Reelle Bewertungen

Karl Mathiak

TU Braunschweig 1994

Inhaltsverzeichnis

1 Definition reeller Bewertungen

Es sei K ein Körper und $\mathbb{R}_+ := \{x \in \mathbb{R} \mid x \geq 0\}$ die Menge der nicht-negativen reellen Zahlen.

DEFINITION Eine Abbildung

$$| \; | : K \to \mathbb{R}_+ , \quad x \mapsto |x|$$

heißt eine *Bewertung* von K, wenn sie folgenden Axiomen genügt:

(1) $|x| = 0 \iff x = 0$

(2) $|x + y| \leq |x| + |y|$

(3) $|x \cdot y| = |x| \cdot |y|$

für alle $x, y \in K$.

Die bekanntesten bewerteten Körper sind die Körper der reellen und der komplexen Zahlen bezüglich des Absolutbetrages. Der Begriff der Bewertung wurde 1913 von Kürschak eingeführt.

Man unterscheidet zwei Arten von Bewertungen.

DEFINITION Eine Bewertung heißt *nicht-archimedisch*, wenn

($2'$) $|x + y| \leq \max(|x|, |y|)$

für alle $x, y \in K$ gilt. Gilt ($2'$) nicht allgemein, so heißt die Bewertung *archimedisch*. Wegen $\max(|x|, |y|) \leq |x| + |y|$ ist ($2'$) eine Verschärfung von (2).

Der gewöhnliche Absolutbetrag auf $\mathbb{R}$ ist eine archimedische Bewertung. Wegen

$$|1 + 1| = 2 > 1 = \max(|1|, |1|)$$

ist ($2'$) verletzt.

Beispiele

1.) Es sei K ein beliebiger Körper. Durch

$$|x| := \begin{cases} 1 & \text{für } x \neq 0 \\ 0 & \text{für } x = 0 \end{cases}$$

wird, wie man leicht zeigt, auf K eine Bewertung definiert, die man als *triviale Bewertung* bezeichnet.

2.) Es sei $K = \mathbb{Q}$ der Körper der rationalen Zahlen und p eine Primzahl sowie $d \in \mathbb{R}$ mit $0 < d < 1$. Dann wird für alle $x \in \mathbb{Q}$ durch

$$|x| := \begin{cases} 0 & \text{falls } x = 0 \\ d^k & \text{falls } x \neq 0,\ x = p^k \dfrac{u}{v},\ k, u \in \mathbb{Z},\ v \in \mathbb{N},\ (u,p) = (v,p) = 1 \end{cases}$$

eine nicht-archimedische Bewertung auf $\mathbb{Q}$ definiert.

Beweis: Axiom (1) gilt definitionsgemäß. Falls x oder y gleich Null ist, so sind (2′) und (3) trivialerweise erfüllt. Seien also $x, y \neq 0$ mit

$$x = p^k \frac{u}{v} \qquad \text{und} \qquad y = p^{k'} \frac{u'}{v'}$$

mit $k, k', u, u' \in \mathbb{Z}$, $v, v' \in \mathbb{N}$ und $(u,p) = (v,p) = (u',p) = (v',p) = 1$. Ist etwa $k \leq k'$, so folgt

$$|x + y| = \left| p^k \frac{u}{v} + p^{k'} \frac{u'}{v'} \right| = \left| p^k \frac{uv' + p^{k'-k} u'v}{vv'} \right| \leq d^k = \max(|x|, |y|)$$

und

$$|xy| = \left| p^{k+k'} \frac{uu'}{vv'} \right| = d^{k+k'} = |x| \cdot |y| \,.$$

Häufig setzt man $d = \frac{1}{p}$.

Definition Man nennt

$$|x|_p := \begin{cases} 0 & \text{falls } x = 0 \\ \dfrac{1}{p^k} & \text{falls } x \neq 0,\ x = p^k \dfrac{u}{v},\ k, u \in \mathbb{Z},\ v \in \mathbb{N},\ (u,p) = (v,p) = 1 \end{cases}$$

die *p-adische Bewertung* von $\mathbb{Q}$.

Die p-adisdche Bewertung mißt die Teilbarkeit der Zahl x durch p. So ist beispielsweise für $p = 2$

$$|2|_2 = |2 \cdot 11|_2 = |2 \cdot 111|_2 = \frac{1}{2}.$$

Die Folge $(2, 2^2, 2^3, \ldots)$ konvergiert bezüglich der 2-adischen Bewertung gegen Null.

Eigenschaften von Bewertungen

(A) $|1| = 1$.

Beweis: Wegen $|1| = |1 \cdot 1| = |1||1|$ und $|1| \neq 0$ folgt $|1| = \frac{|1|}{|1|} = 1$.

(B) Für $x \neq 0$ ist $|x^{-1}| = |x|^{-1}$.

Beweis: $|x||x^{-1}| = |xx^{-1}| = |1| = 1 \quad \Longrightarrow \quad |x^{-1}| = |x|^{-1}$

(C) Ist $a^n = 1$ für $n \in \mathbb{N}$, so gilt $|a| = 1$.

Beweis: Wegen $|a|^n = |a^n| = |1| = 1$ ist $|a|$ Nullstelle des Polynoms $t^n - 1$. In $\mathbb{R}_+$ besitzt dieses Polynom nur die Nullstelle $t = 1$.

Folgerungen

(a) $|-1| = 1$.

(b) $|-x| = |-1||x| = |x|$.

(c) Ist K ein endlicher Körper, $|K| = q < \infty$, so gilt $a^{q-1} = 1$ für alle $a \neq 0$ nach dem Satz von Lagrange, angewendet auf die multiplikative Gruppe des Körpers. Also ist jede Bewertung eines endlichen Körpers trivial.

(D) $||x| - |y||_\infty \leq |x - y|$, wobei $|\ |_\infty$ den gewöhnlichen Absolutbetrag auf $\mathbb{R}$ bezeichnet.

Beweis: Nach (2) ist

$$|x| = |(x-y) + y| \leq |x - y| + |y|,$$

also

$$|x| - |y| \leq |x - y|\,.$$

Analog folgt, wenn man x und y vertauscht,

$$|y| - |x| \leq |y - x| = |x - y|$$

und damit $||x| - |y||_\infty \leq |x - y|$.

(E) $|\ |$ sei nicht-archimedisch. Ist $|x| < |y|$, so gilt

$$|x + y| = |y|\,.$$

Bemerkung Man bezeichnet diese Regel als *Dominanzprinzip.* In der Summe $x + y$ dominiert der Summand mit dem größeren Wert.

Beweis: Nach (2′) ist

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

Wäre $|x+y| < |y|$, so würde

$$|y| = |(x+y)-x| \leq \max(|x+y|, |-x|) < |y|\,,$$

also ein Widerspruch folgen.

(E′) $|\ |$ sei nicht-archimedisch. Ist $|x| \neq |y|$, so folgt

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

DEFINITION Zwei Bewertungen $|\ |_1$ und $|\ |_2$ heißen *äquivalent*, wenn

$$|x|_1 \leq |y|_1 \iff |x|_2 \leq |y|_2$$

für alle $x, y \in K$ gilt.

Satz 1.1 *Zwei Bewertungen $|\ |_1$ und $|\ |_2$ sind genau dann äquivalent, wenn es eine reelle Zahl $s > 0$ mit*

$$|x|_2 = |x|_1^s$$

für alle $x \in K$ gibt.

Beweis: 1.) Die Funktion $f(x) = x^s$ ist auf $\mathbb{R}_+$ monoton wachsend, also gilt

$$|x|_1 \leq |y|_1 \iff |x|_2 = |x|_1^s \leq |y|_1^s = |y|_2\,.$$

Damit sind $|\ |_1$ und $|\ |_2$ äquivalent.

2.) Seien $|\ |_1$ und $|\ |_2$ äquivalent. Ist etwa $|\ |_1$ die triviale Bewertung, so folgt für $x \neq 0$

$$|1|_1 \leq |x|_1 \leq |1|_1 \quad\Longrightarrow\quad |1|_2 \leq |x|_2 \leq |1|_2\,,$$

also $|x|_2 = 1$, d.h. $|\ |_2$ ist ebenfalls die triviale Bewertung. Folglich gilt die Behauptung mit $s = 1$.

Sei nun $|\ |_1$ nicht trivial. Dann existiert ein $a \in K^\times$ mit $|a|_1 \neq 1$. Man kann $|a|_1 > 1$ annehmen (anderenfalls betrachtet man a^{-1}). Da beide Bewertungen äquivalent sind, ist dann auch $|a|_2 > 1$.

Behauptung: Es gilt

$$(*) \qquad \frac{\log|x|_1}{\log|a|_1} = \frac{\log|x|_2}{\log|a|_2}$$

für alle $x \in K^\times$. (Der Logarithmus kann bezüglich einer beliebigen Basis gewählt werden.)
Beweis: Angenommen, es gibt ein $x \in K^\times$ mit

$$\frac{\log|x|_1}{\log|a|_1} < \frac{\log|x|_2}{\log|a|_2}.$$

Dann gibt es eine rationale Zahl $\frac{n}{m}$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$ zwischen beiden Werten, also

$$\frac{\log|x|_1}{\log|a|_1} < \frac{n}{m} < \frac{\log|x|_2}{\log|a|_2}.$$

Aus der ersten Ungleichung folgt

$$\log|x^m|_1 < \log|a^n|_1\,, \quad \text{also} \quad |x^m|_1 < |a^n|_1\,,$$

und aus der zweiten Ungleichung folgt analog

$$\log|a^n|_2 < \log|x^m|_2\,, \quad \text{also} \quad |a^n|_2 < |x^m|_2\,,$$

im Widerspruch zur Äquivalenz der beiden Bewertungen. Also gilt $(*)$.

Setzt man in $(*)$

$$s = \frac{\log|a|_2}{\log|a|_1} > 0\,,$$

so erhält man

$$s \cdot \log|x|_1 = \log|x|_2\,,$$

also

$$|x|_2 = |x|_1^s$$

für alle $x \in K^\times$. Offensichtlich gilt diese Gleichung auch für $x = 0$ und damit für alle $x \in K$. □

Bemerkung Ist $|\ |_1$ eine Bewertung, so ist $|x|_2 = |x|_1^s$ wieder eine Bewertung, falls $0 < s \leq 1$ ist, denn:

$$|x+y|_1^s \leq (|x|_1 + |y|_1)^s \overset{s\leq 1}{\leq} |x|_1^s + |y|_1^s$$

Für nicht-archimedische Bewertungen gilt dies sogar für alle positiven s. Für archimedische Bewertungen ist die Bedingung $s \leq 1$ notwendig. So ist beispielsweise $|\ |_\infty^2$ wegen $(1+1)^2 > 1^2 + 1^2$ keine Bewertung.

Im folgenden wird mehrfach folgender aus der Analysis bekannte Grenzwert benutzt

Lemma 1.2 *Sind $A, B \in \mathbb{R}$ mit $A > 0$ und $B \geq 0$, so gilt*

$$\lim_{m\to\infty} \sqrt[m]{Am + B} = 1\,.$$

Satz 1.3 *Eine Bewertung ist genau dann nicht-archimedisch, wenn die Menge der Werte*

$$\{|n \cdot 1| \mid n \in \mathbb{N}\}$$

nach oben beschränkt ist.

Beweis: 1.) Es sei $A \in \mathbb{R}$ mit

$$|n \cdot 1| \leq A$$

für alle $n \in \mathbb{N}$. Für $x, y \in K$ mit $|x| \geq |y|$ gilt

$$\begin{aligned} |x+y|^m = |(x+y)^m| &= \left| \sum_{n=0}^{m} \binom{m}{n} x^n y^{m-n} \right| \\ &\leq \sum_{n=0}^{m} \left| \binom{m}{n} \cdot 1 \right| \cdot |x|^n \cdot |y|^{m-n} \\ &\leq A \cdot (m+1) \cdot |x|^m\,, \end{aligned}$$

also

$$|x+y| \leq \sqrt[m]{Am + A} \cdot |x|$$

für alle $m \in \mathbb{N}$. Mit Lemma 1.2 folgt

$$|x+y| \leq 1 \cdot |x| = |x| = \max(|x|, |y|)\,,$$

also ist die Bewertung nicht-archimedisch.

2.) Ist die Bewertung nicht-archimedisch, so ist

$$|x_1 + \ldots + x_n| \leq \max_{1\leq i\leq n} (|x_i|)\,.$$

Speziell gilt also

$$|n \cdot 1| = |1 + \ldots + 1| \leq \max(|1|) = 1\,.$$

Die Werte sind also durch 1 nach oben beschränkt. □

Korollar 1.4 *Hat K eine Charakteristik $p \neq 0$, so ist jede Bewertung von K nicht-archimedisch.*

Korollar 1.5 *Ist eine Bewertung auf K archimedisch, so ist sie auch archimedisch auf jedem Teilkörper von K.*

Korollar 1.6 *Gibt es ein $n \in \mathbb{N}$ mit $|n \cdot 1| < 1$, so ist die Bewertung nicht-archimedisch.*

Beweis: Sei $m \in \mathbb{N}$ und

$$m = a_0 + a_1 \cdot n + \ldots + a_r n^r\,, \qquad r \in \mathbb{N},\ 0 \le a_i < n,$$

die n-adische Darstellung von m. Ist $A = \max\{|k \cdot 1| \mid 0 \le k < n\}$, so gilt

$$|a_i \cdot 1| \le A\,.$$

Dann ist

$$|m \cdot 1| = \left|\sum_{i=0}^{n} a_i n^i\right| \le \sum_{i=0}^{n} |a_i \cdot 1| \cdot |n_i \cdot 1|^i \le A \cdot \sum_{i=0}^{\infty} |n \cdot 1|^i = \frac{A}{1 - |n \cdot 1|}\,,$$

also ist die Menge der Werte

$$\{|m \cdot 1| \mid m \in \mathbb{N}\}$$

nach oben durch $\frac{A}{1-|n\cdot 1|}$ beschränkt. Nach Satz 1.3 ist die Bewertung damit nicht-archimedisch. □

Satz 1.7 (Ostrowski) *Jede nicht-triviale Bewertung von $\mathbb{Q}$ ist äquivalent zum gewöhnlichen Absolutbetrag oder zu einer p-adischen Bewertung.*

Beweis: 1.) Es gibt ein $n \in \mathbb{N}$ mit $|n| < 1$. Nach Korollar 1.6 ist die Bewertung dann nicht-archimedisch, also $|m| \le 1$ für alle $m \in \mathbb{N}$. Sei p die kleinste natürliche Zahl mit $|p| < 1$. p ist eine Primzahl, denn wäre $p = r \cdot s$ mit $1 < r, s < p$, so wäre wegen der Minimalität von p

$$|r| = |s| = 1 \quad \Longrightarrow \quad |p| = |r \cdot s| = |r| \cdot |s| = 1$$

im Widerspruch zur Wahl von p.
Sei nun $n \in \mathbb{Z}$ und $|n| < 1$. Ist

$$n = kp + r$$

mit $0 \le r < p$, $k \in \mathbb{Z}$, so folgt

$$|r| = |n - kp| \le \max(|n|, |kp|) < 1\,.$$

Wegen der Minimalität von p folgt deshalb $r = 0$ und $n = kp$.
Ist also $n \in \mathbb{Z}$ teilerfremd zu p, so gilt $|n| = 1$.
Setze

$$s := -\frac{\log|p|}{\log p} > 0\,.$$

Dann ist
$$\log|p| = \log\frac{1}{p^s}\,,$$
also
$$|p| = \frac{1}{p^s}\,.$$
Sei nun $x \in \mathbb{Q}^\times$ und
$$x = p^k\,\frac{u}{v}$$
mit $k, u \in \mathbb{Z}$, $v \in \mathbb{N}$ und $(u,p) = (v,p) = 1$. Dann ist
$$|x| = \left|p^k\,\frac{u}{v}\right| = |p|^k = \left(\frac{1}{p^s}\right)^k = \left(\frac{1}{p^k}\right)^s = |x|_p^s\,.$$
Diese Gleichung gilt auch für $x = 0$. Damit ist nach Satz 1.1 die vorgegebene Bewertung von $\mathbb{Q}$ zur p-adischen Bewertung äquivalent.

2.) Es sei $|n| \geq 1$ für alle $n \in \mathbb{N}$. Seien $n, m \in \mathbb{N}$, $n, m > 1$. Für $t \in \mathbb{N}$ sei
$$m^t = a_0 + a_1 n + \ldots + a_r n^r$$
mit $r \in \mathbb{N}$, $0 \leq a_i < n$ und $a_r \neq 0$ die n-adische Darstellung von m^t. Nach Axiom (2) ist
$$|a_i| = |1 + \ldots + 1| < n\,,$$
also
$$|m^t| \leq \sum_{i=0}^{r} |a_i| \cdot |n|^i \leq (r+1)\cdot n \cdot |n|^r\,.$$
Wegen $m^t \geq a_r n^r \geq n^r$ ist
$$r \leq t\cdot\frac{\log m}{\log n}\,,$$
also
$$|m|^t \leq n\,\left(t\,\frac{\log m}{\log n} + 1\right)\,\left(|n|^{\frac{\log m}{\log n}}\right)^t\,,$$
also
$$|m| \leq \sqrt[t]{t\,\frac{\log m}{\log n}\cdot n + n}\;\cdot\;|n|^{\frac{\log m}{\log n}}$$
für alle $t \in \mathbb{N}$. Mit Lemma 1.2 folgt
$$|m|^{\frac{1}{\log m}} \leq |n|^{\frac{1}{\log n}}\,.$$
Aus Symmetriegründen ist daher
$$|m|^{\frac{1}{\log m}} = |n|^{\frac{1}{\log n}}\,.$$

Also ist
$$c := |n|^{\frac{1}{\log n}}$$
unabhängig von $n > 1$. Ferner ist $c > 1$, denn andernfalls wäre $|n| = 1$ für alle $n \in \mathbb{N}$ und daher $|\ |$ die triviale Bewertung. Sei
$$s := \frac{1}{\log c} > 0\,.$$
Für $n > 1$ ist dann
$$|n|^s = \left(c^{\log n}\right)^s = c^{\frac{\log n}{\log c}} = n = |n|_\infty\,.$$
Diese Gleichung gilt auch für $n = 1$ und damit für alle $n \in \mathbb{N}$.
Sei $x \in \mathbb{Q}^\times$, also
$$x = \pm\frac{n}{m}$$
mit $n, m \in \mathbb{N}$. Dann ist
$$|x|^s = \left|\pm\frac{n}{m}\right|^s = \frac{|n|^s}{|m|^s} = \frac{n}{m} = |x|_\infty\,.$$
Also ist $|\ |^s$ der gewöhnliche Absolutbetrag und die vorgegebene Bewertung $|\ |$ äquivalent zu diesem. $\square$

Bemerkung Der obige Satz stammt von Ostrowski 1918. (Beweis von Artin 1932).

2 Komplettierung bewerteter Körper

Im folgenden sei K stets ein bewerteter Körper.

Definition (1) Eine Folge (a_n) aus K *konvergiert* gegen $a \in K$

$$:\iff \bigwedge_{\varepsilon>0} \bigvee_{n_0} \bigwedge_{n \geq n_0} |a - a_n| < \varepsilon$$

(2) Eine Folge (a_n) heißt eine *Cauchy-Folge*

$$:\iff \bigwedge_{\varepsilon>0} \bigvee_{n_0} \bigwedge_{n,m \geq n_0} |a_n - a_m| < \varepsilon$$

(3) K heißt *vollständig (komplett)* , wenn jede Cauchy-Folge in K konvergiert.

Wie in der reellen Analysis zeigt man

(A) Der Grenzwert einer konvergenten Folge ist eindeutig, geschrieben $a = \lim a_n$.

(B) Ist $a = \lim a_n$ und $b = \lim b_n$, so gilt

(1) $\lim(a_n \pm b_n) = \lim a_n \pm \lim b_n$
(2) $\lim(a_n \cdot b_n) = \lim a_n \cdot \lim b_n$
(3) $\lim |a_n| = |a|$

(C) Jede konvergente Folge ist eine Cauchy-Folge.

(D) Jede Cauchy-Folge ist beschränkt.

z.B. **Beweis von (D):** Zu $\varepsilon = 1$ gibt es ein $n_0 \in \mathbb{N}$ mit $|a_n - a_m| < 1$ für $n, m \geq n_0$. Es sei

$$M := \max(|a_1|, \ldots, |a_{n_0}|) + 1.$$

Für $n \leq n_0$ gilt dann $|a_n| \leq M$. Für $n > n_0$ ist $|a_n - a_{n_0}| < 1$, also ebenfalls

$$|a_n| = |a_{n_0} + (a_n - a_{n_0})| \leq |a_{n_0}| + 1 \leq M.$$

Folglich gilt $|a_n| \leq M$ für alle $n \in \mathbb{N}$. □

Sei $F :=$ Menge aller Folgen (a_n) aus K. Dann ist F bzgl.

$$(a_n) + (b_n) = (a_n + b_n), \quad (a_n)(b_n) = (a_n b_n)$$

ein kommutativer Ring. Die konstante Folge $(1, 1, \ldots)$ ist das Einselement von F.

Lemma 2.1 *Die Menge C aller Cauchy-Folgen aus K bildet einen Teilring von F.*

Beweis: Es seien $(a_n), (b_n)$ Cauchy-Folgen. Wegen (D) gibt es ein M mit

$$|a_n|, |b_n| \leq M.$$

Zu $\varepsilon > 0$ gibt es ein n_0 mit

$$|a_n - a_m| < \varepsilon, \quad |b_n - b_m| < \varepsilon$$

für $n, m \geq n_0$.

$$|(a_n \pm b_n) - (a_m \pm b_m)| \leq |a_n - a_m| + |b_n - b_m| < 2\varepsilon$$

$$|a_n b_n - a_m b_m| = |a_n(b_n - b_m) + (a_n - a_m)b_m| \leq M|b_n - b_m| + |a_n - a_m|M \leq 2\varepsilon M$$

für $n, m \geq n_0$.

Damit sind $(a_n) \pm (b_n)$, $(a_n)(b_n)$ Cauchy-Folgen. Da die konstanten Folgen zu C gehören, ist $C \neq \emptyset$. □

Definition Es sei R ein Ring. Eine nicht-leere Teilmenge I heißt ein *Ideal*, wenn gilt

$$\begin{array}{lrcl} (1) & a, b \in I & \Longrightarrow & a - b \in I \\ (2) & a \in I, b \in R & \Longrightarrow & ab, ba \in I \end{array}$$

Der *Faktorring* R/I ist definiert als

$$R/I := \{a + I | a \in R\}$$

mit den Verknüpfungen

$$(a + I) + (b + I) = a + b + I, \quad (a + I)(b + I) = ab + I.$$

Lemma 2.2 *Die Menge N der Nullfolgen bildet ein Ideal in C.*

Beweis: Wegen $(0) = (0, 0, \dots) \in N$ ist $N \neq \emptyset$. Weil

$$\lim(a_n - b_n) = \lim a_n - \lim b_n = 0$$

gilt, ist die Differenz zweier Nullfolgen wieder eine Nullfolge.

Es sei $(a_n) \in N, (b_n) \in C$. Nach (D) gilt $|b_n| \leq M$, also $|a_n b_n| \leq |a_n| M$, also $(a_n)(b_n) \in N$. □

Lemma 2.3 *Ist (x_n) eine Cauchy-Folge, die keine Nullfolge ist, so gibt es ein $\varepsilon > 0$ und n_0 mit $|x_n| \geq \varepsilon$ für alle $n \geq n_0$.*

Beweis: Weil (x_n) eine Cauchy-Folge ist, gibt es zu $\varepsilon > 0$ ein n_0 mit $|x_n - x_m| < \varepsilon$ für alle $n, m \geq n_0$. Nehmen wir an, daß die Aussage des Lemmas falsch ist, so gibt es ein $n_1 \geq n_0$ mit $|x_{n_1}| < \varepsilon$. Damit ist für $n \geq n_0$

$$|x_n| \leq |x_n - x_{n_1}| + |x_{n_1}| < 2 \cdot \varepsilon,$$

also (x_n) eine Nullfolge, im Widerspruch zur Voraussetzung. □

Definition Ein Teilkörper K eines bewerteten Körpers $\hat{K}$ heißt **dicht** in $\hat{K}$, wenn gilt

$$\bigwedge_{\varepsilon > 0} \bigwedge_{x \in \hat{K}} \bigvee_{a \in K} |x - a| < \varepsilon.$$

Definition Ein bewerteter Körper $\hat{K}$ heißt eine *Komplettierung* eines bewerteten Körpers K, wenn gilt

1. $\hat{K}$ ist vollständig
2. K liegt dicht in $\hat{K}$
3. Die Bewertung von K ist induziert durch die Bewertung von $\hat{K}$.
   (d.h. $|a|_K = |a|_{\hat{K}}$ für alle $a \in K$)

Satz 2.4 *Jeder bewertete Körper K besitzt eine Komplettierung $\hat{K}$.*

Beweis: 1.) Nach Lemma 2 ist $\hat{K} = C/N$ ein kommutativer Ring mit Eins $(= (1, 1, \ldots) + N)$.
$\hat{K}$ ist sogar ein Körper. Sei $(a_n) + N \neq 0$, also (a_n) keine Nullfolge. Nach Lemma 3 gibt es ein $\varepsilon > 0$ und ein n_0 mit $|a_n| \geq \varepsilon$ für $n \geq n_0$. Definiere

$$b_n := \begin{cases} 0 & \text{für } n < n_0 \\ \frac{1}{a_n} & \text{für } n \geq n_0 \end{cases}$$

Wegen

$$|b_n - b_m| = \left| \frac{1}{a_n} - \frac{1}{a_m} \right| = \left| \frac{a_m - a_n}{a_n a_m} \right| \leq \frac{1}{\varepsilon^2} |a_n - a_m|$$

für $n, m \geq n_0$ ist (b_n) eine Cauchy-Folge und wegen

$$((a_n) + N)((b_n) + N) = (a_n)(b_n) + N = (0, \ldots, 0, 1, 1, \ldots) + N$$

$$= (1, \ldots, 1, 1, 1, \ldots) + N = \underline{1}$$

ist $(b_n) + N$ das Inverse von $(a_n) + N$.

2.) Definition der Bewertung auf $\hat{K}$.
Sei (x_n) eine Cauchy-Folge aus K. Wegen

$$||x_n| - |x_m||_\infty \leq |x_n - x_m|$$

ist $(|x_n|)$ eine Cauchy-Folge in $\mathbb{R}$. Weil $\mathbb{R}$ vollständig ist, existiert $\lim |x_n| \in \mathbb{R}_+$.
Definiere

$$|\ \ |_{\hat{K}} : \hat{K} \to \mathbb{R}_+, \quad x = (x_n) + N \mapsto |x|_{\hat{K}} = \lim |x_n|$$

(a) $|\ \ |_{\hat{K}}$ ist wohldefiniert:
Sei $(x_n) + N = (x'_n) + N$, also $(x_n - x'_n)$ Nullfolge. Wegen

$$|x'_n| \leq |x_n| + |x'_n - x_n|, \quad |x_n| \leq |x'_n| + |x_n - x'_n|$$

ist $\lim |x'_n| = \lim |x_n|$.
(b) $|\,|_{\hat{K}}$ erfüllt die Bewertungsaxiome:
Ist $x = (x_n) + N$, so folgt aus

$$|x|_{\hat{K}} = \lim |x_n| = 0\,,$$

daß (x_n) eine Nullfolge, also $x = (x_n) + N = 0$ ist. Umgekehrt impliziert $x = (x_n) + N = 0$ auch $|x|_{\hat{K}} = 0$.
Die Gültigkeit der Axiome (2) und (3) folgt aus

$$|x + y|_{\hat{K}} = \lim |x_n + y_n| \leq \lim(|x_n| + |y_n|) = |x|_{\hat{K}} + |y_n|_{\hat{K}}$$

und

$$|xy|_{\hat{K}} = \lim |x_n y_n| = \lim(|x_n|\,|y_n|) = |x|_{\hat{K}} |y|_{\hat{K}}\,.$$

3.) Einbettung von K in $\hat{K}$:
Sei $x \in K$. Definiere

$$\varphi : K \to \hat{K}\,, \quad x \mapsto (x) + N = (x, x, \ldots) + N\,.$$

φ ist ein injektiver Homomorphismus und wegen

$$|\varphi(x)|_{\hat{K}} = |(x) + N|_{\hat{K}} = \lim |x| = |x|$$

auch werterhaltend.
4.) $\varphi(K)$ liegt dicht in $\hat{K}$:
Sei $\varepsilon > 0$ und $x = (x_n) + N \in \hat{K}$. Da (x_n) eine Cauchy-Folge in K ist, gibt es ein $n_0 \in \mathbb{N}$ mit

$$|x_n - x_m| < \frac{\varepsilon}{2}$$

für alle $n, m \geq n_0$. Dann gilt für $y = (x_{n_0}) + N = \varphi(x_{n_0}) \in \varphi(K)$

$$|x - y|_{\hat{K}} = \lim |x_n - x_{n_0}| \leq \frac{\varepsilon}{2} < \varepsilon\,.$$

Also liegt $\varphi(K)$ dicht in $\hat{K}$.
5.) $\hat{K}$ ist vollständig:
Es sei (x_n) eine Cauchy-Folge in $\hat{K}$. Da $\varphi(K)$ dicht in $\hat{K}$ liegt, gibt es zu jedem $x_n \in \hat{K}$ ein $a_n \in K$ mit

$$(*) \qquad |x_n - \varphi(a_n)| < \frac{1}{n}.$$

Wegen

$$\begin{aligned} |a_n - a_m|_K &= |\varphi(a_n) - \varphi(a_m)|_{\hat{K}} \\ &= |(x_n - x_m) + (x_m - \varphi(a_m)) - (x_n - \varphi(a_n))|_{\hat{K}} \\ &\leq |x_n - x_m|_{\hat{K}} + \frac{1}{m} + \frac{1}{n} \end{aligned}$$

ist (a_n) eine Cauchy-Folge in K.
Setze $y = (a_n) + N$. Wegen $(*)$ ist $(x_n - y)$ eine Nullfolge in $\hat{K}$. Also ist $\lim x_n = y$, d.h. (x_n) konvergiert.

5.) Identifiziert man nun noch a mit $\varphi(a)$, so ist $K = \varphi(K) \subseteq \hat{K}$ und $\hat{K}$ ist Komplettierung von K. □

Bemerkung Die grundlegende Idee, die Komplettierung über die Menge der Cauchy-Folgen zu gewinnen, stammt von Cantor (1883). Er benutzte sie bei der Konstruktion der reellen Zahlen. Das Verfahren läßt sich fast wörtlich auf allgemeinere Strukturen übertragen, beispielsweise – wie oben ausgeführt – auf bewertete Körper, aber auch auf normierte Vektorräume, metrische Räume usw..

Ergänzungen:

1. Jedes $x \in \hat{K}$ ist Grenzwert einer Cauchy-Folge aus K.
   Beweis: Sei $x \in \hat{K}$. Da K dicht in $\hat{K}$ liegt, gibt es zu jedem $n \in \mathbb{N}$ ein $a_n \in K$ mit
   $$|x - a_n| < \frac{1}{n}.$$
   Also ist $\lim a_n = x$ und (a_n) Cauchy-Folge in K. □

   Bemerkung Diese Darstellung ist nicht eindeutig. Ist $(a_n - a_n')$ eine Nullfolge in K, so gilt auch $\lim a_n' = x$.

Der Dezimaldarstellung einer reellen Zahl, etwa $\sqrt{2} \approx 1,414\ldots$, entspricht die Cauchy-Folge

$$\left(1, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \ldots\right).$$

Die Kettenbruchentwicklung

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ldots}}}$$

liefert die Cauchy-Folge

$$\left(1, \frac{3}{2}, \frac{7}{5}, \ldots\right),$$

die ebenfalls gegen $\sqrt{2}$ konvergiert.

2. Ist K vollständig, so ist $K = \hat{K}$.
   Beweis: Sei $x \in \hat{K}$, etwa $x = \lim a_n$ mit (a_n) Cauchy-Folge in K. Weil K vollständig ist, hat (a_n) einen Grenzwert in K. Wegen der Eindeutigkeit des Grenzwertes ist dies x, also $x \in K$. Also $K = \hat{K}$. $\square$

Definition Es seien K_1 und K_2 bewertete Körper mit den Bewertungen $|\ |_1$ und $|\ |_2$. Eine Abbildung

$$f : K_1 \to K_2$$

heißt *werterhaltend* , wenn

$$|f(x)|_2 = |x|_1$$

für alle $x \in K_1$ gilt.

Satz 2.5 *$\hat{K}_1$ und $\hat{K}_2$ seien Komplettierungen von K_1 bzw. K_2. Ist*

$$f : K_1 \to K_2$$

ein werterhaltender Homomorphismus, so existiert eine eindeutige Fortsetzung

$$\hat{f} : \hat{K}_1 \to \hat{K}_2 ,$$

die ein werterhaltender Homomorphismus ist.

Beweis: 1.) Sei (x_n) eine konvergente Folge in K_1 und $x = \lim x_n$. Dann ist wegen

$$|f(x) - f(x_n)|_2 = |f(x - x_n)|_2 = |x - x_n|_1$$

$(f(x))$ eine konvergente Folge in K_2 mit

$$f(x) = \lim f(x_n)\,.$$

2.) Sei (x_n) eine Cauchy-Folge in K_1. Wegen

$$|f(x_n) - f(x_m)|_2 = |f(x_n - x_m)|_2 = |x_n - x_m|_1$$

für alle $n, m \in \mathbb{N}$ ist dann $(f(x_n))$ eine Cauchy-Folge in K_2.
3.) Definition von $\hat{f}$:
Sei $x \in \hat{K}_1$. Dann gibt es eine Cauchy-Folge (x_n) in K_1 mit

$$x = \lim x_n\,.$$

Nach 2.) ist $(f(x_n))$ eine Cauchy-Folge in K_2, die auf Grund der Vollständigkeit von $\hat{K}_2$ in $\hat{K}_2$ konvergiert. Definiere

$$\hat{f}(x) := \lim f(x_n)\,.$$

Ist nun (x'_n) eine weitere Folge in K_1, die ebenfalls den Grenzwert x besitzt, so ist $(x_n - x'_n)$ eine Nullfolge in K_1. Da f werterhaltend ist, ist dann $(f(x_n) - f(x'_n)$ eine Nullfolge in K_2. Es folgt

$$\lim f(x'_n) = \lim f(x)\,.$$

Damit ist $\hat{f}$ wohldefiniert. Des weiteren ist für $x, y \in \hat{K}_1$ mit den Darstellungen

$$x = \lim x_n \qquad \text{und} \qquad y = \lim y_n\,,$$

wobei (x_n) und (y_n) Cauchy-Folgen in K_1 sind,

$$\hat{f}(x+y) = \lim f(x_n + y_n) = \lim f(x_n) + \lim f(y_n) = \hat{f}(x) + \hat{f}(y)\,,$$
$$\hat{f}(xy) = \lim f(x_n y_n) = \lim f(x_n) \cdot \lim f(y_n) = \hat{f}(x) \cdot \hat{f}(y)$$

und

$$|\hat{f}(x)|_2 = |\lim f(x_n)|_2 = \lim |f(x_n)|_2 = \lim |x_n|_1 = |x|_1\,,$$

also ist $\hat{f}$ ein werterhaltender Homomorphismus. Ferner ist für $x \in K_1$

$$\hat{f}(x) = \lim f(x) = f(x)\,,$$

d.h. $\hat{f}$ ist eine Fortsetzung von f.
4.) Eindeutigkeit von $\hat{f}$:

Sei $\tilde{f}$ eine weitere Fortsetzung von f mit den gleichen Eigenschaften wie $\hat{f}$. Dann ist für $x \in K_1$ mit der Darstellung

$$x = \lim x_n ,$$

wobei (x_n) eine Cauchy-Folge in K_1 ist,

$$|\tilde{f}(x) - f(x_n)|_2 = |\tilde{f}(x) - \tilde{f}(x_n)|_2 = |\tilde{f}(x - x_n)|_2 = |x - x_n|_1 ,$$

also

$$\tilde{f}(x) = \lim f(x_n) = \hat{f}(x) .$$

Damit ist $\tilde{f} = \hat{f}$. □

Korollar 2.6 *Die Komplettierung $\hat{K}$ von K ist bis auf einen werterhaltenden Isomorphismus eindeutig bestimmt.*

Beweis: Es seien $\hat{K}$ und $\tilde{K}$ Komplettierungen von K. Die Einbettungen

$$f : K \to \hat{K} \qquad \text{und} \qquad g : K \to \tilde{K}$$

sind werterhaltende Homomorphismen. Nach Satz 2.5 existieren eindeutige werterhaltende Fortsetzungen

$$\hat{f} : \hat{K} \to \tilde{K} \qquad \text{und} \qquad \tilde{g} : \tilde{K} \to \hat{K} .$$

Für $x \in K$ gilt

$$\hat{f} \circ \tilde{g}(x) = x ,$$

also ist

$$\hat{f} \circ \tilde{g} : \tilde{K} \xrightarrow{\tilde{g}} \hat{K} \xrightarrow{\hat{f}} \tilde{K}$$

eine Fortsetzung von

$$\mathrm{id}_K : K \to K .$$

Da $\hat{f} \circ \tilde{g}$ ein werterhaltender Homomorphismus ist, gilt wegen der Eindeutigkeit der Fortsetzung

$$\hat{f} \circ \tilde{g} = \mathrm{id}_{\tilde{K}} .$$

Enstprechend folgt

$$\tilde{g} \circ \hat{f} = \mathrm{id}_{\hat{K}} .$$

Also sind $\hat{f}$ und $\tilde{g}$ Isomorphismen. □

3 Endliche Erweiterungen vollständiger Körper

Es sei E ein Erweiterungskörper von K, $K \subseteq E$. Dann läßt sich E als Vektorrraum über K auffassen. Dabei heißt

$$[E : K] = \dim_K E$$

der Erweiterungsgrad. Ist $[E : K] = n < \infty$, so heißt E endliche Erweiterung von K. Ist $[E : K] = 2$, so heißt E eine quadratische Erweiterung von K.

Sei $a \in E$. Durch

$$\varphi_a(x) = ax \qquad (x \in E)$$

wird eine lineare Abbildung

$$\varphi_a : E \to E$$

definiert:

$$\varphi_a(x + y) = a(x + y) = ax + ay = \varphi_a(x) + \varphi_a(y)$$
$$\varphi_a(bx) = a\,(bx) = b\,(ax) = b\varphi_a(x) \qquad (x, y \in E,\ b \in K)$$

Eigenschaften

1. Ist $a \neq 0$, so ist φ_a bijektiv.
   Beweis: Aus $\varphi_a(x) = ax = 0$ folgt $x = 0$, also ist φ_a injektiv. Für alle $x \in E$ gilt $x = \varphi_a(a^{-1}x)$, also ist φ_a surjektiv.

2. Für alle $a, b \in E$ gilt $\varphi_{ab} = \varphi_a \circ \varphi_b$.
   Beweis: Es ist
   $$\varphi_{ab}(x) = abx = a\varphi_b(x) = \varphi_a \circ \varphi_b(x)$$
   für alle $x \in E$.

Definition Sei $[E : K] = n < \infty$. Die Abbildung

$$N : E \to K\,, \qquad N(a) = \det \varphi_a \quad \text{für } a \in E$$

heißt *Norm* von E nach K.

Berechnung der Norm

Sei $\{v_1, \ldots, v_n\}$ eine Basis von E über K und für $i = 1, \ldots, n$

$$a \cdot v_i = \sum_{j=1}^{n} a_{ij} v_j \,.$$

Dann wird φ_a durch die (n,n)-Matrix

$$A = (a_{ij})$$

dargestellt. Damit ist

$$N(a) = \det A\,.$$

Beispiel

$E = K(\vartheta)$ sei eine quadratische Erweiterung und

$$\operatorname{Irr}(\vartheta, K) = t^2 + bt + c \qquad (b, c \in K)\,.$$

Dann gilt

$$(*) \qquad \vartheta^2 = -b\vartheta - c\,.$$

Eine Basis von E über K ist $\{1, \vartheta\}$, also

$$E = \{x + \vartheta y \mid x, y \in K\}\,.$$

Zur Berechnung der Norm eines allgemeinen Elementes $x + \vartheta y \in E$ bilden wir

$$(x + \vartheta y) \cdot 1 = x \cdot 1 + y\vartheta$$

$$(x + \vartheta y) \cdot \vartheta = x\vartheta + y\vartheta^2 \overset{(*)}{=} x\vartheta + y\,(-b\vartheta - c) = -yc \cdot 1 + (x - yb) \cdot \vartheta\,.$$

Die Matrix von $\varphi_{x+y\vartheta}$ ist somit

$$A = \begin{pmatrix} x & y \\ -yc & x - by \end{pmatrix},$$

also

$$N(x + y\vartheta) = \begin{vmatrix} x & y \\ -yc & x - by \end{vmatrix} = x^2 - bxy + cy^2\,.$$

Hieraus folgt zum Beispiel $N(\vartheta) = c$ und $N(1 + \vartheta) = 1 - b + c$.

Für $E = \mathbb{C} = \mathbb{R}(i)$, $\operatorname{Irr}(i, \mathbb{R}) = t^2 + 1$, so erhält man

$$N(x + iy) = x^2 + y^2\,,$$

also das Quadrat des gewöhnlichen Absolutbetrages.

Eigenschaften der Norm

(A) $N(ab) = N(a) \cdot N(b)$ für $a, b \in E$.
Beweis: $N(ab) = \det \varphi_{ab} = \det(\varphi_a \circ \varphi_b) = \det \varphi_a \cdot \det \varphi_b = N(a) \cdot N(b)$.

(B) Liegt a im Grundkörper K, und ist $[E : K] = n$, so gilt

$$N(a) = a^n \, .$$

Beweis: Für $a \in K$ ist $\varphi_a = a \cdot \mathrm{id}_E$. Damit wird φ_a durch

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & a \end{pmatrix}$$

dargestellt, also ist $N(a) = a^n$.

(C) Es ist $N(a) = 0$ genau dann, wenn $a = 0$ ist.
Beweis: Ist $a = 0$, so ist $N(a) = 0^n = 0$ nach (B). Ist umgekehrt

$$N(a) = \det \varphi_a = 0 \, ,$$

so ist φ_a nicht regulär. Da φ_a für $a \neq 0$ regulär ist, folgt $a = 0$.

Quadratische Gleichungen in vollständigen Körpern

Eine quadratische Gleichung

$$t^2 + bt + c = 0$$

ist bekanntlich lösbar in $\mathbb{R}$, falls $b^2 \geq 4c$ ist. Für beliebige vollständige Körper gilt

Satz 3.1 *Sei K vollständig und $f(t) = t^2 + bt + c$ mit $b, c \in K$. Gilt $|b|^2 > 4|c|$, so existiert eine Nullstelle von f.*

Beweis: Es sei zunächst $f(t) = t^2 - t - a$, $a \in K$ mit $4|a| < 1$. Wir definieren induktiv

$$x_0 = 1, \qquad x_{n+1} = 1 + \frac{a}{x_n}.$$

1.) Es ist $|x_n| \geq \frac{1}{2}$:
Das gilt für $n = 0$. Sei $|x_n| \geq \frac{1}{2}$, dann ist

$$|x_{n+1}| = \left|1 + \frac{a}{x_n}\right| \geq 1 - \left|\frac{a}{x_n}\right| \geq 1 - \frac{\frac{1}{4}}{\frac{1}{2}} = \frac{1}{2}.$$

2.) (x_n) ist eine Cauchy-Folge in K:

$$\begin{aligned} |x_n - x_{n+1}| &= \left|1 + \frac{a}{x_{n-1}} - 1 - \frac{a}{x_n}\right| = |a| \frac{|x_n - x_{n-1}|}{|x_n||x_{n-1}|} \\ &\leq 4|a| \cdot |x_{n-1} - x_n| \leq \ldots \\ &\leq (4|a|)^n |x_0 - x_1| = |a|(4|a|)^n, \end{aligned}$$

also

$$\begin{aligned} |x_n - x_{n+m}| &= |x_n - x_{n+1} + x_{n+1} - x_{n+2} + \ldots + x_{n+m-1} - x_{n+m}| \\ &\leq \sum_{i=0}^{m} |a|(4|a|)^{n+i} \leq |a|(4|a|)^n \sum_{i=0}^{\infty} (4|a|)^i \leq \frac{|a|(4|a|)^n}{1 - 4|a|}. \end{aligned}$$

Wegen $4|a| < 1$ wird $|x_n - x_{n+m}|$ für große n beliebig klein. Daher ist (x_n) eine Cauchy-Folge. Weil K vollständig ist, existiert $x = \lim x_n$.

3.) Wegen 1. ist $|x_n| \geq \frac{1}{2}$, also $|x| \geq \frac{1}{2}$. Wir erhalten dann

$$\begin{aligned} |x - 1 - \frac{a}{x}| &= |x - 1 - \frac{a}{x} - (x_{n+1} - 1 - \frac{a}{x_n})| \\ &= |x - x_{n+1} + a\left(\frac{1}{x_n} - \frac{1}{x}\right)| \\ &\leq |x - x_{n+1}| + \frac{|a||x - x_n|}{|x_n|\;|x|} \\ &\leq |x - x_{n+1}| + 4|a||x - x_n|. \end{aligned}$$

Weil die rechte Seite für große n beliebig klein wird, folgt $x^2 - x - a = 0$, also ist x Nullstelle von $t^2 - t - a$.

4.) Im allgemeinen Fall

$$f(t) = t^2 + bt + c$$

betrachten wir $f(-bt) = b^2(t^2 - t + \frac{c}{b^2})$. Wegen $4|c| < |b|^2$ ist $4|\frac{-c}{b^2}| < 1$. Also besitzt $t^2 - t + \frac{c}{b^2}$ eine Nullstelle in K, also auch $f(t)$. □

Unter der Voraussetzung, daß die Bewertung nicht-archimedisch ist, läßt sich die Bedingung $4|c| < |b|^2$ abschwächen. Es gilt

Satz 3.2 *Sei K vollständig bezüglich einer nicht-archimedischen Bewertung und $f(t) = t^2 + bt + c$ mit $b, c \in K$. Gilt $|b|^2 > |c|$, so existiert eine Nullstelle von f.*

Dieser Satz ist eine Folgerung des folgenden Verfahrens, das zur Newtonschen iterativen Nullstellenbestimmung reeller differenzierbarer Funktionen analog ist. Die Ableitung eines Polynoms

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_0.$$

bildet man dabei formal

$$f'(t) = n a_n t^{n-1} + \ldots + a_1.$$

Hiermit gilt aufgrund der Binomialformel

$$f(t+h) = f(t) + h \cdot f'(t) + h^2 \cdot g(t,h),$$

wobei $g(t,h)$ ein Polynom in t und h ist.

Satz 3.3 (Newtonsches Näherungsverfahren) *Es sei K vollständig bezüglich einer nicht-archimedischen Bewertung und*

$$B = \{x \in K \mid |x| \leq 1\}.$$

Ist $f(t)$ ein Polynom mit Koeffizienten aus B und existiert ein $x_1 \in B$ mit

$$|f(x_1)| < |f'(x_1)|^2,$$

so besitzt $f(t)$ eine Nullstelle $x \in K$. Es ist

$$|x - x_1| \leq \frac{|f(x_1)|}{|f'(x_1)|}.$$

Beweis: Wir definieren induktiv

$$x_{n+1} := x_n + h_n \qquad \text{mit} \qquad h_n := -\frac{f(x_n)}{f'(x_n)} \qquad (n \in \mathbb{N}).$$

Mit

$$d := \frac{|f(x_1)|}{|f'(x_1)|^2} < 1$$

gilt für $n \in \mathbb{N}$

(1) $x_n \in B$,

(2) $|f'(x_1)| = |f'(x_2)| = \ldots = |f'(x_n)| \leq 1$,

(3) $\quad \dfrac{|f(x_n)|}{|f'(x_n)|^2} \leq d^{2^{n-1}}.$

Der Beweis erfolgt durch Induktion nach n.

a) $n = 1$: Nach Voraussetzung ist $x_1 \in B$. Mit f hat auch f' Koeffizienten aus B, also ist $f'(x_1) \in B$. Ferner ist nach Voraussetzung und der Definition von d

$$\frac{|f(x_1)|}{|f'(x_1)|^2} = d = d^{2^{1-1}}\,.$$

b) Sei (1) – (3) für $k = 1, 2, \ldots, n$ bereits gezeigt. Dann gilt

(1): Wegen

$$|h_n| = \frac{|f(x_n)|}{|f'(x_n)|} = \frac{|f(x_n)|}{|f'(x_n)|^2} \cdot |f'(x_n)| \leq d^{2^{n-1}} \cdot 1 < 1$$

ist $h_n \in B$, also $x_{n+1} = x_n + h_n \in B$.

(2): Es ist

$$f'(x_{n+1}) = f'(x_n + h_n) = f'(x_n) + h_n \cdot g(x_n, h_n)\,,$$

wobei $g(x_n, h_n)$ ein Polynom mit Koeffizienten aus B, also

$$|g(x_n, h_n)| \leq 1$$

ist. Wegen

$$|h_n \cdot g(x_n, h_n)| \leq |h_n| = \frac{|f(x_n)|}{|f'(x_n)|^2} \cdot |f'(x_n)| < |f'(x_n)|$$

ist

$$|f'(x_{n+1})| = \max\left(|f'(x_n)|, |h_n \cdot g(x_n, h_n)|\right) = |f'(x_n)| \leq 1\,.$$

(3): Es gilt

$$f(x_{n+1}) = f(x_n + h_n) = f(x_n) + h_n f'(x_n) + h_n^2 g_1(x_n, h_n)\,,$$

wobei $g_1(x_n, h_n)$ wieder ein Polynom mit Koeffizienten aus B, also

$$|g_1(x_n, h_n)| \leq 1$$

ist. Setzt man $h_n = -\frac{f(x_n)}{f'(x_n)}$ ein, so folgt

$$f'(x_{n+1}) \;=\; \left(\frac{f(x_n)}{f'(x_n)}\right)^2 \cdot g_1(x_n, h_n)\,,$$

also

$$\frac{|f(x_{n+1})|}{|f'(x_{n+1})|^2} \;\leq\; \frac{|f(x_n)|^2}{|f'(x_n)|^4} \leq \left(d^{2^{n-1}}\right)^2 = d^{2^n}\,.$$

c) Aus (2) und (3) folgt für alle $n \in \mathbb{N}$

$$|x_{n+1} - x_n| = |h_n| = \frac{|f(x_n)|}{f'(x_n)|^2}\,|f'(x_n)| \le d^{2^{n-1}}|f'(x_n)| = d^{2^{n-1}}|f'(x_1)|,$$

also wegen

$$x_{n+m} - x_n = \sum_{i=0}^{m-1}(x_{n+i+1} - x_{n+i})$$

erhält man

$$(*) \qquad |x_{n+m} - x_n| \le \max_{0 \le i \le m-1}(|x_{n+i+1} - x_{n+i}|) \le d^{2^{n-1}}|f'(x_1)|$$

für alle $m \in \mathbb{N}$. Damit ist (x_n) eine Cauchy-Folge und konvergiert in K, weil K vollständig ist. Für $n \in \mathbb{N}$ ist nach Definition der Folge (x_n)

$$f(x_n) = (x_n - x_{n+1})\,f'(x_n)\,,$$

also wegen (2)

$$|f(x_n)| \le |x_n - x_{n-1}|.$$

Für $x := \lim x_n$ folgt daher

$$f(x) = 0$$

und aus $(*)$ durch Grenzwertbildung $m \to \infty$ mit $n = 1$

$$|x - x_1| \le d\,|f'(x_1)| = \frac{|f(x_1)|}{|f'(x_1)|}\,.$$

□

Wir kommen nun zum Beweis von Satz 3.2.

Ist speziell

$$f(t) = t^2 + bt + c \text{ und } f'(t) = 2t + b,$$

so erhält man unter der Voraussetzung $|c| < |b|^2$ für $x_1 = -b$

$$|f(x_1)| = |c| < |b|^2 = |f'(x_1)|^2$$

die Existenz einer Nullstelle, also Satz 3.2.

Beispiel

$K = \mathbb{Q}_5$, $f(t) = t^2 + 1$. Für $x_1 = 2$ ist $f(2) = 5$ und $f'(2) = 4$, also

$$|f(2)|_5 = \frac{1}{5} < 1 = |f'(2)|_5^2.$$

Damit existiert eine Nullstelle x. Iteration:

$$x_2 = \frac{3}{4}, \qquad x_3 = -\frac{7}{24}, \qquad x_4 = \frac{527}{336}$$

Der Fehler ist dann

$$|x - x_4| \le \left|\frac{f(x_4)}{f'(x_4)}\right| = \left|\frac{\left(\frac{527}{336}\right)^2 + 1}{2 \cdot \frac{527}{336}}\right| = \left|\frac{5^8}{2 \cdot 336 \cdot 527}\right|_5 = |5|^8 = \frac{1}{5^8}$$

Dies zeigt das gute Konvergenzverhalten des Verfahrens.

Satz 3.4 *Sei K vollständig und E ein Erweiterungskörper vom Grad 2. Dann wird durch*

$$|a|_E = \sqrt{|N(a)|_K} \qquad (a \in E)$$

eine Bewertung auf E definiert, die die Bewertung von K fortsetzt.

Beweis: Nachweis der Bewertungsaxiome:
(1) Für $a \in E$ ist

$$|a|_E = 0 \iff |N(a)|_K = 0 \iff N(a) = 0 \iff a = 0\,.$$

(3) Für $a, b \in E$ gilt

$$|ab|_E = \sqrt{|N(ab)|_K} = \sqrt{|N(a)|_K} \cdot \sqrt{|N(b)|_K} = |a|_E \cdot |b|_E\,.$$

(2) Um Axiom (2), die Dreiecksungleichung nachzuweisen, genügt es wegen

$$|c + d| = |d| \left|1 + \frac{c}{d}\right| \qquad (c, d \in E,\ d \neq 0)$$

nur

$$(*) \qquad |1 + a|_E \le 1 + |a|_E \qquad (a \in E)$$

nachzuweisen.
Ist $a \in K$, so gilt $(*)$, weil $|\ |_E$ eine Fortsetzung von $|\ |_K$ ist. Ist nun $a \in E \backslash K$, so folgt wegen $[E : K] = 2$

$$E = K(a)\,.$$

Sei

$$\operatorname{Irr}(a, K) = t^2 + bt + c \qquad (b, c \in K).$$

Dann ist

$$N(a) = c \qquad \text{und} \qquad N(1+a) = 1 - b + c$$

nach dem obigen Beispiel. Weil $t^2 + bt + c$ als irreduzibles Polynom keine Nullstelle in K besitzt, gilt

$$|b|_K^2 \leq 4\,|c|_K$$

nach Satz 3.1. Es folgt

$$\begin{aligned} |1+a|_E^2 = |N(1+a)|_K &= |1 - b + c|_K \leq 1 + |b|_K + |c|_K \\ &\leq 1 + 2\sqrt{|c|_K} + |c|_K = (1 + \sqrt{|c|_K}\,)^2 = (1 + \sqrt{|N(a)_K|}\,)^2 , \end{aligned}$$

also

$$|1+a|_E \leq 1 + |a|_E .$$

Damit gilt $(*)$. □

Bemerkung Ist K vollständig und $[E : K] = n < \infty$, so ist

$$|a|_E = \sqrt[n]{|N(a)|_K}$$

eine Bewertung auf E. Schwierig ist hierbei jedoch der Nachweis der Dreiecksungleichung.

Sei K ein Körper mit der Bewertung $|\ |$ und V ein Vektorraum über K.

Definition V heißt ein *normierter Raum*, wenn eine Abbildung

$$\|\ \| : V \to \mathbb{R}_+ , \quad u \mapsto \|u\|$$

mit folgenden Eigenschaften existiert:

1. $\|u\| = 0 \iff u = 0$
2. $\|u + v\| \leq \|u\| + \|v\|$
3. $\|a \cdot u\| = |a|\,\|u\|$ $\qquad (u, v \in V,\ a \in K)$

V heißt *vollständig*, wenn jede Cauchy-Folge in V konvergiert.

Beispiele

1.) V sei der Vektorraum aller stetigen Funktionen

$$f : [a,b] \to \mathbb{R} \qquad (a,b \in \mathbb{R})$$

und

$$\|f\| := \sup_{x\in[a,b]} |f(x)|\,.$$

Dann ist V ein normierter Raum über $\mathbb{R}$ und vollständig.

2.) V sei der Vektorraum der differenzierbaren Funktionen

$$f : [a,b] \to \mathbb{R} \qquad (a,b \in \mathbb{R})$$

und

$$\|f\| := \sup_{x\in[a,b]} |f(x)|\,.$$

In diesem Fall ist V ein Vektorraum über $\mathbb{R}$, jedoch nicht vollständig, denn nach dem Satz von WEIERSTRASS läß sich jede stetige Funktion gleichmäßig durch Polynome approximieren.

3.) Sei V ein endlich-dimensionaler Vektorraum über einem bewerteten Körper K und $\{v_1,\ldots,v_n\}$ eine Basis von V. Definiere für

$$u = \sum_{i=1}^{n} a_i v_i \in V\,, \qquad a_i \in K$$

die *Maximumsnorm*

$$\|u\|_0 := \max_{1\le i\le n}(|a_i|)\,.$$

Hierfür gilt:

Ist K vollständig, so ist V bezüglich der Maximumsnorm vollständig.

Beweis: Sei (u_j) eine Cauchy-Folge in V und

$$u_j = \sum_{i=1}^{n} a_{ji} v_i\,, \qquad a_{ji} \in K$$

für alle $j \in \mathbb{N}$. Wegen

$$|a_{ni} - a_{mi}| \le \|u_n - u_m\|_0 \qquad (n,m \in \mathbb{N})$$

sind die Koeffizientenfolgen

$$(a_{ji}) = (a_{1i}, a_{2i}, \ldots)$$

für $i = 1, \ldots, n$ Cauchy-Folgen in K und konvergieren, weil K vollständig ist. Ist

$$a_i = \lim_{j\to\infty} a_{ji} \ \ (1 \le i \le n) \qquad \text{und} \qquad u = \sum_{i=1}^{n} a_i v_i \in V\,,$$

so wird

$$\|u - u_j\|_0 = \max_{1\le i\le n}(|a_i - a_{ji}|)$$

für genügend große $j \in \mathbb{N}$ beliebig klein. Also ist

$$u = \lim u_j\,. \quad \square$$

Satz 3.5 *Sei V ein endlich-dimensionaler Vektorraum mit Norm $\| \ \|$ über einem vollständigen Körper. Dann ist auch V vollständig, und es gibt reelle Zahlen $A, B > 0$ mit*

$$(*) \qquad A\|u\|_0 \le \|u\| \le B\|u\|_0$$

für alle $u \in V$, wobei $\| \ \|_0$ die bezüglich einer Basis von V gebildete Maximumsnorm ist.

Beweis: 1.) Aus $(*)$ folgt die Vollständigkeit von V:
Sei (u_j) eine Cauchy-Folge in V bezüglich $\| \ \|$. Wegen

$$\|u_n - u_m\|_0 \le \frac{1}{A}\,\|u_n - u_m\| \qquad (n, m \in \mathbb{N})$$

ist (u_j) auch eine Cauchy-Folge bezüglich $\| \ \|_0$ und konvergiert daher nach Beispiel 3.) gegen ein $u \in V$ bezüglich $\| \ \|_0$. Wegen

$$\|u - u_j\| \le B\,\|u - u_j\|_0 \qquad (j \in \mathbb{N})$$

ist u auch Grenzwert von (u_j) bezüglich $\| \ \|$.

2.) Wir zeigen $(*)$ durch Induktion nach der Dimension von V. Für $\dim V = 0$ ist nichts zu zeigen. Sei also $\dim V = n \ge 1$ und $(*)$ für alle Vektorräume mit einer Dimension kleiner als n bereits gezeigt. Die Maximumsnorm sei bezüglich der Basis $\{v_1, \ldots, v_n\}$ von V gebildet. Dann ist für alle $u = \sum_{i=1}^{n} a_i v_i \in V$

$$\|u\| = \left\| \sum_{i=1}^{n} a_i v_i \right\| \le \sum_{i=1}^{n} |a_i|\,\|v_i\| \le \left(\sum_{i=1}^{n} \|v_i\| \right) \cdot \|u\|_0\,.$$

Man kann also

$$B = \sum_{i=1}^{n} \|v_i\|$$

setzen. Definiere nun

$$A := \inf\{\|u\| \mid u \in V,\ \|u\|_0 = 1\}\,.$$

Sei $0 \neq u \in V$, $u = \sum_{i=1}^n a_i v_i$. Dann gibt es ein $j \in \{1, \ldots, n\}$ mit $\|u\|_0 = |a_j| > 0$, also ist

$$\left\|\frac{u}{a_j}\right\|_0 = 1\,,$$

und es folgt

$$A \leq \left\|\frac{u}{a_j}\right\| = \frac{1}{|a_j|}\,\|u\|\,,$$

also gilt

$$A\,\|u\|_0 = A\,|a_j| \leq \|u\|\,.$$

Offensichtlich gilt diese Gleichung auch für $u = 0$.

3.) Es ist noch $A > 0$ zu zeigen. Nach Definition ist $A \geq 0$. Annahme: $A = 0$. Dann gibt es eine Folge (u_k) aus V mit

$$\|u\|_0 = 1 \qquad \text{und} \qquad \|u_k\| < \varepsilon_k$$

für alle $k \in \mathbb{N}$, wobei (ε_k) eine reelle Nullfolge ist. Für $k \in \mathbb{N}$ sei

$$u_k = \sum_{i=1}^n a_{ki} v_i \qquad (a_{ki} \in K \text{ für } i = 1, \ldots, n)\,.$$

Dann gibt es wegen

$$\|u_k\|_0 = \max_{1 \leq i \leq n}(|a_{ki}|) = 1$$

zu jedem $k \in \mathbb{N}$ ein $j \in \{1, \ldots, n\}$ mit $|a_{kj}| = 1$. Da für j nur endlich viele Werte in Frage kommen, gibt es ein j, so daß $|a_{kj}| = 1$ für unendlich viele Indizes k gilt. Ohne Beschränkung der Allgemeinheit sei $j = n$. Durch Übergang zu einer Teilfolge, die ebenfalls wieder mit (u_k) bezeichnet wird, kann man daher $|a_{kn}| = 1$ für alle $k \in \mathbb{N}$ annehmen. Für

$$u'_k = \frac{u_k}{a_{kn}} \qquad (k \in \mathbb{N})$$

gilt dann

$$u'_k = \sum_{i=1}^{n-1} a'_{ki} v_i + v_n\,,$$

wobei $a'_{ki} = \dfrac{a_{ki}}{a_{kn}}$ gesetzt ist. Wegen

$$\|u'_k\| = \left\|\frac{u_k}{a_{kn}}\right\| = \frac{1}{|a_{kn}|}\,\|u_k\| = \|u_k\| < \varepsilon_k \qquad (k \in \mathbb{N})$$

bildet (u'_k) ebenfalls eine Nullfolge bezüglich $\| \ \|$. Die Vektoren

$$u'_k - v_n = \sum_{i=1}^{n-1} a_{ki} v_i \qquad (k \in \mathbb{N})$$

bilden daher eine konvergente Folge in V und damit eine Cauchy-Folge im Unterraum

$$V' = \langle v_1, \ldots, v_{n-1} \rangle \, .$$

Wegen $\dim V' = n - 1$ gelten in V' nach Induktion die Ungleichungen $(*)$. V' ist somit vollständig, und die Folge $(u'_k - v_n)$ konvergiert daher in V'. Ihr Grenzwert ist jedoch $-v_n$ im Widerspruch zur linearen Unabhängigkeit der $v_1, \ldots, v_{n-1}$ von v_n. Also ist die Annahme falsch, d.h. es ist $A > 0$. □

Bemerkung Wie Beispiel 2.) zeigt, ist dieser Satz ohne die Voraussetzung, daß V endlich-dimensional ist, im allgemeinen nicht richtig.

Satz 3.6 *Sei K vollständig, E eine endliche Erweiterung von K und $| \ |_E$ eine Fortsetzung der Bewertung $| \ |_K$ von K auf E. Dann ist auch E bezüglich $| \ |_E$ vollständig, und die Bewertungsfortsetzung ist eindeutig.*

Beweis: Durch

$$\|a\| := |a|_E$$

für alle $a \in E$ wird E ein endlich-dimensionaler normierter Vektorraum über dem vollständigen Körper K und ist daher nach Satz 3.5 vollständig.

Seien nun $| \ |_1$ und $| \ |_2$ Fortsetzungen von $| \ |_K$. Nach Satz 3.5 gibt es reelle Zahlen $A, B > 0$ mit

$$A \, \|x\|_0 \le |x|_1 \qquad \text{und} \qquad |x|_2 \le B \, \|x\|_0$$

für alle $x \in E$, wobei $\| \ \|_0$ die Maximumsnorm von E über K ist. Es folgt

$$|x|_2 \le B \, \|x\|_0 \le \frac{B}{A} \, |x|_1$$

für alle $x \in E$. Damit gilt für alle $x \in E$ und alle $n \in \mathbb{N}$

$$|x^n|_2 \le \frac{B}{A} \, |x^n|_1 \, ,$$

also

$$|x|_2 \le \sqrt[n]{\frac{B}{A}} \cdot |x|_1 \, ,$$

woraus für $n \to \infty$

$$|x|_2 \le |x|_1$$

folgt. Aus Symmetriegründen gilt auch die umgekehrte Ungleichung, also ist

$$|x|_2 = |x|_1$$

für alle $x \in E$, d.h. die Bewertungsfortsetzung von K nach E ist eindeutig. $\square$

Bemerkung 1.) Daß eine Fortsetzung $|\ |_E$ stets existiert und durch die Formel

$$|x|_E = \sqrt[n]{|N(x)|_K}\,, \qquad n = [E : K],\ x \in E,$$

explizit gegeben wird, soll später gezeigt werden.
2.) Die Eindeutigkeitsaussage gilt für beliebige algebraische Erweiterungen, da jedes Element in einer endlichen Erweiterung liegt.

4 Archimedische Bewertungen

Lemma 4.1 *K sei ein Körper. Für eine Abbildung*

$$\varphi : K \to \mathbb{R}_+$$

gelte $\varphi(0) = 0$ und $\varphi(xy) = \varphi(x) \cdot \varphi(y)$ für alle $x, y \in K$. Dann sind folgende Aussagen äquivalent:

(1) *$\varphi(x+y) \leq \varphi(x) + \varphi(y)$ für alle $x, y \in K$.*

(2) *$\varphi(x+y) \leq 2 \max(\varphi(x), \varphi(y))$ für alle $x, y \in K$.*

Beweis: (1) $\Rightarrow$ (2): Für alle $x, y \in K$ gilt

$$\varphi(x+y) \leq \varphi(x) + \varphi(y) \leq 2 \cdot \max(\varphi(x), \varphi(y)).$$

(2) $\Rightarrow$ (1): Wir zeigen zunächst für alle $n \in \mathbb{N}$ und alle $x_1, \ldots, x_n \in K$

$$(*) \qquad \varphi(x_1 + \ldots + x_n) \leq 2n \cdot \max_{1 \leq i \leq n}(\varphi(x_i)).$$

Durch Induktion nach $k \in \mathbb{N}$ folgt aus (2)

$$\varphi(x_1 + x_2 + \ldots + x_{2^k}) \leq 2^k \cdot \max_{1 \leq i \leq 2^k}(\varphi(x_i)).$$

Ist $2^k \leq n < 2^{k+1}$, so ergibt sich durch Addition von $(2^{k+1} - n)$ Nullen

$$\begin{aligned} \varphi(x_1 + x_2 + \ldots + x_n) &= \varphi(x_1 + x_2 + \ldots + x_n + 0 + \ldots + 0) \\ &\leq 2^{k+1} \cdot \max_{1 \leq i \leq n}(\varphi(x_i), \varphi(0)) = 2^{k+1} \cdot \max_{1 \leq i \leq n}(\varphi(x_i)) \\ &\leq 2n \cdot \max_{1 \leq i \leq n}(\varphi(x_i)). \end{aligned}$$

Also gilt $(*)$. Insbesondere gilt dann

$$(**) \qquad \varphi(nx) \leq 2n\varphi(x)$$

für alle $n \in \mathbb{N}$ und alle $x \in K$. Damit folgt

$$\begin{aligned} \varphi(x+y)^n = \varphi\left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right) &\leq 2\,(n+1) \max_{0 \leq k \leq n}\left[\varphi\left(\binom{n}{k} x^k y^{n-k}\right)\right] \\ &\overset{(**)}{\leq} 4\,(n+1) \max_{0 \leq k \leq n}\left[\binom{n}{k} \varphi(x)^k \varphi(y)^{n-k}\right] \\ &\leq 4\,(n+1) \sum_{k=0}^{n} \binom{n}{k} \varphi(x)^k \varphi(y)^{n-k} \\ &\leq 4\,(n+1)\,(\varphi(x) + \varphi(y))^n, \end{aligned}$$

also
$$\varphi(x+y) \leq \sqrt[n]{4\,(n+1)} \cdot (\varphi(x)+\varphi(y))\,.$$
Durch Grenzwertbildung $n \to \infty$ folgt
$$\varphi(x+y) \leq \varphi(x)+\varphi(y)\,.$$
□

Lemma 4.2 *Es sei E ein bewerteter Körper, der die komplexen Zahlen $\mathbb{C}$ enthält, $\mathbb{C} \subseteq E$, und dessen Bewertung den gewöhnlichen Absolutbetrag auf $\mathbb{C}$ induziert. Dann ist $E = \mathbb{C}$.*

Beweis: Annahme: $\mathbb{C} \setminus E$: Sei $a \in E \backslash \mathbb{C}$. Die Abbildung
$$f : \mathbb{C} \to \mathbb{R}_+\,, \qquad z \mapsto |a-z|$$
ist stetig. Sei
$$\varrho = \inf\{|a-z| \mid z \in \mathbb{C}\}$$
und
$$A = \{z \in \mathbb{C} \mid |z| \leq |a| + \varrho + 1\}\,.$$
Aus

(1) $$|z-a| \leq \varrho + 1$$

folgt

(2) $$|z| - |a| \leq \varrho + 1\,,$$

also $z \in A$. Für $z \in \mathbb{C}\backslash A$ gilt daher
$$f(z) = |z-a| > \varrho + 1\,.$$
Es folgt
$$\varrho = \inf\{|a-z| \mid z \in \mathbb{C}\} = \inf\{|a-z| \mid z \in A\}\,.$$
Weil f stetig und A kompakt ist, nimmt f das Infimum an. Es gibt also ein $z_0 \in A$ mit
$$\varrho = |a-z_0|\,.$$
Nach Definition ist $\varrho \geq 0$. Wäre $\varrho = 0$, so ergäbe sich $a = z_0 \in A \subseteq \mathbb{C}$, im Widerspruch zur Wahl von a. Also ist $\varrho > 0$.
Sei
$$B = \{z \in \mathbb{C} \mid |a-z| = \varrho\}\,.$$

Weil f mit $f(z) = |a - z|$ stetig ist, ist B abgeschlossen. Wegen $z_0 \in B$ ist B nicht leer.
B ist offen: Sei $z' \in B$ und $z \in U_\varrho(z') = \{z \in \mathbb{C} \mid |z - z'| < \varrho\}$. Dann ist für alle $n \in \mathbb{N}$

$$\begin{aligned}(a - z')^n - (z - z')^n &= \prod_{\substack{\varepsilon \\ \varepsilon^n = 1}} ((a - z') - \varepsilon(z - z')) \\ &= (a - z) \prod_{\substack{\varepsilon \neq 1 \\ \varepsilon^n = 1}} \Big(a - (z' + \varepsilon(z - z'))\Big) \\ &= (a - z) \prod_{i=1}^{n-1} (a - z_i)\,,\end{aligned}$$

wobei $z_i := z' + \varepsilon_i(z - z')$ mit $\varepsilon_i^n = 1$ und $\varepsilon_i \neq 1$ ist. Es folgt

$$|a - z|\varrho^{n-1} \leq |a - z| \prod_{i=1}^{n-1} |a - z_i| \leq |a - z'|^n + |z - z'|^n\,.$$

Für alle $n \in \mathbb{N}$ erhält man somit

$$\varrho \leq |a - z| \leq \varrho \left(1 + \left(\frac{|z - z'|}{\varrho}\right)^n\right)\,,$$

durch Grenzwertbildung $n \to \infty$ wegen

$$\frac{|z - z'|}{\varrho} < 1$$

also

$$|a - z| = \varrho$$

für alle $z \in U_\varrho(z')$. Damit ist $U_\varrho(z') \subseteq B$, also ist B offen. Weil $\mathbb{C}$ zusammenhängend ist, folgt $B = \mathbb{C}$. Für $z \in B$ gilt aber

$$|z| - |a| \leq |a - z| = \varrho\,,$$

also

$$|z| \leq |a| + \varrho\,,$$

d.h. es ist $\mathbb{C} = B \subseteq U_{|a|+\varrho+1}(0)$. Dies ist ein Widerspruch. Also ist $\mathbb{C} = E$. □

Satz 4.3 (Ostrowski) *Sei K bezüglich einer archimedischen Bewertung vollständig. Dann ist K isomorph zu $\mathbb{R}$ oder zu $\mathbb{C}$. Geht man in K zu einer geeigneten äquivalenten Bewertung über, so ist der Isomorphismus werterhaltend.*

Beweis: Da K archimedisch bewertet ist, hat K die Charakteristik Null. Also ist $\mathbb{Q} \subseteq K$. Die Bewertung von K induziert eine archimedische Bewertung auf $\mathbb{Q}$, die nach Satz 1.7 zum gewöhnlichen Absolutbetrag äquivalent ist. Es gibt daher ein $s > 0$, so daß

$$\varphi : K \to \mathbb{R}_+ \quad \varphi(x) := |x|^s$$

für die rationalen Zahlen den gewöhnlichen Absolutbetrag liefert.
φ ist eine Bewertung auf K:
Axiom (1): $\varphi(x) = |x|^s = 0 \iff |x| = 0 \iff x = 0$.
Axiom (3): Für $x, y \in K$ gilt

$$\varphi(xy) = |xy|^s = |x|^s|y|^s = \varphi(x)\varphi(y)\,.$$

Axiom (2): Für $n \in \mathbb{N}$ ist

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k}\,,$$

also

$$\binom{n}{k} \leq 2^n$$

für $0 \leq k \leq n$. Weil $|\ |$ auf $\mathbb{Q}$ zum gewöhnlichen Absolutbetrag äquivalent ist, folgt für alle $n \in \mathbb{N}$ und alle $0 \leq k \leq n$

$$\left|\binom{n}{k}\right| \leq |2|^n\,.$$

Dann ist für $x, y \in K$

$$\begin{aligned}
|x+y|^n &= \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right| \\
&\leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| |x|^k |y|^{n-k} \\
&\leq |2|^n (n+1) \max(|x|, |y|)^n\,,
\end{aligned}$$

also

$$|x+y| \leq \sqrt[n]{n+1} \cdot 2 \cdot \max(|x|, |y|)\,.$$

Durch Grenzwertbildung $n \to \infty$ folgt für alle $x, y \in K$

$$|x+y| \leq |2| \max(|x|, |y|)$$

oder

$$\varphi(x+y) = |x+y|^s \leq |2|^s \max(|x|^s, |y|^s) = 2 \max(\varphi(x), \varphi(y)))\,.$$

Mit Lemma 4.1 folgt damit

$$\varphi(x+y) \leq \varphi(x) + \varphi(y)$$

für alle $x, y \in K$.
Die Bewertungen φ und $|\ |$ sind äquivalent. Damit ist K auch vollständig bezüglich φ. Man kann daher annehmen, daß bereits $|\ |$ auf $\mathbb{Q}$ den gewöhnlichen Absolutbetrag induziert (andernfalls gehe man zu φ über). Hiernach ist dann die Injektion

$$\jmath : \mathbb{Q} \to K\,, \quad x \mapsto x$$

ein werterhaltender Homomorphismus, der sich nach Satz 2.5 zu einem werterhaltenden Homomorphismus

$$\hat{\jmath} : \hat{\mathbb{Q}} = \mathbb{R} \to \hat{K} = K$$

fortsetzen läßt. Definiert man

$$E = \begin{cases} K(\sqrt{-1}) & \text{falls } t^2+1 \text{ irreduzibel über } K \\ K & \text{falls } t^2+1 \text{ reduzibel über } K \end{cases}$$

so kann $\hat{\jmath}$ zunächst algebraisch zu einem Homomorphismus

$$\tilde{\jmath} : \mathbb{C} \to E$$

fortgesetzt werden: Man setzt $\tilde{\jmath}(x+iy) = \hat{\jmath}(x) + \sqrt{-1}\hat{\jmath}(y)$, wobei $\sqrt{-1}$ eine Nullstelle von t^2+1 in E bezeichnet. Wegen $[E:K] \leq 2$ kann die Bewertung von K nach Satz 3.4 zu einer Bewertung auf E fortgesetzt werden. Durch

$$|x|_1 := |\tilde{\jmath}(x)|_E \qquad (x \in \mathbb{C})$$

wird eine Bewertung $|\ |_1$ auf $\mathbb{C}$ induziert, die, weil $\hat{\jmath}$ werterhaltend ist, auf $\mathbb{R}$ den gewöhnlichen Absolutbetrag induziert. Wegen der Eindeutigkeit der Bewertungsfortsetzung bei vollständigen Körpern (Satz 3.6) folgt, daß $|\ |_1$ der gewöhnliche Absolutbetrag auf $\mathbb{C}$ ist. Also ist $\tilde{\jmath}$ werterhaltend.

Da $\tilde{\jmath}(\mathbb{C})$ algebraisch und bezüglich der Bewertung isomorph zu $\mathbb{C}$ ist, folgt $\tilde{\jmath} = E$ nach Lemma 4.2, also

$$\hat{\jmath}(\mathbb{R}) \subseteq K \subseteq E = \tilde{\jmath}(\mathbb{C})\,.$$

Weil der Erweiterunggrad 2 ist, sind nur zwei Fälle möglich: Es ist $K = \hat{\jmath}(\mathbb{R})$ oder $K = \tilde{\jmath}(\mathbb{C})$. Im ersten Fall ist $\hat{\jmath}$, im zweiten Fall ist $\tilde{\jmath}$ der gesuchte werterhaltende Isomorphismus. □

Korollar 4.4 *Jeder archimedisch bewertete vollständige Körper K läßt sich als Unterkörper der komplexen Zahlen auffassen. Seine Bewertung ist dabei äquivalent zum gewöhnlichen Absolutbetrag.*

Beweis: Nach Satz 4.3 ist die Komplettierung $\hat{K}$ von K isomorph zu $\mathbb{R}$ oder zu $\mathbb{C}$. □

Anwendung

Die archimedischen Bewertungen von K ergeben sich durch die Einbettungen von K in $\mathbb{C}$. Zu einem Monomorphismus $f : K \to \mathbb{C}$ ist

$$|x| = |f(x)|_\infty \qquad (x \in K)$$

eine archimedische Bewertung von K, wobei $|\ |_\infty$ den gewöhnlichen Absolutbetrag auf $\mathbb{C}$ bezeichnet. Man erhält auf diese Weise bis auf Äquivalenz alle archimedischen Bewertungen von K.

Beispiele

1.) Es sei $K = \mathbb{Q}(\vartheta)$ und $\operatorname{Irr}(\vartheta, \mathbb{Q}) = t^2 - 2$. Ist

$$f : K \to \mathbb{C}$$

ein Monomorphismus, so gilt aufgrund der Homomorphieeigenschaft $f(a) = a$ für alle $a \in \mathbb{Q}$, also

$$f(a + b\vartheta) = f(a) + f(b) \cdot f(\vartheta) = a + bf(\vartheta)$$

für alle $a, b \in \mathbb{Q}$. Also ist f bereits durch $f(\vartheta)$ bestimmt. Wegen

$$\vartheta^2 - 2 = 0$$

ist

$$f(\vartheta)^2 - 2 = 0\,.$$

Für $f(\vartheta)$ kommen daher nur die Werte $+\sqrt{2}$ und $-\sqrt{2}$ in Frage. Man erhält zwei Einbettungen

$$f_1(a + b\vartheta) = a + b\sqrt{2}\,, \quad f_2(a + b\vartheta) = a - b\sqrt{2} \qquad (a, b \in \mathbb{Q})$$

und damit zwei archimedische Bewertungen

$$|a + b\vartheta|_1 = |f_1(a + b\vartheta)|_\infty = |a + b\sqrt{2}|_\infty$$
$$|a + b\vartheta|_1 = |f_1(a + b\vartheta)|_\infty = |a - b\sqrt{2}|_\infty$$

Diese Bewertungen sind nicht äquivalent, denn es ist

$$|1 + \vartheta|_1 = 1 + \sqrt{2} = 2{,}414\ldots > 1$$

und

$$|1 + \vartheta|_2 = |1 - \sqrt{2}|_\infty = 0{,}414\ldots < 1\,.$$

2.) Es sei $K = \mathbb{Q}(\vartheta)$ und $\mathrm{Irr}\,(\vartheta, \mathbb{Q}) = t^2 + 2$. Für $f(\vartheta)$ kommen die Werte $+\sqrt{-2}$ und $-\sqrt{-2}$ in Frage, also

$$f_1(a + b\vartheta) = a + bi\sqrt{2} \quad \text{und} \quad f_2(a + b\vartheta) = a - bi\sqrt{2}$$

für $a, b \in \mathbb{Q}$, wobei i die imaginäre Einheit ist. Man erhält

$$|a + b\vartheta|_1 = |a + bi\sqrt{2}|_\infty = \sqrt{a^2 + 2b^2}$$

und

$$|a + b\vartheta|_2 = |a - bi\sqrt{2}|_\infty = \sqrt{a^2 + 2b^2}\,.$$

für alle $a, b \in \mathbb{Q}$, also sind beide Bewertungen gleich (obwohl f_1 und f_2 verschieden sind).

5 Vollständige diskret bewertete Körper

Satz 5.1 *Eine Bewertung ist genau dann nicht-archimedisch, wenn der* Ganzheitsbereich

$$B = \{x \in K \mid |x| \leq 1\}$$

ein Teilring von K ist.

Beweis: 1.) Sei $|\ |$ nicht-archimedisch. Sind $x, y \in B$, so gilt wegen

$$|x - y| \leq \max(|x|, |y|) \leq 1 \qquad \text{und} \qquad |xy| = |x|\,|y| \leq 1$$

$x - y \in B$ und $xy \in B$. Wegen $0 \in B$ ist $B \neq \emptyset$. Also ist B ein Teilring von K.
2.) Sei nun B Teilring von K. Für $x, y \in K^\times$ gelte $|x| \leq |y|$. Dann ist

$$|y^{-1}x| = |y^{-1}|\,|x| = |y|^{-1}|x| \leq 1$$

also ist $y^{-1}x \in B$. Wegen $1 \in B$ ist damit auch $1 + y^{-1}x \in B$. Es folgt

$$|1 + y^{-1}x| \leq 1 \quad \Longrightarrow \quad |x + y| \leq |y| = \max(|x|, |y|)\,.$$

Für $|x| \geq |y|$ analog. □

Satz 5.2 $E := \{x \in K \mid |x| = 1\}$ *ist die Einheitengruppe von B.*

Beweis: 1.) Ist $x \in B$ und $|x| = 1$, so ist $|x^{-1}| = 1$, also $x^{-1} \in B$, also x invertierbar in B und damit eine Einheit.
2.) Ist x eine Einheit in B, also $|x| \leq 1$ und $|x^{-1}| = |x|^{-1} \leq 1$, so ist $|x| = 1$. □

Satz 5.3 $M := \{x \in K \mid |x| < 1\}$ *ist ein Ideal in B.*

Beweis: Es ist $0 \in M$. Ferner gilt

$$\begin{aligned} x, y \in M &\Longrightarrow |x - y| \leq \max(|x|, |y|) < 1 \Longrightarrow x - y \in M, \\ x \in M, y \in B &\Longrightarrow |xy| = \underbrace{|x|}_{<1} \cdot \underbrace{|y|}_{\leq 1} < 1 \Longrightarrow xy \in M. \end{aligned}$$

□

Satz 5.4 *Der Faktorring $\overline{K} = B/M$ ist ein Körper. $\overline{K}$ heißt Restklassenkörper der Bewertung.*

Beweis: Sei $x + M \in B/M$ von Null verschieden, also $x \neq M$. Dann ist $|x| = 1$, also x Einheit. Wegen

$$(x + M)(x^{-1} + M) = xx^{-1} + M = 1 + M$$

ist $x + M$ invertierbar. Folglich ist $\overline{K}$ ein Körper. □

DEFINITION Es sei K ein bewerteter Körper. Die Menge der Werte

$$G = \{|x| \mid x \in K^\times\} \subseteq \mathbb{R}_+$$

heißt *Wertegruppe* der Bewertung.

Satz 5.5 *G ist bezüglich der Multiplikation eine Untergruppe der Gruppe $\{a \in \mathbb{R} \mid a > 0\}$.*

Beweis: $a = |x|$, $b = |y| \in G \Longrightarrow ab^{-1} = |xy^{-1}| \in G$. □

Satz 5.6 *Es sei K nicht-archimedisch bewertet. Die Wertegruppe $\hat{G}$ der Komplettierung $\hat{K}$ stimmt mit der Wertegruppe G von K überein.*

Beweis: Wegen $K \subseteq \hat{K}$ ist $G \subseteq \hat{G}$.
Sei $|\hat{x}| \in \hat{G}$ mit $\hat{x} \in \hat{K}^\times$. Da K dicht in $\hat{K}$ liegt, gibt es zu $\hat{x}$ ein $x \in K^\times$ mit $|\hat{x} - x| < |\hat{x}|$.
Dominanzprinzip: $|x| = |\hat{x} + (x - \hat{x})| = |\hat{x}|$, also $|\hat{x}| = |x| \in G \Longrightarrow G = \hat{G}$. □

DEFINITION Eine Bewertung heißt *diskret*, wenn zu jedem Element der Wertegruppe eine Umgebung existiert, die kein weiteres Element der Wertegruppe enthält.

Satz 5.7 *Eine Bewertung ist genau dann diskret, wenn die Wertegruppe zyklisch ist.*

Beweis: Ist $|\ |$ trivial, so ist $G = \{1\}$ zyklisch und diskret.
Wir können daher annehmen, daß $|\ |$ nicht trivial ist. Es gibt dann ein $x \in K^\times$ mit $|x| < 1$.

1.) Es sei $|\ |$ diskret und

$$S := \{a \in G \mid a < 1\}.$$

S ist beschränkt und $\neq$ *emptyset*. Sei $d = \sup S$.

1. *Es ist $d < 1$:*
   Wegen $1 \in G$ gibt es $b_1 < 1 < b_2$, so daß das Intervall (b_1, b_2) kein Element $\neq 1$ aus G enthält. Also gilt $a \leq b_1$ für alle $a \in S$, also $d \leq b_1 < 1$.

2. *Es ist $d \in G$:*
   Wegen $d = \sup S$ gibt es ein $a \in G$ mit $d^2 < a \leq d$. Falls $a < d$ wäre, gäbe es ein $b \in S$ mit $d^2 < a < b \leq d$. Es folgt $d < \frac{a}{b} < 1$, $\frac{a}{b} \in G$: Widerspruch zu $d = \sup S$. Also $d = a \in G$.

Sei nun $a \in G$ beliebig. Es gibt ein $n \in \mathbb{Z}$ mit $d^{n+1} < a \leq d^n$. Also $d < \dfrac{a}{d^n} \leq 1$. Wegen $d = \sup S$ ist $\frac{a}{d^n} = 1$, also $a = d^n$. Es folgt $G = \{d^n \mid n \in \mathbb{Z}\}$, also ist G zyklisch.

Sei umgekehrt G zyklisch, also $G = \{d^n \mid n \in \mathbb{Z}\}$. Folglich ist G diskret. □

Definition Es sei K diskret bewertet und $G = \{d^n \mid n \in \mathbb{Z}\}$ mit $d < 1$. Ein Element $p \in K$ heißt **Primelement**, wenn $|p| = d$ ist. Mit p ist auch $p' = ep$ Primelement mit $|e| = 1$.

Definition Es sei $\overline{K} = B/M$, der Restklassenkörper und $\varphi : B \to \overline{K}$, $\varphi(a) = a + M$. der Restklassenhomomorphismus.

Eine Teilmenge R von B heißt ein *Repräsentantensystem* , wenn zu jedem $\overline{x} \in \overline{K}$ genau ein $x \in R$ mit $\varphi(x) = \overline{x}$ existiert. Es sei stets $0, 1 \in R$.

Beispiel

Sei $L = K(x)$ der rationale Funktionenkörper über K, $p(x) = x - a$ ein irreduzibles Polynom ersten Grades und $0 < d < 1$. $|\ |$ sei die zu p gehörige Bewertung:

$$|h(x)| := \begin{cases} d^r & \text{falls } h(x) = p^r(x)\,\dfrac{u(x)}{v(x)} \text{ und } (u,p) = (v,p) = 1 \\ 0 & \text{für } h(x) = 0 \end{cases}$$

Dann ist $\overline{L} = K$.
Beweis: Es ist

$$B = \left\{ \frac{u(x)}{v(x)} \,\middle|\, (v,p) = 1 \right\}$$

und

$$M = \left\{ p(x)\,\frac{u(x)}{v(x)} \,\middle|\, (v,p) = 1 \right\} = p(x)\,B\,.$$

Es sei

$$\varphi : B \to \overline{L}$$

der Restklassenhomomorphismus und

$$\varphi_{|K} : K \to \overline{L}$$

seine Restriktion auf K. $\varphi_{|K}$ ist surjektiv: Sei $h(x) = \frac{u(x)}{v(x)} \in B$ mit $(v, p) = 1$. Dann ist

$$u(x) = n(x) \cdot v(x) + m(x) \cdot p(x) .$$

Wegen $\operatorname{grad} n < \operatorname{grad} p = 1$ folgt $n \in K$. Also ist

$$h(x) = n + p(x) \, \frac{m(x)p(x)}{v(x)} .$$

Damit ist $\varphi(h) = \varphi(n)$, also ist $\varphi_{|K}$ surjektiv. Wegen $\operatorname{Kern} \varphi = M \cap K = 0$ folgt

$$\overline{L} \cong K$$

nach dem Homomorphiesatz und K ist gleichzeitig ein Repräsentantensystem.

Satz 5.8 *Sei K diskret bewertet, p ein Primelement und R ein Repräsentantensystem. Zu jedem $x \neq 0$ aus der Komplettierung $\hat{K}$ von K gibt es ein $n \in \mathbb{Z}$ und Elemente $a_0, a_1, \ldots$ aus R, $a_0 \neq 0$, so daß die Folge*

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

gegen x konvergiert und

$$(*) \qquad |x - x_k| \leq |p|^{n+k+1}$$

gilt.

Beweis: Nach Satz 5.6 stimmen die Wertegruppen von K und $\hat{K}$ überein, und nach Satz 5.7 ist $G = \{d^n \mid n \in \mathbb{Z}\}$ mit $d \in \mathbb{R}$.
Sei $x \in \hat{K}^\times$. Dann gibt es ein $n \in \mathbb{Z}$ mit $|x| = d^n$. Setze $e := xp^{-n}$. Dann ist

$$|e| = |x| \, |p|^{-n} = 1 \qquad \text{und} \qquad x = p^n e .$$

Ist φ der Restklassenhomomorphismus, so gibt es ein $a_0 \in R$ mit $\varphi(e) = \varphi(a_0)$. Wegen $|e| = 1$ ist $\varphi(a_0) = \varphi(e) \neq 0$, also $a_0 \neq 0$. Setze

$$x_0 := p^n a_0 .$$

Hierfür gilt dann $(*)$

$$|x - x_0| = |p^n|\,|e - a_0| \le |p|^{n+1}\,,$$

denn wegen $\varphi(e - a_0) = \overline{0}$ ist $|e - a_0| < 1$, und nach dem Beweis zu Satz 5.7 ist $|p| = d = \sup\{b \in G \mid b < 1\}$.
Seien nun $a_0, \dots, a_k \in R$ und damit $x_0, \dots, x_k$ bereits bestimmt, so daß $(*)$ gilt. Aus

$$|x - x_k| \le |p|^{n+k+1}$$

folgt

$$\left|\frac{x - x_k}{p^{n+k+1}}\right| \le 1$$

also

$$\frac{x - x_k}{p^{n+k+1}} \in B\,.$$

Es gibt daher ein $a_{k+1} \in R$ mit

$$f(a_{k+1}) = f\left(\frac{x - x_k}{p^{n+k+1}}\right)\,.$$

Für

$$x_{k+1} := x_k + a_{k+1}p^{n+k+1}$$

ist dann

$$|x - x_{k+1}| = |x - x_k - a_{k+1}p^{n+k+1}| = \left|\frac{x - x_k}{p^{n+k+1}} - a_{k+1}\right|\,|p|^{n+k+1} \le |p|^{n+k+2}\,.$$

Damit ist die Folge (x_k) induktiv definiert. Wegen $(*)$ konvergiert sie gegen x. $\square$

Unter Benutzung der Bezeichnungen von Satz 5.8 schreibt man abkürzend

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

und nennt dies die *kanonische* Darstellung von x.

Satz 5.9 *Sei K diskret bewertet, $\hat{K}$ die Komplettierung, p festes Primelement, R festes Repräsentantensystem. Dann gilt:*

(1) *Die kanonische Darstellung ist eindeutig.*

(2) *Zu beliebigen* $n \in \mathbb{Z}$, $a_i \in R$, $a_0 \neq 0$ *gibt es ein* $x \in \hat{K}$ *mit* $x = p^n \sum a_i p^i$.

Beweis:

(1) Es ist

$$|x_k| = \left| p^n \sum_{i=0}^{k} a_i p^i \right| = |p|^n |a_0 + b_0| = |p|^n$$

mit $|a_0| = 1$, $|b_0| < 1$. Also ist

$$|x| = \lim |x_k| = |p|^n,$$

also ist n eindeutig bestimmt. Es sei auch

$$x = p^n \sum_{i=0}^{\infty} a'_i p^i$$

und j der erste Index mit $a_j \neq a'_j$.
Wegen $a_j, a'_j \in R \subseteq B$ ist $a_j - a'_j \in B$, also $|a_j - a'_j| \leq 1$. Wäre $|a_j - a'_j| < 1$, also $a_j - a'_j \in M$, so würde durch Anwendung der Restklassenabbildung φ folgen

$$\varphi(a_j) = \varphi(a'_j + (a_j - a'_j)) = \varphi(a'_j):$$

Widerspruch zur Definition des Repräsentantensystems R.
Also ist $|a_j - a'_j| = 1$. Für die Teilsummen gilt dann

$$|x_k - x'_k| = \left| p^n \sum_{i=0}^{k} (a_i - a'_i) p^i \right| = |p|^{n+j} \left| \sum_{i=j}^{k} (a_i - a'_i) p^{i-j} \right| = |p|^{n+j}.$$

Wegen

$$|x_k - x'_k| = |x_k - x + x - x'_k| \leq \max(|x_k - x|, |x - x'_k|)$$

wird dieser Wert beliebig klein: Widerspruch
$\Longrightarrow a_i = a'_i$ für alle i.

(2) Definiere

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

x_k ist eine Cauchy-Folge, konvergiert also gegen ein $x \in \hat{K}$. □

6 Die p-adischen Zahlen

Sei $K = \mathbb{Q}$ mit der p-adischen Bewertung. Dann ist $|p|_p = \frac{1}{p}$, also p Primelement. Ein Repräsentantensystem ist $R = \{0, 1, \dots, p-1\}$:

Beweis: Es ist

$$B = \left\{ \frac{u}{v} \mid u \in \mathbb{Z},\ v \in \mathbb{N},\ (v,p) = 1 \right\}$$

Wegen $(v,p) = 1$ gibt es eine Darstellung

$$u = nv + mp, \quad n, m \in \mathbb{Z}.$$

Man kann außerdem oBdA. $0 \le n < p$ annehmen: Ist nämlich $n = qp + n'$ mit $0 \le n' < p$, so gilt

$$u = n'v + (qv + m)p.$$

Also gilt

$$x = \frac{u}{v} = n + \underbrace{\frac{m}{v}p}_{\in M} \Longrightarrow \varphi(x) = \varphi(n)$$

Aus $\varphi(n) = \varphi(n')$, $n, n' \in R$, folgt $n - n'$ ist teilbar durch p, also ist $n = n'$.

Die Komplettierung von $\mathbb{Q}$ bezüglich der p-adischen Bewertungen liefert die Körper $\mathbb{Q}_p$ der p-adische Zahlen. Sie wurden 1898 von Hensel eingeführt. Man bezeichnet sie auch als *Henselsche Körper* .

Für $x \in \mathbb{Q}_p$ gibt es die Darstellung

$$\begin{aligned} x &= \textstyle\sum_{i=n}^{\infty} a_i p^i, \quad n \in \mathbb{Z}, \quad a_i \in R \\ &= \text{„}a_n \dots a_0, a_1 a_2 \dots\text{“} \end{aligned}$$

Satz 6.1 *$\mathbb{Q}_p$ ist überabzählbar.*

Beweis: (Cantorsches Diagonalverfahren)
Sei $x_1, x_2, \dots$ eine Abzählung der Elemente aus $\mathbb{Q}_p$, etwa

$$\begin{array}{rll} x_1 = & a_{n_1,1} \dots a_{0,1} & , a_{1,1} a_{2,1} \dots \\ x_2 = & a_{n_2,2} \dots a_{0,2} & , a_{1,2} a_{2,2} \dots \\ \dots = & \dots & , \dots \end{array}$$

Betrachte $x = 0, b_1 b_2 b_3 \dots$ mit $b_i \neq a_{i,i}$, $b_i \in R$. Dann tritt x wegen der Eindeutigkeit der kanonischen Darsatellung nicht in dieser Aufzählung auf. □

Rechnen in $\mathbb{Q}_p$

1. Addition: Die Summe $x + y = \sum_{n=n_0} c_n p^n$ zweier Elemente

$$x = \sum_{n=n_0} a_n p^n \qquad \text{und} \qquad y = \sum_{n=n_1=n_0} b_n p^n$$

($n_0 = n_1$ wird durch Nullauffüllung erreicht) berechnet man sukzessive mit den Koeffizienten niedrigster Ordnung beginnend. Zu berücksichtigen ist hierbei der Ziffernübertrag ε_n. Man setzt

$$\varepsilon_n = 0 \quad \text{für} \quad n \leq n_0$$

und ermittelt für $n \geq n_0$ c_n und ε_{n+1} aus

$$\varepsilon_n + a_n + b_n = c_n + \varepsilon_{n+1} \cdot p \qquad \text{mit} \qquad 0 \leq c_n < p\,.$$

Beispiel

Es sei $p = 7$. Für die in der kanonischen Darstellung auftretenden Ziffern a_i gilt dann $0 \leq a_i < 7$.

$$\begin{array}{cccccccc}
 & & 5, & 4 & 3 & 2 & 6 & \cdots \\
+ & 1 & 5, & \underset{1}{3} & \underset{1}{2} & 5 & \underset{1}{6} & \cdots \\
\hline
 & 1 & 3, & 1 & 6 & 0 & 6 & \cdots
\end{array}$$

2. Subtraktion: Das Negative von $x = a_{n_0} \ldots a_0, a_1 \ldots$ mit $a_{n_0} \neq 0$ ist $-x = b_{n_0} \ldots b_0, b_1 \ldots$ mit $b_{n_0} = p - a_{n_0}$ und $b_n = p - a_n - 1$ für $n > n_0$.

Beispiel

Es sei $p = 7$ und $x = 5,4326\ldots$. Dann ist $-x = 2,2340\ldots$, denn

$$\begin{array}{cccccccc}
 & x = & 5, & 4 & 3 & 2 & 6 & \cdots \\
+ & -x = & 2, & \underset{1}{2} & \underset{1}{3} & \underset{1}{4} & \underset{1}{0} & \cdots \\
\hline
 & & 0, & 0 & 0 & 0 & 0 & \cdots
\end{array}$$

3. Multiplikation: Man führt die Multiplikation formal aus

$$\sum_{n=n_0}^{\infty} a_n p^n \cdot \sum_{k=n_1}^{\infty} b_k p^k = \sum_{k=n_1}^{\infty} \sum_{n=n_0} a_n b_k p^{n+k} = \sum_{j=n_1+n_0}^{\infty} c_j p^j$$

mit

$$c_j = \sum_{i=n_0}^{j-n_1} a_i b_{j-i} \qquad \text{und} \qquad c_j = 0 \text{ für } j < n_0 + n_1$$

und ordnet dann nach Potenzen von p. Anschließend muß man noch reduzieren.

Beispiel

Es sei $p = 7$.

$$\begin{array}{cccccccccccccc}
 & 1 & 1, & 4 & 1 & 3 & \cdots & \cdot & 2 & 1, & 5 & 4 & 2 & \cdots \\
\hline
2 & 2 & 8, & 2 & 6 & & \cdots & & & & & & & \\
 & 1 & 1, & 4 & 1 & 3 & \cdots & & & & & & & \\
 & & 5, & 5 & 20 & 5 & \cdots & & & & & & & \\
 & & 0, & 4 & 4 & 16 & \cdots & & & & & & & \\
 & & 0, & {}_{2}0 & {}_{2}2 & {}_{5}2 & \cdots & & & & & & & \\
\hline
2 & 3 & 0, & 3 & 0 & 3 & \cdots & & & & & & &
\end{array}$$

Die Frage nach der Darstellung der $x = \sum_{n=n_0}^{\infty} a_n p^n \in \mathbb{Q} \subseteq \mathbb{Q}_p$ beantwortet

Satz 6.2 *Ein Element $x = \sum_{n=n_0}^{\infty} a_n p^n \in \mathbb{Q}_p$ ist genau dann ein Element von $\mathbb{Q}$, wenn die Darstellung periodisch ist, d.h. wenn ein $m \in \mathbb{Z}$ und ein $t \in \mathbb{N}$ existieren, so daß*

$$a_n = a_{n+t}$$

für alle $n \geq m$ ist.

Beweis: 1.) Die Darstellung sei periodisch. Dann ist

$$\begin{aligned}
x &= \sum_{n=n_0}^{m-1} a_n p^n + \sum_{n=m}^{\infty} a_n p^n \\
&= u + a_m p^m + \ldots + a_{m+t-1} p^{m+t-1} \\
&\qquad + a_{m+t} p^{m+t} + \ldots + a_{m+2t-1} p^{m+2t-1} \\
&\qquad + a_{m+2t} p^{m+2t} + \ldots + a_{m+3t-1} p^{m+3t-1} \\
&\qquad\qquad\qquad\qquad \vdots \\
&= u + p^m \left(a_m + a_{m+1} p + \ldots + a_{m+t-1} p^{t-1}\right) \sum_{k=0}^{\infty} (p^t)^k \\
&= u + \frac{p^m v}{1 - p^t} \in \mathbb{Q}
\end{aligned}$$

mit $v := a_m + \ldots + a_{m+t-1}p^{t-1}$.

2.) Sei $x \in \mathbb{Q}$ mit der Darstellung

$$x = p^n \, \frac{u}{v}$$

mit $n, u \in \mathbb{Z}$, $v \in \mathbb{N}$ und $(u,p) = (v,p) = 1$. Wegen $(v,p) = 1$ liegt p in der primen Restklassengruppe mod$v$. Nach dem Satz von Lagrange gibt es daher ein $t \in \mathbb{N}$ mit

$$p^t \equiv 1 \bmod v\,,$$

d.h. v teilt $1 - p^t$. Durch geeignetes Erweitern erhält man

$$x = p^n \, \frac{b}{1-p^t}\,, \qquad b \in \mathbb{Z}\,.$$

Sei nun $m \in \mathbb{Z}$ so groß gewählt, daß

$$(*) \qquad -p^m < b < p^m$$

gilt. Wegen $(1 - p^t, p^m) = 1$ ist

$$b = z\,(1-p^t) + yp^m$$

mit $y, z \in \mathbb{Z}$ und $0 \leq z < p^m$.
Dann ist $0 \leq y < p^t$: Es ist $b \leq yp^m$. Wäre $y < 0$, so würde $b \leq -p^m$ im Widerspruch zu $(*)$ folgen. Weiter ist

$$\begin{aligned} y &= p^{-m}\,(b + z(p^t - 1)) \\ &\leq p^{-m}\,(p^m + (p^m - 1)(p^t - 1)) \\ &= 1 + p^t - 1 - p^{-m}\,(p^t - 1) \\ &< p^t \end{aligned}$$

Wegen $0 \leq z < p^m$ folgt

$$z = a_0 + a_1 p + \ldots + a_{m-1}p^{m-1}\,, \qquad 0 \leq a_i < p \quad (0 \leq i < m)\,,$$

und wegen $0 \leq y < p^t$ folgt

$$y = a_m + a_{m+1}p + \ldots + a_{m+t-1}p^{t-1}\,, \qquad 0 \leq a_j < p \quad (m \leq j < m+t)\,.$$

Also ist

$$x = p^n \, \frac{b}{1-p^t} = p^n \, \frac{z\,(1-p^t) + yp^m}{1-p^t} = p^n \, \left(z + p^m \, \frac{y}{1-p^t}\right)\,.$$

Dies liefert die periodische Darstellung von x. $\square$

Beispiel

Es sei $p = 5$.
(a) Sei $x = 41,\overline{31}$. Dann ist

$$x = 41,\overline{31} = \frac{4}{5} + 1 + \frac{5 \cdot (3+5)}{1-25} = \frac{4}{5} + 1 - \frac{20}{12} = \frac{48+60-10}{60} = \frac{2}{15}$$

(b) Sei $x = \frac{2}{15} = 5^{-1} \cdot \frac{2}{3}$. Man ermittelt das kleinste t so, daß $3 \mid (1-5^t)$ (3 teilt $1-5^t$) gilt. Man findet $t = 2$, also

$$x = 5^{-1} \frac{-16}{1-5^2}.$$

Es ist

$$-5^2 < -16 < 5^2,$$

also $m = 2$ und

$$-16 = z\,(-24) + y \cdot 25 = 9 \cdot (-24) + 8 \cdot 25$$

und damit $z = 9 = 4 + 1 \cdot 5$ und $y = 8 = 3 + 1 \cdot 1$. Man erhält

$$x = 5^{-1}\left(9 + 5^2 \frac{8}{1-5^2}\right) = 5^{-1}\left(4 + 5 + 5^2 \frac{3+5}{1-5^2}\right) = 41,\overline{31}.$$

Quadrate in $\mathbb{Q}_p$

Hilfssatz 6.3 *Jedes $x \neq 0$ aus $\mathbb{Q}_p$ besitzt eine Darstellung*

$$x = p^n \cdot a, \quad |a| = 1, \quad n \in \mathbb{Z}.$$

Beweis: Weil die Wertegruppe von $d = |p|$ erzeugt wird, ist $|x| = |p|^n$. Für $a = p^{-n}x$ gilt dann $|a| = |p|^{-n} \cdot |p|^n = 1$ und $x = p^n \cdot a$. □

Satz 6.4 *Ein Element $x = p^n \cdot a$, $|a| = 1$ ist genau dann ein Quadrat, wenn n gerade und a ein Quadrat ist.*

Beweis:

1. Ist $n = 2k$ und $a = b^2$, so folgt

$$x = p^{2k} b^2 = (p^k b)^2.$$

2. Sei $x = p^n a = b^2$ und $b = p^k c$ mit $|c| = 1$. Dann ist
$$|x| = |p|^n = |b|^2 = |p|^{2k},$$
also $n = 2k$ und $a = p^{-2k} b^2 = (p^{-k} b)^2$.

□

Problem: Wann ist a mit $|a| = 1$ ein Quadrat?
Sei $\varphi : B \to B/M = \overline{K}$ Restklassenhomomorphismus.
$$a = b^2 \Longrightarrow 1 = |a| = |b|^2 \Longrightarrow |b| = 1 \Longrightarrow \varphi(a) = (\varphi(b))^2$$
$\Longrightarrow \varphi(a)$ ist ein Quadrat in $\overline{K}$.
$$\mathbb{Q}_p : \quad B = \{a_0 + a_1 p + a_2 p^2 + \ldots\} \to B/M = \mathbb{Z}_p$$

Satz 6.5 *1. Sei $p \neq 2$ und $a \in \mathbb{Q}_p$ mit $|a| = 1$. a ist genau dann ein Quadrat in $\mathbb{Q}_p$, wenn $\varphi(a)$ Quadrat in $\mathbb{Z}_p$ ist.*

2. Sei $p = 2$ und $a \in \mathbb{Q}_2$ mit $|a| = 1$. a ist genau dann ein Quadrat in $\mathbb{Q}_2$, wenn $|a-1| \leq |2|^3$ ist.

Beweis:

1. Sei $\varphi(a) = (\varphi(b))^2 \Longrightarrow |b| = 1$, also $\varphi(b^2 - a) = 0 \Longrightarrow b^2 - a \in M$.
Betrachte $f(t) = t^2 - a$:
$$|f(b)| = |b^2 - a| < 1, \qquad |f'(b)| = |2b| = 1$$
Nach Satz 3.3 existiert eine Nullstelle von $f(t)$, also ist a ist Quadrat.

2. $f(t) = t^2 - a$ besitzt wegen
$$|f(1)| = |1 - a| \leq |2|^3 < |f'(1)|^2 = |2|^2$$
eine Nullstelle in $\mathbb{Q}_2$.
Umgekehrt gilt: Sei a ein Quadrat in $\mathbb{Q}_2$, also $a = b^2$, $b \in \mathbb{Q}_2$.
$$|a| = |b^2| = 1 \Longrightarrow |b| = 1 \Longrightarrow b \in B \Longrightarrow \varphi(b) = 1 \in \mathbb{Z}_2$$
$\varphi(b-1) = 0 \Longrightarrow b = 1 + 2c$ mit $c \in B$.
$$\Longrightarrow a - 1 = b^2 - 1 = (1+2c)^2 - 1 = 4(c + c^2) = 4 \cdot 2d$$
wegen $\varphi(c + c^2) = 1 + 1 = 0$.
$\Longrightarrow |a - 1| \leq |2|^3$.

□

Ergebnis:

Quadrate in $\mathbb{Q}_2$: $a = 2^{2k}(1 + a_3 2^3 + a_4 2^4 + \dots)$

Quadrate in $\mathbb{Q}_p$, $p \neq 2$: $a = p^{2k}(a_0 + a_1 p + \dots)$, $\quad \left(\frac{a_0}{p}\right) = 1$.

Korollar 6.6 *Sind p und q verschiedene Primzahlen, so sind $\mathbb{Q}_p$ und $\mathbb{Q}_q$ nicht isomorph.*

Beweis: Annahme: Es gibt einen Isomorphismus $f : \mathbb{Q}_p \to \mathbb{Q}_q$, also eine bijektive Abbildung mit

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y).$$

Wir können annehmen, daß $\mathbb{Z}$ in $\mathbb{Q}_p$ enthalten ist. Wegen $f(0) = f(0+0) = f(0) + f(0)$ also $f(0) = f(0) - f(0) = 0$ ist $f(1) \neq 0$, da f bijektiv ist. Wegen $f(1) = f(1 \cdot 1) = f(1)f(1)$, also $f(1) = \dfrac{f(1)}{f(1)} = 1$ folgt $f(n) = f(1+\ldots+1) = f(1)+\ldots+f(1) = n$ für $n \in \mathbb{Z}$. Ist $n = x^2$, $x \in \mathbb{Q}_p$, so ist $n = f(n) = (f(x))^2$.

Insgesamt erhalten wir: Ist $n \in \mathbb{Z}$ ein Quadrat in $\mathbb{Q}_p$, so ist auch $f(n) = n$ ein Quadrat in $\mathbb{Q}_q$. Dies können wir dazu benutzen, um die Existenz eines Isomorphismus auszuschließen.

Fallunterscheidung:

1. Sei $p < q$, $p \neq 2$:
   Wegen $(p, q) = 1$ ist
   $$1 = -ap + bq, \qquad 0 < b < p < q, \quad a \in \mathbb{N}$$
   $n = 1 + ap$ ist ein Quadrat in $\mathbb{Q}_p$, da $f(1)$ Quadrat in $\mathbb{Z}$ ist.
   $n = bq$ ist kein Quadrat in $\mathbb{Q}_q$, da q in 1. Potenz.

2. $p = 2$, $q > 8$:
   $$1 = -a8 + bq, \qquad 0 < b < 8 < q$$
   $n = 1 + a8$ ist Quadrat in $\mathbb{Q}_2$
   $n = bq$ ist kein Quadrat in $\mathbb{Q}_q$, da q in 1. Potenz.

3. $p = 2$, $q = 3, 5, 7$:
   7 ist ein Quadrat in $\mathbb{Q}_3$, aber kein Quadrat in $\mathbb{Q}_2$.
   6 ist ein Quadrat in $\mathbb{Q}_5$, aber kein Quadrat in $\mathbb{Q}_2$.
   2 ist ein Quadrat in $\mathbb{Q}_7$, aber kein Quadrat in $\mathbb{Q}_2$.

Der Isomorphismus f existiert daher nicht. □

DEFINITION Ein Körper K heißt ein *geordneter Körper*, wenn gilt:

(1) K ist linear angeordnet bezüglich $\leq$,

(2) $a \leq b \Longrightarrow a + c \leq b + c$,

(3) $0 \leq a, b \Longrightarrow 0 \leq ab$.

Folgerung: $a^2 \geq 0$ für alle $a \in K$.

Hilfssatz 6.7 *Der Körper der rationale Zahlen $\mathbb{Q}$ besitzt nur eine Anordnung.*

Beweis: Sei $\leq$ eine beliebig Anordnung auf $\mathbb{Q}$. Wegen $1 = 1^2 > 0$ ist $n = 1 + \ldots + 1 > 0$, also $\frac{n}{m} > 0$ für $n, m \in \mathbb{N}$, also

$$x \overset{gew.}{>} 0 \Longrightarrow x > 0.$$

Daraus folgt

$$(*) \qquad x \overset{gew.}{>} y \Longrightarrow x - y \overset{gew.}{>} 0 \Longrightarrow x - y > 0 \Longrightarrow x > y.$$

und durch Kontraposition: $x \leq y \Longrightarrow x \overset{gew.}{\leq} y$. Aus $(*)$ folgt weiter durch Vertauschung von x und y:

$$x \overset{gew.}{\leq} y \Longrightarrow x \leq y$$

Also gilt

$$x \overset{gew.}{\leq} y \iff x \leq y.$$

Korollar 6.8 *Die Körper $\mathbb{Q}_p$ lassen sich nicht anordnen.*

Beweis: Eine Anordnung auf $\mathbb{Q}_p$ induziert eine Anordnung auf $\mathbb{Q}$. Nach dem Hilfssatz ist dies die gewöhnliche Anordnung, also $\frac{1}{1-p^3} < 0$. Wegen

$$\frac{1}{1-p^3} = 1 + p^3 + p^6 + \ldots$$

ist $\frac{1}{1-p^3}$ ein Quadrat in $\mathbb{Q}_p$: Widerspruch. $\square$

Korollar 6.9 *$\mathbb{R}$ ist zu keinem der Körper $\mathbb{Q}_p$ isomorph.*

Beweis: Ist $f : \mathbb{Q}_p \to \mathbb{R}$ ein Isomorphismus, so liefert

$$a \leq b :\iff f(a) \leq f(b)$$

eine Anordnung auf $\mathbb{Q}_p$: Widerspruch. $\square$

7 Bewertungsfortsetzungen

Es sei K ein nicht-archimedisch bewerteter Körper, $B = \{x \in K \mid |x| \leq 1\}$ der Bewertungsring und $B[t]$ der Polynomring über B.

Definition Ein Polynom $f(t) = a_n t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in K[t]$ heißt *primitiv*, wenn

$$\max_{0\leq i\leq n}(|a_i|) = 1$$

ist.

Bemerkung Ist $f(t) = a_n t^n + a_{n-1}t^{n-1} \ldots + a_0 \in K[t]$ $(a_n \neq 0)$ und $a_j = \max_{0\leq i\leq n}(|a|_i)$, so ist

$$\frac{1}{a_j} f(t) \in B[t]$$

primitiv.

Hilfssatz 7.1 *Das Produkt primitiver Polynome ist wieder primitiv.*

Beweis: Sei

$$f(t) = a_n t^n + \ldots + a_0\,, \qquad \text{und} \qquad g(t) = b_m t^m + \ldots + b_0\,,$$

$j \in \{0, 1, \ldots, n\}$ mit $|a_j| = 1$ und $|a_i| < 1$ für $i < j$ sowie $k \in \{0, 1, \ldots, m\}$ mit $|b_k| = 1$ und $|b_i| < 1$ für $i < k$.
Für $f(t) \cdot g(t) = \sum_{i=0}^{n+m} c_i t^i$ ist der Koeffizient

$$c_{j+k} = (a_0 b_{j+k} + \ldots + a_{j-1}b_{k+1}) + a_j b_k + (a_{j+1}b_{k-1} + \ldots + a_{j+k}b_j)\,,$$

also

$$|c_{j+k}| = |a_j b_k| = 1\,.$$

Also ist $f(t) \cdot g(t)$ primitiv, denn für alle $i \in \{0, 1, \ldots, m+n\}$ ist $c_i \in B$. □

Hilfssatz 7.2 *Es sei*

$$f(t) = g(t) \cdot h(t)$$

primitiv und $g(t), h(t) \in K[t]$. Dann gibt es zwei primitive Polynome $g_1(t)$ und $h_1(t)$ und Körperelemente c_1, c_2 mit

$$f(t) = g_1(t) \cdot h_1(t)$$

und $g_1(t) = c_1 g(t)$, $h_1(t) = c_2 h(t)$.

Beweis: Seien $a, b \in K$, so daß $a \cdot g(t)$ und $b \cdot h(t)$ primitiv sind. Nach Hilfssatz 7.1 ist dann

$$a \cdot g(t) \cdot b \cdot h(t) = ab \cdot f(t)$$

primitiv. Ist $f(t) = \sum_{i=0}^{n} a_i t^i$, so ist

$$1 = \max_{0 \le i \le n} (|ab|\,|a_i|) = |ab| \max_{0 \le i \le n} (|a_i|) = |ab| \cdot 1 = |ab|\,,$$

also sind

$$g_1(t) = \frac{a}{ab}\, g(t) \qquad \text{und} \qquad h_1(t) = b \cdot h(t)$$

primitiv, und es gilt

$$f(t) = g_1(t) \cdot h_1(t)\,. \quad \square$$

$\square$

Der Restklassenhomomorphismus $B \to \overline{K}$, $a \mapsto \overline{a}$ induziert eine Abbildung $B[t] \to \overline{K}[t]$ durch

$$f(t) = \sum_{i=0}^{n} a_i t^i \mapsto \overline{f}(t) = \sum_{i=0}^{n} \overline{a_i} t^i$$

für alle $f(t) \in B[t]$.

Es gilt

$$\overline{f+g} = \overline{f} + \overline{g} \qquad \text{und} \qquad \overline{f \cdot g} = \overline{f} \cdot \overline{g}$$

für alle $f, g \in B[t]$. Ferner ist $f \in B[t]$ genau dann primitiv, wenn $\overline{f} \neq \overline{0}$ ist.

Satz 7.3 *Ist $f(t) \in B[t]$ und $\overline{f}(t)$ irreduzibel über $\overline{K}$, $\operatorname{grad} f = \operatorname{grad} \overline{f}$, so ist f irreduzibel über K.*

Beweis: Annahme: f ist reduzibel über K, etwa $f = g \cdot h$ mit $1 \le \operatorname{grad} g, \operatorname{grad} h < \operatorname{grad} f$. Weil f primitiv ist, kann man dann nach Hilfssatz 7.2 g und h als primitiv annehmen. Also ist $\overline{f} = \overline{g} \cdot \overline{h}$ eine echte Zerlegung von $\overline{f}$, also ist $\overline{f}$ reduzibel, im Widerspruch zur Voraussetzung. $\square$

Beispiel

Es ist $f(t) = t^3 + 2t^2 + 5t + 3$ irreduzibel über $\mathbb{Q}_2$. Denn wäre

$$\overline{f}(t) = \overline{1}t^3 + \overline{2}t^2 + \overline{5}t + \overline{3} = t^3 + t + \overline{1}$$

reduzibel, so müßte ein Linearfaktor abspaltbar sein, also $\overline{f}$ eine Nullstelle in $\mathbb{Z}_2$ besitzen. Für die beiden Elemente $\overline{0}$ und $\overline{1}$ aus $\mathbb{Z}_2$ gilt jedoch $\overline{f}(\overline{0}) = \overline{f}(\overline{1}) = \overline{1}$.

Korollar 7.4 *Gibt es eine separable Erweiterung $\overline{E}$ über $\overline{K}$ mit $[\overline{E}:\overline{K}] = n$, so existiert auch eine Erweiterung E über K vom gleichen Grad n.*

Beweis: Weil $\overline{E}$ eine separable Erweiterung über $\overline{K}$ ist, ist $\overline{E} = \overline{K}(\vartheta)$ mit $\overline{f}(t) = \mathrm{Irr}\,(\vartheta, \overline{K}) = t^n + \overline{a}_{n-1}t^{n-1} + \ldots + \overline{a}_0$. Sei $f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$ ein Urbild von $\overline{f}$. Dann ist f irreduzibel und $E = K(\vartheta)$ mit $\mathrm{Irr}\,(\vartheta, K) = f(t)$ hat den Grad n über K. □

Korollar 7.5 *Über $\mathbb{Q}_p$ gibt es zu jedem $n \in \mathbb{N}$ einen Erweiterungskörper E vom Grad n (und damit auch irreduzible Polynome vom Grad n).*

Beweis: Das Galoisfeld $\mathrm{GF}(p^n)$ ist eine separable Erweiterung vom Grad n über $\mathbb{Z}_p$. □

Satz 7.6 *[Henselsches Lemma] Sei K vollständig bezüglich einer nicht-archimedischen Bewertung. Sei f ein primitives Polynom, für das $\overline{f} = \overline{g}_0\overline{h}_0$ und $\overline{K}[t]$ gilt. Sind $\overline{g}_0$ und $\overline{h}_0$ teilerfremd, so gibt es $g, h \in K[t]$ mit*

$$f = g \cdot h$$

und $\mathrm{grad}\, g = \mathrm{grad}\, \overline{g}_0$, $\overline{g} = \overline{g}_0$, $\overline{h} = \overline{h}_0$.

Beweis: Sei $\mathrm{grad}\, f = m$ und $k = \mathrm{grad}\, \overline{g}_0$. Seien g_0 und h_0 Urbilder von $\overline{g_0}$ und $\overline{h}_0$, jeweils vom gleichen Grad. Wegen

$$\mathrm{grad}\, \overline{g}_0 + \mathrm{grad}\, \overline{h}_0 = \mathrm{grad}\, \overline{f} \leq \mathrm{grad}\, f$$

ist dann

$$\mathrm{grad}\, h_0 = \mathrm{grad}\, \overline{h}_0 \leq m - k\,.$$

Da $\overline{g}_0$ und $\overline{h}_0$ teilerfremd sind, gibt es $\overline{u}_0, \overline{v}_0 \in \overline{K}[t]$ mit

$$\overline{g}_0\overline{v}_0 + \overline{h}_0\overline{u}_0 = \overline{1}\,.$$

u_0 und v_0 seien Urbilder von $\overline{u}_0$ und $\overline{v}_0$. Die Polynome

$$F = f - g_0h_0 \qquad \text{und} \qquad G = 1 - g_0v_0 - h_0u_0$$

werden durch die Restklassenabbildung auf $\overline{0}$ abgebildet, ihre Koeffizienten liegen daher in M. Es sei $p \in M$, so daß $|p|$ größer oder gleich den Werten aller Koeffizienten von F und G ist. (Man nehme etwa für p einen Koeffizienten von F und G mit maximalem Wert.) Man schreibt dann

$$\begin{aligned} f &\equiv g_0 h_0 \bmod p \\ 1 &\equiv g_0 v_0 + h_0 u_0 \bmod p\,, \end{aligned}$$

um anzudeuten, daß jeder Koeffizient von $f - g_0 h_0$ und $1 - g_0 v_0 - h_0 u_0$ in B durch p teilbar ist. Wegen $p \in M$ ist $|p| < 1$. (Ist die Bewertung diskret, so kann für p ein Primelement genommen werden.)

Wir definieren nun induktiv zwei Folgen von Polynomen

$$g_0, g_1, \ldots \qquad \text{und} \qquad h_0, h_1, \ldots$$

aus $B[t]$ mit folgenden Eigenschaften:

1. $f \equiv g_n h_n \bmod p^{n+1}$

2. $g_{n+1} \equiv g_n \bmod p^{n+1}$, $h_{n+1} \equiv h_n \bmod p^{n+1}$ für $n \geq 1$.

3. $\operatorname{grad} g_n = k$, $\operatorname{grad} h_n \leq m - k$.

g_0 und h_0 erfüllen die Bedingungen (1) und (3). Wir setzen nun voraus, daß g_n und h_n bereits definiert sind und machen den Ansatz

$$\begin{aligned} g_{n+1} &= g_n + p^{n+1} u_n \\ h_{n+1} &= h_n + p^{n+1} v_n\,. \end{aligned}$$

g_n und h_n sollen hierbei (1) und (3) genügen. Also ist

$$f - g_n h_n = p^{n+1} p_n$$

mit $p_n \in B[t]$. Der Ausdruck

$$\begin{aligned} f - g_{n+1} h_{n+1} &= f - (g_n + p^{n+1} u_n)(h_n - p^{n+1} v_n) \\ &= p^{n+1}\,(p_n - u_n h_n - v_n g_n) - p^{2n+2} u_n v_n \end{aligned}$$

ist $\equiv 0 \bmod p^{n+2}$, falls u_n und v_n so bestimmt werden können, daß

$$p_n \equiv u_n h_n + v_n g_n \bmod p$$

ist. Aus

$$1 \equiv u_0 h_0 + v_0 g_0 \bmod p$$

folgt durch Multiplikation mit p_n

$$p_n \equiv u_0 p_n h_0 + v_0 p_n g_0 \bmod p\,.$$

Um die Bedingung über den Grad zu erfüllen, dividiere man

$$u_0 p_n = q g_0 + u_n$$

durch $\operatorname{grad} u_n < \operatorname{grad} g_0$. Dann ist

$$p_n \equiv u_n h_0 + (q h_0 + v_0 p_n)\, g_0 \bmod p\,.$$

Wegen $\operatorname{grad}(p_n - u_n h_0) \leq m$ gibt es ein v_n mit $\operatorname{grad} v_n \leq m - k$ und

$$v_n \equiv q h_0 + v_0 p_n \bmod p\,.$$

Also ist

$$p_n \equiv u_n h_0 + v_n g_0 \equiv u_n h_n + v_n g_n \bmod p\,,$$

weil nach (2) $h_n \equiv h_0 \bmod p$ und $g_n \equiv g_0 \bmod p$ ist.

Für g_{n+1} und h_{n+1} sind daher (1) und wegen des Ansatzes

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

auch (2) erfüllt. Wegen $\operatorname{grad} u_n < k = \operatorname{grad} g_n$ hat g_{n+1} den gleichen höchsten Koeffizienten und den gleichen Grad wie g_n. Schließlich haben h_n und v_n einen Grad $\leq m - k$. Damit ist auch $\operatorname{grad} h_{n+1} \leq m - k$. Hiermit ist die Existenz der Folgen (g_n) und (h_n) mit den Eigenschaften (1) – (3) gezeigt.

Wir setzen

$$g_n = a_k t^k + a_{k-1}^{(n)} t^{k-1} + \ldots + a_0^{(n)}\,.$$

Wegen (2) ist

$$g_n \equiv g_{n+k} \bmod p^{n+1}\,,$$

also

$$|a_i^{(n)} - a_i^{(n+k)}| \leq |p|^{n+1}\,.$$

Da $|p| < 1$ ist, bilden für festes i die Koeffizienten $(a_i^{(n)})$, $0 \leq i \leq k-1$, Cauchy-Folgen in K. Da K vollständig ist, konvergieren sie. Ist nun

$$a_i = \lim a_i^{(n)} \;\; (0 \leq i \leq k-1) \qquad \text{und} \qquad g = a_k t^k + a_{k-1} t^{k-1} + \ldots + a_0\,,$$

so folgt
$$g \equiv g_n \bmod p^{n+1}\,, \quad \overline{g} = \overline{g}_0 \quad \text{und} \quad \operatorname{grad} g = k\,.$$
Entsprechend erhält man ein Grenzpolynom h der Folge (h_n) mit
$$h \equiv h_n \bmod p^{n+1} \qquad \text{und} \qquad \operatorname{grad} h \leq m - k\,.$$
Wegen
$$f - gh = f - g_n h_n + g_n\,(h_n - h) + (g_n - g)\,h \equiv 0 \bmod p^{n+1}$$
für alle $n \in \mathbb{N}$ folgt $f = g \cdot h$. □

Beispiel

Es sei $K = \mathbb{Q}_2$.
1.) Für die Anwendbarkeit des Henselschen Lemmas ist es notwendig, daß die Faktoren des Restklassenpolynoms teilerfremd sind. Denn es ist $f(t) = t^2 + 3$ irreduzibel, weil -3 kein Quadrat in $\mathbb{Q}_2$ ist, aber
$$\overline{f}(t) = t^2 + \overline{1} = (t + \overline{1})(t + \overline{1})\,.$$
2.) Ist $f(t) = t^3 + 3$, so ist
$$\overline{f}(t) = t^3 + \overline{1} = (t + \overline{1})(t^2 + t + \overline{1})\,,$$
also besitzt f nach dem Henselschen Lemma die Zerlegung
$$f(t) = (t + a)(t^2 + bt + c)$$
mit Koeffizienten $a, b, c \in \mathbb{Q}_2$. ($t^2 + bt + c$ ist irreduzibel, weil $t^2 + t + \overline{1}$ irreduzibel ist.)
3.) Für
$$f(t) = t^5 + 3t^4 + 2t^2 + 1$$
ist
$$\overline{f}(t) = t^5 + t^4 + \overline{1} = (t^2 + t + \overline{1})(t^3 + t + \overline{1})\,.$$
Nach dem Henselschen Lemma ist $f(t)$ reduzibel.

Zwei Spezialfälle im Henselschen Lemma

1). Sei $\operatorname{grad} f = \operatorname{grad} \overline{f}$ und $\overline{f} = \overline{p}_1^{k_1} \cdot \ldots \cdot \overline{p}_r^{k_r}$ $(r, k_1, \ldots, k_r \in \mathbb{N})$ die Primfaktorzelegung von $\overline{f}$ in $\overline{K}[t]$. Dann ist
$$f = f_1 \cdot \ldots \cdot f_r \qquad \text{mit} \qquad \overline{f}_i = \overline{p}_i^{k_i} \ \ (1 \leq i \leq r)\,.$$

Ist $k_i = 1$ $(1 \leq i \leq r)$, so ist f_i irreduzibel. (Ist $k_i > 1$ $(1 \leq i \leq r)$, so hat man keine Aussage über die Irreduzibilität von f_i.)

Beispiel: Es sei $K = \mathbb{Q}_p$. Dann ist

$$f(t) = t^2 - p \ \text{ irreduzibel mit } \overline{f}(t) = t^2\,,$$

aber

$$g(t) = t^2 - p^2 = (t-p)(t+p) \ \text{ reduzibel mit } \overline{g}(t) = t^2\,.$$

2.) Sei $\operatorname{grad} \overline{f} = m < n = \operatorname{grad} f$. Dann ist $\overline{f} = \overline{f} \cdot \overline{1}$, also $f = g \cdot h$ mit $\operatorname{grad} g = m$ und $\operatorname{grad} h = n - m$.

Beispiel: Es sei $K = \mathbb{Q}_p$. Für $f(t) = pt^2 + t + 1$ ist $\overline{f}(t) = t + \overline{1}$, also muß eine Zerlegung $f(t) = (t+a)(pt+b)$ mit $a, b \in \mathbb{Q}_2$ möglich sein.

Satz 7.7 *Ist K vollständig bezüglich einer nicht-archimedischen Bewertung, und ist*

$$f(t) = a_n t^n + \ldots + a_0 \in K[t]$$

irreduzibel über K, so gilt

$$|a_i| \leq \max\left(|a_n|, |a_0|\right) \qquad \textit{für } i = 0, 1, \ldots, n\,.$$

Beweis: 1.) Sei zunächst f primitiv und

$$|a_r| = 1 \qquad \text{sowie} \qquad |a_i| < 1 \text{ für } 0 \leq r < i \leq n\,.$$

Dann ist

$$\overline{f}(t) = (\overline{a}_r t^r + \ldots + \overline{a}_0) \cdot \overline{1}\,.$$

Nach dem Henselschen Lemma ist dann von f ein Faktor vom Grad abspaltbar. Da aber f irreduzibel ist, sind nur die Fälle

$$r = n \qquad \text{und} \qquad r = 0$$

möglich. Also ist

$$\max\left(|a_n|, |a_0|\right) = 1\,.$$

2.) Sei $a \in K^\times$ so gewählt, daß $f^*(t) := a \cdot f(t)$ primitiv ist. Dann gilt für $i = 0, 1, \ldots, n$

$$|aa_i| \leq \max\left(|aa_n|, |aa_0|\right) = |a| \max\left(|a_n|, |a_0|\right),$$

also

$$|a_i| \leq \max\left(|a_n|, |a_0|\right) \quad \square$$

Hilfssatz 7.8 *Sei E ein Erweiterungskörper des bewerteten Körpers K mit $[E : K] = n < \infty$ und $N : E \to K$ die Norm. Ist $a \in E$ und $Irr(a, K) = t^k + \ldots + a_0 \in K[t]$, so ist*

$$\sqrt[n]{|N(a)|_K} = \sqrt[k]{|a_0|_K}\,.$$

Beweis: Es ist $K \subseteq K(a) \subseteq E$. Sei $\{u_1, \ldots, u_r\}$ eine Basis von E über $K(a)$. Dann ist

$$\mathcal{B} = \{u_1, \ldots, u_r, au_1, \ldots, au_r, \ldots, a^{k-1}u_1, \ldots, a^{k-1}u_r\}$$

eine Basis von E über K:

a) $\mathcal{B}$ spannt E über K auf: Sei $x \in E$. Dann ist

$$x = \sum_{i=1}^{r} b_i u_i \qquad \text{mit } b_i \in K(a) \text{ für } i = 1, \ldots, r\,.$$

Wegen

$$b_i = \sum_{j=0}^{k-1} a_{ij} a^j \qquad \text{mit } a_{ij} \in K \text{ für } 0 \leq j \leq k-1 \text{ und } 1 \leq i \leq r$$

ist daher

$$x = \sum_{i=1}^{r} \sum_{j=0}^{k-1} a_{ij} a^j u_j\,.$$

b) $\mathcal{B}$ ist linear unabhängig über K: Ist

$$0 = \sum_{i=1}^{r} \left(\sum_{j=0}^{k-1} a_{ij} a^j \right) u_i\,,$$

so folgt für alle $i = 1, \ldots, r$

$$\sum_{j=0}^{k-1} a_{ij} a^j = 0\,,$$

weil $\{u_1, \ldots, u_r\}$ eine Basis von E über $K(a)$ ist. Weil $\{1, a, a^2, \ldots, a^{k-1}\}$ eine Basis von $K(a)$ über K ist, folgt

$$a_{ij} = 0$$

für alle $i = 1, \ldots, r$ und alle $j = 0, \ldots, k-1$. Insgesamt folgt somit die lineare Unabhängigkeit von $\mathcal{B}$ über K. Außerdem folgt $n = r \cdot k$.

Ist $\{v_1, \ldots, v_n\}$ eine Basis von E über K und

$$av_i = \sum_{i=1}^{n} a_{ij} v_j \qquad (i = 1, \ldots, r),$$

so ist $N(a) = \det(a_{ij})$. Speziell für die Basis $\mathcal{B}$ ist

$$a \cdot a^j u_i = \begin{cases} a^{j+1} u_i & \text{für } j < k-1 \\ a^k \cdot u_i = \sum_{\ell=0}^{k-1} a_\ell a^\ell u_i & \text{für } j = k-1\,, \end{cases}$$

also

$$(a_{ij}) = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_r \end{pmatrix}$$

mit

$$A_1 = \ldots = A_r = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{k-1} \end{pmatrix}$$

Es folgt

$$N(a) = \det(a_{ij}) = (\det A_1)^r = \left((-1)^{k-1} \cdot a_0\right)^r.$$

Damit ist

$$\sqrt[n]{|N(a)|_K} = \sqrt[k \cdot r]{|(-1)^{k-1} a_0|_K^r} = \sqrt[k]{|a_0|_K}\,. \quad \square$$

$\square$

Satz 7.9 (Kürschak) *Sei K vollständig und E eine endliche Erweiterung von K, $[E : K] = n < \infty$. Dann ist*

$$|a|_E := \sqrt[n]{|N(a)|_K} \qquad (a \in E)$$

eine Bewertung von E, die die Bewertung von K fortsetzt.

(Nach Satz 3.6 ist diese auch die einzige Fortsetzung.)

Beweis: 1.) Ist K archimedisch bewertet, so ist $n \leq 2$ nach Satz 4.3. Die Behauptung folgt dann aus Satz 3.4.

2.) Sei K nicht-archimedisch bewertet. Daß $|\ |_E$ eine Fortsetzung von $|\ |_K$ ist und den Bewertungsaxiomen (1) und (3) genügt, folgt unmittelbar aus den Normeigenschaften (siehe Beweis von Satz 3.4). Für den Nachweis der Dreiecksungleichung (2′) genügt es,

$$|a|_E \leq 1 \quad \Longrightarrow \quad |1+a|_E \leq 1$$

zu zeigen. Sei also $a \in E$ mit $|a|_E \leq 1$. Ist

$$f(t) = \mathrm{Irr}\,(a, K) = t^k + a_{k-1}t^{k-1} + \ldots + a_0\,,$$

so folgt nach Hilfssatz 7.8

$$|a_0|_K = |a|_E^k \leq 1\,.$$

Da f irreduzibel ist, ist nach Korollar 7.7

$$|a_i|_K \leq \max\,(|a_0|_k, 1) \leq 1$$

für $i = 0, 1, \ldots, k-1$.
Das irreduzible Polynom von $1+a$ ist

$$\mathrm{Irr}\,(1+a, K) = f(t-1)$$

mit dem absoluten Glied

$$f(-1) = a_0 - a_1 + \ldots + (-1)^{k-1}a_{k-1} + (-1)^k\,,$$

also

$$|f(-1)|_K \leq \max_{0\leq i<k}(|a_i|, 1) \leq 1\,.$$

Es folgt

$$|1+a|_E = \sqrt[k]{f(-1)|_K} \leq 1\,. \quad \square$$

Korollar 7.10 *Sei K vollständig und E eine algebraische Erweiterung von K. Dann existiert genau eine Bewertungsfortsetzung $|\ |_E$ auf E, und zwar ist*

$$|a|_E = \sqrt[k]{|a_0|_K} \qquad (a \in E)\,,$$

wenn

$$Irr(a, K) = t^k + ak - 1t^{k-1} + \ldots + a_0$$

ist.

Beweis: 1.) Eindeutigkeit: Seien $|\ |_1$ und $|\ |_2$ zwei verschiedene Fortsetzungen. Dann gibt es ein $a \in E$ mit
$$|a|_1 \neq |a|_2 .$$
Damit wäre die Fortsetzung auf die endliche Erweiterung $K(a)$ nicht eindeutig, im Widerspruch zu Satz 3.6.
2.) $|a|_E := \sqrt[k]{|a_0|_K}$ ist eine Bewertungsfortsetzung: Seien $a, b \in E$. Dann ist $L = K(a, b)$ eine endliche Erweiterung. In L gelten daher die Bewertungsaxiome, also gelten sie allgemein. □

Korollar 7.11 *Sei K ein bewerteter Körper und E eine algebraische Erweiterung von K. Dann existiert eine Bewertungsfortsetzung auf E.*

Beweis: Sei $\hat{K}$ die Komplettierung von K und $\mathcal{C}$ der algebraische Abschluß von $\hat{K}$. Die Bewertung von K läßt sich zu einer Bewertung von $\hat{K}$ und diese nach Korollar 7.11 zu einer Bewertung $|\ |_{\mathcal{C}}$ fortsetzen (diese Fortsetzung ist sogar eindeutig). Da E algebraisch über K ist, gibt es eine Einbettung $\jmath : E \to \mathcal{C}$, die auf K die Identität ist. Durch
$$|x|_E := |\jmath(x)|_{\mathcal{C}} \qquad (x \in E)$$
wird dann eine Bewertungsfortsetzung auf E definiert. □

BEMERKUNG Da es mehrere Einbettungen $\jmath : E \to \mathcal{C}$ geben kann, existieren bei nicht vollständigen Körpern im allgemeinen auch mehrere Bewertungsfortsetzungen.

Beispiel

Es sei $E = \mathbb{Q}(\vartheta)$ mit $\operatorname{Irr}(\vartheta, \mathbb{Q}) = t^2 - 5$.
1. Fall: $t^2 - 5$ ist irreduzibel über $\mathbb{Q}_p$, d.h. 5 ist kein Quadrat in $\mathbb{Q}_p$, also $p = 2, 3, 5, 7, 13, \ldots$ (nach dem Reziprozitätsgesetz sind dies neben 5 die Primzahlen $p \equiv 2 \bmod 5$ oder $p \equiv 3 \bmod 5$). Im algebraischen Abschluß $\mathcal{C}$ von $\mathbb{Q}_p$ gilt
$$t^2 - 5 = (t - c)(t + c)$$
mit $c \in \mathcal{C}$. Bei einer Einbettung
$$\jmath : \mathbb{Q}(\vartheta) \to \mathcal{C}$$
muß notwendig $\jmath(\vartheta) = \pm c$ sein. Somit gibt es zwei Einbettungen
$$\jmath_1(a + b\vartheta) = a + bc \qquad \text{und} \qquad \jmath_2(a + b\vartheta) = a - bc$$
für $a + b\vartheta \in \mathbb{Q}(\vartheta)$.
Wegen

$$\operatorname{Irr}(a + b\vartheta, \mathbb{Q}) = (t - a)^2 - 5b^2 = t^2 - 2at + (a^2 - 5b^2)$$

und

$$\operatorname{Irr}(a - b\vartheta, \mathbb{Q}) = (t - a)^2 - 5b^2 = t^2 - 2at + (a^2 - 5b^2)$$

für $b \neq 0$ führen die beiden Einbettungen zur gleichen Bewertungsfortsetzung

$$|a + b\vartheta|_E = \sqrt{|a^2 - 5b^2|_p} \qquad (a + b\vartheta \in E = \mathbb{Q}(\vartheta))$$

nach Korollar 7.10

2. Fall: $t^2 - 5$ ist reduzibel in $\mathbb{Q}_p$, d.h. 5 ist ein Quadrat in $\mathbb{Q}_p$. Dies gilt für $p = 11, 19, 29, \ldots$ (allgemein nach dem Reziprozitätsgesetz für alle Primzahlen p mit $p \equiv 1 \bmod 5$ oder $p \equiv 4 \bmod 5$). Dann ist

$$t^2 - 5 = (t - c)(t - c) \qquad \text{mit } c \in \mathbb{Q}_p\,,$$

und man erhält die Einbettungen

$$\jmath_1(a + b\vartheta) = a + bc \quad \text{und} \quad \jmath_2(a + b\vartheta) = a - b\vartheta \qquad (a + b\vartheta \in \mathbb{Q}(\vartheta))$$

Die zwei Fortsetzungen sind also

$$|a + b\vartheta|_1 := |a + bc|_p \qquad \text{und} \qquad |a + b\vartheta|_2 := |a - bc|_p\,.$$

Zahlenbeispiel: Sei $p = 11$, und man berechne $|24 - \frac{1}{2}\vartheta|_i$, $i = 1, 2$. $t^2 - 5$ hat in $\mathbb{Q}_{11}$ eine Lösung $c = 4 + 4 \cdot 11 + 6 \cdot 11^2 + \cdots$. Also ist

$$\begin{aligned}\left|24 - \frac{1}{2}\,\vartheta\right|_1 &= \left|2 + 2 \cdot 11 - \frac{1}{2}\,(4 + 4 \cdot 11 + 6 \cdot 11^2 + \cdots)\right|_{11} \\ &= |6 \cdot 11^2 + \cdots|_{11} = |11|_{11}^2 < 1\end{aligned}$$

und

$$\begin{aligned}\left|24 - \frac{1}{2}\,\vartheta\right|_1 &= \left|2 + 2 \cdot 11 + \frac{1}{2}\,(4 + 4 \cdot 11 + 6 \cdot 11^2 + \cdots)\right|_{11} \\ &= |4 + \cdots|_{11} = |11|_{11}^2 = 1\,.\end{aligned}$$

Also sind die beiden Bewertungen verschieden.

Satz 7.12 *Man erhält durch die Einbettungen von E in $\mathcal{C}$ auch jede Bewertungsfortsetzung.*

Beweis: Sei zur Vereinfachung $E = K(\vartheta)$ und $|\ |_E$ eine Bewertungsfortsetzung von $|\ |_K$. Die Komplettierung $\hat{E}$ von E bezüglich $|\ |_E$ enthält die Komplettierung $\hat{K}$ von K und damit $\hat{K}(\vartheta)$. Weil $\hat{K}(\vartheta)$ algebraisch über $\hat{K}$ ist, gibt es eine Einbettung

$$\jmath : \hat{K}(\vartheta) \to \mathcal{C}\,,$$

die auf $\hat{K}$ die Identität ist. Durch

$$|x| := |\jmath(x)|_{\mathcal{C}} \qquad (x \in \hat{K}(\vartheta))$$

wird auf $\hat{K}(\vartheta)$ eine Bewertung definiert. Wegen des Eindeutigkeitssatzes ist $|x|_{\hat{E}} = |\jmath(x)|_{\mathcal{C}}$, $x \in \hat{E}$, also

$$|x|_E = |\jmath(x)|_{\mathcal{C}} \qquad \text{für } x \in E\,,$$

d.h. $|\ |_E$ wird durch die Einbettung

$$\jmath_{|E} : E \to \mathcal{C}$$

induziert. □

8 Satz von Gelfand-Mazur

Es sei A eine Algebra über einem bewerteten Körper K. Dann heißt A *normiert*, wenn eine Norm

$$A \to \mathbb{R}_+, \qquad x \mapsto \|x\|$$

definiert ist und folgende Axiome gelten

(N1) $\quad \|x\| = 0 \iff x = 0,$

(N2) $\quad \|x + y\| \le \|x\| + \|y\|,$

(N3) $\quad \|x\,y\| \le \|x\|\,\|y\|,$

(N4) $\quad \|\alpha\,x\| = |\alpha|\,\|x\|$

für alle $x, y \in A$, $\alpha \in K$. Wir setzen außerdem voraus, daß A ein Einselement besitzt und daß $\|1\| = 1$ ist. Wie üblich läßt sich K mittels der Abbildung $\alpha \mapsto \alpha \cdot 1$ in A einbetten. Aus (N4) folgt $\|\alpha\| = |\alpha|$ für $\alpha \in K$.

Eine Algebra A heißt reell oder komplex, je nachdem ob der Koeffizientenbereich der Körper der reellen oder komplexen Zahlen und die Bewertung der gewöhnliche Absolutbetrag ist.

Bemerkung Fordert man statt (N1) nur $\|0\| = 0$, so spricht man von einer *Halbnorm.* Dann ist $I = \{x \in A \mid \|x\| = 0\}$ ein Ideal in A. Ist A eine Divisionsalgebra (die von Null verschiedenen Elemente sind invertierbar), so folgt $I = 0$ oder $I = A$. Im ersten Fall ist die Halbnorm eine Norm, im zweiten ist $\|x\| = 0$ für alle $x \in A$, also die Halbnorm trivial.

Hilfssatz 8.1 *Es sei $f : \mathbb{N} \to \mathbb{R}$ eine Abbildung mit*

$$f(n+m) \le \frac{n\,f(n) + m\,f(m)}{n+m}.$$

Dann ist $f(n) \le f(1)$ für alle $n \in \mathbb{N}$. Die Folge $(f(n))$ konvergiert gegen ihr Infimum. (Dieses kann eventuell auch $-\infty$ sein.)

Beweis: 1.) Wir beweisen zuerst $f(nm) \le f(m)$ durch Induktion nach n. Für $n = 1$ ist die Ungleichung trivial.

Es sei $n > 1$ und die Ungleichung für $n - 1$ bereits bewiesen. Dann gilt

$$\begin{aligned} f(nm) = f((n-1)m + m) &\le \frac{(n-1)m\,f((n-1)m) + m\,f(m)}{nm} \\ &\le \frac{(n-1)m\,f(m) + m\,f(m)}{nm} = f(m). \end{aligned}$$

Für $m = 1$ ist $f(n) \leq f(1)$.

2.) Es sei $a = \inf f(n)$ und $b \in \mathbb{R}$ mit $a < b$. Ferner sei $\varepsilon > 0$ so gewählt, daß $a < b - \varepsilon$ ist. Dann existiert ein $m \in \mathbb{N}$ mit $f(m) < b - \varepsilon$. Um die Konvergenz der Folge $(f(n))$ gegen a zu zeigen, sei $n \in \mathbb{N}$ und

$$n = qm + r, \qquad 0 \leq r < m.$$

Für $r = 0$ folgt sofort $f(n) = f(qm) \leq f(m) \leq b$. Für $r > 0$ gilt

$$\begin{aligned} f(n) = f(qm + r) &\leq \frac{qm\, f(qm) + r\, f(r)}{n} \\ &\leq (1 - \frac{r}{n}) f(m) + \frac{r}{n} f(1) \\ &\leq f(m) + \frac{r}{n}(f(1) - f(m)) \\ &\leq f(m) + \frac{m}{n}(f(1) - f(m)). \end{aligned}$$

Wählen wir n_0 so groß, daß

$$\frac{m}{n_0}(f(1) - f(m)) \leq \varepsilon$$

ist, so folgt $f(n) \leq f(m) + \varepsilon \leq b$ für alle $n \geq n_0$. Folglich konvergiert $f(n)$ gegen a. □

Definition Für ein Element $x \in A$ sei $s_n(x) := \sqrt[n]{\|x^n\|}$. Dann heißt

$$s(x) = \inf_{n \in \mathbb{N}} \quad s_n(x)$$

Spektralnorm von x.

Satz 8.2 *Es ist*

$$s(x) = \lim_{n \to \infty} s_n(x) \qquad \text{und} \qquad s(x) \leq s_n(x) \leq \|x\|.$$

Beweis: Die Folge $f(n) = \log s_n(x)$ erfüllt die Ungleichung des Hilfssatzes. Damit konvergiert $f(n)$ und folglich auch $s_n(x)$ gegen das Infimum. Aus $f(n) \leq f(1)$ folgt

$$s(x) \leq s_n(x) \leq s_1(x) = \|x\|.$$

□

Korollar 8.3 *Folgende Aussagen sind äquivalent.*

(1) *Norm und Spektralnorm sind gleich.*

(2) *Es gilt* $\|x^n\| = \|x\|^n$ *für alle* $x \in A, \quad n \in \mathbb{N}$.

(3) *Es gilt* $\|x^2\| = \|x\|^2$ *für alle* $x \in A$.

BEMERKUNG Eine Norm mit dieser Eigenschaft heißt *potenzmultiplikativ.*

Beweis: (1)⇒(2): Aus $s(x) = \|x\|$ und

$$s(x) \leq \|x^n\|^{\frac{1}{n}} \leq \|x\|$$

folgt $\|x^n\| = \|x\|^n$.

(3)⇒(1): Durch Induktion folgt aus (3) $\|x^{2^k}\| = \|x\|^{2^k}$, also, weil $(s_{2^k}(x))$ eine Teilfolge von $(s_n(x))$ ist,

$$s(x) = \lim_{n\to\infty} s_n(x) = \lim_{k\to\infty} s_{2^k}(x) = \|x\|.$$

□

Satz 8.4 *Ist A ein kommutative normierte Algebra, so ist*

$$s(x) = \lim_{n\to\infty} \|x^n\|^{\frac{1}{n}}$$

eine potenzmultiplikative Halbnorm auf A.

Beweis: $s(0) = 0$ ergibt sich unmittelbar aus der Definition, (N3) für die Spektralnorm folgt aufgrund der Kommutativität. Ferner gilt (N4) und $s(1) = 1$. Es bleibt der Nachweis der Dreiecksungleichung:

Es sei $\varepsilon > 0$ und $s(x) + \varepsilon = \alpha,\ s(y) + \varepsilon = \beta$. Dann existiert ein $n_0 \in \mathbb{N}$ mit $\|x^n\| \leq \alpha^n$ und $\|y^n\| < \beta^n$ für alle $n \geq n_0$. Ist

$$M = \max_{n<n_0}(1, \frac{\|x^n\|}{\alpha^n}, \frac{\|y^n\|}{\beta^n}),$$

so gilt

$$\|x^n\| \leq M\,\alpha^n, \qquad \|y^n\| \leq M\,\beta^n$$

für alle $n \geq 0$. Für $k \in \mathbb{N}$ gilt dann

$$s_k(x+y)^k = \|(x+y)^k\| \leq \sum_{n=0}^{k} \binom{k}{n} \|x^n\|\,\|y^{k-n}\| \leq M^2\,(\alpha+\beta)^k,$$

also
$$s(x+y) \leq s_k(x+y) \leq M^{2/k}(\alpha+\beta).$$
Weil k beliebig groß gewählt werden kann, folgt
$$s(x+y) \leq \alpha+\beta = s(x)+s(y)+2\,\varepsilon$$
und, weil $\varepsilon > 0$ beliebig ist,
$$s(x+y) \leq s(x)+s(y).$$
□

Satz 8.5 *Es sei A eine vollständige normierte Algebra und $x \in A$. Gilt $s(x) < 1$, so ist $1-x$ invertierbar in A.*

Beweis: 1.) Es sei $s(x) < \alpha < 1$ für $\alpha \in A$. Dann existiert ein $n_0 \in \mathbb{N}$ mit $\|x^n\| < \alpha^n$ für $n \geq n_0$. Wegen $\alpha < 1$ konvergiert $\|x^n\|$ gegen 0. Die Folge
$$y_n = 1 + x + \ldots + x^{n-1}$$
ist eine Cauchy-Folge in A, weil
$$\begin{aligned}\|y_m - y_n\| &= \|x^m + x^{m+1} + \ldots + x^{n-1}\| \\ &\leq \|x^m\| \left(\|1\| + \|x\| + \|x^2\| + \ldots\right) \\ &\leq \|x^m\| \left(\sum_{i=0}^{n_0-1} \|x^i\| \quad + \frac{\alpha^{n_0}}{1-\alpha}\right)\end{aligned}$$
für genügend große n, m beliebig klein wird.

2.) Weil A vollständig ist, konvergiert die Folge (y_n) gegen ein $y \in A$. Es ist $(1-x)y_n = 1 - x^n$, also
$$\|1-(1-x)\,y\| = \|x^n + (1-x)(y_n-y)\| \leq \|x^n\| + \|1-x\|\,\|y_n-y\|.$$
Der rechtsstehende Ausdruck konvergiert gegen Null, also ist $(1-x)y = 1$. Ähnlich folgt $y(1-x) = 1$. Damit ist $1-x$ invertierbar. □

Hilfssatz 8.6 *Es sei A eine komplexe normierte Algebra und G eine kompakte Teilmenge von $\mathbb{C}$. Ist $1-x\alpha$ für jedes $\alpha \in G$ invertierbar in A, so ist die Funktion*
$$f : G \to A, \qquad f(\alpha) = (1-x\alpha)^{-1},$$
beschränkt auf G, d.h. es gibt eine reelle Zahl M mit
$$\|f(\alpha)\| \leq M \qquad \textit{für alle } \alpha \in G.$$

Beweis: Für $\alpha, \beta \in G$ gilt $f(\alpha) - f(\beta) = f(\alpha)\, f(\beta)\, x\, (\alpha - \beta)$, also

$$\|f(\alpha) - f(\beta)\| = \|f(\alpha)\|\, \|f(\beta)\|\, \|x\|\, |\alpha - \beta|.$$

Wegen $\|f(\alpha)\| \leq \|f(\beta)\| + \|f(\alpha) - f(\beta)\|$ folgt

$$\|f(\alpha)\|(1 - f(\beta)\|\, \|x\|\, |\alpha - \beta|) \leq \|f(\beta)\|.$$

Die Menge

$$U(\beta) = \{\alpha \in \mathbb{C} \mid \|f(\beta)\|\, \|x\|\, |\alpha - \beta| < \frac{1}{2}\}$$

ist eine Umgebung von β. Hiermit folgt

$$\|f(\alpha)\| \leq 2\, \|f(\beta)\| \qquad \text{für alle } \alpha \in U(\beta).$$

Die Umgebungen $U(\beta)$ überdecken G, wenn β die Menge G durchläuft. Weil G kompakt ist, wird G bereits durch endlich viele Umgebungen, etwa durch

$$U(\beta_1), \ldots, U(\beta_n)$$

überdeckt. Es sei

$$M = \max_{i=1,\ldots,n} \{2\, \|f(\beta_i)\|\}.$$

Dann gilt $\|f(\alpha)\| \leq M$ für alle $\alpha \in G$, also ist f beschränkt auf G. □

Definition Es sei $x \in A$. Die Menge der $\alpha \in \mathbb{C}$, für die $\alpha - x$ nicht invertierbar ist, heißt *Spektrum* von x.

Bemerkung Besteht A aus linearen Abbildungen eines endlich dimensionalen Vektorraums V, so ist α genau dann Eigenwert von x, wenn die Determinante von $\alpha - x$ gleich Null, also $\alpha - x$ nicht invertierbar ist. Folglich ist das Spektrum die Menge der Eigenwerte.

Satz 8.7 *Es sei A eine komplexe normierte Algebra und $x \in A$ mit $s(x) \neq 0$. Dann existiert ein α im Spektrum von x mit $|\alpha| \geq s(x)$.*

Beweis: 1.) Wir setzen zunächst $s(x) = 1$ voraus. Wir betrachten die kompakte Kreisscheibe

$$G = \{\alpha \in \mathbb{C} \mid |\alpha| \leq 1\}$$

und nehmen an, daß $f(\alpha) = (1 - x\alpha)^{-1}$ für alle $\alpha \in G$ existiert.

Nach Hilfssatz 8.6 gilt dann

(3) $$\|f(\alpha)\| \leq M \qquad \text{für alle } \alpha \in G.$$

Für jedes $n \in \mathbb{N}$ sei F_n die auf dem Intervall $[0,1]$ definierte Funktion

$$F_n(r) = \frac{1}{n} \sum_{\varepsilon} f(r\varepsilon) = \frac{1}{n} \sum_{\varepsilon} (1 - xr\varepsilon)^{-1},$$

wobei ε die n-ten Einheitswurzeln durchläuft. Aus (3) folgt

$$\|F_n(r)\| \leq M \qquad \text{für alle } r \in [0,1]. \tag{4}$$

Durch Partialbruchzerlegung ergibt sich

$$\frac{1}{1 - X^n} = \frac{1}{n} \sum_{\varepsilon} \frac{1}{1 - X\varepsilon},$$

wobei wieder ε die n-ten Einheitswurzeln durchläuft. Eingesetzt erhalten wir

$$F_n(r) = (1 - (xr)^n)^{-1}. \tag{5}$$

Daraus folgt $F_n(r) - 1 = (xr)^n F_n(r)$, also wegen (4)

$$\|F_n(r) - 1\| \leq \|(xr)^n\| \, M.$$

Aus $f(\alpha) - f(\beta) = f(\alpha)\, f(\beta)\, x\, (\alpha - \beta)$, folgt

$$\|F_n(1) - F_n(r)\| \leq M^2 \, \|x\| \, |1 - r|,$$

also

$$\begin{aligned} \|F_n(1) - 1\| &\leq \|F_n(1) - F_n(r)\| + \|F_n(r) - 1\| \\ &\leq M^2 \, \|x\| \, |1 - r| + \|(xr)^n\| \, M. \end{aligned}$$

Es sei $r < 1$. Wegen $s(xr) = r < 1$ konvergiert dann $\|(xr)^n\|$ gegen 0 (siehe Beweis von Satz 8.5). Für genügend großes n und genügend kleines $|1 - r|$ wird der obige Ausdruck beliebig klein. Es gibt daher ein $n \in \mathbb{N}$ mit

$$\|F_n(1) - 1\| \leq \frac{1}{3}.$$

Hieraus folgt

$$\|x^n\| = \|(F_n(1) - 1)(1 - x^n)\| \leq \frac{1}{3}(1 + \|x^n\|),$$

also

$$\|x^n\| \leq \frac{1}{2}.$$

Andrerseits gilt aber wegen $s_n(x) \geq s(x) = 1$

$$\|x^n\| = s_n(x)^n \geq 1.$$

Folglich gibt es ein $\alpha \in G$, für das $1 - x\alpha$ nicht invertierbar ist.

2.) Es sei jetzt $x \in A$ mit $s(x) \neq 1$. Dann ist

$$y = \frac{x}{s(x)}$$

ein Element mit $s(y) = 1$. Wie eben gezeigt wurde, gibt es ein $\beta \in G$, für das $1 - y\beta$ nicht invertierbar ist. Offensichtlich ist dann $\beta \neq 0$. Für $\alpha = \beta^{-1}$ gilt dann die Behauptung des Satzes. □

Bemerkung Ist die Algebra außerdem vollständig, so kann Satz 8.5 angewendet werden. Danach ist $1 - x\alpha$ invertierbar, wenn $s(x\alpha) = s(x)|\alpha| < 1$ gilt. Daraus ergibt sich, daß das Spektrum von x in $\{\alpha \in \mathbb{C} \mid |\alpha| \leq s(x)\}$ enthalten ist und daß auf dem Kreis mindestens ein Punkt des Spektrums liegt.

Satz 8.8 (Gelfand-Mazur) *Eine kommutative normierte Divisionsalgebra A über $\mathbb{C}$ ist zu den komplexen Zahlen isomorph.*

Beweis: Nach Satz 8.4 ist die Spektralnorm s eine Halbnorm. Für $x \neq 0$ ist

$$1 = s(1) = s(x \cdot x^{-1}) \leq s(x)s(x^{-1}),$$

also $s(x) \neq 0$, d.h. S ist sogar eine Norm auf A. Nach Satz 8.7 ist das Spektrum von x nicht leer. Es gibt es also ein $\alpha \in \mathbb{C}$, für da $\alpha - x$ nicht invertierbar ist. Da A eine Divisionsalgebra ist, folgt $x = \alpha \in \mathbb{C}$. Wegen $\|1\| = 1$ ist $\|\alpha\| = \|\alpha \cdot 1\| = |\alpha|$. □

Unter Verwendung der Spektralnorm erhalten wir auch eine reelle Fassung des Satzes von Gelfand-Mazur. Eine reelle normierte Algebra erfüllt analog zu (N4) das Axiom

(N4′) $$\|\alpha x\| = |\alpha|\,\|x\|, \qquad \alpha \in \mathbb{R}, \qquad x \in A.$$

Wir zeigen zuerst

Hilfssatz 8.9 *Es sei E eine reelle normierte Algebra, die die komplexen Zahlen enthält. Dann gilt für die Spektralnorm*

$$s(\alpha x) = |\alpha|\,\|x\|$$

für alle $\alpha \in \mathbb{C}$ und $x \in A$.

Beweis: Es sei $\alpha = u + iv \in \mathbb{C}$ mit $|\alpha| = u^2 + v^2 = 1$. Dann ist $|u|,\ |v| \leq 1$, also

$$\|\alpha\| \leq |u| + |v| \, \|i\| \leq 1 + \|i\| =: M.$$

Da mit α auch α^n, $n \in \mathbb{N}$, auf dem Einheitskreis liegt, folgt

$$s(\alpha) \leq \|\alpha^n\|^{\frac{1}{n}} \leq M^{\frac{1}{n}},$$

also $s(\alpha) \leq 1$.

Es sei jetzt $\alpha = x + iy \in \mathbb{C}$ beliebig. Wir schreiben $\alpha = r(u + iv)$ mit $r = |\alpha|$. Dann ist nach (N4′)

$$s(\alpha) = r\, s(u + iv) \leq r = |\alpha|.$$

Daraus ergibt sich für $x \in E$

$$s(\alpha x) \leq s(\alpha)s(x) \leq |\alpha| s(x).$$

Aber $s(\alpha x) < |\alpha| s(x)$ für ein $\alpha \in \mathbb{C}$ führt zum Widerspruch

$$s(x) = s(\alpha^{-1}\alpha x) \leq |\alpha^{-1}| s(\alpha x) < |\alpha^{-1}| \, |\alpha| s(x) = s(x).$$

Somit gilt

$$s(\alpha x) = |\alpha| \, s(x)$$

für alle $\alpha \in \mathbb{C}$ und $x \in A$. □

Satz 8.10 *Eine reelle kommutative normierte Divisionsalgebra A ist zu $\mathbb{R}$ oder zu $\mathbb{C}$ isomorph.*

Beweis: Wir betrachten zwei Fälle.

1.) Das Polynom $f(t) = t^2 + 1$ besitzt eine Nullstelle in A. Dann enthält A einen zu $\mathbb{C}$ isomorphen Teilkörper. Nach dem Hilfssatz ist A eine komplexe normierte Algebra bezüglich der Spektralnorm und damit nach dem Satz von Gelfand-Mazur isomorph zu den komplexen Zahlen.

2.) Das Polynom $f(t) = t^2 + 1$ besitzt keine Nullstelle in A und ist daher irreduzibel über der Körper A. Es sei $E = A(i)$ mit $f(t)$ als ireduziblen Polynom von i. E enthält dann einen zu $\mathbb{C}$ isomorphen Körper. Durch

$$\|x + iy\| := \|x\| + \|y\|$$

definieren wir eine Norm auf E, die die Norm von A fortsetzt. Die Eigenschaften (N1) und (N2) für diese Norm ergeben sich unmittelbar. (N3) folgt aus

$$\begin{aligned} \|z\, z'\| \ & \|xx' - yy'\| + \|xy' + x'y\| \\ & \leq \|x\| \, \|x'\| + \|y\| \, \|y'\| + \|x\| \, \|y'\| + \|x'\| \, \|y\| \\ & (\|x\| + \|y\|)(\|x'\| + \|y'\|) = \|z\| \, \|z'\| \end{aligned}$$

und (N4′) für $\alpha \in \mathbb{R}$

$$\begin{aligned}\|\alpha(x+iy)\| &= \|\alpha x\| + \|\alpha y\| \\ &= |\alpha|\ \|x+iy\|.\end{aligned}$$

Nach dem Satz von GELFAND-MAZUR ist $E = \mathbb{C}$, also $\mathbb{R} \subseteq A \subset E = \mathbb{C}$, woraus $A = \mathbb{R}$ folgt. □

BEMERKUNG Die Isomorphie von A und $\mathbb{C}$ im Satz von GELFAND-MASUR bezieht sich auf die algebraischen Operationen und auf die Spektralnorm, also $s(\alpha) = |\alpha|$. Es gilt daher $|\alpha| \leq \|\alpha\|$. Es braucht also nicht $|\alpha| = \|\alpha\|$ zu gelten. Als Beispiel betrachte man $\mathbb{C}$ als Divisionsalgebra über $\mathbb{R}$ bezüglich der Norm $\|x+iy\| = |x| + |y|$.

9 Aufgaben

Aufgabe 1 Zeige, daß für $x \in \mathbb{Q}^\times$ gilt:

(a) $|x|_p = 1$ für fast alle Primzahlen $p \in \mathbb{P}$.

(b)
$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |x|_p = 1$$

Aufgabe 2 K sei nicht-archimedisch bewertet. Zeige:
Ist $a_1 + \cdots + a_n = 0$, so werden zwei der Summanden gleich bewertet.

Aufgabe 3 In einem bewerteten Körper K heißt

$$K_r(a) := \{x \in K \mid |x - a| = r\}$$

Kreis mit dem Radius r und dem Zentrum a, und

$$U_r(a) := \{x \in K \mid |x - a| < r\}$$

heißt Kreisscheibe. Zeige für einen nicht-archimedisch bewerteten Körper:

(a) Jeder Punkt $b \in U_r(a)$ ist Zentrum von $K_r(a)$.

(b) Für $y \notin U_r(a)$ ist der Abstand $|y - x|$ von allen Punkten $x \in U_r(a)$ gleich.

(c) Zwei Kreisscheiben sind entweder disjunkt, oder eine ist in der anderen enthalten.

Aufgabe 4 (a) Zeige, daß der gewöhnliche Absolutbetrag auf $\mathbb{C}$ der Gleichung

$$(*) \qquad |x + y|^2 + |x - y|^2 = 2 \cdot |x|^2 + 2 \cdot |y|^2$$

genügt.
(b) Zeige, daß es bei nicht-archimedisch bewerteten Körpern K stets $x, y \in K$ gibt, so daß die Gleichung $(*)$ verletzt ist.

Aufgabe 5 Ist (a_n) eine Cauchy-Folge in einem bewerteten Körper, die keine Nullfolge ist, so gibt es ein $\varepsilon > 0$ und ein $n_0 \in \mathbb{N}$ mit

$$|a_n| \geq \varepsilon \quad \text{für } n \geq n_0.$$

Aufgabe 6 Zeige, daß die Folgen

(a) $a_n = 1 + 2 + 2^2 + \cdots + 2^n$

(b) $b_n = 1 \cdot 2 + 2 \cdot 2^2 + \cdots + n \cdot 2^n$

in $\mathbb{Q}$ bezüglich der 2-adischen Bewertung konvergieren. Berechne die Grenzwerte.

Aufgabe 7 Es sei K ein vollständiger Körper.

(a) Zeige, daß ein $\varepsilon > 0$ existiert, so daß alle $a \in K$ mit $|1 - a| < \varepsilon$ Quadrate in K sind.

(b) Zeige, daß alle positiven reellen Zahlen Quadrate sind

(Hinweis: Betrachte das quadratische Polynom $(t + 1)^2 - a$, bei Teil (b) zunächst den Fall $0 < a \leq 1$.)

Aufgabe 8 Es sei K ein nicht-archimedisch bewerteter Körper.

(a) Zeige, daß (a_n) eine Cauchy-Folge ist, wenn zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ existiert mit

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

für alle $n \geq n_0$.

(b) Zeige, daß eine Reihe $\sum a_n$ konvergiert, wenn K vollständig und $\lim a_n = 0$ ist.

Aufgabe 9 Ein Teilring B eines Körpers K heißt ein Bewertungsring, wenn für $x \in K^\times$ stets x oder x^{-1} in B liegt. Zeige:

(a) Ist I eine nicht-leere Teilmenge von B mit

$$x \in B,\, a \in I \quad \Longrightarrow \quad xa \in I\,,$$

so ist I ein Ideal von B.

(b) Die Ideale von B sind durch Inklusion linear geordnet (d.h. für zwei Ideale I_1, I_2 von B gilt $I_1 \subseteq I_2$ oder $I_2 \subseteq I_1$).

Aufgabe 10 Zeige unter Verwendung der geometrischen Reihe, daß in $\mathbb{Q}_p$

$$x = \sum_{i=0}^{\infty} a_i p^i\,, \qquad 0 \leq a_i \leq p - 1$$

mit periodischen Koeffizienten (d.h. für ein $t \in \mathbb{N}$ gilt $a_i = a_{i+t}$ für alle i) eine rationale Zahl darstellt.
Berechne speziell $x = 1 + p + p^3 + p^4 + p^6 + p^7 + p^9 + p^{10} + \cdots$

Aufgabe 11 Begründe, daß 7 ein Quadrat in $\mathbb{Q}_3$ ist.
Berechne die Wurzeln von 7

(a) mit dem Newtonschen Verfahren

(b) mit dem Ansatz $x = a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + \cdots$ aus der Gleichung $x^2 = 7$ durch Koeffizientenvergleich (möglich ist $a_0 = 1$ und $a_0 = 2$!)

jeweils bis auf einen Fehler $\leq |3|_3^5$.

Aufgabe 12 Zeige, daß eine rationale Zahl a genau dann ein Quadrat in $\mathbb{Q}$ ist, wenn a ein Quadrat in allen p-adischen Körpern $\mathbb{Q}_p$ und in $\mathbb{R}$ ist. (Beachte die Primfaktorzerlegung von a.)

Aufgabe 13 Berechne für $x = \dfrac{3}{5}$ zwei Zahlen $a_0, b_0 \in \mathbb{N}$, $a_0 < 41$, $b_0 < 641$, so daß

$$|x - a_0|_{41} < 1 \qquad \text{und} \qquad |x - b_0|_{641} < 1$$

ist.
Stelle hiermit fest, ob x ein Quadrat in $\mathbb{Q}_{41}$ oder $\mathbb{Q}_{641}$ ist.

Aufgabe 14 Ermittle mit dem chinesischen Restsatz eine natürliche Zahl, die ein Quadrat in $\mathbb{Q}_2$ und $\mathbb{Q}_3$, aber nicht in $\mathbb{Q}_5$ und $\mathbb{Q}_7$ ist.

Literatur

[1] Artin, E.: *Theory of Algebraic Numbers.*
Vorlesung Göttingen 1959

[2] Bachmann, G.: *Introduction to p-adic Numbers and Valuation Theory.*
Academic Press 1964

[3] Borevich, S. I. & Shafarevich, J. R.: *Zahlentheorie.*
Birkhäuser 1966

[4] Bourbaki, N.: *Algèbre Commutative.*
Hermann 1965
englisch: *Commutative Algebra.*
Addison-Wesley 1970

[5] Endler, O.: *Valuation Theory.*
Springer 1972

[6] McCarthy, P. J.: *Algebraic Extensions of Fields.*
Blaisdell 1966

[7] Nagata, M.: *Field Theory.*
Dekker 1977

[8] Ribenboim, P.: *Théorie des Valuations.*
Vorleung Montreal 1964

[9] Schilling, O. F. G.: *The Theory of Valuations.*
American Mathematical Society 1950

[10] van der Waerden, B. L.: *Algebra II.*
Springer 1936/67

[11] Zariski, O. & Samuel, P.: *Commutative Algebra I, II.*
Van Nostrand 1960

Index