
Chapter 1

Arithmetic of the p -adic Numbers

The aim of the first chapter of this book is to introduce its main protagonist: the *field of p -adic numbers* \mathbb{Q}_p , defined for any prime p .

Just like the field of real numbers \mathbb{R} , the field \mathbb{Q}_p can be constructed from the rational numbers \mathbb{Q} as its *completion* with respect to a certain norm. This norm depends on the prime number p and differs drastically from the standard Euclidean norm used to define \mathbb{R} . Nevertheless, in each of the two cases, completion yields a *normed field* (\mathbb{R} and \mathbb{Q}_p), and this general concept is studied in detail in §1.2. But first (§1.1), we recall the completion procedure in the more familiar case of the reals (this takes us from \mathbb{Q} to \mathbb{R}), and only then do we go on to its generalization to arbitrary normed fields (§1.3).

Putting these preliminaries aside, we come to the central section of Chapter 1 (§1.4), where the construction of \mathbb{Q}_p is actually carried out.

§§1.5–1.8 are devoted to the algebraic and structural properties of the p -adic numbers. Here, as in subsequent parts, we will be constantly comparing \mathbb{Q}_p and \mathbb{R} , stressing both their similarities and their differences. Finally, §§1.9 and 1.10 treat additional topics and are not closely related to the rest of the book.

1.1. From \mathbb{Q} to \mathbb{R} ; the concept of completion

The real numbers, denoted by \mathbb{R} , are obtained from the rationals by a procedure called *completion*. This procedure can be applied to any *metric space*, i.e., to a space M with a metric d on it. Recall that a function

$$d : M \times M \rightarrow \mathbb{R}$$

defined on all ordered pairs (x, y) of elements of a nonempty set M is said to be a *metric* if it possesses the following properties:

- (1) $d(x, y) \geq 0$; $d(x, y) = 0$ if and only if $x = y$;
- (2) $d(x, y) = d(y, x) \forall x, y \in M$;
- (3) $d(x, y) \leq d(x, z) + d(z, y) \forall x, y, z \in M$.

The function d is also called the *distance function*.

We say that a sequence $\{r_n\}$ in a metric space M is a *Cauchy sequence* if for any $\varepsilon > 0$ there exists a positive integer N such that $n, m > N$ implies $d(r_n, r_m) < \varepsilon$. If any Cauchy sequence in M has a limit in M , then M is called a *complete metric space*.

Theorem 1.1 (Completion Theorem). *Every metric space M can be completed, i.e., there exists a metric space (\widehat{M}, D) such that*

- (1) \widehat{M} is complete with respect to the metric D ;
- (2) \widehat{M} contains a subset \widehat{M}_0 isometric to M ;
- (3) \widehat{M}_0 is dense in \widehat{M} (i.e., each point in \widehat{M} is a limit point for \widehat{M}_0).

The proof that can be found e.g. in [13, Theorem 76] consists in an explicit construction of the completion \widehat{M} and the metric D on it. We start with the collection $\{M\}$ of all Cauchy sequences in M , convergent or not, and turn it into a metric space. But first we introduce an equivalence relation on $\{M\}$: two Cauchy sequences a_n and b_n are called *equivalent*, we write $\{a_n\} \sim \{b_n\}$, if $d(a_n, b_n) \rightarrow 0$. (It is easy to check that this is an equivalence relation on $\{M\}$.) We define \widehat{M} to be the set of equivalence classes, $\widehat{M} = \{M\} / \sim$. The metric D between two equivalence classes of Cauchy sequences

$A = (\{a_n\})$ and $B = (\{b_n\})$ is defined by the formula

$$(1.1) \quad D(A, B) = \lim_{n \rightarrow \infty} d(a_n, b_n).$$

We leave it to the reader to check that the limit above always exists and does not depend on the choice of representatives in the equivalence classes (Exercise 7) and that D indeed is a metric on \widehat{M} (Exercise 8). In §1.3 we will give the complete proof of this theorem in the particular case of metric spaces called *normed fields*, which includes \mathbb{Q} .

The completion procedure applied to $M = \mathbb{Q}$ with the usual *Euclidean distance* between rational numbers,

$$(1.2) \quad d(r_1, r_2) = |r_1 - r_2|,$$

yields the real numbers \mathbb{R} . Notice that this distance “came from” the *Euclidean norm* on \mathbb{Q} , which is the ordinary *absolute value*.

Another description of the completion of \mathbb{Q} yielding \mathbb{R} , more familiar and less sophisticated than the one above, is based on infinite decimal fractions. Every positive real number a can be written as an infinite decimal fraction

$$(1.3) \quad a = \sum_{k=m}^{\infty} a_k 10^{-k},$$

where m is a certain integer and the coefficients or *digits* a_k take the values

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

This representation is unique unless $a_k = 0$ for all $k > n$ and $a_n \neq 0$, in which case a has a second representation with $a'_k = a_k$ for $k < n$, $a'_n = a_n - 1$, and $a'_k = 9$ for all $k > n$. Conversely, any infinite decimal fraction represents a point on the “number axis”; thus it is convenient to identify *real numbers* with infinite decimal fractions.

If represented as infinite decimal fractions, rational numbers are characterized by the property that they are eventually periodic (Exercise 2). It is easy to construct a Cauchy sequence of rational numbers which has no limit in \mathbb{Q} :

$$.1, .1011, .10110111, .1011011101111, \dots;$$

hence \mathbb{Q} is not complete with respect to the Euclidean distance. On the other hand, any equivalence class of Cauchy sequences of rational numbers has a representative which is a sequence of partial sums of a series of the form (1.3) whose limit is an infinite decimal fraction (Exercise 1), and the same is true for any Cauchy sequence of infinite decimal fractions. In other words, the set of real numbers is complete with respect to the Euclidean distance (Exercise 3), and the construction of real numbers by means of infinite decimal fractions is equivalent to the completion procedure with respect to the Euclidean distance.

This representation can be generalized to the *representation to the base g* , where g is an integer greater than or equal to 2 and thus

$$a = \sum_{k=m}^{\infty} a_k g^{-k},$$

where the coefficients a_k take values in the set $\{0, 1, \dots, g-1\}$. Note that the exponents $-k$ of g are descending and tend to $-\infty$.

The following notions can be defined in every metric space.

Definition 1.2. Let (M, d) be a metric space, and \mathbb{R}^+ denotes the set of positive real numbers. The *open ball* of radius $r \in \mathbb{R}^+$ centered at $a \in M$ is the set

$$B(a, r) = \{x \in M \mid d(a, x) < r\}.$$

The *closed ball* of radius $r \in \mathbb{R}^+$ centered at $a \in M$ is the set

$$\overline{B}(a, r) = \{x \in M \mid d(a, x) \leq r\}.$$

A set $A \subset M$ is called *open* if for any $x \in M$ there exists an open ball $B(a, r) \subset M$ containing x . A set $A \subset M$ is called *closed* if its complement $M \setminus A$ is open.

Practically, completion of a metric space is often obtained by a different construction described below:

Proposition 1.3. *Let M be a complete metric space and let X be a subset of M . Then X is complete if and only if it is closed in M . In particular, the closure of X in M can be taken as its completion.*

Example 1.4. The completion of an open interval (a, b) with respect to the usual Euclidean distance is the segment $[a, b]$, the closure of (a, b) in \mathbb{R} .

For other examples, see Exercise 5.

Exercises 1–8

Exercise 1. Prove that any Cauchy sequence of rational numbers with respect to the Euclidean distance has a representative which is a sequence of partial sums of a series of the form (1.3).

Exercise 2. Prove that a number is rational if and only if its representation by an infinite decimal fraction is eventually periodic.

Exercise 3. Use the representation of real numbers as infinite decimal fractions to prove that the set of real numbers is complete with respect to the Euclidean distance, i.e., that any Cauchy sequence of real numbers has a limit.

Exercise 4. Prove Proposition 1.3.

Exercise 5. Prove that the following metric spaces are not complete, and construct their completions:

- (1) \mathbb{R} with the distance $d(x, y) = |\arctan x - \arctan y|$;
- (2) \mathbb{R} with the distance $d(x, y) = |e^x - e^y|$.

Exercise 6. Prove that a metric space is complete if and only if the intersection of every nested sequence of closed balls $\{B_n\}$, $B_1 \supset B_2 \supset B_3 \supset \dots$ whose radii approach zero consists of a single point.

Exercise 7. Let $\{a_n\}$ and $\{b_n\}$ be two Cauchy sequences in a metric space (M, d) . Prove that the limit $\lim_{n \rightarrow \infty} d(a_n, b_n)$ exists and does not depend on the choice of representatives in the equivalence classes, i.e., if $\{a'_n\} \sim \{a_n\}$ and $\{b'_n\} \sim \{b_n\}$, then $\lim_{n \rightarrow \infty} d(a_n, b_n) = \lim_{n \rightarrow \infty} d(a'_n, b'_n)$.

Exercise 8. Prove that D defined in (1.1) is a metric on \widehat{M} .

1.2. Normed fields

Both rational numbers and real numbers are prime examples of an algebraic structure called a field. A *field* F is a set with two binary operations usually called *addition* and *multiplication* which satisfy the most basic properties of these two operations for numbers. Namely,

- (1) $\forall a, b \in F, a + b = b + a$ (commutativity of addition),
- (2) $\forall a, b, c \in F, a + (b + c) = (a + b) + c$ (associativity of addition),
- (3) $\exists 0 \in F$ such that $\forall a \in F, 0 + a = a$ (existence of zero),
- (4) $\forall a \in F \exists -a \in F$ such that $a + (-a) = 0$ (existence of the additive inverse),
- (5) $\forall a, b \in F, a \cdot b = b \cdot a$ (commutativity of multiplication),
- (6) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity of multiplication),
- (7) $\exists 1 \in F$ such that $\forall a \in F^\times = F \setminus \{0\}, 1 \cdot a = a$ (existence of identity),
- (8) $\forall a \in F^\times \exists a^{-1} \in F^\times$ such that $a \cdot a^{-1} = 1$ (existence of the multiplicative inverse),
- (9) $\forall a, b, c \in F, a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivity),
- (10) $0 \neq 1$.

An algebraic structure with only one binary operation satisfying the properties (1) – (4) is called an *abelian (or commutative) group*. Correspondingly, F with addition is called the *additive group* of the field F , and F^\times with multiplication is called the *multiplicative group* of the field F . An algebraic structure with two binary operations satisfying the properties (1) – (6) and (9) is called a *commutative ring*.

An important property of a field is that it does not contain *zero divisors*, i.e., $a, b \in F^\times$ such that $a \cdot b = 0$ (see Exercise 9).

Definition 1.5. Let F be a field. A *norm* on F is a map denoted $\|\cdot\|$ from F to the nonnegative real numbers such that

- (1) $\|x\| = 0$ if and only if $x = 0$;
- (2) $\|xy\| = \|x\| \|y\| \quad \forall x, y \in F$;
- (3) $\|x + y\| \leq \|x\| + \|y\| \quad \forall x, y \in F$ (*the triangle inequality*).

The norm is called *trivial* if $\|0\| = 0$ and $\|x\| = 1$ for all $x \neq 0$.

Notice that, for any natural number $n \in \mathbb{N}$, we have

$$n \cdot 1 := \underbrace{1 + \dots + 1}_{n \text{ times}} \in F.$$

We shall denote this element by the same symbol n as the corresponding natural number.

Proposition 1.6. *For any $x, y \in F$ we have*

- (a) $\|1\| = \|-1\| = 1$;
- (b) $\|x\| = \|-x\|$;
- (c) $\|x \pm y\| \geq |\|x\| - \|y\||$;
- (d) $\|x - y\| \leq \|x\| + \|y\|$;
- (e) $\|x/y\| = \|x\|/\|y\|$;
- (f) $\|n\| \leq n \ \forall n \in \mathbb{N}$.

Proof.

- (a) $\|1\| = \|\pm 1 \cdot \pm 1\| = \|\pm 1\|^2 \implies \|\pm 1\| = 1$.
- (b) $\|-x\| = \|(-1) \cdot x\| = 1 \cdot \|x\|$.
- (c) Follows from (b) and the triangle inequality for the norm (see Exercise 10).
- (d) Follows from (b) and the triangle inequality.
- (e) Follows from (a) and the property (2) of the norm.
- (f) Follows by induction from (a) and the triangle inequality.

□

Let $d(x, y) = \|x - y\|$. It follows immediately from Definition 1.5 and Proposition 1.6 that d is a distance function; indeed, Definition 1.5(1) implies that $d(x, y) = 0$ if and only if $x = y$, while Proposition 1.6(b) implies symmetry, and Proposition 1.6(d) yields the triangle inequality. We say that this distance is *induced by* the norm $\|\cdot\|$ and we will regard $(F, \|\cdot\|)$ as a metric space.

Definition 1.7. A sequence $\{a_n\}$ in F is said to be

- *bounded* if there is a constant $C > 0$ such that

$$\|a_n\| \leq C \quad \forall n;$$

- a *null* sequence if

$$\lim_{n \rightarrow \infty} \|a_n\| = 0,$$

i.e., for any $\varepsilon > 0$ there is an N such that for all $n > N$ $\|a_n\| < \varepsilon$;

- a *Cauchy* sequence if

$$\lim_{n, m \rightarrow \infty} \|a_n - a_m\| = 0,$$

i.e., for any $\varepsilon > 0$ there is an N such that for all $n, m > N$ we have $\|a_n - a_m\| < \varepsilon$;

- *convergent* to $a \in F$ (we write $a = \lim_{n \rightarrow \infty} a_n$) if

$$\lim_{n \rightarrow \infty} \|a_n - a\| = 0,$$

i.e., for any $\varepsilon > 0$ there is an N such that for all $n > N$ $\|a_n - a\| < \varepsilon$.

It follows from the definition that any null sequence converges to 0, and it follows from the triangle inequality that any converging sequence is a Cauchy sequence: suppose $\lim_{n \rightarrow \infty} a_n = a$; then

$$\|a_n - a_m\| = \|a_n - a + a - a_m\| \leq \|a_n - a\| + \|a - a_m\| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

for $n, m > N$ chosen for $\varepsilon/2$ in the definition of limit. In particular, every null sequence is a Cauchy sequence. Further properties are listed below and are obtained by the same standard technique (Exercise 11).

- (1) Every Cauchy sequence is bounded.
- (2) Let $\{a_n\}$ be a Cauchy sequence and let $\{n_1, n_2, \dots\}$ be an increasing sequence of positive integers. If the subsequence a_{n_1}, a_{n_2}, \dots is a null sequence, then $\{a_n\}$ itself is a null sequence.
- (3) If $\{a_n\}$ and $\{b_n\}$ are null sequences, so is $\{a_n \pm b_n\}$, and if $\{a_n\}$ is a null sequence and $\{b_n\}$ is a bounded sequence, then $\{a_n b_n\}$ is a null sequence.

The following is a simple but very useful result.

Proposition 1.8. $\|x\| < 1$ if and only if $\lim_{n \rightarrow \infty} x^n = 0$.

Proof. Let $\|x\| < 1$. Since $\|x^n\| = \|x\|^n$, we obtain

$$\lim_{n \rightarrow \infty} \|x^n\| = 0,$$

i.e., $\lim_{n \rightarrow \infty} x^n = 0$. Conversely, if $\|x\| \geq 1$, then for all positive n we have $\|x^n\| \geq 1$, and therefore $0 \neq \lim_{n \rightarrow \infty} x^n$. \square

Definition 1.9. We say that two metrics d_1 and d_2 on F are *equivalent* if a sequence is Cauchy with respect to d_1 if and only if it is Cauchy with respect to d_2 . We say that two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ are *equivalent* ($\|\cdot\|_1 \sim \|\cdot\|_2$) if they induce equivalent metrics.

Proposition 1.10. Let $\|\cdot\|_1$ and $\|\cdot\|_2$ be two norms on a field F . Then $\|\cdot\|_1 \sim \|\cdot\|_2$ if and only if there exists a positive real number α such that

$$(1.4) \quad \|x\|_2 = \|x\|_1^\alpha, \quad \forall x \in F.$$

Proof. Suppose $\|\cdot\|_1 \sim \|\cdot\|_2$. If $\|\cdot\|_1$ is trivial, then by Exercise 12 $\|\cdot\|_2$ is also trivial, and hence (1.4) is satisfied for any α .

If $\|\cdot\|_1$ is nontrivial, then we can choose an element $a \in F$ such that $\|a\|_1 \neq 1$. Replacing a by a^{-1} if necessary, we can assume that $\|a\|_1 < 1$. Define

$$\alpha = \frac{\log \|a\|_2}{\log \|a\|_1}.$$

Notice that since the norms are equivalent, by Exercise 13 we have $\|a\|_2 < 1$ as well; hence both logarithms are negative and $\alpha > 0$.

We will show that this α satisfies (1.4). First take $x \in F$ with $\|x\|_1 < 1$; the cases $\|x\|_1 > 1$ and $\|x\|_1 = 1$ will follow from Exercise 13. Consider the set

$$(1.5) \quad S = \{r = m/n \mid m, n \in \mathbb{N}, \|x\|_1^r < \|a\|_1\}.$$

For any $r \in S$ we have

$$\|x\|_1^m < \|a\|_1^n, \text{ so } \left\| \frac{x^m}{a^n} \right\|_1 < 1.$$

Then by Exercise 13,

$$\left\| \frac{x^m}{a^n} \right\|_2 < 1,$$

and so $\|x\|_2^m < \|a\|_2^n$, and $\|x\|_2^r < \|a\|_2$. The same argument holds with $\|\cdot\|_2$ and $\|\cdot\|_1$ interchanged, so we also find that

$$(1.6) \quad S = \{r = m/n \mid m, n \in \mathbb{N}, \|x\|_2^r < \|a\|_2\}.$$

By taking logarithms, we can rewrite conditions (1.5) and (1.6) as

$$(1.7) \quad r > \frac{\log \|a\|_1}{\log \|x\|_1}, \quad r > \frac{\log \|a\|_2}{\log \|x\|_2}$$

since all logarithms involved are negative. But then we must have

$$\frac{\log \|a\|_1}{\log \|x\|_1} = \frac{\log \|a\|_2}{\log \|x\|_2},$$

because otherwise there would be a rational r between these two numbers and only one of the conditions in (1.7) would be satisfied. Therefore,

$$\frac{\log \|x\|_2}{\log \|x\|_1} = \frac{\log \|a\|_2}{\log \|a\|_1} = \alpha,$$

and (1.4) follows.

Conversely, suppose $\|x\|_2 = \|x\|_1^\alpha$, and suppose $\{a_n\}$ is a Cauchy sequence with respect to the distance induced by $\|\cdot\|_1$. Given $\epsilon > 0$, let N be chosen for $\epsilon^{1/\alpha}$. Then for $n, m > N$ we have $\|x_n - x_m\|_1 < \epsilon^{1/\alpha}$ and therefore $\|x_n - x_m\|_2 < \epsilon$. The same argument holds with $\|\cdot\|_2$ and $\|\cdot\|_1$ interchanged, which concludes the proof. \square

Now we will describe all norms on \mathbb{Q} equivalent to the absolute value $|\cdot|$.

Proposition 1.11. $\|x\| = |x|^\alpha$, $\alpha > 0$, is a norm on \mathbb{Q} if and only if $\alpha \leq 1$. In that case it is equivalent to the norm $|\cdot|$.

Proof. Suppose $\alpha \leq 1$. The first two properties of the norm are obvious, so we only need to check the triangle inequality. Assume that $|y| \leq |x|$. Then

$$\begin{aligned} |x+y|^\alpha &\leq (|x|+|y|)^\alpha = |x|^\alpha \left(1 + \frac{|y|}{|x|}\right)^\alpha \\ &\leq |x|^\alpha \left(1 + \frac{|y|}{|x|}\right) \leq |x|^\alpha \left(1 + \frac{|y|^\alpha}{|x|^\alpha}\right) = |x|^\alpha + |y|^\alpha. \end{aligned}$$

The first inequality follows from the fact that $t^\alpha \leq t$ for $t \geq 1$, and the second because $t^\alpha \geq t$ for $0 \leq t \leq 1$.

On the other hand, if $\alpha > 1$, the triangle inequality is not satisfied: for example, $|1 + 1|^\alpha = 2^\alpha > |1|^\alpha + |1|^\alpha = 2$. \square

It will follow from Ostrowski's Theorem (Theorem 1.50) that Proposition 1.11 describes all norms on \mathbb{Q} equivalent to the absolute value $|\cdot|$.

Definition 1.12. A norm is called *non-Archimedean* if it satisfies the additional condition

$$(4) \quad \|x + y\| \leq \max(\|x\|, \|y\|);$$

otherwise, we say that the norm is *Archimedean*.

Remark 1.13. The condition (4) of the norm implies the condition (3), the triangle inequality, since $\max(\|x\|, \|y\|)$ does not exceed the sum $\|x\| + \|y\|$. We will call this property the *strong triangle inequality*.

The metric induced by a non-Archimedean norm is said to be an *ultra-metric*. Instead of the triangle inequality for the usual metric

$$d(x, z) \leq d(x, y) + d(y, z),$$

it satisfies the strong triangle inequality

$$d(x, z) \leq \max(d(x, y), d(y, z)).$$

The corresponding metric spaces are called *ultra-metric spaces*.

The following theorem is a necessary and sufficient condition for a norm to be non-Archimedean.

Proposition 1.14. *The following statements are equivalent:*

- (a) $\|\cdot\|$ is non-Archimedean;
- (b) $\|n\| \leq 1$ for every integer n .

Proof. (a) \Rightarrow (b). We will prove this implication by induction.

Base of Induction. $\|1\| = 1 \leq 1$.

Induction Step. Suppose that $\|k\| \leq 1$ for all $k \in \{1, \dots, n-1\}$; let us prove that $\|n\| \leq 1$.

Observe that $\|n\| = \|(n-1) + 1\| \leq \max\{\|n-1\|, 1\} = 1$.

From the inequality $\|1\| = 1 \leq 1$ and the induction assumption, we have $\|n\| \leq 1$ for all $n \in \mathbb{N}$. Since $\|-n\| = \|n\|$, we conclude that $\|n\| \leq 1$ for all integers $n \in \mathbb{Z}$.

(b) \Rightarrow (a). We have

$$\begin{aligned} \|x + y\|^n &= \|(x + y)^n\| = \left\| \sum_{k=0}^n \binom{n}{k} x^k y^{n-k} \right\| \\ &\leq \sum_{k=0}^n \left\| \binom{n}{k} \right\| \|x\|^k \|y\|^{n-k} \leq \sum_{k=0}^n \|x\|^k \|y\|^{n-k} \\ &\leq (n+1) [\max(\|x\|, \|y\|)]^n. \end{aligned}$$

So, for every integer n we have

$$\|x + y\| \leq \sqrt[n]{n+1} \max(\|x\|, \|y\|).$$

Letting n tend to ∞ , we obtain

$$\|x + y\| \leq \max(\|x\|, \|y\|).$$

Here we used both the fact that $\binom{n}{k}$ is an integer and the well-known limit

$$\lim_{n \rightarrow \infty} \sqrt[n]{n+1} = 1.$$

□

This proposition helps explain the difference between Archimedean and non-Archimedean norms. It can be restated as follows: a norm is Archimedean if and only if it has the *Archimedean property*: given $x, y \in F$, $x \neq 0$, there exists a positive integer n such that $\|nx\| > \|y\|$. To see that, take $x, y \in F$ with $\|y\| > \|x\|$. Then the Archimedean property implies the existence of a positive integer n such that $\|n\| > \|y\|/\|x\| > 1$, i.e., the norm is Archimedean. Conversely, if the norm is Archimedean, there exists a positive integer n with $\|n\| > 1$. Then $\|n\|^k \rightarrow \infty$ as $k \rightarrow \infty$, and for some k , $\|n^k\| > \|y\|/\|x\|$, which implies the Archimedean property $\|n^k x\| > \|y\|$.

It is easy to see that the Archimedean property is equivalent to the assertion that there are integers with arbitrarily large norms:

$$(1.8) \quad \sup\{\|n\| : n \in \mathbb{Z}\} = +\infty.$$

We leave it to the reader to check that a norm is Archimedean if and only if (1.8) is satisfied (Exercise 14).

The non-Archimedean property has other surprising implications.

Proposition 1.15. *If the elements a, x of a non-Archimedean field F satisfy the inequality $\|x - a\| < \|a\|$, then $\|x\| = \|a\|$.*

Proof. By the strong triangle inequality,

$$\|x\| = \|x - a + a\| \leq \max(\|x - a\|, \|a\|) = \|a\|.$$

On the other hand,

$$\|a\| = \|a - x + x\| \leq \max(\|x - a\|, \|x\|).$$

Now $\|x - a\| > \|x\|$ would imply $\|a\| \leq \|x - a\|$, a contradiction. Therefore $\|x - a\| \leq \|x\|$, and $\|a\| \leq \|x\|$. So, $\|x\| = \|a\|$. This completes the proof. \square

Remark 1.16. This property can be restated in the following way: for a, b in a non-Archimedean field F

$$\|a\| > \|b\| \implies \|a + b\| = \|a\| : \textit{the strongest wins}.$$

Using the geometrical language, we can say: *Any triangle in an ultrametric space is isosceles and the length of its base does not exceed the lengths of the sides.*

We leave the proof of the next rather surprising proposition to the reader (Exercise 15).

Proposition 1.17. *If $\|\cdot\|$ is non-Archimedean, then any point of an open ball $B(a, r) = \{x : \|x - a\| < r\}$ in F is its center, i.e., if b is in $B(a, r)$, then $B(b, r) = B(a, r)$. The same is true for closed balls.*

We shall conclude this section by showing that an Archimedean norm and a non-Archimedean norm cannot be equivalent.

Proposition 1.18. *Two equivalent norms $(\|\cdot\|_1 \sim \|\cdot\|_2)$ on a field F are either both non-Archimedean or both Archimedean.*

Proof. It follows from Exercise 13 that if $\|\cdot\|_1 \sim \|\cdot\|_2$, then for any integer n we have $\|n\|_1 > 1$ if and only if $\|n\|_2 > 1$. Hence by Proposition 1.14 either both norms are non-Archimedean or both are Archimedean. \square

Exercises 9–16

Exercise 9. Prove that a field does not contain zero divisors.

Exercise 10. From the triangle inequality for the norm on a field F (Definition 1.5(3)) deduce that

$$\left| \|x\| - \|y\| \right| \leq \|x \pm y\| \quad \forall x, y \in F.$$

Exercise 11. Prove that in a normed field the following assertions hold:

- (1) Every Cauchy sequence is bounded.
- (2) Let $\{a_n\}$ be a Cauchy sequence and let $\{n_1, n_2, \dots\}$ be an increasing sequence of positive integers. If the subsequence

$$a_{n_1}, a_{n_2}, \dots$$

is a null sequence, then $\{a_n\}$ itself is a null sequence.

- (3) If $\{a_n\}$ and $\{b_n\}$ are null sequences, so is $\{a_n \pm b_n\}$, and if $\{a_n\}$ is a null sequence and $\{b_n\}$ is a bounded sequence, then $\{a_n b_n\}$ is a null sequence.
- (4) Let $\{a_n\}$ be a Cauchy sequence, but not a null sequence. Prove that there exist a number $c > 0$ and a positive integer N such that for all $n > N$ either $a_n > c$ or $a_n < -c$.

Exercise 12. Prove that if $\|\cdot\|_1 \sim \|\cdot\|_2$ and if $\|\cdot\|_1$ is trivial, so is $\|\cdot\|_2$.

Exercise 13. Prove that if $\|\cdot\|_1 \sim \|\cdot\|_2$, then $\|x\|_1 < 1$ if and only if $\|x\|_2 < 1$, $\|x\|_1 > 1$ if and only if $\|x\|_2 > 1$, and $\|x\|_1 = 1$ if and only if $\|x\|_2 = 1$.

Exercise 14. Prove that the norm $\|\cdot\|$ is Archimedean if and only if

$$\sup\{\|n\| : n \in \mathbb{Z}\} = +\infty.$$

Exercise 15. Prove Proposition 1.17.

Exercise 16. Prove that if $\|\cdot\|$ is a non-Archimedean norm, then $\|\cdot\|^\alpha$ is also a non-Archimedean norm for any $\alpha > 0$. (Compare with Proposition 1.11 for the Euclidean absolute value on \mathbb{Q} .)

1.3. Construction of the completion of a normed field

In this section, starting from an arbitrary normed field F (not necessarily complete with respect to its norm $\|\cdot\|$), we will construct another field, \widehat{F} , containing F , and supply it with a norm (induced from the norm $\|\cdot\|$ of F) in such a way that \widehat{F} will be a *complete* normed field.

We have already seen (§1.1) that in the case of the rational numbers supplied with the ordinary (Euclidean) norm, the completion procedure yields the reals \mathbb{R} . The same procedure will be applied later (see §1.4) to \mathbb{Q} endowed with a completely different norm and will yield the p -adic numbers. In the completion procedure, the main role will be played by Cauchy sequences: it is equivalence classes of Cauchy sequences from F that will be declared elements of the field \widehat{F} . So we begin by discussing Cauchy sequences in an arbitrary normed field.

Cauchy sequences can be added, subtracted and multiplied (Exercise 17), so the set of all Cauchy sequences in $(F, \|\cdot\|)$, denoted by $\{F\}$, becomes a commutative ring. Its identity element under addition is the sequence

$$\widehat{0} = \{0, 0, 0, \dots\},$$

and its identity element under multiplication is the sequence

$$\widehat{1} = \{1, 1, 1, \dots\}.$$

It is clear that $\{F\}$ is not a field since it contains zero divisors:

$$\{1, 0, 0, \dots\}\{0, 1, 0, 0, \dots\} = \widehat{0}.$$

For every $a \in F$ the constant sequence

$$\widehat{a} = \{a, a, a, \dots\}$$

is Cauchy and therefore lies in $\{F\}$. Hence $\{F\}$ contains a subring isomorphic to F . Of particular importance is the set P of all null

sequences. We saw that P is a subset of $\{F\}$. In fact, P is an *ideal* in $\{F\}$ (i.e., a subring such that for all $p \in P$ and all $a \in F$ we have $ap \in P$). Indeed, if $\{a_n\}$ and $\{b_n\}$ are in P , so is $\{a_n \pm b_n\}$, and if $\{a_n\}$ is in P and $\{b_n\}$ is a bounded sequence (in particular if it is Cauchy), then $\{a_n b_n\}$ is in P (Exercise 11(3)).

Let $\widehat{F} = \{F\}/P$. Its elements are equivalence classes of Cauchy sequences in $(F, \|\cdot\|)$, two Cauchy sequences being *equivalent* if their difference is a null sequence. Notice that constant sequences

$$\widehat{a} = \{a, a, a, \dots\},$$

where the $a \in F$ belong to different equivalent classes in \widehat{F} for different a . We shall denote the equivalence class of a Cauchy sequence $\{a_n\}$ by $(\{a_n\})$, so $(\{a_n\})$ is an element of \widehat{F} . We will think of F as a subset of \widehat{F} , identifying $a \in F$ with $(\widehat{a}) \in \widehat{F}$.

Theorem 1.19. \widehat{F} is a field.

Proof. It is easy to check that \widehat{F} , with operations defined as follows: if $\{a_n\} \in A$ and $\{b_n\} \in B$, then $A + B = (\{a_n + b_n\})$ and $A \cdot B = (\{a_n \cdot b_n\})$, is a commutative ring with the additive identity $(\widehat{0})$ and the multiplicative identity $(\widehat{1})$. By Exercise 18, these operations do not depend on the choice of representatives. Let us prove that \widehat{F} is a field. Let A be an equivalence class in \widehat{F} different from the zero class $(\widehat{0}) = P$, and let $\{a_n\}$ be any Cauchy sequence in A . By Exercise 11(4) there exist a positive number c and a positive integer N such that

$$\|a_n\| > c \quad \forall n \geq N.$$

Define a new sequence $\{a_n^*\}$ by

$$a_n^* = \begin{cases} 0 & \text{if } 1 \leq n \leq N-1, \\ 1/a_n & \text{if } n \geq N. \end{cases}$$

We claim that this is a Cauchy sequence. Indeed, if $n, m \geq N$, then

$$0 \leq \|a_m^* - a_n^*\| = \left\| \frac{1}{a_m} - \frac{1}{a_n} \right\| = \frac{\|a_m - a_n\|}{\|a_m\| \cdot \|a_n\|} \leq c^{-2} \|a_m - a_n\|,$$

1.3. Construction of the completion of a normed field 17

and the claim follows since $\{a_n\}$ is a Cauchy sequence. Let us denote the equivalence class of the sequence $\{a_n^*\}$ by A^{-1} . Then

$$\{a_n\}\{a_n^*\} = \{ \underbrace{0, \dots, 0}_{N-1 \text{ zeros}}, 1, 1, 1 \dots \},$$

where the Cauchy sequence on the right differs from $\widehat{1}$ by the null sequence

$$\{ \underbrace{-1, \dots, -1}_{N-1 \text{ } (-1)\text{'s}}, 0, 0, 0 \dots \}.$$

Thus $AA^{-1} = (\widehat{1})$, which proves that \widehat{F} is a field. □

Now we extend the norm $\|\cdot\|$ from F to \widehat{F} .

Definition 1.20. For any $A \in \widehat{F}$ put

$$\|A\| = \lim_{n \rightarrow \infty} \|a_n\|,$$

where $\{a_n\}$ is any Cauchy sequence in A .

In order to see that this norm is well defined, we must show that the limit exists and does not depend on the choice of the Cauchy sequence $\{a_n\}$ in A . We have

$$\left| \|a_n\| - \|a_m\| \right| \leq \|a_n - a_m\|$$

by Exercise 10, which implies that the sequence of real numbers $\{\|a_n\|\}$ is Cauchy with respect to the absolute value. Since the set of real numbers \mathbb{R} is complete, the limit defining $\|\cdot\|$ exists. Now take a second sequence $\{a'_n\} \in A$. By the same inequality we have

$$0 \leq \lim_{n \rightarrow \infty} \left| \|a_n\| - \|a'_n\| \right| \leq \lim_{n \rightarrow \infty} \|a_n - a'_n\| = 0;$$

hence $\lim_{n \rightarrow \infty} \|a_n\| = \lim_{n \rightarrow \infty} \|a'_n\|$.

Proposition 1.21. $\|\cdot\|$ is a norm on \widehat{F} .

Proof. We must verify the three properties listed in Definition 1.5.

- (1) If $A = (\widehat{0})$, then $\{a_n\}$ is a null sequence, and therefore $\|A\| = 0$. If $A \neq (\widehat{0})$ and $A = (\{a_n\})$, then there exist positive numbers c and N such that for all $n \geq N$ we have $\|a_n\| \geq c > 0$. Hence $\|A\| > 0$.

(2) Now let $A = (\{a_n\})$ and $B = (\{b_n\})$. By the properties of real limits,

$$\begin{aligned}\|AB\| &= \lim_{n \rightarrow \infty} \|a_n b_n\| = \lim_{n \rightarrow \infty} \|a_n\| \|b_n\| \\ &= \lim_{n \rightarrow \infty} \|a_n\| \lim_{n \rightarrow \infty} \|b_n\| = \|A\| \|B\|.\end{aligned}$$

(3) Similarly, we obtain $\|A + B\| \leq \|A\| + \|B\|$.

□

Now we can define bounded, Cauchy, and null sequences in \widehat{F} with respect to the norm $\|\cdot\|$.

Theorem 1.22. \widehat{F} is complete with respect to the norm $\|\cdot\|$, and F is a dense subset of \widehat{F} .

Proof. We first prove the second part. Let $A \in \widehat{F}$, and let $\{a_m\}$ be a Cauchy sequence in F representing A . For each fixed positive integer n , we consider the constant sequence \widehat{a}_n . Then the sequence $\{a_m - a_n\}_{m=1}^{\infty}$ represents $A - (\widehat{a}_n)$, and since $\{a_m\}$ is Cauchy, we can write

$$(1.9) \quad \lim_{n \rightarrow \infty} \|A - (\widehat{a}_n)\| = \lim_{n, m \rightarrow \infty} \|a_m - a_n\| = 0.$$

This proves that F is dense in \widehat{F} . Now suppose $\{A_n\} = \{A_1, A_2, \dots\}$ is a Cauchy sequence in \widehat{F} . By the density of F in \widehat{F} , for any A_n there exists an element $a_n \in F$ such that

$$(1.10) \quad \|A_n - (\widehat{a}_n)\| < \frac{1}{n}.$$

Therefore $\{A_n - (\widehat{a}_n)\}$ is null sequence, hence a Cauchy sequence in \widehat{F} . We have

$$\{(\widehat{a}_n)\} = \{A_n\} - \{A_n - (\widehat{a}_n)\};$$

hence $\{(\widehat{a}_n)\}$ is a Cauchy sequence in \widehat{F} , but since all its elements belong to F , $\{a_n\}$ itself is a Cauchy sequence in F . Let us denote the equivalence class of $\{a_n\}$ by A (in our notation, $(\{a_n\}) = A$). From (1.9) and (1.10) it follows that $\{A - (\widehat{a}_n)\}$ and $\{A_n - (\widehat{a}_n)\}$ are null sequences in \widehat{F} , and hence their difference

$$\{A - A_n\} = \{A - (\widehat{a}_n)\} - \{A_n - (\widehat{a}_n)\}$$

is a null sequence in \widehat{F} . This implies that

$$\lim_{n \rightarrow \infty} \|A - A_n\| = 0,$$

but this means exactly that $A = \lim_{n \rightarrow \infty} A_n$. \square

Proposition 1.23. *The operations on \widehat{F} are extended from F by continuity, i.e., if*

$$A = \lim_{n \rightarrow \infty} (\widehat{a}_n), \quad B = \lim_{n \rightarrow \infty} (\widehat{b}_n),$$

then

$$A + B = \lim_{n \rightarrow \infty} (\widehat{a}_n + \widehat{b}_n), \quad A \cdot B = \lim_{n \rightarrow \infty} (\widehat{a}_n \cdot \widehat{b}_n).$$

Proof. Exercise 19. \square

Exercises 17–19

Exercise 17. Prove that if $\{a_n\}$ and $\{b_n\}$ are Cauchy sequences, then so are

$$\{a_n + b_n\}, \{a_n - b_n\}, \text{ and } \{a_n b_n\}.$$

Exercise 18. Prove that if $\{a_n\} \sim \{a'_n\}$ and $\{b_n\} \sim \{b'_n\}$ are two pairs of equivalent Cauchy sequences, then $\{a_n \pm b_n\} \sim \{a'_n \pm b'_n\}$ and $\{a_n \cdot b_n\} \sim \{a'_n \cdot b'_n\}$.

Exercise 19. Prove Proposition 1.23.

1.4. The field of p -adic numbers \mathbb{Q}_p

The basic example of a norm on the field \mathbb{Q} of rational numbers is the absolute value $|\cdot|$. The induced metric $d(x, y) = |x - y|$ is the ordinary Euclidean distance on the number line, and as was explained in §1.1, the field of real numbers \mathbb{R} is the completion of \mathbb{Q} with respect to this norm.

Now let us ask ourselves the following question: Is the Euclidean distance between rational numbers really the most “natural” one? Is there any other way to describe the “closeness” between rationals? It turns out that the answer to this question is YES.

The new ways of measuring distance between rational numbers come from the following “arithmetical” construction.

Let $p \in \mathbb{N}$ be any prime number. Define a map $|\cdot|_p$ on \mathbb{Q} as follows:

$$(1.11) \quad |x|_p = \begin{cases} p^{-\text{ord}_p x} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0, \end{cases}$$

where

$$\text{ord}_p x = \begin{cases} \text{the highest power of } p \text{ which divides } x, & \text{if } x \in \mathbb{Z}, \\ \text{ord}_p a - \text{ord}_p b, & \text{if } x = a/b, a, b \in \mathbb{Z}, b \neq 0 \end{cases}$$

is the p -adic order of x (also called the p -adic valuation).

Remark 1.24. Notice that $|\cdot|_p$ can take only a “discrete” set of values, namely, $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$.

Remark 1.25. If $a, b \in \mathbb{N}$, then $a \equiv b \pmod{p^n}$ if and only if $|a - b|_p \leq 1/p^n$.

Proposition 1.26. $|\cdot|_p$ is a non-Archimedean norm on \mathbb{Q} .

Proof. Property (1) in Definition 1.5 is obvious, and (2) follows from

$$(1.12) \quad \text{ord}_p(xy) = \text{ord}_p(x) + \text{ord}_p(y).$$

Let us verify (3). If $x = 0$ or $y = 0$, (3) is trivial, so assume $x, y \neq 0$. Let $x = a/b$ and $y = c/d$. Then we have

$$x + y = \frac{ad + bc}{bd},$$

and

$$\begin{aligned} \text{ord}_p(x + y) &= \text{ord}_p(ad + bc) - \text{ord}_p(bd) \\ &\geq \min(\text{ord}_p(ad), \text{ord}_p(bc)) - \text{ord}_p b - \text{ord}_p d \\ &= \min(\text{ord}_p a - \text{ord}_p b, \text{ord}_p c - \text{ord}_p d) \\ &= \min(\text{ord}_p x, \text{ord}_p y). \end{aligned}$$

Therefore,

$$\begin{aligned} |x + y|_p &= p^{-\text{ord}_p(x+y)} \leq \max(p^{-\text{ord}_p x}, p^{-\text{ord}_p y}) \\ &= \max(|x|_p, |y|_p) \leq |x|_p + |y|_p. \end{aligned}$$

Observe that we have also proved that $|\cdot|_p$ satisfies the strong triangle inequality, i.e., it is non-Archimedean. \square

Remark 1.27. We shall see later that \mathbb{Q} is not complete with respect to the norm $|\cdot|_p$.

Remark 1.28. The norm $|\cdot|_{p_1}$ is not equivalent to $|\cdot|_{p_2}$ if p_1 and p_2 are different primes (indeed, for the sequence $x_n = (p_1/p_2)^n$ we have $|x_n|_{p_1} \rightarrow 0$, but $|x_n|_{p_2} \rightarrow \infty$).

We are now ready for the definition of the main protagonist of these lectures. Let p be a fixed prime. We define \mathbb{Q}_p to be the completion of \mathbb{Q} with respect to the p -adic norm $|\cdot|_p$ of (1.11). The p -adic norm is extended to \mathbb{Q}_p according to Definition 1.20, and $(\mathbb{Q}_p, |\cdot|_p)$ is a complete normed field. We call \mathbb{Q}_p the *field of p -adic numbers*. The elements of \mathbb{Q}_p are equivalence classes of Cauchy sequences in \mathbb{Q} with respect to the extension of the p -adic norm. As has been pointed out earlier, \mathbb{Q} can be identified with the subfield of \mathbb{Q}_p consisting of equivalence classes of constant Cauchy sequences.

For some $a \in \mathbb{Q}_p$ let $\{a_n\}$ be a Cauchy sequence of rational numbers representing a . Then by definition

$$(1.13) \quad |a|_p = \lim_{n \rightarrow \infty} |a_n|_p.$$

Therefore, the set of values that $|\cdot|_p$ takes on \mathbb{Q}_p is the same as it takes on \mathbb{Q} , namely $\{p^n, n \in \mathbb{Z}\} \cup \{0\}$ — a phenomenon quite different from what happens with the Euclidean absolute value which, when extended from \mathbb{Q} to \mathbb{R} , takes all nonnegative real values. Moreover, if $|a|_p \neq 0$, then the sequence of norms $\{|a_n|_p\}$ must stabilize for sufficiently large n !

Let us consider the series

$$(1.14) \quad \frac{d_{-m}}{p^m} + \frac{d_{-m+1}}{p^{m-1}} + \cdots + d_0 + d_1p + d_2p^2 + \cdots,$$

where $0 < d_{-m} < p$ and $0 \leq d_i < p$ for all $i > -m$. Its partial sums form a Cauchy sequence since for every $\epsilon > 0$ we can choose N such that $p^{-N} < \epsilon$, and for $k > n > N$ we have

$$\left| \sum_{-m}^k d_i p^i - \sum_{-m}^n d_i p^i \right|_p = \left| \sum_{n+1}^k d_i p^i \right|_p \leq \max_{n < i \leq k} (|d_i p^i|_p) \leq p^{-N} < \epsilon.$$

Therefore, each series of the form (1.14) represents an element of \mathbb{Q}_p . The converse statement is also true. We will show that each equivalence class of Cauchy sequences in \mathbb{Q} contains a unique *canonical*

representative Cauchy sequence — the sequence of partial sums of a series in the form (1.14).

In order to describe its construction, we need the following lemma.

Lemma 1.29. *If $x \in \mathbb{Q}$ and $|x|_p \leq 1$, then for any i there exists an integer $\alpha \in \mathbb{Z}$ such that $|\alpha - x|_p \leq p^{-i}$. The integer α can be chosen in the set $\{0, 1, 2, \dots, p^i - 1\}$ and is unique if chosen in this range.*

Proof. Let $x = a/b$, where a and b are relatively prime (this is denoted $(a, b) = 1$). Since $|x|_p \leq 1$, it follows that p does not divide b , and hence b and p^i are relatively prime. So, we can find integers m and n such that $mb + np^i = 1$. Let $\alpha = am$. Then

$$\begin{aligned} |\alpha - x|_p &= |am - a/b|_p = |a/b|_p |mb - 1|_p \\ &\leq |mb - 1|_p = |np^i|_p = |n|_p p^{-i} \leq p^{-i}. \end{aligned}$$

Finally, using the strong triangle inequality, we can add a multiple of p^i to the integer α to get an integer between 0 and p^i for which $|\alpha - x|_p \leq p^{-i}$ still holds. \square

Theorem 1.30. *Every equivalence class a in \mathbb{Q}_p satisfying $|a|_p \leq 1$ has exactly one representative Cauchy sequence $\{a_i\}$ such that*

- (1) $a_i \in \mathbb{Z}$, $0 \leq a_i < p^i$ for $i = 1, 2, \dots$,
- (2) $a_i \equiv a_{i+1} \pmod{p^i}$ for $i = 1, 2, \dots$

Proof. Let $\{b_i\}$ be a Cauchy sequence representing a . We want to find an equivalent sequence $\{a_i\}$ satisfying (1) and (2). Since

$$|b_i|_p \longrightarrow |a|_p \leq 1 \text{ as } i \rightarrow \infty,$$

throwing away several initial terms, if necessary, we may assume that $|b_i|_p \leq 1$ for all i .

For every $j = 1, 2, \dots$ let $N(j)$ be a positive integer such that

$$|b_i - b_{i'}|_p \leq p^{-j}, \quad \forall i, i' \geq N(j).$$

Observe that we may take the sequence $N(j)$ to be strictly increasing with j , so $N(j) \geq j$.

From Lemma 1.29, we can find integers a_j , $0 \leq a_j < p^j$, such that

$$|a_j - b_{N(j)}|_p \leq \frac{1}{p^j}.$$

Let us show that $a_j \equiv a_{j+1} \pmod{p^j}$ and $(b_i) \sim (a_j)$.

The first assertion follows since

$$\begin{aligned} |a_{j+1} - a_j|_p &= |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \\ &\leq \max(|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |a_j - b_{N(j)}|_p) \\ &\leq \max(1/p^{j+1}, 1/p^j, 1/p^j) = 1/p^j, \end{aligned}$$

so that $a_j \equiv a_{j+1} \pmod{p^j}$.

To prove the second assertion, take any j ; then for $i \geq N(j)$ we have

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\ &\leq \max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p) \\ &\leq \max(1/p^j, 1/p^j, 1/p^j) = 1/p^j. \end{aligned}$$

Hence

$$|a_i - b_i|_p \longrightarrow 0 \text{ as } i \rightarrow \infty.$$

Now, let us prove uniqueness. If $\{a'_i\}$ is a different sequence satisfying the requirements of the theorem with $a_{i_0} \neq a'_{i_0}$ for some i_0 , then we have $a_{i_0} \not\equiv a'_{i_0} \pmod{p^{i_0}}$, since both a_{i_0} and a'_{i_0} are between 0 and p^{i_0} . Then it follows from (2) that for $i > i_0$

$$a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i \pmod{p^{i_0}},$$

i.e., $a_i \not\equiv a'_i \pmod{p^{i_0}}$. But this means exactly that

$$|a_i - a'_i|_p > \frac{1}{p^{i_0}}, \quad \forall i \geq i_0,$$

which implies that $(a_i) \not\sim (a'_i)$. \square

If $a \in \mathbb{Q}_p$ with $|a|_p \leq 1$, then it is convenient to write all the terms a_i of the representative sequence given by the previous theorem in the following way:

$$a_i = d_0 + d_1p + \dots + d_{i-1}p^{i-1},$$

where all the d_i 's are integers in $\{0, 1, \dots, p-1\}$. Our condition (2) means precisely that

$$a_{i+1} = d_0 + d_1p + \dots + d_{i-1}p^{i-1} + d_i p^i,$$

where the “ p -adic digits” d_0 through d_{i-1} are all the same as for a_i . Thus a is represented by the convergent (in the p -adic norm, of course) series

$$a = \sum_{n=0}^{\infty} d_n p^n,$$

which can be thought of as a number, written in the base p , that extends infinitely far to the left or has infinitely many p -adic digits. We will write

$$a = \dots d_n \dots d_2 d_1 d_0$$

and call this the *canonical p -adic expansion* or *canonical form* of a .

If $|a|_p > 1$, then we can multiply a by a power of p (namely by $p^m = |a|_p$) so as to get a p -adic number $a' = ap^m$ that satisfies $|a'|_p = 1$.

Then we can write

$$(1.15) \quad a = \sum_{n=-m}^{\infty} d_n p^n,$$

where $d_{-m} \neq 0$ and $b_i \in \{0, 1, 2, \dots, p-1\}$, and represent the given p -adic number a as a fraction in the base p with infinitely many p -adic digits before the point and finitely many digits after:

$$(1.16) \quad a = \dots d_n \dots d_2 d_1 d_0 . d_{-1} \dots d_{-m};$$

this representation is called the *canonical p -adic expansion* of a .

The following proposition shows that the norm of a p -adic number is determined by the index of the first nonzero coefficient in its canonical expansion.

Proposition 1.31. *If $a = \sum_{n=0}^{\infty} d_n p^n$ with $d_n = 0$ for $0 \leq n < k$ and $d_k \neq 0$, then $|a|_p = p^{-k}$, and if $a = \sum_{n=-m}^{\infty} d_n p^n$, where $d_{-m} \neq 0$, then $|a|_p = p^m$.*

Proof. By the definition (1.13), $|a|_p$ is a limit of the sequence of p -adic norms of the partial sums of this series. In the first case we obtain the constant sequence $p^{-k}, p^{-k}, p^{-k}, \dots$ since $|d_k|_p = 1$ (remember that $0 < d_k < p$) and by the strong triangle inequality. Thus $|a|_p = p^{-k}$. If $a = \sum_{n=-m}^{\infty} d_n p^n$, where $d_{-m} \neq 0$, the same argument shows that $|a|_p = p^m$. \square

Moreover, the notion of *order* defined in the beginning of §1.4 for rational numbers can be extended to all p -adic numbers: for $a \in \mathbb{Q}_p$, $\text{ord}_p(a)$ is equal to the index of the first nonzero coefficient in the canonical expansion of a .

Remark 1.32. The uniqueness assertion in Theorem 1.30 is something we do not have in the representation of numbers as infinite fractions to the base g mentioned in §1.1, e.g. for $g = 10$

$$1.0000\dots = 0.9999\dots$$

There are no such exceptions in the p -adic case. If two p -adic expansions converge to the same p -adic number, they are the same, i.e., all their digits are the same.

Definition 1.33. A p -adic number $a \in \mathbb{Q}_p$ is said to be a *p -adic integer* if its canonical expansion contains only nonnegative powers of p .

The set of p -adic integers is denoted by \mathbb{Z}_p , so

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \right\}.$$

It is easy to see (Exercise 21) that $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$.

Theorem 1.34. *Every infinite sequence of p -adic integers has a convergent subsequence.*

Proof. Recall that a *subsequence* $\{x_{n_k}\}$ of a sequence $\{x_k\}$ is given by a sequence of positive integers $\{n_k\}$ such that $n_1 < n_2 < n_3 < \dots$

Let $\{x_k\}$ be a sequence in \mathbb{Z}_p . Let us write out the canonical expansion of each term,

$$x_k = \dots a_2^k a_1^k a_0^k.$$

Since there are only finitely many possibilities for the digits a_0^k (namely, $0, 1, \dots, p-1$), we can find $b_0 \in \{0, 1, \dots, p-1\}$ and an infinite subsequence of $\{x_k\}$, denoted by $\{x_{0k}\}$, such that the first digit of all x_{0k} is always b_0 . The same trick yields $b_1 \in \{0, 1, \dots, p-1\}$ and a subsequence $\{x_{1k}\}$ of $\{x_{0k}\}$ for which the first two digits are $b_1 b_0$.

This procedure can be continued, and we obtain b_0, b_1, b_2, \dots together with a sequence of sequences

$$\begin{aligned} &x_{00}, x_{01}, x_{02}, \dots, x_{0s}, \dots, \\ &x_{10}, x_{11}, x_{12}, \dots, x_{1s}, \dots, \\ &x_{20}, x_{21}, x_{22}, \dots, x_{2s}, \dots, \\ &\dots \end{aligned}$$

such that each sequence is a subsequence of the preceding one, and such that each element of the $(j + 1)$ th row begins with $b_j \dots b_1 b_0$. For each $j = 0, 1, \dots$ we have

$$x_{jj} \in \{x_{j-1j}, x_{j-1j+1}, \dots\}.$$

Therefore the diagonal sequence x_{00}, x_{11}, \dots is still a subsequence of the original sequence, and it obviously converges to $\dots b_3 b_2 b_1 b_0$. \square

Remark 1.35. It is not difficult to extend this result to bounded sequences (see Exercise 25). The same result is true for bounded sequences of real numbers (Bolzano-Weierstrass Theorem), and a proof for a sequence of real numbers $0 \leq x_n \leq 1$ can be modeled on the above proof using the representation of real numbers by infinite decimal fractions.

Exercises 20–25

Exercise 20. What is the cardinality of \mathbb{Z}_p ? Justify your answer.

Exercise 21. Prove that $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$.

Exercise 22. Find the p -adic norm and the p -adic expansion of

- (1) 15, -1 , -3 in \mathbb{Q}_5 ,
- (2) $6!$ in \mathbb{Q}_3 ,
- (3) $1/3!$ in \mathbb{Q}_3 .

Exercise 23. Find the p -adic expansion of $1/p$. What about $1/p^k$?

Exercise 24. Find the p -adic expansion of $1/2$ if p is an odd prime.

Exercise 25. Prove that any infinite bounded sequence in \mathbb{Q}_p has a convergent subsequence.

1.5. Arithmetical operations in \mathbb{Q}_p

The p -adic expansion allows us to perform arithmetical operations in \mathbb{Q}_p in a way very similar to that in \mathbb{R} . Moreover, we will see that the operations in \mathbb{Q}_p are, in fact, easier to perform than in \mathbb{R} ! Let

$$a = \sum_{n=-m}^{\infty} a_n p^n, \quad b = \sum_{n=-m}^{\infty} b_n p^n,$$

where a_n and b_n are p -adic digits, $a_{-m} \neq 0$, but possibly one or more of the first digits b_{-m}, b_{-m+1}, \dots are equal to 0. Then each

$$a \pm b = \sum_{n=-m}^{\infty} (a_n \pm b_n) p^n$$

is a convergent series; however, in general it will not be in the canonical form (1.15). The reduction to canonical form given by Theorem 1.30 corresponds to the standard addition (or subtraction) procedure from right to left applied to p -adic numbers given in the form (1.16) and uses a system of carries (similar to the one used for decimal fractions).

In order to illustrate the addition algorithm, let us find the canonical p -adic expansion of -1 in \mathbb{Q}_p . We have $1 = \dots 00001$. Let $a = \dots a_3 a_2 a_1 a_0$ satisfy $1 + a = 0$ (then $a = -1$). Starting from the right, we must have $1 + a_0 = 0$, but since a_0 is in the range $\{0, 1, \dots, p-1\}$, the only way to achieve this is to have $1 + a_0 = p$ and to carry 1 to the left. Thus $a_0 = p-1$. Continuing the procedure, we see that all the a_n are equal to $p-1$, i.e.,

$$-1 = \dots (p-1)(p-1)(p-1).$$

Multiplication can be performed in a similar way. Let

$$a = \sum_{n=-m}^{\infty} a_n p^n, \quad b = \sum_{n=-k}^{\infty} b_n p^n$$

be given in canonical form. Multiplying the series term by term and rearranging terms, we obtain

$$ab = \sum_{n=-m-k}^{\infty} u_n p^n,$$

where

$$\begin{aligned} u_{-m-k} &= a_{-m} b_{-k}, \\ u_{-m-k+1} &= a_{-m+1} b_{-k} + a_{-m} b_{-k+1}, \\ &\dots \end{aligned}$$

This series again, in general, is not in the canonical form, but the method of Theorem 1.30 allows us to reduce it to such a form. Again, this corresponds to the standard multiplication procedure performed on p -adic numbers given in the canonical form (1.16).

To illustrate division, suppose we have $a, b \in \mathbb{Q}_p$ and $b \neq 0$. Without loss of generality we may assume that $b \in \mathbb{Z}_p$, $b = \dots b_2 b_1 b_0$ with $b_0 \neq 0$, while

$$a = \dots a_3 a_2 a_1 a_0 \cdot a_{-1} \dots a_{-k}$$

is an arbitrary p -adic number. Since $b_0 \neq 0$ and since the ring of residues $\mathbb{Z}/p\mathbb{Z}$ for a prime p is a field, we can always find a $c_{-k} \in \{0, 1, \dots, p-1\}$ such that $c_{-k} b_0 \equiv a_{-k} \pmod{p}$. Continuing the usual division procedure (carrying, if necessary, 1 to the left), we obtain the quotient a/b in the canonical form.

It follows that if $a = \dots a_2 a_1 a_0$ is a p -adic integer with $a_0 \neq 0$, then its multiplicative inverse a^{-1} is also a p -adic integer! (This property of p -adic integers may seem strange at first glance, but it is admittedly a nice one to have.) On the other hand, since

$$p \cdot \sum_{i=0}^{\infty} a_i p^i = a_0 p + a_1 p^2 + \dots \neq 1 + 0p + 0p^2 + \dots,$$

it follows that p has no multiplicative inverse in \mathbb{Z}_p (of course, p has a multiplicative inverse in \mathbb{Q}_p (Exercise 23)!). A similar argument shows that a p -adic integer whose first digit a_0 is zero has no multiplicative inverse in \mathbb{Z}_p . We summarize this in the following proposition.

Proposition 1.36. *A p -adic integer*

$$a = \dots a_1 a_0 \in \mathbb{Z}_p$$

has a multiplicative inverse in \mathbb{Z}_p if and only if $a_0 \neq 0$.

We will denote the group of invertible elements in \mathbb{Z}_p by \mathbb{Z}_p^\times ,

$$\mathbb{Z}_p^\times = \left\{ \sum_{i=1}^{\infty} a_i p^i \mid a_0 \neq 0 \right\}.$$

This group is also called the group of *p-adic units*. By Exercise 26,

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

The following proposition follows at once from the definition of the *p*-adic norm and Exercise 26.

Proposition 1.37. *Let x be a p -adic number of norm p^{-n} . Then x can be written as the product $x = p^n u$, where $u \in \mathbb{Z}_p^\times$.*

Notice that the arithmetical operations in \mathbb{Q}_p extend the ordinary arithmetical operations on natural numbers (written in base p). The familiar algorithms for addition, subtraction and multiplication are simply pursued indefinitely from right to left. The *p*-adic division algorithm also proceeds from right to left, and in that way it is different from the familiar “long division” algorithm which begins by finding the digit in the highest position and proceeds from left to right.

Here are some examples of arithmetical operations in \mathbb{Q}_7 :

			... 615
) ... 421
... 46530.25	... 263	... 153	... 161
+ 230
... 20656.41	× ... 154 153
... 00516.66	... 445 400
... 46530.2	... 141 4
-
... 20656.4	... 263	...	
... 25540.5	... 455	...	

Exercises 26–31

Exercise 26. Prove that $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$.

Exercise 27. If $a \in \mathbb{Q}_p$ has the canonical p -adic expansion

$$\dots a_n \dots a_2 a_1 a_0 \cdot a_{-1} \dots a_{-m},$$

what is the canonical p -adic expansion of $-a$?

Exercise 28. The integers 2, 3, 4 are invertible in \mathbb{Z}_5 . Find the 5-adic expansions of their inverses. Find the expansion of $1/3$ in \mathbb{Z}_7 .

Exercise 29. Find the canonical p -adic expansion of:

- (1) $\dots 1246 \times \dots 6003$ in \mathbb{Q}_7 to 4 digits,
- (2) $1 : \dots 1323$ in \mathbb{Q}_5 to 4 digits,
- (3) $900 - \dots 312.3$ in \mathbb{Q}_{11} to 4 digits.

Exercise 30. Find the p -adic norm of $(p^n)!$.

Exercise 31.* Find the p -adic norm of $n!$.

1.6. The p -adic expansion of rational numbers

Any rational integer is also a p -adic integer (simply write its expansion in base p). However, there are p -adic integers among rational fractions! We have seen that

$$-1 = (p-1) \sum_{i=0}^{\infty} p^i,$$

so that

$$\sum_{i=0}^{\infty} p^i = \frac{1}{1-p}, \quad \frac{1}{1-p} = \dots 1111,$$

which is in \mathbb{Z}_p . Note that the p -adic expansion of this p -adic integer is infinite! See Exercise 34 for necessary and sufficient conditions for a p -adic expansion to terminate.

The following theorem shows that we can recognize rational numbers by their p -adic expansion just as we recognize rationals among reals by their decimal expansion.

Theorem 1.38. *The canonical p -adic expansion (1.16) represents a rational number if and only if it is eventually periodic to the left.*

Proof. Assume that the canonical p -adic expansion is eventually periodic. Multiplying (if necessary) the given p -adic number x by a power of p and subtracting a rational number, we may consider the case in which $x \in \mathbb{Z}_p$ has a periodic expansion of the form

$$x = x_0 + x_1p + x_2p^2 + \cdots + x_{k-1}p^{k-1} + x_0p^k + x_1p^{k+1} + \cdots$$

The number $a = x_0 + x_1p + x_2p^2 + \cdots + x_{k-1}p^{k-1}$ is a rational integer and x can be expressed in the form

$$x = a(1 + p^k + p^{2k} + \cdots) = a \frac{1}{1 - p^k},$$

and hence x is a rational number.

Conversely, suppose that

$$(1.17) \quad \frac{a}{b} = \sum_{i \geq 0} x_i p^i \in \mathbb{Z}_p.$$

We may assume that a and b are relatively prime integers and b is relatively prime to p . Since $(b, p^n) = 1$, there exist c_n, d_n such that

$$1 = c_n b + d_n p^n.$$

Multiplying both sides by a , we obtain

$$a = ac_n b + ad_n p^n.$$

By adding a multiple of p^n to the integer ac_n , we obtain two integers, A_n with $0 \leq A_n \leq p^n - 1$ and r_n such that the equality

$$a = A_n b + r_n p^n$$

holds. Dividing both sides by b , we obtain

$$\frac{a}{b} = A_n + p^n \frac{r_n}{b}.$$

Hence $r_n = (a - A_n b)/p^n$, and therefore

$$\frac{a - (p^n - 1)b}{p^n} \leq r_n \leq \frac{a}{p^n}.$$

For sufficiently large n , this implies $-b \leq r_n \leq 0$, which means that r_n takes only finitely many values. Now we can write

$$(1.18) \quad \frac{a}{b} = A_n + p^n \frac{r_n}{b} = A_{n+1} + p^{n+1} \frac{r_{n+1}}{b}.$$

Since $A_{n+1} - A_n = p^n \left(\frac{r_n - pr_{n+1}}{b} \right)$ is an integer and $(b, p^n) = 1$, the expression $\frac{r_n - pr_{n+1}}{b}$ is an integer. Hence $A_{n+1} \equiv A_n \pmod{p^n}$, and by the uniqueness of Theorem 1.30 the sequence $\{A_n\}$ is the sequence of partial sums of the canonical p -adic representation (1.17) of a/b . Thus $A_{n+1} = A_n + x_n p^n$, and (1.18) implies $r_n = x_n b + pr_{n+1}$ for all n . Since r_n takes only finitely many values, there exist an index m and a positive integer P such that $r_m = r_{m+P}$; hence

$$(1.19) \quad x_m b + pr_{m+1} = x_{m+P} b + pr_{m+P+1},$$

so that

$$(x_m - x_{m+P})b = p(r_{m+P+1} - r_{m+1}).$$

Since $(b, p) = 1$, it follows that p divides $x_m - x_{m+P}$. But both x_m and x_{m+P} are digits in $\{0, 1, \dots, p-1\}$; therefore $x_m = x_{m+P}$. If we substitute this into (1.19), we also see that $r_{m+1} = r_{m+P+1}$. Repeating this argument, we obtain

$$r_n = r_{n+P} \text{ and } x_n = x_{n+P} \quad (n \geq m),$$

which proves that not only the sequence of digits x_n , but also the sequence of numerators r_n , has a period of length P for $n \geq m$. \square

Is it possible to determine from a p -adic expansion of a rational number whether it is positive or negative? The answer is YES, and it is given in Exercise 33.

Exercises 32–34

Exercise 32. Prove that

- (1) $\mathbb{Z}_p \cap \mathbb{Q} = \{a/b \in \mathbb{Q} : p \nmid b\}$,
- (2) $\mathbb{Z}_p^\times \cap \mathbb{Q} = \{a/b \in \mathbb{Q} : p \nmid ab\}$.

Exercise 33.* Let $r \in \mathbb{Q}$. Prove that for an appropriate $k \geq 1$, rp^k is a p -adic integer and its p -adic expansion can be represented in the form $\dots aaaaab$, where the fragments a and b have the same number of digits. Prove that $r > 0$ is equivalent to $b > a$ in the usual sense (as integers written in base p).

Exercise 34. Prove that the p -adic expansion of $a \in \mathbb{Q}_p$ terminates (i.e., $a_i = 0$ for all i greater than some N) if and only if a is a *non-negative* rational number whose denominator is a power of p .

1.7. Hensel's Lemma and congruences

Let us extract $\sqrt{6}$ in \mathbb{Q}_5 ; this means we want to find a sequence of 5-adic digits a_0, a_1, a_2, \dots , $0 \leq a_i \leq 4$, such that

$$(1.20) \quad (a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \dots)^2 = 1 + 1 \cdot 5.$$

From (1.20) we obtain $a_0^2 \equiv 1 \pmod{5}$, which implies $a_0 = 1$ or 4. If $a_0 = 1$, then

$$2a_1 \cdot 5 \equiv 1 \cdot 5 \pmod{5^2} \Rightarrow 2a_1 \equiv 1 \pmod{5} \Rightarrow a_1 = 3.$$

At the next step we have

$$1 + 1 \cdot 5 \equiv (1 + 3 \cdot 5 + a_2 \cdot 5^2)^2 \equiv 1 + 1 \cdot 5 + 2a_2 \cdot 5^2 \pmod{5^3},$$

which implies $2a_2 \equiv 0 \pmod{5}$ and therefore $a_2 = 0$.

So, we get a series

$$a = 1 + 3 \cdot 5 + 0 \cdot 5^2 + \dots,$$

where each a_i after a_0 is uniquely determined.

If we choose $a_0 = 4$, then we obtain the solution

$$-a = 4 + 1 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + \dots$$

It is not very difficult to see that there exist numbers in \mathbb{Q}_5 which have no square root (for example $2 + 1 \cdot 5$).

The above method of solving equations (like $x^2 - 6 = 0$ in \mathbb{Q}_5) can be generalized by using an extremely important result called “Hensel’s Lemma”.

Generalizing Remark 1.25, we say that a and $b \in \mathbb{Q}_p$ are *congruent modulo p^n* and write

$$a \equiv b \pmod{p^n}$$

if and only if $|a - b|_p \leq 1/p^n$.

Theorem 1.39. (Hensel’s Lemma) *Let $F(x) = c_0 + c_1x + \dots + c_nx^n$ be a polynomial whose coefficients are p -adic integers. Let*

$$F'(x) = c_1 + 2c_2x + 3c_3x^2 + \dots + nc_nx^{n-1}$$

be the derivative of $F(x)$. Suppose \bar{a}_0 is a p -adic integer which satisfies $F(\bar{a}_0) \equiv 0 \pmod{p}$ and $F'(\bar{a}_0) \not\equiv 0 \pmod{p}$. Then there exists a unique p -adic integer a such that $F(a) = 0$ and $a \equiv \bar{a}_0 \pmod{p}$.

Proof. We will prove the existence of a by constructing its canonical p -adic expansion $a = b_0 + b_1p + b_2p^2 + \dots$ inductively. At the k th step of induction, we will find $a_k = b_0 + \dots + b_kp^k$, the k th approximation of a , by using a p -adic version of Newton’s method (cf. the remark at the end of this proof). Each a_k will not be a true root of $F(x)$, but only a “root modulo p^{k+1} ” (i.e., we will have $F(a_k) \equiv 0 \pmod{p^{k+1}}$) for all k . In the limit as $k \rightarrow \infty$ we will obtain a , the required true root of F .

More precisely, we will prove the following statement by induction on k :

$S(k)$: *there exists a p -adic integer of the form*

$$a_k = b_0 + b_1p + \dots + b_kp^k$$

(whose digits b_i are in $\{0, 1, \dots, p - 1\}$ for all i) such that

$$F(a_k) \equiv 0 \pmod{p^{k+1}} \quad \text{and} \quad a_k \equiv \bar{a}_0 \pmod{p}.$$

The base of induction is obvious: taking b_0 equal to the first p -adic digit of \bar{a}_0 , we will have $a_0 \equiv \bar{a}_0$ and $F(a_0) \equiv 0 \pmod{p}$.

Now let us perform the induction step, i.e., prove that $S(k-1)$ implies $S(k)$. To do this, we set $a_k = a_{k-1} + b_k p^k$ for some (as yet unknown) digit b_k satisfying $0 \leq b_k < p$ and expand $F(a_k)$, ignoring terms divisible by p^{k+1} :

$$\begin{aligned} F(a_k) &= F(a_{k-1} + b_k p^k) = \sum_{i=0}^n c_i (a_{k-1} + b_k p^k)^i \\ &= c_0 + \sum_{i=1}^n c_i (a_{k-1}^i + i a_{k-1}^{i-1} b_k p^k + \text{terms divisible by } p^{k+1}) \\ &\equiv F(a_{k-1}) + b_k p^k F'(a_{k-1}) \pmod{p^{k+1}}. \end{aligned}$$

Since $F(a_{k-1}) \equiv 0 \pmod{p^k}$ by the inductive assumption, we can write

$$F(a_k) \equiv \alpha_k p^k + b_k p^k F'(a_{k-1}) \pmod{p^{k+1}}$$

for some integer $\alpha_k \in \{0, 1, \dots, p-1\}$. Thus we come to the following equation for the unknown digit b_k :

$$\alpha_k + b_k F'(a_{k-1}) \equiv 0 \pmod{p},$$

which we can easily solve provided $F'(a_{k-1}) \not\equiv 0 \pmod{p}$. But this is indeed the case because we obviously have $a_{k-1} \equiv \bar{a}_0 \pmod{p}$, so that

$$F'(a_{k-1}) \equiv F'(\bar{a}_0) \not\equiv 0 \pmod{p}.$$

Dividing by $F'(a_{k-1})$, we can find the required digit b_k ,

$$b_k = \frac{-\alpha_k}{F'(a_{k-1})} \pmod{p},$$

for which we will have $F(a_k) \equiv 0 \pmod{p^{k+1}}$, completing the induction step.

Now, let

$$a = b_0 + b_1 p + b_2 p^2 + \dots$$

Observe that $F(a) = 0$ since for all k we have

$$F(a) \equiv F(a_k) \equiv 0 \pmod{p^{k+1}}.$$

The uniqueness of a follows from the uniqueness of the sequence $\{a_k\}$. \square

Remark 1.40. The second condition ($F'(\bar{a}_0) \not\equiv 0 \pmod{p}$) in Theorem 1.39 is essential (see Exercise 35). However, there are many different versions of Theorem 1.39 in the literature, all of which are referred to as “Hensel’s Lemma”. Exercise 40 gives a version that can be used when the hypothesis $F'(\bar{a}_0) \not\equiv 0 \pmod{p}$ does not hold.

Remark 1.41. The method of approximation used in the proof of Hensel’s Lemma essentially coincides with Newton’s method of finding a real root of a polynomial $f(x)$ with real coefficients. In the real case, if $f'(a_{n-1}) \neq 0$, according to Newton’s method, the next approximation a_n is given by the formula

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})}.$$

The correction term looks very much like the “correction term” in the proof of Hensel’s Lemma:

$$b_n p^n \equiv -\frac{\alpha_n p^n}{F'(a_{n-1})} \equiv -\frac{F(a_{n-1})}{F'(a_{n-1})} \pmod{p^{n+1}}.$$

In one respect, however, Hensel’s Lemma is better than Newton’s method in the real case: in the p -adic case the convergence to a root of the polynomial is guaranteed by universal conditions on the approximate solution \bar{a}_0 whose form does not depend on the polynomial. In the real case, Newton’s method converges if the approximate solution is sufficiently close to the actual root, but the condition of closeness depends on the polynomial. For example, for $f(x) = x^3 - x$ and the unfortunate choice $a_0 = 1/\sqrt{5}$, we get $a_1 = -1/\sqrt{5}$, $a_2 = 1/\sqrt{5}$, etc., so the sequence $\{a_n\}$ does not converge.

Let us recall that in Theorem 1.30 the canonical expansion of p -adic numbers came out of a sequence of congruences. Hensel’s Lemma confirms this connection. The following theorem makes the connection between p -adic numbers and congruences even more prominent.

Theorem 1.42. *A polynomial with integer coefficients has a root in \mathbb{Z}_p if and only if it has an integer root modulo p^k for any $k \geq 1$.*

Proof. Let $F(x)$ be a polynomial with coefficients in \mathbb{Z} . Suppose $a \in \mathbb{Z}_p$ is its root, i.e.,

$$(1.21) \quad F(a) = 0.$$

By Theorem 1.30 there exists a sequence of integers $\{a_1, a_2, \dots, a_k, \dots\}$, where $a_k = b_0 + b_1p + b_2p^2 + \dots + b_{k-1}p^{k-1}$, such that

$$a \equiv a_k \pmod{p^k}.$$

Then $F(a_k) \equiv F(a) \pmod{p^k}$ and $F(a) = 0$ imply

$$(1.22) \quad F(a_k) \equiv 0 \pmod{p^k}.$$

Conversely, suppose the congruence (1.22) has an integer solution a_k for any $k \geq 1$. According to Theorem 1.34, the sequence $\{a_k\}$ contains a convergent subsequence $\{a_{k_i}\}$, $\lim_{i \rightarrow \infty} a_{k_i} = a$. We want to show that a is a solution of equation (1.21). Since a polynomial is a continuous function, we have

$$F(a) = \lim_{i \rightarrow \infty} F(a_{k_i})$$

(here we just use the fact that the limit of the sum is the sum of the limits and the limit of the product is the product of limits, i.e., Proposition 1.23). On the other hand,

$$F(a_{k_i}) \equiv 0 \pmod{p^{k_i}}.$$

Therefore $\lim_{i \rightarrow \infty} F(a_{k_i}) = 0$, and thus $F(a) = 0$. \square

A practical consequence of Theorem 1.42 is the following. If a polynomial with integer coefficients has no roots modulo p , then it has no roots in \mathbb{Z}_p . It is usually not too hard to find its roots modulo p if it has any. If a root modulo p is not a root of the derivative modulo p , then by Hensel's Lemma, we can find a root in \mathbb{Z}_p .

We say that a rational integer a not divisible by p is a *quadratic residue modulo p* if the congruence

$$x^2 \equiv a \pmod{p}$$

has a solution in $\{1, 2, \dots, p-1\}$. Otherwise a is called a *quadratic nonresidue*.

Proposition 1.43. *A rational integer a not divisible by p has a square root in \mathbb{Z}_p ($p \neq 2$) if and only if a is a quadratic residue modulo p .*

Proof. Let $P(x) = x^2 - a$. Then $P'(x) = 2x$. If a is a quadratic residue, then

$$a \equiv a_0^2 \pmod{p}$$

for some $a_0 \in \{1, 2, \dots, p-1\}$. Hence $P(a_0) \equiv 0 \pmod{p}$. But

$$P'(a_0) = 2a_0 \not\equiv 0 \pmod{p}$$

automatically since $(a_0, p) = 1$, so that the solution in \mathbb{Z}_p exists by Hensel's Lemma. Conversely, if a is a quadratic nonresidue, by Theorem 1.42 it has no square root in \mathbb{Z}_p . \square

For example $\sqrt{-1}$ is in \mathbb{Z}_5 since $-1 = 4 - 5 \equiv 2^2 \pmod{5}$ is a quadratic residue modulo 5, while $\sqrt{-1}$ is not in \mathbb{Z}_3 since $-1 = 2 - 3$ is a quadratic nonresidue modulo 3. Is \sqrt{p} in \mathbb{Z}_p ?

Exercises 35–44

Exercise 35. Construct a polynomial with integer coefficients which has a root modulo 2 but no roots in \mathbb{Q}_2 .

Exercise 36. Prove that if $p \neq 2$, a p -adic unit

$$u = c_0 + c_1p + c_2p^2 + \dots$$

is a square in \mathbb{Z}_p if and only if c_0 is a quadratic residue modulo p .

Exercise 37. Let $p \neq 2$ be a prime. Denote $(\mathbb{Q}_p^\times)^2 = \{a^2 \mid a \in \mathbb{Q}_p^\times\}$. Prove that the quotient group $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ has order 4, and find a complete set of coset representatives for it.

Exercise 38. Prove that the equation $x^3 - 1 = 0$ has a solution $a \neq 1$ in \mathbb{Z}_7 and find the first 3 digits in its canonical expansion.

Exercise 39. Prove that the equation $x^5 - 1 = 0$ has no solution $a \neq 1$ in \mathbb{Q}_7 . You must explain why such roots of unity, if they existed, must have been in \mathbb{Z}_7 , not merely in \mathbb{Q}_7 !

Exercise 40. Let $F(x)$ be a polynomial whose coefficients are in \mathbb{Z}_p , and suppose there exists a $\bar{a}_0 \in \mathbb{Z}_p$ such that $|F(\bar{a}_0)|_p \leq |F'(\bar{a}_0)|_p^2$.

Then there exists a unique $a \in \mathbb{Z}_p$ such that $F(a) = 0$ and $|a - \bar{a}_0|_p \leq \left| \frac{F(\bar{a}_0)}{F'(\bar{a}_0)} \right|_p$.

Exercise 41. Give an example of when the original version of Hensel's Lemma (Theorem 1.39) cannot be used to find a root of a polynomial equation, but Exercise 40 can be used and gives a root.

Exercise 42. Show that a unit $u \in \mathbb{Z}_2$ is a square if and only if $u \equiv 1 \pmod{8}$.

Exercise 43. Prove that \mathbb{Q}_2 contains $\sqrt{-7}$ and \mathbb{Q}_p ($p > 2$) contains $\sqrt{1-p}$.

Exercise 44. Prove that the quotient group $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2$ has order 8, is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and admits a complete set of representatives $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.

1.8. Algebraic properties of p -adic integers

We have already seen that the p -adic integers \mathbb{Z}_p differ in many ways from the ordinary integers \mathbb{Z} . Here we will see that their algebraic properties are just as good, if not better, than those of \mathbb{Z} . The ordinary integers \mathbb{Z} form a *commutative ring* (for the definition see §1.2).

Recall that a nonempty subset I of a ring R is said to be an *ideal* if I is a subgroup of R under addition and for any $x \in I$ and $r \in R$, $r \cdot x \in I$. For example, the set $m\mathbb{Z}$ of all integers divisible by a given number m forms an ideal in the ring \mathbb{Z} .

An ideal is called *maximal* if it is not contained in any other proper ideal. In the example above, the ideal $m\mathbb{Z}$ is maximal if and only if m is a prime number.

For a ring R and an ideal $I \subset R$, one can define the factor R/I as the set of additive cosets with canonically defined addition and multiplication. If R is a commutative ring with the multiplicative identity, R/I is a field if and only if I is a maximal ideal. For example, $\mathbb{Z}/p\mathbb{Z}$ is the field of residues modulo p , which is the only field with p elements. For details see [6, §3.5].

A commutative ring without zero divisors is called an *integral domain*.

Proposition 1.44. *The ring \mathbb{Z}_p is an integral domain.*

Proof. This follows because \mathbb{Z}_p is contained in \mathbb{Q}_p , which is a field, and hence contains no zero divisors. \square

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the finite field with p elements. The map

$$a = \sum_{i=0}^{\infty} a_i p^i \mapsto a_0$$

defines a ring homomorphism $\mathbb{Z}_p \rightarrow \mathbb{F}_p$ called *reduction modulo p* . This homomorphism is surjective, and its kernel is

$$\{a \in \mathbb{Z}_p \mid a_0 = 0\} = \left\{ \sum_{i=1}^{\infty} a_i p^i \right\} = \left\{ p \sum_{i=0}^{\infty} a_{i+1} p^i \right\} = p\mathbb{Z}_p.$$

Since the quotient is a field, the kernel $p\mathbb{Z}_p$ is a maximal ideal of the ring \mathbb{Z}_p .

Corollary 1.45. *The ring \mathbb{Z}_p has a unique maximal ideal, namely,*

$$p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^\times.$$

Proof. Suppose I is another maximal ideal. Since $p\mathbb{Z}_p$ is maximal, I must contain an element from its complement, $a \in \mathbb{Z}_p^\times$. Since I is an ideal, $1 = a \cdot a^{-1} \in I$, but then $I = \mathbb{Z}_p$. \square

Proposition 1.46. *The ring \mathbb{Z}_p is a principal ideal domain. More precisely, its ideals are the principal ideals $\{0\}$ and $p^k\mathbb{Z}_p$ for all $k \in \mathbb{N}$.*

Proof. Let $I \neq \{0\}$ be an ideal in \mathbb{Z}_p , and let $0 \neq a \in I$ be an element of maximal norm (since the norm takes discrete set of values, such an element can always be found). Assume that $|a|_p = p^{-k}$ for some $k \in \mathbb{N}$. Then $a = \epsilon p^k$, where ϵ is a unit. Then $p^k = \epsilon^{-1}a \in I$, and hence $(p^k) = p^k\mathbb{Z}_p \subset I$. Conversely, for any $b \in I$, $|b|_p = p^{-w} \leq p^{-k}$. We can write

$$b = p^w \epsilon' = p^k p^{w-k} \epsilon' \in p^k\mathbb{Z}_p.$$

Therefore, $I \subset p^k\mathbb{Z}_p$, and hence $I = p^k\mathbb{Z}_p$. \square

We discussed the existence of square roots in \mathbb{Q}_p in §1.7 as an application of Hensel's Lemma. Another application has to do with finding which roots of unity are in \mathbb{Q}_p .

Recall that an element in the field ζ is called an m th root of unity if $\zeta^m = 1$; it is called a *primitive m th root of unity* if, in addition, $\zeta^n \neq 1$ for $0 < n < m$.

Proposition 1.47. *For any prime p and any positive integer m relatively prime to p , there exists a primitive m th root of unity in \mathbb{Q}_p if and only if $m|(p-1)$. In the latter case, every m th root of unity is also a $(p-1)$ th root of unity. The set of $(p-1)$ th roots of unity is a cyclic subgroup of \mathbb{Z}_p^\times of order $(p-1)$.*

Proof. Let $m|(p-1)$; then $p-1 = km$ for $k \geq 1$, and therefore any m th root of 1 is also a $(p-1)$ th root of 1. Let

$$f(x) = x^{p-1} - 1, \quad f'(x) = (p-1)x^{p-2}.$$

Take $x_0 \in \mathbb{Z}_p^\times$ to be any rational integer satisfying $1 \leq x_0 \leq p-1$. Then

$$f(x_0) \equiv 0 \pmod{p} \quad \text{and} \quad f'(x_0) \not\equiv 0 \pmod{p}$$

since $|f'(x_0)|_p = 1$, and Hensel's Lemma applies, giving exactly $p-1$ solutions, which are $(p-1)$ th roots of 1. The first digits of these roots are $1, 2, \dots, p-1$. Conversely, if $\alpha \in \mathbb{Q}_p$ is an m th root of 1, $\alpha^m = 1$, we must have $|\alpha|_p = 1$, i.e., $\alpha \in \mathbb{Z}_p$. If α_0 is its first digit, then $\alpha_0^m \equiv 1 \pmod{p}$; hence m divides $p-1$, the order of $(\mathbb{Z}/p\mathbb{Z})^\times$. Since a polynomial with coefficients in a field can only have as many roots as its degree ([6, Lemma 5.3.2]), the polynomial $x^{p-1} - 1$ cannot have more than $p-1$ roots, and these roots must be all the roots of unity in \mathbb{Q}_p . It is clear that the roots of unity form a group under multiplication. Finally, since any finite subgroup of the multiplicative group of any field is cyclic ([6, Lemma 7.1.6]), the group of $(p-1)$ th roots of unity is a cyclic subgroup of \mathbb{Z}_p^\times of order $(p-1)$. \square

The (p^n) th roots of unity cannot be handled by means of Hensel's Lemma (why?) and will be discussed in Theorem 3.36.

The $(p-1)$ th roots of unity are related to the *signum function* $\text{sgn}_p(x)$ introduced in the next theorem.

Theorem 1.48. *For any $x \in \mathbb{Z}_p$ the limit $\lim_{n \rightarrow \infty} x^{p^n}$ exists. This limit is denoted by $\text{sgn}_p(x)$ and has the following properties:*

- (a) $\text{sgn}_p(x)$ depends only on the first digit in the canonical p -adic expansion of x , x_0 ;
 (b) $\text{sgn}_p(xy) = \text{sgn}_p(x) \cdot \text{sgn}_p(y)$;
 (c) $\text{sgn}_p(x) = 0$ if $x_0 = 0$, and it is a $(p-1)$ th root of 1 if $x_0 \neq 0$.

Proof. Let $x_0 \in \{1, 2, \dots, p-1\}$. First we show that the sequence $\{x_0^{p^n}\}$ converges. By Euler's Theorem,

$$x_0^{\varphi(p^n)} \equiv 1 \pmod{p^n},$$

where φ is Euler's φ -function: for a positive integer m , $\varphi(m)$ is equal to the number of integers smaller than m and relatively prime to m . Observe that since p is a prime, we have $\varphi(p^n) = p^n - p^{n-1}$. Thus,

$$x_0^{p^n - p^{n-1}} \equiv 1 \pmod{p^n}, \quad x_0^{p^n} \equiv x_0^{p^{n-1}} \pmod{p^n},$$

and hence

$$\left| x_0^{p^n} - x_0^{p^{n-1}} \right|_p \leq \frac{1}{p^n}.$$

Since $1/p^n \rightarrow 0$ as $n \rightarrow \infty$, the sequence $\{x_0^{p^n}\}$ is Cauchy, and by the completeness of \mathbb{Z}_p , it converges to a limit in \mathbb{Z}_p , which we denote by

$$\text{sgn}_p(x_0) = \lim_{n \rightarrow \infty} x_0^{p^n}.$$

The limit obviously exists for $x_0 = 0$, so $\text{sgn}_p(x)$ is defined for $x_0 \in \{0, 1, 2, \dots, p-1\}$, and $\text{sgn}_p(0) = 0$. Next we show that the limit exists for all $x \in \mathbb{Z}_p$ and is defined by the first digit x_0 of x . For this we will need the following lemma.

Lemma 1.49. *Suppose $x \in \mathbb{Z}_p$ with the first digit x_0 . Then we have $|x^p - x_0^p|_p \leq p^{-1}|x - x_0|_p$.*

Proof of the lemma. Let $x = x_0 + \alpha$, with $|\alpha|_p \leq p^{-1}$. Then

$$\begin{aligned} x^p - x_0^p &= \binom{p}{1} x_0^{p-1} \alpha + \binom{p}{2} x_0^{p-2} \alpha^2 + \cdots + \binom{p}{p} \alpha^p \\ &= (x - x_0) \left(\binom{p}{1} x_0^{p-1} + \binom{p}{2} x_0^{p-2} \alpha + \cdots + \binom{p}{p} \alpha^{p-1} \right). \end{aligned}$$

Since $|\binom{p}{j} x_0^{p-j} \alpha^{j-1}|_p \leq p^{-1}$ for $j \geq 1$, by the strong triangle inequality we obtain $|x^p - x_0^p|_p \leq p^{-1}|x - x_0|_p$. \square

Applying the lemma, we obtain

$$\left| x^{p^n} - x_0^{p^n} \right|_p \leq p^{-1} \left| x^{p^{n-1}} - x_0^{p^{n-1}} \right|_p \leq \cdots \leq p^{-n} |x - x_0|_p,$$

which implies that $\lim_{n \rightarrow \infty} x^{p^n}$ exists and is equal to $\lim_{n \rightarrow \infty} x_0^{p^n}$. Thus we have defined $\text{sgn}_p(x)$ for all $x \in \mathbb{Z}_p$, and property (a) of Theorem 1.48 is satisfied. Property (b) follows from the property of limits:

$$\lim_{n \rightarrow \infty} (xy)^{p^n} = \lim_{n \rightarrow \infty} (x^{p^n})(y^{p^n}) = \lim_{n \rightarrow \infty} x^{p^n} \lim_{n \rightarrow \infty} y^{p^n}.$$

It remains to show that if $x_0 \in \{1, 2, \dots, p-1\}$, then $\text{sgn}_p(x_0)$ is a $(p-1)$ th root of 1. Using property (b) and Fermat's Little Theorem (which is Euler's Theorem for $n = p$), we obtain

$$\text{sgn}_p^{p-1}(x_0) = \text{sgn}_p(x_0^{p-1}) = \text{sgn}_p(1) = 1.$$

The values of $\text{sgn}_p(x)$ are thus solutions of the equation $y^p - y = 0$. Since \mathbb{Q}_p is a field, this equation cannot have more than p solutions in \mathbb{Q}_p , and hence in \mathbb{Z}_p . Consequently, the only solutions of this equation are the values of the signum function. \square

1.9. Metrics and norms on the rational numbers. Ostrowski's Theorem

We have seen that the field \mathbb{Q} admits the p -adic norm $|\cdot|_p$ for each prime p , as well as the ordinary absolute value $|\cdot|$ (which is sometimes denoted by $|\cdot|_\infty$ for $p = \infty$, also referred to as the infinite prime). We shall prove now that there are no other norms on \mathbb{Q} , and hence the only completions of \mathbb{Q} are \mathbb{Q}_p for all prime p , and $\mathbb{R} = \mathbb{Q}_\infty$.

Theorem 1.50. (Ostrowski's Theorem). *Every nontrivial norm $\|\cdot\|$ on \mathbb{Q} is equivalent to $|\cdot|_p$ for some prime p or for $p = \infty$.*

Proof. Suppose first that $\|\cdot\|$ is Archimedean, i.e., there exists a positive integer n such that $\|n\| > 1$, and let n_0 be the least such n . Then we can write $\|n_0\| = n_0^\alpha$ for some positive real number α .

Now, write any positive integer n to the base n_0 , i.e., in the form

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s,$$

where $0 \leq a_i < n_0$, $i = 0, \dots, s$, and $a_s \neq 0$. Then

$$\begin{aligned} \|n\| &\leq \|a_0\| + \|a_1 n_0\| + \|a_2 n_0^2\| + \dots + \|a_s n_0^s\| \\ &= \|a_0\| + \|a_1\| n_0^\alpha + \|a_2\| n_0^{2\alpha} + \dots + \|a_s\| n_0^{s\alpha}. \end{aligned}$$

Since all of the digits a_i are less than n_0 , by our choice of n_0 , we have $\|a_i\| \leq 1$, and hence

$$\begin{aligned} \|n\| &\leq 1 + n_0^\alpha + n_0^{2\alpha} + \dots + n_0^{s\alpha} \\ &\leq n_0^{s\alpha} (1 + n_0^{-\alpha} + n_0^{-2\alpha} + \dots + n_0^{-s\alpha}) \\ &\leq n^\alpha \left(\sum_{i=0}^{\infty} \left(\frac{1}{n_0^\alpha} \right)^i \right), \end{aligned}$$

because $n \geq n_0^s$. The expression in brackets is a finite positive constant independent of n , which we call C . Thus

$$\|n\| \leq C n^\alpha \text{ for all } n = 1, 2, \dots$$

The same argument with n^N in place of n yields

$$\|n^N\| \leq C n^{N\alpha} \Rightarrow \|n\| \leq \sqrt[N]{C} n^\alpha.$$

Letting $N \rightarrow \infty$ for n fixed, we obtain

$$(1.23) \quad \|n\| \leq n^\alpha.$$

Let us prove the opposite inequality. First, observe that

$$n_0^{s+1} > n \geq n_0^s.$$

Since

$$n_0^{(s+1)\alpha} = \|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leq \|n\| + \|n_0^{s+1} - n\|,$$

we have

$$\|n\| \geq \|n_0^{s+1}\| - \|n_0^{s+1} - n\| \geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^\alpha,$$

because

$$\|n_0^{s+1} - n\| \leq (n_0^{s+1} - n)^\alpha$$

as was proved in (1.23). Thus

$$\begin{aligned} \|n\| &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^\alpha \text{ (since } n \geq n_0^s) \\ &= n_0^{(s+1)\alpha} \left[1 - \left(1 - \frac{1}{n_0} \right)^\alpha \right] = C' n_0^{(s+1)\alpha} \geq C' n^\alpha \end{aligned}$$

for some positive constant C' that does not depend on n .

As before, we now use this inequality for n^N , take N th roots, and let $N \rightarrow \infty$, obtaining

$$(1.24) \quad \|n\| \geq n^\alpha.$$

From (1.23) and (1.24), we deduce that $\|n\| = n^\alpha$ for all $n \in \mathbb{N}$. Using property (2) of the norm, we readily see that $\|x\| = |x|^\alpha$ for all $x \in \mathbb{Q}$. In view of Proposition 1.10, we can conclude that such a norm is equivalent to the absolute value $|\cdot|$.

Now suppose that $\|\cdot\|$ is non-Archimedean, i.e., we have $\|n\| \leq 1$ for all positive integers n . Because we have assumed that $\|\cdot\|$ is nontrivial, we can find n_0 , the least n such that $\|n\| < 1$. Observe that n_0 must be a prime number, because if $n_0 = n_1 n_2$, with $n_1, n_2 < n_0$, then $\|n_1\| = \|n_2\| = 1$, and so $\|n_0\| = \|n_1\| \|n_2\| = 1$. Denote the prime number n_0 by p .

Next, we will prove that if n is not divisible by p , then $\|n\| = 1$. Write $n = rp + s$ with $0 < s < p$. By the minimality of p , $\|s\| = 1$. We also have $\|rp\| < 1$ since $\|p\| < 1$ (by choice) and $\|r\| \leq 1$ (by the non-Archimedean property, since r is an integer). Consequently,

$$\|n - s\| < \|s\|,$$

and by Proposition 1.15, $\|n\| = \|s\| = 1$. Finally, given any $n \in \mathbb{Z}$, we can write $n = p^v n'$, where p does not divide n' . Hence

$$\|n\| = \|p\|^v \|n'\| = \|p\|^v.$$

Let $\rho = \|p\| < 1$. Then $\rho = (1/p)^\alpha$ for some positive real α . Therefore

$$\|n\| = |n|_p^\alpha.$$

Now, it is easy to show (using property (2) of the norm) that the same formula holds with any nonzero rational number x in place of n . In view of Proposition 1.10, we have $\|\cdot\| \sim |\cdot|_p$ and this concludes the proof of the theorem. \square

Proposition 1.51. (Product Formula). *Let $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$. For any $x \in \mathbb{Q}^\times$ we have*

$$\prod_{p \leq \infty} |x|_p = 1,$$

where the product is taken over all primes of \mathbb{Q} including the “prime at infinity”.

Proof. It is sufficient to prove this formula when x is a positive integer; the rest follows from the multiplicative property of the norm. So, suppose that $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. Then $|x|_q = 1$ if $q \neq p_i$, $|x|_{p_i} = p_i^{-a_i}$ for $i = 1, \dots, k$, and $|x| = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. The result follows. \square

The product formula establishes a close relationship between the norms on \mathbb{Q} . For instance, if we know the values of all but one norm, this allows us to recover the value of the missing one. This is very important in many applications to algebraic geometry.

Suppose we want to find a root of a polynomial in \mathbb{Q} . Evidently, if there are roots in \mathbb{Q} , then there are roots in \mathbb{R} and in all \mathbb{Q}_p . Hence we can certainly conclude that there are *no* rational roots if there is some $p \leq \infty$ for which there are no p -adic roots (again, “ ∞ -adic” means “real”). A converse statement would be more interesting, but is it true? If a polynomial has p -adic roots for all p including ∞ , does it follow that it has a rational root? Here is a simple example when such a converse statement holds.

Proposition 1.52. *A number $x \in \mathbb{Q}$ is a square if and only if it is a square in every \mathbb{Q}_p , $p \leq \infty$.*

Proof. For any $x \in \mathbb{Q}^\times$ we have

$$x = \pm \prod_{p < \infty} p^{\text{ord}_p(x)}.$$

Notice that x is a square in \mathbb{R} if and only if it is positive. In \mathbb{Q}_p we can write $x = p^{\text{ord}_p(x)}u$, where $u \in \mathbb{Z}_p^\times$ (Proposition 1.37). Then x is a square in \mathbb{Q}_p if and only if $\text{ord}_p(x)$ is even and $u = v^2$ for some unit $v \in \mathbb{Z}_p^\times$. If we write out the factorization, we see that x is a square in \mathbb{Q} if and only if it is a square in each \mathbb{Q}_p . \square

This is a manifestation of the so-called *Local-to-Global Principle*, which asserts that the existence or nonexistence of solutions in \mathbb{Q} (global solutions) of a Diophantine equation can be detected by studying, for each $p \leq \infty$, the solutions in \mathbb{Q}_p (local solutions). Unfortunately, this principle is not universal, but it holds in some important cases, for instance for quadratic forms in several variables (the

Hasse-Minkowski Theorem, [17]). Exercise 46 gives an example when this principle does not hold.

Exercises 45–46

Exercise 45. Two fields F and K are called *isomorphic* if there exists a bijective map $\varphi : F \rightarrow K$ such that

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

- (1) Prove that \mathbb{Q}_p and \mathbb{R} are not isomorphic.
- (2)* Prove that if $p \neq q$ are two primes, then \mathbb{Q}_p and \mathbb{Q}_q are not isomorphic.

Exercise 46. Prove that an equation

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$$

has a root in \mathbb{Q}_p for all $p \leq \infty$ but not in \mathbb{Q} .

1.10. A digression: what about \mathbb{Q}_g if g is not a prime?

In order to fully appreciate the beauty of p -adic numbers, let us see what happens if we use a nonprime number g instead of a prime p . In order to use the formula (1.11) to define $|\cdot|_g$, we have to be a little more careful in the definition of $\text{ord}_g(x)$ for a rational number a . If $x \in \mathbb{Z}$, $\text{ord}_g(x)$ is still the highest power of g which divides x . If $x = a/b$, the definition is different from the case in which $g = p$ is a prime, and in order to give it, we need the following lemma.

Lemma 1.53. *Let $x = a/b$, $a, b \in \mathbb{N}$, $(a, b) = 1$. Then there exist a unique integer v and a pair of integers a' and b' such that $a/b = g^v a'/b'$, $g \nmid a'$ (a', b') = $(g, b') = 1$.*

Proof. Obviously, if $g \nmid a$ and $(g, b) = 1$, then we can choose $v = 0$.

If $g|a$, denote by g^ϕ , where $\phi \geq 1$, the highest power of g that divides a . Putting $a' = ag^{-\phi}$ and $b' = b$, we obtain $g \nmid a'$ and

$(a', b') = (g, b') = 1$, and furthermore

$$\frac{a}{b} = g^\phi \frac{a'}{b'},$$

which proves the assertion with $v = \phi > 0$.

Now assume that $g \nmid a$ and $(g, b) > 1$. Then b can be factored as $b = b_1 b_2$, ($b_1, b_2 > 0$) so that all prime factors of b_1 divide g and $(b_2, g) = 1$. Similarly, g can be written as $g = g_1 g_2$ ($g_1, g_2 > 0$) so that all prime factors of g_1 divide b_1 , but $(g_2, b_1) = (g_2, b) = 1$. There is a smallest positive integer ψ such that $b_1 | g^\psi$ and hence also $b_1 | g_1^\psi$. In the equation

$$g^\psi \frac{a}{b} = \frac{g_1^\psi g_2^\psi}{b_1 b_2} a,$$

the quotient g_1^ψ / b_1 is an integer. Therefore if we put

$$a' = \frac{g_1^\psi}{b_1} g_2^\psi a \quad \text{and} \quad b' = b_2,$$

we obtain

$$\frac{a}{b} = g^{-\psi} \frac{a'}{b'}, \quad g \nmid a', \quad (a', b') = (g, b') = 1,$$

proving the assertion with $v = -\psi < 0$. \square

Now for $x = a/b$, we define $\text{ord}_g(x)$ to be the integer v from Lemma 1.53, and we define the corresponding norm as

$$(1.25) \quad |a/b|_g = g^{-v}.$$

This norm, however, will not satisfy the multiplicative property (2) of Definition 1.5. For example,

$$\left| \frac{1}{20} \right|_{10} = 10^2, \quad \left| \frac{1}{50} \right|_{10} = 10^2, \quad \text{but} \quad \left| \frac{1}{20} \cdot \frac{1}{50} \right|_{10} = \left| \frac{1}{1000} \right|_{10} = 10^3;$$

therefore

$$\left| \frac{1}{20} \cdot \frac{1}{50} \right|_{10} < \left| \frac{1}{20} \right|_{10} \cdot \left| \frac{1}{50} \right|_{10}.$$

In general

$$(1.26) \quad |ab|_g \leq |a|_g |b|_g,$$

and $|\cdot|_g$ is not a norm but a so-called *pseudo-norm* (see Exercise 47). Nevertheless, $d(x, y) = |x - y|_g$ is still a metric, and one can consider the completion of \mathbb{Q} with respect to this metric. Denoted by \mathbb{Q}_g , it is

a ring but not a field if g is not a prime (see Exercise 48). Of course, if $g = p$ is a prime, then the definition in (1.25) coincides with the definition in (1.11).

The following theorem is due to Hensel:

Theorem 1.54. *If $g = p_1 p_2 \dots p_k$ is a product of distinct primes, then $\mathbb{Q}_g = \mathbb{Q}_{p_1} \oplus \dots \oplus \mathbb{Q}_{p_k}$, the direct sum of p -adic fields.*

Proof. We will construct this isomorphism in the case $g = 10$, $p_1 = 2$, $p_2 = 5$, but the general case is handled similarly without any complications.

Consider a Cauchy sequence in \mathbb{Q} relative to $|\cdot|_{10}$. It defines a 10-adic number

$$A = \lim_{n \rightarrow \infty}^{(10)} a_n,$$

and the existence of the 10-adic limit implies the existence of the 2-adic and the 5-adic limits which we denote by

$$A_2 = \lim_{n \rightarrow \infty}^{(2)} a_n, \quad A_5 = \lim_{n \rightarrow \infty}^{(5)} a_n,$$

respectively. Conversely, the existence of the limits A_2 and A_5 evidently implies that of A . It is easy to see that the digits of A_2 and A_5 do not depend on the Cauchy sequence $\{a_n\}$ by means of which A was defined.

In particular, if $A \in \mathbb{Q}_{10}$, it can be canonically expanded as

$$(1.27) \quad A = \sum_{n=-f}^{\infty} b_n 10^n.$$

In order to find the digits of A_2 and A_5 , we write

$$A_2 = \sum_{n=-f}^{\infty} (b_n 5^n) 2^n = \sum_{n=-f}^{\infty} c_n 2^n, \quad A_5 = \sum_{n=-f}^{\infty} (b_n 2^n) 5^n = \sum_{n=-f}^{\infty} d_n 5^n,$$

where the coefficients c_n and d_n in the respective canonical expansions are obtained by reduction to the canonical form (Theorem 1.30). Thus we have $A = \langle A_2, A_5 \rangle$, and from the rules for the sum, difference, and product of g -adic and p -adic limits, we see that if $B = \langle B_2, B_5 \rangle$ is a second 10-adic number with $B_2 \in \mathbb{Q}_2$ and $B_5 \in \mathbb{Q}_5$, then

$$A \pm B = \langle A_2 \pm B_2, A_5 \pm B_5 \rangle \text{ and } AB = \langle A_2 B_2, A_5 B_5 \rangle.$$

Conversely, let $A_2 \in \mathbb{Q}_2$ and $A_5 \in \mathbb{Q}_5$ be arbitrary. We will show that there exists an $A \in \mathbb{Q}_{10}$ such that $A = \langle A_2, A_5 \rangle$. For $p = 2, 5$, let $\{a_n^{(p)}\}$ be a sequence of rational numbers such that $A_p = \lim_{n \rightarrow \infty} a_n^{(p)}$ in $|\cdot|_p$.

There is no reason why the sequence $\{a_n^{(p)}\}$ should converge in $|\cdot|_q$ for $q \neq p$, and it may not even be bounded relative to $|\cdot|_q$. In order to overcome this difficulty, we consider the sequences

$$e_n^{(2)} = \frac{5^n}{2^n + 5^n}, \quad e_n^{(5)} = \frac{2^n}{2^n + 5^n}.$$

It is easy to see that

$$\lim_{n \rightarrow \infty} e_n^{(p)} = \delta_{pq} \text{ in } |\cdot|_q, \text{ where } \delta_{pq} = \begin{cases} 1 & \text{if } p = q, \\ 0 & \text{if } p \neq q. \end{cases}$$

It follows that there is an infinite subsequence $e_{r_n}^{(p)}$ such that

$$\lim_{n \rightarrow \infty} a_n^{(p)} e_{r_n}^{(p)} = \begin{cases} A_p & \text{if } p = q, \\ 0 & \text{if } p \neq q. \end{cases}$$

Hence

$$\lim_{n \rightarrow \infty} a_n^{(2)} e_{r_n}^{(2)} = \langle A_2, 0 \rangle, \text{ and } \lim_{n \rightarrow \infty} a_n^{(5)} e_{r_n}^{(5)} = \langle 0, A_5 \rangle.$$

Finally, we see that the sequence $a_n = a_n^{(2)} e_{r_n}^{(2)} + a_n^{(5)} e_{r_n}^{(5)}$ converges to $\langle A_2, A_5 \rangle = A$. \square

Exercises 47–50

Exercise 47. Prove that if g is not a prime, then $|\cdot|_g$ is a pseudo-norm on \mathbb{Q} , i.e., it satisfies (1) and (3) of Definition 1.5 and (1.26).

Exercise 48. Prove that \mathbb{Q}_{10} is not a field by displaying zero divisors.

Exercise 49.* Look at the following sequence of integers:

$$6, 76, 376, 9376, 109376 \dots$$

-
- (1) Prove that it can be continued in a unique way to obtain a 10-adic integer $\alpha = \dots 109376$ such that $\alpha^2 = \alpha$.
 - (2) Prove that the equation $x^2 = x$ has 4 solutions in \mathbb{Z}_{10} , namely $0, 1, \alpha$ and β .
 - (3) Find the first 6 digits of β .
 - (4) Prove that $\mathbb{Z}_{10} \approx \mathbb{Z}_5 \oplus \mathbb{Z}_2$ (direct product of groups).

Exercise 50. Prove that there is no relation of *total order* \leq on \mathbb{Q}_p possessing the following properties:

- (1) if $x \leq y$, then $z + x \leq z + y$ for any z ;
- (2) if $0 \leq x$ and $0 \leq y$, then $0 \leq xy$.