P-ADIC NUMBERS

JAN-HENDRIK EVERTSE

March 2011

Literature:

Z.I. Borevich, I.R. Shafarevich, Number Theory, Academic Press, 1966, Chap. 1,4.

A. Fröhlich, Local Fields, in: Algebraic Number Theory, edited by J.W.S. Cassels, A. Fröhlich, Academic Press, 1967, Chap. 1.

N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, 2nd edition, Graduate Texts in Mathematics 58, Springer Verlag 1984, corrected 2nd printing 1996, Chap. I,III.

C. Lech, A note on recurring sequences, Arkiv för mathematik, Band 2, no. 22 (1953), 417–421.

L.J. Mordell, Diophantine Equations, Academic Press, 1969, Chap. 23.

1. Absolute values

The *p-adic absolute value* $|\cdot|_p$ on $\mathbb{Q}$ is defined as follows: if $a \in \mathbb{Q}$, $a \neq 0$ then write $a = p^m b/c$ where b, c are integers not divisible by p and put $|a|_p = p^{-m}$; further, put $|0|_p = 0$.

Example. Let $a = -2^{-7}3^8 5^{-3}$. Then $|a|_2 = 2^7$, $|a|_3 = 3^{-8}$, $|a|_5 = 5^3$, $|a|_p = 1$ for $p \geqslant 7$.

We give some properties:

$$|ab|_p = |a|_p |b|_p \text{ for } a, b \in \mathbb{Q};$$
$$|a+b|_p \leqslant \max(|a|_p, |b|_p) \text{ for } a, b \in \mathbb{Q} \quad \text{(ultrametric inequality)}.$$

Notice that the last property implies that

$$|a+b|_p = \max(|a|_p, |b|_p) \text{ if } |a|_p \neq |b|_p.$$

It is common to write the ordinary absolute value $|a| = \max(a, -a)$ on $\mathbb{Q}$ as $|a|_\infty$, to call ∞ the 'infinite prime' and to define $M_{\mathbf{Q}} := \{\infty\} \cup \{\text{primes}\}$.

Then we have the important *product formula:*

$$\prod_{p \in M_{\mathbf{Q}}} |a|_p = 1 \text{ for } a \in \mathbb{Q},\ a \neq 0.$$

Absolute values on fields. We define more generally absolute values on fields. Let K be any field. An absolute value on K is a function $|\cdot| : K \to \mathbb{R}_{\geqslant 0}$ with the following properties:

$$\begin{aligned} &|ab| = |a| \cdot |b| \text{ for } a, b \in K; \\ &|a+b| \leqslant |a| + |b| \text{ for } a, b \in K \quad \text{(triangle inequality)}; \\ &|a| = 0 \Longleftrightarrow a = 0. \end{aligned}$$

Note that these properties imply that $|1| = 1$. The absolute value $|\cdot|$ is called non-trivial if there is $a \in K$ with $|a| \neq \{0, 1\}$.

The absolute value $|\cdot|$ is called *non-archimedean* if the triangle inequality can be replaced by the stronger ultrametric inequality

$$|a+b| \leqslant \max(|a|, |b|) \text{ for } a, b \in K\,.$$

An absolute value not satisfying the ultrametric inequality is called *archimedean.*

If K is a field with absolute value $|\cdot|$ and L an extension of K, then an extension or continuation of $|\cdot|$ to L is an absolute value on L whose restriction to K is $|\cdot|$.

Examples.
1) The ordinary absolute value $|\cdot|$ on $\mathbb{Q}$ is archimedean, while the p-adic absolute values are all non-archimedean.
2) Let K be any field, and $K(t)$ the field of rational functions of K. For a polynomial $f \in K[t]$ define $|f| = 0$ if $f = 0$ and $|f| = e^{\deg f}$ if $f \neq 0$. Further, for a rational function f/g with $f, g \in K[t]$ define $|f/g| = |f|/|g|$. Verify that this defines a non-archimedean absolute value on $K(t)$.

Two absolute values $|\cdot|_1, |\cdot|_2$ on K are called equivalent if there is $\alpha > 0$ such that $|x|_2 = |x|_1^{\alpha}$ for all $x \in K$. We state without proof the following result:

Theorem 1.1 (Ostrowski)**.** *Every non-trivial absolute value on* $\mathbf{Q}$ *is equivalent to either the ordinary absolute value or a p-adic absolute value for some prime number p.*

Valuations. In algebra and number theory, one quite often deals with valuations instead of absolute values. A *valuation* on a field K is a function $v : K \to \mathbb{R} \cup \{\infty\}$ such that for some constant $c > 1$, $c^{-v(\cdot)}$ defines a non-archimedean absolute value on K. That is,

$$v(x) = \infty \iff x = 0;$$
$$v(xy) = v(x) + v(y) \text{ for } x, y \in K;$$
$$v(x + y) \geqslant \min(v(x), v(y)) \text{ for } x, y \in K.$$

The valuation is called non-trivial if there is $a \in K^*$ with $v(a) \neq 0$. The set $v(K^*)$ is an additive subgroup of $\mathbb{R}$. The valuation v is called *discrete* if $v(K^*)$ is a discrete subgroup of $\mathbb{R}$. A normalized discrete valuation is one for which $v(K^*) = \mathbb{Z}$.

2. Completions

An absolute value preserving isomorphism between two fields K_1, K_2 with absolute values $|\cdot|_1$, $|\cdot|_2$, respectively, is an isomorphism $\varphi : K_1 \to K_2$ such that $|\varphi(x)|_2 = |x|_1$ for $x \in K_1$.

Let K be a field, $|\cdot|$ a non-trivial absolute value on K, and $\{a_k\}_{k=0}^{\infty}$ a sequence in K.
We say that $\{a_k\}_{k=0}^{\infty}$ *converges to* α *with respect to* $|\cdot|$ if $\lim_{k\to\infty} |a_k - \alpha| = 0$.
Further, $\{a_k\}_{k=0}^{\infty}$ is called a *Cauchy sequence with respect to* $|\cdot|$ if
$\lim_{m,n\to\infty} |a_m - a_n| = 0$.
Notice that any convergent sequence is a Cauchy sequence.

We say that K is *complete* with respect to $|\cdot|$ if every Cauchy sequence w.r.t. $|\cdot|$ in K converges to a limit in K. For instance, $\mathbb{R}$ and $\mathbb{C}$ are complete w.r.t. the ordinary absolute value.

By mimicking the construction of $\mathbb{R}$ from $\mathbb{Q}$, one can show that every field K with an absolute value can be extended to an essentially unique field $\widetilde{K}$, such that $\widetilde{K}$ is complete and every element of $\widetilde{K}$ is the limit of a Cauchy sequence from K.

Theorem 2.1. *Let K be a field with absolute value $|\cdot|$. There is an up to absolute value preserving isomorphism unique extension field $\widetilde{K}$ of K, called the* completion *of K, having the following properties:*

(i) $|\cdot|$ *can be continued to an absolute value on* $\widetilde{K}$*, also denoted* $|\cdot|$*, such that* $\widetilde{K}$ *is complete w.r.t.* $|\cdot|$*;*
(ii) K *is dense in* $\widetilde{K}$*, i.e., every element of* $\widetilde{K}$ *is the limit of a sequence from* K*.*

Proof. We give a sketch. Cauchy sequences, limits, etc. are all with respect to $|\cdot|$.

The set of Cauchy sequences in K with respect to $|\cdot|$ is closed under termwise addition and multiplication $\{a_n\}+\{b_n\} := \{a_n+b_n\}$, $\{a_n\}\cdot\{b_n\} := \{a_n\cdot b_n\}$. With these operations they form a ring, which we denote by $\mathcal{R}$. It is not difficult to verify that the sequences $\{a_n\}$ such that $a_n \to 0$ with respect to $|\cdot|$ form a maximal ideal in $\mathcal{R}$, which we denote by $\mathcal{M}$. Thus, the quotient $\mathcal{R}/\mathcal{M}$ is a field, which is our completion $\widetilde{K}$.

We define the absolute value $|\alpha|$ of $\alpha \in \widetilde{K}$ by choosing a representative $\{a_n\}$ of α, and putting $|\alpha| := \lim_{n\to\infty} |a_n|$, where now the limit is with respect to the ordinary absolute value on $\mathbb{R}$. It is not difficult to verify that this is well-defined, that is, the limit exists and is independent of the choice of the representative $\{a_n\}$.

We may view K as a subfield of $\widetilde{K}$ by identifying $a \in K$ with the element of $\widetilde{K}$ represented by the constant Cauchy sequence $\{a\}$. In this manner, the absolute value on $\widetilde{K}$ constructed above extends that of K, and moreover, every element of $\widetilde{K}$ is a limit of a sequence from K. So K is dense in $\widetilde{K}$. One shows that $\widetilde{K}$ is complete, that is, any Cauchy sequence $\{a_n\}$ in $\widetilde{K}$ has a limit in $\widetilde{K}$, by taking very good approximations $b_n \in K$ of a_n and then taking the limit of the b_n.

Finally, if K' is another complete field with absolute value extending that on K such that K is dense in K' one obtains an isomorphism from $\widetilde{K}$ to K' as follows: Take $\alpha \in \widetilde{K}$. Choose a sequence $\{a_k\}$ in K converging to α; this is necessarily a Cauchy sequence. Then map α to the limit of $\{a_k\}$ in K'. □

Corollary 2.2. *Assume that* $|\cdot|$ *is a non-archimedean absolute value on* K*. Then the extension of* $|\cdot|$ *to* $\widetilde{K}$ *is also non-archimedean.*

Proof. Let $a, b \in \widetilde{K}$. Choose sequences $\{a_k\}$, $\{b_k\}$ in K that converge to a, b, respectively. Then taking the limit of $|a_k + b_k| \leqslant \max(|a_k|, |b_k|)$ gives $|a+b| \leqslant \max(|a|, |b|)$. □

Ostrowski proved that any field complete with respect to an archimedean absolute value is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. As a consequence, any field that can be endowed with an archimedean absolute value is isomorphic to a subfield of $\mathbb{C}$. On the other hand, there is a much larger variety of fields with a non-archimedean absolute value.

It is possible to define notions such as convergence, continuity, differentiability, etc. for complete fields with a non-archimedean absolute value similarly as for $\mathbb{R}$ or $\mathbb{C}$, and this leads to *non-archimedean analysis.* One of the striking features of non-archimedean analysis is the following very easy criterion for convergence of series.

Lemma 2.3. *Let K be a field complete w.r.t. a non-archimedean absolute value $|\cdot|$. Let $\{a_k\}_{k=0}^{\infty}$ be a sequence in K. Then $\sum_{k=0}^{\infty} a_k$ converges in K if and only if $\lim_{k\to\infty} a_k = 0$.*

Proof. Suppose that $\alpha := \sum_{k=0}^{\infty} a_k$ converges. Then

$$a_n = \sum_{k=0}^{n} a_k - \sum_{k=0}^{n-1} a_k \;\to\; \alpha - \alpha = 0.$$

Conversely, suppose that $a_k \to 0$ as $k \to \infty$. Let $\alpha_n := \sum_{k=0}^{n} a_k$. Then for any integers m, n with $0 < m < n$ we have

$$|\alpha_n - \alpha_m| = |\sum_{k=m+1}^{n} a_k| \leqslant \max(|a_{m+1}|, \ldots, |a_n|) \to 0 \text{ as } m, n \to \infty\,.$$

So the partial sums α_n form a Cauchy sequence, hence must converge to a limit in K. □

Corollary 2.4. *Let K be a field complete w.r.t. a non-archimedean absolute value $|\cdot|$. Then the sequence $\{a_k\}_{k=0}^{\infty}$ converges in K if and only if*

$$\lim_{k\to\infty} (a_k - a_{k-1}) = 0.$$

Proof. Apply Lemma 2.3 to the series $\sum_{k=0}^{\infty} b_k$ where $b_0 := a_0$ and $b_k := a_k - a_{k-1}$ for $k \geqslant 1$. □

Lemma 2.5. *Let again K be a field complete w.r.t. a non-archimedean absolute value $|\cdot|$. Then every series $\sum_{k=0}^{\infty} a_k$ convergent in K w.r.t. $|\cdot|$ is unconditionally convergent, i.e., neither the convergence, nor the value of the series, are affected if the terms a_k are rearranged.*

Proof. Let σ be a bijection from $\mathbb{Z}_{\geqslant 0}$ to $\mathbb{Z}_{\geqslant 0}$. We have to prove that $\sum_{k=0}^{\infty} a_{\sigma(k)} = \sum_{k=0}^{\infty} a_k$, or equivalently, that $S_M \to 0$ as $M \to \infty$, where $S_M := \sum_{k=0}^{M} a_k - \sum_{k=0}^{M} a_{\sigma(k)}$.

Let $\varepsilon > 0$. There is N such that $|a_k| < \varepsilon$ for all $k \geqslant N$. Choose N_ε such that $\{\sigma(0), \ldots, \sigma(N_\varepsilon)\}$ contains $\{0, \ldots, N\}$. Then for every $M > N_\varepsilon$, S_M contains only terms a_k with $k > N$ and $a_{\sigma(k)}$ with $\sigma(k) > N$. Hence each term in S_M has absolute value $< \varepsilon$ and therefore, by the ultrametric inequality, $|S_M| < \varepsilon$. This proves our lemma. □

For interchanging two infinite summations we have the following criterion:

Lemma 2.6. *Let K be a field complete w.r.t. a non-archimedean absolute value $|\cdot|$. Let $\{a_{mn}\}_{m,n=0}^{\infty}$ be a double sequence such that $\lim_{\max(m,n)\to\infty} a_{mn} = 0$. Then both the expressions*

$$\sum_{m=0}^{\infty}\left(\sum_{n=0}^{\infty} a_{mn}\right), \quad \sum_{n=0}^{\infty}\left(\sum_{m=0}^{\infty} a_{mn}\right)$$

converge and are equal.

Proof. Exercise. □

3. P-adic numbers and p-adic integers

In everything that follows, p is a prime number. The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is called the *field of p-adic numbers,* notation $\mathbb{Q}_p$.

The continuation of $|\cdot|_p$ to $\mathbb{Q}_p$ is also denoted by $|\cdot|_p$. This is a non-archimedean absolute value. Convergence, limits, Cauchy sequences and the like will all be with respect to $|\cdot|_p$.

Lemma 3.1. *The value set of $|\cdot|_p$ on $\mathbb{Q}_p$ is $\{0\} \cup \{p^m : m \in \mathbb{Z}\}$.*

Proof. Let $x \in \mathbb{Q}_p$, $x \neq 0$. Choose a sequence $\{x_k\}$ in $\mathbb{Q}$ converging to x. For k sufficiently large we have $x_k \neq 0$ and thus, $|x_k|_p = p^{m_k}$ for some $m_k \in \mathbb{Z}$. Clearly, $|x|_p = \lim_{k\to\infty} p^{m_k} = p^m$ for some $m \in \mathbb{Z}$. □

The *ring of p-adic integers* is defined by

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\}.$$

This is indeed a ring, since for any two $x, y \in \mathbb{Z}_p$ we have $|x-y|_p \leqslant \max(|x|_p, |y|_p) \leqslant 1$, and $|xy|_p \leqslant 1$. Hence $x - y \in \mathbb{Z}_p$ and $xy \in \mathbb{Z}_p$.

The group of units, i.e., invertible elements of $\mathbb{Z}_p$ is equal to

$$\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : \, |x|_p = 1\}.$$

Notice that $\mathbb{Z}_p$ contains $\mathbb{Z}$, but also all numbers in $\mathbb{Q}$ with p-adic absolute value $\leqslant 1$, these are the rational numbers of the form a/b with $a, b \in \mathbb{Z}$ and b not divisible by p. Further, the group $\mathbb{Z}_p^*$ contains all rational numbers with p-adic absolute value 1, these are the numbers of the form a/b with $a, b \in \mathbb{Z}$ and $p \nmid ab$.

For $x, y \in \mathbb{Q}_p$ and $m \in \mathbb{Z}$ we write $x \equiv y \,(\mathrm{mod}\, p^m)$ if $(x-y)/p^m \in \mathbb{Z}_p$. Thus,

$$x \equiv y \,(\mathrm{mod}\, p^m) \Longleftrightarrow |x - y|_p \leqslant p^{-m}.$$

For p-adic numbers, "very small" means "divisible by a high power of p", and two p-adic numbers x and y are p-adically close if and only if $x - y$ is divisible by a high power of p.

The above definition applies also to rational numbers of the form a/b with $a, b \in \mathbb{Z}$ and $p \nmid b$ since these are contained in $\mathbb{Z}_p$. It is not difficult to show that if a_1, a_2, b_1, b_2 are integers with $p \nmid b_1 b_2$ and m is a positive integer, then

$$a_1 \equiv a_2 \,(\mathrm{mod}\, p^m), \;\; b_1 \equiv b_2 \,(\mathrm{mod}\, p^m) \Longrightarrow \frac{a_1}{b_1} \equiv \frac{a_2}{b_2} \,(\mathrm{mod}\, p^m).$$

Lemma 3.2. *For every $\alpha \in \mathbb{Z}_p$ and every positive integer m there is a unique $a_m \in \mathbb{Z}$ such that*

$$\alpha \equiv a_m \,(\mathrm{mod}\, p^m), \quad 0 \leqslant a_m < p^m.$$

Hence $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

Proof. There is a rational number a/b (with coprime $a, b \in \mathbb{Z}$) such that $|\alpha - (a/b)|_p \leqslant p^{-m}$ since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. At most one of a, b is divisible by p and it cannot be b since $|a/b|_p \leqslant 1$. Hence there is an integer a_m with $ba_m \equiv a \pmod{p^m}$ and $0 \leqslant a_m < p^m$. Thus, $\alpha \equiv a/b \equiv a_m \,(\mathrm{mod}\, p^m)$. This shows the existence of a_m. It is unique, since any residue class mod p^m contains only one integer from $\{0, \ldots, p^m - 1\}$. □

We prove some algebraic properties of the ring $\mathbb{Z}_p$.

Theorem 3.3. **(i)** *The non-zero ideals of $\mathbb{Z}_p$ are $p^m\mathbb{Z}_p$ ($m = 0, 1, 2, \ldots$). In particular, $p\mathbb{Z}_p$ is the only maximal ideal of $\mathbb{Z}_p$.*
(ii) *$\mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{Z}/p^m\mathbb{Z}$. In particular, $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.*

Proof. (i). let I be a non-zero ideal of $\mathbb{Z}_p$ and choose $\alpha \in I$ for which $|\alpha|_p$ is maximal. Let $|\alpha|_p = p^{-m}$. Then $p^{-m}\alpha \in \mathbb{Z}_p^*$, hence $p^m \in I$. Further, for $\beta \in I$ we have $|\beta p^{-m}|_p \leqslant 1$, hence $\beta \in p^m\mathbb{Z}_p$. So $I \subset p^m\mathbb{Z}_p$. This implies $I = p^m\mathbb{Z}_p$.

(ii). The homomorphism $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}_p/p^m\mathbb{Z}_p$: residue class of a mod $p^m\mathbb{Z}$ $\mapsto$ residue class of a mod $p^m\mathbb{Z}_p$ is injective since $p^m\mathbb{Z}_p \cap \mathbb{Z} = p^m\mathbb{Z}$. It is also surjective in view of Lemma 3.2. So it is an isomorphism. □

We now show that every element of $\mathbb{Z}_p$ has a "Taylor series expansion," and every element of $\mathbb{Q}_p$ a "Laurent series expansion" where instead of powers of a variable X one takes powers of p.

Theorem 3.4. **(i)** *Every element of $\mathbb{Z}_p$ can be expressed uniquely as $\sum_{k=0}^{\infty} b_k p^k$ with $b_k \in \{0, \ldots, p-1\}$ for $k \geqslant 0$ and conversely, every such series belongs to $\mathbb{Z}_p$.*
(ii) *Every element of $\mathbb{Q}_p$ can be expressed uniquely as $\sum_{k=-k_0}^{\infty} b_k p^k$ with $k_0 \in \mathbb{Z}$ and $b_k \in \{0, \ldots, p-1\}$ for $k \geqslant -k_0$ and conversely, every such series belongs to $\mathbb{Q}_p$.*

Proof. (i). First observe that by Lemma 2.3, a series $\sum_{k=0}^{\infty} b_k p^k$ with $b_k \in \{0, \ldots, p-1\}$ converges in $\mathbb{Q}_p$. Further, it belongs to $\mathbb{Z}_p$, since $|\sum_{k=0}^{\infty} b_k p^k|_p \leqslant \max_{k\geqslant 0} |b_k p^k|_p \leqslant 1$.

Let $\alpha \in \mathbb{Z}_p$ and let $\{a_m\}_{m=1}^{\infty}$ be the sequence from Lemma 3.2. Write these integers in their p-adic expansion. Since $a_{m+1} \equiv a_m \pmod{p^m}$ for $m \geqslant 1$, we have $a_1 = b_0$, $a_2 = b_0 + b_1 p$, $a_3 = b_0 + b_1 p + b_2 p^2, \ldots, a_m = b_0 + b_1 p + \cdots + b_{m-1} p^{m-1}$ where $b_0, b_1, \ldots \in \{0, \ldots, p-1\}$. It follows that

$$\alpha = \lim_{m\to\infty} \sum_{k=0}^{m} b_k p^k = \sum_{k=0}^{\infty} b_k p^k$$

This expansion is unique since the integers a_m are uniquely determined.

(ii). As above, any series $\sum_{k=-k_0}^{\infty} b_k p^k$ with $b_k \in \{0, \ldots, p-1\}$ converges in $\mathbb{Q}_p$. Let $\alpha \in \mathbb{Q}_p$ with $\alpha \neq 0$. Suppose that $|\alpha|_p = p^{k_0}$. Then $\beta := p^{k_0}\alpha$ has $|\beta|_p = 1$, so it belongs to $\mathbb{Z}_p$. Now multiply the p-adic expansion of β with p^{-k_0}. □

Corollary 3.5. *$\mathbb{Z}_p$ is uncountable.*

Proof. Apply Cantor's diagonal method. □

We use the following notation:

$$\begin{aligned} &\alpha = 0.\, b_0 b_1 \dots \ (p) && \text{if } \alpha = \textstyle\sum_{k=0}^{\infty} b_k p^k, \\ &\alpha = b_{-k_0} \cdots b_{-1} \,.\, b_0 b_1 \dots \ (p) && \text{if } \alpha = \textstyle\sum_{k=-k_0}^{\infty} b_k p^k \text{ with } k_0 < 0. \end{aligned}$$

We can describe various of the definitions given above in terms of p-adic expansions. For instance, for $\alpha \in \mathbb{Q}_p$ we have $|\alpha|_p = p^{-m}$ where $\alpha = \sum_{k=m}^{\infty} b_k p^k$ with $b_k \in \{0, \dots, p-1\}$ for $k \geqslant m$ and $b_m \neq 0$. next, if $\alpha = \sum_{k=0}^{\infty} a_k p^k$, $\beta = \sum_{k=0}^{\infty} b_k p^k \in \mathbb{Z}_p$ with $a_k, b_k \in \{0, \dots, p-1\}$, then

$$\alpha \equiv \beta \,(\mathrm{mod}\, p^m) \iff a_k = b_k \text{ for } k < m.$$

For p-adic numbers given in their p-adic expansions, one has the same addition with carry algorithm as for real numbers given in their decimal expansions, except that for p-adic numbers one has to work from left to right instead of right to left. Likewise, one has subtraction and multiplication algorithms for p-adic numbers which are precisely the same as for real numbers apart from that one has to work from left to right instead of right to left.

We describe an algorithm to compute the digits of the p-adic expansion of $\alpha \in \mathbb{Z}_p$. Let

$$\alpha = \sum_{k=0}^{\infty} b_k p^k = \ 0 \,.\, b_0 b_1 b_2 \dots \ (p)$$

with $b_k \in \{0, \dots, p-1\}$. Define

$$\alpha_k := \sum_{m=k}^{\infty} b_m p^{m-k} = \ 0 \,.\, b_k b_{k+1} b_{k+2} \dots \ (p)$$

Then the p-adic integers α_k and digits b_k can be computed inductively as follows:

$\alpha_0 := \alpha$;
For $k = 0, 1, \dots,$ determine b_k such that $\alpha_k \equiv b_k \pmod{p}$ and $b_k \in \{0, \dots, p-1\}$, and compute $\alpha_{k+1} := (\alpha_k - b_k)/p$.

Theorem 3.6. *Let $\alpha = \sum_{k=-k_0}^{\infty} b_k p^k$ with $b_k \in \{0, \dots, p-1\}$ for $k \geqslant -k_0$. Then*

$$\alpha \in \mathbb{Q} \iff \{b_k\}_{k=-k_0}^{\infty} \text{ is ultimately periodic.}$$

Proof. $\Longleftarrow$ Exercise.

$\Longrightarrow$ Without loss of generality, we assume that $\alpha \in \mathbb{Z}_p$ (if $\alpha \in \mathbb{Q}_p$ with $|\alpha|_p = p^{k_0}$, say, then we proceed further with $\beta := p^{k_0}\alpha$ which is in $\mathbb{Z}_p$).

Suppose that $\alpha = A/B$ with $A, B \in \mathbb{Z}$, $\gcd(A, B) = 1$. Then p does not divide B (otherwise $|\alpha|_p > 1$). Let $C := \max(|A|, |B|)$. Let $\{\alpha_k\}_{k=0}^{\infty}$ be the sequence defined above. Notice that α_k determines uniquely the numbers $b_k, b_{k+1}, \ldots$.

Claim. $\alpha_k = A_k/B$ with $A_k \in \mathbb{Z}$, $|A_k| \leqslant C$.

This is proved by induction on k. For $k = 0$ the claim is obviously true. Suppose the claim is true for $k = m$ where $m \geqslant 0$. Then

$$\alpha_{m+1} = \frac{\alpha_m - b_m}{p} = \frac{(A_m - b_m B)/p}{B}.$$

Since $\alpha_m \equiv b_m \pmod{p}$ we have that $A_m - b_m B$ is divisible by p. So $A_{m+1} := (A_m - b_m B)/p \in \mathbb{Z}$. Further,

$$|A_{m+1}| \leqslant \frac{C + (p-1)B}{p} \leqslant C.$$

This proves our claim.

Now since the integers A_k all belong to $\{-C, \ldots, C\}$, there must be indices $l < m$ with $A_l = A_m$, that is, $\alpha_l = \alpha_m$. But then, $b_{k+m-l} = b_k$ for all $k \geqslant l$, proving that $\{b_k\}_{k=0}^{\infty}$ is ultimately periodic. $\square$

Example. We determine the 3-adic expansion of $-\frac{2}{135} = -\frac{2}{5} \cdot 3^{-3}$. We start with the 3-adic expansion of $-\frac{2}{5}$. Notice that $\frac{a}{5} \equiv 2a \pmod{3}$ for $a \in \mathbb{Z}$.

k	0	1	2	3	4
α_k	$-\frac{2}{5}$	$-\frac{4}{5}$	$-\frac{3}{5}$	$-\frac{1}{5}$	$-\frac{2}{5}$
b_k	2	1	0	1	2

It follows that the sequence of 3-adic digits $\{b_k\}_{k=0}^{\infty}$ of $-\frac{2}{5}$ is periodic with period $2, 1, 0, 1$ and that

$$\begin{aligned} -\frac{2}{5} &= 2 \times 3^0 + 1 \times 3^1 + 0 \times 3^2 + 1 \times 3^3 + 2 \times 3^4 + 1 \times 3^5 + 0 \times 3^6 + 1 \times 3^7 + \cdots \\ &= 0\,.2101\,2101\ldots\ (3). \end{aligned}$$

Hence

$$-\frac{2}{135} = 210\,.\,1210\,1210\ \ldots\ (3).$$

Conversely, we can recover the rational number from its expansion. Check that if $|x|_p < 1$ then $1 + x + x^2 + \cdots = 1/(1-x)$. Thus,

$$\begin{aligned} &210\,.\,1210\,1210\,\ldots \quad (3) \\ &\quad = 2\times 3^{-3} + 1\times 3^{-2} + 0\times 3^{-1} + \\ &\qquad\quad + \left(1\times 3^0 + 2\times 3^1 + 1\times 3^2 + 0\times 3^3\right)\left(1 + 3^4 + 3^8 + \cdots\right) \\ &\quad = \frac{5}{27} + \frac{16}{1-3^4} = -\frac{2}{135}. \end{aligned}$$

4. The p-adic topology

The ball with center $a \in \mathbb{Q}_p$ and radius r in the value set $\{0\}\cup\{p^m : m \in \mathbb{Z}\}$ of $|\cdot|_p$ is defined by $B(a,r) := \{x \in \mathbb{Q}_p : |x-a|_p \leqslant r\}$. Notice that if $b \in B(a,r)$ then $|b-a|_p \leqslant r$. So by the ultrametric inequality, for $x \in B(a,r)$ we have $|x-b|_p \leqslant \max(|x-a|_p, |a-b|_p) \leqslant r$, i.e. $x \in B(b,r)$. So $B(a,r) \subseteq B(b,r)$. Similarly one proves $B(b,r) \subseteq B(a,r)$. Hence $B(a,r) = B(b,r)$. In other words, any point in a ball can be taken as center of the ball.

We define the p-adic topology on $\mathbb{Q}_p$ as follows. A subset U of $\mathbb{Q}_p$ is called open if for every $a \in U$ there is $m > 0$ such that $B(a,p^{-m}) \subset U$. It is easy to see that this topology is Hausdorff: if a, b are distinct elements of $\mathbb{Q}_p$, and m is an integer with $p^{-m} < |a-b|_p$, then the balls $B(a,p^{-m})$ and $B(b,p^{-m})$ are disjoint.

But apart from this, the p-adic topology has some strange properties.

Theorem 4.1. *Let $a \in \mathbb{Q}_p$, $m \in \mathbb{Z}$. Then $B(a,p^{-m})$ is both open and compact in the p-adic topology.*

Proof. The ball $B(a,p^{-m})$ is open since for every $b \in B(a,p^{-m})$ we have $B(b,p^{-m}) = B(a,p^{-m})$.

To prove the compactness we modify the proof of the Heine-Borel theorem stating that every closed bounded set in $\mathbb{R}$ is compact. Assume that $B_0 := B(a,p^{-m})$ is not compact. Then there is an infinite open cover $\{U_\alpha\}_{\alpha\in A}$ of B_0 no finite subcollection of which covers B_0. Take $x \in B(a,p^m)$. Then $|(x-a)/p^m|_p \leqslant 1$. Hence there is $b \in \{0,\ldots,p-1\}$ such that $\frac{x-a}{p^m} \equiv b \pmod p$. But then, $x \in B(a+bp^m, p^{-m-1})$. So $B(a,p^m) = \cup_{b=0}^{p-1} B(a+bp^m, p^{-m-1})$ is the union of p balls of radius p^{-m-1}. It follows that there is a ball $B_1 \subset B(a,p^{-m})$ of radius p^{-m-1} which can not be covered by finitely many sets from

$\{U_\alpha\}_{\alpha\in A}$. By continuing this argument we find an infinite sequence of balls $B_0 \supset B_1 \supset B_2 \supset \cdots$, where B_i has radius p^{-m-i}, such that B_i can not be covered by finitely many sets from $\{U_\alpha\}_{\alpha\in A}$.

We show that the intersection of the balls B_i is non-empty. For $i \geqslant 0$, choose $x_i \in B_i$. Thus, $B_i = B(x_i, p^{-m-i})$. Then $\{x_i\}_{i\geqslant 0}$ is a Cauchy sequence since $|x_i - x_j|_p \leqslant p^{-m-\min(i,j)} \to 0$ as $i, j \to \infty$. Hence this sequence has a limit x^* in $\mathbb{Q}_p$. Now we have $|x_i - x^*|_p = \lim_{j\to\infty} |x_i - x_j|_p \leqslant p^{-m-i}$, hence $x^* \in B_i$, and so $B_i = B(x^*, p^{-m-i})$ for $i \geqslant 0$.

The point x^* belongs to one of the sets, U, say, of $\{U_\alpha\}_{\alpha\in A}$. Since U is open, for i sufficiently large the ball B_i must be contained in U. This gives a contradiction. □

Corollary 4.2. *Every non-empty open subset of $\mathbb{Q}_p$ is disconnected.*

Proof. Let U be an open non-empty subset of $\mathbb{Q}_p$. Take $a \in U$. Then $B := B(a, p^{-m}) \subset U$ for some $m \in \mathbb{Z}$. By increasing m we can arrange that B is strictly smaller than U. Now B is open and also $U \setminus B$ is open since B is compact. Hence U is the union of two non-empty disjoint open sets. □

5. P-adic power series

We consider power series

$$f(x) = \sum_{k=0}^{\infty} a_k (x - x_0)^k$$

where $x_0 \in \mathbb{Q}_p$ and $a_k \in \mathbb{Q}_p$ for all k. By Lemma 2.3, we have

$$f(x) \text{ converges on } B(x_0, p^{-m}) \iff \lim_{k\to\infty} |a_k|_p p^{-mk} = 0. \tag{5.1}$$

In particular, $f(x) = \sum_{k=0}^{\infty} a_k x^k$ converges on $\mathbb{Z}_p = B(0, 1)$ if and only if $\lim_{k\to\infty} |a_k|_p = 0$. Consider the set of power series converging on $\mathbb{Z}_p$,

$$\mathcal{O} := \left\{ \sum_{k=0}^{\infty} a_k x^k : a_k \in \mathbb{Z}_p \text{ for } k \geqslant 0, \quad \lim_{k\to\infty} |a_k|_p = 0 \right\}.$$

Then $\mathcal{O}$ is a ring under addition and multiplication of power series. Notice that $\mathcal{O}$ contains $\mathbb{Z}_p[x]$.

Given power series $f = \sum_{k=0}^{\infty} a_k x^k$, $g = \sum_{k=0}^{\infty} b_k x^k \in \mathcal{O}$ and a non-negative integer m, we write $f \equiv g \pmod{p^m}$ if $a_k \equiv b_k \pmod{p^m}$ for all $k \geqslant 0$.

In this section, we prove the following result.

Theorem 5.1 (Strassman)**.** *Let $f(x) = \sum_{k=0}^{\infty} a_k x^k \in \mathcal{O}$ be a power series of which not all coefficients are 0. Let k_0 be the index such that*

$$|a_k|_p \leqslant |a_{k_0}|_p \text{ for } k \leqslant k_0, \quad |a_k|_p < |a_{k_0}|_p \text{ for } k > k_0.$$

Then $f(x)$ has at most k_0 zeros in $\mathcal{O}$.

By dividing f by a_{k_0}, we see that there is no loss of generality to assume that

$$a_{k_0} = 1, \quad a_k \in \mathbb{Z}_p \text{ for } k \leqslant k_0, \quad a_k \in p\mathbb{Z}_p \text{ for } k > k_0. \tag{5.2}$$

We need some lemmas.

Lemma 5.2. *Let R be a ring and g a monic polynomial in $R[x]$. Then for every polynomial $f \in R[x]$ there exist $q, r \in R[x]$ such that*

$$f = qg + r, \quad r = 0 \text{ or } \deg r < \deg g.$$

Proof. This is the usual division with remainder algorithm for polynomials. Since g is monic, it holds for polynomials with coefficients in an arbitrary ring R. □

Lemma 5.3. *Suppose that f satisfies* (5.2)*. Then there are a monic polynomial $g \in \mathbb{Z}_p[x]$ of degree k_0, and $h \in \mathcal{O}$, such that*

$$f = g \cdot h, \quad h \equiv 1 \,(\mathrm{mod}\, p). \tag{5.3}$$

Proof. We prove by induction on m that for $m \geqslant 0$ there are polynomials g_m, h_m such that

$$\begin{cases} f \equiv g_m h_m \,(\mathrm{mod}\, p^{m+1}), \quad g_m \text{ is monic, } \deg g_m = k_0,\ h_m \equiv 1 \,(\mathrm{mod}\, p), \\ g_m \equiv g_{m-1} \,(\mathrm{mod}\, p^m),\ \ h_m \equiv h_{m-1} \,(\mathrm{mod}\, p^m), \end{cases} \tag{5.4}$$

where $g_{-1} = h_{-1} := 0$. Suppose we have constructed such polynomials. Let $0 \leqslant k \leqslant k_0$. Then the coefficients of X^k in $g_0, g_1, \ldots$, form a Cauchy sequence, and thus, they converge to a limit in $\mathbb{Z}_p$. As a consequence, the polynomials g_m converge to a monic polynomial $g \in \mathbb{Z}_p[x]$ of degree k_0. Likewise, for every $k \geqslant 0$, the coefficients of X^k in h_m form a Cauchy sequence and thus converge to a limit in $\mathbb{Z}_p$. We note that the degrees of the polynomials h_m may increase to ∞. As a consequence, the polynomials h_m converge to a power series $h \in \mathcal{O}$. We have $h \equiv 1 \,(\mathrm{mod}\, p)$ since $h_m \equiv 1 \,(\mathrm{mod}\, p)$ for all m. The

coefficients of $f - g_m h_m$ converge to the coefficients of $f - gh$ and on the other hand to 0. Hence $f = g \cdot h$.

We now come to the construction of the polynomials g_m, h_m. Note that (5.4) holds for $m = 0$ with $g_0 := \sum_{k=0}^{k_0} a_k x^k$, $h_0 = 1$. Assume that (5.4) holds for some $m \geqslant 0$. We have to construct g_{m+1}, h_{m+1} such that (5.4) holds for $m+1$ instead of m.

We truncate f after an index k_1 such that $|a_k|_p \leqslant p^{-m-2}$ for $k > k_1$, that is, we take $f_1 := \sum_{k=0}^{k_1} a_k x^k$. Then $f \equiv f_1 \,(\mathrm{mod}\, p^{m+2})$, and thus, $f_1 \equiv g_m h_m \,(\mathrm{mod}\, p^{m+1})$. This implies that there is a polynomial $a \in \mathbb{Z}_p[x]$ such that

$$f_1 = g_m h_m + p^{m+1} a.$$

By Lemma 5.2, there are polynomials $q, r \in \mathbb{Z}_p[X]$ such that

$$a = q g_m + r, \quad \text{with } r = 0 \text{ or } \deg r < \deg g_m.$$

Now take

$$g_{m+1} := g_m + p^{m+1} r, \quad h_{m+1} := h_m + p^{m+1} q.$$

Then we have the following congruences modulo p^{m+2}:

$$\begin{aligned} f - g_{m+1} h_{m+1} &\equiv f_1 - (g_m + p^{m+1} r)(h_m + p^{m+1} q) \\ &\equiv g_m h_m + p^{m+1} a - g_m h_m - p^{m+1}(q g_m + r h_m) - p^{2m+2} q r \\ &\equiv p^{m+1}(a - q g_m - r h_m) \\ &\equiv p^{m+1}(a - q g_m - r - r(h_m - 1)) \\ &\equiv 0 \,(\mathrm{mod}\, p^{m+2}). \end{aligned}$$

Hence g_{m+1}, h_{m+1} satisfy (5.4) with $m+1$ instead of m. This completes our induction step, and the proof of our lemma. □

Proof of Theorem 5.1. Take g, h as in Lemma 5.3. Clearly, for $x \in \mathbb{Z}_p$ we have $h(x) \equiv 1 \,(\mathrm{mod}\, p)$, hence $h(x) \neq 0$. Therefore, the zeros of f in $\mathbb{Z}_p$ are those of g. So f has at most $\deg g = k_0$ zeros in $\mathbb{Z}_p$. □

6. Algebraic extensions of $\mathbb{Q}_p$

The completion $\mathbb{R}$ of $\mathbb{Q}$ with respect to the ordinary absolute value has only one non-trivial algebraic extension, namely $\mathbb{C}$. Further, the ordinary absolute value $|\cdot|$ on $\mathbb{R}$ has precisely one extension to $\mathbb{C}$, given by $|\alpha| := |\alpha \cdot \overline{\alpha}|^{1/2} = |N_{\mathbb{C}/\mathbb{R}}(\alpha)|^{1/2}$ for $\alpha \in \mathbb{C}$.

In contrast, $\mathbb{Q}_p$ has finite extensions of arbitrarily large degrees: for instance, for every positive integer d, $X^d - p$ is irreducible in $\mathbb{Q}_p[X]$ and thus, $\mathbb{Q}_p$ has an algebraic extension of degree d. An interesting fact is, that for every positive integer d, $\mathbb{Q}_p$ has up to isomorphism only finitely many extensions of degree d. We state without proofs some results on the extension of $|\cdot|_p$ to finite extensions of $\mathbb{Q}_p$.

Let K be a finite extension of $\mathbb{Q}_p$ of degree d, say. Completely similarly as for algebraic number fields, there is $\alpha \in K$ such that $K = \mathbb{Q}_p(\alpha)$. Let $f(X) = X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Q}_p[X]$ be the minimal polynomial of α over $\mathbb{Q}_p$. Let $\alpha_1, \ldots, \alpha_d$ be the distinct zeros of f in the algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$. These give rise to precisely d distinct $\mathbb{Q}_p$-embeddings (i.e., injective homomorphisms leaving elements of $\mathbb{Q}_p$ unchanged) of K in $\overline{\mathbb{Q}_p}$, say $\sigma_1, \ldots, \sigma_d$ with $\sigma_i(\alpha) = \alpha_i$ for $i = 1, \ldots, d$.

We define the *norm* of K over $\mathbb{Q}_p$ by

$$N_{K/\mathbb{Q}_p}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha) \quad \text{for } \alpha \in K.$$

We state without proof the following result.

Theorem 6.1. *Let K be a finite extension of $\mathbb{Q}_p$. Then $|\cdot|_p$ can be continued in precisely one way to K, and K is complete with respect to this continuation. If we denote this continuation also by $|\cdot|_p$, then we have*

$$|\alpha|_p = |N_{K/\mathbb{Q}_p}(\alpha)|_p^{1/[K:\mathbb{Q}_p]} \text{ for } \alpha \in K.$$

One can show that if $\mathbb{Q}_p(\alpha) = K$ and $f(X) = X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Q}_p[X]$ is the minimal polynomial of α over $\mathbb{Q}_p$, then

$$N_{K/\mathbb{Q}_p}(\alpha) = (-1)^d a_d.$$

More generally, if $\mathbb{Q}_p(\alpha) \neq K$, then the degree d of f divides $[K : \mathbb{Q}_p]$, and we have

$$N_{K/\mathbb{Q}_p}(\alpha) = \big((-1)^d a_d\big)^{[K:\mathbb{Q}_p]/d}.$$

This yields

$$|\alpha|_p = |a_d|_p^{1/d}. \tag{6.1}$$

Given a finite extension K of $\mathbb{Q}_p$, we define the ring of p-adic integers of K,

$$O_{p,K} := \{\alpha \in K : |\alpha|_p \leqslant 1\}.$$

Then

$$m_{p,K} := \{\alpha \in K : |\alpha|_p < 1\}$$

is a maximal ideal of $O_{p,K}$ and

$$O_{p,K}/m_{p,K}$$

is a field, the *residue class field* of K.

Let $d := [K : \mathbb{Q}_p]$. Then the value group $|K^*|_p := \{|\alpha|_p : \alpha \in K^*\}$ is a subgroup of the multiplicative cyclic group generated by $p^{-1/d}$. So $|K^*|_p$ is generated by p^{-1/e_K} for some positive divisor e_K of d. We call e_K the *ramification index* of K.

One can show that $O_{p,K}/m_{p,K}$ is a finite extension of $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$. The degree $f_K := [O_{p,K}/m_{p,K} : \mathbb{Z}_p/p\mathbb{Z}_p]$ is called the *residue class degree* of K. We state without proof the following results. Given $\alpha \in O_{p,K}$, we write $\overline{\alpha}$ for the corresponding residue class in $O_{p,K}/m_{p,K}$.

Theorem 6.2. *Let K be a finite extension of $\mathbb{Q}_p$ with ramification index $e = e_K$ and residue class degree $f = f_K$.*
(i) $[K : \mathbb{Q}_p] = e \cdot f$.
(ii) *Let π be an element of $O_{p,K}$ with $|\pi|_p = p^{-1/e}$, and let $\omega_1, \ldots, \omega_f$ be elements of $O_{p,K}$ such that $\overline{\omega_1}, \ldots, \overline{\omega_f}$ form a basis of $O_{p,K}/m_{p,K}$ over $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$. Then $O_{p,K}$ is a free $\mathbb{Z}_p$-module with basis*

$$\{\pi^i\omega_j : i = 0, \ldots, e-1,\ j = 1, \ldots, f\},$$

i.e., every element of $O_{p,K}$ can be expressed uniquely in the form

$$\sum_{i=0}^{e-1}\sum_{j=1}^{f} x_{ij}\pi^i\omega_j \quad \text{with } x_{ij} \in \mathbb{Z}_p.$$

Examples.
1. Let $K = \mathbb{Q}_3(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}_3\}$, where $\sqrt{3}$ is one of the roots of $X^2 - 3$. Notice that $\sqrt{3} \notin \mathbb{Q}_3$. For $|\sqrt{3}|_3^2 = 3^{-1}$, hence $|\sqrt{3}|_3$ does not belong to the value set of $|\cdot|_3$ on $\mathbb{Q}_3$. In general, we have for $a, b \in \mathbb{Q}_3$,

$$\begin{aligned} |a + b\sqrt{3}|_3 &= |N_{\mathbb{Q}_3(\sqrt{3})/\mathbb{Q}_3}(a + b\sqrt{3})|_3^{1/2} = |a^2 - 3b^2|_3^{1/2} \\ &= \max(|a|_3,\ 3^{-1/2}|b|_3). \end{aligned}$$

This implies

$$\begin{aligned} O_{3,K} &= \{a + b\sqrt{3} : a, b \in \mathbb{Z}_3\}, \\ m_{3,K} &= \{a + b\sqrt{3} : a \in 3\mathbb{Z}_3,\, b \in \mathbb{Z}_3\} = \sqrt{3}O_{3,K}, \\ O_{3,K}/m_{3,K} &\cong \mathbb{Z}_3/3\mathbb{Z}_3 = \mathbb{F}_3. \end{aligned}$$

This confirms that $e_K = 2$, $f_K = 1$.

2. Let $K = \mathbb{Q}_3(i) = \{a + bi : a, b \in \mathbb{Q}_3\}$, where i is a root of $X^2 + 1$. The polynomial $X^2 + 1$ does not have roots modulo 3, so it is irreducible in $\mathbb{Q}_3[X]$. We have for $a, b \in \mathbb{Q}_3$,

$$|a + bi|_3 = |a^2 + b^2|_3^{1/2} = \max(|a|_3, |b|_3),$$

hence

$$\begin{aligned} O_{3,K} &= \{a + bi : a, b \in \mathbb{Z}_3\}, \\ m_{3,K} &= \{a + bi : a, b \in 3\mathbb{Z}_3\} = 3O_{3,K}, \\ O_{3,K}/m_{3,K} &= \{a + bi : a, b \in \mathbb{F}_3\} = \mathbb{F}_3(i). \end{aligned}$$

This confirms that $e_K = 1, f_K = 2$.

We can extend $|\cdot|_p$ to the algebraic closure $\overline{\mathbb{Q}_p}$: given $\alpha \in \overline{\mathbb{Q}_p}$, take any finite extension K of $\mathbb{Q}_p$ containing α and put

$$|\alpha|_p := |N_{K/\mathbb{Q}_p}(\alpha)|_p^{1/[K:\mathbb{Q}_p]}.$$

(6.1) gives an alternative expression which is independent of the choice of K. We finish with stating some facts without proof.

Theorem 6.3. (i) $\overline{\mathbb{Q}_p}$ *is* **not** *complete with respect to* $|\cdot|_p$.
(ii) *The completion* $\mathbb{C}_p$ *of* $\overline{\mathbb{Q}_p}$ *with respect to* $|\cdot|_p$ *is algebraically closed.*

7. The zero set of a linear recurrence sequence

The Norwegian mathematician Thoralf Skolem introduced techniques from p-adic analysis to prove results on Diophantine equations. As an example we prove a result on linear recurrence sequences.

A *linear recurrence sequence* in $\mathbb{C}$ is a sequence $U = \{u_k\}_{k=0}^{\infty}$ given by a *linear recurrence*

$$u_n = c_1 u_{n-1} + \cdots + c_k u_{n-k} \quad (n \geqslant k) \tag{7.1}$$

with coefficients $c_1, \ldots, c_k \in \mathbb{C}$ and $c_k \neq 0$, and by *initial values*

$$u_0, \ldots, u_{k-1} \in \mathbb{C}. \tag{7.2}$$

The linear recurrence relation satisfied by U is not uniquely determined. It is however not difficult to show that there is only one linear recurrence relation of minimal length satisfied by U. This minimal length is called the *order* of U.

Let (7.1) be the linear recurrence of minimal length satisfied by U. Then the polynomial

$$f_U(X) := X^k - c_1 X^{k-1} - \cdots - c_k \tag{7.3}$$

is called the *companion polynomial* of f.

Remark. Denote by I_U the set of polynomials $a_0 X^m + a_1 X^{m-1} + \cdots + a_m \in \mathbb{C}[X]$ such that

$$a_0 u_n + a_1 u_{n-1} + \cdots + a_m u_{n-m} = 0 \text{ for all } n \geqslant m.$$

Then I_U is an ideal of the polynomial ring $\mathbb{C}[X]$ generated by f_U, i.e., all polynomials in I_U are divisible by f_U, see Exercise 10.

Theorem 7.1. *Let $f = X^k - c_1 X^{k-1} - \cdots - c_k \in \mathbb{C}[X]$ with $c_k \neq 0$. Suppose that f factorizes over $\mathbb{C}$ as*

$$f = (X - \alpha_1)^{e_1} \cdots (X - \alpha_t)^{e_t}, \tag{7.4}$$

where $\alpha_1, \ldots, \alpha_t$ are distinct, and $e_1, \ldots, e_t$ are positive integers. let $U = \{u_n\}_{n=0}^{\infty}$ be a sequence in $\mathbb{C}$. Then the following two assertions are equivalent:

(i) U satisfies

$$u_n = c_1 u_{n-1} + c_2 u_{n-2} + \cdots + c_k u_{n-k} \quad (n \geqslant k). \tag{7.1}$$

(ii) There are polynomials $f_1, \ldots, f_t \in \mathbb{C}[X]$ of degrees at most $e_1 - 1, \ldots, e_t - 1$, respectively such that

$$u_n = \sum_{h=1}^{t} f_h(n) \alpha_h^n \quad \text{for } n \geqslant 0. \tag{7.5}$$

Moreover, the polynomials $f_1, \ldots, f_t$ are uniquely determined by U.

Proof. We first show that (i) implies (ii). Take a sequence U with (7.1). Define the $k \times k$-matrix

$$A = \begin{pmatrix} 0 & 1 & & & 0 \\ & 0 & 1 & & 0 \\ & & & \ddots & \\ & & & & 1 \\ c_k & c_{k-1} & \cdots & \cdots & c_1 \end{pmatrix}$$

For $n \geqslant 0$ let $\mathbf{u}_n := (u_n, \ldots, u_{n+k-1})^T$. Then $\mathbf{u}_{n+1} = A\mathbf{u}_n$ for $n \geqslant 0$ and thus,

$$\mathbf{u}_n = A^n \mathbf{u}_0 \quad \text{for } n \geqslant 0. \tag{7.6}$$

Check that the characteristic polynomial of A is $\det(XI - A) = f(X)$. There is a non-singular matrix C such that $A = C^{-1}JC$, where J is a Jordan Normal Form of A. We may take

$$J = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_t \end{pmatrix}$$

where for $h = 1, \ldots, t$, J_h is the Jordan block of order e_h associated with α_h, i.e.,

$$J_h = \begin{pmatrix} \alpha_h & 1 & & \\ & \alpha_h & 1 & \\ & & \ddots & 1 \\ & & & \alpha_h \end{pmatrix} = \alpha_h \cdot \begin{pmatrix} 1 & \alpha_h^{-1} & & \\ & 1 & \alpha_h^{-1} & \\ & & \ddots & \alpha^{-1} \\ & & & 1 \end{pmatrix}.$$

By induction on n we have

$$J_h^n = \alpha_h^n \cdot \begin{pmatrix} \binom{n}{0} & \binom{n}{1}\alpha_h^{-1} & \cdots & \binom{n}{e_h-1}\alpha_h^{-e_h+1} \\ & \binom{n}{0} & \cdots & \binom{n}{e_h-2}\alpha_h^{-e_h+2} \\ & & \ddots & \vdots \\ & & & \binom{n}{0} \end{pmatrix}.$$

This implies that $A^n = C^{-1}J^nC = \Big(E_{ij}(n)\Big)_{i,j=1,\ldots,k}$, where

$$E_{ij}(n) = \sum_{h=1}^{t} f_h^{(ij)}(n)\alpha_h^n \quad \text{with } f_h^{(ij)} \in \mathbb{C}[X], \deg f_h^{(ij)} \leqslant e_h - 1.$$

By substituting this into (7.6) and taking the first coordinate, we get (7.5) with some polynomials $f_1, \ldots, f_t$ of degrees at most $e_1 - 1, \ldots, e_t - 1$, respectively. This implies (ii).

We still have to prove (ii)$\Longrightarrow$(i) and the unicity of $f_1, \ldots, f_t$. Let V be the set of sequences U satisfying (7.1). Then V is a complex vector space. Its dimension is k, since any k-tuple of initial values $u_0, \ldots, u_{k-1} \in \mathbb{C}$ can be extended uniquely to a sequence U satisfying (7.1). Next, let W be the set of sequences U satisfying (7.5) for certain polynomials $f_1, \ldots, f_t$ of degrees at most $e_1 - 1, \ldots, e_t - 1$, respectively. Also W is a complex vector space, generated by the sequences $\{n^j \alpha_h^n\}_{n=0}^{\infty}$, for $h = 1, \ldots, t$, $j = 0, \ldots, e_h - 1$. Note that the number of these generators is $e_1 + \cdots + e_t = k$; so W has dimension $\leqslant k$. We have just shown that $V \subseteq W$. Hence W must have dimension equal to $k = \dim V$ and so, $V = W$. This implies the equivalence of (i) and (ii). Further, $\{n^j \alpha_h^n\}_{n=0}^{\infty}$, $(h = 1, \ldots, t, j = 0, \ldots, e_h - 1)$ must form a basis of $W = V$. Hence any sequence in V can be expressed uniquely in the form (7.5). This completes our proof. □

Corollary 7.2. *Let again*

$$f = X^k - c_1 X^{k-1} - \cdots - c_k = (X - \alpha_1)^{e_1} \cdots (X - \alpha_t)^{e_t} \in \mathbb{C}[X],$$

where $c_k \neq 0$, $\alpha_1, \ldots, \alpha_t$ are distinct, and $e_1 > 0, \ldots, e_t > 0$, and let $U = \{u_n\}_{n=0}^{\infty}$ be a sequence in $\mathbb{C}$. Then the following two assertions are equivalent:

(i) U is a linear recurrence sequence with companion polynomial f.

(ii) There are polynomials $f_1, \ldots, f_t \in \mathbb{C}[X]$ of degrees exactly $e_1 - 1, \ldots, e_t - 1$, respectively such that

$$u_n = \sum_{h=1}^{t} f_h(n) \alpha_h^n \quad \text{for } n \geqslant 0. \tag{7.5}$$

Proof. First assume that U has companion polynomial f. Then $k := \deg f$ is the length of the minimal recurrence satisfied by U. By Theorem 7.1 we know that $u_n = \sum_{h=1}^{t} f_h(n) \alpha_n$ with $\deg f_h =: e'_h - 1 \leqslant e_h - 1$ for $h = 1, \ldots, t$. Then again by Theorem 7.1, U satisfies a linear recurrence of length $e'_1 + \cdots + e'_t$ corresponding to the polynomial $(X - \alpha_1)^{e'_1} \cdots (X - \alpha_t)^{e'_t}$. So $e'_1 + \cdots e'_t \geqslant k$. Hence $e'_h = e_h$ for $h = 1, \ldots, t$.

Conversely, let $U = \{u_n\}$ with $u_n = \sum_{h=1}^{t} f_h(n) \alpha_h^n$ where $\deg f_h = e_h - 1$ for $h = 1, \ldots, t$. By Theorem 7.1, U satisfies (7.1). By the above remark, the companion polynomial of U divides f, so it is of the shape $(X - \alpha_1)^{e'_1} \cdots (X - \alpha_t)^{e'_t}$ with $e'_h \leqslant e_h$, say. But then, by Theorem 7.1, f_h has degree at most

$e'_h - 1$, for $h = 1, \ldots, t$. Hence $e'_h = e_h$ for $h = 1, \ldots, t$, and the companion polynomial of U is f. □

We are interested in the zero set of a linear recurrence sequence,

$$Z_U := \{n \in \mathbb{Z}_{\geqslant 0} :, u_n = \sum_{h=1}^{t} f_h(n)\alpha_h^n = 0\}. \tag{7.7}$$

Equations of the shape $\sum_{h=1}^{t} f_h(n)\alpha_h^n = 0$ are called *exponential-polynomial equations.*

Example. Let U be given by

$$u_n := \tfrac{1}{2}\left(2^n + (-2)^n\right) + (n-1)\left(\frac{\omega^{n+1} - \omega^{-n-1}}{\omega - \omega^{-1}}\right) \quad (\omega = e^{2\pi i/3}).$$

By Corollary 7.2, U has companion polynomial

$$(X-2)(X+2)(X-\omega)^2(X-\omega^{-1})^2 = X^6 + 2X^5 - X^4 - 6X^3 - 11X^2 - 8X - 4,$$

so it is a linear recurrence sequence of order 6.
By considering $n \equiv 0 \pmod 6$, $n \equiv 1 \pmod 6, \ldots$ one verifies that

$$Z_U = \{0, 1\} \cup \{n \in \mathbb{Z}_{\geqslant 0} : n \equiv 5 \pmod 6\}$$

(check this). This example was specifically constructed to make it easy to compute the set Z_U. In case that $k := \deg f_U \leqslant 3$ and the α_i and the coefficients of the f_i are algebraic numbers there exists an algorithm to determine the set Z_U which is based on lower bounds for linear forms in logarithms. But for $k > 3$ such an algorithm is not known.

The next theorem describes the structure of the set of solutions of (7.7). It was proved first by Skolem in 1934 for the case that U is a sequence in $\mathbb{Z}$, then by Mahler in 1935 for the case that U consists of algebraic numbers, and finally, in 1953 by Lech for arbitrary linear recurrence sequences in $\mathbb{C}$.

Theorem 7.3 (Skolem, Mahler, Lech)**.** *The set Z_U is either finite, or a union of a finite set and a finite number of infinite arithmetic sequences.*

Under an additional hypothesis, it can be shown that there are no infinite arithmetic sequences in Z_U, and thus, that the set of solutions is finite.

Corollary 7.4. *Let $t \geqslant 2$. Suppose that the polynomials f_i in (7.7) are non-zero, and that none of the quotients α_i/α_j $(1 \leqslant i < j \leqslant t)$ is a root of unity. Then the set Z_U is finite.*

Proof. Suppose that Z_U contains an infinite arithmetic sequence, say $\{a+dm : m \in \mathbb{Z}_{\geqslant 0}\}$. That is,

$$v_m := \sum_{h=1}^{t} g_h(m)\beta_h^m = 0 \text{ for all } m \in \mathbb{Z}_{\geqslant 0},$$

where

$$g_h(X) = f_h(a + dX)\alpha_h^a,\ \beta_h = \alpha_h^d.$$

If any two numbers β_i, β_j were equal, we would have $(\alpha_i/\alpha_j)^d = 1$, contradicting our assumption. Hence $\beta_1, \ldots, \beta_t$ are distinct. Theorem 7.1 implies that the polynomials $g_1, \ldots, g_t$ are identically 0, hence the polynomials $f_1, \ldots, f_t$ are identically 0, which is again against our assumption. □

To prove Theorem 7.3, we want to apply techniques from p-adic analysis. For this, we have to map U to a sequence in $\mathbb{Q}_p$.

Denote by $\{v_1, \ldots, v_m\}$ the set of coefficients of the polynomials $f_1, \ldots, f_t$ in (7.5), and let

$$K = \mathbb{Q}(v_1, \ldots, v_m, \alpha_1, \ldots, \alpha_t)$$

be the field generated by the v_i and the α_h, i.e., consisting of all expressions f/g where f, g are polynomials in the v_i and α_h with coefficients from $\mathbb{Q}$. Clearly, $u_n \in K$ for all $n \geqslant 0$. Note that a priori the v_i and α_h are just complex numbers, with the $\alpha_h \neq 0$. So these numbers may be algebraic or transcendental.

First suppose that $v_1, \ldots, v_m$, $\alpha_1, \ldots, \alpha_t$ are algebraic, i.e., K is an algebraic number field. Similarly as one may embed K in $\mathbb{C}$, one may embed K in any algebraically closed field that contains $\mathbb{Q}$. So in particular, one may embed K in $\overline{\mathbb{Q}_p}$ for any prime number p. Thus, we can map the sequence U to a sequence in $\overline{\mathbb{Q}_p}$ with the same set of zeros, and apply techniques from p-adic analysis on $\overline{\mathbb{Q}_p}$.

The Chebotarev density theorem from algebraic number theory implies that there are infinitely many primes p such that K can be embedded in $\mathbb{Q}_p$. Thus, by choosing the prime p appropriately, we can work also on $\mathbb{Q}_p$ itself instead of an algebraic extension.

Now assume that not all $v_1, \ldots, v_m$, $\alpha_1, \ldots, \alpha_t$ are algebraic. Lech showed that also in this general case, there are infinitely many primes p, such that the field K can be embedded in $\mathbb{Q}_p$. We leave aside the intricate proof of this fact.

Thus, in all cases, the sequence U can be mapped to a sequence of which the coefficients of the polynomials f_h and the numbers α_h all lie in $\mathbb{Q}_p$. In fact, by a careful choice of the prime p we can see to it that

$$f_h \in \mathbb{Z}_p[X],\ \alpha_h \in \mathbb{Z}_p^* \ \text{ for } h = 1, \ldots, t.$$

This is what we assume henceforth.

The idea of the proof is then to define a power series

$$u(x) := \sum_{h=1}^{t} f_h(x)\alpha_h^x$$

and to apply Theorem 5.1, to get a hand on the zeros in $\mathbb{Z}_p$. The problem is that for this, we have to define α_h^x as a power series and this is not always possible.

In analogy to the well-known expansion over $\mathbb{R}$ or $\mathbb{C}$, we define

$$(1+\beta)^x = \sum_{k=0}^{\infty} \binom{x}{k} \beta^k \ \text{ for } \beta, x \in \mathbb{Z}_p \text{ with } |\beta|_p \leqslant 1/p,$$

where

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}.$$

Notice that for $x = n$ a non-negative integer, this coincides with the usual definition for $(1+\beta)^n$.

We show that the series converges. Choose a sequence of positive integers $x_n \to x$. Then $\binom{x_n}{k} \to \binom{x}{k}$ since also in the p-adic setting, polynomials are continuous. The numbers $\binom{x_n}{k}$ are all integers, so $\binom{x}{k} \in \mathbb{Z}_p$. This implies that $|\binom{x}{k}\beta^k|_p \leqslant |\beta^k|_p \to 0$ as $k \to \infty$. Hence indeed, the series converges.

We want to express $(1+\beta)^x$ as a power series in x. Put $r := 1$ if $p > 2$, $r := 2$ if $p = 2$.

Lemma 7.5. . *Suppose that $|\beta|_p \leqslant p^{-r}$. Then there is a power series expansion*

$$(1+\beta)^x = \sum_{k=0}^{\infty} c_k x^k$$

which converges for $x \in \mathbb{Z}_p$.

Proof. Assume that we have shown that $|\beta^k/k!|_p \to 0$ as $k \to \infty$. Let $x \in \mathbb{Z}_p$. Then

$$\begin{aligned}(1+\beta)^x &= \sum_{k=0}^{\infty} \frac{\beta^k}{k!} x(x-1)\cdots(x-k+1) \\ &= \sum_{k=0}^{\infty} \frac{\beta^k}{k!} \sum_{j=0}^{k} a_{kj} x^j \quad \text{with } a_{kj} \in \mathbb{Z} \\ &= \sum_{j=0}^{\infty} \left(\sum_{k=j}^{\infty} \frac{\beta^k}{k!} a_{kj} \right) x^j.\end{aligned}$$

Interchanging the summations is allowed by Lemma 2.6, and the expressions between the parentheses converge. This yields our power series expression.

It remains to show that $|\beta^k/k!|_p \to 0$ as $k \to \infty$. We first estimate $|k!|_p$. Among $\{1, \ldots, k\}$ there are precisely $[k/p]$ multiples of p which together contribute $[k/p]$ factors p to the prime factorization of $k!$. Further, among these integers there are precisely $[k/p^2]$ multiples of p^2 which contribute another $[k/p^2]$ factors p; and so on. Thus, the maximal power of p dividing $k!$ is

$$[k/p] + [k/p^2] + [k/p^3] + \cdots < \frac{k}{p-1},$$

and so, $|\beta^k/k!|_p \leqslant p^{k/(p-1)-kr} \to 0$ as $k \to \infty$. This completes our proof. □

We are now ready to complete the proof of Theorem 7.3. Put again $r = 1$ if $p > 2$ and $r = 2$ if $p = 2$. Further, set $D = p - 1$ if $p > 2$ and $D = 2$ if $p = 2$. Then the unit group $(\mathbb{Z}_p/p^r\mathbb{Z}_p)^*$ has order D. This implies that $\alpha_h^D \equiv 1 \pmod{p^r}$, i.e., $\alpha_h^D = 1 + \beta_h$ with $|\beta_h|_p \leqslant p^{-r}$. We now split up Z_U into residue classes modulo D, i.e., we consider the sets

$$Z_a := \{m \in \mathbb{Z}_{\geqslant 0} : \, u_{a+Dm} = 0\} \quad \text{for } a = 0, \ldots, D-1.$$

Now indeed,

$$u_a(x) := \sum_{h=1}^{t} f_i(a+Dx)\alpha_h^{a+Dx} = \sum_{h=1}^{t} f_i(a+Dx)\alpha_h^a(1+\beta_h)^x$$

is a power series converging on $\mathbb{Z}_p$ with $u_a(m) = u_{a+Dm}$ for $m \in \mathbb{Z}_{\geqslant 0}$. By Theorem 5.1, $u_a(x)$ is either identically 0, or it has only finitely many zeros on $\mathbb{Z}_p$. This implies that either $Z_a = \mathbb{Z}_{\geqslant 0}$, or is finite. As a consequence, the

solution set of (7.7) is indeed the union of a finite set and finitely many infinite arithmetic sequences. □

An important problem is to estimate the cardinality of the finite set and of the number of arithmetic sequences that occur in the set of solutions of (7.7). The following result is due to W.M. Schmidt. Let U be a linear recurrence sequence in $\mathbb{C}$ of order k. Let $A(U)$ denote the cardinality of the finite set in Z_U, and $B(U)$ the number of arithmetic sequences in Z_U. Then

$$A(U) + B(U) \leqslant \exp\exp\exp(20k).$$

The importance of this bound is that it depends only on k and not on any other parameter. It is very likely far from best possible. Schmidt's very difficult proof does not use p-adic analysis like above, but is based on Diophantine approximation.

We give an application to *cubic Thue equations.* Let $f(X) = X^3 + aX^2 + bX + c$ be an irreducible polynomial in $\mathbb{Z}[X]$ with one real root, say α_1 and two complex roots α_2, $\alpha_3 = \overline{\alpha_2}$. Consider the equation

$$F(x,y) = x^3 + ax^2y + bxy^2 + cy^3 = 1 \text{ in } x, y \in \mathbb{Z}. \tag{7.8}$$

Theorem 7.6. *Eq.* (7.8) *has only finitely many solutions.*

Proof. Let $K = \mathbb{Q}(\alpha_1)$. Then K is a cubic field with one real embedding and two complex embeddings. Then the unit group $\mathcal{O}_K^*$ has rank 1. That is, there is η_1 such that $\mathcal{O}_K^* = \{\pm\eta_1^n : n \in \mathbb{Z}\}$. Let (x, y) be a solution of (7.8). The conjugates of $x - \alpha_1 y$ are $x - \alpha_i y$ for $i = 1, 2, 3$. Hence

$$N_{K/\mathbb{Q}}(x - \alpha_1 y) = \prod_{i=1}^{3}(x - \alpha_i y) = F(x, y) = 1.$$

So $x-\alpha_1 y$ is a unit, i.e., $x-\alpha_1 y = \pm\eta_1^n$ for some $n \in \mathbb{Z}$. Then also $x-\alpha_i y = \pm\eta_i^n$ for $i = 1, 2, 3$. We use the identity

$$(\alpha_2 - \alpha_3)(x - \alpha_1 y) + (\alpha_3 - \alpha_1)(x - \alpha_2 y) + (\alpha_1 - \alpha_2)(x - \alpha_3 y) = 0.$$

This implies

$$(\alpha_2 - \alpha_3)\eta_1^n + (\alpha_3 - \alpha_1)\eta_2^n + (\alpha_1 - \alpha_2)\eta_3^n = 0.$$

We leave as Exercise 13 to prove that none of the quotients η_i/η_j $(i \neq j)$ is a root of unity. Then by Corollary 7.4, this last equation has only finitely many solutions $n \in \mathbb{Z}_{\geqslant 0}$. We prove in the same manner that there are only finitely

many solutions $n < 0$ by applying 7.4 again, but now with η_i^{-1} instead of η_i and taking $n' := -n > 0$. As a consequence, the equation $F(x, y) = 1$ has only finitely many solutions. □

8. Exercises.

In the exercises below, p always denotes a prime number and convergence is with respect to $|\cdot|_p$.

Exercise 1.

(a) Determine the p-adic expansion of -1.
(b) Let $\alpha = \sum_{k=0}^{\infty} b_k p^k$ with $b_k \in \{0, \ldots, p-1\}$ for $k \geqslant 0$. Determine the p-adic expansion of $-\alpha$.

Exercise 2.

(a) Let $\alpha \in \mathbb{Q}_p$. Prove that α has a finite p-adic expansion if and only if $\alpha = a/p^r$ where a is a positive integer and r a non-negative integer.
(b) Let $\alpha = \sum_{k=-k_0}^{\infty} b_k p^k$ where $b_k \in \{0, \ldots, p-1\}$ for $k \geqslant -k_0$. Suppose that the sequence $\{b_k\}_{k=-k_0}^{\infty}$ is ultimately periodic, i.e., there exist r, s with $s > 0$ such that $b_{k+s} = b_s$ for all $k \geqslant r$. Prove that $\alpha \in \mathbb{Q}$.
Hint. Prove first that $\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k$ for all $x \in \mathbb{Z}_p$ with $|x|_p \leqslant p^{-1}$.

Exercise 3. In this exercise you are asked to work out a p-adic analogue of Newton's method to approximate the roots of a polynomial. Let $f = a_0 X^n + \cdots + a_0 \in \mathbb{Z}_p[X]$. The derivative of f is $f' = n a_0 X^{n-1} + \cdots + a_1$.

(a) Let $a, x \in \mathbb{Z}_p$ and suppose that $x \equiv 0 \pmod{p^m}$ for some positive integer m. Prove that $f(a + x) \equiv f(a) \pmod{p^m}$ and $f(a + x) \equiv f(a) + f'(a)x \pmod{p^{2m}}$.
Hint. Use that $f(a + X) \in \mathbb{Z}_p[X]$.
(b) Let $x_0 \in \mathbb{Z}$ such that $f(x_0) \equiv 0 \pmod{p}$, $f'(x_0) \not\equiv 0 \pmod{p}$. Define the sequence $\{x_n\}_{n=0}^{\infty}$ recursively by

$$x_{n+1} := x_n - \frac{f(x_n)}{f'(x_n)} \quad (n \geqslant 0).$$

Prove that $x_n \in \mathbb{Z}_p$, $f(x_n) \equiv 0 \pmod{p^{2^n}}$, $f'(x_n) \not\equiv 0 \pmod{p}$ for $n \geqslant 0$.
(c) Prove that x_n converges to a zero of f in $\mathbb{Z}_p$.
(d) Prove that f has precisely one zero $\xi \in \mathbb{Z}_p$ such that $\xi \equiv x_0 \pmod{p}$.

Exercise 4. Denote by $\mathbb{C}((t))$ the field of formal Laurent series

$$\sum_{k=k_0}^{\infty} b_k t^k$$

with $k_0 \in \mathbb{Z}$, $b_k \in \mathbb{C}$ for $k \geqslant k_0$. We define an absolute value $|\cdot|_0$ on $\mathbb{C}((t))$ by $|0|_0 := 0$ and $|\alpha|_0 := c^{-k_0}$ ($c > 1$ some constant) where

$$\alpha = \sum_{k=k_0}^{\infty} b_k t^k \quad \text{with } b_{k_0} \neq 0.$$

This absolute value is clearly non-archimedean.

(a) Prove that $\mathbb{C}((t))$ is complete w.r.t. $|\cdot|_0$.
(b) Define $|\cdot|_0$ on the field of rational functions $\mathbb{C}(t)$ by $|0|_0 := 0$ and $|\alpha|_0 := c^{-k_0}$ if $\alpha \neq 0$, where k_0 is the integer such that $\alpha = t^{k_0} f/g$ with f, g polynomials not divisible by t. Prove that $\mathbb{C}((t))$ is the completion of $\mathbb{C}(t)$ w.r.t. $|\cdot|_0$.

Exercise 5. In this exercise, p is a prime > 2.

(a) Let d be a positive integer such that $d \not\equiv 0 \pmod p$ and $x^2 \equiv d \pmod p$ is solvable. Show that $x^2 = d$ is solvable in $\mathbb{Z}_p$.
(b) Let a, b be two positive integers such that none of the congruence equations $x^2 \equiv a \pmod p$, $x^2 \equiv b \pmod p$ is solvable in $x \in \mathbb{Z}$. Prove that $ax^2 \equiv b \pmod p$ is solvable in $x \in \mathbb{Z}$.
Hint. Use that the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$. This implies that there is an integer g such that $(\mathbb{Z}/p\mathbb{Z})^* = \{g^m \bmod p : m = 0, \ldots, p-2\}$.
(c) Let K be a quadratic extension of $\mathbb{Q}_p$. Prove that $K = \mathbb{Q}_p(\sqrt{d})$ for some $d \in \mathbb{Z}_p$. Next, prove that $\mathbb{Q}_p(\sqrt{d_1}) = \mathbb{Q}_p(\sqrt{d_2})$ if and only if d_1/d_2 is a square in $\mathbb{Q}_p$.
(d) Determine all quadratic extensions of $\mathbb{Q}_5$.
(e) Prove that for any prime $p > 2$, $\mathbb{Q}_p$ has up to isomorphism only three distinct quadratic extensions.

Exercise 6.

(a) Prove that $x^{p-1} = 1$ has precisely $p-1$ solutions in $\mathbb{Z}_p$, and that these solutions are different modulo p.

(b) Let S consist of 0 and of the solutions in $\mathbb{Z}_p$ of $x^{p-1} = 1$. Let $\alpha \in \mathbb{Z}_p$. Prove that for any positive integer m, there are $\xi_0, \ldots, \xi_{m-1} \in S$ such that $\alpha \equiv \sum_{k=0}^{m-1} \xi_k p^k \pmod{p^m}$. Then prove that there is a sequence $\{\xi_k\}_{k=0}^{\infty}$ in S such that $\alpha = \sum_{k=0}^{\infty} \xi_k p^k$. (This is called the *Teichmüller representation* of α).

Exercise 7.

(a) Prove that for any two positive integers x, y and any integer $n \geqslant 0$, one has
$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{n-k}\binom{y}{k}.$$
(b) Prove the same with $x, y \in \mathbb{Z}_p$.
(c) Let $\beta \in \mathbb{Z}_p$ with $|\beta|_p \leqslant p^{-1}$ and let $x, y \in \mathbb{Z}_p$. Prove that $(1+\beta)^{x+y} = (1+\beta)^x(1+\beta)^y$.
Hint. You may use that if $a := \sum_{n=0}^{\infty} a_n$, $b := \sum_{n=0}^{\infty} b_n$ are two convergent series in $\mathbb{Z}_p$, then $\sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_{n-k}b_k)$ converges also and is equal to $a \cdot b$.

Exercise 8. In this exercise you may use the following facts on p-adic power series (the coefficients are always in $\mathbb{Q}_p$, and $m, m' \in \mathbb{Z}$).
1) Suppose $f(x) = \sum_{n=0}^{\infty} a_n(x-x_0)^n$, $g(x) = \sum_{n=0}^{\infty} b_n(x-x_0)^n$ converge and are equal on $B(x_0, p^{-m})$. Then $a_n = b_n$ for all $n \geqslant 0$.
2) Suppose that for $x \in B(x_0, p^{-m})$, $f(x) = \sum_{n=0}^{\infty} a_n(x-x_0)^n$ converges and $|f(x) - f(x_0)|_p \leqslant p^{-m'}$. Further, suppose that $g(x) = \sum_{n=0}^{\infty} b_n(x-f(x_0))^n$ converges on $B(f(x_0), p^{-m'})$. Then the composition $g(f(x))$ can be expanded as a power series $\sum_{n=0}^{\infty} c_n(x-x_0)^n$ which converges on $B(x_0, p^{-m})$.
3) We define the derivative of $f(x) = \sum_{n=0}^{\infty} a_n(x-x_0)^n$ by
$$f'(x) := \sum_{n=1}^{\infty} n a_n (x-x_0)^{n-1}.$$
If f converges on $B(x_0, p^m)$ then so does f'. The derivative satisfies the same sum rules, product rule, quotient rule and chain rule as the derivative of a function on $\mathbb{R}$, e.g., $g(f(x))' = g'(f(x))f'(x)$.

Now define the p-adic exponential function and p-adic logarithm by
$$\exp_p x := \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \log_p x := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \cdot (x-1)^n.$$

Further, let $r = 1$ if $p > 2$, $r = 2$ if $p = 2$. Prove the following properties.

(a) Prove that $\exp_p(x)$ converges and $|\exp_p(x)-1|_p = |x|_p$ for $x \in B(0, p^{-r})$.
Hint. Prove that $|x^n/n!|_p \to 0$ as $n \to \infty$, and $|x^n/n!|_p < |x|_p$ for $n \geqslant 2$.

(b) Prove that $\log_p(x)$ converges and $|\log_p x|_p = |x-1|_p$ for $x \in B(1, p^{-r})$.

(c) Prove that $\exp_p(x+y) = \exp_p(x)\exp_p(y)$ for $x, y \in B(0, p^{-r})$.
Hint. Fix y and consider the function in x,

$$f(x) := \exp_p(y)^{-1}\exp_p(x+y).$$

Then $f(x)$ can be expanded as a power series $\sum_{n=0}^{\infty} a_n x^n$. Its derivative $f'(x)$ can be computed in the same way as one should do it for real or complex functions. This leads to conditions on the coefficients a_n.

(d) Prove that $\log_p(xy) = \log_p(x) + \log_p(y)$ for $x, y \in B(1, p^{-r})$.

(e) Prove that $\log_p(\exp_p x) = x$ for $x \in B(0, p^{-r})$.

(f) Prove that $\exp_p(\log_p x) = x$ for $x \in B(1, p^{-r})$.

Exercise 9. Consider the sequence $U = \{u_n\}_{n=0}^{\infty}$

$$u_n = \frac{(2\omega)^n - (2\omega^{-1})^n}{2\omega - 2\omega^{-1}} + (-1)^n + 1 \quad (\omega = e^{2\pi i/3}).$$

(a) Determine the companion polynomial and initial values of U.
(b) Determine the set Z_U and show that it is infinite.
(c) Show that there is a linear recurrence sequence $V = \{v_n\}_{n=0}^{\infty}$, with the same companion polynomial as U, such that the set Z_V is finite.

Exercise 10. Let $U = \{u_n\}_{n=0}^{\infty}$ be a linear recurrence sequence in $\mathbb{C}$. Consider the set I_U of polynomials $f = a_0 + a_1 X + \cdots + a_m X^m$ with $a_0, \ldots, a_m \in \mathbb{C}$, $m \geqslant 0$ such that

$$a_0 u_{n+m} + a_1 u_{n+m-1} + \cdots + a_m u_n = 0 \quad \text{for } n \geqslant m.$$

(a) Prove that I is an ideal of $\mathbb{C}[X]$, generated by the companion polynomial of U.
(b) Give a necessary and sufficient condition in terms of the companion polynomial of U such that U is periodic.

Exercise 11. Let $U = \{u_n\}_{n=0}^{\infty}$, $V = \{v_n\}_{n=0}^{\infty}$ be two linear recurrence sequences in $\mathbb{C}$.

(a) Prove that $\{u_n v_n\}_{n=0}^{\infty}$ is a linear recurrence sequence.
(b) Define the sequence $W = \{w_n\}_{n=0}^{\infty}$ by $w_n = u_{n/2}$ if n is even, and $w_n = v_{(n-1)/2}$ if n is odd. Prove that W is a linear recurrence sequence.

Exercise 12. Let $\alpha_1, \ldots, \alpha_t$ be reals with $0 < \alpha_1 < \alpha_2 \cdots < \alpha_t$, and let $f_1, \ldots, f_t$ be polynomials in $\mathbb{R}[X]$ with $\deg f_h \leqslant e_h - 1$ for $h = 1, \ldots, t$, and $e_1 + \cdots + e_t = k$. Define the linear recurrence sequence $U = \{u_n\}_{n=0}^{\infty}$ by

$$u_n = \sum_{h=1}^{t} f_h(n)\alpha_h^n \quad (n \geqslant 0).$$

Prove that Z_U has cardinality at most $k - 1$.
Hint. Prove by induction on k that the number of zeros $x \in \mathbb{R}$ of the real function $u(x) := \sum_{h=1}^{t} f_h(x)\alpha_h^x$ is a most $k-1$. The induction step is at follows. There is no loss of generality to assume that $\alpha_t = 1$ since dividing $u(x)$ by α_t^x does not change the cardinality of Z_U. Now consider the derivative $u'(x)$ and apply Rolle's Theorem.

Exercise 13. Let K be a cubic field with one real embedding σ_1 and two complex embeddings σ_2, σ_3.

(a) Suppose that $K = \mathbb{Q}(\alpha)$. Prove that $\sigma_i(\alpha)$ $(i = 1, 2, 3)$ are all distinct.
(b) Let $\alpha \in K$ be such that at least two among the numbers $\sigma_1(\alpha), \sigma_2(\alpha), \sigma_3(\alpha)$ are equal. Prove that $\alpha \in \mathbb{Q}$.
Hint. What is the degree of α?
(c) Let η be a unit in $\mathcal{O}_K$ with $\eta \neq \pm 1$. Prove that none of the quotients $\sigma_i(\eta)/\sigma_j(\eta)$, with $i, j \in \{1, 2, 3\}$, $i \neq j$ is a root of unity.