Chapter 8

P-adic numbers

Literature:
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

8.1 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:*

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

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:

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

Notice that these properties imply that $|1| = 1$. The absolute value $|\cdot|$ is called *non-archimedean* if the triangle inequality can be replaced by the stronger *ultrametric inequality* or *strong triangle 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) Every field K can be endowed with the *trivial* absolute value $|\cdot|$, given by $|a| = 0$ if $a = 0$ and $|a| = 1$ if $a \neq 0$. It is not hard to show that if K is a finite field then there are no non-trivial absolute values on K.

2) The ordinary absolute value $|\cdot|_\infty$ on $\mathbb{Q}$ is archimedean, while the p-adic absolute values are all non-archimedean.

3) 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 $K(t)$.

Let K be a field. 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 8.1. (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.

8.2 Completions

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 w.r.t. $|\cdot|$.

For instance, $\mathbb{R}$ and $\mathbb{C}$ are complete w.r.t. the ordinary absolute value. Ostrowski proved that any field complete with respect to an archimedean absolute value is isomorphic to $\mathbb{R}$ or $\mathbb{C}$.

Every field K with an absolute value can be extended to an up to isomorphism complete field, the completion of K.

Theorem 8.2. *Let K be a field with non-trivial 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. Basically one has to mimic the construction of $\mathbb{R}$ from $\mathbb{Q}$ or the construction of a completion of a metric space in topology. 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 the one 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 8.3. *Assume that $|\cdot|$ is a non-trivial, 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

$$|a+b| = \lim_{k\to\infty} |a_k + b_k| \leqslant \lim_{k\to\infty} \max(|a_k|, |b_k|) = \max(|a|, |b|).$$

□

8.3 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 $\mathbf{Q}_p$.
The continuation of $|\cdot|_p$ to $\mathbb{Q}_p$ is also denoted by $|\cdot|_p$. This is a non-archimedean absolute value on $\mathbb{Q}_p$. Convergence, limits, Cauchy sequences and the like will all be with respect to $|\cdot|_p$. As mentioned before, by identifying $a \in \mathbb{Q}$ with the class of the constant Cauchy sequence $\{a\}$, we may view $\mathbb{Q}$ as a subfield of $\mathbb{Q}_p$.

Lemma 8.4. *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 again a sequence $\{x_k\}$ in $\mathbb{Q}$ converging to x. Then $|x|_p = \lim_{k\to\infty} |x_k|_p$. For k sufficiently large we have $|x_k|_p = p^{m_k}$ for some $m_k \in \mathbb{Z}$. Since the sequence of numbers p^{m_k} converges we must have $m_k = m \in \mathbb{Z}$ for k sufficiently large. Hence $|x|_p = p^m$. $\square$

The set $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\}$ is called the *ring of p-adic integers*. Notice that if $x, y \in \mathbb{Z}_p$ then $|x - y|_p \leqslant \max(|x|_p, |y|_p) \leqslant 1$. Hence $x - y \in \mathbb{Z}_p$. Further, if $x, y \in \mathbb{Z}_p$ then $|xy|_p \leqslant 1$ which implies $xy \in \mathbb{Z}_p$. So $\mathbb{Z}_p$ is indeed a ring. Viewing $\mathbb{Q}$ as a subfield of $\mathbb{Q}_p$, we have

$$\mathbb{Z}_p \cap \mathbb{Q} = \left\{ \tfrac{a}{b} : a, b \in \mathbb{Z}, p \nmid b \right\}.$$

It is not hard to show that the group of units of $\mathbb{Z}_p$, these are the elements $x \in \mathbb{Z}_p$ with $x^{-1} \in \mathbb{Z}_p$, is equal to

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

Further, $M_p := \{x \in \mathbb{Q}_p : |x|_p < 1\}$ is an ideal of $\mathbb{Z}_p$. In fact, M_p is the only maximal ideal of $\mathbb{Z}_p$ since any ideal of $\mathbb{Z}_p$ not contained in M_p contains an element of $\mathbb{Z}_p^*$, hence generates the whole ring $\mathbb{Z}_p$. Noting

$$|x|_p < 1 \Longleftrightarrow |x|_p \leqslant p^{-1} \Longleftrightarrow |x/p|_p \leqslant 1 \Longleftrightarrow x/p \in \mathbb{Z}_p$$

for $x \in \mathbb{Q}_p$, we see that $M_p = p\mathbb{Z}_p$.

For $\alpha, \beta \in \mathbb{Q}_p$ we write $\alpha \equiv \beta \pmod{p^m}$ if $(\alpha - \beta)/p^m \in \mathbb{Z}_p$. This is equivalent to $|\alpha - \beta|_p \leqslant p^{-m}$. Notice that if $\alpha = \frac{a_1}{b_1}$, $\beta = \frac{a_2}{b_2}$ with $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ and $p \nmid b_1 b_2$, then

$$a_1 \equiv a_2 \pmod{p^m}, \quad b_1 \equiv b_2 \pmod{p^m} \Longrightarrow \alpha \equiv \beta \pmod{p^m}.$$

For p-adic numbers, "very small" means "divisible by a high power of p", and two p-adic numbers α and β are p-adically close if and only if $\alpha - \beta$ is divisible by a high power of p.

Lemma 8.5. *For every $\alpha \in \mathbb{Z}_p$ and every positive integer m there is a unique $a_m \in \mathbb{Z}$ such that $|\alpha - a_m|_p \leqslant p^{-m}$ and $0 \leqslant a_m < p^m$. 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,

$$|\alpha - a_m|_p \leqslant \max(|\alpha - (a/b)|_p, |(a/b) - a_m|_p) \leqslant p^{-m}.$$

This shows the existence of a_m. As for the unicity, if a'_m is another integer with the properties specified in the lemma, we have $|a_m - a'_m|_p \leqslant p^{-m}$, hence $a_m \equiv a'_m \pmod{p^m}$, implying $a_m = a'_m$. □

Theorem 8.6. *The non-zero ideals of $\mathbb{Z}_p$ are $p^m\mathbb{Z}_p$ ($m = 0, 1, 2, \ldots$) and $\mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{Z}/p^m\mathbb{Z}$. In particular, $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.*

Proof. Let I be a non-zero ideal of $\mathbb{Z}_p$ and choose $\alpha \in I$ for which $|\alpha|_p$ is maximal. Then $|\alpha|_p = p^{-m}$ with $m \in \mathbb{Z}_{\geqslant 0}$. We have $p^{-m}\alpha \in \mathbb{Z}_p^*$, hence $p^m \in I$. Further, for $\beta \in I$ we have $|\beta p^{-m}|_p \leqslant 1$, hence $\beta \in p^m\mathbb{Z}_p$. Hence $I \subset p^m\mathbb{Z}_p$. This implies $I = p^m\mathbb{Z}_p$.

The homomorphism $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}_p/p^m\mathbb{Z}_p$: $a \pmod{p^m} \mapsto a \pmod{p^m}$ is clearly injective. and also surjective in view of Lemma 8.5. Hence $\mathbb{Z}/p^m\mathbb{Z} \cong \mathbb{Z}_p/p^m\mathbb{Z}_p$. □

Lemma 8.7. *Let $\{a_k\}_{k=0}^\infty$ be a sequence in $\mathbb{Q}_p$. Then $\sum_{k=0}^\infty a_k$ converges in $\mathbb{Q}_p$ if and only if $\lim_{k\to\infty} a_k = 0$.*
Further, every convergent series in $\mathbb{Q}_p$ is unconditionally convergent, i.e., neither the convergence, nor the value of the series, are affected if the terms a_k are rearranged.

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

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

So the partial sums α_n form a Cauchy sequence, hence must converge to a limit in $\mathbb{Q}_p$.

To prove the second part of the lemma, let σ be a bijection from $\mathbb{Z}_{\geqslant 0}$ to $\mathbb{Z}_{\geqslant 0}$. We have to prove that $\sum_{k=0}^{\infty} a_{\sigma(k)} = \sum_{k=0}^{\infty} a_k$. Equivalently, we have to prove that $\sum_{k=0}^{M} a_k - \sum_{k=0}^{M} a_{\sigma(k)} \to 0$ as $M \to \infty$, i.e., for every $\varepsilon > 0$ there is N such that

$$|\sum_{k=0}^{M} a_k - \sum_{k=0}^{M} a_{\sigma(k)}|_p < \varepsilon \text{ for every } M > N.$$

Let $\varepsilon > 0$. There is N such that $|a_k|_p < \varepsilon$ for all $k \geqslant N$. Choose $N_1 > N$ such that $\{\sigma(0), \ldots, \sigma(N_1)\}$ contains $\{0, \ldots, N\}$ and let $M > N_1$. Then in the sum $S := \sum_{k=0}^{M} a_k - \sum_{k=0}^{M} a_{\sigma(k)}$, only terms a_k with $k > N$ and $a_{\sigma(k)}$ with $\sigma(k) > N$ occur. Hence each term in S has p-adic absolute value $< \varepsilon$ and therefore, by the ultrametric inequality, $|S|_p < \varepsilon$. □

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 8.8. **(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 $k_0 \in \mathbb{Z}$, $b_k \in \{0, \ldots, p-1\}$ for $k \geqslant -k_0$ and $b_{-k_0} \neq 0$ and conversely, every such series belongs to $\mathbb{Q}_p$.*

Proof. We first prove part (i). First observe that by Lemma 8.7, 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 $\alpha \in \mathbb{Z}_p$. Define sequences $\{\alpha_k\}_{k=0}^{\infty}$ in $\mathbb{Z}_p$, $\{b_k\}_{k=0}^{\infty}$ in $\{0, \ldots, p-1\}$ inductively as follows:

$$(8.1) \qquad \begin{cases} \alpha_0 := \alpha; \\ \text{For } k = 0, 1, \ldots, \text{ let } b_k \in \{0, \ldots, p-1\} \text{ be the integer with} \\ \ \alpha_k \equiv b_k \pmod{p} \text{ and put } \alpha_{k+1} := (\alpha_k - b_k)/p. \end{cases}$$

By induction on k, one easily deduces that for $k \geqslant 0$,

$$\alpha_k \in \mathbb{Z}_p, \quad \alpha = \sum_{j=0}^{k} b_j p^j + p^{k+1} \alpha_k.$$

Hence $|\alpha - \sum_{j=0}^{k} b_j p^j|_p \leqslant p^{-k-1}$ for $k \geqslant 0$. It follows that

$$\alpha = \lim_{k\to\infty} \sum_{j=0}^{k} b_j p^j = \sum_{j=0}^{\infty} b_j p^j.$$

Notice that the integer a_m from Lemma 8.5 is precisely $\sum_{k=0}^{m-1} b_k p^k$. Since a_m is uniquely determined, so must be the integers b_k.

We prove part (ii). As above, any series $\sum_{k=-k_0}^{\infty} b_k p^k$ with $b_k \in \{0,\dots,p-1\}$ 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 $\mathbb{Z}_p$. Applying (i) to β we get

$$\alpha = p^{-k_0}\beta = p^{-k_0} \sum_{k=0}^{\infty} c_k p^k$$

with $c_k \in \{0,\dots,p-1\}$ which implies (ii). $\square$

Corollary 8.9. *$\mathbb{Z}_p$ is uncountable.*

Proof. Apply Cantor's diagonal method. $\square$

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 $|\alpha|_p = p^{-m}$ if $\alpha = \sum_{k=m}^{\infty} b_k p^k$ 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

$$\alpha \equiv \beta \pmod{p^m} \Longleftrightarrow a_k = b_k \text{ for } k < m.$$

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.

Theorem 8.10. *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*

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

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 by (8.1). Notice that α_k determines uniquely the numbers $b_k, b_{k+1}, \dots$.

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 $\{-C, \dots, C\}$, 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. $\square$

Examples. (i) We determine the 3-adic expansion of $-\frac{2}{5}$. We compute the numbers α_k, b_k according to (8.1).
Notice that $\frac{1}{5} \equiv 2 \pmod{3}$.

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

$$\begin{aligned} -\frac{2}{5} &= 2\times 3^0 + 1\times 3^1 + 0\times 3^2 + 1\times 3^3 + 2\times 3^4 + 1\times 3^5 + 0\times 3^6 + 1\times 3^7 + \cdots \\ &= 0.2101\,2101\ldots\ (2) = 0.\overline{2101}\ (2). \end{aligned}$$

(ii) We determine the 2-adic expansion of $\frac{1}{56}$. Notice that $\frac{1}{56} = 2^{-3}\times\frac{1}{7}$. We start with the 2-adic expansion of $\frac{1}{7}$.

k	0	1	2	3	4
α_k	$\frac{1}{7}$	$-\frac{3}{7}$	$-\frac{5}{7}$	$-\frac{6}{7}$	$-\frac{3}{7}$
b_k	1	1	1	0	1

So

$$\frac{1}{7} = 0.1\,\overline{110}\ (2), \qquad \frac{1}{56} = 111.\overline{011}\ldots\ (2).$$

8.4 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 8.11. *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 and 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 8.12. *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. □

8.5 Algebraic extensions of $\mathbb{Q}_p$

We fix an algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$, i.e., a minimal extension of $\mathbb{Q}_p$ over which every non-zero polynomial in $\mathbb{Q}_p[X]$ factors into linear factors. We construct an extension of $|\cdot|_p$ to $\overline{\mathbb{Q}_p}$.

For polynomials $f, g \in \mathbb{Z}_p[X]$ we write $f \equiv g \pmod{p^m}$ if $p^{-m}(f-g) \in \mathbb{Z}_p[X]$. Given $f \in \mathbb{Z}_p[X]$ and a sequence of polynomials $f_m \in \mathbb{Z}_p[X]$ $(m = 1, 2, \ldots)$, we write $\lim_{m\to\infty} f_m = f$ if for every $k \geqslant 0$, the sequence of coefficients of X^k in f_m converges to the coefficient of X^k in f. Clearly, $\lim_{m\to\infty} f_m = f$ if and only if there is a sequence of non-negative integers a_m with $\lim_{m\to\infty} a_m \to \infty$ (in $\mathbb{R}$) such that $f_m \equiv f \pmod{p^{a_m}}$.

An important tool is the so-called *Hensel's Lemma*, which gives a method to derive, from a factorization of a polynomial $f \in \mathbb{Z}_p[X]$ modulo p, a factorization of f in $\mathbb{Z}_p[X]$.

Theorem 8.13. *Let f, g_1, h_1 be polynomials in $\mathbb{Z}_p[X]$ such that $f \neq 0$,*

$$\begin{aligned}&f \equiv g_1 h_1 \pmod{p}, \quad \gcd(g_1, h_1) \equiv 1 \pmod{p},\\ &g_1 \textit{ is monic, } \ 0 < \deg g_1 < \deg f, \ \deg g_1 h_1 \leqslant \deg f.\end{aligned}$$

Then there exist polynomials $g, h \in \mathbb{Z}_p[X]$ such that

$$f = gh, \quad g \equiv g_1 \pmod{p}, \ h \equiv h_1 \pmod{p}, \quad g \textit{ is monic, } \ \deg g = \deg g_1.$$

Proof. By induction on m, we prove that there are polynomials $g_m, h_m \in \mathbb{Z}_p[X]$ such that

$$(8.2) \qquad \left\{\begin{array}{l} f \equiv g_m h_m \pmod{p^m}, \quad g_m \equiv g_1 \pmod{p}, \ h_m \equiv h_1 \pmod{p}, \\ g_m \text{ is monic}, \quad \deg g_m = \deg g_1, \ \deg g_m h_m \leqslant \deg f. \end{array}\right.$$

For $m = 1$ this follows from our assumption. Let $m \geqslant 2$, and suppose that there are polynomials g_{m-1}, h_{m-1} satisfying (8.2) with $m-1$ instead of m. We try to find $u, v \in \mathbb{Z}_p[X]$ such that $g_m = g_{m-1} + p^{m-1}u$, $h_m = h_{m-1} + p^{m-1}v$ satisfy (8.2). By assumption,

$$A := p^{1-m}(f - g_{m-1}h_{m-1}) \in \mathbb{Z}_p[X].$$

Notice that $f \equiv g_m h_m \pmod{p^m}$ if and only if

$$\begin{aligned}&f - (g_{m-1} + p^m u)(h_{m-1} + p^m v) \equiv 0 \pmod{p^m}\\ &\Longleftrightarrow A \equiv v g_{m-1} + u h_{m-1} \pmod{p} \Longleftrightarrow A \equiv v g_1 + u h_1 \pmod{p}.\end{aligned}$$

Thanks to our assumption $\gcd(g_1, h_1) \equiv 1 \pmod{p}$ such u, v exist, and in fact, we can choose u with $\deg u < \deg g_1$. Then clearly, $g_m = g_{m-1} + p^{m-1}u$, $h_m = h_{m-1} + p^{m-1}v$ satisfy (8.2).

Now for each term X^k, the coefficients of X^k in the g_m form a Cauchy sequence, hence have a limit, so we can take $g := \lim_{m\to\infty} g_m$. Then g is monic, and $0 < \deg g < \deg f$. Likewise, we can define $h := \lim_{m\to\infty} h_m$. Then

$$f - gh = \lim_{m\to\infty}(f - g_m h_m) = 0.$$

This completes our proof. $\square$

Corollary 8.14. *Let $f = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Q}_p[X]$ be irreducible. Put $M := \max(|a_0|_p, \ldots, |a_n|_p)$. Let k be the smallest index i such that $|a_i|_p = M$. Then $k = 0$ or $k = n$.*

Proof. Assume that $0 < k < n$. So $|a_i|_p < |a_k|_p$ for $i < k$ and $|a_i|_p \leqslant |a_k|_p$ for $i \geqslant k$. Put $\tilde{f} := b_k^{-1} f$. Then

$$\widetilde{f} = b_0X^n + \cdots + b_{k-1}X^{n-k+1} + X^{n-k} + b_{k+1}X^{n-k-1} + \cdots + b_n$$

with $|b_i|_p < 1$ for $i < k$ and $|b_i|_p \leqslant 1$ for $i > k$. Now $\widetilde{f} \in \mathbb{Z}_p[X]$, $b_0, \ldots, b_{k-1}$ are divisible by p, and thus,

$$\widetilde{f} \equiv (X^{n-k} + b_{k+1}X^{n-k-1} + \cdots + b_n) \cdot 1 \pmod{p}.$$

By applying Hensel's Lemma, we infer that there are polynomials $g, h \in \mathbb{Z}_p[X]$ such that $\widetilde{f} = gh$ and $\deg g = n - k$. Then $\widetilde{f}$, hence f, is reducible, contrary to our assumption. $\square$

We are now ready to define an extension of $|\cdot|_p$ to $\overline{\mathbb{Q}_p}$. Given $\alpha \in \overline{\mathbb{Q}_p}$, let

$$f = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Q}_p[X]$$

be the monic minimal polynomial of α over $\mathbb{Q}_p$, that is the monic polynomial in $\mathbb{Q}_p[X]$ of smallest degree having α as a root. Then we put

$$|\alpha|_p := |a_n|_p^{1/n}.$$

Let $\alpha^{(1)} = \alpha, \ldots, \alpha^{(n)}$ be the conjugates of α, i.e., the roots of f in $\overline{\mathbb{Q}}_p$. Let L be any finite extension of $\mathbb{Q}_p$ containing α, and suppose that $[L : \mathbb{Q}_p] = m$. Completely similarly as for algebraic number fields, the field L has precisely m embeddings in $\overline{\mathbb{Q}}_p$ that leave the elements of $\mathbb{Q}_p$ unchanged, say $\sigma_1, \ldots, \sigma_m$. Now in the sequence $\sigma_1(\alpha), \ldots, \sigma_m(\alpha)$, each of the conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$ occurs precisely m/n times. Define the norm $N_{L/\mathbb{Q}_p}(\alpha) := \sigma_1(\alpha) \cdots \sigma_m(\alpha)$. Then

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

In case that $\alpha \in \mathbb{Q}_p$, the minimal polynomial of α is $X - \alpha$, and thus we get back our already defined $|\alpha|_p$.

Theorem 8.15. *$|\cdot|_p$ defines a non-archimedean absolute value on $\overline{\mathbb{Q}_p}$.*

Proof. Let $\alpha, \beta \in \overline{\mathbb{Q}_p}$, and take $L = \mathbb{Q}_p(\alpha, \beta)$. Then

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

To prove that $|\alpha + \beta|_p \leqslant \max(|\alpha|_p, |\beta|_p)$, assume without loss of generality that $|\alpha|_p \leqslant |\beta|_p$ and put $\gamma := \alpha/\beta$. Then $|\gamma|_p \leqslant 1$, and we have to prove that $|1+\gamma|_p \leqslant 1$. Let $f = X^n + a_1 X^{n-1} + \cdots + a_n$ be the minimal polynomial of γ over $\mathbb{Q}_p$. Then $|a_n|_p = |\gamma|_p^n \leqslant 1$, and by Corollary 8.14, also $|a_i|_p \leqslant 1$ for $i = 1, \ldots, n-1$. Now the minimal polynomial of $\gamma + 1$ is $f(X-1) = X^n + \cdots + f(-1)$ and so

$$\begin{aligned} |\gamma + 1|_p = |f(-1)|_p^{1/n} &= |(-1)^n + a_1(-1)^{n-1} + \cdots + a_0|_p^{1/n} \\ &\leqslant \max(1, |a_1|_p, \ldots, |a_n|_p)^{1/n} \leqslant 1, \end{aligned}$$

as required. $\square$

We recall Eisenstein's irreducibility criterion for polynomials in $\mathbb{Z}_p$.

Lemma 8.16. *Let $f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n \in \mathbb{Z}_p[X]$ be such that $a_i \equiv 0 \pmod{p}$ for $i = 1, \ldots, n$, and $a_n \not\equiv 0 \pmod{p^2}$. Then f is irreducible in $\mathbb{Q}_p[X]$.*

Proof. Completely similar as the Eisenstein criterion for polynomials in $\mathbb{Z}[X]$. $\square$

Example. Let α be a zero of $X^3 - 8X + 10$ in $\overline{\mathbb{Q}_2}$. The polynomial $X^3 - 8X + 10$ is irreducible in $\mathbb{Q}_2[X]$, hence it is the minimal polynomial of α. It follows that $|\alpha|_2 = |10|_2^{1/3} = 2^{-1/3}$.

We finish with some facts which we state without proof.

Theorem 8.17. (i) *Let K be a finite extension of $\mathbb{Q}_p$. Then there is precisely one absolute value on K whose restriction to $\mathbb{Q}_p$ is $|\cdot|_p$, and this is given by $|N_{K/\mathbb{Q}_p}(\cdot)|_p^{1/[K:\mathbb{Q}_p]}$. Further, K is complete with respect to this absolute value.*
(ii) *$\overline{\mathbb{Q}_p}$ is* **not** *complete with respect to $|\cdot|_p$.*
(iii) *The completion $\mathbb{C}_p$ of $\overline{\mathbb{Q}_p}$ with respect to $|\cdot|_p$ is algebraically closed.*

8.6 Exercises

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

Exercise 8.1. *(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 8.2. *Let $\alpha \in \mathbb{Q}_p$, $\alpha \neq 0$. 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.*

Exercise 8.3. *Let $\alpha = \sum_{k=-k_0}^{\infty} b_k p^k \in \mathbb{Q}_p$ where $b_k \in \{0, \ldots, p-1\}$ for $k \geqslant -k_0$ and $b_{-k_0} \neq 0$. Suppose that the sequence $\{b_k\}_{k=-k_0}^{\infty}$ is ultimately periodic, i.e., there exist r, s with $r \geqslant -k_0$, $s > 0$ such that $a_{k+s} = a_k$ for all $k \geqslant r$. Prove that $\alpha \in \mathbb{Q}$.*

Exercise 8.4. *Let $\alpha \in \mathbb{Z}_p$ with $|\alpha - 1|_p \leqslant p^{-1}$. In this exercise you are asked to define α^x for $x \in \mathbb{Z}_p$ and to show that this exponentiation has the expected properties. You may use without proof that the limit of the sum, product etc. of two sequences in $\mathbb{Z}_p$ is the sum, product etc. of the limits.*

(a) Prove that $\left|\frac{\alpha^p - 1}{\alpha - 1}\right|_p \leqslant p^{-1}$.

(b) Let u be a positive integer. Prove that $|\alpha^u - 1|_p \leqslant |u|_p |\alpha - 1|_p$.
Hint. *Write $u = p^m b$ where b is not divisible by p and use induction on m.*

(c) Let u, v be positive integers. Prove that $|\alpha^u - \alpha^v|_p \leqslant |u - v|_p |\alpha - 1|_p$.

(d) We now define α^x for $x \in \mathbb{Z}_p$ as follows. Take a sequence of positive integers $\{a_k\}_{k=0}^{\infty}$ such that $\lim_{k\to\infty} a_k = x$ and define

$$\alpha^x := \lim_{k\to\infty} \alpha^{a_k}.$$

Prove that this is well-defined, i.e., the limit exists and is independent of the choice of the sequence $\{a_k\}_{k=0}^{\infty}$.

*(e) Prove that for $x, y \in \mathbb{Z}_p$ we have $|\alpha^x - \alpha^y|_p \leqslant |x - y|_p |\alpha - 1|_p$. (**Hint.** Take sequences of positive integers converging to x, y.)*
Then show that if $\{x_k\}_{k=0}^{\infty}$ is a sequence in $\mathbb{Z}_p$ such that $\lim_{k\to\infty} x_k = x$ then $\lim_{k\to\infty} \alpha^{x_k} = \alpha^x$ (so the function $x \mapsto \alpha^x$ is continuous).

(f) *Prove the following properties of the above defined exponentiation:*
(i) $(\alpha\beta)^x = \alpha^x\beta^x$ *for* $\alpha, \beta \in \mathbb{Z}_p$, $x \in \mathbb{Z}_p$ *with* $|\alpha - 1|_p \leqslant p^{-1}$, $|\beta - 1|_p \leqslant p^{-1}$;
(ii) $\alpha^{x+y} = \alpha^x\alpha^y$, $(\alpha^x)^y = \alpha^{xy}$ *for* $\alpha \in \mathbb{Z}_p$ *with* $|\alpha - 1|_p \leqslant p^{-1}$, $x, y \in \mathbb{Z}_p$.

Remark. In 1935, Mahler proved the following p-adic analogue of the Gel'fond-Schneider Theorem: let α, β be elements of $\mathbb{Z}_p$, both algebraic over $\mathbb{Q}$, such that $|\alpha - 1|_p \leqslant p^{-1}$ and $\beta \notin \mathbb{Q}$. Then α^β is transcendental over $\mathbb{Q}$.

Exercise 8.5. *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*

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

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 8.6. *In this exercise you are asked to work out a p-adic analogue of Newton's method to approximate the roots of a polynomial (which is in fact a special case of Hensel's Lemma). Let* $f = a_0X^n + \cdots + a_n \in \mathbb{Z}_p[X]$. *The derivative of* f *is* $f' = na_0X^{n-1} + \cdots + a_{n-1}$.

(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 $f(x_0) \equiv 0 \,(\mathrm{mod}\, p)$, $f'(x_0) \not\equiv 0 \,(\mathrm{mod}\, p)$. 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 $x_n \in \mathbb{Z}_p$, $f(x_n) \equiv 0 \,(\mathrm{mod}\, p^{2^n})$, $f'(x_n) \not\equiv 0 \,(\mathrm{mod}\, p)$ 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 $\xi \equiv x_0 \,(\mathrm{mod}\, p)$.

Exercise 8.7. *In this exercise, p is a prime > 2.*

(a) Let d be a positive integer such that $d \not\equiv 0 \,(\mathrm{mod}\, p)$ and $x^2 \equiv d \,(\mathrm{mod}\, p)$ 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 $x^2 \equiv a \,(\mathrm{mod}\, p)$, $x^2 \equiv b \,(\mathrm{mod}\, p)$ is solvable in $x \in \mathbb{Z}$. Prove that $ax^2 \equiv b \,(\mathrm{mod}\, p)$ 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 8.8. *(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 $\alpha \equiv \sum_{k=0}^{m-1} \xi_k p^k \,(\mathrm{mod}\, p^m)$. 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 8.9. *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* $x \in B(1, p^{-r})$.