Skript zur Vorlesung

# Nicht-archimedische Zahlen

**Wintersemester 2012/13**
**Frankfurt am Main**

**Prof. Dr. Annette Werner**

# Inhaltsverzeichnis

# 1 Einleitung

In dieser Vorlesung werden wir neue Zahlbereiche kennenlernen, die den Raum der rationalen Zahlen erweitern. Aus der Analysis ist der Erweiterungskörper $\mathbb{R}$ der reellen Zahlen $\mathbb{Q}$ bekannt. Die reellen Zahlen sind vollständig bezüglich des gewöhnlichen Absolutbetrages, d.h. jede Cauchyfolge hat einen Grenzwert in $\mathbb{R}$. Mehr noch, $\mathbb{R}$ ist der kleinste Erweiterungskörper von $\mathbb{Q}$, der vollständig ist. Daher nennt man $\mathbb{R}$ auch Komplettierung von $\mathbb{Q}$ bezüglich des gewöhnlichen Absolutbetrages.

Nun trägt $\mathbb{Q}$ aber auch andere interessante Beträge.

Sei $p$ eine Primzahl. Für jede ganze Zahl $m$ definieren wir $v_p(m)$ als den Exponenten von $p$ in der Primfaktorzerlegung von $m$, d.h. es gilt

$$m = p^{v_p(m)} n$$

für eine ganze Zahl $n$, die teilerfremd zu $p$ ist.

**Definition 1.1.** *Der $p-$adische Absolutbetrag auf $\mathbb{Q}$ ist folgendermaßen definiert: Für $m, n \in \mathbb{Z}$ mit $n \neq 0$ sei*

$$\left|\frac{m}{n}\right|_p = \begin{cases} 0 & m = 0 \\ p^{-v_p(m)+v_p(n)} & m \neq 0 \end{cases}$$

**Beispiel:** Für $p = 3$ ist $|1|_3 = 1, |2|_3 = 1, |3|_3 = \frac{1}{3}$.

Außerdem ist $|3^n|_3 = \frac{1}{3^n}$, das heißt, die Folge $(3^n)_{n\geqq 1}$ ist eine Nullfolge bezüglich $|\cdot|_3$.

Für jede Primzahl $p$ ist

$$|m|_p = p^{-v_p(m)} \leqq 1$$

für alle ganzen Zahlen $m$. Die ganzen Zahlen sind also im $p-$adischen Einheitsball enthalten!

Das verletzt das sogenannte Archimedische Prinzip:

**Definition 1.2.** *Ein Betrag $|\cdot|$ auf einem Körper $K$ heißt archimedisch, falls für alle $x, y \in K$ mit $x \neq 0$ eine positive natürliche Zahl $n$ existiert mit $|nx| > |y|$.*

Hier ist $nx = \underbrace{x + x + \ldots + x}_{n-\text{mal}} \in K$.

Der reelle Absolutbetrag auf $\mathbb{R}$ ist offenbar archimedisch, der $p-$adische Absolutbetrag $|\cdot|_p$ auf $\mathbb{Q}$ allerdings nicht! Betrachten wir nämlich $x = p$ und $y$ teilerfremd zu $p$, so gilt

$$|nx|_p = |np|_p = |n|_p \, |p|_p \leqq |p|_p = \frac{1}{p},$$

aber $|y|_p = 1$.

In dieser Vorlesung wollen wir Zahlbereiche untersuchen, die mit Beträgen ausgestattet sind, die nicht-archimedisch sind — das sind die nicht-archimedischen Zahlen aus dem Titel der Vorlesung.

# 2 Nicht-archimedische Absolutbeträge

Wir beginnen mit ein paar Grundbegriffen über Absolutbeträge.

**Definition 2.1.** *Es sei $K$ ein Körper. Ein Absolutbetrag auf $K$ ist eine Funktion*

$$|\cdot| : K \to \mathbb{R}_{\geqq 0} = \{x \in \mathbb{R} : x \geqq 0\}$$

*mit folgenden Eigenschaften:*

*i)* $|x| = 0$ *genau dann, wenn* $x = 0$

*ii)* $|xy| = |x|\,|y|$ *für alle* $x, y \in K$

*iii) Dreiecksgleichung:* $|x + y| \leqq |x| + |y|$ *für alle* $x, y \in K$.

**Beispiel:**

1. Jeder Körper kann mit dem trivialen Absolutbetrag ausgestattet werden. Dieser ist definiert als:
$$|x| = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0. \end{cases}$$
2. $\mathbb{Q}$ und $\mathbb{R}$ tragen den gewöhnlichen reellen Absolutbetrag
$$|x| = \begin{cases} x, & x \geqq 0 \\ -x, & x < 0. \end{cases}$$
3. $\mathbb{Q}$ kann außerdem für jede Primzahl $p$ mit dem $p-$adischen Absolutbetrag $|\cdot|_p$ aus Definition 1.1 versehen werden.

**Lemma 2.2.** *Sei $|\cdot|$ ein Absolutbetrag auf einem Körper $K$. Dann gilt*

*i)* $|1| = 1$.

*ii) Für jedes* $x \in K$ *mit* $|x^n| = 1$ *ist auch* $|x| = 1$.

*iii) Für jedes* $x \in K$ *ist* $|-x| = |x|$.

*iv) Ist $K$ ein endlicher Körper, so ist der triviale Absolutbetrag der einzige Betrag auf $K$.*

**Beweis :**

i) Es ist $|1| = |1 \cdot 1| = |1| \cdot |1| = |1|^2$. Da $|1| \neq 0$ ist, folgt $|1| = 1$.

ii) Aus $|x^n| = 1$ folgt $|x|^n = 1$, also ist $|x|$ eine positive reelle Zahl mit $|x|^n = 1$. Daraus folgt $|x| = 1$.

iii) Es ist $|-1| = |(-1)^3| = |-1|^3$, also ist $|-1| = 1$ nach ii). Daraus folgt $|-x| = |(-1)x| = |-1|\ |x| = |x|$.

iv) Übungsaufgabe (Tipp: Betrachte den Frobenius)

□

Für jeden Körper $K$ haben wir eine Abbildung $\varphi : \mathbb{Z} \to K$, die folgendermaßen definiert ist:

$$n \mapsto \begin{cases} \underbrace{1+1+\ldots+1}_{n-\text{mal}} & n > 0 \\ 0 & n = 0 \\ \underbrace{-(1+1+\ldots+1)}_{(-n)-\text{mal}} & n < 0. \end{cases}$$

$\varphi$ ist offenbar ein Gruppenhomomorphismus von $\mathbb{Z}$ in die additive Gruppe von $K$. Falls $\varphi$ injektiv ist, so setzen wir char $K = 0$ und sagen, $K$ hat Charakteristik 0. Falls $\varphi$ nicht injektiv ist, so ist char $K$ die kleinste positive ganze Zahl mit $\varphi(\text{char } K) = 0$. Man kann leicht zeigen, dass dann char $K$ eine Primzahl ist, denn $K$ ist nullteilerfrei.

**Proposition 2.3.** *Ein Absolutbetrag $|\cdot|$ auf $K$ ist genau dann nicht-archimedisch, wenn*

$$|\varphi(n)| \leqq 1$$

*für alle $n \in \mathbb{Z}$ gilt.*

**Beweis :** „$\Rightarrow$“ Ist $|\cdot|$ nicht-archimedisch, so existieren $x, y \in K$ mit $x \neq 0$ und $\underbrace{|x+\ldots+x|}_{n-\text{mal}} = |nx| \leqq |y|$ für alle positiven ganzen Zahlen $n$. Aus $nx = \varphi(n) \cdot x$ folgt daraus

$$|\varphi(n)| \leqq \left|\frac{y}{x}\right|.$$

für alle $n$. Angenommen, es existiert ein $n$ mit $|\varphi(n)| > 1$. Dann wächst

$$\left|\varphi(n^k)\right| \overset{\text{ÜA}}{=} \left|\varphi(n)^k\right| = |\varphi(n)|^k$$

für $k \to \infty$ über alle Grenzen, im Widerspruch zu $\left|\varphi(n^k)\right| \leqq \left|\frac{y}{x}\right|$. Also folgt die Behauptung.

„$\Leftarrow$“: Ist $|\varphi(n)| \leqq 1$ für alle $n \in \mathbb{Z}$, so gilt für $x = 1, y = 1$ trivialerweise

$$|nx| = |\varphi(n)| \leqq 1 = |y|,$$

also ist der Betrag nicht-archimedisch. □

Betrachten wir den $p-$adischen Absolutbetrag $|\cdot|_p$ genauer, so stellen wir fest, dass hierfür eine verschärfte Version der Dreiecksungleichung gilt.

**Lemma 2.4.** *Für alle $r, s \in \mathbb{Q}$ gilt*

$$|r+s|_p \leqq max\{|r|_p, |s|_p\}.$$

**Beweis :** Wir schreiben $r = p^a \frac{r_1}{r_2}$ und $s = p^b \frac{s_1}{s_2}$ mit $a, b \in \mathbb{Z}$ und zu $p$ teilerfremden Zahlen $r_1, r_2, s_1, s_2$. Dazu klammern wir aus Zähler und Nenner den $p-$Anteil der Primfaktorzerlegung aus.

Wir nehmen ohne Einschränkung $a \leqq b$ an. Dann ist

$$\begin{aligned} r+s &= p^a \tfrac{r_1}{r_2} + p^b \tfrac{s_1}{s_2} \\ &= p^a \left( \tfrac{s_2 r_1 + p^{b-a} s_1 r_2}{r_1 s_2} \right). \end{aligned}$$

Der Nenner $r_1 s_2$ ist eine zu $p$ teilerfremde ganze Zahl und $v_p(s_2 r_1 + p^{b-a} s_1 r_2) \geqq 0$, also folgt

$$|r+s|_p \leqq p^{-a} = \max\{p^{-a}, p^{-b}\} = \max\{|r|_p, |s|_p\}.$$

□

**Definition 2.5.** *Ein Betrag $|\cdot|$ auf einem Körper $K$ erfüllt die nicht-archimedische Dreiecksungleichung (auch starke Dreiecksungleichung oder ultrametrische Dreiecksungleichung genannt), falls für alle $x, y \in K$ gilt*

$$|x+y| \leqq \ max\{|x|, |y|\}.$$

**Satz 2.6.** *Ein Betrag $|\cdot|$ auf $K$ ist genau dann nicht-archimedisch, wenn er die nicht-archimedische Dreiecksungleichung erfüllt.*

**Beweis :** Falls $|\cdot|$ die nicht-archimedische Dreiecksungleichung erfüllt, so kann man leicht mit Induktion zeigen, dass $|\varphi(n)| = |\underbrace{1+1+\ldots+1}_{n-\text{mal}}| \leqq 1$ für alle $n \in \mathbb{N}$ gilt.

Also ist $|\cdot|$ nach Proposition 2.3 nicht-archimedisch. Ist umgekehrt $|\cdot|$ ein nicht-archimedischer Betrag, so gilt nach Proposition 2.3

$$|\varphi(n)| \leqq 1$$

für alle $n \in \mathbb{Z}$. Gegeben seien $x, y \in K$. Wir wollen $|x+y| \leqq \max\{|x|, |y|\}$ zeigen. Dafür können wir $y \neq 0$ annehmen. Dann genügt es

$$|x+1| \leqq \max\{|x|, 1\}$$

für alle $x \in K$ zu zeigen, denn daraus folgt

$$\begin{aligned} |x+y| &= |y| \left| \tfrac{x}{y} + 1 \right| \\ &\leqq |y| \max\{\left| \tfrac{x}{y} \right|, 1\} \\ &\leqq \max\{|x|, |y|\}, \end{aligned}$$

also die gewünschte nicht-archimedische Dreiecksungleichung.

Für jede positive ganze Zahl $m$ gilt

$$(x+1)^m = \sum_{k=0}^{m} \binom{m}{k} x^k.$$

Nach Voraussetzung gilt $\left|\varphi\left(\binom{m}{k}\right)\right| \leqq 1$, also folgt

$$\begin{aligned} |x+1|^m &= \left| \sum_{k=0}^{m} \tbinom{m}{k} x^k \right| \\ &\leqq \sum_{k=0}^{m} \left| \tbinom{m}{k} x^k \right| \\ &= \sum_{k=0}^{m} \left|\varphi\left(\tbinom{m}{k}\right)\right| |x|^k \\ &\leqq \sum_{k=0}^{m} |x|^k \\ &\leqq (m+1) \max\{1, |x|^m\}, \end{aligned}$$

denn für $|x| > 1$ ist $|x|^k \leqq |x|^m$ für $0 \leq k \leq m$ und für $|x| \leqq 1$ ist $|x|^k \leqq 1$ für $0 \leqq k \leqq m$.

Wir nehmen die $m-$te Wurzel der nicht-negativen reellen Zahlen auf beiden Seiten und erhalten

$$|x+1| \leqq \sqrt[m]{m+1}\max\{1,|x|\}.$$

Nun gilt $\sqrt[m]{m+1} \to 1$ für $m \to \infty$, also folgt in der Tat $|x+1| \leqq \max\{1,|x|\}$. □

**Satz 2.7.** *Es sei $|\cdot|$ ein nicht-archimedischer Betrag auf $K$. Für $x, y \in K$ mit $|x| \neq |y|$ gilt*

$$|x+y| = max\{|x|, |y|\}.$$

**Beweis :** Wir können $|x| < |y|$ annehmen. Nach der nicht-archimedischen Dreiecksungleichung gilt

$$|y| = |(x+y)-x| \leqq max\{|x+y|, |x|\}.$$

Da $|x| < |y|$ ist, wird das Maximum in $|x+y|$ angenommen, und es gilt $|y| \leqq |x+y|$. Daraus folgt

$$|y| = max\{|x|, |y|\} \leqq |x+y|.$$

Da nach der nicht-archimedischen Dreiecksungleichung

$$|x+y| \leqq max\{|x|, |y|\} = |y|$$

ist, folgt die Behauptung. □

Wir zeigen jetzt noch, dass jeder nicht-archimedische Betrag von einer Bewertung kommt.

**Erinnerung:** Ein Integritätsring ist ein Ring ohne Nullteiler. Dabei heißt ein Element $a \neq 0$ in einem Ring $A$ ein Nullteiler, falls es ein $b \neq 0$ in $A$ gibt mit $ab = 0$. Für jeden Integritätsring $A$ existiert der Quotientenkörper Quot $A = \{\frac{x}{y} : x, y \in A, y \neq 0\}$ mit den üblichen Rechenregeln.

**Definition 2.8.** *Sei $A$ ein Integritätsring. Eine Bewertung auf $A$ ist eine Abbildung*

$$v : A\backslash\{0\} \to \mathbb{R},$$

*so dass gilt*

*B1)* $v(xy) = v(x) + v(y)$
*B2)* $v(x+y) \geqq \min\{v(x), v(y)\}$.

Durch $v\left(\frac{x}{y}\right) = v(x) - v(y)$ kann man jede Bewertung auf $A$ zu einer Bewertung auf dem Quotientenkörper Quot $A$ fortsetzen.

**Beispiel:**

$$\begin{array}{rcl} v_p : \mathbb{Z}\backslash\{0\} & \to & \mathbb{R} \\ m & \mapsto & v_p(m) \end{array}$$

ist eine Bewertung auf $\mathbb{Z}$.

Durch $v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n)$ kann man sie zu einer Bewertung auf $\mathbb{Q}\backslash\{0\}$ fortsetzen.

**Lemma 2.9.** *Es sei $K$ ein Körper und $v : K\backslash\{0\} \to \mathbb{R}$ eine Bewertung von $K$. Sei $e$ die Eulersche Zahl. Dann ist*

$$|x| := \begin{cases} 0 & , x = 0 \\ e^{-v(x)} & , x \neq 0 \end{cases}$$

*ein nicht-archimedischer Betrag auf $K$.*

**Beweis :** Wir prüfen die Eigenschaften aus Definition 2.1 nach, wobei wir die Dreiecksungleichung durch die nicht-archimedische Dreiecksungleichung ersetzen.

i) Offenbar ist $e^{-v(x)} \neq 0$ für alle $x \in K\backslash\{0\}$, also ist $|x| = 0$ genau dann, wenn $x = 0$.

ii) Ist $x = 0$ oder $y = 0$, so gilt offenbar $|xy| = |x|\,|y|$. Sind $x$ und $y$ von Null verschieden, so folgt

$$|xy| = e^{-v(xy)} = e^{-v(x)-v(y)}$$

nach Eigenschaft B1) aus Definition 2.8. Also folgt

$$|xy| = e^{-v(x)}e^{-v(y)} = |x|\,|y|\,.$$

iii) Nach Eigenschaft B2) aus Definition 2.8 gilt für $x \neq 0$ und $y \neq 0$ :

$$|x+y| = e^{-v(x+y)} \leqq e^{\max\{-v(x),-v(y)\}} = \max\{e^{-v(x)}, e^{-v(y)}\} = \max\{|x|\,, |y|\}.$$

Hier haben wir benutzt, dass aus

$$\begin{array}{rcl} v(x+y) & \geqq & \min\{v(x), v(y)\} \text{ die Abschätzung} \\ -v(x+y) & \leqq & -\min\{v(x), v(y)\} \\ & = & \max\{-v(x), -v(y)\} \text{ folgt} \end{array}$$

und dass die Exponentialfunktion monoton wächst. □

Jede Bewertung liefert also einen nicht-archimedischen Betrag. Umgekehrt zeigen wir jetzt, dass jeder nicht-archimedische Betrag von einer Bewertung induziert wird.

**Satz 2.10.** *Es sei $|\cdot|$ ein nicht-archimedischer Betrag auf $K$. Dann ist die Funktion*

$$\begin{array}{rcl} v : K\backslash\{0\} & \to & \mathbb{R} \\ x & \mapsto & -\log|x| \end{array}$$

*eine Bewertung auf $K$.*

**Beweis :** Die Multiplikativität des Betrages liefert die Eigenschaft B1) aus Definition 2.8. Ferner liefert die nicht-archimedische Dreiecksungleichung zusammen mit der Monotonie des Logarithmus

$$\log|x+y| \leqq \max\{\log|x|\,, \log|y|\},$$

also auch

$$\begin{array}{rcl} -\log|x+y| & \leqq & -\max\{\log|x|\,, \log|y|\} \\ & = & \min\{-\log|x|\,, -\log|y|\} \end{array}$$

und daher Eigenschaft B2). □

Offenbar (Übungsaufgabe) sind die Zuordnungen aus Lemma 2.9 und Satz 2.10 invers zueinander.

# 3 Bälle und Topologie

Sei $K$ ein Körper mit einem nicht-archimedischen Absolutbetrag. Dann können wir auf $K$ einen Abstandsbegriff einführen.

**Definition 3.1.** *Für $x, y \in K$ definieren wir*

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

*Wir nennen $d(x, y)$ den Abstand von $x$ und $y$.*

Die Funktion $d$ ist eine Metrik auf $K$ im Sinne der folgenden Definition.

**Definition 3.2.** *Sei $X$ eine Menge und $d : X \times X \to \mathbb{R}$ eine Funktion. $d$ heißt Metrik auf $X$, falls für alle $x, y, z \in X$ gilt:*

*i)* $d(x, y) \geqq 0$. *Ferner ist* $d(x, y) = 0$ *genau dann, wenn* $x = y$.

*ii)* $d(x, y) = d(y, x)$.

*iii)* $d(x, z) \leqq d(x, y) + d(y, z)$.

Die Metrik $d$ aus Definition 3.1 erfüllt sogar die folgende nicht-archimedische Dreiecksungleichung. Für alle $x, y, z \in K$ gilt

$$d(x, z) \leqq max\{d(x, y), d(y, z)\}.$$

Falls $d(x, y) \neq d(y, z)$ ist, gilt sogar

$$d(x, z) = max\{d(x, y), d(y, z)\}.$$

(Übungsaufgabe)

Diese starke Form der Dreiecksungleichung hat überraschende Konsequenzen. Sind $x, y, z$ drei Elemente aus $K$, so gilt

$$\begin{array}{ll} & d(x, y) = d(y, z) \\ \text{oder} & d(x, z) = d(x, y) \\ \text{oder} & d(x, z) = d(y, z). \end{array}$$

Zwei dieser drei Zahlen sind also immer gleich. Man kann $d(x, y)$ als "Länge der Strecke" in $K$ zwischen $x$ und $y$ auffassen.
Dann hat das Dreieck mit den Eckpunkten $x, y$ und $z$ die Eigenschaft, dass mindestens zwei seiner drei Seiten gleich lang sind. Jedes nicht-archimedische Dreieck ist also gleichschenklig!

**Definition 3.3.** *Für $a \in K$ und eine reelle Zahl $r > 0$ setzen wir*

$$\begin{aligned} B(a, r) &= \{x \in K : d(a, x) < r\} \\ &= \{x \in K : |a - x| < r\} \end{aligned}$$

*und*

$$\begin{aligned} \overline{B}(a, r) &= \{x \in K : d(a, x) \leqq r\} \\ &= \{x \in K : |a - x| \leqq r\} \end{aligned}$$

Wir nennen $B(a,r)$ den offenen Ball um $a$ mit Radius $r$ und $\overline{B}(a,r)$ den abgeschlossenen Ball um $a$ mit Radius $r$.

**Definition 3.4.** *Eine Teilmenge $U \subset K$ heißt offen, falls für jedes $a \in U$ ein $r > 0$ existiert mit $B(a,r) \subset U$.*

Die Menge $U$ enthält also für jeden Punkt auch noch einen kleinen offenen Ball um diesen Punkt.

**Beispiel:**

i) $\emptyset$ und $K$ sind offen.

ii) Für jedes $a \in K$ und $r > 0$ ist $B(a,r) \subset K$ offen.

iii) Beliebige Vereinigungen und endliche Schnitte offener Mengen sind offen. (Übungsaufgabe)

**Definition 3.5.** *Eine Teilmenge $A \subset K$ heißt abgeschlossen, falls $K \backslash A$ offen ist.*

**Beispiel:**

i) $\emptyset$ und $K$ sind abgeschlossen.

ii) Für jedes $a \in K$ und $r > 0$ ist $K \backslash B(a,r) \subset K$ abgeschlossen.

iii) Beliebige Schnitte und endliche Vereinigungen abgeschlossener Mengen sind abgeschlossen.

Jetzt wollen wir zeigen, dass Bälle sogar offen und abgeschlossen sind.

**Lemma 3.6.** *Sei $a \in K$ und $r \in \mathbb{R}_{>0}$.*

*i) Die Kreislinie $\{x \in K : d(a,x) = r\}$ ist offen und abgeschlossen in $K$.*

*ii) Der abgeschlossene Ball $\overline{B}(a,r)$ ist offen und abgeschlossen in $K$.*

*iii) Der offene Ball $B(a,r)$ ist offen und abgeschlossen in $K$.*

**Beweis :**

i) Ist $y \in K$ mit $d(a,y) = r$ gegeben, so gilt für jedes $z \in B(y,r) : d(y,z) < r$, also nach der nicht-archimedischen Dreiecksungleichung

$$d(a,z) = max\{d(a,y), d(y,z)\} = r.$$

Daher ist mit $y$ auch der Ball $B(y,r)$ in der Kreislinie

$$\{x \in K : d(a,x) = r\}$$

enthalten. Diese ist also offen.
Das Komplement der Kreislinie in $K$ ist

$$\{x \in K : d(a,x) < r\} \cup \{x \in K : d(a,x) > r\}.$$

Da beide Teilmengen offen sind (Übungsaufgabe), ist auch die Vereinigung offen. Also ist die Kreislinie abgeschlossen.

ii) Wir zeigen zunächst, dass $\overline{B}(a,r)$ offen ist. Sei $y \in \overline{B}(a,r)$, also

$$d(a,y) =: s \leqq r.$$

Nach i) ist die Kreislinie $\{x \in K : d(a,x) = s\}$ offen. Sie enthält $y$, daher ist wegen $\{x \in K : d(a,x) = s\} \subset \overline{B}(a,r)$ ein offener Ball um $y$ in $\overline{B}(a,r)$ enthalten. Somit ist $\overline{B}(a,r)$ offen. Das Komplement von $\overline{B}(a,r)$ ist

$$K \backslash \overline{B}(a,r) = \{x \in K : d(a,x) > r\}.$$

Das ist offen (Übungsaufgabe, siehe i)). Also ist $\overline{B}(a,r)$ abgeschlossen.

iii) Wir haben schon gesehen, dass $B(a,r)$ offen ist. Das Komplement von $B(a,r)$ ist

$$K \backslash B(a,r) = \{x \in K : d(a,x) \geqq r\}.$$

Mit demselben Argument wie im Beweis von ii) zeigt man, dass diese Menge offen ist (Übungsaufgabe). Also ist $B(a,r)$ abgeschlossen.

□

Es gibt also viele interessante Teilmengen von $K$, die gleichzeitig offen und abgeschlossen sind. Das ist ein nicht-archimedisches Phänomen, das wir aus dem reellen Anschauungsraum nicht kennen. Es sorgt dafür, dass $K$ "total unzusammenhängend" ist, wie wir jetzt erklären wollen.

**Definition 3.7.** *Eine Teilmenge $S \subset K$ (oder allgemeiner in einem topologischen Raum) heißt unzusammenhängend, wenn es $U_1, U_2 \subset K$ gibt mit*

*i)* $U_1, U_2$ *sind offen in* $K$

*ii)* $U_1 \cap U_2 = \emptyset$

*iii)* $S = (S \cap U_1) \cup (S \cap U_2)$

*iv)* $S \cap U_1 \neq \emptyset$ *und* $S \cap U_2 \neq \emptyset$.

Ist $S$ unzusammenhängend, dann zerfällt $S$ in zwei nicht leere, offene und abgeschlossene Stücke.
Eine Teilmenge heißt zusammenhängend, wenn sie nicht unzusammenhängend ist.

**Beispiel:**

i) In den reellen Zahlen sind alle Intervalle zusammenhängend.

ii) In $K$ sind alle Einpunktmengen $\{x\}$ für $x \in K$ zusammenhängend.

iii) In $K$ ist der abgeschlossene Einheitsball

$$\overline{B}(a,r) = B(a,r) \cup \{x \in K : d(a,x) = r\}$$

unzusammenhängend.

**Definition 3.8.** *Für jedes $x \in K$ nennen wir die Vereinigung aller zusammenhängenden Mengen, die $x$ enthalten, die Zusammenhangskomponente von $x$.*
*(Diese Definition gilt allgemeiner in jedem topologischen Raum.)*

Die Zusammenhangskomponente von $x$ ist eine zusammenhängende Menge (Übungsaufgabe).

**Satz 3.9.** *In dem nicht-archimedischen Körper $K$ ist die Zusammenhangskomponente von $x \in K$ die Einpunktmenge $\{x\}$. Außer den Einpunktmengen enthält $K$ also keine zusammenhängenden Teilmengen.*

**Beweis :** Sei $S$ eine zusammenhängende Menge mit $x \in S$. Falls $S \backslash \{x\} \neq \emptyset$ ist, so existiert ein $y \in S$ mit $r = d(y,x) > 0$. Dann betrachten wir die nach Lemma 3.6 offenen Mengen

$$U_1 = B(x,r) \text{ und } U_2 = K \backslash B(x,r).$$

Ihr Schnitt ist leer und wegen $x \in U_1$ und $y \in U_2$ gilt $S \cap U_1 \neq \emptyset$ und $S \cap U_2 \neq \emptyset$.
Da

$$S = (S \cap U_1) \cup (S \cap U_2),$$

ist $S$ unzusammenhängend. □

Nicht-archimedische Bälle haben noch andere überraschende Eigenschaften.

**Lemma 3.10.** *Sei $a \in K$ und $r > 0$.*

*i) Ist $b \in B(a,r)$, so gilt*

$$B(a,r) = B(b,r).$$

*Jeder Punkt im offenen Ball $B(a,r)$ ist also ein Mittelpunkt.*

*ii) Ist $b \in \overline{B}(a,r)$, so gilt*

$$\overline{B}(a,r) = \overline{B}(b,r).$$

*Jeder Punkt im abgeschlossenen Ball $\overline{B}(a,r)$ ist also ein Mittelpunkt.*

**Beweis :**

i) Ist $b \in B(a,r)$, so gilt $d(a,b) < r$. Wir zeigen die Gleichheit

$$B(a,r) = B(b,r)$$

durch zwei Inklusionen.
„$\subset$“: Ist $c \in B(a,r)$, so gilt $d(a,c) < r$. Also ist nach der nicht-archimedischen Dreiecksungleichung

$$d(b,c) \leqq max\{d(b,a), d(a,c)\} < r,$$

denn sowohl $d(b,a) = d(a,b)$ als auch $d(a,c)$ sind kleiner als $r$. Somit ist $c \in B(b,r)$.
„$\supset$“: Ist $c \in B(b,r)$, so gilt $d(c,b) < r$. Also folgt mit der nicht-archimedischen Dreiecksungleichung

$$d(a,c) \leqq max\{d(a,b), d(b,c)\} < r.$$

Somit ist $c \in B(a,r)$.

ii) Analog zu *i)* (Übungsaufgabe).

□

**Korollar 3.11.** *Zwei offene, nicht-archimedische Bälle $B(a,r)$ und $B(b,s)$ sind entweder disjunkt oder einer der Bälle ist im anderen enthalten.*
*Ein analoges Resultat gilt für abgeschlossene Bälle.*

**Beweis :** Wir nehmen $B(a,r) \cap B(a,s) \neq \emptyset$ an und betrachten $x \in B(a,r) \cap B(a,s)$. Nach Lemma 3.10 folgt

$$B(a,r) = B(x,r)$$

und

$$B(b,s) = B(x,s).$$

Ist $r > s$, so gilt also

$$B(b,s) = B(x,s) \subset B(x,r) = B(a,r).$$

Ist umgekehrt $r \leqq s$, so gilt

$$B(a,r) = B(x,r) \subset B(x,s) = B(b,s).$$

Die entsprechende Aussage für abgeschlossene Bälle zeigt man analog. □

# 4 Ganzheitsringe

**Definition 4.1.** *Ein Ring ist eine Menge $A$ zusammen mit zwei Verknüpfungen $+ : A \times A \to A$ und $\cdot : A \times A \to A$, so dass gilt:*

*i) $(A,+)$ ist eine abelsche Gruppe.*

*ii) Die Multiplikation $\cdot$ ist assoziativ und $A$ enthält ein neutrales Element $1$ bezüglich der Multiplikation.*

*iii) Es gilt das Distributivgesetz*

$$a(b+c) = ab + ac$$

*für alle $a, b, c \in A$.*

**Beispiel:**

i) $\mathbb{Z}$ ist ein kommutativer Ring.

ii) Für $n \geqq 2$ ist $GL_n(\mathbb{R})$ ein Ring, der nicht kommutativ ist.

iii) Jeder Körper ist ein kommutativer Ring.

**Definition 4.2.** *Sei $A$ ein kommutativer Ring. Eine Teilmenge $\mathfrak{a} \subset A$ heißt Ideal, falls gilt:*

*i) $(\mathfrak{a}, +)$ ist eine Untergruppe von $(A, +)$.*

*ii) Für jedes $a \in A$ und $b \in \mathfrak{a}$ ist $ab \in \mathfrak{a}$.*

**Beispiel:** Für jede natürliche Zahl $d$ ist

$$d\mathbb{Z} = \{dk : k \in \mathbb{Z}\}$$

ein Ideal in $\mathbb{Z}$.

Ist $A$ ein kommutativer Ring und $\mathfrak{a} \subset A$ ein Ideal, so ist die Menge der Nebenklassen

$$\{a + \mathfrak{a} : a \in A\}$$

ein Ring (Übungsaufgabe). Hier ist die Addition von Nebenklassen definiert als

$$(a_1 + \mathfrak{a}) + (a_2 + \mathfrak{a}) = (a_1 + a_2) + \mathfrak{a},$$

entsprechend ist die Multiplikation definiert als

$$(a_1 + \mathfrak{a}) \cdot (a_2 + \mathfrak{a}) = (a_1 a_2) + \mathfrak{a}.$$

Nebenklassen sind Mengen, und es gilt

$$a + \mathfrak{a} = b + \mathfrak{a}$$

genau dann, wenn

$$a - b \in \mathfrak{a}.$$

Man muss also bei der obigen Definition der Addition und der Multiplikation nachprüfen, dass sie wohldefiniert, d.h. unabhängig von der Wahl von $a_1$ und $a_2$ ist.

**Beispiel:** Für $d \geqq 1$ ist

$$\mathbb{Z}/d\mathbb{Z} = \{0, 1, \ldots, d-1\},$$

wobei in der Menge $\{0, 1, \ldots, d-1\}$ gerechnet wird, indem man nach jeder Rechenoperation den Rest bei Division durch $d$ nimmt.

**Satz 4.3.** *Sei $K$ ein Körper mit einem nicht-archimedischen Absolutbetrag. Dann ist der abgeschlossene Einheitsball*

$$\overline{B}(0,1) = \{x \in K : d(0,x) \leqq 1\}$$

*ein kommutativer Ring.*
*Der offene Einheitsball*

$$B(0,1) = \{x \in K : d(0,x) < 1\}$$

*ist ein Ideal in $\overline{B}(0,1)$.*
*Wir schreiben $\mathcal{O}_K = \overline{B}(0,1)$ und nennen $\mathcal{O}_K$ den Ganzheitsring oder Bewertungsring in $K$. Außerdem schreiben wir*

$$\mathfrak{p} = B(0,1)$$

*und nennen $\mathfrak{p}$ das Bewertungsideal in $K$.*

**Beweis :** Sind $x$ und $y$ in $\overline{B}(0,1)$, so ist

$$|x| = d(0,x) \leqq 1 \text{ und } |y| = d(0,y) \leqq 1.$$

Also ist

$$d(0,xy) = |xy| = |x|\,|y| \leqq 1$$

und

$$d(0,x+y) = |x+y| \leqq max\{|x|\,,|y|\} \leqq 1.$$

$\overline{B}(0,1)$ ist also abgeschlossen unter der Addition und der Multiplikation in $K$. Daraus folgt, dass $\overline{B}(0,1)$ ein kommutativer Ring im Sinne von Definition 4.1 ist.
Ist $x \in \overline{B}(0,1)$ und $y \in B(0,1)$, so gilt

$$|x| = d(0,x) \leqq 1 \text{ und } |y| = d(0,y) < 1,$$

also ist

$$d(0,xy) = |xy| = |x|\,|y| < 1.$$

Somit ist $xy \in B(0,1)$. Daraus folgt, dass $B(0,1)$ ein Ideal in $\overline{B}(0,1)$ ist. □

**Satz 4.4.** *Sei $K$ ein Körper mit einem nicht-archimedischen Absolutbetrag. Dann ist der Quotientenring*

$$\mathfrak{K} = \mathcal{O}_K/\mathfrak{p}$$

*ein Körper. Er heißt Restklassenkörper von $K$.*

**Beweis :** Der Quotient $\mathfrak{K} = \mathcal{O}_K/\mathfrak{p}$ ist ein kommutativer Ring. Wir müssen nur noch zeigen, dass $1 \neq 0$ ist und dass jedes Element $\neq 0$ aus $\mathfrak{K}$ ein Inverses besitzt. Da $|1| = 1$ und $|0| = 0$ ist, folgt $1 + \mathfrak{p} \neq \mathfrak{p} = 0 + \mathfrak{p}$.
Sei $a + \mathfrak{p}$ ein Element aus $\mathfrak{K}$ mit $a \in \mathcal{O}_K$ und

$$a + \mathfrak{p} \neq 0 = 0 + \mathfrak{p}.$$

Dann ist $a \notin \mathfrak{p}$, das heißt $|a| = 1$. Mit $b$ bezeichnen wir das Inverse von $a$ in $K$. Aus $ab = 1$ folgt $|a||b| = |ab| = 1$, also ist $|b| = 1$. Somit ist $b \in \mathcal{O}_K$. Die Restklasse $b + \mathfrak{p} \in \mathfrak{K}$ erfüllt

$$(a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p} = 1 + \mathfrak{p},$$

also ist $a + \mathfrak{p}$ invertierbar in $\mathfrak{K}$. □

**Beispiel:** Wir betrachten $K = \mathbb{Q}$ mit dem $p$-adischen Absolutbetrag $|\cdot|_p$.
Dann ist

$$\begin{aligned} \mathcal{O}_K &= \left\{ \tfrac{m}{n} \in \mathbb{Q} : p \nmid n \right\}, \\ \mathfrak{p} &= \left\{ \tfrac{m}{n} \in \mathbb{Q} : p \nmid n \text{ und } p \mid m \right\} \end{aligned}$$

und

$$\mathfrak{K} = \mathcal{O}_K/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p,$$

wobei $\mathbb{F}_p$ der Körper mit $p$ Elementen ist. Der Isomorphismus $\mathfrak{K} \simeq \mathbb{F}_p$ wird durch die Einbettung

$$\begin{aligned} \mathbb{Z} &\hookrightarrow \mathcal{O}_K \\ m &\mapsto \tfrac{m}{1} \end{aligned}$$

induziert, die $p\mathbb{Z}$ nach $\mathfrak{p}$ abbildet und daher eine Abbildung

$$\mathbb{Z}/p\mathbb{Z} \to \mathfrak{K}$$

auf den Restklassenringen induziert.
Diese ist ein Isomorphismus (Übungsaufgabe).

# 5 Beträge auf $\mathbb{Q}$: Der Satz von Ostrowski

Wir wollen jetzt bestimmen, welche Beträge es auf dem Körper $\mathbb{Q}$ der rationalen Zahlen gibt. Wir kennen schon den reellen Absolutbetrag, den wir mit $|\cdot|_\infty$ bezeichnen, den trivialen Absolutbetrag sowie für jede Primzahl $p$ den $p$-adischen Absolutbetrag $|\cdot|_p$.

**Definition 5.1.** *Wir nennen zwei Absolutbeträge $|\cdot|_1$ und $|\cdot|_2$ auf einem Körper $K$ äquivalent, falls jede Teilmenge von $K$, die offen bezüglich $|\cdot|_1$ ist, auch offen bezüglich $|\cdot|_2$ ist und umgekehrt.*

**Lemma 5.2.** *Es seien $|\cdot|_1$ und $|\cdot|_2$ zwei Absolutbeträge auf dem Körper $K$. Dann sind die folgenden Aussagen äquivalent*

*i)* $|\cdot|_1$ *und* $|\cdot|_2$ *sind äquivalente Beträge.*

*ii) Für jedes $x \in K$ gilt*

$$|x|_1 < 1 \Leftrightarrow |x|_2 < 1.$$

*iii) Es gibt eine positive reelle Zahl $\alpha$ mit*

$$|x|_1 = |x|_2^\alpha$$

*für alle $x \in K$.*

**Beweis :** *i)* $\Rightarrow$ *ii)*: Sei $x \in K$ mit $|x|_1 < 1$. Dann ist $|x|_1^n$ für $n \to \infty$ eine Nullfolge.
Jede offene Umgebung von 0 bezüglich der $|\cdot|_1$-Topologie enthält also fast alle $x^n$ ($n \in \mathbb{N}$).
Für jedes $\varepsilon > 0$ ist die Menge

$$\{y \in K : |y|_2 < \varepsilon\}$$

offen in der von $|\cdot|_2$ definierten Topologie, also nach Voraussetzung auch in der von $|\cdot|_1$ definierten Topologie. Damit enthält sie fast alle Folgenglieder $x^n$. Daher ist $(x^n)_{n\geqq 1}$ eine Nullfolge bezüglich $|\cdot|_2$, also konvergiert

$$|x|_2^n = |x^n|_2$$

gegen 0. Somit ist $|x|_2 < 1$.
Mit demselben Argument zeigt man, dass $|x|_2 < 1$ die Ungleichung $|x|_1 < 1$ impliziert.

*ii)* $\Rightarrow$ *iii)*: Ist $|\cdot|_1$ der triviale Absolutbetrag, so muss auch $|\cdot|_2$ der triviale Absolutbetrag sein (Übungsaufgabe). In diesem Fall ist *iii)* mit $\alpha = 1$ erfüllt.
Wir können also annehmen, dass $|\cdot|_1$ nicht der triviale Absolutbetrag ist. Wir wählen ein $x \in K$ mit $x \neq 0$ und $|x|_1 < 1$. Dann ist auch $|x|_2 < 1$ und wir setzen

$$\alpha = \frac{\log |x|_1}{\log |x|_2} \in \mathbb{R}_{>0}.$$

Es folgt $|x|_2^\alpha = |x|_1$.
Sei nun $y \in K \setminus \{0\}$. Falls $|y|_1 = 1$ ist, so kann nach Voraussetzung weder $|y|_2$ noch $|1/y|_2$ echt kleiner als 1 sein. Also folgt $|y|_2 = 1$. Somit gilt für das oben definierte $\alpha$ trivialerweise

$$|y|_2^\alpha = |y|_1 .$$

Falls $|y|_1 < 1$ ist, so ist nach Voraussetzung auch $|y|_2 < 1$.
Also ist $\log |y|_1 \neq 0$ und $\log |y|_2 \neq 0$. Wir betrachten die beiden reellen Zahlen

$$\frac{\log |x|_1}{\log |y|_1} \quad \text{und} \quad \frac{\log |x|_2}{\log |y|_2}.$$

Beide sind das Supremum aller echt kleineren rationalen Zahlen. Gilt nun für $n, m \in \mathbb{Z}$ mit $m \neq 0$

$$\frac{n}{m} < \frac{\log |x|_1}{\log |y|_1},$$

so folgt $n \log |y|_1 > m \log |x|_1$, da $\log |y|_1 < 0$ ist.
Also ist $\log |y^n|_1 > \log |y^m|_1$, woraus

$$\left|\frac{x^m}{y^n}\right|_1 < 1$$

folgt. Nach Voraussetzung ist dann auch

$$\left|\frac{x^m}{y^n}\right|_2 < 1,$$

woraus wir $|x^m|_2 < |y^n|_2$, also auch $m \log |x|_2 < n \log |y|_2$ und damit

$$\frac{n}{m} < \frac{\log |x|_2}{\log |y|_2}$$

schließen. Also folgt

$$\frac{\log |x|_1}{\log |y|_1} \;=\; \sup \left\{ \frac{n}{m} : \frac{n}{m} < \frac{\log |x|_1}{\log |y|_1} \right\} \;\leqq\; \frac{\log |x|_2}{\log |y|_2}.$$

Dasselbe Argument mit vertauschten Rollen zeigt

$$\frac{\log |x|_2}{\log |y|_2} \leqq \frac{\log |x|_1}{\log |y|_1},$$

also folgt

$$\frac{\log |x|_2}{\log |y|_2} = \frac{\log |x|_1}{\log |y|_1}.$$

Daher ist

$$\alpha = \frac{\log |x|_1}{\log |x|_2} = \frac{\log |y|_1}{\log |y|_2}$$

und somit $|y|_1 = |y|_2^\alpha$.
Starten wir mit einem $y$ mit $|y| > 1$, so folgt

$$\left|\frac{1}{y}\right|_1 = \left|\frac{1}{y}\right|_2^\alpha,$$

also ebenfalls $|y|_1 = |y|_2^\alpha$. Damit ist *iii)* bewiesen.

*iii)* $\Rightarrow$ *i)*: Gilt $|x|_1 = |x|_2^\alpha$ für alle $x \in K$, so schließen wir

$$|x-a|_1 < r \Leftrightarrow |x-a|_2 = |x-a|_1^\alpha < r^\alpha.$$

Ist $U$ eine offene Teilmenge in $K$ bezüglich $|\cdot|_1$, so enthält $U$ mit jedem Punkt $a$ noch einen offenen Ball

$$B(a,r) = \{x \in K : |x-a|_1 < r\}.$$

Da $B(a,r) = \{x \in K : |x-a|_2 < r^\alpha\}$ ist, enthält $U$ mit jedem Punkt $a$ auch einen Ball bezüglich $|\cdot|_2$, ist also offen bezüglich $|\cdot|_2$. Die andere Richtung zeigt man analog. □

Wir können nun den wichtigen Satz von Ostrowski beweisen, der besagt, dass wir bis auf Äquivalenz schon alle Beträge auf $\mathbb{Q}$ kennengelernt haben.

**Satz 5.3.** *Jeder nicht-triviale Absolutbetrag auf $\mathbb{Q}$ ist entweder äquivalent zum reellen Absolutbetrag $|\cdot|_\infty$ oder zu einem p-adischen Absolutbetrag $|\cdot|_p$ für eine Primzahl p.*

**Beweis :** Sei $|\cdot|$ ein nicht-trivialer Absolutbetrag auf $\mathbb{Q}$. Wir betrachten zwei Fälle.

1.Fall: Der Betrag $|\cdot|$ ist archimedisch. Dann existiert ein $n \in \mathbb{N}$ mit $|n| > 1$. Wir wählen $n_0 \in \mathbb{N}$ minimal mit der Eigenschaft $|n_0| > 1$ und setzen

$$\alpha = \frac{\log |n_0|}{\log n_0}.$$

Dann ist $n_0^\alpha = |n_0|$. Offenbar ist $\alpha > 0$. Nun sei $n$ eine beliebige natürliche Zahl. Wir betrachten ihre $n_0$-adische Entwicklung

$$n = c_0 + c_1 n_0 + c_2 n_0^2 + \cdots + c_k n_0^k$$

mit $k \geqq 0$ und $c_0, \ldots, c_k \in \{0, \ldots, n_0 - 1\}$ sowie $c_k \neq 0$. Es gilt

$$n_0^k \leqq n < n_0^{k+1},$$

woraus

$$k \leqq \frac{\log n}{\log n_0} < k + 1,$$

also

$$k = \left[\frac{\log n}{\log n_0}\right] \qquad \text{(Gaussklammer)}$$

folgt. Nach der Dreiecksungleichung ist

$$\begin{array}{rcl} |n_0| & = & \left|c_0 + c_1 n_0 + \cdots + c_k n_0^k\right| \\ & \leqq & |c_0| + |c_1|\,|n_0| + \cdots + |c_k|\,\left|n_0^k\right| \\ & \leqq & 1 + |n_0| + \cdots + |n_0|^k, \end{array}$$

Denn alle $c_i$ sind kleiner als $n_0$ und erfüllen daher wegen der Minimalität von $n_0$ die Bedingung $|c_i| \leqq 1$. Aus $n_0^\alpha = |n_0|$ folgt dann

$$\begin{array}{rcl} |n| & \leqq & 1 + n_0^\alpha + \cdots + n_0^{\alpha k} \\ & = & n_0^{\alpha k}(n_0^{-\alpha k} + n_0^{-\alpha(k+1)} + \cdots + n_0^{-\alpha} + 1) \\ & \leqq & n_0^{\alpha k} \sum_{j=1}^{\infty} n_0^{-j\alpha} \\ & = & n_0^{\alpha k} \dfrac{1}{1 - n_0^{-\alpha}} \\ & = & n_0^{\alpha k} \dfrac{n_0^\alpha}{n_0^\alpha - 1}. \end{array}$$

Wir setzen $c = \frac{n_0^\alpha}{n_0^\alpha - 1}$ und erhalten

$$|n| \leqq c n_0^{\alpha k} \leqq c n^\alpha,$$

da $n_0^k \leqq n$ ist. Die Ungleichung $|n| \leqq cn^\alpha$ gilt also für jede natürliche Zahl $n$.
Insbesondere gilt sie für alle Zahlen der Form $n^N$ für $n, N \in \mathbb{N}$.
Daher ist

$$|n|^N = \left|n^N\right| \leqq c n^{N\alpha},$$

woraus

$$|n| \leqq \sqrt[N]{c}\, n^\alpha$$

folgt.
Aus $\sqrt[N]{c} \overset{N\to\infty}{\longrightarrow} 1$ folgt somit

$$|n| \leqq n^\alpha.$$

Nun wollen wir auch die andere Ungleichung $n^\alpha \leqq |n|$ zeigen.
Dazu betrachten wir erneut die $n_0$-adische Entwicklung

$$n \;=\; c_0 + c_1 n_0 + \cdots + c_k n_0^k$$

von $n$. Aus $n_0^{k+1} > n$ folgt

$$\begin{array}{rcl} n_0^{(k+1)\alpha} & = & |\; n_0^{k+1} \;| = |\; n_0^{k+1} + n - n \;| \\ & \leqq & |\; n_0^{k+1} - n \;| + |\; n \;| \end{array}$$

nach der Dreiecksungleichung.
Für die natürliche Zahl $n_0^{k+1} - n$ gilt

$$\left|n_0^{k+1} - n\right| \leqq (n_0^{k+1} - n)^\alpha.$$

Aus $n \geqq n_0^k$ folgt

$$n_0^{k+1} - n \leqq n_0^{k+1} - n_0^k,$$

also auch

$$\left|n_0^{k+1} - n\right| \leqq (n_0^{k+1} - n_0^k)^\alpha.$$

Somit gilt

$$\begin{aligned} |n| &\geqq n_0^{(k+1)\alpha} - \left|n_0^{k+1} - n\right| \\ &\geqq n_0^{(k+1)\alpha} - (n_0^{(k+1)} - n_0^k)^\alpha \\ &= n_0^{(k+1)\alpha}(1 - (1 - n_0^{-1})^\alpha) \\ &= n_0^{(k+1)\alpha} c' \end{aligned}$$

mit $c' = (1 - (1 - n_0^{-1})^\alpha)$. Diese reelle Konstante hängt nur von $n_0$ ab.
Aus $n_0^{(k+1)} > n$ folgt daher für alle $x \in \mathbb{N}$

$$|n| \geqq n^\alpha c'.$$

Mit demselben Trick wie oben wenden wir diese Ungleichung auf $n^N$ an und erhalten

$$|n| \geqq n^\alpha \sqrt[N]{c'}.$$

Für $N \to \infty$ folgt $|n| \geqq n^\alpha$. Insgesamt erhalten wir also

$$|n| = n^\alpha = |n|_\infty^\alpha,$$

für alle natürlichen Zahlen $n$. Daraus folgt

$$|-n| = |n| = n^\alpha = |-n|_\infty^\alpha,$$

woraus sofort $|x| = |x|_\infty^\alpha$ für alle $x \in \mathbb{Q}$ folgt.
Also ist $|\cdot|$ äquivalent zum reellen Absolutbetrag $|\cdot|_\infty$.

2.Fall $|\cdot|$ ist nicht-archimedisch. Dann gilt $|n| \leqq 1$ für jedes $n \in \mathbb{N}$ nach Proposition 2.3. Es gibt eine kleinste natürliche Zahl $n_0$ mit $|n_0| < 1$. Wir zeigen zunächst, dass $n_0$ eine Primzahl ist. Wenn wir $n_0 = ab$ als Produkt von natürlichen Zahlen schreiben, dann muss wegen

$$1 > |n_0| = |a|\,|b|$$

mindestens einer der Faktoren $|a|, |b|$ kleiner als 1 sein. Wegen der Minimalität von $n_0$ folgt daraus $a = n_0$ oder $b = n_0$. Also ist $n_0 =: p$ eine Primzahl.

Wir zeigen nun, dass $|\cdot|$ äquivalent zu $|\cdot|_p$ ist.
Sei $m \in \mathbb{Z}$ eine zu $p$ teilerfremde Zahl. Dann ist $m = kp + r$ mit einem Rest $r \in \{1, \ldots, p-1\}$. Also folgt aus der Minimalität von $p$, dass

$$|r| = 1$$

ist. Ferner gilt

$$|kp| = |k|\,|p| \leqq |p| < 1,$$

so dass nach der nicht-archimedischen Dreiecksungleichung

$$\begin{aligned} |m| &= \max\{|kp|\,, |r|\} \\ &= 1 \end{aligned}$$

folgt. Jede zu $p$ teilerfremde ganze Zahl hat also den Betrag 1.
Jede durch $p$ teilbare ganze Zahl $m$ ist von der Form

$$m = kp^{\mu}$$

mit $\mu > 0$ und einem zu $p$ teilerfremden $k \in \mathbb{Z}$. Also gilt

$$\begin{aligned} |m| &= |k|\,|p^{\mu}| \\ &= |p|^{\mu} \end{aligned}$$

Setzen wir $\alpha = \dfrac{\log p^{-1}}{\log |p|}$, so gilt $|p|^{\alpha} = p^{-1} = |p|_p$. Es folgt

$$|m|^{\alpha} = |p|^{\mu\alpha} = p^{-\mu} = |p^{\mu}|_p = |kp^{\mu}|_p = |m|_p\,.$$

Für die zu $p$ teilerfremden $m \in \mathbb{Z}$ gilt ohnehin

$$|m|^{\alpha} = 1 = |m|_p\,,$$

also folgt für alle $x \in \mathbb{Q}$

$$|x|^{\alpha} = |x|_p\,.$$

□

# 6 Komplettierung nach einem Absolutbetrag

In der Analysis konstruiert man den Körper der reellen Zahlen als Komplettierung der rationalen Zahlen nach dem reellen Absolutbetrag. Dabei nimmt man alle Grenzwerte von Cauchyfolgen hinzu. Wir wollen dieses Prinzip jetzt allgemein erklären. Sei $K$ ein Körper und $|\cdot|$ ein Absolutbetrag auf $K$.

**Definition 6.1.** *i) Eine Folge $(a_n)_{n\geq 1}$ mit $a_n \in K$ heißt Cauchyfolge, falls es für jedes $\varepsilon > 0$ eine natürliche Zahl $N$ gibt mit*

$$|x_m - x_n| < \varepsilon$$

*für alle $m, n \geqq N$.*

*ii) Eine Folge $(a_n)_{n\geq 1}$ aus $K$ konvergiert gegen einen Grenzwert $a \in K$, falls es für jedes $\varepsilon > 0$ eine natürliche Zahl $n_0$ gibt mit $|a_n - a| < \varepsilon$ für alle $n \geqq n_0$.*

*iii) Der Körper $K$ heißt vollständig bezüglich des Betrags $|\cdot|$, falls jede Cauchyfolge $(a_n)_{n\geq 1}$ aus $K$ gegen einen Grenzwert $a \in K$ konvergiert.*

**Beispiel:** Der Körper $\mathbb{R}$ der reellen Zahlen ist vollständig bezüglich des reellen Absolutbetrags $|\cdot|_\infty$.

Für einen nicht-archimedischen Betrag lassen sich Cauchyfolgen einfacher charakterisieren.

**Lemma 6.2.** *Falls der Betrag $|\cdot|$ auf $K$ nicht-archimedisch ist, so ist eine Folge $(a_n)_{n\geqq 1}$ von Elementen in $K$ genau dann eine Cauchyfolge, wenn*

$$|a_{n+1} - a_n| \underset{n\to\infty}{\longrightarrow} 0$$

*konvergiert.*

**Beweis :** Falls $(a_n)_{n\geqq 1}$ eine Cauchyfolge ist, so konvergiert $|a_{n+1} - a_n|$ definitionsgemäß gegen 0. Umgekehrt betrachten wir Indizes $m \geqq n$. Nach der nicht-archimedischen Dreiecksungleichung gilt

$$\begin{aligned} |a_m - a_n| &= |(a_m - a_{m-1}) + \cdots + (a_{n+1} - a_n)| \\ &\leqq \max_{r=0,\ldots,m-n-1} \{|a_{n+r+1} - a_{n+r}|\}. \end{aligned}$$

Für jedes $\varepsilon > 0$ finden wir nach Voraussetzung ein $N$ mit

$$|a_{n+1} - a_n| < \varepsilon$$

für alle $n \geqq N$. Daraus folgt also

$$|a_m - a_n| < \varepsilon$$

für alle $m, n \geqq N$. □

Wir benutzen die folgende übliche Schreibweise für $a, b, c \in \mathbb{Z}$:

$$a \equiv b \mod c$$

genau dann, wenn $c$ ein Teiler von $a - b$ ist.

**Lemma 6.3.** *Seien $n \geqq 1$ und eine Primzahl $p \neq 2$ gegeben. Ferner seien $a, b \in \mathbb{Z}$ mit $p \nmid a$ und $b^2 \equiv a \mod p^n$. Dann existiert ein $x \in \mathbb{Z}$ mit*

$$\begin{aligned} x &\equiv b \mod p^n \qquad \text{und} \\ x^2 &\equiv a \mod p^{n+1} \end{aligned}$$

**Beweis :** Nach Voraussetzung ist $b^2 \equiv a \mod p^n$, also ist $p^n$ ein Teiler von $(b^2 - a)$. Daher existiert ein $c \in \mathbb{Z}$ mit

$$a = b^2 + cp^n.$$

Wir suchen ein $x$ von der Form

$$x = b + dp^n$$

für ein $d \in \mathbb{Z}$ mit

$$x^2 \equiv a \mod p^{n+1}.$$

Es ist

$$\begin{aligned} (b + dp^n)^2 &= b^2 + 2bdp^n + p^{2n} \\ &= (a - cp^n) + 2bdp^n + p^{2n} \\ &= a + p^n(2bd - c) + p^{2n} \end{aligned}$$

Wählen wir $d$ so, dass $2bd - c$ ein Vielfaches von $p$ ist (Übungsaufgabe: Wieso geht das?), so folgt

$$(b + dp^n)^2 \equiv a \mod p^{n+1},$$

und $x = b + dp^n$ leistet das Verlangte. □

Sei $p \neq 2$ eine Primzahl. Wir zeigen nun mit Hilfe dieses Lemmas, dass der Körper $\mathbb{Q}$ nicht vollständig bezüglich des $p$-adischen Absolutbetrags $|\cdot|_p$ ist.

Sei $a \in \mathbb{Z}$ eine ganze Zahl mit $p \nmid a$, die keine Quadratzahl ist, aber ein quadratischer Rest modulo $p$. Das heißt, es existiert ein $b \in \mathbb{Z}$ mit

$$b^2 \equiv a \mod p.$$

(Übungsaufgabe: Wieso existiert solch ein $a$?)

Wir konstruieren nun induktiv eine Folge $(b_n)_{n\geqq 0}$ mit $b_n^2 \equiv a \mod p^{n+1}$ wie folgt:

i) $b_0 = b$, das heißt, $b_0^2 \equiv a \mod p$.

ii) Ist $b_{n-1}$ mit $b_{n-1}^2 \equiv a \mod p^n$ gefunden, so wählen wir mit Hilfe von Lemma 6.3 ein $b_n \in \mathbb{Z}$ mit

$$b_n \equiv b_{n-1} \mod p^n$$

und

$$b_n^2 \equiv a \mod p^{n+1}.$$

Die entstehende Folge $(b_n)_{n\geqq 0}$ erfüllt

$$p^n \mid (b_n - b_{n-1}),$$

also

$$|b_n - b_{n-1}| \leqq p^{-n} \underset{n\to\infty}{\longrightarrow} 0.$$

Nach Lemma 6.2 ist $(b_n)_{n\geqq 0}$ also eine Cauchyfolge. Angenommen, es gäbe ein $b \in \mathbb{Q}$ mit $b_n \underset{n\to\infty}{\longrightarrow} b$. Aus

$$b_n^2 \equiv a \mod p^{n+1}$$

folgt dann

$$\left|b_n^2 - a\right| \leqq p^{-n+1} \underset{n\to\infty}{\longrightarrow} 0,$$

also konvergiert $(b_n^2)_{n\geqq 0}$ gegen $a$, woraus $b^2 = a$ folgt. Aber das steht im Widerspruch zu der Tatsache, dass $a$ keine Quadratzahl ist.
Übrigens ist $\mathbb{Q}$ auch nicht für den 2-adischen Absolutbetrag $|\cdot|_2$ vollständig, doch für diesen muss ein anderer Beweis geführt werden.

Jetzt konstruieren wir die Komplettierung eines Körpers $K$, der mit einem Absolutbetrag $|\cdot|$ versehen ist, wie folgt.

**Definition 6.4.** *Es sei $\mathfrak{C} = \mathfrak{C}(K, |\cdot|)$ die Menge aller Cauchyfolgen $(x_n)_{n\geqq 1}$ in $K$ bezüglich des Betrages $|\cdot|$.*

Wir können Cauchyfolgen gliedweise addieren und multiplizieren. Außerdem können wir $K$ in $\mathfrak{C}$ einbetten, indem wir jedem $a \in K$ die konstante Cauchyfolge $(a, a, a, \dots)$ zuordnen.

**Lemma 6.5.** *$\mathfrak{C}$ ist ein kommutativer Ring mit Einselement $1 \in K$ und Nullelement $0 \in K$.*

**Beweis :** In den Übungen. □

**Definition 6.6.** *i) Wir nennen eine Cauchyfolge $(x_n)_{n\geqq 1}$ aus $K$ eine Nullfolge, falls $|x_n|$ für $n \to \infty$ gegen Null konvergiert.*

*ii) Mit $\mathfrak{N} \subset \mathfrak{C}$ bezeichnen wir die Menge aller Nullfolgen:*

$$\mathfrak{N} = \left\{ (x_n)_{n\geqq 1} \in \mathfrak{C} : |x_n| \underset{n\to\infty}{\longrightarrow} 0 \right\}.$$

**Lemma 6.7.** *$\mathfrak{N}$ ist ein Ideal in $\mathfrak{C}$ (siehe Definition 4.2).*

**Beweis :** In den Übungen. □

Wie in Kapitel 4 beschrieben, existiert der Quotientenring $\mathfrak{C}/\mathfrak{N}$.

**Satz 6.8.** *Der Quotientenring $\mathfrak{C}/\mathfrak{N}$ ist ein Körper, der $K$ enthält. Wir bezeichnen ihn mit $\widehat{K}$ und nennen $\widehat{K}$ die Komplettierung von $K$ bezüglich $|\cdot|$. Der Betrag $|\cdot|$ lässt sich auf eindeutige Weise auf den Erweiterungskörper $\widehat{K}$ von $K$ fortsetzen.*

**Beweis :** $\widehat{K} = \mathfrak{C}/\mathfrak{N}$ ist nach Konstruktion ein kommutativer Ring. Die Einbettung $K \hookrightarrow \mathfrak{C}$ vermittelt eine Einbettung $K \hookrightarrow \mathfrak{C}/\mathfrak{N} = \widehat{K}$, denn die konstante Folge $(a, a, a, \dots)$ ist genau dann eine Nullfolge, wenn $a = 0$ gilt. Wir betrachten für jede Cauchyfolge $(x_n)_{n\geqq 1}$ in $K$ die Folge der Beträge $(|x_n|)_{n\geqq 1}$ in $\mathbb{R}$. Für alle $m, n \in \mathbb{N}$ gilt

$$||x_m| - |x_n|| \leqq |x_m - x_n|, \qquad \text{(Übungsaufgabe)}$$

daher ist auch $(|x_n|)_{n\geqq 1}$ eine Cauchyfolge und hat somit in $\mathbb{R}$ einen Grenzwert $r$.
Wir setzen

$$\left|(x_n)_{n\geqq 1}\right| = r.$$

Ist $(x_n)_{n\geqq 1}$ eine Nullfolge, so gilt mit dieser Definition $\left|(x_n)_{n\geqq 1}\right| = 0$, also erhalten wir so einen Betrag $|\cdot|$ auf $\widehat{K}$, der den gegebenen Betrag auf $K$ fortsetzt (Übungsaufgabe).
Wir zeigen jetzt, dass $\widehat{K} = \mathfrak{C}/\mathfrak{N}$ ein Körper ist. Dazu sei $(x_n)_{n\geqq 1}$ eine Cauchyfolge, die keine Nullfolge ist. Ihre Restklasse in $\mathfrak{C}/\mathfrak{N}$ ist also nicht Null. Da $(|x_n|)_{n\geqq 1}$ keine Nullfolge ist, gibt es eine Konstante $c > 0$ und ein $n_0 \in \mathbb{N}$ mit $|x_n| > c$ für alle $n \geqq n_0$ (Übungsaufgabe).
Wir definieren

$$y_n = \begin{cases} 0 & n < n_0 \\ 1/x_n & n \geqq n_0 \end{cases}$$

Dann ist für $m, n \geqq n_0$

$$\begin{aligned} |y_m - y_n| &= \left|\frac{1}{x_m} - \frac{1}{x_n}\right| = \left|\frac{x_n - x_m}{x_n x_m}\right| \\ &\leqq \frac{1}{c^2}\,|x_n - x_m|. \end{aligned}$$

Da $(x_n)_{n\geqq 1}$ eine Cauchyfolge ist, muss also auch $(y_n)_{n\geqq 1}$ eine Cauchyfolge sein (Übungsaufgabe). Somit ist $(y_n)_{n\geqq 1} \in \mathfrak{C}$. Die Produktfolge $(x_n)_{n\geqq 1} \cdot (y_n)_{n\geqq 1} = (x_n y_n)_{n\geqq 1}$ besteht aus einer endlichen Anfangssequenz von Nullen, gefolgt von Einsen. Also ist

$$(1)_{n\geqq 1} - (x_n)_{n\geqq 1}(y_n)_{n\geqq 1} = (1, \dots, 1, 0, 0, \dots)$$

eine Nullfolge und somit in $\mathfrak{N}$ enthalten. In $\widehat{K} = \mathfrak{C}/\mathfrak{N}$ gilt also

$$1 = (1)_{n\geqq 1} + \mathfrak{N} = \left((x_n)_{n\geqq 1} + \mathfrak{N}\right)\left((y_n)_{n\geqq 1} + \mathfrak{N}\right),$$

daher ist die Restklasse von $(x_n)_{n\geqq 1}$ in $\mathfrak{C}/\mathfrak{N}$ invertierbar.

□

Wir wollen jetzt noch zeigen, dass $\widehat{K}$ vollständig ist, d.h. dass in $\widehat{K}$ jede Cauchyfolge konvergiert.

**Lemma 6.9.** *Jeder offene Ball $B(a,r)$ in $\widehat{K}$ enthält mindestens ein Element aus $K$. In anderen Worten: $K$ ist dicht in $\widehat{K}$.*

**Beweis :** Es sei $a \in \widehat{K}$ und $r > 0$. Dann ist $a = (x_n)_{n\geqq 1}$ eine Cauchyfolge aus $K$. Wir müssen zeigen, dass es ein $b \in K$ gibt, so dass für die konstante Folge $(b, b, b, \dots)$ gilt:

$$\left|(x_n)_{n\geqq 1} - (b)_{n\geqq 1}\right| < r.$$

Der Betrag ist hier der in Satz 6.8 definierte Betrag auf $\widehat{K}$. Da $(x_n)_{n\geqq 1}$ eine Cauchyfolge ist, existiert ein $N \geqq 1$, so dass für alle $n, m \geqq N$ gilt:

$$|x_n - x_m| < \frac{r}{2}.$$

Wir setzen $b = x_N$ und betrachten

$$\left|(x_n)_{n\geqq 1} - (b)_{n\geqq 1}\right| = \left|(x_n - x_N)_{n\geqq 1}\right|.$$

Für $n \geqq N$ gilt

$$|x_n - x_N| < \frac{r}{2}.$$

Nach Definition ist $\left|(x_n - x_N)_{n\geqq 1}\right|$ der Limes für $n \to \infty$ der Beträge $|x_n - x_N|$. Aus $|x_n - x_N| < \frac{r}{2}$ für $n \geqq N$ folgt

$$\lim_{n\to\infty} |x_n - x_N| \leqq \frac{r}{2} < r.$$

Somit liegt die konstante Folge $(b)_{n\geqq 1}$ in $B(a,r)$. □

**Satz 6.10.** *Der Körper $\widehat{K}$ ist vollständig, das heißt, jede Cauchyfolge in $\widehat{K}$ hat einen Grenzwert in $\widehat{K}$.*

**Beweis :** Wir müssen hier nicht nur Cauchyfolgen aus $K$ betrachten, sondern auch Cauchyfolgen aus $\widehat{K}$, also "Folgen von Folgen".

Sei $(\bar{a}_k)_{k\geqq 1}$ eine Cauchyfolge aus $\widehat{K}$. Nach Konstruktion ist $\bar{a}_k = a_k + \mathfrak{N}$ für eine Cauchyfolge $a_k = (a_k^{(n)})_{n\geqq 1}$ aus $K$. Nach Definition des Betrages auf $\widehat{K}$ ist die Folge $(a_k)_{k\geqq 1}$ eine Cauchyfolge in $\widehat{K}$. Nach Lemma 6.9 gibt es für jedes $k \in \mathbb{N}$ ein Element $x_k \in K$, sodass

$$(x_k)_{n\geqq 1} \in B(a_k, \tfrac{1}{k})$$

gilt. Hier bezeichnet $(x_k)_{n\geqq 1}$ die konstante Folge zu $x_k$.
Wir zeigen nun, dass $(x_k)_{k\geqq 1}$ eine Cauchyfolge aus $K$ ist. Nach Voraussetzung ist $(\bar{a}_k)_{\geqq 1}$ eine Cauchyfolge aus $\widehat{K}$. Also existiert für jedes $\varepsilon > 0$ ein $N$ mit $|\bar{a}_k - \bar{a}_l| < \dfrac{\varepsilon}{3}$ für alle $k, l \geqq N$. Daraus folgt in $\widehat{K}$

$$\begin{aligned} |x_k - x_l| &< |x_k - \bar{a}_k| + |\bar{a}_k - \bar{a}_l| + |\bar{a}_l - x_l| \\ &\leqq \frac{1}{k} + \frac{\varepsilon}{3} + \frac{1}{l} \quad \leqq \quad \varepsilon \end{aligned}$$

für $k, l \geqq \max\{3, N\}$. Also ist $a = (x_k)_{k\geqq 1}$ eine Cauchyfolge aus $K$ und somit ein Element in $\mathfrak{C}$. Mit $\bar{a} = (x_k)_{k\geqq 1} + \mathfrak{N}$ bezeichnen wir seine Restklasse in $\widehat{K} = \mathfrak{C}/\mathfrak{N}$.
Wir behaupten nun, dass die gegebene Cauchyfolge $\bar{a}_k \in \widehat{K}$ gegen $\bar{a}$ konvergiert. Dazu untersuchen wir

$$|\bar{a} - \bar{a}_k|\,.$$

Definitionsgemäß ist dies der Grenzwert von $|\, x_n - a_k^{(n)} \,|$ für $n \to \infty$. Nun ist $x_k \in B(a_k, \frac{1}{k})$, was

$$|x_k - \bar{a}_k| = \lim_{n\to\infty} |\, x_k - a_k^{(n)} \,| < \frac{1}{k}$$

impliziert.
Sei $\varepsilon > 0$. Da $(x_k)_k$ eine Cauchyfolge ist, existiert ein $N$ mit $|x_m - x_l| < \dfrac{\varepsilon}{2}$ für alle $m, l \geqq N$. Ohne Einschränkung können wir

$$\frac{1}{N} < \frac{\varepsilon}{3}$$

annehmen (sonst vergrößern wir $N$).
Zu gegebenem $k \geqq N$ existiert nun ein $n_0 = n_0(k)$ mit

$$|\, x_k - a_k^{(n)} \,| < \frac{1}{k} \leqq \frac{1}{N} < \frac{\varepsilon}{3}$$

für alle $n \geqq n_0$. Das impliziert

$$\begin{aligned} |\, x_n - a_k^{(n)} \,| &\leqq |\, x_n - x_k \,| + |\, x_k - a_k^{(n)} \,| \\ &< \frac{2\varepsilon}{3}. \end{aligned}$$

Also ist für festes $k \geqq N$

$$\lim_{n\to\infty} |\, x_n - a_k^{(n)} \,| \leqq \frac{2}{3}\varepsilon < \varepsilon.$$

Somit folgt in der Tat

$$|\bar{a} - \bar{a}_k| \underset{n\to\infty}{\longrightarrow} 0,$$

das heißt, $\bar{a}_k \underset{n\to\infty}{\longrightarrow} \bar{a}$ in $\widehat{K}$. □

Jetzt wollen wir die spezielle Situation eines nicht-archimedischen Betrages untersuchen.

**Proposition 6.11.** *Es sei $K$ ein Körper mit einem nicht-archimedischen Betrag $|\cdot|$. Falls $(a_n)_{n\geqq 1}$ eine Cauchyfolge in $K$ ist, die keine Nullfolge ist, dann wird die Folge $(|a_n|)_{n\geqq 1}$ stationär. Mit anderen Worten: Es gibt ein $n_0$ mit $|a_n| = |a_{n_0}|$ für alle $n \geqq n_0$.*

**Beweis :** Die Folge $(|a_n|)_{n\geqq 1}$ ist eine Cauchyfolge in $\mathbb{R}$ (vgl. den Beweis von Satz 6.8), hat also einen Grenzwert $r \in \mathbb{R}$. Da $(a_n)_{n\geqq 1}$ keine Nullfolge ist, gilt $r > 0$. Also gibt es ein $n_0$, so dass für alle $n \geqq n_0$

$$|a_n| \ \geqq \ \frac{r}{2}$$

ist. Nach Vergrößern von $n_0$ können wir nach der Cauchyfolgen-Eigenschaft annehmen, dass

$$|a_n - a_m| \ < \ \frac{r}{2}$$

für $n, m \geqq n_0$ gilt. Somit gilt für alle $n \geqq n_0$

$$|a_n| \ \geqq \ \frac{r}{2}, \quad |a_{n_0}| \ \geqq \ \frac{r}{2}$$

und $|a_n - a_{n_0}| < \frac{r}{2}$. Nach der nicht-archimedischen Dreiecksungleichung Satz 2.10 folgt hieraus

$$|a_n| = |a_{n_0}| .$$

□

**Korollar 6.12.** *Ist $K$ ein Körper mit einem nicht-archimedischen Betrag und $(a_n)_{n\geqq 1}$ eine konvergente Folge in $K$, deren Grenzwert $a \neq 0$ ist, so wird die Folge der Beträge $(|a_n|)_{n\geqq 1}$ stationär.*

**Beweis :** Das folgt aus Proposition 6.11, denn jede konvergente Folge ist eine Cauchyfolge (Übungsaufgabe). □

Für einen nicht-archimedischen Körper $K$ ist die Definition des Betrages auf der Komplettierung $\widehat{K}$ somit etwas einfacher.

# 7 Der Körper $\mathbb{Q}_p$

Im letzten Kapitel haben wir gesehen, wie man einen Körper bezüglich eines Absolutbetrages komplettieren kann.

**Definition 7.1.** *Sei $p$ eine Primzahl. Die Komplettierung von $\mathbb{Q}$ nach dem $p$-adischen Absolutbetrag $|\cdot|_p$ heißt Körper der $p$-adischen Zahlen. Wir bezeichnen ihn mit $\mathbb{Q}_p$.*

Nach Satz 6.8 gilt:

- $\mathbb{Q}_p$ ist der Quotientenring $\mathfrak{C}/\mathfrak{N}$, wobei $\mathfrak{C}$ die Menge aller Cauchyfolgen in $\mathbb{Q}$ bezüglich $|\cdot|_p$ ist und $\mathfrak{N}$ die Menge aller Nullfolgen.
- $\mathbb{Q}_p$ ist ein Erweiterungskörper von $\mathbb{Q}$.
- Der Betrag $|\cdot|_p$ auf $\mathbb{Q}$ lässt sich zu einem Betrag auf $\mathbb{Q}_p$ fortsetzen. Diesen bezeichnen wir ebenfalls mit $|\cdot|_p$. Nach Konstruktion ist der Betrag eines Elements $(a_n)_{n\geqq 1}+\mathfrak{N}$ in $\mathbb{Q}_p=\mathfrak{C}/\mathfrak{N}$, wobei $(a_n)_{n\geqq 1}$ eine Cauchyfolge ist, gerade $\lim\limits_{n\to\infty}|a_n|_p$.

Ist $(a_n)_{n\geqq 1}$ keine Nullfolge, d.h. gilt $\lim\limits_{n\to\infty}|a_n|_p\neq 0$, so wird nach Proposition 6.11 die Folge $(|a_n|_p)_{n\geqq 1}$ stationär. Daher ist $\left|(a_n)_{n\geqq 1}+\mathfrak{N}\right|_p=|a_{n_o}|_p$ mit $|a_n|_p=|a_{n_0}|_p$ für $n\geqq n_0$. Wir sehen also, dass der $p$-adische Betrag $|\cdot|_p$ auf $\mathbb{Q}_p$ dieselben Werte annimmt wie $|\cdot|_p$ auf $\mathbb{Q}$. Das wollen wir noch einmal festhalten.

**Lemma 7.2.** *Für jedes $x\in\mathbb{Q}_p$ gibt es ein $n\in\mathbb{Z}$ mit $|x|_p=p^{-n}$.*

**Beweis :** Siehe oben. □

**Definition 7.3.** *Für jedes $x\in\mathbb{Q}_p$ definieren wir*

$$v_p(x)=\frac{-\log|x|_p}{\log p},$$

*wobei* log *den natürlichen Logarithmus bezeichnet. Dann ist $v_p:\mathbb{Q}_p\backslash\{0\}\to\mathbb{Z}$ eine Bewertung auf $\mathbb{Q}_p$ (siehe Definition 2.8).*

**Beweis :** Nach Satz 2.10 ist $x\mapsto -\log|x|_p$ eine Bewertung auf $\mathbb{Q}_p$, also auch $x\mapsto\frac{-\log|x|_p}{\log p}$ (Übungsaufgabe). □

Wir haben hier den Quotienten nach $\log p$ gewählt, um eine Fortsetzung der bekannten Funktion $v_p$ auf $\mathbb{Z}\backslash\{0\}$ zu erhalten, die als Exponent von $p$ in der Primfaktorzerlegung definiert war.

**Definition 7.4.** *Den Bewertungsring zu $v_p$ bezeichnen wir mit $\mathbb{Z}_p$. Es gilt also*

$$\begin{aligned}\mathbb{Z}_p &= \{x\in\mathbb{Q}_p : v_p(x)\geqq 0\}\\ &= \{x\in\mathbb{Q}_p : |x|_p\leqq 1\}.\end{aligned}$$

$\mathbb{Z}_p$ enthält den Ring $\mathbb{Z}$ der ganzen Zahlen.

**Lemma 7.5.** *Das Bewertungsideal in $\mathbb{Z}_p$ ist das Hauptideal*

$$p\mathbb{Z}_p:=\{pa : a\in\mathbb{Z}_p\}$$

*Es gilt also:*

$$\{x\in\mathbb{Q}_p : |x|_p<1\}=\{pa : a\in\mathbb{Z}_p\}.$$

**Beweis :** Nach Satz 4.3 ist das Bewertungsideal in $\mathbb{Z}_p$ der offene Einheitsball. Wir müssen also nur

$$\{x \in \mathbb{Q}_p : |x|_p < 1\} = \{pa : a \in \mathbb{Z}_p\}$$

zeigen. Dazu zeigen wir zwei Inklusionen.
Ist $x = pa$ für $a \in \mathbb{Z}_p$, so gilt

$$|x|_p = |p|_p \, |a|_p = \frac{1}{p} \, |a|_p \leqq \frac{1}{p} < 1.$$

Gilt umgekehrt $|x|_p < 1$, so existiert nach Lemma 7.2 ein $n \in \mathbb{Z}$ mit

$$p^{-n} = |x|_p .$$

Aus $|x|_p < 1$ folgt $n \geqq 1$. Daher gilt in $\mathbb{Q}_p$:

$$\left|\frac{x}{p}\right|_p = \left|\frac{1}{p}\right|_p |x|_p = p \, |x|_p = p^{-(n-1)} \leqq 1,$$

denn $(n-1) \geqq 0$. Somit ist $b = \frac{x}{p} \in \mathbb{Z}_p$ und $x = pb$. □

**Korollar 7.6.** *Es ist* $\mathbb{Z}_p \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\}$ *in* $\mathbb{Q}_p$.

**Beweis :** Ist $x \in \mathbb{Z}_p \cap \mathbb{Q}$, so können wir $x = \frac{a}{b}$ als gekürzten Bruch darstellen. Nach Lemma 7.5 folgt aus $px \in p\mathbb{Z}_p$, dass $|px|_p < 1$. Daher ist

$$\left|\frac{pa}{b}\right|_p = p^{-v_p(pa)+v_p(b)} < 1.$$

Falls nun $p$ ein Teiler von $b$ wäre, so könnte $p$ nicht $a$ teilen, also folgte

$$-v_p(pa) + v_p(b) = -1 - v_p(a) + v_p(b) = -1 + v_p(b) \geqq 0,$$

was $p^{-v_p(pa)+v_p(b)} < 1$ widerspricht. Daher teilt $p$ nicht $b$.
Gilt umgekehrt $x = \frac{a}{b} \in \mathbb{Q}$ mit $p \nmid b$, so ist

$$|x|_p = \frac{|a|_p}{|b|_p} = |a|_p \leqq 1,$$

also liegt $x \in \mathbb{Z}_p$. □

**Proposition 7.7.** *i) Für jedes* $x \in \mathbb{Z}_p$ *und jedes* $n \geqq 1$ *existiert ein* $a \in \mathbb{Z}$ *mit*

$$|x - a| \leqq p^{-n}.$$

*Es gibt ein solches Element a im Intervall* $[0, p^n - 1]$.

*ii) Die Inklusion* $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ *hat dichtes Bild.*

*iii) Für jedes* $x \in \mathbb{Z}_p$ *existiert genau eine Cauchyfolge* $(a_n)_{n \geqq 1}$ *mit folgenden Eigenschaften:*

- $a_n \in \mathbb{Z}$ *mit* $0 \leqq a_n \leqq p^n - 1$

- $a_n \underset{n\to\infty}{\longrightarrow} x$
- *Für jedes* $n \geqq 1$ *ist* $a_n \equiv a_{n-1} \mod p^{n-1}$ *in* $\mathbb{Z}$.

**Beweis :**

i) Nach Lemma 6.9 ist $\mathbb{Q}$ dicht in $\mathbb{Q}_p$, das heißt zu $x \in \mathbb{Z}_p \subset \mathbb{Q}_p$ und $n \geqq 1$ existiert ein $q \in \mathbb{Q}$ mit

$$|x - q|_p \leqq p^{-n}.$$

Wir müssen noch zeigen, dass wir $q \in \mathbb{Z}$ wählen können. Aus $|x|_p \leqq 1$ und $|x - q|_p \leqq 1$ folgt zunächst mit der nicht-archimedischen Dreiecksungleichung

$$|q| \leqq \max\{|x|_p, |q - x|_p\} \leqq 1.$$

Also ist $q \in \mathbb{Q} \cap \mathbb{Z}_p$, woraus mit Lemma 7.5 folgt:

$$q = \frac{c}{d}$$

für $c, d \in \mathbb{Z}$ mit $p \nmid d$. Aus $p \nmid d$ folgt, dass es eine ganze Zahl $d$ gibt mit

$$dd' \equiv 1 \mod p^n.$$

(Das folgt aus der Tatsache, dass $p^n$ und $d$ teilerfremd sind.)
Aus $p \nmid d$ folgt $p \nmid d'$. Also gilt

$$|q - cd'|_p = \left|\frac{c}{d} - cd\right|_p = \left|\frac{c(1 - dd')}{dd'}\right|_p = |c|_p |1 - dd'|_p \leqq p^{-n}.$$

Somit gibt es auch eine ganze Zahl, nämlich $a = cd'$ mit

$$|x - a|_p \leqq \max\{|x - q|_p, |q - a|_p\} \leqq p^{-n}.$$

Jede ganze Zahl $a'$ mit

$$|x - a'|_p \leqq p^{-n}$$

erfüllt

$$|a' - a|_p \leqq \max\{|x - a'|_p, |x - a|_p\} \leqq p^{-n},$$

also ist $p^n$ ein Teiler von $a' - a$.
Umgekehrt ist erfüllt jedes

$$a' = a - p^n d$$

mit $d \in \mathbb{Z}$ beliebig die Abschätzung

$$|x - a'|_p \leqq \max\{|x - a|_p, |p^n d|_p\} \leqq p^{-n},$$

also existiert im Intervall $[0, p^n - 1]$ genau eine ganze Zahl $a'$ mit

$$|x - a'| \leqq p^{-n}.$$

ii) Wir müssen zeigen, dass jeder offene Ball in $\mathbb{Z}_p$, also jedes

$$B(x, \varepsilon) = \{y \in \mathbb{Z}_p : |x - y|_p < \varepsilon\}$$

um $x \in \mathbb{Z}_p$ mit Radius $\varepsilon > 0$ ein Element aus $\mathbb{Z}$ enthält. Das folgt aus $i$) (Übungsaufgabe).

iii) Für jedes $n \geqq 1$ gibt es nach $i)$ ein $a_n \in \mathbb{Z}$ mit $a_n \in [0, p^n - 1]$, so dass

$$|x - a_n|_p \leqq p^{-n}.$$

Da $|x - a_n|_p \underset{n\to\infty}{\longrightarrow} 0$, konvergiert die Folge $(a_n)_{n\geqq 1}$ gegen $x$. Insbesondere ist $(a_n)_{n\geqq 1}$ eine Cauchyfolge. Es ist

$$\begin{array}{rcl} |a_n - a_{n-1}|_p & \leqq & \max\{|a_n - x|_p, |x - a_{n-1}|_p\} \\ & \leqq & \max\{p^{-n}, p^{-(n-1)}\} \\ & = & p^{-(n-1)}. \end{array}$$

Also ist $p^{n-1}$ ein Teiler von $a_n - a_{n-1}$, woraus

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

folgt.

□

Wir betrachten nun den Restklassenring $\mathbb{Z}_p/p^n\mathbb{Z}_p$. Seine Elemente sind die Restklassen $a + p^n\mathbb{Z}_p$ für $a \in \mathbb{Z}_p$, wobei gilt: $a + p^n\mathbb{Z}_p = b + p^n\mathbb{Z}_p$ genau dann, wenn $a - b \in p^n\mathbb{Z}_p$. Wir wollen folgende bereits verwendete Tatsachte noch einmal ausdrücklich festhalten.

**Lemma 7.8.** *Für $a, b \in \mathbb{Z}_p$ ist $a - b \in p^n\mathbb{Z}_p$ genau dann, wenn $|a - b| \leqq p^{-n}$.*

**Beweis :** Aus der Definition von $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leqq 1\}$ folgt

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leqq p^{-n}\}.$$

Ist nämlich $x = p^n a$ für ein $a \in \mathbb{Z}_p$, so folgt

$$\begin{array}{rcl} |x|_p & = & |p^n a|_p \\ & = & |p^n|_p |a|_p \\ & = & p^{-n} |a|_p \\ & \leqq & p^{-n}. \end{array}$$

Umgekehrt folgt für jedes $x \in \mathbb{Q}_p$ mit $|x|_p \leqq p^{-n}$, dass $|p^{-n}x|_p = |p^{-n}|_p |x|_p = p^n |x|_p \leqq 1$ ist, woraus $p^{-1}x \in \mathbb{Z}_p$, also $x \in p^n\mathbb{Z}_p$ folgt. Daraus ergibt sich die Behauptung des Lemmas.
□

Also sind zwei Restklassen $a + p^n\mathbb{Z}_p$ und $b + p^n\mathbb{Z}_p$ genau dann gleich, wenn $|a - b|_p \leqq p^{-n}$ gilt. Die Einbettung $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ liefert eine Einbettung $p^n\mathbb{Z} \hookrightarrow p^n\mathbb{Z}_p$. So erhalten wir eine Abbildung

$$\alpha_n : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$$

der Restklassenringe. Diese ist definiert durch

$$\alpha_n(a + p^n\mathbb{Z}) = a + p^n\mathbb{Z}_p.$$

**Definition 7.9.** *Es sei $\alpha : R_1 \longrightarrow R_2$ eine Abbildung zwischen zwei Ringen $R_1, R_2$. Dann heißt $\alpha$ Ringhomomorphismus, falls für alle $x, y \in R_1$ gilt:*

*i)* $\alpha(x+y) = \alpha(x) + \alpha(y)$

*ii)* $\alpha(xy) = \alpha(x)\alpha(y)$

*iii)* $\alpha(1) = 1$.

*Die Abbildung $\alpha$ heißt Isomorphismus von Ringen, falls sie ein bijektiver Ringhomomorphismus ist. In diesem Fall ist die Umkehrabbildung $\alpha^{-1}$ ebenfalls ein Ringhomomorphismus.*

**Proposition 7.10.** *Die Abbildung*

$$\alpha_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$$

*ist ein Isomorphismus von Ringen.*

**Beweis :** Offenbar ist $\alpha_n$ ein Ringhomomorphmismus (Übungsaufgabe). Wir zeigen jetzt die Injektivität. Falls $\alpha_n(a + p^n\mathbb{Z}) = \alpha_n(b + p^n\mathbb{Z})$ für Restklassen $a + p^n\mathbb{Z}, b + p^n\mathbb{Z}$ gilt, so ist $|a-b|_p \leqq p^{-n}$, also teilt $p^n$ die Differenz $(a-b)$. Diese liegt daher in $p^n\mathbb{Z}$, so dass $a + p^n\mathbb{Z} = b + p^n\mathbb{Z}$ folgt. Um die Surjektivität zu prüfen, betrachten wir ein $x \in \mathbb{Z}_p$. Nach Proposition 7.7*i*) existiert ein $a \in \mathbb{Z}$ mit

$$|x - a|_p \leqq p^{-n},$$

also ist $x + p^n\mathbb{Z}_p = a + p^n\mathbb{Z}_p = \alpha_n(a + p^n\mathbb{Z})$. Somit ist $\alpha_n$ auch surjektiv. □

Für jedes $n \geqq 1$ betrachten wir jetzt die Projektionsabbildung

$$\begin{array}{rccc} \varphi_n : & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p/p^n\mathbb{Z}_p \\ & x & \mapsto & x + p^n\mathbb{Z}_p. \end{array}$$

Wir haben soeben gesehen, dass

$$\varphi_n(x) = a + p^n\mathbb{Z}_p$$

für jedes $a \in \mathbb{Z}$ mit $|x-a|_p \leqq p^{-n}$ gilt. Es gibt genau solch ein $a \in \mathbb{Z}$ im Intervall $[0, p^n - 1]$ nach Proposition 7.7*i*). Nun setzen wir alle $\varphi_n$ zu einer Abbildung

$$\begin{array}{rccc} \varphi : & \mathbb{Z}_p & \longrightarrow & \displaystyle\prod_{n\geqq 1} \mathbb{Z}_p/p^n\mathbb{Z}_p \\ & x & \mapsto & (x + p^n\mathbb{Z}_p)_{n\geqq 1} \end{array}$$

in das Produkt aller $\mathbb{Z}_p/p^n\mathbb{Z}_p$ zusammen.
Nach Proposition 7.10 ist $\mathbb{Z}_p/p^n\mathbb{Z}_p \xleftarrow[\alpha_n]{\sim} \mathbb{Z}/p^n\mathbb{Z}$. Durch Verknüpfung mit dem Produkt aller $\alpha_n^{-1}$ erhalten wir eine Abbildung

$$\psi : \mathbb{Z}_p \to \prod_{n\geqq 1} \mathbb{Z}/p^n\mathbb{Z}.$$

**Satz 7.11.** *Die Abbildung $\psi$ ist ein injektiver Ringhomomorphismus. Das Bild von $\psi$ ist der Unterring aller Elemente $(a_n)_{n\geqq 1}$ in $\prod_{n\geqq 1}\mathbb{Z}/p^n\mathbb{Z}$, sodass für alle $n \geqq 1$ unter der Abbildung*

$$\begin{array}{rccc} q_{n+1}: & \mathbb{Z}/p^{n+1}\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} \\ & a+p^{n+1}\mathbb{Z} & \mapsto & a+p^n\mathbb{Z}. \end{array}$$

*$\alpha_{n+1}$ auf $\alpha_n$ abgebildet wird. Also ist $\mathbb{Z}_p$ isomorph zum Unterring all dieser Elemente in $\prod_{n\geqq 1}\mathbb{Z}/p^n\mathbb{Z}$. (Für Topologen: Dieser Isomorphismus wird ein Homöomorphismus, wenn $\mathbb{Z}_p$ seine Betragstopologie bekommt, und wenn $\prod_{n\geqq 1}\mathbb{Z}/p^n\mathbb{Z}$ mit der Produkttopologie zu den diskreten Topologien auf den $\mathbb{Z}/p^n\mathbb{Z}$ versehen wird.)*
*Es sei $\psi(x) = (b_n)_{n\geqq 1}$. Wählen wir für jedes $b_n \in \mathbb{Z}/p^n\mathbb{Z}$ den eindeutigen Vertreter $a_n \in \mathbb{Z}$ mit $0 \leqq a_n \leqq p^n - 1$, so ist die Folge $(a_n)_{n\geqq 1}$ die Cauchyfolge aus Proposition 7.7iii).*

**Beweis :** Da alle $\varphi_n$ Ringhomomorphismen sind, ist auch $\psi$ ein Ringhomomorphismus (Übungsaufgabe). Wir zeigen nun die Injektivität. Ist $\psi(x) = \psi(y)$, so ist $x+p^n\mathbb{Z}_p = y+p^n\mathbb{Z}_p$ für alle $n \geqq 1$. Daraus folgt

$$|x-y|_p \leqq p^{-n}$$

für alle $n \geqq 1$, das heißt, $x = y$. Ist $(a_n)_{n\geqq 1} \in \prod_{n\geqq 1}\mathbb{Z}/p^n\mathbb{Z}$ ein Element im Bild von $\psi$, so gilt $\alpha_n(a_n) = x + p^n\mathbb{Z}_p$. Das Diagramm

$$\begin{array}{ccc} \mathbb{Z}/p^{n+1}\mathbb{Z} & \xrightarrow{q_{n+1}} & \mathbb{Z}/p^n\mathbb{Z} \\ \downarrow{\scriptstyle \alpha_{n+1}} & & \downarrow{\scriptstyle \alpha_n} \\ \mathbb{Z}_p/p^{n+1}\mathbb{Z}_p & \xrightarrow{q_{n+1}} & \mathbb{Z}_p/p^n\mathbb{Z}_p, \end{array}$$

in dem die horizontalen Abbildungen $q^{n+1}$ durch $a + p^{n+1}\mathbb{Z} \mapsto a + p^n\mathbb{Z}$ beziehungsweise $a + p^{n+1}\mathbb{Z}_p \mapsto a + p^n\mathbb{Z}_p$ gegeben sind, ist kommutativ. Also folgt

$$\begin{array}{rcl} \alpha_n \circ q_{n+1}(a_{n+1}) & = & q_{n+1} \circ \alpha_{n+1}(a_{n+1}) \\ & = & q_{n+1}(x + p^{n+1}\mathbb{Z}_p) \\ & = & x + p^n\mathbb{Z}_p. \end{array}$$

Aufgrund der Injektivität von $\alpha_n$ folgt

$$q_{n+1}(a_{n+1}) = a_n.$$

Die letzte Aussage des Satzes folgt aus Proposition 7.7*iii*). □

Dieser Satz zeigt also, dass wir für jedes Element $x \in \mathbb{Z}_p$ eine Cauchyfolge aus $\mathbb{Z}$ konstruieren können, die gegen $x$ konvergiert, indem wir die Quotientenabbildungen $\mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ betrachten.
Wir wollen jetzt noch eine verwandte Darstellung von Elementen aus $\mathbb{Z}_p$ herleiten. Es sei $x \in \mathbb{Z}_p$ und $(a_n)_{n\geqq 1}$ die Cauchyfolge aus ganzen Zahlen aus Proposition 7.7*iii*).
Es gilt also

$$\begin{array}{rcl} x + p^n\mathbb{Z}_p & = & a_n + p^n\mathbb{Z}_p \\ a_{n+1} & \equiv & a_n \mod p^n \\ 0 \leqq & a_n & \leqq p^n - 1. \end{array}$$

Wir betrachten nun für alle $a_n$ ihre $p$-adische Entwicklung.
Da $0 \leqq a_1 \leqq p-1$ ist, ist $a_1 = a_1$ die $p$-adische Entwicklung von $a_1$. Wir setzen $b_0 = a_1$. Weiter ist $a_2 = a_1 \mod p$, also gilt

$$a_2 = b_0 + pb_1$$

für ein $b_1 \in \mathbb{Z}$. Aus $0 \leqq a_2 \leqq p^2 - 1$ folgt

$$-p + 1 \leqq -b_0 \leqq pb_1 \leqq a_2 - b_0 \leqq p^2 - 1,$$

daher ist $0 \leqq b_1 \leqq p - 1$. Also ist

$$a_2 = b_0 + pb_1,$$

somit folgt die $p$-adische Entwicklung von $a_2$.
So fahren wir fort. Falls $a_n = b_0 + pb_1 + \cdots + p^{n-1}b_{n-1}$ mit $b_0, b_1, \ldots, b_{n-1} \in \{0, \ldots, p-1\}$ gilt, so gibt es ein $b_n \in \{0, \ldots, p-1\}$ mit

$$a_{n+1} = b_0 + pb_1 + \cdots + p^{n-1}b_{n-1} + p^n b_n.$$

Die $p$-adische Entwicklung von $a_n$ bildet also den Anfang der $p$-adischen Entwicklung von $a_m$ für alle $m \geqq n$.

**Lemma 7.12.** *In der obigen Situation ist*

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

*das heißt die Folge der Partialsummen*

$$\sum_{k=0}^{n} p^k b_k \in \mathbb{Z}$$

*konvergiert für $n \to \infty$ gegen $x \in \mathbb{Z}_p$.*

**Beweis :** Die Partialsumme $\sum\limits_{k=0}^{n-1} p^k b_k$ ist gleich $a_n$, und es gilt

$$x - a_n \in p^n \mathbb{Z}_p.$$

Also ist $|x - a_n|_p \leqq p^{-n} \underset{n\to\infty}{\longrightarrow} 0$. □

**Korollar 7.13.** *Jedes $x \in \mathbb{Z}_p$ lässt sich auf genau eine Weise als unendliche Reihe von der Form*

$$x = \sum_{k=0}^{\infty} p^k b_k$$

*mit $b_k \in \{0, \ldots, p-1\}$ darstellen.*

**Beweis :** Die Existenz dieser Darstellung folgt aus Lemma 7.12. Ist $x = \sum\limits_{k=0}^{\infty} p^k b'_k$ eine zweite solche Darstellung, so ist

$$x + p\mathbb{Z}_p = b_0 + p\mathbb{Z}_p = b_0 + p\mathbb{Z}_p.$$

Nach Proposition 7.10 folgt daraus

$$b'_0 + p\mathbb{Z} = b_0 + p\mathbb{Z},$$

also $b'_0 = b_0$, da $0 \leqq b_0, b'_0 \leqq p - 1$ gilt.
Wir zeigen die Gleichheit der Koeffizienten nun per Induktion nach $k$. Gilt für alle $i \leqq n-1$

$$b_i = b'_i,$$

so ist

$$\begin{aligned} x + p^{n+1}\mathbb{Z}_p &= (b_0 + pb_1 + \cdots + p^n b_n) + p^{n+1}\mathbb{Z}_p \\ &= (b'_0 + pb'_1 + \cdots + p^n b'_n) + p^{n+1}\mathbb{Z}_p \end{aligned}$$

woraus $p^n b_n - p^n b'_n \in p^{n+1}\mathbb{Z}_p$ folgt. Aus $0 \leqq b_n, b'_n \leqq p^n - 1$ folgt $b_n = b'_n$. □

**Lemma 7.14.** *Für jedes $x \in \mathbb{Q}_p$ ist $\left|p^{-v_p(x)}x\right|_p = 1$. Insbesondere gilt*

$$p^{-v_p(x)}x \in \mathbb{Z}_p.$$

*Insbesondere können wir $x$ durch Multiplikation mit einer $p$-Potenz in den Bewertungsring $\mathbb{Z}_p$ transportieren.*

**Beweis :** Definitionsgemäß ist $v_p(x) = \frac{-\log|x|_p}{\log p}$, also ist $|x|_p = p^{-v_p(x)}$. Daraus folgt

$$\left|p^{-v_p(x)}x\right|_p = \left|p^{-v_p(x)}\right|_p |x|_p = p^{v_p(x)}p^{-v_p(x)} = 1.$$

Daher ist in der Tat $p^{-v_p(x)}x \in \mathbb{Z}_p$. □

**Korollar 7.15.** *Jedes $x \in \mathbb{Q}_p$ lässt sich als*

$$\sum_{k \geq k_0}^{\infty} p^k b_k$$

*mit einem $k_0 \in \mathbb{Z}$ und $b_k \in \{0, \ldots, p-1\}$ darstellen. Wir können $k_0 = v_p(x)$ wählen. Die $b_k$ sind eindeutig bestimmt.*

**Beweis :** Nach Lemma 7.14 ist

$$p^{-v_p(x)}x \in \mathbb{Z}_p,$$

also gilt

$$p^{-v_p(x)}x = \sum_{k=0}^{\infty} p^k b'_k$$

mit eindeutig bestimmten $b'_k \in \{0, \ldots, p-1\}$. Also folgt

$$x = \sum_{k=0}^{\infty} p^{k+v_p(x)} b'_k = \sum_{k=v_p(x)}^{\infty} p^k b_k$$

mit $b_n = b'_{n-v_p(x)}$.
Die Eindeutigkeit der $b_n$ folgt aus der Eindeutigkeitsaussage in Korollar 7.13.

□

Ist $R$ ein beliebiger Ring, so ist die Teilmenge

$$R^\times = \{x \in R : \text{ es gibt ein } y \in R \text{ mit } xy = 1\}$$

die Einheitengruppe von $R$.
(Übungsaufgabe: $R^\times$ ist eine Gruppe bezüglich der Multiplikation.)

**Proposition 7.16.** *Die Eineitengruppe von $\mathbb{Z}_p$ ist*

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

**Beweis :** Wir zeigen zwei Inklusionen.
„$\subset$“: Ist $x \in \mathbb{Z}_p^\times$, so existiert ein $y \in \mathbb{Z}_p$ mit $xy = 1$. Daraus folgt

$$|x|_p |y|_p = |xy|_p = |1|_p = 1.$$

Zusammen mit $|x|_p \leqq 1$ und $|y| \leqq 1$ folgt $|x|_p = 1$.
„$\supset$“: Ist $x \in \mathbb{Q}_p$ mit $|x|_p = 1$, so ist $x \neq 0$, daher existiert $y = \frac{1}{x}$ in $\mathbb{Q}_p$. Aus $xy = 1$ folgt

$$|y|_p = \frac{1}{|x|_p} = 1.$$

Daher ist $|x|_p \leqq 1$ und $|y|_p \leqq 1$, also sind $x$ und $y$ in $\mathbb{Z}_p$. Es folgt $x \in \mathbb{Z}_p^\times$. □

Aus $\mathbb{Z} \subset \mathbb{Z}_p$ folgt $\mathbb{Z}^\times \subset \mathbb{Z}_p^\times$. Die Einheitengruppe von $\mathbb{Z}$ ist

$$\mathbb{Z}^\times = \{1, -1\}.$$

(Übungsaufgabe).
Die Einheitengruppe von $\mathbb{Z}_p^\times$ hat hingegen unendlich viele Elemente, denn es gilt

$$\mathbb{Z}_p^\times \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid ab\},$$

(Übungsaufgabe).

# 8 Hensels Lemma

Sei $p$ eine Primzahl. Dann ist der Restklassenring

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

ein Körper. Der Körper $\mathbb{F}_p$ hat $p$ Elemente. Ist

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

mit $a_1, \ldots, a_n \in \mathbb{Z}$ ein Polynom über den ganzen Zahlen, so können wir den $a_i$ ihre Restklasse $\overline{a}_i$ in $\mathbb{Z}/p\mathbb{Z}$ zuordnen und erhalten ein Polynom

$$\overline{f}(X) = \overline{a}_n X^n + \overline{a}_{n-1} X^{n-1} + \cdots + \overline{a}_1 X + \overline{a}_0$$

über dem Körper $\mathbb{F}_p$. Ist $p$ nicht zu groß, so kann man durch Ausprobieren aller $p$ Elemente in $\mathbb{F}_p$ leicht testen, ob $\overline{f}$ eine Nullstelle in $\mathbb{F}_p$ besitzt. Nun kann es passieren, dass $\overline{f}$ eine Nullstelle in $\mathbb{F}_p$ besitzt, aber $f$ keine Nullstelle in $\mathbb{Z}$, wie das folgende Beispiel zeigt.

**Beispiel:** Das Polynom $f(X) = X^2 + 1$ hat keine Nullstelle in $\mathbb{Z}$ (oder $\mathbb{Q}$), aber $\overline{f}(X) = X^2 + 1$ hat die Nullstelle $1 \in \mathbb{F}_2$.

Eine fundamentale Eigenschaft der $p$-adischen Zahlen ist das Lemma von Hensel, das besagt, dass ein Polynom $f(X)$ mit Koeffizienten in $\mathbb{Z}_p$ unter gewissen Voraussetzungen genau dann

eine Nullstelle in $\mathbb{Z}_p$ hat, wenn $\overline{f}(X)$ eine Nullstelle in $\mathbb{F}_p$ hat. Hier bezeichnen wir wie oben für $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ mit $a_i \in \mathbb{Z}_p$ mit $\overline{f}(X)$ das Polynom

$$\overline{f}(X) = \overline{a}_nX^n + \overline{a}_{n-1}X^{n-1} + \cdots + \overline{a}_1X + \overline{a}_0,$$

wobei $\overline{a}_i$ das Bild von $a_i$ unter der Restklassenabbildung

$$\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \quad \overset{7.10}{\simeq} \quad \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

ist. Ferner bezeichnen wir mit $f'(X)$ die formale Ableitung des Polynoms $f(X)$

$$f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1.$$

**Satz 8.1** (Hensels Lemma)**.** *Es sei $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ ein Polynom in $\mathbb{Z}_p[X]$, das heißt, $a_0, \ldots a_n \in \mathbb{Z}_p$. Falls es ein $c \in \mathbb{F}_p$ gibt mit*

$$\begin{aligned} \overline{f}(c) &= 0, \\ \text{aber } \overline{f}'(c) &\neq 0, \end{aligned}$$

*so existiert ein $r \in \mathbb{Z}_p$ mit*

$$\begin{aligned} f(r) &= 0 \text{ und} \\ \overline{r} &= c. \end{aligned}$$

**Beweis :** Wir konstruieren das gesuchte $r$ als Grenzwert einer Cauchyfolge von ganzen Zahlen. Dazu konstruieren wir mit Induktion nach $k$ eine Folge von ganzen Zahlen $r_1, \ldots, r_k$, so dass folgende Bedingungen gelten

i) $f(r_i) \in p^i\mathbb{Z}_p$ für alle $i \leqq k$

ii) $r_i \equiv r_{i+1} \mod p^k$ für alle $i \leqq k-1$.

Für den Induktionsanfang wählen wir ein $r_1 \in \mathbb{Z}$ mit $\overline{r}_1 = c \in \mathbb{F}_p$. Aus $\overline{f}(c) = 0$ folgt $\overline{f(r_1)} = \overline{f}(\overline{r}_1) = \overline{f}(c) = 0$, also ist $f(r_1) \in p\mathbb{Z}_p$. Somit leistet die Folge $r_1$ das Verlangte, da die Bedingung ii) für $k = 1$ leer ist.
Für den Induktionsschluss nehmen wir an, wir haben eine Folge $r_1, \ldots, r_k$ konstuiert, die den Bedingungen i) und ii) genügt. Dann setzen wir an

$$r_{k+1} = r_k + p^ks$$

mit einem noch zu wählenden $s \in \mathbb{Z}_p$. Jedes solche $r_{k+1}$ erfüllt Bedingung ii) für $i = k$.
Wir suchen ein $s \in \mathbb{Z}_p$, so dass $r_{k+1} = r_k + p^ks$ auch Bedingung i) erfüllt. Dazu berechnen wir

$$\begin{aligned} f(r_{k+1}) &= f(r_k + p^ks) \\ &= a_n(r_k + p^ks)^n + a_{n-1}(r_k + p^ks)^{n-1} + \cdots + a_1(r_k + p^ks) + a_0 \\ &= (a_nr_k^n + a_{n-1}r_k^{n-1} + \cdots + a_1r_k + a_0) \\ &\quad + (a_nn(p^ks)r_k^{n-1} + a_{n-1}(n-1)(p^ks)r_k^{n-2} + \cdots + a_1p^ksr_k) \\ &\quad + \text{Terme, die Vielfache von } p^{2k} \text{ sind.} \end{aligned}$$

Also folgt

$$f(r_{k+1}) - \big(f(r_k) + p^ksf'(r_k)\big) \in p^{k+1}\mathbb{Z}_p.$$

Nun ist nach Induktionsvoraussetzung

$$f(r_k) \in p^k \mathbb{Z}_p,$$

also existiert ein $t \in \mathbb{Z}_p$ mit

$$f(r_k) = p^k t.$$

Ferner gilt nach Induktionsvoraussetzung

$$r_k \equiv r_1 \mod p$$

(Übungsaufgabe), also folgt

$$f'(r_k) - f'(r_1) \in p\mathbb{Z}_p.$$

Nach Voraussetzung ist

$$\overline{f'(r_1)} = \overline{f'}(\overline{r_1}) = \overline{f'}(c) \neq 0,$$

also folgt $\overline{f'(r_k)} \neq 0$ in $\mathbb{F}_p$. Daher existiert in $\mathbb{F}_p$ die Zahl

$$-\overline{t} \left(\overline{f'(r_k)}\right)^{-1}.$$

Wir wählen ein $s \in \mathbb{Z}$ mit

$$\overline{s} = -\overline{t} \left(\overline{f'(r_k)}\right)^{-1}.$$

Dann folgt

$$\overline{s}\ \overline{f'(r_k)} \ \equiv \ -\overline{t} \ \text{ in } \ \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$$

und somit

$$sf'(r_k) + t \in p\mathbb{Z}_p.$$

Daraus folgt wie gewünscht

$$\begin{aligned} f(r_{k+1})\mathbb{Z}_p + p^{k+1}\mathbb{Z}_p &= \left(f(r_k) + p^k s f'(r_k)\right) + p^{k+1}\mathbb{Z}_p \\ &= p^k\left(t + sf'(r_k)\right) + p^{k+1}\mathbb{Z}_p \\ &= 0 + p^{k+1}\mathbb{Z}_p. \end{aligned}$$

Für jedes solche $s \in \mathbb{Z}$ erfüllt die Folge

$$r_1, \ldots, r_k, r_{k+1} = r_k + p^k s$$

daher die Bedingungen i) und ii).
Nach Satz 7.11 gibt es nun genau ein Element $r \in \mathbb{Z}_p$ mit

$$\psi(r) = (r_k + p^k\mathbb{Z}_p)_{k \geqq 1},$$

mit anderen Worten mit

$$r + p^k\mathbb{Z}_p = r_k + p^k\mathbb{Z}_p$$

für alle $k \geqq 1$. Insbesondere ist

$$\overline{r} = r + p\mathbb{Z}_p = r_1 + p\mathbb{Z}_p = c.$$

Ferner gilt für alle $k \geqq 1$ (Übungsaufgabe)

$$f(r) + p^k\mathbb{Z}_p = f(r_k) + p^k\mathbb{Z}_p.$$

Aus $f(r_k) \equiv 0 \mod p^k\mathbb{Z}_p$ folgt also

$$f(r) \in p^k\mathbb{Z}_p \qquad \text{für alle } k \geqq 1$$

und somit $f(r) = 0$ nach Lemma 7.8. □

**Beispiel:** Wir betrachten wieder das Polynom $f(X) = X^2 + 1$. In $\mathbb{F}_5$ gilt $\overline{f}(2) = 0$ und $\overline{f'}(2) = 4 \neq 0$. Daher gibt es nach Hensels Lemma ein $r \in \mathbb{Z}_5$ mit $r^2 = -1$.

Wir wollen jetzt mit Hensels Lemma bestimmen, welche Einheitswurzeln in $\mathbb{Q}_p$ liegen.

**Definition 8.2.** *Ein Element $\zeta$ eines beliebigen Ringes $R$ heißt $m$-te Einheitswurzel in $R$, falls*

$$\zeta^m = 1$$

*gilt.*
*$\zeta$ heißt primitive $m$-te Einheitswurzel, falls für alle $k$ mit $0 < k < m$*

$$\zeta^k \neq 1$$

*gilt.*

In den reellen Zahlen gibt es genau zwei Einheitswurzeln, nämlich 1 und $-1$. Dies gilt erst recht für $\mathbb{Q}$ und $\mathbb{Z}$.

**Definition 8.3.** *Eine Gruppe $G$ heißt zyklisch, falls es ein Element $g \in G$ gibt mit*

$$G = \{g^n : n \in \mathbb{Z}\}.$$

*Das Element $g$ heißt dann Erzeuger von $G$.*

**Proposition 8.4.** *Sei $K$ ein Körper. Dann ist jede endliche Untergruppe der Einheitengruppe $K^\times$ zyklisch.*

**Beweis :** (Wir setzen in diesem Beweis Grundlagen über Ordnungen von Gruppen und Elementen voraus.)
Sei $H \subset K^\times$ eine endliche Untergruppe. Dann hat jedes $h \in H$ endliche Ordnung. Wir wählen ein $h_0 \in H$ mit maximaler Ordnung, das heißt, für alle $h \in H$ gilt

$$\mathrm{ord}(h) \geqq \mathrm{ord}(h_0) =: m.$$

Mit $H_m \subset H$ bezeichnen wir die Teilmenge

$$H_m = \{h \in H : \mathrm{ord}(h) \mid m\}.$$

Dann ist $H_m$ eine Untergruppe von $H$ (Übungsaufgabe).
Jedes $h \in H$ ist Nullstelle des Polynoms

$$X^m - 1.$$

Nach dem Fundamentalsatz der Algebra gibt es in $K$ höchstens $m$ Elemente, die Nullstelle dieses Polynoms sind. Also hat $H_m$ höchstens $m$ Elemente. Da $H_m$ die von $h_0$ erzeugte zyklische Untergruppe

$$\langle h_0 \rangle = \{h_0^k : k \in \mathbb{Z}\}$$

enthält, die wegen $\mathrm{ord}(h_0) = m$ genau $m$ Elemente hat, folgt

$$H_m = \langle h_0 \rangle.$$

Also genügt es zu zeigen, dass

$$H_m = H$$

gilt. Sei $b \in H \backslash H_m$. Dann gilt

$$\mathrm{ord}(b) \nmid m.$$

Also gibt es eine Primzahl $p$ mit

$$v_p(\mathrm{ord}(b)) > v_p(m).$$

Wir schreiben

$$\begin{aligned} m &= m'\alpha \\ \mathrm{ord}(b) &= n'\beta\alpha \end{aligned}$$

mit $\alpha = p^{v_p(m)}, p \nmid m$ und $\beta = p^{v_p(\mathrm{ord}(b))}$. Dann ist $\mathrm{ggT}(n', \alpha) = 1$, $\mathrm{ggT}(m', \beta) = 1$ und $\beta m' > m$.
Nun betrachten wir das Element

$$b^{n'} h_0^{\alpha} \in H.$$

Wir wollen seine Ordnung bestimmen. Aus $(b^{n'} h_0^{\alpha})^r = 1$ folgt $b^{n'r} h_0^{\alpha r} = 1$, also auch

$$1 = (b^{n'r} u^{\alpha r})^{m'} = b^{n'rm'} h_0^{(m'\alpha)r} = b^{n'rm'},$$

da $m = m'\alpha = \mathrm{ord}(h_0)$ ist. Also folgt

$$n'\beta = \mathrm{ord}(b) \mid n'rm',$$

und somit wegen $\mathrm{ggT}(v, m') = 1$

$$\beta \mid r.$$

Analog schließen wir aus

$$1 = (b^{n'r} h_0^{\alpha r})^{\beta} = b^{(n'\beta)r} h_0^{\alpha r\beta} = h_0^{\alpha r\beta},$$

dass $m = m'\alpha$ ein Teiler von $\alpha r\beta$ ist. Daraus folgt wie oben

$$m' \mid r.$$

Insgesamt folgt $\beta m' \mid r$, denn $\beta$ und $r$ sind teilerfremd. Also ist

$$\mathrm{ord}(b^{n'} h_0^{\alpha}) = \beta m' > m$$

im Widerspruch zur Definition von $h_0$. Also kann kein $b \in H \backslash H_m$ existieren und wir erhalten

$$h = H_m.$$

□

Insbesondere ist für jede Primzahl $p$ die multiplikative Gruppe $\mathbb{F}_p^{\times}$ zyklisch. Sie enthält $p-1$ Elemente.

**Satz 8.5.** *Sei $p$ eine Primzahl. Für jeden Teiler $m$ von $p-1$ existiert in $\mathbb{Q}_p$ eine primitive $m$-te Einheitswurzel.*

**Beweis :** Wir betrachten das Polynom $f(X) = X^m - 1$. Da $m$ ein Teiler von $p-1$ ist, gilt $1 \leqq m \leqq p-1$, also gilt insbesondere $p \nmid m$. Wir setzen $d = \frac{p-1}{m}$. Sei $\zeta$ ein Erzeuger der zyklischen Gruppe $\mathbb{F}_p^\times$. Dann gilt $\zeta^{p-1} = 1$, also auch $(\zeta^d)^m = 1$. Somit ist

$$\overline{f}(\zeta^d) = 0.$$

Aus $\overline{f'}(X) = mX^{m-1}$ folgt $\overline{f'}(\zeta^d) = m(\zeta^d)^{m-1}$. Da $p \nmid m$ ist dieser Wert $\neq 0$. Daher können wir mit Hensels Lemma Satz 8.1 schließen, dass es ein $r \in \mathbb{Z}_p$ gibt mit

$$r^m = 1 \quad \text{und} \quad \overline{r} = \zeta^d.$$

Also ist $r$ eine $m$-te Einheitswurzel.
Angenommen $r^k = 1$ für ein $k \leqq m$. Dann folgt $1 = \overline{r}^k = \zeta^{dk}$, also ist $(p-1)$ ein Teiler von $dk = \frac{p-1}{m}k$. Daraus folgt $k = m$. Somit ist $r$ eine primitive $m$-te Einheitswurzel. □

Mit Hilfe von Hensels Lemma können wir auch die Quadratzahlen in $\mathbb{Z}_p$ bestimmen.

**Proposition 8.6.** *Sei $p \neq 2$. Eine Zahl $r \in \mathbb{Z}_p^\times$ ist genau dann ein Quadrat einer Zahl in $\mathbb{Z}_p^\times$, wenn $\overline{r}$ ein Quadrat in $\mathbb{F}_p$ ist, das heißt, wenn es ein $c \in \mathbb{F}_p$ gibt mit*

$$c^2 = \overline{r}.$$

**Beweis :** Falls $r = s^2$ in $\mathbb{Z}_p^\times$ ist, so folgt $\overline{r} = \overline{s}^2$, also ist $\overline{r}$ ein Quadrat in $\mathbb{F}_p$. Wir nehmen umgekehrt an, es gilt $c^2 = \overline{r}$. Dann gilt für das Polynom $f(X) = X^2 - r$:

$$\overline{f}(c) = c^2 - \overline{r} = 0.$$

Gleichzeitig ist $\overline{f'}(c) = 2\overline{c} \neq 0$, denn $p \nmid 2$ und $\overline{c} \neq 0$, da $r \notin p\mathbb{Z}_p$ ist. Somit können wir mit Hensels Lemma Satz 8.1 auf die Existenz eines $s \in \mathbb{Z}_p$ mit $s^2 = r$ schließen. Aus $r \in \mathbb{Z}_p^\times$ folgt $|r| = 1$, also ist auch $|s| = 1$ und daher $s \in \mathbb{Z}_p^\times$. □

**Korollar 8.7.** *Sei $p \neq 2$. Eine Zahl $x \in \mathbb{Q}_p$ ist genau dann ein Quadrat in $\mathbb{Q}_p$, wenn gilt*

*i)* $v_p(x) \in 2\mathbb{Z}$

*ii) Das Element $y = x/p^{v_p(x)} \in \mathbb{Z}_p$ hat die Eigenschaft, dass $\overline{y}$ ein Quadrat in $\mathbb{F}_p$ ist.*

**Beweis :** Wir schreiben nach Lemma 7.14 $x = p^{v_p(x)}y$ mit einem $y \in \mathbb{Z}_p^\times$. Ist $x = x_1^2$ für ein $x_1 \in \mathbb{Q}_p$, so existiert ein $y_1 \in \mathbb{Z}_p^\times$ mit $x_1 = p^{v_p(x_1)}y_1$, also $x = x_1^2 = p^{2v_p(x_1)}y^2$. Zusammen mit Proposition 8.6 folgt die Gültigkeit der Bedingungen *i)* und *ii)*.
Erfüllt $x$ umgekehrt die Bedingungen *i)* und *ii)*, so ist $v_p(x) = 2k$ für ein $k \in \mathbb{Z}$. Also ist $p^{v_p(x)} = (p^k)^2$. Somit ist $x$ genau dann ein Quadrat in $\mathbb{Q}_p$, falls $x/p^{v_p(x)}$ ein Quadrat in $\mathbb{Q}_p$ ist. Nun liegt $x/p^{v_p(x)}$ in $\mathbb{Z}_p^\times$. Bedingung *ii)* garantiert nach Proposition 8.6, dass $x/p^{v_p(x)}$ ein Quadrat in $\mathbb{Z}_p^\times$, also erst recht in $\mathbb{Q}_p$ ist. Daher ist auch $x$ ein Quadrat in $\mathbb{Q}_p$. □

# 9 Analysis in $\mathbb{Q}_p$

Nach Definition 6.1ii) konvergiert eine Folge $(a_n)_{n\geqq 1}$ in $\mathbb{Q}_p$ genau dann gegen $a \in \mathbb{Q}_p$, wenn

$$|a_n - a|_p \underset{n\to\infty}{\longrightarrow} 0.$$

In Lemma 6.2 haben wir gezeigt, das eine Folge $(a_n)_{n\geqq 1}$ in $\mathbb{Q}_p$ genau dann eine Cauchyfolge ist, wenn

$$|a_{n+1} - a_n|_p \underset{n\to\infty}{\longrightarrow} 0$$

konvergiert. Da $\mathbb{Q}_p$ vollständig ist, hat jede Cauchyfolge einen Grenzwert in $\mathbb{Q}_p$.
In Lemma 7.12 haben wir bereits unendliche Reihen in $\mathbb{Q}_p$ kennengelernt. Wir schreiben

$$\sum_{n=0}^{\infty} a_n = a,$$

falls die Folge der Partialsummen

$$b_m = \sum_{n=0}^{m} a_n$$

für $m \to \infty$ gegen $a$ konvergiert. Die Konvergenz unendlicher Reihen ist in $\mathbb{Q}_p$ viel leichter zu testen als in $\mathbb{R}$, wie das folgende Lemma zeigt.

**Lemma 9.1.** *Sei $(a_n)_{n\geqq 0}$ eine Folge in $\mathbb{Q}_p$. Dann konvergiert die unendliche Reihe $\sum\limits_{n=0}^{\infty} a_n$ genau dann in $\mathbb{Q}_p$, wenn $(a_n)_{n\geqq 0}$ eine Nullfolge ist. In diesem Fall gilt*

$$\left|\sum_{n=0}^{\infty} a_n\right|_p \leqq \max_{n\geqq 0} |a_n|_p .$$

**Beweis :** Falls $\sum\limits_{n=0}^{\infty} a_n = a$ konvergiert, so konvergiert definitionsgemäß die Folge $b_m = \sum\limits_{n=0}^{m} a_n$ für $m \to \infty$ gegen $a$. Die Folge der $(b_m)_{m\geqq 0}$ ist also eine Cauchyfolge, daher folgt mit Lemma 6.2

$$|a_{m+1}|_p = |b_{m+1} - b_m|_p \underset{m\to\infty}{\longrightarrow} 0.$$

Also ist $(a_n)_{n\geqq 0}$ eine Nullfolge. Ferner ist nach der nicht-archimedischen Dreiecksungleichung

$$\left|\sum_{n=0}^{m} a_n\right|_p \leqq \max_{0\leqq n\leqq m} |a_n|_p \leqq \max_{n\geqq 0} |a_n|_p ,$$

denn da $|a_m|_p \underset{m\to\infty}{\longrightarrow} 0$ geht, existiert das Maximum über alle $|a_n|_p$. Daraus folgt

$$\left|\sum_{n=0}^{\infty} a_n\right|_p \leqq \max_{n\geqq 0} |a_n|_p .$$

Wir nehmen nun an, dass $(a_n)_{n\geqq 0}$ eine Nullfolge ist. Dann gilt für die Folge $b_m = \sum\limits_{n=0}^{m} a_n$, dass

$$|b_{m+1} - b_m|_p = |a_{m+1}|_p \underset{m\to\infty}{\longrightarrow} 0.$$

Nach Lemma 6.2 ist daher $(b_m)_{m\geqq 0}$ eine Cauchyfolge. Da $\mathbb{Q}_p$ vollständig ist, konvergiert $(b_m)_{m\geqq 0}$ in $\mathbb{Q}_p$. Also konvergiert definitionsgemäß $\sum\limits_{n=0}^{\infty} a_n$ in $\mathbb{Q}_p$. □

Wir definieren nun Stetigkeit und Differenzierbarkeit analog zur reellen Situation.

**Definition 9.2.** *Sei $U \subset \mathbb{Q}_p$ eine offene Teilmenge. Eine Funktion $f : U \to \mathbb{Q}_p$ heißt stetig in $a \in U$, falls es für jedes $\varepsilon > 0$ ein $\delta > 0$ gibt, so dass für jedes $x \in U$ gilt:*

$$|x - a|_p < \delta \quad \Rightarrow \quad |f(x) - f(a)|_p < \varepsilon.$$

*Die Funktion $f$ heißt stetig auf $U$, falls sie in allen $a \in U$ stetig ist.*

**Beispiel:**

i) Die Funktion $x \mapsto x^n$ ist stetig auf $\mathbb{Q}_p$ für jedes $n \in \mathbb{N}$.

ii) Summen und Produkte stetiger Funktionen sind stetig.

**Definition 9.3.** *Sei $U \subset \mathbb{Q}_p$ eine offene Teilmenge. Eine Funktion $f : U \to \mathbb{Q}_p$ heißt differenzierbar in $a \in U$, falls der Grenzwert*

$$f'(a) = \lim_{h \to 0} \frac{f(a+h) - f(a)}{h}$$

*in $\mathbb{Q}_p$ existiert. Die Funktion $f$ heißt differenzierbar auf $U$, falls sie in allen $a \in U$ differenzierbar ist.*

**Beispiel:** Die Funktion $x \mapsto x^n$ ist differenzierbar auf $\mathbb{Q}_p$ für jedes $n \in \mathbb{N}$ (Übungsaufgabe).

Eigenschaften von Stetigkeit und Differenzierbarkeit in der nicht-archimedischen Situation unterscheiden sich allerdings oft von der reellen Situation.

**Beispiel:** Wir betrachten die folgende Funktion $f : \overline{B}(0,1) \to \mathbb{Q}_p$:

$$f(x) = \begin{cases} 0 & \text{für } x \in B(0,1) = \{x : |x|_p < 1\} \\ 1 & \text{für } |x|_p = 1. \end{cases}$$

Dann ist $f$ stetig auf $\overline{B}(0,1)$, denn für alle $x$ mit $|x|_p = 1$ und $y$ mit $|x - y|_p < 1$ ist auch $|y|_p = 1$ nach der nicht-archimedischen Dreiecksungleichung. Also gilt für jedes $\varepsilon > 0$ und jedes $y \in \mathbb{Q}_p$ mit $|x - y|_p < 1$, dass

$$|f(x) - f(y)|_p = 0 < \varepsilon$$

ist. Ferner ist $f$ sogar differenzierbar und $f'(x) = 0$ für alle $x \in \overline{B}(0,1)$. Das ist klar für alle $x \in B(0,1)$. Ist $|x|_p = 1$, so ist für $h$ mit $|h|_p < 1$

$$|x + h|_p = 1,$$

also folgt

$$f(x+h) - f(x) = 0$$

und daher

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} = 0.$$

Solche Funktionen erschweren die Entwicklung eines $p$-adischen Differentialkalküls.
Wir wollen jetzt $p$-adische Potenzreihen studieren.

**Definition 9.4.** *Für eine Folge $(a_n)_{n\geqq 0}$ in $\mathbb{Q}_p$ sei $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n$ die zugehörige (formale) Potenzreihe. Wir sagen, $f$ konvergiert in $x \in \mathbb{Q}_p$, falls die unendliche Reihe*

$$\sum_{n=0}^{\infty} a_n x^n$$

*in $\mathbb{Q}_p$ konvergiert.*

Nach Lemma 9.1 konvergiert $\sum\limits_{n=0}^{\infty} a_n X^n$ genau dann in $x \in \mathbb{Q}_p$, wenn

$$|a_n x^n|_p \underset{n\to\infty}{\longrightarrow} 0.$$

**Satz 9.5.** *Sei $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n$ eine Potenzreihe mit $a_n \in \mathbb{Q}_p$ für alle $n \geqq 0$. Wir definieren*

$$\rho = \frac{1}{\limsup \sqrt[n]{|a_n|_p}},$$

*wobei wir $\rho = 0$ setzen, wenn die Folge $\sqrt[n]{|a_n|_p}$ unbeschränkt ist, und $\rho = \infty$ setzen, wenn $\limsup \sqrt[n]{|a_n|_p} = 0$ ist. Dann gilt:*

*i) Ist $\rho = 0$, so konvergiert $f$ nur in $x = 0$.*

*ii) Ist $\rho = \infty$, so konvergiert $f$ für jedes $x \in \mathbb{Q}_p$.*

*iii) Ist $0 < \rho < \infty$ und $(|a_n|_p \rho^n)_{n\geqq 0}$ eine Nullfolge, so konvergiert $f$ auf $\overline{B}(0,\rho) = \{x : |x|_p \leqq \rho\}$ und für kein weiteres $x$.*

*iv) Ist $0 < \rho < \infty$ und $(|a_n|_p \rho^n)_{n\geqq 0}$ keine Nullfolge, so konvergiert $f$ auf $B(0,1) = \{x : |x|_p < \rho\}$ und für kein weiteres $x$.*

**Beweis :**

i) Ist $\rho = 0$, dann ist die Folge $\sqrt[n]{|a_n|_p}$ unbeschränkt, also ist für kein $x \neq 0$ die Folge

$$|a_n|_p |x|^n = \left(\sqrt[n]{|a_n|_p}\,|x|\right)^n$$

eine Nullfolge.

ii) Ist $\rho = \infty$, so ist $\sqrt[n]{|a_n|_p}$ eine Nullfolge, also ist für jedes $x \in \mathbb{Q}_p$ die Folge

$$\left(\sqrt[n]{|a_n|_p}\,|x|_p\right)^n = |a_n|_p\,|x|_p^n$$

eine Nullfolge, woraus die Konvergenz von $f$ in $x$ folgt.

iii) Sei nun $0 < \rho < \infty$. Wir betrachten zunächst alle $x \in B(0,\rho)$. Die Folge

$$\sqrt[n]{|a_n|_p}\ \rho$$

ist eine Nullfolge. Wegen $|x|_p < \rho$ ist also auch

$$\sqrt[n]{|a_n|_p}\,|x|_p$$

eine Nullfolge, und daher ist

$$|a_n|_p\,|x|_p^n = \left(\sqrt[n]{|a_n|_p}\,|x|_p\right)^n$$

ebenfalls eine Nullfolge. Somit konvergiert $f$ in allen $x \in B(0,\rho)$.
Ist $x \notin \overline{B}(0,\rho)$, gilt also $|x|_p > \rho$, so ist die Folge $\left(\frac{|x|_p}{\rho}\right)^n$ unbeschränkt. Es gibt eine Teilfolge von $\sqrt[n]{|a_n|_p}$, die gegen $1/\rho$ konvergiert. Für diese Folgenglieder ist dann auch $|a_n|_p\,|x|_p^n$ unbeschränkt. Also ist $|a_n|_p\,|x|_p^n$ keine Nullfolge.
Nun nehmen wir an, dass $\left(|a_n|_p\,\rho^n\right)_{n\geqq 0}$ eine Nullfolge ist. Dann ist für jedes $x$ mit $|x|_p = \rho$ auch $\left(|a_n|_p\,|x|_p^n\right)_{n\geqq 0}$ eine Nullfolge, daher konvergiert $f$ in diesem Fall tatsächlich auf ganz $\overline{B}(0,\rho)$. Damit ist *iii)* gezeigt.

iv) Für *iv)* nehmen wir nun noch an, dass $|a_n|_p\,\rho^n$ keine Nullfolge ist. Dann konvergiert tatsächlich $\sum\limits_{n=0}^{\infty} a_n x^n$ für kein $x$ mit $|x|_p = \rho$.

□

Auch im Konvergenzverhalten von Potenzreihen ist die $p$-adische Situation also einfacher als die reelle, wo auf dem Rand des Konvergenzkreises komplizierte Dinge passieren können. Man beachte hierbei, dass $p$-adisch der Kreis mit Radius $\rho$ nicht mit dem topologischen Rand des Balls $B(0,\rho)$ übereinstimmt, denn dieser ist ja abgeschlossen!

**Beispiel:** Wir betrachten die Potenzreihe

$$\begin{aligned} f(X) &= \sum_{n=1}^{\infty}(-1)^{n+1}\tfrac{X^n}{n} \\ &= X - \tfrac{X^2}{2} + \tfrac{X^3}{3} - \tfrac{X^4}{4} + \ldots. \end{aligned}$$

Hier ist $a_n = \frac{(-1)^{n+1}}{n}$, also

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

Wir schreiben $n = p^{v_p(n)}m(n)$ für eine natürliche Zahl $m(n)$ mit $p \nmid n$. Also ist

$$\log n = v_p(n)\log p + \log m(n) \geqq v_p(n)\log p.$$

Also gilt

$$\frac{v_p(n)}{n} \leqq \frac{\log n}{n}\frac{1}{\log p} \underset{n\to\infty}{\longrightarrow} 0.$$

Also folgt

$$\sqrt[n]{|a_n|_p} \;=\; p^{\frac{v_p(n)}{n}} \;\underset{n\to\infty}{\longrightarrow}\; 1,$$

so dass

$$\rho \;=\; \frac{1}{\limsup \sqrt[n]{|a_n|_p}} \;=\; 1$$

ist. Daher konvergiert $f$ nach Satz 9.5 für alle $x \in D(0,1)$. Da

$$|a_n|_p \, \rho^n = \left|\frac{1}{n}\right|_p$$

keine Nullfolge ist (Übungsaufgabe), konvergiert $f$ für kein $x$ außerhalb $B(0,1)$. Die Reihe

$$f(X-1) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(X-1)^n}{n}$$

konvergiert also genau für alle $x \in \mathbb{Q}_p$ mit $|x-1|_p < 1$, also für alle $x \in B(1,1)$.

**Definition 9.6.** *Wir nennen die Funktionen*

$$\begin{array}{rcl} B(1,1) & \to & \mathbb{Q}_p \\ x & \mapsto & \sum\limits_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n} \end{array}$$

*den p-adischen Logarithmus und bezeichnen sie mit* $\log_p$. *Da* $B(0,1) = p\mathbb{Z}_p$ *ist (siehe Lemma 7.5), ist* $B(1,1) = 1 + p\mathbb{Z}_p$.

**Beispiel:** Wir betrachten die Potenzreihe

$$f(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!} = 1 + X + \frac{X^2}{2} + \frac{X^3}{6} + \ldots$$

und wollen ihren Konvergenzradius bestimmen. Dazu müssen wir die Folge

$$\sqrt[n]{|a_n|_p} = \frac{1}{\sqrt[n]{|n!|_p}} = p^{\frac{v_p(n!)}{n}}$$

betrachten.

**Lemma 9.7.** *Es ist*

$$v_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] < \frac{n}{p-1},$$

*wobei* $[\,\cdot\,]$ *die Gauss-Klammer bezeichnet.*

**Beweis :** Die Summe $\sum\limits_{i=0}^{\infty} \left[\frac{n}{p^i}\right]$ ist eine endliche Summe, denn für $p^i > n$ ist $\left[\frac{n}{p^i}\right] = 0$.
Wir zeigen die Gleichheit

$$v_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

per Induktion nach $n$.
Für $n = 1$ sind beide Seiten gleich Null. Angenommen, die behauptete Gleichheit gilt für ein $n \geqq 1$. Ist dann $(n+1)$ kein Vielfaches von $p$, so ist $v_p\left((n+1)!\right) = v_p(n!)$ und $\left[\frac{n}{p^i}\right] = \left[\frac{n+1}{p^i}\right]$ für alle $i \geqq 1$, also stimmt die Behauptung auch für $n+1$. Ist $(n+1) = p^k m$ für ein zu $p$ teilerfremdes $n$, so folgt

$$v_p((n+1)!) = v_p(n!) + k.$$

Andererseits ist $\left[\frac{n+1}{p^i}\right] = \left[\frac{n}{p^i}\right] + 1$ für alle $i$ mit $1 \leqq i \leqq k$ und $\left[\frac{n+1}{p^i}\right] = \left[\frac{n}{p^i}\right]$ für alle $i > k$. Also folgt auch in diesem Fall die Behauptung für $n+1$.
Um die Abschätzung in der Behauptung zu zeigen, verwenden wir

$$\left[\frac{n}{p^i}\right] \leqq \frac{n}{p^i}$$

und die geometrische Reihe. Daraus ergibt sich

$$\begin{aligned} \sum_{i=1}^{\infty} \left[\tfrac{n}{p^i}\right] &< \sum_{i=1}^{\infty} \tfrac{n}{p^i} \\ &= n\left(\sum_{i=0}^{\infty} \tfrac{1}{p^i} - 1\right) = n\left(\tfrac{1}{1-p^{-1}} - 1\right) = n\left(\tfrac{p^{-1}}{1-p^{-1}}\right) \\ &= \tfrac{n}{p-1}. \end{aligned}$$

□

Mit Lemma 9.7 können wir den Konvergenzradius von

$$f(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$$

berechnen. Aus

$$\sqrt[n]{|a_n|_p} = p^{\frac{v_p(n!)}{n}} \leqq p^{\frac{1}{p-1}}$$

folgt

$$\rho \geqq p^{-\frac{1}{1-p}}.$$

Also konvergiert die Reihe für alle $x$ mit

$$|x|_p < p^{-\frac{1}{p-1}}.$$

Sei $x \in \mathbb{Q}_p$ ein Element mit $|x|_p = p^{-\frac{1}{p-1}}$. Dann gilt für jede $p$-Potenz $n = p^m$

$$\begin{aligned} v_p(n!) &= v_p(p^m!) \\ &= 1 + p + \cdots + p^{m-1} \\ &= \tfrac{p^m - 1}{p-1}, \end{aligned}$$

nach Lemma 9.7. Also ist

$$\begin{aligned} \left|\tfrac{1}{p^m!}\right|_p |x|_p^{p^m} &= p^{v_p(p^m!)} p^{-\frac{p^m}{p-1}} \\ &= p^{-\frac{1}{p-1}}. \end{aligned}$$

Also ist $|a_n|_p |x|_p^n$ keine Nullfolge. Nach Satz 9.5 ist somit $f(X)$ genau in $B(0, p^{-\frac{1}{p-1}})$ konvergent.

**Definition 9.8.** *Die Funktion*

$$\begin{array}{ccc} D(0, p^{-\frac{1}{p-1}}) & \longrightarrow & \mathbb{Q}_p \\ X & \mapsto & \sum_{n=0}^{\infty} \frac{x^n}{n!} \end{array}$$

*heißt p-adische Exponentialfunktion. Wir bezeichnen sie auch mit* $\exp_p(x)$.

Anders als über den reellen Zahlen konvergiert die Exponentialreihe nur in einem kleinen Kreis!

Die $p$-adischen Logarithmus- und Exponentialfunktionen erfüllen die bekannten Funktionalgleichungen auf ihren Definitionsbereichen:

$$\begin{array}{rcl} \log_p(ab) & = & \log_p(a) + \log_p(b) \\ \exp_p(a+b) & = & \exp_p(a)\exp_p(b). \end{array}$$