Universität Bielefeld

Algebra

Die p-adischen Zahlen

Seminararbeit

von

Denny Otten

FAKULTÄT FÜR MATHEMATIK

Datum: 29. Oktober 2006

Betreuung:
Prof. Dr. Dr. K. Tent
Dipl.-Math. G. Hainke
Dipl.-Math. L. Scheele

Inhaltsverzeichnis

3 Die p-adischen Zahlen

Dieser Vortrag ist eine kurze Einführung in das Themengebiet der p-adischen Zahlen". Da die eigentliche Theorie der p-adischen Zahlen jedoch dermaßen umfangreich ist, werden wir uns nur mit einem kleinen Teil dessen beschäftigen, was die Zahlen so interessant macht.

In Kapitel 3.1 gilt unser Hauptaugenmerk der Herleitung der p-adischen Zahlen. Wir werden dabei lediglich die analytische Konstruktion betrachten und im Anschluss dazu den Zusammenhang zur Hensel'schen Definition der p-adischen Zahlen verdeutlichen. Auf die algebraische Konstruktion über den projektiven Limes wird jedoch nicht näher eingegangen. Zum Abschluss des Kapitels werden wir noch einige Eigenschaften der p-adischen Zahlen aufzeigen und beweisen.

Kapitel 3.2 ist eine erste Anwendung der p-adischen Zahlen. Es enthält ein sehr interessantes Prinzip, das so genannte Lokal-Global-Prinzip"(oder auch Lokalisation"genannt) von Hasse-Minkowski. Die Aussage ist dabei vereinfacht ausgesprochen, dass eine Gleichung genau dann über den rationalen Zahlen $\mathbb{Q}$ lösbar ist, wenn sie über den reellen Zahlen $\mathbb{R}$ und über allen p-adischen Zahlen $\mathbb{Q}_p$ gelöst werden kann.

In Kapitel 3.3 kommen wir als zweite Anwendung der p-adischen Zahlen auf das Hensel'sche Lemma zu sprechen. Dieses Lemma ist von enormer Bedeutung. Denn es garantiert uns für ein Polynom f aus einem Bewertungsring A, dass es genau dann Nullstellen in A besitzt, wenn das modulo p reduzierte Polynom $\overline{f}$ eine einfache Nullstelle im Restklassenkörper von A besitzt. Der interessante Hintergrund hierbei ist, dass der Restklassenkörper von A wesentlich weniger Elemente besitzt, als A selbst enthält.

Kapitel 3.4 enthält schlussendlich alle zugrunde liegenden Beweise.

Im Anhang A, Anhang B und Anhang C sind einige Definitionen aufgeführt, die in diesem Vortrag als bekannt vorausgesetzt werden. Dabei handelt es sich zum größten Teil um Definitionen aus den mathematischen Teilgebieten der Analysis (Analysis I, II) und der Algebra (Algebra I).

In Anhang D ist zum Abschluss eine zusammengefasst Auflistung aller wichtigen Eigenschaften der p-adischen Zahlen.

3.1 Konstruktion der p-adischen Zahlen

Bei der Konstruktion der p-adischen Zahlen gibt es zwei grundlegende Herangehensweisen:

- Analytische Konstruktion (Bewertungen, Vervollständigung)
- Albegraische Konstruktion (projektiver Limes)

Wir werden uns in diesem Vortrag jedoch lediglich mit der zuerst genannten Konstruktionsmethode auseinandersetzen.

Funktionentheoretische Konstruktion über Potenzreihen:

Die p-adischen Zahlen wurden erstmals 1897 von Kurt Hensel eingeführt in der Absicht, die machtvolle Methode der Potenzreihenentwicklung, welche in der Funktionentheorie eine sehr zentrale Rolle spielt, auch der Zahlentheorie zur Verfügung zu stellen. In diesem ersten Abschnitt definieren wir die p-adischen Zahlen also mit Hilfe unserer Analysis Kenntnisse über Potenzreihen und Laurentreihen. Dazu sei von nun an $p \in \mathbb{P}$ eine Primzahl, wobei

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots\} \quad (\textit{Primzahlenmenge})$$

die Primzahlenmenge darstellt. Bevor wir nun zur Herleitung der p-adischen Zahlen kommen, beginnen wir aus Motivationsgründen mit einem kurzen Beispiel.

BEISPIEL 3.1.1:
Die Zahl 137 lässt sich zur Basis p=3 auch schreiben als

$$137 = 2 \cdot 3^0 + 0 \cdot 3^1 + 0 \cdot 3^2 + 2 \cdot 3^3 + 1 \cdot 3^4 = \sum_{i=0}^{\infty} a_i 3^i$$

wobei $a_0 = 2, a_1 = 0, a_2 = 0, a_3 = 2, a_4 = 1, a_n = 0$ $(\forall\, n \geqslant 5)$. Gelegentlich findet man diesbezüglich auch die folgende Schreibweise

$$137 = (20021)_3$$

Betrachten wir nun die Folge der Partialsummen

$$(s_n)_{n\in\mathbb{N}} = \left(\sum_{i=0}^{n-1} a_i 3^i \right)_{n\in\mathbb{N}} = (2, 2, 2, 56, 137, 137, \ldots)$$

dann sehen wir, dass diese Folge gegen unsere Zahl 137 konvergiert.

Allgemeiner gilt:

SATZ 3.1.2:
Sei $p \in \mathbb{P}$ beliebig aber fest. Dann gilt: Jede natürliche Zahl $n \in \mathbb{N}$ lässt sich eindeutig darstellen als

$$n = \sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \cdots \quad (\text{wobei } a_i \in \{0, 1, \ldots, p-1\})$$

BEWEIS:

$\longrightarrow$ zum Beweis ■

DEFINITION 3.1.3:
Die Darstellung der Zahl $n \in \mathbb{N}$ in Satz 3.1.2 heißt *p-adische Entwicklung von n*.

Betrachten wir nun allgemein für

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

(wobei $n \in \mathbb{N}$) die Folge der Partialsummen

$$(s_n)_{n\in\mathbb{N}} = \left(\sum_{i=0}^{n-1} a_i p^i \right)_{n\in\mathbb{N}}$$

so erkennen wir sofort, dass diese Folge gegen unsere natürliche Zahl n konvergiert.
Wollen wir auf diese Weise nun auch negative und gebrochene Zahlen darstellen, so sind wir gezwungen auch unendliche Reihen der Form

$$\sum_{i=-k}^{\infty} a_i p^i \quad (\text{wobei } a_i \in \{0, 1, \ldots, p-1\})$$

zuzulassen, wobei $k \in \mathbb{N}_0$. Dabei steht die obige Summe stellvertretend für den Grenzwert der Folge der Partialsummen

$$(s_n)_{n\in\mathbb{N}} = \left(\sum_{i=-k}^{n-1} a_i p^i \right)_{n\in\mathbb{N}} \quad (\text{wobei } a_i \in \{0, 1, \ldots, p-1\})$$

Mit diesen zwei Vorüberlegungen erhalten wir:

DEFINITION 3.1.4: *(p-adische Zahl)*
Sei $p \in \mathbb{P}$. Dann:

(i) $\sum_{i=0}^{\infty} a_i p^i$ (wobei $a_i \in \{0,1,\dots,p-1\}$) heißt *ganze p-adische Zahl*

(ii) $\sum_{i=-k}^{\infty} a_i p^i$ (wobei $a_i \in \{0,1,\dots,p-1\}$) heißt *p-adische Zahl*

(iii) $\mathbb{Z}_p := \{\sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0,1,\dots,p-1\}\}$ heißt *Menge der ganzen p-adischen Zahlen*

(iv) $\mathbb{Q}_p := \{\sum_{i=-k}^{\infty} a_i p^i \mid a_i \in \{0,1,\dots,p-1\}\}$ heißt *Menge der p-adischen Zahlen*

Die ganzen p-adischen Zahlen $\mathbb{Z}_p$ können wir daher gewissermaßen als Potenzreihen aufgefassen, wobei wir eine Folge $(a_n)_{n\in\mathbb{N}_0} \subset \{0,1,\dots,p-1\}$ vorliegen haben und die Funktion

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

im Punkt $x = p$ betrachten. Der Entwicklungspunkt ist hierbei $x_0 = 0$ gewählt.
Für die p-adischen Zahlen $\mathbb{Q}_p$ haben wir eine Zahlenfolge $(a_n)_{n\geqslant -k} \subset \{0,1,\dots,p-1\}$ vorliegen. Setzten wir nun die Folge $(a_n)_{n\geqslant -k}$ zu einer Folge $(a_n)_{n\in\mathbb{Z}}$ fort, indem wir $a_n := 0 \;\forall\, n < -k$, so können wir die p-adischen Zahlen gleichsam als Laurentreihen

$$f(x) = \sum_{i=-\infty}^{\infty} a_i x^i$$

im Punkt $x = p$ auffassen. Auch hier wurde der Entwicklungspunkt $x_0 = 0$ gewählt.
Es gilt:

SATZ 3.1.5:

(i) $\mathbb{Z}_p$ in ein Ring mit 1

(ii) $\mathbb{Q}_p$ in ein Körper

BEWEIS:

⟶ zum Beweis ■
Wir beenden diesen ersten kurzen Abschnitt mit einem interessanten

SATZ 3.1.6:
Sei $a = \sum_{i=-k}^{\infty} a_i p^i \in \mathbb{Q}_p$, wobei $a_i \in \{0,1,\dots,p-1\} \;\forall\, i \geqslant -k$. Dann gilt:

$$a \in \mathbb{Q} \iff (a_i)_{i\geqslant -k} \text{ ist periodisch (Vorperiode ist zugelassen)}$$

BEWEIS:

⟶ zum Beweis ■

Analytische Konstruktion über Bewertungen (Vervollständigung):

In diesem Abschnitt versuchen wir den Körper der p-adischen Zahlen $\mathbb{Q}_p$ aus dem Körper der rationalen Zahlen zu konstruieren. Die Vorgehensweise ähnelt dabei der Konstruktion der reellen Zahlen $\mathbb{R}$ aus den rationalen Zahlen $\mathbb{Q}$, die uns bereits aus der Analysis bekannt ist. Diesen Prozess, den wir also bereits früher schon kennengelernt haben, nennt man *Vervollständigung* eines Körpers. Um ihn zu beschreiben, benötigen wir einen angeordneten Körper zusammen mit einer Bewertung. Für diese Zwecke befinden sich im Anhang A einige Definitionen (zur Wiederholung), die wir uns ratsamerweise ins Gedächtnis rufen sollten.
Gemäß unserer Konstruktionsvorhaben von $\mathbb{Q}_p$, dem Körper der p-adischen Zahlen, betrachten wir im Folgenden den Körper der rationalen Zahlen $\mathbb{Q}$. Von diesem wissen wir bereits aus der Analysis, dass er gemeinsam mit der Ordnung $\leqslant$ einen angeordneten Körper $(\mathbb{Q}, \leqslant)$ bildet, den wir abkürzend mit $\mathbb{Q}$ bezeichnen. Um nun eine Bewertung von $\mathbb{Q}$ herzuleiten, benötigen wir zunächst den *p-adischen Betrag*.
Dazu sei $p \in \mathbb{P}$ eine beliebige aber feste Primzahl. Wir betrachten nun:

$$x = \frac{a}{b} \in \mathbb{Q} \quad \text{, wobei } a, b \in \mathbb{Z} \text{ und } b \neq 0$$

Dann lässt sich x auch schreiben als:

$$x = p^m \cdot \frac{a'}{b'} \quad \text{, wobei } m, a', b' \in \mathbb{Z} \text{ und } p \nmid a' \cdot b'$$

Man überlege sich an dieser Stelle leicht, dass der Exponent $m \in \mathbb{Z}$ eindeutig bestimmt ist. Wir definieren somit:

DEFINITION 3.1.7: *(p-adischer Absolutbetrag (1. Version))*
Sei $p \in \mathbb{P}$ eine beliebige aber feste Primzahl. Dann:

$$|\,.\,|_p : \mathbb{Q} \longrightarrow \mathbb{R} \quad \text{mit} \quad |x|_p := \frac{1}{p^m} = p^{-m}$$

heißt *p-adischer Betrag* (oder auch *p-adischer Absolutbetrag*).
Wir setzen:

$$|0|_p := 0$$

BEISPIEL 3.1.8:

$$x = \frac{63}{550} = \frac{3^2 \cdot 7^1}{2^1 \cdot 5^2 \cdot 11^1} = 2^{-1} \cdot 3^2 \cdot 5^{-2} \cdot 7^1 \cdot 11^{-1}$$

Dann ist:

$$|x|_2 = \frac{1}{2^{-1}} = 2$$
$$|x|_3 = \frac{1}{3^2} = \frac{1}{9}$$
$$|x|_5 = \frac{1}{5^{-2}} = 5^2 = 25$$
$$|x|_7 = \frac{1}{7^1} = \frac{1}{7}$$
$$|x|_{11} = \frac{1}{11^{-1}} = 11$$
$$|x|_p = \frac{1}{p^0} = 1 \qquad \forall\, p \in \mathbb{P}\backslash\{2, 3, 5, 7, 11\}$$

Es wäre an dieser Stelle anzumerken, dass der soeben definierte p-adische Betrag nicht wie gewohnt die Größe einer Zahl misst. Vielmehr werden große Potenzen von p betragsmäßig klein.
Wir entwickeln nun mit Hilfe unserer Vorüberlegungen zunächst eine Bewertung für die ganzen Zahlen $\mathbb{Z}$ und versuchen anschließend diese Bewertung auf $\mathbb{Q}$ fortzusetzen. Seien dazu $p \in \mathbb{P}$ weiterhin eine beliebige aber feste Primzahl und $n \in \mathbb{Z}\backslash\{0\}$. Dann lässt sich n nach dem *Hauptsatz der elementaren Zahlentheorie* eindeutig (bis auf die Reihenfolge der Faktoren) in Primfaktoren $p, p_1, \ldots, p_k$ mit Vielfachheiten $m, a_1, \ldots, a_k$ zerlegen, d.h.

$$n = \pm p^m \cdot p_1^{a_1} \cdot \cdots \cdot p_k^{a_k}$$

Dieser Exponent m wie ebenso die $a_1, \ldots, a_k$ sind also wiederum allesamt eindeutig bestimmt. Wir definieren daher:

$$v_p : \mathbb{Z} \longrightarrow \mathbb{Z} \cup \{\infty\} \quad \text{mit} \quad v_p(n) := m$$

und setzen:

$$v_p(0) := \infty$$
$$v_p(n) := 0 \quad \text{, falls } p \not| n$$

Um diese Bewertung nun auf $\mathbb{Q}$ fortzusetzen, definieren wir für ein $x = \frac{a}{b} \in \mathbb{Q}$ mit $a, b \in \mathbb{Z}\backslash\{0\}$:

$$v_p(x) = v_p(\frac{a}{b}) := v_p(a) - v_p(b)$$

Bei dieser Notation verwenden wir:

$$\infty + \infty := \infty$$
$$\infty - x := \infty \quad \forall\, x \in \mathbb{Z}$$
$$x < \infty \quad \forall\, x \in \mathbb{Z}$$

Zusammengefasst erhalten wir folgende Definition:

DEFINITION 3.1.9: *(p-adische Bewertung)*

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\} \quad \text{mit} \quad x \mapsto v_p(x)$$

heißt *p-adische Bewertung* (oder *p-Bewertung*, oder auch *p-Exponent*)

BEISPIEL 3.1.10:

$$x \;=\; \frac{63}{550} \;=\; \frac{3^2 \cdot 7^1}{2^1 \cdot 5^2 \cdot 11^1}$$

Dann ist:

$$\begin{aligned}
v_2(x) &= v_2(63) - v_2(550) = 0 - 1 = -1 \\
v_3(x) &= v_3(63) - v_3(550) = 2 - 0 = 2 \\
v_5(x) &= v_5(63) - v_5(550) = 0 - 2 = -2 \\
v_7(x) &= v_7(63) - v_7(550) = 1 - 0 = 1 \\
v_{11}(x) &= v_{11}(63) - v_{11}(550) = 0 - 1 = -1 \\
v_p(x) &= v_p(63) - v_p(550) = 0 - 0 = 0 \qquad \forall\, p \in \mathbb{P}\backslash\{2,3,5,7,11\}
\end{aligned}$$

Die Funktion v_p ist surjektv und erfüllt die folgenden Eigenschaften:

SATZ 3.1.11: *(Bewertungseigenschaften)*

(i) $v_p(x) = \infty \iff x = 0$

(ii) $v_p(x \cdot y) = v_p(x) + v_p(y) \quad \forall\, x, y \in \mathbb{Q}$

(iii) $v_p(x + y) \geqslant \min\{v_p(x), v_p(y)\} \quad \forall\, x, y \in \mathbb{Q}$

BEWEIS:
⟶ zum Beweis ■

Mit den drei Eigenschaften aus dem vorangegangenen Satz 3.1.11 ist die p-adische Bewertung eine *diskrete Bewertung* und $\mathbb{Q}$ zusammen mit ihr ein *diskret bewerteter Körper*. Darüberhinaus gilt folgender interessanter Satz:

SATZ 3.1.12:
Die einzigen nicht-trivialen Bewertungen auf $\mathbb{Q}$ sind die p-adischen Bewertungen.

BEWEIS:
⟶ zum Beweis ■

Anhand der neu erlangten Bewertung definieren wir den p-adischen Absolutbetrag ein zweites Mal in eine etwas abgeänderte Form, jedoch mit der selben Wertzuweisung wie zuvor, durch:

DEFINITION 3.1.13: *(p-adischer Absolutbetrag (2. Version))*

$$|\,.\,|_p : \mathbb{Q} \longrightarrow \mathbb{R} \quad \text{mit} \quad |x|_p := \frac{1}{p^{v_p(x)}} = p^{-v_p(x)}$$

heißt *p-adischer Betrag* (oder auch *p-adischer Absolutbetrag*).

Für den p-adischen Betrag gelten folgende Betragseigenschaften bzw. Normeigenschaften, denn jeder Absolutbetrag ist eine spezielle Norm. (Den Begriff der Norm kann man als eine Verallgemeinerung des Absolutbetrages verstehen.)

SATZ 3.1.14: *(Normeigenschaften, Betragseigenschaften)*

(i) $|x|_p = 0 \iff x = 0$

(ii) $|x|_p \cdot |y|_p = |x \cdot y|_p \qquad \forall\, x, y \in \mathbb{Q}$

(iii) $|x + y|_p \leqslant |x|_p + |y|_p \qquad \forall\, x, y \in \mathbb{Q} \quad$ (*Dreiecksungleichung*)

(iv) $|x + y|_p \leqslant \max\{|x|_p, |y|_p\} \qquad \forall\, x, y \in \mathbb{Q} \quad$ (*ultrametrische Dreiecksungleichung*)

BEWEIS:
⟶ zum Beweis ■

Mit der Eigenschaft (iv), der *ultrametrischen Dreiecksungleichung* aus dem obigen Satz 3.1.11, wird der p-adische Absolutbetrag zu einem *ultramerischen* (oder auch *nichtarchimedischen*) *Betrag* (falls (iv) nicht gilt, so nennt man einen Betrag *archimedisch*), was eine bedeutsame Eigenschaft ist. Denn die *ultrametrische Dreiecksungleichung* hat ungewohnte Konsequenzen für die Topologie auf $\mathbb{Q}_p$. Dies soll der nun eingeschobene Satz verdeutlichen. Man stelle sich dazu eine p-adische Zahl wie im vorherigen Abschnitt als formale Potenzreihe vor.

SATZ 3.1.15:

$$\sum_{n=-k}^{\infty} z_n \text{ ist p-adisch konvergent} \quad \Longleftrightarrow \quad (z_n)_{n\in I} \text{ ist eine p-adische Nullfolge}$$

BEWEIS:

$\longrightarrow$ zum Beweis ■

Damit konvergieren die formalen Potenzreihen bereits dann, wenn wir eine Nullfolge vorliegen haben. Wir erinnern daran, dass wir in der Analysis für $\mathbb{R}$ gezeigt haben, dass die Nullfolge ein notwendiges dennoch kein hinreichendes Kriterium für die Konvergenz einer Reihe war.
Der obige p-adische Betrag $|\,.\,|_p : \mathbb{Q} \longrightarrow \mathbb{R}$ bildet zusammen mit den vier Eigenschaften eine ultrametrische Norm auf $\mathbb{Q}$, d.h. $(\mathbb{Q}, |\,.\,|_p)$ ist ein *metrischer Raum*. Wir weisen an dieser Stelle darauf hin, dass sich die *Dreiecksungleichung* (iii) unmittelbar aus der ultrametrischen Dreicksungleichung (iv) folgern lässt. Aus diesem Grunde bezeichnet man in einem solchen Fall die Eigenschaft (iv) auch als *verschärfte Dreiecksungleichung*.
Ultrametrische Räume haben ebenso unerwartete Eigenschaften:

BEMERKUNG 3.1.16:

(i) Jedes Dreieck ist gleichschenklig (d.h. 2 Seiten haben dieselbe Länge)

(ii) Jeder Punkt einer Kreisscheibe ist Mittelpunkt dieser Kreisscheibe.

Wir kommen nun zu einem interessanten Satz. Hierbei bezeichne $|\,.\,|_\infty$ den uns bereits schon bekannten euklidischen Betrag $|\,.\,|$.

SATZ 3.1.17: *(Geschlossenheitsrelation, Produktformel)*

$$\forall\, x \in \mathbb{Q}\backslash\{0\} : \quad \prod_{p\in\mathbb{P}}^{\infty} |x|_p = 1$$

BEWEIS:

$\longrightarrow$ zum Beweis ■

Falls wir also alle p-adischen Beträge bis auf einen einzigen kennen, so verrät uns die Gleichung aus Satz 3.1.16, wie der unbekannte p-adische Betrag auszusehen hat. Genauer gibt uns die Gleichung sogar die Funktionswerte des fehlenden p-adischen Betrags an, und zwar für alle $\mathbb{Q}_p$.
Als nächstes definieren wir uns unter Verwendung des p-adische Betrags eine Metrik auf $\mathbb{Q}$:

DEFINITION 3.1.18: *(p-adische Metrik)*

$$d_p : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{R} \quad \text{mit} \quad d_p(x,y) := |x-y|_p$$

heißt *p-adische Metrik*.

Damit wird $(\mathbb{Q}, d_p)$ zu einem *metrischen Raum*, wobei die Metrikeigenschaften unmittelbar aus den Normeigenschaften von $|\,.\,|_p$ folgen. Wir definieren nun den Körper $\mathbb{Q}_p'$ der p-adischen Zahlen aufs Neue, indem wir genauso vorgehen werden, wie bei der Konstruktion des Körpers der reellen Zahlen. Die Vervollständigung des metrischen Raums $(\mathbb{Q}, d_p)$ wird der metrische Raum $\left(\mathbb{Q}_p', d_p'\right)$ der p-adischen Zahlen werden. Wir erinneren an dieser Stelle an die Definitionen einer *p-adischen Cauchy-Folge*, einer *p-adischen konvergenten Folge*, einer *p-adisch beschränkten Folge* und einer *p-adischen Nullfolge*, die im Anhang A beigefügt sind. Ohne Zweifel unterscheiden sich die Definitionen zu den uns geläufigen Definitionen einer Cauchy-Folge (bzw. einer konvergenten Folge) lediglich im gewählten Betrag $|\,.\,|_p$ ($p \in \mathbb{P} \cup \{\infty\}$). So ist beispielsweise die Folge $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ bzgl. $|\,.\,|_\infty$ eine Nullfolge und bzgl. $|\,.\,|_p$ ($p \in \mathbb{P}$) unbeschränkt und somit insbesondere nicht konvergent. Die Abbildung 1 veranschaulicht dies speziell für $p = 3$.

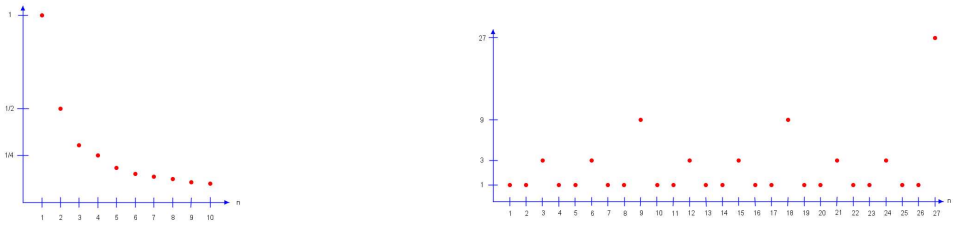


Abbildung 1: Graphische Darstellung der Folge $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ bzgl. $|\,.\,|_\infty$ (links) und $|\,.\,|_3$ (rechts)

Wie wir bereits in der Analysis bewiesen haben, ist jede konvergente Folge $(x_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ eine Cauchy-Folge. Die Umkehrung gilt bzgl. $|\,.\,|_p$ nicht. Daher ist unser Ziel die rationalen Zahlen $\mathbb{Q}$ mit der Betragsfunktion $|\,.\,|_p$ zu einem derartigen Körper zu erweitern, dass die Umkehrung der Aussage gilt.
Wir definieren uns nun eine komponentenweise Addition und Multiplikation für zwei rationale Folgen $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ durch:

$$(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} := (x_n + y_n)_{n\in\mathbb{N}}$$
$$(x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} := (x_n \cdot y_n)_{n\in\mathbb{N}}$$

Mit den obigen Verknüpfungen erhalten wir:

SATZ 3.1.19:

(i) $R := \{(x_n)_{n\in\mathbb{N}} \subset \mathbb{Q} \mid (x_n)_{n\in\mathbb{N}}$ ist p-adische Cauchy-Folge$\}$ ist ein kommutativer Ring mit 1

(ii) $I := \{(x_n)_{n\in\mathbb{N}} \subset \mathbb{Q} \mid (x_n)_{n\in\mathbb{N}}$ ist p-adische Nullfolge$\}$ ist ein maximales Ideal von R

BEWEIS:
$\longrightarrow$ zum Beweis ■

Wir definieren nun die p-adischen Zahlen durch den Faktorring R/I, d.h.

$$\mathbb{Q}_p' := R/I = \{r + I \mid r \in R\}$$

Da R sogar ein kommutativer Ring mit Einselement $(1, 1, 1, \ldots)$ und I ein maximales Ideal ist, wissen wir aus der Algebra 1, dass der Faktoring R/I, demnach auch $\mathbb{Q}_p'$, ein Körper ist. Man bezeichnet $\mathbb{Q}_p'$, also den

Körper der p-adischen Zahlen, aufgrund der Definition über den Faktorring auch als den *Restklassenkörper von R*.
Der Strich ' von $\mathbb{Q}_p'$ dient an dieser Stelle lediglich dazu, die zwei verschiedenen Definitionen der p-adischen Zahlen nicht zu verwechseln, da an dieser Stelle noch kein Zusammenhang zwischen $\mathbb{Q}_p$ und $\mathbb{Q}_p'$ erkennbar ist. Darauf gehen wir jedoch später noch ein.
Im folgenden Schritt betten wir $\mathbb{Q}$ in $\mathbb{Q}_p'$ ein, indem wir jeder rationalen Zahl $x \in \mathbb{Q}$ die entsprechende konstante Folge $(x, x, x, \ldots) \subset \mathbb{Q}_p'$ zuordnen. Mit anderen Worten verwenden wir zur Inklusion den folgenden injektiven Homomorphismus:

$$i : \mathbb{Q} \hookrightarrow \mathbb{Q}_p' \quad \text{mit} \quad x \longmapsto (x, x, x, \ldots)$$

Damit haben wir gezeigt, dass $\mathbb{Q}$ ein Teilkörper von $\mathbb{Q}_p'$ ist. Da $\mathbb{Q}$ zudem nach Algebra 1 die Charakteristik 0 besitzt, muss auch $\mathbb{Q}_p'$ als Oberkörper von $\mathbb{Q}$ die *Charakteristik* 0 haben, d.h. $char\left(\mathbb{Q}_p'\right) = 0$. Damit gilt in $\mathbb{Q}_p'$:

$$\forall\, n \in \mathbb{N} : \quad n \cdot (1) \;=\; \underbrace{(1,1,1,\ldots) + \cdots + (1,1,1,\ldots)}_{\text{n Faktoren}} \;\neq\; (0,0,0,\ldots) \;=\; (0)$$

Man beachte an dieser Stelle, dass zwischen den verschiedenen Körpern $\mathbb{Q}_p'$ kein derartiger kanonischer Homomorphismus existiert. Ferner sind die verschiedenen $\mathbb{Q}_p'$ nicht isomorph zueinander.
Wir müssen nun den p-adischen Absolutbetrag $|\,.\,|_p$ sowie die p-adische Bewertung v_p auf $\mathbb{Q}_p'$ fortsetzen und anschließend noch zeigen, dass jede Cauchy-Folge in $\mathbb{Q}_p'$ bezüglich dieser Fortsetzung konvergiert.
Im folgenden Verlauf weist der Strich $'$ stets auf eine Fortsetzung auf $\mathbb{Q}_p'$ hin. Wir behalten dabei die Bezeichungen bei und definieren:

DEFINITION 3.1.20: *(p-adischer Absolutbetrag auf $\mathbb{Q}_p'$)*

$$|\,.\,|_p' : \mathbb{Q}_p' \longrightarrow \mathbb{R} \quad \text{mit} \quad |x|_p' := \lim_{n\to\infty} |x_n|_p \in \mathbb{R}$$

Bemerke:

(i) Die Dastellung eines Elements $x \in \mathbb{Q}_p'$ ist zur Erinnerung:

$$x = \{x_n\} \mod I \quad \in \mathbb{Q}_p \;=\; R \backslash I$$

(ii) Der Limes existert, da $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge in $\mathbb{R}$ ist.

DEFINITION 3.1.21: *(p-adische Bewertung auf $\mathbb{Q}_p'$)*

$$v_p' : \mathbb{Q}_p' \longrightarrow \mathbb{Z} \cup \{\infty\} \quad \text{mit} \quad v_p'(x) := -\log_p |x|_p'$$

Bemerke:

$$v_p'(x) := -\log_p |x|_p' = -\log_p \lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} \left(-\log_p |x_n|_p\right) = \lim_{n\to\infty} v_p(x_n)$$

BEMERKUNG 3.1.22:
Sei $p \in \mathbb{P}$ beliebig aber fest. Dann gilt wieder:

$$|x|_p' = p^{-v_p'(x)} \quad \forall\, x \in \mathbb{Q}_p'$$

BEWEIS:

$\longrightarrow$ zum Beweis ■

Wir weisen an dieser Stelle darauf hin, dass die Fortsetzung der Bewertung sowie des Absolutbetrages die dazugehörigen Rechenregeln erfüllen (siehe: Satz 3.1.11 (Bewertungseigenschaften) und Satz 3.1.14 (Betragseigenschaften)). Ebenso setzen wir die p-adische Metrik auf $\mathbb{Q}_p'$ fort, durch

$$d_p' : \mathbb{Q}_p' \times \mathbb{Q}_p' \longrightarrow \mathbb{R} \quad \text{mit} \quad d_p'(x,y) := |x-y|_p'$$

Der Körper $\mathbb{Q}_p'$ ist zusammen mit der durch den fortgesetzten p-adischen Absolutbetrag induzierten p-adischen Metrik d_p' wieder ein *metrischer Raum*. Kommen wir nun zum

SATZ 3.1.23:

(i) : $\mathbb{Z}_p'$ ist (als metrischer Raum) vollständig
(ii) : $\mathbb{Q}_p'$ ist (als metrischer Raum) vollständig

d.h.: Jede Cauchy-Folge in $\mathbb{Q}_p'$ (bzw. in $\mathbb{Z}_p'$) konvergiert.

BEWEIS:
$\longrightarrow$ zum Beweis ■

Wir erhalten durch Vervollständigung des metrischen Raums $(\mathbb{Q}, d_p)$ den vollständigen metrischen Raum $(\mathbb{Q}_p', d_p')$. Desweiteren haben wir bereits früher gezeigt, dass $\mathbb{Q}_p'$ ein Körper, genauer eine Körpererweiterung von $\mathbb{Q}$ ist. Durch die Vervollständigung ist er somit ein vollständiger Oberkörper von $\mathbb{Q}$.
Die unendlich vielen Körper

$$\mathbb{Q}_2', \mathbb{Q}_3', \mathbb{Q}_5', \mathbb{Q}_7', \mathbb{Q}_{11}', \mathbb{Q}_{13}', \mathbb{Q}_{17}', \ldots \quad \text{und} \quad \mathbb{Q}_\infty' = \mathbb{R}$$

die alle nach dem gleichen Konstruktionsprinzip gewonnen worden sind, heißen auch *lokale Körper*. $\mathbb{Q}$ wird in diesem Zusammenhang auch als *globaler Körper* bezeichnet.
Da wir $\mathbb{Q}_p'$ gerade so konstruiert haben, dass jede Cauchy-Folge aus $\mathbb{Q}$ bezüglich der p-adischen Norm $|\,.\,|_p$ in $\mathbb{Q}_p'$ konvergiert, gilt:

$$\mathbb{Q}_p' = \overline{\mathbb{Q}} \quad \text{bezüglich } |\,.\,|_p$$

D.h. $\mathbb{Q}_p'$ ist der Abschluß von $\mathbb{Q}$ bezüglich der obigen Norm und damit liegt $\mathbb{Q}$ *dicht* in $\mathbb{Q}_p'$ $(\forall\, p \in \mathbb{P} \cup \{\infty\})$.
Man nennt $\mathbb{Q}_p'$ daher auch die *p-adische Komplettierung von* $\mathbb{Q}$.
Kommen wir noch einmal kurz auf die ganzen p-adischen Zahlen $\mathbb{Z}_p'$ zurück. Sie werden in diesem Zusammenhang folgendermaßen definiert:

DEFINITION 3.1.24:

$$\mathbb{Z}_p' := \{x \in \mathbb{Q}_p' \mid v_p'(x) \geqslant 0\} = \{x \in \mathbb{Q}_p' \mid |x|_p' \leqslant 1\}$$

Auf $\mathbb{Z}_p'$ ist eine Reihe von Sätzen der Ringtheorie aus der Algebra anwendbar, was der folgende Satz erlaubt. Im Beweis werden wir sehen, dass die ultrametrische Eigenschaft von enormer Bedeutung für den Satz ist.

SATZ 3.1.25:

(i) $\mathbb{Z}'_p \subset \mathbb{Q}'_p$ ist ein Unterring von $\mathbb{Q}'_p$

(ii) $Z'^*_p := \{x \in \mathbb{Q}'_p \mid v'_p(x) = 0\} = \{x \in \mathbb{Q}'_p \mid |x|'_p = 1\}$ enthält alle Einheiten von $\mathbb{Z}'_p$

(iii) Z'_p ist nullteilerfrei (also ein Integritätsring)

(iv) Z'_p ist ein lokaler Ring

(v) Z'_p ist ein Hauptidealring

BEWEIS:
$\longrightarrow$ zum Beweis ■

Dieser Unterring $\mathbb{Z}'_p$ von $\mathbb{Q}'_p$ hat einen speziellen Namen, man nennt ihn *Bewertungsring* von v'_p. Da es sich bei v'_p um eine diskrete Bewertung handelt, heißt $\mathbb{Z}'_p$ auch *diskreter Bewertungsring* von v'_p. Desweiteren heißt $\mathbb{Z}'^*_p$ *Menge der p-adischen Einheiten*.
Ebenso, wie wir in der Analysis für die reellen Zahlen $\mathbb{R}$ die Überabzählbarkeit mit Hilfe des Cantorschen Diagonalverfahren gezeigt haben, gilt auch hier

SATZ 3.1.26:

$\mathbb{Q}'_p$ ist überabzählbar

BEWEIS:

$\longrightarrow$ zum Beweis ■

Zusammenhang der Konstuktionsmethoden:

Nachdem wir nun zwei Darstellungsmethoden der p-adischen Zahlen kennengelernt haben, stellen wir uns mit Recht die Frage

In wiefern hängen die konstruierten Körper $\mathbb{Q}_p$ und $\mathbb{Q}'_p$ (bzw. die Ringe $\mathbb{Z}_p$ und $\mathbb{Z}'_p$) zusammen?

Und falls ein Zusammenhang zwischen ihnen bestehen sollte

Welche Eigenschaften übertragen sich von dem einen auf den anderen Körper (bzw. Ring)?

Die Antworten dieser interessanten Fragen wollen wir im Folgenden klären. In der Tat ist es aufgrund der Herleitungen keineswegs offensichtlich, dass es sich bei $\mathbb{Q}_p$ und $\mathbb{Q}'_p$ sowie bei $\mathbb{Z}_p$ und $\mathbb{Z}'_p$ um dieselben Körper (bzw. Ringe) handelt. Der erste Schritt zur Aufklärung der ersten Frage ist der

SATZ 3.1.27:
Seien $a_i \in \{0, 1, \ldots, p-1\}$, $p \in \mathbb{P}$ eine beliebige aber feste Primzahl und $k \in \mathbb{Z}$. Dann:

(i) $f : \mathbb{Z}_p \longrightarrow \mathbb{Z}'_p$ mit $\left(\sum_{i=0}^{\infty} a_i p^i\right) \mapsto \left(\sum_{i=0}^{n} a_i p^i\right)_{n \in \mathbb{N}_0}$ ist Ringisomorphismus

(ii) $g : \mathbb{Q}_p \longrightarrow \mathbb{Q}'_p$ mit $\left(\sum_{i=-k}^{\infty} a_i p^i\right) \mapsto \left(\sum_{i=-k}^{n} a_i p^i\right)_{n \geqslant -k}$ ist Körperisomorphismus

BEWEIS:

⟶ zum Beweis ■
Man bemerke an dieser Stelle

BEMERKUNG 3.1.28:

$$\text{(i)}\ \forall\, x \in \mathbb{Z}_p' \ \exists_1\ (x_n)_{n\in\mathbb{N}_0} \subset \{0,1,\ldots,p-1\}: \quad x \ = \ \sum_{i=0}^{\infty} x_i p^i$$

$$\text{(ii)}\ \forall\, x \in \mathbb{Q}_p' \ \exists_1\ (x_n)_{n\in\mathbb{Z}} \subset \{0,1,\ldots,p-1\}: \quad x \ = \ \sum_{i=-k}^{\infty} x_i p^i$$

BEWEIS:

⟶ zum Beweis ■

Dem Satz 3.1.27 nach zufolge stimmen die Körper (bzw. Ringe) tatsächlich (bis auf Isomorphie) überein. Desweiteren gilt nun zusätzlich eine wichtige Eigenschaft (ohne Beweis), die es uns erlaubt, die Körper- und Ringeigenschaften auf den jeweiligen anderen Körper (bzw. Ring) zu übertragen. Es gelten nämlich:

$$\text{(i)}\ \ |a|_p \ = \ |f(a)|_p' \qquad \forall\, a \in \mathbb{Z}_p$$

$$\text{(ii)}\ \ |a|_p \ = \ |g(a)|_p' \qquad \forall\, a \in \mathbb{Q}_p$$

Damit erhalten wir abschließend zur Konstruktion der p-adischen Zahlen

COROLLAR 3.1.29:

(1) $\mathbb{Q}_p$ ist überabzählbar

(2) $\mathbb{Q} \subset \mathbb{Q}_p \quad \forall\, p \in \mathbb{P}$

(3) $\mathbb{Z}_p$ ist (als metrischer Raum) vollständig

(4) $\mathbb{Q}_p$ ist (als metrischer Raum) vollständig

(5) $\mathbb{Z}_p$ ist ein lokaler Ring, sogar ein diskreter Bewertungsring

(6) $\mathbb{Z}_p$ ist ein Hauptidealring

(7) $\mathbb{Z}_p$ ist nullteilerfrei, also ein Integritätsring

(8) $\mathbb{Q}_p$ hat Charakteristik 0, also $char\,(\mathbb{Q}_p) = 0$

BEWEIS:
⟶ zum Beweis ■

3.2 Lokal-Global-Prinzip

Kommen wir nun zu einer ersten Anwendung der p-adischen Zahlen im Bereich der Arithmetik. Wir betrachten dazu im Folgenden *Diophantische Gleichungen*. Eine *Diophantische Gleichung* ist eine Gleichung der Form

$$F(x_1,\ldots,x_n) = 0$$

wobei F ein Polynom in mehreren Veränderlichen $x_1,\ldots,x_n$ mit ganzzahligen Koeffizienen darstellt. Man stellt sich hierbei stets die Frage nach der Lösbarkeit von $F(x_1,\ldots,x_n) = 0$ in ganzen Zahlen. Dieses schwierige Problem können wir dadurch abschwächen, dass wir anstelle der Gleichung die sämtlichen Kongruenzen

$$F(x_1,\ldots,x_n) \equiv 0 \mod m \qquad \forall\, m \in \mathbb{N}$$

betrachten. Dabei hoffen wir, auf diesem Wege später Rückschlüsse auf die Lösbarkeit über $\mathbb{Z}$ zu erlangen. Diese Kongruenzgleichung ist nach dem chinesischen Restsatz (Algebra 1) gleichbedeutend zu der folgenden Formulierung:

$$F(x_1,\ldots,x_n) \equiv 0 \mod p^v \qquad \forall\, p \in \mathbb{P} \;\wedge\; \forall\, v \geqslant 1$$

Die Vielzahl dieser Kongruenzen wird nun durch die ganzen p-adischen Zahlen wieder zu einer Gleichung zusammengefasst. Denn es gilt:

Satz 3.2.1:
Seien $p \in \mathbb{P}$ beliebig aber fest und $F(x_1,\ldots,x_n)$ ein Polynom mit ganzzahligen Koeffizienten. Dann gilt:

$$F(x_1,\ldots,x_n) \equiv 0 \mod p^v \text{ lösbar } \forall\, v \geqslant 1 \quad\Longleftrightarrow\quad F(x_1,\ldots,x_n) = 0 \text{ lösbar in } \mathbb{Z}_p$$

Beweis:

$\longrightarrow$ zum Beweis ■

Beispiel 3.2.2:
p=7. Wir betrachten die Funktion

$$F(x) = x^2 - 2$$

und suchen ein $x \in \mathbb{Z}_7$, derart dass

$$F(x) = x^2 - 2 \overset{!}{=} 0$$

erfüllt ist. Dazu untersuchen wir die Lösbarkeit von

$$x^2 - 2 \equiv 0 \mod 7^v \quad \forall\, v \geqslant 1 \quad\Longleftrightarrow\quad x^2 \equiv 2 \mod 7^v \quad \forall\, v \geqslant 1$$

$\underline{v = 1:}$

$$x^2 \equiv 2 \mod 7 \quad\Longleftrightarrow\quad 7 \mid (x^2 - 2) \quad\Longrightarrow\quad \text{Lösung } \boxed{x_0 = \pm 3}$$

$\underline{v = 2:}$

$$\begin{aligned} x^2 \equiv 2 \mod 7^2 \quad &\Longrightarrow\quad x^2 \equiv 2 \mod 7 \\ &\Longrightarrow\quad \text{Lösung besitzt die Form } \pm 3 + t_1 \cdot 7, \text{ wobei } t_1 \in \{0,1,\ldots,6\} \end{aligned}$$

Wir definieren nun

$$x_1 := 3 + t_1 \cdot 7$$

und setzen x_1 in die Kongruenzgleichung ein, also:

$$\begin{aligned}
x_1^2 &\equiv 2 \mod 7^2 \\
(3+t_1\cdot 7)^2 &\equiv 2 \mod 7^2 \\
9+6\cdot 7\cdot t_1+7^2\cdot t_1^2 &\equiv 2 \mod 7^2 \\
7+6\cdot 7\cdot t_1+7^2\cdot t_1^2 &\equiv 0 \mod 7^2 \\
7+6\cdot 7\cdot t_1 &\equiv 0 \mod 7^2 \\
7\,(1+6\cdot t_1) &\equiv 0 \mod 7^2 \\
1+6\cdot t_1 &\equiv 0 \mod 7 \\
6\cdot t_1 &\equiv -1 \mod 7 \overset{!}{=} 6 \mod 7 \\
t_1 &\equiv 1 \mod 7
\end{aligned}$$

Wir erhalten somit $t_1 = 1$ als Lösung und insgesamt damit

$$\boxed{x_1 = 3+1\cdot 7}$$

<u>$v = 3$:</u>

$$\begin{aligned}
x^2 \equiv 2 \mod 7^3 \quad &\Longrightarrow \quad x^2 \equiv 2 \mod 7^2 \\
&\Longrightarrow \quad \text{Lösung besitzt die Form } \pm 3+1\cdot 7+t_2\cdot 7^2, \text{ wobei } t_2\in\{0,1,\ldots,6\}
\end{aligned}$$

Wir definieren nun

$$x_2 := 3+1\cdot 7+t_2\cdot 7^2$$

und setzen x_2 in die Kongruenzgleichung ein, also:

$$\begin{aligned}
x_2^2 &\equiv 2 \mod 7^3 \\
\left(3+1\cdot 7+t_2\cdot 7^2\right)^2 &\equiv 2 \mod 7^3 \\
100+2\cdot 10\cdot 7^2\cdot t_2+t_2^2\cdot 7^4 &\equiv 2 \mod 7^3 \\
98+2\cdot 10\cdot 7^2\cdot t_2+t_2^2\cdot 7^4 &\equiv 0 \mod 7^3 \\
2\cdot 7^2+2\cdot 10\cdot 7^2\cdot t_2 &\equiv 0 \mod 7^3 \\
7^2\,(2+2\cdot 10\cdot t_2) &\equiv 0 \mod 7^3 \\
2+2\cdot 10\cdot t_2 &\equiv 0 \mod 7 \\
2\cdot 10\cdot t_2 &\equiv -2 \mod 7 \\
10\cdot t_2 &\equiv -1 \mod 7 \overset{!}{=} 6 \mod 7 \\
3\cdot t_2 &\equiv 6 \mod 7 \\
t_2 &\equiv 2 \mod 7
\end{aligned}$$

Wir erhalten somit $t_2 = 2$ als Lösung und insgesamt damit

$$\boxed{x_2 = 3+1\cdot 7+2\cdot 7^2}$$

<u>$v = 4$:</u>
Mit dem Ansatz

$$x_3 := 3+1\cdot 7+2\cdot 7^2+t_3\cdot 7^3 \quad , t_3\in\{0,1,\ldots,6\}$$

erhält man als Lösung $t_3 = 6$ und insgesamt damit

$$\boxed{x_3 = 3+1\cdot 7+2\cdot 7^2+6\cdot 7^3}$$

$\underline{v = 5:}$
Mit dem Ansatz

$$x_4 := 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + t_4 \cdot 7^4 \quad , t_4 \in \{0, 1, \ldots, 6\}$$

erhält man als Lösung $t_4 = 1$ und insgesamt damit

$$\boxed{x_3 = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4}$$

$\underline{v = n:}$
Man sieht leicht, dass sich dieser Prozess bis ins Unendliche fortsetzen lässt, so dass wir bei genauerem Hinsehen eine Rekursionsformel erhalten. Dabei setzen wir stets

$$x_{n-1} = x_{n-2} + t_{n-1} \cdot 7^{n-1}$$

und lösen die Kongruenzgleichung

$$x_{n-1}^2 \equiv 2 \mod 7^n$$

Auf diesem Wege erhalten wir eine 7-adische Lösung

$$\boxed{x = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 + \cdots \in \mathbb{Z}_7}$$

die die Gleichung

$$x^2 - 2 = 0$$

in $\mathbb{Z}_7$ löst. Dabei wird die Lösung mit $\sqrt{2} := x \in \mathbb{Z}_7$ bezeichnet. Man beachte jedoch, dass sie nichts im Geringsten mit $\sqrt{2} \in \mathbb{R}$ zu tun und ist daher strikt von ihr zu trennen.

Für den Fall, dass es sich bei dem Polynom $F(x_1, \ldots, x_n)$ um ein homogenes Polynom vom Grad $d \geqslant 1$ handelt, dürfte klar sein, dass die Gleichung $F(x_1, \ldots, x_n) = 0$ immer die triviale Lösung $(0, \ldots, 0)$ besitzt. Hier stellt man sich die Frage nach einer nicht-trivialen Lösung für das Problem.

Corollar 3.2.3:
Seien $p \in \mathbb{P}$ beliebig aber fest und $F(x_1, \ldots, x_n)$ ein Polynom mit ganzzahligen Koeffizienten. Dann gilt:

$$F(x_1, \ldots, x_n) \equiv 0 \mod p^v \text{ nicht-trivial lösbar } \forall\, v \geqslant 1 \iff F(x_1, \ldots, x_n) = 0 \text{ nicht-trivial lösbar in } \mathbb{Z}_p$$

Beweis:

$\longrightarrow$ zum Beweis ■

Die Frage zu Begin des Abschnitts war

$$F(x_1, \ldots, x_n) = 0 \text{ lösbar in } \mathbb{Z}_p \quad \forall\, p \in \mathbb{P} \quad \overset{?}{\Longrightarrow} \quad F(x_1, \ldots, x_n) = 0 \text{ lösbar in } \mathbb{Z}$$

und die dazugehörige Antwort lautet: „Dies trifft nur sehr selten zu“. Diese Schlussfolgerung hängt auch immer sehr stark von der Form des Polynoms ab. Speziell für quadratische Formen hat man jedoch das sogenannte *Lokal-Global-Prizip* (oder *Lokalisation*) von Hasse-Minkowsik, mit dem wir diesen Abschnitt nun beenden wollen.

Satz 3.2.4: *(Lokal-Global-Prinzip, Hasse-Minkowski)*
Sei $F(x_1, \ldots, x_n)$ eine quadratische Form mit rationalen Koeffizienten. Dann gilt:

$$F(x_1, \ldots, x_n) = 0 \text{ nicht-trivial lösbar in } \mathbb{Q} \iff F(x_1, \ldots, x_n) = 0 \begin{cases} \text{nicht-trivial lösbar in } \mathbb{R} \\ \text{ und} \\ \text{nicht-trivial lösbar in } \mathbb{Q}_p \quad \forall\, p \in \mathbb{P} \end{cases}$$

Beweis:

$\longrightarrow$ zum Beweis ■

3.3 Henselsches Lemma

Abschließend mit dem Kapitel der p-adischen Zahlen behandeln wir nun das *Henselsche Lemma*, das, wie wir noch sehen werden, eine enorme Aussagekraft besitzt und unerwartete Konsequezen mit sich bringt. Wir beschäftigen uns nun mit Gleichungen der Form

$$f(X) \;=\; a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \;=\; 0 \qquad \text{, wobei } f(X) \in \mathbb{Z}_p[X]$$

in einer Variablen. Wie wir bereits im zweiten Abschnitt (3.2 Lokal-Global-Prinzip) festgestellt haben, ist diese Gleichung genau dann in $\mathbb{Z}_p$ lösbar, wenn ihre sämtlichen Kongruenzen lösbar sind. Wir erinnern an dieser Stelle daher nochmals an den Satz 3.2.1, dessen Aussage folgende war:

$$F(x_1,\ldots,x_n) \equiv 0 \mod p^v \text{ lösbar } \forall\, v \geqslant 1 \quad \Longleftrightarrow \quad F(x_1,\ldots,x_n) = 0 \text{ lösbar in } \mathbb{Z}_p$$

Wir werden nun eine neue Feststellung machen: Beschränkt man sich ausschließlich auf einfache Nullstellen, so genügt es lediglich die Lösbarkeit der Kongruenz

$$f(x) \equiv 0 \mod p$$

zu prüfen. Dazu das

Lemma 3.3.1: *(Henselsches Lemma)*
Sei $f \in \mathbb{Z}_p[X]$ ein Polynom und $\overline{f} \in \mathbb{F}_p[X]$, wobei $F_p = \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p/p\mathbb{Z}_p$ der Restklassenkörper von $\mathbb{Z}_p$ ist. Falls

$$\exists\, \overline{g}, \overline{h} \in \mathbb{F}_p[X] \text{ mit } \overline{g}, \overline{h} \text{ teilerfremd} : \;\; \overline{f} = \overline{g} \cdot \overline{h}$$

Dann gilt:

$$\exists\, g, h \in \mathbb{Z}_p[X] : \begin{cases} \text{(i)} & f = g \cdot h \\ \text{(ii)} & \overline{g} \text{ ist die Reduktion von } g \\ \text{(iii)} & \overline{h} \text{ ist die Reduktion von } h \end{cases}$$

Beweis:

$\longrightarrow$ zum Beweis ■

Da die Bedeutung dieses Lemmas so gewaltig ist, wiederholen wir kurz nocheinmal dessen Aussage.

> *Sei $f \in \mathbb{Z}_p[X]$ und $\overline{f}$ das Polynom, welches sich ergibt, wenn man die Koeffizienten mod p reduziert. Dann ist jede einfache Nullstelle von $\overline{f}$ in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ $\cong \mathbb{Z}_p/p\mathbb{Z}_p$ eine Nullstelle von f in $\mathbb{Z}_p$.*

Diese Feststellung ist äußerst erstaunlich, da der Restklassenkörper $\mathbb{F}_p$ viel weniger Elemente (genauer nur p-Elemente) besitzt als $\mathbb{Z}_p$ selbst. Man spricht daher auch vom „Hochheben“ bzw. vom „Liften“ einer Nullstelle von $\mathbb{F}_p$ in $\mathbb{Z}_p$.
Wir weisen an dieser Stelle daraufhin, dass es eine Vielzahl von unterschiedlichen Formulierungen des Henselschen Lemmas gibt. Auch das von uns aufgezeigte Lemma 3.3.1 ist ein Spezialfall, denn das Henselschen Lemmas gilt viel allgemeiner, wie es die folgende Bemerkung zeigt:

Bemerkung 3.3.2:
Seien K ein vollständig bewerteter Körper, A der Bewertungsring von K und k der Restklassenkörper von A. Weiter sei $f \in A[X]$ und $\overline{f} \in k[X]$. Falls

$$\exists\, \overline{g}, \overline{h} \in k[X] \text{ mit } \overline{g}, \overline{h} \text{ teilerfremd} : \;\; \overline{f} = \overline{g} \cdot \overline{h}$$

Dann gilt:

$$\exists\, g,h \in A[X]: \begin{cases} \text{(i)} & f = g \cdot h \\ \text{(ii)} & \bar{g} \text{ ist die Reduktion von } g \\ \text{(iii)} & \bar{h} \text{ ist die Reduktion von } h \end{cases}$$

BEWEIS:

$\longrightarrow$ zum Beweis ■

Kommen wir nun zu zwei Beispielen in Bezug auf das Henselsche Lemma:

BEISPIEL 3.3.3: *((p-1)-ten Einheitswurzeln)*

$p \in \mathbb{P}$, $K = \mathbb{Q}_p$, $A = \mathbb{Z}_p$, $k = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Wir betrachten die Funktion

$$\boxed{f(X) = X^{p-1} - 1 \in \mathbb{Z}_p[X]}$$

Es gilt:

$$\overline{f(X)} = X^{p-1} - 1 = \overline{(X-1)} \cdot \overline{(X-2)} \cdot \cdots \cdot \overline{(X-(p-1))} \in \mathbb{F}_p[X]$$

Weiter sind $(X-i), (X-j)$ paarweise teilerfremd (wobei $i,j \in \{0,1,\ldots,p-1\}$ und $i \neq j$). Demnach sind die Voraussetzungen des Hensel'schen Lemmas erfüllt. Das Lemma besagt nun:

$$\exists\, g_1, \ldots, g_{p-1} \in \mathbb{Z}_p[X]: \begin{cases} \text{(i)} & f = g_1 \cdot \cdots \cdot g_{p-1} \\ \text{(ii)} & g_i(X) \equiv (X-i) \mod p \quad \forall\, i = 1, \ldots, p-1 \end{cases}$$

Damit müssen die Polynome g_i die Form

$$g_i(X) = a_i X + b_i$$

besitzen, wobei $a_i \in \overline{1} = \{\ldots, 1+(-2)\cdot p, 1+(-1)\cdot p, 1, 1+1\cdot p, 1+2\cdot p, \ldots\} = 1+p\cdot\mathbb{Z}$. Sei also o.B.d.A. $a_i = 1$. Dann haben die Polynome die Form

$$g_i(X) = X + b_i$$

Also gibt es $\zeta_1, \ldots, \zeta_{p-1} \in \mathbb{Z}_p$, so dass

$$f(X) = X^{p-1} - 1 = (X-\zeta_1) \cdot (X-\zeta_2) \cdot \cdots \cdot (X-\zeta_{p-1}) \in \mathbb{Z}_p[X]$$

$\zeta_k = e^{i\frac{2k\pi}{p-1}}$ $(k = 1, \ldots, p-1)$ sind gerade die $(p-1)$-ten Einheitswurzeln. Man kann somit, wie wir gerade gezeigt haben, das Hensel'sche Lemma dazu verwenden, die Existenz der $(p-1)$-ten Einheitswurzeln in $\mathbb{Z}_p$ zu beweisen.

BEISPIEL 3.3.4:

$p \in \mathbb{P}$, $K = \mathbb{Q}_p$, $A = \mathbb{Z}_p$, $k = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Wir betrachten die Funktion

$$\boxed{f(X) = X^p - 1 \in \mathbb{Z}_p[X]}$$

Es gilt:

$$\overline{f(X)} = X^p - 1 = \underbrace{\overline{(X-1)} \cdot \overline{(X-1)} \cdot \cdots \cdot \overline{(X-1)}}_{p-mal} \in \mathbb{F}_p[X]$$

Da wir bei der Zerlegung jedoch keine teilerfremden Polynome erhalten, ist das Hensel'sche Lemma nicht anwendbar.

Wir haben nun also das überraschende Resultat erhalten, dass die (p-1)-ten Einheitswurzeln in $\mathbb{Z}_p$ und damit auch in $\mathbb{Q}_p$ liegen. Dies sollte uns an die komplexen Zahlen erinnern, denn auch sie enthielten die (p-1)-ten Einheitswurzeln, denen wiederum eine imaginäre Komponente angehörte, wie man es im ersten Beispiel deutlich erkennt. In diesem Zusammenhang stellt man sich die Frage:

Sind die p-adischen Zahlen $\mathbb{Q}_p$ eine Teilmenge der komplexen Zahlen $\mathbb{C}$, also $\mathbb{Q}_p \subset \mathbb{C}$?

Und wenn dies zutrifft, dann frage man sich:

Ist $\mathbb{Q}_p$ oder vielmehr $\mathbb{Z}_p$ überhaupt angeordnet?

Die Anwort auf die erste Frage ist „ja“. In der Tat liegen die p-adischen Zahlen $\mathbb{Q}_p$ in dem komplexen Zahlenkörper $\mathbb{C}$, was jedoch nicht ohne Weiteres trivial ist, denn die Inklusionsabbildung ist keineswegs kanonisch. Auf den Beweis hierfür werden wir jedoch an dieser Stelle verzichten.
Viel interessanter ist die Beantwortung der zweiten Frage. Sie führt uns abschließend zur letzten Folgerung dieses Kapitels, die sich erstaunlicherweise mit dem Henselschen Lemma beweisen lässt.

Corollar 3.3.5:

$\forall\, p \in \mathbb{P}:$ $\mathbb{Q}_p$ und $\mathbb{Z}_p$ sind nicht angeordnet.

Beweis:

$\longrightarrow$ zum Beweis ■

3.4 Beweise

Beweise zu: 3.1 Konstruktion der p-adischen Zahlen:

BEWEIS: *(Satz 3.1.2)*
zurück zum Satz 3.1.2
Existenz:
Die Existenz einer solchen Potenzreihe lässt sich mit Hilfe einer fortgesetzten Division durch p zeigen. Wir betrachten dazu das folgende System von Gleichungen

$$\begin{aligned} n &= a_0 + p \cdot n_1 \\ n_1 &= a_1 + p \cdot n_2 \\ &\vdots \quad \vdots \quad \vdots \quad \vdots \\ n_{k-1} &= a_{k-1} + p \cdot n_k \\ n_k &= a_k \end{aligned}$$

wobei $a_i \in \{0, 1, \ldots, p-1\} = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ und $n_i \in \mathbb{N}_0$. Damit erhalten wir

$$n = \sum_{i=0}^{k} a_i p^i$$

Setzen wir nun $a_i = 0 \; \forall \, i > k$, so erhalten wir

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

und somit die Existenz einer solchen Darstellung von n durch eine Potenzreihe im Punkt p mit Entwicklungspunkt $x_0 = 0$. (Bemerke: Für konkrete natürliche Zahlen $n \in \mathbb{N}$ erhält man eine derartige Darstellung, indem man die Gleichungen des obigen Systems der Reihe nach von oben beginnend nach untenhin löst.)
Eindeutigkeit:
Die Eindeutigkeit ist nach dem Konstruktionsprinzip klar.
zurück zum Satz 3.1.2 ■

BEWEIS: *(Satz 3.1.5)*
zurück zum Satz 3.1.5
zu (i):
Wir haben in diesem Teil die Ringeigenschaften aus Definition A.5 zu zeigen. Dazu sollten wir uns zunächst überlegen, wie wir die Verknüpfungen $+$ und $\cdot$ definieren:

$$+ \; : \; \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \quad \text{mit} \quad \left(\sum_{i=0}^{\infty} a_i p^i\right) + \left(\sum_{i=0}^{\infty} b_i p^i\right) := \left(\sum_{i=0}^{\infty} (a_i + b_i)\, p^i\right)$$

$$\cdot \; : \; \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \quad \text{mit} \quad \left(\sum_{i=0}^{\infty} a_i p^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i p^i\right) := \left(\sum_{i=0}^{\infty} \sum_{k=0}^{i} a_k b_{i-k} p^i\right)$$

wobei $a_i, b_i \in \{0, 1, \ldots, p-1\}$. Man beachte jedoch in beiden Fällen, dass Überträge auftreten können, weswegen sich der mathematische Beweis nicht im Einzelnen niederschreiben lässt.
$(\mathbb{Z}_p, +)$ abelsche Gruppe:
Das Assotiativgesetz sowie das Kommutativgesetz dürften klar sein, da sich diese Gesetze auf den reellen

Fall zurückführen lassen. Das neutrale Element der Addition in $\mathbb{Z}_p$ ist die Reihe

$$0 := \sum_{i=0}^{\infty} a_i p^i \qquad \text{mit } a_i = 0 \quad \forall\, i \in \mathbb{N}_0$$

Das zu $\sum_{i=0}^{\infty} a_i p^i$ $(a_i \in \{0, 1, \ldots, p-1\})$ additive Inverselement in $\mathbb{Z}_p$ ist

$$-\left(\sum_{i=0}^{\infty} a_i p^i\right) := \sum_{i=0}^{\infty} (-a_i)\, p^i$$

Damit ist $(\mathbb{Z}_p, +)$ eine abelsche Gruppe.
$(\mathbb{Z}_p, \cdot)$ Halbgruppe mit Einselement:
Das Assotiativgesetz ist klar, denn auch dies lässt sich (wie bereits bei der Additon) auf den reellen Fall zurückführen. Das Einselement ist die Reihe

$$1 := \sum_{i=0}^{\infty} a_i p^i \qquad \text{mit } a_0 = 1 \text{ und } a_i = 0 \quad \forall\, i \in \mathbb{N}$$

Damit ist $(\mathbb{Z}_p, \cdot)$ eine Halbgruppe mit Einselement.
Distributivgesetze:
Wir zeigen hier lediglich das erste in Definition A.5 angegebene Distribuivgesetz. Das zweite lässt sich analog zeigen. Dem Leser sei gesagt, dass die Überträge in dieser allgemeinen Form nicht ersichtlich sind! Seien $a_i, b_i, c_i \in \{0, 1, \ldots, p-1\} \quad \forall\, i \in \mathbb{N}_0$. Dann:

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

Damit ist $\mathbb{Z}_p$ ein Ring mit Einselement.
zu (ii):
Wir haben hier nun die Körpereigenschaften aus Definition A.5 zu überprüfen, d.h. im Vergleich zum ersten Teil des Beweises muss $(Q_p, \cdot)$ eine abelsche Gruppe sein. Wir definieren uns auch hier ähnlich wie zuvor die Addition und Multiplikation auf $\mathbb{Q}_p$ durch

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

wobei $a_i, b_i \in \{0, 1, \ldots, p-1\}$ und $n, m \in \mathbb{Z}$. Auch hier gebe man Obacht mit den möglicherweise auftretenden Überträgen! Der mathematische Beweis lässt sich daher auch hier nicht im Einzelnen aufführen.
$(\mathbb{Q}_p, +)$ abelsche Gruppe:
Das Assotiativgesetz sowie das Kommutativgesetz dürften klar sein, da sich diese Gesetze auf den reellen Fall zurückführen lassen. Das neutrale Element der Addition in $\mathbb{Q}_p$ ist die Reihe

$$0 := \sum_{i=-\infty}^{\infty} a_i p^i \qquad \text{mit } a_i = 0 \quad \forall\, i \in \mathbb{Z}$$

Das zu $\sum_{i=-n}^{\infty} a_i p^i$ ($a_i \in \{0,1,\ldots,p-1\}$, $n \in \mathbb{Z}$) additive Inverselement in $\mathbb{Q}_p$ ist

$$-\left(\sum_{i=-n}^{\infty} a_i p^i\right) := \sum_{i=-n}^{\infty} (-a_i)\, p^i$$

Damit ist $(\mathbb{Q}_p, +)$ eine abelsche Gruppe. Insbesondere stimmt das Nullelement mit dem von $\mathbb{Z}_p$ überein.
$(\mathbb{Q}_p, \cdot)$ abelsche Gruppe:
Das Assotiativgesetz ist klar, denn auch dies lässt sich (wie bereits bei der Additon) auf den reellen Fall zurückführen. Das Einselement ist die Reihe

$$1 := \sum_{i=-\infty}^{\infty} a_i p^i \qquad \text{mit } a_0 = 1 \text{ und } a_i = 0 \quad \forall\, i \in \mathbb{Z}\backslash\{0\}$$

Das inverse Element der Multiplikation lässt sich nicht allgemein definieren, es ist jedoch in $\mathbb{Q}_p$ enthalten. Man erhält es unter Betrachtung von $a^{-1} = \frac{1}{a}$ mit $a \in \mathbb{Q}_p\backslash\{0\}$ und unter Verwendung des *p-adischen Divisionsalgorithmus*, der unter *www.wikipedia.com* und dem Suchbegriff *p-adic division algorithm* zu finden ist.
Damit ist $(\mathbb{Q}_p, \cdot)$ eine abelsche Gruppe.
Distributivgesetze:
Wir zeigen hier lediglich das erste in Definition A.5 angegebene Distribuivgesetz. Das zweite lässt sich analog zeigen. Dem Leser sei gesagt, dass die Überträge in dieser allgemeinen Form nicht ersichtlich sind! Seien

$$\sum_{i=-n}^{\infty} a_i p^i,\ \sum_{i=-m}^{\infty} b_i p^i,\ \sum_{i=-l}^{\infty} c_i p^i \ \in \mathbb{Q}_p$$

wobei $a_i, b_i, c_i \in \{0,1,\ldots,p-1\}$ und $n, m, l \in \mathbb{Z}$. Dann:

$$\begin{aligned}
\left(\sum_{i=-n}^{\infty} a_i p^i\right) \cdot \left[\left(\sum_{i=-m}^{\infty} b_i p^i\right) + \left(\sum_{i=-l}^{\infty} c_i p^i\right)\right] &= \left(\sum_{i=-n}^{\infty} a_i p^i\right) \cdot \left(\sum_{i=\min\{-m,-l\}}^{\infty} (b_i + c_i)\, p^i\right) \\
&= \sum_{i=-n+\min\{-m,-l\}}^{\infty} \sum_{k=-n}^{i-\min\{-m,-l\}} a_k\, (b_{i-k} + c_{i-k})\, p^i \\
&= \sum_{i=-n+\min\{-m,-l\}}^{\infty} \sum_{k=-n}^{i+\max\{m,l\}} a_k b_{i-k} p^i + a_k c_{i-k} p^i \\
&= \left(\sum_{i=-n-m}^{\infty} \sum_{k=-n}^{i+m} a_k b_{i-k} p^i\right) + \left(\sum_{i=-n-l}^{\infty} \sum_{k=-n}^{i+l} a_k c_{i-k} p^i\right) \\
&= \left(\sum_{i=-n}^{\infty} a_i p^i\right) \cdot \left(\sum_{i=-m}^{\infty} b_i p^i\right) + \left(\sum_{i=-n}^{\infty} a_i p^i\right) \cdot \left(\sum_{i=-l}^{\infty} c_i p^i\right)
\end{aligned}$$

Es dürfte klar sein, dass

$$i - \min\{-m, -l\} \ = \ i + \max\{m, l\}$$

Damit ist $\mathbb{Q}_p$ ein Körper.
zurück zum Satz 3.1.5

■

BEWEIS: *(Satz 3.1.6)*
zurück zum Satz 3.1.6
$\Longleftarrow$:
Sei $(a_i)_{i\geqslant -k}$ periodisch. Wir dürfen annehmen, dass $k = 0$ und $a_0 \neq 0$ ist (z.B.: durch Indizeumbenennung). Dann ist $(a_i)_{i\in\mathbb{N}_0}$ von der Gestalt

$$(a_0, a_1, \ldots) \;=\; (b_0, b_1, \ldots, b_{k-1}, \overline{c_0, c_1, \ldots, c_{n-1}})$$

wobei $\overline{c_0, c_1, \ldots, c_{n-1}}$ die Periode und $b_0, b_1, \ldots, b_{k-1}$ die Vorperiode darstellen. Wir setzen nun:

$$\begin{aligned} b \;&:=\; b_0 + b_1 p^1 + b_2 p^2 + \cdots + b_{k-1} p^{k-1} \\ c \;&:=\; c_0 + c_1 p^1 + c_2 p^2 + \cdots + c_{n-1} p^{n-1} \end{aligned}$$

Dann ist

$$a \;=\; b + c \cdot p^k \cdot \left(1 + p^n + p^{2n} + \cdots\right) \;=\; b + c \cdot \frac{p^k}{1 - p^n} \;\in \mathbb{Q}$$

$\Longrightarrow$:
ohne Beweis. (siehe [1] im Literaturverzeichnis)
zurück zum Satz 3.1.6

■

BEWEIS: *(Satz 3.1.11)*
zurück zum Satz 3.1.11
zu (i):
$\Longleftarrow$:
Sei $x = 0$. Dann gilt:

$$v_p(x) \;=\; v_p(0) \;=\; \infty$$

$\Longrightarrow$:
Sei $v_p(x) = \infty$. Angenommen $x \neq 0$. Sei $x = \frac{a}{b}$ mit $a, b \in \mathbb{Z}\backslash\{0\}$. Dann gilt:

$$v_p(x) \;=\; v_p(a) - v_p(b) \quad \text{und nach Voraussetzung} \quad v_p(a) - v_p(b) \;=\; \infty$$

Da $a, b \in \mathbb{Z}\backslash\{0\}$ sind, gilt nach Definition von v_p, dass $v_p(a), v_p(b) \in \mathbb{Z}$ und damit

$$v_p(a) - v_p(b) \in \mathbb{Z} \quad \text{also} \quad v_p(a) - v_p(b) \neq \infty$$

Dies ist jedoch ein Widerspruch zur Voraussetzung. Wir erhalten somit, dass $x = 0$ sein muss.
zu (ii):
1.Fall: $x = 0, y = 0$

$$\begin{aligned} v_p(x) + v_p(y) \;&=\; v_p(0) + v_p(0) \;=\; \infty + \infty \;=\; \infty \\ v_p(x \cdot y) \;&=\; v_p(0 \cdot 0) \;=\; v_p(0) \;=\; \infty \end{aligned}$$

2.Fall: $x = 0, y \neq 0$

$$\begin{aligned} v_p(x) + v_p(y) \;&=\; v_p(0) + \underbrace{v_p(y)}_{=:z\in\mathbb{Z}} \;=\; \infty + z \;=\; \infty \\ v_p(x \cdot y) \;&=\; v_p(0 \cdot y) \;=\; v_p(0) \;=\; \infty \end{aligned}$$

3.Fall: $x \neq 0, y \neq 0$
Seien $x = \frac{a}{b}, y = \frac{c}{d} \in \mathbb{Q}$ mit $a, b, c, d \in \mathbb{Z}\backslash\{0\}$. Es ist klar, dass folgendes gilt:

$$v_p(z) + v_p(w) \;=\; v_p(z \cdot w) \quad \forall\, z, w \in \mathbb{Z}$$

Damit erhalten wir:

$$\begin{aligned} v_p(x)+v_p(y) &= v_p\left(\frac{a}{b}\right)+v_p\left(\frac{c}{d}\right) = v_p(a)-v_p(b)+v_p(c)-v_p(d) \\ &= v_p(a)+v_p(c)-[v_p(b)+v_p(d)] = v_p(a\cdot c)-v_p(b\cdot d) \\ &= v_p\left(\frac{a}{b}\cdot\frac{c}{d}\right) = v_p(x\cdot y) \end{aligned}$$

zu (iii):
1.Fall: $x=0, y=0$

$$\begin{aligned} &v_p(x+y) = v_p(0+0) = v_p(0) = \infty \\ &v_p(x) = v_p(0) = \infty \text{ und } v_p(y) = v_p(0) = \infty \quad\Longrightarrow\quad \min\{v_p(x),v_p(y)\} = \infty \end{aligned}$$

2.Fall: $x=0, y\neq 0$

$$\begin{aligned} &v_p(x+y) = v_p(0+y) = v_p(y) \in \mathbb{Z} \\ &v_p(x) = v_p(0) = \infty \text{ und } v_p(y)\in\mathbb{Z} \quad\Longrightarrow\quad \min\{v_p(x),v_p(y)\} = v_p(y) \end{aligned}$$

3.Fall: $x\neq 0, y\neq 0$
Seien $x=\frac{a}{b}, y=\frac{c}{d}\in\mathbb{Q}$ und $a,b,c,d\in\mathbb{Z}\backslash\{0\}$. Dann gilt:

$$\begin{aligned} v_p(x+y) &= v_p\left(\frac{a}{b}+\frac{c}{d}\right) = v_p\left(\frac{ad+cb}{bd}\right) = v_p(ad+cb)-v_p(bd) \\ &\geqslant \min\{v_p(ad),v_p(cb)\}-v_p(bd) \\ &= \min\{v_p(a)+v_p(d),v_p(c)+v_p(b)\}-v_p(b)-v_p(d) \\ &= \min\{v_p(a)-v_p(b),v_p(c)-v_p(d)\} = \min\{v_p\left(\frac{a}{b}\right),v_p\left(\frac{c}{d}\right)\} \\ &= \min\{v_p(x),v_p(y)\} \end{aligned}$$

zurück zum Satz 3.1.11

■

BEWEIS: *(Satz 3.1.12)*
zurück zum Satz 3.1.12
Bevor wir nun mit dem Beweis beginnen, erwähnen wir vorweg zunächst noch ein Theorem, auf das wir im Verlauf des Beweises zurückgreifen werden:

> *Jeder Körper K besitzt eine Bijektion zwischen den Äquivalenzklassen der Bewertung v auf K (d.h. $K/\sim := \{[a]_\sim \mid a\in K\}$) und den Bewertungsringen V von K. (In diesem Zusammenhang ensprechen Bewertungsringe und Bewertungen einander.)*

Dieses Theorem sagt also aus:

$$\exists\, f: K/\sim \longrightarrow V \text{ bijektiv}$$

Kommen wir nun zum Beweis des Satzes.
Dem Theorem nach zufolge reicht es aus, die Bewertungsringe von $\mathbb{Q}$ zu bestimmen, da wir mit Hilfe der Bewertungsringe und dem Theorem Rückschlüsse auf die Bewertung selbst erzielen können. Sei dazu V ein beliebiger Bewertungsring von $\mathbb{Q}$. Da V ein Bewertungsring ist, ist V insbesondere ein lokaler Ring und besitzt somit ein eindeutig bestimmtes maximales Ideal. Sei I nun dieses maximale Ideal von V.
Da $1\in\mathbb{Q}$ und 1 zu sich selbst invers ist, muss aufgrund der Definition eines Bewertungsrings

$$\forall\, x\in\mathbb{Q}: \quad x\in V \text{ oder } x^{-1}\in V$$

auch $1 \in V$ liegen. Diese Eigenschaft gewährleistet uns sogar, dass $\mathbb{Z} \subset V$. Nach Algebra 1 gilt:

$$I \subset V \text{ maximale Ideal von } V \quad \Longrightarrow \quad I \subset V \text{ Primideal von } V$$

Wir verwenden nun einen Satz aus der Algebra 1:

S (hier: $\mathbb{Z}$), R (hier: V) Ringe mit $S \subset R$ (hier: $\mathbb{Z} \subset V$) und p Primideal von R (hier: I Primideal von V). Dann gilt:
$p \cap S$ ist Primideal in S (hier: $I \cap \mathbb{Z}$ ist Primideal in $\mathbb{Z}$)

Man überlege sich auch leicht ohne Verwendung des Satzes, dass $I \cap \mathbb{Z}$ ein Primideal in $\mathbb{Z}$ ist, denn: Da I ein Primideal in V ist, gilt definitionsgemäß:

$$\forall\, a,b \in V \text{ mit } a \cdot b \in I: \quad a \in I \ \vee \ b \in I$$

Seien nun $a, b \in \mathbb{Z}$ mit $a \cdot b \in I \cap \mathbb{Z}$ beliebig, dann gilt:

1. $a \cdot b \in I \quad \overset{I \text{ Primideal}}{\Longrightarrow} \quad a \in I \ \vee \ b \in I$
2. $a \cdot b \in \mathbb{Z} \quad \overset{\text{n. Vor.}}{\Longrightarrow} \quad a \in \mathbb{Z} \ \wedge \ b \in \mathbb{Z}$

Insgesamt ergibt sich daher

$$\forall\, a,b \in \mathbb{Z} \text{ mit } a \cdot b \in I \cap \mathbb{Z}: \quad a \in I \cap \mathbb{Z} \ \vee \ b \in I \cap \mathbb{Z}$$

Damit ist $I \cap \mathbb{Z}$ ein Primideal von $\mathbb{Z}$. Allgemein besitzen die Ideale J von $\mathbb{Z}$ nach Algebra 1 die Form

$$J = (n) = \{z \cdot n \mid z \in \mathbb{Z}\} \quad , n \in \mathbb{N}_0$$

Weiter gilt:

$$J = (n) \text{ Primideal} \quad \Longleftrightarrow \quad n = 0 \text{ oder } n \in \mathbb{P}$$

Daher unterscheiden wir zwei Fälle:
1.Fall: $I \cap \mathbb{Z} = (0) = \{0\}$
Da I ein maximales Ideal von V ist und als maximales Ideal von V alle Nicht-Einheiten von V enthält, gilt:

$$\forall\, x \in \mathbb{Z} \text{ mit } x \neq 0: \quad x \text{ ist Einheit in } V \quad (\text{d.h. } \exists\, x^{-1} \in V: \ x \cdot x^{-1} = 1 = x^{-1} \cdot x)$$

Damit besitzt jede ganze Zahl $0 \neq x \in \mathbb{Z} \subset V$ ein multiplikatives Inverses x^{-1} in V. Somit muss V der Quotientenkörper von $\mathbb{Z}$ sein, d.h.

$$V = Q(\mathbb{Z}) := \{\frac{a}{b} \mid a,b \in \mathbb{Z} \wedge b \neq 0\} \overset{!}{=} \mathbb{Q}$$

Wir erhalten auf diese Weise $V = \mathbb{Q}$, also den trivialen Bewertungsring. Nach dem Theorem muss es sich bei der Bewertung um die triviale Bewertung handeln. Wir können dies auch zeigen indem wir zwei Fälle betrachten:
1.Unterfall: $x \in \mathbb{Z}\backslash\{0\}$
Sei $x \in \mathbb{Z}\backslash\{0\}$, dann ist x eine Einheit in V und es gilt:

$$|x|_p = 1 \quad \overset{\text{Def.3.1.13}}{\Longrightarrow} \quad p^{-v(x)} = 1 \quad \Longrightarrow \quad v(x) = 0 \quad \forall\, x \in \mathbb{Z}\backslash\{0\} \text{ (also } \forall\, x \neq 0)$$

2.Unterfall: $x = 0$
Sei $x = 0$, dann gilt nach Definition des p-adischen Betrags:

$$|0|_p = 0 \quad \overset{\text{Def.3.1.13}}{\Longrightarrow} \quad p^{-v(0)} = 0 \quad \overset{p^{-\infty}:=0}{\Longrightarrow} \quad v(0) = \infty \quad \text{für } x = 0$$

Damit erhalten wir genau die triviale Bewertung.
2.Fall: $I \cap \mathbb{Z} = (p) = p\mathbb{Z}$ $(p \in \mathbb{P})$
In diesem Fall gilt

$$\forall\, n \in \mathbb{Z}: \quad \begin{cases} p \mid n & , n \in p\mathbb{Z} \\ p \nmid n & , n \notin p\mathbb{Z} \text{ (d.h. } n \in \mathbb{Z}\backslash p\mathbb{Z}) \end{cases}$$

Betrachten wir nun also diese beiden Fälle:
1.Unterfall: $n \in p\mathbb{Z}$
Sei $n \in p\mathbb{Z}$, also $p \mid n$ (insbesondere ist n eine Nicht-Einheit). Dann gilt:

$$\exists\, x \in \mathbb{Z} \text{ mit } p \nmid x \;\wedge\; \exists\, m \in \mathbb{Z}\backslash\{0\}: \quad n \;=\; x \cdot p^m$$

Nach der Definition 3.1.7 des p-adischen Betrags gilt nun

$$|n|_p \;=\; |x \cdot p^m|_p \overset{p\nmid x}{=} \frac{1}{p^m} \;=\; p^{-m}$$

Machen wir nun auch Gebrauch von der Definition 3.1.13, so erhalten wir

$$|n|_p \;=\; p^{-m} \;=\; v^{-v(n)} \quad\Longrightarrow\quad v(n) \;=\; m \quad \forall\, n \in p\mathbb{Z}$$

Speziell für $n = 0 \in p\mathbb{Z}$ gilt mit Hilfe von Definition 3.1.13:

$$|0|_p \;=\; 0 \quad \overset{\text{Def.3.1.13}}{\Longrightarrow} \quad p^{-v(0)} \;=\; 0 \quad \overset{p^{-\infty}:=0}{\Longrightarrow} \quad v(0) \;=\; \infty \quad \text{für } x = 0$$

2.Unterfall: $n \notin p\mathbb{Z}$
Sei $n \in \mathbb{Z}\backslash p\mathbb{Z}$, also $p \nmid n$ (insbesondere ist n einen Einheit). Dann gilt:

$$ggT(p,n) \;=\; 1 \quad \overset{p\nmid n}{\Longrightarrow} \quad |n|_p \;=\; 1 \quad\Longrightarrow\quad p^{-v(n)} \;=\; 1 \quad\Longrightarrow\quad v(n) \;=\; 0 \quad \forall\, n \in \mathbb{Z}\backslash p\mathbb{Z}$$

also für alle n mit $p \nmid n$. Wir erhalten somit im 2. Fall die p-adische Bewertung und damit die Behauptung.
zurück zum Satz 3.1.12

■

BEWEIS: *(Satz 3.1.14)*
zurück zum Satz 3.1.14
zu (i):
$\Longleftarrow$:
Sei $x = 0$. Dann gilt:

$$|x|_p \;=\; |0|_p \;=\; 0$$

$\Longrightarrow$:
Sei $|x|_p = 0$. Angenommen $x \neq 0$. Dann gilt:

$$\exists_1\, m \in \mathbb{Z}: \quad x = p^m \cdot \frac{a'}{b'} \quad \text{mit } a', b' \in \mathbb{Z}\backslash\{0\} \text{ und } p \nmid a' \cdot b'$$

Damit gilt:

$$|x|_p \;=\; p^{-m} \quad \text{und nach Voraussetzung} \quad p^{-m} \;=\; 0$$

Aber wir wissen:

$$p^{-m} \;\neq\; 0 \quad \forall\, m \in \mathbb{Z}$$

Dies ist ein Widerspruch zur Voraussetzung. Wir erhalten somit, dass $x = 0$ sein muss.
zu (ii):
1.Fall: $x = 0, y = 0$

$$|x|_p = |0|_p = 0 \quad , \quad |y|_p = |0|_p = 0 \quad \Longrightarrow \quad |x|_p \cdot |y|_p = 0$$
$$|x \cdot y|_p = |0 \cdot 0|_p = |0|_p = 0$$

2.Fall: $x = 0, y \neq 0$

$$|x|_p = |0|_p = 0 \quad , \quad |y|_p \in \mathbb{R}\backslash\{0\} \quad \Longrightarrow \quad |x|_p \cdot |y|_p = 0 \cdot |y|_p = 0$$
$$|x \cdot y|_p = |0 \cdot y|_p = |0|_p = 0$$

3.Fall: $x \neq 0, y \neq 0$

$$|x|_p \cdot |y|_p = p^{-v_p(x)} \cdot p^{-v_p(y)} = p^{-v_p(x)-v_p(y)} = p^{-(v_p(x)+v_p(y))} = p^{-v_p(x \cdot y)} = |x \cdot y|_p$$

zu (iv):
1.Fall: $x = 0, y = 0$

$$|x + y|_p = |0 + 0|_p = |0|_p = 0$$
$$|x|_p = |0|_p = 0 \quad , \quad |y|_p = |0|_p = 0 \quad \Longrightarrow \quad \max\{|x|_p, |y|_p\} = 0$$

2.Fall: $x = 0, y \neq 0$

$$|x + y|_p = |0 + y|_p = |y|_p$$
$$|x|_p = |0|_p = 0 \quad \Longrightarrow \quad \max\{|x|_p, |y|_p\} = \max\{0, |y|_p\}$$

3.Fall: $x \neq 0, y \neq 0$

$$\begin{aligned} & v_p(x + y) \geqslant \min\{v_p(x), v_p(y)\} \\ \Longleftrightarrow \quad & -v_p(x + y) \leqslant -\min\{v_p(x), v_p(y)\} = \min\{-v_p(x), -v_p(y)\} \\ \Longleftrightarrow \quad & -v_p(x + y) \leqslant \min\{-v_p(x), -v_p(y)\} \leqslant \max\{-v_p(x), -v_p(y)\} \\ \Longleftrightarrow \quad & p^{-v_p(x+y)} \leqslant p^{\max\{-v_p(x), -v_p(y)\}} = \max\{p^{-v_p(x)}, p^{-v_p(y)}\} \end{aligned}$$

Damit erhalten wir:

$$|x + y|_p = p^{-v_p(x+y)} \leqslant \max\{p^{-v_p(x)}, p^{-v_p(y)}\} = \max\{|x|_p, |y|_p\}$$

zu (iii):
Wir verwenden (iv) und erhalten:

$$|x + y| \leqslant \max\{|x|_p, |y|_p\} \leqslant |x|_p + |y|_p$$

zurück zum Satz 3.1.14

■

BEWEIS: *(Satz 3.1.15)*
zurück zum Satz 3.1.15
$\Longrightarrow$:
Wir betrachten ohne Einschränkung lediglich

$$\sum_{n=0}^{\infty} z_n$$

denn falls die Reihe konvergiert, so konvergiert sie auch mit den k weggelassenen Summanden. Sei $\sum_{n=0}^{\infty} z_n$ konvergent, dann gilt nach dem Cauchyschen Konvergenz Kriterium

$$\forall\, \varepsilon > 0\ \exists\, N \in \mathbb{N}\ \forall\, n \geqslant m \geqslant N: \quad \left| \sum_{k=m}^{n} z_k \right|_p < \varepsilon$$

Insbesondere gilt daher für $m = n$:

$$|z_n|_p \leqslant \varepsilon \quad \forall\, n \geqslant N$$

Somit ist $(z_n)_{n\in\mathbb{N}}$ eine p-adische Nullfolge. Ergänzen wir die Folge mit den fehlenden Folgengliedern, so ist auch $(z_{-k}, \ldots, z_{-1}, z_0, \ldots)$, also $(z_n)_{n\in I}$ eine p-adische Nullfolge.

$\Longleftarrow$:

Sei $(z_n)_{n\in I}$ eine p-adische Nullfolge, dann ist auch $(z_n)_{n\in\mathbb{N}}$ eine solche und es gilt:

$$\forall\, \varepsilon > 0\ \exists\, N \in \mathbb{N}\ \forall\, n \geqslant N: \quad |z_n|_p < \varepsilon$$

Damit gilt $\forall\, n \geqslant m \geqslant N$:

$$\left| \sum_{k=m}^{n} z_k \right|_p \overset{3.1.13(iv)}{\leqslant} \max_{m\leqslant k\leqslant n} \{\underbrace{|z_k|_p}_{<\varepsilon}\} < \varepsilon$$

Nun gilt nach dem Cauchysche Konvergenz Kriterium:

$$\sum_{n=0}^{\infty} z_n \quad \text{ist konvergent}$$

Fügen wir nun noch die k fehlenden Summanden hinzu, so ändert dies nichts am Konvergenzverhalten, also gilt

$$\sum_{n=-k}^{\infty} z_n \quad \text{ist konvergent}$$

zurück zum Satz 3.1.15

■

BEWEIS: *(Satz 3.1.17)*

zurück zum Satz 3.1.17

Sei $x \in \mathbb{Q}\backslash\{0\}$ beliebig. Dann lässt sich x eindeutig in Primfaktoren zerlegen:

$$x = \pm p_1^{a_1} \cdot \cdots \cdot p_n^{a_n}$$

Dabei gilt:

$$|x|_\infty = p_1^{a_1} \cdot \cdots \cdot p_n^{a_n} = \prod_{i=1}^{n} p_i^{a_i}$$
$$|x|_{p_i} = p_i^{-a_i} \quad \forall\, i = 1, \ldots, n$$
$$|x|_p = p^0 = 1 \quad \forall\, p \in \mathbb{P}\backslash\{p_1, \ldots, p_n\}$$

Damit gilt insgesamt:

$$\prod_{p\in\mathbb{P}}^{\infty} |x|_p = |x|_{p_1} \cdot \cdots \cdot |x|_{p_n} \cdot |x|_\infty \cdot \underbrace{\prod_{p\in\mathbb{P}\backslash\{p_1,\ldots,p_n\}} |x|_p}_{=1}$$

$$= p_1^{-a_1} \cdot \cdots \cdot p_n^{-a_n} \cdot \prod_{i=1}^{n} p_i^{a_i} = \prod_{i=1}^{n} p_i^{-a_i} \cdot \prod_{i=1}^{n} p_i^{a_i} = \prod_{i=1}^{n} p_i^{0} = 1$$

zurück zum Satz 3.1.17

■

BEWEIS: *(Satz 3.1.19)*
zurück zum Satz 3.1.19
zu (i):
Wir haben folgende Eigenschaften zu beweisen:

(1) $(R,+)$ ist abelsche Gruppe

(2) $(R,\cdot)$ ist abelsche Halbgruppe mit Einselement

(3) Distributivgesetze

Seien $(x_n)_{n\in\mathbb{N}},(y_n)_{n\in\mathbb{N}} \in R$ Cauchy-Folgen, dann sind auch die Summe $(x_n+y_n)_{n\in\mathbb{N}}$ wie auch das Produkt $(x_n\cdot y_n)_{n\in\mathbb{N}}$ Cauchy-Folgen, d.h. R ist abgeschlossen bezüglich $+$ und $\cdot$.
zu (1):
(a) Assoziativgesetz:

$$\begin{aligned}(x_n)+[(y_n)+(z_n)] &= (x_1+[y_1+z_1],x_2+[y_2+z_2],\ldots)\\ &= ([x_1+y_1]+z_1,[x_2+y_2]+z_2,\ldots) = [(x_n)+(y_n)]+(z_n)\end{aligned}$$

(b) Nullelement:
$(0) := (0,0,0,\ldots)$ ist p-adisch konvergent gegen 0 und damit eine Cauchy-Folge, also $(0)\in R$. Es gilt:

$$(x_n)+(0) = (x_1+0,x_2+0,\ldots) = (x_n) = (0+x_1,0+x_2,\ldots) = (0)+(x_n)$$

Dass (0) eindeutig bestimmt ist, dürfte klar sein und wird daher nicht bewiesen.
(c) Inverses Element:
$-(x_n) := (-x_1,-x_2,\ldots)$ ist eine Cauchy-Folge, falls (x_n) eine solche ist, also $-(x_n)\in R$. Es gilt:

$$\begin{aligned}(x_n)+[-(x_n)] &= (x_1+(-x_1),x_2+(-x_2),\ldots) = (0,0,0,\ldots)\\ &= ((-x_1)+x_1,(-x_2)+x_2,\ldots) = [-(x_n)]+(x_n)\end{aligned}$$

Dass $-(x_n)$ eindeutig bestimmt ist, dürfte klar sein und wird daher nicht bewiesen.
(d) Kommutativgesetz:

$$(x_n)+(y_n) = (x_1+y_1,x_2+y_2,\ldots) = (y_1+x_1,y_2+x_2,\ldots) = (y_n)+(x_n)$$

zu (2):
(a) Assoziativgesetz:

$$\begin{aligned}(x_n)\cdot[(y_n)\cdot(z_n)] &= (x_1\cdot[y_1\cdot z_1],x_2\cdot[y_2\cdot z_2],\ldots)\\ &= ([x_1\cdot y_1]\cdot z_1,[x_2\cdot y_2]\cdot z_2,\ldots) = [(x_n)\cdot(y_n)]\cdot(z_n)\end{aligned}$$

(b) Einselement: $(1) := (1,1,1,\ldots)$ ist p-adisch konvergent gegen 1 und damit eine Cauchy-Folge, also $(1)\in R$. Es gilt:

$$(x_n)\cdot(1) = (x_1\cdot 1,x_2\cdot 1,\ldots) = (x_n) = (1\cdot x_1,1\cdot x_2,\ldots) = (1)\cdot(x_n)$$

Dass (1) eindeutig bestimmt ist, dürfte klar sein und wird daher nicht bewiesen.
(c) Kommutativgesetz:

$$(x_n)\cdot(y_n) = (x_1\cdot y_1,x_2\cdot y_2,\ldots) = (y_1\cdot x_1,y_2\cdot x_2,\ldots) = (y_n)\cdot(x_n)$$

zu (3):
(a) 1.Distributivgesetz:

$$\begin{aligned}(x_n)\cdot[(y_n)+(z_n)] &= (x_1\cdot[y_1+z_1],x_2\cdot[y_2+z_2],\ldots)\\ &= (x_1\cdot y_1+x_1\cdot z_1,x_2\cdot y_2+x_2\cdot z_2,\ldots) = (x_n)\cdot(y_n)+(x_n)\cdot(z_n)\end{aligned}$$

(b) 2.Distributivgesetz:

$$\begin{aligned}[(x_n)+(y_n)]\cdot(z_n) &= ([x_1+y_1]\cdot z_1,[x_2+y_2]\cdot z_2,\ldots)\\ &= (x_1\cdot z_1+y_1\cdot z_1,x_2\cdot z_2+y_2\cdot z_2,\ldots) = (x_n)\cdot(z_n)+(y_n)\cdot(z_n)\end{aligned}$$

zu (ii):
Wir haben folgende Eigenschaften zu beweisen:

(1) I ist ein Ideal von R

(2) I ist maximal

zu (1):
(a): z.z.: $(0)\in I$
$(0):=(0,0,0,\ldots)$ ist p-adisch konvergent gegen 0 und damit eine Nullfolge, also $(0)\in I$
(b): z.z.: $\forall\,(x_n)_{n\in\mathbb{N}},(y_n)_{n\in\mathbb{N}}\in I:\quad (x_n-y_n)_{n\in\mathbb{N}}\in I$
Seien $(x_n)_{n\in\mathbb{N}},(y_n)_{n\in\mathbb{N}}\in I$, also zwei Nullfolgen. Damit gilt:

$$\forall\,\varepsilon>0\;\exists\,N_1\in\mathbb{N}\;\forall\,n>N_1:\;|x_n|_p\leqslant\frac{\varepsilon}{2}$$
$$\forall\,\varepsilon>0\;\exists\,N_2\in\mathbb{N}\;\forall\,n>N_2:\;|y_n|_p\leqslant\frac{\varepsilon}{2}$$

Sei $\varepsilon>0$ beliebig. Wähle $N:=\max\{N_1,N_2\}$. Dann gilt:

$$|x_n-y_n|_p\;\leqslant\;|x_n|_p+|y_n|_p\;\leqslant\;\frac{\varepsilon}{2}+\frac{\varepsilon}{2}\;=\;\varepsilon$$

also eine p-adische Nullfolge. Folglich ist $(x_n-y_n)_{n\in\mathbb{N}}\in I$.
(c): z.z.: $\forall\,(a_n)_{n\in\mathbb{N}}\in R\;\wedge\;\forall\,(x_n)_{n\in\mathbb{N}}\in I:\quad (a_n\cdot x_n)_{n\in\mathbb{N}}\in I$
Seien $(a_n)_{n\in\mathbb{N}}\in R$ und $(x_n)_{n\in\mathbb{N}}\in I$. $(a_n)_{n\in\mathbb{N}}$ ist als Cauchy-Folge beschränkt. Damit gilt:

$$\exists\,K\in\mathbb{Q}\;\forall\,n\in\mathbb{N}:\;|a_n|_p\leqslant K$$
$$\forall\,\varepsilon>0\;\exists\,N\in\mathbb{N}\;\forall\,n>N:\;|x_n|_p\leqslant\frac{\varepsilon}{K}$$

Sei $\varepsilon>0$ beliebig. Dann gilt:

$$|a_n\cdot x_n|_p\;=\;|a_n|_p\cdot|x_n|_p\;\leqslant\;K\cdot\frac{\varepsilon}{K}\;=\;\varepsilon$$

also eine p-adische Nullfolge. Folglich ist $(a_n\cdot x_n)_{n\in\mathbb{N}}\in I$.
zu (2):
Angenommen I ist kein maximales Ideal von R. Dann gilt:

$$\exists\,J\text{ Ideal von }R\text{ mit }I\subseteq J\text{ und }J\neq R:\quad I\neq J$$

Sei $(x_n)_{n\in\mathbb{N}}\in R\backslash I$ beliebig. Dann ist $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge, jedoch keine Nullfolge, d.h. es gilt:

$$\exists\,k\in\mathbb{N}\;\forall\,n\geqslant k:\quad x_n\neq 0$$

(denn falls andernfalls gelten würde

$$\forall\,k\in\mathbb{N}\;\exists\,n\geqslant k:\quad x_n=0$$

dann wäre $(x_n)_{n\in\mathbb{N}}$ (da $(x_n)_{n\in\mathbb{N}}$) eine Nullfolge und somit $(x_n)_{n\in\mathbb{N}} \in I$, was ein Widerspruch zur Wahl von $(x_n)_{n\in\mathbb{N}} \in R\backslash I$ wäre.) Sei nun

$$J := I \cup \{x_n \mid n \in \mathbb{N}\}$$

ein Ideal. Wir wollen nun zeigen, dass eine solche Erweiterung von I stets dazu führt, dass $J = R$ ist, was nach Voraussetzung nicht sein darf. Dazu sei

$$y_n := \begin{cases} 1 & , n < k \ \wedge \ x_n \neq -1 \\ 2 & , n < k \ \wedge \ x_n = -1 \\ 0 & , n \geqslant k \end{cases}$$

d.h.

$$y_n = \left(\underbrace{y_1, y_2, \ldots, y_{k-1}}_{\neq 0}, 0, 0, 0, \ldots \right)$$

ist nach Definition eine Nullfolge und damit ist $(y_n)_{n\in\mathbb{N}} \in J$. Mit Hilfe der zweiten Idealeigenschaft gilt:

$$(x_n + y_n) = \left(\underbrace{x_1 + y_1, x_2 + y_2, \ldots, x_{k-1} + y_{k-1}}_{\neq 0}, \underbrace{x_k, x_{k+1}, \ldots}_{\neq 0} \right) \in J$$

Da $(x_n + y_n) \neq 0 \quad \forall\, n \in \mathbb{N}$, gibt es eine multiplikativ inverse Folge

$$(x_n + y_n)^{-1} := \left(\frac{1}{x_1 + y_1}, \frac{1}{x_2 + y_2}, \ldots, \frac{1}{x_{k-1} + y_{k-1}}, \frac{1}{x_k}, \frac{1}{x_{k+1}}, \ldots \right)$$

Diese Folge ist eine Cauchy-Folge, also $(x_n + y_n)^{-1} \in R$. (Denn sei $(a_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge mit $a_n \neq 0 \quad \forall\, n \in \mathbb{N}$, so ist die Folge zudem beschränkt (insbesondere nach unten) und es gilt:

$$\exists\, K \in \mathbb{Q}\ \forall\, n \in \mathbb{N} : \quad |a_n|_p \leqslant K$$
$$\forall\, \varepsilon > 0\ \exists\, N \in \mathbb{N}\ \forall\, n, m \geqslant N : \quad |a_n - a_m|_p \leqslant \varepsilon \cdot 2K$$

Betrachten wir nun die Folge $\left(\frac{1}{a_n}\right)_{n\in\mathbb{N}}$. Sei $\varepsilon > 0$ beliebig, dann gilt:

$$\left| \frac{1}{a_n} - \frac{1}{a_m} \right|_p = \left| \frac{a_m - a_n}{a_n \cdot a_m} \right|_p = \underbrace{\underbrace{\underbrace{\frac{1}{|a_n|_p}}_{\geqslant K} \cdot \underbrace{\frac{1}{|a_m|_p}}_{\geqslant K}}_{\geqslant 2K}}_{\leqslant \frac{1}{2K}} \cdot \underbrace{|a_m - a_n|_p}_{\leqslant \varepsilon \cdot 2K} \leqslant \frac{1}{2K} \cdot \varepsilon \cdot 2K = \varepsilon$$

Damit ist $\left(\frac{1}{a_n}\right)_{n\in\mathbb{N}}$ eine Cauchy-Folge.) Also ist auch $(x_n + y_n)^{-1}$ eine solche und da

$$(x_n + y_n)^{-1} \cdot (x_n + y_n) = (1, 1, 1, \ldots) = (1)$$

enthält J mit $(x_n + y_n) \in J$ eine Einheit von R. Nach Algebra 1 ist jedoch das einzige Ideal von R, dass eine Einheit enthält, R selbst (das sogenannte *Einheitsideal*). Also gilt $J = R$, was ein Widerspruch dazu ist, dass J ein maximales Ideal von R ist. Damit muss I das maximale Ideal von R sein.
zurück zum Satz 3.1.19

■

BEWEIS: *(Bemerkung 3.1.22)*
zurück zur Bemerkung 3.1.22

$$v'_p(x) = -\log_p |x|'_p \iff v'_p(x) = \log_p \frac{1}{|x|'_p} \iff p^{v'_p(x)} = \frac{1}{|x|'_p}$$
$$\iff |x|'_p \cdot p^{v'_p(x)} = 1 \iff |x|'_p = p^{-v'_p(x)}$$

zurück zur Bemerkung 3.1.22

■

BEWEIS: *(Satz 3.1.23)*
zurück zum Satz 3.1.23
ohne Beweis.
zurück zum Satz 3.1.23

■

BEWEIS: *(Satz 3.1.25)*
zurück zum Satz 3.1.25
zu (i):
Wir haben folgende Eigenschaften zu beweisen:

(1) $(1) \in \mathbb{Z}'_p$

(2) $\forall\, x, y \in \mathbb{Z}'_p : \quad (x - y) \in \mathbb{Z}'_p$

(3) $\forall\, x, y \in \mathbb{Z}'_p : \quad (x \cdot y) \in \mathbb{Z}'_p$

zu (1):
$(1) := (1, 1, 1, \ldots) \in \mathbb{Q}'_p$ ist Einselement. Es gilt:

$$|(1)|'_p = \lim_{n\to\infty} |1|_p = |1|_p = p^0 = 1 \overset{!}{\leqslant} 1$$

also $(1) \in \mathbb{Z}'_p$.
zu (2):
Seien $x, y \in \mathbb{Z}'_p$. Dann ist $|x|'_p \leqslant 1$ und $|y|'_p \leqslant 1$. Weiter gilt nun:

$$|x - y|'_p = |x + (-y)|'_p \leqslant \max\{|x|'_p, \underbrace{|-y|'_p}_{=|(-1)|'_p \cdot |y|'_p} \} \leqslant \max\{|x|'_p, \underbrace{|(-1)|'_p}_{=1} \cdot |y|'_p\}$$
$$= \max\{\underbrace{|x|'_p}_{\leqslant 1}, \underbrace{|y|'_p}_{\leqslant 1}\} \leqslant 1$$

also $(x - y) \in \mathbb{Z}'_p$.
zu (3):
Seien $x, y \in \mathbb{Z}'_p$. Dann ist $|x|'_p \leqslant 1$ und $|y|'_p \leqslant 1$. Weiter gilt nun:

$$|x \cdot y|'_p = \underbrace{|x|'_p}_{\leqslant 1} \cdot \underbrace{|y|'_p}_{\leqslant 1} \leqslant 1$$

also $(x \cdot y) \in \mathbb{Z}'_p$.
zu (ii):
Sei $x \in \mathbb{Z}'_p$ eine beliebige Einheit von $\mathbb{Z}'_p$, dann gilt:

$$\begin{aligned} & v'_p(x) \geqslant 0 && (\text{da } x \in \mathbb{Z}'_p) \\ & \exists\, x^{-1} \in \mathbb{Z}'_p : \quad x \cdot x^{-1} = 1 && (\text{da } x \text{ Einheit in } \mathbb{Z}'_p) \end{aligned}$$

Da $x^{-1} \in \mathbb{Z}'_p$ liegt, gilt $v'_p(x^{-1}) \geqslant 0$. Wenden wir nun auf die Gleichung $x \cdot x^{-1} = 1$ die Bewertungsfunktion v'_p an, so erhalten wir:

$$0 = v'_p(1) = v'_p(x \cdot x^{-1}) \overset{\text{Satz 3.1.11 (ii)}}{=} \underbrace{v'_p(x)}_{\substack{x \in \mathbb{Z}'_p \\ \geqslant 0}} + \underbrace{v'_p(x^{-1})}_{\substack{x^{-1} \in \mathbb{Z}'_p \\ \geqslant 0}}$$

Damit folgt, dass $v'_p(x) = 0$ und $v'_p(x^{-1}) = 0$. Demnach liegen alle Einheiten von $\mathbb{Z}'_p$ in der Menge

$$Z'^{*}_p := \{x \in \mathbb{Q}'_p \mid v'_p(x) = 0\} = \{x \in \mathbb{Q}'_p \mid |x|'_p = 1\}$$

zu (iii):
Angenommen $a \in \mathbb{Z}'_p \backslash \{0\}$ ist ein Nullteiler von $\mathbb{Z}'_p$, dann gilt

$$\exists\, b \in \mathbb{Z}'_p \backslash \{0\} : \quad a \cdot b = 0$$

Wir erinneren zunächst daran, dass

$$\mathbb{Z}_p \backslash \{0\} = \{x \in \mathbb{Q}'_p \mid v'_p(x) \geqslant 0 \text{ und } v'_p(x) \neq \infty\}$$

Dann gilt nun:

$$a \cdot b = 0 \iff \underbrace{v'_p(a \cdot b)}_{= v'_p(a) + v'_p(b)} = \underbrace{v'_p(0)}_{= \infty} \iff v'_p(a) + v'_p(b) = \infty$$

Damit muss entweder $v'_p(a) = \infty$ oder $v'_p(b) = \infty$ (oder beide $v'_p(a) = v'_p(b) = \infty$) sein, und damit muss entweder $a = 0$ oder $b = 0$ (oder beide $a = b = 0$) sein. Dies sind in allen drei Fällen jedoch Widersprüche dazu, dass a ein Nullteiler von $\mathbb{Z}'_p$ ist. Da $a \in \mathbb{Z}'_p \backslash \{0\}$ beliebig war, folgt, dass $\mathbb{Z}'_p$ nullteilerfrei und damit ein Integritätsring ist.
zu (iv):
Nach der Definition eines lokalen Rings gilt:

$$\mathbb{Z}'_p \text{ lokaler Ring} \quad :\iff \quad \exists_1\, I \subset \mathbb{Z}'_p \text{ Ideal von } \mathbb{Z}'_p : \; I \text{ maximales Ideal}$$

Wir müssen also zeigen, dass $\mathbb{Z}'_p$ genau ein maximales Ideal I besitzt. Kommen wir zunächst zur Existenz:
Existenz:
Aus der Algebra 1 wissen wir, dass echte Ideale niemals Einheiten enthalten. Die Einheiten von $\mathbb{Z}'_p$ sind nach Teil (ii) gerade diejenigen $x \in \mathbb{Z}'_p$ mit $|x|'_p = 1$. Wir betrachten also

$$I := \{x \in \mathbb{Z}'_p \mid |x|'_p < 1\}$$

Diese Menge I bildet ein Ideal von $\mathbb{Z}'_p$. Dazu überprüfen wir die Idealeigenschaften

(1) $(0) := (0, 0, 0, \ldots) \in I$

(2) $\forall\, a, b \in I : \quad a - b \in I$

(3) $\forall\, a \in I \;\wedge\; \forall\, x \in \mathbb{Z}'_p : \quad a \cdot x \in I$

zu (1):

$$|(0)|'_p \;=\; \lim_{n\to\infty} |0|_p \;=\; |0|_p \;=\; 0 \;<\; 1 \quad\Longrightarrow\quad (0)\in I$$

zu (2):
Seien $a,b\in I$ beliebig, d.h. $|a|'_p<1$ und $|b|'_p<1$. Dann gilt:

$$|a-b|'_p \;\leqslant\; \max\{|a|'_p\,,|-b|'_p\} \;=\; \max\{\underbrace{|a|'_p}_{<1},\underbrace{|b|'_p}_{<1}\} \;<\; 1$$

Damit ist $a-b\in I$.
zu (3):
Seien $a\in I$ und $x\in\mathbb{Z}'_p$ beide beliebig, d.h. $|a|'_p<1$ und $|x|'_p\leqslant 1$. Dann gilt:

$$|a\cdot x|'_p \;=\; \underbrace{|a|'_p}_{<1}\cdot\underbrace{|x|'_p}_{\leqslant 1} \;<\; 1$$

Damit ist $a\cdot x\in I$ und I somit ein Ideal von $\mathbb{Z}'_p$.
Die Maximalität von I kann man sich nun leicht denken, denn: Angenommen I ist nicht maximal, dann gilt:

$$\exists\, J\supset I \text{ Ideal von } \mathbb{Z}'_p \text{ mit } J\neq\mathbb{Z}'_p: \quad I\neq J$$

Da das Ideal I gerade alle Nicht-Einheiten von $\mathbb{Z}'_p$ enthält, wäre das Einbinden eines Elements $x\in\mathbb{Z}'_p$ mit $|x|'_p=1$ (also einer Einheit von $\mathbb{Z}'_p$) die einzige Möglicheit ein solches J zu konstruieren. Nun wissen wir wieder aus Algebra 1:

> Das einzige Ideal von $\mathbb{Z}'_p$, das eine Einheit enthält, ist $\mathbb{Z}'_p$ selbst.

Damit ist also $J=\mathbb{Z}'_p$, was ein Widerspruch zur Voraussetzung $J\neq\mathbb{Z}'_p$ ist. Somit ist I tatsächlich ein maximales Ideal von $\mathbb{Z}'_p$.
Eindeutigkeit:
Die Eindeutigkeit ist eigentlich nach Konstruktion klar, aber dennoch ein kurzes Wort dazu: Seien I,J maximale Ideale von $\mathbb{Z}'_p$, wobei I wie oben definiert ist. Da I nun alle Elemente bis auf Einheiten von $\mathbb{Z}'_p$ besitzt und ein echtes Ideal keine Einheiten besitzen darf, muss $J\subseteq I$ sein. Wir unterscheiden dann zwei Fälle:
1.Fall: $J\subset I$
Dies ist ein Widerspruch zur Maximalität von J, also muss $J=I$ gelten.
2.Fall: $J=I$
Beide Fälle zeigen, dass $J=I$ sein muss. Damit ist I tatsächlich das einzige maximale Ideal von $\mathbb{Z}'_p$ und $\mathbb{Z}'_p$ ist somit ein lokaler Ring.
zu (v):
Um zu zeigen, dass $\mathbb{Z}'_p$ ein Hauptidealring ist, müssen wir beweisen, dass jedes Ideal $\{0\}\neq I\subset\mathbb{Z}'_p$ ein Hauptideal ist. Sei I nun ein beliebiges echtes Ideal von $\mathbb{Z}'_p$ (d.h. $I\neq\mathbb{Z}'_p$), so heißt I Hauptideal genau dann, wenn es von einem seiner Elemente erzeugt wird.
Wir wählen nun $a\in I$ derart, dass

$$v'_p(a) \;=\; \min\{v'_p(b)\mid b\in I\}$$

erfüllt ist, d.h.

$$v'_p(a) \;\leqslant\; v'_p(b) \quad \forall\, b\in I$$

Ein solches $a\in I$ existiert selbstverständlich. Wir wollen nun zeigen

$$I \;=\; (a) \;=\; \{r\cdot a\mid r\in\mathbb{Z}'_p\}$$

d.h. I wird von a erzeugt. Dazu sei $b \in I$ ein beliebiges Element. Da $\mathbb{Q}_p'$ nun ein Körper ist, liegt a^{-1} in ihm und somit auch das Produkt $a^{-1} \cdot b =: c \in \mathbb{Q}_p'$. Genauer:

$$\exists\, c \in \mathbb{Q}_p' : \quad a \cdot c \;=\; b$$

Wenden wir nun die p-adische Bewertungsfunktion auf beiden Seiten an, so erhalten wir

$$0 \overset{b \in \mathbb{Z}_p'}{\leqslant} v_p'(b) \;=\; v_p'(a \cdot c) \overset{\text{Satz 3.1.11 (ii)}}{=} \underbrace{v_p'(a)}_{\leqslant v_p'(c)} + v_p'(c) \;\leqslant\; 2 \cdot v_p'(c)$$

Also

$$0 \;\leqslant\; 2 \cdot v_p'(c) \quad \Longrightarrow \quad 0 \;\leqslant\; v_p'(c)$$

und damit ist $c \in \mathbb{Z}_p'$. Da I nun ein Ideal von $\mathbb{Z}_p'$ ist und die Eigenschaft

$$\forall\, a \in I\; \forall\, c \in \mathbb{Z}_p' : \quad a \cdot c \in I$$

besitzt, muss $b \in I = (a)$ sein. Damit ist I ein Hauptideal. Da I ein beliebiges Ideal war, ist $\mathbb{Z}_p'$ somit ein Hauptidealring.
zurück zum Satz 3.1.25

■

BEWEIS: *(Satz 3.1.26)*
zurück zum Satz 3.1.26
Angenommen $\mathbb{Q}_p'$ ist abzählbar, dann gilt:

$$\exists\, \varphi : \mathbb{N} \longrightarrow \mathbb{Q}_p' \text{ surjektiv}$$

Setzte

$$\varphi(n) \;:=\; x_n \;\in \mathbb{Q}_p'$$

dann ist $(x_n)_{n \in \mathbb{N}} \subset \mathbb{Q}_p'$ eine Folge in $\mathbb{Q}_p'$. Wir verwenden an dieser Stelle *Cantors zweite Diagonalargument*, was auch in der Analysis im Beweis der Überabzählbarkeit der reellen Zahlen $\mathbb{R}$ verwendet wurde. Eine solche Folge $(x_n)_{n \in \mathbb{N}} \subset \mathbb{Q}_p'$ sieht also wie folgt aus:

$$\begin{aligned}
x_1 &= (z_{11}, z_{12}, z_{13}, z_{14}, \ldots) \mod I \\
x_2 &= (z_{21}, z_{22}, z_{23}, z_{24}, \ldots) \mod I \\
x_3 &= (z_{31}, z_{32}, z_{33}, z_{34}, \ldots) \mod I \\
x_4 &= (z_{41}, z_{42}, z_{43}, z_{44}, \ldots) \mod I \\
\vdots \;\; \vdots \qquad & \qquad \vdots \qquad\qquad\quad \vdots
\end{aligned}$$

Wir konstruieren nun eine Zahl $r \in \mathbb{Q}_p'$ mit $\varphi(n) \neq r \;\forall\, n \in \mathbb{N}$:

$$r_i \;:=\; \begin{cases} 0 & , z_{ii} = 1 \\ 1 & , z_{ii} \neq 1 \end{cases}$$

wobei $i = 1, 2, 3, \ldots$. So erhalten wir eine neue Folge $r = (r_1, r_2, r_3, \ldots) \mod I$. Diese unterscheidet sich von jeder Folge $(z_{i1}, z_{i2}, z_{i3}, \ldots)$ an mindestens genau einer Stelle, und zwar in z_{ii}.
Jedoch dürfte es noch nicht ganz klar sein, dass es sich bei der soeben konstruierten Folge um eine Cauchy-Folge handelt. Dazu überlegen man sich jedoch ganz einfach, dass wir mit der Folge

$$r \;:=\; (0, 0, 0, \ldots)$$

begonnen haben. Dies ist eine Cauchy-Folge (sogar eine Nullfolge) und im maximalen Ideal I enthalten. Dann:
1.Fall: $z_{ii} = 1$
Dann setzte $r_i = 0$, d.h. die Folge r bleibt unverändert und somit eine Cauchy-Folge.
2.Fall: $z_{ii} \neq 1$
Wir addieren zu der Folge r die Folge

$$\underbrace{(0,\ldots,0,1,0,\ldots)}_{i\text{-te Stelle } 1}$$

hinzu. Diese Folge ist eine Cauchy-Folge (sogar eine Nullfolge) und wieder im maximalen Ideal I enthalten. Weiter wissen wir, dass Cauchy-Folgen gegenüber Addition abgeschlossen sind, daher ist die Summe wieder eine Cauchy-Folge und wir haben ein Element $r \in \mathbb{Q}_p'$ gefunden, dass nach Konstruktion nicht im Bild $\varphi(\mathbb{N})$ liegen kann, also $r \notin \varphi(\mathbb{N})$. Das ist jedoch ein Widerspruch dazu, dass φ surjektiv ist. Demnach ist $\mathbb{Q}_p'$ von größerer Mächtigkeit als $\mathbb{N}$ und $\nexists\, \varphi : \mathbb{N} \longrightarrow \mathbb{Q}_p'$ surjektiv, also ist $\mathbb{Q}_p'$ überabzählbar.
zurück zum Satz 3.1.26

■

BEWEIS: *(Satz 3.1.27)*
zurück zum Satz 3.1.27
ohne Beweis
zurück zum Satz 3.1.27

■

BEWEIS: *(Bemerkung 3.1.28)*
zurück zur Bemerkung 3.1.28
zu (i):
Existenz:
Sei $x \in \mathbb{Z}_p'$ beliebig. Dann gilt:

$$|x|_p' \leqslant 1$$

Wir wissen nun

$$\exists\, x_0 \in \mathbb{N}_0 \;\text{ mit } 0 \leqslant x_0 \leqslant p-1 : \quad |x - x_0|_p' < 1$$

Damit ist $|x - x_0|_p' \leqslant \frac{1}{p}$ und somit $\frac{(x-x_0)}{p} \in \mathbb{Z}_p'$. Wiederholt man den letzten Schritt nun, dann:

$$\exists\, x_1 \in \mathbb{N}_0 \;\text{ mit } 0 \leqslant x_1 \leqslant p-1 : \quad |x - (x_0 + x_1 p)|_p' < \frac{1}{p}$$

Durch ständiges Wiederholen erhalten wir nun eine Folge $(x_n)_{n\in\mathbb{N}}$, für die Folgendes gilt:

$$|x - (x_0 + x_1 p + \cdots + x_n p^n)|_p' < \frac{1}{p^n} \qquad \text{, wobei } 0 \leqslant x_i \leqslant p-1 \text{ , } i = 1,\ldots,n$$

Wir definieren uns daher nun:

$$\alpha_n := x_0 + x_1 p + \cdots + x_n p^n$$

Die Folge $(\alpha_n)_{n\in\mathbb{N}}$ ist eine Cauchy-Folge bzgl. $|\,.\,|_p'$. Desweiteren ist der zugehörige Grenzwert x, denn

$$|x - \alpha_n|_p' < \frac{1}{p^n}$$

Somit haben wir die p-adische Entwicklung

$$x = x_0 + x_1 p + x_2 p^2 + \cdots$$

Eindeutigkeit:
Angenommen es existiert eine weitere p-adische Entwicklung von x. Diese sei gegeben durch

$$x = x_0' + x_1' p + x_2' p^2 + \cdots$$

Sei d der erste Index, für den gilt

$$x_d \neq x_d'$$

Sei o.B.d.A. $x_d < x_d'$ $(0 \leqslant x_d \leqslant p-1, 0 \leqslant x_d' \leqslant p-1)$. Dann ist

$$0 < x_d' - x_d \leqslant p-1$$

Genauer gilt sogar $1 \leqslant x_d' - x_d \leqslant p-1$ (da x_d', x_d ganzzahlig sind). Seien nun

$$\alpha_n := x_0 + x_1 p + \cdots + x_n p^n$$
$$\alpha_n' := x_0' + x_1' p + \cdots + x_n' p^n$$

Dann gilt:

$$\alpha_d' - \alpha_d = (x_d' - x_d) \cdot p^d$$

Wir erhalten nun zweierlei

$$(1)\ |\alpha_d' - \alpha_d|_p' = \left|(x_d' - x_d) \cdot p^d\right|_p' = \frac{1}{p^d}$$

$$(2)\ |\alpha_d' - \alpha_d|_p' = |(\alpha_d' - x) + (x - \alpha_d)|_p' \leqslant \max\{\underbrace{|\alpha_d' - x|_p'}_{<\frac{1}{p^d}}, \underbrace{|x - \alpha_d|_p'}_{<\frac{1}{p^d}}\} < \frac{1}{p^d}$$

Damit erhalten wir einen Widerspruch zu $\alpha_d' \neq \alpha_d$. Somit kann ein solches d nicht existieren, d.h. es gilt $\alpha_d' = \alpha_d \quad \forall\, d \in \mathbb{N}_0$ und damit ist die Eindeutigkeit gezeigt.
zu (ii):
Sei $x \in \mathbb{Q}_p'$ beliebig. Wir betrachten nun zwei Fälle:
1.Fall: $|x|_p' \leqslant 1$
In diesem Fall ist $x \in \mathbb{Z}_p'$ und die Behauptung folgt aus Teil (i). Die Existenz und Eindeutigkeit wurde dort ebenfalls gezeigt.
2.Fall: $|x|_p' > 1$
Sei o.B.d.A. $|x|_p' = p^k$ mit $k > 0$. Wir setzen

$$\beta := p^k x$$

Dann ist

$$|\beta|_p' = \left|p^k x\right|_p' = \left|p^k\right|_p' \cdot |x|_p' = p^{-k} \cdot p^k = p^0 = 1$$

Damit ist $\beta \in \mathbb{Z}_p'$ und besitzt nach (i) eine eindeutige Darstellung

$$\beta = \beta_0 + \beta_1 p + \cdots$$

Dann ist

$$x = \frac{1}{p^k} \cdot \beta = \frac{1}{p^k} \cdot \sum_{i=0}^{\infty} \beta_i p^i = \sum_{i=0}^{\infty} \beta_i p^{i-k}$$
$$= \frac{\beta_0}{p^k} + \frac{\beta_1}{p^{k-1}} + \cdots + \frac{\beta_{k-1}}{p} + \beta_k + \beta_{k+1} p + \cdots + \beta_{k+r} p^r + \cdots$$

wobei $0 \leqslant \beta_i \leqslant (p-1)\ \forall\, i = 0, 1, 2, \ldots$. Wir sind an dieser Stelle eigentlich bereits fertig. Um das Ganze jedoch noch etwas zu verdeutlichen: Definieren wir nun $x_i := \beta_{i+k}$ für $i = -k, -k+1, \ldots$, dann erhalten wir:

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

Damit haben wir die Existenz der Darstellung gezeigt. Da wir durch die Umformung $\beta := p^k x$ auf Teil (i) zurückgreifen konnten und für Teil (i) bereits die Eindeutigkeit gezeigt haben, folgt in diesem Fall die Eindeutigkeit direkt aus Teil (i).
zurück zur Bemerkung 3.1.28

■

BEWEIS: *(Corollar 3.1.29)*
zurück zum Corollar 3.1.29
Die Aussagen (1)-(8) folgen aus den im Verlaufe des Kapitels bewiesenen Aussagen für $\mathbb{Q}'_p$ (bzw. $\mathbb{Z}'_p$) mit Verwendung des jeweiligen Isomorphismus aus Satz 3.1.27 und den zwei Betragseigenschaften, die kurz vor diesem Corollar genannt wurden.
zurück zum Corollar 3.1.29

■

Beweise zu: 3.2 Lokal-Global-Prinzip:

BEWEIS: *(Satz 3.2.1)*
zurück zum Satz 3.2.1
ohne Beweis. (siehe [1] im Literaturverzeichnis)
zurück zum Satz 3.2.1

■

BEWEIS: *(Corollar 3.2.3)*
zurück zum Corollar 3.2.3
ohne Beweis.
zurück zum Corollar 3.2.3

■

BEWEIS: *(Satz 3.2.4)*
zurück zum Satz 3.2.4
ohne Beweis.
zurück zum Satz 3.2.4

■

Beweise zu: 3.3 Henselsches Lemma:

BEWEIS: *(Lemma 3.3.1)*
zurück zum Lemma 3.3.1
Seien $f \in \mathbb{Z}_p[X]$ und $g_0, h_0 \in \mathbb{Z}_p[X]$, wobei

$$f \equiv g_0 \cdot h_0 \mod p$$

Weiter seien g_0 und h_0 modulo p *teilerfremd*, d.h.

$$ggT\,(g_0 \mod p, h_0 \mod p) = 1$$

und es sei g_0 normiert. Wir definieren:

$$\begin{aligned} d &:= grad\,(f) \\ m &:= grad\,(g_0) \end{aligned}$$

Damit kann der Grad des Polynoms h_0 nicht größer als $d-m$ sein, da ansonsten $grad\,(f) > d$ wäre. Sei daher nun o.B.d.A.

$$grad\,(h_0) \leqslant d-m$$

Wir wollen nun Folgendes zeigen:

$$\exists\, g,h \in \mathbb{Z}_p\,[X]: \quad \begin{cases} (1): & f = g \cdot h \\ (2): & g \text{ ist normiert} \\ (3): & g \equiv g_0 \mod p \\ (4): & h \equiv h_0 \mod p \end{cases}$$

Um die Polynome $g,h \in \mathbb{Z}_p\,[X]$ zu bestimmen, setzten wir

$$\begin{aligned} g &= g_0 + y_1 p + y_2 p^2 + \cdots \\ h &= h_0 + z_1 p + z_2 p^2 + \cdots \end{aligned}$$

wobei $y_i \in \mathbb{Z}_p\,[X]$ $(i = 1,2,\ldots)$ mit $grad\,(y_i) < m$ (denn, ...) und $z_i \in \mathbb{Z}_p\,[X]$ $(i = 1,2,\ldots)$ mit $grad\,(z_i) \leqslant d-m$ (denn, falls $grad\,(z_i) > d-m$ ist, dann ist $grad\,(h) > d-m$ und somit $grad\,(g \cdot h) > d-m+m = d$, aber nach Voraussetzung ist $grad\,(g \cdot h) = grad\,(f) = d$. Damit hätten wir einen Widerspruch).
Da der $grad\,(y_i p^i) < m$ und $grad\,(g_0) = m$ ist, folgt, dass $grad\,(g) = m$ ist. Da g_0 normiert ist, wird damit auch das Polynom g stets normiert sein, d.h. es gilt (2).
Wir bestimmen nun der Reihe nach die Polynome g_n, h_n $(n = 1,2,\ldots)$, die gegeben sind durch

$$\begin{aligned} g_n &:= g_0 + y_1 p + \cdots + y_{n-1} p^{n-1} \qquad \text{mit } g_1 := g_0 \\ h_n &:= h_0 + z_1 p + \cdots + z_{n-1} p^{n-1} \qquad \text{mit } h_1 := h_0 \end{aligned}$$

so dass die folgende Kongruenzbedingung erfüllt ist

$$f \equiv g_n h_n \mod p^n$$

Dass diese Bedingung stets erfüllt ist, zeigen wir durch Induktion über n. Dazu:

$$\boxed{f \equiv g_n h_n \mod p^n} \quad \textit{(Induktionsvoraussetzung)}$$

IA: $n = 1$

z.z.: $\boxed{f \equiv g_1 h_1 \mod p}$ *(Induktionsanfang)*

Nach Definition der g_n's und h_n's gilt:

$$\begin{aligned} g_1 &= g_0 \\ h_1 &= h_0 \end{aligned}$$

Dann ist auch $g_1 h_1 = g_0 h_0$ und damit gilt nach Voraussetzung:

$$f \overset{n.Vor.}{\equiv} g_0 h_0 \mod p \equiv g_1 h_1 \mod p$$

IS: $n \longmapsto n+1$

z.z.: $\boxed{f \equiv g_{n+1} h_{n+1} \mod p^{n+1}}$ *(Induktionsschluß)*

Nach Definition der g_n's und h_n's gilt:

$$\begin{aligned} g_{n+1} &= g_n + y_n p^n \\ h_{n+1} &= h_n + z_n p^n \end{aligned}$$

Durch Multiplikation erhalten wir:

$$g_{n+1} \cdot h_{n+1} = g_n h_n + (g_n z_n + h_n y_n)\, p^n + z_n y_n p^{2n} \qquad (\alpha)$$

Es soll folgendes gelten:

$$\begin{aligned} & f \equiv g_{n+1} h_{n+1} \mod p^{n+1} \overset{(\alpha)}{\equiv} \left(g_n h_n + (g_n z_n + h_n y_n)\, p^n + z_n y_n p^{2n}\right) \mod p^{n+1} \\ \iff\ & f - g_n h_n \equiv (g_n z_n + h_n y_n)\, p^n + z_n y_n p^{2n} \mod p^{n+1} \qquad (\beta) \end{aligned}$$

Da $n \geqslant 2$ ist, gilt weiter:

$$z_n y_n p^{2n} \equiv 0 \mod p^{n+1} \qquad (\gamma)$$

Nach den Rechenregeln für Kongruenzen gilt nun nach Addition von (β) und (γ):

$$\begin{aligned} & f - g_n h_n + z_n y_n p^{2n} \equiv (g_n z_n + h_n y_n)\, p^n + z_n y_n p^{2n} \mod p^{n+1} \\ \iff\ & f - g_n h_n \equiv (g_n z_n + h_n y_n)\, p^n \mod p^{n+1} \end{aligned}$$

Nach Induktionsvoraussetzung gilt:

$$f \equiv g_n h_n \mod p^n \iff f - g_n h_n \equiv 0 \mod p^n$$

Daher definieren wir nun

$$f_n := \frac{1}{p^n}(f - g_n h_n) \implies f - g_n h_n = f_n \cdot p^n$$

Somit erhalten wir mit Hilfe der Divison durch p^n:

$$\begin{aligned} & f_n p^n \equiv (g_n z_n + h_n y_n)\, p^n \mod p^{n+1} \\ \iff\ & f_n \equiv g_n z_n + h_n y_n \mod p \\ \iff\ & f_n \equiv \left(g_0 + \sum_{i=1}^{n-1} y_i p^i\right) z_n + \left(h_0 + \sum_{i=1}^{n-1} z_i p^i\right) y_n \mod p \\ \iff\ & f_n \equiv g_0 z_n + h_0 y_n \mod p \end{aligned}$$

Wegen der Teilerfremdheit von g_0 und h_0 in $\mathbb{F}_p[X]$ gibt es derartige Polynome $z_n, y_n \in \mathbb{Z}_p[X]$. Diese lassen sich mit dem Ansatz $g_0 z_n + h_0 y_n = 1$ und unter Verwendung des Euklidischen Algorithmus konkret bestimmen. Dabei kann y_n auf den kleinsten Rest modulo g_0 reduziert werden, so dass gilt:

$$grad(y_n) < m$$

Da nach Voraussetzung $grad(h_0) \leqslant d - m$ und $grad(f_n) \leqslant d$ sind, gilt

$$grad(g_0 z_n) < d$$

und damit

$$grad(z_n) \leqslant d - m$$

Damit folgt die Behauptung.
zurück zum Lemma 3.3.1

■

BEWEIS: *(Bemerkung 3.3.2)*
zurück zur Bemerkung 3.3.2
ohne Beweis.
zurück zur Bemerkung 3.3.2

■

BEWEIS: *(Corollar 3.3.5)*
zurück zum Corollar 3.3.5
Um zu zeigen, dass $\mathbb{Z}_p$ als Ring und $\mathbb{Q}_p$ als Körper nicht angeordnet sind, müssen wir folgendes zeigen:

$$\exists\, a \in \mathbb{Z}_p \text{ mit } a > 0 \text{ (im Sinne von } \mathbb{Z}) \; \exists\, x \in \mathbb{Z}_p : \quad x^2 = -a$$

Dazu betrachten wir nun zwei Fälle.
1.Fall: $p \in \mathbb{P}\backslash\{2\}$
Wir betrachten das Polynom

$$\mathbb{Z}_p[X] \ni f(X) = X^2 + (p-1) \stackrel{!}{=} 0 \quad \Longleftrightarrow \quad X^2 = -(p-1)$$

Es existieren nun zwei Polynome $\overline{g} := \overline{(X-1)} \in \mathbb{F}_p[X]$ und $\overline{h} := \overline{(X+1)} \in \mathbb{F}_p[X]$ und es gilt:

$$\overline{f(X)} = \overline{X^2 + (p-1)} = \overline{X^2 - 1} = \overline{(X-1)} \cdot \overline{(X+1)} = \overline{g} \cdot \overline{h}$$

Weiter sind $\overline{g}, \overline{h}$ in $\mathbb{F}_p[X]$ teilerfremd (da $p \in \mathbb{P}\backslash\{2\}$). Damit sind die Voraussetzungen des Henselschen Lemmas erfüllt und es garantiert uns eine einfache Nullstelle in $\mathbb{Z}_p$. Damit zerfällt das Polynom $f(X) = X^2 + (p-1)$ über $\mathbb{Z}_p[X]$ in Linearfaktoren (d.h. $f(X)$ ist reduzibel über $\mathbb{Z}_p[X]$). Das Resultat ist also nun:

$$\sqrt{-(p-1)} = \sqrt{1-p} \in \mathbb{Z}_p \subset \mathbb{Q}_p \qquad \forall\, p \in \mathbb{P}\backslash\{2\}$$

und daher gilt

$$\exists\, x \in \mathbb{Z}_p : \quad x^2 = -(p-1) < 0$$

$\Longrightarrow$ $\mathbb{Z}_p$ und $\mathbb{Q}_p$ sind nicht angeordnet $\forall\, p \in \mathbb{P}\backslash\{2\}$.
2.Fall: $p = 2$
In diesem Fall müssen wir uns ein anderes Polynom suchen. Denn, wenn wir analog wie oben vorgehen, so erhalten wir die Polyome $\overline{g} := \overline{(X-1)} \in \mathbb{F}_p[X]$ und $\overline{h} := \overline{(X+1)} \in \mathbb{F}_p[X]$, die in $\mathbb{F}_2[X]$ sicherlich nicht teilerfremd sind. Genauer liegen sie in der selben Restklasse des Polynomrestklassenkörpers $\mathbb{F}_2[X]$ und es gilt daher: $\overline{(X-1)} = \overline{(X+1)}$.
Wir betrachten daher das Polynom

$$\mathbb{Z}_2[X] \ni f(X) = X^2 + 7 \stackrel{!}{=} 0 \quad \Longleftrightarrow \quad X^2 = -7$$

Um zu zeigen, dass ein solches x tatsächlich existiert, müssen wir in die Trickkiste greifen. Wir verwenden das Newton-Verfahren (aus der Analysis und Numerik I zur Berechnung von Nullstellen) mit Startwert $x_0 = 5$.

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \qquad \forall\, n \geqslant 0$$

Die Frage, die man sich vorweg jedoch stellen sollte ist die, ob man dieses Verfahren in diesem Fall überhaupt anwenden darf. Denn die Ableitung $f'(X)$ liegt offensichtlich im maximalen Ideal. Doch das ist nicht weiter tragisch, wenn für den Startwert $x_0 = 5$ der Funktionswert $f(5)$ in einer deutlich höheren Potenz des maximalen Ideals liegt.
Das Newton-Verfahren konvergiert und wir erhalten, dass Resultat

$$\sqrt{-7} \in \mathbb{Z}_2 \subset \mathbb{Q}_2$$

und daher gilt

$$\exists\, x \in \mathbb{Z}_2 : \quad x^2 = -7 < 0$$

$\Longrightarrow$ $\mathbb{Z}_2$ und $\mathbb{Q}_2$ sind nicht angeordnet.
zurück zum Corollar 3.3.5

■

Anhang A: (Konstruktion der p-adischen Zahlen)

DEFINITION A.1: *(Potenzreihe)*
Sei $(a_n)_{n\in\mathbb{N}_0} \subset \mathbb{R}$ (oder: $(a_n)_{n\in\mathbb{N}_0} \subset \mathbb{C}$) eine Zahlenfolge. Weiter sei $x_0 \in \mathbb{R}$ (oder: $x_0 \in \mathbb{C}$). Dann:

$$\sum_{n=0}^{\infty} a_n \, (x - x_0)^n \quad \text{heißt } \textit{Potenzreihe mit Entwicklungspunkt } x_0$$

DEFINITION A.2: *(Laurentreihe)*
Sei $(a_n)_{n\in\mathbb{Z}} \subset \mathbb{R}$ (oder meist: $(a_n)_{n\in\mathbb{Z}} \subset \mathbb{C}$) eine Zahlenfolge. Weiter sei $x_0 \in \mathbb{R}$ (oder meist: $x_0 \in \mathbb{C}$). Dann:

$$\sum_{n=-\infty}^{\infty} a_n \, (x - x_0)^n \quad \text{heißt } \textit{Laurentreihe mit Entwicklungspunkt } x_0$$

DEFINITION A.3: *(Bewertung)*
Sei K ein Körper und $(G, +)$ (oder kurz: G) eine totalgeordnete abelsche Gruppe. Weiter sei $v : K \longrightarrow G \cup \{\infty\}$ surjektiv. Dann:

$$v \text{ heißt } \textit{Bewertung} \quad :\Longleftrightarrow \quad \begin{cases} v(a \cdot b) = v(a) + v(b) & \forall\, a, b \in K \\ v(a) = \infty \iff a = 0 & \\ v(a + b) \geqslant \min\{v(a), v(b)\} & \forall\, a, b \in K \end{cases}$$

Bemerke:
(i): (K, v) (oder kurz: K) heißt in einem solchen Fall *bewerteter Körper*.
(ii): Falls $G = \mathbb{Z}$ ist, so heißt v *diskrete Bewertung* und (K, v) (oder kurz: K) *diskret bewerteter Körper*.
(iii): Jeder Körper besitzt die *triviale Bewertung* v, die gegeben ist durch:

$$v : K \longrightarrow \{0\} \cup \{\infty\} \quad \text{mit} \quad v(x) := \begin{cases} 0 & , x \neq 0 \\ \infty & , x = 0 \end{cases}$$

In diesem Fall ist $G = \{0\}$.

DEFINITION A.4: *(Cauchy-Folge, konvergente Folge, Nullfolge, beschränkte Folge)*
Sei $(x_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ eine Zahlenfolge. Dann:

$(x_n)_{n\in\mathbb{N}}$ heißt *p-adisch konvergent gegen* x $:\Longleftrightarrow$ $\forall\, \varepsilon > 0\, (\varepsilon \in \mathbb{Q})\, \exists\, N \in \mathbb{N}\, \forall\, n > N :\ |x_n - x|_p < \varepsilon$
$(x_n)_{n\in\mathbb{N}}$ heißt *p-adische Nullfolge* $:\Longleftrightarrow$ $(x_n)_{n\in\mathbb{N}}$ ist p-adische konvergent gegen $x = 0$
$(x_n)_{n\in\mathbb{N}}$ heißt *p-adische Cauchy-Folge* $:\Longleftrightarrow$ $\forall\, \varepsilon > 0\, (\varepsilon \in \mathbb{Q})\, \exists\, N \in \mathbb{N}\, \forall\, n, m > N :\ |x_n - x_m|_p < \varepsilon$
$(x_n)_{n\in\mathbb{N}}$ heißt *p-adisch beschränkt* $:\Longleftrightarrow$ $\exists\, K \in \mathbb{Q}\, \forall\, n \in \mathbb{N} :\ |x_n|_p \leqslant K$

Bemerke:

$(x_n)_{n\in\mathbb{N}}$ p-adisch konvergent $\Longrightarrow$ $(x_n)_{n\in\mathbb{N}}$ p-adische Cauchy-Folge $\Longrightarrow$ $(x_n)_{n\in\mathbb{N}}$ p-adisch beschränkt

DEFINITION A.5: *(Ring, Ring mit 1, kommutativer Ring)*
Sei R eine nichtleere Menge. Dann:

$$(R,+,\cdot) \text{ (oder kurz: } R\text{) heißt } \textit{Ring} \quad :\Longleftrightarrow \quad \begin{cases} (R,+) \text{ ist abelsche Gruppe} \\ (R,\cdot) \text{ ist Halbgruppe} \\ a\cdot(b+c) = a\cdot b + a\cdot c \qquad \forall\, a,b,c \in R \\ (a+b)\cdot c = a\cdot c + b\cdot c \qquad \forall\, a,b,c \in R \end{cases}$$

Falls die Verknüpfung $\cdot$ zusätzlich kommutativ in R ist, so heißt R *kommutativer Ring* oder falls R zusätzlich das neutrale Einselement für die Verknüpfung $\cdot$ enthält, so heißt R *Ring mit 1* (oder auch *Ring mit Einselement*). Ein kommutativer Ring mit Einselement, der zu jedem Element genau ein multiplikatives Inverselement enthält, heißt *Körper*. Mit anderen Worten ist in diesem Fall $(R,\cdot)$ eine abelsche Gruppe.

DEFINITION A.6: *(Ideal, maximales Ideal, echtes Ideal, Hauptideal)*
Sei R ein kommutativer Ring. Weiter sei $\emptyset \neq I \subset R$. Dann:

$$I \text{ heißt } \textit{Ideal von } R \quad :\Longleftrightarrow \quad \begin{cases} 0 \in I \\ \forall\, a,b \in I: \quad a-b \in I \\ \forall\, r \in R \;\wedge\; \forall\, a \in I: \quad r\cdot a \in I \end{cases}$$

$$I \text{ heißt } \textit{maximales Ideal von } R \quad :\Longleftrightarrow \quad \begin{cases} I \text{ Ideal von } R \\ \text{und} \\ \forall\, J \subset R \text{ Ideal von } R \text{ mit } J \neq R \text{ und } I \subset J: \quad I = J \end{cases}$$

$$I \text{ heißt } \textit{echtes Ideal von } R \quad :\Longleftrightarrow \quad \begin{cases} I \text{ Ideal von } R \\ \text{und} \\ I \neq R \end{cases}$$

$$I \text{ heißt } \textit{Hauptideal von } R \quad :\Longleftrightarrow \quad \exists\, a \in R: \quad I = (a) = \{r\cdot a \mid r \in R\}$$

$$I \text{ heißt } \textit{Primideal von } R \quad :\Longleftrightarrow \quad \forall\, a,b \in R \text{ mit } a\cdot b \in I: \quad a \in I \;\vee\; b \in I$$

Bemerke:

$$I \text{ maximales Ideal} \quad \Longrightarrow \quad I \text{ Primideal}$$

DEFINITION A.7: *(Faktorring, Restklassenring)*
Sei R ein kommutativer Ring und sei $I \subset R$ ein Ideal von R. Weiter sei

$$R/I := \{a+I \mid a \in R\} \text{ heißt } \textit{Menge der Äquivalenzklassen} \text{ (}\textit{Restklassen}\text{)}$$
$$(a+I)+(b+I) := (a+c)+I \qquad \forall (a+I),(b+I) \in R/I$$
$$(a+I)\cdot(b+I) := (a\cdot b)+I \qquad \forall (a+I),(b+I) \in R/I$$

Dann ist $(R/I,+,\cdot)$ ein kommutativer Ring mit dem Nullelement I und dem Einselement $1+I$. Dieser Ring $(R/I,+,\cdot)$ heißt *Faktorring* (oder auch: *Restklassenring*).
Bemerke:
Sei $I \subset R$ ein maximales Ideal von R, dann gilt:

$$(R/I,+,\cdot) \text{ ist ein Körper}$$

DEFINITION A.8: *(Unterring)*
Sei R ein kommutativer Ring mit Einselement $1 \neq 0$. Weiter sei $\emptyset \neq R' \subset R$. Dann:

$$R' \text{ heißt } \textit{Unterring von } R \quad :\Longleftrightarrow \quad (R', +, \cdot) \text{ ist Ring}$$

Beachte, dass die Addition $+$ und die Multiplikation $\cdot$ mit der von R übereinstimmen. Die Definitionsbereiche der Verknüpfungen werden in $(R', +, \cdot)$ beide lediglich eingeschränkt auf $R' \times R'$.

DEFINITION A.9: *(Einheit, Menge der Einheiten, Nicht-Einheit)*
Sei R ein kommutativer Ring. Dann:

$$a \in R \text{ heißt } \textit{Einheit in } R \quad :\Longleftrightarrow \quad \exists\, b \in R: \quad a \cdot b = b \cdot a = 1$$
$$R^* := E(R) := \{a \in R \mid \exists\, b \in R:\ a \cdot b = b \cdot a = 1\} \text{heißt } \textit{Menge der Einheiten von } R$$

Bemerke:
Existiert kein solches $b \in R$, so nennt man $a \in R$ eine *Nicht-Einheit*.

DEFINITION A.10: *(Lokaler Ring)*
Sei R ein Ring. Dann:

$$R \text{ heißt } \textit{lokaler Ring} \quad :\Longleftrightarrow \quad \exists_1\, I \subset R \text{ Ideal von } R: \quad I \text{ ist maximales Ideal}$$

DEFINITION A.11: *(Hauptidealring)*
Sei R ein kommutativer Ring. Dann:

$$R \text{ heißt } \textit{Hauptidealring} \text{ (oder kurz: } \textit{HIR}) \quad :\Longleftrightarrow \quad \forall\, I \subset R \text{ Ideal von } R: \quad I \text{ ist Hauptideal}$$

DEFINITION A.12: *(Nullteiler, nullteilerfrei, Integritätsring)*
Sei R ein kommutativer Ring. Dann:

$$a \in R\backslash\{0\} \text{ heißt } \textit{Nullteiler in } R \quad :\Longleftrightarrow \quad \exists\, b \in R\backslash\{0\}: \quad a \cdot b = 0$$

Ein Ring der keinen Nullteiler besitzt heißt *nullteilerfrei* (oder auch: *Integritätsring*).

DEFINITION A.13: *(Bewertungsring, diskreter Bewertungsring)*
(i): Sei K ein Körper und v eine Bewertung von K. Dann:

$$B := \{x \in K \mid v(x) \geqslant 0\} \text{ heißt } \textit{Bewertungsring von } v \textit{ in } K$$

Bemerke:
Falls v eine diskrete Bewertung ist, so heißt B *diskreter Bewertungsring*. Bewertungsringe sind Unterringe

von Körpern.
(ii): Sei B ein nullteilerfreier kommutativer Ring. Dann:

$$B \text{ heißt } \textit{Bewertungsring} \quad :\Longleftrightarrow \quad \forall\, x,y \in B : \begin{cases} \exists\, a \in B : & y = a \cdot x \\ \text{oder} & \\ \exists\, b \in B : & x = b \cdot y \end{cases}$$

$$:\Longleftrightarrow \quad \forall\, x \in Q(B) := \{\frac{a}{b} \mid a,b \in A \ \wedge\ b \neq 0\} : \begin{cases} x \in B \\ \text{oder} \\ x^{-1} \in B \end{cases}$$

Bemerke:

$$B \text{ Bewertungsring} \quad \Longrightarrow \quad B \text{ lokaler Ring}$$

DEFINITION A.14: *(Charakteristik)*
Sei R ein kommutativer Ring. Dann:

$$Char(R) = n \in \mathbb{N} \quad :\Longleftrightarrow \quad \begin{cases} n \cdot 1 \ = \ 0 \\ \forall\, k < n : \quad k \cdot 1 \ \neq \ 0 \end{cases}$$

d.h. R hat die *Charakteristik n*. Genauer:

$$n \ := \ \min\{k \in \mathbb{N} \mid k \cdot 1 = 0\}$$

Bemerke:
Eine solche Zahl muss nicht notwendig existieren. Falls eine derartige Zahl n nicht existiert, so hat der Ring definitionsgemäß die *Charakteristik 0*.
Es gilt zudem:

$$R \text{ Integritätsring} \quad \Longrightarrow \quad Char(R) \in \mathbb{P}$$

DEFINITION A.15: *(dicht)*
Sei (X,T) ein metrischer Raum (oder ein topologischer Raum). Dann:

$$\begin{aligned} M \subset X \textit{ liegt dicht in } X \quad &:\Longleftrightarrow \quad \overline{M} = X \text{ (d.h. der Abschluss von } M \text{ bzgl. } T \text{ stimmt mit } X \text{ überein)} \\ &:\Longleftrightarrow \quad \forall\, A \subset X \text{ abgeschlossen mit } M \subset A : \quad A = X \\ &:\Longleftrightarrow \quad \forall\, B_\varepsilon(x) \text{ mit } x \in X\ \exists\, y \in M : \quad y \in B_\varepsilon(x) \end{aligned}$$

DEFINITION A.16: *(abzählbar, überabzählbar)*
Sei M eine nichtleere Menge. Dann:

$$\begin{aligned} M \text{ heißt } \textit{abzählbar} \quad &:\Longleftrightarrow \quad \exists\, f : \mathbb{N} \longrightarrow M \text{ surjektiv} \\ &:\Longleftrightarrow \quad \exists\, (x_n)_{n\in\mathbb{N}} \subset M \text{ Folge} : \quad M = \{x_n \mid n \in \mathbb{N}\} \end{aligned}$$

$$M \text{ heißt } \textit{überabzählbar} \quad :\Longleftrightarrow \quad M \text{ ist nicht abzählbar}$$

Bemerke:
Die leere Menge ist definitionsgemäß abzählbar.

Anhang B: (Lokal-Global-Prinzip)

DEFINITION B.1: *(Kongruenzgleichung)*
Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann stellt

$$a \equiv b \mod n$$

eine *Kongruenzgleichung* dar. Dabei definiert man

$$a \equiv b \mod n \quad :\Longleftrightarrow \quad n \mid (b-a)$$

Falls $a \equiv b \mod n$ gilt, so sagt man, dass *a kongruent zu b modulo n* ist.

SATZ B.2: *(Kongruenzrechenregeln auf $\mathbb{Z}$)*
Seien $a \equiv b \mod n$ und $c \equiv d \mod n$. Dann gilt:

(i) $a + c \equiv b + d \mod n$

(ii) $a \cdot c \equiv b \cdot d \mod n$

(iii) $a^m \equiv b^m \mod n$

SATZ B.3: *(Chinesischer Restsatz)*
Seien $m_1, \ldots, m_n \in \mathbb{N}\backslash\{1\}$ paarweise teilerfremd und $a_1, \ldots, a_n \in \mathbb{Z}$. Dann gilt:
Das Kongruenzsystem

$$\begin{array}{rcll} x & \equiv & a_1 & \mod m_1 \\ x & \equiv & a_2 & \mod m_2 \\ \vdots & \vdots & \vdots & \vdots \quad \vdots \\ x & \equiv & a_n & \mod m_n \end{array}$$

ist eindeutig lösbar und die Lösungsmenge ist eine Restklasse modulo $m_1 \cdot \cdots \cdot m_n$.

DEFINITION B.4: *(Quadratische Form, Quadrik)*
Sei $A \in \mathbb{R}^{n \times n}$ symmetrisch. Dann:

$$q : \mathbb{R}^n \longrightarrow \mathbb{R} \quad \text{mit} \quad x \to q(x) := x^T \cdot A \cdot x = \sum_{i,j=1}^{n} a_{ij} \cdot x_i \cdot x_j$$

heißt *quadratische Form* (oder: *Quadrik*)
Bemerke:
Quadratische Formen (oder: Quadriken) bezeichnen somit spezielle Polynomfunktionen zweiten Grades mit mehreren Veränderlichen. In Abhängigkeit von der Anzahl der Variablen beschreibt die Funktion q eine Kurve ($n = 2$), eine Fläche ($n = 3$) oder sogar eine Hyperfläche ($n \geqslant 4$). Speziell für das Lokal-Global-Prinzip betrachte man $\mathbb{Q}$ an Stelle von $\mathbb{R}$ (d.h. $A \in \mathbb{Q}^{n \times n}$ und $q : \mathbb{Q}^n \longrightarrow \mathbb{Q}$), da dort rationale Koeffizienten gefordert werden.

Anhang C: (Henselsches Lemma)

DEFINITION C.1: *(Henselscher Ring)*
Sei R ein Ring und $I \subset R$ ein maximales Ideal von R. Dann:

R heißt *Henselscher Ring bzgl.* I $\quad :\Longleftrightarrow \quad$ Henselsches Lemma gilt bzgl. der Reduktion $\kappa = R/I$

DEFINITION C.2: *(henselsch)*
Sei K ein bewerteter Körper und sei R ein bewerteter Ring. Dann:

K heißt *henselsch* $\quad :\Longleftrightarrow \quad$ Henselsches Lemma ist in K anwendbar
R heißt *henselsch* $\quad :\Longleftrightarrow \quad$ Henselsches Lemma ist in R anwendbar

DEFINITION C.3: *(Restklassenkörper modulo p)*
Sei $p \in \mathbb{P}$ eine beliebige aber feste Primzahl, so ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper (genauer ein endlicher Körper mit p Elementen). Dann:

$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p/p\mathbb{Z}_p$ heißt *Restklassenkörper modulo p*

Anhang D: (Eigenschaften der p-adischen Zahlen)

SATZ D.1:

(i) $\mathbb{Q}_p$ ist überabzählbar

(ii) $\mathbb{Q} \subset \mathbb{Q}_p \quad \forall\, p \in \mathbb{P}$

(iii) $\mathbb{Q}_p$ ist nicht angeordnet

(iv) $\mathbb{Z}_p$ ist kompakt

(v) $\mathbb{Q}_p$ ist lokal kompakt

(vi) $\mathbb{Z}_p$ ist (als metrischer Raum) vollständig

(vii) $\mathbb{Q}_p$ ist (als metrischer Raum) vollständig

(viii) $\mathbb{Z}_p$ ist ein lokaler Ring, sogar ein diskreter Bewertungsring

(ix) $\mathbb{Z}_p$ ist ein Hauptidealring

(x) $\mathbb{Z}_p$ ist nullteilerfrei, also ein Integritätsring

(xi) $\mathbb{Q}_p$ hat Charakteristik 0, also $char\,(\mathbb{Q}_p) = 0$

Literatur

[1] NEUKIRCH, J.: *Algebraische Zahlentheorie*, Springer Verlag, 1992

[2] COHN, P.M.: *Basic Algebra*, Springer Verlag, 1992, London

[3] GRUNDHÖFER, T.: *The classical fields*, noch nicht erschienen

[4] WIKIPEDIA: *www.wikipedia.de*

[5] BAKER, A.J..: *An Introduction to p-adic Numbers and p-adic Analysis*, University of Glasgow, Internetskript

[6] TÖRNER, G.: *Bewertungsringe*, 1978, Internetskript

[7] HOLZ, M.: *Repetitorium der Algebra*, Binomi Verlag, 2004, Hannover, 1.Auflage

[8] KERSTEN, I.: *Algebra-Arbeitsversion*, Internetskript

[9] FORSTER, O.: *Analysis 1-Differential- und Integralrechnung einer Veränderlichen*, Vieweg Verlag, 2001, 6.Auflage

[10] FORSTER, O.: *Analysis 2-Differentialrechnung im $\mathbb{R}^n$, gewöhnliche Differentialgleichungen*, Vieweg Verlag, 1999, 5.Auflage

Index

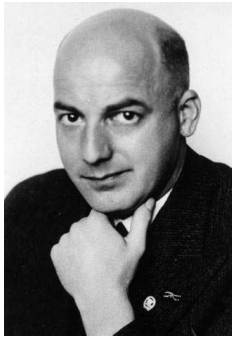
Namens- und Sachverzeichnis

Symbolverzeichnis

$\mathbb{Q}_p$	Menge der p-adischen Zahlen
$\mathbb{Q}'_p$	Faktorring R/I, Menge der p-adischen Zahlen (2. Variante)
$\mathbb{Z}_p$	Menge der ganzen p-adischen Zahlen
$\mathbb{Z}'_p$	Menge der ganzen p-adische Zahlen (2. Variante)
$\mathbb{Z}'^*_p$	Menge der Einheiten von $\mathbb{Z}'_p$
$\lvert x\rvert_p$	p-adischer Betrag auf $\mathbb{Q}$, p-adische Norm auf $\mathbb{Q}$
$\lvert x\rvert'_p$	p-adischer Betrag auf $\mathbb{Q}'_p$, p-adische Norm auf $\mathbb{Q}'_p$
$v_p(x)$	p-adische Bewertung auf $\mathbb{Q}$
$v'_p(x)$	p-adische Bewertung auf $\mathbb{Q}'_p$
$d_p(x)$	p-adische Metrik auf $\mathbb{Q}$
$d'_p(x)$	p-adische Metrik auf $\mathbb{Q}'_p$
$\mathbb{F}_p$	Restklassenkörper modulo p, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p/p\mathbb{Z}_p$

Personenverzeichnis

Helmut Hasse (geb. 25.08.1898 in Kassel; gest. 26.12.1979 in Ahrensberg bei Hamburg) war als Ma-



thematiker einer der führenden *Algebraiker* und *Zahlentheoretiker* seiner Zeit. Nach ihm benannt sind die *Hasse-Diagramme*. Weiter hört man seinen Namen gemeinsam mit dem von Hermann Minkowski im Zusammenhang mit den *p-adischen Zahlen*. Sie entwickelten dort ein Prinzip für die Teilbarkeit von p-adischen Zahlen, dass sogenannte *Lokal-Global-Prinzip* von Hasse-Minkowski.

Kurt Hensel (geb. 29.12.1861 in Königsberg; gest. 01.06.1941 in Marburg) war ein deutscher Mathe-

matiker. Er war an der Universität Berlin Schüler von *Leopold Kronecker*, der ihn förderte und bei dem er promovierte. Nachdem er im Anschluss ein freiwilliges Jahr zum Militär ging, habilitierte er wiederum bei Kronecker (1886). 1897 führte er das *Konzept der p-adischen Zahlen* in der *Zahlentheorie* ein. Nach ihm benannt sind das *Henselsche Lemma*, der *Henselsche Ring* sowie die Eigenschaft *henselsch*.

Hermann Minkwoski (geb. 22.06.1864 in Aleksotas (damals Russland, heute Kaunas/Litauen); gest.

12.01.1909 in Göttingen) war ein deutscher Mathematiker und Physiker. Er war befreundet mit *Adolf Hurwitz* und *David Hilbert*. Im Alter von 44 Jahren erlitt Minkowski an einem Blinddarmbruch. Zu dieser Zeit waren operative Eingriffe zur Heilung von Krankheiten noch nicht üblich und sein Tod absehbar. Nach ihm benannt sind das *Minkowski-Diagramm*, die *Minkowski-Dimension*, das *Minkowski-Funktional*, der *Minkowski-Gitterpunktsatz*, die *Minkowski-Metrik* sowie die *Minkowski-Ungleichung*. Unter anderem hört man seinen Namen auch im Zusammenhang mit dem *Lokal-Global-Prinzip* von Hasse-Minkowski.