p-adic numbers, p-adic analysis, and zeta-functions

Neal Koblitz

Springer-Verlag
New York Heidelberg Berlin
1977

Richtlinien für das Seminar

Jeder Teilnehmer sollte sich die im Seminar behandelten Abschnitte vorher durchlesen. Das Ziel des Seminars besteht in der Behandlung der beim Durchlesen auftretenden Fragen: alle Teilnehmer sollten in der Lage sein, Fragen zum Gegenstand zu stellen.

Der Vortragende gibt einen Überblick zum behandelten Gegenstand. Die Zeit wird nicht ausreichen, alle Details im Vortrag zu behandeln: es muß Stoff weggelassen werden.

Die wichtigsten Beweise sollten im Seminar vorgetragen werden. Der Vortragende hat die Freiheit, in manchen Punkten ausführlicher als das Buch zu sein.

Die Zeit wird i.a. nicht ausreichen, Übungsaufgaben im Seminar zu behandeln. Jeder Teilnehmer sollte aber versuchen, wenigsten einige dieser Übungsaufgaben zu lösen.

Contents

Vorträge

1.Die p-adischen Metriken (1.1-1.3) S. 1
2. Die p-adischen Zahlen (1.4-1.5) S. 10
3. p-adische Interpolation (2.1-2.2) S. 22
4. Andreas Klaiber**: p-adische Distributionen, Maße und Integrale** (2.3-2.5) S. 30
5. Giulio Schober: **Die p-adische ζ-Funktion** (2.6-2.7) S.42
6. Pia Scheld: Endliche Körper und die Fortsetzung von Normen (3.1+3.2) S. 52
7. Philipp Balzarek: **Die algebraische Abschließung von $\mathbb{Q}_p$ und der Körper** Ω (3.3 + 3.4) S.66
8. Susann Scholz: **Potenzreihen** (4.1) S. 76
9. Annegret Schalke: **Logarithmus, Gamma, und Artin-Hasse-Funktionen** (4.2) S. 87
10. Susanne Kürsten: **Newton-Polygone** (4.3 + 4.4) S. 97
11. Norman Metzner: **Hyperflächen und ihre Zeta-Funktionen** (5.1) S. 109
12. Anna Schenk: **Charaktere und ihre Anhebungen** (5.2) S.116
13. Bernd Herzog: **Eine lineare Abbildung auf dem Raum der Potenzreihen** (5.3) S. 118
14. Martin Huschenbett: **p-adische analytische Formeln für die Zeta-Funktion** (5.4) S. 122
15. Heinrich-Gregor Zirnstein: **Die Rationalität der Zeta-Funktion einer Menge von Gleichungen über einem endlichen Körper** S.125-129

Chapter I: p-adic numbers

1.1. Basic concepts

1.1.1 Begriff der Metrik

Sei X eine nicht-leere Menge. Ein Abstand auf X oder auch eine Metrik auf X ist eine Funktion

$$d: X \times X \to \mathbb{R}$$

mit folgenden Eigenschaften.

(1) $d(x,y) \geq 0$ für alle $x,y \in X$ und es gilt $d(x,y) = 0$ genau dann wenn $x = y$ ist.

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

(3) $d(x,y) \leq d(x,z) + d(z,y)$ für beliebige $x,y,z \in X$.

Bedingung (3) heißt auch Dreiecksungleichung. Eine (nicht-leeere) Menge X zusammen mit einem Abstand d auf X heißt metrischer Raum.

Bemerkungen

1. Dasselbe X kann auf viele verschiedene Weisen ein metrischer Raum sein.
2. In unserem Fall wird X meistens ein Körper sein, zum Beispiel $\mathbb{Q}$ oder $\mathbb{R}$.
3. Die von uns betrachteten Metriken werden von einer Norm kommen.

1.1.2 Begriff der Norm

Sei F ein Körper. Eine Norm auf F ist eine Abbildung

$$\|.\|: F \to \mathbb{R}$$

mit folgenden Eigenschaften.

(1) $\|x\| \geq 0$ für alle $x \in F$ und $\|x\| = 0$ genau dann wenn $x = 0$.

(2) $\|x \cdot y\| = \|x\| \cdot \|y\|$ für alle $x,y \in F$.

(3) $\|x+y\| \leq \|x\| + \|y\|$.

Bedingung (3) heißt Dreiecksungleichung. Die durch die gegebene Norm $\|.\|$ definierte Metrik ist gegeben durch

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

Bemerkungen

1. Es ist leicht zu sehen, die oben definierte Abbildung $d: F \times F \to \mathbb{R}$ ist tatsächlich eine Metrik auf F.
2. Ein grundlegendes Beispiel für eine Norm auf den rationalen Zahlen $\mathbb{Q}$ ist der gewöhnliche (archimedische) Absolutbetrag

   $$|.|: \mathbb{Q} \to \mathbb{R}, \; x \mapsto |x|.$$

   Die zugehörige Metrik $d(x,y) := |x-y|$ liefert gerade den gewöhnlichen Abstandsbegriff für die Punkte der rationalen Zahlengeraden.
3. Der Grund dafür, daß wir die Definition des Abstandsbegriffs als Ausgangspunkt für unsere Betrachtungen gewählt haben, besteht darin, daß sich die hier angestrebten Untersuchungen von den klassischen Untersuchungen gerade in der Wahl des Abstands unterscheiden werden.
4. Wir werden bald in der Situation sein, daß wir Abstände nicht nur auf $\mathbb{Q}$ sondern auch auf Erweiterungskörpern von $\mathbb{Q}$ betrachten müssen.

1.2 Metriken auf den rationen Zahlen

Im folgenden sei

$$p \in \{2,3,5,7,11,13,...\}$$

eine Primzahl. Wir werden jetzt in mehreren Schritten für jedes fest vorgegebene p eine Metrik auf $\mathbb{Q}$ definieren.

1.2.1 Begriff der p-adischen Ordnung einer ganzen Zahl

Sei a eine ganze Zahl. Dann ist die p-adische Ordnung von a definiert als

$$\text{ord}_p\, a := \sup \{ n \in \mathbb{Z} \mid n \geq 0, a \equiv^1 0 \pmod{p^n} \}$$

die Vielfachheit, mit der p in der Primfaktorzerlegung von a vorkommt (bzw. ∞ falls a = 0 ist). Mit anderen Worten, für $a \neq 0$ ist

$$\text{ord}_p\, a = n$$

äquivalent zu

$$a = p^n a' \text{ mit } a' \text{ teilerfremd zu } p.$$

Bemerkungen

1. Zum Beispiel gilt
   $\text{ord}_5\, 35 = \text{ord}_5\, 5 \cdot 7 = 1$
   $\text{ord}_5\, 250 = \text{ord}_5\, 2 \cdot 5 \cdot 5 \cdot 5 = 3$
   $\text{ord}_2\, 96 = \text{ord}_2\, 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 5$
   $\text{ord}_2\, 97 = 0$
2. Die Ordnungsfunktion hat eine gewissen Ähnlichkeit mit der Logarithmusfunktion: es gilt
   $$\text{ord}_p\, (ab) = \text{ord}_p\, (a) + \text{ord}_p\, (b).$$
3. Eine weitere wesentliche Eigenschaft der Ordnungsfunktion ist die folgende.
   $$\text{ord}_p\, (a+b) \quad \geq \min (\text{ord}_p(a), \text{ord}_p(b)).$$
4. Falls $\text{ord}_p(a)$ und $\text{ord}_p(b)$ verschieden sind, so gilt in 3. das Gleichheitszeichen.

Beweis von 3. Bezeichne n das Minimum auf der rechten Seite. Dann teilt p^n sowohl a als auch b,

$$p^n \mid a \text{ und } p^n \mid b.$$

Damit gilt aber auch $p^n \mid a+b$, also $\text{ord}_p\, (a+b) \geq n$.

QED.

Beweis von 4. Mit $m := \text{ord}\, \text{ord}_p(a)$ und $n := \text{ord}_p(b)$ gilt

$$a = p^m a' \text{ und } b = p^n b',$$

wobei a' und b' teilerfremd sind zu p. O.B.d.A. sei $n > m$, d.h.
$n = m + n'$ mit $n' > 0$.
Dann ist

$$a + b = p^m (a' + p^{n'} b'),$$

und der Faktor in Klammern ist teilerfremd zu p. Damit ist

$$\text{ord}_p(a+b) = m = \min (m, n) = \min(\text{ord}_p(a), \text{ord}_p(b).$$

QED.

1.2.2 Begriff der p-adischen Ordnung einer rationalen Zahl

Für jede rationale Zahl $x = \frac{a}{b}$, $a,b \in \mathbb{Z}$, definieren wir die p-adische Ordnung durch

$$\text{ord}_p\, x := \text{ord}_p\, a - \text{ord}_p\, b.$$

Bemerkungen

1. Die eben definierte Ordnung hängt nur von x und nicht von der speziellen Darstellung von x mit Hilfe von a und b ab.
2. Die oben erwähnten Eigenschaften der Ordnung von ganzen Zahlen bestehen auch im Fall rationaler Zahlen.

---

[1] $a \equiv b \bmod m$ bedeutet, die Differenz a - b ist durch m teilbar, d.h. a und b unterscheiden sich um ein Veilfaches von m.

1.2.3 Begriff der p-adischen Norm einer rationalen Zahl

Für jede rationale Zahl $x \in \mathbb{Q}$ heißt

$$|x|_p := p^{-\operatorname{ord}_p x}$$

p-adische Norm von x.

Bemerkung

Im Fall $x = 0$ ist $\operatorname{ord}_p x = \infty$ und auf der rechten Seite steht $p^{-\infty}$ dies soll nach Vereinbarung gleich Null sein,

$$p^{-\infty} := 0.$$

1.2.4 Proposition: die Normeigenschaft der p-adischen Norm

Für jede Primzahl p ist die die Abbildung

$$|\,.\,|_p : \mathbb{Q} \to \mathbb{R}$$

eine Norm auf $\mathbb{Q}$.

Beweis. Die Eigenschaften (1) und (2) von 1.1.2 sind leicht zu überprüfen. Wir ersparen uns die Details. Beweisen wir die Dreiecksungleichung (3),

$$|x + y|_p \le |x|_p + |y|_p .$$

Wegen

$$\operatorname{ord}_p (x+x) \ge \min (\operatorname{ord}_p(x), \operatorname{ord}_p(x))$$

gilt

$$-\operatorname{ord}_p (x+x) \le \max (-\operatorname{ord}_p(x), -\operatorname{ord}_p(x))$$

also

$$p^{-\operatorname{ord}_p(x+y)} \le \max (p^{-\operatorname{ord}_p x}, p^{-\operatorname{ord}_p y}) \le p^{-\operatorname{ord}_p x} + p^{-\operatorname{ord}_p y}.$$

Dies ist die behauptete Ungleichung.

QED.

Bemerkung

Wir haben sogar mehr bewiesen: für die p-adische Norm gilt

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

1.2.5 Begriff der nicht-Archimedischen Norm

Eine Norm $\| \,.\, \|$ auf einem Körper F heißt <u>nicht-Archimedisch</u>, wenn gilt

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

Anderfalls heißt sie Archimedisch.

Ein Abstand d(. , ..) auf einem Körper F heißt <u>nicht-Archimedisch</u>, wenn gilt

$$d(x,y) \le \max (d(x,z), d(z,y)).$$

Anderfalls heißt er Archimedisch.

Bemerkung

Eine Metrik ist insbesondere nicht-Archimedisch, wenn sie von einer nicht-Archimedischen Norm kommt.

1.2.6 Begriff der Cauchy-Folge

Seien (X, d) ein metrischer Raum und $\{x_n\}_{n=1,2,...}$ eine Folge von Punkten aus X. Die Folge heißt Cauchy-Folge, wenn es für jede reelle Zahl $\varepsilon>0$ ein natürliche Zahl N gibt mit

$$d(x_n , x_m) < \varepsilon \text{ für } n \ge N \text{ und } m \ge N.$$

1.2.7 Äquivalenz von Metriken und Normen

Zwei Metriken d' und d" auf der Menge X heißen äquivalent, wenn jede Folge von Punkten aus X genau dann Cauchy-Folge bezüglich d' ist, wenn sie es bezüglich d" ist.

Zwei Normen auf einem Körper F heißen genau dann äquivalent, wenn sie äquivalenten Metriken definieren.

Bemerkungen

1. Bei der Definition von $|x|_p$ hättte man anstelle von
$$p^{-ord_p x} = (\frac{1}{p})^{ord_p x}$$
auch $\rho^{ord_p x}$ wählen können mit einer beliebigen reellen Zahl zwischen 0 und 1. Für je zwei solche Werte von ρ sind alle diese Normen äquivalent.
2. Ein Grund für die Wahl $\rho = 1/p$ ist die Produktformel
$$\prod_p |x|_p = 1 \text{ für alle } x \in \mathbb{Q}$$
Dabei ist das Produkt über alle Primzahlen p einschließlich der "unendlichen Primzahl" $p = \infty$ zu erstrecken (mit $|x|_\infty = |x|$). Man beachte für fast alle p ist $|x|_p = 1$, so daß das Produkt in Wahrheit ein endliches Produkt ist (vgl. Aufgabe 18).
3. Für $0 < \alpha \leq 1$ ist durch $|x|^\alpha$ eine Familie von paarweise äquivalenten archimedischen Normen gegeben.
4. Die triviale Norm ist die Norm mit $\|0\| = 0$ und $\|x\| = 1$ für alle $x \neq 0$.

1.2.8 Theorem 1 (Ostrowski): die Normen von $\mathbb{Q}$

Jede nicht-triviale Norm von $\mathbb{Q}$ ist äquivalent zu einer Norm der Gestalt $|\,.\,|_p$ mit einer Primzahl p oder mit $p = \infty$.

Beweis. Sei $\|\,.\,\|$ eine nicht-triviale Norm auf $\mathbb{Q}$.

Fall (i). Wir nehmen an, es gibt eine positive ganze Zahl n mit $\|n\| > 1$. Wir zeigen in diesem Fall, $\|\,.\,\|$ ist äquivalent zur gewöhnlichen Betragsnorm $|\,.\,|_\infty$

Sei n_0 die kleinste positive ganze Zahl mit $\|n_0\| > 1$. Dann gibt es eine positive reelle Zahl α mit
$$\|n_0\| = (n_0)^\alpha.$$
Sie jetzt n irgendeine positive ganze Zahl. Seien $a_0, \ldots, a_s$ die Ziffern von n im Zahlensystem mit der Basis n_0, d.h.
$$n = a_0 + a_1 n_0 + a_2 (n_0)^2 + \ldots + a_s (n_0)^s \text{ mit } 0 \leq a_i < n_0 \text{ und } a_s \neq 0.$$
Dann gilt
$$\begin{aligned} \|n\| &= \|a_0\| + \|a_1 n_0\| + \|a_2 (n_0)^2\| + \ldots + \|a_s (n_0)^s\| \\ &= \|a_0\| + \|a_1\|(n_0)^\alpha + \|a_2\|(n_0)^{2\alpha} + \ldots + \|a_s\|(n_0)^{s\alpha} \end{aligned}$$
Da die a_i kleiner als n_0 sind, gilt $\|a_i\| \leq 1$, also
$$\begin{aligned} \|n\| &\leq 1 + (n_0)^\alpha + (n_0)^{2\alpha} + \ldots + (n_0)^{s\alpha} \\ &= (n_0)^{s\alpha}(1 + (n_0)^{-\alpha} + (n_0)^{-2\alpha} + \ldots + (n_0)^{-s\alpha}) \end{aligned}$$

$$\leq (n_0)^{s\alpha} \cdot \sum_{i=0}^{\infty} \left(\frac{1}{n_0^{\alpha}}\right)^i$$

Wegen $a_s \neq 0$ ist $(n_0)^s \leq n$, also folgt

$$\|n\| \leq Cn^{\alpha}$$

mit der von n unabhängigen Konstanten $C := \sum_{i=0}^{\infty} \left(\frac{1}{n_0^{\alpha}}\right)^i$. Dies gilt für jede nicht-negative ganze Zahl n. Wir ersetzen n durch n^N mit N sehr groß und ziehen die N-te Wurzel. Es ergibt sich

$$\|n\| \leq \sqrt[N]{C} \cdot n^{\alpha}.$$

Für $N \to \infty$ erhalten wir

(1) $\|n\| \leq n^{\alpha}$ für jedes nicht-negative ganze n.

Als nächstes wollen wir zeigen, es gilt in (1) das Gleichheitszeichen. Dazu schreiben wir n wieder im System zur Basis n_0 auf und erhalten

(2) $$(n_0)^s \leq n < (n_0)^{s+1}.$$

Wegen $\|(n_0)^{s+1}\| = \| n + (n_0)^{s+1} - n\| \leq \|n\| + \|(n_0)^{s+1} - n\|$ folgt

$$\begin{aligned} \|n\| &\geq \|(n_0)^{s+1}\| - \|(n_0)^{s+1} - n\| \\ &\geq n_0^{(s+1)\alpha} - \|(n_0)^{s+1} - n\| \qquad \text{(nach Definition von } \alpha) \\ &\geq n_0^{(s+1)\alpha} - ((n_0)^{s+1} - n)^{\alpha} \qquad \text{(nach (1)).} \end{aligned}$$

Damit ist

$$\begin{aligned} \|n\| &\geq n_0^{(s+1)\alpha} - ((n_0)^{s+1} - (n_0)^s)^{\alpha} \qquad \text{(wegen der 1. Ungleichung (2))} \\ &= n_0^{(s+1)\alpha} \left(1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right) \\ &\geq C' \cdot n^{\alpha} \qquad \text{(wegen der 2. Ungleichung (2))} \end{aligned}$$

mit einer von n unabhängigen Konstanten. Die Ungleichung

$$\|n\| \geq C' \cdot n^{\alpha}$$

gilt für jedes nicht-negative ganze n. Wir können wieder n durch n^N ersetzen, die N-te Wurzel ziehen und N gegen ∞ gehen lassen und erhalten die zu (1) umgekehrte Ungleichung. Zusammen ist also

(3) $\|n\| = n^{\alpha}$ für jedes nicht-negative ganze n.

Aus der Multiplikativität der Norm (Eigenschaft (2)) ergibt sich damit

$$\|x\| = |x|^{\alpha}$$

Daraus ergibt sich aber, $\| \ . \ \|$ ist äquivalent zum gewöhnlichen Absolutbetrag (vgl. Aufgabe 8).

Fall (ii). Für jedes nicht-negative ganz n gilt $\|n\| \leq 1$.

Sei n_0 die kleinste positive ganze Zahl mit $\|n_0\| < 1$. Die Zahl n_0 existiert, weil die gegebene Norm nach Voraussetzung nicht trivial sein soll. Es handelt sich um eine Primzahl, denn aus

$$n_0 = n' \cdot n'' \text{ mit } n' < n_0 \text{ und } n'' < n_0$$

folgte $\|n_0\| = \|n'\| \cdot \|n''\| = 1 \cdot 1 = 1$ im Widerspruch zur Wahl von n_0. Also ist

$$n_0 = p \text{ Primzahl.}$$

Sei jetzt q eine von p verschiedene Primzahl. Wir wollen zeigen, dann gilt $\|q\| = 1$. Angenommen, das ist nicht der Fall. Dann gilt

$$\|q\| < 1.$$

Für N groß genug ist dann

$$\|q^N\| = \|q\|^N < \frac{1}{2}$$

Analog gilt für M groß genug auch

$$\|p^M\| < \frac{1}{2}.$$

Nun sind p^M und q^N teilerfremd, d.h. es gibt ganze Zahlen n und m mit

$$mp^M + nq^N = 1$$

(vgl. Aufgabe 10). Damit gilt aber

$$1 = \|1\| = \| mp^M + nq^N\| \le \|mp^M\| + \|nq^N\| = \|m\| \cdot \|p^M\| + \|n\| \cdot \|q^N\|.$$

Nach Voraussetzung des Falls (ii) ist aber die Norm jeder ganzen Zahl ≤ 1, d.h. es gilt

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

Da dies nicht möglich ist, folgt

$\|q\| = 1$ für jede von p verschiedene Primzahl q.

Damit ist der Beweis der Behauptung im Prinzip abgeschlossen: jede rationale Zahl a läßt sich in der Gestalt

$$a = \pm p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$$

mit paarweise verschiedenen Primzahlen p_i und ganzen Zahlen n_i schreiben. Damit ist

$$\|a\| = \|p_1\|^{n_1} \cdot \ldots \cdot \|p_r\|^{n_r} = \|p\|^{n_i}$$

falls $p_i = p$ ist, d.h. $n_i = \mathrm{ord}_p(a)$. Mit $\rho := \|p\| < 1$ ist dann

$$\|a\| = \rho^{\mathrm{ord}_p a},$$

d.h. $\| \cdot \|$ ist äquivalent zur p-adischen Norm.

QED.

Bemerkungen

1. Unsere Vorstellungen zum Abstandsbegriff basieren natürlich auf unserer Erfahrung mit dem Archimedischen Abstand des $\mathbb{R}^3$. Einige Eigenschaften der nicht-Archimedischen Normen $|\ |_p$ werden uns zunächst ziemlich seltsam vorkommen, und es wird eine Weile dauern, bis wir uns an sie gewöhnt haben., Wir führen hier zwei Beispiele an.
2. Jedes Dreieck ist gleichschenklig (d.h. zwei Seiten haben dieselbe Länge).
3. Jeder Punkt einer Kreisscheibe ist Mittelpunkt dieser Kreisscheibe.

1.3. Zur Konstruktion der komplexen Zahlen

Die Konstruktion der komplexen Zahlen aus den natürlichen Zahlen beruht im wesentlichen auf zwei Prinzipien.

(1) Hinzufügen von Lösungen algebraischer Gleichungen.

(2) Hinzufügen von Grenzwerten von Cauchy-Folgen.

Beschreibung der Übergänge

$$\mathbb{N} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$$

Der Vorgang im p-adischen Fall:

1. Der Erweiterungs $\mathbb{Q} \to \mathbb{R}$ hängt von der Wahl einer Metrik ab. Verwendet man die p-adische Norm anstelle des Absolutbetrags, so erhält man den Körper
$$\mathbb{Q}_p$$
der p-adischen Zahlen anstelle von $\mathbb{R}$.
2. Beim Übergang zur algebraischen Abschließung
$$\overline{\mathbb{Q}}_p$$
wird es nicht genügen eine Lösung einer algebraischen Gleichung hinzuzufügen: wir werden unendlich viele solche Gleichungen brauchen.
3. Der bereits riesengroße Körper $\overline{\mathbb{Q}}_p$ ist nicht vollständig, d.h. wir haben erneut sämtliche Limiten sämtlicher Cauchy-Folgen hinzuzufügen. Wir erhalten so einen noch größeren Körper
$$\Omega.$$

Von diesem Körper wird sich herausstellen, daß er sowohl algebraisch abgeschlossen als auch vollständig ist. Er stellt also das p-adische Analogon zum Körper $\mathbb{C}$ der komplexen Zahlen dar.

Dieser Körper ist weit weniger erforscht als $\mathbb{C}$. Zum Beispiel kennt man bis heute keine befriedigende Beschreibung der $\mathbb{Q}_p$-linearen Körperautomorphismen von Ω.

1.4 Der Körper der p-adischen Zahlen

Für den Rest des ersten Kapitels bezeichne p eine Primzahl,

$$p \neq \infty.$$

1.4.1 Definition von $\mathbb{Q}_p$ als Menge

Bezeichne S die Menge der p-adischen Cauchy-Folgen in $\mathbb{Q}$, d.h. die Menge aller Folgen

$$\{a_i\}$$

reeller Zahlen mit der Eigenschaft, daß es für jedes reelle $\varepsilon>0$ ein N gibt mit

$$|a_i - a_{i'}|_p < \varepsilon \text{ für } i, i' > N.$$

Zwei Elemente $\{a_i\}$ und $\{b_i\}$ von S heißen äquivalent,

$$\{a_i\} \sim \{b_i\},$$

wenn die zugehörige Differenzfolge eine Nullfolge ist, d.h. für jedes reelle $\varepsilon>0$ gibt es ein $N>0$ mit

$$|a_i - b_i|_p < \varepsilon \text{ für } i > N.$$

Die p-adischen Zahlen sind dann definiert als Äquivalenzklassen von p-adischen Cauchy-Folgen,

$$\mathbb{Q}_p := S/\sim := \{ \overline{\{a_i\}} \mid \{a_i\} \in S \}$$

mit

$$\overline{\{a_i\}} := \{ \{b_i\} \in S \mid \{b_i\} \sim \{a_i\} \}.$$

Bemerkung

Es ist leicht zu sehen, daß je zwei Äquivalenzklassen $\overline{\{a_i\}}$ identisch oder disjunkt sind.

1.4.2 Einbettung von $\mathbb{Q}$ in die Menge $\mathbb{Q}_p$

Für jede rationale Zahl $x\in\mathbb{Q}$ bezeichne

$$\{x\} \in S$$

die konstante Folge, deren sämtliche Glieder gleich x sind. Wenn keine Verwechslungsgefahr besteht, werden wir die Äquivalenzklasse dieser Folge wieder mit x bezeichnen,

$$x = \overline{\{x\}} \in \mathbb{Q}_p.$$

Insbesondere sei 0 die Äquivalenzklasse zur konstanten Folge {0}.

Bemerkung

Wir haben damit eine Abbildung

$$\mathbb{Q} \to \mathbb{Q}_p \text{ , } x \mapsto x = \overline{\{x\}},$$

definiert. Diese Abbildung ist injektiv, denn aus $\overline{\{x\}} = \overline{\{y\}}$ folgt $|x-y|_p < \varepsilon$ für jedes reelle $\varepsilon>0$, d.h. $|x-y|_p = 0$, d.h. $x = y$ in $\mathbb{Q}$.

1.4.3 Fortsetzung der p-adische Norm auf $\mathbb{Q}_p$

Sei $a = \overline{\{a_i\}}$ eine p-adische Zahl. Dann setzen eir

$$|a|_p := \lim_{i\to\infty} |a_i|_p .$$

Beweis der Korrektheit der Definition.Wir haben zu zeigen, dieser Limes existiert und ist unabhängig von der speziellen Wahl des Repräsentanten $\{a_i\}$.

1. Unabhängigkeit von der Wahl des Repräsentanten

Aus $\overline{\{a_i\}} = \overline{\{b_i\}}$, d.h. $\{a_i\} \sim \{b_i\}$, folgt $|a_i - b_i|_p \to 0$ für $i \to \infty$, und wegen

$$||a_i|_p - |b_i|_p| \le |a_i - b_i|_p$$

auch

$$||a_i|_p - |b_i|_p \to 0 \text{ für } i \to \infty.$$

Insbesondere existiert $\lim_{i\to\infty} |a_i|_p$ genau dann, wenn $\lim_{i\to\infty} |b_i|_p$ existiert, und die beiden Limiten stimmen, falls sie existieren überein.

2. Existenz des Limes im Fall a = 0.

Die Aussage ist trivial: die konstante Folge zu $|0|_p = 0$ konvergiert gegen 0.

3. Existenz im Limes im Fall $a \neq 0$.

Dann ist $\{a_i\}$ nicht äquivalent zu {0}, d.h. $\{a_i\}$ ist keine p-adische Nullfolge, d.h. es gibt ein reelles $\varepsilon>0$ derart, daß zu jedem $N\in\mathbb{N}$ ein $i_N > N$ existiert mit

(1) $$|a_{i_N}|_p > \varepsilon.$$

Wir wählen N so groß, daß gilt

$$|a_i - a_{i'}|_p < \varepsilon \text{ für beliebige } i, i' > N.$$

Speziell für $i' := i_N$ ist damit

(2) $$|a_i - a_{i_N}|_p < \varepsilon \text{ für jedes } i > N.$$

Nach dem Prinzip des gleichschenkligen Dreiecks folgt aus (1) und (2)

$$|a_i|_p = \max\{|a_{i_N}|_p, |a_i - a_{i_N}|_p\} = |a_{i_N}|_p \text{ für } i > N.$$

Mit anderen Worten, die Folge der $|a_i|_p$ ist von einer gewissen Stelle an konstant. Insbesonder existiert ihr Grenzwert.
QED.
Bemerkung
Wir weisen auf einen wichtigen Unterschied bei der Fortsetzung der Norm auf die "Vervollständigung" hin: beim Übergang von $\mathbb{Q}$ nach $\mathbb{R}$ vergrößert sich die Menge der Werte der Norm ganz erheblich: $|\mathbb{Q}|$ ist abzählbar und $|\mathbb{R}|$ ist überabzählbar. Dagegen bleibt die Menge der Werte beim Übergang von $\mathbb{Q}$ nach $\mathbb{Q}_p$ unverändert:

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

1.4.4 Fortsetzung der Multiplikation von $\mathbb{Q}$ auf $\mathbb{Q}_p$

Seien zwei p-adische Zahlen

$$a = \overline{\{a_i\}}, \quad b = \overline{\{b_i\}}$$

gegeben. Es ist leicht zu sehen, daß dann $\{a_i b_i\}$ ein p-adische Cauchy-Folge ist. Wir setzen

$$a \cdot b := \overline{\{a_i b_i\}}.$$

Beweis der Korrektheit der Definiton. Wir haben zu zeigen, daß diese Definition korrekt, d.h. unabhängig von der Wahl der Repräsentanten $\{a_i\}$ und $\{b_i\}$, ist. Seien weitere Repräsentanten gegeben.

$$a = \overline{\{a'_i\}}, \quad b = \overline{\{b'_i\}}.$$

Dann gilt

$$|a'_i b'_i - a_i b_i|_p = |a'_i (b'_i - b_i) + b_i (a'_i - a_i)|_p \le \max(|a'_i (b'_i - b_i)|_p, |b_i (a'_i - a_i)|_p).$$

Der erste Ausdruck rechts konvergiert gegen

$$|a| \cdot \lim_{i \to \infty} |b'_i - b_i|_p = 0$$

und der zweite Ausdruck rechts gegen

$$|b| \cdot \lim_{i \to \infty} |a'_i - a_i|_p = 0.$$

Deshalb gilt

$$\{a_i b_i\} \sim \{a'_i b'_i\},$$

d.h.

$$\overline{\{a_i b_i\}} = \overline{\{a'_i b'_i\}}.$$

hängt nicht von der speziellen Wahl der Repräsentanten ab.
QED.

1.4.5 Zur Fortsetzung der übrigen Grundrechenoperationen

Die Fortsetzung von Addition und Subtraktion von $\mathbb{Q}$ auf $\mathbb{Q}_p$ erfolgt in analoger Weise.
Bei der Fortsetzung der Division muß man etwas mehr Sorgfalt walten lassen, weil einige Glieder der betrachteten Cauchy-Folgen Null sein können.

Es ist jedoch leicht, einzusehen, daß jede Cauchy-Folge $\{b_i\}$ äquivalent ist zu einer Cauchy-Folge $\{b'_i\}$ mit von Null verschiedenen Gliedern. Ist $b_i = 0$, so kann man b_i zum Beispiel durch $b'_i = p^i$ ersetzen. Zu der veränderten Folge gehört dann die Folge

$$\{\frac{1}{b'_i}\}.$$

Dies ist eine Cauchy-Folge, außer im Fall $|b_i|_p \to 0$, d.h. im Fall $\{b_i\} \sim \{0\}$, Den Quotienten von

$$a = \overline{\{a_i\}} \text{ und } b = \overline{\{b_i\}}$$

kann man dann (im Fall $b \neq 0$) definieren als die Äquivalenzklasse

$$a/b := \overline{a_i/b'_i}\ .$$

1.4.6 Eigenschaften der fortgesetzen Operationen

Es ist leicht zu sehen, daß $\mathbb{Q}_p$ mit den fortgesetzen Operationen ein Körper ist. Durch die Einbettung

$$\mathbb{Q} \to \mathbb{Q}_p\ ,\ a \mapsto \overline{\{a\}}\ ,$$

wird $\mathbb{Q}$ ein Teilkörper von $\mathbb{Q}_p$ mit der Eigenschaft, daß jedes Element Limes einer Folge von Elementen aus $\mathbb{Q}$ ist.

Genauer: für $a = \overline{\{a_i\}}$ gilt $a_i \to a$ in $\mathbb{Q}_p$.

1.4.7 Die Vollständigkeit von $\mathbb{Q}_p$

Sei $\{a_j\}$ eine Cauchy-Folge in $\mathbb{Q}_p$. Wir haben zu zeigen, $\{a_j\}$ konvergiert gegen ein $a \in \mathbb{Q}_p$.

Konvergenzbeweis. Mit $a_j = \overline{\{a_{ji}\}}$ gilt

$$a_{ji} \to a_j \text{ in } \mathbb{Q}_p \text{ für } i \to \infty.$$

Indem wir $\{a_{ji}\}$ durch eine Teilfolge ersetzen, können wir erreichen, es gilt

$$|a_{ji} - a_j|_p < p^{-j} \text{ für alle } i,$$

also

$$|a_{ii} - a_{i'}|_p \leq \max (|a_{ii} - a_i|\ ,\ |a_{i'i'} - a_{i'}|) < \max (p^{-i},p^{-i'}).$$

Mit anderen Worten, $\{a_{ii}\}$ ist eine Cauchy-Folge in $\mathbb{Q}$, repräsentiert also ein

$$a := \overline{\{a_{ii}\}} \in \mathbb{Q}_p.$$

Nach Konstruktion gilt

$$|a - a_{ii}|_p \to 0 \text{ für } i \to \infty.$$

Wegen

$$|a - a_i|_p \leq |a - a_{ii}|_p + |a_{ii} - a_i| \leq p^{-i} + |a - a_{ii}|_p\ (\to 0 \text{ für } i \to \infty)$$

ist deshalb $| a - a_i |_p \to 0$, d.h. $a_i \to a$.

QED.

Bemerkung

Der Leser sollte versuchen wenigstens die eine oder andere Teilaussage dieses Satzes zu beweisen, um die axiomatischen Grundlagen auf denen die ganze Theorie beruht nicht vollständig zu vergessen. Die hier angedeutete abstrakte Vorgehensweise liefert uns außerdem eine Möglichkeit die p-adischen Konstruktionen mit den analogen Konstruktionen im Fall der reellen Zahlen zu vergleichen, und zu erkennen, daß es sich formal um dieselben Konstruktionen handelt.

Nach dem Beweis des nachfolgenden Satzes sollte man aber möglichst schnell den Gesichtspunkt der Äquivalenzklassen vergessen und eine konkretere Betrachtungsweise beginnen.

1.4.8 Theorem 2: repräsentierende Folgen für p-adische Zahlen aus dem Einheitskreis

Jede p-adische Zahl $a \in \mathbb{Q}_p$ mit $|a|_p \leq 1$ besitzt genau eine repräsentierende Cauchy-Folge

$$\{a_i\}$$

mit

(1) $0 \leq a_i < p^i$ für $i = 1,2,3,...$

(2) $a_i \equiv a_{i+1} \pmod{p^i}$ für $i = 1,2,3,...$

Beweis. Eindeutigkeitsbeweis. Angenommen, es gibt eine zweite repräsentierende Cauchy-Folge $\{a'_i\}$. Dann gibt es ein i_0 mit

$$a_{i_0} \neq a'_{i_0}.$$

Weil beide Glieder zwischen 0 und $p^{i_0} - 1$ liegen, folgt

$$a_{i_0} \neq a'_{i_0} \bmod p^{i_0}.$$

Für $i > i_0$ ist dann aber

$$a_i \equiv a_{i_0} \neq a'_{i_0} \equiv a'_i \pmod{p^{i_0}},$$

d.h.

$$|a_i - a'_i|_p > p^{-i_0} \text{ für alle } i > i_0.$$

Dann können aber die beiden Folgen $\{a_i\}$ und $\{a'_i\}$ nicht gegen denselben Grenzwert konvergieren, d.h. sie repräsentieren nicht dieselbe p-adische Zahl.

Existenzbeweis. Zum Beweis benötigen wir das folgende Lemma, welches wir anschließend beweisen.

Lemma

Für jede rationale Zahl $x \in \mathbb{Q}$ mit $|x|_p \leq 1$ und jede nicht-negative ganze Zahl i gibt es eine ganze Zahl

$$\alpha \in \mathbb{Z}$$

mit

$$|\alpha - x|_p \leq p^{-i}.$$

Die ganze Zahl α kann man sogar aus dem Intervall zwischen 0 und p^i-1 wählen:

$$0 \le \alpha < p^i$$

Der Existenzbeweis. Sei $\{b_i\}$ eine Cauchy-Folge in $\mathbb{Q}$. Wir konstruieren eine Cauchy-Folge $\{a_i\}$ in $\mathbb{Q}$ die den Bedingungen 1 und 2 des Satzes genügt.

Für j = 1,2,3,... wählen wir nacheinander eine natürliche Zahl N(j) mit

(1) $$|b_i - b_{i'}|_p \le p^{-j} \text{ für } i,i' \ge N(j).$$

Wir können die N(j) dabei so wählen, daß sie eine streng monoton steigende Folge bilden,

$$N(j) < N(j+1).$$

Insbesondere ist dann

$$j \le N(j).$$

Man beachte, es gilt

(2) $$|b_i|_p \le 1 \text{ für } i \ge N(1).$$

Ist ist nämlich für alle $i' \ge N(1)$

$$|b_i|_p \le \max(|b_{i'}|_p, |b_i - b_{i'}|_p) \le \max(|b_{i'}|_p, 1/p)$$

und $|b_{i'}|_p \to |a|_p \le 1$ für $i' \to \infty$. Es gilt also (2).

Auf Grund des Lemmas gibt es für jedes j eine ganze Zahl a_j mit

(3) $$|a_j - b_{N(j)}| \le p^{-j}.$$

Es reicht zu zeigen, $\{a_i\}$ ist eine Folge mit den gesuchten Eigenschaften. Wir haben zu zeigen,

(*) $$a_{j+1} \cong a_j \pmod{p^j} \text{ und } \{a_i\} \sim \{b_i\}.$$

Es gilt

$$\begin{aligned} |a_{j+1} - a_j|_p &\le \max(|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |b_{N(j)} - a_j|_p) \\ &\le \max(p^{-j-1}, p^{-j}, p^{-j}) \quad \text{(nach (3), (1) und (3)} \\ &\le p^{-j} \end{aligned}$$

Damit ist die erste Bedingung von (*) erfüllt. Weiter gilt für jedes j und jedes $i \ge N(j)$

$$\begin{aligned} |a_i - b_i|_p &\le \max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_{N(j)} - b_i|_p) \\ &\le \max(p^{-j}, p^{-j}, p^{-j}) = p^{-j}. \end{aligned}$$

Man beachte, es gilt $|a_i - a_j|_p \le p^{-j}$ wegen $i \ge N(j) \ge j$ und der gerade bewiesenen Abschätzung. Die beiden anderen Ungleichungen ergeben sich aus (3) bzw. (1). Damit gilt

$$|a_i - b_i|_p \to 0,$$

d.h. die zweite Bedingung (*) ist erfüllt.

Beweis des Lemmas. Wir schreiben x = a/b mit teilerfremden ganzen Zahlen a und b,

$$x = a/b \text{ , } ggT(a,b) = 1.$$

Wegen $|x|_p \le 1$ ist p kein Teiler von b, d.h. p und p^i sind teilerfremd,

$$ggT(b, p^i) = 1.$$

Es gibt deshalb ganze Zahlen m und n mit

$$mb + np^i = 1.$$

Wir setzen

$$\alpha := am.$$

Bemerkung
Die Idee für diese Definition beruht auf der Tatsache, daß sich mb von 1 um ein p-adisch kleines Element unterscheidet, d.h. 1/b liegt p-adisch nahe bei m, a/b nahe bei am.

Genauer gilt:

$$|\alpha - x|_p = |am - (a/b)|_p = |a/b|_p \cdot |mb - 1|_p = |np^i|_p = |n|_p \cdot p^{-i} \le p^{-i}.$$

Die letzte Ungleichung besteht, weil n eine ganze Zahl ist.

Bei Addition eines ganzzahligen Vielfachen von p^i zu α bleibt die Ungleichung

$$|\alpha - x|_p \le p^{-i}.$$

erhalten (weil $||_p$ nicht-Archimedisch ist). Wir können deshalb α so abändern, daß auch die letzte Bedingung erfüllt ist.
QED.

Bemerkung
Der nachfolgende Satz ist das Analogon zu der Aussage, daß sich jede reelle Zahl als ein unendlicher Dezimalbruch schreiben läßt. Die Rolle der Basis 10 spielt dabei die Primzahl p.

1.4.9 Die p-adische Entwicklung

Für jede p-adische Zahl $a \in \mathbb{Q} - \{0\}$ läßt sich auf genau eine Weise in der Gestalt

$$a = \frac{1}{p^m} \sum_{i=0}^{\infty} b_i p^i$$

mit $m := -\mathrm{ord}_p$, $b_0 \neq 0$ und einer eindeutig bestimmten Folge $\{b_i\}_{i=0,1,...}$ von ganzen Zahlen b_i mit

(1) $0 \le b_i < p^i$ für i = 1,2,3,...

(2) $b_i \cong b_{i+1} \pmod{p^i}$ für i = 1,2,3,...

Die unendliche Summe steht dabei wie üblich für den Limes ihrer endlichen Partialsummen.
Beweis. Wir können a mit einer p-Potentz multiplizieren und daher annehmen,

$$|a|_0 = 1.$$

Existenz. Sei $\{a_i\}$ die nach 1.4.8 zu a gehörige Folge. Dann gilt

(*) $$a = \lim_{i \to \infty} a_i$$

Wir schreiben a_i als Zahl im Zahlensystem mit der Basis p,

$$a_i = b_0 + b_1 p + b_2 p^2 + ... + b_{i-1} p^{i-1} \text{ mit } 0 \le b_j < p.$$

Analog erhält man für a_{i+1} die Darstellung

$$a_{i+1} = b'_0 + b'_1 p + b'_2 p^2 + ... + b'_i p^i \text{ mit } 0 \le b'_j < p.$$

Nach Bedingung (2) von 1.4.8 gilt aber $a_i \cong a_{i+1} \pmod{p^i}$, d.h.

$$b_0 + b_1 p + b_2 p^2 + ... + b_{i-1} p^{i-1} = b'_0 + b'_1 p + b'_2 p^2 + ... + b'_{i-1} p^{i-1},$$

und wegen der Eindeutigkeit der Ziffern im System zur Basis p folgt

$$b_j = b'_j \text{ für } i = 0, \ldots, i-1.$$

Die ersten i Ziffern von a_i und a_{i+1} stimmen also überein. Es gibt damit eine Folge von ganzen Zahlen b_i die den obigen Bedingungen (1) und (2) genügen mit

$$a_i = \sum_{j=0}^{i} b_j p^j$$

Zusammen mit (*) ist dies gerade die Existenzaussage des Satzes.

Eindeutigkeit. Ist $a = \sum_{i=0}^{\infty} b_i p^i$, so sind die Partialsummen $a_i = \sum_{j=0}^{i} b_j p^j$ gerade die Glieder einer Folge wie in 1.4.8. Die Eindeutigkeitsaussage von 1.4.8 liefert damit die Eindeutigkeitsaussage des vorliegenden Satzes.
QED.

1.4.10 Der Ring $\mathbb{Z}_p$ der ganzen p-adischen Zahlen

Wir setzen

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

Dies ist gerade die Menge aller p-adischen Zahlen, deren p-adische Entwicklung keine negative p-Potenzen enthält. Ein Element von $\mathbb{Z}_p$ heißt ganze p-adische Zahl. Summen, Differenzen und Produkte von Elementen aus $\mathbb{Z}_p$ liegen wieder in $\mathbb{Z}_p$. Mit anderen Worten, $\mathbb{Z}_p$ ist ein Teilring von $\mathbb{Q}_p$.

Weiter schreiben wir für die Einheitengruppe von $\mathbb{Z}_p$,

$$\begin{aligned} \mathbb{Z}_p^{\times} &:= \{x \in \mathbb{Z}_p \mid 1/x \in \mathbb{Z}_p \} \\ &= \{ x \in \mathbb{Z}_p \mid |x|_p = 1 \} \\ &= \{ x \in \mathbb{Z}_p \mid x = \sum_{i=0}^{\infty} b_i p^i \text{ (p-adische Entw.)}, b_0 \neq 0 \} \end{aligned}$$

1.4.10 Kongruenzrelationen in $\mathbb{Q}_p$

Seien $a,b \in \mathbb{Q}_p$ zwei p-adische Zahlen. Dann schreiben wir

$$a \cong b \pmod{p^n},$$

wenn gilt

$$|a-b|_p \leq p^{-n}.$$

Diese Bedingung ist äquivalent zu

$$\frac{a-b}{p^n} \in \mathbb{Z}_p ,$$

was seinerseits bedeutet,

die p-adische Entwicklung von a-b beginnt mit der Potenz p^n oder spater.

Bemerkung
Die letzte Bedingung zeigt, für gewöhnliche ganze Zahlen (“rationale ganze Zahlen”) stimmt die obige Definition von “$\cong \pmod{p^n}$” mit der ursprünglichen überein.

1.4.12 Konvergenz von Reihen p-adischer Zahlen

Sei $\{c_i\}$ eine Folge p-adischer Zahlen . Dann sind die beiden folgenden Bedingungen äquivalent.

(i) $\sum_{i=1}^{\infty} c_i$ ist konvergent (die Folge der Partialsummen konvergiert).

(ii) $|c_i|_p \to 0$.

Beweis. Wir beschränken uns auf den Beweis der interessanten Implikation (ii)⇒(i). Sei Bedingung (ii) erfüllt. Wir setzen

$$s_n = \sum_{i=1}^{n} c_i .$$

Dann gilt für $n \geq m$

$$|s_n - s_m|_p \leq \max(|c_n|_p , |c_{n-1}|_p , \ldots , |c_{m+1}|_p).$$

Wegn (ii) kann man den Ausdruck rechts beliebig klein machen, wenn man nur m und n hinreichend groß wählt. Mit anderen Worten, $\{s_n\}$ ist eine Cauchy-Folge von p-adischen Zahlen und als solche konvergent in $\mathbb{Q}_p$.

QED.

1.4.13 Systeme von Ziffern für die p-adische Entwicklung

Anstelle der p-adischen Ziffern 0, 1, ... , p-1 hätten wir ein beliebiges System

$$\alpha_0, \alpha_1 , \ldots , \alpha_{p-1}$$

von ganzen Zahlen wählen können mit

$$\alpha_i \cong i \pmod p.$$

Alle Aussagen über die p-adische Entwicklung hätten wir auch für diese Ziffern in analoger Weise erhalten. Für die meisten Zwecke reichen die von uns gewählten Ziffern aus.

Es gibt jedoch ein anderes System von Ziffern, die sogenannn Teichmüller-Repräsentanten die in gewisser Weise die natürlichere Wahl darstellen.

1.5 Arithmetik im Körper $\mathbb{Q}_p$

Das Rechnen mit p-adischen Zahlen ist dem Rechnen mit Dezimalbrüchen recht ähnlich. Der Unterschied besteht darin, daß die niedrigen Kommastellen zuerst verarbeitet werden (statt zuletzt wie im klassischem Fall) und daß Überträge in der umgekehrt Richtung stattfinden. Betrachten wir die Multiplikation anhand eines einfachen Beispiels.

$(3 + 6\cdot 7 + 2\cdot 7^2)\cdot(4 + 5\cdot 7 + 1\cdot 7^2)$

$5\cdot 7^0$	$+1\cdot 7^1$			
	$3\cdot 7^1$	$+3\cdot 7^2$		
		$+1\cdot 7^2$	$+1\cdot 7^3$	
	$1\cdot 7^1$	$+2\cdot 7^2$		
		$2\cdot 7^2$	$+4\cdot 7^3$	
			$3\cdot 7^3$	$+1\cdot 7^4$
		$3\cdot 7^2$	$+6\cdot 7^3$	$+2\cdot 7^4$
			1	2

$$5\cdot 7^0 \quad +5\cdot 7^1 \quad +4\cdot 7^2 \quad +1\cdot 7^3 \quad +5\cdot 7^4$$

In ähnlicher Weise werden Summen, Differenzen und Quotienten gebildet. Wurzeln aus p-adischen Zahlen berechnet man, indem man beginnend mit dem niedrigsten Glied immer höhere Glieder der p-Entwicklung berechnet.

Existiert die gesuchte Wurzel in $\mathbb{Q}_p$ nicht, so ergibt sich bei diesen Berechnungen ein Widerspruch (zum Beispiel existiert $\sqrt{6}$ in $\mathbb{Q}_5$, dagegen $\sqrt{7}$ existiert dort nicht).

Theorem 3 (Henselsches Lemma)

Sei $F(x) = c_0 + c_1 x + ... + c_n x^n$ ein Polynom mit Koeffizienten aus $\mathbb{Z}_p$ und mit der Ableitung F'(x). Dann gibt es für jede ganze p-adische Zahl a_0 mit

$$F(a_0) \cong 0 \pmod{p} \text{ und } F'(a_0) \neq 0 \pmod{p}$$

genau eine ganze p-adische Zahl a mit

$$F(a) = 0 \text{ und } a \cong a_0 \pmod{p}.$$

Beweis.

QED.