Grundkonzept der p-adischen Zahlen anhand von Potenzreihen

Alina Jankowsky

12.01.2022

Fachseminar Algebra und Logik Wintersemester 2021/22

Universität Konstanz

Zusammenfassung

In diesem Fachseminar beschäftigen wir uns mit der Herleitung p-adischer Zahlen anhand von Potenzreihen. Angelehnt an die Zahlensysteme aus der Informatik, wie zum Beispiel das Binärsystem, werden wir rationale und einige reelle und komplexe Zahlen bezüglich Primzahlen und ihren Potenzen in Potenzreihen darstellen. In Abschnitt 2–4 beschäftigen wir uns damit, wie man natürliche, ganze und rationale Zahlen p-adisch entwickeln kann. In Abschnitt 5 fassen wir interessante Eigenschaften der p-adischen Entwicklungen zusammen. Im vorletzten Abschnitt zeigen wir, dass die Menge der ganzen p-adischen Zahlen ein diskreter Bewertungsring ist. Zuletzt geben wir einen Ausblick auf die Menge der p-adischen Zahlen, welche mit geeigenten Operationen einen Körper bilden.

Inhaltsverzeichnis

In dieser Arbeit bezeichnet $\mathbb{N}$ die Menge der positiven natürlichen Zahlen und wir definieren $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Mit $\mathbb{P}$ bezeichnen wir die Menge der Primzahlen und mit $\mathbb{F}_p$ den endlichen Körper mit den Elementen $0, \dots, p-1$, wobei $p \in \mathbb{P}$ gilt.

1 Einleitung

Kurt Hensel (1861–1941) beschrieb 1897 erstmals die p-adischen Zahlen. Sie wurden daraufhin in der Zahlentheorie unter anderem für das Lokal-Global-Prinzip von Hasse–Minkowski sowie für Hensels Lemma benutzt (siehe [6]).

Beim Lokal-Global-Prinzip geht es darum, ob Gleichungen über $\mathbb{Q}$ lösbar sind, wenn sie über $\mathbb{R}$ und den p-adischen Zahlen lösbar sind (siehe [1, Seiten 99–108]).

Das Lemma von Hensel findet Anwendung, wenn man wissen möchte, ob eine Gleichung eine Lösung in den p-adischen Zahlen hat (siehe [1, Seiten 88–99]).

Beides sind sehr wichtige Aussagen, aber um diese verstehen und anwenden zu können, müssen wir zunächst verstehen, was die p-adischen Zahlen sind. Dies ist das Thema dieses Seminars.

Wir benutzen stets Primzahlen, jedoch könnten wir die Resultate in den Abschnitten 2–6 auch mit natürlichen Zahlen beweisen. In Abschnitt 7 ist die Primeigenschaft notwendig, um zeigen zu können, dass die Menge aller p-adischen Zahlen ein Körper ist.

2 p-adische Entwicklung natürlicher Zahlen

Um an die p-adischen Zahlen heranzuführen, beginnen wir mit einem Beispiel.

Beispiel 2.1. Wir wollen 127 bezüglich der Basis $p = 5$ darstellen.
Es gilt

$$\begin{aligned} 127 &= 25 \cdot 5 + 2, \\ 25 &= 5 \cdot 5 + 0. \end{aligned}$$

Also gilt

$$127 = 25 \cdot 5 + 2 = (5 \cdot 5 + 0) \cdot 5 + 2 = 5 \cdot 5^2 + 2 \cdot 5^0 = 1 \cdot 5^3 + 0 \cdot 5^2 + 0 \cdot 5^1 + 2 \cdot 5^0.$$

Oft wird auch $127 = (1, 0, 0, 2)_{(5)}$ geschrieben.

Allgemein können wir alle natürlichen Zahlen bezüglich einer Primzahl p darstellen:

Satz 2.2. *Sei $p \in \mathbb{P}$ beliebig. Dann gibt es für jedes $n \in \mathbb{N}_0$ eine eindeutige Darstellung*

$$n = \sum_{k=0}^{\infty} a_k p^k,$$

wobei $a_k \in \{0, \ldots, p-1\}$ für alle $k \in \mathbb{N}_0$.

Beweis. Wir führen mehrmalige Divisionen durch p durch. Nach dem Divisionsalgorithmus (DA) erhalten wir

$$\begin{aligned} n &= n_1 \cdot p + a_0 \\ n_1 &= n_2 \cdot p + a_1 \\ n_2 &= n_3 \cdot p + a_2 \\ &\vdots \\ n_{j-1} &= n_j \cdot p + a_{j-1} \\ n_j &= 0 \cdot p + a_j, \end{aligned}$$

wobei $a_i < p$ nach DA, also $a_i \in \mathbb{F}_p$, und $n_i \in \mathbb{N}_0$ für alle $i \in \{0, \dots, j\}$ gilt.
Durch Rückwärtseinsetzen erhalten wir nun

$$\begin{aligned} n &= n_1 \cdot p + a_0 \\ &= (n_2 \cdot p + a_1) \cdot p + a_0 \\ &= n_2 \cdot p^2 + a_1 \cdot p + a_0 \\ &= (n_3 \cdot p + a_2) \cdot p^2 + a_1 \cdot p + a_0 \\ &= n_3 \cdot p^3 + a_2 \cdot p^2 + a_1 \cdot p + a_0 \\ &\vdots \\ &= \sum_{k=0}^{j} a_k p^k. \end{aligned}$$

Setze nun $a_k = 0$ für $k > j$. Dann gilt

$$n = \sum_{k=0}^{\infty} a_k p^k.$$

Die Eindeutigkeit folgt aus dem Konstruktionsprinzip und der Eindeutigkeit des Divisionsalgorithmus. □

3 p-adische Entwicklung ganzer Zahlen

Nun betrachten wir die ganzen Zahlen. Hierfür müssen wir Potenzreihen zulassen, also unendliche Summen, um negative Zahlen darstellen zu können. Um stets Wohldefiniertheit zu gewährleisten, betrachten wir die formalen Potenzreihen:

Definition 3.1 (formale Potenzreihe)**.** *Sei R ein kommutativer Ring mit 1, dann ist*

$$a_0 + a_1 X^1 + a_2 X^2 + \cdots = \sum_{k=0}^{\infty} a_k X^k$$

eine formale Potenzreihe, wobei $a_k \in R$ für alle $k \in \mathbb{N}_0$.
Manchmal schreibt man auch $(\dots, a_3, a_2, a_1, a_0)$, statt der Summenschreibweise.

Die Menge aller formalen Potenzreihen der Unbekannten X mit Koeffizienten in R wird mit $R[[X]]$ bezeichnet.

Sei nun R stets ein kommutativer Ring mit 1.

Definition 3.2 (Operationen auf formalen Potenzreihen)**.** *Wir definieren eine Addition und eine Multiplikation auf $R[[X]]$ durch*

$$+ : R[[X]] \times R[[X]] \to R[[X]], \quad \left(\sum_{k=0}^{\infty} a_k X^k\right) + \left(\sum_{k=0}^{\infty} b_k X^k\right) := \sum_{k=0}^{\infty} (a_k + b_k) X^k$$

$$\cdot : R[[X]] \times R[[X]] \to R[[X]], \quad \left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i X^i\right) := \sum_{i=0}^{\infty} \sum_{k=0}^{i} a_k b_{i-k} X^i$$

Die Addition ist wohldefiniert, da die Summe zweier Elemente aus R wieder in R liegt, da R unter Addition abgeschlossen ist.

Die Multiplikation ist wohldefiniert, da $\sum\limits_{k=0}^{i} a_k b_{i-k}$ als endliche Summe von endlichen Produkten von Elementen aus R wieder in R liegt, da R unter Addition und Multiplikation abgeschlossen ist.

Proposition 3.3. *Sei R ein Ring, dann ist $R[[X]]$ mit den Operationen aus Definition 3.2 ein Ring.*

Beweis. Siehe [2, Kapitel 1]. □

Wir betrachten nun formale Potenzreihen aus dem Ring $\mathbb{Z}[[p]]$ für ein beliebiges $p \in \mathbb{P}$.

Definition 3.4 (unechte p-adische Zahlen)**.** *Sei $p \in \mathbb{P}$. Wir nennen formale Potenzreihen, welche ausschließlich ganze Zahlen als Koeffizienten haben,* unechte p-adische Zahlen*. Eine unechte p-adische Zahl hat als die Form*

$$\sum_{k=0}^{\infty} a_k p^k,$$

wobei $a_k \in \mathbb{Z}$ für alle $k \in \mathbb{N}_0$.

Wir bezeichnen mit $\mathbb{U}_p$ die Menge aller unechten p-adischen Zahlen:

$$\mathbb{U}_p := \left\{ \sum_{k=0}^{\infty} a_k p^k \mid a_k \in \mathbb{Z} \, \forall k \in \mathbb{N}_0 \right\}.$$

Definition 3.5 (ganze p-adische Zahl)**.** *Sei $p \in \mathbb{P}$. Dann nennen wir eine formale Potenzreihe der Form*

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

wobei $a_i \in \{0, \ldots, p-1\}$ für alle $i \in \mathbb{N}_0$, eine ganze p-adische Zahl*.*

Wir bezeichnen mit $\mathbb{Z}_p$ die Menge aller ganzen p-adischen Zahlen:

$$\mathbb{Z}_p := \left\{ \sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, \ldots, p-1\} \, \forall i \in \mathbb{N}_0 \right\}.$$

Definition 3.6 (p-adische Zahlen)**.** *Sei $p \in \mathbb{P}$. Dann nennen wir eine formale Potenzreihe der Form*

$$\sum_{i=-n}^{\infty} a_i p^i,$$

wbei $a_i \in \{0, \dots, p-1\}$ für alle $i \in \mathbb{Z}$ und $n \in \mathbb{N}_0$, eine p-adische Zahl.

Wir bezeichnen mit $\mathbb{Q}_p$ die Menge aller p-adischen Zahlen:

$$\mathbb{Q}_p := \left\{ \sum_{i=-n}^{\infty} a_i p^i \mid a_i \in \{0, \dots, p-1\} \, \forall i \in \mathbb{Z}, n \in \mathbb{N}_0 \right\}.$$

Bemerkung 3.7. Wir wollen nun eine Möglichkeit finden, unechte p-adische Zahlen p-adisch darzustellen, damit wir im Folgenden bei Beweisen keine Probleme mit den Überträgen der Koeffizienten von Potenzreihen bekommen. Wir werden induktiv aus einer beliebigen unechten p-adischen Zahl eine zugehörige p-adische Zahl ableiten:
Sei dazu $a = \sum_{k=0}^{\infty} a_k p^k \in \mathbb{U}_p$ beliebig. Wir beginnen mit a_0. Nach dem DA existieren eindeutige $b_0, r_0 \in \mathbb{Z}$ mit $a_0 = b_0 \cdot p + r_0$, wobei $0 \leq r_0 < p$ gilt. Wir setzen $\bar{a}_0 := r_0$ und erhalten den Übertrag $b_0 \in \mathbb{Z}$. Wir definieren $a_1' := a_1 + b_0$. Nach dem DA existieren nun eindeutige $b_1, r_1 \in \mathbb{Z}$, mit $a_1' = b_1 \cdot p + r_1$, wobei $0 \leq r_1 < p$ gilt. Wir setzen $\bar{a}_1 := r_1$ und bekommen den Übertrag $b_1 \in \mathbb{Z}$.
Induktiv definieren wir nun $\bar{a}_k := r_k$, und $a_{k+1}' = a_{k+1} + b_k$. Nach dieser Konstruktion erhalten wir eine eindeutige p-adische Zahl $\bar{a} := \sum_{k=0}^{\infty} \bar{a}_k p^k$, wobei $\bar{a}_k \in \{0, \dots, p-1\}$ für alle $k \in \mathbb{N}_0$ gilt.

Lemma 3.8. *Sei p eine Primzahl. Wir definieren eine Funktion f durch*

$$f : \mathbb{U}_p \to \mathbb{Z}_p, \quad \sum_{k=0}^{\infty} a_k p^k \mapsto \sum_{k=0}^{\infty} \bar{a}_k p^k,$$

wobei $a_k \in \mathbb{Z}$ und $\bar{a}_k \in \mathbb{F}_p$ für alle $k \in \mathbb{N}_0$ definiert ist wie in Bemerkung 3.7. Dann gelten:

(i) f ist wohldefiniert,

(ii) f ist surjektiv,

(iii) Die Relation $\sim$, welche durch $a \sim b :\Leftrightarrow f(a) = f(b)$ definiert ist, ist eine Äquivalenzrelation auf $\mathbb{U}_p$.

Beweis.

(i) Nach dem Konstruktionsprinzip in Bemerkung 3.7 erhalten wir direkt die Wohldefiniertheit aufgrund des DA.

(ii) Fassen wir $\mathbb{F}_p$ als Menge auf, so gilt $\mathbb{F}_p \subset \mathbb{Z}$. Also kann jede p-adische Zahl auch als eine unechte p-adische Zahl verstanden werden. Somit gilt für alle $\bar{a} \in \mathbb{Z}_p$, dass $\bar{a} \in \mathbb{U}_p$. Da alle Koeffizienten von $\bar{a}$ bereits in $\mathbb{F}_p$ liegen, gilt $\bar{\bar{a}}_k = 0 \cdot p + \bar{a}_k = \bar{a}_k$, da $\bar{a}_k < p$ für alle $k \in \mathbb{N}_0$ gilt. Also gilt nach Definition $f(\bar{a}) = \bar{a}$, was die Surjektivität von f impliziert.

(iii) Seien $a, b, c \in \mathbb{U}_p$ beliebig.

- Reflexivität: Es gilt $f(a) = f(a)$, da f nach (i) wohldefiniert ist. Also folgt $a \sim a$ nach Definition der Äquivalenzrelation.

- Symmetrie: Gelte $a \sim b$, also $f(a) = f(b)$. Dann folgt sofort $f(b) = f(a)$, und somit $b \sim a$.
- Transitivität: Gelte $a \sim b$ und $b \sim c$. Dann gilt $f(a) = f(b)$ und $f(b) = f(c)$. Es folgt nun $f(a) = f(b) = f(c)$, also insbesondere $f(a) = f(c)$, und damit $a \sim c$.

Also definiert $\sim$ eine Äquivalenzrelation auf $\mathbb{U}_p$.

□

Da f surjektiv ist, erhalten wir, dass jede p-adische Zahl in einer Äquivalenzklasse enthalten ist. Da für $f|_{\mathbb{Z}_p} : \mathbb{Z}_p \to \mathbb{Z}_p$ gerade $f|_{\mathbb{Z}_p} = \mathrm{id}_{\mathbb{Z}_p}$ gilt, ist $f|_{\mathbb{Z}_p}$ bijektiv und wir erhalten, dass jede Äquivalenzklasse genau eine p-adische Zahl enthält. Wir wählen nun stets die p-adische Zahl als Repräsentanten der jeweiligen Äquivalenzklasse. Somit können wir in allen folgenden Beweisen ohne Einschränkung auch Zwischenschritte über unechte p-adische Zahlen machen.

Beispiel 3.9. Wir stellen -1 bezüglich einer beliebigen Basis $p \in \mathbb{P}$ dar. Es gilt

$$\begin{aligned} -1 &= -1 \cdot p^0 \\ &= (p-1) \cdot p^0 - 1 \cdot p^1 \\ &= (p-1) \cdot p^0 + (p-1) \cdot p^1 - 1 \cdot p^2 \\ &= (p-1) \cdot p^0 + (p-1) \cdot p^1 + (p-1) \cdot p^2 - 1 \cdot p^3 \\ &= \dots \end{aligned}$$

Wir erhalten also

$$-1 = \lim_{n\to\infty} \sum_{i=0}^{n} (p-1) \cdot p^i = (p-1) \cdot \sum_{i=0}^{\infty} p^i.$$

Wähle $a_i = p - 1$ für jedes $i \in \mathbb{N}$, dann gilt $-1 = \lim_{n\to\infty} \sum_{i=0}^{n} a_i p^i$ mit $a_i \in \{0, \dots, p-1\}$.
Für $p = 3$ erhalten wir zum Beispiel $-1 = (\dots, 2, 2, 2, 2)_{(3)}$.

Um negative Zahlen darzustellen, müssen wir also unendliche Potenzreihen zulassen.

Satz 3.10. *Sei $p \in \mathbb{P}$ beliebig. Dann gibt es für jedes $z \in \mathbb{Z}$ eine eindeutige Darstellung*

$$z = \sum_{k=0}^{\infty} a_k \cdot p^k,$$

wobei $a_k \in \{0, \dots, p-1\}$ für alle $k \in \mathbb{N}_0$ gilt.

Beweis. Für $z \in \mathbb{N}_0$ gilt dies bereits nach Satz 2.2. Für $z \in \mathbb{Z} \setminus \mathbb{N}_0$ definieren wir z als additives Inverses von $-z \in \mathbb{N}$.
Wir erhalten das additive Inverse induktiv:
Schreibe $z = \sum_{k=0}^{\infty} z_k p^k$ mit $z_k \in \mathbb{Z}$. Wir wollen z_k für alle $k \in \mathbb{N}_0$ bestimmen.
Außerdem soll $z + (-z) = 0$ gelten. Da $-z \in \mathbb{N}$ gilt, können wir $-z$ nach Satz 2.2 als formale Potenzreihe darstellen:

$$-z = \sum_{k=0}^{\infty} y_k p^k$$

wobei $y_k \in \{0, \dots, p-1\}$ für jedes $k \in \mathbb{N}_0$.
Sei nun $l \in \mathbb{N}_0$ minimal mit der Eigenschaft $y_l \neq 0$. Für $i \in \{0, \dots, l-1\} \backslash \{0, -1\}$ folgt direkt $z_i = 0$ nach der Definition der Addition von Potenzreihen.
Nun vergleichen wir die Koeffizienten von p^l:

$$z_l + y_l \equiv 0 \mod p \quad \Rightarrow \quad z_l \equiv -y_l \mod p \quad \Rightarrow \quad z_l = -y_l + p$$

Da $z_l + y_l = -y_l + p + y_l = p$ gilt, erhalten wir einen Übertrag von 1.
Wir betrachten nun die Koeffizienten von p^{l+1}:

$$z_{l+1} + 1 + y_{l+1} = 0 \mod p \quad \Rightarrow \quad z_{l+1} = -y_{l+1} - 1 + p$$

Wir erhalten wieder einen Übertrag von 1, da $z_{l+1}+1+y_{l+1} = -y_l-1+p+1+y_{l+1} = p$. Wir fahren induktiv fort und erhalten dadurch eindeutig z. Da die Koeffizienten von $-z$ irgendwann 0 werden, denn die p-adische Entwicklung natürlicher Zahlen ist endlich, erhalten wir, dass die Entwicklung der Koeffizienten von z irgendwann stationär mit $p-1$ wird.
Wir erhalten $z = (\dots,\ -y_{l+2} - 1 + p,\ -y_{l+1} - 1 + p,\ -y_l - 1 + p,\ -y_l + p\ \underbrace{0, \dots, 0}_{l-\text{mal}})_{(p)}$. Es gilt nun

$$\begin{aligned} z + (-z) &= (\dots, -y_{l+2} - 1 + p, -y_{l+1} - 1 + p, -y_l + p, \underbrace{0, \dots, 0}_{l-\text{mal}})_{(p)} + (\dots, y_{l+2}, y_{l+1}, y_l, \underbrace{0, \dots 0,}_{l-\text{mal}})_{(p)} \\ &= (\dots, p-1, p-1, p, \underbrace{0, \dots, 0}_{l-\text{mal}})_p = (\dots, 0, \dots, 0)_{(p)} \end{aligned}$$

Also ist $z \in \mathbb{Z}$ nach obiger Konstruktion das additive Inverse zu $-z \in \mathbb{N}$. □

4 p-adische Entwicklung rationaler Zahlen

Nun betrachten wir rationale Zahlen.

Beispiel 4.1. Wir wollen $\frac{1}{3}$ bezüglich 5 darstellen.
Zunächst bestimmen wir die Linearkombination von 5 und 3:

$$\begin{aligned} 5 &= 1 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Wir erhalten daraus die Linearkombination

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) = 1 \cdot 3 - 1 \cdot 5 + 1 \cdot 3 = 2 \cdot 3 - 1 \cdot 5.$$

Es gilt also

$$\frac{1}{3} = 2 - \frac{5}{3} = 2 \cdot 5^0 - \frac{1}{3} \cdot 5.$$

Es gilt nach dem euklidischen Algorithmus

$$-\frac{1}{3} = -2 + \frac{5}{3} = 1 \cdot 3 - 5 + \frac{5}{3} = 3 - \frac{10}{3}.$$

Es folgt also

$$\frac{1}{3} = 2 - \frac{1}{3} \cdot 5 = 2 + \left(3 - \frac{10}{3}\right) \cdot 5 = 2 + 15 - \frac{50}{3} = 2 \cdot 5^0 + 3 \cdot 5 - \frac{2}{3} \cdot 5^2.$$

Ebenfalls folgt aus dem euklidischen Algorithmus, dass

$$-\frac{2}{3} = 1 - \frac{5}{3}.$$

Einsetzen liefert nun

$$\frac{1}{3} = 2 + 3 \cdot 5 - \frac{2}{3} \cdot 5^2 = 2 + 3 \cdot 5 + \left(1 - \frac{5}{3}\right) \cdot 5^2 = 2 + 3 \cdot 5 + 1 \cdot 5^2 - \frac{1}{3} \cdot 5^3.$$

Wir haben $-\frac{1}{3}$ bereits vorher bestimmt, es folgt

$$\frac{1}{3} = 2 \cdot 5^0 + 3 \cdot 5^1 + 1 \cdot 5^2 + \left(3 - \frac{10}{3}\right) \cdot 5^3 = 2 \cdot 5^0 + 3 \cdot 5^1 + 1 \cdot 5^2 + 3 \cdot 5^3 - \frac{2}{3} \cdot 5^4.$$

Da wir $-\frac{2}{3}$ auch schon bestimmt haben, sehen wir, dass die Entwicklung periodisch wird. Wir erhalten also

$$\frac{1}{3} = 2 + \sum_{k=1}^{\infty} a_k \cdot 5^k,$$

mit $a_k = 3$, falls k ungerade ist, und $a_k = 1$, falls k gerade ist.
Man schreibt dann auch

$$\frac{1}{3} = (\ldots, 1, 3, 1, 3, 1, 3, 2)_{(5)}.$$

Satz 4.2. *Sei $p \in \mathbb{P}$ beliebig. Dann lässt sich jede rationale Zahl $r \in \mathbb{Q}$ eindeutig darstellen als*

$$r = \sum_{k=-n}^{\infty} a_k p^k,$$

wobei $a_k \in \{0, \ldots, p-1\}$ für alle $k \in \mathbb{Z}$ und $n \in \mathbb{N}_0$ gilt.

Beweis. Sei $r \in \mathbb{Q}$. Dann können wir r eindeutig darstellen als $r = p^k \frac{l}{m}$ mit $l, m \in \mathbb{Z}$, $m \neq 0$, wobei sowohl l und m als auch m und p teilerfremd sind und $k \in \mathbb{Z}$ minimal ist.
Da m und p teilerfremd sind, existieren $s, t \in \mathbb{Z}$, sodass $1 = sm + tp$ gilt.
Es gilt nun

$$r = p^k \frac{l}{m} = p^k \frac{l}{m} \cdot 1 = p^k \frac{l}{m} \cdot (sm + tp) = p^k sl + p^{k+1} \frac{lt}{m}.$$

Nach dem DA existieren $a, b \in \mathbb{Z}$, sodass $sl = b \cdot p + a$, wobei $0 \leq a < p$ gilt. Dies liefert nun

$$\begin{aligned} r &= p^k sl + p^{k+1} \frac{lt}{m} = p^k(bp + a) + p^{k+1} \frac{lt}{m} = ap^k + bp^{k+1} + p^{k+1} \frac{lt}{m} \\ &= ap^k + p^{k+1} \left(b + \frac{lt}{m}\right) = a \cdot p^k + \frac{lt + bm}{m} p^{k+1}. \end{aligned}$$

Also hat p^k bereits einen Koeffizienten in $\{0, \ldots, p-1\}$. Da $\frac{lt+bm}{m} \in \mathbb{Q}$ gilt, können wir das Verfahren erneut auf diese Zahl anwenden. Induktiv erhalten wir dadurch die p-adische Darstellung von r.

Wir zeigen nun die Eindeutigkeit:
Sei $ap^k + bp^{k+1} = \bar{a}p^k + \bar{b}p^{k+1}$. Dann folgt durch Äquivalenzumformungen $a - \bar{a} + (b - \bar{b})p = 0$. Ein Koeffizientenvergleich liefert $a - \bar{a} = 0$, also $a = \bar{a}$, und $b - \bar{b} = 0$, also $b = \bar{b}$. □

Beispiel 4.3. Wir wollen nun ein Beispiel für eine p-adische Zahl betrachten, welche nicht in $\mathbb{Q}$ liegt. Wir zeigen, dass $\sqrt{-1}$ sich 5-adisch darstellen lässt:
Dafür betrachten wir die Funktion $f(x) = x^2 + 1$.
Unser Ziel ist eine Potenzreihe $x = \sum_{k=0}^{\infty} a_i p^i$ zu finden, welche $x^2 + 1 = 0$ löst. Es muss also gelten $(\ldots, a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)_5^2 + 1_5 = 0$.
Über einen Koeffizientenvergleich von 5^0 erhalten wir

$$a_0^2 + 1 = 0 \mod 5 \quad \Rightarrow \quad a_0 = 2.$$

Da $a_0 \in \{0, \ldots, 4\}$ gelten muss, ist dies eindeutig. Wir erhalten $\sqrt{-1} = (\ldots, a_7, a_6, a_5, a_4, a_3, a_2, a_1, 2)_5$.
Nun wollen wir a_1 bestimmen. Wir verwenden wieder den Koeffizientenvergleich, dieses mal von 5^1 und berücksichtigen den Übertrag von $a_0^2 + 1 = 5$:

$$a_1 \cdot 2 + 2 \cdot a_1 + \overbrace{1}^{\text{Übertrag}} = 0 \mod p \quad \Rightarrow \quad 4 \cdot a_1 + 1 = 0 \mod 5 \quad \Rightarrow \quad a_1 = 1,$$

da $a_1 \in \{0, \ldots, 4\}$ gelten muss, ist dies eindeutig. Wir erhalten also $\sqrt{-1} = (\ldots, a_7, a_6, a_5, a_4, a_3, a_2, 1, 2)_5$.
Der Koeffizientenvergleich von 5^2 liefert nun

$$a_2 \cdot 2 + 2 \cdot a_2 + 1^2 + \overbrace{1}^{\text{Ü.}} = 0 \mod 5 \quad \Rightarrow \quad 4 \cdot a_2 + 2 = 0 \mod 5 \quad \Rightarrow \quad a_2 = 2$$

Hier erhalten wir einen Übertrag von 2, da $4 \cdot 2 + 2 = 10 = 2 \cdot 5$ gilt.
Wir wissen nun $\sqrt{-1} = (\ldots, a_7, a_6, a_5, a_4, a_3, 2, 1, 2)_5$.
Mit dem Koeffizientenvergleich von 5^3 erhalten wir nun

$$\begin{aligned} 2 \cdot a_3 + a_3 \cdot 2 + 2 \cdot a_2 \cdot a_1 + \overbrace{2}^{\text{Ü.}} = 0 \mod 5 \quad &\Rightarrow \quad 4 \cdot a_3 + 2 \cdot 2 \cdot 1 + 2 = 4 \cdot a_3 + 6 = 0 \mod 5 \\ &\Rightarrow \quad a_3 = 1. \end{aligned}$$

Es folgt $\sqrt{-1} = (\ldots, a_7, a_6, a_5, a_4, 1, 2, 1, 2)_5$. Da $4 \cdot 1 + 6 = 10$ gilt, erhalten wir einen Übertrag von 2.
Wir fahren mit dem Koeffizientenvergleich von 5^4 fort:

$$\begin{aligned} 4 \cdot a_4 + 2 \cdot a_3 \cdot a_1 + a_2^2 + \overbrace{2}^{\text{Ü.}} = 0 \mod 5 \quad &\Rightarrow \quad 4 \cdot a_4 + 2 \cdot 1 \cdot 1 + 2^2 + 2 = 4 \cdot a_4 + 8 = 0 \mod 5 \\ &\Rightarrow \quad a_4 = 3 \end{aligned}$$

Wir erhalten $\sqrt{-1} = (\ldots, a_7, a_6, a_5, 3, 1, 2, 1, 2)_5$ und einen Übertrag von 4, da $4 \cdot 3 + 8 = 20 = 4 \cdot 5$ gilt.
Der Koeffizientenvergleich von 5^5 liefert uns

$$\begin{aligned} & 4 \cdot a_5 + 2 \cdot a_4 \cdot a_1 + 2 \cdot a_3 \cdot a_2 + \overbrace{4}^{\text{Ü.}} = 0 \mod 5 \\ \Rightarrow \quad & 4 \cdot a_5 + 2 \cdot 3 \cdot 1 + 2 \cdot 2 \cdot 1 + 4 = 4 \cdot a_5 + 14 = 0 \mod 5 \\ \Rightarrow \quad & a_5 = 4 \end{aligned}$$

Also folgt $\sqrt{-1} = (\ldots, a_7, a_6, 4, 3, 1, 2, 1, 2)_5$ und wir bekommen den Übertrag 6, da $4 \cdot 4 + 14 = 30 = 6 \cdot 5$ gilt.
Für a_6 betrachten wir nun den Koeffizientenvergleich von 5^6:

$$\begin{aligned} & 4 \cdot a_6 + 2 \cdot a_5 \cdot a_1 + 2 \cdot a_4 \cdot a_2 + a_3^2 + \overbrace{6}^{\text{Ü.}} = 0 \mod 5 \\ \Rightarrow \quad & 4 \cdot a_6 + 2 \cdot 4 \cdot 1 + 2 \cdot 3 \cdot 2 + 1^2 + 6 = 4 \cdot a_6 + 27 = 0 \mod 5 \\ \Rightarrow \quad & a_6 = 2 \end{aligned}$$

Es folgt $\sqrt{-1} = (\ldots, a_7, 2, 4, 3, 1, 2, 1, 2)_5$ und der Übertrag 7, da $4 \cdot 2 + 27 = 35 = 7 \cdot 5$.
Für den Koeffizientenvergleich von 5^7 erhalten wir

$$\begin{aligned} & 4 \cdot a_7 + 2 \cdot a_6 \cdot a_1 + 2 \cdot a_5 \cdot a_2 + 2 \cdot a_4 \cdot a_3 + \overbrace{7}^{\text{Ü.}} = 0 \mod 5 \\ \Rightarrow \quad & 4 \cdot a_7 + 2 \cdot 2 \cdot 1 + 2 \cdot 4 \cdot 2 + 2 \cdot 3 \cdot 1 + 7 = 4 \cdot a_7 + 33 = 0 \mod 5 \\ \Rightarrow \quad & a_7 = 3 \end{aligned}$$

Wir erhalten $\sqrt{-1} = (\ldots, 3, 2, 4, 3, 1, 2, 1, 2)_5$ sowie den Übertrag 9.
Es ergibt sich keine Regelmäßigkeit, da $\sqrt{-1}$ nicht rational ist. Wir können diesen Algorithmus endlos fortführen.

5 Eigenschaften von p-adischen Zahlen

(i) Jede natürliche Zahl hat eine endliche p-adische Entwicklung.

Beweis. Da der Divisionslagorithmus nach endlich vielen Schritten terminiert, folgt die Aussage sofort nach dem Konstruktionsprinzip. □

(ii) Jede negative ganze Zahl wird in der p-adischen Entwicklung nach endlich vielen Stellen periodisch mit Periode $p - 1$.

Beweis. Siehe Konstruktionsprinzip im Beweis von Satz 3.10. □

(iii) Eine p-adische Zahl $\sum_{k=-n}^{\infty} a_k p^k$ ist genau dann rational, wenn die Folge $(a_k)_{k \geq -n}$ periodisch ist. (Eine Vorperiode ist zugelassen, das heißt, wenn es ein $l \geq -n$ gibt, sodass $(a_k)_{k \geq l}$ periodisch ist.)

Beweis. Siehe [5, Seiten 131–132, Satz 3] □

(iv) Jede irrationale Zahl wird in der p-adischen Darstellung nicht periodisch.

Beweis. Folgt direkt aus (iii). □

6 Der diskrete Bewertungsring $\mathbb{Z}_p$

Definition 6.1. *Sei $p \in \mathbb{P}$. Wir definieren die Addition und Multiplikation auf $\mathbb{Z}_p$ wie folgt:*

$$\begin{aligned} + : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p, \quad & \left(\sum_{i=0}^{\infty} a_i p^i \right) + \left(\sum_{i=0}^{\infty} b_i p^i \right) := \sum_{i=0}^{\infty} (a_i + b_i) p^i, \\ \cdot : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p, \quad & \left(\sum_{i=0}^{\infty} a_i p^i \right) \cdot \left(\sum_{i=0}^{\infty} b_i p^i \right) := \sum_{i=0}^{\infty} \sum_{k=0}^{i} a_k b_{i-k} p^i, \end{aligned}$$

wobei $a_i, b_i \in \{0, \ldots, p-1\}$ für alle $i \in \mathbb{N}_0$.

Die Addition ist wohldefiniert, da für alle $i \in \mathbb{N}_0$ gilt, dass $a_i + b_i \in \mathbb{N}_0$ gilt. Darauf können wir Lemma 3.8 anwenden und erhalten eine p-adische Zahl.

Die Multiplikation ist wohldefiniert, da für alle $i \in \mathbb{N}_0$ die endliche Summe $\sum_{k=0}^{i} a_k b_{i-k}$ in $\mathbb{N}_0$ liegt, woraufhin wir wieder Lemma 3.8 anwenden können

Definition 6.2 (diskreter Bewertungsring)**.** *Ein diskreter Bewertungsring B ist ein lokaler Hauptidealring, der kein Körper ist.*

Satz 6.3. *$\mathbb{Z}_p$ ist ein diskreter Bewertungsring.*

Beweis. Wir zeigen zunächst, dass $\mathbb{Z}_p$ ein Ring mit 1 ist.
Wir haben bereits gezeigt, dass sich jede unechte p-adische Zahl als p-adische Zahl schreiben lässt. Wir können hier also im Beweis stellenweise unechte p-adische Zahlen betrachten.

- $(\mathbb{Z}_p, +)$ ist eine abelsche Gruppe:
  Das Assoziativgesetz sowie das Kommutativgesetz folgen direkt, da wir komponentenweise addieren, und somit die Addition auf die reellen Zahlen zurückführen können, welche assoziativ und kommutativ ist.
  Das neutrale Element von $(\mathbb{Z}_p, +)$ ist
  $$0 := \sum_{k=0}^{\infty} a_k \cdot p^k$$
  mit $a_k = 0$ für alle $k \in \mathbb{N}_0$:
  Sei $b = \sum_{k=0}^{\infty} b_k p^k \in \mathbb{Z}_p$ mit $b_k \in \{0, \dots, p-1\}$ für $k \in \mathbb{N}_0$. Dann gilt
  $$\begin{aligned} 0 + b &= \sum_{k=0}^{\infty} 0 \cdot p^k + \sum_{k=0}^{\infty} b_k p^k \\ &= \sum_{k=0}^{\infty} (0 + b_k) \cdot p^k \\ &= \sum_{k=0}^{\infty} b_k \cdot p^k \\ &= b, \end{aligned}$$
  Die Gleichung $b = b + 0$ folgt analog.

  Das additive Inverse einer p-adischen Zahl lässt sich wie in Satz 3.10 bestimmen.

- $(\mathbb{Z}_p, \cdot)$ ist eine Halbgruppe mit neutralem Element:
  Das Assoziativgesetz lässt sich wie bei der Addition auf die reellen Zahlen zurückführen.
  Das neutrale Element von $(\mathbb{Z}_p, \cdot)$ ist
  $$1 := \sum_{k=0}^{\infty} a_k \cdot p^k,$$
  mit $a_0 = 1$ und $a_k = 0$ für $k > 0$:
  Sei $b = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$ mit $b_i \in \{0, \dots, p-1\}$ für $i \in \mathbb{N}_0$. Dann gilt
  $$b \cdot 1 = \sum_{i=0}^{\infty} b_i p^i \cdot \sum_{l=0}^{\infty} a_k p^k = \sum_{i=0}^{\infty} \sum_{k=0}^{i} b_k a_{i-k} p^i = \sum_{i=0}^{\infty} b_i a_0 p^i = \sum_{i=0}^{\infty} b_i \cdot 1 \cdot p^i = \sum_{i=0}^{\infty} b_i p^i = b.$$
  Die Gleichung $b = 1 \cdot b$ folgt analog.

- Distributivität:

  Seien $a_i, b_i, c_i \in \mathbb{F}_p$ für alle $i \in \mathbb{N}_0$. Dann gilt

$$\begin{aligned}\left(\sum_{i=0}^{\infty} a_i p^i\right) \cdot \left(\left(\sum_{i=0}^{\infty} b_i p^i\right) + \left(\sum_{i=0}^{\infty} c_i p^i\right)\right) &= \left(\sum_{i=0}^{\infty} a_i p^i\right) \cdot \left(\sum_{i=0}^{\infty} (b_i + c_i) p^i\right) \\ &= \sum_{i=0}^{\infty} \sum_{k=0}^{i} a_k (b_{i-k} + c_{i-k}) p^i \\ &= \sum_{i=0}^{\infty} \sum_{k=0}^{i} a_k b_{i-k} p^i + a_k c_{i-k} p^i \\ &= \sum_{i=0}^{\infty} \sum_{k=0}^{i} a_k b_{i-k} p^i + \sum_{i=0}^{\infty} \sum_{k=0}^{i} a_k c_{i-k} p^i \\ &= \left(\sum_{i=0}^{\infty} a_i p^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i p^i\right) + \left(\sum_{i=0}^{\infty} a_i p^i\right) \cdot \left(\sum_{i=0}^{\infty} c_i p^i\right).\end{aligned}$$

  Analog folgt

$$\left(\sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty} b_i p^i\right) \cdot \left(\sum_{i=0}^{\infty} c_i p^i\right) = \left(\sum_{i=0}^{\infty} a_i p^i\right) \cdot \left(\sum_{i=0}^{\infty} c_i p^i\right) + \left(\sum_{i=0}^{\infty} b_i p^i\right) \cdot \left(\sum_{i=0}^{\infty} c_i p^i\right).$$

- Hauptidealring und eindeutiges maximales Ideal:
  Wir werden die beiden Eigenschaften hier nicht beweisen. Der vollständige Beweis kann in [3, Seite 107-108, Satz 13.2] nachgelesen werden.

□

7 Ein Ausblick auf $\mathbb{Q}_p$

Definition 7.1. *Sei $p \in \mathbb{P}$. Wir definieren analog zu $\mathbb{Z}_p$ die Addition und Multiplikation auf $\mathbb{Q}_p$:*

$$\begin{aligned}+ : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p, \quad \left(\sum_{k=-n}^{\infty} a_k p^k\right) + \left(\sum_{k=-m}^{\infty} b_k p^k\right) &:= \sum_{i=\min\{-n,-m\}}^{\infty} (a_i + b_i) p^i, \\ \cdot : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p, \quad \left(\sum_{k=-n}^{\infty} a_k p^k\right) \cdot \left(\sum_{k=-m}^{\infty} b_k p^k\right) &:= \sum_{i=-n-m}^{\infty} \sum_{k=-n}^{i+m} a_k b_{i-k} p^i,\end{aligned}$$

wobei $a_i, b_i \in \{0, \ldots, p-1\}$ für alle $i \in \mathbb{Z}$.

Die Addition ist wohldefiniert, da $a_i + b_i \in \mathbb{N}_0$ für alle $i \in \mathbb{Z}$ gilt. Wir können Lemma 3.8 anpassen und die Summe bei negativen Zahlen beginnen und erhalten wieder eine p-adische Zahl. Die Multiplikation ist nach gleicher Argumentation ebenfalls abgeschlossen.

Satz 7.2. *Sei $p \in \mathbb{P}$. Dann ist $\mathbb{Q}_p$ ein Körper.*

Beweis. Wir können den Beweis, dass $(\mathbb{Q}_p, +, \cdot)$ ein Ring ist, ähnlich wie den Beweis von $\mathbb{Z}_p$ führen, indem wir die Summen immer ab $k = -n$ für ein $n \in \mathbb{N}_0$ laufen lassen. Es fehlt also nur die Existenz von multiplikativen Inversen.

Sei dazu $a = \sum_{k=-n}^{\infty} a_k p^k \in \mathbb{Q}_p \backslash \{0\}$ beliebig. Wir können nun eine Indexverschiebung durchführen und erhalten

$$\begin{aligned} a &= \sum_{k=-n}^{\infty} a_k p^k \\ &= \sum_{k=0}^{\infty} a_{k-n} p^{k-n} \\ &= a_{-n} p^{-n} \left(1 + \overbrace{\sum_{k=1}^{\infty} \underbrace{a_{-n}^{-1} a_{k-n}}_{\in \mathbb{F}_p} p^k}^{=:-\varepsilon} \right) \\ &= a_{-n} p^{-n} (1 - \varepsilon). \end{aligned}$$

Hieraus folgt

$$a^{-1} = a_{-n}^{-1} p^n \underbrace{(1-\varepsilon)^{-1}}_{\underbrace{=\sum_{j=0}^{\infty} \varepsilon^j}_{\in \mathbb{Q}_p}} \in \mathbb{Q}_p,$$

wobei wir hier Neumanns Lemma auf $\mathbb{F}_p((\mathbb{Z}))$ anwenden [4].

Wir erhalten also ein multiplikatives Inverses von a in $\mathbb{Q}_p$, somit ist $\mathbb{Q}_p$ ein Körper.

□

Bemerkung. Hier geht das einzige Mal ein, dass p eine Primzahl sein muss, da sonst $\mathbb{F}_p$ kein Körper ist, und somit kein multiplikatives Inverses existieren muss.

Wir können nun den Beweis von Satz 4.2 auch über die multiplikativen Inversen konstruieren, statt über den DA.

Literatur

[1] Fernando Q. Gouvêa. "Exploring $\mathbb{Q}_p$". In: *p-adic Numbers: An Introduction*. Cham: Springer International Publishing, 2020, S. 73–108. ISBN: 978-3-030-47295-5. DOI: 10.1007/978-3-030-47295-5_4. URL: https://doi.org/10.1007/978-3-030-47295-5_4.

[2] Prof.'in Dr. Salma Kuhlmann. *Gesamtscript zur Vorlesung Lineare Algebra II*. https://www.mathematik.uni-konstanz.de/kuhlmann/lehre/teaching-history/ab-wintersemester-20182019/sommersemester-2020/lineare-algebra-ii/script-zur-vorlesung/. zuletzt aufgerufen am 05.01.2022 um 15:54 Uhr.

[3] Stefan Müller-Stach und Jens Piontkowski. "p-adische Zahlen". In: *Elementare und algebraische Zahlentheorie: Ein moderner Zugang zu klassischen Themen*. Wiesbaden: Vieweg, 2007, S. 105–117. ISBN: 978-3-8348-9064-1. DOI: 10.1007/978-3-8348-9064-1_13. URL: https://doi.org/10.1007/978-3-8348-9064-1_13.

[4] Leonhard Nenno. "Handout: Neumann's Lemma". Online verfügbar im Cloud-Order des Fachseminars Algebra und Logik. Dezember 2021.

[5] Jürgen Neukirch. "Die p-adischen Zahlen". In: *Zahlen*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, S. 126–145. ISBN: 978-3-642-58155-7. DOI: 10.1007/978-3-642-58155-7_7. URL: https://doi.org/10.1007/978-3-642-58155-7_7.

[6] *p-adische Zahl*. https://de.wikipedia.org/wiki/P-adische_Zahl. zuletzt aufgerufen am 18.12.2021 um 19:54 Uhr.