# $p$-adic numbers, LTCC 2010

Manuel Breuning
King's College London

---

Contents



## Notation

In this course we will use the following standard notations:

$$\begin{aligned}
\mathbb{N} &= \{1, 2, 3, \dots\},\\
\mathbb{Z} &= \{\dots, -2, -1, 0, 1, 2, \dots\},\\
\mathbb{Q} &= \text{rational numbers},\\
\mathbb{R} &= \text{real numbers},\\
\mathbb{C} &= \text{complex numbers}.
\end{aligned}$$

Furthermore we will need the following sets:

$$\begin{aligned}
\mathbb{Z}_{\geq 0} &= \{0, 1, 2, \dots\},\\
\mathbb{R}_{>0} &= \text{positive real numbers},\\
\mathbb{R}_{\geq 0} &= \text{non-negative real numbers}.
\end{aligned}$$

By a ring we will always mean a commutative ring with 1. If $R$ is a ring then $R^\times$ denotes the group of units in $R$, so in particular if $R$ is a field then $R^\times = R \setminus \{0\}$.

## 1. Absolute values and completion

In this chapter we define absolute values on fields, construct all absolute values on the field of rational numbers $\mathbb{Q}$, and discuss the completion of a valued field.

### 1.1. **Absolute values.** We write $\mathbb{R}_{\geq 0}$ for the set of non-negative real numbers.

**Definition 1.1.** Let $K$ be a field. An *absolute value* on $K$ is a function

$$| \ | : K \to \mathbb{R}_{\geq 0}$$

that satisfies the following conditions.

(1) $|x| = 0$ if and only if $x = 0$
(2) $|xy| = |x| \cdot |y|$ for all $x, y \in K$
(3) $|x + y| \leq |x| + |y|$ for all $x, y \in K$

We say that an absolute value $| \ |$ on $K$ is *non-archimedean* if it satisfies the following strengthening of (3).

(3') $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$

We say that an absolute value $| \ |$ on $K$ is *archimedean* if it is not non-archimedean.

Some authors use the word *norm* or *valuation* instead of absolute value. A pair $(K, | \ |)$ consisting of a field $K$ and an absolute value $| \ |$ on $K$ is called a *valued field*. We will sometimes refer to $K$ as a valued field if the absolute value $| \ |$ is clear from the context.

If $| \ |$ is an absolute value on $K$ then one easily sees that $|1| = 1$ and $|-x| = |x|$ for all $x \in K$.

**Example 1.2.** Let $K$ be any field and define $| \ | : K \to \mathbb{R}_{\geq 0}$ by

$$|x| = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \neq 0. \end{cases}$$

One easily sees that this defines a non-archimedean absolute value on $K$. It is called the *trivial absolute value* on $K$.

**Remark 1.3.** If $K$ is a field and $n \in \mathbb{N}$ then we also write $n$ for the element $1+1+\cdots+1 \in K$ (where $1+1+\cdots+1$ has $n$ summands, and 1 is the multiplicative identity of $K$). Now if $| \ |$ is a non-archimedean absolute value on $K$, then for every $n \in \mathbb{N}$ we have $|n| \leq 1$ (this follows by induction using $|n| = |(n-1)+1| \leq \max\{|n-1|, |1|\}$). One can show that the converse of this statement is also true, i.e. if an absolute value $| \ |$ on $K$ has the property that $|n| \leq 1$ for all $n \in \mathbb{N}$ then $| \ |$ is non-archimedean; for a proof see e.g. [Schikhof, §8].

**Example 1.4.** The usual absolute value $|x + iy|_{\mathbb{C}} = \sqrt{x^2 + y^2}$ is an absolute value on the field of complex numbers $\mathbb{C}$. This absolute value is archimedean (because since $|2|_{\mathbb{C}} = 2 > 1$ it is not non-archimedean by the previous remark).

**Exercise 1.5.** Let $K$ be a finite field. Show that $K$ has no non-trivial absolute values.

### 1.2. **The topology of a valued field.** Let $(K, | \ |)$ be a valued field.

**Lemma 1.6.** *The function $d : K \times K \to \mathbb{R}_{\geq 0}$ defined by $d(x, y) = |x - y|$ is a metric on $K$. We call $d$ the metric induced by the absolute value $| \ |$.*

*Proof.* Clear. □

If $|\ |$ is a non-archimedean absolute value, then the induced metric satisfies the *ultrametric inequality*

$$d(x,z) \leq \max\{d(x,y), d(y,z)\} \text{ for all } x,y,z \in K.$$

**Definition 1.7.** Let $x \in K$ and $\varepsilon > 0$.

(1) The set $B_{<\varepsilon}(x) = \{y \in K : |y-x| < \varepsilon\}$ is called the *open ball* with radius $\varepsilon$ and centre $x$.
(2) The set $B_{\leq\varepsilon}(x) = \{y \in K : |y-x| \leq \varepsilon\}$ is called the *closed ball* with radius $\varepsilon$ and centre $x$.

From the metric $d$ we obtain a topology on $K$ which we call *the topology induced by* $|\ |$. The set of all open balls $B_{<\varepsilon}(x)$ (with $x \in K$ and $\varepsilon > 0$) is a basis of this topology. So a valued field $(K, |\ |)$ has a natural metric and topology, therefore it makes sense to talk about open sets in $K$, limits of sequences in $K$, continuous functions $K \to K$, etc.

**Proposition 1.8.** *$K$ is a topological field, i.e. the field operations*

(1) $K \times K \to K$, $(x,y) \mapsto x+y$
(2) $K \times K \to K$, $(x,y) \mapsto xy$
(3) $K \to K$, $x \mapsto -x$
(4) $K \setminus \{0\} \to K \setminus \{0\}$, $x \mapsto x^{-1}$

*are continuous.*

*Proof.* Let's prove statement (2) in detail. We must show that if $(x,y) \in K \times K$ and $\varepsilon > 0$ then there exists a $\delta > 0$ such that the open neighbourhood $B_{<\delta}(x) \times B_{<\delta}(y)$ of $(x,y)$ in $K \times K$ is mapped into $B_{<\varepsilon}(xy)$ under the multiplication map. Now if $(u,v) \in B_{<\delta}(x) \times B_{<\delta}(y)$ then

$$\begin{aligned} |uv - xy| &= |(u-x)(v-y) + (u-x)y + (v-y)x| \\ &\leq |u-x| \cdot |v-y| + |u-x| \cdot |y| + |v-y| \cdot |x| \\ &\leq \delta \cdot \delta + \delta \cdot |y| + \delta \cdot |x|. \end{aligned}$$

So for sufficiently small $\delta > 0$ (where sufficiently small depends on $|x|$ and $|y|$ but not on $u$ and $v$) we have $|uv - xy| < \varepsilon$, i.e. $uv \in B_{<\varepsilon}(xy)$ as required.

The proofs of statements (1),(3) and (4) are similar. □

**Exercise 1.9.** Show that the function $K \to \mathbb{R}_{\geq 0}$, $x \mapsto |x|$ is continuous.

1.3. **Absolute values on the rational numbers.** We now consider absolute values on the field of rational numbers $\mathbb{Q}$.

We will denote the usual absolute value on $\mathbb{Q}$ by $|\ |_\infty$, so

$$|x|_\infty = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x < 0. \end{cases}$$

Clearly $|\ |_\infty$ is an archimedean absolute value on $\mathbb{Q}$.

Now fix a prime number $p$. We will define a non-archimedean absolute value $|\ |_p$ on $\mathbb{Q}$, the *$p$-adic absolute value*. First let $x \in \mathbb{Q}^\times$. By the fundamental theorem of arithmetic we can write $x = \pm p^e q_1^{e_1} \cdots q_r^{e_r}$ where $q_1, \ldots, q_r$ are non-zero prime numbers different from $p$ and $e, e_1, \ldots, e_r \in \mathbb{Z}$. We define $|x|_p = p^{-e}$. For $x = 0$ we define $|0|_p = 0$.

**Lemma 1.10.** *$|\ |_p$ is a non-archimedean absolute value on $\mathbb{Q}$.*

*Proof.* Conditions (1) and (2) of an absolute value are clearly satisfied. It remains to prove condition (3'). We first observe that if $x = 0$ or $y = 0$ or $x + y = 0$ then condition (3') is clearly true, so we can assume that $x, y, x + y \in \mathbb{Q}^\times$. We write $x = \pm p^e q_1^{e_1} \cdots q_r^{e_r}$, $y = \pm p^f q_1^{f_1} \cdots q_r^{f_r}$ and $x + y = \pm p^g q_1^{g_1} \cdots q_r^{g_r}$. Then

$$\begin{aligned} x &= p^{\min\{e,f\}} q_1^{\min\{e_1,f_1\}} \cdots q_r^{\min\{e_r,f_r\}} \cdot x', \\ y &= p^{\min\{e,f\}} q_1^{\min\{e_1,f_1\}} \cdots q_r^{\min\{e_r,f_r\}} \cdot y' \end{aligned}$$

for some $x', y' \in \mathbb{Z} \setminus \{0\}$. It follows that

$$x + y = p^{\min\{e,f\}} q_1^{\min\{e_1,f_1\}} \cdots q_r^{\min\{e_r,f_r\}} \cdot (x' + y'),$$

hence

$$p^g q_1^{g_1} \cdots q_r^{g_r} = p^{\min\{e,f\}} q_1^{\min\{e_1,f_1\}} \cdots q_r^{\min\{e_r,f_r\}} \cdot z$$

for some $z \in \mathbb{Z} \setminus \{0\}$. From this we can deduce that $g \geq \min\{e, f\}$. It follows that

$$\begin{aligned} |x + y|_p = p^{-g} &\leq p^{-\min\{e,f\}} \\ &= p^{\max\{-e,-f\}} \\ &= \max\{p^{-e}, p^{-f}\} = \max\{|x|_p, |y|_p\}. \end{aligned}$$

This completes the proof of condition (3'). □

Hence for each prime number $p$ we obtain a non-archimedean absolute value $| \ |_p$ on $\mathbb{Q}$. Furthermore we have the archimedean absolute value $| \ |_\infty$ on $\mathbb{Q}$ and the trivial absolute value. Theorem 1.12 below shows that this is essentially the complete list of absolute values on $\mathbb{Q}$.

**Definition 1.11.** Two absolute values on a field $K$ are called *equivalent* if they induce the same topology on $K$.

One can show that two absolute values $| \ |$ and $\| \ \|$ on $K$ are equivalent if and only if there exists a positive real number $\alpha$ such that $|x| = \|x\|^\alpha$ for all $x \in K$. In particular it follows that a sequence in $K$ is Cauchy with respect to $| \ |$ if and only if it is Cauchy with respect to $\| \ \|$. Hence two equivalent absolute values give rise to the same completion of $K$.

**Theorem 1.12.** *(Ostrowski) Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to either the archimedean absolute value $| \ |_\infty$ or to the non-archimedean absolute value $| \ |_p$ for some prime number $p$.*

For a proof of Ostrowski's theorem and the statements about equivalent absolute values see e.g. [Gouvea, §3.1].

**Exercise 1.13.** The *product formula* states that

$$|x|_\infty \cdot \prod_p |x|_p = 1$$

for all $x \in \mathbb{Q}^\times$ (where the product runs over all prime numbers $p$). Prove this formula.

1.4. **Completion.** Let $K$ be a field with an absolute value $| \ | : K \to \mathbb{R}_{\geq 0}$ and let $d(x, y) = |x - y|$ be the induced metric. A *Cauchy sequence* in $K$ is a sequence $x_1, x_2, x_3, \dots \in K$ with the property that for every $\varepsilon > 0$ there exists an $N \in \mathbb{N}$ such that $d(x_i, x_j) < \varepsilon$ for all $i, j \geq N$. We call $K$ *complete* if every Cauchy sequence in $K$ has a limit.

**Definition 1.14.** Let $(K, | \ |)$ be a valued field. A *completion* of $K$ is a valued field $(\hat{K}, \| \ \|)$ where $\hat{K}$ is a field extension of $K$ and $\| \ \|$ is an absolute value on $\hat{K}$ which extends the absolute value on $K$ such that

(1) $\hat{K}$ is complete,
(2) $K$ is dense in $\hat{K}$, i.e. every non-empty open subset of $\hat{K}$ contains an element from $K$.

**Theorem 1.15.** *Let $(K, |\ |)$ be a valued field. Then there exists a completion $(\hat{K}, \|\ \|)$ of $K$.*

*Proof.* In this proof we will write $(x_i)$ for a sequence $x_1, x_2, x_3, \dots$ in $K$.

Let $C$ be the set of all Cauchy sequences in $K$. Then $C$ becomes a commutative ring if we define the sum and product of two sequences $(x_i), (y_i) \in C$ by $(x_i)+(y_i) = (x_i + y_i)$ and $(x_i) \cdot (y_i) = (x_i y_i)$ (check that these are again Cauchy sequences).

Define $M$ to be the set of all sequences in $K$ that converge to 0 (these are automatically Cauchy sequences). It is easy to check that $M$ is an ideal of the ring $C$. In fact, $M$ is a maximal ideal of $C$. To see this, let $I \subseteq C$ be an ideal that properly contains $M$. We must show that $I = C$. Let $(x_i) \in I \setminus M$. Then $(x_i)$ is a Cauchy sequence that does not converge to 0, therefore there exists a $\delta > 0$ such that $|x_i| \geq \delta$ for all sufficiently large $i$. In particular $x_i \neq 0$ for all sufficiently large $i$. Define a sequence $(y_i)$ by $y_i = 0$ if $x_i = 0$ and $y_i = x_i^{-1}$ if $x_i \neq 0$. It is easy to check that $(y_i)$ is a Cauchy sequence, i.e. $(y_i) \in C$, hence $(y_i) \cdot (x_i) \in I$ since $I$ is an ideal. But the sequence $(x_i y_i)$ is equal to 1 for all but finitely many $i$, hence $(1, 1, \dots) = (x_i y_i) + (z_i)$ for some sequence $(z_i) \in M \subset I$ (here $(1, 1, \dots)$ denotes the constant sequence $1, 1, 1, \dots$). This shows that $(1, 1, \dots) \in I$ and thus $I = C$ as required.

We define $\hat{K}$ to be the quotient ring, $\hat{K} = C/M$. This is a field because $M$ is maximal. The (injective) homomorphism $h : K \to \hat{K}$, $x \mapsto h(x) = (x, x, \dots) + M$ (where $(x, x, \dots)$ denotes the constant sequence $x, x, x, \dots$) allows us to consider $K$ as a subfield of $\hat{K}$.

Next we define an absolute value $\|\ \| : \hat{K} \to \mathbb{R}_{\geq 0}$. First note that if $(x_i)$ is a Cauchy sequence in $K$ then $|x_1|, |x_2|, |x_3|, \dots$ is a Cauchy sequence in $\mathbb{R}$, and since $\mathbb{R}$ is complete the limit $\lim_{i\to\infty}|x_i|$ exists. Now for $(x_i) + M \in \hat{K}$ we define $\|(x_i)+M\| = \lim_{i\to\infty}|x_i|$. It is easy to check that this gives a well-defined absolute value on $\hat{K}$ which extends the absolute value on $K$.

To remains to show that $K$ is dense in $\hat{K}$ and that $\hat{K}$ is complete.

Let $(x_i) + M \in \hat{K}$ and $\varepsilon > 0$. Choose $N \in \mathbb{N}$ such that $|x_i - x_j| < \varepsilon/2$ for all $i, j \geq N$. Then

$$\|(x_i) + M - h(x_N)\| = \|(x_1 - x_N, x_2 - x_N, \dots) + M\| = \lim_{i\to\infty} |x_i - x_N| \leq \varepsilon/2 < \varepsilon.$$

This shows that the $\varepsilon$-ball in $\hat{K}$ with centre $(x_i) + M$ contains the element $h(x_N)$ from $K$, i.e. $K$ is dense in $\hat{K}$.

Finally let $a_1, a_2, a_3, \dots$ be a Cauchy sequence in $\hat{K}$. Since $K$ is dense in $\hat{K}$, for every $i \in \mathbb{N}$ we can choose an $x_i \in K$ such that $\|a_i - h(x_i)\| < 1/i$. It is not difficult to see that the sequence $x_1, x_2, x_3, \dots$ is a Cauchy sequence in $K$, so $a = (x_1, x_2, x_3, \dots) + M \in \hat{K}$. Furthermore for every $i \in \mathbb{N}$ we have

$$\|a_i - a\| \leq \|a_i - h(x_i)\| + \|h(x_i) - a\| < 1/i + \lim_{j\to\infty} |x_i - x_j|.$$

Since $x_1, x_2, x_3, \dots$ is a Cauchy sequence, the right hand side of this inequality tends to 0 as $i \to \infty$. This shows that $\lim_{i\to\infty} a_i = a$ in $\hat{K}$. Thus $\hat{K}$ is complete. □

**Exercise 1.16.** Let $(K, |\ |)$ be a valued field with completion $(\hat{K}, \|\ \|)$. Show that $|\ |$ is non-archimedean if and only if $\|\ \|$ is non-archimedean.

**Exercise 1.17.** Formulate and prove a uniqueness statement for completions.

The previous exercise shows that completions are essentially unique. From now on we will talk about *the* completion $\hat{K}$ of $K$ and write $|\ |$ instead of $\|\ \|$ for the absolute value on $\hat{K}$.

The completion of $\mathbb{Q}$ with respect to the archimedean absolute value $|\ |_\infty$ (i.e. the usual absolute value) is canonically isomorphic to $\mathbb{R}$ (with its usual absolute value). The completion of $\mathbb{Q}$ with respect to the $p$-adic absolute value $|\ |_p$ (for some fixed prime number $p$) is denoted by $\mathbb{Q}_p$ and called the *field of $p$-adic numbers.* The absolute value on $\mathbb{Q}_p$ will again be denoted by $|\ |_p$ (or simply by $|\ |$ if $p$ is clear from the context).

1.5. **Archimedean absolute values.** For a proof of the following theorem see e.g. [Cassels, Chapter 3].

**Theorem 1.18.** *Let $L$ be a complete archimedean valued field. Then either $L \cong \mathbb{R}$ or $L \cong \mathbb{C}$ as topological fields.*

From this we can deduce a complete classification of archimedean valued fields. If $K$ is a field with an archimedean absolute value $|\ |$ and $\hat{K}$ its completion, then by the theorem either $\hat{K} \cong \mathbb{R}$ or $\hat{K} \cong \mathbb{C}$ as topological field. Therefore there exists an embedding $i : K \to \mathbb{C}$ such that the given absolute value $|\ |$ on $K$ and the absolute value $|\ |_{\mathbb{C}} \circ i$ which is induced by the embedding are equivalent (here $|\ |_{\mathbb{C}}$ denotes the usual absolute value on $\mathbb{C}$).

In the rest of this course we will only consider non-archimedean valued fields.

## 2. The fields $\mathbb{Q}_p$ and $\mathbb{C}_p$

In the first two sections of this chapter we sketch the construction of the complete and algebraically closed extension $\mathbb{C}_p$ of $\mathbb{Q}_p$. In the remaining sections we then develop some general properties of (complete) non-archimedean valued fields, with particular emphasis on the cases $\mathbb{Q}_p$ and $\mathbb{C}_p$.

2.1. **Algebraic extensions of a complete field.**

**Theorem 2.1.** *Let $(K, |\ |)$ be a complete non-archimedean valued field. Let $L$ be a finite field extension of $K$. Then there exists a unique absolute value on $L$ that extends the absolute value on $K$. Furthermore $L$ is complete with respect to this absolute value.*

*Idea of proof.* The proof is quite long and we will omit the details. Many books prove the result only under the additional assumption that $K$ is locally compact; a complete proof in the general case can be found for example in [Schikhof, §14 and 15] or [Cassels, Chapter 7]. The following are the main ideas of the proof.

Uniqueness: Let $\|\ \|_1$ and $\|\ \|_2$ be two absolute values on the field $L$ which extend the absolute value of $K$. If we consider $L$ as a vector space over $K$, then $\|\ \|_1$ and $\|\ \|_2$ become norms on the vector space $L$ (as defined in the next chapter). But $L$ is finite dimensional as a vector space over $K$, and any two norms on a finite dimensional vector space over a complete field are equivalent as norms, i.e. they induce the same topology on $L$. But then $\|\ \|_1$ and $\|\ \|_2$ are also equivalent as absolute values, hence there exists an $\alpha > 0$ such that $\|x\|_1 = \|x\|_2^\alpha$ for all $x \in L$. By choosing $x \in K^\times$ for which $|x| \neq 1$ we obtain $|x| = \|x\|_1 = \|x\|_2^\alpha = |x|^\alpha$, hence $\alpha = 1$, and thus $\|\ \|_1 = \|\ \|_2$. (The last step does not work if $|\ |$ is trivial, however in this case one can show that every extension of $|\ |$ to $L$ is trivial.)

Completeness: A finite dimensional normed vector space over a complete field is automatically complete.

Existence: Let $d$ be the degree of the extension $L/K$, and let $N_{L/K} : L \to K$ be the norm map of the field extension $L/K$. We define a function $\|\ \| : L \to \mathbb{R}_{\geq 0}$ by

$$\|x\| = \sqrt[d]{|N_{L/K}(x)|}.$$

From the standard properties of the norm it follows immediately that $\|x\| = |x|$ if $x \in K$, $\|x\| = 0$ if and only if $x = 0$, and that $\|xy\| = \|x\| \cdot \|y\|$. The most difficult step is to show that $\|x + y\| \leq \max\{\|x\|, \|y\|\}$. For a proof of this inequality see e.g. [Cassels, Chapter 7, §3]. (A completely different proof of the existence of the absolute value on $L$ can be found in [Schikhof, §14].) $\square$

**Corollary 2.2.** *Let $(K, |\ |)$ be a complete non-archimedean valued field. Let $K^{\mathrm{alg}}$ be an algebraic closure of $K$. Then there exists a unique absolute value on $K^{\mathrm{alg}}$ that extends the absolute value on $K$.*

*Proof.* This follows immediately from the previous theorem because $K^{\mathrm{alg}}$ is a union of finite field extensions of $K$. □

2.2. **The field $\mathbb{C}_p$.** We want to construct a complete and algebraically closed extension of $\mathbb{Q}_p$. First we consider an algebraic closure $\mathbb{Q}_p^{\mathrm{alg}}$ of $\mathbb{Q}_p$. In the previous section we have seen that the absolute value of $\mathbb{Q}_p$ can be extended uniquely to $\mathbb{Q}_p^{\mathrm{alg}}$. However one can show that $\mathbb{Q}_p^{\mathrm{alg}}$ is not complete (see e.g. [Robert, III.1.4]). We define $\mathbb{C}_p$ to be the completion of $\mathbb{Q}_p^{\mathrm{alg}}$. Then by definition $\mathbb{C}_p$ is a complete non-archimedean valued field. The next theorem shows that $\mathbb{C}_p$ is algebraically closed.

**Theorem 2.3.** *Let $K$ be a non-archimedean valued field and $\hat{K}$ its completion. If $K$ is algebraically closed then $\hat{K}$ is algebraically closed.*

*Idea of proof.* Let $f(X) \in \hat{K}[X]$ be a polynomial of degree $\geq 1$. We must show that $f(X)$ has a root in $\hat{K}$.

Now $K$ is dense in $\hat{K}$, therefore we can find a sequence of polynomials $f_1(X), f_2(X), f_3(X), \dots \in K[X]$ (all of the same degree as $f(X)$) that converges to $f(X)$, more precisely all coefficients of $f(X) - f_i(X)$ tend to 0 as $i \to \infty$.

Since $K$ is algebraically closed, each polynomial $f_i(X)$ has a root $\lambda_i \in K$. Using that $f_i(X) \to f(X)$ as $i \to \infty$ one can then show that $|f(\lambda_i)| \to 0$ as $i \to \infty$. From this it easily follows that $\lambda_1, \lambda_2, \dots$ has a subsequence that converges to a root $\xi$ of $f(X)$ in $\hat{K}^{\mathrm{alg}}$. But since all terms of this subsequence lie in $K \subseteq \hat{K}$ and $\hat{K}$ is complete, it follows that $\xi \in \hat{K}$.

For more details see [Schikhof, §17]. □

2.3. **Sequences and series.** Let $(K, |\ |)$ be a complete non-archimedean valued field. In this section we prove some basic properties of sequences and series in $K$.

**Lemma 2.4.** *Let $x, y \in K$. If $|x| \neq |y|$ then $|x + y| = \max\{|x|, |y|\}$.*

*Proof.* Without loss of generality we can assume that $|x| < |y|$. We will show that $|x + y| \leq \max\{|x|, |y|\}$ and $\max\{|x|, |y|\} \leq |x + y|$.

The inequality $|x + y| \leq \max\{|x|, |y|\}$ holds by definition. On the other hand we have

$$|y| = |x + y - x| \leq \max\{|x + y|, |-x|\} = \max\{|x + y|, |x|\},$$

but since $|y| \not\leq |x|$ it follows that $|y| \leq |x+y|$. Hence $\max\{|x|, |y|\} = |y| \leq |x+y|$. □

**Lemma 2.5.** *Let $a_1, a_2, a_3, \dots$ be a convergent sequence in $K$ and assume that $\lim_{i\to\infty} a_i \neq 0$. Then $|\lim_{i\to\infty} a_i| = |a_n|$ for all sufficiently large $n$.*

*Proof.* Let $a = \lim_{i\to\infty} a_i$. Since $a \neq 0$ by assumption, there exists an $N \in \mathbb{N}$ such that $|a_i - a| < |a|$ for all $i \geq N$. Using the previous lemma we find that $|a_i| = |(a_i - a) + a| = |a|$ for all $i \geq N$. □

Let $a_1, a_2, a_3, \dots \in K$. As usual we define $\sum_{i=1}^{\infty} a_i$ to be $\lim_{N\to\infty} \sum_{i=1}^{N} a_i$ if this limit exists.

**Lemma 2.6.** *Let $a_1, a_2, a_3, \dots \in K$. The series $\sum_{i=1}^{\infty} a_i$ converges in $K$ if and only if $\lim_{i\to\infty} a_i = 0$. In this case we have*

$$\left|\sum_{i=1}^{\infty} a_i\right| \leq \sup_{i\in\mathbb{N}} |a_i|.$$

*If moreover there exists an index $N \in \mathbb{N}$ such that $|a_N| > |a_i|$ for all $i \neq N$, then*

$$\left|\sum_{i=1}^{\infty} a_i\right| = \sup_{i\in\mathbb{N}}|a_i| = |a_N|.$$

*Proof.* It is clear that if the series converges then $\lim_{i\to\infty} a_i = 0$. Conversely assume that $\lim_{i\to\infty} a_i = 0$. Let $b_1, b_2, b_3, \dots$ be the sequence of partial sums, i.e. $b_n = \sum_{i=1}^n a_i$. Then for $i > j$ we have

$$|b_i - b_j| = |a_{j+1} + a_{j+2} + \cdots + a_i| \le \max\{|a_{j+1}|, |a_{j+2}|, \dots, |a_i|\}$$

which is arbitrarily small for sufficiently large $i, j$. Hence $b_1, b_2, b_3, \dots$ is a Cauchy sequence. Since $K$ is complete it follows that $\sum_{i=1}^{\infty} a_i = \lim_{n\to\infty} b_n$ exists.

Now assume that the series converges. Clearly we have

$$|b_n| \le \max\{|a_1|, \dots, |a_n|\} \le \sup_{i\in\mathbb{N}}|a_i|$$

for every $n \in \mathbb{N}$, hence $|\sum_{i=1}^{\infty} a_i| = |\lim_{n\to\infty} b_n| = \lim_{n\to\infty}|b_n| \le \sup_{i\in\mathbb{N}}|a_i|$.

Finally assume that $|a_N| > |a_i|$ for all $i \neq N$. Then by Lemma 2.4 we have $|b_i| = |a_N|$ for all $i \ge N$. Hence $|\sum_{i=1}^{\infty} a_i| = |\lim_{n\to\infty} b_n| = \lim_{n\to\infty}|b_n| = |a_N|$. $\square$

**Exercise 2.7.** Let $(K, |\ |)$ be a complete non-archimedean valued field. Let $a_1, a_2, a_3, \dots \in K$, and let $\sigma : \mathbb{N} \to \mathbb{N}$ be a bijective map. Show that

$$\sum_{i=1}^{\infty} a_i = \sum_{i=1}^{\infty} a_{\sigma(i)},$$

i.e. if the series on the left hand side converges then the series on the right hand side converges and has the same value.

**Exercise 2.8.** Let $p$ be a prime number. Compute $\sum_{i=1}^{\infty} i \cdot i!$ in $\mathbb{Q}_p$.

2.4. **The residue class field.** Let $(K, |\ |)$ be a non-archimedean valued field (not necessarily complete). Let $R = \{x \in K : |x| \le 1\}$ and $M = \{x \in K : |x| < 1\}$. Clearly there are inclusions $\{0\} \subseteq M \subset R \subseteq K$.

**Lemma 2.9.** *$R$ is a subring of $K$, and $M$ is the unique maximal ideal of $R$. The units $R^\times$ of $R$ are given by $R^\times = R \setminus M = \{x \in K : |x| = 1\}$.*

*Proof.* If $x, y \in R$ then $|-x| = |x| \le 1$, $|x + y| \le \max\{|x|, |y|\} \le 1$ and $|xy| = |x| \cdot |y| \le 1$, so $-x \in R$, $x + y \in R$ and $xy \in R$. Furthermore $|0| = 0 \le 1$ and $|1| = 1 \le 1$, so $0 \in R$ and $1 \in R$. Therefore $R$ is a subring of $K$.

Next we show that $M$ is an ideal of $R$. It is an additive subgroup because $0 \in M$ and $x, y \in M$ implies $-x \in M$ and $x + y \in M$ since $|-x| = |x| < 1$ and $|x + y| \le \max\{|x|, |y|\} < 1$ . Furthermore if $x \in R$ and $y \in M$ then $|xy| < 1$, so $xy \in M$.

Suppose that $x \in R$ is a unit. Then there exists $y \in R$ such that $xy = 1$. It follows that $|x| \cdot |y| = |xy| = |1| = 1$, hence $|x| = 1$ (since $|x| \le 1$ and $|y| \le 1$). Conversely suppose that $x \in K$ with $|x| = 1$. Then $x \in R$ and $x^{-1} \in R$ (since $|x^{-1}| = 1$), hence $x \in R^\times$. We have shown that $R^\times = \{x \in K : |x| = 1\}$. Clearly this set is equal to $R \setminus M$.

Finally, assume that $I$ is any proper ideal of $R$. Then $I$ cannot contain any units, so $I \cap R^\times = \emptyset$. Since $R^\times = R \setminus M$ this implies $I \subseteq M$. As $M \neq R$ this shows that $M$ is the unique maximal ideal of $R$. $\square$

The ring $R$ is called the *ring of integers of* $K$, and the quotient field $R/M$ is called the *residue class field* of $K$.

**Exercise 2.10.** Let $K$ be a non-archimedean valued field and $\hat{K}$ its completion. Let $R$ and $M$ be the ring of integers and maximal ideal of $K$, and let $\hat{R}$ and $\hat{M}$ be the ring of integers and maximal ideal of $\hat{K}$. Show that $R \subseteq \hat{R}$ and $M \subseteq \hat{M}$, and that the induced map of residue class fields $R/M \to \hat{R}/\hat{M}$ is an isomorphism.

**Lemma 2.11.** *Let $p$ be a prime number. For the valued field $(\mathbb{Q}, |\ |_p)$ we have $R = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\}$ and $M = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b, p \mid a\} = pR$. The inclusion $\mathbb{Z} \subset R$ induces an isomorphism $\mathbb{Z}/p\mathbb{Z} \cong R/M$.*

*Proof.* If $x = \pm p^e q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r} \in \mathbb{Q}^\times$ then $|x|_p = p^{-e} \leq 1$ if and only if $e \geq 0$, and $|x|_p = p^{-e} < 1$ if and only if $e > 0$. This immediately implies $R = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\}$ and $M = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b, p \mid a\}$, and from this description of $R$ and $M$ it easily follows that $M = pR$.

Clearly $\mathbb{Z} \subset R$ and $p\mathbb{Z} \subset pR = M$, so we obtain a natural homomorphism $f : \mathbb{Z}/p\mathbb{Z} \to R/M$, $f(a + p\mathbb{Z}) = a + M$ for $a \in \mathbb{Z}$. We claim that $f$ is bijective. It is easy to see that $M \cap \mathbb{Z} = p\mathbb{Z}$ which implies that $f$ is injective. To see that $f$ is surjective, let $\frac{a}{b} \in R$. Since $p \nmid b$ there exists $c \in \mathbb{Z}$ such that $bc \equiv a \pmod p$. It follows that $f(c + p\mathbb{Z}) = c + M = \frac{bc}{b} + M = \frac{a}{b} + M$. □

The ring of integers of $\mathbb{Q}_p$ is called the ring of $p$-adic integers and denoted by $\mathbb{Z}_p$, so $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x| \leq 1\}$. Clearly $\mathbb{Z} \subset \mathbb{Z}_p$.

**Corollary 2.12.** *The inclusion $\mathbb{Z} \subset \mathbb{Z}_p$ induces an isomorphism from $\mathbb{Z}/p\mathbb{Z}$ to the residue class field of $\mathbb{Q}_p$.*

*Proof.* This follows from Lemma 2.11 and Exercise 2.10. □

**Example 2.13.** One can show that the residue class field of $\mathbb{Q}_p^{\mathrm{alg}}$ (the algebraic closure of $\mathbb{Q}_p$) is the algebraic closure of the finite field $\mathbb{Z}/p\mathbb{Z}$ (see e.g. [Schikhof, §16]). Hence by Exercise 2.10 the residue class field of $\mathbb{C}_p$ is the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$.

2.5. **The value group.** Let $(K, |\ |)$ be a non-archimedean valued field (not necessarily complete). In this section we will assume that $|\ |$ is not the trivial absolute value. Note that the restriction of $|\ |$ to $K^\times$ is a homomorphism $K^\times \to \mathbb{R}_{>0}$. Let $\Gamma$ denote the image of this homomorphism, i.e. $\Gamma = \{|x| : x \in K^\times\}$. This is a (non-trivial) subgroup of the multiplicative group $\mathbb{R}_{>0}$ which is called the *value group* of $K$ (or of $|\ |$).

**Definition 2.14.** An absolute value $|\ | : K \to \mathbb{R}_{\geq 0}$ is called *discrete* if its value group is a discrete subgroup of $\mathbb{R}_{>0}$.

**Remark 2.15.** Let $\Gamma$ be a non-trivial discrete subgroup of $\mathbb{R}_{>0}$. We claim that then there exists a unique $\gamma \in \Gamma$ with $0 < \gamma < 1$ such that $\Gamma = \gamma^{\mathbb{Z}}$. To see this note that the logarithm is an isomorphism $\log : \mathbb{R}_{>0} \to \mathbb{R}$. Under this isomorphism $\Gamma$ is mapped to a discrete subgroup of $\mathbb{R}$. Hence $\log(\Gamma) = \mathbb{Z} \cdot \delta$ for a unique $\delta \in \log(\Gamma)$ with $\delta < 0$, and it follows that $\Gamma = \gamma^{\mathbb{Z}}$ with $\gamma = \exp(\delta)$.

**Lemma 2.16.** *Let $R = \{x \in K : |x| \leq 1\}$ and $M = \{x \in K : |x| < 1\}$. The following are equivalent.*

1. *The absolute value $|\ |$ is discrete.*
2. *The ideal $M$ is principal.*
3. *The ring $R$ is a principal ideal domain.*
4. *The ideal $M$ is finitely generated.*
5. *The ring $R$ is noetherian.*

*Proof.* The implications (3)⇒(2)⇒(4) and (3)⇒(5)⇒(4) are clear. It therefore suffices to show (1)⇒(3) and (4)⇒(1).

(1)⇒(3): We assume that $|\ |$ is non-trivial and discrete, so its value group $\Gamma$ is a non-trivial discrete subgroup of $\mathbb{R}_{>0}$. Let $I \neq \{0\}$ be an ideal of $R$. Choose an element $a \in I$ with maximal absolute value $|a|$ (the existence of such an $a$ follows easily from the description of $\Gamma$ in Remark 2.15). We claim that $I$ is equal to the principal ideal generated by $a$. The inclusion $(a) \subseteq I$ is obvious. Conversely, let $x \in I$. Then $|x/a| = |x|/|a| \leq 1$ by the choice of $a$, so $x/a \in R$. Hence $x = x/a \cdot a \in (a)$ as required.

(4)⇒(1): exercise □

**Exercise 2.17.** Prove the implication (4)⇒(1).

**Exercise 2.18.** Let $K$ be a non-archimedean valued field and $\hat{K}$ its completion. Show that $K$ and $\hat{K}$ have the same value groups.

**Example 2.19.** By definition of the $p$-adic absolute value $|\ |_p$ on $\mathbb{Q}$ it is clear that its value group is $p^{\mathbb{Z}}$. By the previous exercise $\mathbb{Q}_p$ has the same value group, so in particular it is a discrete absolute value. It easily follows from the proof of the implication (1)⇒(3) in Lemma 2.16 that the maximal ideal of the ring of $p$-adic integers $\mathbb{Z}_p$ is generated by any element with absolute value $p^{-1}$, e.g. by the element $p \in \mathbb{Z} \subset \mathbb{Z}_p$.

**Example 2.20.** One can show that the value group of $\mathbb{C}_p$ is $p^{\mathbb{Q}}$ (see e.g. [Schikhof, §16]), so the absolute value on $\mathbb{C}_p$ is not discrete.

2.6. **The ring $\mathbb{Z}_p$.** Recall that $\mathbb{Z}_p$ denotes the ring of $p$-adic integers, so $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x| \leq 1\}$. The following lemma summarises some results about $\mathbb{Z}_p$ which we have shown in the previous two sections.

**Lemma 2.21.** *The ring $\mathbb{Z}_p$ is a principal ideal domain, $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$, and the inclusion $\mathbb{Z} \subset \mathbb{Z}_p$ induces an isomorphism from $\mathbb{Z}/p\mathbb{Z}$ to the residue class field $\mathbb{Z}_p/p\mathbb{Z}_p$.*

We will now give a more concrete description of the elements of $\mathbb{Z}_p$.

**Theorem 2.22.** *Every $x \in \mathbb{Z}_p$ can be written uniquely in the form*

$$x = a_0 + a_1 p + a_2 p^2 + \cdots = \sum_{i=0}^{\infty} a_i p^i$$

*with $a_i \in \{0, 1, \ldots, p-1\}$.*

*Proof.* Let $x \in \mathbb{Z}_p$. Then $x + p\mathbb{Z}_p \in \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$, hence there exists a unique $a_0 \in \{0, 1, \ldots, p-1\}$ such that $x + p\mathbb{Z}_p = a_0 + p\mathbb{Z}_p$. It follows that $x - a_0 \in p\mathbb{Z}_p$, so $x - a_0 = x_1 p$ for some $x_1 \in \mathbb{Z}_p$. Similarly we can find $a_1 \in \{0, 1, \ldots, p-1\}$ and $x_2 \in \mathbb{Z}_p$ such that $x_1 - a_1 = x_2 p$. Continuing like this gives sequences $a_0, a_1, a_2, \cdots \in \{0, 1, \ldots, p-1\}$ and $x_1, x_2, x_3, \cdots \in \mathbb{Z}_p$ such that

$$x = a_0 + x_1 p = a_0 + a_1 p + x_2 p^2 = \cdots = a_0 + a_1 p + \cdots + a_n p^n + x_{n+1} p^{n+1} = \ldots.$$

This implies

$$\left| x - \sum_{i=0}^{n} a_n p^n \right| = |x_{n+1} p^{n+1}| \leq p^{-n-1},$$

hence $x = \sum_{i=0}^{\infty} a_i p^i$.

To see the uniqueness, assume that $x = \sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{\infty} b_i p^i$ with $a_i, b_i \in \{0, 1, \ldots, p-1\}$. Then $x + p\mathbb{Z}_p = a_0 + p\mathbb{Z}_p = b_0 + p\mathbb{Z}_p \in \mathbb{Z}_p/p\mathbb{Z}_p$. Using the isomorphism $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p/p\mathbb{Z}_p$ this gives $a_0 + p\mathbb{Z} = b_0 + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$, hence $a_0 = b_0$. It follows that $\sum_{i=1}^{\infty} a_i p^{i-1} = \sum_{i=1}^{\infty} b_i p^{i-1}$, which implies that $a_1 = b_1$, etc. □

**Exercise 2.23.** Find $a_0, a_1, a_2, \cdots \in \{0, 1, \ldots, p-1\}$ such that $-1 = a_0 + a_1 p + a_2 p^2 + \ldots$ in $\mathbb{Z}_p$.

**Lemma 2.24.** *$\mathbb{Z}_{\geq 0}$ is dense in $\mathbb{Z}_p$.*

*Proof.* Let $x \in \mathbb{Z}_p$ and $\varepsilon > 0$. We must show that there exists an $n \in \mathbb{Z}_{\geq 0}$ such that $|x - n| < \varepsilon$. Write $x = a_0 + a_1 p + a_2 p^2 + \dots$ as in Theorem 2.22. Choose $i \in \mathbb{Z}_{\geq 0}$ such that $p^{-i-1} < \varepsilon$. Let $n = a_0 + a_1 p + \dots + a_i p^i \in \mathbb{Z}_{\geq 0}$. Then $|x - n| = |a_{i+1} p^{i+1} + a_{i+2} p^{i+2} + \dots| = |p^{i+1}| \cdot |a_{i+1} + a_{i+2} p + \dots| \leq p^{-i-1} < \varepsilon$. □

**Exercise 2.25.** Show that $\mathbb{Z}_p$ is compact. (Hint: Since $\mathbb{Z}_p$ is a metric space, compactness is equivalent to sequential compactness. Use Theorem 2.22 to show that every sequence in $\mathbb{Z}_p$ has a convergent subsequence.)

2.7. **Topology of $\mathbb{Q}_p$ and $\mathbb{C}_p$.** We discuss some topological properties of non-archimedean valued fields in general and of the fields $\mathbb{Q}_p$ and $\mathbb{C}_p$ in particular.

Let $(K, |\ |)$ be a non-archimedean valued field (not necessarily complete). Recall that in §1.2 we defined open and closed balls in $K$. However in the case of a non-archimedean valued field this terminology can be misleading.

**Lemma 2.26.** *Let $x \in K$ and $\varepsilon > 0$.*

(1) *The set $B_{<\varepsilon}(x)$ is open and closed in $K$.*
(2) *The set $B_{\leq\varepsilon}(x)$ is open and closed in $K$.*
(3) *The sphere $\{y \in K : |y - x| = \varepsilon\}$ is open and closed in $K$.*

*Proof.* It is clear that $B_{<\varepsilon}(x)$ is open. Let $y \in K \setminus B_{<\varepsilon}(x)$. Then $B_{<\varepsilon}(y) \subset K \setminus B_{<\varepsilon}(x)$ because $z \in B_{<\varepsilon}(x) \cap B_{<\varepsilon}(y)$ would imply $|x-y| \leq \max\{|x-z|, |z-y|\} < \epsilon$. This shows that $K \setminus B_{<\varepsilon}(x)$ is open, i.e. $B_{<\varepsilon}(x)$ is closed. This proves statement (1). The proof of (2) is similar, and (3) follows immediately from (1) and (2) because $\{y \in K : |y - x| = \varepsilon\} = B_{\leq\varepsilon}(x) \setminus B_{<\varepsilon}(x)$. □

**Corollary 2.27.** *The topological space $K$ is totally disconnected.*

**Exercise 2.28.** Let $B = B_{<\varepsilon}(x)$ be an open ball in $K$. Show that every point in $B$ is a centre of $B$, i.e. $B = B_{<\varepsilon}(y)$ for all $y \in B$. Similarly for closed balls.

It follows from Exercise 2.25 that $\mathbb{Q}_p$ is locally compact, because $x + \mathbb{Z}_p$ is a compact neighbourhood of $x \in \mathbb{Q}_p$. More generally one has the following theorem (for a proof see e.g. [Cassels, Chapter 4, §1]).

**Theorem 2.29.** *Let $(K, |\ |)$ be a non-archimedean valued field. Then $K$ is locally compact if and only if $K$ is complete, the residue class field of $K$ is finite, and the absolute value $|\ |$ is discrete.*

Recall that a topological space is called separable if it contains a countable dense subset.

**Theorem 2.30.** *The spaces $\mathbb{Q}_p$ and $\mathbb{C}_p$ are separable.*

*Proof.* $\mathbb{Q}_p$ is separable because it contains $\mathbb{Q}$ as a countable dense subset.

To show that $\mathbb{C}_p$ is separable, one first shows that the countable set $\mathbb{Q}^{\mathrm{alg}}$ is dense in $\mathbb{Q}_p^{\mathrm{alg}}$ and that therefore $\mathbb{Q}_p^{\mathrm{alg}}$ is separable (see e.g. [Robert, III.1.5]). Since $\mathbb{Q}_p^{\mathrm{alg}}$ is dense in $\mathbb{C}_p$ it follows that $\mathbb{C}_p$ is separable. □

## 3. Normed spaces

Throughout this chapter we assume that $(K, |\ |)$ is a complete non-archimedean valued field and that $|\ |$ is non-trivial. We define normed spaces and Banach spaces over $K$, develop some of the basic properties of such spaces and of continuous linear maps between such spaces, and discuss some standard examples.

3.1. **Basic definitions.**

**Definition 3.1.** Let $V$ be a vector space over $K$ and let $\| \ \| : V \to \mathbb{R}_{\geq 0}$ be a function satisfying

(1) $\|x\| = 0$ if and only if $x = 0$
(2) $\|\lambda x\| = |\lambda| \cdot \|x\|$ for all $\lambda \in K$, $x \in V$
(3) $\|x + y\| \leq \max\{\|x\|, \|y\|\}$ for all $x, y \in V$

Then $\| \ \|$ is called a *norm* on $V$, and the pair $(V, \| \ \|)$ is called a *normed space* over $K$.

A normed space $(V, \| \ \|)$ has a natural induced metric which is given by $V \times V \to \mathbb{R}_{\geq 0}, (x, y) \mapsto \|x - y\|$.

**Definition 3.2.** A normed space $(V, \| \ \|)$ is called a *Banach space* if $V$ is complete with respect to the induced metric.

**Exercise 3.3.** Let $(V, \| \ \|_V)$ and $(W, \| \ \|_W)$ be normed spaces over $K$. For $(v, w) \in V \oplus W$ define $\|(v, w)\| = \max\{\|v\|_V, \|w\|_W\}$. Show that $\| \ \|$ is a norm on $V \oplus W$, and that (with respect to this norm) $V \oplus W$ is a Banach space if and only if both $V$ and $W$ are Banach spaces.

**Example 3.4.** If we consider $K$ as a vector space over itself then the absolute value $| \ |$ becomes a norm, and by assumption $K$ is complete with respect to this norm. Thus $K$ is a 1-dimensional Banach space over $K$. The construction from the previous exercise then gives the Banach space $K^2 = K \oplus K$ with the norm $\|(x_1, x_2)\| = \max\{|x_1|, |x_2|\}$. More generally, for every $n \in \mathbb{N}$ we obtain the Banach space $K^n$ with the norm $\|(x_1, \ldots, x_n)\| = \max\{|x_1|, \ldots, |x_n|\}$.

**Definition 3.5.** Let $V$ be a vector space over $K$. Two norms $\| \ \|_1$ and $\| \ \|_2$ on $V$ are called *equivalent* if they induce the same topology on $V$.

**Lemma 3.6.** *Two norms $\| \ \|_1$ and $\| \ \|_2$ on a vector space $V$ are equivalent if and only if there exist constants $c, d \in \mathbb{R}_{>0}$ such that $c\|v\|_1 \leq \|v\|_2 \leq d\|v\|_1$ for all $v \in V$.*

*Proof.* Let $T : V \to V$ be the identity map, considered as a map from $(V, \| \ \|_1)$ to $(V, \| \ \|_2)$. If the two norms are equivalent then $T$ is continuous, hence bounded by Lemma 3.11, so there exists $d \in \mathbb{R}_{>0}$ such that $\|v\|_2 \leq d\|v\|_1$ for all $v \in V$. By considering the inverse of $T$ we obtain $c \in \mathbb{R}_{>0}$ such that $c\|v\|_1 \leq \|v\|_2$.

Conversely, if there exist $c, d \in \mathbb{R}_{>0}$ such that $c\|v\|_1 \leq \|v\|_2 \leq d\|v\|_1$ for all $v \in V$, then it is easy to see that every open ball with respect to $\| \ \|_1$ contains an open ball with respect to $\| \ \|_2$, and that every open ball with respect to $\| \ \|_2$ contains an open ball with respect to $\| \ \|_1$. Hence we obtain the same induced topology, i.e. $\| \ \|_1$ and $\| \ \|_2$ are equivalent. $\square$

For a proof of the following theorem see e.g. [Schikhof, §13].

**Theorem 3.7.** *Let $V$ be a finite dimensional vector space over $K$. Then all norms on $V$ are equivalent, and $V$ is complete with respect to each norm.*

3.2. **Bounded linear maps.** Let $V$ and $W$ be normed spaces over $K$. We will denote the norm on each of these spaces by $\| \ \|$; it will always be clear from the context which norm is meant.

**Definition 3.8.** Let $T : V \to W$ be a linear map. We call $T$ *bounded* if there exists a constant $c \in \mathbb{R}_{\geq 0}$ such that $\|Tv\| \leq c\|v\|$ for all $v \in V$. If $T$ is bounded then the *norm* of $T$ is defined by

$$\|T\| = \inf\{c \in \mathbb{R}_{\geq 0} : \|Tv\| \leq c\|v\| \text{ for all } v \in V\}.$$

**Exercise 3.9.** Let $T : V \to W$ be a bounded linear map.

(1) Show that if $V \neq \{0\}$ then

$$\|T\| = \sup\left\{\frac{\|Tv\|}{\|v\|} : v \in V \setminus \{0\}\right\}.$$

(2) Show that if the absolute value $|\ |$ on $K$ is not discrete (and hence $|K^\times|$ is dense in $\mathbb{R}_{>0}$) then

$$\|T\| = \sup\{\|Tv\| : \|v\| \leq 1\}.$$

It follows immediately from Exercise 3.9(1) (or directly from the definition) that $\|Tv\| \leq \|T\| \cdot \|v\|$ for all $v \in V$.

**Exercise 3.10.** Let $T : V \to W$ and $S : U \to V$ be bounded linear maps. Show that $T \circ S : U \to W$ is bounded and $\|T \circ S\| \leq \|T\| \cdot \|S\|$.

**Lemma 3.11.** *A linear map $T : V \to W$ is continuous if and only if it is bounded.*

*Proof.* If $T$ is continuous then it is continuous at $0 \in V$. Therefore there exists a $\delta > 0$ such that $\|Tv\| < 1$ whenever $\|v\| < \delta$. Fix any $\lambda \in K$ with $0 < |\lambda| < 1$. Now if $v \in V \setminus \{0\}$ then there exists a (unique) $n \in \mathbb{Z}$ such that $\delta|\lambda|^{n+1} \leq \|v\| < \delta|\lambda|^n$. Then $\|v/\lambda^n\| < \delta$ and hence $\|T(v/\lambda^n)\| < 1$. It follows that

$$\|Tv\| = \|\lambda^n T(v/\lambda^n)\| < |\lambda|^n \leq \frac{1}{\delta|\lambda|}\|v\|.$$

Thus if we take $c = (\delta|\lambda|)^{-1}$ then $\|Tv\| \leq c\|v\|$ for all $v \in V$, i.e. $T$ is bounded.

Conversely assume that $T$ is bounded, i.e. there exists a $c > 0$ such that $\|Tv\| \leq c\|v\|$ for all $v \in V$. If $\varepsilon > 0$ then

$$\|Tv - Tw\| = \|T(v - w)\| \leq c\|v - w\| < \varepsilon$$

for all $v, w \in V$ with $\|v - w\| < \varepsilon/c$. This shows that $T$ is continuous. □

We write $L(V, W)$ for the set of all bounded linear maps $V \to W$. Clearly this is a vector space over $K$.

**Lemma 3.12.** *The function $\|\ \| : L(V, W) \to \mathbb{R}_{\geq 0}$ is a norm on $L(V, W)$. If $W$ is complete then $L(V, W)$ is a Banach space.*

*Proof.* It is straightforward to verify that $\|\ \|$ is a norm on $L(V, W)$.

Now assume that $W$ is complete. Let $T_1, T_2, T_3, \dots$ be a Cauchy sequence in $L(V, W)$. For every $v \in V$ we have $\|T_n v - T_m v\| \leq \|T_n - T_m\| \cdot \|v\|$, hence the sequence $T_1 v, T_2 v, T_3 v, \dots$ is a Cauchy sequence in $W$ and therefore has a limit $Tv$. This defines a map $T : V \to W$. It is easy to see that $T$ is linear. Now let $\varepsilon > 0$ and choose $N \in \mathbb{N}$ such that $\|T_n - T_m\| < \varepsilon$ for all $m, n \geq N$. Then for every $m \geq N$ and every $v \in V$ we obtain (by choosing a sufficiently large $n$)

$$\begin{aligned}\|Tv - T_m v\| &\leq \max\{\|Tv - T_n v\|, \|T_n v - T_m v\|\} \\ &\leq \max\{\|Tv - T_n v\|, \|T_n - T_m\| \cdot \|v\|\} \\ &\leq \varepsilon\|v\|.\end{aligned}$$

This proves that $T - T_m$ is bounded, hence $T$ is bounded. Furthermore $\|T - T_m\| \leq \varepsilon$ for all $m \geq N$, hence $T_m \to T$ as $m \to \infty$. □

If $V$ is a normed space we define its *topological dual* $V'$ to be $V' = L(V, K)$. The previous lemma shows that $V'$ is always a Banach space.

3.3. **Examples.**

**Example 3.13.** Let $l^\infty(K)$ be the space of bounded sequences in $K$, i.e.

$$l^\infty(K) = \{(x_i)_{i\in\mathbb{N}} \in K^{\mathbb{N}} : \text{there exists a } c \in \mathbb{R}_{\geq 0} \text{ such that } |x_i| \leq c \text{ for all } i \in \mathbb{N}\}.$$

This is a vector space over $K$. We define a function $\| \ \| : l^\infty(K) \to \mathbb{R}_{\geq 0}$ by

$$\|(x_i)_{i\in\mathbb{N}}\| = \sup_{i\in\mathbb{N}} |x_i|.$$

We claim that $(l^\infty(K), \| \ \|)$ is a Banach space.

It is easy to check that $\| \ \|$ is a norm on $l^\infty(K)$. Let $x^{(1)}, x^{(2)}, x^{(3)}, \ldots$ be a Cauchy sequence in $l^\infty(K)$. We write $x^{(m)} = (x_i^{(m)})_{i\in\mathbb{N}}$. Then for every $i \in \mathbb{N}$ we have $|x_i^{(m)} - x_i^{(n)}| \leq \sup_{j\in\mathbb{N}} |x_j^{(m)} - x_j^{(n)}| = \|x^{(m)} - x^{(n)}\|$, hence $x_i^{(1)}, x_i^{(2)}, x_i^{(3)}, \ldots$ is a Cauchy sequence in $K$, and we can define $y_i = \lim_{m\to\infty} x_i^{(m)} \in K$ and $y = (y_i)_{i\in\mathbb{N}} \in K^{\mathbb{N}}$. Now let $\varepsilon > 0$ and choose $N \in \mathbb{N}$ such that $\|x^{(n)} - x^{(m)}\| < \varepsilon$ for all $n, m \geq N$. Then for every $m \geq N$ and every $i \in \mathbb{N}$ we obtain (by choosing a sufficiently large $n$)

$$|y_i - x_i^{(m)}| \leq \max\{|y_i - x_i^{(n)}|, |x_i^{(n)} - x_i^{(m)}|\} \leq \max\{|y_i - x_i^{(n)}|, \|x^{(n)} - x^{(m)}\|\} < \varepsilon.$$

Hence $|y_i| \leq \max\{|y_i - x_i^{(m)}|, |x_i^{(m)}|\} \leq \max\{\varepsilon, \|x^{(m)}\|\}$, so the sequence $y = (y_i)_{i\in\mathbb{N}}$ is bounded. Furthermore $\|y - x^{(m)}\| \leq \varepsilon$ for all $m \geq N$, hence $x^{(m)} \to y$ as $m \to \infty$. This shows that every Cauchy sequence in $l^\infty(K)$ has a limit, i.e. $l^\infty(K)$ is complete.

**Example 3.14.** We define $c_0(K)$ to be the complete subspace of $l^\infty(K)$ consisting of the sequences in $K$ that converge to 0, i.e.

$$c_0(K) = \{(x_i)_{i\in\mathbb{N}} \in K^{\mathbb{N}} : \lim_{i\to\infty} x_i = 0\} \subset l^\infty(K).$$

To see the completeness, we only need to show that if $x^{(1)}, x^{(2)}, x^{(3)}, \ldots$ is a sequence in $c_0(K)$ that converges to $y \in l^\infty(K)$, then $y \in c_0(K)$. Let $\varepsilon > 0$ and choose $N \in \mathbb{N}$ such that $\|y - x^{(N)}\| < \varepsilon$. Let $I \in \mathbb{N}$ be such that $|x_i^{(N)}| < \varepsilon$ for all $i \geq I$. Then for all $i \geq I$ we have $|y_i| \leq \max\{|y_i - x_i^{(N)}|, |x_i^{(N)}|\} < \varepsilon$, so $\lim_{i\to\infty} y_i = 0$ as required.

**Definition 3.15.** Two normed spaces $V$ and $W$ are called *isometrically isomorphic* if there exists a bijective linear map $T : V \to W$ such that $\|Tv\| = \|v\|$ for all $v \in V$.

**Exercise 3.16.** Show that the topological dual of $c_0(K)$ is isometrically isomorphic to $l^\infty(K)$.

**Exercise 3.17.** Let $X$ be a non-empty compact topological space and $C(X, K)$ the set of all continuous functions $X \to K$. Note that since $X$ is compact every continuous function $f : X \to K$ is bounded so that we can define $\|f\| = \sup_{x\in X} |f(x)| \in \mathbb{R}_{\geq 0}$. Show that $(C(X, K), \| \ \|)$ is a Banach space over $K$.

## 4. Continuous functions on $\mathbb{Z}_p$

Let $p$ be a prime number and let $(K, | \ |)$ be a complete extension of $(\mathbb{Q}_p, | \ |)$ (e.g. $K = \mathbb{Q}_p$ or $K = \mathbb{C}_p$). In this chapter we first discuss the Mahler expansion of continuous functions $\mathbb{Z}_p \to K$. As specific examples of such continuous functions we then consider the function $x \mapsto a^x$ and the $p$-adic gamma function $\Gamma_p$.

4.1. **Mahler expansion: statement of main result.** Recall that $C(\mathbb{Z}_p, K)$ denotes the $K$-Banach space of continuous functions $\mathbb{Z}_p \to K$ with the supremum norm (cf. Exercise 3.17). For an integer $n \in \mathbb{Z}_{\geq 0}$ we define $\binom{x}{n}$ by

$$\binom{x}{n} = \begin{cases} 1 & \text{if } n = 0 \\ \frac{x(x-1)\cdots(x-n+1)}{n!} & \text{if } n \geq 1. \end{cases}$$

Clearly $x \mapsto \binom{x}{n}$ is a continuous function $\mathbb{Z}_p \to \mathbb{Q}_p \subseteq K$. In the following we write $\binom{\cdot}{n}$ for this function considered as an element of $C(\mathbb{Z}_p, K)$.

For a continuous function $f : \mathbb{Z}_p \to K$ we define a new function $\Delta f : \mathbb{Z}_p \to K$ by

$$(\Delta f)(x) = f(x+1) - f(x).$$

Clearly $\Delta f$ is continuous and the map $\Delta : C(\mathbb{Z}_p, K) \to C(\mathbb{Z}_p, K)$ is linear. We call $\Delta$ the *difference operator* on $C(\mathbb{Z}_p, K)$. We let $\Delta^0 = \mathrm{id} : C(\mathbb{Z}_p, K) \to C(\mathbb{Z}_p, K)$ and define $\Delta^n = \Delta \circ \Delta^{n-1}$ for $n \in \mathbb{N}$.

**Exercise 4.1.** What is the kernel of $\Delta : C(\mathbb{Z}_p, K) \to C(\mathbb{Z}_p, K)$?

Recall that $c_0(K)$ denotes the $K$-Banach space of sequences in $K$ that converge to 0 with the supremum norm (cf. Example 3.14). In this section it will be convenient to index all sequences by $\mathbb{Z}_{\geq 0}$ instead of $\mathbb{N}$.

**Theorem 4.2** (Mahler)**.** *The map*

$$(a_n)_{n \geq 0} \mapsto \sum_{n=0}^{\infty} a_n \binom{\cdot}{n}$$

*is an isometric isomorphism of Banach spaces $c_0(K) \to C(\mathbb{Z}_p, K)$. The inverse of this map is given by*

$$f \mapsto \big((\Delta^n f)(0)\big)_{n \geq 0}.$$

So in particular every continuous function $f : \mathbb{Z}_p \to K$ can be written as $f = \sum_{n=0}^{\infty} a_n \binom{\cdot}{n}$ for unique $a_0, a_1, a_2, \dots \in K$ with $\lim_{n\to\infty} a_n = 0$. We call $\sum_{n=0}^{\infty} a_n \binom{\cdot}{n}$ the *Mahler expansion* of $f$ and $a_0, a_1, a_2, \dots$ the *Mahler coefficients*.

4.2. **Mahler expansion: proof.** We first show some preliminary results on binomial coefficients and on the difference operator $\Delta$.

**Lemma 4.3.** *Let $n \geq 0$. Then $\|\binom{\cdot}{n}\| = 1$.*

*Proof.* This is obvious for $n = 0$, so assume that $n \geq 1$. We have $|\binom{n}{n}| = |1| = 1$, hence $\|\binom{\cdot}{n}\| \geq 1$. If $x \in \mathbb{Z}_{\geq 0}$ then $\binom{x}{n}$ is an integer (because if $0 \leq x \leq n-1$ then $\binom{x}{n} = 0$, and if $x \geq n$ then $\binom{x}{n}$ is the usual binomial coefficient "$x$ choose $n$"). Hence $|\binom{x}{n}| \leq 1$ for all $x \in \mathbb{Z}_{\geq 0}$. But since $\mathbb{Z}_{\geq 0}$ is dense in $\mathbb{Z}_p$, it follows that $|\binom{x}{n}| \leq 1$ for all $x \in \mathbb{Z}_p$, i.e. $\|\binom{\cdot}{n}\| \leq 1$. □

**Lemma 4.4.** (1) *Let $n \geq 0$. Then*

$$\Delta \binom{\cdot}{n} = \begin{cases} 0 & \text{if } n = 0 \\ \binom{\cdot}{n-1} & \text{if } n \geq 1. \end{cases}$$

(2) *Let $f \in C(\mathbb{Z}_p, K)$ and $n \geq 0$. Then*

$$(\Delta^n f)(x) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(x+k).$$

*Proof.* The first statement follows by a direct computation: if $n \geq 1$ then

$$\begin{aligned} \left(\Delta \binom{\cdot}{n}\right)(x) &= \binom{x+1}{n} - \binom{x}{n} \\ &= \frac{(x+1)x\cdots(x-n+2)}{n!} - \frac{x(x-1)\cdots(x-n+1)}{n!} \\ &= \big((x+1)-(x-n+1)\big) \cdot \frac{x(x-1)\cdots(x-n+2)}{n\cdot(n-1)!} \\ &= \binom{x}{n-1}. \end{aligned}$$

The second statement follows by induction on $n$. If $n=0$ then both sides of the equation are equal to $f(x)$. If $n \geq 1$, then

$$\begin{aligned}
(\Delta^n f)(x) &= (\Delta(\Delta^{n-1}f))(x) = (\Delta^{n-1}f)(x+1) - (\Delta^{n-1}f)(x) \\
&= \sum_{k=0}^{n-1}(-1)^{n-1-k}\binom{n-1}{k}f(x+1+k) - \sum_{k=0}^{n-1}(-1)^{n-1-k}\binom{n-1}{k}f(x+k) \\
&= (-1)^0 f(x+n) + \sum_{k=1}^{n-1}(-1)^{n-k}\left(\binom{n-1}{k-1}+\binom{n-1}{k}\right)f(x+k) \\
&\qquad + (-1)^n f(x) \\
&= \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(x+k)
\end{aligned}$$

as required. □

**Lemma 4.5.** *The difference operator $\Delta : C(\mathbb{Z}_p, K) \to C(\mathbb{Z}_p, K)$ has the following properties.*

1. *For all $f \in C(\mathbb{Z}_p, K)$ we have $\|\Delta f\| \leq \|f\|$. In particular, the map $\Delta : C(\mathbb{Z}_p, K) \to C(\mathbb{Z}_p, K)$ is bounded and hence continuous.*
2. *Let $f \in C(\mathbb{Z}_p, K)$. Then there exists an $n \in \mathbb{N}$ (depending on $f$) such that $\|\Delta^n f\| \leq p^{-1}\|f\|$.*

*Proof.* The first statement is clear because

$$|(\Delta f)(x)| = |f(x+1) - f(x)| \leq \max\{|f(x+1)|, |f(x)|\} \leq \|f\|$$

for all $x \in \mathbb{Z}_p$. To prove the second statement, we first note that $f$ is uniformly continuous because $f$ is continuous on the compact space $\mathbb{Z}_p$. Hence there exists a $t \in \mathbb{N}$ such that $|f(x) - f(y)| \leq p^{-1}\|f\|$ whenever $|x-y| \leq p^{-t}$. Then for any $x \in \mathbb{Z}_p$ we have

$$\begin{aligned}
(\Delta^{p^t} f)(x) &= \sum_{k=0}^{p^t}(-1)^{p^t-k}\binom{p^t}{k}f(x+k) \\
&= f(x+p^t) + (-1)^{p^t}f(x) + \sum_{k=1}^{p^t-1}(-1)^{p^t-k}\binom{p^t}{k}f(x+k).
\end{aligned}$$

Now

$$\left|f(x+p^t) + (-1)^{p^t}f(x)\right| \leq p^{-1}\|f\|$$

because if $p$ is odd then $|f(x+p^t)+(-1)^{p^t}f(x)| = |f(x+p^t)-f(x)| \leq p^{-1}\|f\|$ by the choice of $t$, and if $p=2$ then $|f(x+p^t)+(-1)^{p^t}f(x)| = |f(x+p^t)-f(x)+2f(x)| \leq \max\{|f(x+p^t)-f(x)|, |2f(x)|\} \leq p^{-1}\|f\|$ by the choice of $t$ and since $|2| = 2^{-1}$. Furthermore for $1 \leq k \leq p^t - 1$ we have $p \mid \binom{p^t}{k}$ and hence

$$\left|(-1)^{p^t-k}\binom{p^t}{k}f(x+k)\right| \leq p^{-1}\|f\|.$$

Thus we obtain $|(\Delta^{p^t}f)(x)| \leq p^{-1}\|f\|$ for all $x \in \mathbb{Z}_p$. Hence $\|\Delta^n f\| \leq p^{-1}\|f\|$ where $n = p^t$. □

*Proof of Theorem 4.2.* Let $F : c_0(K) \to C(\mathbb{Z}_p, K)$, $(a_n)_{n\geq 0} \mapsto \sum_{n=0}^{\infty} a_n\binom{\cdot}{n}$, and $G : C(\mathbb{Z}_p, K) \to c_0(K)$, $f \mapsto \big((\Delta^n f)(0)\big)_{n\geq 0}$, be the two maps from the statement of the theorem.

*Claim 1:* The map $F$ is well defined and linear. Furthermore $\|Fa\| \leq \|a\|$ for all $a \in c_0(K)$.

Let $a = (a_n)_{n\geq 0} \in c_0(K)$. Then $\|a_n\binom{\cdot}{n}\| = |a_n| \to 0$ as $n \to \infty$, hence the series $\sum_{n=0}^{\infty} a_n\binom{\cdot}{n}$ converges in $C(\mathbb{Z}_p, K)$. This shows that the map $F$ is well defined, and clearly it is linear. Furthermore

$$\begin{aligned}\|Fa\| &= \left\|\sum_{n=0}^{\infty} a_n \binom{\cdot}{n}\right\| \\ &\leq \sup\left\{\left\|a_n\binom{\cdot}{n}\right\| : n \geq 0\right\} = \sup\{|a_n| : n \geq 0\} = \|a\|.\end{aligned}$$

*Claim 2:* The map $G$ is well defined and linear. Furthermore $\|Gf\| \leq \|f\|$ for all $f \in C(\mathbb{Z}_p, K)$.

Let $f \in C(\mathbb{Z}_p, K)$ and let $a_n = (\Delta^n f)(0)$ for $n \geq 0$. By Lemma 4.5(2) applied to $f$ there exists $n_1 \in \mathbb{N}$ such that $\|\Delta^{n_1} f\| \leq p^{-1}\|f\|$. Then for all $n \geq n_1$ we have

$$|a_n| = |(\Delta^n f)(0)| \leq \|\Delta^n f\| = \|\Delta^{n-n_1}(\Delta^{n_1} f)\| \leq \|\Delta^{n_1} f\| \leq p^{-1}\|f\|.$$

Next by Lemma 4.5(2) applied to $\Delta^{n_1} f$ there exists $n_2 \in \mathbb{N}$ such that

$$\|\Delta^{n_1+n_2} f\| = \|\Delta^{n_2}(\Delta^{n_1} f)\| \leq p^{-1}\|\Delta^{n_1} f\| \leq p^{-2}\|f\|.$$

Then for all $n \geq n_1 + n_2$ we have

$$|a_n| = |(\Delta^n f)(0)| \leq \|\Delta^n f\| = \|\Delta^{n-n_1-n_2}(\Delta^{n_1+n_2} f)\| \leq \|\Delta^{n_1+n_2} f\| \leq p^{-2}\|f\|.$$

Continuing like this, we see that for every $\varepsilon > 0$ there exists an $N \in \mathbb{N}$ such that $|a_n| \leq \varepsilon$ for all $n \geq N$, i.e. $\lim_{n\to\infty} a_n = 0$. This shows that $(a_n)_{n\geq 0} \in c_0(K)$, so the map $G$ is well defined. It is easy to see that $G$ is linear. Furthermore

$$|a_n| = |(\Delta^n f)(0)| \leq \|\Delta^n f\| \leq \|f\|$$

for every $n \geq 0$, i.e. $\|Gf\| = \|(a_n)_{n\geq 0}\| \leq \|f\|$.

*Claim 3:* $G \circ F$ is the identity on $c_0(K)$.

Let $a = (a_n)_{n\geq 0} \in c_0(K)$, and $f = F(a) = \sum_{i=0}^{\infty} a_i\binom{\cdot}{i} \in C(\mathbb{Z}_p, K)$. Since the map $\Delta : C(\mathbb{Z}_p, K) \to C(\mathbb{Z}_p, K)$ is linear and continuous, it follows that $\Delta^n f = \sum_{i=0}^{\infty} a_i \Delta^n\binom{\cdot}{i} = \sum_{i=n}^{\infty} a_i\binom{\cdot}{i-n}$. Hence $(\Delta^n f)(0) = \sum_{i=n}^{\infty} a_i\binom{0}{i-n} = a_n$. This shows that $G(F(a)) = a$ as required.

*Claim 4:* $G$ is injective.

Suppose that $f \in C(\mathbb{Z}_p, K)$ and $G(f) = 0$ in $c_0(K)$. This means that $(\Delta^n f)(0) = 0$ for all $n \geq 0$, i.e. $\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k} f(k) = 0$ for all $n \geq 0$. From this it easily follows that $f(k) = 0$ for all $k \in \mathbb{Z}_{\geq 0}$. Since $f$ is continuous and $\mathbb{Z}_{\geq 0}$ is dense in $\mathbb{Z}_p$, it follows that $f = 0$. This shows that $G$ is injective.

*Completion of the proof:*

$G$ is bijective because it is injective by Claim 4 and surjective by Claim 3. Claim 3 then implies that $F$ is the inverse of $G$. If $a \in c_0(K)$ then by Claims 1 and 2 we have

$$\|a\| = \|G(F(a))\| \leq \|F(a)\| \leq \|a\|,$$

hence $\|F(a)\| = \|a\|$, i.e. $F$ is an isometry. □

**Exercise 4.6.** Show that for every function $f \in C(\mathbb{Z}_p, K)$ there exists a unique function $Sf \in C(\mathbb{Z}_p, K)$ satisfying $\Delta(Sf) = f$ and $(Sf)(0) = 0$. The function $Sf$ is called the *indefinite sum* of $f$.

4.3. **The function $x \mapsto a^x$.** We write $M$ for the maximal ideal of the ring of integers of $K$, i.e. $M = \{x \in K : |x| < 1\}$. Note that $1 + M \subset K^\times$ since $-1 \notin M$.

**Lemma 4.7.** *The set $1 + M$ is a subgroup of the multiplicative group $K^\times$.*

*Proof.* Clearly $1 \in 1+M$. If $1+x, 1+y \in 1+M$ then $(1+x)(1+y) = 1+x+y+xy \in 1 + M$ because $|x + y + xy| \leq \max\{|x|, |y|, |xy|\} < 1$. Finally we claim that if $1 + x \in 1 + M$ then $(1 + x)^{-1} \in 1 + M$. To see this first note that the series $1 - x + x^2 - x^3 + \dots$ converges since $|(-1)^i x^i| \to 0$ as $i \to \infty$. Then clearly $(1 + x)(1 - x + x^2 - x^3 + \dots) = 1$, so $(1 + x)^{-1} = 1 - x + x^2 - x^3 + \dots$, and this lies in $1 + M$ because $|-x + x^2 - x^3 + \dots| \leq \sup_{i \geq 1} |(-1)^i x^i| = |x| < 1$. □

**Theorem 4.8.** *Let $a \in 1 + M$. Then there exists a unique continuous function $f_a : \mathbb{Z}_p \to K$ such that $f_a(x) = a^x$ for all $x \in \mathbb{Z}_{\geq 0}$.*

*Proof.* Since $|a - 1| < 1$, we have $\lim_{n\to\infty}(a - 1)^n = 0$. Therefore the series $\sum_{n=0}^{\infty}(a - 1)^n \binom{\cdot}{n}$ converges in $C(\mathbb{Z}_p, K)$, i.e. there exists a continuous function $f_a : \mathbb{Z}_p \to K$ such that

$$f_a(x) = \sum_{n=0}^{\infty}(a-1)^n \binom{x}{n}$$

for all $x \in \mathbb{Z}_p$ (and the convergence is uniform). Now if $x \in \mathbb{Z}_{\geq 0}$ then

$$f_a(x) = \sum_{n=0}^{\infty}(a-1)^n \binom{x}{n} = \sum_{n=0}^{x}(a-1)^n \binom{x}{n} = ((a-1)+1)^x = a^x.$$

This shows the existence of a continuous function $f_a : \mathbb{Z}_p \to K$ such that $f_a(x) = a^x$ for all $x \in \mathbb{Z}_{\geq 0}$. This is the unique function with this property because any continuous function $\mathbb{Z}_p \to K$ is already uniquely determined by its values on the dense subset $\mathbb{Z}_{\geq 0}$ of $\mathbb{Z}_p$. □

If $a \in 1 + M$ and $x \in \mathbb{Z}_p$ then one usually writes $a^x$ instead of $f_a(x)$. Note that $a^x \in 1 + M$ for all $x \in \mathbb{Z}_p$ because this is true for $x \in \mathbb{Z}_{\geq 0}$ and $1 + M$ is closed in $K$.

**Exercise 4.9.** Show that the abelian group $1 + M$ becomes a $\mathbb{Z}_p$-module with respect to the operation $\mathbb{Z}_p \times (1 + M) \to 1 + M$, $(x, a) \mapsto a^x$.

4.4. **The $p$-adic gamma function.** Recall that the classical gamma function is a meromorphic function $\Gamma : \mathbb{C} \to \mathbb{C}$ satisfying $\Gamma(n) = (n - 1)!$ for all $n \in \mathbb{N}$. It is easy to see that there is no continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ satisfying $f(n) = (n - 1)!$ for all $n \in \mathbb{N}$ (because for any $a \in \mathbb{N}$ we have $\lim_{i\to\infty}(a + p^i) = a$, but $\lim_{i\to\infty}((a + p^i) - 1)! = 0 \neq (a - 1)!$). However we will show that by slightly modifying $(n - 1)!$ we can find a $p$-adic analogue of the classical gamma function. For simplicity we assume in this section that the prime number $p$ is odd.

**Theorem 4.10.** *There exists a unique continuous function $\Gamma_p : \mathbb{Z}_p \to \mathbb{Q}_p$ such that*

$$\Gamma_p(n) = (-1)^n \prod_{\substack{1 \leq j < n \\ p \nmid j}} j$$

*for all integers $n \geq 2$.*

We first show a general result on the existence of continuous functions on $\mathbb{Z}_p$ that take specified values on certain subsets of $\mathbb{Z}$. Let $K$ be any complete extension of $\mathbb{Q}_p$. Suppose we are given a function $f : \mathbb{Z}_{\geq b} \to K$ (for some $b \in \mathbb{Z}$). We say that a continuous function $\tilde{f} : \mathbb{Z}_p \to K$ *interpolates* $f$ if $\tilde{f}(n) = f(n)$ for all $n \in \mathbb{Z}_{\geq b}$.

**Proposition 4.11.** *Let $b \in \mathbb{Z}$ and let $f : \mathbb{Z}_{\geq b} \to K$ be a function. Then there exists a continuous function $\tilde{f} : \mathbb{Z}_p \to K$ interpolating $f$ if and only if for every $\varepsilon > 0$ there exists an $s \in \mathbb{N}$ such that $|f(n) - f(n+p^s)| < \varepsilon$ for all $n \in \mathbb{Z}_{\geq b}$. Furthermore the function $\tilde{f}$ is unique if it exists.*

*Proof.* Using that $\mathbb{Z}_{\geq 0}$ is dense in $\mathbb{Z}_p$ we easily deduce that $\mathbb{Z}_{\geq b}$ is dense in $\mathbb{Z}_p$. This implies the uniqueness of the function $\tilde{f}$ if it exists.

Now suppose that a continuous function $\tilde{f}$ interpolating $f$ exists. Since $\tilde{f}$ is continuous and $\mathbb{Z}_p$ is compact, it follows that $\tilde{f}$ is uniformly continuous, i.e. for every $\varepsilon > 0$ there exists $\delta > 0$ such that $|x-y| < \delta$ implies $|\tilde{f}(x) - \tilde{f}(y)| < \varepsilon$. Hence if $p^{-s} < \delta$ then $|f(n) - f(n+p^s)| < \varepsilon$ for all $n \in \mathbb{Z}_{\geq b}$ as required.

Conversely assume that for every $\varepsilon > 0$ there exists an $s \in \mathbb{N}$ such that $|f(n) - f(n+p^s)| < \varepsilon$ for all $n \in \mathbb{Z}_{\geq b}$. We claim that this assumption already implies that $f : \mathbb{Z}_{\geq b} \to K$ is uniformly continuous (where we consider the $p$-adic metric on $\mathbb{Z}_{\geq b}$). Let $\varepsilon > 0$ and choose $s$ as above. Now if $x, y \in \mathbb{Z}_{\geq b}$ satisfy $|x-y| \leq p^{-s}$ then (assuming without loss of generality that $y \geq x$) we have $y = x + kp^s$ for some $k \in \mathbb{Z}_{\geq 0}$. Hence

$$\begin{aligned} |f(x) - f(y)| \leq \max \bigl\{ &|f(x) - f(x+p^s)|, |f(x+p^s) - f(x+2p^s)|, \\ &\ldots, |f(x+(k-1)p^s) - f(y)| \bigr\} < \varepsilon. \end{aligned}$$

This proves the uniform continuity of $f : \mathbb{Z}_{\geq b} \to K$.

For $x \in \mathbb{Z}_p$ we then define $\tilde{f}(x) = \lim_{i \to \infty} f(n_i)$ where $n_1, n_2, n_3, \ldots$ is a sequence in $\mathbb{Z}_{\geq b}$ that converges to $x$ (such a sequence exists since $\mathbb{Z}_{\geq b}$ is dense in $\mathbb{Z}_p$). Using the uniform continuity of $f$, it is not difficult to verify that $\tilde{f}$ is well defined (i.e. the limit in the definition of $\tilde{f}(x)$ exists and is independent of the choice of sequence $(n_i)_{i \in \mathbb{N}}$) and continuous. Furthermore it is obvious that $\tilde{f}(n) = f(n)$ for all $n \in \mathbb{Z}_{\geq b}$. This shows the existence of $\tilde{f}$ with the required properties. ☐

**Lemma 4.12.** *Let $n \in \mathbb{Z}$ and $s \in \mathbb{N}$. Then*

$$\prod_{\substack{n \leq j < n+p^s \\ p \nmid j}} j \equiv -1 \pmod{p^s}.$$

*Proof.* Let $\pi : \mathbb{Z} \to \mathbb{Z}/p^s\mathbb{Z}$ be the canonical homomorphism. The numbers $j$ with $n \leq j < n + p^s$ form a complete set of residues modulo $p^s$, and we have $p \nmid j$ if and only if $\pi(j) \in (\mathbb{Z}/p^s\mathbb{Z})^\times$. Therefore

$$\pi\Biggl( \prod_{\substack{n \leq j < n+p^s \\ p \nmid j}} j \Biggr) = \prod_{g \in (\mathbb{Z}/p^s\mathbb{Z})^\times} g.$$

Every factor $g \in (\mathbb{Z}/p^s\mathbb{Z})^\times$ cancels with its inverse $g^{-1}$, except for those $g$ where $g = g^{-1}$. But $g = g^{-1}$ if and only if $g^2 = 1$, i.e. $(g-1)(g+1) = 0$. This is the case if and only if $g = 1$ or $g = -1$ (here we use that $p$ is odd). Hence

$$\prod_{g \in (\mathbb{Z}/p^s\mathbb{Z})^\times} g = \prod_{\substack{g \in (\mathbb{Z}/p^s\mathbb{Z})^\times \\ g = g^{-1}}} g = 1 \cdot (-1) = -1.$$

We have shown that

$$\pi\Biggl( \prod_{\substack{n \leq j < n+p^s \\ p \nmid j}} j \Biggr) = -1$$

in $\mathbb{Z}/p^s\mathbb{Z}$, hence

$$\prod_{\substack{n \le j < n+p^s \\ p \nmid j}} j \equiv -1 \pmod{p^s}$$

as required. □

*Proof of Theorem 4.10.* Let $f(n) = (-1)^n \prod_{\substack{1 \le j < n \\ p \nmid j}} j$ for $n \in \mathbb{Z}_{\ge 2}$. By Proposition 4.11 it suffices to show that for every $\varepsilon > 0$ there exists an $s \in \mathbb{N}$ such that $|f(n) - f(n+p^s)| < \varepsilon$ for all $n \in \mathbb{Z}_{\ge 2}$. But using the lemma we find that

$$\begin{aligned} f(n) - f(n+p^s) &= (-1)^n \prod_{\substack{1 \le j < n \\ p \nmid j}} j - (-1)^{n+p^s} \prod_{\substack{1 \le j < n+p^s \\ p \nmid j}} j \\ &= (-1)^n \prod_{\substack{1 \le j < n \\ p \nmid j}} j \cdot \left( 1 + \prod_{\substack{n \le j < n+p^s \\ p \nmid j}} j \right) \\ &\equiv 0 \pmod{p^s}. \end{aligned}$$

Hence if $p^{-s} < \varepsilon$ then $|f(n) - f(n+p^s)| \le p^{-s} < \varepsilon$ for all $n \in \mathbb{Z}_{\ge 2}$ as required. □

**Exercise 4.13.** Define $h_p : \mathbb{Z}_p \to \mathbb{Q}_p$ by

$$h_p(x) = \begin{cases} -x & \text{if } |x| = 1 \\ -1 & \text{if } |x| < 1. \end{cases}$$

Show that $\Gamma_p(x+1) = h_p(x)\Gamma_p(x)$ for all $x \in \mathbb{Z}_p$. Use this to compute $\Gamma_p(1)$ and $\Gamma_p(0)$.

For a description of $\Gamma_2$, the Mahler coefficients of $\Gamma_p$, and many other properties of the $p$-adic gamma function see [Robert, §7.1] and [Schikhof, §35–39 and §52].

## 5. Differentiation

Let $p$ be a prime number and let $(K, |\ |)$ be a complete extension of $(\mathbb{Q}_p, |\ |)$ (e.g. $K = \mathbb{Q}_p$ or $K = \mathbb{C}_p$). In this chapter we discuss the definition and some basic properties of (strictly) differentiable functions $X \to K$ where $X \subseteq K$.

### 5.1. **Differentiability and strict differentiability.**

We say that a non-empty subset $X$ of $K$ has *no isolated points* if for every $a \in X$ and every neighbourhood $U$ of $a$ in $X$ the set $U \setminus \{a\}$ is non-empty.

**Definition 5.1.** Let $X$ be a non-empty subset of $K$ without isolated points, and let $f : X \to K$ be a function.

(1) We say that $f$ is *differentiable at a point* $a \in X$ (with derivative $f'(a)$) if the limit $f'(a) = \lim_{x \to a} \frac{f(x)-f(a)}{x-a}$ exists.
(2) We say that $f$ is *differentiable* (on $X$) if $f$ is differentiable at every point $a \in X$. In this case the derivative $f'$ is again a function $X \to K$.

**Exercise 5.2.** Show that if $f : X \to K$ is differentiable at a point $a \in X$ then $f$ is continuous at $a$.

A function $f : X \to K$ is called *locally constant* if every point $a \in X$ has a neighbourhood $U$ in $X$ such that the restriction of $f$ to $U$ is a constant function. Clearly every locally constant function is differentiable with derivative 0. The following example shows that the converse of this statement is not true.

**Example 5.3.** For every $n \in \mathbb{N}$ let $B_n = \{x \in \mathbb{Z}_p : |x - p^n| < p^{-2n}\} \subset \mathbb{Z}_p$. Note that the balls $B_n$ are pairwise disjoint. Define a function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ $(\subset \mathbb{Q}_p)$ by

$$f(x) = \begin{cases} p^{2n} & \text{if } x \in B_n, \\ 0 & \text{if } x \in \mathbb{Z}_p \setminus \bigcup_{n\in\mathbb{N}} B_n. \end{cases}$$

We claim that

(1) $f$ is differentiable with $f' = 0$,
(2) $f$ is not locally constant.

It is easy to see that on $\mathbb{Z}_p \setminus \{0\}$ the function $f$ is locally constant. Hence if $a \in \mathbb{Z}_p \setminus \{0\}$ then $f$ is differentiable at $a$ with derivative $f'(a) = 0$. Furthermore $f$ is differentiable at the point 0 with derivative $f'(0) = 0$, because for $x \neq 0$ we have

$$\left|\frac{f(x) - f(0)}{x - 0}\right| = \begin{cases} |p^{2n}|/|p^n| = p^{-n} & \text{if } x \in B_n, \\ 0 & \text{if } x \in \mathbb{Z}_p \setminus \bigcup_{n\in\mathbb{N}} B_n \end{cases}$$

and hence $\lim_{x\to 0} \frac{f(x)-f(0)}{x-0} = 0$. Finally, $f$ is not locally constant on $\mathbb{Z}_p$ because $f(0) = 0$ but in every neighbourhood of 0 there exists a point $x$ with $f(x) \neq 0$.

**Definition 5.4.** Let $X$ be a non-empty subset of $K$ without isolated points, and let $f : X \to K$ be a function.

(1) We say that $f$ is *strictly differentiable at a point* $a \in X$ if the difference quotient
$$\Phi f(x, y) = \frac{f(x) - f(y)}{x - y}$$
has a limit as $(x, y) \to (a, a)$, $x \neq y$.
(2) We say that $f$ is *strictly differentiable* (on $X$) if $f$ is strictly differentiable at every point $a \in X$.

Some authors (e.g. [Schikhof]) use the expression *continuously differentiable* instead of strictly differentiable.

**Lemma 5.5.** (1) *If $f$ is strictly differentiable at a point $a \in X$ then $f$ is differentiable at $a$ and $f'(a) = \lim_{(x,y)\to(a,a)} \Phi f(x, y)$.*
(2) *If $f$ is strictly differentiable on $X$ then $f$ is differentiable on $X$ and the function $f' : X \to K$ is continuous.*

*Proof.* Everything is clear except for the continuity of $f'$. Let $a \in X$ and $\varepsilon > 0$. We must show that there exists a neighbourhood $U$ of $a$ in $X$ such that $|f'(a) - f'(b)| < \varepsilon$ for all $b \in U$. Since $f$ is strictly differentiable in $a$, there exists an open neighbourhood $U$ of $a$ in $X$ such that $|f'(a) - \Phi f(x, y)| < \varepsilon$ for all $(x, y) \in U \times U$ with $x \neq y$. Now let $b \in U$. Then since $f$ is strictly differentiable in $b$, the point $b$ has a neighbourhood $V \subseteq U$ such that $|f'(b) - \Phi f(x, y)| < \varepsilon$ for all $(x, y) \in V \times V$ with $x \neq y$. Fix $y \in V \setminus \{b\}$. Then

$$\begin{aligned} |f'(a) - f'(b)| &= |f'(a) - \Phi f(b, y) + \Phi f(b, y) - f'(b)| \\ &\leq \max\{|f'(a) - \Phi f(b, y)|, |\Phi f(b, y) - f'(b)|\} \\ &< \varepsilon \end{aligned}$$

as required. □

By Lemma 5.5(2), every strictly differentiable function is differentiable with continuous derivative. However the following example shows that the converse of this statement is false.

**Example 5.6.** Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be the function from Example 5.3. We have already seen that $f$ is differentiable and $f'$ is continuous (because $f' = 0$). However $f'$ is not strictly differentiable at the point 0, i.e. the limit $\lim_{(x,y)\to(0,0)} \Phi f(x, y)$

does not exist. Indeed, taking the sequence $(x_n, y_n) = (p^n, 0)$ (which converges to $(0,0)$) gives the limit $\lim_{n\to\infty} \Phi f(x_n, y_n) = 0$ (as seen in Example 5.3), but taking the sequence $(x_n, y_n) = (p^n, p^n - p^{2n})$ (which also converges to $(0,0)$) gives the limit

$$\lim_{n\to\infty} \Phi f(x_n, y_n) = \lim_{n\to\infty} \frac{p^{2n} - 0}{p^n - (p^n - p^{2n})} = 1.$$

**Exercise 5.7.** Let $X$ and $Y$ be non-empty subsets of $K$ without isolated points. Let $f : X \to K$ and $g : Y \to K$ be functions such that $f(X) \subseteq Y$. Show that if $f$ is strictly differentiable at a point $a \in X$ and $g$ is strictly differentiable at the point $f(a)$, then $g \circ f$ is strictly differentiable at $a$ with derivative $(g \circ f)'(a) = g'(f(a))f'(a)$.

5.2. **Local invertibility of strictly differentiable functions.**

**Lemma 5.8.** *Let $X$ be a non-empty subset of $K$ without isolated points. Let $f : X \to K$ be strictly differentiable at a point $a \in X$. If $f'(a) \neq 0$ then there exists a neighbourhood $U$ of $a$ in $X$ such that*

$$|f(x) - f(y)| = |f'(a)| \cdot |x - y|$$

*for all $x, y \in U$. In particular, $f$ is injective on $U$.*

*Proof.* Since $f'(a) \neq 0$ and $\Phi f(x,y) \to f'(a)$ as $(x,y) \to (a,a)$ (with $x \neq y$), there exists a neighbourhood $U$ of $a$ in $X$ such that $|\Phi f(x,y) - f'(a)| < |f'(a)|$ for all $x, y \in U$ with $x \neq y$. But this implies that $|\Phi f(x,y)| = |f'(a)|$ (because otherwise Lemma 2.4 would give the contradiction $\max\{|\Phi f(x,y)|, |f'(a)|\} = |\Phi f(x,y) - f'(a)| < |f'(a)|$). After multiplying by $|x-y|$ we obtain $|f(x) - f(y)| = |f'(a)| \cdot |x - y|$ for all $x, y \in U$ with $x \neq y$. But clearly this equality is also true if $x, y \in U$ and $x = y$. □

**Example 5.9.** The lemma is not true if strictly differentiable is replaced by differentiable. For example, if $g : \mathbb{Z}_p \to \mathbb{Z}_p$ is defined by $g(x) = f(x) + x$ where $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is the function from Example 5.3, then $g$ is differentiable at 0 with derivative $g'(0) = 1 \neq 0$. However $g$ is not injective on any neighbourhood of 0 because $g(p^n) = p^n + p^{2n} = g(p^n + p^{2n})$ for all $n \in \mathbb{N}$.

**Theorem 5.10.** *Let $X$ be a non-empty and open subset of $K$. Let $f : X \to K$ be strictly differentiable at a point $a \in X$. If $f'(a) \neq 0$ then for all sufficiently small $r > 0$ the function $f$ maps the closed ball $B_{\leq r}(a)$ bijectively onto the closed ball $B_{\leq |f'(a)|r}(f(a))$, and the local inverse $g : B_{\leq |f'(a)|r}(f(a)) \to B_{\leq r}(a)$ is strictly differentiable at $f(a)$ with $g'(f(a)) = f'(a)^{-1}$.*

Before proving Theorem 5.10 we recall Banach's contraction theorem.

**Theorem 5.11** (Banach's contraction theorem)**.** *Let $(X, d)$ be a non-empty complete metric space. Let $F : X \to X$ be a contraction (i.e. there exists a constant $0 < \tau < 1$ such that $d(F(x), F(y)) \leq \tau d(x,y)$ for all $x, y \in X$). Then $F$ has precisely one fixed point (i.e. there exists precisely one $b \in X$ such that $F(b) = b$).*

For a proof of Banach's contraction theorem see e.g. [Schikhof, Appendix A.1].

*Proof of Theorem 5.10.* Fix a constant $\tau$ with $0 < \tau < 1$. Since $\Phi f(x,y) \to f'(a)$ as $(x,y) \to (a,a)$ (with $x \neq y$), there exists a neighbourhood $U$ of $a$ in $X$ such that

$$\left| \frac{f(x) - f(y)}{x - y} - f'(a) \right| \leq \tau |f'(a)|$$

for all $x, y \in U$ with $x \neq y$. For all sufficiently small $r > 0$ we have $B_{\leq r}(a) \subseteq U$. We claim that for such $r$ the map $f$ maps $B_{\leq r}(a)$ bijectively onto $B_{\leq |f'(a)|r}(f(a))$.

As in the proof of Lemma 5.8 we have $\left|\frac{f(x)-f(y)}{x-y}\right| = |f'(a)|$ for all $x, y \in B_{\leq r}(a)$ with $x \neq y$. By choosing $y = a$ this implies that $|f(x) - f(a)| = |f'(a)| \cdot |x - a|$

for all $x \in B_{\leq r}(a)$. Hence $f(x) \in B_{\leq |f'(a)|r}(f(a))$ for all $x \in B_{\leq r}(a)$ as required. Furthermore the equality $|f(x) - f(y)| = |f'(a)| \cdot |x - y|$ also implies that $f$ is injective on $B_{\leq r}(a)$.

Now let $c \in B_{\leq |f'(a)|r}(f(a))$. Define a function $F$ by $F(x) = x - (f(x) - c)/f'(a)$. If $x \in B_{\leq r}(a)$ then $|f(x) - c| \leq \max\{|f(x) - f(a)|, |f(a) - c|\} \leq |f'(a)|r$ and hence

$$|F(x) - a| = |x - a - (f(x) - c)/f'(a)| \leq \max\{|x - a|, |f(x) - c|/|f'(a)|\} \leq r.$$

This shows that $F$ is a map $B_{\leq r}(a) \to B_{\leq r}(a)$. Furthermore $F$ is a contraction because for any $x, y \in B_{\leq r}(a)$ we have

$$\begin{aligned} |F(x) - F(y)| &= \left| x - y - \frac{f(x) - f(y)}{f'(a)} \right| \\ &= \frac{|x - y|}{|f'(a)|} \cdot \left| f'(a) - \frac{f(x) - f(y)}{x - y} \right| \\ &\leq \frac{|x - y|}{|f'(a)|} \cdot \tau |f'(a)| = \tau |x - y|. \end{aligned}$$

Now the space $B_{\leq r}(a)$ is complete because it is closed in the complete space $K$. Hence by Banach's contraction theorem the map $F$ has a fixed point $b \in B_{\leq r}(a)$. But clearly $F(b) = b$ implies $f(b) = c$. This shows that $B_{\leq |f'(a)|r}(f(a)) \subseteq f(B_{\leq r}(a))$ as required.

Let $g : B_{\leq |f'(a)|r}(f(a)) \to B_{\leq r}(a)$ be the inverse of $f$. From $|f(x) - f(y)| = |f'(a)| \cdot |x - y|$ for all $x, y \in B_{\leq r}(a)$ we obtain $|f'(a)|^{-1} \cdot |t - u| = |g(t) - g(u)|$ for all $t, u \in B_{\leq |f'(a)|r}(f(a))$. This implies that $g$ is continuous. Now

$$\Phi g(t, u) = \frac{g(t) - g(u)}{f(g(t)) - f(g(u))} = \big(\Phi f(g(t), g(u))\big)^{-1}.$$

If $(t, u) \to (f(a), f(a))$ with $t \neq u$, then $(g(t), g(u)) \to (g(f(a)), g(f(a)) = (a, a)$. Hence we see that $\lim_{(t,u) \to (f(a), f(a))} \Phi g(t, u)$ exists and is equal to $f'(a)^{-1}$. □

5.3. **Further results on strictly differentiable functions.** Finally we mention some further results without proof.

**Theorem 5.12.** *Let $f : \mathbb{Z}_p \to K$ be a continuous function with Mahler expansion $f = \sum_{n=0}^{\infty} a_n \binom{\cdot}{n}$. Then $f$ is strictly differentiable if and only if* $\lim_{n \to \infty} n|a_n| = 0$.

For a proof see [Schikhof, §53]. Recall that if $a \in 1 + M \subset K$, i.e. $|a - 1| < 1$, and $x \in \mathbb{Z}_p$ then $a^x$ is given by the Mahler series

$$a^x = \sum_{n=0}^{\infty} (a - 1)^n \binom{x}{n}$$

(cf. §4.3). Since $\lim_{n \to \infty} n|a - 1|^n = 0$, it follows from the theorem that the function $x \mapsto a^x$ is strictly differentiable.

**Theorem 5.13.** *Let $X$ be a non-empty subset of $K$ without isolated points, and let $f : X \to K$ be a continuous function. Then there exists a strictly differentiable function $F : X \to K$ such that $F' = f$.*

For a proof of this theorem and many more results on (strictly) differentiable functions see [Schikhof].

## References

[Cassels] J.W.S. Cassels, *Local fields*, Cambridge University Press, 1986.
[Gouvea] F.Q. Gouvêa, *p-adic numbers*, 2nd edition, Springer, 1997.
[Robert] A.M. Robert *A course in p-adic analysis*, Springer, 2000.
[Schikhof] W.H. Schikhof, *Ultrametric calculus. An introduction to p-adic analysis*, Cambridge University Press, 1984.