

VORTRAGSSKRIPT

# $p$ -adische Zahlen und das Henselsche Lemma

*Emma Bach*

Proseminar Elementare Zahlentheorie  
Wintersemester 2025

27/10/2025

# Inhalt

<b>1</b>	<b>Umgang mit Basen ungleich 10</b>	<b>2</b>
<b>2</b>	<b>Bewertungen und Metriken auf <math>\mathbb{Z}</math></b>	<b>3</b>
2.1	Der $p$ -adische Betrag .....	3
<b>3</b>	<b>Die <math>p</math>-adischen Zahlen</b>	<b>5</b>
3.1	Konstruktion der $p$ -adischen Zahlen .....	5
<b>4</b>	<b>Das Henselsche Lemma</b>	<b>7</b>
4.1	Konstruktion $p$ -adischer Darstellungen .....	8
<b>A</b>	<b>Quellen</b>	<b>11</b>

# Chapter 1

## Umgang mit Basen ungleich 10

Die gewohnte Dezimaldarstellung natürlicher Zahlen basiert auf der Erkenntnis, dass sich jede natürliche Zahl  $n$  als Summe

$$n = \sum_{i=1}^j a_i \cdot (10)^i$$

von Zehnerpotenzen schreiben lässt, wobei  $a_i \in \{0, 1, \dots, 9\}$ . Schreiben wir die Zahl "152", so meinen wir formell die Zahl  $1 \cdot 10^2 + 5 \cdot 10 + 2$ . Analog existiert jedoch eine ähnliche Darstellung für jedes  $b \in \mathbb{N}$ :

$$n = \sum_{i=1}^j a_i b^i$$

mit  $a_i \in \{0, 1, \dots, b-1\}$ .

So ist zum Beispiel  $152 = 128 + 16 + 8 = 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 0$ . Somit ist die Binärdarstellung von 152 10011000.

Es ist außerdem  $152 = 2 \cdot 64 + 1 \cdot 16 + 2 \cdot 4 + 0$ , also ist  $[152]_{10} = [2120]_4$ .

Zählen in Basen ungleich 10 funktioniert ähnlich wie in Basis 10, nur dass man eben eine Ziffer nach links übertragen muss, wenn man  $b$  erreicht (statt 10). Die natürlichen Zahlen in Basis 3 sind somit 0, 1, 2, 10, 11, 12, 20, 21, 22, 100, ...

## Chapter 2

# Bewertungen und Metriken auf $\mathbb{Z}$

Wir betrachten die Folge:

$$a_n = 10^n$$

In den reellen Zahlen mit der Standardtopologie hat diese Folge keinen Grenzwert. Betrachten wir allerdings die Glieder in Dezimaldarstellung, fällt aber intuitiv trotzdem eine Art "Grenzwertverhalten" auf:

$$\begin{aligned} a_1 &= 10 \\ a_2 &= 100 \\ a_3 &= 1000 \\ a_4 &= 10000 \\ a_5 &= 100000 \\ a_6 &= 1000000 \\ &\dots \\ \implies \lim_{n \rightarrow \infty} a_n &= \dots 000? \end{aligned}$$

Ein analoges "Konvergenzverhalten" sehen wir für eine beliebige Folge der Form  $a_n = p^n$ , solange wir die Zahlen in Basis  $p$  schreiben.

Unser erstes Ziel in diesem Vortrag, wird es sein, diese Form von Konvergenz und die daraus entstehenden "Zahlen mit unendlich vielen Stellen vor dem Komma" zu formalisieren. Wir werden eine Familie von Metriken  $|\cdot|_p$  einführen, sodass in jeder Metrik  $|\cdot|_p$  die Folge  $a_n = p^n$  tatsächlich zur Nullfolge wird.

## 2.1 Der $p$ -adische Betrag

**Definition 2.1.** Sei  $K$  ein Körper. Seien  $x, y \in K$ . Ein **Betrag** auf  $K$  ist eine Funktion  $|\cdot| : K \rightarrow \mathbb{R}$  mit folgenden Eigenschaften:

- i.)  $|0_K| = 0$
- ii.) Positivität:  $x \neq 0_K \implies |x| > 0$

iii.)  $|x \cdot_K y| = |x| \cdot |y|$

iv.) Subadditivität:  $|x +_K y| \leq |x| + |y|$

**Proposition 2.2.** Sei  $K$  ein Körper und  $||$  ein Betrag auf  $K$ . So ist

$$\begin{aligned} d : K \times K &\rightarrow \mathbb{R} \\ (x, y) &\mapsto |x - y| \end{aligned}$$

eine Metrik auf  $K$ .

Sei  $(G, +, \geq)$  eine linear geordnete Gruppe. Wir fügen zu  $G$  ein Element  $\infty$  hinzu, welches die erwarteten Eigenschaften bezüglich der Ordnung und Gruppenoperation hat:

- $\forall g \in G : \infty \geq g$
- $\forall g \in G : \infty + g = g + \infty = \infty + \infty = \infty$

**Definition 2.3.** Sei  $p$  eine Primzahl. Die  **$p$ -adische Bewertung** auf  $\mathbb{Z}$  ist folgende Abbildung:

$$\nu_p(n) = \begin{cases} \max\{k \in \mathbb{N}_0 : p^k \mid n\} & n \neq 0 \\ \infty & n = 0 \end{cases}$$

**Beispiel 2.4.** Es gilt  $\nu_5(75) = \nu_5(3 \cdot 5^2) = 5^2 = 25$  und  $\nu_5(50) = \nu_5(2 \cdot 5^2) = 5^2 = 25$ . Für die Summe gilt  $\nu_5(125) = \nu_5(5^3) = 5^3$ .

Intuitiv gibt uns die  $p$ -adische Bewertung einer ganzen Zahl  $n$  also die größte Potenz von  $p$ , durch die  $n$  teilbar ist.

Die  $p$ -adische Bewertung ist das Standardbeispiel einer Bewertung. Es existieren viele andere wichtige Bewertungen in der kommutativen Algebra, in der komplexen Analysis und in der algebraischen Geometrie, diese sind allerdings in der Regel leider nichttrivial und würden den Rahmen dieses Proseminarvortrags sprengen.

**Definition 2.5.** Wir erweitern die  $p$ -adische Bewertung auf ganz  $\mathbb{Q}$  durch:

$$\nu_p\left(\frac{r}{s}\right) = \nu_p(r) - \nu_p(s)$$

**Definition 2.6.** Wir definieren den  $p$ -adischen Betrag  $|\cdot|_p$  auf  $\mathbb{Q}$  durch:

$$|n|_p = \frac{1}{p^{\nu_p(n)}}$$

**Satz 2.7.** Der  $p$ -adische Betrag erfüllt die **ultrametrische Dreiecksungleichung**:

$$|x + y| \leq \max(|x|, |y|)$$

Wir nennen einen solchen Betrag **nichtarchimedisch**.

**Proposition 2.8. Satz von Ostrowski:** Jeder Betrag auf  $\mathbb{Q}$  ist entweder:

- Der triviale Betrag  $|x|_0 = \begin{cases} 0 & x = 0_K \\ 1 & x \neq 0_K \end{cases}$ ,
- oder äquivalent zu  $|\cdot|_p$  für eine Primzahl  $p$ ,
- oder äquivalent zum Standardabsolutbetrag  $|\cdot|$ .

## Chapter 3

# Die $p$ -adischen Zahlen

### 3.1 Konstruktion der $p$ -adischen Zahlen

**Definition 3.1.** Wir bezeichnen die Vervollständigung des Rings  $\mathbb{Z}$  gemäß der  $p$ -adischen Metrik als die  **$p$ -adischen** ganzen Zahlen  $\mathbb{Z}_p$ . Analog bezeichnen wir die Vervollständigung des Rings  $\mathbb{Q}$  gemäß der  $p$ -adischen Metrik als die  **$p$ -adischen** Zahlen  $\mathbb{Q}_p$ .

Wir erhalten die gefragten Vervollständigungen durch eine Äquivalenzklassenkonstruktion von Cauchyfolgen, in der Cauchyfolgen äquivalent sind, wenn ihre Differenz eine Nullfolge ist, analog zur Konstruktion von  $\mathbb{R}$  als Vervollständigung gemäß des Standardabsolutbetrags.

**Proposition 3.2.**  $\mathbb{Z}_p$  ist ein Ring, der  $\mathbb{Z}$  als dichte Teilmenge enthält.  $\mathbb{Q}_p$  ist ein Körper, der  $\mathbb{Q}$  als dichte Teilmenge enthält.

**Proposition 3.3.**

$$\mathbb{Z}_p = \{z \in \mathbb{Q}_p : |z|_p \leq 1\} = \{z \in \mathbb{Q}_p : \nu_p(z) \geq 0\}$$

**Proposition 3.4.** Jede Reihe der Form

$$x = \sum_{n=m}^{\infty} d_n p^n,$$

wobei  $m \in \mathbb{Z}$ ,  $d_n \in \mathbb{Z}/p\mathbb{Z}$ , konvergiert in  $\mathbb{Q}_p$ . Wir nennen die Folge  $d_n$  die  **$p$ -adische Darstellung von  $x$** .

Wir schreiben eine  $p$ -adische Zahl  $z$  analog zur Standarddarstellung Basis  $p$  als

$$z = \dots d_4 d_3 d_2 d_1 d_0, d_{-1} \dots d_{-m}$$

mit der kleinsten Ziffer rechts. In manchen Quellen werden  $p$ -adische Zahlen umgekehrt geschrieben, mit der kleinsten Ziffer links.

Die  $p$ -adischen ganzen Zahlen sind genau die  $p$ -adischen Zahlen mit  $m = 0$ . Die Zahlen  $\mathbb{Z} \subsetneq \mathbb{Z}_p$  sind genau die Zahlen, deren  $p$ -adische Darstellungen endlich sind, und diese Darstellung ist genau die Übliche.

**Beispiel 3.5.** Wir wollen die 2-adische Darstellung von  $-1$  finden.

Wir brauchen also eine Folge  $d_n$ , sodass für jedes  $n$

$$d_0 + d_1 2 + \dots + d_n 2^n \equiv -1 \pmod{2^{n+1}}$$

Für  $n = 0$  erhalten wir:

$$-d_0 \equiv -1 \pmod{2}$$

also  $d_0 = 1$ . Wir wollen induktiv zeigen, dass alle anderen Ziffern ebenfalls 1 sind. Angenommen,  $d_0 = d_1 = \dots = d_{n-1} = 1$ . Dann gilt:

$$\begin{aligned} d_0 + 2d_1 + \dots + 2^n d_n &= \left( \sum_{i=0}^{n-1} 2^i + d_n 2^n \right) \equiv -1 \pmod{2^{n+1}} \\ \implies (2^n - 1) - d_n 2^n &\equiv -1 \pmod{2^{n+1}} \\ \implies 2^n - d_n 2^n &\equiv 0 \pmod{2^{n+1}} \\ \implies 1 - d_n &\equiv 0 \pmod{2^{n+1}} \end{aligned}$$

Also  $d_n = 1$ . Die 2-adische Darstellung von  $-1$  ist also  $\dots 1111$ .

**Proposition 3.6.** *Als Hausaufgabe: In der  $p$ -adische Darstellung von  $-1$  für beliebiges  $p$  ist jede Ziffer  $p - 1$ . Die 5-adische Darstellung ist also  $\dots 4444$  und die 7-adische Darstellung ist  $\dots 6666$ .*

(Hier Bezug zum Zweierkomplement in der Informatik ziehen)

## Chapter 4

# Das Henselsche Lemma

Das Henselsche Lemma ist eine Methode, um Polynomgleichungen in  $\mathbb{Z}_p$  zu lösen. Es liefert uns somit insbesondere eine einfache Möglichkeit, die  $p$ -adische Darstellung bestimmter algebraischer Zahlen zu finden.

**Satz 4.1.** *Sei*

$$f(x) = \sum_{i=0}^n c_i x^i$$

*ein Polynom mit Koeffizienten  $c_i \in \mathbb{Z}_p$ . Sei  $f'(x)$  die Ableitung von  $f(x)$ , also*

$$f'(x) = \sum_{i=0}^{n-1} i c_{i+1} x^i$$

*Sei außerdem  $a \in \mathbb{Z}_p$ , sodass:*

$$\begin{aligned} f(a) &\equiv 0 \pmod{p} \\ f'(a) &\not\equiv 0 \pmod{p} \end{aligned}$$

*Dann existiert ein eindeutiges  $\alpha \in \mathbb{Z}_p$ , sodass:*

$$\begin{aligned} f(\alpha) &= 0 \\ \alpha &\equiv a \pmod{p} \end{aligned}$$

*Beweis.* Wir konstruieren eine eindeutige Folge  $a_n$  in  $\mathbb{Z}_p$ , sodass:

- i.)  $f(a_n) \equiv 0 \pmod{p^{n+1}}$
- ii.)  $a_n \equiv a_{n-1} \pmod{p}$
- iii.)  $a_n \in \{0, \dots, p^{n+1} - 1\}$

Daraufhin werden wir zeigen, dass  $\lim_{n \rightarrow \infty} a_n = \alpha$ .

Sei erst einmal als Induktionsbasis  $a_0 \in \{0, \dots, p-1\}$  mit  $a_0 \equiv a \pmod{p}$ .

Seien nun  $a_0, \dots, a_{n-1}$  bereits mit den gewünschten Eigenschaften konstruiert. Aus ii.) folgt, dass  $a_n$  die Form  $a_{n-1} + b_n p$  haben muss, und aus iii.) folgt  $b_n \in \{0, \dots, p^n - 1\}$ .



Also gilt:

$$\begin{aligned}
 f(a_n) &= f(a_{n-1} + b_n p^n) = \sum_{i=0}^n c_i (a_{n-1} + b_n p^n)^i \\
 &\equiv \sum_{i=0}^n c_i (a_{n-1}^i + i(a_{n-1}^{i-1})(b_n p^n)) \pmod{p^{n+1}} \quad (\text{Binomischer Lehrsatz}) \\
 &= \sum_{i=0}^n c_i a_{n-1}^i + \left( \sum_{i=0}^n i c_i a_{n-1}^{i-1} \right) b_n p^n \\
 &= f(a_{n-1}) + f'(a_{n-1}) b_n p^n
 \end{aligned}$$

(Dies ist eine Taylorapproximation erster Ordnung - wir sehen, dass diese in diesem Fall exakt ist!)

Da  $f(a_{n-1}) \equiv 0 \pmod{p^n}$  per Annahme gilt  $f(a_{n-1}) \equiv kp \pmod{p^n}$  für ein  $k \in \{0, \dots, p-1\}$ .

Für  $f(a_n) \equiv 0 \pmod{p^{n+1}}$  brauchen wir also  $kp + f'(a_{n-1})b_n p^n \equiv 0 \pmod{p^{n+1}}$ . Klammern wir  $p$  aus, sehen wir dass dies gegeben ist, falls:

$$\begin{aligned}
 k + f'(a_{n-1})b_n &\equiv 0 \pmod{p} \\
 \implies f'(a_{n-1})b_n &\equiv -k \pmod{p}
 \end{aligned}$$

Es gilt per Induktionsannahme  $a_{n-1} \equiv a_0 \pmod{p}$ , also  $f'(a_{n-1}) \equiv f'(a_0) \not\equiv 0 \pmod{p}$ , also existiert die Lösung

$$b_n \equiv -\frac{k}{f'(a_{n-1})} \pmod{p}$$

Es bleibt noch zu Zeigen, dass  $\alpha = a_0 + b_1 p + b_2 p^2 \dots$  eine exakte  $p$ -adische Lösung ist.

Es gilt  $\alpha \equiv a_0 \equiv a \pmod{p}$ , und es gilt  $f(\alpha) \equiv 0 \pmod{p^n}$  für alle  $n$ , also  $|f(\alpha)|_p < \frac{1}{p^n}$  für alle  $n$ , also  $|f(\alpha)|_p = 0$ . Somit ist  $\alpha$  tatsächlich eine Lösung.

Es bleibt noch die Eindeutigkeit der Lösung zu zeigen. Angenommen,  $\beta$  sei eine weitere Lösung, also  $f(\beta) = 0$  und  $\beta \equiv a \pmod{p}$ . Aus der zweiten Bedingung folgt bereits  $\alpha \equiv \beta \pmod{p}$ .

Angenommen,  $\alpha \equiv \beta \pmod{p^n}$ . Dann gilt  $\beta = \alpha + p^n \gamma_n$  mit  $\gamma_n \in \mathbb{Z}_p$ . Dieselbe Polynomweiterung, welche bereits im Beweis verwendet wurde, liefert:

$$f(\beta) = f(\alpha + p^n \gamma_n) \equiv f(\alpha) + f'(\alpha) p^n \gamma_n \pmod{p^{n+1}}$$

Es gilt  $f(\beta) = 0$ , also  $f'(\alpha) \gamma_n \equiv 0 \pmod{p}$ . Wir wissen  $f'(\alpha) \equiv f'(a) \not\equiv 0 \pmod{p}$ , also  $\gamma_n \equiv 0 \pmod{p}$ , also  $\alpha \equiv \beta \pmod{p^{n+1}}$ .

Somit gilt  $\alpha = \beta$ , also ist die Lösung eindeutig. □

## 4.1 Konstruktion $p$ -adischer Darstellungen

Hensel's Lemma liefert uns einen praktischen Weg,  $p$ -adische Darstellungen vieler algebraischer Zahlen zu konstruieren.

**Beispiel 4.2.** Wir wollen  $\sqrt{2} \in \mathbb{Z}_7$  finden. Sei also  $f(x) = x^2 - 2$ , also  $f'(x) = 2x$ . Wir suchen zuerst unser  $a = a_0$ . Da  $f'(a) \not\equiv 0 \pmod{7}$  brauchen wir  $2a \not\equiv 0$ . Die Bedingung  $f(a) \equiv 0 \pmod{7}$  liefert:

$$a^2 - 2 \equiv 0 \pmod{7}$$

also  $a^2 \equiv 2 \pmod{7}$ . Eine Möglichkeit ist 3, eine weitere Möglichkeit ist  $4 \equiv -3 \pmod{7}$ . Da also Nullstellen existieren, garantiert das Henselsche Lemma eine Lösung - wir haben also eine irrationale reelle Zahl gefunden, welche in den  $p$ -adischen ganzen Zahlen enthalten sind.

Wir wollen nun die letzten paar Ziffern berechnen. Wir entscheiden uns für die positive Wurzel. Nun wollen wir  $k$  bestimmen, sodass

$$f(3) = 7 \equiv 7k \pmod{49}$$

Es reicht also  $k = 1$ . Nun gilt:

$$\begin{aligned} b_1 &\equiv -\frac{1}{f'(3)} \pmod{7} \\ \implies b_1 &\equiv -\frac{1}{6} \pmod{7} \\ \implies 6b_1 + 1 &\equiv 0 \pmod{7} \\ \implies b_1 &= 1 \end{aligned}$$

Also  $a_1 = 3 + 1 \cdot 7 = 10$ . Für die dritte Ziffer brauchen wir  $f(a_1) = f(10) = 98 \equiv 49k \pmod{343}$ , also  $k = 2$ . Nun gilt:

$$\begin{aligned} b_2 &\equiv -\frac{2}{f'(10)} \pmod{7} \\ &\equiv -\frac{2}{20} \pmod{7} \\ &\equiv -\frac{1}{10} \pmod{7} \\ \implies 10b_2 + 1 &\equiv 0 \pmod{7} \\ \implies 3b_2 + 1 &\equiv 0 \pmod{7} \\ \implies b_2 &\equiv 2 \pmod{7} \end{aligned}$$

Also  $a_2 = 3 + 1 \cdot 7 + 2 \cdot 7^2 = 108$ .

Die 7-adische Darstellung von  $\sqrt{2}$  endet also in ...213.

**Anwendung 4.3.** Eine  $p$ -adische Zahl  $u$  hat eine  $k$ -te Wurzel in den  $p$ -adischen Zahlen, wenn  $k \not\equiv 0 \pmod{p}$  und eine Zahl  $n$  mit  $n \equiv u \pmod{p}$  existiert, sodass  $n$  eine  $k$ -te Wurzel in  $\mathbb{Z}/p\mathbb{Z}$  hat.

*Beweis.* Wähle  $f(x) = x^k - u$ . So gilt  $f'(x) = kx \not\equiv 0$ , und das Henselsche Lemma garantiert eine Lösung, falls wir eine initiale Nullstelle  $n = x^k \equiv u \pmod{p}$  finden können  $\square$

**Anwendung 4.4.**  $i = \sqrt{-1} \in \mathbb{Z}_3$

*Beweis.* Wähle  $f(x) = x^2 + 1$ , also  $f'(x) = 2x$ . Wir wollen  $x^2 \equiv -1 \equiv 2 \pmod{3}$ . Unsere Möglichkeiten sind also wieder 3 und 4, wir wählen wieder  $a_0 = a = 3$ . Es gilt  $f'(x) = 6 \not\equiv 0 \pmod{7}$ , also existiert eine eindeutige  $p$ -adische Erweiterung von  $a$ , deren Quadrat  $-1$  ist.  $\square$

# Appendix A

## Quellen

Hauptquellen sind "p-adic Numbers, p-adic Analysis and Zeta Functions", geschrieben von Neal Koblitz, "Algebraic Number Theory", geschrieben von Jürgen Neukirch, und Keith Conrads Notizen zum Henselschen Lemma. Eine weitere Quelle ist  $p$ -adic Numbers,  $Q_p$  and Hensels Lemma, geschrieben von Yiduan Zheng.