Vortragsskript

p-adische Zahlen und das Henselsche Lemma

Emma Bach

Proseminar Elementare Zahlentheorie
Wintersemester 2025

28/10/2025

Inhalt

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 $a_i \in \{0, 1, \ldots, 9\}$. 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 $a_i \in \{0, 1, \ldots, b-1\}$.

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 $[10011000]_2$.

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 $0, 1, 2, 10, 11, 12, 20, 21, 22, 100, \ldots$

Chapter 2

Alternative Topologien auf $\mathbb{Z}$ und $\mathbb{Q}$

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:

$$\begin{aligned} a_1 &= 10 \\ a_2 &= 100 \\ a_3 &= 1000 \\ a_4 &= 10000 \\ a_5 &= 100000 \\ a_6 &= 1000000 \\ &\cdots \\ \implies \lim_{a\to\infty} a_n &= ...000? \end{aligned}$$

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 $|-|_p$ einführen, sodass in jeder Metrik $|-|_p$ die Nullfolgen genau die Folgen sind, in denen die Basis-p-Darstellung immer späterer Folgenglieder in immer mehr Nullen endet.

Genau so, wie in den reellen Zahlen in der Folge 0.1^n die 1 "verschwindet", indem sie unendlich weit "nach rechts wandert", und die Folge somit gegen 0 konvergiert, kann dann in unserem neuen Zahlensystem die 1 "verschwinden", indem sie "unendlich weit nach links wandert".

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 $|-| : K \to \mathbb{R}$ 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*

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

eine Metrik auf K.

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

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

Die p-adische Bewertung ist auch bekannt als die **Vielfachheit von p in n**.

Beispiel 2.4. Es gilt:

- $v_5(1) = 0$
- $v_5(25) = v_5(5^2) = 2$
- $v_5(100) = v_5(4 \cdot 5^2) = 2$.
- $v_5(25 + 100) = v_5(125) = v_5(5^3) = 3$.

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

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

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

Dies entspricht der Potenz von p, die wir erhalten, wenn wir alle Potenzen von p aus dem Bruch "rausziehen".

Beispiel 2.6.

$$v_5\left(\frac{75}{125}\right) = 2 - 3 = -1$$

bzw.

$$\begin{aligned} v_5\left(\frac{75}{125}\right) &= v_5\left(\frac{3}{5}\right) \\ &= v_5\left(5^{-1} \cdot \frac{3}{1}\right) \\ &= -1 \end{aligned}$$

Definition 2.7. Wir definieren den p-adischen Betrag $|-|_p$ auf $\mathbb{Q}$ durch:

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

Der p-adische Betrag einer rationalen Zahl ist also genau dann gering, wenn ihre Darstellung in Basis p in vielen aufeinanderfolgenden Nullen endet.

Korollar 2.8. *Der p-adische Betrag einer Zahl z ist genau dann 0, wenn $\forall n \in \mathbb{N} : z \equiv 0 \mod p^{n+1}$*

> *Beweis.* Dann gilt $\forall n \in \mathbb{N} : |z| < \frac{1}{p^n}$ □

Wir notieren die dazugehörige Metrik als $d_p(x, y)$. In dieser Metrik sind zwei Zahlen genau dann nah aneinander, wenn für ein Großes n die letzten n Ziffern ihrer Darstellung in Basis p identisch sind.

Beispiel 2.9.

$$\begin{aligned} d_2(24, 25) &= d_2([11.000]_2, [11.001]_2) \\ &= |1|_2 \\ &= \frac{1}{2^0} \\ &= 1 \end{aligned}$$

$$\begin{aligned} d_2(24, 1816) &= |1792|_2 \\ &= \left|7 \cdot 2^8\right| \\ &= \frac{1}{2^8} = \frac{1}{256} \end{aligned}$$

$$\begin{aligned} d_2(24, 1816) &= d_2([11.000]_2, [11.100.011.000]_2) \\ &= \Big|[-11.100.000.000]_2\Big|_2 \\ &= \frac{1}{2^8} = \frac{1}{256} \end{aligned}$$

Satz 2.10. *Der p-adische Betrag erfüllt die* ***ultrametrische Dreiecksungleichung****:*

$$|x + y|_p \le \max(|x|_p, |y|_p)$$

Wir nennen einen solchen Betrag ***nichtarchimedisch****.*

Beispiel 2.11.

$$|54|_3 = \left|2 \cdot 3^3\right| = \frac{1}{27}$$

$$|81|_3 = \left|3^5\right|_3 = \frac{1}{81}$$

$$|54 + 81|_3 = |135|_3 = \left|5 \cdot 3^3\right|_3 = \frac{1}{27}$$

Proposition 2.12. **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* $|-|_p$ *für eine Primzahl* p,
- *oder äquivalent zum Standardabsolutbetrag* $|-|$.

Chapter 3

Die p-adischen Zahlen

3.1 Konstruktion der p-adischen Zahlen

Erinnerung: Die Reellen Zahlen können als die "Vervollständigung der Rationalen Zahlen" definiert werden, also als die Menge aller Cauchyfolgen in $\mathbb{Q}$, sodass zwei Cauchyfolgen äquivalent sind, wenn ihre Differenz eine Nullfolge ist.

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

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 $m \in \mathbb{Z}_{\leq 0}$, $d_n \in \{0, 1, \dots, p-1\}$, konvergiert in $\mathbb{Q}_p$. Wir nennen die Folge d_n die **p-adische Darstellung von** x. Jede p-adische Zahl kann als eine solche Reihe dargestellt werden.*

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 die Darstellung positiver ganzer Zahlen ist genau die übliche Darstellung Basis p.

Beispiel 3.5. Wir wollen die p-adische Darstellung von -1 finden.

Lemma 3.6. *In der p-adische Darstellung von -1 für beliebiges p ist jede Ziffer $p-1$. Die 2-adische Darstellung ist also $\dots 1111$, die 5-adische Darstellung ist $\dots 4444$ und die 7-adische Darstellung ist $\dots 66666$.*

Beweis. $d_0 \equiv -1 \mod p \implies d_0 = p - 1$. Wir nehmen also als Induktionsannahme an, dass $d_0 = \ldots = d_{n-1} = p - 1$.

$$\begin{aligned} d_0 + d_1 p + \ldots + d_n p^n = \left((p-1) \sum_{i=0}^{n-1} p^i + d_n p^n \right) &\equiv -1 \mod p^{n+1} \\ \implies \quad (p-1)\frac{(1-p^n)}{1-p} + d_n p^n &\equiv -1 \mod p^{n+1} \\ \implies \quad (p^n - 1) + d_n p^n &\equiv -1 \mod p^{n+1} \\ \implies \quad p^n + d_n p^n &\equiv 0 \mod p^{n+1} \\ \implies \quad 1 + d_n &\equiv 0 \mod p \end{aligned}$$

□

Diese Darstellung ist tatsächlich analog zur Darstellung negativer Zahlen in binär in den meisten modernen Computern. Negative Zahlen werden in der Regel im **Zweierkomplement** dargestellt, was bedeutet, dass das höchstmögliche Bit negativ gezählt wird. Da wir hierfür vorher ein "höchstmögliches Bit" wählen müssen, ist unser Zahlenbereich beschränkt, und die Addition großer Zahlen kann zu Problemen wie dem bekannten *Integer Overflow* führen. Die p-adischen Zahlen lösen dieses Problem, indem sie Zahlen erlauben, die beliebig hochwertige Ziffern enthalten, und haben so trotzdem den selben Vorteil, dass sie kein Vorzeichen benötigen.

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:

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

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

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

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

i.) $f(a_n) \equiv 0 \mod p^{n+1}$

ii.) $a_n \equiv a_{n-1} \mod p^n$

iii.) $a_n \in \{0, \ldots, p^{n+1} - 1\}$

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

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

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

$b_n \in \{0, \ldots, p-1\}$.

Also gilt:

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

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

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

Für $f(a_n) \equiv 0 \mod p^{n+1}$ brauchen wir also $kp^n + f'(a_0) b_n p^n \equiv 0 \mod p^{n+1}$. Klammern wir p^n aus, sehen wir dass dies gegeben ist, falls:

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

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

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

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

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

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

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

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

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

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

4.1 Bezug zum Newton-Verfahren

Das Newton-Verfahren im reellen Fall findet Nullstellen durch die Iteration

$$a_n = a_{n-1}\frac{f(a_{n-1})}{f'(a_{n-1})}$$

Analog findet das Henselsche Lemma Nullstellen durch die Iteration

$$b_n p^n \equiv -\frac{kp^n}{f'(a_{n-1}} \equiv -\frac{f(a_{n-1})}{f'(a_{n-1})} \mod p^{n+1}$$

Das Henselsche Lemma ist somit auch als das "p-adische Newton-Verfahren" bekannt. Im reellen Newton-Verfahren kann es Fälle geben, in denen die Iteration nicht konvergiert. Wählt man zum Beispiel $f(x) = x^3 - x$ und $a_0 = \frac{1}{\sqrt{5}}$, so gilt $a_n = (-1)^n \frac{1}{\sqrt{5}}$.

Das p-adische Newton-Verfahren konvergiert hingegen immer.

4.2 Konstruktion p-adischer Darstellungen

Hensel's Lemma liefert uns einen praktischen Weg, p-adische Darstellungen vieler algebraischer Zahlen zu approximieren:

Algorithmus: p-adisches Newton-Verfahren

Eingabe 1: Polynom $f \in \mathbb{Z}_p[x]$.
Eingabe 2: $a_0 \in \mathbb{Z}_p$, sodass $f(a_0) \equiv 0 \mod p$ und $f'(a_0) \not\equiv 0 \mod p$.
Eingabe 3: $n \in \mathbb{N}$

Ausgabe: $\alpha \in \mathbb{Z}_p$, sodass $f(\alpha) \equiv 0 \mod p^{n+1}$ und $\alpha \equiv a_0 \mod p$

---

for $i = 1, i \leq n, i++$ **do**
  Bestimme k mit $f(a) \equiv kp^i \mod p^{i+1}$
  Bestimme $b_i \equiv -\dfrac{k}{f'(a)} \mod p$
  $a_i = a_{i-1} + b_i p^i$
end for

Ausgabe: $\alpha \leftarrow a$

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 $f'(a) \not\equiv 0 \mod 7$ brauchen wir $2a \not\equiv 0$. Die Bedingung $f(a) \equiv 0 \mod 7$ liefert:

$$a^2 - 2 \equiv 0 \mod 7$$

also $a^2 \equiv 2 \mod 7$. Eine Möglichkeit ist 3, eine weitere Möglichkeit ist $4 \equiv -3 \mod 7$. 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

$$f(3) = 7 \equiv 7k \mod 49$$

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

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

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

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

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

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

Anwendung 4.3. *Sei $u \in \mathbb{Z}_p$. Sei $k \not\equiv 0 \mod p$. Sei n eine Zahl mit $n \equiv u \mod p$, welche eine k-te Wurzel in $\mathbb{Z}/p\mathbb{Z}$ hat. Dann hat u eine k-te Wurzel in $\mathbb{Z}_p$.*

> *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 $n = x^k \equiv u \mod p$ finden können □

Anwendung 4.4. $i = \sqrt{-1} \in \mathbb{Z}_5$

> *Beweis.* Wähle $f(x) = x^2 + 1$, also $f'(x) = 2x$. Wir wollen $x^2 \equiv -1 \equiv 4 \mod 5$. Die Lösungen hierzu sind 2 und 3. wir wählen $a_0 = a = 2$. Es gilt $f'(x) = 4 \not\equiv 0 \mod 5$, also existiert eine eindeutige p-adische Erweiterung von a, deren Quadrat -1 ist. □

Appendix A

Anwendungen der p-adischen Zahlen

Die Relevanz der p-adischen Zahlen besteht hauptsächlich im sogenannten **Lokal-Global-Prinzip**, auch bekannt als **Hasse-Prinzip** - hiervon gibt es zwei Varianten:

i.) Traditionell bestand das Prinzip in der Erkenntnis, dass aus der Lösbarkeit einer diophantinischen Gleichung modulo aller Primzahlen oft die generelle Lösbarkeit folgt.

ii.) Die algebraischen Zahlentheorie beruht starkt auf eine modernere Variante, in der man oft die Lösbarkeit von Problemen in sogenannten **lokalen Körpern** ($\mathbb{Q}$ ist ein Beispiel) aus der Lösbarkeit in deren Vervollständigungen (Im Fall $\mathbb{Q}$ also $\mathbb{R}$ und $\mathbb{Q}_p$) folgert.

Das Prinzip wird zum Beispiel im folgenden Satz klar:

Proposition A.1. **Satz von Hasse-Minkowski:** *Sei f eine quadratische Form über $\mathbb{Q}$. So hat $f = 0$ genau dann eine nichttriviale Lösung in $\mathbb{Q}$, wenn es nichttriviale Lösungen in $\mathbb{R}$ und in jedem $\mathbb{Q}_p$ hat.*

Hier eine Sammlung einiger Sätze, deren Beweise p-adische Zahlen benötigen, obwohl die Sätze selbst nicht direkt etwas mit ihnen zu tun haben:

Proposition A.2. **Satz von Monsky:** *Es ist nicht möglich, ein Quadrat in eine ungerade Anzahl an Dreiecken gleicher Fläche zu unterteilen.*

Der Beweis färbt die Punkte des Quadrats basierend auf ihrer 2-adischen Bewertung und führt die Eigenschaften, die eine solche Färbung unter den gegebenen Bedingungen haben muss, zu einem Widerspruch.

Proposition A.3. **Satz von Skolem:** *Sei u_n eine Folge komplexer Zahlen, sodass jedes Folgenglied eine Linearkombination der vorherigen Glieder ist. So ist die Nullstellenmenge*

$$Z = \{n \in \mathbb{N} \mid u_n = 0\}$$

eine endliche Vereinigung arithmetischer Folgen (also von Folgen mit konstantem Abstand).

Appendix B

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 weiter Quelle ist p-adic Numbers, Q_p and Hensels Lemma, geschrieben von Yiduan Zheng.