Introduction to p-adic numbers

An overview of ultrametric spaces and p-adic numbers.

Eichlinghofen, the 28th August 2015

by

Gilles Bellot
TU Dortmund University
Faculty of Mathematics

Acknowledgements

I would like to thank Blizzard for their commitment to developing amazing and competitive games, my friends Sarah Louise Kerrigan and James Eugene Raynor for the action-filled nights we spend together hunting down some Zerg and my mentors Tassadar and Zeratul for teaching me about tolerance and the true way of a Protoss warrior. A special thank you belongs to HaileyMarie for making the world a more beautiful place.

Abstract

Overview of ultrametric spaces and p-adic numbers.

Contents

Chapter 1

Introduction

The p-adic numbers were *invented* and introduced to number theory by Kurt Hensel[1] around the year 1900 - motivated by the idea of bringing the powerful tool of power series to this area of mathematics. In his book, [Hen08], he defines p-adic numbers as formal objects as follows: "[...] von einer p-adischen Zahl will ich jede Reihe: $c_0 + c_1 p + c_2 p^2 + c_3 p^3 + \ldots$ mit modulo p reduzierten Koeffizienten, [...], verstehen, [...] .". In the following chapters we want to give an introduction to Hensel's numbers and some of his most famous ideas and theorems.

Hensel's doctoral supervisor was Leopold Kronecker[2] who once said "Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk". Thus, by defining the p-adic numbers as the set of all Laurent[3] series in p, the student came true to his masters vision.

At first Hensel was mainly interested in applying his new theory to the theory of numbers, especially the theory of quadratic forms, but later on found satisfaction from studying the properties of the field p-adic numbers by itself.

Influenced by this new theory, Ernst Steinitz[4] presented, in the year 1910, the first abstract algebraic definition of a field in his paper *Algebraische Theorie der Körper.* Two years later, József Kürschák[5] founded the

[1] German mathematician (* 1861 in Königsberg in Preußen, today Kaliningrad, Russia; † 1941 in Marburg).

[2] German mathematician (* 1823; in Legnica, today a town in the Legnica Voivodeship in Poland; † 1891 in Berlin).

[3] Pierre Alphonse Laurent, French mathematician (* 1813 in Paris; † 1854 ibidem).

[4] German mathematician (* 1871 in Laurahütte, today Siemianowice Śląskie in the Sileasian Voivodeship, Poland; † 1928 in Kiel).

[5] Hungarian mathematician (* 1864 in Budapest; † 1933 ibidem).

theory of valuations by giving a first axiomatic definition of a valuation. Our first chapter gives an introduction to those topics.

Another important contribution to the p-adic theory was published in 1917 by Aleksandr Markovič Ostrovskij[6], cataloguing all the possible valuations on $\mathbb{Q}$, which was one of the most important founding stones of the theory of p-adic analysis. We will discuss his theorem in the second chapter.

Last but not least, even Helmut Hasse[7], one of the greatest algebraist and number theorist of his time, was influenced by Hensel's p-adic theory. In 1920 he went to Marburg to study under Hensel himself and in the month of October of the same year he discovered his famous local-global principle which states that *some* equations which have local solutions in $\mathbb{R}$ and $\mathbb{Q}_p$, for each prime number p, have a global solution in $\mathbb{Q}$ as well. This famous theorem, which showed the enormous potential of Hensel's new numbers, will be mentioned in the third chapter of this exposure.

It might be interesting to note that the modern p-adic theory has manifold applications in the world of physics as well. In chapter three we will briefly mention one of them, related to high-energy physics, but the p-adic numbers also find applications in quantum physics, string theory, molecular biology and chaotic physical systems.

The general outline of this introduction to p-adic numbers follows [Kat].

1.1 Notation

Throughout this text $\mathbb{P}$ will denote the set of all prime numbers.

[6] Russian mathematician (* 1893 in Kiev, today Ukraine; † 1986 in Montagnola, Switzerland).

[7] German mathematician (* 1898 in Kassel; † 1979 in Ahrensburg).

Chapter 2

Topology of ultrametric spaces

The language of general topology is well known to mathematicians and the concept of valuations introduces this language into the theory of algebraic numbers in a very natural way. We will give a brief introduction to this theory and illustrate a few connections between valuation theory, topology and algebra, but we will not go beyond the ideas that we need to later on introduce the field of p-adic numbers. For readers who are interested in the more general theory of valuations we refer to chapter 1 of [O'M99]. For a thorough introduction into topological preliminaries and continuous functions, we refer to [HS65].

2.1 Introduction to the theory of valuations

Definition 2.1.1. *Let K be a field. A mapping $|\ | : K \to \mathbb{R}$ is called an absolute value on K if the following properties hold for all $x, y \in K$.*

1. *$|x| \geq 0$ and $|x| = 0 \Leftrightarrow x = 0$,*
2. *$|xy| = |x|\,|y|$ and*
3. *$|x + y| \leq |x| + |y|$.*

The third property is called triangle inequality.

Example 2.1.2.

- *On $K = \mathbb{R}$ we have the usual definition of the absolute value: $|x| = x$ if $x \geq 0$ and $-x$ else.*
- *On $K = \mathbb{C}$ we have the well-known definition of the absolute value $|z| = \sqrt{x^2 + y^2}$, for $z = x + iy \in \mathbb{C}$, $x, y \in \mathbb{R}$.*
- *On any field K we have the discrete absolute value $\delta_K(x) := |x| = 1$ if $x \neq 0$ and 0 else. This is clearly an absolute value, but it is also clearly boring.*

Remark 2.1.3. *Finite fields only possess the discrete absolute value, as for $x \in \mathbb{F}_q$, $q = p^n$, $p \in \mathbb{P}$, we have $|x|^{q-1} = |x^{q-1}| = |1| = 1$.*

Proposition 2.1.4. *Let K be a field with an arbitrary absolute value $|\ |$ and $x, y \in K$, then:*

1. *$|\pm 1| = 1$, the same holds for every root of unity,*
2. *$|-x| = |x|$ and*
3. *$||x| - |y|| \leq |x - y|$.*

The proof of those statements is straight forward and left as an exercise.

Definition 2.1.5. *Let $p \in \mathbb{P}$, $n \in \mathbb{Z}$ and $\operatorname{ord}_p(n)$ be the largest integer such that $n = p^{\operatorname{ord}_p(n)}m$. We call $\operatorname{ord}_p(n)$ the p-adic order of n. For $n = 0$, we set $\operatorname{ord}_p(n) = \infty$.*

The p-adic order of a rational number $x \in \mathbb{Q}$, $x = \frac{a}{n}$, $a \in \mathbb{Z}, b \in \mathbb{N}$ with $\gcd(a, b) = 1$, is defined as $\operatorname{ord}_p(x) = \operatorname{ord}(a) - \operatorname{ord}_p(b)$.

Remark 2.1.6. *For $p \in \mathbb{P}$ and arbitrary $x, y \in \mathbb{Q}$ the following two properties hold:*

- *$\operatorname{ord}_p(xy) = \operatorname{ord}_p(x) + \operatorname{ord}_p(y)$ and*
- *$\operatorname{ord}_p(x + y) \geq \min\{\operatorname{ord}_p(x), \operatorname{ord}_p(y)\}$.*

It is easy to see that the p-adic order is well-defined, as for any $c \in \mathbb{Z} \setminus \{0\}$ and $x = \frac{a}{b} = \frac{ac}{bc}$, we have

$$\operatorname{ord}_p(x) = \operatorname{ord}_p(ac) - \operatorname{ord}_p(bc) = \operatorname{ord}_p(a) - \operatorname{ord}_p(b).$$

Definition 2.1.7. *Let $p \in \mathbb{P}$ be an arbitrary prime number. The p-adic absolute value is defined as the map $|\ |_p : \mathbb{Q} \to \mathbb{R}$, $x \mapsto p^{-\operatorname{ord}_p(x)}$ if $x \neq 0$ and $|0|_p = 0$.*

Proposition 2.1.8. *$|\ |_p$ is an absolute value on $\mathbb{Q}$, the so called p-adic absolute value.*

Proof. The value set of $|\ |_p$ is $\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}$, which shows the first property. The second property is very easy to see as well, as $|xy|_p = p^{\operatorname{ord}_p(xy)} = p^{-\operatorname{ord}_p(x)} p^{-\operatorname{ord}_p(y)} = |x|_p \, |y|_p$.

Now for the triangle inequality, there is nothing to do for the cases $x = 0$, $y = 0$ or $x + y = 0$. Thus consider $x, y \in \mathbb{Q}$ with $x \neq 0$ and $y \neq 0$ and $x + y \neq 0$ and write $x = \frac{a}{b}$ and $y = \frac{c}{d}$, $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}$ with $\gcd(a, b) = 1 = \gcd(c, d)$, then $x + y = \frac{ad+cb}{bd}$ and $\operatorname{ord}_p(x + y) = \operatorname{ord}_p(ad + cb) - \operatorname{ord}_p(b) - \operatorname{ord}_p(d)$, hence

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

All told we have:

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

□

We thusly see that the p-adic absolute value suffices a stronger condition than the triangle inequality, namely the strong triangle inequality $\left|x+y\right|_p \leq \max\{\left|x\right|_p, \left|y\right|_p\}$, which leads to the following

Definition 2.1.9. *An absolute value on a field K is called non-Archimedean if it satisfies the strong triangle inequality. If it does not satisfy this inequality, it is called Archimedean.*

As always in such situations, we want to know when equality holds:

Proposition 2.1.10. *Let K be a field with a non-Archimedean absolute value $|\ |$, then, for $x, y \in K$ with $|x| \neq |y|$, we have $|x+y| = \max\{|x|, |y|\}$.*

The proof is trivial and left to the reader, but we want to at least give an example of this behaviour.

Example 2.1.11. *Let $p \in \mathbb{P}$ be arbitrarily chosen and $x, y \in \mathbb{Z}$ with $\operatorname{ord}_p(x) = n$ and $\operatorname{ord}_p(y) = m$, that is, $x = p^n x^{'}$ and $y = p^m y^{'}$ with $x^{'}, y^{'} \in \mathbb{Z}$ with $p \nmid x^{'} y^{'}$. We have $\left|x\right|_p = p^{-n}$ and $\left|y\right|_p = p^{-m}$.*

Now let $n < m$, then $\left|x\right|_p > \left|y\right|_p$ and $x + y = p^n(x^{'} + p^{m-n}y^{'})$. From $p \nmid x^{'}$ it follows that $p \nmid x^{'} + p^{m-n}y^{'}$ and $\left|x+y\right|_p = p^{-n} = \max\{\left|x\right|_p, \left|y\right|_p\}$.

Now if $n = m$, then $\left|x\right|_p = \left|y\right|_p$ and $x + y = p^n(x^{'} + y^{'})$. We have $p \nmid x^{'}$ and $p \nmid y^{'}$, but it is possible that $p \mid x^{'} + y^{'}$, thus $\operatorname{ord}_p(x+y) \geq n = \min\{\operatorname{ord}_p(x), \operatorname{ord}_p(y)\}$ and we finally get $\left|x+y\right|_p \leq \max\{\left|x\right|_p, \left|y\right|_p\} = \left|x\right|_p = |y|$.

Remark 2.1.12. *Let $|\ |$ be a non-Archimedean absolute value on a field K. We can then define a mapping $\nu : K \to \mathbb{R} \cup \{\infty\}$, $x \mapsto -\log|x|$, if $x \neq 0$, and ∞ else, and we call ν a valuation on K. It has the following properties:*

1. *$\forall x, y \in K : \nu(x+y) \geq \min\{\nu(x), \nu(y)\}$,*
2. *$\forall x, y \in K : \nu(xy) = \nu(x) + \nu(y)$ and*
3. *$\nu(x) = \infty \Leftrightarrow x = 0$.*

Conversely, if ν is a valuation on a field K, then, for $\tau \in \mathbb{R}$ with $\tau > 1$, the map $|\ | : K \to \mathbb{R}$, $x \mapsto \tau^{-\nu(x)}$ defines an absolute value on K. Let us put this into the context of p-adic absolute values. For $x \in \mathbb{Q} \setminus \{0\}$ we have defined the p-adic absolute value as $|x|_p = p^{-\operatorname{ord}_p(x)}$ and we get $\nu(x) = \operatorname{ord}_p(x) \cdot \log p$, thus the valuation ν only differs by a constant from the p-adic order.

Definition 2.1.13. *In the light of the previous remark - to be in conformity with the likes of [Lam], [Ger08], [O'M99] and [Ser70] - we will henceforth call $|\ |_p$ a p-adic valuation and denote by $\nu_p(x) := \operatorname{ord}_p(x)$ the p-adic order of x. The pair $(K, |\ |_p)$ is then called a valuated field. By abuse of language, we will also call an Archimedean absolute value on a field K a valuation on K.*

Non-Archimedean valuations can be used to describe divisibility properties in algebraic number theory, for example we have already seen that a rational number is *small* under a p-adic valuation if it is highly divisible by that prime number.

2.2 Ultrametric spaces

In this section we will take a closer look at the topological properties of fields with non-Archimedean valuations.

Definition 2.2.1. *The pair (X, d) is called a metric space if, for $x, y, z \in X$, the following properties hold:*
1. $d(x, y) \geq 0$ and $d(x, y) = 0 \Leftrightarrow x = y$,
2. $d(x, y) = d(y, x)$ and
3. $d(x, z) \leq d(x, y) + d(y, z)$.

Definition / Remark 2.2.2. *Let $(K, |\ |)$ be a valuated field, then $(K, d_{|\ |})$, with $d_{|\ |}(x, y) := |x - y|$, for all $x, y \in K$, is a metric space.*

Definition 2.2.3. *A metric space (X, d) with*

$$d(x, z) \leq \max\{d(x, y), d(y, z)\},$$

for all $x, y, z \in X$, is called an ultrametric space, the corresponding metric is called an ultrametric.

Proposition 2.2.4. *Let $(K, |\ |)$ be a valuated field, then $d_{|\ |}$ is an ultrametric if and only if $|\ |$ is a non-Archimedean valuation.*

Proof. Let $x, y, z \in K$ be arbitrarily chosen. If

$$d_{|\ |}(x, z) \leq \max\{d_{|\ |}(x, y), d_{|\ |}(y, z)\},$$

then, if we set $x = -y$ and $z = 0$, we get the desired property for the valuation. Now if the valuation is non-Archimedean, then $d_{|\ |}(x, z) = |x - z| = |x - y + y - z| \leq \max\{|x - y|, |y - z|\} = \max\{d_{|\ |}(x, y), d_{|\ |}(y, z)\}$. □

Now we will take the first steps on the path down to the crazy topological world of ultrametric spaces, as in such a space, each triangle is isosceles with at most one shortest side, c.f. Proposition 2.1.10.

Proposition 2.2.5. *Let (X, d) be an ultrametric space and $x, y, z \in X$. If $d(x, y) \neq d(y, z)$, then $d(x, z) = \max\{d(x, y), d(y, z)\}$.*

Definition 2.2.6. *Let (X, d) be a metric space, $c \in X$ and $r \in \mathbb{R}_+^*$. We denote the open, resp. closed, ball with radius r and centre c by*

$$B_r(c) := \{x \in X \mid d(x, c) < r\}$$

and

$$\overline{B_r(c)} := \{x \in X \mid d(x, c) \leq r\}$$

respectively.

Now let $U \subset X$ be a subset of X. U is called open if and only if $\forall x \in U \exists \delta > 0 : B_\delta(x) \subseteq U$. $U^c := X \setminus U$ defines the complement of U and we call U closed if and only if U^c is open.

A point $u \in U$ is a boundary point if for all $\varepsilon > 0$: $B_\varepsilon(u) \cap U \neq \emptyset$ and $B_\varepsilon(u) \cap U^c \neq \emptyset$. We define the set of all boundary points of U with δU.

We define the diameter of U as $\operatorname{diam}(U) := \sup\{d(x,y) \mid x, y \in U\}$ and we call U bounded, if and only if $\operatorname{diam}(U) < \infty$.

For two subsets $U_1, U_2 \subseteq X$, we define the distance between U_1 and U_2 as $d(U_1, U_2) := \inf\{d(u_1, u_2) \mid u_1 \in U_1, u_2 \in U_2\}$.

Now it is time to peek at another marvellous topological wonder in ultrametric spaces.

Proposition 2.2.7. *Let (X, d) be an ultrametric space, $c \in X$ and $r \in \mathbb{R}_+$ then the following statements are true.*

1. *$B_r(c)$ is open and closed.*

2. *For $r > 0$, $\overline{B_r(c)}$ is open and closed.*

Proof. We know that $B_r(c)$ is open (in any metric space). To see that $B_r(c)$ is closed, we have a look at its boundary points. Thus let x be an arbitrary boundary point, $s \leq r$ and $a \in B_r(c) \cap B_s(x)$, thus $d(c,x) \leq \max\{d(c,a), d(a,x)\} < \max\{r,s\} = r$, which means that $x \in B_r(c)$ for all $x \in B_\delta(c)$.

Now we also know that $\overline{B_r(c)}$ is closed (in any metric space). To see that it is open as well, we chose $s \leq r$ and let $x \in \overline{B_r(c)}$ and $a \in B_s(x)$ be arbitrarily chosen, then we get $d(c,a) \leq \max\{d(x,a), d(a,c)\} \leq r$, thus $a \in \overline{B_r(c)}$, which means that $B_s(x) \subseteq \overline{B_r(c)}$ as desired. □

Please note that it was necessary to require $r > 0$ in the second case, otherwise every one-elementary set were an open set, thus every set were open and we were in the case of the discrete topology which isn't too interesting for us. In the first case, this isn't a problem, as $B_0(c)$ is open and closed by definition.

Now we know how balls behave in ultrametric spaces - and as a side node that reminds me of a quote from an analysis professor: "*One day you will learn to appreciate balls*"- but what about the spheres?

Proposition 2.2.8. *In an ultrametric space (X, d) the spheres $S_r(c) := \{x \in X \mid d(x,c) = r\}$, $c \in X$, $r \in \mathbb{R}_+$, are open and closed.*

Proof. $S := S_r(c)$ is closed, because $\overline{B_r(c)} \cap B_r(c)^c = S$, thus as an intersection of closed sets, a closed set itself. This is true for any metric space. Now let $x \in S_r(c)$ and $s < r$. If $a \in B_s(x)$, then from the equality $d(c,a) = \max\{d(a,x), d(x,c)\} = r$, it immediately follows that each point in S possesses an open neighbourhood contained in all of S, thus S is open. □

Remark 2.2.9. *In an ultrametric space (X,d), $S_r(c)$ is no longer the boundary of the open ball $B_r(c)$ and $\delta B_r(c) = \emptyset$. As there are so many sets in an ultrametric space that are both open and closed, the term* clopen *was synthesised to describe those sets.*

Proposition 2.2.10. *Let (X,d) be an ultrametric space, $B_1, B_2 \subseteq X$ open sets, $c \in X$ and $r \in \mathbb{R}_+$, then the following statements are true.*

1. *$\forall x \in B_r(c) : B_r(c) = B_r(x)$, that is, each point of a ball can be chosen as centre of that ball.*

2. *$B_1 \cap B_2 \neq \emptyset \Rightarrow B_1 \subseteq B_2 \vee B_2 \subseteq B_1$, i.e. if two balls have as little as one point in common, one is completely contained in the other.*

3. *$B_1 \cap B_2 = \emptyset \Rightarrow d(b_1, b_2) = d(B_1, B_2)\ \forall b_1 \in B_1, b_2 \in B_2$.*

4. *$\operatorname{diam}(B_r(c)) \leq r$.*

Proof. 1. Let $x \in B_r(c)$ be arbitrarily chosen, then we have $d(c,x) < r$ and

$$\begin{aligned} a \in B_r(c) &\Leftrightarrow d(c,a) < r \\ &\Leftrightarrow d(x,a) \leq \max\{d(x,c), d(c,a)\} \\ &\Leftrightarrow a \in B_r(x). \end{aligned}$$

It follows that $B_r(c) = B_r(x)$. It is now easy to see that this is true for $\overline{B_r(c)}$ as well - simply replace the $<$ with $\leq$.

2. Let B_1, B_2 be open or closed and assume that none of the assertions $B_1 \cap B_2 = \emptyset$, $B_1 \subseteq B_2$ or $B_2 \subseteq B_1$ were true. Then there exist $r, s \in R_+$ and $c \in B_1 \cap B_2$, such that $B_1 = B_r(c)$ and $B_2 = B_s(c)$. Furthermore there exist $x \in B_1 \setminus B_2$ and $y \in B_2 \setminus B_1$. Now from all of this we get $d(y,c) > d(x,c)$, as $x \in B_1$, but $y \notin B_1$, and, at the same time, $d(x,c) > d(y,c)$, as $x \notin B_2$ but $y \in B_2$, which is a contradiction.

3. Again let B_1, B_2 be open or closed, $b_{11}, b_{12} \in B_1$ and $b_2 \in B_2$, then $d(b_{11}, b_{12}) < d(b_{11}, b_2)$ and $d(b_{11}, b_{12}) < d(b_{12}, b_2)$, thus $d(b_{11}, b_2) = d(b_{12}, b_2)$. The desired statement now follows from a symmetry argument.

4. This immediately follows from what we have just seen above.

□

We now want to have a look at p-adic valuations again, remember that a space with a p-adic valuation is an ultrametric space.

Example 2.2.11. *We consider the valuated field $(\mathbb{Q}, |\ |_p)$.*

1. *For $c \in \mathbb{Q}$ we have $B_1(c) = \overline{B_{p^{-1}}(c)}$, thus $B_1(c) = \overline{B_r(c)} = B_r(c)$ for all $r \in (p^{-1}, 1)$. This means that the unit ball in $(\mathbb{Q}, |\ |_p)$ has infinitely many different radii and* $\operatorname{diam}(B_1(c)) = p^{-1} \leq r$.
2. *As an easy exercise one can show that $B_1(0) = \dot{\bigcup}_i^{p-1}(i)$.*

From analysis we recall the following

Definition 2.2.12. *Let X and Y be topological spaces and consider a map $f : X \to Y$, then f is called continuous at a point $x \in X$ if for each neighbourhood V of $f(x)$ there exists a neighbourhood U of x such that $f(U) \subseteq V$. The mapping is called continuous on X if f is continuous at each point of X.*

To further analyse the geometry and topology on p-adic valuations, we need yet another

Definition 2.2.13. *A topological field K, is a field K with a topology, such that the maps $(x, y) \mapsto x + y$, $(x, y) \mapsto xy$ and $K^* \to K^*$, $x \mapsto x^{-1}$ are continuous.*

Remark 2.2.14. *A metric space (X, d) is a topological space, with the topology being induced from the metric d.*

Proposition 2.2.15. *Let $(K, |\ |)$ be a valuated field, then $(K, d_{|\ |})$ is a topological field.*

Proof. It is not too difficult to see that the addition and multiplication maps are continuous mappings from $K \times K$ to K, as for $x_0, y_0 \in K$ arbitrarily chosen, but fixed, $\varepsilon > 0, \delta = \frac{\varepsilon}{2}$ and for all $x \in B_\delta(x_0)$, $y \in B_\delta(y_0)$ we have

$$\begin{aligned} d(x + y, x_0 + y_0) &= |x + y - x_0 - y_0| \\ &= |x - x_0 + y - y_0| \\ &\leq |x - x_0| + |y - y_0| < \varepsilon \end{aligned}$$

and one can deal with the multiplication with a similar computation and argument.

To see that the map $K^* \times K^*$, $x \mapsto x^{-1}$ is continuous, we fix $x_0 \in K^*$ and chose $\delta < \frac{|x_0|}{2}$, for then we have for all $x \in B_\delta(x_0)$:

$$\begin{aligned} d\left(\frac{1}{x}, \frac{1}{x_0}\right) &= \left|\frac{1}{x} - \frac{1}{x_0}\right| \\ &= \frac{|x_0 - x|}{|x|\,|x_0|} < \frac{2\delta}{|x_0|^2}. \end{aligned}$$

□

Definition 2.2.16. *A topological space X is called disconnected, if there exist two disjoint, non-empty open set $X_1, X_2 \subseteq X$ such that $X_1 \cap X_2 = \emptyset$ and $X = X_1 \cup X_2$. If X can not be fragmented like this, X is called a connected space. The connected component of an element $x \in X$ is the union of all sets that contain x. If the connected component of each $x \in X$ is $\{x\}$, then X is called totally disconnected.*

Remark 2.2.17. *Let X be a topological field. For $x \in X$ the set $\{x\}$ is not open, otherwise we were back in the case of the discrete topology, which we have outlawed for being boring.*

As as open ball in an ultrametric space is clopen, we get the following

Proposition 2.2.18. *In an ultrametric space (X, d) each ball $B_r(c)$, $c \in X$, $r > 0$, is disconnected.*

Proposition 2.2.19. *An ultrametric space (X, d) is totally disconnected.*

Proof. Let $x \in X$ be arbitrarily chosen, with connected component Z, and assume that there exists an $y \in Z \setminus \{x\}$ with $r := d(x, y) \neq 0$. Let $Z_1 = B_{\frac{r}{2}}(x)$, we know that $y \notin X_1$. Z_1 is clopen, thus $Z_2 := Z \setminus Z_1$ is open and we found a fragmentation of $Z = Z_1 \dot\cup Z_2$. The desired result now follows from the above proposition. □

Remark 2.2.20. *In ultrametric spaces there exist no connected sets with more than one element.*

2.3 Completions of metric spaces

From a first course in analysis we know that we can complete $(\mathbb{Q}, |\ |_\infty)$ to $\mathbb{R}$, see for example [HS65] chapter one, section 5. In this chapter we will have a look at the completion of arbitrary metric spaces.

Definition / Remark 2.3.1. *Let (X, d) be a metric space. A sequence (x_n) is called a Cauchy-sequence if and only if*

$$\forall \varepsilon > 0\, \exists N \in \mathbb{N} : x_m \in B_\varepsilon(x_n)\ \forall n, m > N.$$

The metric space (X, d) is called complete, if each Cauchy-sequence converges in X. A closed subset $Y \subseteq X$ is complete, if and only if Y is closed.

From the previous chapter we want to recall the notion of a continuous mapping.

Definition / Remark 2.3.2. *Let (X_1, d_1), (X_2, d_2) be two metrical spaces and $x_0 \in X$. A map $f : X_1 \to X_2$ is called continuous in x_0, if*

$$\forall \varepsilon > 0\, \exists \delta > 0\, \forall x \in B_\delta(x_0) : f(x) \in B_\varepsilon(f(x_0)).$$

The map f is called uniformly continuous if

$$\forall \varepsilon > 0\, \exists \delta > 0\, \forall x, y \in X : x \in B_\delta(y) \Rightarrow f(x) \in B_\varepsilon(f(y)).$$

A uniformly continuous map f is continuous and for a Cauchy-sequence (x_n), the image sequence $(f(x_n))$ is again a Cauchy-sequence.

Proposition 2.3.3. *Let (X, d) be a metric space and $Y \subseteq X$ a dense subset of X. Further, let (X', d') be a complete metric space and $f : Y \to X'$ a uniformly continuous map, then there exists exactly one uniformly continuous mapping $\bar{f} : X \to X'$ with $\bar{f}_{|Y} = f$.*

Proof. Assume that we have two extensions of f, namely $\bar{f}_1$ and $\bar{f}_2$, then the set $\bar{X} := \{x \in X \mid \bar{f}_1(x) = \bar{f}_2(x)\}$ is closed. Note that Y is contained in this set and thus, since Y is dense, $\bar{X} = X$, hence $\bar{f}_1 = \bar{f}_2$.

Now how to we construct $\bar{f}$? Let $x \in X$ be arbitrarily chosen, then there exists a sequence $(y_n) \in Y$ with $x = \lim_{n\to\infty} y_n$, thus (x_n) is a Cauchy-sequence in X and, as X' is complete, its image is a converging Cauchy-sequence in X'. Now consider another sequence (z_n) in Y which converges to x as well, which implies that $\lim_{n\to\infty} d(y_n, z_n) = 0$, thus $\lim_{n\to\infty} d(f(y_n), f(z_n)) = 0$. Now we can define $\bar{f}(x) := \lim_{n\to\infty} f(x_n)$, this uniquely defines $\bar{f}$ and by construction we have $\bar{f}_{|Y} = f$ as desired.

To see that $\bar{f}$ is uniformly continuous, we chose an arbitrary $\varepsilon > 0$, then there exists a $\delta > 0$ such, that for $y, z \in Y$ with $z \in B_\delta(y)$ it follows from the uniform continuity of f, that $f(z) \in B_\varepsilon(f(y))$. By considering Cauchy-sequences (y_n) and (z_n) in Y, respectively converging to x_1 and x_2 in X, and applying the same reasoning as above, it is easy to see that, for large enough n, $z_n \in B_\delta(y_n)$ and thus $f(z_n) \in B_\varepsilon(f(y_n))$. Taking this to the limit we get $\bar{f}(x_2) \in B_\varepsilon(\bar{f}_(x_1))$, as desired. □

Definition / Remark 2.3.4. *Again consider two metric space (X_1, d_1), (X_2, d_2) and a surjective mapping $f : X_1 \to X_2$ between them. If for all $x, y \in X$ the map satisfies $d_1(x, y) = d_2(f(x), f(y))$, then we call f an isometry and the two metric spaces are called isometric.*

Isometries are injective and uniformly continuous.

Definition 2.3.5. *Let (X, d) be a metric space and $(\widehat{X}, \widehat{d})$ a complete metric space. If there exists a surjective map $j : X \to \widehat{X}$ such, that* im j *is closed in $\widehat{X}$ and for all $x, y \in X$ we have $d(x, y) = \widehat{d}(j(x), j(y))$, then we call $(\widehat{X}, \widehat{d}, j)$ a completion of (X, d).*

The proof of the following important theorem is given as a guided exercise in [HS65] exercise 6.85.

Theorem 2.3.6. *For any metric space (X, d) there exists exactly one completion, that is, if $(\widehat{X_1}, \widehat{d_1}, j_1)$ and $(\widehat{X_2}, \widehat{d_2}, j_2)$ are two completions of (X, d), then there exists an isometry $\varphi : \widehat{X_1} \to \widehat{X_2}$ with $\varphi \circ j_1 = j_2$.*

Remark 2.3.7. *If $(\widehat{X}, \widehat{d}, j)$ is a completion of (X, d), then j is injective. Thus we can construct a canonical completion of (X, d) with $X \subseteq \widehat{X}$ and we call this canonical completion* the *completion of (X, d) and $j : X \to \widehat{X}$ is then said to be the canonical immersion map.*

We often write $\widehat{X}$ for the completion of (X, d).

Proposition 2.3.8. *Let $(K, |\ |)$ be a valuated field and $\widehat{K}$ its completion, then*

- *The addition and multiplication mappings can uniquely be extended to mappings on $\widehat{K} \times \widehat{K}$.*
- *$\widehat{K}$ is a topological field.*
- *The valuation on K can uniquely be extended to a valuation $\widehat{|\ |} : \widehat{K} \to R_+$, inducing a topology on $\widehat{K}$.*

Proof. As the addition mapping is uniformly continuous on $K \times K$, the statement follows directly from Proposition 2.3.3. The statement for the multiplication on $K \times K$ follows from exercise 18 in [Sch15] (bilinear forms on topological groups).

The fact that $\widehat{K}$ fulfills all the properties of a ring follows readily from what we just said and from Proposition 2.3.3, which basically says that we can extend identities (and inequalities) from a dense subset of X to all of X, as long as the identities (and inequalities) are a composition of continuous mappings. To see that the map $i : K^* \to \widehat{K}$, $x \mapsto x^{-1}$ can be continuously extended, we use the same argumentation as in the proof of Proposition 2.3.3, i.e. we consider a Cauchy-sequence (x_n) in $\widehat{K}$ that converges in $\widehat{K} \setminus \{0\}$, thus $|x_n^{-1} - x_m^{-1}| = \left|\frac{x_m - x_n}{x_m x_n}\right| \leq \frac{1}{C^2} |x_m - x_n|$, for a constant C, which means that we can extend i to a continuous mapping on all of $\widehat{K}^*$.

From $||x| - |y|| \leq |x - y|$ we see that the valuation is uniformly continuous and the last statement again follows from Proposition 2.3.3 or the principle of extending equalities and inequalities. □

Definition / Remark 2.3.9. *We denote with $(\widehat{K}, \widehat{|\ |})$ the completion of a valuated field $(K, |\ |)$ and by $|K| := \{r \in \mathbb{R} \mid \exists k \in K : |k| = r\}$ the value set of $|\ |$. The valuation $\widehat{|\ |}$ is non-Archimedean if and only if $|\ |$ is non-Archimedean. If the valuation is non-Archimedean, then $|K| = \widehat{\left|\widehat{K}\right|}$.*

Proof. The equivalence is clear as the maximum function is continuous. Let $x \in \widehat{K} \setminus \{0\}$ be arbitrarily chosen. As K is dense in $\widehat{K}$, there exists an $y \in K$ such, that $\widehat{|x - y|} < \widehat{|x|}$, thus $|y| = \widehat{|y|} = \widehat{|(y - x) + x|} = \max\{\widehat{|y - x|}, \widehat{|x|}\} = \widehat{|x|}$, which means that $\widehat{|x|} \in |K|$. The fact that $\widehat{K}$ fulfills the properties of a ring follows from □

2.4 The residue class field

In this section we will take a look at the connection between algebraic properties of a field and the properties of a non-Archimedean valuation. For a more detailed and abstract description, see [O'M99] part one, chapter 13.

Proposition 2.4.1. *Let $(K, |\ |)$ be a valuated field with a non-Archimedean valuation, then the set $\mathfrak{o} := \mathfrak{o}_{|\ |} := \overline{B_1(0)}$ is a maximal subring of K and the set $\mathfrak{m} := \mathfrak{m}_{|\ |} := B_1(0)$ is a maximal ideal in $\mathfrak{o}$. Furthermore each $x \in \mathfrak{o} \setminus \mathfrak{m}$ is invertible.*

Proof. It is easy to see that $0 \in \mathfrak{o}$ and $1 \in \mathfrak{o}$. Now let $\alpha, \beta \in \mathfrak{o}$ be arbitrarily chosen, then, from Proposition 2.1.4 and the definition of a non-Archimedean valuation, it immediately follows that $-\alpha, \alpha + \beta$ and $\alpha\beta$ are elements of $\mathfrak{o}$ as well.

To see that $\mathfrak{o}$ is a maximal subring, assume that there exists a subring $\mathfrak{o}'$, with $\mathfrak{o} \subsetneq \mathfrak{o}'$, then there exists $\alpha \in \mathfrak{o}'$ with $|\alpha| > 1$. Define $r = |\alpha|$, then the closed ball $\overline{B_{r^n}(0)}$ is a subset of $\mathfrak{o}'$. Now if we let the radius go to infinity, we see that $K = \bigcup_{n \geq 1} B_{r^n}(0) = \mathfrak{o}'$.

From $|\alpha| \leq 1$ and $|\beta| < 1$, for $\alpha \in \mathfrak{o}$ and $\beta \in \mathfrak{m}$, it immediately follows that $\alpha\beta \in \mathfrak{m}$.

Now let $\alpha \in \mathfrak{o} \setminus \mathfrak{m}$ be arbitrarily chosen. We know that $|\alpha| = 1$, thus α is invertible in $\mathfrak{o}$, since $\left|\frac{1}{\alpha}\right| = 1$, which means that $\frac{1}{\alpha} \in \mathfrak{o}$.

The above argument also shows that $\mathfrak{m}$ is a maximal ideal in $\mathfrak{o}$, as any other $\mathfrak{o}$-ideal $\mathfrak{m}'$ with $\mathfrak{m} \subsetneq \mathfrak{m}'$ contains a unit element ($1 = \alpha\alpha^{-1}$, $\alpha \in \mathfrak{m}' \setminus \mathfrak{m}$) and is thusly equal to $\mathfrak{o}$. □

Definition 2.4.2. *Let $(K, |\ |)$ be a valuated field with a non-Archimedean valuation.*

We define the integers of K w.r.t. the valuation as the elements of the set

$$\mathfrak{o} = \{x \in K \mid |x| \leq 1\}.$$

As a maximal subring of K, $\mathfrak{o}$ is also called the valuation ring of $|\ |$.

The maximal ideal

$$\mathfrak{m} = \{x \in K \mid |x| < 1\}$$

is the valuation ideal of K.

The set

$$\mathfrak{u} = \mathfrak{o} \setminus \mathfrak{m} = \{x \in K \mid |x| = 1\}$$

is the group of units of K w.r.t the valuation.

Remark 2.4.3. *By the strong triangle law it is easy to see that $\mathbb{Z} \subset \mathfrak{o}$. The reader may also show that $K = \mathrm{Quot}(\mathfrak{o})$ and $K = \mathfrak{o}$ if and only if the valuation under consideration is the discrete valuation, which again, is boring. Similarly, and necessarily, $\mathfrak{m} = 0$, if and only if we are working with the trivial valuation.*

Definition / Remark 2.4.4. *A ring R with a unique maximal ideal $\mathfrak{m}$ is called a local ring and in that case we have $\mathfrak{m} = R \setminus R^*$.*

We are now ready to define the residue class field of a valuated field K. Essentially it is the field ${}^{\mathfrak{o}}\!/_{\mathfrak{m}}$, but we want to have more flexibility than the quotient ring permits, for later use, which leads to the following

Definition 2.4.5. *Let $(K, |\ |)$ be a valuated field with a non-Archimedean valuation. A residue class field of K is a pair $(\mathfrak{K}, \varphi)$, with a field $\mathfrak{K}$ and a ring homomorphism $\varphi : \mathfrak{o} \to \mathfrak{K}$ with $\ker \varphi = \mathfrak{m}$.*

Remark 2.4.6. *A valuated field $(K, |\ |)$, with a non-Archimedean valuation, always has at least one residue class field, namely the above mentioned ${}^{\mathfrak{o}}\!/_{\mathfrak{m}}$ with the canonical ring homomorphism. The residue class field is unique, in the sense that if $(\mathfrak{K}_1, \varphi_1)$ and $(\mathfrak{K}_2, \varphi_2)$ are two residue class fields of $(K, |\ |)$, then there exists an unique ring homomorphism $\psi : \mathfrak{K}_1 \to \mathfrak{K}_2$ such that $\psi \circ \varphi_1 = \varphi_2$.*

Example 2.4.7. *In Example 2.2.11 we saw that the closed unit ball is the disjoint union of open balls with radius 1. In algebraic terminology we can interpret the open balls as the residue classes of $\mathfrak{m}$ in $\mathfrak{o}$.*

Remark 2.4.8. *For a p-adic valuation, we also write $\mathfrak{o}_p$, $\mathfrak{m}_p$ and $\mathfrak{u}_p$ instead of $|\ |_p$ in the subscript.*

We will often talk about the residue class field without mentioning the associated homomorphism.

Proposition 2.4.9. *Consider the valuated field $(\mathbb{Q}, |\ |_p)$, then the sets discussed above are as follows.*

1. *The valuation ring is $\mathfrak{o} := \mathfrak{o}_p = \{\frac{x}{y} \in \mathbb{Q} \mid p \nmid b\}$.*
2. *The valuation ideal is $\mathfrak{m} := \mathfrak{m}_p = p\mathfrak{o} = \{\frac{x}{y} \in \mathbb{Q} \mid p \nmid b \wedge p \mid a\}$.*
3. *The residue class field $\mathfrak{K}$ of $(\mathbb{Q}, |\ |_p)$ is isomorphic to $\mathbb{F}_p$.*

Proof. The first two statements immediately follow from the definition of the p-adic valuation. For an element $x = \frac{a}{b} \in \mathbb{Q}$ we know that $|x|_p = p^{-\nu_p(x)}$ and thus x is an element of $\mathfrak{o}$, if and only if its p-adic order $\nu_p(x)$ is greater or equal than 0. As we are obviously working with the irreducible representative of each coset, the previous condition means that $p \nmid b$. With the same argument we see that $x \in \mathfrak{m}$, if and only if $\nu_p(x) > 0$, which means that $p \nmid b \wedge p \mid a$.

Now the only thing left to do is to find an isomorphism between $\mathfrak{K} = {}^{\mathfrak{o}}\!/_{\mathfrak{m}}$ and $\mathbb{F}_p \cong {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. Thereunto define a map

$$\begin{aligned} \varphi : \mathfrak{o} &\to {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \\ \frac{a}{b} &\mapsto (a + p\mathbb{Z})(b^{-1} + p\mathbb{Z}). \end{aligned}$$

This mapping is well-defined, as if $\frac{a^{'}}{b^{'}} \equiv \frac{a}{b}$, then multiplication by the inverse residue class of both b and $b^{'}$ leads to $(a^{'} + p\mathbb{Z})(b^{'-1} + p\mathbb{Z}) = (a + p\mathbb{Z})(b^{-1} + p\mathbb{Z})$, as desired.

To see that φ is surjective, we arbitrarily chose $(a + p\mathbb{Z}) \in {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ and note that $\varphi(\frac{1}{a}) = (a + p\mathbb{Z})$. Particularly we have $\varphi(1) = (1 + p\mathbb{Z})$ and an easy calculation shows that φ is an epimorphism.

From the equation $\varphi(\frac{a}{b}) = (a + p\mathbb{Z})(b^{-1} + p\mathbb{Z}) = 0 \Leftrightarrow a \equiv_p 0$ it follows that $\ker \varphi = p\mathfrak{o}$. The third part of the proposition now follows from the fundamental theorem on homomorphisms. □

Chapter 3

The field of rational numbers

3.1 Valuations on the field of rational numbers

In this chapter we will answer the question how many valuations there are on $\mathbb{Q}$.

Definition 3.1.1. *Two metrics on the same metric space X are called equivalent, if and only if they induce the same topology on X. Two valuations are called equivalent if and only if they induce the same metrics. We use the symbol $\sim$ to denote equivalence of valuations.*

Lemma 3.1.2. *Let $| \ |_1$ and $| \ |_2$ be two valuations on a field K, then the following assertions are equivalent.*
(i) $| \ |_1 \sim | \ |_2$.
(ii) $|\alpha|_1 < 1 \Leftrightarrow |\alpha|_2 < 1$ *for all* $\alpha \in K$.
(iii) $\exists \lambda \in \mathbb{R}_+^* : |\alpha|_1^\lambda = |\alpha|_2$ *for all* $\alpha \in K$.

Proof. [O'M99] 11:4. □

Proposition 3.1.3. *If $| \ |$ is the ordinary absolute value on $\mathbb{Q}$ and $\lambda \in \mathbb{R}_+^*$, then $| \ |^\lambda$ is a valuation on $\mathbb{Q}$, if and only if $\lambda \leq 1$ and in that case, $| \ |^\lambda$ is again equivalent to the ordinary absolute value.*

The proof of this proposition follows readily after a few easy computations, however we do want to show what happens if one choses a $\lambda > 1$.

Remark 3.1.4. *Chose $\lambda \in \mathbb{R}$ with $\lambda > 1$, then $|1+1|^\lambda = |2|^\lambda > 2 = |1|^\lambda + |1|^\lambda$, thus $| \ |^\lambda$ is not a valuation anymore.*

Proposition 3.1.5. *For any non-archimedean valuation $|\ |$ on $\mathbb{Q}$ and $\lambda > 0$, $|\ |^{\lambda}$ is a non-Archimedean valuation on $\mathbb{Q}$.*

Proof. The first two properties of a valuation are clearly satisfied and for $x, y \in \mathbb{Q}$ we have $|x+y|^{\lambda} \leq (\max\{|x|, |y|\})^{\lambda} = \max\{|x|^{\lambda}, |y|^{\lambda}\}$. The equivalence of the two valuations follows from Lemma 3.1.2. □

Remark 3.1.6. *If $|\ | \sim \delta_{\mathbb{Q}}$, then $|\ | = \delta_{\mathbb{Q}}$, as $\forall \lambda > 0 : \delta_{\mathbb{Q}}^{\lambda}(x) = 1^{\lambda} = 1$, for all $x \in \mathbb{Q}$ and $\delta_{\mathbb{Q}}^{\lambda}(0) = 0^{\lambda} = 0$. In other words, the discrete valuation is equivalent to itself and itself alone.*

Proposition 3.1.7. *For two distinct primes p and q, the p-adic and q-adic valuations are not equivalent.*

Proof. Consider the sequence $(x_n)_{n\geq 1} = \left(\left(\frac{p}{q}\right)^n\right)_{n\geq 1}$. With Lemma 3.1.2 it then follows that $\lim_{n\to\infty} |x_n|_p = 0$, but $\lim_{n\to\infty} |x_n|_q = \infty$. □

Remark 3.1.8. *If two valuations are equivalent, they are either both Archimedean or both non-Archimedean.*

Definition / Remark 3.1.9. *From now on we denote the ordinary absolute value on $\mathbb{Q}$ with $|\ |_{\infty}$.*

We will soon give a brief explanation as to why we chose to make the above definition, but first we will finally have a look at one of the most important theorems in the field of p-adic numbers.

Theorem 3.1.10 (Theorem of Ostrovskij)**.** *Every non-trivial valuation on $\mathbb{Q}$ is equivalent to $|\ |_{\infty}$ or $|\ |_p$, for a $p \in \mathbb{P}$.*

Proof. It is clear that a p-adic valuation is not equivalent to $|\,|_{\infty}$, since the former is non-Archimedean and the latter is Archimedean, see Remark 3.1.8. That, for two distinct primes p and q, the p-adic and q-adic valuations are not equivalent was stated and proven in Proposition 3.1.7. For further details and a complete proof see [O'M99] 31:1. □

Now that we know all the possible valuations on $\mathbb{Q}$ we want to see how they are connected.

Proposition 3.1.11. *Let $x \in \mathbb{Q} \setminus \{0\}$ be arbitrarily chosen, then*

$$|x|_{\infty} \cdot \prod_{p\in\mathbb{P}} |x|_p = 1$$

.

Proof. W.l.o.g. we can assume that $x \in \mathbb{N}$, else we use the first two properties of valuations. Now we can write $x = \prod_{i=1}^{r} p_i^{k_i}$ and we see that

- $|x|_q = 1$, for $q \neq p_i$, $1 \leq i \leq r$,
- $|x|_{p_i} = p_i^{-k_i}$, for $1 \leq i \leq r$ and
- $|x|_\infty = \prod_{i=1}^{r} p_i^{k_i}$.

□

Corollary 3.1.12. *For any number $n \in \mathbb{N}$ we have $|n|_p \geq \frac{1}{n}$.*

Proof. It is clear that $|n|_\infty = n$ and we again write $n = \prod_{i=1}^{r} p_i^{k_i}$, then it follows that $|n|_q = 1$, if $q \neq p_i$, for all $1 \leq i \leq r$, and $|n|_{p_i} = p_i^{-k_i} = \frac{\prod_{j=1}^{i-1} p_j^{k_j} \cdot \prod_{j=i+1}^{r} p_j^{k_j}}{n} \geq \frac{1}{n}$ else, as desired. □

Remark 3.1.13. *This product formula is a, rather simple, example as to why looking at all the valuations of $\mathbb{Q}$ at the same time can lead to interesting results. For example, knowing all the values w.r.t. to all the norms, but one, we can easily recover the missing value - this is a very important concept in number theory. We will come back to this topic in a later chapter, when we briefly talk about the Hasse-Minkowski principle.*

Furthermore, to emphasize the close relation of all those valuations, mathematicians introduced the idea of attaching a prime number *to the absolute value, the so called* prime *at infinity. Thus, for example, we could write the above product formula as $\prod_{p \in \mathbb{P} \cup \{\infty\}} = 1$. Note that not all mathematicians adhere to that convention.*

3.2 The incompleteness of the field of rational numbers

It is well known that $(\mathbb{Q}, |\ |_\infty)$ is not complete, see Example 3.2.3. Now, after Ostrovskij told us the secret about all the different valuations on $\mathbb{Q}$, we want to answer the obvious question whether the $(\mathbb{Q}, |\ |_p)$ are complete or not.

Lemma 3.2.1. *A sequence (x_n) in $\mathbb{Q}$ is a Cauchy-sequence w.r.t $|\ |_p =: |\ |$, if and only if*

$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0.$$

Proof. If (x_n) is a Cauchy-sequence, then with $m = n + 1$ the desired follows immediately. Conversely, w.l.o.g. let $m > n$. As the valuation is non-Archimedean, we have

$$\begin{aligned} |x_m - x_n| &= |x_m - x_{m-1} + x_{m-1} - x_{m-2} + \ldots + x_n| \\ &\leq \max\{|x_m - x_{m-1}|, |x_{m-1} - x_{m-2}| \ldots |x_{n-1} - x_n|\}. \end{aligned}$$

□

Note that in the above lemma the necessary condition is true for any valuation, but it is not sufficient for Archimedean valuations, as shows the next

Example 3.2.2. *Consider the sequence $x_n = \sum_{i=1}^n \frac{1}{n}$, then $|x_{n+1} - x_n|_\infty = \frac{1}{n+1}$ and thus $\lim_{n\to\infty} |x_{n+1} - x_n|_\infty = 0$, but the sequence can't be a Cauchy-sequence since it doesn't even converge.*

The next example will be a crucial role in what is yet to come.

Example 3.2.3. *There exists a Cauchy-sequence $(x_n)_{n\geq 1}$ in $\mathbb{Q}$ such, that $|x_n^2 - 2|_\infty < 10^{-n}$, but $\lim x_n = \sqrt{2} \notin \mathbb{Q}$.*

We are now ready to answer the above question.

Theorem 3.2.4. *For all $p \in \mathbb{P} \cup \{\infty\}$, the valuated field $(\mathbb{Q}, |\ |_p)$ is not complete.*

Proof. This requires a rather lengthy computation, thus for now we will just sketch the idea of the proof. The idea is to find a Cauchy-sequence in $\mathbb{Q}$ with a limit not in $\mathbb{Q}$. Now chose $a \in \mathbb{Q}$ such, that a is not a square, $p \nmid a$ and a is a square modulo p (this is possible, since there are $\frac{1}{2}(p-1)$ quadratic residues smaller than p, but only $\sqrt{p}$ squares).

To construct the desired Cauchy-sequence, we chose a solution x_0 of $x^2 \equiv_p a$ and extend it, that is, we want x_1 to fulfill $x_1 \equiv_p x_0$ and $x_1^2 \equiv_{p^2} a$ and we further chose x_n such, that $x_n \equiv_{p^n} x_{n-1}$ and $x_n^2 \equiv_{p^{n+1}} a$.

To show that such a sequence exists, corresponds to show the existence of solutions of $f(x) \equiv_{p^n}= 0$, where f is a polynomial in $\mathbb{Z}[X]$, which can be done by induction, but is rather tedious and we will come back to similar questions in a later section on Hensels lemmas.

Using Lemma 3.2.1, we immediately see that the constructed sequence is really a Cauchy-sequence in $\mathbb{Q}$ (without a limit in $\mathbb{Q}$). □

Remark 3.2.5. $(\mathbb{Q}, \delta_{\mathbb{Q}})$ *is complete. Since the only possible values are* 0 *and* 1*, a sequence* (x_n) *is a Cauchy-sequence w.r.t.* $\delta_{\mathbb{Q}}$*, if and only if there exists a natural number* $N \in \mathbb{N}$ *such, that* $\forall n, m > N : \delta_{\mathbb{Q}}(x_m - x_n) = 0$*, from which it immediately follows that* $x_m = x_n$*. Thus the sequence will eventually become constant, thus convergent, yet, as said before, this case is boring.*

Exercise 3.2.6. *Only considering prime numbers up to* 100*, we see that* $X^2 \equiv_{p^n} 2$*,* $n \in \mathbb{N}$*, has no solutions for* $p = 3, 5, 11, 13, 29, 37, 43, 47, 53, 59, 61, 67, 83$*, one solution for* $p = 2$ *and in all other cases, that is, for* $p = 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97$*, there are two solutions.*

Work out the details of the above construction for a suitable prime of your choice.

Chapter 4

The field of p-adic numbers

In this chapter we will finally introduce the field of p-adic numbers.

4.1 p-adic numbers and integers

We have seen that every metric space possesses a completion w.r.t. its metric, c.f. Theorem 2.3.6, so what exactly does $(\widehat{\mathbb{Q}}, \widehat{|\ |_p})$ look like?

Definition 4.1.1. *Let $p \in \mathbb{P}$ be an arbitrary chosen prime number. The completion of $(\mathbb{Q}, |\ |_p)$ is called the field of p-adic numbers and denoted by $\mathbb{Q}_p$.*

Remark 4.1.2. *Using results from the previous two chapters we immediately see that*

- *$\mathbb{Q}$ is dense in $\mathbb{Q}_p$,*
- *$|\ |_p$ can be uniquely extended to a non-Archimedean valuation on $\mathbb{Q}_p$, we will denote the extension again by $|\ |_p$ and*
- *$|\mathbb{Q}_p|_p = |\mathbb{Q}|_p = \{p^n \mid n \in \mathbb{Z}\} \cup \{0\}$, i.e. $\forall x \in \mathbb{Q}_p \, \exists n \in \mathbb{Z}$ such, that $|x|_p = p^{-n}$.*

Definition 4.1.3. *A p-adic integer is an element of the ring*

$$\mathbb{Z}_p := \mathfrak{o}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}.$$

Remark 4.1.4. *As for all $z \in \mathbb{Z}$ we have $|z|_p \leq 1$, it is clear that $\mathbb{Z} \subseteq \mathbb{Z}_p$.*

Proposition 4.1.5. *Let $a \in \mathbb{Z}_p$ be arbitrary chosen, then there exists a unique sequence (a_i) of integers (representing a) such, that for all $i \geq 0$ the sequence fulfills $0 \leq a_i < p^{i+1}$ and $a_i \equiv_{p^{i+1}} a_{i+1}$. This sequence converges to a, w.r.t. $|\ |_p$ and it immediately follows that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.*

Proof. As $\mathbb{Q}$ lies dense in $\mathbb{Q}_p$, there exists a sequence $\left(\frac{a_n}{b_n}\right)_{n\geq 0} \in \mathbb{Q}$ with $\gcd(a_n, b_n) = 1$ for all n such, that $a = \lim_{n\to\infty}\left(\frac{a_n}{b_n}\right)$. Now if we chose n large enough, p is not a divisor of b_n, else, since $\gcd(a_n, b_n) = 1$ and $p \nmid a_n$, we had $\frac{|a_n|_p}{|b_n|_p} = \frac{1}{|b_n|_p} \geq p > 1$, which is a contradiction to $x \in \mathbb{Z}_p$. Thus there exists $u_n \in \mathbb{Z}$ with $b_n u_n \equiv_{p^n} 1$ and because $|b_n|_p = 1$ and $|a_n|_p \leq 1$, we get the following equation:

$$\begin{aligned}
|a - a_n u_n|_p &= |b_n|_p\,|a - a_n u_n|_p \\
&= |b_n a - b_n a_n u_n|_p \\
&\leq |b_n a - a_n|_p + |a_n - b_n a_n u_n|_p \\
&= |b_n|_p \left|a - \frac{a_n}{b_n}\right|_p + |a_n|_p\,|1 - b_n u_n|_p \\
&\leq \left|a - \frac{a_n}{b_n}\right|_p + p^{-n}.
\end{aligned}$$

From this equation we immediately see that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Thus there exists an integer $z_0 \in \mathbb{Z}$ with $z_0 \in B_{p^{-1}}(a)$ and a_0 can be chosen in such a way, that $a_0 \equiv_p z_0$, which means that $a_0 \in B_{p^{-1}}(a)$. The rest of the proof is done by induction on the length of the sequence, thus assume that $a_0, \ldots, a_s$ have already been constructed, which means that $\frac{a-a_s}{p^{s+1}} \in \mathbb{Z}_p$ and thus the existence of an integer $z \in B_{p^{-1}}(\frac{a-a_s}{p^{s+1}})$ in ensured. By defining $a_{s+1} := a_s + zp^{s+1}$ we get $a_{s+1} \equiv_{p^{s+1}} a_s$ and $0 \leq a_{s+1} < p^{s+1} + (p-1)p^{s+1} \leq p^{-s-2}$, as desired, as by this construction we have $a_i \in B_{p^{-i-1}}(a)$, for all i, and thus the constructed sequence converges to a w.r.t. the p-adic valuation.

To see that this sequence is unique, we simply chose a second sequence (b_i) with the same properties. Now assuming that j is the smalled index such, that $a_j \neq b_j$, we notice that $a_j \equiv_{p^{j+1}} a_{j-1} = b_{j-1} \equiv_{p^{j+1}} b_j$, with $0 \leq a_j, b_j \leq p^{j+1}$, which means that $a_j = b_j$ after all. □

Remark 4.1.6. *$\mathbb{Z}_p$ is, as a closed subset of a complete space, complete. As the valuation on $\mathbb{Q}$ can be uniquely extended to a valuation on $\mathbb{Q}_p$, for $x, y \in \mathbb{Z}$ we obviously get that $|x - y|_p$ takes the same value in $\mathbb{Z}$ as it would in $\mathbb{Z}_p$, thus, in the light of chapter 2, section 3, we can consider $\mathbb{Z}_p$ as the completion of $\mathbb{Z}$ w.r.t. $|\ |_p$.*

Proposition 4.1.7. *Each $a \in \mathbb{Z}_p$ can be uniquely written in the form*

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

with $0 \leq a_i \leq p - 1$.

Proof. To see that the series converges to a, we notice that the partial sums correspond to the a_i in the sequence of the previous theorem. □

We can generalize this idea to the p-adic numbers as follows: let $x \in \mathbb{Q}_p$, $x \notin \mathfrak{o}(p)$, then $|x|_p = p^m$, $m \in \mathbb{N}$. Now a multiplication of x by p^m yields $x' := xp^m$, $x' \in \mathfrak{u}(p)$ and

$$\begin{aligned} x &= \frac{1}{p^m} \sum_{i=0}^{\infty} x_i' p^i \\ &= \sum_{i=-m}^{\infty} x_i p^i, \end{aligned}$$

which leads to the following

Theorem 4.1.8. *Each element $x \in \mathbb{Q}_p$ can be written as*

$$x = \sum_{i=-m}^{\infty} x_i p^i,$$

where $x_{-m} \neq 0$ and $x_i \in \{0, 1, \ldots, p-1\}$. This representation is unique and called the p-adic representation of x.

Now the natural question to ask is how exactly are p-adic valuations and the p-adic representation of rational numbers connected?

Proposition 4.1.9. *Let $x := \sum_{i=0}^{\infty} x_i p^i$, $x_i = 0$ for $0 \leq i \leq k$, $k \in \mathbb{N}$ and $x_k \neq 0$, then $|x|_p = p^{-k}$. For $x := \sum_{i=-m}^{\infty} x_i p^i$, $x_{-m} \neq 0$, we have $|x|_p = p^m$.*

Proof. The partial sums a_n of the series $\sum_{i=0}^{\infty} x_i p^i$ converge to x, thus, in the first case, we get

$$\begin{aligned} |x|_p &= |x - a_n + a_n|_p \\ &\leq \max \left\{ \left| \sum_{i=k}^{n} x_i p^i \right|_p, \left| \sum_{i=n+1}^{\infty} x_i p^i \right|_p \right\} \\ &\leq \max\{p^{-k}, p^{-n-1}\}, \end{aligned}$$

from which it immediately follows that $|x|_p = p^{-k}$ for all $n \geq k$.

The proof of the second case is similar. □

Remark 4.1.10. *What we just said is that it is easy to compute the distance between two p-adic integers a, b if their p-adic expansion is known, as clearly, if their first n digits are equal, then p^n divides $a - b$, that is, in that case, $b \in B_{p^{-n}}(a)$.*

Due to the previous propositions we can extend our definition of the order of an element to all of $\mathbb{Q}_p$, namely $\nu_p(x) = \mathrm{ord}_p(x) = k$, or $\nu_p(x) = \mathrm{ord}_p(x) = -m$.

Corollary 4.1.11. *The p-adic units are $Z_p^* := \mathfrak{u}_p = \{a \in \mathbb{Z}_p \mid |a|_p = 1\}$. Using the unique p-adic representation, this set can be written as*

$$\{a = \sum_{i=0}^{\infty} a_i p^i \mid x_0 \neq 0\}.$$

Corollary 4.1.12. *For $x \in \mathbb{Z}_p$ with $|x|_p = p^{-n}$, $n \in \mathbb{Z}$, there exists a unit $\varepsilon \in \mathfrak{u}_p$ such, that $x = \varepsilon \cdot p^n$.*

Example 4.1.13. $-1 \in \mathbb{Q}_p$*: $0 = 1+\sum_{i=0}^{\infty} p^i(p-1)$, thus $-1 = \sum_{i=0}^{\infty} p^i(p-1)$ and $\nu_p(p) = 1$, which means that the series actually converges. There is no notion of* negative *numbers in $\mathbb{Q}_p$.*

Example 4.1.14. $x = \frac{90}{109} = 2^1 \cdot 3^2 \cdot 5^1 \cdot 23^{-1} \cdot 83^{-1}$*, thus $|x|_2 = \frac{1}{2}$, $|x|_3 = \frac{1}{9}$, $|x|_5 = \frac{1}{5}$, $|x|_2 3 = 23$, $|x|_8 3 = 83$ and $|x|_p = 1$ for all other $p \in \mathbb{P}$.*

Example 4.1.15. $51 - 3 = 48 = 2^4 \cdot 3^1$*, thus $d_2(3, 51) = \frac{1}{16}$, $d_3(3, 51) = \frac{1}{3}$ and $d_p(3, 51) = 1$ for all other $p \in \mathbb{P}$.*

Example 4.1.16. *In $\mathbb{Q}_5$ the sequence $(1, 5, 5^2, 5^3, \ldots)$ is a zero sequence and the sequence $(1, \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots)$ is bounded, but not a Cauchy-sequence, since $d_5(\frac{1}{2^n}, \frac{1}{2^{n+1}}) = \left|\frac{1}{2^{n+1}}\right|_5 = 1$.*

Remark 4.1.17. *The unique p-adic representation yields a bijection*

$$\begin{aligned} \left(\mathbb{Z}/p\mathbb{Z}\right)^{\mathbb{N}} &\to \mathbb{Z} \\ (\ldots, a_2, a_1, a_0) &\mapsto \sum_{i=0}^{\infty} a_i p^i, \end{aligned}$$

thus the cardinality of $\mathbb{Z}_p$ equals the cardinality of the continuum, i.e. $\#\mathbb{Z}_p = p^{\#\mathbb{N}} = 2^{\aleph_0}$.

4.2 Algebraic and topological properties

We recall the definitions of the valuation ring

$$\mathfrak{o} = \{x \in K \mid \nu(x) \geq 0\} = \{x \in K \mid |x| \leq 1\},$$

the units

$$\mathfrak{u} = \{x \in K \mid \nu(x) = 0\} = \{x \in K \mid |x| = 1\}$$

and the corresponding maximal ideal

$$\mathfrak{m} = \{x \in K \mid \nu(x) > 0\} = \{x \in K \mid |x| < 1\}.$$

We have seen that $Z_p := \overline{B_1(0)} \cong \mathfrak{o}_p$, i.e. the open unit ball in $\mathbb{Q}_p$ is the valuation ring. This ring $\mathfrak{o}_p$ is a local ring with maximal ideal $\mathfrak{m} = \mathbb{Z}_p \backslash \mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid |x|_p < 1\} = \{x \in \mathbb{Z}_p \mid x_0 = 0\} = \{x = p \sum_{i=0}^{\infty} x_{i+1} p^i\} = p\mathbb{Z}_p$.

Remark 4.2.1. *The map $\varphi_p : \mathbb{Z}_p \to \mathbb{Z}$, $a = \sum_{i=0}^{\infty} a_i p^i \mapsto a_0$, defines an epimorphism from $\mathbb{Z}_p$ to $\mathbb{F}_p = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ and is called the reduction map modulo p. Furthermore the kernel of φ_p is $\ker \varphi_p = \{x \in \mathbb{Z}_p \mid x_0 = 0\} = p\mathbb{Z}_p$, thus, from the fundamental theorem of homomorphisms, we see that*

$${}^{\mathbb{Z}_p}\!/_{p\mathbb{Z}_p} \cong \mathbb{F}_p = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}.$$

Remark 4.2.2. *For the valuation ring, units and maximal ideal, we have the following set equalities:*

- $\mathbb{Z}_p \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\} = \mathfrak{o}_p$,
- $p\mathbb{Z}_p \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b \land p \mid a\} = \mathfrak{m}_p$ *and*
- $\mathbb{Z}_p^* \cap \mathbb{Q} = {}^{\mathbb{Z}_p}\!/_{p\mathbb{Z}_p} \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid ab\} = \mathfrak{u}_p = {}^{\mathfrak{o}_p}\!/_{\mathfrak{m}_p}$.

Proposition 4.2.3. *The valuation ring $\mathfrak{o}_p = \mathbb{Z}_p$ is a principal ideal domain, with the principal ideals $\{0\}$ and $p^n\mathbb{Z}_p$ for all $n \in \mathbb{N}$.*

Proof. As $\mathbb{Z}_p \subseteq \mathbb{Q}_p$, it is an integral domain.

Now let $\mathfrak{a} \neq \{0\}$ be an ideal in $\mathfrak{o}_p$ and consider an element $a \in \mathfrak{a} \setminus \{0\}$ of maximal absolute value. Such an element can be found, since the value set is discrete. Furthermore let n be the p-adic order of a, then $a = \varepsilon \cdot p^n$, for a unit $\varepsilon \in \mathfrak{u}_p$, thus $p^n = \varepsilon^{-1} \cdot a \in \mathfrak{a}$, which means that $(p^n) = p^n\mathfrak{o}_p \subset \mathfrak{a}$.

Conversely, for each $a \in \mathfrak{a}$ we have $|a|_p = p^{-m} \leq p^{-n}$, thus $a = \varepsilon p^m = \varepsilon p^n p^{m-n} \in p^n\mathfrak{o}_p$, therefore $\mathfrak{a} \subseteq p^n\mathfrak{o}_p$. □

Remark 4.2.4. *As $\mathfrak{o}_p = \mathbb{Z}_p$ is an integral domain, $\mathbb{Q}_p$ can be considered as its quotient field* $\mathrm{Quot}(\mathbb{Z}_p)$ *and $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$. For $a \in \mathbb{Z}_p \setminus \{0\}$, $a = \varepsilon p^n$, for a unit $\varepsilon \in \mathfrak{u}_p$, it is easy to see that $a^{-1} \in p^{-n}\mathbb{Z}_p$.*

We have seen that we can write each $x \in \mathbb{Q}_p$ as $x = p^m x^{'}$, with $m \in \mathbb{Z}$ and $x^{'} \in \mathbb{Z}_p$. What does this mean in a more topological language?

Proposition 4.2.5. *The balls $p^n\mathbb{Z}_p$, for all $n \in \mathbb{Z}$, constitute a neighbourhood basis of 0, which covers all of $\mathbb{Q}_p$.*

Proof. $B_1(0) = \mathbb{Z}_p \subseteq \mathbb{Q}_p$ is clopen, thus it is an open neighbourhood of 0. The map $\mathbb{Q}_p \to \mathbb{Q}_p$, $x \mapsto px$ is a homeomorphism, thus $p^n\mathbb{Z}_p$ is an open neighbourhood of 0. Now from the p-adic representation it follows that $\mathbb{Q}_p = \bigcup_{n\in\mathbb{Z}} p^n\mathbb{Z}_p$ and those $p^n\mathbb{Z}_p$ actually are a neighbourhood basis for 0, as for any arbitrary open set U around 0, there exists a $n_0 \in \mathbb{Z}$ such, that $B_{p^{-n_0}}(0) \subseteq U$. □

Remark 4.2.6. *Once again we have a strong connection between the topological and algebraic properties of p-adic numbers, as for an element $x \in \mathbb{Q}_p$ we can consider $\nu_p(x)$ as the largest number, such that $x \in p^{\nu_p(x)}\mathbb{Z}_p$.*

Example 4.2.7. *Consider $x = x_{-5}p^{-5} + x_{-4}p^{-4} + \ldots + x_{-1}p^{-1} + x_0 + x_1 p + x_2 p^2 + \ldots$, $x_{-5} \neq 0$, then it is clear that $x \in p^{-5}\mathbb{Z}_p$, but $x \notin p^{-4}\mathbb{Z}_p$, as from $x = p^{-4}(x_{-5}p^{-1} + x_{-4} + x_{-3}p + \ldots + x_0 p^4 + x_1 p^5 + \ldots) = p^{-2}x^{'}$ we see that $x^{'} \notin \mathbb{Z}_p$ and thus $\nu_p(x) = -5$.*

Remark 4.2.8. *For $n \in \mathbb{N}$ and $x, y \in \mathbb{Q}_p$ we have*

$$y \in B_{p^{-n}}(x) \Leftrightarrow x - y \in p^n\mathbb{Z}_p$$

and we write $x \equiv_{p^n} y$, or even shorter $x \equiv_n y$.

Definition 4.2.9. *A Hausdorff[1] space is a topological space in which each pair of distinct points of X have disjoint neighbourhoods.*

Proposition 4.2.10. *Every metric space (X, d) is a Hausdorff space.*

Proof. We have to show that the topology induced by the metric d is Hausdorff. Let $x, y \in X$ be two distinct points, that is, $d(x, y) \neq 0$ and consider the open balls $B_x := B_{\frac{d(x,y)}{2}}(x)$ and $B_y := B_{\frac{d(x,y)}{2}}(y)$. Those are obviously open sets in X and to see that they are disjoint, we assume there exists a $z \in B_x \cap B_y$, but that means that $d(x, z) < \frac{d(x,y)}{2}$ and $d(y, z) < \frac{d(x,y)}{2}$, thus $d(x, z) + d(z, y) < d(x, y)$, which is a contradiction to the triangle inequality. □

[1] Felix Hausdorff (* 1868; Breslau, today Wrocław, capital of the Lower Silesian Voivodeship in Poland; † 1942 Bonn), one of the founders of the theory of topology, was a German mathematician and a philosopher under the pseudonym Paul Mongré.

Example 4.2.11. *The converse of the above remark is not true, for example consider the set of all ordinal numbers with the discrete order topology.*

The following well known proposition and its corollary seem inconspicuous, but they play an important role in what is yet to come, as well as in [Sch15].

Proposition 4.2.12. *Let X be a Hausdorff space. Suppose that $Y \subseteq X$ and that a is a limit point of A. Then each neighbourhood of a contains infinitely many points of A.*

Corollary 4.2.13. *In a Hausdorff space the limit of a sequence is uniquely defined. This astonishing fact is not true for general topological spaces.*

Proposition 4.2.14. *The p-adic field $\mathbb{Q}_p$ is a totally disconnected Hausdorff space.*

Proof. As a metric space $\mathbb{Q}_p$ is a Hausdorff space (Proposition 4.2.10) and since its metric is an ultrametric, $\mathbb{Q}_p$ is totally disconnected, as seen in Proposition 2.2.19. □

Definition 4.2.15. *A metric space (X, d) is called compact, if and only if for each open cover of X there exists a finite subcover of X. The metric space is called locally compact, if and only if every $x \in X$ has a compact neighbourhood.*

Proposition 4.2.16. *The set of all the the balls in $\mathbb{Q}_p$ is countable.*

Proof. For any arbitrary ball $B_r(x)$ with radius r, we know that there exists an integer $z \in \mathbb{Z}$, such that $r = p^{-z}$. With Proposition 4.1.8 we can write $x = \sum_{i=-m}^{\infty} x_i p^i$. Now if we take the z-th partial sum z_0 of this series, we easily see that $z_0 \in B_{p^{-z}}(a)$ and this, together with the fact that the set of possible radii is countable, see Example 2.2.11, proves the proposition. □

Proposition 4.2.17. *The field $\mathbb{Q}_p$ is locally compact with compact valuation ring $\mathbb{Z}_p$.*

Proof. Using the uniqueness of the p-adic expansion (Proposition 4.1.7) and the pigeonhole principle, we can construct a sequence of subsequences, proving that $\mathbb{Z}_p$ is sequentially compact, thus as a metric space, compact, see for example [HS65] theorem 6.37. Let (a_n) be a sequence in $\mathbb{Z}_p$ and for each n write $a_n = \sum_{i=0}^{\infty} a_i^{(n)} p^i$, then, by the pigeonhole principle, we can find an element $b_0 \in \{0, \dots, p-1\}$, with $a_0^{(n)} = b_0$, for infinitely many n. This yields a subsequence of (a_n), namely $(a_{b_0 n})$, whose terms all have b_0 as first digit in their p-adic expansion. Repeating this construction inductively we obtain the desired sequence of subsequences of (a_n), $((a_{b_k n})_n)_k$ with $(a_{b_k n})_n$ being a subsequence of $(a_{b_{k+1} n})_n$, as well as a p-adic integer $b = \sum_{i=0}^{\infty} b_k p^k$ such, that every term of $(a_{b_k n})_n$ has the same $k+1$-first digits as b. It is then clear that the sequence of the diagonals $(a_{b_k k})$ is a subsequence of (a_n) which converges to b, which proves that $\mathbb{Z}$ is sequentially compact, as desired.

As $\mathbb{Z}_p = \mathfrak{o}_p = \overline{B_1(0)} = B_p(0)$, it is evident that every ball in $\mathbb{Q}_p$ is compact, thus $\mathbb{Q}_p$ is locally compact. □

4.3 Visualization of p-adic numbers

Our visual perception, whether due to high exposure from a young age or simply because of the biological properties of our brain I do not know, is based on standard Euclidean geometry. I doubt the physical universe is Euclidean in its geometry, but it is very clear that humankind relies on Euclidean geometry to perceive the universe. So strong is this reliance that even in the setting of p-adic topology, which clearly is not Euclidean, we have found a way to picture it using Euclidean geometry - as a matter of fact, we even used a language borrowed from Euclidean geometry and topology, such as balls and spheres, to talk about p-adic topology. However, the landscape created by p-adic topology is completely different to our intuition, thus, for example, as we have already seen, the notions of open and closed balls becomes meaningless.

The goal of this section is to visualize the p-adic integers within our familiar framework of Euclidean geometry.

It is interesting to note that the topology on $\mathbb{Z}_p$ is inherently fractal, that is, $\mathbb{Z}_p$ is homeomorphic to the Cantor set and $\mathbb{Q}_p$ is homeomorphic to a finite disjoint union of Cantor sets. Consider the open set $C_0 := [0, 1]$ and *delete* the middle third, obtaining the compact set $C_1 = [0, \frac{1}{3}] \cup [\frac{2}{3}, 1]$. Iterating on this construction we get a decreasing sequence of nested compact subspaces of the unit interval C_0, where each C_n consists of 2^n closed intervals of length 3^{-n}.

Definition 4.3.1. *A topological space that is homeomorphic to a complete metric space with a countable dense subset is called a Polish space, that is, a Polish space is a separable, completely metrizable topological space. The spaces are named in honour of Polish topologists - Sierpiński[2], Kuratowski[3] and Tarski[4] who, among others, extensively studied them first.*

Remark 4.3.2. *Note that Polish spaces are not necessarily metric spaces, they admit many different complete metrics which then induce the same topology. A polish space with an unique metric is called a Polish metric space.*

Example 4.3.3. $\mathbb{R}^n, \mathbb{C}^n, [0, 1]$, $\mathbb{Z}_p^n$ *and* $\mathbb{Q}_p^n$ *are Polish spaces.*

[2] Wacław Franciszek Sierpiński (* 1882 Warsaw; † 1969 ibidem)

[3] Kazimierz Kuratowski (* 1896 Warsaw; † 1980 ibidem)

[4] Alfred Tarski Tajtelbaum (* 1901 Warsaw; † 1983 Berkeley, USA)

Definition / Remark 4.3.4. *Let $C_A := \bigcup_{i\in\mathbb{Z}}(2i, 2i+1)$ and for $n \in \mathbb{N}$ inductively define $C_n = C_{n-1} \cap (3^{-n}C_A)$, then the set $C := \bigcap_{i=0}^{\infty} C_i$, the so called Cantor*[5] *set, is uncountably infinite and compact.*

Now consider the 3-adic expansion of a natural number $x = \sum_{i=0}^{\infty} x_i 3^i$, then the construction of C_1 corresponds to removing those $x \in C_0$ with $x_0 = 1$, the construction of C_2 corresponds to removing those x with $x_1 = 1$ and so on. In iteration we see that the Cantor set C consists of elements that admit a 3-adic expansion of the form: $\sum_{i=1}^{\infty} \alpha_i 3^{-i}$, with $\alpha_i \in \{0, 2\}$. This *doubling* of the binary representation leads to the following

Remark 4.3.5. *The Cantor set is homeomorphic to the Cantor space $(C, |\ |)$ with the discrete topology. The Cantor space is a perfect, totally disconnected, uncountably infinite, compact Polish space. The actual homeomorphism is given by the above construction using the ternary numeral system.*

Proposition 4.3.6. *The sets $(\mathbb{Z}_2, |\ |_2)$ and $(C, |\ |)$ are homeomorphic. A homeomorphism is given by $\varphi : \mathbb{Z}_2 \to C$, $\sum_{i=0}^{\infty} x_i 2^i \mapsto \sum_{i=0}^{\infty}(2x_i)3^{-(i+1)}$.*

Proof. This proof is rather straightforward and left to the astute reader. □

The case of an odd prime number is analog to the even case, we just need a more general

Definition 4.3.7. *Let $p \in \mathbb{P}$ be arbitrarily chosen, $C_A = \bigcup_{i\in\mathbb{Z}}[2i, 2i+1]$ and $C_0^p := [0, 1]$. We define, by induction, $C_n^p := C_{n-1}^p \cap ((2p-1)^{-n}C_A)$ and the p-Cantor set C^p is then defined as $C^p := \bigcap_{i=0}^{\infty} C_i^p$.*

Remark 4.3.8. *For a fixed $n \in \mathbb{N}$, the set C_n^p consists of $\frac{2p-1}{2}^n$ disjoint open sets of length each $(2p-1)^{-n}$. The p-Cantor set is obtained by dividing those disjoint sets into $2p-1$ subintervals of equal length and then deleting every second open interval.*

Proposition 4.3.9. *The p-Cantor set is compact and uncountably infinity.*

If we once again consider the $(2p-1)$-adic expansion of a natural number x, then, completely analog to the even case, we see that $x \in C^p$ if and only if in its $(2p-1)$-adic expansion, each x_n is even, which leads to the following

[5] Georg Ferdinand Ludwig Philipp Cantor (* 1845 Saint Petersburg, Russian Federation; † 1918 Halle an der Saale, Germany) was a German mathematician.

Remark 4.3.10. *The Cantor sets C^p are homeomorphic to the Cantor spaces $(C^p, |\ |)$ with the discrete topology. The Cantor spaces are perfect, totally disconnected, uncountably infinite, compact Polish spaces. The actual homeomorphisms are given by the above construction using the $(2p-1)$-ary numeral system.*

Theorem 4.3.11. *There is a homeomorphism between the metric spaces $(\mathbb{Z}_p, |\ |_p)$ and $(C, |\ |)$, given by*

$$\begin{aligned} \varphi : \mathbb{Z}_p &\to C^p \\ x = \sum_{i=0}^{\infty} x_i p^i &\mapsto \sum_{i=0}^{\infty} (2x_i)(2p-1)^{-(i+1)}. \end{aligned}$$

Definition 4.3.12. *A closed metric space (X, d) is called perfect if it has no isolated points, that is, if it is equal to the set of its own limit points.*

From [Bro10] we cite the following

Proposition 4.3.13. *Every uncountable Polish space contains a subset that is homeomorphic to C. In particular, every totally disconnected, perfect and compact metric space is homeomorphic to the Cantor set. A complete topological characterization of Cantor spaces is given by Brouwer*[6] *in the following sense: any two compact Hausdorff spaces with countable clopen bases are homeomorphic.*

Summarizing the above discussion, we obtain the following, rather surprising

Proposition 4.3.14. *The p-adic fields $\mathbb{Z}_2$ and $\mathbb{Z}_p$ are homeomorphic for all $p \in \mathbb{P}$.*

Example 4.3.15. *The 3-adic field $\mathbb{Z}_3$ is homeomorphic to the Sierpinsky triangle. See Figure 4.1.*

Although this might seem rather strange at first, it has important applications in high-energy physics and quantum mechanics, see [Vol10] for more information on this very recent development in the field of quantum mechanics.

[6] Luitzen Egbertus Jan Brouwer (* 1881 Overschie (Rotterdam); † 1966 Blaricum) was a Dutch mathematician.

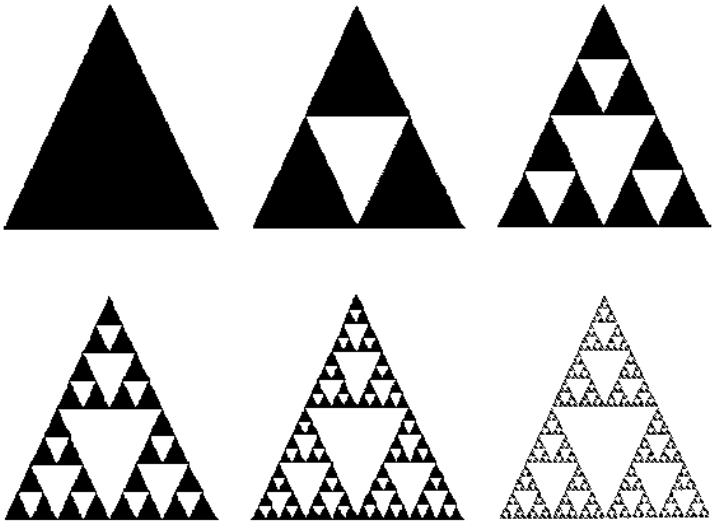

Figure 4.1: The Sierpinsky triangle

4.4 Calculating with p-adic numbers

The addition in $\mathbb{Q}_p$ is very straightforward:

Proposition 4.4.1. *For $x, y \in \mathbb{Q}_p$, $x = \sum_{i=-m}^{\infty} x_i p^i$, $y = \sum_{i=-n}^{\infty} y_i p^i$ and w.l.o.g. $m \geq n$ we have*

$$x \pm y = \sum_{i=-m}^{\infty} (x_i \pm y_i) p^i,$$

where $y_i = 0$, for all $i \in \{-m, \ldots, -n-1\}$.

Example 4.4.2. *Take $x = 1 \in \mathbb{Q}_p$, then $y = \sum_{i=0}^{\infty} (p-1)p^n$ solves $x + y = 0$.*

Proposition 4.4.3. *For $x = \sum_{i=-m}^{\infty} x_i p^i$ and $y = \sum_{i=-n}^{\infty} y_i p^i$ elements in $\mathbb{Q}_p$ we define*

$$xy := \sum_{i=-m-n}^{\infty} z_i p^i,$$

where $z_{-m-n} = x_{-m} y_{-n}$, $z_{-m-n+1} = x_{-m} y_{-n} + x_{-m} y_{-n+1}$ and $z_{-m-n-j} = \sum_{i=0}^{j} x_{-m+j-i} y_{-n+i}$ (compare this with the well known Cauchy product for sequences).

Exercise 4.4.4. *Show that $p \in \mathbb{Z}_p$ has no multiplicative inverse in $\mathbb{Z}_p$.*

Exercise 4.4.5. *Write $a = \dots a_2 a_1 a_0 \in \mathbb{Z}_p$, then show that a admits a multiplicative inverse in $\mathbb{Z}_p$ if and only if $a_0 \neq 0$.*

This is obviously completely different from the situation we are used to in $\mathbb{Z}$, nevertheless $\mathbb{Z}_p$ is still not a field.

Remark 4.4.6. *PARI / GP[7] by H. Cohen[8], a computer algebra system with the main aim of facilitating number theory computations, has an inbuild support for p-adic numbers. One can create a p-adic number by simply typing: $x = x + O(p^k)$, where k is the desired precision.*

PARI Example 1 p-adic numbers in PARI - additive inverse

PARI Input: ? x=15 * 17^-3 + 9 * 17^-1 + 5 + 6*17 + 12*17^2 + 3*17^3 + 17^4 + O(17^20)
%1 = 15*17^-3 + 9*17^-1 + 5 + 6*17 + 12*17^2 + 3*17^3 + 17^4 + O(17^20)
? -x

PARI Output: %2 = 2*17^-3 + 16*17^-2 + 7*17^-1 + 11 + 10*17 + 4*17^2 + 13*17^3 + 15*17^4 + 16*17^5 + 16*17^6 + 16*17^7 + 16*17^8 + 16*17^9 + 16*17^10 + 16*17^11 + 16*17^12 + 16*17^13 + 16*17^14 + 16*17^15 + 16*17^16 + 16*17^17 + 16*17^18 + 16*17^19 + O(17^20)

Example 4.4.7. *Consider $x = \frac{9}{670183865} \in \mathbb{Q}_{13}$, using PARI we see that $|x|_{13} = \left|13^{-5} \cdot \frac{9}{1008}\right|_{13} = 13^5$, thus $x \notin \mathbb{Z}_{13}$, but $x' = x \cdot 13^5 = \frac{9}{1008} \in \mathbb{Z}_{13}$.*

Proposition 4.4.8. *A p-adic number $x \in \mathbb{Q}_p$ has a finite p-adic representation, if and only if $x = \frac{z}{p^n}$, for $z \in \mathbb{Z}$, $n \in \mathbb{N}$ and $p \in \mathbb{P}$.*

Proof. Write

$$x = \sum_{i=-m}^{n} x_i p^i = p^{-m} \sum_{i=-m}^{n} x_i p^{-m+i} = \frac{z}{p^m}, z \in \mathbb{Z},$$

as desired.

Conversely, if $x = p^{-m} y$, $y \in \mathbb{N}$, then we can write y in the basis p and get $y = \sum\limits_{i=0}^{m} y_i p^i$, as desired. □

In analog to decimal fraction decomposition, we have the following

[7] http://pari.math.u-bordeaux.fr/

[8] French mathematician at the University of Bordeaux (* 1947).

Proposition 4.4.9. *Consider an arbitrary p-adic number* $x = \sum\limits_{i=-m}^{\infty} \in \mathbb{Q}_p$*, then* $x \in \mathbb{Q}$*, if and only if there exist* $N, k \in \mathbb{N}$ *such, that* $x_{n+k} = x_n$*, for all* $n > N$*, that is, if* x *becomes periodic.*

Proof. This proof is rather technical, but a complete proof can be found in [Kat]. □

4.5 An algebraic construction of the p-adic numbers

In this section we will present an algebraic construction of the field of p-adic numbers, based on [Ser70].

Definition 4.5.1. *A projective system is a sequence (X_n, φ_n) of sets and so called transition maps $\varphi_n : X_n \to X_{n-1}$. The projective limit of this sequence is a set X with maps $\psi_n : X \to X_n$ such, that $\psi_n = \varphi_n \circ \psi_{n+1}$ and satisfying the following condition: for each set Y and maps $f_n : Y \to X_n$ with $f_n = \varphi_n \circ f_{n+1}$, there is a unique factorization f of the f_n through the set X, that is $f_n = \psi_n \circ f : Y \to X \to X_n$.*

Remark 4.5.2. *A projective system can be represented by a diagram:*

$$\dots \xrightarrow{\varphi_{n+1}} X_n \xrightarrow{\varphi_n} X_{n-1} \xrightarrow{\varphi_1} \dots X_1 \xrightarrow{\varphi_0} X_0.$$

Proposition 4.5.3. *For every projective system (X_n, φ_n) there exists a unique projective limit $\varprojlim X_n := (X, \psi_n) \subseteq \prod_n^\infty X_n$.*

Proof. To see that a limit actually exists, consider the set

$$X := \{(x_n) \mid \varphi_n(x_{n+1}) = x_n \; \forall n \geq 0\} \subseteq \prod_{n=0}^{\infty} X_n.$$

Then, by definition, for each $x \in X$ we have $\varphi_n(\pi_{n+1}(x)) = \pi_n(x)$, where the $\pi_n : X_n \to X_n$ are the canonical projection maps. Thus the restrictions ψ_n of those projections to X fulfill $\varphi_n \circ \psi_{n+1} = \psi_n$ and it is clear that (X, ψ_n) is an upper bound for the given sequence.

Now we still have to prove that (X, ψ_n) has the required universal property. To see this, consider another tuple (X', ψ_n') satisfying the desired condition. We have to show that there is a unique factorization of ψ_n' by ψ_n, alas by the universal property of the product of sets and the projection maps, we know that there exists a unique map $g : X' \to \prod_{n=0}^{\infty} X_n$ such, that the following diagram

$$\begin{tikzcd}
 & \prod_{n=0}^{\infty} X_n \arrow[d, "\pi_n"] \\
X' \arrow[ur, "g"] \arrow[r, "\psi_n'"] & X_n
\end{tikzcd}$$

commutes. Chosing $g = (\psi_n^{'})$ finishes the proof, as then $\operatorname{im} g \subseteq X$ and we can define the factoring function f, as in the definition, by restricting the codomain of g, that is, $f : X^{'} \to X$, $x \mapsto g(x)$.

The uniqueness follows again from the universal property. □

Note that a projective limit neet not to be of the same *kind* as the sets (or groups, or rings or spaces) of the projective sequence. For example, in general, the projective limit of a sequence of fields is usually only a ring. Another example is that the projective limit of finite abelian groups need not to be finite. However in certain situations we can still save a lot of information from our spaces.

Proposition 4.5.4. *For a projective system (X_n, φ_n) of topological spaces and continuous maps, the projective limit is closed in $\prod_{i=0}^{\infty} X_n$, if the X_n are Hausdorff spaces.*

Proof. This follows immediately from the Hausdorff property, i.e. we can find disjoint open neighbourhoods of x_i and $\varphi(x_{i+1})$, thus it is easy to see that $\prod_{i=0}^{\infty} X_i \setminus X$ is open. □

Now we return to the actual matter at hand, the construction of p-adic numbers. There is a natural, or canonical, surjective homomorphism $\varphi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$ with $\ker \varphi = p^{n-1}\mathbb{Z}$ and the sequence

$$\cdots \xrightarrow{\varphi_{n+1}} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\varphi_n} \mathbb{Z}/p^{n-1}\mathbb{Z} \xrightarrow{\varphi_{n-2}} \cdots \xrightarrow{\varphi_3} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\varphi_2} \mathbb{Z}/p\mathbb{Z},$$

forms a projective system.

Definition 4.5.5. *The ring of p-adic integers $\mathbb{Z}_p$ is defined as the projective limit of the above system.*

Thus by definition, an element of $\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z}, \varphi_n)$ is a sequence $a = (\ldots, a_n, \ldots, a_1)$, with:

$$a_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ and } \varphi_n(a_n) = a_{n-1} \text{ if } n \geq 2.$$

The $\mathbb{Z}/p^n\mathbb{Z}$, with the discrete topology, are compact topological spaces, thus by Tikhonov[9], their cartesian product is compact as well (in the product topology), see [HS65] 6.43 for a proof of Tikhonov's theorem. Thus, as a closed subspace of a compact space, $\mathbb{Z}_p$ is a totally disconnected compact space.

[9] Andrey Nikolayevich Tikhonov (* 1906 Gzhatsk (Russian Empire) today Gagarin (Russia); † 1993 Moscow) was a Russian mathematician.

For an element $a \in \mathbb{Z}_p$, we define the reduction modulo p^n, for $n \in \mathbb{N}$, by $\varepsilon_n : \mathbb{Z}_p \to {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}$, $a \mapsto a_n$ and we then get a commutative diagram:

$$\begin{tikzcd}
 & {}^{\mathbb{Z}}\!/_{p^{n+1}\mathbb{Z}} \arrow[dr, "\varphi_n"] & \\
\mathbb{Z}_p \arrow[ur, "\varepsilon_{n+1}"] \arrow[rr, "\varepsilon_n"] & & {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}
\end{tikzcd}$$

In English: $\mathbb{Z}_p$ is closer to ${}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}$ than it is to ${}^{\mathbb{Z}}\!/_{p^{n+1}\mathbb{Z}}$.

Since $\mathbb{Z}_p$ is an integral domain (Proposition 4.2.3), the following definition makes sense.

Definition 4.5.6. *The field of p-adic numbers $\tilde{\mathbb{Q}}_p$ is the field of fractions of $\mathbb{Z}_p$.*

Proposition 4.5.7. *$\tilde{\mathbb{Q}}_p$ is isomorphic to $\mathbb{Q}_p$ (c.f. Remark 4.2.4).*

Proof. This immediately follows from the universal property of the field of fractions of an integral domain. □

In [Ser70], we find another proof of Corollary 4.1.11, using this algebraic interpretation of p-adic integers.

Proposition 4.5.8. *The following sequence is exact:*

$$0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}} \to 0.$$

With other words, ${}^{\mathbb{Z}_p}\!/_{p^n\mathbb{Z}_p}$ is isomorphic to ${}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}$.

Proposition 4.5.9. *An element $a \in \mathbb{Z}_p$ lies in $\mathfrak{u}_p$ if and only if $p \nmid a$. Furthermore, each element $a \in \mathbb{Z}_p$ can be written as $a = \varepsilon p^n$, with $\varepsilon \in \mathfrak{u}_p$.*

For a proof of both propositions, see [Ser70] chapter 2, section 1.2.

4.6 Lemmas of Hensel

One of Hensel's most famous works is a theorem about the irreducibility of polynomials, which also figures in the title of the second chapter in [Hen08] is: "Der Zerlegung der ganzen Funktionen mit p-adischen Koeffizienten in ihre irreduktiblen Faktoren". We will formulate those famous theorems in this chapter, many ideas are similar to those used in the proof of Ostrovskij's theorem 3.1.10. We will start with a

Definition 4.6.1. *An element $x \in \mathbb{Q}_p$ is called a n-th root of unity of $a \in \mathbb{Q}_p$, if and only if $x^n - a = 0$.*

Example 4.6.2. *The equation $x_0^2 \equiv_{11} 7$ is not solvable. The polynomial $X^3 - a = 0$ has no solutions for $a \in \{2, 3, 4, 5, 7, 9, \ldots\}$, but three solutions for $a = 6$.*

Exercise 4.6.3. *Compute the square roots $\sqrt{6}$ and $\sqrt{7}$ in $\mathbb{Z}_5$.*

Proposition 4.6.4. *Just like $\mathbb{R}$, the p-adic fields $\mathbb{Q}_p$ are not algebraically closed, for no $p \in \mathbb{P}$.*

Proof. For $\mathbb{R}$ we easily see that $x^2 + 1 = 0$ has no solution in $\mathbb{R}$. Now consider the equation $X^2 - a$ over the field $\mathbb{Q}_p$, $p \neq 2$, with $\left(\frac{a}{p}\right) = -1$, i.e. a must not be a square modulo p. For $p = 2$ simply chose $a = 5$. □

We thusly need a method to quickly find solutions to polynomial equations, or to at least be able to see whether a solution exists or not. Hensel's first lemma gives an answer to that question.

Theorem 4.6.5 (Hensel's first lemma). *Let $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}_p[X]$ and let $f^{'}(x)$ be its formal derivation. If there exists an $x \in \mathbb{Z}_p$ with*

$$f(x) \equiv_p 0 \wedge f^{'}(x) \not\equiv_p 0,$$

then there exists an uniquely determined $a \in \mathbb{Z}_p$ such, that $f(a) = 0$ and $a \equiv_p x$.

Proof. We inductively construct p-adic integers $a_j := \sum_{i=0}^{j} b_i p^i$ that satisfy $f(a_j) \equiv_{p^{j+1}} 0$ and $a_j \equiv_p x$. Evidently, to satisfy the second condition, we must chose $b_0 \equiv_p x$.

Now assume that $b_0, \ldots, b_{j-1}$ are already constructed. We then know that $a_j = a_{j-1} + b_j p^j$ and

$$\begin{aligned} f(a_j) &= f(a_{j-1} + b_j p^j) \\ &= \sum_{i=0}^{n} c_i (a_{j-1} + b_j p^j)^i \\ &\equiv_p c_0 + \sum_{i=1}^{n} c_i a_{j-1}^i + \sum_{i=1}^{n} i c_i a_{j-1}^{i-1} b_j p^j \\ &= f(a_{j-1}) + b_j p^j f^{'}(a_{j-1}). \end{aligned}$$

We need to fulfill $f(x) \equiv_{p^{j+1}} 0$, thus $f(a_{j-1}) + b_j p^j f^{'}(a_{j-1}) \equiv_p 0$. Since $f(a_{j-1}) \equiv_{p^j} 0$, we have $b_j f^{'}(a_{j-1}) \equiv_p -p^{-j} f(a_{j-1})$. Furthermore, since $a_{j-1} \equiv_p x$ and $f^{'}(x) \not\equiv_p 0$, thus $f^{'}(a_{j-1}) \not\equiv_p 0$, we have

$$b_j \equiv_p -(f^{'}(a_{j-1}))^{-1} p^{-j} f(a_{j-1}).$$

Now if we take a convergent subsequence of the sequence constructed above, then its limit point a is the desired root of f. □

Remark 4.6.6. *This is analog to the Newton-algorithm to find roots of polynomials, but unlike Newton's method, Hensels always converges.*

Example 4.6.7. *Do the square roots of x in $\mathbb{Q}_2$ exist, for any x? We don't know, since $f^{'}(a_0) \not\equiv_p 0$ is not possible, for any a_0. What about the cubic roots of x in $\mathbb{Q}_3$ for any x? Well, once again we see that $f^{'}(a_0) \not\equiv_p 0$ is not possible, for any a_0.*

We therefore need a stronger Hensel!

Proposition 4.6.8 (Hensel's second lemma). *Let $f(x)$ and $f'(x)$ be defined as in Hensel's first lemma and consider an $a_0 \in \mathbb{Z}_p$ with*

$$|f(a_0)|_p \leq \left|f^{'}(a_0)\right|_p^2,$$

then there exists an $a \in \mathbb{Z}_p$ such, that $f(a) = 0$.

Proof. soon □

Example 4.6.9. *Consider $f(x) = x^2 - 33 \in \mathbb{Z}_2[X]$. Its derivative is $f^{'}(x) = 2X$. Now chose $a_0 = 1$, then $|1 - 33|_2 = 2^{-5} < 2^{-2} = |2|_2^2$, thus, with Hensel's second lemma we know that there exists an $a \in \mathbb{Z}_2$ with $f(a) = 0$.*

Now consider $f(x) = x^3 - 2188 \in \mathbb{Z}_3[X]$ and again chose $a_0 = 1$, then $|-2188|_3 = 3^{-7} < 3^{-2} = |3|_3^2$, thus, with Hensel's second lemma we know that there exists an $a \in \mathbb{Z}_3$ such, that $f(a) = 0$.

Remark 4.6.10. *PARI has methods to find roots of polynomial equations:*

- *polrootspadic(pol, p, r)*
- *factorpadic(pol,p,r)*
- *sqrt(x), sqrt(x,n)*
- *valuation(x,p)*
- *deriv(x,y)*
- *Mod(x,y)*
- *subst(x,y,z)*

PARI Example 2 p-adic numbers in PARI - roots

PARI Input: ? a=221+O(251^10)

%1 = 221 + O(251^10)

? sqrt(a)

PARI Output: %2 35 + 86*251 + 145*251^2 + 73*251^3 + 60*251^4 + 197*251^5 + 207*251^6 + 9*251^7 + 151*251^8 + 186*251^9 + O(251^10)

PARI Input: ? f=X^2-a

%3 = X^2 + (30 + 250*251 + 250*251^2 + 250*251^3 + 250*251^4 + 250*251^5 + 250*251^6 + 250*251^7 + 250*251^8 + 250*251^9 + O(251^10))

? polrootspadic(f,251,10)

PARI Output: %4 = [216 + 164*251 + 105*251^2 + 177*251^3 + 190*251^4 + 53*251^5 + 43*251^6 + 241*251^7 + 99*251^8 + 64*251^9 + O(251^10), 35 + 86*251 + 145*251^2 + 73*251^3 + 60*251^4 + 197*251^5 + 207*251^6 + 9*251^7 + 151*251^8 + 186*251^9 + O(251^10)]

PARI Input: ? factorpadic(f,251,10)

PARI Output: %5 = (1 + O(251^10))*X + (216 + 164*251 + 105*251^2 + 177*251^3 + 190*251^4 + 53*251^5 + 43*251^6 + 241*251^7 + 99*251^8 + 64*251^9 + O(251^10)) 1

(1 + O(251^10))*X + (35 + 86*251 + 145*251^2 + 73*251^3 + 60*251^4 + 197*251^5 + 207*251^6 + 9*251^7 + 151*251^8 + 186*251^9 + O(251^10)) 1

4.7 Quadratic residues in the p-adic numbers

Remark 4.7.1. *An element $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p^*$ is a square, if and only if a_0 is a quadratic residue modulo p.*

Proof. If $\left(\frac{a_0}{p}\right) = 1$, then, by Hensel's first lemma, we know that $X^2 - a$ has a zero in $\mathbb{Z}_p^*$. Conversely, if a_0 is a quadratic residue modulo p, then there exists no $b = \sum_{i=0}^{\infty} b_i p^i$ with $b_0^2 \equiv_p a_0$. □

With this ideas, we can classify the squares in $\mathbb{Q}_p$:

Theorem 4.7.2. *For an arbitrary prime $p \neq 2$, we have*

$$a \in \mathbb{Q}_p \text{ is a square } \Leftrightarrow a = p^{2n} \cdot \varepsilon^2,$$

where $n \in \mathbb{Z}$ and $\varepsilon \in \mathbb{Z}_p^*$. The quotient group ${\mathbb{Q}_p^*}/{\mathbb{Q}_p^{*2}}$ has order 4 and, if we fix an $u \in \mathfrak{u}_p = \mathbb{Z}_p^*$ with $\left(\frac{u}{p}\right) = -1$, then the set $\{1, p, u, up\}$ is a complete system of representatives.

Proof. We have to consider the polynomial $f(x) = x^2 - a$. For $b \in \mathbb{Q}_p$ with $f(b) = 0$ it holds that $\mathrm{ord}_p(b^2) = 2 \cdot \mathrm{ord}_p(b) = \mathrm{ord}_p(a)$. We know that b can be written as $b = p^{\mathrm{ord}_p(b)} \cdot \varepsilon$, $\varepsilon \in \mathbb{Z}_p^*$, thus $a = b^2 = p^{2\,\mathrm{ord}_p(b)} \cdot \varepsilon^2$. Now if conversely we have $a = p^{2n} \cdot \varepsilon^2$, then $b = p^n \cdot \varepsilon$.

The quadratic residues modulo p form a subgroup of $\left({\mathbb{Z}}/{p\mathbb{Z}}\right)^*$ of index 2, c.f. [Ser70] p.14, from which it immediately follows that ... Rest des Beweises bald. □

Theorem 4.7.3. *An element $a \in \mathbb{Z}_2^*$ is a square in $\mathbb{Z}_2$, if and only if $a \equiv_8 1$. The factor group ${\mathbb{Q}_2}/{\mathbb{Q}_2^{*2}}$ has order 8 and a complete system of representatives is given by $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.*

Proof. soon □

Now, how do all those valuations play together?

Proposition 4.7.4. *An element $x \in \mathbb{Q}$ is a square, if and only if, it is a square in $\mathbb{Q}_p$ for all $p \in \mathbb{P} \cup \{\infty\}$.*

Proof. Arbitrarily chose $x = \pm \prod_{p \in \mathbb{P}} p^{\mathrm{ord}_p(x)}$, $x \neq 0$, then x is a square in $\mathbb{Q}_\infty = \mathbb{R}$ if and only if $x > 0$ and it is a square in $\mathbb{Q}_p$ if and only if it can be written as $x = p^{2n} \cdot \varepsilon^2$, with $n \in \mathbb{Z}$ and $\varepsilon \in \mathfrak{u}_p$, thus $\nu_p(x) \in 2\mathbb{Z}$ for all $p \in \mathbb{P}$, which means that x is a square in $\mathbb{Q}$. □

Remark 4.7.5. *The above proposition is an example of the very important local-global-principle in number theory, which states that for some types of Diophantine equations, from the knowledge about local solutions ($\mathbb{Q}_p$, $\mathbb{R}$), we can conclude the existence or non-existence of global solutions, i.e. solutions in $\mathbb{Q}$.*

In general, the local-global-principle does not hold:

Example 4.7.6. *Consider the equation $f(x) = (X^2-2)\cdot(X^2-11) = 0$, then we know its roots in $\mathbb{R}$ to be $\pm\sqrt{2}$ and $\pm\sqrt{11}$ and, with Hensel's lemmas, we can prove the existence of p-adic roots as well, but it is clear that f has no roots in $\mathbb{Q}$.*

Thus everywhere locally solvable does not always mean everywhere globally solvable!

However, in the important case of quadratic forms, a famous theorem guarantees us that the local-global-principle holds.

Theorem 4.7.7 (Hasse-Minkowski)**.** *For a quadratic form q over $\mathbb{Q}$ - seen as a homogeneous polynomial of degree 2 in n-variables with coefficients in $\mathbb{Q}$ - it holds that f admits non-trivial roots in $\mathbb{Q}$, if and only if, there exist non-trivial roots in $\mathbb{Q}_p$, for all $p \in \mathbb{P} \cup \{\infty\}$.*

Proof. See for example [Ser70] chapter 4, section 3.2, theorem 8 or [Sch15]. □

Exercise 4.7.8. *Using the local-global-principle, show that $\sqrt{2} \notin \mathbb{Q}$.*

4.8 Roots of unity

Definition 4.8.1. *Let K be a field. An element $\zeta \in K$ is called a n-th root of unity, for $n \in \mathbb{N}$, if $\zeta^n = 1$. If additionally $\zeta^m \neq 1$, for $m \in \mathbb{N}$ with $0 \leq m \leq n$, then ζ is called a primitive n-th root of unity.*

Now if $\zeta \in \mathbb{Q}_p$ with $\zeta^n = 1$ for an $n \in \mathbb{N}$, then $|\zeta|_p = 1$, which means that all p-adic roots of unity are elements of $\mathfrak{u}_p$. Once again Hensel's lemmas give a complete answer to the question when p-adic roots of unity actually exist and what they look like.

Theorem 4.8.2. *Let $p \in \mathbb{P}$ be arbitrarily chosen and $n \in \mathbb{N}$ such, that $\gcd(p, n) = 1$, then there exists a n-th p-adic root of unity in $\mathbb{Q}_p$, if and only if $n \mid (p-1)$. If a n-th root of unity exists, it is automatically a $(p-1)$-th root of unity as well and the set of all $(p-1)$-th roots of unity is a subgroup of $\mathfrak{u}_p$ with index $p-1$.*

Proof. soon □

PARI Example 3 p-adic numbers in PARI - roots of unity

PARI Input: ? polrootspadic(x^6-1,13,10)

PARI Output:
```
%1 = [1 + O(13^10), 3 + 11*13 + 6*13^2 + 9*13^3 +
    7*13^4 + 2*13^5 + 4*13^6 + 4*13^7 + 8*13^8 + 8*13^9 + O(13^10),
    4 + 11*13 + 6*13^2 + 9*13^3 + 7*13^4 + 2*13^5 + 4*13^6 + 4*13^7
    + 8*13^8 + 8*13^9 + O(13^10),
    9 + 13 + 6*13^2 + 3*13^3 + 5*13^4 + 10*13^5 + 8*13^6 + 8*13^7 +
    4*13^8 + 4*13^9 + O(13^10),
    10 + 13 + 6*13^2 + 3*13^3 + 5*13^4 + 10*13^5 + 8*13^6 + 8*13^7
    + 4*13^8 + 4*13^9 + O(13^10),
    12 + 12*13 + 12*13^2 + 12*13^3 + 12*13^4 + 12*13^5 + 12*13^6 +
    12*13^7 + 12*13^8 + 12*13^9 + O(13^10)]
```

Remark 4.8.3. *The $(p-1)$-th roots of unity, together with 0, constitute a complete system of representatives for $\mathbb{Q}_p$, called the Teichmüller[10] representative system. That is, instead of using the set $\{0, 1, \ldots, p-1\}$, we can represent p-adic numbers using a system of roots of unity.*

Remark 4.8.4. *The Teichmüller lift is a map $\omega : \mathbb{F}_p^* \to \mathfrak{u}_p$, $\omega(0) = 0$ and $\omega(x)$ is the unique $(p-1)$-th root of unity which is congruent to $xp^{-\operatorname{ord}_p(x)}$*

[10] Paul Julius Oswald Teichmüller (* 1913 Nordhausen; † 1943 Dnieper area (Borysthenes)) was a German mathematician.

modulo p. To find the Teichmüller representative of an element $x \in \mathbb{Q}_p$, PARI offers us the function teichmuller(x). See [Coh07] chapter 4 *for further information about this.*

4.9 Algorithms for p-adic numbers

soon, as in, probably not very soon

Bibliography

[Bro10] L. E. J. Brouwer, *On the structure of perfect sets of points*, Proc. Koninklijke Akademie van Wetenschappen **12** (1910), no. 1, 785–794.

[Coh07] H. Cohen, *Number theory: Volume i: Tools and diophantine equations*, Graduate Texts in Mathematics, Springer New York, 2007.

[Ger08] L.J. Gerstein, *Basic quadratic forms*, Graduate studies in mathematics, American Mathematical Society, 2008.

[Hen08] K. Hensel, *Theorie der algebraischen zahlen*, Cornell University Library historical math monographs, no. Bd. 1, B. G. Teubner, 1908.

[HS65] E. Hewitt and K. Stromberg, *Real and Abstract Analysis*, 1965.

[Kat] S. Katok, *P-adic analysis compared with real*, Student mathematical library, American Mathematical Soc.

[Lam] T.Y. Lam, *Introduction to quadratic forms over fields*, American Mathematical Soc.

[O'M99] O.T. O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer Berlin Heidelberg, 1999.

[Sch15] R. Scharlau, *Quadratic Forms - lecture notes*, TU Dortmund 2015.

[Ser70] J.P. Serre, *Cours d'arithmétique: par jean-pierre serre*, SUP. Le mathématicien, Presses universitaires de France, 1970.

[Vol10] IgorV. Volovich, *Number theory as the ultimate physical theory*, P-Adic Numbers, Ultrametric Analysis, and Applications **2** (2010), no. 1, 77–87 (English).