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

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

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 $d(a_n, b_n) \to 0$. (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

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

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,

$$d(r_1, r_2) = |r_1 - r_2|, \tag{1.2}$$

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

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

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 $\mathbb{Q}$:

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

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 $\{0, 1, \ldots, g-1\}$. 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 $x \in \overset{A}{\cancel{M}}$ there exists an open ball $B(a, r) \subset \overset{A}{\cancel{M}}$ 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 $\{B_n\}$, $B_1 \supset B_2 \supset B_3 \supset \ldots$ 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 $\lim_{n\to\infty} d(a_n, b_n)$ 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 $\lim_{n\to\infty} d(a_n, b_n) = \lim_{n\to\infty} d(a'_n, b'_n)$.

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) $\|x + y\| \le \|x\| + \|y\| \quad \forall\, x, y \in F$ (*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

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

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) $\|x \pm y\| \ge |\,\|x\| - \|y\|\,|$;

(d) $\|x - y\| \le \|x\| + \|y\|$;

(e) $\|x/y\| = \|x\|/\|y\|$;

(f) $\|n\| \le n\ \forall\, n \in \mathbb{N}$.

Proof.

(a) $\|1\| = \|\pm 1 \cdot \pm 1\| = \|\pm 1\|^2 \Longrightarrow \|\pm 1\| = 1$.

(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
$$\|a_n\| \le C \ \forall n;$$
- a *null* sequence if
$$\lim_{n\to\infty} \|a_n\| = 0,$$
i.e., for any $\varepsilon > 0$ there is an N such that for all $n > N$ $\|a_n\| < \varepsilon$;
- a *Cauchy* sequence if
$$\lim_{n,m\to\infty} \|a_n - a_m\| = 0,$$
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 $a = \lim_{n\to\infty} a_n$) if
$$\lim_{n\to\infty} \|a_n - a\| = 0,$$
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 $\lim_{n\to\infty} a_n = a$; then
$$\|a_n - a_m\| = \|a_n - a + a - a_m\| \le \|a_n - a\| + \|a - a_m\| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$
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* $\lim_{n\to\infty} x^n = 0$.

Proof. Let $\|x\| < 1$. Since $\|x^n\| = \|x\|^n$, we obtain
$$\lim_{n\to\infty} \|x^n\| = 0,$$
i.e., $\lim_{n\to\infty} x^n = 0$. Conversely, if $\|x\| \ge 1$, then for all positive n we have $\|x^n\| \ge 1$, and therefore $0 \ne \lim_{n\to\infty} x^n$. □

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*

$$\|x\|_2 = \|x\|_1^{\alpha}, \quad \forall\, x \in F. \tag{1.4}$$

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 $\|a\|_1 \ne 1$. 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

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

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

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

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

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. □

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

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

The first inequality follows from to 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, $|1+1|^\alpha = 2^\alpha > |1|^\alpha + |1|^\alpha = 2$. □

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

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 $k \in \{1, \cdots, n-1\}$; let us prove that $\|n\| \leq 1$.

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

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

(b) $\Rightarrow$ (a). We have

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

So, for every integer n we have

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

Letting n tend to ∞, we obtain

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

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

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

□

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 $\|n\|^k \to \infty$ as $k \to \infty$, 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:

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

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,

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

On the other hand,

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

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

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. □

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

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

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 $\{n_1, n_2, \ldots\}$ be an increasing sequence of positive integers. If the subsequence

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

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

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

and its identity element under multiplication is the sequence

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

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

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

For every $a \in F$ the constant sequence

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

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