Prof. Dr. K. Mathiak

Bewertungstheorie

Braunschweig, 1993

Prof. Dr. K. Mathiak
Technische Universität Braunschweig
Institut für Algebra und Zahlentheorie
Pockelsstraße 14
38106 Braunschweig

Dieses Skript wurde mit dem LaTeX 2_ε-Makropaket $\mathcal{AMS}$-LaTeX 2_ε erstellt.
Satz: Dr. W. Oelke, Institut für Algebra und Zahlentheorie

Inhaltsverzeichnis

Kapitel 1. Reelle Bewertungen 5

Kapitel 2. Vollständige Körper 15

1. Die Komplettierung 15

2. Quadratische Gleichungen 21

Kapitel 3. Endliche Erweiterungen vollständiger Körper 23

Kapitel 4. Archimedische Bewertungen 31

Kapitel 5. Die p-adischen Zahlen 37

1. Allgemeine Eigenschaften 37

2. Quadrate in $\mathbb{Q}_p$ 50

Kapitel 6. Bewertungsfortsetzungen 53

Kapitel 7. Geordnete Gruppen 63

Kapitel 8. Krullbewertungen 71

1. Multiplikative Krullbewertungen 71

2. Additive Krullbewertungen 79

Kapitel 9. Fortsetzungssatz für Krullbewertungen 83

Kapitel 10. Der Approximationssatz 91

Kapitel 11. Prüferringe 99

Kapitel 12. Algebraische Erweiterungen 109

Kapitel 13. Relativ vollständige Körper 113

Literatur 117

Index 119

KAPITEL 1

Reelle Bewertungen

Es sei K ein Körper und

$$\mathbb{R}_+ := \{a \in \mathbb{R} \mid a \geq 0\}$$

die Menge der nicht-negativen reellen Zahlen.

DEFINITION 1.1. Eine Abbildung

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

heißt eine *reelle Bewertung* von K, wenn sie für alle $x, y \in K$ folgenden Axiomen genügt:

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

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

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

Man unterscheidet zwei Arten reeller Bewertungen:

DEFINITION 1.2. Eine reelle Bewertung $|\ |: K \to \mathbb{R}_+$ 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*.

BEMERKUNG. Weil für alle $x, y \in K$

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

gilt, ist (2′) eine Verschärfung von (2).

BEISPIEL. 1.) Es sei K ein Teilkörper von $\mathbb{C}$. Der gewöhnliche Absolutbetrag

$$|x + iy| := \sqrt{x^2 + y^2} \qquad (x, y \in \mathbb{R},\ i^2 = -1)$$

ist wegen

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

eine archimedische Bewertung.
(Hiernach kann man die reellen Bewertungen als eine Verallgemeinerung des Absolutbetrages ansehen.)

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

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

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

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

und

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

Häufig setzt man $d = \dfrac{1}{p}$ und nennt

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

die *p-adische Bewertung* von $\mathbb{Q}$. Sie mißt die Teilbarkeit der Zahl x durch p. So ist beispielsweise für $p = 2$

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

und die Folge $\left(2, 2^2, 2^3, \ldots\right)$ bezüglich der 2-adischen Bewertung eine Nullfolge.

3.) Es sei K der Körper der in einem Gebiet $G \subseteq \mathbb{C}$ meromorphen Funktionen, $a \in G$ und $d \in \mathbb{R}$ mit $0 < d < 1$. Jede von der Nullfunktion verschiedene Funktion $f \in K$ besitzt eine Darstellung

$$(*) \qquad f(z) = (z-a)^k \frac{g(z)}{h(z)}$$

mit in G holomorphen Funktionen g und h, die an der Stelle $a \in G$ von Null verschieden sind. Dann wird für alle $f \in K$ durch

$$|f| := \begin{cases} d^k & \text{falls } f \neq 0 \text{ die Darstellung } (*) \text{ besitzt} \\ 0 & \text{falls } f = 0 \text{ ist} \end{cases}$$

eine nicht-archimedische Bewertung auf K definiert. (Der Beweis erfolgt analog dem zu Beispiel 2.)

4.) Es sei K ein beliebiger Körper. Definiert man

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

so erhält man eine nicht-archimedische Bewertung von K, die als die *triviale Bewertung* von K bezeichnet wird.

Einfache Folgerungen aus den Axiomen

(A) Es gilt

$$\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$$

für alle $x, y \in K$ mit $y \neq 0$.

BEWEIS. Nach Axiom (3) ist

$$|x| = \left|\frac{x}{y} \cdot y\right| = \left|\frac{x}{y}\right| \cdot |y|\,. \quad \square$$

(B) Für das Einselement 1 in K gilt: $|1| = |-1| = 1$.

BEWEIS. Aus (A) ergibt sich

$$|1| = \left|\frac{1}{1}\right| = \frac{|1|}{|1|} = 1\,.$$

Angenommen, es ist $|1| \leq |-1|$. Wegen $|-1| > 0$ folgt dann

$$|-1| = |-1| \cdot |1| \leq |-1| \cdot |-1| = |(-1)(-1)| = |1| = 1\,.$$

Ebenso folgt aus der Annahme $|-1| \leq |1|$

$$|-1| = |-1| \cdot |1| \geq |-1| \cdot |-1| = |1|\,. \quad \square$$

(C) Es gilt $|x| = |-x|$ für alle $x \in K$.

BEWEIS. Nach Axiom (3) und Eigenschaft (B) ist

$$|-x| = |-1| \cdot |x| = |1| \cdot |x| = |x|\,. \quad \square$$

(D) Es gilt

$$\big||x| - |y|\big|_\infty \leq |x - y|$$

für alle $x, y \in K$, wobei $|\ |_\infty$ den gewöhnlichen Absolutbetrag auf $\mathbb{R}$ bezeichnet.

BEWEIS. Gemäß Axiom (2) ist

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

also

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

Entsprechend folgt

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

und man erhält

$$\big||x| - |y|\big|_\infty \leq |x - y|\,. \quad \square$$

(E) Ist $|\ |$ nicht-archimedisch, so folgt für alle $x, y \in K$ mit $|x| \neq |y|$

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

Man nennt diese Eigenschaft das *Dominanzprinzip*.

BEWEIS. Sei etwa $|x| < |y|$. Nach Axiom $(2')$ 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. □

DEFINITION 1.3. 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.

BEISPIEL. Die Bewertungen von $\mathbb{Q}$ mit fester Primzahl p

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

sind für alle $d \in \mathbb{R}$, $0 < d < 1$ äquivalent.

SATZ 1.1. *Zwei Bewertungen $|\ |_1$ und $|\ |_2$ von K 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.) Da die Abbildung $\mathbb{R}_+ \to \mathbb{R}_+$, $a \to a^s$ für $s > 0$ isoton ist, gilt

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

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

2.) Seien nun $|\ |_1$ 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 (andernfalls betrachte 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 gäbe ein $x \in K^\times$ mit

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

Dann gäbe es ein $\frac{n}{m} \in \mathbb{Q}$, $n \in \mathbb{Z}$, $m \in \mathbb{N}$ mit

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

Aus der ersten Ungleichung folgte dann

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

und aus der zweiten Ungleichung folgte 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 $x \in K$. □

Ist eine Bewertung nicht-archimedisch, so gilt nach Axiom $(2')$

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

für alle $x, y \in K$. Hieraus folgt sofort durch Induktion nach $n \in \mathbb{N}$

$$|x_1 + \cdots + x_n| \leq \max(|x_1|, \ldots, |x_n|)$$

für alle $x_i \in K$, $1 \leq i \leq n$. daher ist

$$|n \cdot 1| = \left|\sum_{i=1}^{n} 1\right| \leq 1$$

für alle $n \in \mathbb{N}$, und man erhält

FOLGERUNG 1.1. *Ist eine Bewertung nicht-archimedisch, so ist die Menge*

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

nach oben durch 1 *beschränkt.*

LEMMA 1.1. *Sind* $A, B \in \mathbb{R}$ *mit* $A > 0$ *und* $B \geq 0$, *so gilt*

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

BEWEIS. Es ist

$$\begin{aligned}\lim_{m\to\infty} \sqrt[m]{Am+B} &= \lim_{m\to\infty} \exp\left(\frac{1}{m}\ln(Am+B)\right)\\ &= \exp\left(\lim_{m\to\infty}\frac{\ln(Am+B)}{m}\right)^{\dagger}\\ &= \exp\left(\lim_{m\to\infty}\frac{A}{Am+B}\right)^{\ddagger}\\ &= \exp(0) = 1\,. \quad \square\end{aligned}$$

SATZ 1.2. *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

$$|n\cdot 1|\le A$$

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

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

also

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

für alle $m\in\mathbb{N}$. Mit Lemma 1.1 folgt

$$|x+y|\le 1\cdot|x| = |x| = \max\left(|x|,|y|\right),$$

also ist die Bewertung nicht-archimedisch.

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

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

nach Folgerung 1.1 nach oben beschränkt. $\square$

KOROLLAR 1.1. *Hat K die Charakteristik $p\neq 0$, so ist jede Bewertung von K nicht-archimedisch.*

KOROLLAR 1.2. *Ist eine Bewertung auf K archimedisch, so ist sie auch auf jedem Teilkörper von K archimedisch.*

---

†Stetigkeit von exp

‡Regel von L'HOSPITAL

KOROLLAR 1.3. *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

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

die n-adische Darstellung von m. Da nur endlich viele Werte für die Koeffizienten a_i möglich sind, gibt es ein $A \in \mathbb{R}$ mit

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

Dann ist

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

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 1.2 ist die Bewertung damit nicht-archimedisch. □

Bisher haben wir auf $\mathbb{Q}$ drei Arten von Bewertungen kennengelernt:

1.) den gewöhnliche Absolutbetrag (archimedisch),
2.) die p-adischen Bewertungen (nicht-archimedisch),
3.) die triviale Bewertung (nicht-archimedisch).

Der folgende Satz von OSTROWSKI besagt, daß dies bis auf Äquivalenz alle Bewertungen sind.

SATZ 1.3. (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 1.3 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

$$m^t = a_0 + a_1 n + \cdots + a_r n^r$$

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

$$|a_i| = |1 + \ldots 1| \leq n ,$$

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 1.1 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. □

KAPITEL 2

Vollständige Körper

1. Die Komplettierung

Im folgenden sei K stets ein Körper mit der Bewertung $|\ |$.

DEFINITION 2.1. Eine Folge (x_n) aus K *konvergiert* gegen $x \in K$, wenn zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ existiert, so daß

$$|x - x_n| < \varepsilon$$

für alle $n \geq n_0$ gilt.

DEFINITION 2.2. Eine Folge (x_n) aus K heißt *Cauchy-Folge*, wenn zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ existiert, so daß

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

für alle $n, m \geq n_0$ gilt.

Wie für reelle Zahlenfolgen zeigt man:

(A) Der Grenzwert $x \in K$ einer konvergenten Folge (x_n) aus K ist eindeutig bestimmt, geschrieben $\lim x_n = x$.
(B) Ist $x = \lim x_n$ und $y = \lim y_n$, so gilt

$$\lim(x_n \pm y_n) = x \pm y\,, \quad \lim(x_n y_n) = xy\,, \quad \lim |x_n| = |x|\,.$$

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

Es sei $\mathfrak{F}$ die Menge aller Folgen aus K. Durch

$$(*) \qquad \begin{aligned} (x_n) + (y_n) &:= (x_n + y_n) \\ (x_n) \cdot (y_n) &:= (x_n y_n) \end{aligned}$$

wird $\mathfrak{F}$ ein kommutativer Ring mit der konstanten Folge $(1) = (1, 1, \ldots)$ als Einselement.

LEMMA 2.1. *Die Menge $\mathfrak{C}$ aller Cauchy-Folgen aus K bildet bezüglich $(*)$ einen kommutativen Ring mit Eins.*

BEWEIS. Sind $(x_n), (y_n) \in \mathfrak{C}$, so gibt es nach (D) ein $M \in \mathbb{R}$ mit

$$|x_n| \leq M \qquad \text{und} \qquad |y_n| \leq M$$

für alle $n \in \mathbb{N}$. Ferner gibt es zu jeden $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ mit

$$|x_n - x_m| < \varepsilon \qquad \text{und} \qquad |y_n - y_m| < \varepsilon$$

für alle $n, m \geq n_0$. Dann ist

$$|x_n - y_n - (x_m - y_m)| \leq |x_n - x_m| + |y_n - y_m| < 2\varepsilon$$

und

$$\begin{aligned} |x_n y_n - x_m y_m| &= |x_n (y_m - y_m) + y_m (x_n - x_m)| \\ &\leq |x_n| \, |y_n - y_m| + |y_m| \, |x_n - y_m| \\ &\leq M \, |y_n - y_m| + M \, |x_n - x_m| \\ &< 2\varepsilon M \end{aligned}$$

für alle $n, m \geq n_0$. Also sind $(x_n) - (y_n)$ und $(x_n)\,(y_n)$ Cauchy-Folgen. Trivialerweise ist die konstante Folge $(1) = (1, 1, \ldots)$ eine Cauchy-Folge. Also ist $\mathfrak{C}$ ein kommutativer Teilring von $\mathfrak{F}$ mit Eins. □

LEMMA 2.2. *Die Menge $\mathfrak{N}$ aller Nullfolgen aus K bildet ein Ideal in $\mathfrak{C}$.*

BEWEIS. Wegen $(0) = (0, 0, \ldots) \in \mathfrak{N}$ ist $\mathfrak{N} \neq \emptyset$. Des weiteren gilt $\mathfrak{N} \subseteq \mathfrak{C}$, weil nach (C) jede konvergente Folge eine Cauchy-Folge ist.
Sind (x_n) und (y_n) Nullfolgen, so ist

$$\lim(x_n - y_n) = 0$$

nach (B), also ist auch $(x_n - y_n)$ eine Nullfolge.
Sei schließlich $(x_n) \in \mathfrak{N}$ und $(y_n) \in \mathfrak{C}$. Dann gibt es wegen (D) ein $M \in \mathbb{R}$ mit

$$|y_n| \leq M$$

für alle $n \in \mathbb{N}$. Daher ist

$$|x_n y_n| = |x_n| \, |y_n| \leq M \, |x_n|$$

für alle $n \in \mathbb{N}$. Also ist $(x_n)\,(y_n)$ eine Nullfolge.
Insgesamt ist damit $\mathfrak{N}$ ein Ideal in $\mathfrak{C}$. □

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

$$|x_n| \geq \varepsilon$$

für alle $n \geq n_0$.

BEWEIS. Annahme: Für alle $\varepsilon > 0$ und für alle $n_0 \in \mathbb{N}$ existiert ein $n \in \mathbb{N}$ mit $|x_n| < \varepsilon$. Weil (x_n) eine Cauchy-Folge ist, gibt es zu $\varepsilon > 0$ ein n_0 mit $|x_n - x_m| < \varepsilon$ für alle $n, m \geq n_0$. Nach Annahme gibt es zu diesem n_0 ein $n_1 \geq n_0$ mit $|x_{n_1}| < \varepsilon$. Es folgt

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

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

DEFINITION 2.3. Ein bewerteter Körper K heißt *vollständig* oder *komplett*, wenn jede Cauchy-Folge aus K in K konvergiert.

DEFINITION 2.4. Ein Teilkörper K eines bewerteten Körpers $\hat{K}$ heißt *dicht* in $\hat{K}$, wenn zu jedem $x \in \hat{K}$ und zu jedem $\varepsilon > 0$ ein $y \in K$ mit

$$|x - y| < \varepsilon$$

existiert.

DEFINITION 2.5. Ein bewerteter Körper $\hat{K}$ heißt eine *Komplettierung* des bewerteten Körpers K, wenn gilt:

(1) $\hat{K}$ ist vollständig.
(2) K ist dichter Teilkörper von $\hat{K}$.
(3) Die Bewertung von K ist induziert von der Bewertung von $\hat{K}$, d.h.

$$|a|_K = |a|_{\hat{K}}$$

für alle $a \in K$.

BEISPIEL. $\mathbb{R}$ ist die Komplettierung von $\mathbb{Q}$ bezüglich des gewöhnlichen Absolutbetrages.

SATZ 2.1. *Jeder bewertete Körper K besitzt eine Komplettierung $\hat{K}$.*

BEWEIS. 1.) Nach Lemma 2.2 ist $\hat{K} := \mathfrak{C}/\mathfrak{N}$ ein kommutativer Ring mit Eins. $\hat{K}$ ist sogar ein Körper:
Sei $(x_n) + \mathfrak{N} \neq 0$, also (x_n) eine Cauchy-Folge, die keine Nullfolge ist. Dann gibt es nach Lemma 2.3 ein $\varepsilon > 0$ und ein n_0 mit

$$|x_n| \geq \varepsilon$$

für alle $n \geq n_0$. Definiere

$$y_n := \begin{cases} 0 & \text{für } n < n_0 \\ \dfrac{1}{x_n} & \text{für } n \geq n_0 \end{cases}$$

Wegen

$$|y_n - y_m| = \left| \frac{1}{x_n} - \frac{1}{x_m} \right| = \left| \frac{x_m - x_n}{x_n x_m} \right| \leq \frac{1}{\varepsilon^2} |x_m - x_n|$$

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

$$\big((x_n) + \mathfrak{N}\big)\big((y_n) + \mathfrak{N}\big) = (x_n y_n) + \mathfrak{N} = (0, 0, \ldots, 0, 1, 1, \ldots) + \mathfrak{N} = (1, 1, \ldots) + \mathfrak{N}$$

ist $(y_n) + \mathfrak{N}$ das Inverse von $(x_n) + \mathfrak{N}$.

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

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

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

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

für alle $x \in \hat{K}$.
(a) $|\ |_{\hat{K}}$ ist wohldefiniert:
Sei $(x_n) + \mathfrak{N} = (x'_n) + \mathfrak{N}$. Dann ist $(x_n - x'_n)$ eine Nullfolge. Wegen

$$|x'_n| \leq |x_n| + |x'_n - x_n| \quad \text{und} \quad |x_n| \leq |x'_n| + |x_n - x'_n|$$

für alle $n \in \mathbb{N}$ ist

$$\lim |x_n| = \lim |x'_n| .$$

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

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

daß (x_n) eine Nullfolge, also $x = (x_n) + \mathfrak{N} = 0$ ist. Umgekehrt impliziert $x = (x_n) + \mathfrak{N} = 0$ 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

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

φ ist ein injektiver Homomorphismus und wegen

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

auch werterhaltend.
4.) $\varphi(K)$ liegt dicht in $\hat{K}$:
Sei $\varepsilon > 0$ und $x = (x_n) + \mathfrak{N} \in \hat{K}$. 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 $y = (x_{n_0}) + \mathfrak{N} = \varphi(x_{n_0}) \in \varphi(K)$

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

Also liegt $\varphi(K)$ dicht in $\hat{K}$.
5.) $\hat{K}$ ist vollständig:
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 $y_n \in K$ mit

$$(*) \qquad |x_n - \varphi(y_n)|_{\hat{K}} < \frac{1}{n} .$$

Wegen

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

für alle $n, m \in \mathbb{N}$ ist (y_n) eine Cauchy-Folge in K. Setzt man nun

$$y := (y_n) + \mathfrak{N} \in \hat{K}$$

so ist $(x_n - y)$ wegen $(*)$ eine Nullfolge in $\hat{K}$. Also konvergiert (x_n) in $\hat{K}$, und es ist

$$\lim x_n = y\,.$$

Also konvergiert in $\hat{K}$ jede Cauchy-Folge.
6.) Identifiziert man nun noch $x \in K$ mit $\varphi(x) \in \hat{K}$, so ist $\hat{K}$ eine Komplettierung von K. □

Ergänzungen

(1) Jedes $x \in \hat{K}$ ist darstellbar als Grenzwert einer Cauchy-Folge in K.

BEWEIS. Sei $x \in \hat{K}$. Da K dicht in $\hat{K}$ liegt, gibt es zu jedem $n \in \mathbb{N}$ ein $x_n \in K$ mit

$$|x - x_n| < \frac{1}{n}\,.$$

Also ist $x = \lim x_n$ und (x_n) eine Cauchy-Folge in K. □

BEMERKUNG. Diese Darstellung ist nicht eindeutig. Ist nämlich

$$x = \lim x_n$$

und (y_n) eine Nullfolge, so gilt auch

$$x = \lim x_n = \lim x_n + \lim y_n = \lim(x_n + y_n)\,.$$

BEISPIEL. Der Dezimaldarstellung von $\sqrt{2} = 1,4141\ldots$ entspricht die Cauchy-Folge

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

Die Kettenbruchentwicklung

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

liefert ebenfalls eine gegen $\sqrt{2}$ konvergierende Cauchy-Folge

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

(2) Ist K vollständig, so ist $K = \hat{K}$.

BEWEIS. Sei $x \in \hat{K}$, etwa $x = \lim x_n$, wobei (x_n) eine Cauchy-Folge in K ist. Weil K vollständig ist, besitzt (x_n) einen Grenzwert in K. Wegen der Eindeutigkeit des Grenzelementes ist dieser gleich x. Es folgt $K \subseteq \hat{K} \subseteq K$ und damit $K = \hat{K}$. □

DEFINITION 2.6. 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 2.2. *$\hat{K}_1$ 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

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

$\big(f(x)\big)$ 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 $\big(f(x_n)\big)$ 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 $\big(f(x_n)\big)$ 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 $\big(f(x_n) - f(x'_n)\big)$ 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,

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

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 2.1. *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

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

sind werterhaltende Homomorphismen. Nach Satz 2.2 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

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

Entsprechend folgt

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

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

2. Quadratische Gleichungen

Nicht in jedem Körper ist eine quadratische Gleichung

$$(*) \qquad t^2 + bt + c = 0$$

lösbar. So ist etwa $(*)$ für $K = \mathbb{R}$ nur unter der Bedingung

$$b^2 \geq 4c$$

lösbar. Allgemein gilt für die Lösbarkeit solcher Gleichungen

SATZ 2.3. *Sei K vollständig und*

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

mit $b, c \in K$. Gilt $|b|^2 > 4|c|$, so besitzt f eine Nullstelle in K.

BEWEIS. Sei zunächst

$$f(t) = t^2 - t - a$$

mit $a \in K$ und $4|a| < 1$. Definiere induktiv

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

(a) Es ist $|x_n| \geq \frac{1}{2}$: Dies gilt für $n = 0$. Sei nun $|x_n| \geq \frac{1}{2}$ bereits gezeigt. Dann ist

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

(b) (x_n) ist eine Cauchy-Folge: Für $n \in \mathbb{N}$ ist

$$|x_n - x_{n+1}| = |a| \left|\frac{1}{x_{n-1}} - \frac{1}{x_n}\right| = \frac{|a|\,|x_n - x_{n-1}|}{|x_{n-1}|\,|x_n|} \leq 4\,|a|\,|x_n - x_{n-1}|$$

$$\leq (4\,|a|)^n\,|x_1 - x_0| = |a|\,(4\,|a|)^n\,.$$

Hieraus folgt für $n, m \in \mathbb{N}$

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

$$\leq \sum_{i=0}^{m-1}|a|\,(4\,|a|)^{n+i} \leq |a|\,(4\,|a|)^n \cdot \sum_{i=0}^{\infty}(4\,|a|)^i = \frac{|a|\,(4\,|a|)^n}{1 - 4\,|a|}\,.$$

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

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

Für alle $n \in \mathbb{N}$ gilt

$$0 = x_n x_{n+1} - x_n - a\,,$$

also folgt

$$0 = \lim(x_n x_{n+1} - x_n - a) = \lim x_n \cdot \lim x_{n+1} - \lim x_n - a = x^2 - x - a\,,$$

d.h. x ist eine Nullstelle von f.

Für den allgemeinen Fall

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

gilt

$$f(-bt) = b^2\,\left(t^2 - t + \frac{c}{b^2}\right)\,.$$

Wegen $4\,|c| < |b|^2$, also $4\left|\frac{-c}{b^2}\right| < 1$, besitzt

$$t^2 - t + \frac{c}{b^2}$$

nach den vorangegangenen Betrachtungen eine Nullstelle in K und damit auch f. □

KAPITEL 3

Endliche Erweiterungen vollständiger Körper

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

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

der Erweiterungsgrad. Ist $[E : K] = n < \infty$, so heißt E endliche 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 3.1. 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

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

Es gilt

$$\vartheta^2 + b\vartheta + c = 0 \,,$$

also

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

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 $N(1 + \vartheta) = 1 - b + c$.
Ist speziell $E = \mathbb{C} = \mathbb{R}(i)$, $\operatorname{Irr}(i, \mathbb{R}) = t^2 + 1$, so erhält man für $x + iy \in \mathbb{C}$

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

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 $a = 0$. □

SATZ 3.1. *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

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

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

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

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 2.3. Es folgt

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

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 3.2. 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.

BEISPIEL. 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 läßt 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*

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

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

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

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

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

so wird

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

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

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

SATZ 3.2. *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*

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

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

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

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

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

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 $\dim V = n \geq 1$ 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 $u = \sum_{i=1}^{n} a_i v_i \in V$

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

Man kann also

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

setzen. Definiere nun

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

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 3.3. *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 3.2 vollständig.

Seien nun $|\ |_1$ und $|\ |_2$ Fortsetzungen von $|\ |_K$. Nach Satz 3.2 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. □

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.

KAPITEL 4

Archimedische Bewertungen

LEMMA 4.1. *K sei ein Körper, und die Abbildung*

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

sei multiplikativ (d.h. $\varphi(xy) = \varphi(x) \cdot \varphi(y)$ 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) *$\varphi(x+y) \leq 2 \max\big(\varphi(x), \varphi(y)\big)$ für alle $x, y \in K$.*

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

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

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

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

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

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

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

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

Also gilt $(*)$.
Insbesondere gilt dann

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

[†] Es ist entweder $\varphi(0) = 0$ oder $\varphi \equiv 1$

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

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

also

$$\varphi(x+y) \leq \sqrt[n]{4\,(n+1)}\cdot\left(\varphi(x)+\varphi(y)\right).$$

Durch Grenzwertbildung $n \to \infty$ folgt

$$\varphi(x+y) \leq \varphi(x)+\varphi(y). \quad \square$$

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: $\mathbb{C} \subsetneqq E$: 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

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

folgt

$$|z| - |a| \leq \varrho + 1,$$

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 $z \in \mathfrak{U}_\varrho(z') = \{z \in \mathbb{C} \mid |z - z'| < \varrho\}$. Dann ist für alle $n \in \mathbb{N}$

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

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

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

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 $z \in \mathfrak{U}_\varrho(z')$. Damit ist $\mathfrak{U}_\varrho(z') \subseteq B$, 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 $\mathbb{C} = B \subseteq \mathfrak{U}_{|a|+\varrho+1}(0)$. Dies ist ein Widerspruch. Also ist $\mathbb{C} = E$. □

Satz 4.1. (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 1.3 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 $x, y \in K$

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

also

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

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

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

oder

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

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

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

ein werterhaltender Homomorphismus, der sich nach Satz 2.2 zu einem werterhaltenden Homomorphismus

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

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 3.1 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 3.3) 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 $\tilde{\jmath}(\mathbb{C}) = E$ nach Lemma 4.2, also

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

Weil der Erweiterungsgrad 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 4.1. *Jeder archimedisch bewertete Körper K läßt sich als Unterkörper der komplexen Zahlen auffassen. Seine Bewertung ist dabei äquivalent zum gewöhnlichen Absolutbetrag.*

BEWEIS. Nach Satz 4.1 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.

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

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

ein Monomorphismus, so gilt

$$f(a) = a$$

und

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

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).

3.) Es sei $K=\mathbb{Q}(\vartheta)$ und $\mathrm{Irr}\,(\vartheta,\mathbb{Q}) = t^3-2$. Dann gibt es drei Monomorphismen mit

$$f_1(\vartheta) = \sqrt[3]{2}\,, \quad f_2(\vartheta) = \varepsilon\sqrt[3]{2}\,, \quad \text{und} \quad f_3(\vartheta) = \varepsilon^2\sqrt[3]{2}\,,$$

wobei ε dritte Einheitswurzel mit $\varepsilon^2+\varepsilon+1=0$ ist. Man erhält für $a,b,c\in\mathbb{Q}$

$$|a+b\vartheta+c\vartheta^2|_1 = |a+b\sqrt[3]{2}+c\sqrt[3]{4}|_\infty$$

$$\begin{aligned}
|a+b\vartheta+c\vartheta^2|_2 &= |a+b\varepsilon\sqrt[3]{2}+c\varepsilon^2\sqrt[3]{4}|_\infty \\
&= \left((a+b\varepsilon\sqrt[3]{2}+c\varepsilon^2\sqrt[3]{4})(a+b\varepsilon^2\sqrt[3]{2}+c\varepsilon\sqrt[3]{4})\right)^{1/2} \\
&= \left(a^2+2bc(\varepsilon^2+\varepsilon)+\left(2c^2+ab(\varepsilon^2+\varepsilon)\right)\sqrt[3]{2}+\left(b^2+ac(\varepsilon^2+\varepsilon)\right)\sqrt[3]{4}\right)^{1/2} \\
&= \left(a^2-2bc+(2c^2-ab)\sqrt[3]{2}+(b^2-ac)\sqrt[3]{4}\right)^{1/2}
\end{aligned}$$

und

$$\begin{aligned}
|a+b\vartheta+c\vartheta^2|_3 &= |a+b\varepsilon^2\sqrt[3]{2}+c\varepsilon\sqrt[3]{4}|_\infty \\
&= \left((a+b\varepsilon^2\sqrt[3]{2}+c\varepsilon\sqrt[3]{4})\,(a+b\varepsilon\sqrt[3]{2}+c\varepsilon^2\sqrt[3]{4}\right)^{1/2} \\
&= |a+b\vartheta+c\vartheta^2|_2\,.
\end{aligned}$$

Man erkennt, daß konjugiert komplexe Nullstellen stets zur gleichen Bewertung führen.

KAPITEL 5

Die p-adischen Zahlen

1. Allgemeine Eigenschaften

LEMMA 5.1. *Es sei K ein nicht-archimedisch bewerteter Körper. Dann gilt*

(A) $B := \{x \in K \mid |x| \leq 1\}$ *ist ein Teilring von K.*
(B) *Die Einheiten von B, d.h. die in B invertierbaren Elemente, sind genau die $x \in B$ mit $|x| = 1$.*
(C) $M := \{x \in K \mid |x| < 1\}$ *ist ein Ideal in B.*
(D) *Ist I ein Ideal von B und $I \not\subseteq M$, so ist $I = B$.*

BEWEIS. (A) Seien $x, y \in B$. Dann 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.

(B) (a) Ist $x \in B$ mit $|x| = 1$, so ist $|x^{-1}| = 1$, also $x^{-1} \in B$, d.h. x ist eine Einheit von B.

(b) Sei nun x eine Einheit von B, also $|x| \leq 1$ und $|x^{-1}| \leq 1$. Wäre $|x| < 1$, so ergäbe sich wegen $1 = |x|\,|x^{-1}| < 1$ ein Widerspruch. Also ist $|x| = 1$.

(C) Für $x, y \in M$ gilt

$$|x - y| \leq \max(|x|, |y|) < 1\,,$$

also ist $x - y \in M$. Für $x \in M$ und $y \in B$ folgt

$$|xy| = |x|\,|y| \leq |x| < 1\,.$$

Daher ist $xy \in M$. Wegen $0 \in M$ ist $M \neq \emptyset$. Also ist M ein Ideal in B.

(D) Wegen $I \not\subseteq M$ gibt es ein $x \in I$ mit $|x| = 1$. Nach (B) ist x eine Einheit in B, also folgt für alle $y \in B$:

$$y = (yx^{-1})\,x \in I\,.$$

Damit ist $I = B$. □

FOLGERUNG 5.1. *Jedes echte Ideal von B ist in M enthalten. Damit ist M das einzige maximale Ideal von B.*

DEFINITION 5.1. $B = \{x \in K \mid |x| \leq 1\}$ heißt der zur Bewertung gehörige *Bewertungsring*.

DEFINITION 5.2. $\bar{K} = B/M$ heißt *Restklassenkörper*.

BEISPIEL. 1.) Sei $K = \mathbb{Q}$ p-adisch bewertet. Dann ist der Restklassenkörper der Primkörper $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

BEWEIS. Für $0 \neq x \in \mathbb{Q}$ ist

$$|x|_p = \left|p^r \frac{u}{v}\right|_p = \frac{1}{p^r},$$

wobei $u \in \mathbb{Z}$ und $v \in \mathbb{N}$ teilerfremd zu p sind. Daher ist

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

und

$$M = \left\{x = p\frac{u}{v} \;\middle|\; u \in \mathbb{Z},\ v \in \mathbb{N},\ (v,p) = 1\right\} = p \cdot B\,.$$

Es sei

$$f : B \to B/M$$

die kanonische Abbildung und

$$f_{|\mathbb{Z}} : \mathbb{Z} \to B/M$$

ihre Restriktion auf $\mathbb{Z}$. $f_{|\mathbb{Z}}$ ist surjektiv: Sei $x = \frac{u}{v} \in B$ mit $u \in \mathbb{Z}$, $v \in \mathbb{N}$ und $(v,p) = 1$. Dann ist $u = vn + pm$ mit $m, n \in \mathbb{Z}$, also

$$x = \frac{u}{v} = n + p\frac{m}{v}\,.$$

Damit ist $f(x) = f(n)$. Damit hat jedes $f(x) \in B/M$ ein Urbild in $\mathbb{Z}$. Wegen $\operatorname{Kern} f_{|\mathbb{Z}} = M \cap \mathbb{Z} = p \cdot \mathbb{Z}$ ist

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \cong B/M$$

nach dem Homomorphiesatz. □

2.) 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 $\bar{L} = K$.

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

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

der Restklassenhomomorphismus und

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

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

$$\bar{L} \cong K$$

nach dem Homomorphiesatz. □

DEFINITION 5.3. Die Menge $G := \{|x| \mid x \in K^\times\}$ heißt *Wertegruppe* der Bewertung.

G ist eine Untergruppe von $\{a \in \mathbb{R} \mid a > 0\}$, denn es ist $1 = |1| \in G$, und für $a = |x|, b = |y| \in G$ ist auch $ab^{-1} = |xy^{-1}| \in G$.

BEISPIEL. 1.) Ist $\mathbb{Q}$ p-adisch bewertet, so ist

$$G = \left\{ \frac{1}{p^n} \mid n \in \mathbb{Z} \right\}$$

eine zyklische Gruppe.

2.) Für den gewöhnlichen Absolutbetrag auf $\mathbb{Q}$ ist

$$G = \{q \in \mathbb{Q} \mid q > 0\} .$$

3.) Die Wertegruppe der trivialen Bewertung ist $G = \{1\}$.

SATZ 5.1. *Ist K nicht-archimedisch bewertet, so stimmt die Wertegruppe G von K mit der Wertegruppe $\hat{G}$ der Komplettierung $\hat{K}$ überein.*

BEWEIS. Wegen $K \subseteq \hat{K}$ ist $G \subseteq \hat{G}$. Sei $|\hat{x}| \in \hat{G}$ mit $\hat{x} \in \hat{K}^\times$. Weil K dicht in $\hat{K}$ liegt, gibt es dann ein $x \in K$ mit

$$|\hat{x} - x| < |\hat{x}| .$$

Es folgt

$$|x| = |\hat{x} + (x - \hat{x})| = \max(|\hat{x}|, |x - \hat{x}|)^\dagger = |\hat{x}| ,$$

also $|\hat{x}| \in G$. Damit ist $G = \hat{G}$. □

DEFINITION 5.4. Eine Bewertung heißt *diskret*, wenn zu jedem Element der Wertegruppe G eine Umgebung existiert, die kein weiteres Element aus G enthält.

---

†Nach dem Dominanzprinzip

SATZ 5.2. *Eine reelle Bewertung ist genau dann diskret, wenn die Wertegruppe G zyklisch ist.*

BEWEIS. Ist die Bewertung trivial, so ist $G = \{1\}$ zyklisch und diskrekt. Sei also die Bewertung nicht-trivial.

1.) Sei G zyklisch, etwa $G = \{d^n \mid n \in \mathbb{Z}\}$ mit $d \in \mathbb{R}$. Weil die Bewertung nicht-trivial ist, ist $d \neq 1$. Dann liegt in den offenen Intervall (d^{n+1}, d^{n-1}) außer d^n $(n \in \mathbb{Z})$ kein weiteres Element aus G, also ist die Bewertung diskret.

2.) Die Bewertung sei diskret. Ist

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

so ist $S \neq \emptyset$, denn die Bewertung ist nicht-trivial, und für $x \in K$ mit $|x| > 1$ ist $1 > |x^{-1}| \in G$. Sei d das Supremum von S. Dann gilt:

(a) $d < 1$: Weil $1 \in G$ und G diskret ist, gibt es ein offenes Intervall (b_0, b_1) mit $b_0 < 1 < b_1$, das außer 1 kein weiteres Element aus G enthält. Dann ist $a \leq b_0$ für alle $a \in S$, also auch $d \leq b_0 < 1$.

(b) Es gibt kein $a \in G$ mit $d < a < 1$.

(c) Es ist $d \in G$: Wegen $d = \sup S < 1$ gibt es ein $a \in G$ mit

$$d^2 < a \leq d.$$

Wäre $a < d$, so gäbe es noch ein $b \in S$ mit

$$d^2 < a < b \leq d.$$

Es folgt

$$d = \frac{d^2}{d} < \frac{a}{b} < 1,$$

also ein Widerspruch zu (b) wegen $\frac{a}{b} \in G$. Also ist $d = a \in G$.

Sei nun $a \in G$ beliebig. Dann gibt es ein $n \in \mathbb{Z}$ mit

$$d^{n+1} < a \leq d^n,$$

also

$$d < \frac{a}{d^n} \leq 1.$$

Wegen (b) ist $\frac{a}{d^n} = 1$, also $a = d^n$. Damit ist $G = \{d^n \mid n \in \mathbb{Z}\}$ zyklisch. □

DEFINITION 5.5. Sei K diskret bewertet und $G = \{d^n \mid n \in \mathbb{Z}\}$ die Wertegruppe mit $d < 1$. Ein Element $p \in K$ heißt *Primelement*, wenn $|p| = d$ ist.

DEFINITION 5.6. Sei K nicht-archimedisch bewertet und $f : B \to \bar{K} = B/M$ der Restklassenhomomorphismus. Eine Teilmenge R von B heißt ein *Repräsentantensystem*, wenn zu jedem $\bar{x} \in \bar{K}$ genau ein $x \in R$ mit $f(x) = \bar{x}$ existiert. Es seien stets 0 und 1 in R enthalten.

BEISPIEL. Sei $K = \mathbb{Q}$ p-adisch bewertet. Es ist

$$G = \left\{\frac{1}{p^n} \mid n \in \mathbb{Z}\right\}.$$

Wegen $|p|_p = \frac{1}{p}$ ist p Primelement der Bewertung. Ist $e \in \mathbb{Q}$ mit $|e|_p = 1$, so ist auch $p \cdot e$ ein Primelement.
Ein Repräsentantensystem ist

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

Es ist

$$B = \left\{ \frac{u}{v} \mid u \in \mathbb{Z},\ v \in \mathbb{N},\ (v,p) = 1 \right\} \quad \text{und} \quad f : B \to \mathbb{Z}_p\,.$$

Für $\frac{u}{v} \in B$ ist wegen $(v,p) = 1$

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

Man kann $0 \leq n < p$ annehmen, weil andernfalls mit $n = kp + n'$, $k \in \mathbb{Z}$, $0 \leq n' < p$

$$u = n'v + (kv + m)\,p$$

eine solche Darstellung wäre. Wegen

$$\frac{u}{v} = n + p\,\frac{m}{v}$$

folgt hieraus $f\left(\frac{u}{v}\right) = f(n) + \bar{0} = f(n)$.

Satz 5.3. *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 5.1 stimmen die Wertegruppen von K und $\hat{K}$ überein, und nach Satz 5.2 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 f der Restklassenhomomorphismus, so gibt es ein $a_0 \in R$ mit $f(e) = f(a_0)$. Wegen $|e| = 1$ ist $f(a_0) = f(e) \neq 0$, also $a_0 \neq 0$. Setze

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

Hierfür gilt dann $(*)$

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

denn wegen $f(e - a_0) = \bar{0}$ ist $|e - a_0| < 1$, und nach dem Beweis zu Satz 5.2 ist $|p| = d = \sup\{b \in G \mid b < 1\}$.

Seien nun $a_0, \ldots, a_k \in R$ und damit $x_0, \ldots, x_k$ bereits bestimmt, so daß $(*)$ gilt. Aus

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

folgt

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

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

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

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

Unter Benutzung der Bezeichnungen von Satz 5.3 schreibt man abkürzend

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

und nennt dies die kanonische Darstellung von x.

KOROLLAR 5.1. *$\hat{K}$ sei die Komplettierung des diskret bewerteten Körpers K. Dann ist*

$$\hat{K} = \left\{ \sum\nolimits_{n=n_0}^{\infty} a_n p^n \,\middle|\, a_n \in R,\, n_0 \in \mathbb{Z} \right\}\,.$$

Hierbei ist die Darstellung der Elemente von $\hat{K}$ bei fest gewähltem Primelement p und Repräsentantensystem R eindeutig.

BEWEIS. Seien $a_n \in R$ beliebig gewählt, so daß nur $a_n = 0$ für $n \leq n_0$ ist. Die Elemente

$$s_k = \sum_{n=n_0}^{k} a_n p^n \qquad (n_0 \leq k \in \mathbb{Z})$$

bilden wegen

$$|s_k - s_{k'}| = \left| \sum_{n=k+1}^{k'} a_n p^n \right| \leq \max_{k+1 \leq n \leq k'} \left(|a_n|\, |p|^n \right) \leq \max_{k+1 \leq n \leq k'} \left(|p|^n \right) = |p|^{k+1}$$

eine Cauchy-Folge in K und konvergieren daher in $\hat{K}$. Also ist

$$\left\{ \sum\nolimits_{n=n_0}^{\infty} a_n p^n \,\middle|\, a_n \in R,\, n_0 \in \mathbb{Z} \right\} \subseteq \hat{K}\,.$$

Nach Satz 5.3 folgt dann die Gleichheit.

Eindeutigkeit: Sei

$$x = \sum_{n=n_0}^{\infty} a_n p^n = s_k + p^{k+1} \cdot u$$

und

$$y = \sum_{n=n_1}^{\infty} b_n p^n = s'_k + p^{k+1} \cdot v$$

mit $|u|, |v| \leq 1$, wobei durch Nullauffüllung $n_0 = n_1$ angenommen werden kann. Es sei $a_k \neq b_k$ und $a_n = b_n$ für $n_0 \leq n < k$. Wegen $a_k, b_k \in B$ ist $|a_k - b_k| \leq 1$. Wäre $|a_k - b_k| < 1$, also $a_k - b_k \in M$, so würde

$$f(a_k) = f\big(b_k + (a_k - b_k)\big) = f(b_k)$$

im Widerspruch zur Definition von R folgen. Also ist $|a_k - b_k| = 1$ und damit

$$|x - y| = |(a_k - b_k)\, p^k + (u - v)\, p^{k+1}| = \max\left(|p|^k, |u - v|\, |p|^{k+1}\right) = |p|^k .$$

Aus $x = y$ folgt daher $a_n = b_n$ für alle $n \geq n_0$. □

Spezialfall. Sei $\mathbb{Q}_p$ die Komplettierung von $\mathbb{Q}$ bezüglich einer p-adischen Bewertung. Dann ist

$$\mathbb{Q}_p = \left\{ \sum\nolimits_{n=n_0}^{\infty} a_n p^n \;\middle|\; a_n \in \mathbb{Z},\ 0 \leq a_n < p,\ n_0 \in \mathbb{Z} \right\} .$$

$\mathbb{Q}_p$ heißt Körper der p-adischen Zahlen oder nach Hensel (1897) Henselscher Körper.

Behauptung. $\mathbb{Q}_p$ ist überabzählbar.

Beweis. Der Beweis erfolgt mit den Cantorschen Diagonalverfahren. Angenommen, es gibt eine Abzählung

$$\begin{aligned} x_1 &= a_{n_1 1} p^{n_1} + \cdots + a_{01} p^0 + \sum_{i=1}^{\infty} a_{i1} p^i \\ x_2 &= a_{n_2 2} p^{n_2} + \cdots + a_{02} p^0 + \sum_{i=1}^{\infty} a_{i2} p^i \\ &\vdots \qquad\qquad\qquad\quad \vdots \end{aligned}$$

Betrachte nun

$$x = \sum_{i=1}^{\infty} b_i p^i$$

mit $b_i \neq a_{ii}$, $b_i \in R$. x tritt in der Aufzählung nicht auf. Also ist die Annahme falsch, d.h. $\mathbb{Q}_p$ ist überabzählbar. □

Rechnen in $\mathbb{Q}_p$

Man schreibt abkürzend

$$a_{n_0}\dots a_0, a_1a_2\dots \qquad \text{für} \qquad \sum_{n=n_0} a_n p^n = a_{n_0}p^{n_0} + \cdots + a_0p^0 + a_1p^1 + \cdots ,$$

wobei $a_n \in R$ für $n \geq n_0$ ist. Hier sei $R = \{0, 1, \dots, p-1\}$ gewählt.

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 $0 \leq a_i < 7$.

$$\begin{array}{rcccccccc} & & 5, & 4 & 3 & 2 & 6 & \cdots \\ + & 1 & 5, & {}_1 3 & {}_1 2 & 5 & {}_1 6 & \cdots \\ \hline & 1 & 3, & 1 & 6 & 0 & 6 & \cdots \end{array}$$

2. Subtraktion: Das Negative von $x = a_{n_0}\dots a_0, a_1\dots$ mit $a_{n_0} \neq 0$ ist $-x = b_{n_0}\dots b_0, b_1\dots$ 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 $x = 5,4326\dots$. Dann ist $-x = 2,2340\dots$, denn

$$\begin{array}{rrcccccc} & x = & 5, & 4 & 3 & 2 & 6 & \cdots \\ + & -x = & 2, & {}_1 2 & {}_1 3 & {}_1 4 & {}_1 0 & \cdots \\ \hline & & 0, & 0 & 0 & 0 & 0 & \cdots \end{array}$$

3. Multiplikation: Man führt die Multiplikation formal aus

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

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 $p = 7$.

	1	1,	4	1	3	$\cdots$	$\cdot$	2	1,	5	4	2	$\cdots$
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	$\cdots$							
2	3	0,	3	0	3	$\cdots$							

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 5.4. *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

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

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

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 $0 \le z < p^m$.
Dann ist $0 \le y < p^t$: Es ist $b \le yp^m$. Wäre $y < 0$, so würde $b \le -p^m$ im Widerspruch zu $(*)$ folgen. Weiter ist

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

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

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

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

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

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. □

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

$$x = 41,\overline{31} = \frac{4}{5} + 1 + \frac{5\cdot(3+5)}{1-25} = \frac{4}{5} + 1 - \frac{20}{12} = \frac{48+60-100}{60} = \frac{2}{15}$$

(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 $y = 8 = 3 + 1\cdot 5$. Man erhält

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

Nullstellen von Polynomen

Sei

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

ein Polynom über K. Definiere formal die Ableitung

$$f'(t) := n a_n t^{n-1} + (n-1) a_{n-1} t^{n-2} + \cdots + a_1 \,.$$

SATZ 5.5. (*Newtonsches Verfahren*) *Es sei K vollständig bezüglich einer nichtarchimedischen Bewertung und $f(t)$ ein Polynom mit Koeffizienten aus dem Bewertungsring B. Existiert ein $x_1 \in B$ mit*

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

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

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

BEWEIS. Definiere 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) $|f'(x_1)| = |f'(x_2)| = \cdots = |f'(x_n)| \leq 1$

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

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 $n \in \mathbb{N}$

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

also

$(*)$

$$|x_{n+m} - x_n| = \left|\sum_{i=0}^{m-1}(x_{n+i+1} - x_{n+i})\right| \leq \max_{0\leq i\leq m-1}(|x_{n+i+1} - x_{n+i}|) \leq d^{2^{n-1}}|f'(x_1)|$$

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

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

also folgt für $x := \lim x_n$

$$f(x) = 0$$

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

$$|x - x_1| \leq d\,|f'(x_n)| = \frac{|f(x_1)|}{|f'(x_1)|}\,. \quad \square$$

Bemerkung. Bei der Iteration

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

ist

$$|x - x_n| \leq \frac{|f(x_n)|}{|f'(x_n)|} \qquad (n \in \mathbb{N}) .$$

BEISPIEL. Es sei $K = \mathbb{Q}_5$ und $f(t) = t^2 + 1$. Für $x_1 = 2$ ist

$$|f(2)|_5 = |5|_5 = \frac{1}{5} < 1 = |4|_5^2 = |f'(2)|_5^2 ,$$

also existiert eine Nullstelle. Mit dem Startwert $x_1 = 2$ ergibt sich

$$\begin{aligned} x_2 &= x_1 - \frac{x_1^2 + 1}{2x_1} = 2 - \frac{5}{4} = \frac{3}{4} \\ x_3 &= \frac{3}{4} - \frac{5^2}{24} = -\frac{7}{24} \\ x_4 &= -\frac{7}{24} + \frac{54}{336} = \frac{527}{336} \end{aligned}$$

Für den Fehler gilt nach der obigen Formel

$$|x - x_4|_5 \leq \left| \frac{f(x_4)}{f'(x_4)} \right|_5 = \left| \frac{\left(\frac{527}{336}\right)^2 + 1}{2 \cdot \frac{527}{336}} \right|_5 = \left| \frac{5^8}{2^5 \cdot 3 \cdot 7 \cdot 17 \cdot 31} \right|_5 = \left(\frac{1}{5}\right)^8 .$$

Dies zeigt das gute Konvergenzverhalten der Iteration.

ANWENDUNG. Das Polynom $f(t) = t^{p-1} - 1$ zerfällt in $\mathbb{Q}_p$ in $p - 1$ verschiedene Linearfaktoren.

BEWEIS. Setze $x_1 = n$ mit $1 \leq n < p$. Wegen

$$n^{p-1} \equiv 1 \bmod p \qquad \text{(Fermatscher Satz)}$$

ist

$$|f(n)|_p < |(p-1)\, n^{p-2}|_p^2 = 1 .$$

Nach Satz 5.5 gibt es zu jedem n mit $1 \leq n < p$ eine Nullstelle $x(n)$ von $f(t)$ mit

$$|x(n) - n|_p \leq \frac{|f(n)|}{|f'(n)|} < 1 .$$

Man erhält somit $p - 1$ Nullstellen

$$x(1), \ldots, x(p-1) .$$

Sie sind alle verschieden: Aus $x = x(n) = x(k)$ und

$$|x - n|_p < 1 \qquad \text{bzw.} \qquad |x - k|_p < 1$$

folgt

$$|n - k|_p = |(n - x) + (x - k)|_p \leq \max\left(|x - n|_p, |x - k|_p\right) < 1 .$$

Wegen $1 \leq n, k < p$ ist $-p < n - k < p$, also $n = k$, weil $n - k$ den Teiler p besitzt. □

2. Quadrate in $\mathbb{Q}_p$

SATZ 5.6. *Ein Element $x = p^n a$, $n \in \mathbb{Z}$, mit $|a|_p = 1$ ist genau dann ein Quadrat in $\mathbb{Q}_p$, wenn n gerade und a ein Quadrat ist.*

BEWEIS. 1.) Ist $n = 2k$ und $a = b^2$, so folgt $x = \left(p^k \cdot b\right)^2$.
2.) Sei nun $x = p^n a$ ein Quadrat, etwa $x = b^2$ mit $b = p^k c$ und $|c|_p = 1$. Dann ist

$$|p|_p^n = |x|_p = |b|_p^2 = |p|_p^{2k},$$

also $n = 2k$ und

$$a = b^2 p^{-2k} = \left(bp^{-k}\right)^2. \quad \square$$

Damit ist die Frage, wann x ein Quadrat in $\mathbb{Q}_p$ ist, zurückgeführt auf die Frage, wann a mit $|a|_p = 1$ ein Quadrat in $\mathbb{Q}_p$ ist.

SATZ 5.7. *Sei $p \neq 2$ und $a \in \mathbb{Q}_p$ mit $|a|_p = 1$. a ist genau dann ein Quadrat in $\mathbb{Q}_p$, wenn a beim Restklassenhomomorphismus*

$$\varphi : B \to B/M = \mathbb{Z}_p$$

auf ein Quadrat in $\mathbb{Z}_p$ abgebildet wird.

BEWEIS. 1.) Sei $a = b^2$. Wegen $1 = |a|_p = |b|_p^2$ ist $|b|_p = 1$ und $\varphi(a) = \varphi(b)^2$. Also ist $\varphi(a)$ ein Quadrat in $\mathbb{Z}_p$.
2.) Sei nun $\varphi(a) = \varphi(b)^2$ mit $|b|_p = 1$. Für $x_1 = b$ und $f(t) = t^2 - a$ ist

$$|f(b)|_p = |b^2 - a|_p < 1^\dagger = |2b|_p = |f'(b)|_p^2,$$

also besitzt f nach Satz 5.5 eine Nullstelle, also ist a ein Quadrat in $\mathbb{Q}_p$. $\square$

SATZ 5.8. *Sei $p = 2$ und $a \in \mathbb{Q}_2$ mit $|a|_2 = 1$. a ist genau dann ein Quadrat in $\mathbb{Q}_2$, wenn*

$$|a - 1|_2 \leq |2|_2^3$$

ist.

BEWEIS. 1.) Das Polynom $f(t) = t^2 - a$ besitzt nach Satz 5.5 wegen

$$|f(1)|_2 = |1 - a|_2 \leq |2|_2^3 < |2|_2^2 = |f'(1)|_2^2$$

eine Nullstelle, also ist a ein Quadrat in $\mathbb{Q}_2$.
2.) Sei nun $a = b^2$, $b \in \mathbb{Q}_2$. Dann ist wegen $1 = |a|_2 = |b|_2^2$ auch $|b|_2 = 1$. Ist φ der Restklassenhomomorphismus

$$\varphi : B = \{x \in \mathbb{Q}_2 \mid |x|_2 \leq 1\} \to \mathbb{Z}_2,$$

so ist $\varphi(b - 1) = 0$, also $b = 1 + 2c$ mit $|c|_2 \leq 1$. Dann ist

$$a - 1 = b^2 - 1 = (1 + 2c)^2 - 1 = 4\,(c + c^2).$$

---

†wegen $\varphi(b^2 - a) = 0$ ist $b^2 - a \in M$

Wegen

$$\varphi(c+c^2) = \varphi(c) + \varphi(c)^2 = 0^{\ddagger}\,,$$

also $|c+c^2|_2 < 1$, ist

$$|a-1|_2 = |4\,(c+c^2)|_2 = |4|_2\,|c+c^2|_2 \le |2|_2^3 \quad \square$$

ERGEBNIS. Quadrate in $\mathbb{Q}_2$: $\quad a = 2^{2k}\,(1 + a_3 2^3 + \cdots)$
Quadrate in $\mathbb{Q}_p$, $p \neq 2$: $\quad a = p^{2k}\,(a_0 + a_1 p + a_2^2 + \cdots)$,
wobei $\varphi(a_0)$ ein Quadrat in $\mathbb{Z}_p$ ist.

BEISPIEL. $a = 7^{2k}\,(a_0 + a_1 \cdot 7 + \cdots) \in \mathbb{Q}_7$ ist genau dann ein Quadrat, wenn a_0 ein quadratischer Rest modulo 7 ist, also $a_0 \in \{1, 2, 4\}$.

KOROLLAR 5.2. *Die p-adischen Körper $\mathbb{Q}_p$ lassen sich nicht anordnen.*

BEWEIS. Annahme: $\mathbb{Q}_p$ ist ein geordneter Körper. Dann ist

$$1 = 1^2 > 0\,, 2 = 1 + 1 > 0,\ 3 = 2 + 1 > 0,\ \ldots\,,$$

folglich ist $-n < 0$ für alle $n \in \mathbb{N}$, also $-n$ kein Quadrat in $\mathbb{Q}_p$. Es ist aber -7 ein Quadrat in $\mathbb{Q}_2$ nach Satz 5.8 und $1 - p$ ein Quadrat in $\mathbb{Q}_p$ für $p \neq 2$ nach Satz 5.7. Dies ist ein Widerspruch. $\square$

KOROLLAR 5.3. *Sind p und q verschiedene Primzahlen, so sind $\mathbb{Q}_p$ und $\mathbb{Q}_q$ nicht isomorph.*

BEWEIS. Annahme: Sei $f : \mathbb{Q}_p \to \mathbb{Q}_q$ ein Isomorphismus und $p < q$. Wegen $f(1) = 1$ ist dann $f(n) = n$ für alle $n \in \mathbb{Z}$. Aus $n = x^2$, $x \in \mathbb{Q}_p$ folgt

$$n = f(n) = f(x)^2\,.$$

Ist also n ein Quadrat in $\mathbb{Q}_p$, so ist n auch ein Quadrat in $\mathbb{Q}_q$.

1. Fall: $p, q \neq 2$: Wegen $(p, q) = 1$ ist

$$1 = ap + bq$$

mit $a, b \in \mathbb{Z}$ und $0 < b < p < q$. Wegen $\bar{1} - \overline{ap} = \bar{1}$ in $\mathbb{Z}_p$ ist $1 - ap$ nach Satz 5.7 ein Quadrat in $\mathbb{Q}_p$, also auch ein Quadrat in $\mathbb{Q}_q$. Es ist jedoch $1 - ap = bq$ kein Quadrat in $\mathbb{Q}_q$ nach Satz 5.6.

2. Fall: $p = 2$: $\mathbb{Q}_2$ ist nicht isomorph zu $\mathbb{Q}_3$, $\mathbb{Q}_5$ und $\mathbb{Q}_7$, denn:

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 $\mathbb{Q}_2$

Man kann also $q > 8$ voraussetzen. Sei

$$1 = a \cdot 8 + bq$$

mit $a, b \in \mathbb{Z}$ und $0 < b < 8 < q$. Dann ist $1 - 8a$ nach Satz 5.8 ein Quadrat in $\mathbb{Q}_2$, aber bq nach Satz 5.7 kein Quadrat in $\mathbb{Q}_q$.

Also sind $\mathbb{Q}_p$ und $\mathbb{Q}_q$ nicht isomorph. $\square$

‡in $\mathbb{Z}_2$ ist $x^2 = x$

KOROLLAR 5.4. *$\mathbb{R}$ ist zu keinem der Körper $\mathbb{Q}_p$ isomorph.*

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

$$a \sqsubseteq b \quad :\Longleftrightarrow \quad f(a) \leq f(b)$$

eine Anordnung auf $\mathbb{Q}_p$, was nach Korollar 5.2 nicht möglich ist. □

KAPITEL 6

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

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

ist.

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

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

primitiv.

HILFSSATZ 6.1. *Das Produkt primitiver Polynome ist wieder primitiv.*

BEWEIS. Sei

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

$j \in \{0, 1, \ldots, n\}$ 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

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

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 6.2. *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. Dann ist nach Hilfssatz 6.1

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

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

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

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

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

für alle $f(t) \in B[t]$.

Es gilt

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

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

SATZ 6.1. *Ist* $f(t) \in B[t]$ *und* $\bar{f}(t)$ *irreduzibel über* $\bar{K}$, $\operatorname{grad} f = \operatorname{grad} \bar{f}$, *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 6.2 g und h als primitiv annehmen. Also ist $\bar{f} = \bar{g} \cdot \bar{h}$ eine echte Zerlegung von $\bar{f}$, also ist $\bar{f}$ reduzibel, im Widerspruch zur Voraussetzung. $\square$

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

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

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

KOROLLAR 6.1. *Gibt es eine separable Erweiterung* $\bar{E}$ *über* $\bar{K}$, *mit* $[\bar{E} : \bar{K}] = n$, *so existiert auch eine Erweiterung* E *über* K *vom gleichen Grad* n.

BEWEIS. Weil $\bar{E}$ eine separable Erweiterung über $\bar{K}$ ist, ist $\bar{E} = \bar{K}(\vartheta)$ mit $\bar{f}(t) = \operatorname{Irr}(\vartheta, \bar{K}) = t^n + \bar{a}_{n-1} t^{n-1} + \cdots + \bar{a}_0$. Sei $f(t) = t^n + a_{n-1} t^{n-1} + \cdots + a_0$ ein Urbild von $\bar{f}$. Dann ist f irreduzibel, und $E = K(\vartheta)$ mit $\operatorname{Irr}(\vartheta, K) = f(t)$ hat den Grad n über K. $\square$

KOROLLAR 6.2. *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 $\mathbb{Z}_p$. $\square$

SATZ 6.2. (*Henselsches Lemma*) *Sei K vollständig bezüglich einer nicht-archimedischen Bewertung. Sei f ein primitives Polynom, für das $\bar{f} = \bar{g}_0\bar{h}_0$ in $\bar{K}[t]$ gilt. Sind $\bar{g}_0$ und $\bar{h}_0$ teilerfremd, so gibt es $g, h \in K[t]$ mit*

$$f = g \cdot h$$

und $\operatorname{grad} g = \operatorname{grad} \bar{g}_0$, $\bar{g} = \bar{g}_0$, $\bar{h} = \bar{h}_0$.

BEWEIS. Sei $\operatorname{grad} f = m$ und $k = \operatorname{grad} \bar{g}_0$. Seien g_0 und h_0 Urbilder von $\bar{g}_0$ und $\bar{h}_0$, jeweils vom gleichen Grad. Wegen

$$\operatorname{grad} \bar{g}_0 + \operatorname{grad} \bar{h}_0 = \operatorname{grad} \bar{f} \leq \operatorname{grad} f$$

ist dann

$$\operatorname{grad} h_0 = \operatorname{grad} \bar{h}_0 \leq m - k\,.$$

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

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

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

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

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

$$\begin{aligned} f &\equiv g_0h_0 \bmod \pi \\ 1 &\equiv g_0v_0 + h_0u_0 \bmod \pi\,, \end{aligned}$$

um anzudeuten, daß jeder Koeffizient von $f - g_0h_0$ und $1 - g_0v_0 - h_0u_0$ in B durch π teilbar ist. Wegen $\pi \in M$ ist $|\pi| < 1$. (Ist die Bewertung diskret, so kann für π 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) $f \equiv g_nh_n \bmod \pi^{n+1}$

(2) $g_{n+1} \equiv g_n \bmod \pi^{n+1}$, $h_{n+1} \equiv h_n \bmod \pi^{n+1}$ 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

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

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

$$f - g_nh_n = \pi^{n+1}p_n$$

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

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

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

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

ist. Aus

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

folgt durch Multiplikation mit p_n

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

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

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

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

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

Also ist

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

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

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

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

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 $\le m - k$. Damit ist auch $\operatorname{grad} h_{n+1} \le m - k$. Hiermit ist die Existenz der Folgen (g_n) und (h_n) mit den Eigenschaften (1) – (3) gezeigt.

Wir setzen

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

Wegen (2) ist

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

also

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

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

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

so folgt

$$g \equiv g_n \bmod \pi^{n+1}\,, \quad \bar{g} = \bar{g}_0 \quad \text{und} \quad \operatorname{grad} g = k\,.$$

Entsprechend erhält man ein Grenzpolynom h der Folge (h_n) mit

$$h \equiv h_n \bmod \pi^{n+1} \qquad \text{und} \qquad \operatorname{grad} h \leq m - k\,.$$

Wegen

$$f - gh = f - g_n h_n + g_n\,(h_n - h) + (g_n - g)\,h \equiv 0 \bmod \pi^{n+1}$$

für alle $n \in \mathbb{N}$ folgt $f = g \cdot h$. $\square$

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

$$\bar{f}(t) = t^2 + \bar{1} = (t + \bar{1})(t + \bar{1})\,.$$

2.) Ist $f(t) = t^3 + 3$, so ist

$$\bar{f}(t) = t^3 + \bar{1} = (t + \bar{1})(t^2 + t + \bar{1})\,,$$

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 $t^2 + t + \bar{1}$ irreduzibel ist.)

3.) Für

$$f(t) = t^5 + 3t^4 + 2t^2 + 1$$

ist

$$\bar{f}(t) = t^5 + t^4 + \bar{1} = (t^2 + t + \bar{1})(t^3 + t + \bar{1})\,.$$

Nach dem Henselschen Lemma ist $f(t)$ reduzibel.

Zwei Spezialfälle im Henselschen Lemma

1). Sei $\operatorname{grad} f = \operatorname{grad} \bar{f}$ und $\bar{f} = \bar{p}_1^{k_1} \cdot \ldots \cdot \bar{p}_r^{k_r}$ $(r, k_1, \ldots, k_r \in \mathbb{N})$ die Primfaktorzerlegung von $\bar{f}$ in $\bar{K}[t]$. Dann ist

$$f = f_1 \cdot \ldots \cdot f_r \qquad \text{mit} \qquad \bar{f}_i = \bar{p}_i^{k_i} \;\; (1 \leq i \leq r)\,.$$

Ist $k_i = 1$ $(1 \leq i \leq r)$, so ist f_i irreduzibel.

BEMERKUNG. 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

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

aber

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

2.) Sei $\operatorname{grad} \bar{f} = m < n = \operatorname{grad} f$. Dann ist $\bar{f} = \bar{f} \cdot \bar{1}$, 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 $\bar{f}(t) = t + \bar{1}$, also muß eine Zerlegung $f(t) = (t + a)(pt + b)$ mit $a, b \in \mathbb{Q}_2$ möglich sein.

KOROLLAR 6.3. *Ist K vollständig bezüglich einer nicht-archimedischen Bewertung, und ist*

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

irreduzibel über K, so gilt

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

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

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

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

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

möglich. Also ist

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

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

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

also

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

HILFSSATZ 6.3. *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 $Irr(a, K) = t^k + \cdots + a_0 \in K[t]$, 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

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

eine Basis von E über K:

a) $\mathfrak{B}$ 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) $\mathfrak{B}$ 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 $\mathfrak{B}$ über K. Außerdem folgt $n = r \cdot k$.

Ist $\{v_1, \ldots, v_n\}$ eine Basis von E über K und

$$a v_i = \sum_{i=1}^{n} a_{ij} v_j \qquad (i = 1, \ldots, r) \,,$$

so ist $N(a) = \det(a_{ij})$. Speziell für die Basis $\mathfrak{B}$ 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

$$A_1 = \cdots = A_r = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{k-1} \end{pmatrix}$$

Es folgt

$$N(a) = \det(a_{ij}) = (\det A_1)^r = \left((-1)^{k-1} \cdot a_0 \right)^r .$$

Damit ist

$$\sqrt[n]{|N(a)|_K} = \sqrt[k \cdot r]{|(-1)^{k-1} a_0|_K^r} = \sqrt[k]{|a_0|_K} \,. \quad \square$$

SATZ 6.3. (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* 3.3 *ist diese auch die einzige Fortsetzung.*)

BEWEIS. 1.) Ist K archimedisch bewertet, so ist $n \leq 2$ nach Satz 4.1. Die Behauptung folgt dann aus Satz 3.1.

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 3.1). 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

$$f(t) = \operatorname{Irr}(a, K) = t^k + a_{k-1}t^{k-1} + \cdots + a_0\,,$$

so folgt nach Hilfssatz 6.3

$$|a_0|_K = |a|_E^k \leq 1\,.$$

Da f irreduzibel ist, ist nach Korollar 6.3

$$|a_i|_K \leq \max\left(|a_0|_k, 1\right) \leq 1$$

für $i = 0, 1, \ldots, k-1$.
Das irreduzible Polynom von $1+a$ ist

$$\operatorname{Irr}(1+a, K) = f(t-1)$$

mit dem absoluten Glied

$$f(-1) = a_0 - a_1 + \cdots + (-1)^{k-1}a_{k-1} + (-1)^k\,,$$

also

$$|f(-1)|_K \leq \max_{0 \leq i < k}\left(|a_i|, 1\right) \leq 1\,.$$

Es folgt

$$|1+a|_E = \sqrt[k]{f(-1)|_K} \leq 1\,. \quad \square$$

KOROLLAR 6.4. *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

$$\mathit{Irr}\,(a, K) = t^k + a_{k-1}t^{k-1} + \cdots + a_0$$

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 3.3.

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. $\square$

KOROLLAR 6.5. *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 $\mathfrak{C}$ der algebraische Abschluß von $\hat{K}$. Die Bewertung von K läßt sich zu einer Bewertung von $\hat{K}$ und diese nach Korollar 6.4 zu einer Bewertung $|\ |_{\mathfrak{C}}$ fortsetzen (diese Fortsetzung ist sogar eindeutig). Da E algebraisch über K ist, gibt es eine Einbettung $\jmath : E \to \mathfrak{C}$, die auf K die Identität ist. Durch

$$|x|_E := |\jmath(x)|_{\mathfrak{C}} \qquad (x \in E)$$

wird dann eine Bewertungsfortsetzung auf E definiert. □

BEMERKUNG. Da es mehrere Einbettungen $\jmath : E \to \mathfrak{C}$ 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 $\mathfrak{C}$ von $\mathbb{Q}_p$ gilt

$$t^2 - 5 = (t - c)(t + c)$$

mit $c \in \mathfrak{C}$. Bei einer Einbettung

$$\jmath : \mathbb{Q}(\vartheta) \to \mathfrak{C}$$

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

$$|a + b\vartheta|_E = \sqrt{|a^2 - 5b^2|_p} \qquad \big(a + b\vartheta \in E = \mathbb{Q}(\vartheta)\big)$$

nach Korollar 6.4

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

$$\jmath_1(a + b\vartheta) = a + bc \quad \text{und} \quad \jmath_2(a + b\vartheta) = a - bc \qquad \big(a + b\vartheta \in \mathbb{Q}(\vartheta)\big)$$

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

$$\begin{aligned}\left|24 - \frac{1}{2}\,\vartheta\right|_1 &= \left|2 + 2 \cdot 11 + \frac{1}{2}\,(4 + 4 \cdot 11 + 6 \cdot 11^2 + \cdots)\right|_{11} \\ &= |4 + \cdots|_{11} = |1|_{11} = 1\,.\end{aligned}$$

Also sind die beiden Bewertungen verschieden.

BEHAUPTUNG. Man erhält durch die Einbettungen von E in $\mathfrak{C}$ 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

$$\jmath : \hat{K}(\vartheta) \to \mathfrak{C}\,,$$

die auf $\hat{K}$ die Identität ist. Durch

$$|x| := |\jmath(x)|_{\mathfrak{C}} \qquad \big(x \in \hat{K}(\vartheta)\big)$$

wird auf $\hat{K}(\vartheta)$ eine Bewertung definiert. Wegen des Eindeutigkeitssatzes ist $|x|_{\hat{E}} = |\jmath(x)|_{\mathfrak{C}}$, $x \in \hat{E}$, also

$$|x|_E = |\jmath(x)|_{\mathfrak{C}} \qquad \text{für } x \in E\,,$$

d.h. $|\ |_E$ wird durch die Einbettung

$$\jmath_{|E} : E \to \mathfrak{C}$$

induziert. □

KAPITEL 7

Geordnete Gruppen

Eine Gruppe G heißt eine *geordnete Gruppe*, wenn gilt:

(1) G ist linear geordnet
(2) Aus $a \leq b$ folgt $ac \leq bc$ und $ca \leq cb$ für alle $a, b, c \in G$.

BEISPIEL. 1.) $(\mathbb{R}, +)$, $(\mathbb{R}^+, \cdot)$. Beide Gruppen sind isomorph: die Abbildung

$$\mathbb{R} \to \mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}, \qquad x \mapsto e^x$$

ist ein ordnungserhaltender Isomorphismus.
2.) Lexikographische Anordnung: Seien $G_1, \ldots, G_n$ geordnete Gruppen und

$$G = G_1 \times \cdots \times G_n = \bigtimes_{i=1}^{n} G_i$$

ihr direktes Produkt. Durch

$$(a_1, \ldots, a_n) < (b_1, \ldots, b_n),$$

falls es ein $1 \leq i \leq n$ mit

$$a_i < b_i \quad \text{und} \quad a_j = b_j \text{ für } j < i$$

gibt, und komponentneweise Verknüpfung wird G eine geordnete Gruppe.
3.) Nichtabelsche geordnete Gruppen: Sei

$$G = \mathbb{R}^+ \times \mathbb{R} = \{(a, b) \in \mathbb{R}^2 \mid a > 0\}.$$

Durch die Verknüpfung

$$(a, b) \circ (c, d) := (ac, ad + b)$$

wird G zu einer Gruppe, die bezüglich der lexikographischen Anordnung geordnet ist. Es ist

$$(a, b) < (c, d) \iff (a < c) \vee (a = c \wedge b < d).$$

4.) Hahnsches Produkt: Seien G_i geordnete Gruppen und i aus einer beliebigen Indexmenge I. Eine Teilmenge A von I heißt *wohlgeordnet*, wenn jede Teilmenge von A ein kleinstes Element besitzt. Der *Träger* eines Elementes

$$x = (x_i) \in \bigtimes_{i \in I} G_i =: \prod_{i \in I} G_i$$

ist

$$\operatorname{Tr} x = \{i \in I \mid x_i \neq e_i\},$$

wobei e_i das Einselement von G_i, $i \in I$, bezeichnet. Es ist $\operatorname{Tr} x \neq \emptyset$ für $x \neq e = (e_i)$.

Das Hahnsche Produkt $\bigsqcap_{i\in I} G_i$ ist die Untergruppe von $\prod_{i\in I}$, die aus allen Elementen mit wohlgeordnetem Träger besteht. (Für jede wohlgeordnete Indexmenge I ist $\bigsqcap_{i\in I} G_i = \prod_{i\in I} G_i$.) $\bigsqcap_{i\in I} G_i$ läßt sich lexikographisch anordnen: Wir definieren

$$e < x \qquad \text{falls } i \text{ kleinstes Element von } \operatorname{Tr} x \text{ und } e_i < x_i \text{ ist.}$$

Hiermit ist

$$y < x \quad \text{falls} \quad e < xy^{-1}$$

gilt ($x, y \in \bigsqcap_{i\in I} G_i$). $\bigsqcap_{i\in I}$ wird hierdurch eine geordnete Gruppe.

Aus den Axiomen für eine geordnete Gruppe erhält man folgende *Eigenschaften*: Es seien $a, b, c \in G$. Dann gilt:

(A)
$$\begin{aligned} a \leq b \wedge c \leq d \quad &\Longrightarrow \quad ac \leq bd \\ a \leq b \wedge c < d \quad &\Longrightarrow \quad ac < bd \end{aligned}$$

(B)
$$\begin{aligned} a \leq b \quad &\Longrightarrow \quad a^n \leq b^n \\ a < b \quad &\Longrightarrow \quad a^n < b^n \end{aligned} \qquad \text{für alle } n \in \mathbb{N}.$$

(C) $$a \leq b \quad \Longrightarrow \quad b^{-1} \leq a^{-1} \quad \Longrightarrow \quad b^{-n} \leq a^{-n} \qquad \text{für alle } n \in \mathbb{N}.$$

SATZ 7.1. *Alle vom Einselement verschiedenen Elemente von G haben unendliche Ordnung.*

BEWEIS. Sei e das Einselement von G. Aus $e < x$ bzw. $x < e$ folgt nach (B) $e < x^n$ bzw. $x^n < e$ für alle $n \in \mathbb{N}$. Also ist stets $e \neq x^n$. □

DEFINITION 7.1. Eine geordnete Gruppe G heißt *archimedisch geordnet*, wenn zu jedem $a > e$ und zu jedem $b \in G$ ein $n \in \mathbb{N}$ mit

$$b \leq a^n$$

existiert.

G ist genau dann archimedisch geordnet, wenn zu jedem $a > e$ und jedem $b \in G$ ein $n \in \mathbb{Z}$ mit

$$a^n \leq b < a^{n+1}$$

existiert.

BEISPIEL. 1.) $(\mathbb{R}, +)$ ist archimedisch geordnet. Aber auch die positiven reellen Zahlen sind bezüglich der Multiplikation archimedisch geordnet: Seien $b > 0$ und $a > 1$, also $a = 1 + h$ mit $h > 0$. Dann ist nach BERNOULLI für genügend großes $n \in \mathbb{N}$

$$a^n = (1+h)^n \geq 1 + nh > b\,.$$

2.) $G = \mathbb{Z} \times \mathbb{Z}$ sei lexikographisch geordnet. G ist nicht archimedisch geordnet, denn es ist $(0,0) < (0,1)$, und für alle $n \in \mathbb{N}$ gilt

$$n\,(0,1) = (0,n) < (1,0)\,.$$

SATZ 7.2. *Eine archimedisch geordnete Gruppe ist kommutativ.*

BEWEIS. 1. Fall: Die Menge $P = \{x \in G \mid e < x\}$ enthält ein kleinstes Element $c > e$.
Sei $a \in G$ beliebig. Weil G archimedisch geordnet ist, gibt es ein $n \in \mathbb{Z}$ mit

$$c^n \leq a < c^{n+1}\,, \qquad \text{also} \qquad e \leq ac^{-n} < c\,.$$

Weil c minimal in P ist, folgt $ac^{-n} = e$, also $a = c^n$. Damit ist G zyklisch, also insbesondere kommutativ.
2. Fall: Die Menge $P = \{x \in G \mid e < x\}$ besitzt kein kleinstes Element. Wir beweisen zuerst eine

ZWISCHENBEHAUPTUNG. Ist $x > e$, so gibt es ein $z \in G$ mit

$$e < z < x \qquad \text{und} \qquad e < z^2 \leq x\,.$$

BEWEIS. Weil P kein kleinstes Element besitzt, gibt es ein $y \in P$ mit

$$e < y < x\,.$$

Ist $y^2 \leq x$, so kann man $z = y$ setzen. Ist dagegen $x < y^2$, so setze man $z = xy^{-1}$. Aus $y < x < y^2$ folgt

$$e < z = xy^{-1} < y$$

und hieraus

$$z < z^2 < zy = x\,. \quad \checkmark$$

Die Kommutativität von G beweist man jetzt indirekt. Angenommen, für zwei Elemente a, b aus G gilt

$$ab \neq ba\,, \qquad \text{etwa } ab > ba\,.$$

Dann ist

$$e < x := aba^{-1}b^{-1}\,.$$

Nach obiger Zwischenbehauptung gibt es daher ein $z \in G$ mit

$$e < z < x \qquad \text{und} \qquad e < z^2 \leq x\,.$$

Weil G archimedisch geordnet ist, gibt es $n, m \in \mathbb{Z}$ mit

$$z^m \leq a < z^{m+1} \qquad \text{und} \qquad z^n \leq b < z^{n+1}\,.$$

Daraus folgt

$$x = aba^{-1}b^{-1} < z^{m+1}z^{n+1}z^{-m}z^{-n} = z^2\,,$$

also ein Widerspruch zu $z^2 \leq x$. Folglich ist G kommutativ. □

Wie der folgende Satz zeigt, lassen sich die archimedisch geordneten Gruppen als Untergruppen von $(\mathbb{R}, +)$ auffassen.

SATZ 7.3. (HÖLDER 1901) *G sei archimedisch geordnet und $a > e$ ein fest gewähltes Element von G. Dann gibt es genau einen isotonen (d.h. ordnungserhaltenden) und injektiven Homomorphismus*

$$f : G \to (\mathbb{R}, +) \qquad \textit{mit } f(a) = 1\,.$$

BEWEIS. Sei $x \in G$. Definiere

$$U(x) := \left\{ \frac{n}{m} \in \mathbb{Q} \;\middle|\; n \in \mathbb{Z},\ m \in \mathbb{N},\ a^n \leq x^m \right\}.$$

Diese Menge rationaler Zahlen besitzt folgende Eigenschaften:

(1) Aus $q' \leq q$ und $q \in U(x)$ folgt $q' \in U(x)$.

BEWEIS. Es sei

$$q' = \frac{n'}{m'} \leq \frac{n}{m} = q$$

mit $n, n' \in \mathbb{Z}$, $m, m' \in \mathbb{N}$ und $a^n \leq x^m$. Dann ist

$$a^{mn'} \leq a^{nm'} \leq x^{mm'},$$

also

$$q' = \frac{mn'}{mm'} \in U(x). \quad \checkmark$$

(2) Es gilt $a^n \leq x^m$ genau dann, wenn $\frac{n}{m} \in U(x)$ ist.

BEWEIS. Die eine Beweisrichtung ergibt sich aus der Definition von $U(x)$. Die andere wird indirekt bewiesen. Angenommen, es wäre

$$\frac{n}{m} = \frac{n'}{m'} \in U(x), \quad a^{n'} \leq x^{m'}, \quad a^n > x^m.$$

Dann würde

$$x^{mm'} < a^{nm'} = a^{n'm} \leq x^{mm'},$$

also ein Widerspruch folgen. $\checkmark$

(3) Es ist $U(x) \neq \emptyset$ und $\sup U(x) < \infty$.

BEWEIS. Weil G archimedisch geordnet ist, gibt es ein $n \in \mathbb{Z}$ mit

$$a^n \leq x < a^{n+1},$$

also ist $n \in U(x)$ und $n+1 \notin U(x)$. Damit ist $U(x) \neq \emptyset$ und $n+1$ eine obere Schranke von $U(x)$ nach (1). Folglich existiert das Supremum von $U(x)$. $\checkmark$

Wir definieren

$$f(x) := \sup U(x) \qquad (x \in G)$$

und erhalten hiermit eine Abbildung $f : G \to \mathbb{R}$. Es gilt

(4) Ist $q < f(x)$, $q \in Q$, so ist $q \in U(x)$.

BEWEIS. Wegen $f(x) = \sup U(x)$ gibt es ein $q' \in U(x)$ mit

$$q < q' < f(x).$$

Nach (1) ist daher $q \in U(x)$. $\checkmark$

(a) Es gilt

$$f(xy) = f(x) + f(y)$$

für alle $x, y \in G$.

BEWEIS. Sei $\varepsilon > 0$ und

$$f(x) - \varepsilon < q_1 < f(x) < q_2 < f(x) + \varepsilon$$

sowie

$$f(y) - \varepsilon < q_3 < f(y) < q_4 < f(y) + \varepsilon$$

Ist $q_i = \frac{n_i}{m_i}$, $n_i \in \mathbb{Z}$, $m_i \in \mathbb{N}$, $i = 1, \ldots, 4$, so kann man $m_i = m$, $i = 1, \ldots, 4$ annehmen (andernfalls erweitere man die Brüche auf ihren Hauptnenner). Damit ist nach (4)

$$a^{n_1} \leq x^m < a^{n_2} \qquad \text{und} \qquad a^{n_3} \leq y^m < a^{n_4}\,.$$

Weil G nach Satz 7.2 kommutativ ist, folgt hieraus

$$a^{n_1+n_3} \leq (xy)^m < a^{n_2+n_4}\,,$$

also

$$q_1 + q_3 = \frac{n_1 + n_3}{m} \leq f(xy) \leq q_2 + q_4 = \frac{n_2 + n_4}{m}\,.$$

Es folgt

$$f(x) + f(y) - 2\varepsilon \leq f(xy) \leq f(x) + f(y) + 2\varepsilon\,.$$

Weil $\varepsilon > 0$ beliebig gewählt werden kann, ist

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

(b) f ist isoton und injektiv.

BEWEIS. Sei $x < y$, also $e < yx^{-1}$. Weil G archimedisch geordnet ist, gibt es ein $n \in \mathbb{N}$ mit

$$a \leq (yx^{-1})^n\,.$$

Es folgt

$$0 < \frac{1}{n} \leq f(yx^{-1}) = f(y) - f(x)\,,$$

also

$$f(x) < f(y)\,.$$

Damit ist f isoton und injektiv. $\checkmark$

(c) Es ist $f(a) = 1$.

BEWEIS. Wegen

$$\begin{aligned} U(a) &= \left\{ \frac{n}{m} \,\middle|\, n \in \mathbb{Z},\, m \in \mathbb{N},\, a^n \leq a^m \right\} \\ &= \left\{ \frac{n}{m} \,\middle|\, n \in \mathbb{Z},\, m \in \mathbb{N},\, n \leq m \right\} \\ &= \{q \in \mathbb{Q} \mid q \leq 1\} \end{aligned}$$

ist $f(a) = \sup U(a) = 1$. $\checkmark$

(d) Die Abbildung f ist eindeutig bestimmt.

BEWEIS. Sei g ein injektiver und isotoner Homomorphismus

$$g : G \to (\mathbb{R}, +) \quad \text{mit} \quad g(a) = 1\,.$$

Wegen

$$\begin{aligned} \frac{n}{m} \in U(x) \quad &\Longrightarrow \quad a^n \le x^m \quad \Longrightarrow \quad n\,g(a) \le m\,g(x) \\ &\Longrightarrow \quad n \le m\,g(x) \quad \Longrightarrow \quad \frac{n}{m} \le g(x) \end{aligned}$$

ist dann

$$g(x) \ge \sup U(x) = f(x) \qquad (x \in G)\,.$$

Aus $\frac{n}{m} \notin U(x)$, also $a^n > x^m$, folgt entsprechend

$$g(x) < \frac{n}{m}\,.$$

Damit ist $g(x)$ die kleinste obere Schranke von $U(x)$, also

$$g(x) = f(x) \qquad \text{für alle } x \in G\,. \quad \checkmark$$

□

Eine wichtige Folgerung von Satz 7.3 ist die Existenz des Logarithmus und damit auch der Exponentialfunktion als Umkehrfunktion des Logarithmus. Sei $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ die Gruppe der positiven reellen Zahlen bezüglich der Multiplikation. Wie wir bereits wissen, ist diese Gruppe archimedisch geordnet. Daher gibt es eine eindeutig bestimmte Abbildung $\log_a : \mathbb{R}^+ \to \mathbb{R}$ mit

$$\begin{aligned} \log_a(xy) &= \log_a(x) + \log_a(y) \\ x < y &\Longrightarrow \log_a(x) < \log_a(y) \\ \log_a(a) &= 1. \end{aligned}$$

BEMERKUNG. Die Auswahl von a und die Bedingung $f(a) = 1$ dienen nur dazu, f eindeutig festzulegen. Ist $g : G \to (\mathbb{R}, +)$ ein beliebiger isotoner und injektiver Homomorphismus, so gilt $g = c \cdot f$ mit $0 \le c \in \mathbb{R}$, d.h. alle isotonen und injektiven Homomorphismen $g : G \to (\mathbb{R}, +)$ ergeben sich durch Multiplikation von f mit einer positiven rellen Zahl.

BEWEIS. Aus $e < a$ folgt $g(e) = 0 < g(a)$. Setze $c := g(a)$. Die Abbildung

$$g^*(x) := \frac{1}{c}\,g(x) \qquad (x \in G)$$

ist dann ebenfalls ein isotoner und injektiver Homomorphismus. Außerdem gilt $g^*(a) = 1$, also ist $g^* = f$ nach Satz 7.3, also $g(x) = cf(x)$ für alle $x \in G$. □

ANWENDUNG. 1.) Die Abbildungen $f : \mathbb{R} \to \mathbb{R}$ mit

(a) $$f(x + y) = f(x) + f(y)$$

(b) $$x < y \;\Rightarrow\; f(x) < f(y)$$

haben die Form $f(x) = cx$ mit $0 < c \in \mathbb{R}$.

2.) Sei $P = \{x \in \mathbb{R} \mid x > 0\}$ die Gruppe der positiven reellen Zahlen bezüglich der Multiplikation. Die Abbildungen $f : P \to \mathbb{R}$ mit

(a) $$f(x+y) = f(x) + f(y)$$

(b) $$x < y \;\Rightarrow\; f(x) < f(y)$$

haben die Form

$$f(x) = c \ln x\,, \qquad (0 < c \in \mathbb{R})\,,$$

wobei die Existenz einer Logarithmusabbildung schon durch Satz 7.3 gesichert ist.

DEFINITION 7.2. Eine Teilmenge S einer geordneten Menge M heißt *konvex*, wenn gilt:

$$s_1 \le x \le s_2\,,\;\; s_1, s_2 \in S,\, x \in M \quad \Longrightarrow \quad x \in S\,.$$

SATZ 7.4. *Die konvexen Untergruppen einer geordneten Gruppe G sind bezüglich der Inklusion linear geordnet, d.h. für zwei konvexe Untergruppen U_1, U_2 von G gilt $U_1 \subseteq U_2$ oder $U_2 \subseteq U_1$.*

BEWEIS. Seien U_1, U_2 konvexe Untergruppen von G mit $U_1 \not\subseteq U_2$, etwa $x \in U_1$ und $x \notin U_2$. Man kann $x > e$ annehmen (andernfalls wähle x^{-1}). Sei $y \in U_2$. Dann ist $y < x$, weil aus $e < x \le y$ wegen der Konvexität von U_2 $x \in U_2$ folgen würde. Außerdem ist $x^{-1} < y$, weil aus $y \le x^{-1} < e$ wegen der Konvexität von U_2 $x^{-1} \in U_2$ folgen würde. Aus $x^{-1} < y < x$ folgt aber $y \in U_1$ wegen der Konvexität von U_1. Also ist $U_2 \subseteq U_1$. □

BEISPIEL. Sei $G = \mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z}$ lexikographisch geordnet. Bezüglich der komponentenweisen Addition ist $\mathbb{Z}^n$ eine abelsche Gruppe.

1.) Die Mengen

$$U_k = \{x = (x_1, \ldots, x_n) \in \mathbb{Z}^n \mid x_1 = \cdots = x_k = 0\} \qquad (k = 0, 1, \ldots, n)$$

sind konvexe Untergruppen von $\mathbb{Z}^n$:
Die Gruppeneigenschaften sind trivialerweise erfüllt. Ferner folgt aus

$$x \le y \le x' \quad \text{mit} \quad x, x' \in U_k\,,$$

daß auch die ersten k Komponenten von y Null sind, also $y \in U_k$.

2.) Jede konvexe Untergruppe U von $\mathbb{Z}^n$ ist eine der Untergruppen U_k:
Wähle k maximal mit $U \subseteq U_k$. Ist $k = n$, so ist $U_k = U_n = 0 = U$. Sei also $k < n$. Dann gibt es ein $x = (x_1, \ldots, x_n) \in U$ mit

$$x_1 = \cdots = x_k = 0 \quad \text{und} \quad x_{k+1} \neq 0\,.$$

Ist $y = (y_1, \ldots, y_n) \in U_k$, so gibt es ein $t \in \mathbb{Z}$ mit

$$-t x_{k+1} \le y_{k+1} \le t x_{k+1}\,.$$

Dann ist

$$-tx \le y \le tx\,,$$

also $y \in U$, weil U konvex ist. Damit ist $U_k \subseteq U$. Insgesamt ist damit $U = U_k$.
Ergebnis:

$$U_0 = \mathbb{Z}^n \supseteq U_1 \supseteq U_2 \supseteq \cdots \supseteq U_n = 0$$

ist die Kette aller konvexen Untergruppen von $\mathbb{Z}^n$.

DEFINITION 7.3. Die Anzahl der echten konvexen Untergruppen heißt *Rang* der geordneten Gruppe.

Wegen $\operatorname{Rang} \mathbb{Z}^n = n$ treten alle natürlichen Zahlen als Rang von geordneten Gruppen auf. Es gibt auch Gruppen von unendlichem Rang.

SATZ 7.5. *Eine Gruppe G ist genau dann archimedisch geordnet, wenn ihr Rang gleich 1 ist.*

BEWEIS. 1.) Sei G archimedisch geordnet und $U \neq \{e\}$ eine konvexe Untergruppe von G. Sei $a \in U$, $a > e$ und $b \in G$. Dann gibt es ein $n \in \mathbb{Z}$ mit

$$a^n \leq b < a^{n+1}\,.$$

Weil U konvex ist, folgt $b \in U$, also ist $G \subseteq U$, d.h. $G = U$. Damit ist $\operatorname{Rang} G = 1$.
2.) Sei $\operatorname{Rang} G = 1$ und $a > e$. Die Menge

$$U_a = \{b \in G \mid \exists\, n \in \mathbb{N} : a^{-n} \leq b \leq a^n\}$$

ist eine konvexe Untergruppe: Seien $b, c \in U_a$. Dann gibt es $n, m \in \mathbb{N}$ mit

$$a^{-n} \leq b \leq a^n$$

und

$$a^{-m} \leq c \leq a^m\,.$$

Wegen

$$a^{-m} \leq c^{-1} \leq a^m$$

folgt hieraus

$$a^{-n+m} \leq bc^{-1} \leq a^{n+m}\,,$$

also $bc^{-1} \in U_a$. Ist $b \leq x \leq c$ mit $x \in G$, so gilt

$$a^{-k} \leq x \leq a^k \quad \text{mit} \quad k := \max(n, m)\,,$$

also $x \in U_a$, d.h. U_a ist eine konvexe Untergruppe.
Wegen $a \in U_a$ ist $U_a \neq \{e\}$. Weil $\operatorname{Rang} G = 1$ ist, folgt daher $U_a = G$. Damit gibt es zu jedem $b \in G$ ein $n \in \mathbb{N}$ mit $b \leq a^n$, d.h. G ist archimedisch geordnet. □

KAPITEL 8

Krullbewertungen

1. Multiplikative Krullbewertungen

DEFINITION 8.1. K sei ein Körper. Ein Teilring B von K heißt ein *Bewertungsring*, wenn für $x \in K^\times$ stets

$$x \in B \quad \text{oder} \quad x^{-1} \in B$$

gilt.

BEISPIEL. 1.) $B = K$ heißt der triviale Bewertungsring.
2.) K sei nicht-archimedisch bewertet. Dann ist

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

ein Bewertungsring, denn aus $|x| > 1$ folgt $|x^{-1}| < 1$.
3.) Sei $K = k(x, y)$, wobei k ein Körper und x, y algebraisch unabhängig über k sind. Jedes $f \in K$, $f \neq 0$ besitzt die Darstellung

$$f = x^k y^\ell \frac{h(x,y)}{g(x,y)},$$

wobei k, ℓ eindeutig bestimmte Elemente aus $\mathbb{Z}$ und h, g zu x, y teilerfremde Polynome sind. Definiert man

$$\operatorname{ord}_x f = k\,, \quad \operatorname{ord}_y f = \ell \qquad \text{für } f \neq 0$$

und

$$\operatorname{ord}_x f = \operatorname{ord}_y f = \infty \qquad \text{für } f = 0\,,$$

so sind

$$B_1 = \{f \in K \mid \operatorname{ord}_x f \geq 0\}$$

und

$$B_2 = \{f \in K \mid \operatorname{ord}_x f > 0 \ \vee \ (\operatorname{ord}_x f = 0 \wedge \operatorname{ord}_y f \geq 0)\}$$

Bewertungsringe von K. Es gilt

$$B_2 \subsetneqq B_1 \subsetneqq K\,,$$

denn es ist

$$\frac{1}{y} \notin B_2\,, \quad \text{aber} \quad \frac{1}{y} \in B_1$$

und

$$\frac{1}{x} \notin B_1\,, \quad \text{aber} \quad \frac{1}{x} \in K\,.$$

BEMERKUNG. Wie wir später sehen werden, ist B_2 nicht Bewertungsring einer nicht-archimedischen Bewertung.

DEFINITION 8.2. Sei K ein Körper. Eine nicht-leere Teilmenge I von K heißt *gebrochenes Ideal* bezüglich eines Bewertungsringes B, wenn IB in I enthalten ist, d.h. wenn gilt:

$$x \in I,\, y \in B \quad \Longrightarrow \quad xy \in I\,. \tag{1}$$

EIGENSCHAFTEN.

$$x \in I \quad \Longrightarrow \quad -x \in I \tag{2}$$

$$x, y \in I \quad \Longrightarrow \quad x + y \in I \tag{3}$$

BEWEIS. (2): Für einen Bewertungsring gilt stets $1 \in B$ und $-1 \in B$, weil $1^{-1} = 1$ und $(-1)^{-1} = -1$ ist. Damit folgt (2) aus (1).
(3): Ist $x = 0$ oder $y = 0$, so ist (3) offensichtlich erfüllt. Seien also x, y von Null verschieden. Weil B ein Bewertungsring ist, ist

$$x^{-1}y \in B \quad \text{oder} \quad (x^{-1}y)^{-1} = y^{-1}x \in B\,,$$

also

$$1 + x^{-1}y \in B \quad \text{oder} \quad y^{-1}x + 1 \in B\,.$$

Damit ist aber nach (1)

$$x + y = x\,(1 + x^{-1}y) = y\,(y^{-1}x + 1) \in I\,. \quad \square$$

FOLGERUNG 8.1. *Ist I in B enthalten, so ist I ein Ideal von B (im ringtheoretischen Sinn).*

Die gebrochenen Ideale, die in B liegen, nennt man auch *ganze Ideale.*

BEISPIEL. 1.) Für jedes $x \in K$ ist

$$xB = \{xy \mid y \in B\}$$

ein gebrochenes Hauptideal. Ist $x \in B$, so ist xB ein ganzes Ideal. Ist $x \notin B$, so ist $xB \nsubseteq B$ wegen $x \cdot 1 = x \notin B$.
2.) Ist B' ein Oberring von B, so ist B' ein gebrochenes Ideal bezüglich B. Außerdem ist B' ein Bewertungsring:

$$x \notin B' \quad \Longrightarrow \quad x \notin B \quad \Longrightarrow x^{-1} \in B \quad \Longrightarrow x^{-1} \in B'\,.$$

SATZ 8.1. *Die Menge der gebrochenen Ideale (bezüglich eines festen Bewertungsringes B) sind bezüglich der Inklusion linear geordnet.*

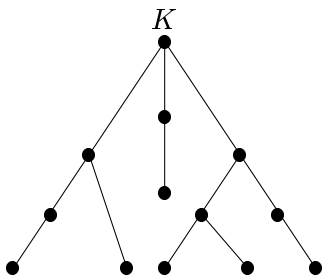
BEWEIS. Seien I_1, I_2 gebrochene Ideale und $I_1 \not\subseteq I_2$. Dann gibt es ein $x \in I_1$ mit $x \notin I_2$. Sei $y \in I_2$, $y \neq 0$. Wegen

$$y\,(y^{-1}x) = x \notin I_2$$

ist $y^{-1}x \notin B$. Weil B ein Bewertungsring ist, folgt $x^{-1}y = (y^{-1}x)^{-1} \in B$ und damit $y = x\,(x^{-1}y) \in I_1$. Also ist $I_2 \subseteq I_1$. □

KOROLLAR 8.1. *Die Menge der Oberringe über einem Bewertungsring ist bezüglich der Inklusion linear geordnet.*

Interpretiert man jeden Bewertungsring von K als Knoten in einem Graphen, dessen Kanten durch die Inklusion der Bewertungsringe gegeben sind, so bildet der so konstruierte Graph einen Baum (das ist ein Graph ohne Kreise).



KOROLLAR 8.2. *Die Menge der von Null verschiedenen gebrochenen Hauptideale*

$$\Gamma = \{xB \mid x \in K^\times\}$$

bildet bezüglich der Verknüpfung

$$xB \cdot yB := xyB \qquad (x, y \in K^\times)$$

eine geordnete Gruppe, wobei die Ordnung durch die Inklusion gegeben ist.

BEWEIS. 1.) Die Verknüpfung ist wohldefiniert, denn aus $xB = x'B$ und $yB = y'B$ folgt

$$xyB = xy'B = y'xB = y'x'B = x'y'B\,.$$

2.) Die Gruppeneigenschaften von Γ folgen direkt aus den Körpereigenschaften von K.

3.) Nach Satz 8.1 ist Γ als Untermenge einer linear geordneten Menge linear geordnet. Ferner gilt für xB, yB, $zB \in \Gamma$ mit $xB \subseteq yB$

$$xB \cdot zB = xzB = zxB \subseteq zyB = yzB = yB \cdot zB$$

und analog

$$zB \cdot xB \subseteq zB \cdot yB\,.$$

Also ist Γ eine geordnete Gruppe. □

Sei Γ eine multiplikativ geschriebene geordnete Gruppe. Erweitere Γ durch ein Element 0 zu $\hat{\Gamma} := \Gamma \cup \{0\}$ und setze

$$0 \leq \gamma \quad \text{und} \quad 0 \cdot \gamma = \gamma \cdot 0 = 0$$

für alle $\gamma \in \Gamma$.

Beispiel. 1.) Es ist $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\} = \{x \in \mathbb{R} \mid x > 0\} \cup \{0\}$, und $\{x \in \mathbb{R} \mid x > 0\}$ ist eine geordnete Gruppe.
2.) Für die geordnete Gruppe Γ aller von Null verschiedenen gebrochenen Hauptideale bezüglich eines festen Bewertungsringes B ist $\hat{\Gamma} = \Gamma \cup \{0B\}$.

Definition 8.3. Sei K ein Körper und Γ eine geordnete Gruppe. Eine Abbildung

$$|\ | : K \to \hat{\Gamma} = \Gamma \cup \{0\}, \quad x \mapsto |x|,$$

heißt eine *Krullbewertung*, wenn für $x, y \in K$ gilt:

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

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

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

Bemerkung. Krullbewertungen sind Verallgemeinerungen der reellen nicht-archimedischen Bewertungen. Die reellen archimedischen Bewertungen sind dagegen keine Krullbewertungen.

Einfache Eigenschaften

(A) Bezeichnet man das neutrale Element von Γ ebenfalls mit 1, so gilt

$$|1| = |-1| = 1.$$

Beweis. Wegen $|1|, |-1| \neq 0$ ist $|1|, |-1| \in \Gamma$. Aus $|1| = |1 \cdot 1| = |1| \cdot |1|$ folgt $|1| = 1$. Wegen $|-1|^2 = |1| = 1$ hat $|-1|$ in Γ endliche Ordnung. Weil Γ eine geordnete Gruppe ist, folgt $|-1| = 1$. □

Folgerung. Für alle $x \in K$ gilt $|x| = |-x|$.

(B) Ist $|x| \neq |y|$, so ist $|x+y| = \max(|x|, |y|)$. Der Beweis erfolgt analog dem für nicht-archimedische reelle Bewertungen.

(C) $B = \{x \in K \mid |x| \leq 1\}$ ist ein Bewertungsring in K.

Beweis. 1.) Für $x, y \in B$ gilt

$$|x - y| \leq \max(|x|, |y|) \leq 1, \qquad \text{also } x - y \in B$$

und

$$|xy| = |x|\,|y| \leq 1, \qquad \text{also } xy \in B.$$

Wegen $1 \in B$ ist $B \neq \emptyset$. Also ist B ein Ring.
2.) Sei $x \in K$ mit $x \notin B$. Dann ist $|x| > 1$, also $|x^{-1}| < 1$, d.h. es ist $x^{-1} \in B$. Damit ist B eine Bewertungsring von K. □

SATZ 8.2. *Zu jedem Bewertungsring B von K existiert eine Krullbewertung $|\ |$, so daß*

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

ist.

BEWEIS. Sei $\hat{\Gamma}$ die Menge aller gebrochenen Hauptideale xB, $x \in K$. Nach Korollar 8.2 ist $\Gamma = \{xB \mid x \in K^\times\}$ eine geordnete Gruppe. Definiere

$$|\ | : K \to \hat{\Gamma}\,, \quad x \mapsto |x| = xB\,.$$

Nachweis der Axiome:

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

(2) Für alle $x, y \in K$ ist wegen

$$(x+y)B \subseteq xB + yB \subseteq \max(xB, yB)$$

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

(3) Für alle $x, y \in K$ ist

$$|xy| = xyB = xB \cdot yB = |x|\,|y|\,.$$

Schließlich ist

$$\{x \in K \mid |x| \leq 1\} = \{x \in K \mid xB \subseteq 1 \cdot B\} = \{x \in K \mid x \in B\} = B\,. \quad \square$$

DEFINITION 8.4. Zwei Krullbewertungen $|\ |_1$ und $|\ |_2$ von K heißen *äquivalent*, ($|\ |_1 \sim |\ |_2$), wenn gilt:

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

für alle $x, y \in K$.

Hierdurch werden die Krullbewertungen in Klassen äquivalenter Bewertungen eingeteilt. Es gilt

$$|\ |_1 \sim |\ |_2 \iff B_1 = \{x \in K \mid |x|_1 \leq 1\} = B_2 = \{x \in K \mid |x|_2 \leq 1\}\,.$$

Satz 8.2 sagt aus, daß die Mengen der Bewertungsringe von K bijektiv der Menge der Klassen äquivalenter Krullbewertungen entspricht.

$G = \{|x| \in \Gamma \mid x \neq 0\}$ ist eine Untergruppe von Γ und heißt *Wertegruppe* der Bewertung.

Die Wertegruppen äquivalenter Bewertungen sind ordnungsisomorph (d.h $f : G_1 \to G_2$, $f(|x|_1) = |x|_2$ ist ein isotoner Isomorphismus).

DEFINITION 8.5. Eine Krullbewertung heißt eine Bewertung vom Rang n, wenn ihre Wertegruppe den Rang n besitzt.

BEHAUPTUNG. Die Bewertungen vom Rang 1 sind genau diejenigen, die zu den reellen nicht-archimedischen Bewertungen äquivalent sind.

BEWEIS. 1.) Hat die Wertegruppe den Rang 1, so ist G archimedisch geordnet. Nach Satz 7.3 gibt es dann einen isotonen und injektiven Homomorphismus

$$f : G \to (\mathbb{R}, +) @ > \exp >> (\{x \in \mathbb{R} \mid x > 0\}, \times)\,.$$

Die durch

$$|x|_1 := \begin{cases} f(|x|) & \text{für } x \neq 0 \\ 0 & \text{für } x = 0 \end{cases}$$

definierte Bewertung ist dann reell und äquivalent zu $|\ |$.

2.) Die Wertegruppe einer reellen nicht-archimedischen Bewertung ist Untergruppe von $(\{x \in \mathbb{R} \mid x > 0\}, \times)$, also archimedisch und hat daher nach Satz 7.5 den Rang 1. □

Ein Ideal P von B heißt *Primideal*, wenn $P \neq B$ ist und für alle $x, y \in B$ mit $xy \in P$ stets $x \in P$ oder $y \in P$ folgt.

BEHAUPTUNG. Ist P ein Primideal eines Bewertungsringes B von K, so gilt

$$\text{(P)}\quad xy \in P \quad \Longrightarrow \quad (x \in P \ \text{ oder } \ y \in P)$$

für alle $x, y \in K$.

BEWEIS. Sind $x, y \in B$, so ergibt sich (P) direkt aus der Definition des Primideals. Ist $x \notin B$ oder $y \notin B$, etwa $y \notin B$, so ist $y^{-1} \in B$, also $x = (xy)\, y^{-1} \in P$. □

Im folgenden soll der Zusammenhang zwischen den konvexen Untergruppen der Wertegruppe und den Primidealen des Bewertungsringes untersucht werden. Wir beweisen zunächst den

HILFSSATZ 8.1. *Ist U eine konvexe Untergruppe der Wertegruppe G, so ist*

$$P = \{x \in B \mid |x| \notin U\}$$

ein Primideal von B.

BEWEIS. 1.) Wegen $0 \in P$ und $1 \notin P$ ist P eine echte nicht-leere Teilmenge von B.

2.) P ist ein Ideal von B: Sei $x \in P$, $y \in B$. Dann ist

$$|xy| = |x|\,|y| \leq |x| \leq 1 = |1|\,.$$

Weil U konvex ist, folgt

$$|xy| \in U \quad \Longrightarrow \quad |x| \in U$$

oder gleichwertig hiermit

$$|x| \notin U \quad \Longrightarrow \quad |xy| \notin U\,.$$

Wegen $x \in P$ ist $|x| \notin U$, also $|xy| \notin U$, d.h. es ist $xy \in P$.
Für $x, y \in P$ ist

$$|x - y| \leq \max\left(|x|, |y|\right) \leq 1 = |1|\,.$$

Wäre nun $x - y \notin P$, so wäre $|x - y| \in U$. Aus der Konvexität von U würde dann $|x|, |y| \in U$, also $x, y \notin P$ folgen, im Widerspruch zur Wahl von x und y. Also ist $x - y \in P$.
Insgesamt ist damit P ein Ideal von B.

3.) P ist ein Primideal: Seien $x, y \in B$. Dann gilt

$$\begin{aligned} xy \in P \quad &\Longrightarrow \quad |xy| = |x|\,|y| \notin U \\ &\Longrightarrow \quad |x| \notin U \ \text{ oder } \ |y| \notin U \\ &\Longrightarrow \quad x \in P \ \text{ oder } \ y \in P\,. \end{aligned}$$

Also ist P ein Primideal. □

SATZ 8.3. *Sei $\mathfrak{U}$ die Menge der konvexen Untergruppen der Wertegruppe G und $\mathfrak{P}$ die Menge der Primideale von B. Dann ist die Abbildung*

$$f : \mathfrak{U} \to \mathfrak{P}, \quad U \mapsto f(U) = \{x \in B \mid |x| \notin U\}$$

eine antitone Bijektion.

BEWEIS. 1.) Sei $U_1 \subseteq U_2$. Aus $|x| \notin U_2$ folgt dann $|x| \notin U_1$. Also ist $f(U_2) \subseteq f(U_1)$, d.h. f ist antiton.
2.) Für $x \neq 0$ gilt

$$|x| \notin U \iff \big(x \in f(U) \text{ oder } x^{-1} \in f(U)\big).$$

BEWEIS. „$\Rightarrow$“: Ist $x \in B$, so folgt $x \in f(U)$ nach Definition von $f(U)$. Ist $x \notin B$, so ist $x^{-1} \in B$. Da U Untergruppe von G ist, gilt mit $|x| \notin U$ auch $|x^{-1}| = |x|^{-1} \notin U$, also ist $x^{-1} \in f(U)$.
„$\Leftarrow$“: Gilt $x \in f(U)$ oder $x^{-1} \in f(U)$, so ist notwendig $|x| \notin U$ oder $|x^{-1}| \notin U$. In beiden Fällen folgt $|x| \notin U$, weil U eine Untergruppe ist. ✓

Durch Kontraposition erhält man für $x \neq 0$

$$(*) \qquad |x| \in U \iff \big(x \notin f(U) \text{ und } x^{-1} \notin f(U)\big).$$

3.) f ist injektiv: Aus $f(U_1) = f(U_2)$ folgt wegen $(*)$

$$|x| \in U_1 \iff |x| \in U_2,$$

also $U_1 = U_2$.
4.) f ist surjektiv: Definiere zu $P \in \mathfrak{P}$

$$U := \{|x| \in G \mid x \neq 0,\ x \notin P,\ x^{-1} \notin P\}.$$

Dann gilt:
(a) U ist eine Untergruppe von G:
Wegen $1 \notin P$ ist $|1| \in U$, also $U \neq \emptyset$. Seien $|x|, |y| \in U$, also $x, y, x^{-1}, y^{-1} \notin P$. Wegen Eigenschaft (P) folgt

$$xy^{-1} \notin P \quad \text{und} \quad yx^{-1} \notin P,$$

also $|xy^{-1}| = |x|\,|y|^{-1} \in U$.
(b) U ist konvex: Seien $|x|, |y| \in U$ und $|z| \in G$ mit

$$|x| \leq |z| \leq |y|.$$

Aus $\quad x = z\,(z^{-1}x) \notin P$ und $z^{-1}x \in B \quad$ folgt $\quad z \notin P$,
aus $\quad y^{-1} = z^{-1}\,(zy^{-1}) \notin P$ und $zy^{-1} \in B \quad$ folgt $\quad z^{-1} \notin P$.

Also ist $|z| \in U$.
(c) Es ist $f(U) = P$: $x \in B$ und $x^{-1} \in P$ führt zu $1 = x^{-1}x \in P$, also zu einem Widerspruch. Damit ist für $x \neq 0$

$$x \in f(U) \iff x \in B \wedge |x| \notin U \iff x \in B \wedge (x \in P \vee x^{-1} \in P) \iff x \in P. \quad \square$$

Sei $\mathfrak{J}$ die Menge der gebrochenen Ideale I bezüglich B. Definiere für $I \in \mathfrak{J}$

$$I^* := \{x \in K \mid 1 \notin xI\}\,.$$

EIGENSCHAFTEN.

(A) Es ist $I^* \in \mathfrak{J}$.

BEWEIS. $x \in I^* \;\Rightarrow\; 1 \notin xI \;\Rightarrow\; 1 \notin xBI^{\dagger} \;\Rightarrow\; xB \subseteq I^* \;\Rightarrow\; I^* \in \mathfrak{J}$ □

(B) $I_1 \subseteq I_2 \quad\Longrightarrow\quad I_2^* \subseteq I_1^*$.

BEWEIS. $x \in I_2^* \;\Rightarrow\; 1 \notin xI_2 \;\Rightarrow\; 1 \notin xI_1 \;\Rightarrow\; x \in I_1^*$.
Also ist $I_2^* \subseteq I_1^*$. □

(C) $I^{**} = I$.

BEWEIS. Sei $x \neq 0$. Dann ist

$$x \notin I \iff 1 \notin x^{-1}I \iff x^{-1} \in I^*\,,$$

also

$$x \in I \iff x^{-1} \notin I^* \iff 1 \notin xI^* \iff x \in I^{**}\,.$$ □

(D) Die Abbildung

$$f : \mathfrak{J} \to \mathfrak{J}\,, \quad I \mapsto f(I) = I^*$$

ist eine antitone Bijektion.

BEWEIS. Wegen (B) ist f antiton. Aus $I_1^* = I_2^*$ folgt

$$I_1 = I_1^{**} = I_2^{**} = I_2\,,$$

also ist f injektiv. Ist $I \in \mathfrak{J}$, so gilt $I = (I^*)^*$. Damit ist f auch surjektiv. □

DEFINITION 8.6. Ein Ring R mit Einselement heißt ein *lokaler Ring*, wenn die nicht invertierbaren Elemente ein Ideal in R bilden.

$$M = \{x \in R \mid x \text{ nicht invertierbar}\}$$

heißt *maximales Ideal* von R. Es enthält jedes echte Ideal I von R, denn ist $x \in I$, so ist x nicht invertierbar, weil andernfalls $1 = xx^{-1} \in I$, also $I = R$ wäre.

BEHAUPTUNG. Jeder Bewertungsring ist ein lokaler Ring. Es ist $M = B^*$.

BEWEIS. Ist $x \in B^*$, so folgt $1 \notin xB$, also $x^{-1} \notin B$. Weil B ein Bewertungsring ist, folgt $x \in B$. Damit ist $B^* \subseteq B$ nach (A) ein Ideal in B. Wegen $1 \notin B^*$ und $1 \in B$ ist B^* sogar ein echtes Ideal. Also enthält B^* nur nicht-intervierbare Elemente. Zu zeigen bleibt noch, daß B^* alle nicht-invertierbaren Elemente von B enthält. Sei also $x \in B$ nicht invertierbar in B. Dann ist $1 \notin xB$, also $x \in B^*$. Damit ist $M = B^*$.
(Nach Satz 8.2 gibt es eine Krullbewertung $|\ |$ mit $B = \{x \in K \mid |x| \leq 1\}$. Dann ist $B^* = M = \{x \in K \mid |x| < 1\}$.) □

[†] Wegen $BI \subseteq I$

FOLGERUNG 8.2. *Es ist* $M^* = B^{**} = B$. *Nach* (B) *gilt für* $I \in \mathfrak{J}$

$$I \subseteq M \quad \Longrightarrow \quad B \subseteq I^* \qquad \textit{und} \qquad B \subseteq I \quad \Longrightarrow \quad I^* \subseteq M\,.$$

SATZ 8.4. *Sei* $\mathfrak{P}$ *die Menge der Primideale von* B *und* $\mathfrak{O}$ *die Menge der Oberringe von* B. *Die Abbildung* $P \mapsto P^*$ *ist eine antitone Bijektion von* $\mathfrak{P}$ *auf* $\mathfrak{O}$.

BEWEIS. 1.) Sei $P \in \mathfrak{P}$. Dann ist $P \subseteq M$, also $P^* \supseteq B$. Nach (A) ist P^* ein gebrochenes Ideal, also bezüglich der Addition eine Gruppe. Zu zeigen bleibt noch, daß P^* auch multiplikativ abgeschlossen ist. Seien also $xy, \in P^*$. Ist $x = 0$ oder $y = 0$, so folgt $xy = 0 \subseteq B \subseteq P^*$. Man kann also $x, y \neq 0$ voraussetzen. Aus $x, y \in P^*$ folgt dann $1 \notin xP$ und $1 \notin yP$, also $x^{-1}, y^{-1} \notin P$. Weil P ein Primideal ist, ist

$$(xy)^{-1} = y^{-1}x^{-1} \notin P\,,$$

also $1 \notin xyP$, d.h. $xy \in P^*$. Damit ist P^* ein Oberring von B.
2.) Sei $B' \in \mathfrak{O}$. Dann ist $B'^* \subseteq M \subsetneqq B$ und $B'^* \in \mathfrak{J}$, also ist B'^* ein echtes Ideal von B. Ist $0 \neq xy \in B'^*$, so folgt

$$1 \notin xyB' \quad \Longrightarrow \quad y^{-1}x^{-1} \notin B'\,,$$

also $x^{-1} \notin B'$ oder $y^{-1} \notin B'$, d.h. $x \in B'^*$ oder $y \in B'^*$. Damit ist $B'^* \in \mathfrak{P}$. □

KOROLLAR 8.3. *Ist der Rang der Krullbewertung gleich* n, *so existieren genau* n *Oberringe von* B. *Die Bewertung ist genau dann reell* (*d.h. vom Rang* 1), *wenn* B *ein maximaler Bewertungsring ist.*

Als Ergänzung zu Satz 8.3 und Satz 8.4 erhält man

SATZ 8.5. *Es gibt eine isotone Bijektion von der Menge* $\mathfrak{U}$ *aller konvexen Untergruppen der Wertegruppe auf die Menge* $\mathfrak{O}$ *aller Oberringe, die explizit durch*

$$U \mapsto B' = \{x \in K \mid |x| \in U\} \cup B$$

gegeben ist.

2. Additive Krullbewertungen

Sei Γ eine additiv geschriebene Gruppe und $\hat{\Gamma} = \Gamma \cup \{\infty\}$ mit

$$\gamma \leq \infty\,, \quad \gamma + \infty = \infty + \gamma = \infty$$

für alle $\gamma \in \Gamma$.

Eine Abbildung

$$\operatorname{ord} : K \to \hat{\Gamma}$$

heißt *additive Krullbewertung*, wenn

(1) $\operatorname{ord} x = \infty \iff x = 0$

(2) $\operatorname{ord}(x + y) \geq \min(\operatorname{ord} x, \operatorname{ord} y)$

(3) $\operatorname{ord} xy = \operatorname{ord} x + \operatorname{ord} y$

für alle $x, y \in K$ gilt.

Jede Krullbewertung läßt sich in eine additive Krullbewertung umschreiben: Sei $|\ | : K \to \Gamma \cup \{0\}$ eine Krullbewertung. Definiere in K

$$a + b := a \cdot b\,, \qquad \text{und} \qquad a \sqsubseteq b \iff a \geq b\,.$$

Hierdurch wird Γ eine additiv geschriebene geordnete Gruppe mit neutralem Element 0 (nach Umbenennung der 1 in 0). Man erweitere Γ zu $\hat{\Gamma} = \Gamma \cup \{\infty\}$ und definiere

$$\operatorname{ord} x = \begin{cases} |x| & \text{für } x \neq 0 \\ \infty & \text{für } x = 0 \end{cases}$$

Für $x, y \in K$ gilt dann

(1) $\operatorname{ord} x = \infty \iff x = 0$

(2) $\operatorname{ord}(x + y) = |x + y| \leq \max(|x|, |y|) = \max(\operatorname{ord} x, \operatorname{ord} y)$, also $\operatorname{ord}(x + y) \sqsupseteq \min(\operatorname{ord} x, \operatorname{ord} y)$.

(3) $\operatorname{ord} xy = |xy| = |x|\,|y| = \operatorname{ord} x \cdot \operatorname{ord} y = \operatorname{ord} x + \operatorname{ord} y$.

Also ist $\operatorname{ord} : K \to \Gamma \cup \{\infty\}$ eine additive Krullbewertung.

Analog ergibt sich aus einer additiven Krullbewertung eine multiplikative Krullbewertung.

Bezüglich einer additiven Krullbewertung ist

$$B = \{x \in K \mid \operatorname{ord} x \geq 0\} \quad \text{und} \quad M = \{x \in K \mid \operatorname{ord} x > 0\}\,.$$

Beispiel. Sei $K = k(x_1, \ldots, x_n)$ mit $x_1, \ldots, x_n$ algebraisch unabhängig über k. $f \neq 0$ aus K besitzt die Darstellung

$$(*) \qquad f(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i^{k_i} \, \frac{g(x_1, \ldots, x_n)}{h(x_1, \ldots, x_n)}\,,$$

wobei $k_i \in \mathbb{Z}$ und g, h zu x_i teilerfremde Polynome sind, $i = 1, \ldots, n$. Definiere

$$\operatorname{ord} f := (k_1, \ldots, k_n) \in \mathbb{Z}^n \qquad \text{für } f \neq 0$$

und

$$\operatorname{ord} f = \infty \qquad \text{für } f = 0\,.$$

$\mathbb{Z}^n$ ist bezüglich der lexikographischen Anordnung und der komponentenweisen Addition eine additiv geschriebene geordnete Gruppe, und ord ist dann eine additive Krullbewertung mit

$$B = \{f \in K \mid \operatorname{ord} f \geq 0\}\,.$$

Die konvexen Untergruppen von $\mathbb{Z}^n$ sind

$$U_r = \{(k_1, \ldots, k_n) \in \mathbb{Z}^n \mid k_1 = \cdots = k_r = 0\}$$

für $r = 0, 1, \ldots, n$ und bilden (vergleiche Kapitel 7) eine Kette

$$U_0 = \mathbb{Z}^n \supset U_1 \supset \cdots \supset U_n = \{0 = (0, \ldots, 0)\}\,.$$

Nach Satz 8.5 gibt es dann n echte Oberringe von B mit

$$B_0 = K \supset B_1 \supset \cdots \supset B_n = B$$

und

$$\begin{aligned} B_r &= \{f \in K \mid \operatorname{ord} f \in U_r\} \cup B \\ &= \{f \in K \mid \operatorname{ord} f = (k_1, \ldots, k_r) \in U_r \text{ oder } \operatorname{ord} f \geq 0\} \end{aligned}$$

für $r = 0, 1, \ldots, n$.

Die Primideale besitzen die Darstellung

$$P_r = \{f \in K \mid \operatorname{ord} f \notin U_r \text{ und } \operatorname{ord} f \geq 0\}$$

für $r = 0, 1, \ldots, n$.

KAPITEL 9

Fortsetzungssatz für Krullbewertungen

Im Beweis des folgenden Satzes benötigen wir das

ZORNSCHE LEMMA. *Jede nicht-leere induktiv geordnete Menge besitzt ein maximales Element.*

Eine Menge $\mathfrak{S}$ heißt *induktiv geordnet*, wenn $\mathfrak{S}$ teilweise geordnet ist und jede linear geordnete Teilmenge von $\mathfrak{S}$ eine obere Schranke in $\mathfrak{S}$ besitzt.

SATZ 9.1. (CHEVALLEY) *Es sei K ein Körper, R_0 ein Teilring von K mit $1 \in R_0$ und I_0 ein echtes Ideal von R_0. Dann existiert ein Bewertungsring von K mit*

$$R_0 \subseteq B \quad \textit{und} \quad I_0 \subseteq M\,,$$

wobei M das maximale Ideal von B ist.

BEWEIS. 1.) Es sei $\mathfrak{S}$ die Menge aller Paare (R, I), wobei R ein Teilring von K, I ein echtes Ideal von R und $R_0 \subseteq R$ sowie $I_0 \subseteq I$ ist. Wegen $(R_0, I_0) \in \mathfrak{S}$ ist $\mathfrak{S}$ nicht leer. Definiere für (R, I), $(R', I') \in \mathfrak{S}$

$$(R, I) \leq (R', I') \quad :\Longleftrightarrow \quad R \subseteq R' \text{ und } I \subseteq I'\,.$$

Hierdurch wird $\mathfrak{S}$ zu einer teilweise geordneten Menge.
$\mathfrak{S}$ ist induktiv geordnet: Sei

$$\cdots \leq (R_i, I_i) \leq \cdots \leq (R_j, I_j) \leq \cdots$$

eine Kette in $\mathfrak{S}$. Definiere

$$R = \bigcup R_i \quad \text{und} \quad I = \bigcup I_i\,.$$

R ist ein Teilring von K und I ein echtes Ideal von R:
Seien $x, y \in R = \bigcup R_i$. Dann gibt es i, j mit $x \in R_i$ und $y \in R_j$. Sei etwa $(R_i, I_i) \leq (R_j, I_j)$, also $R_i \subseteq R_j$. Dann ist $x, y \in R_j$, also $x - y, xy \in R_j \subseteq R$.
Entsprechend zeigt man, daß I ein Ideal ist. Wegen $1 \in R$ und $1 \notin I$ ist I ein echtes Ideal von R.

Nach dem Zornschen Lemma existiert in $\mathfrak{S}$ ein maximales Element (B, I).

2.) B ist ein Bewertungsring von K. Annahme: Es gibt ein $x \in K^\times$ mit $x \notin B$ und $x^{-1} \notin B$. Sei

$$B[x] = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; n \in \mathbb{N}_0,\, a_i \in B \right\}$$

und

$$I[x] = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; n \in \mathbb{N}_0,\, a_i \in I \right\}$$

$I[x]$ ist ein Ideal in $B[x]$. Wegen $x \notin B$ ist B ein echter Teilring von $B[x]$. Weil (B, I) maximales Element in $\mathfrak{S}$ ist, folgt daher $\big(B[x], I[x]\big) \notin \mathfrak{S}$, also $I[x] = B[x]$, also

$$1 \in I[x]\,.$$

Aus $x^{-1} \notin B$ folgt entsprechend

$$1 \in I[x^{-1}]\,.$$

Seien nun n, m minimal gewählt, so daß

(1) $$1 = a_0 + a_1 x + \cdots + a_m x^m\,, \quad a_i \in I \text{ für } i = 0, 1, \ldots, m$$

(2) $$1 = b_0 + b_1 x^{-1} + \cdots + b_n x^{-n}\,, \quad b_i \in I \text{ für } i = 0, 1, \ldots, n$$

gilt. Sei etwa $m \geq n$. Aus (2) folgt

$$(1 - b_0)x^m = b_1 x^{m-1} + \cdots + b_n x^{m-n}\,,$$

und aus (1) folgt

$$1 - b_0 = (1 - b_0)a_0 + \cdots + (1 - b_0)a_m x^m\,,$$

also

(3) $$1 = b_0 + (1 - b_0)a_0 + \cdots + (1 - b_0)a_{m-1}x^{m-1} + a_m(b_1 x^{m-1} + \cdots + b_n x^{m-n})\,.$$

Wegen $1 \notin I$ ist $n, m \geq 1$, und es folgt aus (3)

$$1 = a_0' + \cdots + a_{m-1}' x^{m-1} \qquad \text{mit } a_i' \in I,\ 0 \leq i \leq m-1\,.$$

Dies ist aber ein Widerspruch zur Minimalität von m. Also ist B ein Bewertungsring.

3.) Ist M das maximale Ideal von B, so gilt

$$(B, I) \subseteq (B, M) \in \mathfrak{S}\,.$$

Weil (B, I) maximal in $\mathfrak{S}$ ist, folgt $I = M$. □

Bemerkung. Sei R_0 ein Teilring von K mit $1 \notin R_0$ und I_0 ein echtes Ideal von R_0. Dann ist

$$R_0' = \{n \cdot 1 + x \mid n \in \mathbb{Z},\, x \in R_0\}$$

ein Teilring von K mit $1 \in R_0'$. Da I_0 auch ein echtes Ideal von R_0' ist, existiert nach dem Satz von Chevalley ein Bewertungsring B mit

$$R_0 \subseteq R_0' \subseteq B \quad \text{und} \quad I_0 \subseteq M\,.$$

Folglich kann man in Satz 9.1 die Voraussetzung $1 \in R_0$ fallen lassen.

Mit dem Satz von CHEVALLEY lassen sich jene Körper bestimmen, die nicht-triviale Krullbewertungen besitzen.

BEHAUPTUNG. Gibt es in K einen Teilring R_0 mit $1 \in R_0$, der kein Körper ist, so besitzt K eine nicht-triviale Krullbewertung.

BEWEIS. Sei $x \neq 0$ eine Nichteinheit in R_0. Das Hauptideal $I_0 = xR_0$ ist von 0 und R_0 verschieden, weil $1 \in R_0$ und $x^{-1} \notin R_0$ ist. Nach Satz 9.1 gibt es daher einen Bewertungsring B, so daß $I_0 \subseteq M$, also $M \neq 0$ ist. Damit ist $B \neq K$, also existiert eine nicht-triviale Krullbewertung von K. □

Für den Körper K sind nun drei Fälle möglich:

1. Fall: Ist $\operatorname{char} K = 0$, so ist

$$R_0 = \{n \cdot 1 \mid n \in \mathbb{Z}\}$$

ein solcher Teilring, also existiert eine nicht-triviale Krullbewertung.

2. Fall: Ist $\operatorname{char} K = p$ und existiert ein über $\mathbb{Z}_p$ transzendentes Element $x \in K$, so ist $R_0 = \mathbb{Z}_p[x]$ ein solcher Teilring, d.h. es existiert auch in diesem Fall eine nicht-triviale Krullbewertung.

3. Fall: Ist $\operatorname{char} K = p$ und K algebraisch über $\mathbb{Z}_p$, so existiert keine nicht-triviale Krullbewertung, denn:
Sei $|\ |$ eine Krullbewertung von K und $x \in K^\times$. Weil K algebraisch über $\mathbb{Z}_p$ ist, ist $\mathbb{Z}_p(x)$ ein endlicher Körper. Ist q die Anzahl der Element von $\mathbb{Z}_p(x)$, so ist die multiplikative Gruppe von $\mathbb{Z}_p(x)$ eine Gruppe der Ordnung $q-1$. Nach dem Satz von LAGRANGE ist dann

$$x^{q-1} = 1\,, \quad \text{also} \quad |x|^{q-1} = 1\,.$$

Weil $|x|$ Element einer geordneten Gruppe ist, folgt $|x| = 1$. Also ist $|\ |$ die triviale Bewertung.

ERGEBNIS. Ein Körper besitzt genau dann nur die triviale Krullbewertung, wenn er algebraisch über $\mathbb{Z}_p$ ist.

DEFINITION 9.1. K_2 sei ein Erweiterungskörper von K_1. Eine Bewertung von K_2 heißt eine *Fortsetzung* einer Bewertung von K_1, wenn eine isotone und injektive Abbildung

$$\imath : G_1 \to G_2$$

der Wertegruppen mit

$$|x|_2 = \imath|x|_1$$

für $x \in K_1^\times$ existiert.

HILFSSATZ 9.1. *Sei K_2 eine Erweiterungskörper von K_1 sowie $|\ |_1$ und $|\ |_2$ Bewertungen von K_1 und K_2. $|\ |_2$ ist genau dann eine Fortsetzung von $|\ |_1$, wenn für die zugehörigen Bewertungsringe und maximalen Ideale*

$$B_1 \subseteq B_2 \quad \textit{und} \quad M_1 \subseteq M_2$$

gilt.

BEWEIS. 1.) Sei $|\ |_2$ eine Bewertungsfortsetzung von $|\ |_1$. Dann gilt

$$x \in B_1 \ \Rightarrow\ |x|_1 \leq 1 = |1|_1 \ \Rightarrow\ |x|_2 = \imath|x|_1 \leq \imath|1|_1 = |1|_2 = 1 \ \Rightarrow\ x \in B_2$$

und

$$x \in M_1 \ \Rightarrow\ |x|_1 < |1|_1 \ \Rightarrow\ |x|_2 = \imath|x|_1 < \imath|1|_1 = |1|_2 \ \Rightarrow\ x \in M_2\,,$$

also $B_1 \subseteq B_2$ und $M_1 \subseteq M_2$.
2.) Seien nun $B_1 \subseteq B_2$ und $M_1 \subseteq M_2$. Dann gilt für $x, y \in K^\times$

$$(*) \qquad |x|_1 \leq |y|_1 \iff |x|_2 \leq |y|_2\,.$$

BEWEIS. „⇒“: Es gilt

$$|x|_1 \leq |y|_1 \ \Rightarrow\ \left|\frac{x}{y}\right|_1 \leq 1 \ \Rightarrow\ \frac{x}{y} \in B_1 \subseteq B_2 \ \Rightarrow\ \left|\frac{x}{y}\right|_2 \leq 1 \ \Rightarrow\ |x|_2 \leq |y|_2\,.$$

„⇐“: Der Beweis erfolgt durch Kontraposition. Es gilt

$$|x|_1 > |y|_1 \ \Rightarrow\ \left|\frac{y}{x}\right|_1 < 1 \ \Rightarrow\ \frac{y}{x} \in M_1 \subseteq M_2 \ \Rightarrow\ \left|\frac{y}{x}\right|_2 < 1 \ \Rightarrow\ |x|_2 > |y|_2\,. \quad \checkmark$$

Definiere nun die Abbildung

$$\imath : G_1 \to G_2\,, \quad |x|_1 \mapsto |x|_2 \ \text{ für } x \in K_1^\times\,.$$

Wegen $(*)$ ist $\imath$ wohldefiniert, injektiv und isoton. Also ist $|\ |_2$ eine Bewertungsfortsetzung von $|\ |_1$. □

SATZ 9.2. *Ist K_2 ein Erweiterungskörper von K_1, so gibt es zu jeder Krullbewertung von K_1 eine Fortsetzung auf K_2.*

BEWEIS. Seien B_1 und M_1 der Bewertungsring und das maximale Ideal der Krullbewertung $|\ |_1$ von K_1. Dann ist B_1 ein Teilring von K_2 und M_1 ein echtes Ideal in B_1. Nach Satz 9.1 existiert dann ein Bewertungsring B_2 von K_2 mit

$$B_1 \subseteq B_2 \quad \text{und} \quad M_1 \subseteq M_2\,.$$

Zu B_2 gehört nach Satz 8.2 eine Krullbewertung $|\ |_2$ von K_2, die nach Hilfssatz 9.1 eine Fortsetzung der Bewertung von K_1 ist. □

Bei der Fortsetzung kann sich der Rang einer Krullbewertung ändern. Daher folgt aus diesem Satz nicht unmittelbar Korollar 6.5 über die Fortsetzung reeller nicht-archimedischer Bewertungen auf algebraische Erweiterungskörper. Diese Lücke schließt aber

SATZ 9.3. *Ist $|\ |_2$ eine Fortsetzung von $|\ |_1$ auf eine algebraische Erweiterung K_2 über K_1, so ist der Rang von $|\ |_2$ gleich dem Rang von $|\ |_1$*

Zum Beweis benötigen wir zwei Hilfssätze.

HILFSSATZ 9.2. *Ist $a_1 + \cdots + a_n = 0$ für ein $n \geq 2$ mit $a_i \in K$, $i = 1, \ldots, n$, so werden zwei Summanden gleich bewertet.*

BEWEIS. Sei etwa $|a_i| = \max(|a_1|, \ldots, |a_n|)$. Wäre $|a_i| > |a_j|$ für alle $j \neq i$, so würde

$$|a_i| = \left| -\sum_{\substack{j=1 \\ j\neq i}}^{n} a_j \right| \leq \max_{\substack{1\leq j\leq n \\ j\neq i}} (|a_j|) < |a_j|\,,$$

also ein Widerspruch folgen. □

HILFSSATZ 9.3. *Seien G_1 und G_2 geordnete Gruppen und G_1 eine Untergruppe von G_2. Dann ist*

$$f : \mathfrak{U}_2 \to \mathfrak{U}_1\,, \quad f(U) = U \cap G_1 \text{ für } U \in \mathfrak{U}_2$$

eine isotone und surjektive Abbildung der Menge der konvexen Untergruppen von G_2 auf die Menge der konvexen Untergruppen von G_1. Gibt es zu jedem $a \in G_2$ ein $n \in \mathbb{N}$ mit $a^n \in G_1$, so ist f sogar bijektiv.

BEWEIS. Offenbar ist $U \cap G_1$ für $U \in \mathfrak{U}_2$ eine konvexe Untergruppe von G_1 und f eine isotone Abbildung.
Sei U_1 eine konvexe Untergruppe von G_1. Dann ist

$$U = \{a \in G_2 \mid \exists\, b, c \in U_1 : b \leq a \leq c\}$$

eine konvexe Untergruppe von G_2 und $U_1 = U \cap G_1$. Also ist f surjektiv.
Für $U, U' \in \mathfrak{U}_2$ sei $U \cap G_1 = U' \cap G_1$. Ist $a \in U$, so gibt es nach Voraussetzung ein $n \in \mathbb{N}$ mit $a^n \in G_1$, also

$$a^n \in U \cap G_1 = U' \cap G_1 \subseteq U'\,.$$

Ist $1 \leq a$, so gilt $1 \leq a \leq a^n$, also $a \in U'$ wegen der Konvexität von U'.
Ist $a \leq 1$, so gilt $a^n \leq a \leq 1$, also ebenfalls $a \in U'$. Damit ist $U \subseteq U'$ gezeigt. Aus Symmetriegründen folgt auch $U' \subseteq U$. Insgesamt folgt also $U = U'$, d.h. f ist injektiv. □

BEWEIS VON SATZ 9.3. Man kann annehmen, daß die Wertegruppe G_1 von $|\ |_1$ Untergruppe von G_2 ist. Da K_2 algebraisch über K_1 ist, gibt es zu jedem $x \in K_2^\times$ ein $n \in \mathbb{N}$ und $a_1, \ldots, a_{n-1} \in K_1$ mit

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0\,.$$

Nach Hilfssatz 9.2 gibt es verschiedene Indizes i, j, etwa $i > j$ mit

$$|a_i x^i|_2 = |a_j x^j|_2 \qquad (\text{für } i = n \text{ ist } a_n = 1)\,.$$

Damit ist

$$|x|_2^{i-j} = \left|\frac{a_j}{a_i}\right|_2 = \left|\frac{a_j}{a_i}\right|_1 \in G_1\,.$$

Nach Hilfssatz 9.3 gibt es daher eine isotone Bijektion der konvexen Untergruppen von G_2 auf die konvexen Untergruppen von G_1. Also ist

$$\operatorname{Rang} G_1 = \operatorname{Rang} G_2\,. \quad \square$$

DEFINITION 9.2. Sei R Teilring eines Körpers K. Ein Element $x \in K$ heißt *ganz* über R, wenn eine Gleichung

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

mit $a_1 \ldots, a_n \in R$ besteht. Die Menge aller über R ganzen Elemente von K bezeichnet man als den *ganzen Abschluß* $\bar{R}$ von R. R heißt *ganz-abgeschlossen*, wenn $R = \bar{R}$ ist.

BEHAUPTUNG. Ist K der Quotientenkörper von R, und ist R ein Gaußscher Ring (d.h. ein Ring mit eindeutiger Primfaktorzerlegung), so ist R ganz-abgeschlossen.

BEWEIS. Sei $x \in K$ ganz über R, also

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

mit $a_1, \ldots, a_n \in R$. Sei $x = \frac{a}{b}$ mit $a, b \in R$ teilerfremd. Dann folgt

$$a^n = -(a_1 a^{n-1} + a_2^{n-2} b + \cdots + a_n b^{n-1}) b\,.$$

Ist p ein Primelement, das b teilt, so teilt p auch a, d.h. a und b sind nicht teilerfremd. Es folgt $b = 1$, also $x = a \in R$. Damit ist R ganz-abgeschlossen. □

BEISPIEL. 1.) $\mathbb{Z}$ ist in $\mathbb{Q}$, $k[x]$ in $k(x)$ ganz-abgeschlossen.
2.) $R = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ ist nicht ganz-abgeschlossen in $\mathbb{Q}(\sqrt{-3})$:

$$x = \frac{1}{2}\,(-1 + \sqrt{-3})$$

genügt der Gleichung

$$x^2 + x + 1 = 0\,,$$

ist also ganz über R, liegt jedoch nicht in R. (R ist also auch kein Gaußscher Ring.)

SATZ 9.4. (KRULL 1932) *Ist R ein Teilring von K, so ist der ganze Abschluß $\bar{R}$ gleich dem Durchschnitt aller Bewertungsringe von K, die R enthalten.*

BEWEIS. Sei B ein Bewertungsring von K mit $R \subseteq B$ und $x \neq 0$ aus $\bar{R}$, also

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

mit $a_1, \ldots, a_n \in R$ oder

$$x = -(a_1 + \cdots + a_n x^{1-n})\,.$$

Ist $x^{-1} \in B$, so folgt hieraus $x \in B$. Ist $x^{-1} \notin B$, so folgt ebenfalls $x \in B$, weil B ein Bewertungsring ist. In jedem Fall ist also $x \in B$. Also ist

$$\bar{R} \subseteq \bigcap_{B \supseteq R} B\,.$$

Sei nun $x \notin \bar{R}$ und $R_0 = R[x^{-1}]$. Wäre $x \in R_0$, so würde

$$x = a_0 + a_1 x^{-1} + \cdots + a_{m-1} x^{1-m}$$

mit $a_0, \ldots, a_{m-1}$, also

$$x^m - a_0 x^{m-1} - \cdots - a_{m-1} = 0$$

im Widerspruch zu $x \notin \bar{R}$ folgen. Also ist $x \notin R_0$. Daher ist $x^{-1}R_0$ ein echtes Ideal in R_0. Nach Satz 9.1 gibt es einen Bewertungsring B mit

$$R \subseteq R[x^{-1}] \subseteq B \quad \text{und} \quad x^{-1} \in x^{-1}R_0 \subseteq M\,.$$

Aus $x^{-1} \in M$ folgt $x \notin B$, also $x \notin \bigcap_{B \supseteq R} B$. Damit ist

$$\bar{R} = \bigcap_{B \supseteq R} B\,. \quad \square$$

FOLGERUNGEN. 1.) $\bar{R}$ ist als Durchschnitt von Ringen ein Ring.

2.) Wegen $R \subseteq B \iff \bar{R} \subseteq B$ ist $\bar{\bar{R}} = \bar{R}$.

3.) Die ganz-abgeschlossenen Teilringe von K sind Durchschnitte von Bewertungsringen.

Die Teilbarkeit in einem ganz-abgeschlossenen Ring wird durch die Bewertungen bestimmt: Ist $\bar{R} = \bigcap B_i$ und $|\ |_i$ die Bewertung zu B_i, so gilt für $a, b \in R = \bar{R}$:

$$a|b \iff |b|_i \leq |a|_i \text{ für alle } i\,.$$

KAPITEL 10

Der Approximationssatz

Im folgenden sei K ein Körper mit n Bewertungen $|\ |_1, \ldots, |\ |_n$. Die zugehörigen Wertegruppen bezeichnen wir mit $G_1, \ldots, G_n$, die Bewertungsringe mit $B_1, \ldots, B_n$. Ferner sei

$$R = B_1 \cap \cdots \cap B_n \,.$$

LEMMA 10.1. *Sei $x \in K^\times$. Dann gibt es ein Element $y \in R$ mit*

$$|y|_i = |x|_i \qquad \textit{für die Indizes } i, \textit{ für die } |x|_i \leq 1 \textit{ ist},$$
$$|y|_i \leq |x^{-1}|_i \qquad \textit{für die Indizes } i, \textit{ für die } |x|_i > 1 \textit{ ist}.$$

BEWEIS. (BOURBAKI) Sei $\mathfrak{F}$ die Menge der ganzzahligen Polynome mit höchstem und niedrigstem Koeffizienten 1, also Polynome der Form

$$f(t) = t^k + a_{k-1}t^{k-1} + \cdots + a_1 t + 1\,, \qquad a_i \in \mathbb{Z}\,.$$

Wir wählen aus $\mathfrak{F}$ Polynome $f_1, \ldots, f_n$ in folgender Weise: Gibt es in $\mathfrak{F}$ kein Polynom f mit $|f(x)|_i < 1$, so setzen wird $f_i = 1$. Existieren dagegen für den Index i Polynome mit dieser Eigenschaft, so wählen wir für f_i eines dieser Polynome. Ist

$$F(t) = 1 + t^2 \prod_{j=1}^{n} f_j(t)\,,$$

so definieren wir

$$y = \frac{x}{F(x)}\,.$$

1.) Sei i ein Index mit $|x_i| \leq 1$. Dann ist x und damit auch $F(x)$ ein Element von B_i. Die Annahme $|F(x)|_i < 1$ führt zum Widerspruch:
Wegen $f_i \neq 1$, also

$$\left| x^2 \prod_{j=1}^{n} f_j(x) \right|_i \leq |f_i(x)|_i < 1\,,$$

folgt

$$|F(x)|_i = \left| 1 + x^2 \prod_{j=1}^{n} f_j(x) \right|_i = 1$$

im Widerspruch zur Annahme. Wegen $F(x) \in B_i$ ist $|F(x)|_i = 1$, also

$$|y|_i = \left|\frac{x}{F(x)}\right|_i = |x|_i \,.$$

2.) Sei i ein Index mit $|x|_i > 1$. Ist k der Grad des Polynoms F, so gilt dann $|F(x)|_i = |x^k|_i$, also wegen $k \geq 2$

$$|y|_i = \left|\frac{x}{F(x)}\right|_i = |x^{1-k}|_i \leq |x^{-1}|_i \,.$$

für alle i gilt demnach $|y|_i \leq 1$, also liegt y in R. □

KOROLLAR 10.1. *K ist der Quotientenkörper von R.*

BEWEIS. Sei $x \in K^\times$. Ist etwa

$$|x|_1 \leq 1, \ldots, |x|_k \leq 1, \quad |x|_{k+1}, \ldots, |x|_n > 1 \,,$$

so existiert nach Lemma 10.1 ein $y \in R$ mit

$$|y|_1 \leq 1, \ldots, |y|_k \leq 1, \quad |y|_{k+1} \leq |x^{-1}|_{k+1}, \ldots, |y|_n \leq |x^{-1}|_n \,.$$

Daher liegt xy in R, und es ist $x = \frac{xy}{y}$. □

KOROLLAR 10.2. *Seien ε_i, $i = 1, \ldots, n$, beliebige Elemente aus G_i. Dann gibt es ein $x \in K^\times$ mit $|x|_i \leq \varepsilon_i$.*

BEWEIS. Sei $x_1 \in K$ mit $|x_1|_1 = \varepsilon_1$. Für das in Lemma 10.1 konstruierte y_1 gilt dann

$$|y_1|_1 \leq \varepsilon_1 \qquad \text{und} \qquad |y_1|_j \leq 1 \text{ für } j \neq 1 \,.$$

Entsprechend erhält man $y_2, \ldots, y_n$ mit

$$|y_i|_i \leq \varepsilon_i \qquad \text{und} \qquad |y_i|_j \leq 1 \text{ für } j \neq i \,.$$

Für $x = y_1 \cdots y_n$ gilt dann die Behauptung. □

DEFINITION 10.1. Die Bewertungen $|\ |_1, \ldots, |\ |_n$ heißen *unabhängig*, wenn zu beliebigen $\varepsilon_i \in G_i$ ein $a \in K$ mit

$$|a|_1 = \varepsilon_1, \ldots, |a|_n = \varepsilon_n$$

existiert.

Zum Beweis des Approximationssatzes benötigen wir den folgenden

HILFSSATZ 10.1. *Sind die Bewertungen $|\ |_1, \ldots, |\ |_n$ unabhängig und nicht-trivial, so existiert ein $b \in K$ mit*

$$|b-1|_1 \leq \varepsilon_1, |b|_2 \leq \varepsilon_2, \ldots, |b|_n \leq \varepsilon_n \,.$$

BEWEIS. Man kann $\varepsilon_i < 1$ voraussetzen. Wegen der Unabhängigkeit der Bewertungen existiert ein $a \in K$ mit

$$|a|_1 = \varepsilon_1^{-1} > 1 \quad \text{und} \quad |a|_j = \varepsilon_j < 1 \text{ für } j = 2, \ldots, n\,.$$

Für $b = \frac{a}{1+a}$ ergibt sich

$$|b-1|_1 = \left|\frac{-1}{1+a}\right|_1 = \varepsilon_1\,, \quad \text{und} \quad |b|_j = \left|\frac{a}{1+a}\right|_j = |a|_j = \varepsilon_j \ \text{ für } j = 2, \ldots, n\,. \quad \square$$

SATZ 10.1. (*Approximationssatz*) *Seien* $|\ |_1, \ldots, |\ |_n$ *unabhängige Bewertungen von* K. *Sind* $\varepsilon_i \in G_i$ *und* $a_i \in K$ *beliebig gegeben, so existiert ein* $a \in K$ *mit*

$$|a - a_i|_i \leq \varepsilon_i \qquad \textit{für } i = 1, \ldots, n\,.$$

BEWEIS. Ist eine der Bewertungen, etwa $|\ |_i$ trivial, so ist $G_i = \{1\}$. Die Ungleichung $|a - a_i|_i \leq \varepsilon_i = 1$ gilt dann stets. Man kann daher ohne Beschränkung der Allgemeinheit annehmen, daß sämtliche n Bewertungen nicht-trivial sind.

Wähle nun $\varepsilon_{ij} \in G$, so daß

$$\varepsilon_{ij}\,|a_j|_i \leq \varepsilon_i \qquad \text{für } i = 1, \ldots, n$$

gilt. Nach Hilfssatz 10.1 existieren $b_1, \ldots, b_n$ mit

$$|b_i - 1|_i \leq \varepsilon_{ii}\,, \quad |b_i|_j \leq \varepsilon_{ij} \ \text{ für } j \neq i\,.$$

Für $a = \sum_{i=1}^{n} b_i a_i$ gilt dann

$$|a - a_i|_i = \left|\sum_{j \neq i} b_j a_j + (b_i - 1)a_i\right|_i \leq \max_j\,(\varepsilon_{ij}|a_j|_i) \leq \varepsilon_i\,. \quad \square$$

BEMERKUNG. Die im Beweis des Approximationssatzes gemachte Voraussetzung der Unabhängigkeit der Bewertungen ist sogar notwendig, wie folgende Überlegung zeigt: Seien $|\ |_1, \ldots, |\ |_n$ nicht-triviale Bewertungen, für die der Approximationssatz gilt, und $\varepsilon_i \in G_i$, $i = 1, \ldots, n$. Wir wählen zu jedem Index i ein $a_i \in K$ mit $|a_i|_i = \varepsilon_i$ und ein $\varepsilon_i' \in G_i$ mit $\varepsilon_i' < \varepsilon_i$, was wegen $G_i \neq \{1\}$ möglich ist. Nach dem Approximationssatz gibt es ein $a \in K$ mit $|a - a_i|_i \leq \varepsilon_i' < \varepsilon_i$. Dann gilt $|a|_i = |a_i|_i = \varepsilon_i$. Dies zeigt, daß die Bewertungen unabhängig sind.

Im folgenden untersuchen wir die Frage, unter welchen Bedingungen Bewertungen unabhängig sind, und beweisen zuerst

SATZ 10.2. *Die Bewertungen* $|\ |_1, \ldots, |\ |_n$ *sind unabhängig, wenn sie paarweise unabhängig sind.*

BEWEIS. 1.) Ist eine der gegebenen Bewertungen die triviale Bewertung, so kann in diesem Fall nur der Wert 1 vorgegeben werden, da die Wertegruppe nur aus dem Einselement besteht. Dieser Wert wird aber von jedem von Null verschiedenen Körperelement angenommen. Triviale Bewertungen brauchen daher nicht berücksichtigt zu werden. Wir können der Einfachheit annehmen, daß die gegebenen Bewertungen nicht-trivial sind.

2.) Seien $\varepsilon_i \in G_i$, $i = 1, \ldots, n$ gegeben. Wir nehmen zuerst $\varepsilon_i \leq 1$ an.

Da $|\ |_2$ nicht-trivial ist, gibt es ein $\varepsilon_2' \in G_2$ mit $\varepsilon_2' < \varepsilon_2$ und, da nach Voraussetzung $|\ |_1$ und $|\ |_2$ unabhängig sind, ein $x \in K$ mit $|x|_1 = \varepsilon_1$, $|x|_2 = \varepsilon_2' < \varepsilon_2$. Nach Lemma 10.1 existiert ein $y_2 \in K$ mit

$$|y_2|_1 = \varepsilon_1\,, \quad |y_2|_2 < \varepsilon_2\,, \quad |y_2|_k \leq 1 \text{ für } k = 3, \ldots, n\,.$$

Entsprechend zeigt man die Existenz von $y_3, \ldots, y_n$ mit

$$|y_i|_1 = 1\,, \quad |y_i|_i < \varepsilon_i\,, \quad |y_i|_k \leq 1 \text{ für } k \neq 1, i\,.$$

Ist $z_1 = y_2 \cdot \ldots \cdot y_n$, so gilt

$$|z_1|_1 = \varepsilon_1\,, \quad |z_1|_k < \varepsilon_k \text{ für alle } k \neq 1\,.$$

Entsprechend folgt die Existenz von $z_2, \ldots, z_n$ mit

$$|z_i|_i = \varepsilon_i\,, \quad |z_i|_k < \varepsilon_k \text{ für alle } k \neq i\,.$$

Setzt man nun $a = z_1 + \cdots + z_n$, so gilt

$$|a|_i = \varepsilon_i \quad \text{für } i = 1, \ldots, n\,.$$

3.) Wir betrachten nun den allgemeinen Fall. Sei etwa

$$\varepsilon_1 \leq 1, \ldots, \varepsilon_k \leq 1, \ \ \varepsilon_{k+1} > 1, \ldots, \varepsilon_n > 1\,.$$

Wie oben gezeigt wurde, existieren dann $x, y \in K$ mit

$$|x|_1 = \varepsilon_1, \ldots, |x|_k = \varepsilon_k, \ \ |x|_{k+1} = 1, \ldots, |x|_n = 1$$

und

$$|y|_1 = 1, \ldots, |y|_k = 1, \ \ |y|_{k+1} = \varepsilon_{k+1}^{-1}, \ldots, |y|_n = \varepsilon_n^{-1}\,.$$

Für $a = \frac{x}{y}$ gilt dann $|a|_i = \varepsilon_i$, $i = 1, \ldots, n$. □

Es bleibt nun die Frage, wann zwei Bewertungen unabhängig sind. Bevor wir in Satz 10.3 eine Antwort hierauf geben, beweisen wir zwei Hilfssätze.

HILFSSATZ 10.2. *Folgende Aussagen sind äquivalent:*

(1) *Zu jedem $\varepsilon_1 \in G_1$, $\varepsilon_1 \leq 1$, gibt es ein $x \in K$ mit*

$$|x|_1 \leq \varepsilon_1\,, \qquad |x|_2 \geq 1\,,$$

(2) *Zu jedem $\varepsilon_1 \in G_1$, $\varepsilon_1 \leq 1$, gibt es ein $x \in K$ mit*

$$|x|_1 = \varepsilon_1\,, \qquad |x|_2 \geq 1\,,$$

(3) *Zu jedem $\varepsilon_1 \in G_1$, $\varepsilon_1 \leq 1$, gibt es ein $x \in K$ mit*

$$|x|_1 = \varepsilon_1\,, \qquad |x|_2 = 1\,,$$

(4) *Zu $\varepsilon_1 \in G_1$, $\varepsilon_2 \in G_2$ gibt es ein $x \in K$ mit*

$$|x|_1 = \varepsilon_1\,, \qquad |x|_2 = \varepsilon_2\,.$$

(*d.h. die Bewertungen $|\ |_1$ und $|\ |_2$ sind unabhängig.*)

BEWEIS. (1) $\Rightarrow$ (2): Nach (1) gibt es ein $z \in K$ mit

$$|z|_1 \leq \varepsilon_1\,, \qquad |z|_2 \geq 1\,.$$

Da jedes Element von G_1 als Wert eines Elementes aus K auftritt, gibt es ferner ein $u \in K$ mit $|u|_1 = \varepsilon_1$. Ist $|u|_2 \geq 1$, so setze $x = u$, ist $|z|_1 = \varepsilon_1$, so setze $x = z$. Ist aber $|u|_2 < 1$ und $|z|_1 < \varepsilon_1$, so gilt (2) für $x = u + z$.

(2) $\Rightarrow$ (3): Wir unterscheiden drei Fälle:

(a) Sei $\varepsilon_1 < 1$.

Nach (2) gibt es ein z mit $|z|_1 = \varepsilon_1 < 1$ und $|z|_2 \geq 1$. Ist $|z|_2 = 1$, so gilt (3) für $x = z$. Ist $|z|_2 > 1$, so gilt (3) für $x = \frac{z}{1+z}$.

(b) Sei $\varepsilon_1 = 1$. Dann gilt (3) für $x = 1$.

(c) Sei $\varepsilon_1 > 1$.

Dann gibt es, wie unter (a) gezeigt wurde, ein z mit $|z|_1 = \varepsilon_1^{-1}$ und $|z|_2 = 1$. Für $x = z^{-1}$ gilt dann (3).

(3) $\Rightarrow$ (4) Es gibt ein $y \in K$ mit $|y|_2 = \varepsilon_2$. Sei $|y|_1 = \alpha_1$. Nach (3) existiert ein z mit $|z|_1 = \varepsilon_1 \alpha_1^{-1}$ und $|z|_2 = 1$. Für $x = yz$ gilt dann (4).

(4) $\Rightarrow$ (1): Trivial. □

HILFSSATZ 10.3. *Seien B_1 und B_2 Bewertungsringe von K mit den maximalen Idealen M_1 und M_2. Dann ist*

$$P = \{x \in K \mid xB_1 \subseteq M_2\}$$

ein Primideal von B_1 und von B_2.

BEWEIS. 1.) P ist ein Ideal von B_1:

Aus $x \in P$ folgt $(xB_1)B_1 \subseteq xB_1 \subseteq M_2$, also $xB_1 \subseteq P$. Damit ist P ein gebrochenes Ideal bezüglich B_1. Es gilt sogar $P \subseteq B_1$. Denn wäre $x \in P$, aber $x \notin B_1$, so würde $x^{-1} \in B_1$, also $1 = xx^{-1} \in M_2$ folgen.

2.) Seien nun $x, y \in K$ mit $xy \in P$. Ist $y \notin P$, so folgt $yB_1 \not\subseteq M_2$. Es gibt daher ein $b \in B_1$ mit $yb \notin M_2$, also $(yb)^{-1} \in B_2$. Dann ist

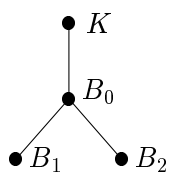
$$xB_1 \subseteq xyb(yb)^{-1}B_1 \subseteq xyB_1 \cdot B_2 \subseteq M_2 \cdot B_2 \subseteq M_2\,,$$

also $x \in P$.

3.) P ist ein Ideal von B_2:

Wegen $1 \in B_1$ ist $P \subseteq M_2$. Wäre $x \in P$, $y \in B_2$, aber $xy \notin P$, so würde aus $x = (xy)y^{-1} \in P$ folgen, daß $y^{-1} \in P \subseteq M_2$, also $y \notin B_2$ ist. □

SATZ 10.3. *Seien $|\ |_1$ und $|\ |_2$ Bewertungen von K mit den Bewertungsringen B_1 und B_2. Die Bewertungen sind genau dann abhängig, wenn es einen Bewertungsring $B_0 \neq K$ mit $B_1, B_2 \subseteq B_0$ gibt.*



BEWEIS. 1.) Sei $B_0 \neq K$ ein Bewertungsring mit $B_1, B_2 \subseteq B_0$. Das maximale Ideal P von B_0 ist ein Primideal von B_1 und B_2. Wegen $B_0 \neq K$ ist $P \neq 0$. Sei $x_0 \in P$, $x_0 \neq 0$, und $|x_0|_1 = \varepsilon_1$. Dann gibt es kein $x \in K$ mit $|x|_1 = \varepsilon_1$ und $|x|_2 = 1$. Würde nämlich ein solches x existieren, so wäre $|x_0^{-1}x|_1 = 1$, also $x_0^{-1}x \in B_1$, also

$x = x_0(x_0)^{-1} \in P \subseteq M_2$ im Widerspruch zu $|x|_2 = 1$.

2.) Nach Satz 8.4 entspricht dem in Hilfssatz 10.3 definierten Primideal P eindeutig ein Bewertungsring B_0, der B_1 und B_2 umfaßt. Nehmen wir an, daß es außer K keinen solchen Bewertungsring gibt, so ist P notwendig das Nullideal, also

$$P = \{x \in K \mid xB_1 \subseteq M_2\} = 0\,.$$

Sei $\varepsilon_1 \in G_1$, $\varepsilon_1 \leq 1$ und $z \in B_1$, $|z|_1 = \varepsilon_1$. Es ist $z \neq 0$, also $z \notin P$. Es gibt daher ein $b \in B_1$, so daß $x = zb \notin M_2$, also

$$|x|_1 = |z|_1\,|b|_1 \leq \varepsilon_1 \quad \text{und} \quad |x|_2 \geq 1$$

gilt. Damit ist die Aussage (1) von Hilfssatz 10.2 erfüllt. Die Bewertungen $|\ |_1$ und $|\ |_2$ sind daher unabhängig. □

Da die Bewertungsringe der Bewertungen vom Rang 1 maximal sind, ergibt sich folgendes

KOROLLAR 10.3. *Bewertungen vom Rang* 1, *d.h. reelle nicht-archimedische Bewertungen sind genau dann unabhängig, wenn die Bewertungsringe paarweise verschieden sind.*

Topologische Betrachtungen. Ist $|\ |$ eine Bewertung eines Körpers K, so wird durch

$$\mathfrak{U} = \{U_\varepsilon \mid \varepsilon \in G\}, \qquad U_\varepsilon = \{x \in K \mid |x| \leq \varepsilon\}$$

eine Umgebungsbasis der Null und damit ein Topologie τ festgelegt, bezüglich der K ein topologischer Körper ist.

Jedes von Null verschiedene Ideal ist eine Umgebung der Null. Ist $x \neq 0$ und $|x| = \varepsilon$, so gilt $U_\varepsilon = xB$, d.h. die gebrochenen Hauptideale xB, $x \neq 0$, bilden gerade die oben angegebene Umgebungsbasis der Null.

SATZ 10.4. *Zwei nicht-triviale Bewertungen* $|\ |_1$ *und* $|\ |_2$ *induzieren genau dann die gleiche Topologie, wenn sie abhängig sind.*

BEWEIS. 1.) Die induzierten Topologien τ_1 und τ_2 seien gleich. M_2 ist eine Nullumgebung bezüglich τ_2, also auch bezüglich τ_1. Es gibt daher ein $x \neq 0$ mit

$$xB_1 \subseteq M_2\,.$$

Damit ist das Primideal $P = \{x \in K \mid xB_2 \subseteq M_2\}$ vom Nullideal verschieden. Ihm entspricht nach Satz 8.4 ein Bewertungsring $B_0 \neq K$, der Oberring von B_1 und B_2 ist.

2.) Seien $|\ |_1$ und $|\ |_2$ abhängig und $P \neq 0$ das B_1 und B_2 gemeinsame Primideal. Dann ist $\{xP \mid x \in K^\times\}$ eine Nullumgebungsbasis für τ_1 und für τ_2. □

BEMERKUNG. Bewertungen, deren Bewertungsringe in einem maximalen Bewertungsring liegen (beispielsweise Bewertungen endlichen Ranges), induzieren die gleichen Topologien wie reelle nicht-archimdische Bewertungen. Eine hiervon verschiedene Klasse von Topologien erhält man durch Bewertungen, deren Bewertungsringe in keinem maximalen Bewertungsring enthalten sind.

Der folgende Satz ist nur eine Umformulierung des Approximationssatzes.

SATZ 10.5. *Sind die von den Bewertungen* $|\ |_1, \ldots, |\ |_n$ *induzierten Topologien* $\tau_1, \ldots, \tau_n$ *sämtlich verschieden und* $\mathcal{O}_\backslash$ *nicht-leere bezüglich* τ_i *offene Teilmengen von* K*, dann gilt*

$$\mathcal{O}_\infty \cap \cdots \cap \mathcal{O}_\backslash \neq \emptyset..$$

BEWEIS. Nach Satz 10.4 sind die Bewertungen paarweise unabhängig, nach Satz 10.2 also unabhängig. Wir wählen $a_i \in \mathcal{O}_\backslash$ und $\varepsilon_i \in G_i$, so daß

$$A_i = \{x \in K \mid |x - a_i|_i \leq \varepsilon_i\}$$

in $\mathcal{O}_\backslash$ enthalten ist. Nach Satz 10.1 existiert ein $a \in K$ mit $|a - a_i|_i \leq \varepsilon_i$ für $i = 1, \ldots, n$, also

$$a \in \bigcap_{i=1}^{n} A_i \subseteq \bigcap_{i=1}^{n} \mathcal{O}_i\,.$$

Damit ist dieser Durchschnitt nicht leer. □

BEMERKUNG. Aus Satz 10.5 folgt umgekehrt der Approximationssatz:
Die Mengen

$$U_i = \{x \in K \mid |x - a_i|_i < \varepsilon_i\}$$

sind offen bezüglich τ_i. Ein Element $a \in \bigcap_{i=1}^{n} U_i$ genügt dann den Ungleichungen

$$|a - a_i|_i < \varepsilon_i$$

für $i = 1, \ldots, n$.

KAPITEL 11

Prüferringe

über Sei R ein Ring und I ein Ideal von R. Unter einer Kongruenz

$$x \equiv y \bmod I$$

versteht man die Aussage $x - y \in I$. Da jeder Kongruenz eine Gleichung im Restklassenring R/I entspricht, kann man Kongruenzen wie Gleichungen behandeln. Es gelten die Regeln

$$x_1 \equiv y_1 \bmod I,\ x_2 \equiv y_2 \bmod I \quad \Longrightarrow \quad \begin{cases} x_1 + x_2 \equiv y_1 + y_2 & \bmod I \\ x_1 x_2 \equiv y_1 y_2 & \bmod I \end{cases}$$

Außerdem gilt, falls $I_1 \subseteq I_2$ ist,

$$x \equiv y \bmod I_1 \quad \Longrightarrow \quad x \equiv y \bmod I_2\,.$$

Ein Kriterium für die Lösbarkeit von Kongruenzsysteme liefert der chinesische Restsatz, der im Spezialfall $R = \mathbb{Z}$ bereits chinesischen Mathematikern bekannt war, die ihn für die Berechnung von Horoskopen benutzten.

Chinesischer Restsatz. *Für $i = 1, \ldots, n$ seien a_i Elemente aus R und I_i Ideale von R. Das Kongruenzsystem*

$$x \equiv a_1 \bmod I_1\,, \quad \ldots\,, \quad x \equiv a_n \bmod I_n$$

besitzt genau dann eine Lösung, wenn jeweils zwei der Kongruenzen eine Lösung besitzen.

Für die Lösbarkeit zweier Kongruenzen läßt sich leicht ein Kriterium aufstellen: Folgendes Aussagen sind äquivalent:

(1) Die Kongruenzen

$$x \equiv a_i \bmod I_i \quad \text{und} \quad x \equiv a_j \bmod I_j$$

besitzen eine Lösung.

(2) Es gilt

$$(*) \qquad a_i \equiv a_j \bmod (I_i + I_j)\,.$$

BEWEIS. (1) $\Rightarrow$ (2): Aus $x - a_i \in I_i$ und $x - a_j \in I_j$ folgt

$$a_i - a_j = (a_i - x) + (x - a_j) \in I_i + I_j \,.$$

(2) $\Rightarrow$ (1): Aus $(*)$ folgt $a_i - a_j = u_1 + u_2$ mit $u_1 \in I_i$ und $u_2 \in I_j$. Dann ist

$$x = a_i - u_1 = a_j + u_2$$

Lösung beider Kongruenzen. $\square$

Ein besonders einfacher Fall liegt vor, wenn die beiden Ideale teilerfremd sind, d.h. wenn $I_i + I_j = R$ ist. In diesem Fall ist die Bedingung $(*)$ unabhängig von a_i und a_j erfüllt, die Kongruenzen sind dann stets lösbar.

Aus der elementaren Zahlentheorie ist der chinesische Restsatz für $R = \mathbb{Z}$ bekannt. Wir werden im folgenden untersuchen, für welche weiteren Ringe der chinesische Restsatz gilt.

DEFINITION 11.1. Der Idealverband eines Ringes R heißt *distributiv*, wenn

$$I \cap (K + L) = (I \cap K) + (I \cap L)$$

für alle Ideale I, K, L von R gilt.

SATZ 11.1. *Der chinesische Restsatz gilt genau dann in einem Ring R, wenn der Idealverband von R distributiv ist.*

BEWEIS. 1.) In R gelte der chinesische Restsatz. Da

$$I \cap (K + L) \supseteq (I \cap K) + (I \cap L)$$

allgemein gilt, ist nur

$$I \cap (K + L) \subseteq (I \cap K) + (I \cap L)$$

zu zeigen. Das Kongruenzsystem

$$x \equiv 0 \bmod I \,, \quad x \equiv 0 \bmod K \,, \quad x \equiv a \bmod L$$

besitzt für $a \in I \cap (K + L)$ wegen

$$a - 0 \in K + L \,, \quad a - 0 \in L + I \,, \quad 0 - 0 \in I + K$$

eine Lösung x. Dann ist $x \in I \cap K$ und $a - x \in I \cap L$, also

$$a = x + (a - x) \in (I \cap K) + (I \cap L) \,.$$

2.) Sei nun der Idealverband von R distributiv. Wir führen einen Induktionsbeweis nach der Anzahl n der Kongruenzen. Der Induktionsanfang für $n = 1$ und $n = 2$ ist klar. Sei also $n > 2$. Für $k = 2, \ldots, n$ löse man zuerst

$$b_k \equiv a_1 \bmod I_1 \,, \quad b_k \equiv a_k \bmod I_k \,. \tag{1}$$

Das System von $n - 1$ Kongruenzen

$$x \equiv b_2 \bmod (I_1 \cap I_2) \,, \quad \ldots \,, \quad x \equiv b_n \bmod (I_1 \cap I_n) \tag{2}$$

ist dann nach Induktion lösbar. Hierzu zeigen wir, daß die Lösbarkeitsbedingungen $(*)$ erfüllt sind: Es ist

$$b_i - b_j = (b_i - a_1) + (a_1 - b_j) \in I_1$$

und

$$b_i - b_j = (b_i - a_i) + (a_i - b_j) \in I_i + I_j\,, \quad i, j \geq 2\,,$$

also

$$b_i - b_j \leq I_1 \cap (I_i + I_j) = (I_1 \cap I_i) + (I_1 \cap I_j)\,,$$

da die Gültigkeit des Distributivgesetzes vorausgesetzt ist. Ist x eine Lösung von (2), so folgt

$$x \equiv b_2 \equiv a_1 \bmod I_1 \quad \text{und} \quad x \equiv b_k \equiv a_k \bmod I_k \ \text{ für } k = 2, \ldots, n\,. \quad \square$$

Bemerkung. Satz 11.1 gilt für beliebige, auch nicht-kommutative Ringe. Im folgenden soll R wieder ein Integritätsbereich sein.

Quotientenbildung. Sei R ein Integritätsbereich und K der Quotientenkörper von R. Ist S eine nicht-leere multiplikativ abgeschlossene Teilmenge von R, die nicht die Null enthält, so ist

$$RS^{-1} := \{as^{-1} \mid a \in R,\, s \in S\}$$

ein Teilring von K, der R umfaßt.

Beweis. Wegen $a = (as)\, s^{-1}$ liegt R in RS^{-1}. Aus $as^{-1}, br^{-1} \in RS^{-1}$ folgt

$$as^{-1} - br^{-1} = (ar - bs)\,(sr^{-1}) \in RS^{-1}$$

und

$$as^{-1} \cdot br^{-1} = ab(sr)^{-1} \in RS^{-1}\,.$$

Also ist RS^{-1} ein Teilring von K. $\square$

Ist I ein Ideal von R, so prüft man leicht nach, daß

$$IS^{-1} = \{as^{-1} \mid a \in I,\, s \in S\}$$

ein Ideal von RS^{-1} ist.

Darüberhinaus ist

$$I \mapsto IS^{-1}$$

eine surjektive Abbildung des Idealverbandes von R auf den Idealverband von RS^{-1}, und es gilt

$$(I_1 + I_2)S^{-1} = I_1S^{-1} + I_2S^{-1} \quad \text{und} \quad (I_1 \cap I_2)S^{-1} = I_1S^{-1} \cap I_2S^{-1}\,.$$

BEWEIS. 1.) Die Abbildung ist surjektiv: Sei I' ein Ideal von RS^{-1}. Dann ist $I = I' \cap R$ ein Ideal von R. Wir zeigen $I' = IS^{-1}$.
Sei $x \in I'$. Wegen $I' \subseteq RS^{-1}$ besitzt x eine Darstellung $x = as^{-1}$ mit $a \in R$ und $s \in S$. Dann ist

$$a = xs \in I' \cap R\,,$$

also $x = as^{-1} \in IS^{-1}$.
Ist umgekehrt $x = as^{-1} \in IS^{-1}$, so folgt

$$x = a \cdot (ss^{-2}) \in I' \cdot RS^{-1} \subseteq I'\,.$$

2.) Der Nachweis, daß die Verbandsoperationen bei der Abbildung erhalten bleiben, macht keine Schwierigkeit. Als Beispiel soll der Beweis von

$$I_1S^{-1} \cap I_2S^{-1} \subseteq (I_1 \cap I_2)S^{-1}$$

ausgeführt werden:
Sei $x \in I_1S^{-1} \cap I_2S^{-1}$, also $x = as^{-1} = br^{-1}$ mit $a \in I_1$, $b \in I_2$ und $r, s \in S$. Dann ist $c = ar = bs \in I_1 \cap I_2$, also

$$x = c\,(sr)^{-1} \in (I_1 \cap I_2)S^{-1}\,. \quad \square$$

BEMERKUNG. Man beachte, daß die Abbildung im allgemeinen nicht injektiv ist. Ist $I \cap S \neq \emptyset$, so enthält IS^{-1} eine Einheit. Damit gilt in diesem Fall $IS^{-1} = RS^{-1}$. Durch die Quotientenbildung vereinfacht sich die Idealstruktur des Ringes.

Wir interessieren uns im weiteren für folgenden Spezialfall der Quotientenbildung: Die *Nennermenge* sei $S = R \setminus P$, wobei P ein Primideal von R ist. Es ergibt sich leicht, daß S multiplikativ abgeschlossen ist. Wir schreiben in diesem Fall

$$R_P = RS^{-1} \qquad \text{und} \qquad I_P = IS^{-1}\,.$$

R_P ist ein lokaler Ring mit dem maximalen Ideal

$$P' = P_P = \{as^{-1} \mid a \in P,\ , s \in R \setminus P\}\,.$$

(Wegen dieser Eigenschaft spricht man von R_P als der *Lokalisierung* von R nach dem Primideal P.)

BEWEIS. Ein lokaler Ring ist nach Definition ein Ring, dessen Nichteinheiten ein Ideal bilden. Aus $bs^{-1} \notin P'$ folgt $b \notin P'$, also $b \notin P$. Also ist $b \in R \setminus P$ und damit bs^{-1} invertierbar in R_P. Alle Nichteinheiten von R_P liegen daher in P'. Aber P' enthält nur Nichteinheiten, da P' ein echtes Ideal von R_P ist (denn wäre $1 \in P'$, also $1 = bs^{-1}$ mit $b \in P$, $s \in R \setminus P$, so würde $b = s$, also ein Widerspruch folgen). P' ist daher gleich der Menge der Nichteinheiten von RS^{-1}. Diese bilden also ein Ideal. $\square$

Mit Hilfe des Zornschen Lemmas zeigt man

HILFSSATZ 11.1. *Jedes echte Ideal eines Ringes mit* 1 *liegt in einem maximalen Ideal.*

SATZ 11.2. *Ist $\mathfrak{M}$ die Menge der maximalen Ideale von R und I ein Ideal von R, so gilt*

$$I = \bigcap_{P \in \mathfrak{M}} I_P\,.$$

BEWEIS. Offensichtlich gilt $I \subseteq \bigcap_{P\in\mathfrak{M}} I_P$. Wir zeigen die umgekehrte Inklusion: Sei $a \in I_P$ für alle $P \in \mathfrak{M}$, also

$$a = x_P s_P^{-1} \qquad \text{mit } x_P \in I,\ s_P \in R \setminus P\,,$$

d.h. zu jedem $P \in \mathfrak{M}$ gibt es ein $s_P \in R \setminus P$ mit $as_P \in I$. Sei C das von den s_P, $P \in \mathfrak{M}$, erzeugte Ideal, also

$$C = \left\{ \sum_{\text{endlich}} b_P s_P \,\middle|\, b_P \in R \right\}.$$

Wäre C ein echtes Ideal, so würde nach Hilfssatz 11.1 $C \subseteq P$ für ein $P \in \mathfrak{M}$ gelten. Damit wäre aber $s_P \in P$ im Widerspruch zu $s_p \in R \setminus P$. Es gilt also $C = R$ und damit

$$1 = b_1 s_{P_1} + \cdots + b_n s_{P_n}$$

also

$$s = b_1 a s_{P_1} + \cdots + b_n a s_{P_n} \in I\,. \quad \square$$

KOROLLAR 11.1. *Es ist*

$$R = \bigcap_{P\in\mathfrak{M}} R_P\,.$$

KOROLLAR 11.2. *Gilt $I_P \subseteq J_P$ für alle $P \in \mathfrak{M}$, so ist $I \subseteq J$.*

BEWEIS. Es ist

$$I = \bigcap_{P\in\mathfrak{M}} I_P \subseteq \bigcap_{P\in\mathfrak{M}} J_P = J\,. \quad \square$$

KOROLLAR 11.3. *Gilt $I_P = J_P$ für alle $P \in \mathfrak{M}$, so ist $I = J$.*

KOROLLAR 11.4. *Besitzen die Ringe R_P für alle $P \in \mathfrak{M}$ einen distributiven Idealverband, so besitzt R selbst einen distributiven Idealverband.*

BEWEIS. Aus

$$\begin{aligned}\big(I \cap (K+L)\big)_P &= I_P \cap (K_P + L_P)\\ &= (I_P \cap K_P) + (I_P \cap L_P)\\ &= \big(I \cap K) + (I \cap L)\big)_P\end{aligned}$$

für alle $P \in \mathfrak{M}$ folgt

$$I \cap (K+L) = (I \cap K) + (I \cap L)$$

nach Korollar 11.3 $\square$

DEFINITION 11.2. Sei R ein Integritätsbereich und K sein Quotientenkörper. R heißt *Prüferring*, wenn R_P für jedes $P \in \mathfrak{M}$ ein Bewertungsring ist.

SATZ 11.3. *R ist genau dann ein Prüferring, wenn der Idealverband von R distributiv ist.*

BEWEIS. 1.) Sei R ein Prüferring. Weil die Menge der Ideale eines Bewertungsringes durch Inklusion linear geordnet ist, besitzt R_P für alle $P \in \mathfrak{M}$ einen distributiven Idealverband. Nach Korollar 11.4 gilt dies dann auch für R.

2.) Der Idealverband von R sei distributiv. Um zu zeigen, daß R_P für $R \in \mathfrak{M}$ ein Bewertungsring von K ist, sei $x \in K^\times$ beliebig gewählt. Wir haben zu zeigen, daß x oder x^{-1} in R_P liegt. Weil K der Quotientenkörper von R ist, gilt $x = ab^{-1}$ mit $a, b \in R$. Wegen

$$a \in aR \cap \big((a-b)R + bR\big) = aR \cap (a-b)R + aR \cap bR^{\dagger}$$

ist

$$a = c\,(a-b) + db = ea + db$$

mit $c, d, e \in R$. Es folgt

$$(1-c)\,a = (d-c)\,b \quad \text{und} \quad cb = (c-e)\,a\,.$$

Ist $c \notin P$, so folgt

$$x^{-1} = ba^{-1} = (c-e)\,c^{-1} \in R_P\,.$$

Ist dagegen $c \in P$, so folgt $1 - c \notin P$ und damit

$$x = ab^{-1} = (d-c)\,(1-c)^{-1} \in R_P\,.$$

Also ist R_P ein Bewertungsring. □

SATZ 11.4. *Jeder Prüferring ist ganz-abgeschlossen.*

BEWEIS. Nach Korollar 11.2 ist $R = \bigcap_{P \in \mathfrak{M}} R_P$. Also ist R Durchschnitt von Bewertungsringen und daher nach Satz 9.4 ganz-abgeschlossen. □

Daß die Umkehrung von Satz 11.4 nicht gilt, zeigt folgendes

BEISPIEL. Sei $R = K[x, y]$ der Polynomring in zwei Unbestimmten über einem Körper K. R ist nach dem Satz von GAUSS ein Gaußscher Ring und daher ganz abgeschlossen (siehe Kapitel 9). R ist jedoch kein Prüferring, da der Idealverband von R nicht distributiv ist. Es ist nämlich

$$(x+y)R \cap (xR + yR) = (x+y)R\,.$$

Das Ideal

$$(x+y)R \cap xR + (x+y)R \cap yR = x\,(x+y)R + y\,(x+y)R$$

enthält dagegen keine Polynome vom Grad 1, ist also von dem obigen Ideal verschieden.

BEMERKUNG. Ohne Beweis sei erwähnt, daß Ringe, in denen die endlich erzeugten Ideale invertierbar sind, Prüferringe sind. Beispiele für Prüferringe sind daher

1.) Dedekindringe (d.h. die Hauptordnungen algebraischer Zahlkörper),

2.) Bezoutringe.

Ein *Bezoutring* ist ein Ring mit folgender Eigenschaft

(B) Jedes endlich erzeugte Ideal ist ein Hauptideal.

---

†Der Idealverband von R ist distributiv

Beispiel eines Bezoutringes ist der Ring $H(G)$ der in einem Gebiet G holomorphen Funktionen. Daß $H(G)$ der Bedingung (B) genügt, ist eine Folgerung des Weierstraßschen Produktsatzes (Satz von HELMER).

SATZ 11.5. *Sei R ein Prüferring in K und $\mathfrak{P}$ die Menge der Primideale von R und $\mathfrak{B}$ die Menge der Bewertungsringe $B \supseteq R$. Die Abbildung*

$$f : \mathfrak{P} \to \mathfrak{B}\,, \quad P \mapsto R_P$$

ist eine antitone Bijektion mit der Umkehrabbildung

$$g : \mathfrak{B} \to \mathfrak{P}\,, \quad B \mapsto M_B \cap R\,,$$

wobei M das maximale Ideal von B ist.

BEWEIS. 1.) f ist offensichtlich antiton. Ist $P \in \mathfrak{P}$ und N ein maximales Ideal, das P umfaßt, so liegt R_N in R_P. Da R_N ein Bewertungsring ist und jeder Oberring eines Bewertungsringes auch Bewertungsring ist, folgt $R_P \in \mathfrak{B}$ für alle $P \in \mathfrak{P}$.

2.) Ist $B \in \mathfrak{B}$ und M_B das maximale Ideal von B, so ist $P = M_B \cap R$ ein Primideal von R. Wir zeigen $B = R_P$:

(a) Sei $ab^{-1} \in R_P$, $a \in R$, $b \in R \setminus P$. Wäre $b \in M_B$, so würde $b \in M_B \cap R = P$ folgen. Also liegt b in $B \setminus M_B$ und ist daher eine Einheit in B. Daraus folgt $ab^{-1} \in B$[†].

(b) Sei $x \notin R_P$. Weil R_P ein Bewertungsring ist, liegt x^{-1} im maximalen Ideal von R_P, besitzt also eine Darstellung $x^{-1} = ab^{-1}$ mit $a \in P$, $b \in R \setminus P$. Es folgt $bx^{-1} \in P \subseteq M_B$ und daher $x^{-1} \in M_B$ wegen $b \notin M_B$, also $x \notin B$.

3.) Sei $P \in \mathfrak{P}$ und M das maximale Ideal von R_P. Wegen

$$\begin{aligned} x \in R \cap M &\iff (x \in R \wedge x = ab^{-1})\,, \quad a \in P,\, b \in R \setminus P \\ &\iff (x \in R \wedge xb \in P)\,, \quad b \in R \setminus P \\ &\iff x \in P \end{aligned}$$

ist $P = R \cap M$.

Damit ist gezeigt, daß die Kompositionen $f \circ g$ und $g \circ f$ jeweils die Identität ergeben. Daher ist f eine Bijektion mit der Umkehrabbildung g. □

FOLGERUNG 11.1. *Den minimalen Elementen von $\mathfrak{B}$ entsprechen bei dieser Bijektion gerade die maximalen Ideale von R.*

HILFSSATZ 11.2. *Sei R ein Ring, I ein Ideal von R und $P_1, \ldots, P_n$ Primideale von R. Gilt*

$$I \subseteq P_1 \cup \cdots \cup P_n\,,$$

so gibt es ein i mit

$$I \subseteq P_i\,.$$

BEWEIS. Induktion nach n: Der Fall $n = 1$ ist trivial.
Wir können $P_i \notin \bigcup_{j \neq i} P_j$ annehmen, weil sonst aus $I \subseteq \bigcup_{j \neq i} P_j$ nach Induktion $I \subseteq P_j$ für ein j folgen würde.

1. Fall: Für ein i gilt

$$I \cap P_i \subseteq \bigcup_{j \neq i} P_j\,.$$

[†]Wegen $R \subseteq B$ ist $a \in B$

Rechts steht nur die Vereinigung von $n-1$ Primidealen. Nach Induktion folgt $I \cap P_i \subseteq P_j$ für ein j. Hieraus ergibt sich aber bereits $I \subseteq P_j$. Denn wegen $P_i \neq P_j$ existiert ein $a \in P_i$, $a \notin P_j$. Ist dann $x \in I$, so folgt $xa \in I \cap P_i \subseteq P_j$, also $x \in P_j$, weil P_j ein Primideal ist, also $I \subseteq P_j$.

2. Fall: Für alle i gilt

$$I \cap P_i \nsubseteq \bigcup_{j \neq i} P_j \,.$$

Wir zeigen, daß dieser Fall nicht eintreten kann. Ist nämlich

$$y_i \in I \cap P_i \,, \quad y_i \notin \bigcup_{j \neq i} P_j \,,$$

so liegt

$$y = y_2 y_3 \cdot \ldots \cdot y_n + y_1 y_3 \cdot \ldots \cdot y_n + \cdots + y_1 y_2 \cdot \ldots \cdot y_{n-1}$$

in I, nicht aber in $\bigcup_{i=1}^n P_i$, was im Widerspruch zu $I \subseteq \bigcup_{i=1}^n P_i$ steht. □

Satz 11.6. *Der Durchschnitt endlich vieler Bewertungsringe ist ein Prüferring mit endlich vielen maximalen Idealen.*

Beweis. Sei $R = \bigcap_{i=1}^n B_i$, wobei die B_i Bewertungsringe von K sind. Sind M_i die maximalen Ideale der B_i und

$$P_i = R \cap M_i \,,$$

so gilt für jedes echte Ideal I von R

$$I \subseteq \bigcup_{i=1}^n P_i \,.$$

Denn $x \in R$, $x \notin P_i$ für alle i bedeutet $|x|_i = 1$ für alle i. Damit ist aber x eine Einheit in R, kann also nicht in I liegen.

Die P_i sind Primideale von R. Nach Hilfssatz 11.2 gilt also $I \subseteq P_i$ für ein i. Ist I speziell ein maximales Ideal, so folgt $I = P_i$ für ein i. Für die Menge $\mathfrak{M}$ der maximalen Ideale von R ergibt sich daher

$$\mathfrak{M} \subseteq \{P_1, \ldots, P_n\} \,. \tag{1}$$

Außerdem gilt

$$B_i = R_{P_i} = \{ab^{-1} \mid a \in R,\, b \in R \setminus P_i\} \,. \tag{2}$$

Ist nämlich $x \in B_i$, $x \neq 0$, so gibt es nach Lemma 10.1 ein y mit

$$\begin{aligned} |y|_j &= |x|_j \qquad \text{für die Indizes } j, \text{ für die } |x|_j \leq 1 \text{ ist}\,, \\ |y|_j &\leq |x^{-1}|_j \qquad \text{für die Indizes } j, \text{ für die } |x|_j > 1 \text{ ist}\,. \end{aligned}$$

Hieraus folgt $y \in R$ und $yx^{-1} \in R \setminus P_i$, also

$$x = y\,(yx^{-1})^{-1} \in R_{P_i} \,.$$

Ist umgekehrt $ab^{-1} \in R_{P_i}$, $a \in R$, $b \in R \setminus P_i$, so folgt $|b|_i = 1$, also $|ab^{-1}|_i = |a|_i \leq 1$, also $ab^{-1} \in B_i$.

Aus (1) und (2) folgt, daß die Lokalisierungen von R nach den maximalen Idealen Bewertungsringe sind. Also ist R ein Prüferring. □

BEMERKUNG. 1.) Ist $R = \bigcap_{i=1}^{n} B_i$, und sind die B_i bezüglich der Inklusion nicht vergleichbar, so gilt schärfer als (1)

$$\mathfrak{M} = \{P_1, \ldots, P_n\}\,.$$

Denn jedes Primideal P_k liegt in einem maximalen Ideal P_j, woraus $B_j \subseteq B_k$, also wegen der Unvergleichbarkeit der B_i $j = k$ folgt.

2.) Man kann zeigen, daß Prüferringe mit nur endlich vielen maximalen Idealen Bezoutringe sind (siehe KAPLANSKY, Commutative Rings, Satz 60).

Als Anwendung von Satz 11.6 erhalten wir einen Approximationssatz, in dem die Unabhängigkeit der Bewertungen nicht vorausgesetzt ist.

SATZ 11.7. *Seien* $|\ |_1, \ldots, |\ |_n$ *Bewertungen von* K *mit den Wertegruppen* G_i *und den Bewertungsringen* B_i. *Seien* $\varepsilon_i \in G_i$ *mit* $a_i \in K$ *gegeben. Es gibt (genau dann) ein* $x \in K$ *mit*

$$|x - a_i|_i \leq \varepsilon_i\,, \quad i = 1, \ldots, n\,,$$

wenn für jedes Paar (i, j) *von Indizes ein* x *mit*

$$|x - a_i|_i \leq \varepsilon_i \quad \textit{und} \quad |x - a_j|_j \leq \varepsilon_j$$

existiert.

BEWEIS. 1.) Sei $R = B_1 \cap \cdots \cap B_n$. Wir setzen zunächst $a_i \in R$ voraus.
Sei

$$I_i = \{x \in R \mid |x|_i \leq \varepsilon_i\}\,.$$

Für ein Indizespaar (i, j) gilt dann $x - a_i \in I_i$ und $x - a_j \in I_j$, woraus $a_i - a_j \in I_i + I_j$ folgt.

Da R ein Prüferring ist, kann der Chinesische Restsatz angewandt werden. Es existiert daher ein $x \in R$ mit

$$x \equiv a_i \bmod I_i\,, \qquad i = 1, \ldots, n$$

oder anders geschrieben

$$|x - a_i|_i \leq \varepsilon_i\,, \qquad i = 1, \ldots, n\,.$$

2.) Wir betrachten nun den allgemeinen Fall $a_i \in K$. Da K Quotientenkörper von R ist (Kapitel 10, Korollar 10.1), gilt $a_i = b_i c_i^{-1}$ mit $b_i, c_i \in R$. Indem man die Brüche geeignet erweitert, kann man $a_i = b_i c^{-1}$ mit festem Hauptnenner c annehmen.

Für eine Teilmenge I der Indexmenge $\{1, \ldots, n\}$ gilt offenbar:
Es gibt genau dann ein $x \in K$ mit

$$|x - a_i|_i \leq \varepsilon_i \qquad i \in I\,,$$

wenn ein $y \in K$ mit

$$|y - b_i|_i \leq \varepsilon_i |c|_i \qquad i \in I$$

existiert.

Ist also für ein Paar (i,j) das System

$$|x-a_i|_i \le \varepsilon_i\,, \qquad |x-a_j|_j \le \varepsilon_j$$

lösbar, so ist auch

$$|y-b_i|_i \le \varepsilon_i|c|_i\,, \qquad |y-b_j|_j \le \varepsilon_j|c|_j$$

lösbar. Hieraus ergibt sich, wie unter 1.) gezeigt wurde, die Lösbarkeit von

$$|y-b_i|_i \le \varepsilon_i|c|_i\,, \qquad i=1,\dots,n\,,$$

woraus wiederum die Lösbarkeit von

$$|x-a_i|_i \le \varepsilon_i\,, \qquad i=1,\dots,n$$

folgt. □

KAPITEL 12

Algebraische Erweiterungen

Sei L eine algebraische Erweiterung von K und B ein Bewertungsring von K. $\mathfrak{B}$ bezeichne die Menge der Bewertungsringe A von L, die den Bewertungsring B umfassen. Der Durchschnitt

$$R = \bigcap_{A \in \mathfrak{B}} A$$

ist nach Satz 9.4 der Ring der über B ganzen Elemente von L. Es gilt

SATZ 12.1. *R ist ein Prüferring.*

BEWEIS. Ist N ein maximales Ideal in R, so haben wir zu zeigen, daß

$$R_N = \{ab^{-1} \mid a \in R,\, b \in R \setminus N\}$$

ein Bewertungsring in L ist.

Sei $x \in L^\times$. Weil L algebraisch über K ist, genügt x einer Gleichung

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n = 0\,, \qquad a_i \in K\,.$$

Durch Multiplikation mit einem geeigneten Körperelement kann man erreichen, daß die Koeffizienten sogar in B liegen und daß einer der Koeffizienten, etwa a_m, eine Einheit von B ist. Wir definieren für $k = 0, 1, \ldots, n$

$$y_k = \sum_{i=0}^{k} a_i x^{k-i} \qquad \text{und} \qquad z_k = \sum_{i=1}^{n-k-1} a_{k+i} x^{-i}\,.$$

Es gilt:

$$y_k = y_{k-1} x + a_k\,, \quad k \geq 0 \tag{1}$$

$$x y_k + z_k = 0 \tag{2}$$

$$y_k\,, z_k \in R\,. \tag{3}$$

Die Gültigkeit von (1) und (2) ergibt sich sofort. Weil R Durchschnitt der Bewertungsringe $A \in \mathfrak{B}$ ist, hat man, um das Bestehen von (3) nachzuweisen, $y_k, z_k \in A$ für alle $A \in \mathfrak{B}$ zu zeigen. Es gilt $x \in A$ oder $x^{-1} \in A$. Im ersten Fall ist $y_k \in A$ und damit auch $z_k = -x y_k \in A$. Im zweiten Fall ist $z_k \in A$ und damit auch $y_k = -x^{-1} z_k \in A$.

Wir zeigen nun $x \in R_N$ oder $x^{-1} \in R_N$, womit dann R_N ein Bewertungsring in L ist. Hierzu unterscheiden wir zwei Fälle:

1.) Für alle k gilt $y_k \in N$.
Weil a_m eine Einheit in B und damit auch in R ist, gilt $a_m \notin N$, also $a_m \in R \backslash N$. Ist $m \neq 0$, so folgt

$$y_{m-1}x = y_m - a_m \in R \setminus N\,,$$

also

$$x^{-1} = y_{m-1}(y_m - a_m)^{-1} \in R_N\,.$$

Ist $m = 0$, so ist $xa_0 + z_0 = 0$, also

$$x = -z_0 a_0^{-1} \in R_N\,.$$

2.) Für ein k gilt $y_k \in R \setminus N$.
Aus $xy_k + z_k = 0$ folgt dann sofort

$$x = -z_k y_k^{-1} \in R_N\,. \quad \square$$

Die beiden folgenden Hilfssätze stammen von Cohen und Seidenberg (1946). Ein Ring R heißt ganz über einem Teilring B, wenn zu jedem $x \in R$ ein nichtkonstantes Polynom

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in B[t]$$

existiert, das x als Nullstelle hat.

Hilfssatz 12.1. *Sei R ganz über B und $\mathfrak{P}$ die Menge der Primideale von R, $\mathfrak{P}'$ die Menge der Primideale von B. Die Abbildung*

$$\mathfrak{P} \to \mathfrak{P}'\,, \quad P \mapsto P \cap B$$

ist streng isoton (d.h. aus $P_1 \subsetneqq P_2$ folgt $P_1 \cap B \subsetneqq P_2 \cap B$).

Beweis. Sei $P_1 \subsetneqq P_2$ und $x \in P_2 \setminus P_1$. Wir wählen $n \in \mathbb{N}$ minimal, so daß

$$y = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in P_1\,, \qquad a_i \in B\,,$$

gilt. Weil R ganz über B ist, gibt es ein solches n. Dann ist

$$a_0 = y - (x^n + a_{n-1}x^{n-1} + \cdots + a_1 x) \in P_2 \cap B\,.$$

Wäre $a_0 \in P_1 \cap B$, so würde

$$x\,(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) \in P_1$$

und $n \geq 2$ folgen. Weil aber $x \notin P_1$ und P_1 ein Primideal ist, ergibt sich

$$x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1 \in P_1\,,$$

was im Widerspruch zur Minimalität von n steht. Damit ist

$$a_0 \in (P_2 \cap B) \setminus (P_1 \cap B)\,.$$

Also ist $P_1 \cap B \subsetneqq P_2 \cap B$. $\square$

Hilfssatz 12.2. *Sei R ganz über B. Ein Primideal P von R ist genau dann ein maximales Ideal von R, wenn $P \cap B$ ein maximales Ideal von B ist.*

BEWEIS. 1.) Sei P ein maximales Ideal von R. Wegen $1 \notin P \cap B$ ist $P \cap B$ ein echtes Ideal von B. Sei M ein maximales Ideal von B mit $P \cap B \subseteq M$. Wir führen die Annahme $P \cap B \subsetneqq M$ zum Widerspruch. Sei $a \in M \setminus P$. Weil P maximal ist, gilt dann $R = P + aR$, also

$$1 = x + ab \quad \text{mit} \quad x \in P,\, b \in R\,.$$

Weil R ganz über B ist, gilt

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

für gewisse $a_i \in B$. Multipliziert man diese Gleichung mit a^n, so folgt

$$(ab)^n + a'_{n-1}(ab)^{n-1} + \cdots + a'_0 = 0$$

mit $a'_i = a^{n-i}a_i \in M$, also wegen $ab = 1 - x$

$$1 + a'_{n-1} + \cdots + a'_0 \in P \cap B \subseteq M$$

und damit $1 \in M$. Dies ist ein Widerspruch. Damit ist $P \cap B = M$, also $P \cap B$ ein maximales Ideal von B.

2.) Sei nun $P \cap B$ ein maximales Ideal in B. Wäre P nicht maximal in R, so gäbe es ein maximales Ideal N von R mit $P \subsetneqq N$. Nach Hilfssatz 12.1 folgt $P \cap B \subsetneqq N \cap B$. Damit wäre aber $P \cap B$ nicht maximal in B. □

Ein Bewertungsring A von L heißt eine *Erweiterung* des Bewertungsringes B, wenn gilt

(1) $B \subseteq A$

(2) $M \subseteq M_A$

Hierbei ist M das maximale Ideal von B und M_A das maximale Ideal von A.

Äquivalent zu (2) ist

(2′) $M = M_A \cap B$.

BEWEIS. Auf Grund von (1) gilt

$$x \in M_A \cap B \quad \Longrightarrow \quad x^{-1} \notin A \quad \Longrightarrow \quad x^{-1} \notin B \quad \Longrightarrow \quad x \in M\,,$$

also $M_A \cap B \subseteq M$. Die umgekehrt Inklusion ergibt sich aus (2). Aus (2′) folgt sofort $M = M_A \cap B \subseteq M_A$, also (2). □

SATZ 12.2. *Die Erweiterungen von B sind genau die minimalen Elemente von $\mathfrak{B} = \{A \mid A \supseteq B\}$.*

BEWEIS. Nach Satz 12.1 ist R ein Prüferring. Nach Satz 11.5 ist die Abbildung

$$\mathfrak{B} \to \mathfrak{P}\,, \quad A \mapsto P = M_A \cap R$$

eine antitone Bijektion. Also gilt für $A \in \mathfrak{B}$ und $P = M_A \cap R$

$$\begin{aligned} A \text{ minimal in } \mathfrak{B} &\iff P \text{ maximales Ideal in } R \\ &\iff P \cap B = M^{\dagger} \\ &\iff M_A \cap B = M \\ &\iff A \text{ ist eine Erweiterung von } B. \quad \square \end{aligned}$$

[†]Nach Hilfssatz 12.2

Wir bezeichnen mit $\mathfrak{A}$ die Menge der minimalen Elemente von $\mathfrak{B}$. In Kapitel 9 wurde gezeigt, daß die Erweiterungen den Bewertungsfortsetzungen entsprechen. Nach Satz 12.2 entsprechen daher die Elemente von $\mathfrak{A}$ eineindeutig den Erweiterungen von B und damit den Bewertungsfortsetzungen der Bewertung von K auf den Erweiterungskörper L.

SATZ 12.3. *Es ist* $|\mathfrak{A}| \leq [L:K]$.

BEWEIS. Seien $A_1, \ldots, A_r \in \mathfrak{A}$. Nach Satz 11.6 ist $S = \bigcap_{i=1}^{r} A_i$ ein Prüferring. In S gilt daher der Chinesische Restsatz. Maximale Ideale von S sind

$$P_i = M_{A_i} \cap S\,, \qquad i = 1, \ldots, r\,.$$

Wegen $P_i + P_j = S$ für $i \neq j$ besitzen die Kongruenzen

$$\begin{aligned} x_i &\equiv 1 \bmod P_i \\ x_i &\equiv 0 \bmod P_j \qquad \text{für } i \neq j \end{aligned}$$

eine Lösung $x_i \in S$.
Behauptung: $x_1, \ldots, x_r$ sind linear unabhängig über K. Wäre nämlich

$$\sum_{j=1}^{r} a_j x_j = 0$$

mit $a_j \in K$ und $|a_i| = \max_j |a_j| \neq 0$, so folgte

$$x_i = -\sum_{\substack{j=1 \\ j\neq i}} a_j a_i^{-1} x_j \in P_i$$

im Widerspruch zu $x_i \equiv 1 \bmod P_i$.
Damit ist $r \leq [L:K]$. Ist $[L:K] < \infty$, so ist auch $|\mathfrak{A}| < \infty$ und $|\mathfrak{A}| \leq [L:K]$. □

Im folgenden Satz sei L eine endliche Galoiserweiterung von K und G die Galoisgruppe. Ist $\sigma \in G$ und A ein Bewertungsring von L, so ist auch σA ein Bewertungsring von L. Ist speziell A aus $\mathfrak{A}$, so ist auch $\sigma A \in \mathfrak{A}$. Damit operiert G auf $\mathfrak{A}$. Es gilt sogar

SATZ 12.4. *G operiert transitiv auf $\mathfrak{A}$.*

BEWEIS. Sei $A_0 \in \mathfrak{A}$ und $S = \bigcap_{\sigma\in G} \sigma A_0$. S ist ein G-invarianter Teilring von L. Wir zeigen $S = R$ mit $R = \bigcap_{A\in\mathfrak{A}}$. Offensichtlich ist $R \subseteq S$. Sei nun $x \in S$ und

$$F(t) = \prod_{\sigma\in G} (t - \sigma x) = t^n + a_{n-1}t^{n-1} + \cdots + a_0\,.$$

Da die Koeffizienten a_i symmetrische Funktionen der σx sind, liegen sie im Grundkörper K, also gilt

$$a_i \in K \cap S \subseteq K \cap A_0 = B\,.$$

Wegen $F(x) = 0$ ist x ganz über B, also $x \in R$. Damit ist $S = R$.
Sei $A \in \mathfrak{A}$. Dann gilt $A \supseteq S$. Nach Satz 11.5 ist dann $A \supseteq \sigma A_0$ für ein $\sigma \in G$. Weil A minimal ist, gilt $A = \sigma A_0$. □

KOROLLAR 12.1. *Ist v eine Fortsetzung der Bewertung von K, so läßt sich jede Fortsetzung in der Form $v \circ \sigma$ mit $\sigma \in G$ schreiben.*

KAPITEL 13

Relativ vollständige Körper

Sei K ein bewerteter Körper, B der Bewertungsring von K und $a \mapsto \bar{a}$ die Restklassenabbildung von B auf den Restklassenkörper $\bar{K}$. Wir betrachten die Abbildung

$$B[t] \to \bar{K}[t]\,, \quad f(t) = \sum_{i=0}^{n} a_i t^i \mapsto \bar{f}(t) = \sum_{i=0}^{n} \bar{a}_i t^i\,.$$

Ein Polynom $f(t)$ heißt primitiv, wenn $f(t) \in B[t]$ und $\bar{f}(t) \neq 0$ ist, wenn also einer der Koeffizienten von f eine Einheit in B ist. Wir können hiermit das Henselsche Lemma formulieren

HENSELSCHES LEMMA. *Ist $f(t) \in K[t]$ primitiv, $\bar{f}(t) = G(t)H(t)$ mit teilerfremden Polynomen $G(t), H(t) \in \bar{K}[t]$, so gibt es eine Zerlegung*

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

mit $\bar{g} = G$, $\bar{h} = H$ und $\operatorname{grad} g = \operatorname{grad} G$.

DEFINITION 13.1. Ein bewerteter Körper K heißt *relativ vollständig*, wenn in K das Henselsche Lemma gilt.

Körper, die bezüglich einer reellen nicht-archimedischen Bewertung vollständig sind, sind nach Satz 6.2 relativ vollständig. Aber auch algebraisch abgeschlossene Körper sind relativ vollständig. Der Begriff des relativ vollständigen Körpers wurde von OSTROWSKI eingeführt. NAGATA bezeichnet relativ vollständige Körper als Henselsche Körper.

Man kann zeigen, daß jede geordnete abelsche Gruppe G sich in eine Gruppe G_w einbetten läßt, in der die Gleichung

$$x^n = a \qquad \text{für } a \in G_w,\ n \in \mathbb{N}$$

stets eine eindeutige Lösung besitzt. Man schreibt $x = \sqrt[n]{a}$.

Der Beweis des folgenden Satzes ist identisch mit dem Beweis von Satz 6.3.

SATZ 13.1. *Ist L algebraisch über K und K relativ vollständig, so ist, falls*

$$\operatorname{Irr}(a, K) = t^k + a_{k-1}t^{k-1} + \cdots + a_0$$

ist,

$$|a|_L = \sqrt[k]{|a_0|_K} \in G_w \cup \{0\}$$

eine Bewertungsfortsetzung von $|\ |_K$ auf L.

Der Beweis der Eindeutigkeit der Bewertungsfortsetzung in Satz 3.3 läßt sich nicht in so einfacher Weise übertragen, da hierin die Vollständigkeit von K wesentlich benutzt wird. Im folgenden Satz beweisen wir die Eindeutigkeit auf einem ganz anderen Weg.

HILFSSATZ 13.1. *Ist*

$$f(t) = t^k + a_{k-1}t^{k-1} + \cdots + a_0 \in K[t]$$

irreduzibel, und ist K relativ vollständig, so gilt

$$|a_{k-j}| \leq \sqrt[k]{|a_0|^j}\,.$$

BEWEIS. Sei L der Zerfällungskörper von $f(t)$ und

$$f(t) = (t - b_1) \cdot \ldots \cdot (t - b_k)$$

die Zerfällung von f in L. Für die in Satz 13.1 betrachtete Bewertungsfortsetzung gilt dann $|b_i|_L = \sqrt[k]{|a_0|_K}$, also

$$|a_{k-j}|_K = |\pm \sum b_{i_1} \cdot \ldots \cdot b_{i_j}|_L \leq \sqrt[k]{|a_0|_K^j}\,. \quad \square$$

SATZ 13.2. *Folgende Aussagen sind äquivalent:*

(1) *K ist relativ vollständig.*

(2) *Die Fortsetzung der Bewertung von K auf eine algebraische Erweiterung ist stets eindeutig.*

(3) *Ist $f(t) \in K[t]$ primitiv und irreduzibel, so gilt*

   (a) $\operatorname{grad} f = \operatorname{grad} \bar{f}$ *und* $\bar{f}(t) = \bar{a}\,p(t)$, *wobei* $\bar{a} \in \bar{K}^\times$ *und* $p(t) \in \bar{K}[t]$ *irreduzibel ist,*

   oder

   (b) $\operatorname{grad} \bar{f} = 0$, *d.h.* $\bar{f}(t) = \bar{a} \in \bar{K}^\times$.

BEWEIS. (1) $\Rightarrow$ (2): Sei $|\ |_1$ eine Bewertung einer algebraischen Erweiterung L von K, die von der in Satz 13.1 betrachteten Bewertung $|\ |_L$ verschieden ist. Es gibt dann ein $b \in L$ mit $|b|_1 \neq |b|_L$. Wir können $|b|_1 < |b|_L$ annehmen (andernfalls ersetze b durch b^{-1}). Sei

$$\operatorname{Irr}(b, K) = t^k + a_{k-1}t^{k-1} + \cdots + a_0\,.$$

Nach Satz 13.1 ist dann $|b|_1 < |b|_L = \sqrt[k]{|a_0|_K}$. Hieraus folgt $|b^k|_1 < |a_0|_K$ und für $0 < j < k$ nach Hilfssatz 13.1

$$|a_{k-j}b^{k-j}|_1 = |a_{k-j}|_K |b|_1^{k-j} < \sqrt[k]{|a_0|_K^j}\,\sqrt[k]{|a_0|_K^{k-j}} = |a_0|_K\,.$$

Damit erhalten wir den Widerspruch

$$0 = |b^k + a_{k-1}b^{k-1} + \cdots + a_0|_1 = |a_0|_K \neq 0\,.$$

(2) $\Rightarrow$ (3): Sei

$$f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in B[t]$$

irreduzibel und primitiv und

$$f(t) = a_n\,(t - b_1) \cdot \ldots \cdot (t - b_n)$$

eine Zerlegung von f in einem Zerfällungskörper L. Ist σ ein Automorphismus von L über K mit $\sigma b_i = b_j$ und v eine Fortsetzung der Bewertung $|\ |$ von K, so ist

$$v(b_i) = v(\sigma b_i) = v(b_j)\,,$$

weil $v \circ \sigma$ ebenfalls eine Fortsetzung von $|\ |$ ist und wegen der Eindeutigkeit der Fortsetzungen mit v übereinstimmt. Wir setzen

$$\beta = v(b_1) = \cdots = v(b_n)\,.$$

Sei A der zu v gehörige Bewertungsring von L und M_A sein maximales Ideal. A und M_A sind invariant gegen Automorphismem von L über K. Wegen $v = v \circ \sigma$ haben nämlich a und σa für jedes $a \in L$ den gleichen Wert.

Es ist eine Fallunterscheidung notwendig.

1. Fall: $|a_n| = 1$.

Dann ist $\operatorname{grad} f = \operatorname{grad} \bar{f}$. Aus $a_0 = (-1)^n a_n b_1 \cdot \ldots \cdot b_n$ folgt $|a_0| = |a_n|\beta^n \leq 1$, also $\beta \leq 1$, d.h. $b_i \in A$. Im Restklassenkörper $\bar{L}$ erhalten wir dann

$$\bar{f}(t) = \bar{a}_n(t - \bar{b}_1) \cdot \ldots \cdot (t - \bar{b}_n)\,.$$

Die Annahme, daß eine Zerlegung $\bar{f}(t) = G(t)H(t)$ mit teilerfremden Polynomen $G, H \in \bar{K}[t]$, $\operatorname{grad} G \geq 1$, $\operatorname{grad} H \geq 1$, existiert, führt zum Widerspruch:

Über dem Restklassenkörper $\bar{L}$ gilt dann

$$G(t) = (t - \bar{b}_i)\, G_1(t) \quad \text{und} \quad H(t) = (t - \bar{b}_j)\, H_1(t)\,.$$

Ist $g(t) \in B[t]$ ein Polynom mit $\bar{g}(t) = G(t)$ und $g_1(t) \in A[t]$ mit $\bar{g}_1(t) = G_1(t)$, so ist

$$g(t) - (t - b_i)\, g_1(t) \in M_A[t]\,.$$

M_A ist invariant gegenüber Automorphismen von L über K. Wählt man einen Automorphismus σ mit $\sigma b_i = b_j$, so folgt

$$g(t) - (t - b_j)\, (\sigma g_1)(t) \in M_A[t]\,,$$

also

$$G(t) = (t - \bar{b}_j)\, (\overline{\sigma g_1})(t)\,.$$

Damit teilt $t - \bar{b}_j$ sowohl G als auch H in $\bar{L}[t]$. Das widerspricht jedoch der Voraussetzung, daß G und H teilerfremd sind.

Zerlegt man $\bar{f}(t)$ in $\bar{K}[t]$ als Produkt irreduzibler Polynome, so ist

$$\bar{f}(t) = \bar{a} p_1^{k_1}(t) \cdot \ldots \cdot p_r^{k_r}(t)\,, \qquad \bar{a} \in \bar{K}\,.$$

Da aber eine Zerlegung in teilerfremde Polynome nicht möglich ist, folgt $r = 1$.

2. Fall: $|a_n| < 1$.

Für $j = 1, \ldots, n$ ist

$$a_{n-j} = \pm a_n \sum b_{i_1} \cdot \ldots \cdot b_{i_j}\,,$$

also

$$|a_{n-j}| \leq |a_n|\beta^j \quad \text{und} \quad |a_0| = |a_n|\beta^n\,.$$

Da f primitiv ist, ist $|a_{n-j_0}| = 1$ für ein j_0. Aus

$$|a_{n-j_0}| = 1 \leq |a_n|\beta^{j_0} \quad \text{und} \quad |a_n| < 1$$

folgt $\beta > 1$. Hiermit gilt

$$1 \leq |a_n|\beta^{j_0} \leq |a_n|\beta^n = |a_0|\,,$$

wegen der Primitivität von f also $|a_0| = 1$. Für $j < n$ ist

$$|a_{n-j}| \leq |a_n|\beta^j < |a_n|\beta^n = |a_0| = 1$$

und damit

$$\bar{f}(t) = \bar{a}_0\,.$$

(3) $\Rightarrow$ (1): Sei f primitiv, $\bar{f} = GH$ mit teilerfremden Polynomen G und H. Wir zerlegen f in $K[t]$ in irreduzible Faktoren,

$$f = q_1 \cdot \ldots \cdot q_r\,.$$

Nach Hilfssatz 6.2 kann man die q_i als primitiv annehmen. In $\bar{K}[t]$ gilt dann

$$\bar{f} = \bar{q}_1 \cdot \ldots \cdot \bar{q}_r\,.$$

Nach (3) ist $\bar{q}_i = \bar{a}_i p_i^{k_i}$, p_i irreduzibel in $\bar{K}[t]$ oder $\bar{q}_i = \bar{a}_i$, $\bar{a}_i \in \bar{K}$. Wegen $\bar{f} = GH$ treten bei der Zerlegung von G nur Primfaktoren von $\bar{f}$ auf. Da G und H teilerfremd sind, besitzt G nach einer eventuellen Umindizierung die Form

$$G = \bar{a} p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}\,.$$

Setzt man dann $g(t) = bq_1 \cdot \ldots \cdot q_s$, wobei b so ermittelt wird, daß

$$\bar{b} \prod_{i=1}^{s} \bar{a}_i = \bar{a}$$

gilt, und $h(t) = b^{-1} q_{s+1} \cdot \ldots \cdot q_r$, so erhält man

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

mit $\bar{g} = G$, $\bar{h} = H$ und $\operatorname{grad} g = \operatorname{grad} G$. Also ist K relativ vollständig. □

Bemerkung. Da für vollständige Körper in Satz 3.3 die Eindeutigkeit der Fortsetzungen gezeigt wurde, liefert Satz 13.2 einen neuen Beweis des Henselschen Lemmas.

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.*
Vorlesung 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

Abbildung
    werterhaltende, 19
Abschluß
    ganzer, 88
additive Krullbewertung, 79
äquivalente Bewertung, 8
äquivalente Krullbewertung, 75
Approximationssatz, 93
archimedisch geordnete Gruppe, 64
archimedische Bewertung, 5

Bewertung
    äquivalente, 8
    archimedische, 5
    diskrete, 39
    Fortsetzung einer, 25
    nicht-archimedische, 5
    p-adische, 6
    reelle, 5
    triviale, 7
    unabhängige, 92
Bewertungsring, 37, 71
    Erweiterung eines, 111
Bezoutring, 104

Cauchy-Folge, 15
Chevalley, Satz von, 83
Chinesischer Restsatz, 99

Darstellung
    kanonische, 42
    periodische, 45
dicht, 17
diskrete Bewertung, 39
distributiver Idealverband, 100
Dominanzprinzip, 8

Eindeutigkeit der Komplettierung, 21
endliche Erweiterung, 23
Erweiterung
    endliche, 23
Erweiterungsgrad, 23

Fortsetzung einer Bewertung, 25
Fortsetzung einer Krullbewertung, 85

ganz, 88
ganz-abgeschlossen, 88
ganzer Abschluß, 88
ganzes Ideal, 72
gebrochenes Ideal, 72
geordnete Gruppe, 63
Gruppe
    archimedisch geordnete, 64
    geordnete, 63

Hahnsches Produkt, 63, 64
Henselscher Körper, 43
Henselsches Lemma, 55
Hölder, Satz von, 65

Ideal
    ganzes, 72
    gebrochenes, 72
    maximales, 78
Idealverband
    distributiver, 100

kanonische Darstellung, 42
Körper
    Henselscher, 43
    kompletter, 16
    relativ vollständiger, 113
    vollständiger, 16
Körper der p-adischen Zahlen, 43
kompletter Körper, 16
Komplettierung, 17
    Eindeutigkeit, 21
konvergente Folge, 15
konvex, 69
Krull
    Satz von, 88
Krullbewertung, 74
    additive, 79
    äquivalente, 75
    Existenz einer, 85
    Existenz einer Fortsetzung, 86
    Fortsetzung, 85
    vom Rang n, 75
Kürschak, Satz von, 59

Lemma
    Henselsches, 55
lokaler Ring, 78
Lokalisierung, 102

maximales Ideal, 78
Maximumsnorm, 26

Menge
    induktiv geordnet, 83
    wohlgeordnete, 63

Nennermenge, 102
Newtonsches Verfahren, 47
nicht-archimedische Bewertung, 5
Norm, 23
normierter Raum, 26

Ostrowski, Satz von, 11

p-adische Bewertung, 6
periodische Darstellung, 45
Polynom
    primitives, 53
Primelement, 40
Primideal, 76
primitives Polynom, 53
Produkt
    Hahnsches, 63, 64
Prüferring, 103

Rang, 70
Raum
    normierter, 26
    vollständiger normierter, 26
reelle Bewertung, 5
Repräsentantensystem, 40
Restklassenkörper, 37
Restsatz
    Chinesischer, 99
Ring
    lokaler, 78

Satz von Hölder, 65
Satz von Kürschak, 59
Satz von Chevalley, 83
Satz von Krull, 88
Satz von Ostrowski, 11

Träger, 63
triviale Bewertung, 7

unabhängige Bewertungen, 92

vollständiger normierter Raum, 26
vollständiger Körper, 16

Wertegruppe, 39, 75
werterhaltende Abbildung, 19
wohlgeordnete Menge, 63

Zornsches Lemma, 83