universität
wien

DIPLOMARBEIT

Titel der Diplomarbeit

Einführung in die Theorie der p-adischen Zahlen und nichtarchimedischen Absolutbeträge

Verfasserin

Julia Neidhardt

angestrebter akademischer Grad

Magistra der Naturwissenschaften (Mag.rer.nat.)

Wien, 2009

Studienkennzahl lt. Studienblatt:	A 405
Studienrichtung lt. Studienblatt:	Mathematik
Betreuer:	Univ.-Prof. Dr. Johannes Schoißengeier

Zusammenfassung

Die vorliegende Arbeit beschäftigt sich mit Körpern, die mit einem nichtarchimedischen Absolutbetrag ausgestattet sind, insbesondere mit dem Körper der p-adischen Zahlen, und stellt eine Einführung in dieses Gebiet dar.

Nichtarchimedische Absolutbeträge sind dadurch gekennzeichnet, dass sie einer stärkeren Form der Dreiecksungleichung genügen: Der Betrag der Summe zweier Elemente ist nicht nur kleiner oder gleich der Summe ihrer Beträge sondern sogar kleiner oder gleich dem Maximum der einzelnen Beträge. Ist ein Körper mit einem solchen Absolutbetrag ausgestattet, hat das weitreichende Auswirkungen auf die Topologie, die Metrik sowie die algebraische Struktur dieses Körpers. Auf dem Körper der rationalen Zahlen kann der p-adische Absolutbetrag definiert werden. Jeder andere nichtarchimedische Absolutbetrag auf $\mathbb{Q}$ ist diesem äquivalent. Der Körper der p-adischen Zahlen stellt die Vervollständigung der rationalen Zahlen bezüglich des p-adischen Absolutbetrags dar. Die Voraussetzungen, eine nichtarchimedische Analysis zu entwickeln, sind somit gegeben. Ebenso wenig wie die reellen Zahlen ist der Körper der p-adischen Zahlen algebraisch abgeschlossen, doch es erweist sich als deutlich aufwändiger als im reellen Fall, einen Erweiterungskörper zu finden, der sowohl algebraisch abgeschlossen als auch vollständig ist.

Inhaltsverzeichnis

Einleitung

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.
Leopold Kronecker[1]

Die p-adischen Zahlen wurden vom deutschen Mathematiker Kurt Hensel (1861-1941) um das Jahr 1900 in die Zahlentheorie eingeführt. Dabei steht „p“ für eine beliebige, jedoch in den Betrachtungen jeweils fest gewählte Primzahl. Seine Motivation dafür war, so heißt es, auch diesem Gebiet der Mathematik das mächtige Werkzeug der Potenzreihenentwicklung zugänglich zu machen.

Basierend auf den Arbeiten von Ernst Kummer (1810-1893), Leopold Kronecker (1823-1891), Richard Dedekind (1831-1916) und Heinrich Weber (1842-1913) verfolgte Hensel die Analogie, die sich von einem algebraischen Standpunkt aus zwischen den ganzen Zahlen $\mathbb{Z}$ und dem Polynomring $\mathbb{C}[X]$ ergibt, weiter.

Diese Analogie beruht zunächst darauf, dass sowohl in $\mathbb{Z}$ als auch in $\mathbb{C}[X]$ eine eindeutige Primfaktorzerlegung möglich ist. Jede ganze Zahl $n \neq 0$ kann daher als Produkt

$$n = \epsilon \cdot p_1 \cdot p_2 \cdots p_k$$

dargestellt werden, wobei die Faktoren p_i Primzahlen sind und $\epsilon = \pm 1$ gilt, und jedes Polynom $f(X) \neq 0$ über $\mathbb{C}$ lässt sich als Produkt

$$f(X) = a \cdot g_1(X) \cdot g_2(X) \cdots g_k(X)$$

schreiben, wobei alle $g_i(X)$ normierte, irreduzible Polynome über $\mathbb{C}$ sind und a eine komplexe Zahl ist. Diese Darstellungen sind bis auf die Reihenfolge der Faktoren eindeutig.

Weiters sind $\mathbb{Z}$ und $\mathbb{C}[X]$ Hauptidealbereiche. Im ersten Fall werden die Hauptideale von den Primzahlen erzeugt und sind von der Form

$$(p) = p\mathbb{Z}.$$

[1] vgl. [7], S. 9

Der Restklassenkörper $\kappa = \mathbb{Z}/p\mathbb{Z}$ ist zu $\mathbb{F}_p$ isomorph, und wir können eine ganze Zahl n folgendermaßen „zur Basis p“ entwickeln:

Zuerst wählen wir jenes $a_0 \in \{0,\, 1,\, \ldots,\, p-1\}$, das

$$n \equiv a_0 \pmod{p}$$

erfüllt, und schreiben n als $n = a_0 + pn_1$. Wiederholen wir diesen Schritt zunächst für n_1, dann für ein n_2, und so weiter, so erhalten wir die Darstellung

$$n = a_0 + a_1 p + \cdots + a_m p^m = \sum_{i=0}^{m} a_i p^i,$$

und da $a_i \in \{0,\, 1,\, \ldots,\, p-1\}$ für $0 \leq i \leq m$ gilt, ist diese eindeutig bestimmt.

Die komplexen Zahlen sind algebraisch abgeschlossen, also sind die irreduziblen Polynome über $\mathbb{C}$ genau jene vom Grad Eins. Die Hauptideale in $\mathbb{C}[X]$ ergeben sich daher durch

$$\wp = (X-a) = \{(X-a)\, g(X) \colon\ g(X) \in \mathbb{C}[X]\}$$

mit $a \in \mathbb{C}$. Wir können so jeder komplexen Zahl a genau ein Hauptideal zuordnen.

Der Restklassenkörper $\mathbb{C}[X]/\wp$ ist isomorph zu $\mathbb{C}$. Denn betrachten wir den Substitutionshomomorphismus $\Phi_a : \mathbb{C}[X] \to \mathbb{C},\ f(X) \mapsto f(a)$, so ist dieser surjektiv, und der Kern dieses Homomorphismus ist $(X-a)$, da ja $f(a) = 0$ genau dann gilt, wenn $X - a$ ein Teiler von $f(X)$ ist.

Es sei nun $f(X)$ ein Polynom über $\mathbb{C}$, dann ist für ein $\alpha_0 \in \mathbb{C}$

$$f(X) \equiv \alpha_0 \pmod{\wp},$$

und wir können $f(X)$ schreiben als $f(X) = \alpha_0 + (X-a)\, f_1$. So gelangen wir zur Entwicklung des Polynoms $f(X)$ um den Punkt $a \in \mathbb{C}$:

$$\begin{aligned} f(X) &= \alpha_0 + \alpha_1 (X-a) + \cdots + \alpha_n (X-a)^n \\ &= \sum_{i=0}^{n} \alpha_i (X-a)^i \end{aligned}$$

mit $\alpha_i \in \mathbb{C}$ für $0 \leq i \leq n$.

Hensel ging aber noch einen Schritt weiter und betrachtete auch die Quotientenkörper. Jener von $\mathbb{C}[X]$ ist der Körper der rationalen Funktionen über den komplexen Zahlen, das heißt,

$$\mathbb{C}(X) = \left\{ \tfrac{f_1(X)}{f_2(X)} \colon\ f_1(X),\, f_2(X) \in \mathbb{C}[X],\ f_2 \neq 0 \right\}.$$

Für eine Funktion $g(X) \in \mathbb{C}(X)$ kann ebenfalls eine Entwicklung im Punkt a gefunden werden. Diese können wir uns als Quotient der entsprechenden Entwicklungen von $f_1(X)$ durch $f_2(X)$ denken, und sie ist von der Form

$$\begin{aligned} f(X) &= \alpha_m (X-a)^m + \alpha_{m+1} (X-a)^{m+1} + \cdots = \\ &= \sum_{i=m}^{\infty} \alpha_i (X-a)^i \end{aligned}$$

mit $\alpha_i \in \mathbb{C}$ für $i \geq m$. Ist a eine Nullstelle von $f_2(X)$, jedoch keine von $f_1(X)$ beziehungsweise ist die Vielfachheit der Nullstelle a von $f_2(X)$ größer als jene von $f_1(X)$, so gilt $m < 0$, und die Reihe beginnt mit einem negativen Exponenten. Auch wird eine derartige Entwicklung in den meisten Fälle nicht abbrechen. Solche Reihenentwicklungen heißen Laurentreihen.

Zu den p-adischen Zahlen gelangte Hensel nun dadurch, dass er auch Elemente des Quotientenkörpers von $\mathbb{Z}$ – also rationale Zahlen – in eine Reihe „zur Basis p“ entwickelte:

Es sei $x = \frac{a}{b}$ eine rationale Zahl, und wir nehmen zunächst an, dass b nicht von p geteilt wird. Hier kann das gleiche Vorgehen wie oben gewählt werden, das heißt, wir suchen zunächst jenes Element $a_0 \in \{0, 1, \ldots, p-1\}$, das $x \equiv a_0 \pmod{p}$ erfüllt und schreiben x als $x = a_0 + px_1$. So fahren wir fort, bis wir die gesuchte Entwicklung erhalten.

Nun kann es allerdings auch vorkommen, dass b von der Primzahl p geteilt wird. Ist dies der Fall, so betrachten wir stattdessen $y = p^m x$, wobei m die größte ganze Zahl ist, sodass p^m ein Teiler von b ist. Die gewünschte Darstellung für x ergibt sich dann durch

$$x = p^{-m}y = p^{-m}a_0 + p^{-m+1}a_1 + \cdots + a_m + a_{m+1}p + \cdots .$$

Kurt Hensel, der 1884 bei jenem Mann promovierte, von dem der eingangs zitierte Ausspruch stammt, vollbrachte also „ein Menschenwerk“ indem er die p-adischen Zahlen als die Menge aller „Laurentreihen in p“ festlegte. Diese bilden einen Körper.

Hensel wandte seine p-adischen Methoden zunächst in der Zahlentheorie und in der Theorie von quadratischen Formen an und beschäftige sich insbesondere auch mit der Entwicklung algebraischer Zahlen in Potenzreihen. Später galt sein Interesse immer mehr dem Körper der p-adischen Zahlen als eigenständiges mathematisches Objekt.

Die Arbeit von Kurt Hensel hatte großen Einfluss auf Ernst Steinitz (1871-1928), in dessen Veröffentlichung *Algebraische Theorie der Körper* aus dem Jahre 1910 erstmalig eine abstrakte, algebraische Definition eines Körpers zu finden ist, und auf József Kürschák (1864-1933), der im Jahre 1912 die Bewertungstheorie begründete.

Der wichtige Satz über die Äquivalenz von Absolutbeträgen auf den rationalen Zahlen, den wir in Abschnitt 2.2 behandeln werden, wurde 1917 vom russischen Mathematiker Alexander Markowich Ostrowski (1893-1986) gezeigt. Das alles waren Voraussetzungen, die das Entstehen einer p-adischen Analysis ermöglichten.

Auch Helmut Hasse (1898-1979) wurde von Hensels p-adischen Methoden stark beeinflusst. Daher ging er 1920 nach Marburg, um bei Hensel, der dort seit 1902 arbeitete, zu studieren. Im Oktober desselben Jahres entdeckte er bei Untersuchungen von quadratischen Formen das sogenannte *Lokal-Global-Prinzip*, welches besagt, dass manche Gleichungen, die in den reellen Zahlen und für jede Primzahl p im Körper der p-adischen Zahlen eine nichttriviale Lösung besitzen, auch über $\mathbb{Q}$ lösbar sind.

Dadurch zeigte sich erst das große Potential, das in der Theorie der p-adischen Zahlen steckt, denn es konnten nun p-adische Methoden bei Fragen der Lösbarkeit diophantischer Gleichungen eingesetzt werden. Wir werden das *Lokal-Global-Prinzip* in Bemerkung 8 auf Seite 58 besprechen.

Ab Mitte des 20. Jahrhunderts wurden p-adische Methoden in vielen verschiedenen mathematischen Gebieten eingeführt, sowie Theorien aus der reellen Analysis auf den Körper der p-adischen Zahlen übertragen.

Einige Bücher, die heute zu den Standardwerken auf dem Gebiet der p-adischen Zahlen und der p-adischen Analysis gehören, erschienen zu dieser Zeit. So zum Beispiel *Introduction to*

P-Adic Numbers and Valuation Theory von George Bachman (1964, vgl. [1]), *Number theory* von Z.I. Borevich und I.R. Shafarevich (1966, vgl. [2]), *A Course in Arithmetic* von Jean-Pierre Serre (1973, vgl. [22]) und ebenfalls 1973 *Introduction to p-adic numbers and their functions* von Kurt Mahler (vgl. [16]).

Mahler (1903-1988) gibt übrigens an, durch Vorlesungen bei Emmy Noether (1882-1935), die er Mitte der 1920er Jahre in Göttingen besuchte, die p-adischen Zahlen kennengelernt zu haben. Diese blieben für ihn sein ganzes Leben lang von größtem Interesse und eines seiner Hauptforschungsgebiete.

Weitere erwähnenswerte Bücher sind *P-Adic Numbers, P-Adic Analysis, and Zeta-Functions* (1977, vgl. [14]) und *P-adic Analysis: A Short Course on Recent Work* (1980, vgl. [15]) von Neal Koblitz, *Ultrametric Calculus: An Introduction to P-Adic Analysis* von W.H. Schikhof (1984, vgl. [19]) sowie *Local Fields* von J.W.S. Cassels (1986, vgl. [6]).

Es werden regelmäßig internationale, mathematische Konferenzen abgehalten, die sich ganz der p-adischen Analysis oder speziell der p-adischen Funktionalanalysis widmen. So fand im Sommer 2008 die *10th International Conference on P-Adic and Non-Archimedean Analysis* an der Michigan State University statt, die Website zu dieser Konferenz ist zurzeit noch unter der Adresse `http://bt.pa.msu.edu/NA08` erreichbar.

Aber auch in die Physik fand die Theorie der p-adischen Zahlen und ultrametrischen Räume Einzug, und p-adische Methoden werden in immer mehr physikalischen Teilgebieten angewandt.

Im September dieses Jahres wird die vierte internationale Konferenz zu p-adischer mathematischer Physik stattfinden. Diese Konferenz gibt es seit 2003, und sie wird alle zwei Jahre abgehalten, dieses Jahr in Hrodna, Belarus.

Auf der Website der heurigen Konferenz, die unter `http://www.padics2009.org` zu finden ist, heißt es, dass die p-adische mathematische Physik ein schnell wachsendes Gebiet mit vielen Anwendungen in verschiedenen Feldern ist. Diese reichen von der Quantentheorie über Stringtheorie, Planck-Skala-Effekte, Nanosysteme, Spin-Glas und chaotische Systeme bis hin zur molekularen Biologie und Informationswissenschaft. Aktuelle Forschungsergebnisse aus diesen Gebieten werden auf der Konferenz präsentiert.

Die vorliegende Arbeit bietet eine Einführung in die Theorie der p-adischen Zahlen und nichtarchimedischen, bewerteten Körper, also Körper, die mit einem nichtarchimedischen Absolutbetrag ausgestattet sind.

Im ersten Kapitel lernen wir grundlegende Eigenschaften von nichtarchimedischen Absolutbeträgen und ultrametrischen Räumen kennen, und wir überlegen uns, wie diese die algebraische Struktur eines Körpers beeinflussen.

In Kapitel 2 definieren wir zunächst, was wir unter äquivalenten Absolutbeträgen verstehen, um uns dann mit dem Satz von Ostrowski zu befassen. Dieser besagt, dass am Körper der rationalen Zahlen jeder nichttriviale Absolutbetrag entweder dem „gewöhnlichen“ oder einem p-adischen Absolutbetrag äquivalent ist, also dieselbe Topologie wie der entsprechende Absolutbetrag induziert.

Wir beschließen das Kapitel indem wir zeigen, dass die rationalen Zahlen bezüglich keines nichttrivialen Absolutbetrags vollständig sind.

Dass es zu jedem metrischen Raum eine Vervollständigung gibt, besagt Kapitel 3.

Kapitel 4 befasst sich mit $\mathbb{Q}_p$ – dem Körper der p-adischen Zahlen. Dieser stellt die Vervollständigung der rationalen Zahlen bezüglich des p-adischen Absolutbetrags dar.

Nach der Definition von p-adischen und ganzen p-adischen Zahlen soll mit Hilfe der p-adischen Entwicklung einerseits eine konkretere Vorstellung dieser Objekte entwickelt und andererseits ihre Handhabung ermöglicht werden. Algebraische und topologische Eigenschaften von $\mathbb{Q}_p$ werden in Abschnitt 4.3 untersucht. Danach widmen wir uns dem Rechnen mit p-adischen Zahlen.

Dass $\mathbb{Q}_p$ nicht algebraisch abgeschlossen ist, sehen wir in Abschnitt 4.5. Danach lernen wir zwei Versionen des Henselschen Lemmas kennen. Dieses wichtige Resultat erleichtert es, bei der Betrachtung von Polynomen eine Aussage über die Existenz von Wurzeln zu treffen. In diesem Zusammenhang betrachten wir Quadratwurzeln und Einheitswurzeln in $\mathbb{Q}_p$. Auch das Lokal-Global-Prinzip findet Erwähnung.

Wir beenden das Kapitel mit einem Blick auf die p-adische Analysis. Dazu untersuchen wir das Konvergenzverhalten von Folgen und Reihen über $\mathbb{Q}_p$, widmen uns Potenzreihen und ihrem Konvergenzradius und lernen den p-adischen Logarithmus und die p-adische Exponentialfunktion kennen. Auch mit Stetigkeit und Differenzierbarkeit befassen wir uns.

Beim Körper der p-adischen Zahlen handelt es sich wie bei den reellen Zahlen um eine Vervollständigung von $\mathbb{Q}$. Keine dieser Vervollständigungen ist algebraisch abgeschlossen. Die komplexen Zahlen stellen den algebraischen Abschluss von $\mathbb{R}$ dar, und wir erhalten diesen Abschluss indem wir $i = \sqrt{-1}$ zu $\mathbb{R}$ adjungieren. Wie $\mathbb{R}$ ist $\mathbb{C}$ vollständig.

Um einen Köper zu erhalten, der sowohl algebraisch abgeschlossen als auch vollständig ist, genügt es also, eine Körpererweiterung über $\mathbb{R}$ vom Grad 2 zu betrachten, denn es ist i eine Lösung der quadratischen Gleichung $X^2 + 1 = 0$.

Analog dazu setzt sich Kapitel 5 zur Aufgabe, den algebraischen Abschluss von $\mathbb{Q}_p$ zu finden. Dies ist jedoch bei weitem aufwändiger als im reellen Fall.

Zunächst betrachten wir endliche Körpererweiterungen über $\mathbb{Q}_p$. Um ihre Eigenschaften genau untersuchen zu können, werden in den ersten beiden Abschnitten des fünften Kapitels einige Resultate über endlichdimensionale, normierte Vektorräume hergeleitet und algebraische Grundlagen zu Körpererweiterungen in Erinnerung gerufen. Insbesondere soll die auf einer Körpererweiterung definierte Norm besprochen werden, denn diese benötigen wir, um den p-adischen Absolutbetrag auf den betrachteten Körpererweiterungen fortzusetzen.

Außerdem betrachten wir die Unterscheidung endlicher Körpererweiterungen in unverzweigte, verzweigte und total verzweigte, und sehen dann, dass über $\mathbb{Q}_p$ endliche Körpererweiterungen beliebigen Grades gefunden werden können.

Das führt uns schließlich zum algebraischen Abschluss $\overline{\mathbb{Q}}_p$. Dieser stellt eine unendliche Körpererweiterung über $\mathbb{Q}_p$ dar. Im Gegensatz zum algebraischen Abschluss von $\mathbb{R}$ ist $\overline{\mathbb{Q}}_p$ jedoch nicht vollständig.

Wiederum ist es notwendig, die Theorie aus Kapitel 3 anzuwenden, und wir gelangen endlich zu einem Körper, der nicht nur vollständig, sondern, wie wir zeigen, auch algebraisch abgeschlossen ist.

Diesen Körper bezeichnen wir mit $\mathbb{C}_p$, was die Analogie zu den komplexen Zahlen ausdrückt. Abschließend werfen wir noch einen Blick auf die Analysis in $\mathbb{C}_p$.

Diese Arbeit basiert vor allem auf drei neueren Bücher zu diesem Gebiet: *P-Adic Numbers: An Introduction* von Fernando Q. Gouvêa, das 1993 in einer ersten Version erschien und in der Zwischenzeit schon mehrmals neu aufgelegt und überarbeitet wurde (vgl. [9]), *A Course in P-Adic Analysis* von Alain M. Robert aus dem Jahr 2000 (vgl. [18]) sowie *P-Adic Analysis Compared with Real* von Svetlana Katok, das 2007 erschien (vgl. [13]).

Von den oben erwähnten Werken wurden alle als Literatur für diese Arbeit verwendet, insbesondere sind aber *Introduction to P-Adic Numbers and Valuation Theory* von George Bachman (vgl. [1]) sowie *P-Adic Numbers, P-Adic Analysis, and Zeta-Functions* von Neal Koblitz (vgl. [14]) zu nennen.

Am Ende eines jeden Kapitels findet sich eine ausführliche Quellenangabe.

Bei unseren Betrachtungen werden Grundbegriffe aus verschiedenen mathematischen Gebieten benötigt. Einige von ihnen sind mit Erklärungen versehen, welche für Begriffe aus der Algebra nachzulesen sind in [3], für Begriffe aus der Zahlentheorie in [5] und für Begriffe aus der Topologie in [12]. Die vor allem in Abschnitt 4.6 erwähnten Definitionen und Resultate aus der reellen Analysis finden sich in [10].

Die hier skizzierte historische Entwicklung ist nachzulesen in [7], S. 126-128, [9], S. 7-14, [15], S. 6, 7, [17], Biographies of H. Hasse, K. Hensel, J. Kürschák, K. Mahler, E. Steinitz, [24], S. 376-377, 392 und [25], S. 127.

In das Symbolverzeichnis, welches auf Seite 107 beginnt, wurden Symbole aufgenommen, die im Verlauf der Abhandlung eingeführt werden oder für diese Arbeit von besonderem Interesse sind. Die üblichen, in der Mathematik gebräuchlichen Schreibweisen werden als bekannt vorausgesetzt und nicht angeführt.

Diese Arbeit wurde mit LaTeX unter der Verwendung verschiedener Makropakete erstellt.

Danksagung

Ich möchte an dieser Stelle meinem Betreuer Prof. Johannes Schoißengeier für die große Unterstützung beim Erstellen dieser Arbeit danken. Der Fakultät für Mathematik an der Universität Wien danke ich für die mir gebotenen Möglichkeiten, während meines Studiums als Tutorin bei den Linux-Übungen viele interessante Erfahrungen zu sammeln sowie im Rahmen der Frauenförderungsaktivitäten der Fakultät wichtige Projekte zu planen und umzusetzen.

Meinen Eltern Frieda Neidhardt und Wolfgang Sagerschnig danke ich für ihre Unterstützung und Geduld in all der Zeit und meinem Freund Ernst Lammer, dass er mir immer zur Seite gestanden ist und die Diplomarbeit sorgfältig lektoriert hat. Außerdem danke ich meinen Freundinnen Kerstin Ammann und Liselotte Tschepen, denen ich mich durch einen gemeinsamen Weg durch das Studium, die Tätigkeit in der ÖH und die Arbeit an der Fakultät sehr verbunden fühle, sowie meinen Freundinnen Sophie Lampl und Katerina Vrtikapa, die mir immer wichtige Gesprächspartnerinnen waren. Indem sie mir die Buchhandlung Gibert Joseph auf dem Boulevard St. Michel in Paris gezeigt hat, hat mir meine Freundin Ina Markova die Literatursuche für diese Arbeit sehr erleichtert, dafür möchte ich ihr danken. Und ich danke auch meiner Freundin Norma Goicochea Estenoz: ¡Voy a mi!

1

Grundlagen

In diesem Kapitel werden wir grundlegende Eigenschaften von nichtarchimedischen Absolutbeträgen kennenlernen und ihre Auswirkungen auf die Metrik und die Topologie eines Körpers, der mit einem solchen Absolutbetrag ausgestattet ist, untersuchen.

1.1 Absolutbeträge

1.1.1 Der *p*-adische Absolutbetrag auf $\mathbb{Q}$

Zunächst wollen wir uns in Erinnerung rufen, wie ein Absolutbetrag definiert ist:

Definition 1: Es sei K ein beliebiger Körper. Eine Abbildung $|\,| : K \to \mathbb{R}$ heißt *Absolutbetrag auf* K, wenn für alle Elemente x und y des Körpers folgende Bedingungen erfüllt sind:

(A1) $|x| \geq 0, \quad |x| = 0 \iff x = 0,$

(A2) $|xy| = |x|\,|y|\,,$

(A3) $|x + y| \leq |x| + |y|\,.$

Die letzte Bedingung wird *Dreiecksungleichung* genannt.

Proposition 1: Es sei K ein Körper und $|\,|$ ein beliebiger Absolutbetrag auf K. Dann gilt:

1. $|1_K| = 1,$
2. $|x^n| = 1,\ x \in K \Longrightarrow |x| = 1,$
3. $|-1_K| = 1,$

4. $|-x| = |x|$ für alle $x \in K$,
5. $||x| - |y|| \leq |x - y|$ für alle $x,\, y \in K$.

Beweis. Unter Berücksichtigung der Tatsache, dass die einzige reelle Zahl $r > 0$ mit der Eigenschaft $r^2 = r$ beziehungsweise $r^n = 1$ die Zahl $r = 1$ ist, sind diese Behauptungen leicht zu zeigen.

1. $|1_K| = |1_K \cdot 1_K| = |1_K|\,|1_K| = |1_K|^2 \Longrightarrow |1_K| = 1$,
2. $1 = |x^n| = |\underbrace{x \cdots x}_{n \text{ mal}}| = \underbrace{|x| \cdots |x|}_{n \text{ mal}} = |x|^n \Longrightarrow |x| = 1$,
3. $|1_K| = |(-1_K)\,(-1_K)| = |-1_K|^2 \Longrightarrow |-1_K| = 1$,
4. $|-x| = |-1_K \cdot x| = |-1_K|\,|x| = |x|$,
5. $|x| = |x - y + y| \leq |x - y| + |y| \Longrightarrow |x| - |y| \leq |x - y|$. Durch Vertauschen von x und y erhalten wir $-|x| + |y| \leq |x - y|$. Insgesamt folgt also

$$||x| - |y|| \leq |x - y|\,.$$

□

Der „gewöhnliche“ Absolutbetrag am Körper der reellen Zahlen, der für alle $x \in \mathbb{R}$ definiert ist durch $|x| = x$ im Falle $x \geq 0$ beziehungsweise durch $|x| = -x$ für $x < 0$, ist sicher der vertrauteste.

Ein anderes Beispiel ist der auf den komplexen Zahlen definierte Absolutbetrag, der für $z = x + iy \in \mathbb{C}$ gegeben ist durch $|z| = \sqrt{x^2 + y^2}$.

Auf jedem beliebigen Körper K kann der sogenannte triviale Absolutbetrag τ_K definiert werden, indem für das Nullelement der Absolutbetrag gleich Null und für alle anderen Elemente des Körpers dieser gleich Eins gesetzt wird, also $|0| = 0$ und $|x| = 1$ für alle $x \in K$, $x \neq 0$.

Auf einem endlichen Körper gibt es nur den trivialen Absolutbetrag. Ist nämlich $q < \infty$ die Anzahl der Elemente dieses Körpers, so gilt $x^q = x$ für jedes $x \in \mathbb{F}_q$. Es ist somit $x^{q-1} = 1$, und die Behauptung folgt aus Proposition 1.

Der nächste Absolutbetrag, den wir betrachten, ist grundlegend für die gesamte Theorie, die im weiteren Verlauf entwickelt werden soll.

Definition 2: Sei p eine Primzahl, $n \neq 0$ eine ganze Zahl und $\mathrm{ord}_p(n)$ die größte ganze Zahl, für die $n = p^{\mathrm{ord}_p(n)} m$ gilt. Dann heißt $\mathrm{ord}_p(n)$ *die p-adische Ordnung von n*. Für $n = 0$ setzen wir $\mathrm{ord}_p(n) = +\infty$.

Die p-adische Ordnung einer rationalen Zahl $x = \frac{a}{b}$, $x \neq 0$ ist definiert als die Differenz der p-adischen Ordnung des Zählers und jener des Nenners, also als $\mathrm{ord}_p(x) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$, wenn $\mathrm{ggT}(a,\, b) = 1$.

Es ist leicht einzusehen, dass für zwei ganze Zahlen m und n gilt $\mathrm{ord}_p(m \cdot n) = \mathrm{ord}_p(m) + \mathrm{ord}_p(n)$. Die p-adische Ordnung weist also in gewissem Sinne Ähnlichkeiten mit dem Logarithmus auf. Daraus ergibt sich, dass die p-adische Ordnung einer rationalen Zahl x nur von der Zahl selbst und nicht von ihrer Darstellung abhängt, das heißt, schreiben wir die eben betrachtete rationale Zahl $x = \frac{a}{b}$ als $x = \frac{ac}{bc}$ für ein $c \in \mathbb{Z}$, $c \neq 0$, dann bleibt ihre p-adische Ordnung dieselbe, denn $\mathrm{ord}_p(x) = \mathrm{ord}_p(ac) - \mathrm{ord}_p(bc) = \mathrm{ord}_p(a) + \mathrm{ord}_p(c) - \mathrm{ord}_p(b) - \mathrm{ord}_p(c) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$.

Definition 3: Sei $x \in \mathbb{Q}$ und $\mathrm{ord}_p(x)$ wie oben. Wir definieren eine Funktion $|\ |_p$ indem wir für $x \neq 0$

$$|x|_p = p^{-\mathrm{ord}_p(x)}$$

sowie $|x|_p = 0$ für $x = 0$ setzen.

Proposition 2: Die Funktion $|\ |_p$ ist ein Absolutbetrag auf $\mathbb{Q}$.

Beweis. Wir müssen zeigen, dass die Eigenschaften (A1)-(A3) aus der Definition des Absolutbetrags erfüllt sind.

Die Wertemenge von $|\ |_p$ umfasst für $x \neq 0$ alle Potenzen der Primzahl p und ist per Definition für $x = 0$ gleich Null, insgesamt also $\{p^n : n \in \mathbb{Z}\} \cup \{0\}$. Somit ist (A1) gezeigt.

Es gilt $|xy|_p = p^{-\mathrm{ord}_p(xy)} = p^{-\mathrm{ord}_p(x)-\mathrm{ord}_p(y)} = p^{-\mathrm{ord}_p(x)}p^{-\mathrm{ord}_p(y)} = |x|_p\,|y|_p$, (A2) ist also erfüllt.

Bei der Dreiecksungleichung (A3) ist für $x = 0$ oder $y = 0$ oder $x + y = 0$ nichts zu zeigen. Wir setzen nun voraus, dass diese Werte ungleich Null sind. Weiters sollen $x = \frac{a}{b}$ und $y = \frac{c}{d}$ in gekürzter Form vorliegen. Dann ist $x + y = \frac{ad+cb}{bd}$ und $\mathrm{ord}_p(x + y) = \mathrm{ord}_p(ad + cb) - \mathrm{ord}_p(b) - \mathrm{ord}_p(d)$. Nun ist die höchste Potenz von p, die die Summe zweier Zahlen teilt, zumindest so groß wie die höchste Potenz von p, durch die sowohl die erste Zahl als auch die zweite noch teilbar ist. Daher gilt

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

Es ist somit

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

und das ist sicher $\leq |x|_p + |y|_p$. □

Es heißt $|\ |_p$ *der p-adische Absolutbetrag auf* $\mathbb{Q}$.

Eine rationale Zahl ist bezüglich dieses Absolutbetrags also „klein“, wenn sie durch eine große Potenz von p teilbar ist.

1.1.2 Nichtarchimedische Absolutbeträge

Wir haben eben gesehen, dass der p-adische Absolutbetrag $|\ |_p$ auf $\mathbb{Q}$ einer noch stärkeren Bedingung als der Dreiecksungleichung genügt, der Betrag der Summe ist nicht nur kleiner oder gleich der Summe der Beträge sondern sogar kleiner oder gleich dem Maximum der einzelnen Beträge. Diese „starke“ Dreiecksungleichung ist fundamental für unsere weiteren Betrachtungen, und die folgende Definition ist Grundlage der gesamten p-adischen Analysis.

Definition 4: Ein nichttrivialer Absolutbetrag $|\ |$ auf einem Körper K heißt *nichtarchimedisch*, wenn $|x+y| \leq \max\{|x|,\ |y|\}$ für alle $x,\ y \in K$ gilt. Ein nichttrivialer Absolutbetrag, der dieser Ungleichung nicht genügt, heißt *archimedisch*.

Bemerkung 1: Auf einem Körper K mit nichtarchimedischem Absolutbetrag $|\ |$ kann für $x \in K$ folgendermaßen eine Funktion ν definiert werden

$$\nu(x) := \begin{cases} -\log|x| & \text{für } x \neq 0, \\ +\infty & \text{für } x = 0. \end{cases}$$

Diese Abbildung ν von K nach $\mathbb{R} \cup \{\infty\}$ heißt *Bewertung auf* K und hat folgende Eigenschaften:

1. $\nu(x+y) \geq \min\{\nu(x),\ \nu(y)\}$ für alle $x,\ y \in K$,
2. $\nu(xy) = \nu(x) + \nu(y)$ für alle $x,\ y \in K$,
3. $\nu(x) = \infty \iff x = 0$.

Umgekehrt definiert jede Bewertung ν für $r \in \mathbb{R},\ r > 1$ durch $|x| = r^{-\nu(x)}$ einen nichtarchimedischen Absolutbetrag.

Betrachten wir in diesem Zusammenhang den p-adischen Absolutbetrag. Für ein $x \in \mathbb{Q},\ x \neq 0$ ist dieser $|x|_p = p^{-\mathrm{ord}_p(x)}$. Wird auf die eben beschriebene Weise eine Bewertung ν definiert, so ergibt das $\nu(x) = \mathrm{ord}_p(x) \cdot \log p$. Die Bewertung ν unterscheidet sich also nur um die multiplikative Konstante $\log p$ von der p-adischen Ordnung und ihr Bild ist $\log p \cdot \mathbb{Z}$, also eine zu $\mathbb{Z}$ isomorphe Untergruppe von $\mathbb{R}$. Viele Autorinnen und Autoren bezeichnen die p-adische Ordnung ord_p als *die* p-adische Bewertung ν_p, definieren also $\nu_p(x) := \mathrm{ord}_p(x)$.

In manchen Fällen bietet es sich an, statt des Absolutbetrags die entsprechende Bewertung zu betrachten.

Proposition 3: Sei $|\ |$ ein nichttrivialer Absolutbetrag auf einem Körper K. Dann sind folgende Aussagen äquivalent:

1. $|\ |$ ist nichtarchimedisch.
2. Es ist $|n \cdot 1_K| \leq 1$ für alle $n \in \mathbb{Z}$.

Beweis. (1) $\Longrightarrow$ (2) Für $n = 1$ stimmt die Aussage, durch vollständige Induktion kann sie für alle $n \in \mathbb{N}$ gezeigt werden:

$$|(n+1) \cdot 1_K| \leq \max\{\underbrace{|n \cdot 1_K|}_{\leq 1},\ 1\}.$$

Für $n < 0$ folgt das Gewünschte wegen $|-n \cdot 1_K| = |n \cdot 1_K|$, und klarerweise ist $|n| = 0$ für $n = 0$.

(1) $\Longleftarrow$ (2) Für $x \in K$ gilt

$$|x+1|^m = \left|\sum_{k=0}^{m} \binom{m}{k} x^k\right| \leq \sum_{k=0}^{m} \underbrace{\left|\binom{m}{k}\right|}_{\in \mathbb{Z}} |x^k| \leq \sum_{k=0}^{m} |x^k| = \sum_{k=0}^{m} |x|^k \leq (m+1)\max\{|x|^m,\ 1\}.$$

Wenn wir auf beiden Seiten die m-te Wurzel nehmen, so ergibt sich

$$|x+1| \leq \sqrt[m]{m+1}\max\{|x|,\,1\},$$

und für $m \to \infty$ folgt

$$|x+1| \leq \max\{|x|,\,1\}.$$

Es seien nun x, y zwei Elemente von K. Ist $y = 0$, so gilt auf jeden Fall

$$|x+y| \leq \max\{|x|,\,|y|\}.$$

Für $y \neq 0$ erhalten wir

$$\left|\frac{x}{y}+1\right| \leq \max\left\{\left|\frac{x}{y}\right|,\,1\right\},$$

können das also auf das eben Gezeigte zurückführen. □

Bemerkung 2: Dieses Resultat erklärt auch, warum wir von nichtarchimedischen Absolutbeträgen sprechen, denn ein Körper K besitzt eine sogenannte archimedische Ordnung, wenn es zu je zwei positiven Elementen x und y eine natürliche Zahl n gibt mit $nx > y$.

Es gilt also, dass ein Absolutbetrag $|\ |$ archimedisch ist, genau dann, wenn die Menge $\{1, 2, 3, \ldots\}$ nicht beschränkt ist, das heißt, wenn $\sup\{|n| :\ n \in \mathbb{Z}\} = +\infty$ ist. Umgekehrt ist ein nichttrivialer Absolutbetrag $|\ |$ nichtarchimedisch, genau dann, wenn $\sup\{|n| :\ n \in \mathbb{Z}\} = 1$ ist.

Hier noch eine wichtige Konsequenz der nichtarchimedischen Ungleichung:

Proposition 4: Sei K ein Körper mit einem nichtarchimedischen Absolutbetrag $|\ |$. Ist $|x| \neq |y|$ für x, $y \in K$, dann gilt für den Absolutbetrag der Summe

$$|x+y| = \max\{|x|,\,|y|\}.$$

Beweis. Es sei o.B.d.A. $|x| > |y|$. Dann wissen wir, dass

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

gelten muss. Anderseits ist

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

Das ergibt insgesamt

$$|x+y| = |x| = \max\{|x|,\,|y|\}.$$ □

Dieses Resultat ist nicht intuitiv und deshalb etwas „gewöhnungsbedürftig“, wird aber klarer, wenn wir es uns anhand des p-adischen Absolutbetrags überlegen:

Beispiel 1: Es seien $x,\ y \in \mathbb{Z}$, $\mathrm{ord}_p(x) = n$ beziehungsweise $\mathrm{ord}_p(y) = m$ und so, dass

$$x = p^n x^{'},\ y = p^m y^{'},\ p \nmid x^{'} y^{'}.$$

Es ist dann $|x|_p = p^{-n}$, $|y|_p = p^{-m}$, und es sei zunächst $n < m$, also $|x|_p > |y|_p$. Daraus folgt für die Summe

$$x + y = p^n (x^{'} + p^{m-n} y^{'}).$$

Da $p \nmid x^{'}$ wird auch $x^{'} + p^{m-n} y^{'}$ nicht von p geteilt, und es gilt

$$|x + y|_p = p^{-n} = \max \left\{ |x|_p ,\ |y|_p \right\}.$$

Gilt andererseits $n = m$, also $|x|_p = |y|_p$, dann ist

$$x + y = p^n (x^{'} + y^{'}).$$

Die Primzahl p teilt ja weder $x^{'}$ noch $y^{'}$, aber es ist möglich, dass die Summe $x^{'} + y^{'}$ von p geteilt wird, das heißt, $\mathrm{ord}_p(x + y) \geq n = \min \{\mathrm{ord}_p(x),\ \mathrm{ord}_p(y)\}$, und somit ist

$$|x + y|_p \leq \max \left\{ |x|_p ,\ |y|_p \right\} = |x|_p = |y|_p .$$

1.2 Ultrametrische Räume

1.2.1 Metrik

In diesem Abschnitt soll die Metrik und die Topologie eines Körpers betrachtet werden, der mit einem nichtarchimedischen Absolutbetrag ausgestattet ist. Wie wir wissen, gibt uns ein Absolutbetrag die Möglichkeit, einen Abstandsbegriff für die Elemente eines Köpers, also eine Metrik, zu definieren.

Zunächst rufen wir uns die Definition einer Metrik in Erinnerung, um danach zu präzisieren, wie diese mit dem Absolutbetrag zusammenhängt.

Definition 5: Unter einem metrischen Raum verstehen wir eine Menge X zusammen mit einer Abbildung $d:\ X \times X \to \mathbb{R}$, die folgenden Bedingungen genügt:

(M1) $d(x,\ y) \geq 0$ für alle $x,\ y \in X$, $\quad d(x,\ y) = 0 \iff x = y$,

(M2) $d(x,\ y) = d(y,\ x)$ für alle $x,\ y \in X$,

(M3) $d(x,\ z) \leq d(x,\ y) + d(y,\ z)$ für alle $x,\ y,\ z \in X$.

Diese Abbildung heißt dann *Metrik*. Die Eigenschaft (M3) wird als Dreiecksungleichung bezeichnet analog zur Eigenschaft (A3) in der Definition des Absolutbetrags auf Seite 7.

Eine Menge X kann mit verschiedenen Metriken ausgestattet sein. Damit eindeutig ist, auf welche Metrik Bezug genommen wird, schreiben wir für den metrischen Raum X auch $(X,\ d)$.

Definition 6: Sei K ein Körper und $|\,|$ ein Absolutbetrag auf K. Dann wird durch

$$d(x,\, y) = |x - y|$$

für $x,\, y \in K$ eine Metrik auf K induziert. K wird so zu einem metrischen Raum.

Es ist unmittelbar einzusehen, dass die so definierte Metrik tatsächlich die Eigenschaften (M1) bis (M3) besitzt.

Analog zur nichtarchimedischen Ungleichung bei Absolutbeträgen betrachten wir auch hier eine „stärkere“ Form der Dreiecksungleichung:

Definition 7: Ein metrischer Raum X, dessen Metrik d der Ungleichung

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

mit $x,\, y,\, z \in X$ genügt, wird *ultrametrischer Raum* genannt. Die Metrik d wird demzufolge auch als *Ultrametrik* bezeichnet und die Ungleichung als *ultrametrische Ungleichung.*

Proposition 5: Sei $|\,|$ ein Absolutbetrag auf einem Körper K. Der Absolutbetrag $|\,|$ ist nichtarchimedisch genau dann, wenn die von ihm induzierte Metrik $d(x,\, y) = |x - y|$ der ultrametrischen Ungleichung genügt.

Beweis. Es sei $|\,|$ nichtarchimedisch. Dann gilt

$$\underbrace{|x - y|}_{=d(x,\, y)} = |x - z + z - y| \leq \max\{\underbrace{|x - z|}_{=d(x,\, z)},\, \underbrace{|z - y|}_{=d(z,\, y)}\},$$

das Gewünschte folgt also unmittelbar.

Umgekehrt sei für alle Elemente des Körpers

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

Setzen wir $y = -y$ und $z = 0$, so folgt

$$\underbrace{d\,(x,\, -y)}_{=|x+y|} \leq \max\{\underbrace{d\,(x,\, 0)}_{=|x|},\, \underbrace{d\,(0,\, y)}_{=|y|}\}. \qquad \square$$

Folgende Proposition, die eng mit Proposition 4 aus dem vorigen Abschnitt zusammenhängt, spiegelt ein wichtiges Prinzip wider, das weitreichende Konsequenzen für die Topologie und die Geometrie eines ultrametrischen Raumes hat und welches oft folgendermaßen veranschaulicht wird: In einem ultrametrischen Raum sind alle Dreiecke gleichschenklig mit höchstens einer kurzen Seite.

Proposition 6: Es sei X ein ultrametrischer Raum mit der Metrik d, und es seien $x,\, y,\, z \in X$. Ist $d(x,\, y) \neq d(y,\, z)$, so gilt

$$d(x,\, z) = \max\left\{d\,(x,\, y)\,,\, d\,(y,\, z)\right\}.$$

Beweis. Die Seiten des „Dreiecks“ haben die Längen $d(x,\, y) = |x - y|\,,\ d(y,\, z) = |y - z|\,,$ und $d(x,\, z) = |x - z|\,.$ Da $|x - z| = |x - y + y - z|$ gilt und vorausgesetzt wurde, dass $|x - y| \neq |y - z|$ ist, folgt mit Hilfe von Proposition 4 auf Seite 11 das Gewünschte. $\square$

1.2.2 Topologie

Auf einem metrischen Raum kann durch die Metrik d eine Topologie induziert werden. Dieser wird so zu einem topologischen Raum, und es können topologische Konzepte und Begriffe wie Konvergenz, offene Menge, Kompaktheit oder Stetigkeit verwendet werden. Es wird sich herausstellen, dass dies bei der Betrachtung ultrametrischer Räume noch einige überraschende und nichtintuitive Ergebnisse mit sich bringen wird.

Definition 8: Es sei $(X,\ d)$ ein metrischer Raum, $a \in X$ und r eine positive reelle Zahl. Die *offene Kugel* mit Radius r und Mittelpunkt a sei die Menge

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

Eine Menge $U \subseteq X$ heißt offen bezüglich der durch die Metrik d induzierten Topologie, wenn es zu jedem $x \in U$ ein $r > 0$ gibt, sodass $B_r(x) \subseteq U$ gilt. Damit wird der metrische Raum zu einem topologischen Hausdorffraum.

Es soll nun wiederum ein Zusammenhang zu einem mit einem Absolutbetrag ausgestatteten Körper hergestellt werden.

Definition 9: Ein *topologischer Körper* K ist ein Körper mit einer Topologie, sodass die Abbildungen

$$\begin{aligned}(x,\ y) \mapsto x + y :&\quad K \times K \to K,\\ (x,\ y) \mapsto xy :&\quad K \times K \to K,\\ x \mapsto x^{-1} :&\quad K^\times \to K^\times\end{aligned}$$

stetig sind.

Proposition 7: Sei K ein Körper mit Absolutbetrag $|\ |$, dann ist K bezüglich der durch $d(x, y) = |x - y|$ induzierten Metrik ein topologischer Körper.

Beweis.

- Addition $(x,\ y) \mapsto x + y$ und Multiplikation $(x,\ y) \mapsto xy$ sind stetige Abbildungen von $K \times K$ nach K. Sind nämlich $x_0,\ y_0 \in K$ fix, $d(x,\ x_0) < \delta$ sowie $d(y,\ y_0) < \delta$, dann gilt

$$\begin{aligned}d(x + y,\ x_0 + y_0) &= |x + y - (x_0 + y_0)|\\ &= |x - x_0 + y - y_0|\\ &\le \underbrace{|x - x_0|}_{\delta = \epsilon/2} + \underbrace{|y - y_0|}_{\delta = \epsilon/2} < \epsilon,\end{aligned}$$

$$\begin{aligned}d(xy,\ x_0y_0) &= |xy - x_0y_0|\\ &= |(x - x_0)\,(y - y_0) + x_0\,(y - y_0) + y_0\,(x - x_0)|\\ &\le |(x - x_0)\,(y - y_0)| + |x_0\,(y - y_0)| + |y_0\,(x - x_0)|\\ &= \underbrace{|x - x_0|}_{<\delta}\underbrace{|y - y_0|}_{<\delta} + \underbrace{|x_0|}_{\text{fix}}\underbrace{|y - y_0|}_{<\delta} + \underbrace{|y_0|}_{\text{fix}}\underbrace{|x - x_0|}_{<\delta}.\end{aligned}$$

- Die Abbildung $x \mapsto x^{-1}$ von $K^\times$ nach $K^\times$ ist stetig. Es sei x_0 fest gewählt und $\delta < \frac{|x_0|}{2}$. Für alle x mit $d(x,\, x_0) < \delta$ ist dann $|x| > \frac{|x_0|}{2}$, und es gilt

$$d\left(\frac{1}{x},\, \frac{1}{x_0}\right) = \left|\frac{1}{x} - \frac{1}{x_0}\right| = \left|\frac{x_0 - x}{x \cdot x_0}\right| = \frac{|x_0 - x|}{|x|\,|x_0|} < \frac{2\delta}{|x_0|^2}.$$ □

Als Nächstes wollen wir die Auswirkungen der ultrametrischen Ungleichung auf die Topologie eines Raumes betrachten.

Den Begriff der offenen Kugel haben wir bereits spezifiziert, damit zusammenhängend hier einige weitere Definitionen:

Definition 10: Die *abgeschlossene Kugel* mit Radius r und Mittelpunkt a sei die Menge

$$\overline{B}_r(a) = \{x \in X :\, d(a,\, x) \leq r\}.$$

Unter dem *Durchmesser* einer nichtleeren Teilmenge A von X verstehen wir

$$d(A) = \sup\{d(x,\, y) :\, x,\, y \in A\},$$

und A heißt *beschränkt*, wenn $d(A) < \infty$. Der *Abstand* zweier nichtleerer Teilmengen A und B ist definiert als

$$d(A,\, B) = \inf\{d(x,\, y) :\, x \in A,\, y \in B\}$$

und der Abstand zwischen einem Element $x \in X$ und einer nichtleeren Teilmenge A als

$$d(x,\, A) = d(\{x\},\, A).$$

Allerdings sei darauf hingewiesen, dass Bezeichnungen wie „offene Kugel“ oder „abgeschlossene Kugel“ in ultrametrischen Räumen auf gewisse Weise ihre Sinnhaftigkeit verlieren, wie wir gleich sehen werden.

Proposition 8: Es sei $(X,\, d)$ ein ultrametrischer Raum. Dann gilt:

1. Die Kugel $B_r(a)$ ist sowohl offen als auch abgeschlossen.
2. Die Kugel $\overline{B}_r(a)$ ist für $r > 0$ sowohl offen als auch abgeschlossen.

Beweis.

1. In einem beliebigen metrischen Raum ist $B_r(a)$ eine offene Menge. Um zu zeigen, dass $B_r(a)$ in einem ultrametrischen Raum auch abgeschlossen ist, betrachten wir einen Randpunkt b. Jede Umgebung von b muss also Punkte von $B_r(a)$ enthalten. Sei nun $s \leq r$ und $c \in B_r(a) \cap B_s(b)$, dann ist

$$d(a,\, b) \leq \max\{d(a,\, c),\, d(b,\, c)\} < \max\{r,\, s\} = r.$$

   Die Kugel $B_r(a)$ enthält also alle ihre Randpunkte und ist somit abgeschlossen.

2. $\overline{B}_r(a)$ ist in einem metrischen Raum abgeschlossen. Dass $\overline{B}_r(a)$ in einem ultrametrischen Raum auch offen ist, sehen wir, indem wir zeigen, dass jeder Punkt $b \in \overline{B}_r(a)$ eine Umgebung besitzt, die ganz in $\overline{B}_r(a)$ liegt. Seien also $b \in \overline{B}_r(a)$, $s \leq r$ sowie $c \in B_s(b)$ beliebig, dann gilt

$$d(a,\, c) \leq \max\{d(b,\, c),\, d(a,\, b)\} \leq r.$$

   Es ist also $c \in B_s(b) \subseteq \overline{B}_r(a)$. □

Bemerkung 3: Die Voraussetzung $r > 0$ in Punkt 2 obiger Proposition ist deshalb notwendig, da ansonsten jede einelementige Menge und somit jede Menge offen wäre. Wir hätten es also mit der diskreten Topologie zu tun, die vom trivialen Absolutbetrag induziert wird, was wir im nichtarchimedischen Fall aber ausgeschlossen haben.

In Punkt 1 hingegen erhalten wir für $r = 0$ die leere Menge. Diese ist immer offen und abgeschlossen.

Proposition 9: Es sei $(X,\ d)$ ein ultrametrischer Raum. Dann ist die Sphäre

$$S_r(a) = \{x \in X :\ d(a,\ x) = r\}$$

sowohl offen als auch abgeschlossen.

Beweis. Die Sphäre ist als Durchschnitt der abgeschlossenen Kugel mit dem Komplement der offenen Kugel, also zweier abgeschlossener Mengen, abgeschlossen. Das gilt bezüglich jeder Metrik.

Im ultrametrischen Fall ist $S_r(a)$ aber auch offen. Es sei nämlich $b \in S_r(a)$ und $s < r$. Ist nun $c \in B_s(b)$, so folgt wegen $d(a,\ c) = \max\{d(b,\ c),\ d(a,\ b)\} = r$, dass jeder Punkt auf der Sphäre eine offene Umgebung besitzt, die ganz in $S_r(a)$ enthalten ist. □

Bemerkung 4: Die Sphäre ist nicht der Rand der Kugel. Denn wäre dies der Fall, dann müsste in jeder Umgebung eines Punktes auch ein Element, das nicht zum Rand gehört, liegen. Das widerspräche aber der Sphäre als offener Menge. Der Rand der Kugel ist also leer.

Bemerkung 5: Da es in ultrametrischen Räumen so viele Mengen gibt, die sowohl offen als auch abgeschlossen sind, wird in der englischsprachigen Literatur dafür meistens der Begriff „clopen“ als Synthese von „open“ und „closed“ verwendet.

Auch für die Geometrie eines ultrametrischen Raumes ergeben sich überraschende Konsequenzen:

Proposition 10: Es sei $(X,\ d)$ ein ultrametrischer Raum. Dann gilt:

1. Jeder Punkt einer Kugel kann als ihr Mittelpunkt gewählt werden.
2. Sind zwei Kugeln B und $B^{'}$ nicht disjunkt, dann ist die eine in der anderen enthalten.
3. Sind zwei Kugeln B und $B^{'}$ disjunkt, dann gilt $d(a,\ b) = d(B,\ B^{'})$ für alle $a \in B$ und für alle $b \in B^{'}$.
4. Der Durchmesser einer Kugel ist kleiner oder gleich ihrem Radius.

Beweis.

1. Es sei $b \in B_r(a)$, dann ist $d(a,\ b) < r$, und es gilt

   $$c \in B_r(a) \Longleftrightarrow d(a,\ c) < r \Longleftrightarrow d(b,\ c) \leq \max\{d(a,\ b),\ d(a,\ c)\} < r \Longleftrightarrow c \in B_r(b).$$

   Es ist also $B_r(a) = B_r(b)$. Dies gilt analog für eine abgeschlossene Kugel, im Beweis ist an den entsprechenden Stellen lediglich „$<$“ durch „$\leq$“ zu ersetzen.

2. Es seien B und $B^{'}$ beliebig offen oder abgeschlossen. Angenommen, keine der Aussagen $B \cap B^{'} = \emptyset$, $B \subseteq B^{'}$ beziehungsweise $B^{'} \subseteq B$ wäre wahr. Dann gäbe es ein Element $a \in B \cap B^{'}$, das nach Punkt 1 als Mittelpunkt von B und auch von $B^{'}$ aufgefasst werden kann. Weiters gäbe es ein $b \in B \backslash B^{'}$ sowie ein Element $c \in B^{'} \backslash B$. Es folgt

$$d(c,\, a) > d(b,\, a), \text{ da } b \in B \text{ und } c \notin B,$$
$$d(b,\, a) > d(c,\, a), \text{ da } c \in B^{'} \text{ und } b \notin B^{'},$$

ein Widerspruch.

3. Es seien B und $B^{'}$ beliebig offen oder abgeschlossen, $a,\, b \in B$ und $c \in B^{'}$. Dann ist $d(a,b) < d(a,c)$ und $d(a,b) < d(b,c)$, woraus $d(a,c) = d(b,c)$ folgt. Aus Symmetriegründen ist auch $d(a,\, c) = d(a,\, d)$ für alle $d \in B^{'}$. Es ist somit $(a,\, c) \mapsto d(a,\, c)$ für alle $a \in B$, $c \in B^{'}$ konstant.

4. Der Durchmesser einer Kugel B (beziehungsweise $\overline{B}$) ist definiert als $\sup\{d(a,\, b) :\, a,\, b \in B\}$. Aus dem bis jetzt Gezeigten folgt, dass $d(a,\, b) \leq r$ für alle $a,\, b \in B$ ist. □

Beispiel 2: Wir betrachten den p-adischen Absolutbetrag auf $\mathbb{Q}$. Dieser nimmt nur die Werte $\{p^n :\, n \in \mathbb{Z}\}$ und Null an. Da $\{x \in \mathbb{Q} :\, |x-a|_p < 1\} = \{x \in \mathbb{Q} :\, |x-a|_p \leq p^{-1}\}$, ist $B_1(a) = \overline{B}_r(a) = B_r(a)$ für alle $r \in (p^{-1}, 1)$. Ist zum Beispiel $p = 3$, dann ist $B_1(a) = B_{1/2}(a) = \overline{B}_{1/3}(a)$. Eine Kugel hat somit unendlich viele Radien. Der Durchmesser ist hier immer p^{-1}, also kleiner oder gleich r.

Beispiel 3: Bezüglich des p-adischen Absolutbetrags auf $\mathbb{Q}$ ist $\overline{B}_1(0)$ genau die Menge $\{x \in \mathbb{Q} : |x|_p \leq 1\}$. Diese lässt sich als disjunkte Vereinigung von $B_1(0)$ und $S_1(0)$ schreiben, denn es gilt

$$p \mid x \Longleftrightarrow |x|_p < 1 \Longleftrightarrow x \in B_1(0) \text{ beziehungsweise } p \nmid x \Longleftrightarrow |x|_p = 1 \Longleftrightarrow x \in S_1(0).$$

Für jedes $x \in S_1(0)$ ist also $x \equiv c \pmod p$ mit $c \in \{1,\, 2,\, \ldots,\, p-1\}$. Das heißt, $p \mid x - c$ beziehungsweise $|x-c|_p < 1$. Das lässt sich auch interpretieren als $x \in B_1(c)$. Es folgt somit $S_1(0) = B_1(1) \cup B_1(2) \cup \cdots \cup B_1(p-1)$. Das ergibt insgesamt

$$\overline{B}_1(0) = B_1(0) \cup B_1(1) \cup B_1(2) \cup \cdots \cup B_1(p-1),$$

das heißt, die abgeschlossene Kugel lässt sich als disjunkte Vereinigung von p offenen Kugeln schreiben.

Die Tatsache, dass es in dieser Topologie so viele Menge gibt, die offen und abgeschlossen sind, hat auch für die Zusammenhangskomponenten ultrametrischer Räume interessante Konsequenzen.

Definition 11: Ein topologischer Raum X heißt *unzusammenhängend*, wenn es zwei nichtleere, disjunkte, offene Mengen O_1, O_2 gibt, deren Vereinigung X ist, also $O_1 \cap O_2 = \emptyset$ und $X = O_1 \cup O_2$.

Kann ein topologischer Raum nicht auf diese Weise zerlegt werden, heißt er *zusammenhängend*.

Eine Teilmenge A eines topologischen Raumes heißt zusammenhängend beziehungsweise unzusammenhängend, wenn sie bezüglich der Spurtopologie zusammenhängend beziehungsweise unzusammenhängend ist.

Unter der *Zusammenhangskomponente eines Punktes* x verstehen wir die Vereinigung aller zusammenhängenden Mengen, in denen x enthalten ist, also die größte zusammenhängende Menge, die diesen Punkt enthält.

Besteht die Zusammenhangskomponente eines jeden Punktes x nur aus diesem Punkt, das heißt, nur aus der Einpunktmenge $\{x\}$, dann heißt der topologische Raum *total unzusammenhängend.*

Proposition 11: In einem ultrametrischen Raum ist jede Kugel mit Radius $r > 0$ unzusammenhängend.

Beweis. Jede Kugel ist sowohl offen als auch abgeschlossen. Betrachten wir eine in ihr enthaltene Kugel mit kleinerem Radius, dann ist diese offen und abgeschlossen. Das ist schon die Zerlegung, die wir suchen. □

Proposition 12: Ein ultrametrischer Raum X ist total unzusammenhängend.

Beweis. Wir betrachten einen Punkt x mit der Zusammenhangskomponente S. Angenommen S enthält noch einen weiteren Punkt y, dann ist $r = d(x, y)$ der Abstand zwischen den Punkten. Es sei $O_1 = B_{r/2}(x)$ die offene Kugel mit Radius $\frac{r}{2}$ um x. In dieser ist y nicht enthalten. Wir wissen, dass diese Kugel auch abgeschlossen ist. Es ist also $O_2 = S \backslash O_1$ offen, und wir haben eine Zerlegung in zwei disjunkte offene Mengen gefunden, deren Vereinigung S ist. Die Zusammenhangskomponente von x besteht also nur aus diesem Punkt. □

Bemerkung 6: Das bedeutet, dass es in ultrametrischen Räumen keine zusammenhängenden Mengen gibt, die aus mehr als einem Element bestehen. Andererseits ist die Menge $\{x\}$ nicht offen. Wäre dies nämlich für alle x der Fall, wäre jede Teilmenge des Raumes offen. Es würde somit die durch den trivialen Absolutbetrag induzierte diskrete Topologie vorliegen, was wir aber ausgeschlossen haben.

1.3 Algebra

In diesem Abschnitt betrachten wir den Zusammenhang zwischen der algebraischen Struktur eines Körpers und eines auf ihm definierten, nichtarchimedischen Absolutbetrags.

Proposition 13: Es sei K ein Körper mit einem nichtarchimedischen Absolutbetrag $|\,|$. Dann ist die Menge

$$\mathcal{O} = \overline{B}_1(0) = \{x \in K : \ |x| \leq 1\}$$

ein Teilring von K, und die Menge

$$\mathcal{P} = B_1(0) = \{x \in K : \ |x| < 1\}$$

ist ein Ideal von $\mathcal{O}$. $\mathcal{P}$ ist sogar ein maximales Ideal von $\mathcal{O}$ und $\mathcal{O}$ ein maximaler Teilring von K. Weiters ist jedes Element in $\mathcal{O} \backslash \mathcal{P}$ invertierbar.

Beweis. Das meiste folgt unmittelbar aus den Eigenschaften eines nichtarchimedischen Absolutbetrags, die wir in Abschnitt 1.1.2 hergeleitet haben. Wir sehen sofort, dass $\mathcal{O}$ sowohl 0 als

auch 1 enthält. Sind x und y in $\mathcal{O}$, dann sind es auch $-x$, $x+y$ und $x \cdot y$, denn $|-x| = |x| \leq 1$, $|x+y| \leq \max\{|x|, |y|\} \leq 1$ sowie $|xy| = |x|\,|y| \leq 1$. $\mathcal{O}$ ist also tatsächlich ein Teilring.

Es ist $\mathcal{O}$ ein maximaler Teilring, denn angenommen, es gäbe einen Teilring $\mathcal{O}'$, der $\mathcal{O}$ echt enthält, dann gäbe es ein $y \in \mathcal{O}'$ mit $|y| > 1$. Es wäre auch $y^n \in \mathcal{O}'$ für alle $n \in \mathbb{N}$.

Sei $r = |y|$, dann ist $\overline{B}_{r^n}(0) = y^n\mathcal{O} \subseteq \mathcal{O}'$.

Für $r^n = |y^n| \to \infty$ sehen wir, dass $K = \bigcup_{n\geq 1} y^n\mathcal{O} = \mathcal{O}'$ gilt. Das heißt, ein Teilring, der $\mathcal{O}$ echt enthält muss der ganze Raum sein.

Analog können wir zeigen, dass $\mathcal{P}$ abgeschlossen unter Addition ist. Ist $x \in \mathcal{O}$ und $y \in \mathcal{P}$, dann ist $x \cdot y \in \mathcal{P}$, denn es gilt ja $|x| \leq 1$, $|y| < 1$ und somit $|xy| < 1$.

Für ein $x \in \mathcal{O}\backslash\mathcal{P}$ ist $|x| = 1$. Somit ist x invertierbar in $\mathcal{O}$, denn es ist dann $\left|\frac{1}{x}\right| = 1$, also $\frac{1}{x} \in \mathcal{O}$.

Daraus folgt auch, dass $\mathcal{P}$ maximales Ideal ist, denn ein Ideal, das echt größer ist als $\mathcal{P}$, enthält eine Einheit und stimmt daher mit ganz $\mathcal{O}$ überein. □

Definition 12: Es sei K ein Körper und $|\,|$ ein nichtarchimedischer Absolutbetrag auf K. Der Teilring

$$\mathcal{O} = \{x \in K : \ |x| \leq 1\}.$$

heißt *der Bewertungsring* von $|\,|$. Das Ideal

$$\mathcal{P} = \{x \in K : \ |x| < 1\}.$$

heißt *das Bewertungsideal* von $|\,|$.

Ein Ring R mit genau einem eindeutig bestimmten maximalen Ideal I heißt *lokaler Ring*. Dieses Ideal ist das Komplement der Einheitengruppe, das heißt, $I = R\backslash R^\times$.

Definition 13: Es sei K ein Körper und $|\,|$ ein nichtarchimedischer Absolutbetrag auf K. Der Quotient κ des maximalen Teilrings $\mathcal{O}$ von K durch das maximale Ideal $\mathcal{P}$, also

$$\kappa = \mathcal{O}/\mathcal{P},$$

heißt *der Restklassenkörper* von $|\,|$.

Bemerkung 7: Wegen dieses Zusammenhangs ist es manchmal sinnvoll, Problemstellungen von einem algebraischen Standpunkt aus zu betrachten. Gesuchte Eigenschaften eines nichtarchimedischen Absolutbetrags werden so zu Eigenschaften des entsprechenden Bewertungsrings.

So kann Beispiel 3 auf Seite 17, in dem gezeigt wurde, dass die abgeschlossene Einheitskugel als disjunkte Vereinigung offener Kugeln mit Radius 1 darstellbar ist, algebraisch ausgedrückt werden, indem die offenen Kugeln als die Restklasse des Ideals $\mathcal{P}$ in $\mathcal{O}$ angesehen werden.

Betrachten wir nun die Resultate dieses Abschnitts in Zusammenhang mit dem p-adischen Absolutbetrag.

Proposition 14: Es sei $K = \mathbb{Q}$ und $|\ | = |\ |_p$ der p-adische Absolutbetrag. Dann gilt:

1. Der assoziierte Bewertungsring ist $\mathcal{O} = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} :\ p \nmid b\}$.
2. Das Bewertungsideal ist $\mathcal{P} = p\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} :\ p \nmid b \text{ und } p \mid a\}$.
3. Der Restklassenkörper ist isomorph zum endlichen Körper mit p Elementen, das heißt, $\kappa \cong \mathbb{F}_p$.

Beweis. Für die ersten zwei Punkte müssen wir uns nur die Definitionen des p-adischen Absolutbetrags in Erinnerung rufen: Für $x = \frac{a}{b} \in \mathbb{Q}$ gilt $\left|\frac{a}{b}\right|_p = p^{-\mathrm{ord}_p(x)}$, wobei $\frac{a}{b} = p^{\mathrm{ord}_p(x)}\frac{a'}{b'}$ ist und so, dass $a'b'$ nicht von p geteilt wird.

Wir sehen, dass $\frac{a}{b}$ genau dann ein Element von $\mathcal{O}$ ist, wenn $\mathrm{ord}_p(x) \geq 0$ ist. Da der Bruch gekürzt vorliegt, ist das genau dann der Fall, wenn p kein Teiler von b ist. Analog sehen wir, dass $\frac{a}{b}$ genau dann in $\mathcal{P}$ liegt, wenn $\mathrm{ord}_p(a) > 0$ ist, wenn also $p \nmid b$ und $p \mid a$ gelten.

Nun zur dritten Behauptung: Wir müssen zeigen, dass es einen Isomorphismus zwischen $\mathcal{O}/\mathcal{P}$ und $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ gibt.

Dazu definieren wir eine Abbildung $f\colon\ \mathbb{Z}_{(p)} \to \mathbb{Z}/p\mathbb{Z}$, $\frac{a}{b} \mapsto \big(a + p\mathbb{Z}\big)\big(b^{-1} + p\mathbb{Z}\big)$, wobei $\big(b^{-1} + p\mathbb{Z}\big)$ die inverse Restklasse von $\big(b + p\mathbb{Z}\big)$ bezeichnet, die ja wegen $b \nmid p$ jedenfalls existiert.

Betrachten wir nun ein Element $\frac{a'}{b'}$ in $\mathbb{Z}_{(p)}$, welches $\frac{a'}{b'} = \frac{a}{b}$ mit $p \nmid bb'$ erfüllt. Dann ist $a'b = ab'$, und es folgt

$$\big(a' + p\mathbb{Z}\big)\big(b + p\mathbb{Z}\big) = \big(a + p\mathbb{Z}\big)\big(b' + p\mathbb{Z}\big).$$

Multiplizieren wir beide Seiten dieser Gleichung mit $\big(b^{-1} + p\mathbb{Z}\big)\left(\big(b'\big)^{-1} + p\mathbb{Z}\right)$, so sehen wir, dass

$$\big(a' + p\mathbb{Z}\big)\left(\big(b'\big)^{-1} + p\mathbb{Z}\right) = \big(a + p\mathbb{Z}\big)\big(b^{-1} + p\mathbb{Z}\big)$$

ist. Das bedeutet aber auch, dass $f\big(\frac{a'}{b'}\big) = f\left(\frac{a}{b}\right)$ gilt. Somit ist die Abbildung f wohldefiniert.

Die Abbildung f ist surjektiv, denn für $a \in \{0,\ 1,\ \ldots,\ p-1\}$ und für $b = 1$ erhalten wir wegen

$$f\left(\frac{a}{1}\right) = \big(a + p\mathbb{Z}\big)\big(1^{-1} + p\mathbb{Z}\big) = \big(a + p\mathbb{Z}\big)$$

jede Restklasse modulo p. Insbesondere ist $f(1) = \big(1 + p\mathbb{Z}\big)$, und da außerdem

$$\begin{aligned} f\left(\frac{a}{b} + \frac{c}{d}\right) = f\left(\frac{ad + cb}{bd}\right) &= \big((ad + cb) + p\mathbb{Z}\big)\big((bd)^{-1} + p\mathbb{Z}\big) \\ &= \big((ad) + p\mathbb{Z}\big)\big((bd)^{-1} + p\mathbb{Z}\big) + \big((cb) + p\mathbb{Z}\big)\big((bd)^{-1} + p\mathbb{Z}\big) \\ &= \big(a + p\mathbb{Z}\big)\big(b^{-1} + p\mathbb{Z}\big) + \big(c + p\mathbb{Z}\big)\big(d^{-1} + p\mathbb{Z}\big) \\ &= f\left(\frac{a}{b}\right) + f\left(\frac{c}{d}\right), \end{aligned}$$

$$\begin{aligned} f\left(\frac{a}{b} \cdot \frac{c}{d}\right) &= \big((ac) + p\mathbb{Z}\big)\big((bd)^{-1} + p\mathbb{Z}\big) \\ &= \big(a + p\mathbb{Z}\big)\big(c + p\mathbb{Z}\big)\big(d^{-1} + p\mathbb{Z}\big)\big(b^{-1} + p\mathbb{Z}\big) \\ &= \big(a + p\mathbb{Z}\big)\big(b^{-1} + p\mathbb{Z}\big) \cdot \big(c + p\mathbb{Z}\big)\big(d^{-1} + p\mathbb{Z}\big) \\ &= f\left(\frac{a}{b}\right) \cdot f\left(\frac{c}{d}\right) \end{aligned}$$

gelten, handelt es sich bei f um einen Ringepimorphismus.

Der Kern dieses Epimorphismus ist gleich $p\mathbb{Z}_{(p)}$, denn es ist

$$f\left(\tfrac{a}{b}\right) = \left(a + p\mathbb{Z}\right)\left(b^{-1} + p\mathbb{Z}\right) = 0$$

genau dann, wenn $a \equiv 0 \pmod{p}$ gilt.

Wir haben somit auch die dritte Behauptung gezeigt, denn mit dem Homomorphiesatz für Ringe folgt jetzt unmittelbar, dass

$$\mathbb{Z}_{(p)}\big/p\mathbb{Z}_{(p)} \cong \mathbb{Z}\big/p\mathbb{Z}$$

ist. □

Quellen und Literatur zu Kapitel 1

Abschnitt 1.1 basiert auf [1], S. 4-8, [9], S. 23-26, 29-31, 33, 34, [13], S. 7, 11-13, 20, [14], S. 2-6, [18], S. 25, 26, 77-79 und [19], S. 18-20.
Zu Abschnitt 1.2 vergleiche [1] S. 15, [9], S. 34-39, [13], S. 53-56, [14], S. 6, [18], S. 69-73 und zu Abschnitt 1.3 [9], S. 39-41 sowie [18], S. 79.

2

Absolutbeträge auf $\mathbb{Q}$

In diesem Kapitel werden wir uns überlegen, wie viele verschiedene Absolutbeträge es auf den rationalen Zahlen gibt. Um zu einer sinnvollen Einteilung zu gelangen, muss definiert werden, was es für Absolutbeträge bedeutet, „verschieden“ oder eben „gleich“ zu sein.

2.1 Äquivalente Absolutbeträge

Definition 1: Es seien d_1 und d_2 zwei Metriken. Wir nennen sie *äquivalent*, wenn sie dieselbe Topologie induzieren, wenn also jede offene Menge bezüglich d_1 auch eine offene Menge bezüglich d_2 ist und umgekehrt. Das ist gleichbedeutend damit, dass jede Folge, die bezüglich der einen Metrik eine Nullfolge bildet, auch eine Nullfolge bezüglich der anderen Metrik ist.

Zwei Absolutbeträge $|\ |_1$ und $|\ |_2$ heißen äquivalent, wenn sie äquivalente Metriken induzieren. Oft wird dafür auch $|\ |_1 \sim |\ |_2$ geschrieben.

Mit Hilfe des folgenden Lemmas kann leicht entschieden werden, ob zwei gegebene Absolutbeträge äquivalent sind:

Lemma 1: Es seien $|\ |_1$ und $|\ |_2$ zwei nichttriviale Absolutbeträge auf einem Körper K. Folgende Aussagen sind äquivalent:

1. $|\ |_1$ und $|\ |_2$ sind äquivalente Absolutbeträge.
2. Für jedes $x \in K$ mit $|x|_1 < 1$ folgt $|x|_2 < 1$.

Es gibt dann eine positive, reelle Zahl α, sodass für jedes $x \in K$ gilt $|x|_2 = |x|_1^{\alpha}$.

Beweis. (1) $\Longrightarrow$ (2) Es sei $|x|_1 < 1$. Da $|x^n|_1 = |x|_1^n$ gilt, ist $(x^n)_{n\geq 0}$ eine Nullfolge bezüglich $|\ |_1$ und wegen der Äquivalenz der Absolutbeträge auch eine bezüglich $|\ |_2$. Das bedeutet, dass $\lim_{n\to\infty} |x|_2^n = 0$ und somit $|x|_2 < 1$ ist.

(1) $\Longleftarrow$ (2) Da die Absolutbeträge nichttrivial sind, gibt es ein $x_0 \in K^\times$ mit $|x_0|_1 > 1$. Es sei $y_0 \neq 0$ ein weiteres Element des Körpers, dann ist $|x_0|_1 = |y_0|_1^\beta$ mit $\beta = \frac{\log|x_0|_1}{\log|y_0|_1}$.

Es sei $\frac{m}{n} \in \mathbb{Q}$ so gewählt, dass $\frac{m}{n} > \beta$ und $n > 0$ ist. Es ist $|x_0|_1 < |y_0|_1^{\frac{m}{n}}$ beziehungsweise $\left|x_0^n y_0^{-m}\right|_1 < 1$. Aus der Voraussetzung folgt $\left|x_0^n y_0^{-m}\right|_2 < 1$, das heißt $|x_0|_2^n < |y_0|_2^m$ beziehungsweise $|x_0|_2 < |y_0|_2^{\frac{m}{n}}$. Somit ist $|x_0|_2 \leq |y_0|_2^\beta$.

Es sei nun $\frac{m}{n} < \beta$. Dann gilt $|x_0|_1 > |y_0|_1^{\frac{m}{n}}$ beziehungsweise $\left|x_0^n y_0^{-m}\right|_1 > 1$.

Wir können uns leicht überlegen, dass, wenn (2) vorausgesetzt wird, für jedes x mit $|x|_1 > 1$ auch $|x|_2 > 1$ ist, denn ist $|x|_1 > 1$ dann ist $|x|_1^{-1} = \left|x^{-1}\right|_1 < 1$, somit auch $\left|x^{-1}\right|_2 < 1$, und es gilt $|x|_2 > 1$.

Also ist auch $\left|x_0^n y_0^{-m}\right|_2 > 1$, woraus $|x_0|_2^n > |y_0|_2^m$ beziehungsweise $|x_0|_2 > |y_0|_2^{\frac{m}{n}}$ folgt. Somit ist $|x_0|_2 \geq |y_0|_2^\beta$.

Insgesamt muss also $|x_0|_2 = |y_0|_2^\beta$ gelten. Nun ist $\beta = \frac{\log|x_0|_1}{\log|y_0|_1} = \frac{\log|x_0|_2}{\log|y_0|_2}$ und daher $\log|x_0|_2 = \frac{\log|y_0|_2}{\log|y_0|_1} \cdot \log|x_0|_1$.

Wir setzen $\alpha = \frac{\log|y_0|_2}{\log|y_0|_1}$ und erhalten $|x_0|_2 = |x_0|_1^\alpha$ für $x_0 \in K^\times$. Da diese Gleichung offensichtlich auch von $x_0 = 0$ erfüllt wird, gilt sie für alle Elemente des Körpers, und wir können $|\,|_2 = |\,|_1^\alpha$ schreiben.

Es bleibt noch zu zeigen, dass die beiden Absolutbeträge äquivalent sind. Dazu betrachten wir eine Nullfolge $(x_n)_{n\geq 0}$ bezüglich $|\,|_2$, das heißt, $\lim_{n\to\infty}|x_n|_2 = 0$.

Dann ist auch $\lim_{n\to\infty}|x_n|_1^\alpha = 0$ und somit $\lim_{n\to\infty}|x_n|_1 = 0$. Mit derselben Argumentation folgt, dass auch jede Nullfolge bezüglich $|\,|_2$ eine Nullfolge bezüglich $|\,|_1$ ist. □

Es ist uns nun möglich, die Beispiele für Absolutbeträge, die wir im ersten Kapitel kennengelernt haben, auf ihre Äquivalenz hin zu untersuchen. Das soll im Folgenden geschehen.

Proposition 1: Es sei $|\,|$ der „gewöhnliche“ Absolutbetrag auf den rationalen Zahlen und α eine positive reelle Zahl. Es ist $|\,|^\alpha$ ein Absolutbetrag auf $\mathbb{Q}$ genau dann, wenn $\alpha \leq 1$ ist. Dieser Absolutbetrag ist dem „gewöhnlichen“ äquivalent.

Beweis. Es sei $\alpha \leq 1$. Dann sind für $|\,|^\alpha$ die Eigenschaften (A1) und (A2) des Absolutbetrags aus Definition 1 auf Seite 7 offensichtlich erfüllt.

Es bleibt noch die Dreiecksungleichung zu zeigen. Es seien x, $y \in \mathbb{Q}$, und wir nehmen o.B.d.A. an, dass $|y| \leq |x|$ ist. Dann gilt

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

Bei dieser Ungleichung haben wir beim Schritt von der ersten auf die zweite Zeile verwendet, dass für eine reelle Zahl $r \geq 1$ und α wie vorausgesetzt $r \geq r^\alpha$ ist, und beim darauffolgenden Schritt, dass $r \leq r^\alpha$ für $0 \leq r \leq 1$ und $\alpha \leq 1$ gilt.

Die Äquivalenz der Absolutbeträge folgt aus Lemma 1.

Ist umgekehrt $\alpha > 1$, so ist die Dreiecksungleichung nicht erfüllt. Es sei zum Beispiel $x = y = 1$, dann ist $|1+1|^\alpha = 2^\alpha$, und das ist jedenfalls größer als $|1|^\alpha + |1|^\alpha = 2$. Es handelt sich somit unter diesen Voraussetzungen bei $|\,|^\alpha$ um keinen Absolutbetrag. □

Proposition 2: Ist $|\,|$ ein nichtarchimedischer Absolutbetrag, dann ist $|\,|^\alpha$ für jedes beliebige $\alpha > 0$ ebenfalls ein nichtarchimedischer Absolutbetrag. Dieser ist zu $|\,|$ äquivalent.

Beweis. Es sei $|\,|$ ein nichtarchimedischer Absolutbetrag und $\alpha > 0$ beliebig. Für $|\,|^\alpha$ sind dann die Eigenschaften (A1) und (A2) des Absolutbetrags klarerweise erfüllt, und auch die „starke" Dreiecksungleichung gilt, denn für $x,\, y \in \mathbb{Q}$ ist

$$\begin{aligned} |x+y|^\alpha &\leq (\max\{|x|\,,\,|y|\})^\alpha \\ &= \max\{|x|^\alpha,\, |y|^\alpha\}\,. \end{aligned}$$

Die beiden Absolutbeträge sind äquivalent, da sie äquivalente Metriken induzieren, wie wir in Lemma 1 gezeigt haben. □

Bemerkung 1: Ist ein Absolutbetrag $|\,|$ dem trivialen Absolutbetrag τ_K äquivalent, dann ist auch $|\,| = \tau_K^\alpha$ trivial, denn für jedes $\alpha > 0$ gilt $\tau_K(x) = 1^\alpha = 1$ für $x \neq 0$ sowie $\tau_K(x)^\alpha = 0^\alpha = 0$ für $x = 0$.

Korollar 1: Für zwei verschiedene Primzahlen p und q sind $|\,|_p$ und $|\,|_q$ nicht äquivalent.

Beweis. Wenn wir die Folge $(x_n)_{n\geq 1} = \left(\left(\frac{p}{q}\right)^n\right)_{n\geq 1}$ betrachten, folgt die Aussage unmittelbar aus Lemma 1, denn für diese ist $\lim_{n\to\infty} |x_n|_p = 0$ aber $\lim_{n\to\infty} |x_n|_q = \infty$. □

Bemerkung 2: Es sei $\rho < 1$ eine positive reelle Zahl, dann ist $|x| = \rho^{\mathrm{ord}_p(x)}$ ein Absolutbetrag auf $\mathbb{Q}$. Dieser ist dem p-adischen Absolutbetrag äquivalent. Um das einzusehen, müssen wir einfach die reelle Zahl α aus Lemma 1 so wählen, dass $\rho^\alpha = p^{-1}$ ist.

Bemerkung 3: Für zwei nichttriviale, äquivalente Absolutbeträge $|\,|_1$ und $|\,|_2$ gilt, dass sie entweder beide archimedisch oder beide nichtarchimedisch sind. Denn, wie wir im ersten Kapitel besprochen haben, wird ein Absolutbetrag genau dann „archimedisch" respektive „nichtarchimedisch" genannt, wenn für jede ganze Zahl $n \neq 0$ gilt, dass $|n| \geq 1$ respektive $|n| \leq 1$ ist, und wir sehen mit Lemma 1 sofort, dass ein archimedischer Absolutbetrag einem nichtarchimedischen nicht äquivalent sein kann.

Bemerkung 4: Um Verwechslungen zu vermeiden, bezeichnen wir im Folgenden den „gewöhnlichen" Absolutbetrag auf den rationalen Zahlen mit $|\,|_\infty$, verwenden also den Index „∞". Diese Wahl ist nicht zufällig und in diesem Zusammenhang in der Literatur weit verbreitet. Den genauen Grund dafür werden wir im Anschluss an den Satz von Ostrowski diskutieren.

2.2 Der Satz von Ostrowski

Satz 1 (Satz von Ostrowski): Jeder nichttriviale Absolutbetrag auf $\mathbb{Q}$ ist entweder dem „gewöhnlichen“ Absolutbetrag $|\ |_\infty$ oder einem der p-adischen Absolutbeträge $|\ |_p$ äquivalent.

Beweis. Es sei $|\ |$ ein nichttrivialer Absolutbetrag auf $\mathbb{Q}$. Wir unterscheiden zwei Fälle:

1. Wir nehmen zunächst an, dass $|\ |$ archimedisch sei. Da der Absolutbetrag nichttrivial ist, gibt es eine kleinste positive ganze Zahl n_0 mit $|n_0| > 1$. Daher können wir eine reelle Zahl $\alpha > 0$ finden mit $|n_0| = n_0^\alpha$.
   Wir wollen zeigen, dass $|x| = |x|_\infty^\alpha$ für dieses α und für alle rationalen Zahlen x gilt, der betrachtete Absolutbetrag also dem „gewöhnlichen“ äquivalent ist. Es genügt, dies für positive ganze Zahlen n zu zeigen, denn mit Hilfe der Eigenschaften (A1) und (A2) aus Definition 1 auf Seite 7 lässt sich die Aussage auf alle rationalen Zahlen verallgemeinern.
   Es sei also n eine beliebige positive ganze Zahl, die wir sozusagen zur Basis n_0 darstellen wollen, das heißt,

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k,$$

   mit $a_k \neq 0$ und $0 \leq a_i \leq n_0 - 1$ für $i = 0, \ldots, k$, wobei k durch die Ungleichung $n_0^k \leq n < n_0^{k+1}$ festgelegt ist. Es gilt also $k = \left\lfloor \frac{\log n}{\log n_0} \right\rfloor$. Betrachten wir den Absolutbetrag von n, erhalten wir

$$\begin{aligned} |n| &= \left|a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k\right| \\ &\leq |a_0| + |a_1|\, n_0^\alpha + |a_2|\, n_0^{2\alpha} + \cdots + |a_k|\, n_0^{k\alpha}. \end{aligned}$$

   Da n_0 nach Voraussetzung die kleinste natürliche Zahl mit Absolutbetrag größer als Eins ist, muss $|a_i| \leq 1$ für $i = 0, \ldots, k$ gelten. Das ergibt

$$\begin{aligned} |n| &\leq 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{k\alpha} \\ &= n_0^{k\alpha}\left(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-k\alpha}\right) \\ &\leq n_0^{k\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha} \\ &= n_0^{k\alpha} \frac{n_0^\alpha}{n_0^\alpha - 1} \\ &\leq n^\alpha C. \end{aligned}$$

   Beim letzten Schritt haben wir berücksichtigt, dass $n_0^k \leq n$ ist. Außerdem haben wir $C = \frac{n_0^\alpha}{n_0^\alpha - 1}$ gesetzt, und es sei darauf hingewiesen, dass diese Konstante nicht von n abhängt.
   Betrachten wir nun die Ungleichung, die ja für jede beliebige natürliche Zahl gilt, für n^N, so erhalten wir $\left|n^N\right| \leq C n^{N\alpha}$ beziehungsweise als N-te Wurzel davon $|n| \leq \sqrt[N]{C} n^\alpha$. Für den Grenzwert $N \to \infty$ ergibt sich $|n| \leq n^\alpha$.
   Um auf die Gleichheit der beiden Seiten schließen zu können, müssen wir noch zeigen, dass auch $|n| \geq n^\alpha$ gilt.
   Es ist

$$n_0^{(k+1)\alpha} = \left|n_0^{k+1}\right| = \left|n + n_0^{k+1} - n\right| \leq |n| + \left|n_0^{k+1} - n\right|,$$

beziehungsweise

$$|n| \geq n_0^{(k+1)\alpha} - \left|n_0^{k+1} - n\right| \geq n_0^{(k+1)\alpha} - \left(n_0^{k+1} - n\right)^{\alpha},$$

da ja

$$\left|n_0^{k+1} - n\right| \leq \left(n_0^{k+1} - n\right)^{\alpha}$$

gilt. Mit $n_0^{k+1} > n \geq n_0^k$ folgt

$$\begin{aligned} |n| &\geq n_0^{(k+1)\alpha} - \left(n_0^{k+1} - n_0^k\right)^{\alpha} \\ &= n_0^{(k+1)\alpha}\left(1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right) \\ &= n_0^{(k+1)\alpha} C' \\ &> n^{\alpha} C'. \end{aligned}$$

Die positive Konstante C' hängt wiederum nicht von n ab. Wenn wir wie oben die Ungleichung für n^N betrachten, die N-te Wurzel nehmen und den Grenzwert bilden, erhalten wir $|n| \geq n^{\alpha}$.
Insgesamt ist also $|n| = n^{\alpha}$ und somit der betrachtete Absolutbetrag $|\,|$ dem „gewöhnlichen“ Absolutbetrag $|\,|_{\infty}$ auf $\mathbb{Q}$ äquivalent.

2. Es sei nun $|\,|$ nichtarchimedisch. Da $|\,|$ nach Voraussetzung nichttrivial ist, gibt es eine kleinste positive ganze Zahl n_0 mit $|n_0| < 1$.
Es muss n_0 eine Primzahl sein, denn angenommen, n_0 wäre eine zusammengesetzte Zahl, so könnten wir diese als Produkt zweier positiver ganzer Zahlen n_1 und n_2 darstellen, also $n_0 = n_1 \cdot n_2$ mit n_1, n_2 kleiner als n_0.
Wegen unserer Wahl von n_0 müsste $|n_1| = |n_2| = 1$ gelten. Das kann aber nicht sein, also ist n_0 tatsächlich eine Primzahl, die wir mit p bezeichnen.
Für jede Primzahl $q \neq p$ gilt $|q| = 1$, denn angenommen, es wäre $|q| < 1$, dann gäbe es ein hinreichend großes N, sodass $\left|q^N\right| = |q|^N < \frac{1}{2}$ wäre.
Da $|p| < 1$ ist, gibt es jedenfalls ein $M \in \mathbb{N}$, sodass $\left|p^M\right| < \frac{1}{2}$ ist, und, weil p^M und q^N relativ prim sind, ganze Zahlen n und m, sodass $mp^M + nq^N = 1$ ist. Es gilt weiters

$$1 = |1| = \left|mp^M + nq^N\right| \leq \left|mp^M\right| + \left|nq^N\right| = |m|\left|p^M\right| + |n|\left|q^N\right|.$$

Der betrachtete Absolutbetrag ist nichtarchimedisch, es sind somit $|m| \leq 1$ und $|n| \leq 1$, und es ergäbe sich für $|q| < 1$ ein Widerspruch:

$$1 \leq \left|p^M\right| + \left|q^N\right| < \frac{1}{2} + \frac{1}{2} = 1.$$

Also gilt für jede Primzahl $q \neq p$, dass $|q| = 1$ ist.
Jede positive ganze Zahl n kann als Produkt ihrer Primfaktoren dargestellt werden, das heißt $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Es ist dann $|n| = |p_1|^{k_1} |p_2|^{k_2} \cdots |p_r|^{k_r}$, wobei ja nur für die Primzahl p gilt, dass $|p| \neq 1$ ist, wie wir uns eben überlegt haben. Die p-adische Ordnung von n ist dann genau das zu diesem p gehörende k_i.
Wir setzen $\rho = |p| < 1$ und erhalten

$$|n| = \rho^{\mathrm{ord}_p(a)}.$$

Mit Hilfe der Eigenschaften (A1) und (A2) aus Definition 1 auf Seite 7 kann leicht gezeigt werden, dass diese Formel für alle rationalen Zahlen x gilt. Der betrachtete Absolutbetrag ist also äquivalent zu $|\,|_p$ und der Satz somit vollständig bewiesen. □

Wir kennen nun alle verschiedenen Absolutbeträge auf den rationalen Zahlen. Durch die sogenannte Produktformel wird ein Zusammenhang all dieser ersichtlich:

Proposition 3 (Produktformel): Für jedes $x \in \mathbb{Q}$, $x \neq 0$ gilt

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

Beweis. Wir müssen die Formel nur für positive ganze Zahlen beweisen, der allgemeine Fall folgt aus den Eigenschaften (A1) und (A2) des Absolutbetrags. Es sei also $n \in \mathbb{N}$, $n \neq 0$ mit der Primfaktorzerlegung $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Dann gilt $|n|_q = 1$ falls $q \neq p_i$, $|n|_{p_i} = p_i^{-k_i}$ für $i = 1, 2, \ldots, k$ und $|n|_\infty = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Das Resultat folgt nun sofort.

Es sei darauf hingewiesen, dass das Produkt $\prod_p |x|_p$ über alle Primzahlen p wohldefiniert ist, denn, wie wir eben gesehen haben, gilt $|x|_{p_i} \neq 1$ nur für endlich viele Primzahlen p_i. □

Bemerkung 5: Aus der Produktformel folgt, dass für eine natürliche Zahl $|n|_p \geq \frac{1}{n}$ ist. Es ist $|n|_\infty = n$, und $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ sei wieder die Primfaktorzerlegung von n. Betrachten wir nun eine fixe Primzahl p_i, dann ist $|n|_{p_i} = 1 \geq \frac{1}{n}$ falls p_i nicht in der Primfaktorzerlegung auftritt beziehungsweise $|n|_{p_i} = p_i^{-k_i} = \frac{p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_r^{k_r}}{n} \geq \frac{1}{n}$ falls p_i in der Primfaktorzerlegung vorkommt.

Bemerkung 6: Die Produktformel ist ein Beispiel dafür, dass die Betrachtung aller Absolutbeträge auf den rationalen Zahlen zu interessanten Resultaten führt. Um den engen Zusammenhang der Absolutbeträge hervorzuheben, hat es sich bei vielen Autorinnen und Autoren durchgesetzt, dem „gewöhnlichen“ Absolutbetrag als Analogie auch eine Art Primzahl, nämlich die „Primzahl im Unendlichen“, zuzuordnen und mit „$p \leq \infty$“ auf *alle* Absolutbeträge $|\ |_p$ zu verweisen.

Das ist auch der Grund für die Verwendung des Index „∞“ beim „gewöhnlichen“ Absolutbetrag.

2.3 Die Vollständigkeit der rationalen Zahlen

Wie wir wissen, sind die rationalen Zahlen bezüglich des „gewöhnlichen“ Absolutbetrags $|\ |_\infty$ nicht vollständig. Wir haben weiter Absolutbeträge auf $\mathbb{Q}$ kennengelernt und im letzten Abschnitt sogar zeigen können, dass es sich bei diesen – bis auf Äquivalenz – um alle Absolutbeträge, die möglich sind, handelt. Eine naheliegende Frage ist, ob die rationalen Zahlen bezüglich dieser Absolutbeträge vollständig oder ebenfalls unvollständig sind.

Zunächst wiederholen wir zwei für diese Fragestellung grundlegende Begriffe:

Es sei (X, d) ein metrischer Raum. Eine Folge $(x_n)_{n \geq 1}$ von Elementen aus X heißt *Cauchyfolge*, wenn es für jedes $\epsilon > 0$ ein $N \in \mathbb{N}$ gibt, sodass $d(x_n, x_m) < \epsilon$ für alle $n, m \geq N$ ist.

Ein metrischer Raum (X, d) heißt *vollständig* bezüglich der Metrik d, wenn jede Cauchyfolge in X konvergiert. Ein Körper mit Absolutbetrag $|\ |$ heißt vollständig, wenn jede Cauchyfolge bezüglich der durch $|\ |$ induzierten Metrik konvergiert.

Lemma 2: Eine Folge $(x_n)_{n\geq 1}$ rationaler Zahlen ist genau dann eine Cauchyfolge bezüglich eines nichtarchimedischen Absolutbetrags $|\ |$, wenn gilt:

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

Beweis. ($\Longrightarrow$) Es sei $(x_n)_{n\geq 1}$ eine Cauchyfolge, dann gilt klarerweise $\lim_{m,n\to\infty} |x_m - x_n| = 0$. Für $m = n + 1$ erhalten wir obige Gleichung.

($\Longleftarrow$) Es sei $m > n$. Da der Absolutbetrag nichtarchimedisch ist, gilt:

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

Daraus folgt die Behauptung. □

Bemerkung 7: Dass eine Cauchyfolge der Bedingung $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$ genügt, gilt bezüglich jedes Absolutbetrags. Für die Umkehrung hingegen lassen sich bezüglich eines archimedischen Absolutbetrags Gegenbeispiele finden. Betrachten wir etwa in $\mathbb{R}$ Folgeglieder der Form $x_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$, dann gilt zwar, dass der Betrag der Differenz $|x_{n+1} - x_n|_\infty = \frac{1}{n+1}$ für $n \to \infty$ gegen Null konvergiert, jedoch ist die Cauchybedingung aus obiger Definition nicht erfüllt, weil die Folge sonst konvergent wäre.

Für den Beweis folgender Proposition ist es hilfreich, sich die Tatsache vor Augen zu führen, dass es eine Cauchyfolge rationaler Zahlen $(x_n)_{n\geq 1}$ gibt, die der Bedingung $\left|x_n^2 - 2\right|_\infty \leq 10^{-n}$ genügt, deren Grenzwert – die irrationale Zahl $\sqrt{2}$ – aber nicht in $\mathbb{Q}$ liegt.

Proposition 4: Die rationalen Zahlen sind bezüglich keines nichttrivialen Absolutbetrags vollständig.

Beweis. Bezüglich des „gewöhnlichen“ Absolutbetrags $|\ |_\infty$ setzten wir dies als bekannt voraus.

Nun zu den p-adischen Absolutbeträgen:

Wir wollen eine Cauchyfolge rationaler Zahlen $(x_n)_{n\geq 0}$ bezüglich $|\ |_p$ finden, deren Grenzwert a jedoch nicht in $\mathbb{Q}$ liegt.

Es sei also p eine Primzahl, $p \neq 2$ und $a \in \mathbb{Z}$ so, dass folgende Bedingungen erfüllt sind:

1. a ist kein Quadrat in $\mathbb{Q}$,
2. $p \nmid a$,
3. $X^2 \equiv a \pmod{p}$ besitzt eine Lösung, das heißt a ist ein quadratischer Rest modulo p.

Es gibt $\frac{1}{2}(p-1)$ quadratische Reste unterhalb von p, aber nur $\sqrt{p}$ Quadrate. Das heißt, wir können so ein a jedenfalls finden, denn es gilt ja $\frac{1}{2}(p-1) > \sqrt{p}$ außer für $p = 3$ und $p = 5$. In diesen Fällen wählen wir für a einfach 7 beziehungsweise 6.

Als Nächstes konstruieren wir eine Cauchyfolge bezüglich $|\ |_p$:

1. Es sei x_0 eine beliebige Lösung von $x_0^2 \equiv a \pmod{p}$.

2. Für x_1 soll gelten, dass $x_1 \equiv x_0 \pmod{p}$ und $x_1^2 \equiv a \pmod{p^2}$ ist.

3. In weiterer Folge wählen wir die x_n so, dass

$$x_n \equiv x_{n-1} \pmod{p^n} \quad \text{und} \quad x_n^2 \equiv a \pmod{p^{n+1}}$$

erfüllt sind.

So eine Folge gibt es. Unsere Konstruktion entspricht dem Lösen der algebraischen Kongruenzen $f(x) \equiv 0 \pmod{p^n}$, wobei $f(X) = \sum_{i=0}^{n} a_i X^i$ ein Polynom mit Koeffizienten aus $\mathbb{Z}$ ist.

In unserem Fall ist $f(X) = X^2 - a$. Die erste Kongruenz $f(x) \equiv 0 \pmod{p}$ ist lösbar, wir haben die Funktion ja entsprechend gewählt.

Wir zeigen den Rest durch Induktion. Es sei also die Kongruenz $f(x) \equiv 0 \pmod{p^{n-1}}$ schon gelöst, A_{n-1} sei die Menge ihrer inkongruenten Lösungen. Gesucht sind nun alle Lösungen von $f(x) \equiv 0 \pmod{p^n}$. Es sei x_n eine solche. Da dieses x_n auch $f(x) \equiv 0 \pmod{p^{n-1}}$ erfüllt, gibt es ein $y \in A_{n-1}$ mit $x_n \equiv y \pmod{p^{n-1}}$. Somit können wir x_n schreiben als $x_n = y + kp^{n-1}$.

Es ist y eine Nullstelle von $f(X) - f(y)$, daher gilt $f(x) - f(y) \equiv (x-y)\,q(x) \pmod{p^n}$, wobei $q(X) \in \mathbb{Z}[X]$ von der Form $\sum_{i=1}^{n} a_i \sum_{j=0}^{i-1} y^{i-j-1} X^j$ sein muss. Somit ist $f(x_n) - f(y) \equiv (x_n - y)\,q(x_n) \equiv kp^{n-1} f'(x_n) \pmod{p^n}$. Dies lässt sich zu $\frac{f(y)}{p^{n-1}} + kf'(x_n) \equiv 0 \pmod{p}$ vereinfachen, da ja $f(x_n) \equiv 0 \pmod{p^n}$ ist. Es ist $x_n \equiv y \pmod{p}$, also auch $f'(x_n) \equiv f'(y) \pmod{p}$. Insgesamt müssen wir also die Kongruenz $\frac{f(y)}{p^{n-1}} + kf'(y) \equiv 0 \pmod{p}$ untersuchen. Mehrere Fälle können auftreten:

1. Es sei $f'(y) \not\equiv 0 \pmod{p}$. Dann hat $kf'(y) \equiv -\frac{f(y)}{p^{n-1}} \pmod{p}$ genau eine Lösung in k modulo p. Die Nullstelle y modulo p^{n-1} von $f(x) \equiv 0 \pmod{p^{n-1}}$ kann eindeutig zu einer Nullstelle $x_n = y + kp^{n-1}$ von $f(x) \equiv 0 \pmod{p^n}$ fortgesetzt werden.

2. Es sei $f'(y) \equiv 0 \pmod{p}$.

   (a) Es sei $f(y) \equiv 0 \pmod{p^n}$. Dann ist jedes k Lösung von $kf'(y) \equiv -\frac{f(y)}{p^{n-1}} \pmod{p}$. In diesem Fall ist jede Fortsetzung von y Nullstelle von $f(x)$ modulo p^n.

   (b) Es sei $f(y) \not\equiv 0 \pmod{p^n}$. Dann gibt es keine Fortsetzung von y.

In der von uns konstruierten Folge ist $x_0^2 \equiv a \pmod{p}$ und $f'(X) = 2X$. Da laut Voraussetzung $p \nmid a$ ist, gilt auch $p \nmid x_0$, somit liegt Fall 1 vor, nämlich $f'(x_0) \not\equiv 0 \pmod{p}$. Es gibt also eine eindeutige Fortsetzung zu $x_1 = x_0 + kp$. Da auch in weiterer Folge $x_n \equiv x_{n-1} \equiv \cdots \equiv x_0 \pmod{p}$ gilt, liegt bei jedem Schritt von x_n nach x_{n+1} Fall 1 vor, die Folge ist somit nicht endend und eindeutig.

Für den Fall $p = 2$ ist obige Folge wegen $p \mid f'(X) = 2X$ nicht geeignet. Um auch hier eindeutige Lösungen zu erhalten, eignet sich zum Beispiel eine kubische Gleichung wie $f(X) = X^3 - 3$.

Als Nächstes müssen wir zeigen, dass tatsächlich ein Cauchyfolge vorliegt. Das folgt aus Lemma 2, denn nach Konstruktion gilt

$$|x_{n+1} - x_n|_p = \left|kp^{n+1}\right|_p \leq p^{-(n+1)} \to 0,$$

für $n \to \infty$ und $k \in \mathbb{Z}$.

Weiters gilt

$$\left|x_n^2 - a\right|_p = \left|lp^{n+1}\right|_p \leq p^{-(n+1)} \to 0,$$

für $n \to \infty$ und $l \in \mathbb{Z}$, sodass der Grenzwert, wenn er existiert, ein Wurzel von a sein muss. Da wir aber a so gewählt haben, dass es kein Quadrat ist, gibt es keinen Grenzwert in $\mathbb{Q}$, die rationalen Zahlen sind also nicht vollständig bezüglich $|\ |_p$.

Wir müssen keine weiteren Absolutbeträge berücksichtigen, das folgt aus Satz 1, dem Satz von Ostrowski. □

Bemerkung 8: Die rationalen Zahlen sind bezüglich des trivialen Absolutbetrags $\tau_{\mathbb{Q}}$ vollständig, denn da nur die Werte 0 und 1 angenommen werden, ist eine Folge genau dann eine Cauchyfolge bezüglich $\tau_{\mathbb{Q}}$, wenn es ein $N \in \mathbb{N}$ gibt, sodass $\tau_{\mathbb{Q}}(x_m - x_n) = 0$ für alle n, $m \geq N$ und somit $x_m = x_n$ ist. Das heißt, die Folge ist ab einem bestimmten Index konstant und damit konvergent. Dieser Fall ist aber von keinem weiteren Interesse.

Beispiel 1: Wir betrachten die Kongruenzen $X^2 \equiv 2 \pmod{7^n}$, $n = 1, 2, 3, \ldots$, das heißt, es ist $f(X) = X^2 - 2$ sowie $f'(X) = 2X$.

Für $n = 1$ gibt es die zwei Lösungen $x_0 \equiv +3 \pmod 7$ und $x_0 \equiv -3 \equiv +4 \pmod 7$.

Nun sei $n = 2$.

1. Wir suchen die Fortsetzung von $+3$. Da $f(3) = 7$ und $f'(3) = 6$ gilt, ist $k \cdot 6 \equiv -1 \pmod 7$ zu lösen. Also ist $k = 1$ und $x_1 = 3 + 1 \cdot 7 = 10$.
2. Es sei nun $x_0 = +4$. Dann gilt $f(4) = 14$ und $f'(4) = 8$. Wir müssen $k \cdot 8 \equiv -1 \pmod 7$ lösen. Es ist dann $k = 5$ und $x_1 = 4 + 5 \cdot 7 = 39$.

Wir wollen noch den Fall $n = 3$ genauer betrachten.

1. Zunächst suchen wir die Fortsetzung von 10. Wegen $f(10) = 98$ und $f'(10) = 20$ müssen wir die Kongruenz $k \cdot 20 \equiv -2 \pmod 7$ lösen. Es ist $k = 2$ und somit $x_2 = 10 + 2 \cdot 49 = 108$.
2. Es ist die Fortsetzung von 39 zu berechnen. Es ist $f(39) = 1519$ und $f'(39) = 78$, und es gilt $k \cdot 78 \equiv -31 \pmod 7$ zu lösen. Als Ergebnis erhalten wir $k = 4$. Es ist in diesem Fall $x_2 = 39 + 4 \cdot 49 = 235$.

u.s.w.

Für jede Lösung x_0 von $X^2 \equiv 2 \pmod 7$ erhalten wir also eine eindeutig bestimmte Folge, die bezüglich des p-adischen Absolutbetrags eine Cauchyfolge bildet, jedoch in $\mathbb{Q}$ nicht konvergiert.

Quellen und Literatur zu Kapitel 2

Abschnitt 2.1 basiert auf [1], S. 13, 16-18, [2], S. 37, [9], S. 43-45, [13], S. 9-11, 21, [18], S. 83-85 sowie [19], S. 20, 21, Abschnitt 2.2 auf [2], S. 37, 38, [9], S. 46-49, [13], S. 43-46, [14], S. 3-5, [18], S. 85, 86 und Abschnitt 2.3 auf [9], S. 50-52.
Für den Beweis von Proposition 4 sowie für Beispiel 1 vergleiche *Kapitel VIII: Algebraische Kongruenzen* aus [11] S. 51-55.

3

Die Vervollständigung metrischer Räume

Im letzten Abschnitt von Kapitel 2 haben wir definiert, was es bedeutet, dass ein metrischer Raum vollständig ist. Wir haben gesehen, dass die rationalen Zahlen bezüglich keines auf ihnen definierten, nichttrivialen Absolutbetrags vollständig sind. Jedoch wissen wir, dass $\mathbb{Q}$ bezüglich des „gewöhnlichen“ Absolutbetrags vervollständigt werden kann und wir so zur „lückenlosen“ Zahlengeraden der reellen Zahlen $\mathbb{R}$ gelangen. Im Folgenden werden wir diese Frage allgemein behandeln und uns überlegen, unter welchen Umständen es eine Vervollständigung eines metrischen Raumes gibt.

Es seien $(X,\, d)$ und $(X^{'},\, d^{'})$ zwei metrische Räume, und es sei $x_0 \in X$. Eine Abbildung $f:\ X \to X^{'}$ heißt *stetig* in x_0, wenn es für jedes $\epsilon > 0$ ein $\delta > 0$ gibt, sodass für alle $x \in X$ mit $d\,(x,\, x_0) < \delta$ auch $d^{'}\,(f\,(x)\,,\ f(x_0)) < \epsilon$ gilt.

Die Abbildung heißt *gleichmäßig stetig*, wenn es zu jedem $\epsilon > 0$ ein $\delta > 0$ gibt, sodass für alle $x,\, y \in X$ mit $d\,(x,\, y) < \delta$ folgt, dass auch $d^{'}\,(f\,(x)\,,\ f(y)) < \epsilon$ ist.

Jede gleichmäßig stetige Funktion ist stetig. Ist $(x_n)_{n\geq 1}$ eine Cauchyfolge in X und f gleichmäßig stetig, so ist $(f\,(x_n))_{n\geq 1}$ eine Cauchyfolge in $X^{'}$.

Proposition 1: Es sei X ein vollständiger metrischer Raum und $A \subseteq X$. Dann sind folgende Aussagen äquivalent:

1. A ist ein vollständiger Teilraum von X.
2. A ist abgeschlossen.

Beweis. (1) $\Longrightarrow$ (2) Es sei $x \in \bar{A}$. Dann gibt es eine Folge von Elementen in A, die gegen x konvergiert. Da A vollständig ist, liegt auch der Grenzwert dieser Folge in A, es ist also $x \in A$.

(1) $\Longleftarrow$ (2) Jede Cauchyfolge $(a_n)_{n\geq 1}$ in A ist auch eine Cauchyfolge in X, wo sie wegen der Vollständigkeit von X jedenfalls auch konvergiert. Dieser Grenzwert muss im Abschluss von A liegen, und da $\bar{A} = A$ gilt, liegt er sogar in A. □

Proposition 2: Es sei $(X,\, d)$ ein metrischer Raum und $A \subseteq X$ eine dichte Teilmenge. Weiters sei $(X^{'},\, d^{'})$ ein vollständiger metrischer Raum und $f:\ A \to X^{'}$ eine gleichmäßig stetige Abbildung. Dann gibt es genau eine stetige Abbildung $\bar{f}:\ X \to X^{'}$, die auf A mit f übereinstimmt. Diese ist wieder gleichmäßig stetig.

Beweis. Es sei $x \in X$. Dann gibt es eine Folge $(a_n)_{n\geq 1}$ in A mit $x = \lim_{n\to\infty} a_n$. Somit ist $(a_n)_{n\geq 1}$ eine Cauchyfolge in X und $(f(a_n))_{n\geq 1}$ eine Cauchyfolge in $X^{'}$, die wegen der Vollständigkeit von $X^{'}$ auch konvergiert. Ist $(b_n)_{n\geq 1}$ nun eine andere Folge in A mit $x = \lim_{n\to\infty} b_n$, dann ist $\lim_{n\to\infty} d(a_n,\, b_n) = 0$ und somit auch $\lim_{n\to\infty} d^{'}(f(a_n),\, f(b_n)) = 0$. Das bedeutet, dass $\lim_{n\to\infty} f(a_n) = \lim_{n\to\infty} f(b_n)$ sein muss. Somit ist durch $\bar{f}(x) := \lim_{n\to\infty} f(a_n)$ eindeutig eine Funktion definiert, die auf A mit f übereinstimmt, wobei wir für $x \in A$ berücksichtigen, dass natürlich $x = \lim_{n\to\infty} x$ ist.

Es sei nun $\epsilon > 0$. Dann gibt es ein $\delta > 0$, sodass aus $(a,\, b) \in A \times A$ mit $d(a,\, b) < \delta$ wegen der gleichmäßigen Stetigkeit von f folgt, dass $d^{'}(f(a),\, f(b)) < \epsilon$ ist. Nun sei $d(x,\, y) < \delta$ für $x,\, y \in X$. Dann gibt es in A Folgen $(a_n)_{n\geq 1}$ und $(b_n)_{n\geq 1}$ mit $x = \lim_{n\to\infty} a_n$ beziehungsweise $y = \lim_{n\to\infty} b_n$. Wegen $\lim_{n\to\infty} d(a_n,\, b_n) = d(x,\, y) < \delta$ ist für hinreichend große n jedenfalls $d(a_n,\, b_n) < \delta$ und somit $d^{'}(f(a_n),\, f(b_n)) < \epsilon$. Betrachten wir den Grenzwert, so folgt, dass $d^{'}\left(\bar{f}(x),\, \bar{f}(y)\right) \leq \epsilon$ gilt. Das heißt, $\bar{f}$ ist gleichmäßig stetig.

Nun nehmen wir an, dass $\bar{f}_1$ und $\bar{f}_2$ zwei Fortsetzungen von f mit den gegebenen Voraussetzungen sind. Die Menge $\left\{x \in X:\ \bar{f}_1(x) = \bar{f}_2(x)\right\}$ ist abgeschlossen und enthält auf jeden Fall A. Da A eine dichte Teilmenge ist, bedeutet das, dass die eben betrachtete Menge mit X übereinstimmt. Somit gilt $\bar{f}_1 = \bar{f}_2$. □

Bemerkung 1: Das Prinzip der Fortsetzbarkeit der Identitäten, das wir in diesem Abschnitt öfters verwenden, besagt Folgendes: Ist eine Formel auf einer dichten Teilmenge einer Menge X erfüllt und setzt sich diese Formel aus stetigen Funktionen zusammen, so lässt sie sich auf ganz X fortsetzen.

Analog dazu besagt das Prinzip der Fortsetzbarkeit von Ungleichungen, dass, falls $f(x) \leq g(x)$ auf einer dichten Teilmenge erfüllt ist, die Ungleichung überall gilt, wenn f und g stetige Funktionen sind.

Definition 1: Es seien $(X,\, d)$ und $(X^{'},\, d^{'})$ zwei metrische Räume und $f:\ X \to X^{'}$ eine surjektive Abbildung, sodass

$$d(x,\, y) = d^{'}(f(x),\, f(y))$$

für alle $x, y \in X$ gilt. Dann heißt f *eine Isometrie*, und die Räume X und $X^{'}$ heißen *isometrisch*.

Isometrien sind immer injektiv und gleichmäßig stetig.

Definition 2: Es sei $(X,\, d)$ ein metrischer Raum und $\left(\hat{X},\, \hat{d}\right)$ ein vollständiger metrischer Raum. Gibt es eine Abbildung $j:\ X \to \hat{X}$, sodass $j(X)$ dicht in $\hat{X}$ liegt und weiters für $x,\, y \in X$

$$d(x,\, y) = \hat{d}(j(x),\, j(y))$$

gilt, dann heißt $\left(\hat{X},\, \hat{d},\, j\right)$ *eine Vervollständigung von* $(X,\, d)$.

Ist X eine Menge, so bezeichnet $l^\infty(X)$ den Raum der beschränkten, reellwertigen Funktionen auf X. Dieser ist vollständig, wenn auf ihm die Metrik

$$d(f,\, g) := \sup_{x\in X} |f(x) - g(x)|$$

definiert wird. Denn ist $(f_n)_{n\geq 1}$ eine Cauchyfolge, so gibt es für jedes $\epsilon > 0$ ein $N \in \mathbb{N}$, sodass $|f_n(x) - f_m(x)| \leq d(f_n,\, f_m) < \epsilon$ für alle $m,\, n \geq N(\epsilon)$ und alle $x \in X$ ist. Daher ist $(f_n(x))_{n\geq 1}$ für alle $x \in X$ eine Cauchyfolge in $\mathbb{R}$ und somit konvergent. Es sei $f : X \to \mathbb{R}$, $f(x) = \lim_{n\to\infty} f_n(x)$. Dann ist $|f(x) - f_n(x)| \leq \epsilon$ für $n \geq N(\epsilon)$ und alle $x \in X$. Setzen wir $\epsilon = 1$, so erhalten wir $|f(x)| \leq \left|f_{N(1)}(x)\right| + 1$. Es ist f also beschränkt, das heißt $f \in l^\infty(X)$. Aus $d(f,\, f_n) \leq \epsilon$ für $n \geq N(\epsilon)$ ergibt sich die Konvergenz von $(f_n)_{n\geq 1}$ gegen f.

Satz 1: Es sei $(X,\, d)$ ein metrischer Raum. Dann gibt es eine Vervollständigung von X. Sind $\left(\hat{X}_1,\, \hat{d}_1,\, j_1\right)$ und $\left(\hat{X}_2,\, \hat{d}_2,\, j_2\right)$ zwei solche, so gibt es genau eine Isometrie $j : \hat{X}_1 \to \hat{X}_2$ mit $j \circ j_1 = j_2$.

Beweis. Wir zeigen zunächst die zweite Behauptung. Da j_1 injektiv ist, gibt es eine Abbildung $j : j_1(X) \to \hat{X}_2$ mit $j \circ j_1 = j_2$. Für $(x,\, y) \in X \times X$ ist

$$\hat{d}_2(j(j_1(x)),\, j(j_1(y))) = \hat{d}_2(j_2(x),\, j_2(y)) = d(x,\, y) = \hat{d}_1(j_1(x),\, j_1(y)).$$

Es ist j gleichmäßig stetig und lässt sich somit nach Proposition 2 auf $\hat{X}_1$ zu einer eindeutig bestimmten, gleichmäßig stetigen Funktion $\bar{j}$ fortsetzen. Diese wollen wir wieder mit „j“ bezeichnen.

Die Gleichung $\hat{d}_2(j(a),\, j(b)) = \hat{d}_1(a,\, b)$ gilt auf einer in $\hat{X}_1 \times \hat{X}_1$ abgeschlossenen Menge, denn beide Seiten sind stetige Funktionen in $(a,\, b)$. Da diese Identität auf der dichten Menge $j_1(X) \times j_1(X)$ erfüllt ist, gilt sie wegen des Prinzips der Fortsetzbarkeit auf ganz $\hat{X}_1 \times \hat{X}_1$.

Es ist $j\left(\hat{X}_1\right)$ ein vollständiger Teilraum von $\hat{X}_2$ und somit abgeschlossen. Da er $j_2(X)$ enthält, ist $j\left(\hat{X}_1\right) = \hat{X}_2$, das heißt, j ist surjektiv.

Wir betrachten zum Nachweis der Existenz ein beliebiges $a \in X$ und setzen

$$j : X \to \mathbb{R}^X, \quad j(x)(y) = d(x,\, y) - d(a,\, y).$$

Für $x,\, y \in X$ ist $|j(x)(y)| \leq d(x,\, a)$. Das bedeutet, dass $j(x) \in l^\infty(X)$ ist. Wir bezeichnen mit $\hat{d}$ die Metrik auf $l^\infty(X)$ und setzen $\hat{X} := \overline{j(X)}$. Dann ist einerseits

$$\hat{d}(j(x),\, j(y)) = \sup_{z\in X} |j(x)(z) - j(y)(z)| = \sup_{z\in X} |d(x,\, z) - d(y,\, z)| \leq d(x,\, y)$$

und andererseits

$$\hat{d}(j(x),\, j(y)) \geq |d(x,\, y) - d(y,\, y)| = d(x,\, y).$$

Da $l^\infty(X)$ vollständig und $\hat{X}$ abgeschlossen ist, ist auch $\hat{X}$ vollständig. □

Ist $\left(\hat{X},\, \hat{d},\, j\right)$ eine Vervollständigung von X, so ist j injektiv. Es kann also auf kanonische Weise eine Vervollständigung von X gefunden werden, die X mengentheoretisch als Teilraum enthält. Wir nennen sie *die* Vervollständigung von X. In diesem Fall ist $j : X \to \hat{X}$ die Einbettung.

Satz 2: Es sei K ein Körper, $|\,|$ ein Absolutbetrag auf K. $\hat{K}$ sei die Vervollständigung von K. Dann gilt:

1. Die Abbildungen $+$ und $\cdot$ von $K \times K$ nach $\hat{K}$ lassen sich eindeutig zu stetigen Abbildungen auf $\hat{K} \times \hat{K}$ fortsetzen.
2. $\hat{K}$ ist dann ein topologischer Körper.
3. $|\,| : K \to \mathbb{R}_+$ lässt sich eindeutig zu einer stetigen Abbildung $|\,|^\wedge : \hat{K} \to \mathbb{R}_+$ fortsetzen.
4. $|\,|^\wedge$ ist ein Absolutbetrag auf $\hat{K}$, der die Topologie auf $\hat{K}$ induziert.

Beweis.

1. Die Aussage folgt für $+$ mit Hilfe von Proposition 2, weil $+$ auf $K \times K$ gleichmäßig stetig ist.
   Um die Aussage für $\cdot$ zu zeigen, verwenden wir ein Resultat aus der allgemeinen Topologie: Eine Abbildung $f : A \times B \to G$ heißt $\mathbb{Z}-$bilinear, wenn für alle $x,\, x^{'} \in A$ und $y,\, y^{'} \in B$ folgende Bedingungen erfüllt sind:
   $$f\big(x + x^{'},\, y\big) = f\,(x,\, y) + f\big(x^{'},\, y\big),$$
   $$f\big(x,\, y + y^{'}\big) = f\,(x,\, y) + f\big(x,\, y^{'}\big).$$
   Es seien G_1, G_2 und G_3 metrisierbare, abelsche, topologische Gruppen, G_3 darüber hinaus auch vollständig, $A \subseteq G_1$, $B \subseteq G_2$ dichte Untergruppen und f eine stetige, $\mathbb{Z}-$bilineare Abbildung von $A \times B$ nach G_3. Dann gibt es genau eine stetige Fortsetzung $\bar{f} : G_1 \times G_2 \to G_3$ von f (siehe zum Beispiel [4], S. 277).
   Die von uns betrachtete Abbildung $\cdot$ ist $\mathbb{Z}-$bilinear, denn es ist ja $\big(x + x^{'}\big)y = xy + x^{'}y$ beziehungsweise $x\big(y + y^{'}\big) = xy + xy^{'}$. Daraus können wir nun schließen, dass die Abbildung $\cdot$ auf $\hat{K} \times \hat{K}$ eindeutig zu einer stetigen Abbildung fortsetzbar ist.
2. Dass in $\hat{K}$ alle Rechenregeln für einen Ring gelten, folgt aus dem Prinzip der Fortsetzbarkeit von Identitäten. Betrachten wir zum Beispiel das Distributivgesetz, so ist $x \cdot (y + z) = x \cdot y + x \cdot z$ jedenfalls auf der dichten Teilmenge $K \times K \times K$ von $\hat{K} \times \hat{K} \times \hat{K}$ erfüllt. Da, wie wir eben gezeigt haben, $+$ und $\cdot$ stetig sind, gilt die Formel überall.
   Die Abbildung $x \mapsto -x$ ist auf $\hat{K}$ stetig, da sie wegen $|-x - (-y)| = |x - y|$ gleichmäßig stetig ist.
   Es bleibt noch zu zeigen, dass $\iota : K^\times \to \hat{K}$, $\iota\,(x) = x^{-1}$ auf $\hat{K} \setminus \{0\}$ stetig fortsetzbar ist. Dazu verwenden wir ein Resultat, das besagt, dass für einen metrischen Raum $(X,\, d)$, einen vollständigen metrischen Raum $(X^{'},\, d^{'})$, eine dichte Teilmenge $A \subseteq X$ und eine stetige Abbildung $f : A \to X^{'}$ folgende Aussagen äquivalent sind:
   (a) Es gibt eine stetige Fortsetzung $\bar{f} : X \to X^{'}$ von f.
   (b) Für jede in X konvergente Folge $(a_n)_{n \geq 1}$ mit $a_n \in A$ ist $(f\,(a_n))_{n \geq 1}$ eine Cauchyfolge, die wegen der Vollständigkeit von $X^{'}$ konvergiert.

   Es sei also $(x_n)_{n \geq 1}$ eine Cauchyfolge in $\hat{K}$, $\lim_{n \to \infty} x_n \in \hat{K} \setminus \{0\}$. Es gibt somit ein $c > 0$, sodass $|x_n| > c$ für alle $n \geq 1$ ist. Es folgt $\left|x_n^{-1} - x_m^{-1}\right| = \left|\frac{x_m - x_n}{x_m x_n}\right| \leq \frac{1}{c^2}\,|x_m - x_n|$, und ι lässt sich daher auf $\hat{K}^\times$ zu einer stetigen Abbildung $\hat{\iota}$ fortsetzen.

3. Es gilt $||x| - |y|| \leq |x - y|$. Daraus folgt, dass $|\,|$ gleichmäßig stetig ist.

4. Die Metrik auf $\hat{K}$ bezeichnen wir mit $\hat{d}$. Für $x,\, y \in K$ gilt

$$\hat{d}\,(x,\, y) = d\,(x,\, y) = |x - y| = |x - y|^{\wedge}\,.$$

Beide Seiten sind stetig. Daher gilt die Gleichung für alle $x,\, y \in \hat{K}$. Ist $|x|^{\wedge} = 0$, $x \in \hat{K}$, dann ist $\hat{d}\,(x,\, 0) = 0$, also $x = 0$. Wegen des Prinzips der Fortsetzbarkeit von Identitäten beziehungsweise Ungleichungen gelten $|xy|^{\wedge} = |x|^{\wedge}\,|y|^{\wedge}$ beziehungsweise $|x + y|^{\wedge} \leq |x|^{\wedge} + |y|^{\wedge}$. Wegen $\hat{d}\,(x,\, y) = |x - y|^{\wedge}$ erhalten wir, dass beide Topologien übereinstimmen. □

Wir nennen ab jetzt $\left(\hat{K},\, |\,|^{\wedge}\right)$ *die* Vervollständigung von $(K,\, |\,|)$.

Ist K ein Körper und $|\,|$ ein Absolutbetrag auf K, dann schreiben wir für die Wertemenge $\{r \in \mathbb{R} :\ r = |x| \text{ für } x \in K\}$ kurz $|K|$.

Korollar 1: Es sei $\left(\hat{K},\, |\,|^{\wedge}\right)$ die Vervollständigung von $(K,\, |\,|)$. Die folgenden Aussagen sind äquivalent:

1. $|\,|$ ist nichtarchimedisch.
2. $|\,|^{\wedge}$ ist nichtarchimedisch.

Es ist dann $\left|\hat{K}\right|^{\wedge} = |K|$.

Beweis. (1) $\Longrightarrow$ (2) Aus der Fortsetzbarkeit von Ungleichungen folgt $|x + y|^{\wedge} \leq \max\left\{|x|^{\wedge},\ |y|^{\wedge}\right\}$, da die Maximumsfunktion stetig ist. (1) $\Longleftarrow$ (2) Diese Implikation gilt klarerweise.

Es sei nun $x \in \hat{K}$, $x \neq 0$. Da K in $\hat{K}$ dicht ist, gibt es ein $y \in K$ mit $|x - y|^{\wedge} < |x|^{\wedge}$. Dann ist

$$|y| = |y|^{\wedge} = |(y - x) + x|^{\wedge} = \max\left\{|y - x|^{\wedge},\ |x|^{\wedge}\right\} = |x|^{\wedge}\,.$$

Es folgt also $|x|^{\wedge} \in |K|$. □

Quellen und Literatur zu Kapitel 3

Dieses Kapitel basiert auf §3 *Metrische Räume* des Kapitels *Grundlagen* aus [20] sowie auf §4 *Die Sätze von Gelfand-Mazur und Ostrowski* des Kapitels *Absolutbeträge* aus [21].

4

Der Körper der *p*-adischen Zahlen $\mathbb{Q}_p$

Jeder metrische Raum besitzt eine Vervollständigung bezüglich der betrachteten Metrik – das haben wir in Kapitel 3 gesehen, und ab jetzt werden wir uns mit jenem Körper beschäftigen, der die Vervollständigung der rationalen Zahlen bezüglich des p-adischen Absolutbetrags darstellt.

4.1 *P*-adische und ganze *p*-adische Zahlen

Definition 1: Es sei p eine Primzahl und $|\,|_p$ der p-adische Absolutbetrag auf $\mathbb{Q}$. Die Vervollständigung von $\mathbb{Q}$ bezüglich $|\,|_p$ heißt *der Körper der p-adischen Zahlen* und wird mit $\mathbb{Q}_p$ bezeichnet.

Aus dem vorangegangenen Kapitel folgt sofort:

Die rationalen Zahlen $\mathbb{Q}$ liegen dicht in $\mathbb{Q}_p$. Der p-adische Absolutbetrag $|\,|_p$ auf $\mathbb{Q}$ lässt sich eindeutig auf $\mathbb{Q}_p$ fortsetzen. Diese Fortsetzung ist nach Korollar 1 im vorigen Kapitel ebenfalls nichtarchimedisch, und wir bezeichnen sie wieder mit $|\,|_p$. Die Wertemenge von $|\,|_p$ auf $\mathbb{Q}_p$ stimmt mit jener auf $\mathbb{Q}$ überein, es gilt somit

$$|\mathbb{Q}_p|_p = |\mathbb{Q}|_p = \{p^n : \ n \in \mathbb{Z}\} \cup \{0\}\,.$$

Das bedeutet also, dass es für jede p-adische Zahl x, $x \neq 0$ ein $n \in \mathbb{Z}$ gibt mit $|x|_p = p^{-n}$.

Da $\mathbb{Q}_p$ ein Körper mit nichtarchimedischem Absolutbetrag ist, können wir den Bewertungsring aus Kapitel 1.3 betrachten:

Definition 2: Als *ganze p-adische Zahlen* bezeichnen wir die Elemente des Rings

$$\mathbb{Z}_p := \left\{x \in \mathbb{Q}_p : \ |x|_p \leq 1\right\}.$$

Da für jede ganze Zahl a gilt, dass $|a|_p \leq 1$ ist, liegt a als p-adische Zahl in $\mathbb{Z}_p$.

Der folgende Satz ermöglicht es uns, eine konkretere Vorstellung von den ganzen p-adischen Zahlen zu entwickeln:

Satz 1: Ist $x \in \mathbb{Z}_p$, so gibt es genau eine Folge $(a_i)_{i\geq 0}$ ganzer Zahlen, sodass für alle $i \geq 0$ sowohl $0 \leq a_i < p^{i+1}$ als auch $a_i \equiv a_{i+1} \pmod{p^{i+1}}$ erfüllt ist. Die betrachtete Folge konvergiert dann bezüglich des p-adischen Absolutbetrags $|\ |_p$ gegen x. Insbesondere liegt $\mathbb{Z}$ dicht in $\mathbb{Z}_p$.

Beweis. Da $\mathbb{Q}$ dicht in $\mathbb{Q}_p$ ist, gibt es eine Folge $\left(\frac{a_n}{b_n}\right)_{n\geq 0}$ rationaler Zahlen mit $\operatorname{ggT}(a_n, b_n) = 1$ für alle n, sodass bezüglich des p-adischen Absolutbetrags $x = \lim_{n\to\infty} \frac{a_n}{b_n}$ ist.

Für hinreichend große n ist p kein Teiler von b_n. Denn wäre dies der Fall, so würde wegen $\operatorname{ggT}(a_n, b_n) = 1$ der Zähler a_n nicht von p geteilt werden, und wir hätten $\frac{|a_n|_p}{|b_n|_p} = \frac{1}{|b_n|_p} \geq p > 1$. Da dies der Annahme widerspräche, dass die Folge gegen $|x|_p \leq 1$ konvergiert, ist das nicht möglich.

Wir können also ein $u_n \in \mathbb{Z}$ finden mit $b_n u_n \equiv 1 \pmod{p^n}$. Da $|b_n|_p = 1$ und $|a_n|_p \leq 1$ ist, folgt:

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

für $n \to \infty$ gilt also $|x - a_n u_n|_p \to 0$.

Das bedeutet, dass $\mathbb{Z}$ dicht in $\mathbb{Z}_p$ liegt. Es gibt also ein $a_0' \in \mathbb{Z}$ mit $\left|x - a_0'\right|_p \leq p^{-1}$, und wir wählen $a_0 \in \{1, \ldots, p-1\}$ so, dass $a_0 \equiv a_0' \pmod{p}$ gilt. Dann ist

$$|x - a_0|_p \leq \max\left\{\left|x - a_0'\right|_p, \ \left|a_0' - a_0\right|_p\right\} \leq p^{-1}.$$

Wir behaupten nun, dass es Elemente $a_0, \ldots, a_t \in \mathbb{Z}$ gibt mit $0 \leq a_i < p^{i+1}$, $|x - a_i|_p \leq p^{-i-1}$ für $0 \leq i \leq t$ sowie $a_i \equiv a_{i+1} \pmod{p^{i+1}}$ für $0 \leq i < t$ und wollen dies durch Induktion zeigen.

Für $t = 0$ gilt die Behauptung, wie wir soeben gesehen haben.

Es seien $a_0, \ldots, a_t$ schon auf diese Weise konstruiert. Dann ist $\frac{x-a_t}{p^{t+1}} \in \mathbb{Z}_p$. Somit gibt es ein $g \in \mathbb{Z}$, $0 \leq g < p$ mit $\left|\frac{x-a_t}{p^{t+1}} - g\right|_p \leq p^{-1}$. Wir setzen $a_{t+1} = a_t + g p^{t+1}$, und es gilt dann $a_{t+1} \equiv a_t \pmod{p^{t+1}}$ sowie $0 \leq a_{t+1} < p^{t+1} + (p-1)\, p^{t+1} = p^{t+2}$. Weiters folgt

$$\begin{aligned} |x - a_{t+1}|_p = \left|x - a_t - g p^{t+1}\right|_p &= \left|p^{t+1}\right|_p \left|\frac{x - a_t}{p^{t+1}} - g\right|_p \\ &\leq p^{-t-1} p^{-1} = p^{-t-2}. \end{aligned}$$

Somit ist $|x - a_i|_p \leq p^{-i-1}$ für alle i, und die Folge $(a_i)_{i\geq 0}$ konvergiert bezüglich des p-adischen Absolutbetrags $|\ |_p$.

Die Folge $(a_i)_{i\geq 0}$ ist eindeutig bestimmt, denn angenommen, das wäre nicht der Fall, so gäbe es eine weitere Folge $\left(a_i'\right)_{i\geq 0}$ mit den gesuchten Eigenschaften und einem kleinsten Index i_0 mit $a_{i_0} \neq a_{i_0}'$. Nun gilt jedoch

$$a_{i_0} \equiv a_{i_0 - 1} = a_{i_0 - 1}' \equiv a_{i_0}' \pmod{p^{i_0+1}}$$

mit $0 \leq a_{i_0},\ a_{i_0}' < p^{i_0+1}$. Somit ist $a_{i_0} = a_{i_0}'$ und die Folge eindeutig bestimmt. □

Bemerkung 1: Wir wissen aus Satz 1, dass $\mathbb{Z}$ dicht in $\mathbb{Z}_p$ liegt. Außerdem ist $\mathbb{Z}_p$ als abgeschlossene Menge im vollständigen Körper $\mathbb{Q}_p$ ebenfalls vollständig.

Da sich der p-adische Absolutbetrag $|\ |_p$ eindeutig von $\mathbb{Q}$ auf $\mathbb{Q}_p$ fortsetzen lässt, gilt natürlich auch für alle ganzen Zahlen x und y, dass $|x-y|_p$ in $\mathbb{Z}$ den gleichen Wert annimmt wie $|x-y|_p$ in $\mathbb{Z}_p$. Wir können also nach Definition 2 in Kapitel 3 die ganzen p-adischen Zahlen $\mathbb{Z}_p$ als die Vervollständigung der ganzen Zahlen $\mathbb{Z}$ bezüglich des p-adischen Absolutbetrags $|\ |_p$ ansehen.

4.2 Die p-adische Entwicklung

Betrachten wir nun noch einmal die Folge $(a_i)_{i\geq 0}$ ganzer Zahlen aus Satz 1, die gegen die ganze p-adische Zahl x konvergiert. Aus der Bedingung $0 \leq a_i < p^{i+1}$ ergibt sich, dass wir ihre Glieder folgendermaßen „zur Basis p“ darstellen können:

$$a_0 = x_0, \quad a_1 = x_0 + x_1 p, \quad \ldots, \quad a_i = x_0 + x_1 p + \cdots + x_i p^i,$$

wobei alle Ziffern x_i in der Menge $\{0,\ 1,\ \ldots,\ p-1\}$ liegen. Wegen der Bedingung $a_i \equiv a_{i+1} \pmod{p^{i+1}}$ in Satz 1 gilt für das nächste Folgeglied a_{i+1}, dass seine Ziffern x_0 bis x_i mit denen von a_i übereinstimmen:

$$a_{i+1} = x_0 + x_1 p + \cdots + x_i p^i + x_{i+1} p^{i+1}.$$

Diesen Überlegungen folgend zeigt es sich, dass die betrachtete ganze p-adische Zahl x als Summe der unendlichen Reihe $\sum_{n=0}^{\infty} x_n p^n$ aufgefasst werden kann:

Korollar 1: Jedes $x \in \mathbb{Z}_p$ kann eindeutig in der Form

$$x = \sum_{i=0}^{\infty} x_i p^i$$

mit $0 \leq x_i < p-1$ dargestellt werden.

Beweis. Wir müssen zeigen, dass die Reihe $\sum_{i=0}^{\infty} x_i p^i$ gegen x konvergiert. Die n-te Partialsumme ist von der Form $x_0 + x_1 p + x_2 p^2 + \cdots + x_n p^n$. Das bedeutet, dass die Partialsummen genau den Folgegliedern a_n aus Satz 1 entsprechen, von denen wir bereits wissen, dass sie die geforderte Eigenschaft besitzen.

Die Darstellung ist eindeutig, denn die Eindeutigkeit der Folgeglieder a_i impliziert auch jene der Ziffern x_i. □

Wir können dieses Resultat auf alle p-adischen Zahlen verallgemeinern:

Erfüllt $x \in \mathbb{Q}_p$ nicht $|x|_p \leq 1$, dann ist $|x|_p = p^m$ für eine positive ganze Zahl m. Multiplizieren wir nun x mit dieser Potenz von p, dann erfüllt die so erhaltene p-adische Zahl $x' = x \cdot p^m$ die Bedingung $|x'|_p = 1$ und kann als unendliche Reihe dargestellt werden. Also ist

$$x = \frac{1}{p^m} \sum_{i=0}^{\infty} x_i' p^i = \frac{x_0'}{p^m} + \frac{x_1'}{p^{m-1}} + \cdots + \frac{x_{m-1}'}{p} + x_m' + x_{m+1}' p + x_{m+2}' p^2 + \cdots .$$

Zusammenfassend gilt:

Korollar 2: Jedes $x \in \mathbb{Q}_p$ kann in der Form

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

geschrieben werden, wobei $x_{-m} \neq 0$ ist und alle x_i in der Menge $\{0,\ 1,\ \ldots,\ p-1\}$ liegen. Diese Darstellung ist eindeutig und heißt *die p-adische Entwicklung von x* oder *die kanonische Darstellung von x*.

Die folgende Proposition zeigt, wie der p-adische Absolutbetrag eines Elementes von $\mathbb{Q}_p$ mit dessen kanonischer Darstellung zusammenhängt:

Proposition 1: Ist $x = \sum_{i=0}^{\infty} x_i p^i$ mit $x_i = 0$ für $0 \leq i < k$ und $x_k \neq 0$, dann ist $|x|_p = p^{-k}$, und ist $x = \sum_{i=-m}^{\infty} x_i p^i$ mit $x_{-m} \neq 0$, dann ist $|x|_p = p^m$.

Beweis. Wir wissen, dass die Partialsummen a_n der Reihe $\sum_{i=0}^{\infty} x_i p^i$ gegen x konvergieren. Im ersten Fall ist

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

Somit ist $|x|_p = p^{-k}$ für alle $n \geq k$.

Der zweite Fall kann auf analoge Weise gezeigt werden. □

Bemerkung 2: Diese Proposition zeigt, dass wir den in Abschnitt 1.1.1 auf $\mathbb{Q}$ definierten Begriff der p-adischen Ordnung ord_p problemlos auf ganz $\mathbb{Q}_p$ erweitern können.

Wir haben die p-adische Ordnung eines Elementes als den Exponenten der größten Potenz von p definiert, die dieses Element teilt. In der kanonischen Darstellung einer p-adischen Zahl x entspricht das genau dem Index der ersten Ziffer, die ungleich Null ist.

In Proposition 1 ist im ersten Fall $\mathrm{ord}_p(x) = k$, im zweiten Fall ist $\mathrm{ord}_p(x) = -m$.

Bemerkung 3: Es wird also jede p-adische Zahl durch eine unendliche Reihe repräsentiert, oder genauer, durch eine „Äquivalenzklasse“ unendlicher Reihen, die alle dieselbe kanonische Darstellung besitzen.

Umgekehrt stellt jede unendliche Reihe der Form $\sum_{i=-m}^{\infty} x_i p^i$ mit $x_i \in \mathbb{Z}$ für alle i eine p-adische Zahl dar, denn dass eine derartige Reihe bezüglich des p-adischen Absolutbetrags konvergiert, ist klar, und da die p-adischen Zahlen vollständig sind, liegt der Grenzwert in $\mathbb{Q}_p$.

Außerdem sei darauf hingewiesen, dass die kanonische Darstellung einer p-adischen Zahl in jedem Fall eindeutig ist – im Gegensatz zur g-adischen Entwicklung reeller Zahlen, wo dies für $x = \sum_{n=n_0}^{\infty} z_n g^{-n}$ nur durch die Bedingung, dass unendlich viele $z_n \neq g-1$ sind, erreicht wird. Ansonsten gilt ja für $g = 10$ zum Beispiel $1{,}000\ldots = 0{,}999\ldots$.

Diese Eindeutigkeit der p-adischen Entwicklung ergibt unmittelbar, dass $\mathbb{Z}_p$ gleichmächtig ist mit $\{0,\ \ldots,\ p-1\}^{\mathbb{Z}_+}$ – was nichts anderes bedeutet, als dass die p-adischen Zahlen von der Mächtigkeit des Kontinuums sind.

Proposition 2: Die Einheitengruppe $\mathbb{Z}_p^\times$ der ganzen p-adischen Zahlen besteht genau aus jenen Elementen, deren p-adische Entwicklung nicht mit Null beginnt. Das heißt

$$\mathbb{Z}_p^\times = \Big\{x \in \mathbb{Z}_p : \ |x|_p = 1\Big\} = \Big\{x = \sum_{i=0}^{\infty} x_i p^i : \ x_0 \neq 0\Big\}.$$

Beweis. Der Beweis folgt sofort aus Proposition 1. □

Aus Proposition 2 und unseren bisherigen Überlegungen lässt sich unmittelbar folgendes Resultat über die Darstellbarkeit p-adischer Zahlen ableiten:

Proposition 3: Jede p-adische Zahl x mit Absolutbetrag $|x|_p = p^{-n}$ mit $n \in \mathbb{Z}$ kann als Produkt

$$x = \epsilon \cdot p^n$$

dargestellt werden, wobei ϵ eine p-adische Einheit ist.

4.3 Algebraische und topologische Eigenschaften

In Kapitel 1 haben wir bereits einige Eigenschaften und Besonderheiten von ultrametrischen Räumen beziehungsweise von Körpern, die mit einem nichtarchimedischen Absolutbetrag ausgestattet sind, kennengelernt. Die dort besprochenen Resultate sollen nun im Kontext der p-adischen Zahlen betrachtet werden.

Wir haben die ganzen p-adischen Zahlen $\mathbb{Z}_p$ als die abgeschlossene Einheitskugel in $\mathbb{Q}_p$ definiert, sie entsprechen also dem Bewertungsring von $|\ |_p$. Das ist ein lokaler Ring, dessen maximales Ideal sich folgendermaßen ergibt:

$$\begin{aligned}\mathbb{Z}_p \backslash \mathbb{Z}_p^\times &= \Big\{x \in \mathbb{Z}_p : \ |x|_p < 1\Big\} = \Big\{x = \sum_{i=0}^{\infty} x_i p^i : \ x_0 = 0\Big\} \\ &= \Big\{x = p\sum_{i=0}^{\infty} x_{i+1} p^i\Big\} = p\mathbb{Z}_p.\end{aligned}$$

Die Abbildung

$$x = \sum_{i=0}^{\infty} x_i p^i \mapsto x_0$$

definiert einen Epimorphismus von $\mathbb{Z}_p$ nach $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Dieser heißt *Reduktion modulo* p und hat den Kern

$$\Big\{x = \sum_{i=0}^{\infty} x_i p^i \in \mathbb{Z}_p : \ x_0 = 0\Big\} = p\mathbb{Z}_p.$$

Nun folgt aus dem Homomorphiesatz für Ringe, dass $\mathbb{Z}_p/p\mathbb{Z}_p$ zu $\mathbb{F}_p$ isomorph ist, und das gilt somit auch für den auf Seite 19 in Abschnitt 1.3 definierten Restklassenkörper κ von $|\ |_p$, denn es ist

$$\kappa = \mathbb{Z}_p/p\mathbb{Z}_p.$$

Für den Bewertungsring $\mathbb{Z}_{(p)}$ und das Bewertungsideal $p\mathbb{Z}_{(p)}$ von $|\,|_p$ auf $\mathbb{Q}$, die wir ebenfalls in Abschnitt 1.3 betrachtet haben, ergeben sich folgende Zusammenhänge:

$$\mathbb{Z}_p \cap \mathbb{Q} = \left\{ \frac{a}{b} \in \mathbb{Q} : \; p \nmid b \right\} = \mathbb{Z}_{(p)},$$
$$p\mathbb{Z}_p \cap \mathbb{Q} = \left\{ \frac{a}{b} \in \mathbb{Q} : \; p \nmid b \text{ und } p \mid a \right\} = p\mathbb{Z}_{(p)},$$
$$\mathbb{Z}_p^\times \cap \mathbb{Q} = \mathbb{Z}_p \backslash p\mathbb{Z}_p \cap \mathbb{Q} = \left\{ \frac{a}{b} \in \mathbb{Q} : \; p \nmid ab \right\} = \mathbb{Z}_{(p)} \backslash p\mathbb{Z}_{(p)}.$$

Ein Integritätsbereich R, also ein nullteilerfreier Ring, heißt ein Hauptidealbereich, wenn jedes Ideal $I \subseteq R$ von einem Element von R erzeugt werden kann. Ein solches Ideal heißt dann Hauptideal. Es gilt:

Proposition 4: Der Ring $\mathbb{Z}_p$ ist ein Hauptidealbereich mit den Hauptidealen $\{0\}$ und $p^k\mathbb{Z}_p$ für alle ganzen Zahlen $k \geq 0$.

Beweis. Der Ring $\mathbb{Z}_p$ ist klarerweise ein Integritätsbereich, denn er ist ja in einem Körper – nämlich in $\mathbb{Q}_p$ – enthalten.

Es sei $I \neq \{0\}$ ein Ideal in $\mathbb{Z}_p$, und es sei $x \neq 0$ ein Element im Ideal I von maximalem Betrag. Da der p-adische Absolutbetrag eine diskrete Wertemenge besitzt, kann ein solches Element immer gefunden werden. Es sei k die p-adische Ordnung von x. Also ist $x = \epsilon p^k$, wobei ϵ eine p-adische Einheit und somit invertierbar ist. Dann ist $p^k = \epsilon^{-1}x \in I$, und es gilt $\left(p^k\right) = p^k\mathbb{Z}_p \subseteq I$.

Umgekehrt gilt für jedes $y \in I$, dass $|y|_p = p^{-l} \leq p^{-k}$ ist. Dann ist $y = p^l\epsilon' = p^k p^{l-k}\epsilon' \in p^k\mathbb{Z}_p$ und somit $I \subseteq p^k\mathbb{Z}_p$. Insgesamt ergibt sich $I = p^k\mathbb{Z}_p$. □

Da die ganzen p-adischen Zahlen ein Integritätsbereich sind, können wir $\mathbb{Q}_p$ auch als den Quotientenkörper von $\mathbb{Z}_p$ ansehen. Dieser kann folgendermaßen dargestellt werden:

$$\mathbb{Q}_p = \mathbb{Z}_p\left[p^{-1}\right].$$

Schreiben wir eine ganze p-adische Zahl x, $x \neq 0$ als Produkt von einer p-adischen Einheit ϵ und einer Potenz von p, ist also $x = \epsilon p^n$, so ergibt sich das multiplikativ inverse Element von x durch $x^{-1} = \epsilon^{-1}p^{-n}$. Das zeigt, dass der Quotientenkörper tatsächlich von $\mathbb{Z}_p$ und den Potenzen von p mit negativen Exponenten erzeugt wird.

Wir sehen also, dass $x^{-1} \in p^{-n}\mathbb{Z}_p$ ist, und es sei noch einmal darauf hingewiesen, dass jede p-adische Zahl y als Produkt $p^m y'$ für $m \in \mathbb{Z}$ und $y' \in \mathbb{Z}_p$ dargestellt werden kann. Es soll nun ein topologischer Aspekt dieser Überlegung hervorgehoben werden:

Proposition 5: Die Kugeln $p^n\mathbb{Z}_p$ mit $n \in \mathbb{Z}$ bilden im Körper der p-adischen Zahlen eine Umgebungsbasis von 0, die ganz $\mathbb{Q}_p$ überdeckt.

Beweis. Als Einheitskugel um 0 ist $\mathbb{Z}_p$ in $\mathbb{Q}_p$ sowohl offen als auch abgeschlossen und kann somit also offene Umgebung von 0 betrachtet werden. Da die Abbildung $x \mapsto px$ als einfache Multiplikation im Körper $\mathbb{Q}_p$ klarerweise ein Homöomorphismus ist, ist auch für jedes n die Menge $p^n\mathbb{Z}_p$ eine offene Umgebung von 0. Dass

$$\mathbb{Q}_p = \bigcup_{n\in\mathbb{Z}} p^n\mathbb{Z}_p$$

gilt, folgt aus der Darstellbarkeit jeder p-adischen Zahl als ein derartiges Produkt.

Die Mengen $p^n\mathbb{Z}_p$ bilden auch eine Umgebungsbasis von 0, denn für jede offene Menge, die 0 enthält, können wir ein $n_0 \in \mathbb{Z}$ finden, sodass eine Kugel mit Radius p^{-n_0} ganz in ihr enthalten ist. □

Bemerkung 4: Auch hier sehen wir, dass die Metrik und die Topologie eines Körpers, der mit einem nichtarchimedischen Absolutbetrag ausgestattet ist, stark in Zusammenhang mit dessen algebraischer Struktur stehen. So können wir die p-adische Ordnung ord_p von $x \in \mathbb{Q}_p$ auch als die größte ganze Zahl n_0 sehen, für die $x \in p^{n_0}\mathbb{Z}_p$ gilt.

Es sei zum Beispiel

$$x = x_{-3}p^{-3} + x_{-2}p^{-2} + x_{-1}p^{-1} + x_0 + \cdots$$

mit $x_{-3} \neq 0$, dann ist x in $p^{-3}\mathbb{Z}_p$ enthalten aber nicht in $p^{-2}\mathbb{Z}_p$, denn bei der Darstellung

$$x = p^{-2}\left(x_{-3}p^{-1} + x_{-2} + x_{-1}p + x_0p^{-2} + \cdots\right) = p^{-2}x'$$

ist x' keine ganze p-adische Zahl. Somit ist $\mathrm{ord}_p(x) = -3$, was natürlich mit unserer früheren Definition übereinstimmt.

Ein Zusammenhang, den es hervorzuheben gilt, ist folgender: Für $x,\ y \in \mathbb{Q}_p$ ist

$$|x - y|_p \leq p^{-n} \qquad \Longleftrightarrow \qquad x - y \in p^n\mathbb{Z}_p.$$

Gilt dies, so sagen wir auch, dass die p-adischen Zahlen x und y kongruent modulo p^n sind und schreiben dafür

$$x \equiv y \pmod{p^n}.$$

Proposition 6: Die p-adischen Zahlen $\mathbb{Q}_p$ sind als topologischer Raum ein total unzusammenhängender Hausdorffraum.

Beweis. Dass $\mathbb{Q}_p$ ein total unzusammenhängender topologischer Raum ist, folgt aus Abschnitt 1.2.2. Da jeder metrische Raum ein Hausdorffraum ist, also ein Raum in dem je zwei verschiedene Punkte disjunkte Umgebungen besitzen, gilt das auch für $\mathbb{Q}_p$. □

Wir wollen uns nun einer weiteren topologischen Eigenschaft, nämlich jener der Kompaktheit, widmen. Dazu wiederholen wir einige in diesem Zusammenhang wichtige Begriffe:

Ein Hausdorffraum X heißt *kompakt*, wenn jede beliebige offene Überdeckung $\{O_i\}_{i\in I}$ von X eine endliche Teilüberdeckung $\{O_{i_1}, O_{i_2}, \ldots, O_{i_N}\}$ besitzt.

Eine Teilmenge M eines Hausdorffraums X heißt kompakt, wenn zu jeder offenen Überdeckung $\{O_i\}_{i\in I}$ von M eine endliche Teilüberdeckung $\{O_{i_1}, O_{i_2}, \ldots, O_{i_N}\}$ existiert. Versehen mit der Spurtopologie ist M dann ein kompakter Raum.

Ein Hausdorffraum, in dem jeder Punkt eine Umgebungsbasis aus kompakten Umgebungen besitzt, heißt *ein lokalkompakter Raum.*

Ist X ein metrischer Raum, so ist eine Teilmenge von X genau dann kompakt, wenn sie vollständig und total beschränkt ist. Eine Teilmenge M eines metrischen Raumes X heißt total beschränkt oder präkompakt, wenn es zu jedem $\epsilon > 0$ eine endliche Überdeckung von M durch offene Kugeln gibt, deren Durchmesser kleiner als ϵ ist.

Satz 2: $\mathbb{Z}_p$ ist kompakt, $\mathbb{Q}_p$ ist lokalkompakt.

Beweis. Wir wollen zunächst zeigen, dass $\mathbb{Z}_p$ als Teilmenge von $\mathbb{Q}_p$ vollständig und total beschränkt ist. Die Vollständigkeit folgt unmittelbar aus der Tatsache, dass $\mathbb{Z}_p$ eine abgeschlossene Menge im vollständigen Körper der p-adischen Zahlen ist.

Da der p-adische Absolutbetrag $|\ |_p$ nur diskrete Werte annimmt, genügt es, eine Überdeckung von $\mathbb{Z}_p$ durch endlich viele Kugeln mit Radius p^{-m}, $m \in \mathbb{N}$ zu finden. Es sei also $\epsilon > 0$ beliebig. Wir wählen dann eine ganze Zahl n so, dass $p^{-n} < \epsilon$ ist.

Die Abbildung

$$f:\ x = \sum_{i=0}^{\infty} x_i p^i \mapsto x_0 + x_1 p + \cdots + x_{n-1} p^{n-1} + p^n \mathbb{Z}$$

definiert einen Homomorphismus von $\mathbb{Z}_p$ nach $\mathbb{Z}/p^n\mathbb{Z}$. Denn es ist ja $f(x) = a_{n-1} \pmod{p^n}$, wobei a_{n-1} das entsprechende Glied der in Satz 1 auf Seite 40 eindeutig bestimmten Folge darstellt. Daher gilt für $x,\ y \in \mathbb{Z}_p$

$$\begin{aligned} f(x) + f(y) &= a_{n-1} \pmod{p^n} + b_{n-1} \pmod{p^n} \\ &= a_{n-1} + b_{n-1} \pmod{p^n} \\ &= f(x+y). \end{aligned}$$

Die Abbildung f hat den Kern

$$\left\{ x = \sum_{i=0}^{\infty} x_i p^i \in \mathbb{Z}_p :\ x_i = 0 \text{ für } 0 \le i < n \right\} = \left\{ x = p^n \sum_{i=0}^{\infty} x_{i+n} p^i \right\} = p^n \mathbb{Z}_p.$$

Aus dem Homomorphiesatz für Gruppen folgt

$$\mathbb{Z}_p / p^n \mathbb{Z}_p \ \cong\ \mathbb{Z}/p^n\mathbb{Z}.$$

Das bedeutet also, dass es p^n Restklassen der Form $a + p^n\mathbb{Z}_p$ mit $a \in \{0,\ 1,\ \ldots,\ p^n - 1\}$ gibt. Weiters gilt

$$a + p^n \mathbb{Z}_p = \left\{ x \in \mathbb{Z}_p :\ |a - x|_p \le p^n \right\} = \overline{B}_{p^{-n}}(a).$$

Wir haben also eine vollständige Überdeckung von $\mathbb{Z}_p$ mit p^n Kugeln gefunden und den ersten Teil des Satzes somit gezeigt.

Um zu beweisen, dass $\mathbb{Q}_p$ lokalkompakt ist, müssen wir zeigen, dass jede p-adische Zahl eine kompakte Umgebung besitzt. Da wir nun wissen, dass 0 eine kompakte Umgebung – nämlich $\mathbb{Z}_p$ – hat, können wir für ein beliebiges $x \in \mathbb{Q}_p$ die gesuchte Umgebung durch

$$x + \mathbb{Z}_p = \left\{ y \in \mathbb{Q}_p :\ |x - y|_p \le 1 \right\} = \{ y \in \mathbb{Q}_p :\ x - y \in \mathbb{Z}_p \}$$

definieren. Diese Menge ist als stetige Verschiebung der kompakten Menge $\mathbb{Z}_p$ wiederum kompakt. □

4.4 Rechnen in $\mathbb{Q}_p$

Die kanonische Darstellung p-adischer Zahlen ermöglicht es uns, konkrete arithmetische Operationen in $\mathbb{Q}_p$ auszuführen. Im Prinzip funktioniert das Rechnen mit p-adischen Zahlen genauso, wie wir es vom Dezimalsystem her kennen.

Es seien $x = \sum_{i=-m}^{\infty} x_i p^i$, $y = \sum_{i=-k}^{\infty} y_i p^i$ zwei p-adische Zahlen, wobei o.B.d.A. $m \geq k$ sei. Dann errechnet sich ihre Summe beziehungsweise ihre Differenz folgendermaßen:

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

wobei wir, falls $m > k$ ist, für $i \in \{-m, \ldots, -k-1\}$ klarerweise $y_i = 0$ setzen.

Da die Rechenoperationen komponentenweise ausgeführt werden, müssen wir, damit die Ziffern des Ergebnisses wiederum in der Menge $\{0, 1, \ldots, p-1\}$ liegen, Überträge berücksichtigen.

Falls also bei der Addition eine Komponente $z_i > p-1$ ist, setzten wir diese gleich $x_i + y_i - p$, und für die nächste Komponente z_{i+1} ergibt sich $z_{i+1} = x_{i+1} + y_{i+1} + 1$. Für die Subtraktion gilt entsprechendes, das heißt, für $z_i < 0$ setzen wir $z_i = x_i - y_i + p$, und es ist $z_{i+1} = x_{i+1} - y_{i+1} - 1$.

Bei der Multiplikation erhalten wir das Produkt zweier p-adischer Zahlen x, y durch

$$z = x \cdot y = \sum_{i=-m-k}^{\infty} z_i p^i,$$

wobei sich die Koeffizienten z_i mit Hilfe des Cauchy-Produkts für unendliche Reihen und unter Berücksichtigung eventuell auftretender Überträge u_i folgendermaßen ergeben:

$$\begin{aligned}
&z_{-m-k} \equiv x_{-m} y_{-k} \pmod{p},\\
&u_0 = (x_{-m} y_{-k} - z_{-m-k})\,/p,\\
&z_{-m-k+1} \equiv u_0 + x_{-m} y_{-k+1} + x_{-m+1} y_{-k} \pmod{p},\\
&u_1 = (u_0 + x_{-m} y_{-k+1} + x_{-m+1} y_{-k} - z_{-m-k+1})\,/p,\\
&\vdots\\
&z_{-m-k+n} \equiv u_{n-1} + \sum_{i=0}^{n} x_{-m+i} y_{-k+n-i} \pmod{p}.
\end{aligned}$$

Für ganze p-adische Zahlen ist $m = k = 0$, dadurch werden die Formeln übersichtlicher.

Bei der Division z/x mit $x \neq 0$ suchen wir diejenige p-adische Zahl y, die multipliziert mit x wieder z ergibt. Der Divisionsalgorithmus beruht nun darauf, dass $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist und wir somit in jedem Fall ein $y_{-k} \in \{0, 1, \ldots, p-1\}$ finden können, sodass $x_{-m} y_{-k} \equiv z_{-m-k} \pmod{p}$ erfüllt ist. Auf diese Weise können wir unter der Berücksichtigung von Überträgen jede Komponente finden.

Das Ganze soll nun an einigen Beispielen verdeutlicht werden. Um das Rechnen (von Hand) zu erleichtern, empfiehlt es sich, die p-adischen Zahlen folgendermaßen anzuschreiben:

$$x = \ldots x_k x_{k-1} \ldots x_1 x_0, x_{-1} \ldots x_{-m}, \qquad y = \ldots y_k y_{k-1} \ldots y_1 y_0, y_{-1} \ldots y_{-k}.$$

So ist es auch möglich, wie gewohnt von „rechts“ nach „links“ zu rechnen.

Beispiel 1: Folgende Rechenoperationen werden in $\mathbb{Q}_7$ ausgeführt:

$\ldots 210635{,}23 / \ldots 246622{,}56$	$\ldots 210635{,}23$	$\ldots 2106\,3\,5{,}23 \times \ldots 246622{,}56$
$-\ldots 3564242\,3 \quad = \ldots 16604$	$+\ldots 246622{,}56$	$\ldots 5654\,1\,4\,0\,4$
$\ldots 5212110\,0$	$\ldots 460561{,}12$	$\ldots 5444\,5\,5\,1$
$-\ldots 0000000$		$\ldots 1603\,4\,6$
$\ldots 521211\,0$	$\ldots 210635{,}23$	$\ldots 6034\,6$
$-\ldots 630301$	$-\ldots 246622{,}56$	$\ldots 1404$
$\ldots 560610$	$\ldots 631012{,}34$	$\ldots 404$
$-\ldots 30301$		$\ldots 25$
$\ldots 25460$	$\ldots 246622{,}56$	$\ldots 6$
$-\ldots 2256$	$-\ldots 210635{,}23$	$\ldots$
$\ldots 0260$	$\ldots 035654{,}33$	$\ldots 5650{,}41\,1\,4$

Beispiel 2: Es sei nun $1 = 1{+}0p{+}0p^2{+}\cdots{+}0p^n{+}\cdots$ die kanonische Darstellung von 1 in $\mathbb{Q}_p$. Wir wollen uns überlegen, wie $x = -1 = \sum_{i=0}^{\infty} x_i p^i$ in $\mathbb{Q}_p$ aussieht. Da $1 + x$ gleich dem Nullelement sein soll und die Addition komponentenweise erfolgt, kommt für $x_0 \in \{0,\, 1,\, \ldots,\, p-1\}$ nur $x_0 = p{-}1$ in Frage. Somit müssen wir beim Berechnen der nächsten Komponente einen Übertrag berücksichtigen. Das heißt, es ist auch $x_1 = p - 1$ und es entsteht wiederum ein Übertrag. Auf diese Weise fortfahrend erhalten wir insgesamt:

$$x = -1 = (p-1) + (p-1)\,p + (p-1)\,p^2 + \cdots + (p-1)\,p^n + \cdots = (p-1)\sum_{i=0}^{\infty} p^i.$$

Mit derselben Argumentation folgt analog, dass für eine beliebige p-adische Zahl x, $x = \sum_{i=-m}^{\infty} x_i p^i$ das additiv inverse Element $-x$ folgende Gestalt haben muss:

$$\begin{aligned} -x &= (p - x_{-m})\,p^{-m} + (p - 1 - x_{-m+1})\,p^{-m+1} + \cdots + (p - 1 - x_0) + (p - 1 - x_2)\,p^2 + \cdots = \\ &= 1 \cdot p^{-m} + \sum_{i=-m}^{\infty} (p - 1 - x_i)\,p^i. \end{aligned}$$

Beispiel 3: Betrachten wir Beispiel 1, so wird diese Formel bestätigt, denn für $x = \ldots 210635{,}23$, $y = \ldots 246622{,}56$ und $z = x - y = \ldots 631012{,}34$ ist in $\mathbb{Q}_7$

$$\begin{aligned} -z &= y - x \\ &= \ldots 035654{,}33 \\ &= \ldots (6-6)\,(6-3)\,(6-1)\,(6-0)\,(6-1)\,(6-2)\,,(6-3)\,(7-4)\,. \end{aligned}$$

Bemerkung 5: Es ist also $-1 = (p-1)\sum_{i=0}^{\infty} p^i$, und das heißt, wir können das Einselement darstellen als $1 = (1-p)\sum_{i=0}^{\infty} p^i$. Weiters sehen wir, dass die unendliche Reihe $1 + p + p^2 + \cdots + p^n + \cdots$ konvergiert. Ihre Summe ist

$$\sum_{i=0}^{\infty} p^i = \frac{1}{1-p}.$$

Bemerkung 6: Unter den diversen Computeralgebrasystemen eignet sich PARI/GP besonders gut, um mit p-adischen Zahlen zu rechen und um symbolisch Gleichungen im Körper der p-adischen Zahlen zu verarbeiten.

PARI/GP wurde 1985 von einem Team um den französischen Mathematiker Henri Cohen entwickelt, die Betreuung und Weiterentwicklung des Projekts, das unter http://pari.math.u-bordeaux.fr erreichbar ist, erfolgt heute an der Université Bordeaux I in Frankreich.

Bei PARI/GP handelt es sich um freie Software, die der GNU General Public License unterliegt.

Dieses Computeralgebrasystem ist vor allem für schnelle zahlentheoretische Berechnung konzipiert, wie zum Beispiel die Faktorisierung ganzer Zahlen in ihre Primfaktoren, enthält aber darüber hinaus eine Menge von Funktionen, die viele Möglichkeiten im Bereich elliptischer Kurven, algebraischer Zahlkörper, Polynome, Matrizen, etc. bieten.

Unter http://pari.math.u-bordeaux.fr/dochtml/html.stable findet sich eine in Kategorien eingeteilte Auflistung der in PARI/GP verfügbaren Funktionen.

Ein weiterer großer Vorteil von PARI/GP ist die Tatsache, dass einige „ausgefallene“ Datentypen direkt eingegeben werden können, wie zum Beispiel p-adische Zahlen.

Eine p-adische Zahl x wird dabei durch $x + O(p^k)$ definiert, wobei k die Genauigkeit darstellt, also die höchste Potenz, die bei der Berechnung berücksichtigt wird, und p ist natürlich die entsprechende Primzahl.

Im folgenden Beispiel ist $p = 17$. Zeilen, die eine Eingabe darstellen, beginnen mit „?“, die Ergebnisse sind nummeriert und beginnen mit „%“.

```
? 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
%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)
? -1+O(17^20)
%3 = 16 + 16*17 + 16*17^2 + 16*17^3 + 16*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)
? -x*-1
%4 = 15*17^-3 + 9*17^-1 + 5 + 6*17 + 12*17^2 + 3*17^3 + 17^4 + O(17^20)
```

Im weiteren Verlauf werden wir immer wieder PARI/GP zur Unterstützung bei Berechnungen oder zur Veranschaulichung einsetzen.

Die Beispiele haben gezeigt, dass einige p-adische Zahlen eine endliche oder abbrechende p-adische Entwicklung besitzen, also dass ab einem Index $N \in \mathbb{N}$ für alle $i > N$ die Ziffer $x_i = 0$ ist. Bei anderen wiederum, wie zum Beispiel bei -1, lässt sich kein solcher Index finden. Wovon das abhängt, zeigt folgende Proposition:

Proposition 7: Es hat $x \in \mathbb{Q}_p$ genau dann eine endliche p-adische Entwicklung, wenn x als rationale Zahl nicht negativ ist und diese als Nenner eine Potenz von p besitzt.

Beweis. ($\Longrightarrow$) Es sei

$$\begin{aligned} x &= \sum_{i=-m}^{N} x_i p^i = x_{-m}p^{-m} + \cdots + x_{-1}p^{-1} + x_0 + x_1 x + \cdots + x_N p^N \\ &= p^{-m}\left(x_{-m} + x_{-m+1}p + \cdots + x_{-1}p^{m-1} + x_0 p^m + \cdots + x_N p^{N-m}\right). \end{aligned}$$

Der Zähler entspricht somit einer positiven ganzen Zahl, geschrieben zur Basis p, der Nenner ist eine Potenz von p.

($\Longleftarrow$) Es sei umgekehrt $x = p^{-k}y$. Da x nach Voraussetzung eine positive rationale Zahl ist, liegt y in $\mathbb{N}$. Stellen wir nun y zur Basis p dar, dann erhalten wir eine endliche Summe der Form $y = \sum_{i=0}^{N} y_i p^i$. Somit besitzt auch x eine endlich p-adische Entwicklung. □

Auch folgendes Resultat beschäftigt sich mit der p-adischen Entwicklung rationaler Zahlen. Wie bei der Dezimalbruchentwicklung reeller Zahlen können wir auch bei der p-adischen Entwicklung die Teilmenge der rationalen Zahlen an der schließlich auftretenden Periodität erkennen.

Proposition 8: Die p-adische Entwicklung $\sum_{i=-m}^{\infty} x_i p^i$ stellt genau dann eine rationale Zahl x dar, wenn sie schließlich periodisch wird, das heißt, es gibt dann einen Index N und ein $k \in \mathbb{N}$, sodass $x_{n+k} = x_n$ für alle $n \geq N$ gilt.

Beweis. ($\Longleftarrow$) Wir nehmen zunächst an, die kanonische Darstellung einer p-adischen Zahl $x = \sum_{i=-m}^{\infty} x_i p^i$ ist ab dem Index N periodisch.

Subtrahieren wir den vorperiodischen Teil $\sum_{i=-m}^{N-1} x_i p^i$ von x und dividieren das Ergebnis durch p^N, so erhalten wir eine ganze p-adische Zahl y in folgender Form

$$y = y_0 + y_1 p + \cdots + y_{k-1}p^{k-1} + y_0 p^k + y_1 p^{k+1} + \cdots + y_0 p^{2k} + \cdots .$$

Wir setzen $z = y_0 + y_1 p + \cdots + y_{k-1}p^{k-1}$, dann ist

$$y = z\left(1 + p^k + p^{2k} + \cdots\right) = z\frac{1}{1-p^k}.$$

Das heißt, y ist eine rationale Zahl und somit auch x. Denn wir erhalten ja x aus y durch Multiplikation mit p^N und anschließender Addition des vorperiodischen Teils $\sum_{i=-m}^{N-1} x_i p^i$, welcher nach Proposition 7 eine positive rationale Zahl darstellt.

($\Longrightarrow$) Es sei umgekehrt $x = \frac{a}{b} \in \mathbb{Q}$. Der Bruch $\frac{a}{b}$ soll in gekürzter Form vorliegen, und wir nehmen an, dass x als p-adische Zahl in $\mathbb{Z}_p$ liegt. Dann sind b und p relativ prim, und es gibt ganze Zahlen c_n, d_n mit

$$1 = c_n b + d_n p^{n+1}.$$

Es folgt

$$a = ac_n b + ad_n p^{n+1}.$$

Wir wählen nun ein $k \in \mathbb{Z}$ so, dass $ac_n - kp^{n+1}$ in $\{0, \ldots, p^{n+1} - 1\}$ liegt. Dann ist

$$\begin{aligned} a &= \underbrace{\left(ac_n - kp^{n+1}\right)}_{=:A_n} b + \underbrace{\left(ad_n + kb\right)}_{=:r_n} p^{n+1} \\ &= A_n b + r_n p^{n+1}. \end{aligned}$$

Dividieren wir beide Seiten durch b, erhalten wir

$$\frac{a}{b} = A_n + p^{n+1}\frac{r_n}{b}.$$

Umformen ergibt

$$r_n = \frac{a - A_n b}{p^{n+1}},$$

und daraus folgt

$$\frac{a - \left(p^{n+1} - 1\right) b}{p^{n+1}} \leq r_n \leq \frac{a}{p^{n+1}}.$$

Für $n \to \infty$ ist

$$-b \leq r_n \leq 0,$$

das bedeutet, dass r_n nur endlich viele Werte annimmt.

Es gilt

$$\frac{a}{b} = A_n + p^{n+1}\frac{r_n}{b} = A_{n+1} + p^{n+2}\frac{r_{n+1}}{b}.$$

Nun ist

$$A_{n+1} - A_n = p^{n+1}\left(\frac{r_n - p r_{n+1}}{b}\right)$$

eine ganze Zahl, und da b und p^{n+1} relativ prim sind, liegt sogar $\frac{r_n - p r_{n+1}}{b}$ in $\mathbb{Z}$. Somit ist $A_{n+1} \equiv A_n \pmod{p^{n+1}}$. Die Zahlen A_n erfüllen genau die Bedingungen aus Satz 1 und stellen somit die Partialsummen der p-adischen Entwicklung von $\frac{a}{b} = \sum_{i=0}^{\infty} x_i p^i$ dar.

Daher ist $A_{n+1} = A_n + x_{n+1}p^{n+1}$, und es folgt

$$A_n + p^{n+1}\frac{r_n}{b} = A_n + x_{n+1}p^{n+1} + p^{n+2}\frac{r_{n+1}}{b}$$

und durch Umformen

$$r_n = x_{n+1}b + p r_{n+1}.$$

Das gilt für alle n, und da r_n nur endlich viele Werte annimmt, gibt es einen Index N und eine positive ganze Zahl P, sodass $r_N = r_{N+P}$ ist. Dann gilt auch

$$x_{N+1}b + p r_{N+1} = x_{N+1+P}b + p r_{N+1+P},$$

was gleichbedeutend ist mit

$$\left(x_{N+1} - x_{N+1+P}\right) b = p\left(r_{N+1+P} - r_{N+1}\right).$$

Da p und b relativ prim sind, wird $(x_{N+1} - x_{N+1+P})$ von p geteilt. Nun liegen aber sowohl x_{N+1} als auch x_{N+1+P} in der Menge $\{0,\, 1,\, \ldots,\, p-1\}$, und daher gilt $x_{N+1} = x_{N+1+P}$. Dann ist aber auch $r_{N+1} = r_{N+1+P}$.

So erhalten wir insgesamt für alle $m > N$

$$x_m = x_{m+P} \text{ und } r_m = r_{m+P}.$$

Ist x keine ganze p-adische Zahl, so kann x als Produkt von einer Potenz von p und von einer ganzen p-adischen Zahl x' dargestellt werden. Wird x' schließlich periodisch, so gilt dies auch für x. □

Beispiel 4: Es sei $p = 7$ und $x = \frac{3}{12005}$. Dann ist $\left|\frac{3}{12005}\right|_7 = \left|7^{-4} \cdot \frac{3}{5}\right|_7 = 7^4$, x ist also keine ganze 7-adische Zahl, $x^{'} = x \cdot 7^4 = \frac{3}{5}$ hingegen schon. Vergleichen wir nun die mit PARI/GP berechneten kanonischen Darstellungen von x und x', so sehen wir, dass sie die gleichen Ziffern und die gleiche Periode besitzen, das Ganze lediglich um eine bestimmte Potenz von p „verschoben“.

```
? 3/12005*7^4+O(7^20)
%1 = 2 + 4*7 + 5*7^2 + 2*7^3 + 7^4 + 4*7^5 + 5*7^6 + 2*7^7 + 7^8 + 4*7^9 + 5*7^10 + 2*7^11 +
7^12 + 4*7^13 + 5*7^14 + 2*7^15 + 7^16 + 4*7^17 + 5*7^18 + 2*7^19 + O(7^20)
? 3/12005+O(7^20)
%2 = 2*7^-4 + 4*7^-3 + 5*7^-2 + 2*7^-1 + 1 + 4*7 + 5*7^2 + 2*7^3 + 7^4 + 4*7^5 + 5*7^6 + 2*7^7
+ 7^8 + 4*7^9 + 5*7^10 + 2*7^11 + 7^12 + 4*7^13 + 5*7^14 + 2*7^15 + 7^16 + 4*7^17 + 5*7^18 +
2*7^19 + O(7^20)
```

4.5 Henselsches Lemma

Als Nächstes wollen wir uns mit Wurzeln von p-adischen Zahlen beschäftigen. Wir nennen $x \in \mathbb{Q}_p$ *eine n-te Wurzel von* $a \in \mathbb{Q}_p$, wenn x eine Lösung des Polynoms $X^n - a = 0$ ist.

Es sei zum Beispiel $a = 11$ in $\mathbb{Q}_7$, dann bezeichnen wir eine p-adische Zahl x, die der Gleichung

$$\left(x_0 + x_1 \cdot 7 + x_2 \cdot 7^2 + \cdots\right)^2 = 4 + 1 \cdot 7$$

genügt, als Quadratwurzel von a.

Hier muss also x folgendermaßen beschaffen sein: Zunächst muss $x_0^2 \equiv 4 \pmod 7$ gelten. Wir sehen sofort, dass $x_0 = 2$ die Eigenschaft besitzt, aber auch $x_0 = 5$ liefert das Gewünschte. Für den nächsten Koeffizienten x_1 folgt aus unseren Überlegungen zur Multiplikation, dass $1 \equiv u + 2x_0x_1 \pmod 7$ gelten muss, wobei u den eventuell auftretenden Übertrag bezeichnet.

Für $x_0 = 2$ ist auch $x_1 = 2$, im Fall $x_0 = 5$ ist $x_1 = 4$, da der Übertrag gleich 3 ist. Die Berechnung ist noch nicht zu Ende, denn in beiden Fällen bleibt ein neuerlicher Übertrag. Die nächste Ziffer x_2 muss der Bedingung $0 = u + 2x_0x_2 + x_1^2 \pmod 7$ genügen. Wenn auch hier wieder ein Übertrag entsteht, fahren wir auf diese Weise fort. Insgesamt erhalten wir die beiden Wurzeln $x = 2 + 2 \cdot 7 + 4 \cdot 7^2 + 4 \cdot 7^3 + 3 \cdot 7^4 + 3 \cdot 7^5 + \cdots$ und $x^{'} = -x = 5 + 4 \cdot 7 + 2 \cdot 7^2 + 2 \cdot 7^3 + 3 \cdot 7^4 + 3 \cdot 7^5 + \cdots$.

Suchen wir hingegen die Quadratwurzeln von $a = 7$ in $\mathbb{Q}_{11}$, so stellt sich heraus, dass wir kein x_0 finden können mit $x_0^2 \equiv 7 \pmod{11}$, denn 7 ist kein quadratischer Rest modulo 11.

In $\mathbb{Q}_7$ besitzt das Polynom $X^3 - a = 0$ für $a = 6$ drei verschiedene Nullstellen, denn es ist $x_0^3 \equiv 6 \pmod 7$ für $x_0 \in \{3, 5, 6\}$. Diese sind $3+3\cdot7+2\cdot7^2+2\cdot7^3+4\cdot7^4+\cdots$, $5+5\cdot7+2\cdot7^2+2\cdot7^3+7^4\cdots$ sowie $6 + 4 \cdot 7 + 7^2 + 2 \cdot 7^3 + 7^4 + \cdots$, und wir nennen sie die Kubikwurzeln von 6 in $\mathbb{Q}_7$.

Für $a \in \{2,\ 3,\ 4,\ 5,\ 7,\ 9,\ \ldots\}$ besitzt dieses Polynom in $\mathbb{Q}_7$ hingegen keine Nullstellen.

Bevor wir uns einer Methode widmen, mit der es leicht möglich ist, über die Existenz von Nullstellen eine Aussage zu treffen, bietet es sich an dieser Stelle an, eine Gemeinsamkeit von $\mathbb{Q}_p$ und $\mathbb{R}$ hervorzuheben. Dazu benötigen wir folgende Definition:

Definition 3: Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nichtkonstante Polynom mit Koeffizienten in K eine Nullstelle besitzt.

Die reellen Zahlen sind nicht algebraisch abgeschlossen, denn das Polynom $X^2+1=0$ hat keine Lösung in $\mathbb{R}$. Auch für $\mathbb{Q}_p$ gilt:

Proposition 9: Der Körper der p-adischen Zahlen ist nicht algebraisch abgeschlossen.

Beweis. Betrachten wir das Polynom X^2-a über $\mathbb{Q}_p$, dann besitzt es keine Nullstellen, wenn wir im Falle $p>2$ für a einen quadratischen Nichtrest in $\mathbb{Z}$ modulo p wählen und im Falle $p=2$ zum Beispiel $a=5$ setzen. □

Nun zu folgendem wichtigen Resultat, mit dem es sich in den meisten Fällen rasch entscheiden lässt, ob ein Polynom über $\mathbb{Z}_p$ eine Nullstelle besitzt oder nicht:

Satz 3 (Henselsches Lemma – 1. Version): Es sei $F(X)=c_0+c_1X+\cdots+c_nX^n$ ein Polynom mit Koeffizienten in $\mathbb{Z}_p$ und $F^{'}(X)=c_1+2c_2X+\cdots+nc_nX^{n-1}$ die (formale) Ableitung von $F(X)$. Gibt es ein $a_0\in\mathbb{Z}_p$ mit

$$F(a_0)\equiv 0 \pmod{p}$$

und

$$F^{'}(a_0)\not\equiv 0 \pmod{p},$$

dann existiert ein eindeutig bestimmtes $a\in\mathbb{Z}_p$, sodass $F(a)=0$ und $a\equiv a_0 \pmod{p}$ erfüllt sind.

Beweis. Wir haben das Henselsche Lemma bereits in Proposition 4 in Kapitel 2 vorweggenommen. Die im dortigen Beweis vorgestellte Theorie des Lösens algebraischer Kongruenz lässt sich hier in gleicher Weise auf das Polynom $X^n-a=0$ anwenden.

Die erste Kongruenz $F(X)\equiv 0 \pmod{p}$ ist lösbar, das ist hier für a_0 vorausgesetzt. Wegen $F^{'}(a_0)\not\equiv 0 \pmod{p}$, was ja ebenfalls Voraussetzung des Satzes ist, ist klar, dass wir eine eindeutig bestimmte Folge $(a_n)_{n\geq 0}$ finden können, die gegen $a\in\mathbb{Z}_p$ konvergiert. Wie sich diese Folge berechnet ist ebenballs in Proposition 4 auf Seite 29 beschrieben. □

Bemerkung 7: Das Henselsche Lemma wird oft mit dem Newtonschen Näherungsverfahren zur Bestimmung einer Nullstelle einer stetig differenzierbaren, reellen Funktion verglichen. Im Gegensatz zu diesem liegt im p-adischen Fall unter den angeführten Voraussetzungen immer Konvergenz vor.

Betrachten wir nun nochmals das eingangs erwähnte Problem, die Quadratwurzeln von 11 in $\mathbb{Q}_7$ zu finden, so ist dies gleichbedeutend damit, die Nullstellen von $F(X)=X^2-11$ in $\mathbb{Q}_7$ zu eruieren. Mit Hilfe des Henselschen Lemmas sehen wir sofort, dass sowohl für $a_0=2$ als auch für $a_0=5$ einerseits $F(a_0)\equiv 4 \pmod{7}$ und andererseits $F^{'}(a_0)=2a_0\not\equiv 0 \pmod{7}$ erfüllt ist.

Allerdings können wir Satz 3 nicht verwenden, um zum Beispiel die Quadratwurzeln von $F(X)=X^2-17$ in $\mathbb{Q}_2$ oder die Kubikwurzel von $F(X)=X^3-82$ in $\mathbb{Q}_3$ zu finden, denn in diesen Fällen ist für die jeweilige Primzahl p die Bedingung $F^{'}(a_0)\not\equiv 0 \pmod{p}$ für kein $a_0\in\mathbb{Z}_p$ erfüllt.

Um Polynome dieser Art zu untersuchen, benötigen wir eine stärkere Version des Henselschen Lemmas:

Satz 4 (Henselsches Lemma – 2. Version): Es seien $F(X)$ und $F^{'}(X)$ wie in Satz 3, und es sei $a_0 \in \mathbb{Z}_p$ mit

$$|F(a_0)|_p < \left|F^{'}(a_0)\right|_p^2,$$

dann gibt es ein $a \in \mathbb{Z}_p$, sodass

$$F(a) = 0$$

ist.

Beweis. Es seien die Polynome $F_j(X)$ $(j = 1, 2, \ldots, n)$ durch folgende Identität definiert

$$\begin{aligned} F(X+Y) &= c_0 + c_1(X+Y) + c_2(X+Y)^2 + \cdots + c_n(X+Y)^n \\ &= c_0 + c_1X + c_1Y + c_2X^2 + 2c_2XY + c_2Y^2 + \cdots + c_n\left(\sum_{k=0}^{n}\binom{n}{k}X^kY^{n-k}\right) \\ &= c_0 + c_1X + c_2X^2 + \cdots + c_nX^n + c_1Y + 2c_2XY + \cdots + nc_nX^{n-1}Y + \cdots \\ &= F(X) + F_1(X)Y + F_2(X)Y^2 + \cdots + F_n(X)Y^n, \end{aligned}$$

wobei X und Y zwei Unbestimmte sind. Dann ist

$$F_1(X) = c_1 + 2c_2X + \cdots + nc_nX^{n-1} = F^{'}(X).$$

Wir wählen ein b_0 so, dass

$$F(a_0) + b_0F_1(a_0) = 0$$

erfüllt ist. Bei b_0 handelt es sich um eine ganze p-adische Zahl, denn es gilt

$$|b_0|_p = \frac{|F(a_0)|_p}{|F'(a_0)|_p} < \left|F^{'}(a_0)\right|_p \leq 1$$

Wegen $F(a_0) + b_0F_1(a_0) = 0$ gilt

$$|F(a_0+b_0)|_p \leq \max_{2\leq j\leq n}\left|F_j(a_0)\,b_0^j\right|_p,$$

und da $F_j(X) \in \mathbb{Z}_p[X]$ und $a_0 \in \mathbb{Z}_p$ sind, gilt $|F_j(a_0)|_p \leq 1$ und somit

$$|F(a_0+b_0)|_p \leq |b_0|_p^2 = \frac{|F(a_0)|_p^2}{|F'(a_0)|_p^2} < |F(a_0)|_p.$$

Es ist

$$\begin{aligned} |F_1(a_0+b_0) - F_1(a_0)|_p &= \left|2c_2b_0 + 6c_3a_0b_0 + 3c_3b_0^2 + \cdots + nc_nb_0^{n-1}\right|_p \\ &= |b_0|_p\left|2c_2 + 6c_3a_0 + 3c_3b_0 + \cdots + nc_nb_0^{n-2}\right|_p \\ &\leq |b_0|_p < \left|F^{'}(a_0)\right|_p = |F_1(a_0)|_p, \end{aligned}$$

und mit Hilfe der nichtarchimedischen Dreiecksungleichung folgt

$$|F_1(a_0+b_0)|_p = |F_1(a_0)|_p.$$

Wir wiederholen das Ganze zunächst für $a_1 := a_0 + b_0$, danach für $a_2 := a_1 + b_1$, etc. Die so erhaltene Folge erfüllt

$$|F_1(a_n)|_p = |F_1(a_0)|_p$$

für alle $a_n = a_{n-1} + b_{n-1}$ sowie

$$|F(a_{n+1})|_p \leq \frac{|F(a_n)|_p^2}{|F_1(a_n)|_p^2} = \frac{|F(a_n)|_p^2}{|F_1(a_0)|_p^2}.$$

Also gilt $F(a_n) \to 0$ für $n \to \infty$. Auch die Folge $(a_n)_{n\geq 0}$ konvergiert gegen ein $a \in \mathbb{Z}_p$, denn es ist

$$|a_{n+1} - a_n|_p = |b_n|_p = \frac{|F(a_n)|_p}{|F_1(a_n)|_p} = \frac{|F(a_n)|_p}{|F_1(a_0)|_p},$$

und wir erhalten insgesamt $F(a) = 0$. □

Beispiel 5: Mit Hilfe des eben Gezeigten wollen wir nun untersuchen, ob das Polynom $F(X) = X^2 - 17$ Wurzeln in $\mathbb{Q}_2$ besitzt.

Es ist $F'(X) = 2X$. Es sei $a_0 = 1$, dann ist $|1 - 17|_2 = 2^{-4} < 2^{-2} = |2|_2^2$. Die Bedingungen von Satz 4 sind somit erfüllt, und wir können folgende zwei Lösungen berechnen: $x_1 = 1 + 2^3 + 2^5 + 2^6 + 2^7 + 2^9 + 2^{10} + \cdots$ und $x_2 = 1 + 2 + 2^2 + 2^4 + 2^8 + 2^{11} + 2^{12} + \cdots$.

Für $F(X) = X^3 - 82$ über $\mathbb{Q}_3$ ist $a_0 = 1$ und $|-81|_3 = 3^{-4} < 3^{-2} = |3|_3^2$. Wir erhalten die Kubikwurzel $x = 1 + 3^3 + 2 \cdot 3^6 + 2 \cdot 3^7 + 3^8 + 3^9 + 2 \cdot 3^{11} + \cdots$.

Beispiel 6: Wir wollen ein paar Funktionen besprechen, die PARI/GP in diesem Zusammenhang zur Verfügung stellt.

Die Funktion `polrootspadic(pol,p,r)` ermöglicht uns genau das, was wir eben besprochen haben, nämlich die Nullstellen eines Polynoms *pol* in $\mathbb{Q}_p$ bis zu der r-ten Potenz von p zu bestimmen. Die Nullstellen werden als Spaltenvektor ausgegeben, mehrfach auftretende Nullstellen werden nur einmal ausgegeben.

Natürlich gibt es auch `sqrt(x)` beziehungsweise `sqrtn(x,n)`, mit denen es möglich ist, eine Quadratwurzel beziehungsweise eine $n-$te Wurzel von x zu eruieren.

Sollen nur einzelne Schritte mit Unterstützung des Computeralgebrasytems durchgeführt werden, sind folgende Befehle von Nutzen: Mit `valuation(x,p)` kann die p-adische Ordnung von x bestimmt werden.

Die Ableitung von x nach y erhalten wir mit `deriv(x,y)`. `Mod(x,y)` berechnet x modulo y. Mit `subst(x,y,z)` wird im Ausdruck x die Variable y durch z ersetzt.

Auch interessant ist `factorpadic(pol,p,r)`. Damit ist es möglich, ein Polynom *pol* über $\mathbb{Q}_p$ zu faktorisieren, wobei die Koeffizienten von *pol* bis zur r-ten Potenz von p berechnet werden. Das Ergebnis wird als zweispaltige Matrix ausgegeben, in der ersten Spalte stehen die irreduziblen Faktoren und in der zweiten deren Exponenten.

```
? a=220+O(233^10)
%1 = 220 + O(233^10)
? sqrt(a)
%2 = 57 + 145*233 + 97*233^2 + 30*233^3 + 75*233^4 + 123*233^5 + 202*233^6 + 233^7 + 80*233^8 +
23*233^9 + O(233^10)
? f=x^2-a
%3 = x^2 + (13 + 232*233 + 232*233^2 + 232*233^3 + 232*233^4 + 232*233^5 + 232*233^6 + 232*233^7
+ 232*233^8 + 232*233^9 + O(233^10))
? polrootspadic(f,233,10)
%4 = [57 + 145*233 + 97*233^2 + 30*233^3 + 75*233^4 + 123*233^5 + 202*233^6 + 233^7 + 80*233^8 +
23*233^9 + O(233^10), 176 + 87*233 + 135*233^2 + 202*233^3 + 157*233^4 + 109*233^5 + 30*233^6 +
231*233^7 + 152*233^8 + 209*233^9 + O(233^10)]~
? factorpadic(f,233,10)
%5 =
[(1 + O(233^10))*x + (57 + 145*233 + 97*233^2 + 30*233^3 + 75*233^4 + 123*233^5 + 202*233^6 +
233^7 + 80*233^8 + 23*233^9 + O(233^10)) 1]
[(1 + O(233^10))*x + (176 + 87*233 + 135*233^2 + 202*233^3 + 157*233^4 + 109*233^5 + 30*233^6 +
231*233^7 + 152*233^8 + 209*233^9 + O(233^10)) 1]
```

4.5.1 Quadratwurzeln in $\mathbb{Q}_p$

Bevor wir uns überlegen, wie Quadratzahlen in $\mathbb{Q}_p$ aussehen, sei darauf hingewiesen, dass für eine p-adische Einheit $a = \sum_{i=0}^{\infty} a_i p^i$ klarerweise gilt, dass sie genau dann eine Quadratwurzel besitzt, wenn a_0 ein quadratischer Rest modulo p ist.

Ist nämlich a_0 ein quadratischer Rest modulo p, so sind die Voraussetzung für das Henselsche Lemma erfüllt, und $X^2 - a$ besitzt Nullstellen in $\mathbb{Z}_p^\times$.

Ist umgekehrt a_0 ein quadratischer Nichtrest modulo p, so können wir natürlich auch keine p-adische Zahl $b = \sum_{i=0}^{\infty} b_i p^i$ finden mit $b_0^2 = a_0 \pmod p$. Das ist aber die Voraussetzung für $b^2 = a$.
Nun zu $\mathbb{Q}_p$:

Korollar 3: Es sei $p \neq 2$ eine Primzahl. Eine p-adische Zahl a ist genau dann ein Quadrat, wenn sie als Produkt $a = p^{2n} \cdot \epsilon^2$ mit $n \in \mathbb{Z}$ und $\epsilon \in \mathbb{Z}_p^\times$ geschrieben werden kann. Die Quotientengruppe $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$, wobei $\left(\mathbb{Q}_p^\times\right)^2$ der Menge $\left\{b^2 :\ b \in \mathbb{Q}_p\right\}$ entspricht, hat die Ordnung vier. Ist $c \in \mathbb{Z}_p^\times$ ein quadratischer Nichtrest modulo p, dann bildet die Menge $\{1,\ p,\ c,\ cp\}$ ein vollständiges Repräsentantensystem.

Beweis. Betrachten wir das Polynom $F(X) = X^2 - a$. Für eine Lösung $b \in \mathbb{Q}_p$ dieser Gleichung muss gelten, dass $\mathrm{ord}_p(b^2) = 2\mathrm{ord}_p(b) = \mathrm{ord}_p(a)$ ist. Wie wir wissen, kann jedes $b \in \mathbb{Q}_p$ als $b = p^{\mathrm{ord}_p(b)}\epsilon$ mit $\epsilon \in \mathbb{Z}_p^\times$ geschrieben werden, daher ist $a = b^2 = p^{2\mathrm{ord}_p(b)}\epsilon^2$. Ist umgekehrt $a = p^{2n} \cdot \epsilon^2$, so ist $b = p^n \cdot \epsilon$.

Die quadratischen Reste modulo p bilden eine Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$ vom Index zwei. Daraus folgt nun

$$\mathbb{Q}_p^\times\Big/\left(\mathbb{Q}_p^\times\right)^2 \ \cong\ p^{\mathbb{Z}}\Big/p^{2\mathbb{Z}} \times \mathbb{Z}_p^\times\Big/\left(\mathbb{Z}_p^\times\right)^2 \ \cong\ \mathbb{Z}\Big/2\mathbb{Z} \times \mathbb{Z}\Big/2\mathbb{Z}.$$

Es sei $c \in \{1,\ \ldots,\ p-1\}$ ein quadratischer Nichtrest modulo p, als quadratischen Rest modulo p wählen wir 1. Dann bildet die Menge $\left\{p^0 \cdot 1,\ p \cdot 1,\ p^0 \cdot c,\ p \cdot c\right\} = \{1,\ p,\ c,\ pc\}$ ein vollständiges Repräsentantensystem. □

Als Nächstes betrachten wir den Fall $p = 2$ noch etwas genauer:

Korollar 4: Es sei $a \in \mathbb{Z}_2^\times$. Es ist a genau dann ein Quadrat in $\mathbb{Z}_2$, wenn $a \equiv 1 \pmod 8$ erfüllt ist. Die Quotientengruppe ${}^{\mathbb{Q}_2^\times}\!/_{(\mathbb{Q}_2^\times)^2}$ hat die Ordnung Acht. Außerdem bildet die Menge $\{1,\ -1,\ 5,\ -5,\ 2,\ -2,\ 10,\ -10\}$ ein vollständiges Repräsentantensystem.

Beweis. Es sei $a = b^2 \in \mathbb{Z}_2^\times$ für ein $b = 1+b_1 2+b_2 2^2+\cdots = 1+2c$. Dann ist $b^2 = 1+4\left(c+c^2\right)$, und da $c \equiv c^2 \pmod 2$ in $\mathbb{Z}_2$ gilt, ist $b^2 \equiv 1 \pmod 8$.

Für die Umkehrung wenden wir Satz 4, also die stärkere Version des Henselschen Lemmas, an. Es sei $a \equiv 1 \pmod 8$ und $F(X) = X^2 - a$. Wir suchen ein $b_0 \in \mathbb{Z}_p$, sodass $F(b_0) \equiv 0 \pmod 2$ und $|F(b_0)|_2 < \left|F'(b_0)\right|_2^2$ erfüllt sind. Klarerweise ist $b_0 = 1$, und somit gilt $|8c|_2 \leq 2^{-3} < 2^{-2} = |2|_2^2$ für $c \in \mathbb{Z}_p$. Die Bedingungen des Lemmas sind erfüllt, es gibt somit ein $b \in \mathbb{Z}_p$ mit $b^2 = a$.

Es ist

$$\mathbb{Q}_2^\times \Big/ \left(\mathbb{Q}_2^\times\right)^2 \ \cong\ 2^{\mathbb{Z}} \Big/ 2^{2\mathbb{Z}} \times \mathbb{Z}_2^\times \Big/ \left(\mathbb{Z}_2^\times\right)^2.$$

Es ist $\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$ und nach oben $\left(\mathbb{Z}_2^\times\right)^2 = 1 + 8\mathbb{Z}_p$. Betrachten wir also ${}^{\mathbb{Z}_2^\times}\!/_{(\mathbb{Z}_2^\times)^2}$, so ergibt sich die Menge aller Restklassen durch

$$\left\{1+2c_1+2^2c_2+2^3\mathbb{Z}_2 :\ c_i \in \{0,1\}\right\} = \left\{1+2^3\mathbb{Z}_2,\ 1+2+2^3\mathbb{Z}_p,\ 1+2^2+2^3\mathbb{Z}_2,\ 1+2+2^2+2^3\mathbb{Z}_2\right\}.$$

In $\mathbb{Z}_2$ gilt $-1 = 1 + 2 + 2^2 + 2^3 + \cdots$ beziehungsweise $-5 = 1 + 2 + 2^3 + \cdots$.

Insgesamt erhalten wir

$$\mathbb{Q}_2^\times \Big/ \left(\mathbb{Q}_2^\times\right)^2 \ \cong\ 2^{\mathbb{Z}} \Big/ 2^{2\mathbb{Z}} \times (1+2\mathbb{Z}_2) \Big/ (1+8\mathbb{Z}_2) \ \cong\ \mathbb{Z} \Big/ 2\mathbb{Z} \times \mathbb{Z} \Big/ 2\mathbb{Z} \times \mathbb{Z} \Big/ 2\mathbb{Z},$$

und als vollständiges Repräsentantensystem der Restklassen

$$\left\{2^0\cdot 1,\ 2^0\cdot(-1),\ 2^0\cdot 5,\ 2^0\cdot(-5),\ 2^1\cdot 1,\ 2^1\cdot(-1),\ 2^1\cdot 5,\ 2^1\cdot(-5)\right\} = \{\pm 1,\ \pm 5,\ \pm 2,\ \pm 10\}. \quad \square$$

In der Produktformel in Proposition 3 auf Seite 28 haben wir gesehen, dass eine enge Verbindung zwischen dem „gewöhnlichen“ Absolutbetrag und den p-adischen Absolutbeträgen besteht. Folgendes Resultat stellt einen Zusammenhang aller Vervollständigungen von $\mathbb{Q}$ her:

Proposition 10: Eine rationale Zahl x ist genau dann ein Quadrat in $\mathbb{Q}$, wenn x in jedem $\mathbb{Q}_p$ für $p \in \mathbb{P}$ und in $\mathbb{R}$ ein Quadrat ist.

Beweis. ($\Longrightarrow$) Ist x ein Quadrat in $\mathbb{Q}$, dann ist x natürlich auch ein Quadrat in $\mathbb{R}$ und in jedem $\mathbb{Q}_p$.

($\Longleftarrow$) Für jede rationale Zahl x, $x \neq 0$ gilt

$$x = \pm \prod_{p \in \mathbb{P}} p^{\operatorname{ord}_p(x)}.$$

In $\mathbb{R}$ ist x genau dann ein Quadrat, wenn x positiv ist. Wie wir uns bereits überlegt haben, ist x in $\mathbb{Q}_p$ genau dann ein Quadrat, wenn x als Produkt $x = p^{2n} \cdot \epsilon^2$ mit $n \in \mathbb{Z}$ und $\epsilon \in \mathbb{Z}_p^\times$ geschrieben werden kann. Somit haben alle Primfaktoren von x gerade Exponenten, x ist also ein Quadrat in $\mathbb{Q}$. $\square$

Bemerkung 8: Diese Proposition ist ein Beispiel für das sogenannte *Lokal-Global-Prinzip* der Zahlentheorie, welches besagt, dass bei manchen diophantischen Gleichungen, also Gleichungen des Typs

$$F(X_1, X_2, \ldots, X_n) = 0, \qquad F(X_1, X_2, \ldots, X_n) \in \mathbb{Z}[X_1, X_2, \ldots, X_n],$$

bei denen nur Lösungen in den ganzen oder rationalen Zahlen von Interesse sind, durch die Betrachtung der *lokalen* Lösungen, also der Lösungen in $\mathbb{R}$ und in $\mathbb{Q}_p$ für alle $p \in \mathbb{P}$, auf die Existenz oder Nicht-Existenz von *globalen* Lösungen, also Lösungen in $\mathbb{Q}$, geschlossen werden kann. Leider ist dieses Prinzip nicht allgemein gültig, wie folgendes Gegenbeispiel beweist: Wir betrachten die Gleichung

$$F(X) = \left(X^2 - 2\right)\left(X^2 - 17\right)\left(X^2 - 34\right) = 0.$$

Diese besitzt in $\mathbb{R}$ die Nullstellen $\pm\sqrt{2}$, $\pm\sqrt{17}$ sowie $\pm\sqrt{34}$. In $\mathbb{Q}_p$ verwenden wir, um die Gleichung zu lösen, das Henselsche Lemma. Die dazu benötige Ableitung von $F(X)$ ist

$$F'(X) = 2X\left(\left(X^2 - 17\right)\left(X^2 - 34\right) + \left(X^2 - 2\right)\left(X^2 - 34\right) + \left(X^2 - 2\right)\left(X^2 - 17\right)\right).$$

Für $p = 2$ verwenden wir die zweite Version des Henselschen Lemmas. Wir wählen $a_0 = 1$. Dann sind $|F(a_0)|_2 = |-528|_2 = 2^{-4}$ und $\left|F'(a_0)\right|_2 = |1154|_2 = 2^{-1}$. Die Bedingung

$$|F(a_0)|_2 < \left|F'(a_0)\right|_2^2$$

ist somit erfüllt, und $F(X)$ ist in $\mathbb{Q}_2$ lösbar. Es ist zum Beispiel $17 = 1 + 2^4$ ein Quadrat in $\mathbb{Q}_2$.

Nun sei $p = 17$. Dann ist $6^2 \equiv 2 \pmod{17}$. Wir wählen also in der ersten Version des Henselschen Lemmas $a_0 = 6$. Es ist

$$F'(6) = 9024 \equiv 14 \pmod{17},$$

die geforderten Bedingungen sind also erfüllt, und $F(X)$ besitzt in $\mathbb{Q}_{17}$ Wurzeln.

Für $p \neq 2$ und $p \neq 17$ gilt folgendes: Es ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch, deshalb gibt es eine Primitivwurzel g modulo p, die diese Gruppe erzeugt, und wir können uns leicht überlegen, dass genau jene Elemente quadratische Reste darstellen, die von einer geraden Potenz von g erzeugt werden.

Denn ist a ein quadratischer Rest modulo p, so ist $x^2 \equiv a \pmod{p}$ lösbar. Es ist also $x \equiv g^j \pmod{p}$ für ein j, und daraus folgt, dass $a \equiv g^{2j} \pmod{p}$ gilt. Ist umgekehrt $a \equiv g^{2j} \pmod{p}$, dann ist $x = g^j$ eine Lösung von $x^2 \equiv a \pmod{p}$.

Tritt nun für eine Primzahl p der Fall ein, dass weder 2 noch 17 quadratische Reste modulo p sind, dann gibt es ungerade ganze Zahlen m und n, sodass $2 \equiv g^m \pmod{p}$ und $17 \equiv g^n \pmod{p}$ für eine Primitivwurzel g modulo p gilt. Dann sehen wir aber, dass $2 \cdot 17 \equiv g^{m+n} \pmod{p}$ von einer geraden Potenz von g erzeugt wird, nach unseren Überlegungen also einen quadratischen Rest modulo p darstellt.

Das heißt, wir können immer ein a_0 finden, sodass $F(a_0) \equiv 0 \pmod{p}$ gilt. Auch die Bedingung $F'(a_0) \not\equiv 0 \pmod{p}$ ist dann erfüllt, denn einer der Terme in der Klammer ist ungleich Null.

Wir haben somit gezeigt, dass die Gleichung in $\mathbb{R}$ und in allen $\mathbb{Q}_p$ lösbar ist. Allerdings gibt es in $\mathbb{Q}$ keine Lösung der Gleichung $F(X)$, da keine der Wurzeln $\pm\sqrt{2}$, $\pm\sqrt{17}$ beziehungsweise $\pm\sqrt{34}$ rational ist.

Denn ist $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ ein normiertes Polynom mit ganzzahligen Koeffizienten und einer rationalen Nullstelle r, so gibt es ganze Zahlen s und t mit $\mathrm{ggT}(s, t) = 1$ und $r = \frac{s}{t}$. Dann ist

$$\left(\frac{s}{t}\right)^n + a_{n-1}\left(\frac{s}{t}\right)^{n-1} + \cdots + a_1\left(\frac{s}{t}\right) + a_0 = 0$$

beziehungsweise

$$s^n + a_{n-1}s^{n-1}t + \cdots + a_1st^{n-1} + a_0t^n = 0.$$

Es muss t den ersten Term s^n teilen, denn t teilt offensichtlich jeden anderen Term wie auch die rechte Seite der Gleichung. Da jedoch t und s relativ prim sind, muss t ein Teiler von Eins sein. Dann ist aber $t \in \{\pm 1\}$, und r ist eine ganze Zahl.

Betrachten wir nun das Polynom $X^2 - a$, $a \in \mathbb{Z}$, so folgt aus dem eben Gezeigten, dass nur die Wurzeln der „Quadratzahlen“ $\{1, 4, 9, 16, 25, 36, \ldots\}$ rational sind, die Quadratwurzeln aller anderen natürlichen Zahlen – also auch jene von 2, 17 und 34 – sind irrational.

Das heißt, „überall lokal lösbar“ zu sein, ist nicht dasselbe wie „global lösbar“ zu sein.

In einigen Fällen gilt jedoch das Prinzip. So besagt zum Beispiel der berühmte *Satz von Hasse-Minkowski*, dass für eine quadratische Form $F(X_1, X_2, \ldots, X_n)$, also für ein homogenes Polynom vom Grad 2 in n Variablen, mit Koeffizienten aus $\mathbb{Q}$, die Gleichung

$$F(X_1, X_2, \ldots, X_n) = 0$$

genau dann nichttriviale Lösungen in $\mathbb{Q}$ besitzt, wenn es nichttriviale Lösungen in $\mathbb{R}$ und in jedem $\mathbb{Q}_p$, $p \in \mathbb{P}$ gibt (siehe zum Beispiel [2], S. 61).

4.5.2 Einheitswurzeln

Zunächst wollen wir uns folgende Definition in Erinnerung rufen:

Definition 4: Ein Element ζ eines Körpers heißt *eine m-te Einheitswurzel*, wenn $\zeta^m = 1$ ist. Gilt zusätzlich $\zeta^n \neq 1$ für $0 < n < m$, dann heißt ζ *eine primitive m-te Einheitswurzel*.

Betrachten wir nun ein $\zeta \in \mathbb{Q}_p$ mit $\zeta^m = 1$. Dann gilt $|\zeta|_p = 1$, was bedeutet, dass alle p-adischen Einheitswurzeln in $\mathbb{Z}_p^\times$ liegen.

Wir wollen uns nun überlegen, welche Einheitswurzeln existieren. Um folgende Proposition zu beweisen, benötigen wir wieder das Henselsche Lemma.

Proposition 11: Für jede Primzahl p und für jede positive ganze Zahl m, die zu p relativ prim ist, gibt es in $\mathbb{Q}_p$ genau dann eine m-te Einheitswurzel, wenn m ein Teiler von $(p-1)$ ist. In diesem Fall ist jede m-te Einheitswurzel auch eine $(p-1)$-te Einheitswurzel. Die Menge der $(p-1)$-ten Einheitswurzeln bildet eine zyklische Untergruppe von $\mathbb{Z}_p^\times$ der Ordnung $(p-1)$.

Beweis. Es sei m ein Teiler von $(p-1)$. Dann ist $p - 1 = km$ für ein $k \geq 1$. Daher ist jede m-te Einheitswurzel auch eine $(p-1)$-te Einheitswurzel.

Wir betrachten das Polynom $F(X) = X^{p-1} - 1$ mit der Ableitung $F'(X) = (p-1)X^{p-2}$ und wählen $x_0 \in \mathbb{Z}_p^\times$ so, dass $1 \leq x_0 \leq p-1$ erfüllt ist.

Nach dem kleinen Fermatschen Satz gilt $x_0^{p-1} \equiv 1 \pmod{p}$, das heißt, es ist $F(x_0) \equiv 0 \pmod{p}$. Weiters ist $\left|F'(x_0)\right|_p = 1$, und das bedeutet, dass $F'(x_0) \not\equiv 0 \pmod{p}$ gilt.

Wir können also das Henselsche Lemma für jedes $x_0 \in \{0, \ldots, p-1\}$ anwenden und erhalten so $(p-1)$ inkongruente Einheitswurzeln.

Es sei umgekehrt $a \in \mathbb{Q}_p$ eine m-te Einheitswurzel. Wir wissen bereits, dass a dann in $\mathbb{Z}_p^\times$ liegt. Es sei a_0 die erste Ziffer von a. Da m ein Teiler von $(p-1)$ ist, gilt auch $a_0^m \equiv 1 \pmod{p}$.

Wie wir wissen, besitzt ein Polynom $F(X) \in K[X]$ vom Grad n höchstens n Nullstellen in K. Deshalb besitzt das von uns betrachtete Polynom $X^{p-1}-1$ in $\mathbb{Q}_p$ nicht mehr als $p-1$ Wurzeln. Da jede Einheitswurzel eine Wurzel dieses Polynoms sein muss, sind das alle Einheitswurzeln in $\mathbb{Q}_p$.

Die Einheitswurzeln bilden eine multiplikative Gruppe. Da jede endliche Untergruppe eines Körpers zyklisch ist, ist die Gruppe der $(p-1)$-ten Einheitswurzeln eine zyklische Untergruppe von $\mathbb{Z}_p^\times$ der Ordnung $(p-1)$. □

Beispiel 7: Die $6-$ten Einheitswurzeln in $\mathbb{Q}_7$ sind folgende:

```
? polrootspadic(x^6-1,7,10)
%1 = [1 + O(7^10), 2 + 4*7 + 6*7^2 + 3*7^3 + 2*7^5 + 6*7^6 + 2*7^7 + 4*7^8 + 3*7^9 + O(7^10),
3 + 4*7 + 6*7^2 + 3*7^3 + 2*7^5 + 6*7^6 + 2*7^7 + 4*7^8 + 3*7^9 + O(7^10), 4 + 2*7 + 3*7^3
+ 6*7^4 + 4*7^5 + 4*7^7 + 2*7^8 + 3*7^9 + O(7^10), 5 + 2*7 + 3*7^3 + 6*7^4 + 4*7^5 + 4*7^7
+ 2*7^8 + 3*7^9 + O(7^10), 6 + 6*7 + 6*7^2 + 6*7^3 + 6*7^4 + 6*7^5 + 6*7^6 + 6*7^7 + 6*7^8 +
6*7^9 + O(7^10)]~
```

Bemerkung 9: Die $(p-1)$-ten Einheitswurzeln bilden also zusammen mit $\{0\}$ ein vollständiges Repräsentantensystem modulo p.

Diese Menge heißt *Teichmüller Repräsentantensystem*, und es wäre absolut äquivalent, die Darstellung einer p-adischen Zahl als „kanonisch“ zu definieren, wenn die Ziffern aus dieser Menge gewählt würden anstatt aus $\{0, 1, \ldots, p-1\}$.

In PARI/GP kann mit der Funktion `teichmuller(x)` der Teichmüller Repräsentant von $x \in \mathbb{Q}_p$ berechnet werden, also jene $(p-1)$-te Einheitswurzel, die kongruent zu $xp^{-\mathrm{ord}_p(x)}$ modulo p ist. Betrachten wir wieder $\mathbb{Q}_7$ und die in Beispiel 7 berechneten Einheitswurzeln:

```
? a=2*7^2+1*7^3+1*7^4+O(7^10)
%1 = 2*7^2 + 7^3 + 7^4 + O(7^10)
? teichmuller(a)
%2 = 2 + 4*7 + 6*7^2 + 3*7^3 + 2*7^5 + 6*7^6 + 2*7^7 + O(7^8)
? b=6*7^-3+5*7^-2+1*7^-1+0+4*7+2*7^2+O(7^10)
%3 = 6*7^-3 + 5*7^-2 + 7^-1 + 4*7 + 2*7^2 + O(7^10)
? teichmuller(b)
%4 = 6 + 6*7 + 6*7^2 + 6*7^3 + 6*7^4 + 6*7^5 + 6*7^6 + 6*7^7 + 6*7^8 + 6*7^9 + 6*7^10 + 6*7^11 +
6*7^12 + O(7^13)
? teichmuller(13+O(7^10))
%5 = 6 + 6*7 + 6*7^2 + 6*7^3 + 6*7^4 + 6*7^5 + 6*7^6 + 6*7^7 + 6*7^8 + 6*7^9 + O(7^10)
```

4.6 Analysis in $\mathbb{Q}_p$

In diesem Abschnitt sollen einige Definitionen und Resultate, die in der reellen Analysis von fundamentaler Bedeutung sind, im p-adischen Kontext betrachtet werden. Die Voraussetzungen dafür sind ja gegeben: Die p-adischen Zahlen bilden einen mit einem Absolutbetrag ausgestatteten Körper, der bezüglich der induzierten Metrik vollständig ist. Wie $\mathbb{R}$ ist $\mathbb{Q}_p$ lokalkompakt und enthält die rationalen Zahlen als dichte Teilmenge.

Jedoch ist der betrachtete Absolutbetrag ein nichtarchimedischer, und wir haben in Kapitel 1 bereits einige „sonderbare“ Konsequenzen dieses Umstands kennengelernt. So ist $\mathbb{Q}_p$ zum Beispiel ein total unzusammenhängender metrischer Raum, Mengen sind sowohl offen als auch abgeschlossen und alle Dreiecke sind „gleichschenklig“. Deshalb stellt sich die Frage, ob es überhaupt möglich ist, in $\mathbb{Q}_p$ auf sinnvolle Weise Analysis zu betreiben. Wie wir gleich sehen werden, ist dies tatsächlich der Fall. Es ist sogar so, dass durch das Vorliegen einer Ultrametrik vieles einfacher wird – gerade auch was das Beurteilen des Konvergenzverhaltens von Folgen und Reihen betrifft.

4.6.1 Folgen und Reihen

In Lemma 2 auf Seite 29 haben wir gesehen, dass eine Folge $(x_n)_{n\geq 0}$ in $\mathbb{Q}$ bezüglich eines nichtarchimedischen Absolutbetrags $|\ |$ genau dann eine Cauchyfolge ist, wenn $|x_{n+1} - x_n| \to 0$ für $n \to \infty$ gilt. Dieses Resultat lässt sich ohne Probleme auf $\mathbb{Q}_p$ übertragen, und da dieser Körper vollständig ist, können wir hier sogar von Konvergenz sprechen, das heißt:

Eine Folge $(x_n)_{n\geq 0}$ in $\mathbb{Q}_p$ konvergiert genau dann, wenn $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$ ist.

Für die Absolutbeträge der Folgeglieder einer konvergenten Folge $(x_n)_{n\geq 0}$ gilt in $\mathbb{Q}_p$ außerdem, dass entweder $\lim_{n\to\infty} |x_n|_p = 0$ oder aber, ab einem Index N, $|x_m|_p = |x_N|_p$ für alle $m \geq N$ ist.

Der erste Fall gilt klarerweise genau dann, wenn es sich bei der betrachteten Folge um eine Nullfolge handelt. Im zweiten Fall konvergiert die Folge daher nicht gegen Null, und wir können für ein $\epsilon > 0$ einen Index N_1 finden, sodass $|x_n|_p > \epsilon$ für alle $n \geq N_1$ erfüllt ist. Da es sich um eine Cauchyfolge handelt, gibt es auch einen Index N_2, sodass für alle $n,\ m \geq N_2$ gilt $|x_m - x_n|_p < \epsilon$. Es sei nun $N := \max\{N_1,\ N_2\}$, dann folgt wegen $|x_m|_p = |x_m - x_N + x_N|_p \leq \max\left\{|x_m - x_N|_p\,,\ |x_N|_p\right\}$, dass $|x_m|_p = |x_N|_p$ für alle $m \geq N$ ist. Ist x der Grenzwert dieser Folge, dann gilt außerdem $|x|_p = \lim_{n\to\infty} |x_n|_p = |x_N|_p$.

Eine Reihe $\sum_{i=0}^{\infty} x_i$ heißt konvergent, wenn die Folge ihrer Partialsummen $s_n = \sum_{i=0}^{n} x_i$ konvergiert. Ist $x = \lim_{n\to\infty} s_n$, dann heißt x auch *die Summe der unendlichen Reihe*, und wir schreiben $x = \sum_{i=0}^{\infty} x_i$.

Proposition 12: Eine Reihe $\sum_{i=0}^{\infty} x_i$ mit $x_i \in \mathbb{Q}_p$ für alle $i \in \mathbb{N}$ konvergiert genau dann, wenn $|x_i|_p \to 0$ für $i \to \infty$ gilt. Es ist dann

$$\left|\sum_{i=0}^{\infty} x_i\right|_p \leq \max_i |x_i|_p\,.$$

Beweis. Da $s_{n+1} - s_n = x_{n+1}$ gilt, ist klar, dass die Konvergenz der Reihe aus $|x_i|_p \to 0$ für $i \to \infty$ folgt und umgekehrt.

Nehmen wir nun an, dass $\sum_{i=0}^{\infty} x_i$ konvergiert. Ist dieser Ausdruck gleich Null, dann ist die Ungleichung klarerweise erfüllt. Andernfalls gilt für jede Partialsumme

$$\Big|\sum_{i=0}^{N} x_i\Big|_p \leq \max_{0\leq i\leq N} |x_i|_p \leq \max_{i\geq 0} |x_i|_p \,.$$

Da $|\,|_p$ stetig ist, können wir den Grenzwert $N \to \infty$ bilden. Daraus folgt die gesuchte Ungleichung. □

Wie wir wissen, gilt dieses Resultat nicht in der reellen Analysis – das sehen wir sofort an der harmonischen Reihe $\sum_{i=1}^{\infty} \frac{1}{i}$. Folgende Überlegung zeigt aber eine Gemeinsamkeit von $\mathbb{R}$ und $\mathbb{Q}_p$ auf:

Beispiel 8: Eine Reihe $\sum_{i=0}^{\infty} x_i$ in einem Körper K mit Absolutbetrag $|\,|$ heißt *absolut konvergent*, wenn $\sum_{i=0}^{\infty} |x_i|$ konvergiert. Wie in $\mathbb{R}$ gilt auch in $\mathbb{Q}_p$, dass aus der absoluten Konvergenz einer Reihe deren Konvergenz folgt, denn aufgrund der Dreiecksungleichung ist

$$|s_m - s_n|_p = \Big|\sum_{i=n+1}^{m} x_i\Big|_p \leq \sum_{i=n+1}^{m} |x_i|_p.$$

Die Umkehrung gilt ebenso wenig wie im reellen Fall. Das sehen wir zum Beispiel an der Reihe

$$\sum_{i=0}^{\infty} x_i = 1 + \underbrace{p + \cdots + p}_{p \text{ mal}} + \underbrace{p^2 + \cdots + p^2}_{p^2 \text{ mal}} + p^3 + \cdots \,.$$

Diese ist wegen $|s_{n+1} - s_n|_p \leq \big|p^{n+1}\big|_p = p^{-(n+1)}$ konvergent, die Reihe der Absolutbeträge hingegen divergiert:

$$\sum_{i=0}^{\infty} |x_i|_p = 1 + p \cdot p^{-1} + p^2 \cdot p^{-2} + p^3 \cdot p^{-3} + \cdots = \infty.$$

Wie in $\mathbb{R}$ gilt in $\mathbb{Q}_p$, dass für zwei konvergente Reihen $x = \sum_{i=0}^{\infty} x_i$ und $y = \sum_{i=0}^{\infty} y_i$ auch $\sum_{i=0}^{\infty} z_i = \sum_{i=0}^{\infty} (x_i + y_i)$ konvergiert, und es ist dann $x + y = \sum_{i=0}^{\infty} z_i$.

Konvergiert zumindest eine der Reihen absolut, so ergibt sich ihr Produkt durch das Cauchy-Produkt, und es gilt

$$z = \sum_{i=0}^{\infty} z_i = \sum_{i=0}^{\infty} \Big(\sum_{j=0}^{i} x_j y_{i-j}\Big) = x \cdot y.$$

Unter *einer Umordnung* $\sum_{i=0}^{\infty} x_{j_i}$ *einer unendlichen Reihe* $\sum_{i=0}^{\infty} x_i$ verstehen wir eine Änderung der Reihenfolge ihrer Glieder x_i, es ist dann $i \mapsto j_i$ eine Bijektion der natürlichen Zahlen auf sich selbst.

Eine konvergente Reihe wird *unbedingt konvergent* genannt, wenn jede ihrer Umordnungen wieder gegen denselben Wert konvergiert. Andernfalls heißt sie *bedingt konvergent.*

In der reellen Analysis sind die unbedingt konvergenten Reihen genau die absolut konvergenten Reihen, und für die anderen gilt der sogenannte Riemannsche Umordnungssatz. Dieser besagt, dass eine bedingt konvergente Reihe immer eine Umordnung besitzt, die gegen eine beliebige vorgegebene Zahl konvergiert.

In $\mathbb{Q}_p$ hingegen folgt die unbedingte Konvergenz bereits aus der Konvergenz einer Reihe:

Proposition 13: Ist $\sum_{i=0}^{\infty} x_i$ eine konvergente Reihe über $\mathbb{Q}_p$, so konvergiert sie auch unbedingt.

Beweis. Es sei $x = \sum_{i=0}^{\infty} x_i$. Die Reihe konvergiert, es gilt also $|x_i|_p \to 0$ für $i \to \infty$. Daher gibt es für jedes $\epsilon > 0$ einen Index N_1, sodass $|x_n|_p < \frac{\epsilon}{2}$ ist für alle $n \geq N_1$. Da die Partialsummen $s_n = \sum_{i=0}^{n} x_i$ eine Cauchyfolge mit Grenzwert x darstellen, gibt es einen Index $N_2 \geq N_1$ mit $|s_m - x|_p < \frac{\epsilon}{2}$ für alle $m \geq N_2$.

Es sei nun $\sum_{i=0}^{\infty} x_{j_i}$ eine Umordnung der Reihe und $s_n^{'}$ seien die entsprechenden Partialsummen. Dann gibt es einen hinreichend großen Index N, sodass die ersten Glieder x_0, x_1, …, x_{N_2} der ursprünglichen Reihe in der Partialsumme $s_N^{'} = \sum_{i=0}^{N} x_{j_i}$ vorkommen. Es gilt daher für alle $n \geq N$ sowohl $\left|s_n^{'} - x\right|_p < \frac{\epsilon}{2}$ als auch $|x_{j_n}|_p < \frac{\epsilon}{2}$, und somit ist

$$\left|\sum_{i=0}^{\infty} x_{j_i} - x\right|_p \leq \left|\sum_{i=0}^{n} x_{j_i} - x\right|_p + \left|\sum_{i=n+1}^{\infty} x_{j_i}\right|_p < \epsilon.$$

Das bedeutet also, dass die Umordnung $\sum_{i=0}^{\infty} x_{j_i}$ konvergiert und zwar gegen den selben Grenzwert x wie die ursprüngliche Reihe. □

Proposition 14: Es seien die Elemente x_{ij} mit $i, j \in \mathbb{N}$ p-adische Zahlen. Existiert für jedes $\epsilon > 0$ ein $N = N(\epsilon)$, sodass $|x_{ij}|_p < \epsilon$ für $\max\{i, j\} \geq N$ gilt, dann konvergieren die Reihen

$$\sum_{i=0}^{\infty}\Big(\sum_{j=0}^{\infty} x_{ij}\Big) \quad \text{und} \quad \sum_{j=0}^{\infty}\Big(\sum_{i=0}^{\infty} x_{ij}\Big)$$

gegen den gleichen Grenzwert.

Beweis. Die Reihen $\sum_{j=0}^{\infty} x_{ij}$ und $\sum_{i=0}^{\infty} x_{ij}$ konvergieren, denn laut unserer Voraussetzung gilt $|x_{ij}|_p \to 0$ für jedes i falls $j \to \infty$ strebt und umgekehrt. Nach Proposition 12 ist daher für $i \geq N$ beziehungsweise $j \geq N$

$$\left|\sum_{j=0}^{\infty} x_{ij}\right|_p \leq \max_j |x_{ij}|_p < \epsilon \quad \text{beziehungsweise} \quad \left|\sum_{i=0}^{\infty} x_{ij}\right|_p \leq \max_i |x_{ij}|_p < \epsilon.$$

Das bedeutet, dass $\lim_{i\to\infty} \sum_{j=0}^{\infty} x_{ij} = 0$ sowie $\lim_{j\to\infty} \sum_{i=0}^{\infty} x_{ij} = 0$ gilt, beide Doppelreihen konvergieren also. Um zu zeigen, dass ihre Summen gleich sind, betrachten wir zunächst

$$\left|\sum_{i=0}^{\infty}\Big(\sum_{j=0}^{\infty} x_{ij}\Big) - \sum_{i=0}^{N}\Big(\sum_{j=0}^{N} x_{ij}\Big)\right|_p = \left|\sum_{i=0}^{N}\Big(\sum_{j=N+1}^{\infty} x_{ij}\Big) + \sum_{i=N+1}^{\infty}\Big(\sum_{j=0}^{\infty} x_{ij}\Big)\right|_p.$$

Mit Hilfe der nichtarchimedischen Dreiecksungleichung folgt der Rest: Ist $j \geq N+1$, so gilt ja $|x_{ij}|_p < \epsilon$ für jedes i und umgekehrt, daher ist

$$\left|\sum_{i=0}^{N}\Big(\sum_{j=N+1}^{\infty} x_{ij}\Big)\right|_p < \epsilon \quad \text{beziehungsweise} \quad \left|\sum_{i=N+1}^{\infty}\Big(\sum_{j=0}^{\infty} x_{ij}\Big)\right|_p < \epsilon.$$

Somit ist auch

$$\left|\sum_{i=0}^{\infty}\Big(\sum_{j=0}^{\infty} x_{ij}\Big) - \sum_{i=0}^{N}\Big(\sum_{j=0}^{N} x_{ij}\Big)\right|_p < \epsilon.$$

Vertauschen wir die Rolle von i und j, so ergibt sich eine äquivalente Ungleichung, und da für endliche Summen jedenfalls

$$\sum_{i=0}^{N}\Big(\sum_{j=0}^{N} x_{ij}\Big) = \sum_{j=0}^{N}\Big(\sum_{i=0}^{N} x_{ij}\Big)$$

ist, erhalten wir schließlich

$$\left|\sum_{i=0}^{\infty}\Big(\sum_{j=0}^{\infty} x_{ij}\Big) - \sum_{j=0}^{\infty}\Big(\sum_{i=0}^{\infty} x_{ij}\Big)\right|_p < \epsilon.$$

Dies gilt für alle ϵ, daher sind die Doppelsummen gleich. □

Um in $\mathbb{R}$ zu einem ähnlichen Resultat wie diesem zu gelangen – nämlich zum Doppelreihensatz von Cauchy – wird für eine der Doppelreihen absolute Konvergenz verlangt, die andere Doppelreihe konvergiert dann ebenfalls absolut.

4.6.2 Potenzreihen

Unter *einer formalen Potenzreihe* in einer Unbestimmten X verstehen wir einen Ausdruck der Form

$$f(X) = \sum_{n=0}^{\infty} a_n X^n,$$

wobei die Koeffizienten a_n in einem kommutativen Ring R mit Einselement liegen. Die Menge aller solcher Potenzreihen bildet einen Ring, welcher *der Ring der formalen Potenzreihen über* R genannt und mit $R[[X]]$ bezeichnet wird.

Diese Reihen heißen „formal“, da keine Fragen nach der Konvergenz gestellt werden. Daher ist es problemlos möglich, folgende Operationen zu betrachten:

Die Summe zweier formaler Potenzreihen $f(X)$ und $g(X)$ ist

$$(f+g)(X) = \sum_{n=0}^{\infty} (a_n + b_n) X^n,$$

ihr Produkt ergibt sich durch das Cauchy-Produkt

$$(fg)(X) = \sum_{n=0}^{\infty}\Big(\sum_{k=0}^{n} a_k b_{n-k}\Big) X^n.$$

Unser Ziel ist es, solche Potenzreihen über $\mathbb{Q}_p$ zu betrachten. Sobald wir statt der Unbestimmten X eine p-adische Zahl x in den Ausdruck einsetzen, stellt sich sehr wohl die Frage nach der Konvergenz der unendlichen Reihe, denn nun konvergiert sie entweder oder sie divergiert. Analog zu den Potenzreihen in der reellen Analysis können wir so den Begriff des Konvergenzradius einführen. Dieser hängt mit dem Resultat aus Proposition 12 auf Seite 61 zusammen, nämlich dass eine Reihe $f(x) = \sum_{n=0}^{\infty} a_n x^n$ genau dann konvergiert, wenn $|a_n x^n|_p \to 0$ für $n \to \infty$ gilt.

Definition 5: Als *Konvergenzradius einer Potenzreihe* $f(X) = \sum_{n=0}^{\infty} a_n X^n$ über $\mathbb{Q}_p$ wird jene reelle Zahl $\rho \geq 0$ bezeichnet, die durch

$$\rho = \sup\left\{ r \geq 0 : \ |a_n|_p \, r^n \to 0 \text{ für } n \to \infty \right\}$$

definiert ist. Konvergiert die Potenzreihe für jedes $r \geq 0$, dann ist $\rho = \infty$, und falls $\rho = 0$ gilt, so liegt nur im Nullpunkt Konvergenz vor.

Proposition 15: Für den Konvergenzradius ρ einer Potenzreihe $f(X) = \sum_{n=0}^{\infty} a_n X^n$ über $\mathbb{Q}_p$ gilt

$$\rho = \frac{1}{\limsup \sqrt[n]{|a_n|_p}}.$$

Diese Formel wird *Formel von Cauchy-Hadamard* genannt.

Beweis. Der Konvergenzradius ρ sei durch die Formel von Cauchy-Hadamard definiert.

Es sei zunächst $|x|_p > \rho$ mit $\rho \neq 0$ sowie $\rho \neq \infty$. Dann gilt

$$\limsup |x|_p \, |a_k|_p^{1/k} = |x|_p \lim_{n\to\infty} \sup_{k\geq n} |a_k|_p^{1/k} = \frac{|x|_p}{\rho} > 1.$$

Das heißt, der Grenzwert der Folge $s_n := |x|_p \sup_{k\geq n} |a_k|_p^{1/k}$ ist größer als Eins. Somit gilt auch $|a_k|_p \, |x|_p^k > 1$ für fast alle k, und es konvergiert $\left|a_k x^k\right|_p$ für $k \to \infty$ nicht gegen Null. Die betrachtete Potenzreihe divergiert also für diese Elemente x.

Im Fall $\rho = 0$ liegt nur im Nullpunkt Konvergenz vor, denn betrachten wir den Grenzwert $\rho \to 0$, so gilt $s_n \to \infty$ für alle x mit $|x|_p > 0$.

Nun sei $|x|_p < \rho$, $\rho \neq 0$. Wir wählen einen Radius r so, dass $|x|_p < r < \rho$ gilt. Dann ist

$$\lim_{n\to\infty} \sup_{k\geq n} r \, |a_k|_p^{1/k} = r \lim_{n\to\infty} \sup_{k\geq n} |a_k|_p^{1/k} = \frac{r}{\rho} < 1.$$

Für ein hinreichend großes $N \in \mathbb{N}$ gilt also $\sup_{k\geq N} r \, |a_k|_p^{1/k} < 1$. Somit ist $|a_k|_p \, r^k < 1$ für alle $k > N$, und für $k \to \infty$ folgt

$$\left|a_k x^k\right|_p = |a_k|_p \, r^k \left(\frac{|x|_p}{r}\right)^k < \frac{|x|_p^k}{r^k} \to 0.$$

Für den Grenzwert $\rho \to \infty$ konvergiert die Potenzreihe für alle x, denn wir können in diesem Fall immer einen Radius r mit $|x|_p < r < \rho$ finden, sodass $r \lim_{n\to\infty} \sup_{k\geq n} |a_k|_p^{1/k} = 0$ gilt. □

Bemerkung 10: In der reellen wie auch in der komplexen Analysis ist über die Konvergenz am Rand des Konvergenzintervalls beziehungsweise des Konvergenzkreises keine allgemeine Aussage möglich, die Randpunkte müssen sich nicht alle gleich verhalten.

In $\mathbb{Q}_p$ hingegen ist genau das der Fall: Entweder es konvergieren alle p-adischen Zahlen x mit $|x|_p = \rho$ oder keine einzige. Der Grund dafür ist, dass nach Proposition 12 die Konvergenz einer p-adischen Potenzreihe ausschließlich davon abhängt, ob $|a_n|_p |x|_p^n$ für $n \to \infty$ gegen Null konvergiert oder nicht.

Insgesamt gilt daher, dass es sich bei dem Bereich, auf dem eine p-adische Potenzreihe $f(X)$ über $\mathbb{Q}_p$ konvergiert, immer um eine Kugel $\mathcal{D} = \left\{x \in \mathbb{Q}_p : \ |x|_p \leq R\right\}$ handelt, wobei entweder $R = \rho$ ist, falls $f(X)$ für alle x mit $|x|_p = \rho$ konvergiert, oder $R = p^{-1}\rho$ gilt, falls die Reihe für diese Elemente divergiert. Die Wertemenge der möglichen Radien R ist also diskret und umfasst $\{p^m : \ m \in \mathbb{Z}\} \cup \{0\} \cup \infty$.

Es ist $f(X)$ dann gleichmäßig konvergent auf $\mathcal{D}$, denn für alle $x \in \mathcal{D}$ und $n \to \infty$ gilt

$$|a_n x^n|_p \leq |a_n R^n|_p \to 0.$$

Proposition 16: Jede Potenzreihe $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Z}_p[[X]]$ konvergiert in $\mathcal{D} = B_1(0)$.

Beweis. Es sei $f(X) \in \mathbb{Z}_p[[X]]$ und $x_0 \in B_1(0) = \left\{x \in \mathbb{Q}_p : \ |x|_p < 1\right\}$. Da laut Voraussetzung die Koeffizienten a_n ganze p-adische Zahlen sind, gilt $|a_n|_p \leq 1$ beziehungsweise $|a_n x_0^n|_p \leq |x_0|_p^n$ für alle n, und da $|x_0|_p < 1$ ist, folgt die Behauptung. □

Beispiel 9: Wir betrachten die Potenzreihe $f(X) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} X^n$ über $\mathbb{Q}_p$. Dann ist

$$|a_n|_p = \left|\frac{(-1)^{n-1}}{n}\right|_p = p^{\mathrm{ord}_p(n)},$$

und wegen $1 \leq p^{\mathrm{ord}_p(n)} \leq n$ gilt

$$\lim_{n\to\infty} \sqrt[n]{|a_n|_p} = \lim_{n\to\infty} \sqrt[n]{p^{\mathrm{ord}_p(n)}} = 1.$$

Das bedeutet also, dass $|a_n x^n|_p$ nur dann gegen Null konvergiert, wenn x in $\mathcal{D} = B_1(0) = \overline{B}_{p^{-1}}(0)$ liegt, denn ist $|x|_p = 1$, so divergiert die Reihe.

Über den reellen Zahlen konvergiert die betrachtete Reihe für alle x im Intervall $-1 < x \leq 1$ und stellt hier die Reihenentwicklung der Logarithmusfunktion um den Entwicklungspunkt -1 dar, es ist also $\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n$.

In gleicher Weise nennen wir die Funktion, die diese Potenzreihe innerhalb ihres Konvergenzbereiches über $\mathbb{Q}_p$ festlegt, *den p-adischen Logarithmus* und schreiben

$$\log_p : \ \mathcal{D} \to \mathbb{Q}_p, \quad \log_p(1+X) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} X^n = X - \frac{X^2}{2} + \frac{X^3}{3} - \frac{X^4}{4} + \cdots.$$

Diese Bezeichnung ist natürlich nur dann sinnvoll, wenn die charakteristische Eigenschaft des Logarithmus erfüllt ist, wenn also für x, $y \in \mathcal{D}$

$$\log_p((1+x)(1+y)) = \log_p(1+x) + \log_p(1+y)$$

gilt. Wir werden uns das in Beispiel 14 auf Seite 72 überlegen.

Beispiel 10: Nach dem Logarithmus wollen wir uns nun mit der p-adischen Reihenentwicklung der Exponentialfunktion beschäftigen.

Es ist bekannt, dass $\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ auf ganz $\mathbb{R}$ sowie auf ganz $\mathbb{C}$ konvergiert.

Um das Konvergenzverhalten der Potenzreihe $f(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$ in $\mathbb{Q}_p$ zu berechnen, müssen wir uns überlegen, wie sich $|a_n|_p^{1/n} = \left|\frac{1}{n!}\right|_p^{1/n}$ für $n \to \infty$ verhält.

Dazu zeigen wir zunächst, dass für eine positive ganze Zahl $n = a_0 + a_1 p + \cdots + a_m p^m$ gilt:

$$\operatorname{ord}_p(n!) = \frac{n - S_n}{p-1},$$

wobei $S_n = \sum_{i=0}^{m} a_i$ die Ziffernsumme von n darstellt.

Wie wir wissen, ist $\operatorname{ord}_p(m \cdot n) = \operatorname{ord}_p(m) + \operatorname{ord}_p(n)$ für zwei ganze Zahlen m und n, daher folgt

$$\operatorname{ord}_p(n!) = \sum_{i=1}^{n} \operatorname{ord}_p(i).$$

Betrachten wir nun eine positive ganze Zahl $k \leq n$ mit $\operatorname{ord}_p(k) = j$. Dann ist die p-adische Entwicklung von k gegeben durch $k = a_j p^j + \cdots + a_l p^l$ mit $j \leq l$ und $a_j \neq 0$. Daher gilt

$$k - 1 = (p-1) + \cdots + (p-1)\,p^{j-1} + (a_j - 1)\,p^j + a_{j+1}p^{j+1} + \cdots + a_l p^l,$$

und es folgt

$$\begin{aligned} S_{k-1} &= j \cdot (p-1) + a_j - 1 + a_{j+1} + \cdots + a_l \\ &= j \cdot (p-1) + S_k - 1 \end{aligned}$$

beziehungsweise

$$\operatorname{ord}_p(k) = j = \frac{1 + S_{k-1} - S_k}{p-1}.$$

Insgesamt erhalten wir so die Teleskopsumme

$$\operatorname{ord}_p(n!) = \frac{1}{p-1} \sum_{i=1}^{n} (1 + S_{i-1} - S_i) = \frac{n + S_0 - S_n}{p-1} = \frac{n - S_n}{p-1}.$$

Es ist also $|a_n|_p = \left|\frac{1}{n!}\right|_p = p^{\operatorname{ord}_p(n!)} < p^{n/(p-1)}$, und daraus ergibt sich für den Konvergenzradius ρ die Abschätzung $\rho \geq \frac{1}{p^{1/(p-1)}}$. Das bedeutet, die Reihe $f(X)$ konvergiert zumindest für alle x mit $|x|_p < p^{-1/(p-1)}$.

Als Nächstes betrachten wir eine p-adische Zahl x mit $|x|_p = p^{-1/(p-1)}$ und wählen eine positive ganze Zahl k so, dass diese eine Potenz von p ist, das heißt, $k = p^m$ für ein $m \in \mathbb{N}$. Dann ist $S_k = 1$ und $\operatorname{ord}_p(k!) = \frac{p^m - 1}{p-1}$. Weiters gilt

$$\begin{aligned} \operatorname{ord}_p\left(\frac{x^k}{k!}\right) = \operatorname{ord}_p\left(\frac{x^{p^m}}{p^m!}\right) &= \operatorname{ord}_p\left(x^{p^m}\right) - \operatorname{ord}_p(p^m!) \\ &= \frac{p^m}{p-1} - \frac{p^m - 1}{p-1} = \frac{1}{p-1}. \end{aligned}$$

Da dieser Ausdruck nicht von m abhängt und in der unendlichen Summe $\sum_{n=0}^{\infty} \frac{X^n}{n!}$ immer wieder Potenzen von p vorkommen, kann $\left|\frac{x^n}{n!}\right|_p$ für $|x|_p = p^{-1/(p-1)}$ und $n \to \infty$ nicht beliebig klein werden.

Insgesamt folgt also, dass der Konvergenzradius $\rho = p^{-1/(p-1)}$ ist und $\sum_{n=0}^{\infty} \frac{X^n}{n!}$ für alle $x \in \mathbb{Q}_p$ mit $|x|_p < p^{-1/(p-1)}$ konvergiert. Es gilt somit $\mathcal{D} = B_\rho(0) = \overline{B}_{\rho p^{-1}}(0)$.

Wir nennen die durch diese Potenzreihe definierte Funktion

$$\exp_p : \mathcal{D} \to \mathbb{Q}_p, \quad \exp_p(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!} = 1 + X + \frac{X^2}{2} + \frac{X^3}{6} + \cdots$$

die p-adische Exponentialfunktion.

Es ist $\rho = 2^{-1}$ für $p = 2$. In diesem Fall gilt daher $\mathcal{D} = 4\mathbb{Z}_2$. Im Körper der p-adischen Zahlen liegt $p^{-1/(p-1)}$ für $p > 2$ nicht im Wertebereich des Absolutbetrags $|\ |_p$. Wegen $p^{-1} < p^{-1/(p-1)} < 1$ ist hier $\mathcal{D} = p\mathbb{Z}_p$.

Für p-adische Zahlen x und y, die in $\mathcal{D}$ liegen, gilt

$$\exp_p(x+y) = \exp_p(x)\exp_p(y),$$

denn es ist

$$\begin{aligned}
\exp_p(x+y) &= \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{n!} \frac{n!}{(n-k)!k!} x^{n-k} y^k \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{x^{n-k}}{(n-k)!} \frac{y^k}{k!} = \left(\sum_{m=0}^{\infty} \frac{x^m}{m!}\right)\left(\sum_{n=0}^{\infty} \frac{y^k}{k!}\right) \\
&= \exp_p(x)\exp_p(y).
\end{aligned}$$

Beispiel 11: Im Programm PARI/GP ist es möglich, dem Logarithmus und der Exponentialfunktion p-adische Argumente zu übergeben. Wir sehen hier auch, dass sich diese beiden Funktionen invers zueinander verhalten. Das heißt, für $x_0 \in \mathcal{D} = \left\{x \in \mathbb{Q}_p : \ |x|_p < p^{-1/(p-1)}\right\}$ gilt

$$\log_p\left(\exp_p(x_0)\right) = x_0 \qquad \text{sowie} \qquad \exp_p\left(\log_p(1+x_0)\right) = 1 + x_0.$$

```
? a=3*7+2*7^2+1*7^3+O(7^5)                  ? log(1+a)
%1 = 3*7 + 2*7^2 + 7^3 + O(7^5)             %4 = 3*7 + 7^2 + 2*7^4 + O(7^5)
? exp(a)                                    ? exp(log(1+a))-1
%2 = 1 + 3*7 + 3*7^2 + 5*7^3 + O(7^5)       %5 = 3*7 + 2*7^2 + 7^3 + O(7^5)
? log(exp(a))                               ? log(0+O(7^5))
%3 = 3*7 + 2*7^2 + 7^3 + O(7^5)             *** log: zero argument in palog.
```

4.6.3 Stetigkeit und Differenzierbarkeit

Viele Definitionen und Resultate, die nur davon abhängen, dass eine metrische Struktur vorhanden ist, können ohne Probleme von der reellen Analysis auf $\mathbb{Q}_p$ übertragen werden. So gilt für den Begriff der Stetigkeit:

Eine Funktion $f:\ \mathcal{D} \to \mathbb{Q}_p$ heißt *stetig* an einer Stelle x_0 ihres Definitionsbereichs $\mathcal{D}$, wenn es zu jedem $\epsilon > 0$ ein $\delta > 0$ gibt, sodass für alle $x \in \mathcal{D} \subseteq \mathbb{Q}_p$ mit $|x - x_0|_p < \delta$ auch $|f(x) - f(x_0)|_p < \epsilon$ gilt. Ist f an jeder Stelle x_0 einer Menge $U \subseteq \mathcal{D}$ stetig, dann heißt f *stetig auf* U.

Es sei jedoch noch einmal darauf hingewiesen, dass der Körper der p-adischen Zahlen als metrischer Raum total unzusammenhängend ist. Das heißt, die Zusammenhangskomponente eines jeden $x \in \mathbb{Q}_p$ besteht nur aus diesem Element, was zur Folge hat, dass in $\mathbb{Q}_p$ keine richtigen Intervalle existieren. Daher ergibt zum Beispiel der Zwischenwertsatz von Bolzano im p-adischen Kontext wenig Sinn. Dieser besagt nämlich, dass eine stetige Funktion f auf einem abgeschlossenen Intervall $[a,\, b] \subseteq \mathbb{R}$ jeden Wert zwischen $f(a)$ und $f(b)$ annimmt.

Proposition 17: Es sei $f(X) = \sum_{n=0}^{\infty} a_n X^n$ eine Potenzreihe über $\mathbb{Q}_p$ und $\mathcal{D}$ ihr Konvergenzbereich. Dann ist die durch die Potenzreihe definierte Funktion $f:\ \mathcal{D} \to \mathbb{Q}_p,\ x \mapsto f(x) = \sum_{n=0}^{\infty} a_n x^n$ stetig auf ganz $\mathcal{D}$.

Beweis. Es sei $x_0 \in \mathcal{D}$ so gewählt, dass $x_0 \neq 0$ gilt. Dann folgt aus der nichtarchimedischen Dreiecksungleichung für alle $x \in \mathcal{D}$ mit $|x - x_0|_p < \delta < |x_0|_p$, dass $|x|_p = |x_0|_p$ ist. Weiters gilt

$$\begin{aligned}
|f(x) - f(x_0)|_p &= \Big|\sum_{n=0}^{\infty} (a_n x^n - a_n x_0^n)\Big|_p \\
&\leq \max_n \left\{|a_n x^n - a_n x_0^n|_p\right\} \\
&= \max_n \left\{|a_n|_p\, |x - x_0|_p\, \left|x_0^{n-1} + x_0^{n-2}x + \cdots + x_0 x^{n-2} + x^{n-1}\right|_p\right\} \\
&\leq \max_n \left\{|a_n|_p\, |x - x_0|_p\, |x_0|_p^{n-1}\right\},
\end{aligned}$$

denn es ist ja $\left|x_0^{n-1} + x_0^{n-2}x + \cdots + x_0 x^{n-2} + x^{n-1}\right|_p \leq \max_{1\leq i\leq n}\left\{\left|x_0^{n-i}x^{i-1}\right|_p\right\} = |x_0|_p^{n-1}$. Insgesamt folgt

$$|f(x) - f(x_0)|_p < \frac{\delta}{|x_0|_p} \max_n \left\{|a_n|_p\, |x_0|_p^n\right\}.$$

Da x_0 im Konvergenzbereich der Potenzreihe liegt, konvergiert $|a_n x_0^n|_p$ gegen Null für $n \to \infty$. Daher ist dieser Ausdruck beschränkt, und für ein passendes $\delta > 0$ folgt $|f(x) - f(x_0)|_p < \epsilon$.

Nun sei $x_0 = 0$. Für $x \in \mathcal{D}$, $x \neq 0$ folgt dann aus $|x - x_0|_p < \delta$, dass $|x|_p < \delta$ ist, und es gilt

$$\begin{aligned}
|f(x) - f(0)|_p = \Big|\Big(\sum_{n=0}^{\infty} a_n x^n\Big) - a_0\Big|_p &= |x|_p \Big|\sum_{n=0}^{\infty} a_{n+1} x^n\Big|_p \\
&\leq |x|_p \max_n \left\{|a_{n+1}x^n|_p\right\} < \delta \max_n \left\{|a_{n+1}x^n|_p\right\}.
\end{aligned}$$

Für $n \to \infty$ ist $\limsup |a_n|_p^{1/n} = \limsup |a_{n+1}|_p^{1/n}$. Daher ist $|a_{n+1}x^n|_p$ beschränkt, und es gilt $|f(x) - f(0)|_p < \epsilon$ für ein passend gewähltes δ. □

Als Nächstes wollen wir uns mit der Ableitung einer p-adischen Funktion beschäftigen:

Definition 6: Eine Funktion $f : \mathcal{D} \to \mathbb{Q}_p$ heißt *differenzierbar bei* $x_0 \in \mathcal{D} \subseteq \mathbb{Q}_p$, wenn der Grenzwert

$$f'(x_0) = \lim_{h \to \infty} \frac{f(x_0 + h) - f(x_0)}{h}$$

existiert. Dieser Grenzwert heißt dann *die Ableitung von* f *an der Stelle* x_0. Existiert dieser Grenzwert für jedes Element einer Menge $U \subseteq \mathcal{D}$, so sagen wir, dass f *differenzierbar auf* U ist.

Folgende Eigenschaften der Ableitung sind aus der reellen Analysis bekannt und lassen sich auf analoge Weise herleiten:

Für zwei Funktionen f und g, die an einer Stelle x_0 differenzierbar sind, gelten die Differentiationsregeln. Es sind dann nämlich $f \pm g$, $f \cdot g$ und, falls $g(x_0) \neq 0$ ist, auch f/g in x_0 differenzierbar, und die entsprechenden Ableitungen sind durch die Summenregel, die Produktregel und die Quotientenregel gegeben.

Für zusammengesetzte Funktionen gilt die Kettenregel. Ist also f in x_0 und g in $f(x_0)$ differenzierbar, dann ist auch $g \circ f$ in x_0 differenzierbar, und es gilt

$$(g \circ f)'(x_0) = g'(f(x_0)) \cdot f'(x_0).$$

Es ist $p'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$ die Ableitung des Polynoms $p(X) = \sum_{i=0}^{n} a_i X^i$. Rationale Funktionen sind als Quotienten von Polynomen differenzierbar.

Außerdem gilt, dass differenzierbare Funktionen stetig sind.

Beispiel 12: Der sogenannte *Mittelwertsatz der Differentialrechnung* aus der reellen Analysis besagt, dass unter der Voraussetzung, dass eine Funktion f auf dem kompakten Intervall $[a, b]$ stetig und auf (a, b) differenzierbar ist, es ein $\xi \in (a, b)$ gibt, sodass Folgendes gilt:

$$f(b) - f(a) = f'(\xi)(b - a).$$

Ein Spezialfall davon ergibt sich, wenn $f(a) = f(b)$ ist. Dann verschwindet nämlich die Ableitung an zumindest einer Stelle $\xi \in (a, b)$, das heißt, $f'(\xi) = 0$. Dieses Resultat wird *der Satz von Rolle* genannt.

Wir wollen nun versuchen, diesen Mittelwertsatz auf $\mathbb{Q}_p$ zu übertragen. Sofort ergibt sich das Problem, dass wir hier nicht von Intervallen sprechen können. Dass ξ in (a, b) liegt, kann aber auch ausgedrückt werden als $\xi = at + b(1 - t)$ für $0 \leq t \leq 1$. Diese Formulierung können wir in $\mathbb{Q}_p$ übernehmen.

Das bedeutet, wir müssen uns nun überlegen, ob es – falls eine Funktion $f(X)$ auf einem Bereich $\mathcal{D} \subseteq \mathbb{Q}_p$ differenzierbar ist und eine gleichmäßig stetige Ableitung besitzt – zu je zwei Elementen x und y in $\mathcal{D}$ ein $\xi \in \mathcal{D}$ gibt, sodass $\xi = xt + y(1 - t)$ für ein t mit $|t|_p \leq 1$ gilt und $f'(\xi)$ die gewünschten Eigenschaften besitzt.

Der Mittelwertsatz ist im Körper der p-adischen Zahlen jedoch nicht gültig. Das beweist folgendes Gegenbeispiel: Wir betrachten das Polynom

$$f(X) = X^p - X$$

über $\mathbb{Q}_p$. Dann ist

$$f'(X) = pX^{p-1} - 1.$$

Es sei also $x = 0$ und $y = 1$. Daher gilt $f(x) = f(y) = 0$.

Wäre nun der Mittelwertsatz beziehungsweise der Satz von Rolle gültig, so gäbe es ein

$$\xi = xt + y(1-t) = 1 - t,$$

das der Gleichung $0 = p\xi^{p-1} - 1$ genügte. Da aber $|t|_p \leq 1$ ist, liegt t in $\mathbb{Z}_p$ und daher auch ξ. Daraus folgt, dass $p\xi^{p-1} - 1$ nicht Null sein kann, sondern von folgender Form ist:

$$p\mathbb{Z}_p - 1 = (p-1) + p\mathbb{Z}_p.$$

Die formale Ableitung einer Potenzreihe $f(X) = \sum_{n=0}^{\infty} a_n X^n$ ist gegeben durch $Df(X) = \sum_{n=1}^{\infty} n a_n X^{n-1}$. Wir wollen nun zeigen, dass für ein Element x im Konvergenzradius die formale Ableitung der analytischen Ableitung $f'(x)$ entspricht:

Proposition 18: Es sei $f(X) = \sum_{n=0}^{\infty} a_n X^n$ eine Potenzreihe über $\mathbb{Q}_p$ mit Konvergenzradius $\rho > 0$, und es sei $Df(X)$ ihre formale Ableitung. Konvergiert $f(x_0)$ für ein $x_0 \in \mathbb{Q}_p$, dann konvergiert auch $Df(x_0)$, und es gilt

$$f'(x_0) = \lim_{h \to \infty} \frac{f(x_0 + h) - f(x_0)}{h} = \sum_{n=1}^{\infty} n a_n x_0^{n-1}.$$

Beweis. Wie wir uns in Bemerkung 10 auf Seite 66 überlegt haben, ist der Konvergenzbereich $\mathcal{D}$ einer Potenzreihe eine abgeschlossene Kugel um Null mit Radius R, wobei entweder $R = \rho$ oder $R = p^{-1}\rho$ gilt, je nachdem ob die „Randpunkte“ konvergieren oder nicht.

Wir können also für $x_0 \in \mathcal{D}$ immer Elemente $x_0 + h$ finden, sodass für $h \to 0$ eine Konvergenz von $f(x_0 + h)$ vorliegt: Ist $x_0 = 0$, so wählen wir ein Element h mit $|h|_p \leq R$, ist $x_0 \neq 0$ eines mit $|h|_p < |x_0|_p \leq R$.

Für $x_0 = 0$ konvergiert $Df(x_0)$ klarerweise. Auch für $x_0 \neq 0$ ist die Ableitung konvergent, denn es gilt

$$\left|n a_n x_0^{n-1}\right|_p \leq \left|a_n x_0^{n-1}\right|_p = \frac{1}{|x_0|_p} |a_n x_0^n|_p \to 0$$

für $n \to \infty$. Nun ist

$$f(x_0 + h) = \sum_{n=0}^{\infty} a_n (x_0 + h)^n = \sum_{n=0}^{\infty} a_n \sum_{k=0}^{n} \binom{n}{k} x_0^{n-k} h^k.$$

Daraus folgt

$$\frac{f(x_0 + h) - f(x_0)}{h} = \sum_{n=1}^{\infty} \sum_{k=1}^{n} a_n \binom{n}{k} x_0^{n-k} h^{k-1}.$$

Da sowohl $|x_0|_p \leq R$ als auch $|h|_p \leq R$ gilt, ist

$$\left| a_n \binom{n}{k} x_0^{n-k} h^{k-1} \right|_p \leq |a_n|_p R^{n-1}.$$

Wie wir wissen, gilt $|a_n|_p R^n \to 0$ für $n \to \infty$. Das heißt, die Reihe konvergiert gleichmäßig in h, und wir können daher den Grenzwert Term für Term berechnen. Insgesamt folgt mit $h \to 0$

$$f'(x_0) = Df(x_0) = \sum_{n=1}^{\infty} n a_n x_0^{n-1}.$$ □

Beispiel 13: Die p-adische Exponentialfunktion aus Beispiel 10 ist für alle $x \in B_\rho(0)$ mit $\rho = p^{-1/(p-1)}$ differenzierbar, und es gilt $\exp_p'(x) = \exp_p(x)$. Der p-adische Logarithmus aus Beispiel 9 ist für alle $x \in B_1(1)$ differenzierbar, und es ist $\log_p'(x) = \frac{1}{x}$. Denn es gilt:

$$\exp_p'(x) = \sum_{n=1}^{\infty} \frac{nx^{n-1}}{n!} = \sum_{n=1}^{\infty} \frac{x^{n-1}}{(n-1)!} = \exp_p(x).$$
$$\log_p'(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{nx^{n-1}}{n} = \sum_{n=1}^{\infty} (-1)^{n-1} x^{n-1} = \frac{1}{1+x}.$$

Beispiel 14: Mit Hilfe seiner Ableitung wollen wir nun zeigen, dass der Logarithmus folgende Eigenschaft besitzt:

$$\log_p((1+x)(1+y)) = \log_p(1+x) + \log_p(1+y).$$

Betrachten wir also $f(X) = \log_p(1+X) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{X^n}{n}$, dann ist für $x \in p\mathbb{Z}_p$

$$f'(x) = \sum_{n=0}^{\infty} (-1)^n x^n = \frac{1}{1+x}.$$

Wir wählen nun ein $y \in p\mathbb{Z}_p$ und definieren

$$g(x) = \log_p((1+x)(1+y)) = f(y + (1+y)x).$$

Es ist $\rho = 1$ der Konvergenzradius von $f(X)$. Da $|y|_p < 1$ und somit $|1+y|_p = 1$ ist, gilt $|y + (1+y)x|_p < 1$ genau dann, wenn $|x|_p < 1$ ist. Das Konvergenzverhalten von $g(X)$ stimmt also mit jenem von $f(X)$ überein.

Da also für $x \in p\mathbb{Z}_p$

$$\begin{aligned} g(x) &= \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (y + (1+y)x)^n \\ &= \sum_{n=1}^{\infty} \left(\sum_{k=1}^{n} \frac{(-1)^{n-1}}{n} \binom{n}{k} (1+y)^k x^k y^{n-k} \right) \end{aligned}$$

konvergiert, können wir die Reihe umordnen und erhalten so

$$g(x) = \sum_{k=1}^{\infty} \left(\sum_{n=k}^{\infty} \frac{(-1)^{n-1}}{n} \binom{n}{k} (1+y)^k y^{n-k} \right) x^k.$$

Das bedeutet, diese Funktion ist durch eine Potenzreihe $g(X) = \sum_{k=1}^{\infty} c_k X^k$ definiert. Berechnen wir nun die Ableitung nach x, so erhalten wir

$$g'(x) = (1+y) f'(y + (1+y)x) = \frac{(1+y)}{1+y+(1+y)x} = \frac{1}{1+x} = f'(x).$$

Die Ableitungen der Potenzreihen $f(X)$ und $g(X)$ stimmen also für Elemente innerhalb des Konvergenzradius überein. Außerdem folgt aus Proposition 18, dass die Ableitungen ebenfalls den Konvergenzradius ρ besitzen.

Wir können also eine Folge $(x_m)_{m\geq 0} \to 0$ im Konvergenzbereich finden mit $x_m \neq 0$ und $g'(x_m) = f'(x_m)$ für alle m und so mit Hilfe des Identitätssatzes für Potenzreihen schließen, dass die Ableitungen ident sind, also in all ihren Koeffizienten übereinstimmen.

Dieser Identitätssatz besagt nämlich, dass zwei Potenzreihen $h_1(X)$ und $h_2(X)$ in allen Koeffizienten übereinstimmen, wenn es eine Nullfolge $(x_m)_{m\geq 0}$ gibt mit $x_m \neq 0$ und $h_1(x_m) = h_2(x_m)$ für alle m. Denn betrachten wir die Differenz

$$h(X) := h_1(X) - h_2(X) = \sum_{n=0}^{\infty} a_n X^n,$$

dann ist $h(x_m) = 0$ für jedes $m \in \mathbb{N}$. Außerdem sind alle Koeffizienten von $h(X)$ gleich Null. Denn angenommen, das wäre nicht der Fall, dann gäbe es einen kleinsten Index k mit $a_k \neq 0$, und wir hätten

$$\begin{aligned} h(X) &= a_k X^k + a_{k+1} X^{k+1} + a_{k+2} X^{k+2} + \cdots \\ &= X^k \left(a_k + a_{k+1} X + a_{k+2} X^2 + \cdots\right) \\ &= X^k \overline{h}(X). \end{aligned}$$

Es ist dann $\overline{h}(0) = a_k \neq 0$. Da $\overline{h}(X)$ stetig ist, gilt $\overline{h}(x_m) \to a_k$ für $m \to \infty$. Insbesondere ist dann $\overline{h}(x_N) \neq 0$ für ein hinreichend großes $N \in \mathbb{N}$. Daraus folgt auch, dass

$$h(x_N) = x_N^k \overline{h}(x_N) \neq 0$$

gilt, was jedoch unseren Voraussetzungen widerspricht. Daher ist $a_n = 0$ für alle $n \in \mathbb{N}$ sowie $h_1(X) = h_2(X)$.

Somit ist $g(x) = f(x) + c$ für eine Konstante $c \in \mathbb{Q}_p$ und alle $x \in p\mathbb{Z}_p$. Für $x = 0$ erhalten wir $c = g(0) = f(y)$. Es ist also $g(x) = f(x) + f(y)$ beziehungsweise

$$\log_p((1+x)(1+y)) = \log_p(1+x) + \log_p(1+y).$$

Quellen und Literatur zu Kapitel 4

Abschnitt 4.1 basiert auf §4 *Die Sätze von Gelfand-Mazur und Ostrowski* des Kapitels *Absolutbeträge* aus [21]. Zu Abschnitt 4.2 vergleiche [9], S. 67, 68, [13], S. 21-25, 29 und [14], S. 13, 14, zu Abschnitt 4.3 [9], S. 62-64, [13], S. 39, 40, 58, 59 sowie [18], S. 5, 6, 36, 37 und zu Abschnitt 4.4 [1], S. 38-43, [13], S. 27-33, [16], S. 27-34, [18], S. 2, 3 und [19], S. 5-8.
Abschnitt 4.5 basiert auf [9], S. 69-73, 77-79, [13], S. 33-39, 46, 47, [14], S. 15-18 und [18], S. 49-52. Der Beweis zu Satz 4 stammt aus [6], S. 49-51.
Zu Abschnitt 4.6 vergleiche [1], S. 25, 26, 43-51, [9], S. 87-97, 102, 105, 111-117, [13], S. 75-86, 89-93, 97, 98, [14], S. 76-81 sowie [18], S. 241, 280-284.
Für die Dokumentation zum Computeralgebrasystem PARI/GP siehe [23].

5

Der algebraische Abschluss von $\mathbb{Q}_p$

Der Körper der p-adischen Zahlen $\mathbb{Q}_p$ ist algebraisch nicht abgeschlossen. Dies wissen wir bereits aus Proposition 9 auf Seite 53. Das bedeutet, dass keine Vervollständigung von $\mathbb{Q}$ – also weder jene bezüglich des „gewöhnlichen“ Absolutbetrags $|\ |_\infty$ noch jene bezüglich $|\ |_p$ für jegliche Primzahl p – diese Eigenschaft besitzt.

Unser nächstes Ziel ist es daher, das p-adische Äquivalent zu den komplexen Zahlen $\mathbb{C}$, die ja den algebraischen Abschluss der reellen Zahlen $\mathbb{R}$ bilden, zu konstruieren, und das wird sich als deutlich aufwändiger erweisen als im reellen Falle.

In den ersten beiden Abschnitten dieses Kapitels wiederholen wir Grundlagen über normierte Vektorräume und Körpererweiterungen und leiten jene allgemeinen Resultate her, die wir ab Abschnitt 5.3 benötigen, um uns speziell mit Erweiterungen von $\mathbb{Q}_p$ zu beschäftigen.

Unter einem bewerteten Körper verstehen wir im Folgenden einen Körper K, der mit einem Absolutbetrag $|\ |$ ausgestattet ist. Von diesem Absolutbetrag nehmen wir an, dass er ein nichttrivialer ist. Außerdem soll K die Charakteristik 0 haben, das heißt, es soll kein $n > 0$ geben, sodass $n \cdot 1_K = 0$ gilt.

5.1 Normierte Vektorräume über vollständigen, bewerteten Körpern

Definition 1: Es sei K ein bewerteter Körper und V ein Vektorraum über K. Dann verstehen wir unter *einer Norm auf* V eine Funktion $\|\ \| : V \to \mathbb{R}$ mit folgenden Eigenschaften:

(N1) $\|\boldsymbol{v}\| \geq 0$ für alle $\boldsymbol{v} \in V$, $\|\boldsymbol{v}\| = 0 \iff \boldsymbol{v} = 0$,

(N2) $\|\lambda \boldsymbol{v}\| = |\lambda|\,\|\boldsymbol{v}\|$ für alle $\boldsymbol{v} \in V$ und $\lambda \in K$,

(N3) $\|\boldsymbol{v} + \boldsymbol{w}\| \leq \|\boldsymbol{v}\| + \|\boldsymbol{w}\|$ für alle $\boldsymbol{v}, \boldsymbol{w} \in V$.

Die Eigenschaft (N3) wird *Dreiecksungleichung* genannt. Ein Vektorraum V, auf dem eine Norm $\| \ \|$ definiert ist, heißt *ein normierter Vektorraum über* K.

Ist V ein normierter Vektorraum über K, dann wird für $\boldsymbol{v},\ \boldsymbol{w} \in V$ durch

$$d(\boldsymbol{v},\ \boldsymbol{w}) = \|\boldsymbol{v} - \boldsymbol{w}\|$$

eine Metrik auf V festgelegt.

Wir können uns leicht davon überzeugen, dass die Bedingungen (M1) bis (M3) aus Definition 5 auf Seite 12 erfüllt sind: Es ist $d(\boldsymbol{v},\ \boldsymbol{w}) \geq 0$ für alle $\boldsymbol{v},\ \boldsymbol{w} \in V$, und $d(\boldsymbol{v},\ \boldsymbol{w}) = 0$ gilt genau dann, wenn $\boldsymbol{v} - \boldsymbol{w} = 0$ und somit $\boldsymbol{v} = \boldsymbol{w}$ ist. Da

$$\|\boldsymbol{v} - \boldsymbol{w}\| = \|-(\boldsymbol{w} - \boldsymbol{v})\| = |-1|\,\|\boldsymbol{w} - \boldsymbol{v}\| = \|\boldsymbol{w} - \boldsymbol{v}\|$$

gilt, ist $d(\boldsymbol{v},\ \boldsymbol{w}) = d(\boldsymbol{w},\ \boldsymbol{v})$, und die Dreiecksungleichung für Metriken $d(\boldsymbol{v},\ \boldsymbol{u}) \leq d(\boldsymbol{v},\ \boldsymbol{u}) + d(\boldsymbol{u},\ \boldsymbol{w})$ folgt aus jener für Normen:

$$\|\boldsymbol{v} - \boldsymbol{u}\| = \|(\boldsymbol{v} - \boldsymbol{w}) + (\boldsymbol{w} - \boldsymbol{u})\| \leq \|\boldsymbol{v} - \boldsymbol{w}\| + \|\boldsymbol{w} - \boldsymbol{u}\|\,.$$

Analog zum Begriff des topologischen Körpers aus Definition 9 auf Seite 14 bezeichnet *ein topologischer Vektorraum* einen Vektorraum V über einem Körper K, der neben der Vektorraumstruktur noch eine Topologie besitzt, sodass die Abbildungen

$$\begin{aligned}(\boldsymbol{v},\ \boldsymbol{w}) \mapsto \boldsymbol{v} + \boldsymbol{w}: &\quad V \times V \to V,\\ (\lambda,\ \boldsymbol{v}) \mapsto \lambda\boldsymbol{v}: &\quad K \times V \to V\end{aligned}$$

stetig sind.

Wie wir eben gesehen haben, ist jeder normierte Vektorraum V ein metrischer Raum, und damit auch ein topologischer Raum – das haben wir uns in Abschnitt 1.2.2 überlegt.

Weiters werden sowohl die Addition im Vektorraum als auch die Multiplikation mit einem Skalar durch die von der Norm induzierte Topologie zu stetigen Operationen. Seien nämlich $\boldsymbol{v}_0,\ \boldsymbol{w}_0 \in V$ fest gewählt und für $\boldsymbol{v},\ \boldsymbol{w} \in V$ sowohl $d(\boldsymbol{v},\ \boldsymbol{v}_0) < \delta$ als auch $d(\boldsymbol{w},\ \boldsymbol{w}_0) < \delta$, so gilt mit $\delta = \frac{\epsilon}{2}$

$$\begin{aligned}d(\boldsymbol{v} + \boldsymbol{w},\ \boldsymbol{v}_0 + \boldsymbol{w}_0) &= \|(\boldsymbol{v} + \boldsymbol{w}) - (\boldsymbol{v}_0 + \boldsymbol{w}_0)\|\\ &\leq \|\boldsymbol{v} - \boldsymbol{v}_0\| + \|\boldsymbol{w} - \boldsymbol{w}_0\|\\ &< \epsilon.\end{aligned}$$

Falls für ein fest gewähltes $\boldsymbol{v}_0 \in V$ und ein $\lambda_0 \in K$ einerseits $d(\boldsymbol{v},\ \boldsymbol{v}_0) < \delta$ für $\boldsymbol{v} \in V$ und andererseits $d(\lambda,\ \lambda_0) < \delta$ für $\lambda \in K$ erfüllt ist, so folgt $d(\lambda\boldsymbol{v},\ \lambda_0\boldsymbol{v}_0) < \epsilon$, denn es gilt

$$\begin{aligned}d(\lambda\boldsymbol{v},\ \lambda_0\boldsymbol{v}_0) &= \|(\lambda - \lambda_0)(\boldsymbol{v} - \boldsymbol{v}_0) + \lambda_0(\boldsymbol{v} - \boldsymbol{v}_0) + \boldsymbol{v}_0(\lambda - \lambda_0)\|\\ &\leq \underbrace{|\lambda - \lambda_0|}_{<\delta}\underbrace{\|\boldsymbol{v} - \boldsymbol{v}_0\|}_{<\delta} + \underbrace{|\lambda_0|}_{\text{fix}}\underbrace{\|\boldsymbol{v} - \boldsymbol{v}_0\|}_{<\delta} + \underbrace{\|\boldsymbol{v}_0\|}_{\text{fix}}\underbrace{|\lambda - \lambda_0|}_{<\delta}.\end{aligned}$$

Wir sehen also, dass V ein topologischer Vektorraum ist.

Definition 2: Zwei Normen $\| \ \|_1$ und $\| \ \|_2$ auf einem Vektorraum V über einem Körper K heißen *äquivalent*, wenn sie die gleiche Topologie auf V induzieren.

Proposition 1: Zwei Normen $\| \|_1$ und $\| \|_2$ auf einem Vektorraum V sind genau dann äquivalent, wenn es positive reelle Zahlen c_1 und c_2 gibt, sodass

$$c_1 \|\boldsymbol{v}\|_2 \leq \|\boldsymbol{v}\|_1 \leq c_2 \|\boldsymbol{v}\|_2$$

für alle $\boldsymbol{v} \in V$ gilt.

Beweis. ($\Longrightarrow$) Es seien $\| \|_1$ und $\| \|_2$ äquivalente Normen, und wir betrachten die Abbildung $\iota : (V, \| \|_1) \to (V, \| \|_2)$, $\iota(\boldsymbol{v}) = \boldsymbol{v}$.

Da die beiden Normen die gleiche Topologie auf V erzeugen, sind ι und ι^{-1} stetig. Es gibt also für alle $\epsilon > 0$ ein $\delta > 0$, sodass für alle $\boldsymbol{v} \in V$ mit $\|\boldsymbol{v} - \boldsymbol{v}_0\|_1 < \delta$ auch $\|\boldsymbol{v} - \boldsymbol{v}_0\|_2 < \epsilon$ gilt.

Es sei nun $\boldsymbol{v}_0 = 0$. Weiters sei δ_1 so gewählt, dass aus $\|\boldsymbol{v}\|_1 < \delta_1$ die Ungleichung $\|\boldsymbol{v}\|_2 < 1$ folgt, also $\epsilon = 1$ ist.

Für $\boldsymbol{v} \in V$, $\boldsymbol{v} \neq 0$ setzen wir

$$\boldsymbol{z} := \frac{\delta_1 - \delta'}{\|\boldsymbol{v}\|_1} \boldsymbol{v},$$

wobei δ' eine reelle Zahl ist, die $0 < \delta' < \delta_1$ erfüllt. Dann ist $\|\boldsymbol{z}\|_1 < \delta_1$ und daher $\|\boldsymbol{z}\|_2 = \frac{\left|\delta_1 - \delta'\right| \|\boldsymbol{v}\|_2}{\|\boldsymbol{v}\|_1} < 1$, was auch bedeutet, dass $\left|\delta_1 - \delta'\right| \|\boldsymbol{v}\|_2 < \|\boldsymbol{v}\|_1$ gilt. Für $\delta' \to 0$ ergibt das

$$|\delta_1| \, \|\boldsymbol{v}\|_2 \leq \|\boldsymbol{v}\|_1 .$$

Wenn wir nun ι^{-1} betrachten, erhalten wir mit der gleichen Argumentation für ein $\delta_2 > 0$ die Ungleichung

$$|\delta_2| \, \|\boldsymbol{v}\|_1 \leq \|\boldsymbol{v}\|_2 .$$

Das gewünschte Resultat folgt mit $c_1 = |\delta_1|$ und $c_2 = \frac{1}{|\delta_2|}$.

($\Longleftarrow$) Im Folgenden bezeichnet die Hochzahl $i \in \{1, 2\}$ bei $B_r^i(a)$ jene Norm $\| \|_i$, von welcher die Topologie stammt bezüglich der die Kugel mit Mittelpunkt a und Radius r offen ist.

Betrachten wir zunächst die Ungleichung $c_1 \|\boldsymbol{v}\|_2 \leq \|\boldsymbol{v}\|_1$. Dann gilt $B^1_{c_1 \cdot \epsilon}(\boldsymbol{v}_0) \subseteq B^2_\epsilon(\boldsymbol{v}_0)$ für $\boldsymbol{v}_0 \in V$ und $\epsilon > 0$. Denn ist $\boldsymbol{v}' \in B^1_{c_1 \cdot \epsilon}(\boldsymbol{v}_0)$, so folgt aus $\left\|\boldsymbol{v}' - \boldsymbol{v}_0\right\|_1 < c_1 \epsilon$, dass $\left\|\boldsymbol{v}' - \boldsymbol{v}_0\right\|_2 \leq \frac{1}{c_1}\left\|\boldsymbol{v}' - \boldsymbol{v}_0\right\|_1 < \epsilon$ ist.

Für $\|\boldsymbol{v}\|_1 \leq c_2 \|\boldsymbol{v}\|_2$ ist $B^2_{c_2^{-1}\epsilon}(\boldsymbol{v}_0) \subseteq B^1_\epsilon(\boldsymbol{v}_0)$ für $\boldsymbol{v}_0 \in V$ und $\epsilon > 0$. Denn aus $\left\|\boldsymbol{v}' - \boldsymbol{v}_0\right\|_2 < c_2^{-1}\epsilon$ folgt $\left\|\boldsymbol{v}' - \boldsymbol{v}_0\right\|_1 \leq c_2 \left\|\boldsymbol{v}' - \boldsymbol{v}_0\right\|_2 < \epsilon$ für $\boldsymbol{v}' \in B^2_{c_2^{-1}\epsilon}(\boldsymbol{v}_0)$.

Wir haben somit gezeigt, dass jede offene Kugel bezüglich einer Norm auch eine offene Kugel bezüglich der anderen Norm ist, die induzierten Topologien stimmen also überein. □

Beispiel 1: Ist V ein endlichdimensionaler Vektorraum mit der Basis $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$, so kann jedes $\boldsymbol{v} \in V$ eindeutig als Linearkombination $\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n$ mit $a_i \in K$ geschrieben werden. Es stellt dann

$$\|a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n\|_\infty := \max_{1 \leq i \leq n} \left|a_i\right|$$

eine Norm auf V bezüglich der von uns gewählten Basis dar: Die Eigenschaften (N1)-(N3) folgen unmittelbar aus den Eigenschaften (A1)-(A3) des Absolutbetrags $|\,|$ auf K aus Definition 1 auf Seite 7. Diese Norm heißt *Supremumsnorm*.

Ist K vollständig bezüglich $|\ |$, dann ist V vollständig bezüglich der Supremumsnorm. Insbesondere ist eine Folge $(\boldsymbol{w}_m)_{m\geq 1}$ mit

$$\boldsymbol{w}_m = a_{1m}\boldsymbol{v}_1 + a_{2m}\boldsymbol{v}_2 + \cdots + a_{nm}\boldsymbol{v}_n$$

genau dann eine Cauchyfolge in V, wenn die Folgen der Koeffizienten $(a_{1m})_{m\geq 1}$, $(a_{2m})_{m\geq 1}$, $\ldots$, $(a_{nm})_{m\geq 1}$ Cauchyfolgen in K sind. Denn da für zwei Folgeglieder $\boldsymbol{w}_{m_k}$ und $\boldsymbol{w}_{m_l}$ die Beziehung

$$|a_{im_k} - a_{im_l}| \leq \max_{1\leq i\leq n} |a_{im_k} - a_{im_l}| = \|\boldsymbol{w}_{m_k} - \boldsymbol{w}_{m_l}\|_\infty$$

gilt, wird $|a_{im_k} - a_{im_l}|$ für $i = 1,\ \ldots, n$ kleiner als jedes $\epsilon > 0$, wenn dies auch für $\|\boldsymbol{w}_{m_k} - \boldsymbol{w}_{m_l}\|_\infty$ der Fall ist.

Aus dieser Ungleichung folgt auch die Umkehrung, dass nämlich $(\boldsymbol{w}_m)_{m\geq 1}$ eine Cauchyfolge in V ist, wenn nur alle $(a_{im})_{m\geq 1}$, $i = 1,\ \ldots,\ n$ Cauchyfolgen in K sind.

Der Grenzwert der Folge $(\boldsymbol{w}_m)_{m\geq 1}$ ergibt sich dann durch den Grenzwert der Koeffizienten:

$$\lim_{m\to\infty} \boldsymbol{w}_m = \big(\lim_{m\to\infty} a_{1m}\big)\boldsymbol{v}_1 + \big(\lim_{m\to\infty} a_{2m}\big)\boldsymbol{v}_2 + \cdots + \big(\lim_{m\to\infty} a_{nm}\big)\boldsymbol{v}_n.$$

Satz 1: Ist V ein endlichdimensionaler Vektorraum über einem vollständigen, bewerteten Körper K, so sind je zwei Normen auf V äquivalent. Es ist V dann vollständig bezüglich jeder dieser Normen.

Beweis. Es sei $\|\ \|_\infty$ die Supremumsnorm aus Beispiel 1 und $\|\ \|_1$ eine beliebige andere Norm auf V. Für $\boldsymbol{v} \in V$, $\boldsymbol{v} = \sum_{i=1}^n a_i\boldsymbol{v}_i$ ist

$$\begin{aligned}\big\|\boldsymbol{v}\big\|_1 = \Big\|\sum_{i=1}^n a_i\boldsymbol{v}_i\Big\|_1 &\leq \sum_{i=1}^n |a_i|\,\|\boldsymbol{v}_i\|_1 \\ &\leq \|\boldsymbol{v}\|_\infty \sum_{i=1}^n \|\boldsymbol{v}_i\|_1 \leq c_2\,\|\boldsymbol{v}\|_\infty\end{aligned}$$

mit $c_2 = n \cdot \max_{1\leq i\leq n} \|\boldsymbol{v}_i\|_1$.

Um die Ungleichung aus Proposition 1 zu vervollständigen und damit die Äquivalenz der Normen zu beweisen, müssen wir noch eine reelle Zahl $c_1 > 0$ finden, sodass auch die Bedingung $c_1\,\|\boldsymbol{v}\|_\infty \leq \big\|\boldsymbol{v}\big\|_1$ erfüllt ist. Dieser Teil ist mit deutlich mehr Aufwand verbunden als der vorige, und wir zeigen ihn mit Induktion nach der Dimension n des Vektorraums V.

Zunächst sei also $n = 1$ und $\boldsymbol{v}_1 \in V$, $\boldsymbol{v}_1 \neq 0$. Dann ist für $\boldsymbol{v} \in V$

$$\big\|\boldsymbol{v}\big\|_1 = \|a_1\boldsymbol{v}_1\|_1 = |a_1|\,\|\boldsymbol{v}_1\|_1 = \|\boldsymbol{v}_1\|_\infty\,\|\boldsymbol{v}_1\|_1 = c_1\,\|\boldsymbol{v}_1\|_\infty$$

mit $c_1 = \|\boldsymbol{v}_1\|_1$.

Als Nächstes betrachten wir unter der Annahme, dass für einen Vektorraum der Dimension $n-1$ schon ein c_1 gefunden ist, das der Ungleichung genügt, einen Vektorraum V der Dimension n und mit der Basis $\{\boldsymbol{v}_1,\ \boldsymbol{v}_2,\ \ldots,\ \boldsymbol{v}_n\}$. Weiters sei W der Teilraum von V, der von $\{\boldsymbol{v}_1,\ \boldsymbol{v}_2,\ \ldots,\ \boldsymbol{v}_{n-1}\}$ aufgespannt wird. Das bedeutet, dass die Normen $\|\ \|_\infty$ und $\|\ \|_1$ auf W äquivalent sind, denn der Teilraum besitzt ja die Dimension $n-1$.

Es sei $(\boldsymbol{w}_m)_{m\geq 1}$ eine Cauchyfolge in W bezüglich $\|\ \|_1$ und daher auch bezüglich $\|\ \|_\infty$ mit den Folgegliedern

$$\boldsymbol{w}_i = a_{1i}\boldsymbol{v}_1 + a_{2i}\boldsymbol{v}_2 + \cdots + a_{n-1i}\boldsymbol{v}_{n-1}.$$

Aus Beispiel 1 wissen wir, dass W bezüglich $\|\ \|_\infty$ vollständig ist, und wir setzen

$$\boldsymbol{w} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_{n-1}\boldsymbol{v}_{n-1},$$

mit $\lim_{i\to\infty} a_{ji} = a_j \in K$ für $j = 1, \ldots, n-1$. Es ist dann $\boldsymbol{w} = \lim_{i\to\infty} \boldsymbol{w}_i$ bezüglich $\|\ \|_\infty$ und auch bezüglich $\|\ \|_1$, die Normen sind ja auf W äquivalent.

Der affine Raum $\boldsymbol{v}_n + W$ ist ebenfalls vollständig, und da jeder vollständige Teilraum eines metrischen Raumes abgeschlossen ist, ist $\boldsymbol{v}_n + W$ abgeschlossen in V.

Es ist $0 \notin \boldsymbol{v}_n + W$, denn wäre dies der Fall, dann könnten wir eine Linearkombination finden, sodass

$$0 = \boldsymbol{v}_n + a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_{n-1}\boldsymbol{v}_{n-1}$$

mit $a_i \in K$ für $i = 1, \ldots, n-1$ erfüllt ist. Dies widerspräche aber der Voraussetzung, dass die Menge $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$ als Basis von V linear unabhängig ist.

Daher ist 0 im Komplement von $\boldsymbol{v}_n + W$ enthalten. Dieses Komplement ist offen in V, es gibt also eine bezüglich $\|\ \|_1$ offene Kugel $B_{r_n}(0) = \{\boldsymbol{v} \in V : \|\boldsymbol{v} - 0\|_1 < r_n\}$ um Null, die ganz in ihm enthalten ist. Das bedeutet aber auch, dass alle $\boldsymbol{w} \in \boldsymbol{v}_n + W$ einen „Mindestabstand“ von Null haben:

$$\|\boldsymbol{w}\|_1 = \|\boldsymbol{w} - 0\|_1 \geq r_n.$$

Für beliebige $a_i \in K$ ist also

$$\|a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_{n-1}\boldsymbol{v}_{n-1} + \boldsymbol{v}_n\|_1 \geq r_n.$$

Daraus folgt auch, dass für alle $\boldsymbol{v} \in V$

$$\|\boldsymbol{v}\|_1 = \|a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_{n-1}\boldsymbol{v}_{n-1} + a_n\boldsymbol{v}_n\|_1 \geq |a_n|\, r_n$$

gilt: Für $a_n = 0$ ist die Ungleichung klarerweise erfüllt, und für $a_n \neq 0$ erhalten wir durch Division wieder die Ungleichung

$$\left\| \frac{a_1}{a_n}\boldsymbol{v}_1 + \frac{a_2}{a_n}\boldsymbol{v}_2 + \cdots + \frac{a_{n-1}}{a_n}\boldsymbol{v}_{n-1} + \boldsymbol{v}_n \right\|_1 \geq r_n.$$

Führen wir analoge Überlegungen für die anderen $(n-1)$-dimensionalen Teilräume von V durch, die von jeweils $(n-1)$ Basisvektoren aufgespannt werden, so sehen wir, dass jedes $\boldsymbol{v} \in V$ insgesamt $\binom{n}{n-1} = n$ Ungleichungen der Form

$$\|\boldsymbol{v}\|_1 = \|a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_{n-1}\boldsymbol{v}_{n-1} + a_n\boldsymbol{v}_n\|_1 \geq |a_i|\, r_i,$$

für $i = 1, \ldots, n$ genügt, wobei alle r_i positiv und von $\boldsymbol{v}$ unabhängig sind. Wir setzen $c_1 = \min_{1\leq i\leq n} r_i$ und erhalten somit

$$\|\boldsymbol{v}\|_1 = \|a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_{n-1}\boldsymbol{v}_{n-1} + a_n\boldsymbol{v}_n\|_1 \geq c_1 \|\boldsymbol{v}\|_\infty$$

mit $\|\boldsymbol{v}\|_\infty = \max_{1\leq i\leq n} |a_i|$.

Damit haben wir gezeigt, dass jede beliebige Norm auf V der Supremumsnorm äquivalent ist. Die Aussage über die Vollständigkeit ergibt sich direkt aus dieser Tatsache.

Da leicht einzusehen ist, dass die Äquivalenz von Normen eine Äquivalenzrelation darstellt, folgt außerdem, dass je zwei Normen $\|\ \|_1$ und $\|\ \|_2$ auf V äquivalent sind. □

Proposition 2: Es sei K ein lokalkompakter, vollständiger, bewerteter Körper und V ein endlichdimensionaler Vektorraum über K. Dann ist V lokalkompakt.

Beweis. Wir wählen für unsere Betrachtungen wiederum die Supremumsnorm $\| \|_\infty$. Es sei darauf hingewiesen, dass lokale Kompaktheit eine topologische Eigenschaft ist, und wir deshalb nach Satz 1 mit jeder anderer Norm auf V zu dem selben Resultat gelangen würden.

Wie in Satz 2 auf Seite 46 genügt es zu zeigen, dass die abgeschlossene Einheitskugel

$$\overline{B}_1(0) = \{\boldsymbol{v} \in V : \ \|\boldsymbol{v}\|_\infty \leq 1\}$$

in V kompakt ist. Für ein beliebiges $\boldsymbol{v} \in V$ finden wir dann eine kompakte Umgebung durch die stetige Verschiebung $\boldsymbol{v} + \overline{B}_1(0)$.

Ist $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$ eine Basis von V, so liegt $\boldsymbol{v} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$ in $\overline{B}_1(0)$ genau dann, wenn $\|\boldsymbol{v}\|_\infty = \max_{1\leq i\leq n}|a_i| \leq 1$ erfüllt ist, das heißt, alle a_i müssen in der abgeschlossenen Einheitskugel in K liegen.

Da K nach Voraussetzung lokalkompakt ist, besitzt 0 eine kompakte Umgebung U. Dann gibt es ein $r > 0$, sodass $\overline{B}_r(0) \subseteq U$ ist.

Wählen wir nun ein $a \in K$ so, dass $|a| \geq \frac{1}{r}$ gilt, dann ist auch aU kompakt, und es folgt $\overline{B}_1(0) \subseteq a\overline{B}_r(0) \subseteq aU$. Das heißt, die abgeschlossene Einheitskugel in K ist kompakt.

Um die Kompaktheit von $\overline{B}_1(0)$ in V zu zeigen, genügt es zu beweisen, dass $\overline{B}_1(0)$ vollständig und total beschränkt ist.

Wegen Satz 1 wissen wir bereits, dass V vollständig ist. Da $\overline{B}_1(0)$ eine abgeschlossene Teilmenge eines vollständigen Raumes ist, ist auch $\overline{B}_1(0)$ vollständig.

Um zu zeigen, dass $\overline{B}_1(0)$ total beschränkt ist, benutzen wir die Tatsache, dass die abgeschlossene Einheitskugel in K kompakt und daher total beschränkt ist. Es sei

$$\{B_\epsilon(c_1)\,,\ B_\epsilon(c_2)\,,\ \ldots,\ B_\epsilon(c_N)\}$$

eine endliche Überdeckung von $\overline{B}_1(0)$ in K.

Für $\nu : \{1, \ldots, n\} \to \{1, \ldots, N\}$ sei $\boldsymbol{w}_\nu = c_{\nu(1)}\boldsymbol{v}_1 + c_{\nu(2)}\boldsymbol{v}_2 + \cdots + c_{\nu(n)}\boldsymbol{v}_n$. Dann ist

$$\{B_\epsilon(\boldsymbol{w}_\nu) : \ \nu : \{1, \ldots, n\} \to \{1, \ldots, N\}\}$$

eine endliche Überdeckung der abgeschlossenen Einheitskugel in V. Denn ist $\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n$ ein beliebiges Element in $\overline{B}_1(0)$, dann gibt es für alle i, da ja a_i in der abgeschlossenen Einheitskugel in K liegt, ein $\nu(i) \in \{1, \ldots, N\}$ mit $\left|c_{\nu(i)} - a_i\right| < \epsilon$. Daraus folgt wegen

$$\|\boldsymbol{w}_\nu - \boldsymbol{v}\|_\infty = \max_{1\leq i\leq n}\left|c_{\nu(i)} - a_i\right| < \epsilon,$$

dass $\boldsymbol{v}$ in der offenen Kugel $B_\epsilon(\boldsymbol{w}_\nu)$ liegt. □

Bemerkung 1: Es gilt auch die Umkehrung, nämlich, dass jeder lokalkompakte, normierte Vektorraum über K endlichdimensional ist (siehe zum Beispiel [18], S. 93).

5.2 Die Norm einer Köpererweiterung

In diesem Abschnitt wiederholen wir einige Grundbegriffe aus der Theorie algebraischer Körpererweiterungen um uns schließlich mit der Norm eines algebraischen Elements zu beschäftigen. Es sei darauf hingewiesen, dass auch in diesem Kontext die Bezeichnung „Norm“ eine lange Tradition besitzt, obwohl sie etwas wesentlich anderes darstellt als die Norm auf einem Vektorraum aus Definition 1 auf Seite 75.

Es sei K ein Körper, der F als Teilkörper enthält. Dann heißt K *ein Erweiterungs- oder Oberkörper von* F, und das Paar $F \subseteq K$ wird *eine Körpererweiterung* genannt. Es ist in der Literatur weit verbreitet, dafür K/F („K über F“) zu schreiben.

Es gilt $\operatorname{char}(K) = \operatorname{char}(F)$, wobei char die Charakteristik von K beziehungsweise F bezeichnet.

Ist K/F eine Körpererweiterung, so kann K auch als Vektorraum über F angesehen werden. Die Dimension dieses Vektorraums bezeichnen wir als *den Grad der Körpererweiterung* $[K : F]$, das heißt,

$$[K : F] := \dim_F K.$$

Wir sprechen von einer endlichen Körpererweiterung, wenn $[K : F]$ endlich ist.

Eine Körpererweiterung K/F heißt *einfach*, wenn sich durch Adjunktion eines Elements α entsteht, es ist dann also $K = F(\alpha)$, und α wird *primitives Element* genannt. Hat F die Charakteristik 0, so ist jede endliche Körpererweiterung einfach.

Ein Element $\alpha \in K$ heißt *algebraisch* über F, wenn es ein $f(X) \in F[X]$ gibt, sodass α Nullstelle dieses Polynoms und $f \neq 0$ ist. Es gibt dann ein eindeutig bestimmtes, normiertes Polynom kleinsten Grades mit dieser Eigenschaft. Dieses heißt *das Minimalpolynom von* α *über* F. Eine Körpererweiterung K heißt algebraisch über F, wenn alle $\alpha \in K$ algebraisch sind. Jede endliche Körpererweiterung ist algebraisch.

Aus Definition 3 auf Seite 53 wissen wir, dass ein Körper F genau dann algebraisch abgeschlossen ist, wenn jedes nichtkonstante Polynom $f(X)$ über F vollständig in Linearfaktoren zerfällt. Wir können das auch so ausdrücken: F ist genau dann algebraisch abgeschlossen, wenn es keine echte algebraische Körpererweiterung K/F gibt.

Ein Erweiterungskörper $\overline{F}$ heißt *algebraischer Abschluss von* F, wenn die Körpererweiterung $\overline{F}/F$ algebraisch und $\overline{F}$ algebraisch abgeschlossen ist.

Der sogenannte *Gradsatz* besagt, dass sich für eine Kette endlicher Körpererweiterung $F \subseteq M \subseteq K$ der Grad der Erweiterung von K/F durch $[K : F] = [K : M][M : F]$ ergibt.

Ist $\{x_1, \ldots, x_n\}$ dann eine Basis von K über M und $\{y_1, \ldots, y_m\}$ eine Basis von M über F, so bilden die Produkte $\{y_1x_1, \ldots, y_jx_i, \ldots, y_mx_n\}$ eine Basis von K über F.

Eine algebraische Körpererweiterung K/F heißt *normal*, wenn jedes irreduzible Polynom $f(X)$ aus $F[X]$, das in K eine Nullstelle besitzt, über K vollständig in Linearfaktoren zerfällt. Das heißt, es liegen dann alle Nullstellen von $f(X)$ in K.

Zu einer algebraischen Körpererweiterung K/F, die nicht normal ist, können wir immer einen Oberkörper L von K finden, sodass L algebraisch über K und normal über F ist. Der kleinste Erweiterungskörper mit dieser Eigenschaft heißt *die normale Hülle*.

Ist $\overline{K}$ ein algebraischer Abschluss von K, dann gilt für eine normale Körpererweiterung K/F, dass jeder Homomorphismus $\sigma : K \to \overline{K}$, der eingeschränkt auf F die Identität darstellt, ein Automorphismus von K ist. Wir können also die Menge dieser Homomorphismen mit der

Gruppe $\mathrm{Aut}_F(K)$ identifizieren, also jener Automorphismen auf K, welche die Identität $F \to F$ fortsetzen.

Zwei Elemente $\alpha_1, \alpha_2 \in K$ heißen *konjugiert über* F, wenn sie Wurzeln desselben Minimalpolynoms über F sind. Ist K/F eine normale, einfache Körpererweiterung vom Grad n mit primitivem Element α und sind $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ die Konjugierten von $\alpha = \alpha_1$ und alle verschieden, dann gibt es genau n Automorphismen $\sigma_i \in \mathrm{Aut}_F(K)$, die durch $\sigma_i(\alpha) = \alpha_i$, $i = 1, \ldots, n$ eindeutig bestimmt sind.

Eine algebraische Körpererweiterung K/F heißt *separabel*, wenn das Minimalpolynom eines jeden Elements $\alpha \in K$ separabel über F ist, wobei ein Polynom separabel genannt wird, wenn es in seinem Zerfällungskörper nur einfache Nullstellen besitzt. Ist $\mathrm{char}(F) = 0$, so ist jede algebraische Körpererweiterung K/F separabel. Eine algebraische Körpererweiterung K/F heißt *galoissch*, wenn sie normal und separabel ist. In diesem Fall wird $\mathrm{Aut}_F(K)$ als *die Galois-Gruppe* der Körpererweiterung bezeichnet und als $\mathrm{Gal}(K/F)$ geschrieben.

Als Nächstes befassen wir uns mit der Norm einer Köpererweiterung:

Definition 3: Es sei K ein Erweiterungskörper von F, und der Grad n dieser Körpererweiterung sei endlich. Wir betrachten für $\alpha \in K$ die F-lineare Abbildung

$$\varphi_\alpha : K \to K, \qquad x \mapsto \alpha x.$$

Es sei $\mathcal{A}_\alpha$ die Matrix von φ_α bezüglich irgendeiner Basis. Dann heißt ihre Determinante *die Norm von α bezüglich der Körpererweiterung K/F*, und wir schreiben $\mathcal{N}_{K/F}(\alpha)$ für diese Norm. Es gilt also

$$\mathcal{N}_{K/F}(\alpha) = \det \mathcal{A}_\alpha.$$

Diese Definition ist unabhängig von der Wahl der Basis, denn ist $\mathcal{A}'_\alpha$ die Matrix von φ_α bezüglich einer anderen Basis, so gilt $M^{-1}\mathcal{A}'_\alpha M = \mathcal{A}_\alpha$ für eine Matrix M zum Basiswechsel.

Wir sehen sofort, dass $\mathcal{N}_{K/F}(\alpha\beta) = \mathcal{N}_{K/F}(\alpha)\mathcal{N}_{K/F}(\beta)$ für alle $\alpha, \beta \in K$ gilt, denn die Matrix, welche die Multiplikation mit $\alpha \cdot \beta$ darstellt, ist durch das Produkt der Matrizen $\mathcal{A}_\alpha$ und $\mathcal{A}_\beta$ gegeben, und die Determinante eines Produkts von Matrizen ist gleich dem Produkt der Determinanten.

Außerdem ist $\mathcal{N}_{K/F}(\alpha) = \alpha^n$ für $\alpha \in F$, denn in diesem Fall wird die Abbildung φ_α durch das α-fache der Einheitsmatrix beschrieben.

Proposition 3: Es sei F ein Körper der Charakteristik 0 und $K = F(\alpha)$. Der Erweiterungskörper K von F wird also von nur einem Element erzeugt. Der Grad dieser Körpererweiterung sei n, und das Minimalpolynom von α sei $X^n + a_1 X^{n-1} + \cdots + a_n$ mit $a_i \in F$ und habe n verschiedene Konjugierte. Dann ist

$$\mathcal{N}_{K/F}(\alpha) = (-1)^n a_n = \prod_{i=1}^{n} \alpha_i,$$

wobei die Elemente α_i, $i = 1, \ldots, n$ die Konjugierten von $\alpha = \alpha_1$ über F darstellen.

Beweis. Die zweite Gleichheit folgt unmittelbar durch Koeffizientenvergleich aus:

$$X^n + a_1 X^{n-1} + \cdots + a_n = \prod_{i=1}^{n} (X - \alpha_i).$$

Um $\mathcal{N}_{K/F}(\alpha) = (-1)^n a_n$ zu zeigen, wählen wir $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ als Basis von K über F. Dann hat die Matrix, die die Multiplikation eines Elements von K mit α darstellt, die Gestalt

$$\mathcal{A}_\alpha = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & & 0 & -a_{n-1} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 0 & -a_2 \\ 0 & \cdots & 0 & 1 & -a_1 \end{pmatrix},$$

wobei wir berücksichtigen, dass $\alpha^n = -a_1\alpha^{n-1} - \cdots - a_{n-1}\alpha - a_n$ gilt. Wenn wir bei der Berechnung der Determinante von $\mathcal{A}_\alpha$ nach der ersten Zeile entwickeln, sehen wir leicht, dass $\det \mathcal{A}_\alpha = (-1)^n a_n$ gilt.

Proposition 4: Es sei K/F eine endliche Körpererweiterung, $\operatorname{char}(K) = 0$ und $\alpha \in K$. Dann ist

$$\mathcal{N}_{K/F}(\alpha) = \left(\mathcal{N}_{F(\alpha)/F}(\alpha)\right)^{[K:F(\alpha)]}.$$

Beweis. Es ist $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ eine Basis von $F(\alpha)$ als Vektorraum über F, und es sei $\{\beta_1, \beta_2, \ldots, \beta_s\}$ eine Basis von K als Vektorraum über $F(\alpha)$, wobei $s = [K : F(\alpha)] = \dim_{F(\alpha)} K$ gelte. Nach dem Gradsatz bildet die Menge

$$\{\beta_1, \alpha\beta_1, \ldots, \alpha^{n-1}\beta_1, \ldots, \beta_s, \alpha\beta_s, \ldots, \alpha^{n-1}\beta_s\}$$

eine Basis von K über F.

Es ist dann $\varphi_\alpha(\alpha^i\beta_j) = \alpha^{i+1}\beta_j$ mit φ_α wie in Definition 3. Wir sehen, dass diese Multiplikation nur auf α^i Einfluss nimmt, β_j bleibt gleich.

Berücksichtigen wir wieder, dass $\alpha^n = -a_1\alpha^{n-1} - \cdots - a_{n-1}\alpha - a_n$ gilt, dann beschreibt die Matrix $\mathcal{A}_\alpha = (a_{lk})_{0\le l,k\le n-1}$ aus dem Beweis der letzten Proposition die Multiplikation mit α auf $F(\alpha)$.

Die Matrix, welche die Multiplikation bezüglich der Basis $\{\beta_1, \alpha\beta_1, \ldots, \alpha^{n-1}\beta_s\}$ darstellt, bezeichnen wir mit $\mathcal{B}_\alpha$, und es ist

$$\mathcal{B}_\alpha = \begin{pmatrix} \mathcal{A}_\alpha & & & 0 \\ & \mathcal{A}_\alpha & & \\ & & \ddots & \\ 0 & & & \mathcal{A}_\alpha \end{pmatrix}$$

mit s Blöcken $\mathcal{A}_\alpha$ in der Diagonalen und Nullen sonst. Denn es ist nun leicht ersichtlich, dass sich φ_α auf K für $i = 0, \ldots, n-1$ folgendermaßen beschreiben lässt:

$$\varphi_\alpha : \alpha^i\beta_j \mapsto \left(a_{0i}\alpha^0 + a_{1i}\alpha^1 + \cdots + a_{(n-1)i}\alpha^{n-1}\right)\beta_j,$$

wobei $\left(a_{0i}, a_{1i}, \ldots, a_{(n-1)i}\right)^T$ genau die $(i+1)$-te Spalte von $\mathcal{A}_\alpha$ dargestellt. Somit folgt

$$\mathcal{N}_{K/F}(\alpha) = \det \mathcal{B}_\alpha = (\det \mathcal{A}_\alpha)^s = \left(\mathcal{N}_{F(\alpha)/F}(\alpha)\right)^s. \qquad \square$$

Bemerkung 2: Ist $F \subseteq M \subseteq K$ eine Kette endlicher Körpererweiterungen von Körpern der Charakteristik 0, so gilt

$$\mathcal{N}_{K/F}(\alpha) = \mathcal{N}_{M/F}\left(\mathcal{N}_{K/M}(\alpha)\right).$$

Es sei nämlich zunächst $\alpha \in F$. Dann ist $\mathcal{N}_{M/F}(\alpha) = \alpha^{[M:F]}$.

Nun sei $\alpha \in K$ beliebig, und wir nehmen an, dass $M = F(\alpha)$ ist. Dann folgt mit Proposition 4:

$$\mathcal{N}_{K/F}(\alpha) = \left(\mathcal{N}_{F(\alpha)/F}(\alpha)\right)^{[K:F(\alpha)]} = \underbrace{\left(\mathcal{N}_{F(\alpha)/F}(\alpha)\right)\cdots\left(\mathcal{N}_{F(\alpha)/F}(\alpha)\right)}_{[K:F(\alpha)] \text{ mal}}$$
$$= \mathcal{N}_{F(\alpha)/F}\left(\alpha^{[K:F(\alpha)]}\right) = \mathcal{N}_{F(\alpha)/F}\left(\mathcal{N}_{K/F(\alpha)}(\alpha)\right).$$

5.3 Endliche Körpererweiterungen über $\mathbb{Q}_p$

5.3.1 Die Fortsetzung des *p*-adischen Absolutbetrags $|\ |_p$

Nun wollen wir uns Erweiterungskörpern der p-adischen Zahlen widmen und uns insbesondere überlegen, ob sich auf diesen der p-adische Absolutbetrag fortsetzen lässt.

Es sei also K ein Erweiterungsköper von $\mathbb{Q}_p$. Dann ist $\operatorname{char}(K) = \operatorname{char}(\mathbb{Q}_p) = 0$, und wir nehmen an, dass $[K : \mathbb{Q}_p] = \dim_{\mathbb{Q}_p} K$ endlich ist.

Für einen Absolutbetrag $|\ |$ auf K gelten die uns bereits bekannten Eigenschaften aus Definition 1 auf Seite 7, nämlich

(A1) $|x| \geq 0$ für alle $x \in K$, $|x| = 0 \iff x = 0$,

(A2) $|xy| = |x|\,|y|$ für alle $x,\ y \in K$,

(A3) $|x + y| \leq |x| + |y|$ für alle $x,\ y \in K$.

Setzt $|\ |$ den p-adischen Absolutbetrag $|\ |_p$ fort, muss zusätzlich noch folgende Bedingung erfüllt sein:

$$|\lambda| = |\lambda|_p \text{ für alle } \lambda \in \mathbb{Q}_p.$$

Proposition 3 auf Seite 10 besagt, dass ein Absolutbetrag genau dann nichtarchimedisch ist, wenn sein Wert für alle ganzen Zahlen n kleiner als Eins oder höchsten Eins ist. Wenn wir nun bedenken, dass $\mathbb{Z}$ in $\mathbb{Q}_p$ enthalten ist, folgt unmittelbar für jeden Absolutbetrag $|\ |$ auf K, der $|\ |_p$ fortsetzt, dass auch er nichtarchimedisch ist, denn für alle $n \in \mathbb{Z}$ gilt dann $|n| = |n|_p \leq 1$.

Da wir wissen, dass K im Falle einer Körpererweiterung $K/\mathbb{Q}_p$ auch als Vektorraum über $\mathbb{Q}_p$ angesehen werden kann, stellt sich die Frage nach einem Zusammenhang zwischen dem Absolutbetrag des Köpers K und der Norm des Vektorraums K. Vergleichen wir also (A1)-(A3) mit (N1)-(N3) aus Definition 1 auf Seite 75, so sehen wir, dass sich diese Eigenschaften fast entsprechen, und sie stimmen sogar überein, wenn wir in (A2) die Multiplikation auf K zu einer Multiplikation $\mathbb{Q}_p \times K \to K$ einschränken.

Halten wir also fest, dass jeder Absolutbetrag auf K auch als Norm auf einem Vektorraum angesehen werden kann. Natürlich ist nicht jede solche Norm ein Absolutbetrag.

Mit diesem Wissen folgt aus Abschnitt 5.1 nun unmittelbar, dass unter der Voraussetzung, dass $[K : \mathbb{Q}_p]$ endlich ist, ein Erweiterungsköper K von $\mathbb{Q}_p$ bezüglich eines auf ihm definierten Absolutbetrags $|\,|$ vollständig ist. Insbesondere ist K dann bezüglich einer Fortsetzung des p-adischen Absolutbetrags vollständig.

Weiters entspricht die von $|\,|$ am Erweiterungskörper induzierte Topologie der Topologie von K als normierten Vektorraum über $\mathbb{Q}_p$, denn auf einem endlichdimensionalen Vektorraum sind alle Normen äquivalent. Die Topologie am Erweiterungskörper ist also unabhängig von der speziellen Wahl eines Absolutbetrags.

Proposition 5: Es sei $K/\mathbb{Q}_p$ eine endliche Körpererweiterung. Dann gibt es höchstens einen Absolutbetrag auf K, der den p-adischen Absolutbetrag $|\,|_p$ fortsetzt.

Beweis. Es seien $|\,|_1$ und $|\,|_2$ zwei Absolutbeträge auf K, und wir nehmen an, dass beide den p-adischen Absolutbetrag $|\,|_p$ fortsetzen.

Als Normen eines Vektorraums betrachtet, sind $|\,|_1$ und $|\,|_2$ äquivalent. Daher gibt es nach Proposition 1 auf Seite 77 zwei reelle Konstanten c_1, c_2 mit $0 < c_1 \leq c_2 < \infty$, sodass für alle $x \in K$

$$c_1 \left|x\right|_2 \leq \left|x\right|_1 \leq c_2 \left|x\right|_2$$

erfüllt ist. Für ein beliebiges $n \in \mathbb{N}$ können wir x durch x^n ersetzen – die Ungleichung gilt ja für alle Elemente des Körpers. So erhalten wir

$$c_1 \left|x^n\right|_2 \leq \left|x^n\right|_1 \leq c_2 \left|x^n\right|_2 .$$

Da es sich bei $|\,|_1$ und $|\,|_2$ um Absolutbeträge handelt, folgt mit (A2)

$$c_1 \left|x\right|_2^n \leq \left|x\right|_1^n \leq c_2 \left|x\right|_2^n ,$$

und das entpricht

$$\sqrt[n]{c_1} \left|x\right|_2 \leq \left|x\right|_1 \leq \sqrt[n]{c_2} \left|x\right|_2 .$$

Dies gilt für alle n, und da für $n \to \infty$ sowohl $\sqrt[n]{c_1} \to 1$ als auch $\sqrt[n]{c_2} \to 1$ konvergiert, folgt für alle $x \in K$

$$\left|x\right|_1 = \left|x\right|_2 . \qquad \square$$

Dieses Resultat zeigt die Eindeutigkeit einer Fortsetzung des p-adischen Absolutbetrags auf einem Erweiterungskörper, nicht aber deren Existenz. Unser nächstes Ziel ist es daher, uns davon zu überzeugen, dass es so eine Fortsetzung tatsächlich gibt, und das machen wir, indem wir sie konstruieren. Eine wichtige Rolle dabei spielt die Norm auf einer Körpererweiterung aus Abschnitt 5.2.
Wir betrachten zunächst eine endliche, normale Körpererweiterung $K/\mathbb{Q}_p$, von der wir wissen, dass sie von einem Element α erzeugt wird, das heißt, $K = \mathbb{Q}_p(\alpha)$. Es sei $[K : \mathbb{Q}_p] = n$ und $|\,|$ ein Absolutbetrag auf K, der den p-adischen Absolutbetrag fortsetzt. Da die Körpererweiterung normal ist, liegen auch alle Konjugierten $\alpha_1, \ldots, \alpha_n$ von $\alpha = \alpha_1$ in K.

Es sei $\sigma' \in \mathrm{Gal}(K/\mathbb{Q}_p)$, dann ist $\sigma'(\alpha) = \alpha_j$ für ein $j \in \{1, \ldots, n\}$. Betrachten wir nun eine Abbildung $|\,|' : K \to \mathbb{R}$, $x \mapsto \left|\sigma'(x)\right|$, so definiert auch diese einen Absolutbetrag auf K.

Das ist leicht einzusehen, denn $\sigma^{'}$ ist ein Automorphismus, daher gilt für alle $x,\ y \in K$: $|xy|^{'} = \left|\sigma^{'}(xy)\right| = \left|\sigma^{'}(x)\,\sigma^{'}(y)\right| = \left|\sigma^{'}(x)\right|\left|\sigma^{'}(y)\right| = |x|^{'}|y|^{'}$ sowie $|x+y|^{'} = \left|\sigma^{'}(x+y)\right| = \left|\sigma^{'}(x)+\sigma^{'}(y)\right| \leq \left|\sigma^{'}(x)\right| + \left|\sigma^{'}(y)\right| = |x|^{'} + |y|^{'}$, und es ist klarerweise auch (A1) erfüllt.

Insbesondere ist aber $|\lambda|^{'} = \left|\sigma^{'}(\lambda)\right| = |\lambda| = |\lambda|_p$ für $\lambda \in \mathbb{Q}_p$, denn $\sigma^{'}$ entspricht auf $\mathbb{Q}_p$ der Identität. In Proposition 5 haben wir gezeigt, dass höchstens ein Absolutbetrag am Erweiterungskörper den p-adischen Absolutbetrag $\left|\ \right|_p$ fortsetzen kann, und das bedeutet, dass $|x| = |x|^{'}$ für alle $x \in K$ gilt.

Für die anderen Automorphismen aus $\mathrm{Gal}(K/\mathbb{Q}_p)$ gilt entsprechendes, daher folgt für das Produkt über alle $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q}_p)$, $i = 1, \ldots, n$

$$\left|\prod_{\sigma_i} \sigma_i(x)\right| = |x|^n,$$

und das gilt für alle $x \in K$.

Vergleichen wir die linke Seite dieser Gleichung mit Proposition 3, dann folgt insgesamt, dass

$$|x|^n = \left|\mathcal{N}_{K/\mathbb{Q}_p}(x)\right|$$

beziehungsweise

$$|x| = \sqrt[n]{\left|\mathcal{N}_{K/\mathbb{Q}_p}(x)\right|}$$

für alle $x \in K$ ist.

Die Berechnung des Absolutbetrags eines jeden Elementes x in K wird also auf die Berechnung des p-adischen Absolutbetrags $|\ |_p$ eines Elementes $\lambda = \mathcal{N}_{K/\mathbb{Q}_p}(x)$, welches in $\mathbb{Q}_p$ liegt, zurückgeführt, denn die Norm stellt eine Funktion von K nach $\mathbb{Q}_p$ dar. Daher gilt

$$|x| = \sqrt[n]{\left|\mathcal{N}_{K/\mathbb{Q}_p}(x)\right|} = \sqrt[n]{\left|\mathcal{N}_{K/\mathbb{Q}_p}(x)\right|_p}.$$

Sind K und L zwei Erweiterungsköper von $\mathbb{Q}_p$, wobei $\mathbb{Q}_p \subseteq L \subseteq K$ gelte, $|\ |_L$ ein Absolutbetrag auf L und $|\ |_K$ einer auf K, die jeweils den p-adischen Absolutbetrag fortsetzen, dann folgt für $x \in L$ wegen der Eindeutigkeit der Fortsetzung aus Proposition 5, dass $|x|_L = |x|_K$ ist. Diese Überlegung stimmt auch mit den Eigenschaften der Norm überein:

Proposition 6: Es seien L und K zwei Erweiterungskörper von $\mathbb{Q}_p$ und zwar so, dass $\mathbb{Q}_p \subseteq L \subseteq K$ gilt und $n = [K : \mathbb{Q}_p]$ endlich ist. Dann gilt für $x \in L$

$$\sqrt[m]{\left|\mathcal{N}_{L/\mathbb{Q}_p}(x)\right|_p} = \sqrt[n]{\left|\mathcal{N}_{K/\mathbb{Q}_p}(x)\right|_p},$$

wobei $m = [L : \mathbb{Q}_p]$ ist.

Beweis. Nach Bemerkung 2 auf Seite 84 gilt

$$\mathcal{N}_{K/\mathbb{Q}_p}(x) = \mathcal{N}_{L/\mathbb{Q}_p}\left(\mathcal{N}_{K/L}(x)\right)$$

sowie $\mathcal{N}_{K/L}(x) = x^{[K:L]}$, und wegen des Gradsatzes ist $n = [K : L] \cdot m$. Insgesamt ergibt das

$$\mathcal{N}_{K/\mathbb{Q}_p}(x) = \left(\mathcal{N}_{L/\mathbb{Q}_p}(x)\right)^{\frac{n}{m}},$$

und wenn wir davon den Absolutbetrag nehmen, so folgt unmittelbar die Gleichung. □

Das bedeutet also, dass der Wert des Absolutbetrag eines Elementes x in allen Erweiterungskörpern, die x enthalten, gleich ist. Insbesondere gilt das auch für nicht normale Körpererweiterungen.

Zusammenfassend können wir daher sagen:

Gibt es auf einem Erweiterungskörper K von $\mathbb{Q}_p$ einen Absolutbetrag, der den p-adischen Absolutbetrag $|\,|_p$ fortsetzt, so muss dieser durch die Formel

$$|x| = \sqrt[n]{\left|\mathcal{N}_{K/\mathbb{Q}_p}(x)\right|_p}$$

gegeben sein, wobei $n = [K : \mathbb{Q}_p]$ endlich ist.

Wir benötigen noch das folgende Resultat, um dann endlich in der Lage zu sein, die Existenz dieser Fortsetzung zu beweisen:

Lemma 1: Es sei $K/\mathbb{Q}_p$ eine endliche Körpererweiterung. Für $x \in K$ definieren wir

$$|x| = \left|\mathcal{N}_{K/\mathbb{Q}_p}(x)\right|_p^{1/[K:\mathbb{Q}_p]}.$$

Ist $|\gamma| \leq 1$ für ein $\gamma \in K$, dann ist auch $|\gamma + 1| \leq 1$.

Beweis. Es sei $K = \mathbb{Q}_p(\gamma)$ und $n = [K : \mathbb{Q}_p]$. $\Gamma := \left\{1, \gamma, \ldots, \gamma^{n-1}\right\}$ ist eine Basis von K als Vektorraum über $\mathbb{Q}_p$.

Für ein Element $\alpha \in K$, $\alpha = \sum_{i=0}^{n-1} a_i\gamma^i$ sei die Supremumsnorm $\|\ \|_\infty$ wie in Beispiel 1 auf Seite 77 definiert, also durch

$$\|\alpha\|_\infty = \max_{0\leq i<n} |a_i|_p,$$

und unter der Supremumsnorm einer $n \times n$ Matrix $A = (\alpha_{ij})_{1\leq i,j\leq n}$ mit $a_{ij} \in \mathbb{Q}_p$ für alle i, j verstehen wir Folgendes:

$$\|A\|_\infty := \max_{1\leq i,j\leq n} |a_{ij}|_p.$$

Ist $\varphi : K \to K$, $\varphi(x) = \gamma x$, so sei $\mathcal{A}$ die Matrix von φ in Bezug auf Γ. Dann entspricht $\mathcal{A}^i$ der Multiplikation mit γ^i sowie $(I_n + \mathcal{A})$ jener mit $1 + \gamma$.

Wir betrachten eine Folge $\left(\left\|\mathcal{A}^i\right\|_\infty\right)_{i\geq 0}$. Diese ist beschränkt, was wir nun indirekt zeigen wollen. Wir nehmen also an, die Folge sei unbeschränkt. Dann können wir für jedes $k \geq 0$ ein Folgeglied finden, sodass $\left\|\mathcal{A}^{i_k}\right\|_\infty > k$ erfüllt ist. Es sei $(b_k)_{k\geq 0} := \left(\left\|\mathcal{A}^{i_k}\right\|_\infty\right)_{k\geq 0}$ die so gefundene Teilfolge, und β_k ein Eintrag von $\mathcal{A}^{i_k}$ mit $|\beta_k|_p = \left\|\mathcal{A}^{i_k}\right\|_\infty > k$.

Wir setzen $\mathcal{B}_k := \frac{1}{\beta_k}\mathcal{A}^{i_k}$. Dann ist klarerweise $\|\mathcal{B}_k\|_\infty = 1$ für alle k, und das bedeutet, dass $\mathcal{B}_k$ in der bezüglich $\|\ \|_\infty$ kompakten Einheitskugel liegt. Wir können also eine konvergente Teilfolge $(\mathcal{B}_{k_s})_{s\geq 0}$ finden, und den Grenzwert dieser Folge bezeichnen wir mit $\mathcal{B}$. Es ist dann $\|\mathcal{B}\|_\infty = 1$.

Für alle $k \in \mathbb{N}$, $k \neq 0$ und $|\gamma|_p \leq 1$ gilt

$$\begin{aligned}|\det \mathcal{B}_k|_p &= \frac{1}{|\beta_k|_p^n} \left|\det \mathcal{A}^{i_k}\right|_p = \frac{1}{|\beta_k|_p^n} \left|\mathcal{N}_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(\gamma)\right|_p^{i_k} \\ &= \frac{1}{|\beta_k|_p^n} |\gamma|^{ni_k} < \frac{1}{k^n}.\end{aligned}$$

Betrachten wir die Teilfolge $(\mathcal{B}_{k_s})_{s\geq 0}$, so folgt $\det \mathcal{B} = \lim_{s\to\infty} \det \mathcal{B}_{k_s} = 0$, und wir werden nun zeigen, dass dann auch $\mathcal{B} = 0$ ist.

Zunächst sei darauf hingewiesen, dass $\mathcal{B}\mathcal{A}^i = \mathcal{A}^i\mathcal{B}$ gilt, denn $\mathcal{B}$ ist ja der Grenzwert von Matrizen der Form $\mathcal{B}_k = \frac{1}{\beta_k}\mathcal{A}^{i_k}$, und es ist $\mathcal{B}_k\mathcal{A}^i = \frac{1}{\beta_k}\mathcal{A}^{i_k}\mathcal{A}^i = \frac{1}{\beta_k}\mathcal{A}^{i_k+i}$.

Es sei $\psi : K \to K$ diejenige $\mathbb{Q}_p-$lineare Abbildung, die in Bezug auf Γ die Matrix $\mathcal{B}$ besitzt. Wegen $\det \mathcal{B} = 0$ gibt es ein $l \in K$ mit $\psi(l) = 0$. Da ψ mit φ vertauschbar ist, gilt für $0 \leq i < n$

$$\psi\left(\gamma^i l\right) = \psi\left(\varphi^i(l)\right) = \gamma^i(\varphi(l)) = 0.$$

Da auch die Menge $\left\{l, \gamma l, \ldots, \gamma^{n-1}l\right\}$ eine Basis von K als Vektorraum über $\mathbb{Q}_p$ bildet, muss somit $\mathcal{B} = 0$ gelten. Das widerspricht aber unserer Annahme, dass $\|\mathcal{B}\|_\infty = 1$ ist.

Daher ist $\left(\left\|\mathcal{A}^i\right\|_\infty\right)_{i\geq 0}$ beschränkt, und es sei c so eine Schranke.

Dann gilt für $N \in \mathbb{N}$, $N > 0$

$$\begin{aligned}|1+\gamma|^N &= |\det(I_n + \mathcal{A})|_p^{N/n} = \left|\det(I_n+\mathcal{A})^N\right|_p^{1/n} \\ &\leq \left\|(I_n+\mathcal{A})^N\right\|_\infty = \left\|\sum_{i=0}^{N}\binom{N}{i}\mathcal{A}^i\right\|_\infty \\ &\leq \max_{0\leq i\leq N}\left\|\mathcal{A}^i\right\|_\infty \leq c,\end{aligned}$$

wobei wir verwendet haben, dass $|\det A|_p \leq \max_{i,j}|a_{ij}|_p^n = \|A\|_\infty^n$ für eine $n\times n$ Matrix A gilt. Es ist also $|1+\gamma| \leq \sqrt[N]{c}$, und das ergibt $|1+\gamma| \leq 1$ für $N \to \infty$. □

Satz 2: Es sei $K/\mathbb{Q}_p$ eine endliche Körpererweiterung mit $[K : \mathbb{Q}_p] = n$. Dann definiert die Abbildung

$$|\,|: K \to \mathbb{R}, \qquad x \mapsto \sqrt[n]{\left|\mathcal{N}_{K/\mathbb{Q}_p}(x)\right|_p}$$

einen nichtarchimedischen Absolutbetrag auf K, der den p-adischen Absolutbetrag $|\,|_p$ fortsetzt.

Beweis. Es sei also für alle $x \in K$

$$|x| = \sqrt[n]{\left|\mathcal{N}_{K/\mathbb{Q}_p}(x)\right|_p}.$$

Für $\lambda \in \mathbb{Q}_p$ stimmt dieser Absolutbetrag mit dem p-adischen überein, denn dann gilt $\mathcal{N}_{K/\mathbb{Q}_p}(\lambda) = \lambda^n$ und somit ist $\sqrt[n]{|\lambda|_p^n} = |\lambda|_p = |\lambda|$.

Nun zeigen wir, dass für $x \in K$ die Eigenschaften (A1) und (A2) sowie die nichtarchimedische Dreiecksungleichung $|x+y| \leq \max\{|x|, |y|\}$ erfüllt sind.

Es ist $|x| = 0$ genau dann, wenn $N_{K/\mathbb{Q}_p}(x) = 0$ ist, das heißt, wenn die Multiplikation mit x nicht invertierbar ist. Da es sich bei K um einen Körper handelt, ist das nur für $x = 0$ der Fall. Damit ist (A1) gezeigt, und die Eigenschaft (A2) folgt aus

$$N_{K/\mathbb{Q}_p}(xy) = N_{K/\mathbb{Q}_p}(x)\, N_{K/\mathbb{Q}_p}(y)\,.$$

Es bleibt noch zu zeigen, dass $|x+y| \leq \max\{|x|, |y|\}$ für alle $x, y \in K$ gilt. Dazu nehmen wir o.B.d.A. an, dass $|x| \leq |y|$ ist. Wir setzen $z = \frac{x}{y}$, dann ist $|z|_p \leq 1$.

Um $|x+y| \leq |y|$ zu erhalten, genügt es also $|z+1| \leq |1|$ zu zeigen. Aber nun folgt der Satz unmittelbar aus Lemma 1. □

Für jede endliche Körpererweiterung $K/\mathbb{Q}_p$ gibt es einen eindeutig bestimmten Absolutbetrag auf dem Erweiterungskörper K, der den p-adischen Absolutbetrag $|\,|_p$ fortsetzt. Diesen bezeichnen wir wiederum als *den* p-adischen Absolutbetrag und schreiben ihn auch ab sofort als $|\,|_p$. Es ist K bezüglich dieses Absolutbetrags vollständig.

5.3.2 Eigenschaften endlicher Körpererweiterungen über $\mathbb{Q}_p$

Es sei nun also $K/\mathbb{Q}_p$ eine endliche Körpererweiterung, und $|\,|_p$ bezeichne den p-adische Absolutbetrag sowohl auf $\mathbb{Q}_p$ als auch K. Die Wertemenge von $|\,|_p$ auf $\mathbb{Q}_p$ umfasst $\{p^m : m \in \mathbb{Z}\} \cup \{0\}$. Da für $x \in K$ der Absolutbetrag gegeben ist durch $\left|\mathcal{N}_{K/\mathbb{Q}_p}(x)\right|_p^{1/n}$, ist auch die Wertemenge am Erweiterungsköper diskret und entspricht $\left\{p^m : m \in \frac{1}{n}\mathbb{Z}\right\} \cup \{0\}$.

Wir können somit die p-adische Ordnung ord_p ebenfalls auf K fortsetzen, indem wir sie für $x \in K$, $x \neq 0$ als jene eindeutig bestimmte rationale Zahl definieren, die $|x|_p = p^{-\mathrm{ord}_p(x)}$ erfüllt, sowie $\mathrm{ord}_p(x) = +\infty$ für $x = 0$ setzen.

Die p-adische Ordnung lässt sich für jedes $x \in K^\times$ durch folgenden Zusammenhang berechnen, wobei auf der rechten Seite die p-adische Ordnung auf $\mathbb{Q}_p$ aus Definition 2 auf Seite 8 gemeint ist:

$$\mathrm{ord}_p(x) = \frac{1}{n}\mathrm{ord}_p\left(N_{K/\mathbb{Q}_p}(x)\right).$$

Aus unseren Überlegungen zum p-adischen Absolutbetrag von $|\,|_p$ auf K folgt, dass die Wertemenge von ord_p in $\frac{1}{n}\mathbb{Z}$ enthalten ist, und das nächste Resultat zeigt, welcher Untergruppe sie genau entspricht:

Proposition 7: Die p-adische Ordnung ord_p ist ein Gruppenhomomorphismus

$$\mathrm{ord}_p : \left(K^\times, \cdot\right) \to (\mathbb{Q}, +)\,,$$

und das Bild dieses Homomorphismus ist von der Form $\frac{1}{e}\mathbb{Z}$, wobei e ein Teiler von $n = [K : \mathbb{Q}_p]$ ist.

Beweis. Es sei

$$f : K^\times \to \mathbb{Z}, \quad f(x) = n \cdot \mathrm{ord}_p(x)\,.$$

Das ist ein Gruppenhomomorphismus, also ist $f(K^\times)$ eine Untergruppe von $\mathbb{Z}$. Es gibt daher eine positive ganze Zahl d mit $f(K^\times) = d\mathbb{Z}$. Da $f(p) = n$ ist, gilt $n \in d\mathbb{Z}$, und somit wird n

von d geteilt. Setzen wir $e = \frac{n}{d}$, so ist $\mathrm{ord}_p\left(K^\times\right) = \frac{1}{e}\mathbb{Z}$ und e ein Teiler von n. □

Die Bildmenge dieses Gruppenhomomorphismus heißt *die Bewertungsgruppe von* K, und die Zahl e stellt eine invariante Größe dar, auf welcher die Unterscheidung von endlichen Körpererweiterung über $\mathbb{Q}_p$ basiert:

Definition 4: Es sei $K/\mathbb{Q}_p$ eine endliche Körpererweiterung, und es sei $e = e\left(K/\mathbb{Q}_p\right)$ jene eindeutig bestimmte natürliche Zahl, die durch

$$\mathrm{ord}_p\left(K^\times\right) = \tfrac{1}{e}\mathbb{Z}$$

gegeben ist. Dann heißt e *der Verzweigungsindex von* K *über* $\mathbb{Q}_p$.

Eine Körpererweiterung $K/\mathbb{Q}_p$ wird *unverzweigt* genannt, wenn $e = 1$ ist, ansonsten heißt sie *verzweigt*. Ist $e = n$, so sagen wir, die Körpererweiterung ist *total verzweigt*.

Definition 5: Es sei $K/\mathbb{Q}_p$ eine endliche Körpererweiterung mit Verzweigungsindex e. Ein Element $\pi \in K$ heißt *eine Uniformisierende*, wenn $\mathrm{ord}_p\left(\pi\right) = \frac{1}{e}$ ist.

Im Allgemeinen gibt es viele Uniformisierende. Ist die Körpererweiterung unverzweigt, so stellt p eine Uniformisierende dar.

Als Nächstes werden wir uns mit der algebraischen Struktur des Erweiterungskörpers K beschäftigen. Der Bewertungsring und das Bewertungsideal aus Definition 12 in Kapitel 1 werden durch folgende Mengen beschrieben:

$$\mathcal{O} = \mathcal{O}_K = \{x \in K :\ |x|_p \leq 1\} = \{x \in K :\ \mathrm{ord}_p\left(x\right) \geq 0\},$$
$$\mathcal{P} = \mathcal{P}_K = \{x \in K :\ |x|_p < 1\} = \{x \in K :\ \mathrm{ord}_p\left(x\right) > 0\}.$$

Wir wissen, dass $\mathcal{O}_K$ ein lokaler Ring und der Restklassenkörper durch den Quotient

$$\kappa = \mathcal{O}_K/\mathcal{P}_K$$

gegeben ist.

Die meisten Behauptungen der nächsten Proposition folgen leicht aus früheren Überlegungen:

Proposition 8: Es sei $K/\mathbb{Q}_p$ eine endliche Körpererweiterung und π eine Uniformisierende. Dann gilt:

1. Das Ideal $\mathcal{P}_K \subseteq \mathcal{O}_K$ ist ein Hauptideal und wird von der Uniformisierenden π erzeugt.
2. Jedes Element $x \in K$ kann in der Form $x = u\pi^{e\mathrm{ord}_p(x)}$ geschrieben werden, wobei $u \in \mathcal{O}_K^\times$ eine Einheit ist, und es gilt $K = \mathcal{O}_K\left[\pi^{-1}\right]$.
3. Es ist $\kappa/\mathbb{F}_p$ eine endliche Körpererweiterung, deren Grad $[\kappa : \mathbb{F}_p]$ kleiner oder gleich $[K : \mathbb{Q}_p]$ ist. Insbesondere ist die Zahl der Elemente von κ eine Potenz p^f von p.

4. Ist $x \in K$ die Wurzel eines normierten Polynoms mit Koeffizienten aus $\mathbb{Z}_p$, dann liegt x in $\mathcal{O}_K$. Umgekehrt ist jedes Element von $\mathcal{O}_K$ die Wurzel eines normierten Polynoms mit Koeffizienten in $\mathbb{Z}_p$.

5. Die Einheitskugel $\mathcal{O}_K$ von K ist kompakt, und die Mengen $\pi^n\mathcal{O}_K$, $n \in \mathbb{Z}$ bilden eine Umgebungsbasis von 0. Es ist K als topologischer Raum ein total unzusammenhängender, lokalkompakter Hausdorffraum.

6. Es sei $C = \{0,\, c_1,\, c_2,\, \ldots,\, c_{p^f-1}\}$ ein vollständiges Repräsentantensystem der Restklassen von $\mathcal{O}_K/\mathcal{P}_K$. Dann kann jedes $x \in K$ eindeutig dargestellt werden als

$$x = \sum_{i=m}^{\infty} a_i \pi^i = a_m \pi^m + a_{m+1}\pi^{m+1} + \cdots,$$

mit $m = e{\cdot}\mathrm{ord}_p(x)$ und $a_i \in C$ für alle $i \geq m$.

Beweis.

1. Es ist $|\pi|_p < 1$ für eine Uniformisierende $\pi \in K$, daher gilt $\pi\mathcal{O}_K \subseteq \mathcal{P}_K$. Umgekehrt ist $\pi\mathcal{O}_K \supseteq \mathcal{P}_K$: Für alle $x \in \mathcal{P}_K$ ist $|x|_p \leq |\pi|_p$, daher liegt $\frac{x}{\pi}$ in $\mathcal{O}_K$ und somit $x = \pi\frac{x}{\pi}$ in $\pi\mathcal{O}_K$. Das zeigt, dass $\mathcal{P}_K = (\pi) = \pi\mathcal{O}_K$ ein von π erzeugtes Hauptideal ist.

2. Multiplizieren wir ein Element $x \in K$, $x \neq 0$ mit $p^{-\mathrm{ord}_p(x)}$, so erhalten wir eine Einheit u. Somit ist $x = up^{\mathrm{ord}_p(x)}$, und wegen $|\pi|_p = p^{-1/e} = |p|_p^{1/e}$ ist $x = u\pi^{e\mathrm{ord}_p(x)}$ für eine Uniformisierende π. Daraus folgt auch die zweite Aussage.

3. Die Abbildung $\mathbb{Z}_p/p\mathbb{Z}_p \to \mathcal{O}_K/\mathcal{P}_K$, $a+p\mathbb{Z}_p \mapsto a+\mathcal{P}_K$ ist wohldefiniert und injektiv, denn für zwei ganze p-adische Zahlen a, b ist genau dann $a+\mathcal{P}_K = b+\mathcal{P}_K$, wenn $a-b$ in $\mathcal{P}_K \cap \mathbb{Z}_p$ liegt. Das trifft genau dann zu, wenn $a+p\mathbb{Z}_p = b+p\mathbb{Z}_p$ gilt, denn es ist ja $\mathcal{P}_K \cap \mathbb{Z}_p = p\mathbb{Z}_p$. Aus Abschnitt 4.3 wissen wir, dass $\mathbb{Z}_p/p\mathbb{Z}_p$ isomorph zu $\mathbb{F}_p$ ist. Wie wir eben gesehen haben, ist die betrachtete Abbildung injektiv, das heißt, $\kappa = \mathcal{O}_K/\mathcal{P}_K$ ist isomorph zu einem Erweiterungskörper von $\mathbb{F}_p$.
Wir zeigen nun, dass $[\mathcal{O}_K/\mathcal{P}_K : \mathbb{Z}_p/p\mathbb{Z}_p] \leq [K : \mathbb{Q}_p]$ gilt, dass also die betrachtete Körpererweiterung $\kappa/\mathbb{F}_p$ endlich ist. Es sei $n = [K : \mathbb{Q}_p]$.
Es kann $\mathcal{O}_K/\mathcal{P}_K$ als Vektorraum über $\mathbb{Z}_p/p\mathbb{Z}_p$ angesehen werden, wobei sich die Multiplikation mit einem Skalar folgendermaßen ergibt:

$$\begin{aligned}\left(\mathbb{Z}_p/p\mathbb{Z}_p\right) \times \left(\mathcal{O}_K/\mathcal{P}_K\right) &\to \mathcal{O}_K/\mathcal{P}_K,\\ (a+p\mathbb{Z}_p)\cdot(b+\mathcal{P}_K) &\mapsto ab+\mathcal{P}_K.\end{aligned}$$

Wir betrachten $n+1$ Restklassen von $\mathcal{O}_K/\mathcal{P}_K$, nämlich $\overline{a}_i = a_i + \mathcal{P}_K$ mit $a_i \in \mathcal{O}_K$, $i = 1, \ldots, n+1$. Da $[K : \mathbb{Q}_p] = n$ ist, müssen die $n+1$ Elemente a_i über $\mathbb{Q}_p$ linear abhängig sein. Daher gibt es $b_i \in \mathbb{Q}_p$, $i = 1, \ldots, n+1$, sodass $a_1b_1 + a_2b_2 + \cdots + a_{n+1}b_{n+1} = 0$ erfüllt ist.
Wir können sogar annehmen, dass alle b_i in $\mathbb{Z}_p$ liegen. Außerdem soll für mindestens ein j aus $\{1, \ldots, n+1\}$ gelten, dass $|b_j|_p = 1$ ist, also dass b_j nicht in $p\mathbb{Z}_p$ liegt. Um das zu erreichen, müssen wir die Elemente b_i lediglich mit einer entsprechenden Potenz von p multiplizieren.

Wenden wir nun auf $a_1b_1+\cdots+a_{n+1}b_{n+1}=0$ die Abbildung $\mathcal{O}_K \to {}^{\mathcal{O}_K}/_{\mathcal{P}_K}$ an, so erhalten wir

$$\sum_{i=1}^{n+1} a_i b_i + \mathcal{P}_K = \sum_{i=1}^{n+1} (a_i + \mathcal{P}_K)(b_i + \mathcal{P}_K) = 0.$$

Da alle b_i ganze p-adische Zahlen sind, können wir dies als Skalarmultiplikation im Vektorraum ${}^{\mathcal{O}_K}/_{\mathcal{P}_K}$ auffassen:

$$\sum_{i=1}^{n+1} (b_i + p\mathbb{Z}_p)(a_i + \mathcal{P}_K) = 0.$$

Nach unserer Voraussetzung liegt b_j nicht in $p\mathbb{Z}_p$. Das bedeutet, es gibt zumindest eine Restklasse $(b_i + p\mathbb{Z}_p)$ ungleich Null. Daher sind die $n+1$ Elemente $a_i \in \mathcal{O}_K$ über $\mathbb{Q}_p$ linear abhängig, und es folgt

$$\left[\mathcal{O}_K/\mathcal{P}_K : {}^{\mathbb{Z}_p}/_{p\mathbb{Z}_p}\right] = \dim_{\mathbb{F}_p} \kappa \leq n.$$

Aus der Algebra ist bekannt, dass die Anzahl der Elemente eines solchen Erweiterungskörpers eine Potenz p^f von p ist.

4. Es sei $\alpha \in K$ Nullstelle des normierten Polynoms

$$f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0$$

mit Koeffizienten aus $\mathbb{Z}_p$. Für alle i ist somit $|a_i|_p \leq 1$, und es gilt

$$\begin{aligned} |\alpha|_p^m = |\alpha^m|_p &= \left|a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0\right|_p \\ &\leq \max_{1\leq i\leq m} \left|\alpha^{m-i}\right|_p = |\alpha|_p^{m-1}. \end{aligned}$$

Daraus würde sich ein Widerspruch ergeben, wenn $|\alpha|_p > 1$ wäre. Daher ist $\alpha \in \mathcal{O}_K$.
Es sei nun umgekehrt $\alpha \in \mathcal{O}_K$. Da es sich bei $K/\mathbb{Q}_p$ um eine endliche Körpererweiterung handelt, ist α algebraisch über $\mathbb{Q}_p$ und daher Nullstelle eines Polynoms $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0$ mit Koeffizienten aus $\mathbb{Q}_p$. Es seien $\alpha_1, \alpha_2, \ldots, \alpha_m$ die Konjugierten von $\alpha = \alpha_1$. Somit ist das Polynom $f(X)$ darstellbar als $f(X) = \prod_{i=1}^m (X - \alpha_i)$. Nun ergibt sich mit Hilfe der aus der Algebra bekannten elementarsymmetrischen Polynome für die Koeffizienten $a_0, \ldots, a_{m-1}$ von $f(X)$

$$a_{m-j} = (-1)^j \sum_{\substack{I\subseteq\{1,\ldots m\} \\ |I|=j}} \prod_{i\in I} \alpha_i.$$

Es gilt $|\alpha_i|_p = |\alpha|_p \leq 1$ für alle Konjugierten α_i von $\alpha = \alpha_1$. Daher ist $|a_{m-j}|_p \leq 1$ für alle $j = 1, \ldots, m$, die Koeffizienten liegen also in $\mathbb{Z}_p$.

5. Die Aussagen folgen analog zu den in Abschnitt 1.2 und Abschnitt 4.3 angestellten Überlegungen.

6. Es sei zunächst $x \in \mathcal{O}_K$. Dann gibt es genau ein $a_0 \in C$, sodass $x + \mathcal{P}_K = a_0 + \mathcal{P}_K$ gilt. Es ist dann $x - a_0 \in \pi\mathcal{O}_K$ beziehungsweise $x = a_0 + \pi x_1$ für ein $x_1 \in \mathcal{O}_K$. Machen wir das Gleiche zunächst für x_1 und fahren dann auf diese Weise fort, so erhalten wir die Darstellung

$$x = a_0 + \pi a_1 + \pi^2 a_2 + \cdots + \pi^{n-1}a_{n-1} + \pi^n x_n$$

mit $a_i \in C$ für $0 \leq i \leq n-1$ und $x_n \in \mathcal{O}_K$. Für $n \to \infty$ gilt

$$\left|x - a_0 - \cdots - \pi^{n-1} a_{n-1}\right|_p = \left|\pi^n x_n\right|_p \leq |\pi|_p^n \to 0,$$

denn es ist ja $|x_n|_p \leq 1$. Die Partialsummen der unendlichen Reihe $\sum_{i=0}^{\infty} a_i \pi^i$ konvergieren also gegen das Element $x \in \mathcal{O}_K$.
Ist nun $x \in K$ beliebig, dann gibt es eine ganze Zahl k, sodass $\left|\pi^k x\right|_p \leq 1$ ist. Wir können also für das Element $\pi^k x$ eine entsprechende Entwicklung in Potenzen von π finden.
Dass $m = e \cdot \operatorname{ord}_p(x)$ gilt, haben wir uns in Punkt 2 dieser Proposition überlegt. □

Bemerkung 3: Ist S ein Ring und R ein Teilring von S, dann heißt ein Element $s \in S$ ganz über R, wenn es ein normiertes Polynom $f(X) \in R[X]$ gibt mit $f(s) = 0$. Die Menge der ganzen Elemente von S über R wird als *ganzer Abschluss von R in S* bezeichnet. Also besagt Punkt 4 in der vorigen Proposition, dass $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z}_p$ in K ist.

In Proposition 8 haben wir gesehen, dass die Anzahl der Elemente des Restklassenkörpers einer endlichen Körpererweiterung $K/\mathbb{Q}_p$ eine Potenz p^f von p ist. Wir werden nun zeigen, dass diese Zahl f mit dem Verzweigungsindex e in Zusammenhang steht und ebenfalls eine invariante Größe der Körpererweiterung darstellt.

Definition 6: Es sei $K/\mathbb{Q}_p$ eine endliche Körpererweiterung mit Restklassenkörper $\kappa \cong \mathbb{F}_{p^f}$. Dann heißt $f = f(K/\mathbb{Q}_p)$ *der Trägheitsgrad von K über $\mathbb{Q}_p$*.

Proposition 9: Es sei K ein Erweiterungskörper von $\mathbb{Q}_p$ mit $[K : \mathbb{Q}_p] = n < \infty$. Der Verzweigungsindex der Körpererweiterung sei e und f sei der Trägheitsgrad. Dann gilt $e \cdot f = n$.

Beweis. Es sei $\{\alpha_1 + \mathcal{P}_K, \ldots, \alpha_f + \mathcal{P}_K\}$ eine Basis von $\mathcal{O}_K/\mathcal{P}_K$ als Vektorraum über $\mathbb{Z}_p/p\mathbb{Z}_p$ und π eine Uniformisierende. Wir werden zeigen, dass die Elemente

$$\begin{aligned}
&\alpha_1, \alpha_2, \ldots, \alpha_f,\\
&\pi\alpha_1, \pi\alpha_2, \ldots, \pi\alpha_f,\\
&\ldots,\\
&\pi^{e-1}\alpha_1, \pi^{e-1}\alpha_2, \ldots, \pi^{e-1}\alpha_f
\end{aligned}$$

eine Basis von K über $\mathbb{Q}_p$ bilden.

Zunächst überlegen wir uns, dass die Menge $\{\alpha_1, \ldots, \alpha_f\}$ linear unabhängig über $\mathbb{Q}_p$ ist.

Es sei also $x_1\alpha_1 + \cdots + x_f\alpha_f = 0$ mit $x_i \in \mathbb{Q}_p$, $x_i \neq 0$ für $1 \leq i \leq f$. Wie im Beweis zu Punkt 3 von Proposition 8 nehmen wir an, dass alle x_i in $\mathbb{Z}_p$ liegen, jedoch so, dass $x_j \notin p\mathbb{Z}_p$ für mindesten ein $j \in \{1, \ldots, f\}$ gelte.

Außerdem interpretieren wir die Produkte $x_i\alpha_i$ wieder als Multiplikation mit einem Skalar im Vektorraum $\mathcal{O}_K/\mathcal{P}_K$ über $\mathbb{Z}_p/p\mathbb{Z}_p$. Das heißt, wir können die Gleichung auch schreiben als

$$\sum_{i=1}^{f} (x_i + p\mathbb{Z}_p)(\alpha_i + \mathcal{P}_K) = 0 + \mathcal{P}_K.$$

Daraus folgt jedoch, dass x_i für alle $i = 1, \ldots, f$ in $p\mathbb{Z}_p$ liegen muss. Das widerspricht aber unserer Voraussetzung, und somit ist die Menge $\{\alpha_1, \ldots, \alpha_f\}$ linear unabhängig über $\mathbb{Q}_p$.

Im nächsten Schritt zeigen wir, dass die Elemente $\{\pi^i\alpha_j\}$ mit $0 \leq i < e$, $1 \leq j \leq f$ ebenfalls linear unabhängig über $\mathbb{Q}_p$ sind.

Wir nehmen wieder an, dass alle x_{ij} in $\mathbb{Z}_p$ liegen, und betrachten

$$\sum_{i=0}^{e-1}\sum_{j=1}^{f} x_{ij}\pi^i\alpha_j = \sum_{i=0}^{e-1}\pi^i\sum_{j=1}^{f} x_{ij}\alpha_j = 0.$$

Für jedes $i \in \{0, \ldots, e-1\}$ ist dann $|x_{i1}\alpha_1 + x_{i2}\alpha_2 + \cdots + x_{if}\alpha_f|_p = \max_{1\leq j\leq f}|x_{ij}|_p$. Denn sind alle $x_{ij} = 0$, so ist auch $\max_{1\leq j\leq f}|x_{ij}|_p = 0$, und die Gleichung ist klarerweise erfüllt. Sind jedoch nicht alle $x_{ij} = 0$, so muss

$$|x_{i1}\alpha_1 + x_{i2}\alpha_2 + \cdots + x_{if}\alpha_f|_p = \max_{1\leq j\leq f}|x_{ij}|_p = 1$$

gelten, denn wäre $|x_{i1}\alpha_1 + x_{i2}\alpha_2 + \cdots + x_{if}\alpha_f|_p < 1$, so würde ja die Summen $\sum_{j=1}^{f} x_{ij}\alpha_j$ von p geteilt werden, und wir hätten

$$0 + \mathcal{P}_K = \sum_{i=1}^{f}(x_{ij}\alpha_i + \mathcal{P}_K) = \sum_{i=1}^{f}(x_{ij} + p\mathbb{Z}_p)(\alpha_i + \mathcal{P}_K).$$

Das ist aber wegen der linearen Unabhängigkeit der Menge $\{\alpha_i + \mathcal{P}_K\}_{1\leq i\leq f}$ nicht möglich.

Daher ist $\left|\pi^i\sum_{j=1}^{f} x_{ij}\alpha_j\right|_p = |\pi^i|_p\left|\sum_{j=1}^{f} x_{ij}\alpha_j\right|_p$ für jedes $i \in \{0, \ldots, e-1\}$ entweder gleich $p^{-i/e}$ oder gleich Null.

Für $i \in \{0, \ldots, e-1\}$ sind die Werte $p^{-i/e}$ paarweise verschieden, was zur Folge hat, dass der Betrag der Summe genau dem Maximum der Beträge der einzelnen Summanden entspricht:

$$\left|\sum_{i=0}^{e-1}\pi^i\sum_{j=1}^{f} x_{ij}\alpha_j\right|_p = \max_{0\leq i\leq e-1}\left\{p^{-\frac{i}{e}}\cdot\left|\sum_{j=1}^{f} x_{ij}\alpha_j\right|_p\right\}.$$

Nun ist aber dieser Ausdruck gleich Null, daher muss $x_{ij} = 0$ für alle i, j gelten. Die Elemente $\pi^i\alpha_j$ sind somit linear unabhängig in K.

Es bleibt noch zu zeigen, dass die Menge $\{\pi^i\alpha_j\}$, $0 \leq i < e$, $1 \leq j \leq f$ den Erweiterungskörper K erzeugt. Da wir jedes Element x von K mit einer entsprechenden Potenz von p multiplizieren können, um ein Element in $\mathcal{O}_K$ zu erhalten, genügt es zu beweisen, dass diese Menge den Bewertungsring $\mathcal{O}_K$ erzeugt.

Es sei also $E := \mathbb{Z}_p\alpha_1 + \cdots + \mathbb{Z}_p\alpha_f$. Dann ist $\mathcal{O}_K = E + \pi\mathcal{O}_K$, denn für $x \in \mathcal{O}_K$ gibt es ganze p-adische Zahlen $x_1, \ldots, x_f$ mit $x + \mathcal{P}_K = \sum_{i=1}^{f}(x_i + p\mathbb{Z}_p)(\alpha_i + \pi\mathcal{O}_K)$, und daher ist $x - \sum_{i=1}^{f} x_i\alpha_i$ ein Element von $\pi\mathcal{O}_K$.

Durch mehrmaliges Iterieren folgt $\mathcal{O}_K = E + \pi(E + \pi\mathcal{O}_K) = \cdots = E + \pi E + \cdots + \pi^{e-1}E + \pi^e\mathcal{O}_K = E + \pi E + \cdots + \pi^{e-1}E + p\mathcal{O}_K$. Dabei haben wir beachtet, dass $p\mathcal{O}_K = \pi^e\mathcal{O}_K$ gilt.

Da ja E von $\alpha_1, \ldots, \alpha_f$ erzeugt wird, folgt das Gewünschte. □

Zusammenfassend gilt also, dass sich der Grad n einer endlichen Körpererweiterung $K/\mathbb{Q}_p$ als Produkt vom Verzweigungsgrad e und Trägheitsgrad f ergibt, wobei

$$e = \left[\left|K^\times\right|_p : \left|\mathbb{Q}_p^\times\right|_p\right]$$

die Änderung der Wertemenge der p-adischen Ordnung ord_p anzeigt und

$$f = \left[\mathcal{O}_K/\mathcal{P}_K : {}^{\mathbb{Z}_p}/_{p\mathbb{Z}_p}\right]$$

die Größenänderung des Restklassenkörpers. Das heißt, eine endlichen Körpererweiterung $K/\mathbb{Q}_p$ ist

- unverzweigt, wenn $e = 1$ ist. Es ist dann $[K : \mathbb{Q}_p] = f$. Die Wertemenge von ord_p ändert sich nicht und ist gleich $\mathbb{Z}$. Außerdem wird $\mathcal{P}_K$ von p erzeugt.
- verzweigt, wenn $e > 1$ und somit $f < n$ ist.
- total verzweigt, wenn $f = 1$ ist. Es ist dann $[K : \mathbb{Q}_p] = e$. In diesem Fall ändert sich die Größe des Restklassenkörpers nicht. Eine total verzweigte Körpererweiterung heißt *zahm*, wenn p kein Teiler von e ist, und *wild*, wenn e eine Potenz von p ist.

Bevor wir zum eigentlichen Ziel dieses Kapitels kommen, nämlich zu der Frage des algebraischen Abschluss von $\mathbb{Q}_p$, zeigen wir noch, dass

- jede total verzweigte Körpererweiterung $K/\mathbb{Q}_p$ einfach ist, das heißt, es gilt $K = \mathbb{Q}_p(\pi)$. Wir werden sehen, dass es sich bei π um eine Uniformisierende handelt, die außerdem Wurzel eines Polynoms mit ganz bestimmten Eigenschaften – eines sogenannten Eisenstein-Polynoms – ist. Mit „zahmen“ und „wilden“ Erweiterungen werden wir uns nicht speziell beschäftigen.
- es für jede positive ganze Zahl f eine eindeutig bestimmte, unverzweigte Körpererweiterung vom Grad f über $\mathbb{Q}_p$ gibt. Wir werden den entsprechenden Erweiterungskörper als K_f^{unv} bezeichnen und sehen, dass dieser von einer primitiven $\left(p^f - 1\right)$-ten Einheitswurzel erzeugt wird.
- sich jede endliche, verzweigte Körpererweiterung $K/\mathbb{Q}_p$ darstellen lässt als eine total verzweigte Körpererweiterung über einer unverzweigten. Es gilt also

  $$[K : \mathbb{Q}_p] = \left[K : K_f^{\mathrm{unv}}\right]\left[K_f^{\mathrm{unv}} : \mathbb{Q}_p\right]$$

  mit $K = K_f^{\mathrm{unv}}(\pi)$.

Da $\mathbb{Z}_p$ ein Hauptidealbereich und somit faktoriell ist, können wir das folgende, aus der Algebra bekannte Irreduzibilitätskriterium anwenden:

Es sei R ein faktorieller Ring, K der Quotientenkörper von R und $f(X) = a_n X^n + \cdots + a_1 X + a_0$ ein Polynom über R. Dieses Polynom sei primitiv, das heißt, seine Koeffizienten seien teilerfremd. Gilt $p \mid a_i$ für $0 \leq i < n$, $p \nmid a_n$ sowie $p^2 \nmid a_0$ für ein irreduzibles und daher primes Element $p \in R$, dann ist $f(X)$ irreduzibel in $R[X]$ *und* in $K[X]$.

Ein Polynom mit diesen Eigenschaften heißt *ein Eisenstein-Polynom.*

Proposition 10: Es sei $K/\mathbb{Q}_p$ eine endliche, total verzweigte Körpererweiterung und π eine Uniformisierende. Dann gilt $K = \mathbb{Q}_p(\pi)$. Außerdem ist π die Wurzel eines Eisenstein-Polynoms.

Beweis. Da die Körpererweiterung total verzweigt ist, gilt $e = n = [K : \mathbb{Q}_p]$.

Es sei $f(X) = \sum_{i=0}^{s} a_i X^i$ das Minimalpolynom von π über $\mathbb{Q}_p$. Dann folgt mit Proposition 3 auf Seite 82 und Proposition 4 auf Seite 83, dass

$$N_{K/\mathbb{Q}_p}(\pi) = \left(N_{\mathbb{Q}_p(\pi)/\mathbb{Q}_p}(\pi)\right)^{[K:\mathbb{Q}_p(\pi)]} = (-1)^e a_0^{e/s}$$

gilt. Für den Absolutbetrag von π ergibt sich daraus $|\pi|_p = \sqrt[e]{\left|a_0^{e/s}\right|_p} = \sqrt[s]{|a_0|_p}$. Andererseits wissen wir, dass $|\pi|_p = p^{-1/e}$ ist. Insgesamt erhalten wir $p^{-1/e} = \sqrt[s]{|a_0|_p} = p^{-m/s}$, wobei $m \in \mathbb{Z}$ die p-adische Ordnung von $a_0 \in \mathbb{Q}_p$ darstellt.

Da außerdem $e \geq s$ ist, folgt wegen $\frac{s}{e} = m \in \mathbb{Z}$, dass $e = s$ und somit $m = 1$ gilt.

Daher entspricht der Grad s des Minimalpolynoms dem Grad e der Körpererweiterung, und es folgt $K = \mathbb{Q}_p(\pi)$.

Wir werden nun zeigen, dass die Koeffizienten von $f(X)$ die Eigenschaften eines Eisenstein-Polynoms aufweisen.

Die Bedingung $|a_0|_p = p^{-1}$ ist jedenfalls erfüllt, und da $f(X)$ normiert ist, gilt $|a_e|_p = 1$.

Um die anderen Eigenschaften zu zeigen, betrachten wir die Konjugierten $\pi_1 = \pi_1, \pi_2, \ldots, \pi_e$ von $\pi = \pi_1$. Diese besitzen alle denselben Absolutbetrag, es ist also $|\pi_i|_p = p^{-1/e} < 1$ für $i = 1, \ldots, e$, und wir schreiben $f(X) = \prod_{i=1}^{e}(X - \pi_i)$.

Dass $|a_j|_p < 1$ für $1 \leq j < e$ erfüllt ist, folgt mit Hilfe der elementarsymmetrischen Polynome analog zum Beweis des vierten Punktes von Proposition 8. □

Bemerkung 4: Ist umgekehrt α die Wurzel eines Eisenstein-Polynoms $f(X)$ über $\mathbb{Q}_p$ mit $e = \deg f$, dann ist $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ eine total verzweigte Körpererweiterung vom Grad e.

Denn es ist $f(X)$ irreduzibel und somit das Minimalpolynom von α über $\mathbb{Q}_p$, daher folgt $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = e$. Wegen $|a_0|_p = p^{-1}$ ergibt sich der Absolutbetrag von α durch $|\alpha|_p = |a_0|_p^{1/e} = p^{-1/e}$. Das bedeutet, dass der Verzweigungsindex gleich dem Grad der Körpererweiterung ist. Außerdem handelt es sich bei α eine Uniformisierende.

Bevor wir die Behauptung zeigen, dass die Adjunktion einer primitiven $\left(p^f - 1\right)$-ten Einheitswurzel eine unverzweigte Körpererweiterung $K/\mathbb{Q}_p$ ergibt, werden wir uns überlegen, welche Einheitswurzeln in einer endlichen Körpererweiterung über $\mathbb{Q}_p$ überhaupt existieren.

In K liegen alle Einheitswurzeln ζ_i auf der Einheitssphäre $\mathcal{O}_K^\times$, denn wegen $\zeta_i^m = 1$ für ein $m \in \mathbb{N}$ ist $|\zeta_i|_p^m = |1|_p$ beziehungsweise $|\zeta_i|_p = 1$.

Betrachten wir nun die kanonische Abbildung $\mathcal{O}_K \to {}^{\mathcal{O}_K}/_{\mathcal{P}_K}$, so sehen wir, dass das Bild aller Einheitswurzeln ζ_i wegen $\kappa \cong \mathbb{F}_{p^f}$ in $\mathbb{F}_{p^f}^\times$ liegt. Bekanntermaßen ist $\mathbb{F}_{p^f}^\times$ eine zyklische Gruppe der Ordnung $p^f - 1$.

Es sei nun a ein Element von $\kappa^\times$. Dann ist die Ordnung m von a ein Teiler von $p^f - 1$. Wir wählen $\alpha_0 \in \mathcal{O}_K$ so, dass $a = \alpha_0 + \mathcal{P}_K$ gilt, und betrachten das Polynom $F(X) = X^m - 1$.

Da K ein vollständiger, nichtarchimedisch bewerteter Körper ist, kann das Henselsche Lemma aus Abschnitt 4.5 ohne Schwierigkeiten für den Erweiterungskörper K gezeigt und auf ein Polynom mit Koeffizienten in $\mathcal{O}_K$ angewendet werden.

Wir haben α_0 so gewählt, dass $F(\alpha_0) \equiv 0 \pmod{p}$ gilt. Es ist $F'(X) = mX^{m-1}$, und da m nicht von p geteilt wird, folgt $F'(\alpha_0) \not\equiv 0 \pmod{p}$. Das heißt, wir können ein eindeutig bestimmtes $\alpha \in \mathcal{O}_K$ finden mit $\alpha^m = 1$ und $\alpha + \mathcal{P}_K = \alpha_0 + \mathcal{P}_K = a$.

Somit haben wir gezeigt, dass $\epsilon : \ G \to (\mathcal{O}_K/\mathcal{P}_K)^\times$ surjektiv ist, wobei G die Gruppe jener Einheitswurzeln in K bezeichnet, deren Ordnung relativ prim zu p ist.

Diese Abbildung ist auch injektiv. Denn ist $x \in G \cap \ker \epsilon$, so gilt $x^t = 1$ für ein $t \geq 0$, $p \nmid t$ sowie $x + \mathcal{P}_K = 1 + \mathcal{P}_K$ beziehungsweise $|x-1|_p < 1$. Dann ist auch $x^k + \mathcal{P}_K = 1 + \mathcal{P}_K$ beziehungsweise $\left|x^k - 1\right|_p < 1$ für $k \geq 0$. Wäre nun $x \neq 1$, so wäre wegen $0 = x^t - 1 = (x-1)\left(x^{t-1} + \cdots + 1\right)$

$$0 = x^{t-1} + x^{t-2} + \cdots + 1 = x^{t-1} - 1 + x^{t-2} - 1 + \cdots + x - 1 + t,$$

was $|t|_p \leq \max_{0 \leq i < t} \left|x^i - 1\right|_p < 1$ ergäbe, und das wäre ein Widerspruch zur Voraussetzung, dass p und t relativ prim sind. Somit ist $x = 1$. Insgesamt erhalten wir, dass G isomorph zu $\kappa^\times$ ist.

Es kann in K auch Einheitswurzeln geben, deren Ordnung nicht relativ prim zu p ist. Es sei also ζ^m eine Einheitswurzel mit $m = p^r$ und $\bar{\zeta}$ die Restklasse von ζ unter der kanonischen Abbildung $\mathcal{O}_K \to \mathcal{O}_K/\mathcal{P}_K$. Da κ die Charakteristik p hat, folgt aus $\bar{\zeta}^{p^r} = \bar{1}$, dass $\bar{\zeta} = \bar{1}$ und somit $\zeta \in 1 + \mathcal{P}_K$ ist.

Ist umgekehrt $\zeta \in 1 + \mathcal{P}_K$ von der Ordnung $m > 1$, dann gibt es ein $\alpha \in \mathcal{P}_K$, sodass $\zeta = 1 + \alpha$ gilt. Es ist

$$1 = (1+\alpha)^m = \sum_{i=0}^{m} \binom{m}{i} \alpha^i = 1 + m\alpha + \sum_{i=2}^{m} \binom{m}{i} \alpha^i.$$

Daher muss $m\alpha + \sum_{i=2}^{m} \binom{m}{i} \alpha^i = 0$ beziehungsweise

$$|m|_p = \Big|\sum_{i=2}^{m} \binom{m}{i} \alpha^{i-1}\Big|_p$$

gelten. Wegen $|\alpha|_p < 1$ und $\left|\binom{m}{i}\right|_p \leq 1$ für alle i ist die rechte Seite kleiner als Eins. Das muss dann auch für die linke gelten und somit ist p ein Teiler von m.

Ist $m = p$, dann sind wir fertig. Für $m \neq p$ wiederholen wir das Ganze mit ζ^p, denn es ist dann ζ^p von der Ordnung $\frac{m}{p} > 1$. Ingesamt ergibt sich, dass m eine Potenz von p ist.

Bemerkung 5: Die Menge der $\left(p^f - 1\right)$-ten Einheitswurzeln bildet zusammen mit $\{0\}$ ein vollständiges Repräsentantensystem des Restklassenkörpers κ. Diese *Teichmüller Repräsentanten* können als Ziffern in der Entwicklung in Punkt 6 der Proposition 8 gewählt werden – vergleiche auch Bemerkung 9 auf Seite 60.

Proposition 11: Für jede positive ganze Zahl f gibt es genau eine unverzweigte Körpererweiterung $K_f^{\text{unv}}/\mathbb{Q}_p$ vom Grad f, und es ist dann

$$K_f^{\text{unv}} = \mathbb{Q}_p(\zeta)$$

für eine primitive $\left(p^f-1\right)$-Einheitswurzel ζ. Ist $K/\mathbb{Q}_p$ eine endliche, verzweigte Körpererweiterung vom Grad $n=e\cdot f$, dann ist

$$K=K_f^{\mathrm{unv}}(\pi),$$

wobei es sich bei π um die Wurzel eines Eisenstein-Polynoms über K_f^{unv} handelt.

Beweis. Wir zeigen zunächst, dass es immer eine unverzweigte Körpererweiterung über $\mathbb{Q}_p$ vom Grad f, $f\in\mathbb{Z}_+$ gibt.

Es sei also $\overline{\alpha}$ ein erzeugendes Element der zyklischen Gruppe $\mathbb{F}_{p^f}^{\times}$, und $\overline{g}(X)=X^f+\overline{a}_{f-1}X^{f-1}+\ldots+\overline{a}_1X+\overline{a}_0$ das Minimalpolynom von $\overline{\alpha}$ über $\mathbb{F}_p$. Dann ist $\mathbb{F}_{p^f}=\mathbb{F}_p(\overline{\alpha})$ und $\left[\mathbb{F}_{p^f}:\mathbb{F}_p\right]=f$.

Für jedes $i\in\{1,\ldots,f-1\}$ sei $a_i\in\mathbb{Z}_p$ so gewählt, dass $a_i\equiv\overline{a}_i \pmod p$ erfüllt ist. Wir setzen $g(X):=X^f+a_{f-1}X^{f-1}+\ldots+a_1X+a_0$. Es ist $g(X)$ irreduzibel über $\mathbb{Z}_p$, denn könnte $g(X)$ als Produkt nichtkonstanter Polynome dargestellt werden, dann müsste dieses Produkt modulo p auch $\overline{g}(X)$ ergeben, was aber nicht geht, denn $\overline{g}(X)$ ist als Minimalpolynom irreduzibel.

Dann ist $g(X)$ auch über $\mathbb{Q}_p$ irreduzibel. Es sei α eine Wurzel von $g(X)$. Wir setzen $K_f=\mathbb{Q}_p(\alpha)$. Dann ist $\left[K_f:\mathbb{Q}_p\right]=f$.

Es ist $\alpha+\mathcal{P}_{K_f}$ eine Wurzel von $\overline{g}(X)$. Deshalb muss $\left[\kappa:\mathbb{F}_p\right]\geq f$ sein. Da andererseits $\left[\kappa:\mathbb{F}_p\right]\leq\left[K_f:\mathbb{Q}_p\right]$ gilt, ist $\left[\kappa:\mathbb{F}_p\right]=f=\left[K_f:\mathbb{Q}_p\right]$. Das bedeutet aber auch, dass $e=1$ und K_f eine unverzweigte Körpererweiterung vom Grad f ist. Für diese schreiben wir nun K_f^{unv}, und es bleibt noch zu zeigen, dass K_f^{unv} eindeutig bestimmt ist.

Es sei nun K eine endliche, verzweigte Körpererweiterung von $\mathbb{Q}_p$ mit Verzweigungsindex $e>1$ und Trägheitsgrad f. Dann ist $\mathcal{O}_K/\mathcal{P}_K\cong\mathbb{F}_{p^f}$. Es sei $\overline{\zeta}\in\mathbb{F}_{p^f}$ ein erzeugendes Element von $\mathbb{F}_{p^f}^{\times}$ und $\zeta_0\in\mathcal{O}_K$ so gewählt, dass ζ_0 in der Restklasse $\overline{\zeta}$ liegt. Weiters sei $\pi\in\mathcal{O}_K$ eine Uniformisierende.

Wir behaupten nun, dass es in $\mathcal{O}_K$ ein Element ζ gibt, welches Nullstelle des Polynoms $g(X)=X^{p^f-1}-1$ ist.

Es gilt $g(\zeta_0)=\zeta_0^{p^f-1}-1\equiv 0 \pmod\pi$. Außerdem ist $g'(\zeta_0)=\left(p^f-1\right)\zeta_0^{p^f-2}\not\equiv 0 \pmod{\pi^2}$, da ja $\left|\pi^2\right|_p=p^{-2/e}$ aber $\left|p^f-1\right|_p=|\zeta_0|_p^{p^f-2}=1$ gelten. Wir können analog wie im Beweis zum Henselschen Lemma auf Seite 53 vorgehen und zeigen, dass es ein Element ζ mit den gewünschten Eigenschaften gibt.

Dann ist $\zeta\equiv\overline{\zeta} \pmod\pi$. Die Restklassen $\overline{\zeta}$, $\overline{\zeta}^2$, $\ldots\overline{\zeta}^{p^f-1}$ sind paarweise verschieden, und dies gilt dann auch für ζ, ζ^2, $\ldots$, ζ^{p^f-1}. Das heißt, ζ ist eine primitive $\left(p^f-1\right)$-te Einheitswurzel, und es gilt $\left[\mathbb{Q}_p(\zeta):\mathbb{Q}_p\right]\geq\left[\kappa:\mathbb{F}_p\right]=f$, denn es ist ja $\kappa=\mathcal{O}_{\mathbb{Q}_p(\zeta)}/\mathcal{P}_{\mathbb{Q}_p}\cong\mathbb{F}_{p^f}$.

Es sei nun K_f^{unv} wie im ersten Teil des Beweises. Da K_f^{unv} alle $\left(p^f-1\right)$-te Einheitswurzel enthält, muss $\mathbb{Q}_p(\zeta)\subseteq K_f^{\mathrm{unv}}$ erfüllt sein. Da aber $f=\left[K_f^{\mathrm{unv}}:\mathbb{Q}_p\right]\geq\left[\mathbb{Q}_p(\zeta):\mathbb{Q}_p\right]\geq f$ gilt, ist $K_f^{\mathrm{unv}}=\mathbb{Q}_p(\zeta)$. Daher ist die unverzweigte Körpererweiterung vom Grad f eindeutig bestimmt.

Es bleibt noch zu zeigen, dass $K=K_f^{\mathrm{unv}}(\pi)$ gilt. Es sei $f(X)=\sum_{i=0}^d c_iX^i$ das Minimalpolynom von π über K_f^{unv}, und es seien π_1, $\ldots$, π_d die Konjugierten von $\pi=\pi_1$. Dann können wir $f(X)$ schreiben als $f(X)=\prod_{i=0}^d(X-\pi_i)$. Daher ist $c_0=(-1)^d\prod_{i=1}^d\pi_i$, und es gilt $\mathrm{ord}_p(c_0)=d\cdot\mathrm{ord}_p(\pi)=\frac{d}{e}$.

Es ist $\left[K:K_f^{\mathrm{unv}}\right]=e$, das folgt aus

$$n=e\cdot f=[K:\mathbb{Q}_p]=\left[K:K_f^{\mathrm{unv}}\right]\left[K_f^{\mathrm{unv}}:\mathbb{Q}_p\right]=\left[K:K_f^{\mathrm{unv}}\right]\cdot f.$$

Da klarerweise $K_f^{\text{unv}}(\pi) \subseteq K$ gilt, ist $d \leq e$. Bei der p-adische Ordnung von c_0 handelt es sich um eine ganze Zahl, denn c_0 liegt in K_f^{unv}. Daraus folgt, dass $d = e$ und somit $\text{ord}_p(c_0) = 1$ beziehungsweise $|c_0|_p = p^{-1}$ ist.

Das bedeutet, dass $c_0 \equiv 0 \pmod{p}$ und $c_0 \not\equiv 0 \pmod{p^2}$ gelten – $f(X)$ erfüllt also die Bedingungen eines Eisenstein-Polynoms, und wir erhalten $K = K_f^{\text{unv}}(\pi)$. □

Bemerkung 6: Die Vereinigung all dieser unverzweigten Körpererweiterungen ergibt eine unendliche Erweiterung über $\mathbb{Q}_p$. Diese wird manchmal mit $\mathbb{Q}_p^{\text{unv}}$ bezeichnet und heißt *die maximale unverzweigte Erweiterung.*

5.4 Der algebraische Abschluss $\overline{\mathbb{Q}}_p$ und dessen Vervollständigung $\mathbb{C}_p$

Der algebraische Abschluss von $\mathbb{Q}_p$ ist jener Erweiterungskörper, über dem jedes Polynom mit Koeffizienten in $\mathbb{Q}_p$ vollständig in Linearfaktoren zerfällt. Wir haben im vorigen Abschnitt gesehen, dass wir endliche Körpererweiterungen beliebigen Grades über $\mathbb{Q}_p$ finden können. So besagt Proposition 11, dass es für jede positive ganze Zahl eine unverzweigte Körpererweiterung von eben diesem Grad über $\mathbb{Q}_p$ gibt.

Auch lässt sich mit Hilfe des im letzten Abschnitt besprochenen Irreduzibilitätskriteriums leicht zeigen, dass für jedes $n \geq 1$ ein irreduzibles Polynom n-ten Grades über $\mathbb{Q}_p$ und eine entsprechende total verzweigte Köpererweiterung existiert.

Daher gilt:

Proposition 12: Der algebraische Abschluss $\overline{\mathbb{Q}}_p$ ist eine unendliche Erweiterung über $\mathbb{Q}_p$.

Wir können den p-adischen Absolutbetrag ohne Schwierigkeiten zu einer Funktion

$$|\,|_p : \overline{\mathbb{Q}}_p \to \mathbb{R}$$

fortsetzen, denn für jedes Element x im algebraischen Abschluss $\overline{\mathbb{Q}}_p$ ist die Körpererweiterung $\mathbb{Q}_p(x)/\mathbb{Q}_p$ endlich. Auf dieser ist $|x|_p$ eindeutig bestimmt, und wir haben uns in Abschnitt 5.3.1 bereits überlegt, dass der Wert des Absolutbetrags von x nicht von der Körpererweiterung abhängt.

Aufgrund dieser Überlegung lassen sich die Eigenschaften eines Absolutbetrags lassen für $|\,|_p : \overline{\mathbb{Q}}_p \to \mathbb{R}$ leicht zeigen, für (A2) und (A3) betrachten wir einfach den Erweiterungskörper $\mathbb{Q}_p(x, y)$.

Wie wir wissen, ist jede endliche Körpererweiterung über $\mathbb{Q}_p$ bezüglich des p-adischen Absolutbetrags vollständig. Jedoch gilt dies nicht notwendigerweise für $\overline{\mathbb{Q}}_p$. Im nächsten Satz soll diese Frage geklärt werden. Dazu benötigen wir noch folgenden Begriff:

Definition 7: Ein topologischer Raum $X \neq \emptyset$ heißt *ein Baire-Raum*, wenn für jede abzählbare Vereinigung von abgeschlossenen Teilmengen X_n mit $\bigcup_{n\geq 1} X_n = X$ gilt, dass mindestens eine Menge X_m einen inneren Punkt besitzt.

Vollständige metrische Räume sowie lokalkompakte Räume sind Baire-Räume.

Eine Menge $X_j \subseteq X$ wird *nirgends dicht* genannt, wenn $\overline{X_j}$ keine inneren Punkte besitzt. Das bedeutet also, dass ein vollständiger metrischer Raum nicht als abzählbare Vereinigung nirgends dichter Teilmengen dargestellt werden kann.

Satz 3: Der algebraische Abschluss von $\mathbb{Q}_p$ ist kein Baire-Raum.

Beweis. Für positive ganze Zahlen n definieren wir

$$X_n := \left\{x \in \overline{\mathbb{Q}}_p : \ [\mathbb{Q}_p(x) : \mathbb{Q}_p] = n\right\} \subseteq \overline{\mathbb{Q}}_p.$$

Dann ist $\overline{\mathbb{Q}}_p = \bigcup_{n\in\mathbb{N}} X_n$. Dass $X_n \neq \overline{\mathbb{Q}}_p$ für alle n gilt, folgt aus unseren Überlegungen am Beginn dieses Abschnitts.

Die Teilmengen X_n sind als endliche Körpererweiterungen vollständig und somit abgeschlossen.

Wir nehmen nun an, dass es eine Teilmenge X_m gibt, die eine in $\overline{\mathbb{Q}}_p$ abgeschlossene Kugel $\overline{B}_r(a)$ mit $r > 0$ enthält. Dann können wir den algebraischen Abschluss schreiben als $\overline{\mathbb{Q}}_p = \mathbb{Q}_p\overline{B}_r(a)$. Für $\lambda \in \mathbb{Q}_p$ gilt $\lambda X_m \subseteq X_m$. Daraus folgt $\overline{\mathbb{Q}}_p \subseteq \lambda X_m \subseteq X_m$, was aber nicht sein kann.

Eine solche Kugel $\overline{B}_r(a)$ ist also in keiner Teilmenge X_n enthalten, und das ist gleichbedeutend damit, dass keine Teilmenge X_n einen inneren Punkt besitzt. □

Bemerkung 7: Daraus folgt auch, dass $\overline{\mathbb{Q}}_p$ nicht lokalkompakt ist.

Im Gegensatz zum algebraischen Abschluss der reellen Zahlen ist jener von $\mathbb{Q}_p$ also nicht mehr vollständig. Bevor wir uns die Frage stellen, ob die Vervollständigung von $\overline{\mathbb{Q}}_p$ algebraisch abgeschlossen ist oder nicht, werden wir noch zwei interessante Resultate besprechen.

Das erste heißt *Krasnersches Lemma* und besagt, dass eine von einem Element α erzeugte Körpererweiterung in einer von einem Element β erzeugten enthalten ist, wenn nur β „näher“ bei α liegt als alle Konjugierten von α :

Satz 4 (Krasnersches Lemma): Es sei F ein vollständiger Körper der Charakteristik 0, der mit einem nichtarchimedischen Absolutbetrag $|\ |$ ausgestattet ist, und es seien α und β zwei Elemente des algebraischen Abschlusses $\overline{F}$ von F. Weiters sei $|\ |$ eindeutig von F auf $\overline{F}$ fortgesetzt. Die Konjugierten von $\alpha = \alpha_1$ über F seien $\alpha_1, \ldots, \alpha_n$, und es gelte

$$|\beta - \alpha| < |\alpha - \alpha_i|$$

für $i = 2, \ldots, n$. Dann ist $F(\alpha) \subseteq F(\beta)$.

Beweis. Es sei $L = F(\beta)$. Wir nehmen an, dass α nicht in L liegt. Daher ist $n = [L(\alpha) : L] > 1$. Es ist n auch die Anzahl der Homomorphismen $\sigma_i : \ L(\alpha) \to \overline{F}$ mit $\sigma_i(\alpha) = \alpha_i$, $1 \leq i \leq n$ und $\sigma_i|L = \mathrm{id}_L$. Wir schreiben σ' für σ_2.

In Abschnitt 5.3.1 haben wir uns bereits überlegt, dass in $\overline{F}$

$$|\sigma_i(x)| = |x|$$

für alle Homomorphismen σ_i und für alle $x \in L(\alpha)$ gilt.

Daher ist $\left|\sigma'(\beta-\alpha)\right| = \left|\sigma'(\beta)-\sigma'(\alpha)\right| = |\beta-\alpha|$. Da β in L liegt, folgt $\left|\beta-\sigma'(\alpha)\right| = |\beta-\alpha|$, und es ist

$$\left|\alpha-\sigma'(\alpha)\right| = |\alpha-\alpha_2| \leq \max\left\{|\alpha-\beta|, \left|\beta-\sigma'(\alpha)\right|\right\} = |\beta-\alpha|.$$

Nach Voraussetzung ist aber $|\beta-\alpha| < |\alpha-\alpha_2|$. Somit kann die Annahme, dass α nicht in L liegt, nicht stimmen, und es folgt $F(\alpha) \subseteq F(\beta)$. □

Folgendes Resultat bringt zum Ausdruck, dass die Wurzeln eines Polynoms über einem nichtarchimedischen Körper stetig von seinen Koeffizienten abhängen. Das bedeutet, dass aus der „Nähe“ zweier Polynome zueinander auch die „Nähe“ der entsprechenden Nullstellen folgt.

Um so eine Aussage überhaupt treffen zu können, benötigen wir noch eine Funktion, die es ermöglicht, den „Abstand“ zweier Polynome zu messen:

Es sei K ein bewerteter Körper und $f(X) = \sum_{i=0}^{n} a_i X^i$ ein Polynom über K. Dann verstehen wir unter der *Norm* $\|\ \|$ *von* f die Supremumsnorm der Koeffizienten von $f(X)$, das heißt, $\|f\| = \max_{1\leq i\leq n} |a_i|$.

Proposition 13: Es sei F ein Körper der Charakteristik 0, $|\ |$ ein nichtarchimedischer Absolutbetrag auf F, der auf $\overline{F}$ fortgesetzt wird, und $f(X) \in F[X]$ ein normiertes, irreduzibles Polynom vom Grad n, das keine doppelten Nullstellen besitzt. Dann gibt es zu jedem $\epsilon > 0$ ein $\delta > 0$, sodass für alle Polynome $g(X) \in F[X]$ mit $\deg g = n$, die der Bedingung $\|f-g\| < \delta$ genügen, folgt, dass für jede Wurzel α von $f(X)$ genau eine Wurzel β von $g(X)$ existiert, sodass $|\alpha-\beta| < \epsilon$ erfüllt ist. Insbesondere ist dann $F(\alpha) = F(\beta)$.

Beweis. Es sei $f(X) = \sum_{i=0}^{n} a_i X^i$ ein Polynom über F, das den Voraussetzungen entspricht, und $\epsilon > 0$. Weiters sei $g(X) \in F[X]$ vom Grad n und β eine Wurzel dieses Polynoms. Dann gilt klarerweise $g(\beta) = 0$. Daher ist

$$\begin{aligned} |f(\beta)| = |f(\beta)-g(\beta)| &= \left|\sum_{i=0}^{n} (a_i-b_i)\beta^i\right| \\ &\leq \max_{0\leq i\leq n}\left\{\left|a_i-b_i\right|\left|\beta^i\right|\right\} \\ &\leq \|f-g\| \max\left\{1, \left|\beta\right|^n\right\} \\ &< \delta c_1^n \end{aligned}$$

für eine entsprechende Konstante c_1. So eine Konstante gibt es, denn ist $\|g\| < c$ für eine Konstante c, dann sind auch die Wurzeln von $g(X)$ nicht so groß, und wir können ein c_1 finden, sodass $\max\left\{1, \left|\beta_i\right|\right\} < c_1$ für jede Wurzel β_i von $g(X)$ erfüllt ist.

Es seien α_i, $i = 1, \ldots, n$ die Nullstellen von $f(X)$. Wir wählen einen Index k, sodass $|\beta-\alpha_k|$ minimal ist, dann gilt

$$\delta c_1^n > |f(\beta)| = \left|\prod_{i=1}^{n}(\beta-\alpha_i)\right| = \prod_{i=1}^{n}|\beta-\alpha_i| \geq |\beta-\alpha_k|^n.$$

Es sei nun $c_2 := \min_{1\leq i<j\leq n}\{|\alpha_i-\alpha_j|\}$. Da die Nullstellen von $f(X)$ paarweise verschieden sind, ist $c_2 \neq 0$. Für höchstens eine Wurzel α_k kann $|\beta-\alpha_k| < c_2$ sein, denn wäre dies auch erfüllt für ein $\alpha_l \neq \alpha_k$, so würde das der Minimalität von c_2 widersprechen, wir hätten dann nämlich

$$|\alpha_l-\alpha_k| \leq \max\{|\alpha_l-\beta|, |\beta-\alpha_k|\} < c_2.$$

Insgesamt folgt also

$$\left|\beta - \alpha_k\right| < \frac{\delta c_1^n}{\prod_{i \neq k} |\beta - \alpha_i|} \leq \frac{\delta c_1^n}{c_2^{n-1}}.$$

Für $\delta \to 0$ wird $\left|\beta - \alpha_k\right|$ somit kleiner als jedes $\epsilon > 0$.

Dass $F(\alpha) \subseteq F(\beta)$ gilt, folgt aus dem Krasnerschen Lemma. Es hat α als Wurzel des irreduziblen Polynoms $f(X)$ den Grad n über F. Der Grad von β über F ist aber auch nicht größer als n, denn wir haben ja vorausgesetzt, dass der Grad von $g(X)$ gleich dem Grad von $f(X)$ ist. Daraus folgt $F(\alpha) = F(\beta)$. □

Unser Ziel ist es, eine Körpererweiterung von $\mathbb{Q}_p$ zu finden, die sowohl vollständig als auch algebraisch abgeschlossen ist. Deshalb werden wir als Nächstes die Vervollständigung von $\overline{\mathbb{Q}}_p$ auf diese Fragestellung hin untersuchen.

Da es sich bei $\overline{\mathbb{Q}}_p$ um einen metrischen Raum handelt, gibt es eine solche Vervollständigung. Wir bezeichnen diese mit $\mathbb{C}_p$.

Proposition 14: Es gibt einen vollständigen Körper $\mathbb{C}_p$ mit folgenden Eigenschaften:

- $\overline{\mathbb{Q}}_p$ liegt dicht in $\mathbb{C}_p$.
- Der p-adische Absolutbetrag $|\ |_p$ auf $\overline{\mathbb{Q}}_p$ lässt sich eindeutig auf $\mathbb{C}_p$ fortsetzen. Diese Fortsetzung ist ebenfalls nichtarchimedisch, und wir bezeichnen sie wieder mit $|\ |_p$.
- Die Wertemenge von $|\ |_p$ auf $\mathbb{C}_p$ stimmt mit jener auf $\overline{\mathbb{Q}}_p$ überein, es gilt also

$$|\mathbb{C}_p|_p = \left|\overline{\mathbb{Q}}_p\right|_p = \{p^n : n \in \mathbb{Q}\} \cup \{0\}.$$

- $\mathbb{C}_p$ ist bezüglich $|\ |_p$ vollständig.

Beweis. Alle Aussagen folgen unmittelbar aus Kapitel 3. □

Wir bezeichnen den Bewertungsring von $\mathbb{C}_p$ mit $\mathcal{O}_{\mathbb{C}_p} = \left\{x \in \mathbb{C}_p : \ |x|_p \leq 1\right\}$ und mit $\mathcal{P}_{\mathbb{C}_p} = \left\{x \in \mathbb{C}_p : \ |x|_p < 1\right\}$ das Bewertungsideal.

Jedes $x \in \mathbb{C}_p$, $x \neq 0$ kann als Produkt

1. einer Potenz p^m von p mit $m \in \mathbb{Q}$,
2. einer $\left(p^f - 1\right)$-ten Einheitswurzel und
3. eines Elements aus $1 + \mathcal{P}_{\mathbb{C}_p}$

geschrieben werden. Denn betrachten wir ein $x \in \mathbb{C}_p$ mit $\mathrm{ord}_p(x) = m = \frac{a}{b}$ und wählen eine Wurzel $\alpha \in \overline{\mathbb{Q}}_p$ von $f(X) = X^b - p^a$, dann gilt $|\alpha|_p = p^{-m}$. Außerdem ist $y = \frac{x}{\alpha}$ eine Einheit, also $|y|_p = 1$.

Als Nächstes versuchen wir, y als entsprechendes Produkt zu schreiben. Da $\overline{\mathbb{Q}}_p$ dicht in $\mathbb{C}_p$ liegt, gibt es ein $y^{'} \in \overline{\mathbb{Q}}_p$, sodass $y + \mathcal{P}_{\mathbb{C}_p} = y^{'} + \mathcal{P}_{\mathbb{C}_p}$ beziehungsweise $\left|y - y^{'}\right|_p < 1$ erfüllt ist. Aus der nichtarchimedischen Dreiecksungleichung folgt $\left|y^{'}\right|_p = 1$.

Da $y^{'}$ im algebraischen Abschluss von $\mathbb{Q}_p$ liegt, gibt es ein Minimalpolynom $g(X) = \sum_{i=0}^{n} a_i X^i$ von $y^{'}$ über $\mathbb{Q}_p$. Die Koeffizienten a_i können aus $\mathbb{Z}_p$ gewählt werden, das folgt mit Hilfe der elementarsymmetrischen Polynome für alle Konjugierten $y_1, \ldots, y_n$ von $y^{'} = y_1$ wegen $\left|y^{'}\right|_p = \left|y_i\right|_p = 1$.

Ist $K/\mathbb{Q}_p$ eine endliche Körpererweiterung und G die Gruppe der Einheitswurzeln in K, deren Ordnung relativ prim zu p ist, dann ist, wie wir in Abschnitt 5.3.2 gesehen haben, $\epsilon : \ G \to (\mathcal{O}_K/\mathcal{P}_K)^{\times}$ ein Isomorphismus.

Betrachten wir nun $\overline{g}(X) = \sum_{i=0}^{n} (a_i + p\mathbb{Z}_p) X^i$, dann ist $y^{'} + \mathcal{P}_{\mathbb{C}_p}$ eine Wurzel von $\overline{g}(X)$ und somit auch $y + \mathcal{P}_{\mathbb{C}_p}$. Das bedeutet, $y + \mathcal{P}_{\mathbb{C}_p}$ ist algebraisch über $\mathbb{Z}_p/p\mathbb{Z}_p$ und liegt daher im Restklassenkörper κ einer endlichen Körpererweiterung $K/\mathbb{Q}_p$. Da κ und $\mathbb{F}_{p^f}$ für eine positive ganze Zahl f isomorph sind, gibt es wegen der Surjektivität von ϵ eine $\left(p^f - 1\right)$-te Einheitswurzel ζ, sodass $\zeta + \mathcal{P}_{\mathbb{C}_p} = y + \mathcal{P}_{\mathbb{C}_p}$ beziehungsweise $|\zeta - y|_p < 1$ gilt, und es ist dann

$$\left(y + \mathcal{P}_{\mathbb{C}_p}\right)^{p^f - 1} = 1 + \mathcal{P}_{\mathbb{C}_p}.$$

Wir setzen nun $z = \frac{y}{\zeta}$. Dann liegt z in der Restklasse $1 + \mathcal{P}_{\mathbb{C}_p}$.

Es ist nämlich $z + \mathcal{P}_{\mathbb{C}_p} = 1 + \mathcal{P}_{\mathbb{C}_p}$ genau dann, wenn $|z - 1|_p = \left|\frac{y}{\zeta} - 1\right|_p < 1$ gilt. Das können wir auch schreiben als $\left|\zeta^{-1}\right|_p |y - \zeta|_p < 1$, und von dieser Ungleichung wissen wir, dass sie erfüllt ist.

Insgesamt folgt also, dass ein Element $x \in \mathbb{C}_p$, $x \neq 0$ geschrieben werden kann als Produkt $x = \alpha y = \alpha\zeta z$, wobei ζ eine $\left(p^f - 1\right)$-te Einheitswurzel darstellt, z ein Element der Restklasse $1 + \mathcal{P}_{\mathbb{C}_p}$ ist und α einer Potenz p^m von p mit $m \in \mathbb{Q}$ entspricht.

Diese Darstellung ist sogar eindeutig: Ist nämlich $\alpha\zeta z = 1$, so sehen wir zunächst, dass $\alpha = 1$ gilt. Dann folgt $1 = \zeta z \in \zeta + \mathcal{P}_K$, das heißt, $\epsilon(\zeta) = 1 + \mathcal{P}_K$. Da ϵ injektiv ist, ist $\zeta = 1$. Somit ist auch $z = 1$.

Das nächste Resultat zeigt: Die Vervollständigung des algebraischen Abschlusses der Vervollständigung der rationalen Zahlen bezüglich des p-adischen Absolutbetrags ist tatsächlich algebraisch abgeschlossen!

Satz 5: $\mathbb{C}_p$ ist algebraisch abgeschlossen.

Beweis. Es sei $L/\mathbb{C}_p$ eine endliche Körpererweiterung, die von einem Element α erzeugt wird, das heißt, $L = \mathbb{C}_p(\alpha)$. Das Minimalpolynom $f(X) \in \mathbb{C}_p[X]$ von α sei vom Grad $n \geq 1$.

Da der algebraische Abschluss von $\mathbb{Q}_p$ dicht in $\mathbb{C}_p$ liegt, können wir ein Polynom $g(X) \in \overline{\mathbb{Q}}_p$ derart wählen, dass – wie in Proposition 13 auf Seite 101 – die Koeffizienten der Polynome nahe genug beieinander liegen, sodass $L = \mathbb{C}_p(\beta)$ für eine Wurzel β von $g(X)$ gilt.

Nun ist aber $\overline{\mathbb{Q}}_p$ algebraisch abgeschlossen, und das bedeutet, dass alle Wurzeln von $g(X)$ in $\overline{\mathbb{Q}}_p$ sind und $\deg g = 1$ gilt. Somit ist auch $n = 1$, und es folgt $L = \mathbb{C}_p$. □

Mit $\mathbb{C}_p$ haben wir also letztendlich eine Körpererweiterung über $\mathbb{Q}_p$ gefunden, die sowohl vollständig als auch algebraisch abgeschlossen ist. Damit stellt $\mathbb{C}_p$ das p-adische Äquivalent zu den komplexen Zahlen dar.

Bemerkung 8: Bemerkung 1 auf Seite 80 besagt, dass ein lokalkompakter, normierter Vektorraum über $\mathbb{Q}_p$ jedenfalls endlichdimensional ist. Daher ist $\mathbb{C}_p$ nicht lokalkompakt.

5.5 Analysis in $\mathbb{C}_p$

Abschnitt 4.6 vermittelt einen Eindruck, welche Gestalt grundlegende Ideen und Methoden aus der Analysis im Körper der p-adischen Zahlen annehmen. Die dort angestellten Überlegungen hängen vor allem von der ultrametrischen Struktur des Körpers und nicht von $\mathbb{Q}_p$ im Speziellen ab, daher lassen sich die meisten Resultate ohne Probleme sowohl auf endliche Körpererweiterungen $K/\mathbb{Q}_p$ als auch auf $\mathbb{C}_p$ übertragen.

Im Falle einer endlichen Körpererweiterung über $\mathbb{Q}_p$ muss dabei der Verzweigungsindex e berücksichtigt werden. Ist dieser größer als Eins, erhöht sich der Werteumfang von $|\ |_p$, und es ist gegebenenfalls eine Uniformisierende π zu verwendet.

Nun wollen wir aber die Resultate, die aus Abschnitt 4.6 für $\mathbb{C}_p$ folgen, zusammenfassen:

- Eine Folge $(x_n)_{n\geq 1}$ in $\mathbb{C}_p$ ist genau dann eine Cauchyfolge, wenn $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$ ist. Da $\mathbb{C}_p$ vollständig ist, konvergiert jede solche Folge.
  Ist $x \neq 0$ der Grenzwert einer Folge $(x_n)_{n\geq 1}$ in $\mathbb{C}_p$, dann gibt es einen Index N, sodass $|x_m|_p = |x|_p$ für alle $m \geq N$ gilt.
- Eine unendliche Reihe $\sum_{i=0}^{\infty} x_i$ über $\mathbb{C}_p$ konvergiert genau dann, wenn $|x_i|_p \to 0$ für $i \to \infty$ gilt. Es ist dann $|\sum_{i=0}^{\infty} x_i|_p \leq \max_i |x_i|_p$.
  Jede konvergente Reihe über $\mathbb{C}_p$ konvergiert unbedingt. Die Doppelreihen
  $$\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} x_{ij}\right) \quad \text{und} \quad \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} x_{ij}\right)$$
  mit $x_{ij} \in \mathbb{C}_p$ für alle i, j konvergieren gegen den gleichen Grenzwert, wenn es für jedes $\epsilon > 0$ ein $N = N(\epsilon)$ gibt, sodass $|x_{ij}|_p < \epsilon$ für $\max\{i, j\} \geq N$ gilt.
- Eine Potenzreihe $f(X) = \sum_{n=0}^{\infty} a_n X^n$ mit Koeffizienten a_n in $\mathbb{C}_p$ und Konvergenzradius
  $$\rho = \frac{1}{\limsup \sqrt[n]{|a_n|_p}}$$
  stellt eine stetige Funktion dar. Der Konvergenzbereich der Potenzreihe entspricht entweder der „offenen“ Kugel $\mathcal{D} = \{x \in \mathbb{C}_p : |x|_p < \rho\}$ oder aber – falls $|a_n|_p \rho^n \to 0$ für $n \to \infty$ gilt – der „abgeschlossenen“ Kugel $\mathcal{D} = \{x \in \mathbb{C}_p : |x|_p \leq \rho\}$.
  Jede Potenzreihe $f(X)$ mit Koeffizienten in $\mathcal{O}_{\mathbb{C}_p}$ konvergiert in der Einheitskugel $B_1(0)$. Es sei darauf hingewiesen, dass im Gegensatz zu der Situation in $\mathbb{Q}_p$, wo $B_1(0) = \overline{B}_{p^{-1}}(0)$ oder allgemein $B_\rho(0) = \overline{B}_{\rho p^{-1}}(0)$ gilt, sich dies in $\mathbb{C}_p$ nicht so darstellen lässt, denn die Wertemenge von ord_p umfasst hier ja ganz $\mathbb{Q}$.
  Durch Potenzreihen definierte Funktionen sind differenzierbar, die jeweilige Ableitung entspricht im Konvergenzbereich der formalen Ableitung der Potenzreihe.

- Der p-adische Logarithmus

$$\log_p : \mathcal{D} \to \mathbb{C}_p$$

mit $\mathcal{D} = B_1(0) = \mathcal{P}_{\mathbb{C}_p}$ ist durch folgende Potenzreihe definiert:

$$\log_p(1+X) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} X^n = X - \frac{X^2}{2} + \frac{X^3}{3} - \frac{X^4}{4} + \cdots .$$

Für Elemente $x,\ y \in \mathcal{D}$ gilt

$$\log_p((1+x)(1+y)) = \log_p(1+x) + \log_p(1+y)$$

sowie

$$\log_p'(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} x^{n-1} = \frac{1}{1+x}.$$

- Die p-adische Exponentialfunktion

$$\exp_p : \mathcal{D} \to \mathbb{C}_p$$

mit $\mathcal{D} = \left\{x \in \mathcal{P}_{\mathbb{C}_p} : |x|_p < p^{-1/(p-1)}\right\} = B_\rho(0)$, $\rho = p^{-1/(p-1)}$ ist durch folgende Potenzreihe definiert:

$$\exp_p(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!} = 1 + X + \frac{X^2}{2} + \frac{X^3}{6} + \cdots .$$

Auf $\mathcal{D}$ gilt für zwei Elemente $x,\ y$

$$\exp_p(x+y) = \exp_p(x)\exp_p(y)$$

sowie

$$\exp_p'(x) = \exp_p(x).$$

In $\mathbb{C}_p$ als p-adisches Äquivalent zu den komplexen Zahlen eröffnet sich das weite Gebiet der „komplexen“ p-adischen Analysis. Viele der klassischen Sätze sind auch im p-adischen Kontext von Interesse, so zum Beispiel *der Vorbereitungssatz von Weierstraß*, welcher bei der Darstellung von ganzen Funktionen auf $\mathbb{C}_p$ eine Rolle spielt, *das p-adische Mittag-Leffler Theorem*, das die Existenz von meromorphen Funktionen mit vorgegebenen Polstellen beschreibt, oder *der Satz von Liouville*, der wie in $\mathbb{C}$ auch in $\mathbb{C}_p$ besagt, dass eine beschränkte, ganze Funktion konstant ist (siehe zum Beispiel [9], Kapitel 6 und [18], Kapitel 6).

Quellen und Literatur zu Kapitel 5

Zu Abschnitt 5.1 vergleiche [1], S. 92-98, [8], S. 288 und [9], S. 134-143.
Abschnitt 5.2 basiert auf [3], S. 194-198, [9], S. 146-148 sowie [14], S. 59, 60 und Abschnitt 5.3 auf [6], S. 95-97, [9], S. 143-146, 150-169, [14], S. 61-69 und [18], S. 94-104.
Zu Abschnitt 5.4 vergleiche [9], S. 176-180, 184, 185, [14], S. 69-73, [18], S. 129-131, 143 sowie [19], S. 43, 44, 269, 270 und zu Abschnitt 5.5 [9], S. 187-189.

Symbolverzeichnis

$\dim_K V$	Dimension des Vektorraums V über dem Körper K
$\exp_p$	p-adische Exponentialfunktion
κ	Restklassenkörper
$[K : F]$	Grad der Körperweiterung K/F
$\| \|_\infty$	Supremumsnorm
$\| \|$	Norm auf einem Vektorraum
$\| \|$	Absolutbetrag auf einem Körper
$\| \|_\infty$	„gewöhnlicher“ Absolutbetrag auf $\mathbb{Q}$
$\| \|_p$	p-adischer Absolutbetrag
$\|K\|$	Wertemenge des Absolutbetrags $\| \|$ auf dem Körper K
$\log_p$	p-adischer Logarithmus
$\mathbb{C}$	komplexe Zahlen
$\mathbb{C}_p$	Vervollständigung von $\overline{\mathbb{Q}}_p$
$\mathbb{F}_q$	Körper mit $q = p^n$ Elementen
$\mathbb{N}$	natürliche Zahlen, einschließlich 0
$\mathbb{P}$	Menge der Primzahlen
$\mathbb{Q}$	rationale Zahlen
$\mathbb{Q}_p$	p-adische Zahlen
$\mathbb{R}$, $\mathbb{R}_+$	reelle Zahlen, positive reelle Zahlen

$\mathbb{R}^X$	reellwertige Funktionen auf der Menge X
$\mathbb{Z}$, $\mathbb{Z}_+$	ganze Zahlen, positive ganze Zahlen
$\mathbb{Z}_p$	ganze p-adische Zahlen
$\mathcal{O}_K$	Bewertungsring eines nichtarchimedischen Absolutbetrags auf K
$\mathcal{P}_K$	Bewertungsideal eines nichtarchimedischen Absolutbetrags auf K
$\mathcal{A}_\alpha$	Matrix der F-linearen Abbildung φ_α
$\mathcal{N}_{K/F}$	Norm der Körpererweiterung K/F
$\mathrm{char}\,(K)$	Charakteristik eines Körpers K
$\mathrm{Aut}_F\,(K)$	Automorphismen von K/F, die die Identität auf F fortsetzen
$\mathrm{Gal}\,(K/F)$	Galois-Gruppe der Körpererweiterung K/F
ord_p	p-adische Ordnung
G/H	Menge der Nebenklassen modulo H
$\overline{B}_r(a)$	abgeschlossene Kugel mit Mittelpunkt a und Radius r
$\overline{\mathbb{Q}}_p$	algebraischer Abschluss von $\mathbb{Q}_p$
$\overline{K}$	algebraischer Abschluss des Körpers K
τ_K	trivialer Absolutbetrag auf einem Körper
φ_α	F-lineare Abbildung, die auf K/F die Multiplikation mit $\alpha \in K$ beschreibt
$B_r(a)$	offene Kugel mit Mittelpunkt a und Radius r
$d(x,y)$	Metrik
K/F	Körpererweiterung K über F
$K_f^{\mathrm{unv}}/\mathbb{Q}_p$	unverzweigte Körpererweiterung über $\mathbb{Q}_p$ vom Grad f
$l^\infty\,(X)$	Raum der beschränkten, reellwertigen Funktionen auf der Menge X
$R\,[[X]]$	Ring der formalen Potenzreihen über R
$R^\times$	Einheitengruppe des Ringes R
$S_r(a)$	Sphäre mit Mittelpunkt a und Radius r

Literaturverzeichnis

[1] G. Bachman. *Introduction to P-Adic Numbers and Valuation Theory.* Academic Press Inc., 1964.

[2] Z.I. Borevich and I.R. Shafarevich. *Number theory (Pure and Applied Mathematics).* Academic Press Inc., New Ed. 1986.

[3] S. Bosch. *Algebra.* Springer-Verlag, 4., überarb. Aufl. 2001.

[4] N. Bourbaki. *Elements of mathematics. General topology: Chapters 1-4.* Springer-Verlag, Softcover edition of the 2nd printing 1989.

[5] P. Bundschuh. *Einführung in die Zahlentheorie.* Springer-Verlag, 5., überarb. und aktualisierte Aufl. 2002.

[6] J.W.S. Cassels. *Local Fields.* Cambridge University Press, First published 1986, digital printing 2003.

[7] H.D. Ebbinghaus. *Zahlen.* Springer-Verlag, 3., verb. Aufl. 1992.

[8] M. Giaquinta and G. Modica. *Mathematical Analysis: Linear and Metric Structures and Continuity.* Birkhäuser, 2007.

[9] F.Q. Gouvêa. *P-Adic Numbers: An Introduction.* Springer-Verlag, 2nd Ed., Corrected 3rd printing 2003.

[10] H. Heuser. Lehrbuch der Analysis, Teil 1. 11., durchges. Aufl. 1994.

[11] E. Hlawka and J. Schoißengeier. *Zahlentheorie: Eine Einführung.* MANZ Verlags- und Universitäsbuchhandlung, 2., neubearb. Aufl. 1990.

[12] K. Jänich. *Topologie.* Springer-Verlag, 8. Aufl., 1. kor. Nachdruck 2006.

[13] S. Katok. *P-Adic Analysis Compared with Real.* American Mathematical Society, 2007.

[14] N. Koblitz. *P-Adic Numbers, P-Adic Analysis, and Zeta-Functions.* Springer-Verlag, 1984.

[15] N. Koblitz. *P-adic Analysis: A Short Course on Recent Work*. Cambridge University Press, First published 1980, digital printing 2004.

[16] K. Mahler. *Introduction to p-adic numbers and their functions*. Cambridge University Press, 1973.

[17] J.J. O'Connor and E.F. Robertson. *The MacTutor History of Mathematics archive*. University of St. Andrews, Scotland. http://www-history.mcs.st-andrews.ac.uk/history/index.html.

[18] A. Robert. *A Course in P-Adic Analysis*. Springer-Verlag, 2000.

[19] W.H. Schikhof. *Ultrametric Calculus: An Introduction to P-Adic Analysis*. Cambridge University Press, First published 1984, digital printing 2006.

[20] J. Schoißengeier. Funktionalanalysis. Skriptum zur Vorlesung. Universität Klagenfurt, Sommersemester 2008.

[21] J. Schoißengeier. Kommutative Algebra. Skriptum zur Vorlesung. Universität Wien, Wintersemester 2006/2007.

[22] J.P. Serre. *A Course in Arithmetic*. Springer-Verlag, 1973.

[23] The PARI Group, Bordeaux. *PARI/GP, version* `2.3.4`, 2008. available from http://pari.math.u-bordeaux.fr.

[24] G. Walz. *Lexikon der Mathematik. Band 2*. Spektrum Akademischer Verlag, 2001.

[25] G. Walz. *Lexikon der Mathematik. Band 4*. Spektrum Akademischer Verlag, 2002.

Lebenslauf

Ich, Julia Neidhardt, wurde am 24. September 1978 in Klagenfurt, Österreich, geboren. Von 1985 bis 1989 besuchte ich die Volksschule und ab 1989 das Bundesgymnasium Mössingerstraße in Klagenfurt, an dem ich im Juni 1997 mit Auszeichnung maturierte. Im Herbst 1997 begann ich die Diplomstudien Mathematik und Physik an der Universität Wien zu studieren. Zusätzlich absolvierte ich zwischen Wintersemester 02/03 und Wintersemester 03/04 Lehrveranstaltungen im Ausmaß von 35 Semesterwochenstunden aus dem Schwerpunkt „Software & Information Engineering“ des Bakkalaureatsstudiums Informatik an der Technischen Universität Wien.

Während meiner Studienzeit engagierte ich mich in der Österreichischen HochschülerInnenschaft (ÖH) in der Studierenden- und Inskriptionsberatung, von 2002 bis 2003 als Sachbearbeiterin im Öffentlichkeitsreferat (Webseitenredaktion) der ÖH Universität Wien, von 2003 bis 2005 als Vorsitzende der Fakultätsvertretung Naturwissenschaften und Mathematik an der Universität Wien und von 2005 bis 2007 als Vorsitzende der Fakultätsvertretung Mathematik an der Universität Wien.

Von 2006 bis 2009 war ich als Tutorin bei Teil 1 und Teil 2 der Übungen zu „Technische Praxis der Computersysteme am Beispiel des Betriebssystems Linux“ an der Fakultät für Mathematik an der Universität Wien tätig und bin seit 2007 als freie Dienstnehmerin im Rahmen des Frauenförderungsprojekts der Fakultät für Mathematik an der Universität Wien bei der Erstellung und Umsetzung des Frauenförderungsplans beschäftigt.

Außerdem nehme ich seit 2003 regelmäßig in Deutschland am jährlich stattfindenden Kongress „Frauen in Naturwissenschaft und Technik“ teil, im Mai 2008 in Bonn auch als Referentin, und besuchte im September 2004 die „Informatica Feminale“, ein Sommerstudium für Frauen in der Informatik an der Universität Bremen, sowie im Juli 2008 die „14th International Conference of Women Engineers and Scientists“ in Lille, Frankreich.