbers

In this section we shall extend $|\ |_p$ to a valuation on the quotient field of $\mathbb{Z}_p$.

FROM NOW ON p IS A PRIME NUMBER

For a nonzero element x of $\mathbb{Z}_p$ we have, according to Exercise 3.I (ii)

$$x = p^n y$$

where $n = \mathrm{ord}_p(x)$ and y is invertible in $\mathbb{Z}_p$. So, to find a concrete representation of 'the smallest field that contains $\mathbb{Z}_p$', we must find an inverse for p. Now the common notation in base p for p^{-1} is 0.1; p^{-2} is written 0.01 etc. This leads to the following definition.

DEFINITION 4.1. Let $\mathbb{Q}_p$ be the set of all two-sided sequences

$$\ldots a_2 a_1 a_0 . a_{-1} a_{-2} \ldots$$

for which $a_i \in \{0, 1, \ldots, p-1\}$ for each i and such that $a_{-n} = 0$ for large n. The elements of $\mathbb{Q}_p$ are *p-adic numbers*. The sequences $\ldots a_2 a_1 a_0 . a_{-1} a_{-2} \ldots$ for which $a_{-1} = a_{-2} = \ldots = 0$ can be identified with the p-adic integers. So we may write

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

Addition and multiplication in $\mathbb{Z}_p$ can be extended to $\mathbb{Q}_p$ in a natural way. (Formally, let $x = \ldots a_2 a_1 a_0 . a_{-1} a_{-2} \ldots$ and $y = \ldots b_2 b_1 b_0 . b_{-1} b_{-2} \ldots$ be elements of $\mathbb{Q}_p$ and suppose that $a_{-n} = b_{-n} = 0$ for $n > N$. Then $x' := \ldots a_0\, a_{-1} \ldots a_{-N}$ and $y' := \ldots b_0 b_{-1} \ldots b_{-N}$ are p-adic integers. Let $x' + y' = \ldots c_2 c_1 c_0$. Define $x + y$ to be $\ldots c_N . c_{N-1} \ldots c_0 00 \ldots$. Similarly one defines the product xy of x and y.) Then the inverse of $p = 1.0$ becomes 0.1, the inverse of $p^2 = 10.0$ becomes 0.01, etc. It follows that every nonzero element of $\mathbb{Q}_p$ can be written as $p^n y$ where $n \in \mathbb{Z}$ and $y \in \mathbb{Z}_p$, $|y|_p = 1$. With this in mind, the following is not hard to prove.

PROPOSITION 4.2. *$\mathbb{Q}_p$ is a field containing $\mathbb{Q}$ as a subfield and $\mathbb{Z}_p$ as a subring. $\mathbb{Q}_p$ is (isomorphic to) the quotient field of $\mathbb{Z}_p$.*

Now we extend $|\ |_p$ to $\mathbb{Q}_p$.