Prof. Dr. K. Mathiak

Dr. W. Oelke

Zahlentheorie

Braunschweig, Juli 1993

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

Dieses Skript wurde mit dem LaTeX 2ε-Makropaket AMS-LaTeX 2ε erstellt.

Satz: Dr. W. Oelke, Institut für Algebra und Zahlentheorie
D. Pape

Inhaltsverzeichnis

KAPITEL 1

Bewertungen

Es sei K ein Körper und

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

die Menge der nicht-negativen reellen Zahlen.

DEFINITION 1.1. Eine Abbildung

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

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

(1) $|x| = 0 \iff x = 0$
(2) $|x + y| \leq |x| + |y|$
(3) $|x \cdot y| = |x| \cdot |y|$

BEISPIEL. 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 Bewertung, die als *triviale Bewertung* von K bezeichnet wird:

(1) nach Definition.
(2) Gilt für $x = y = 0$. Ist $x \neq 0$ oder $y \neq 0$, so steht auf der rechten Seite von (2) mindestens 1 und auf der linken Seite höchstens 1.
(3) Ist $x, y \neq 0$, so ist auch $xy \neq 0$, also $|xy| = 1 = |x||y|$. Für $x = 0$ oder $y = 0$ ist $|xy| = 0 = |x||y|$.

DEFINITION 1.2. Eine Bewertung heißt *nicht-archimedisch*, wenn

(2′) $|x + y| \leq \max(|x|, |y|)$

für alle $x, y \in K$ gilt. (2′) heißt *scharfe Dreiecksungleichung*.
Gilt (2′) nicht allgemein, so heißt die Bewertung *archimedisch*.

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

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

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

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

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

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

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

und

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

Häufig setzt man $d = \frac{1}{p}$.

Definition 1.3. Man nennt

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

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

Eigenschaften von Bewertungen

(A) $|1| = 1$.

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

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

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

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

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

FOLGERUNGEN. (a) $|-1| = 1$.
(b) $|-x| = |-1||x| = |x|$.
(c) *Ist* $K = \mathbb{Z}_p$, *so gilt* $a^{p-1} = 1$ *für alle* $a \in \mathbb{Z}_p^\times$ (FERMAT) *mit* $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash \{0\}$. *Also ist jede Bewertung auf* $\mathbb{Z}_p$ *trivial.*

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

BEWEIS. Nach (2) ist

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

Analog folgt, wenn man x und y vertauscht:

$$|y| - |x| \leq |y-x| = |x-y| \,. \quad \square$$

(E) Eine Bewertung ist genau dann nicht-archimedisch, wenn der *Ganzheitsbereich*

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

ein Teilring von K ist.

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

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

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

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

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

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

Für $|x| \geq |y|$ analog. $\square$

(F) $| \ |$ sei nicht-archimedisch. Ist $|x| < |y|$, so gilt das *Dominanzprinzip*

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

BEWEIS. Nach (2′) ist

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

Wäre $|x+y| < |y|$, so würde

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

also ein Widerspruch folgen. $\square$

(F′) $| \ |$ sei nicht-archimedisch. Ist $|x| \neq |y|$, so folgt $|x+y| = \max(|x|, |y|)$.

DEFINITION 1.4. Zwei Bewertungen $| \ |_1$ und $| \ |_2$ heißen *äquivalent*, wenn

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

für alle $x, y \in K$ gilt.

Satz 1.1. *Zwei Bewertungen $|\ |_1$ und $|\ |_2$ sind genau dann äquivalent, wenn es eine reelle Zahl $s > 0$ mit*
$$|x|_2 = |x|_1^s$$
für alle $x \in K$ gibt.

Beweis. 1.) Die Funktion $f(x) = x^s$ ist auf $\mathbb{R}_+$ monoton wachsend, also gilt
$$|x|_1 \leq |y|_1 \iff |x|_2 = |x|_1^s \leq |y|_1^s = |y|_2 \,.$$
Damit sind $|\ |_1$ und $|\ |_2$ äquivalent.
2.) Seien $|\ |_1$ und $|\ |_2$ äquivalent. Ist etwa $|\ |_1$ die triviale Bewertung, so folgt für $x \neq 0$
$$|1|_1 \leq |x|_1 \leq |1|_1 \quad \Longrightarrow \quad |1|_2 \leq |x|_2 \leq |1|_2 \,,$$
also $|x|_2 = 1$, d.h. $|\ |_2$ ist ebenfalls die triviale Bewertung. Folglich gilt die Behauptung mit $s = 1$.
Sei nun $|\ |_1$ nicht trivial. Dann existiert ein $a \in K^\times$ mit $|a|_1 \neq 1$. Man kann $|a|_1 > 1$ annehmen (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 $x \in K$. $\square$

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

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

So ist beispielsweise $|\ |_\infty^2$ wegen $(1+1)^2 > 1^2 + 1^2$ keine Bewertung.

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

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

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

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

also

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

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

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

---

†Stetigkeit von exp

‡Regel von L'Hospital

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

$$|x_1 + \cdots + x_n| \leq \max_{1 \leq i \leq n} (|x|_i) .$$

Speziell gilt also

$$|n \cdot 1| = |1 + \cdots + 1| \leq \max(|1|) = 1 . \quad \square$$

KOROLLAR 1.1. *Hat K eine 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 archimedisch auf jedem Teilkörper von K.*

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

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

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

$$|a_i \cdot 1| \leq A .$$

Dann ist

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

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. $\square$

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 $|m| \leq 1$ 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 $0 \leq r < p$, $k \in \mathbb{Z}$, so folgt

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

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

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

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. $\square$

Bemerkung. Die Definition der Bewertung stammt von Kürschak 1913, der obige Satz von Ostrowski 1918. (Beweis von Artin 1932).

KAPITEL 2

Komplettierung bewerteter Körper

1. Die Komplettierung

BEMERKUNG. CANTOR gab 1883 mit der Konstruktion der reellen Zahlen über Cauchy-Folgen eine Komplettierung der rationalen Zahlen an. Dieses Verfahren läßt sich auf allgemeine bewertete Körper übertragen. Im folgenden sei K stets ein bewerteter Körper.

DEFINITION 2.1. (1) Eine Folge (a_n) aus K *konvergiert* gegen $a \in K$, wenn zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ existiert, so daß

$$|a - a_n| < \varepsilon$$

für alle $n \geq n_0$ gilt.
(2) Eine Folge (a_n) aus K heißt *Cauchy-Folge*, wenn zu jedem ε ein $n_0 \in \mathbb{N}$ existiert, so daß

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

für alle $n, m \geq n_0$ gilt.
(3) K heißt *vollständig* (*komplett*) wenn jede Cauchy-Folge konvergiert.

Eigenschaften

(A) Der Grenzwert einer konvergenten Folge ist eindeutig, geschrieben $a = \lim a_n$.
(B) Ist $a = \lim a_n$ und $b = \lim b_n$, so gilt
 (1) $\lim(a_n \pm b_n) = \lim a_n \pm \lim b_n$
 (2) $\lim(a_n \cdot b_n) = \lim a_n \cdot \lim b_n$
 (3) $\lim |a_n| = |a|$

BEWEIS VON (3). Sei $a = \lim a_n$. Nach Kapitel 1, Eigenschaft (D) ist

$$\big||a| - |a_n|\big|_\infty \leq |a - a_n|\,.$$

Für wachsendes n wird die rechte Seite beliebig klein, also ist $\lim |a_n| = |a|$ in $\mathbb{R}$. $\square$

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

Beweis. Zu $\varepsilon = 1$ gibt es ein $n_0 \in \mathbb{N}$ mit $|a_n - a_m| < 1$ für $n, m \geq n_0$.
Sei $M := \max(|a_1|, \ldots, |a_{n_0}|) + 1$.
Für $n \leq n_0$ gilt $|a_n| \leq M$. Für $n > n_0$ ist $|a_n - a_m| < 1$, also ebenfalls

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

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

Satz 2.1. *Sei $\mathfrak{F}$ die Menge aller Folgen (a_n) aus K. Durch*

$$(a_n) + (b_n) := (a_n + b_n)$$
$$(a_n) \cdot (b_n) := (a_n b_n)$$

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 obiger Verknüpfungen einen Teilring von $\mathfrak{F}$ mit Eins.*

Beweis. Sind $(a_n), (b_n) \in \mathfrak{C}$, so gibt es nach (D) ein M in $\mathbb{R}$ mit

$$|a_n| \leq M \qquad \text{und} \qquad |b_n| \leq M$$

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

$$|a_n - a_m| < \varepsilon \qquad \text{und} \qquad |b_n - b_m| < \varepsilon$$

für alle $n, m \geq n_0$. Dann ist

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

und

$$\begin{aligned} |a_n b_n - a_m b_m| &= |a_n (b_m - b_m) + b_m (a_n - a_m)| \\ &\leq |a_n| \, |b_n - b_m| + |b_m| \, |a_n - b_m| \\ &\leq M \, |b_n - b_m| + M \, |a_n - a_m| \\ &< 2\varepsilon M \end{aligned}$$

für alle $n, m \geq n_0$. Also sind $(a_n) - (b_n)$ und $(a_n)(b_n)$ 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. $\square$

Definition 2.2. Sei R ein Ring. Eine nicht-leere Teilmenge I heißt ein *Ideal*, wenn gilt

(1) $a, b \in I \implies a - b \in I$,
(2) $a \in I, \, b \in R \implies ab, by \in I$.

Der *Faktorring* R/I ist definiert als

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

mit den Verknüpfungen

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

Lemma 2.2. *Die Menge $\mathfrak{N}$ der 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 (a_n) und (b_n) Nullfolgen, so ist

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

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

$$|b_n| \leq M$$

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

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

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

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

Beweis. Siehe Aufgabe 5.

Definition 2.3. Ein Teilkörper 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 2.4. 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 2.2. *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

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

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 $(x_m - x'_n)$ 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

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

(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 2.5. 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 2.3. *$\hat{K}_1$ und $\hat{K}_2$ seien Komplettierungen von K_1 bzw. K_2. Ist*

$$f : K_1 \to K_2$$

ein werterhaltender Homomorphismus, so existiert eine eindeutige Fortsetzung

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

die ein werterhaltender Homomorphismus ist.

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

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

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

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

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

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

für alle $n, m \in \mathbb{N}$ ist dann $\big(f(x_n)\big)$ 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 $\big(f(x_n) - f(x'_n)$ eine Nullfolge in K_2. Es folgt

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

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

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

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

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

und

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

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

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

d.h. $\hat{f}$ ist eine Fortsetzung von f.

4.) Eindeutigkeit von $\hat{f}$:

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

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

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

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

also

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

Damit ist $\tilde{f} = \hat{f}$. $\square$

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

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

sind werterhaltende Homomorphismen. Nach Satz 2.3 existieren eindeutige werterhaltende Fortsetzungen

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

Für $x \in K$ gilt

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

also ist

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

eine Fortsetzung von

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

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

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

Enstprechend folgt

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

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

2. Quadratische Gleichungen in vollständigen Körpern

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 2.4. *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

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

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

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

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. $\square$

Beispiel. $t^2 + 3t + 8$ besitzt in $\mathbb{Q}_2$ eine Nullstelle, da $4|8|_2 < |3|_2^2$ ist.

KAPITEL 3

Die p-adischen Zahlen

1. Allgemeine Eigenschaften

LEMMA 3.1. *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 $|x| = 1$. $E := \{x \in K \mid |x| = 1\}$ heißt* Einheitengruppe *von B.*

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

(D) *Ist I ein Ideal von B und $I \nsubseteq M$, so ist $I = B$.*

(E) *Der Faktorring $\bar{K} = B/M$ ist ein Körper. $\bar{K}$ heißt* Restklassenkörper *der Bewertung.*

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 $I \nsubseteq M$ 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 $I = B$. (E) Sei $x + M \in B/M$ von Null verschieden, also $x \neq M$. Dann ist $|x| = 1$, also x Einheit. Wegen

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

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

FOLGERUNG 3.1. *Jedes echte Ideal von B ist in M enthalten. Damit ist M das einzige maximale Ideal von B.*

DEFINITION 3.1. $B = \{x \in K \mid |x| \leq 1\}$ heißt der zur Bewertung gehörige *Bewertungsring*.

BEISPIEL. 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

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

und

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

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. □

DEFINITION 3.2. Sei K ein bewerteter Körper. Die Menge der Werte

$$G := \{|x| \mid x \in K^\times\}$$

heißt *Wertegruppe* der Bewertung.

SATZ 3.1. *G ist bezüglich der Multiplikation eine Untergruppe von $\{a \in \mathbb{R} \mid a > 0\}$.*

BEWEIS. Wegen $1 = |1| \in G$ ist $G \neq \emptyset$. Ist nun $a = |x|, b = |y| \in G$, so folgt $ab^{-1} = |x| \cdot |y|^{-1} = |xy^{-1}| \in G$. □

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 3.2. *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 3.3. Eine Bewertung heißt *diskret*, wenn zu jedem Element der Wertegruppe G eine Umgebung existiert, die kein weiteres Element aus G enthält.

SATZ 3.3. *Eine 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 G 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 $b_0 < 1 < b_1$, daß 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

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

---

†Nach dem Dominanzprinzip

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

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

also

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

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

Definition 3.4. 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.

Bemerkung. Ist p ein Primelement und $e \in K$ mit $|e| = 1$, so ist auch $p' = ep$ Primelement.

Definition 3.5. 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.
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 $0 \le n < p$ annehmen, weil andernfalls mit $n = kp + n'$, $k \in \mathbb{Z}$, $0 \le n' < p$

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

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 3.4. *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 3.2 stimmen die Wertegruppen von K und $\hat{K}$ überein, und nach Satz 3.3 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 3.3 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 3.4 schreibt man abkürzend

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

und nennt dies die *kanonische Darstellung* von x.

SATZ 3.5. *$\hat{K}$ 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 3.4 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 $n \geq n_0$. $\square$

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

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

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

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

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

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

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. $\square$

Rechnen in $\mathbb{Q}_p$

Man schreibt abkürzend

$$a_{n_0} \ldots a_0, a_1 a_2 \ldots \qquad \text{für} \qquad \sum_{n=n_0} a_n p^n = a_{n_0} p^{n_0} + \cdots + a_0 p^0 + a_1 p^1 + \cdots ,$$

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

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

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

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

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

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

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

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

3. Multiplikation: Man führt die Multiplikation formal aus

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

mit

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

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

Beispiel. Es sei $p = 7$.

$$\begin{array}{ccccccccccccc}
 & 1 & 1, & 4 & 1 & 3 & \cdots & \cdot & 2 & 1, & 5 & 4 & 2 \;\cdots \\
\hline
2 & 2 & 8, & 2 & 6 & & \cdots & & & & & & \\
 & 1 & 1, & 4 & 1 & 3 & \cdots & & & & & & \\
 & & 5, & 5 & 20 & 5 & \cdots & & & & & & \\
 & & 0, & 4 & 4 & 16 & \cdots & & & & & & \\
 & & 0, & {}_2 0 & {}_2 2 & {}_5 2 & \cdots & & & & & & \\
\hline
2 & 3 & 0, & 3 & 0 & 3 & \cdots & & & & & &
\end{array}$$

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

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

Hiermit gilt

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

Satz 3.6. (Newtonsches Näherungsverfahren)
Es sei K vollständig bezüglich einer nicht-archimedischen 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

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

(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 3.6 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

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

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

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

HILFSSATZ 3.1. *Jedes $x \neq 0$ aus $\mathbb{Q}_p$ besitzt eine Darstellung*

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

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

SATZ 3.7. *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 3.8. *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 3.6 eine Nullstelle, also ist a ein Quadrat in $\mathbb{Q}_p$. $\square$

Satz 3.9. *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 3.6 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

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

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

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

---

†wegen $\varphi(b^2 - a) = 0$ ist $b^2 - a \in M$
‡in $\mathbb{Z}_2$ ist $x^2 = x$

ERGEBNIS. Quadrate in $\mathbb{Q}_2$: $a = 2^{2k}\,(1 + a_3 2^3 + \cdots)$
Quadrate in $\mathbb{Q}_p$, $p \neq 2$: $a = p^{2k}\,(a_0 + a_1 p + a_2^2 + \cdots)$,
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 3.1. *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 3.8 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 3.7.
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 3.9 ein Quadrat in $\mathbb{Q}_2$, aber bq nach Satz 3.8 kein Quadrat in $\mathbb{Q}_q$.
Also sind $\mathbb{Q}_p$ und $\mathbb{Q}_q$ nicht isomorph. $\square$

DEFINITION 3.6. K heißt *geordneter Körper*, wenn gilt:

(1) K ist bezüglich $\leq$ linear angeordnet.
(2) $a \leq b \quad \Longrightarrow \quad a + c \leq b + c$
(3) $0 \leq a, b \quad \Longrightarrow 0 \quad \leq ab$.

FOLGERUNG 3.2. *$a^2 \geq 0$ für alle $a \in K$.*

HILFSSATZ 3.2. *$\mathbb{Q}$ läßt sich nur auf eine Weise anordnen.*

BEWEIS. Sei $\sqsubseteq$ eine beliebige Anordnung auf $\mathbb{Q}$ und $\leq$ die gewöhnliche Anordnung auf $\mathbb{Q}$. Wegen $1 = 1^2 \sqsupset 0$ ist $n = 1 + \cdots + 1 \sqsupset 0$, also $\frac{n}{m} \sqsupset 0$ für $n, m \in \mathbb{N}$. Es folgt

$$x > 0 \quad \Longrightarrow \quad x \sqsupset 0$$

und damit

$$(*) \qquad x > y \quad \Longrightarrow \quad x - y > 0 \quad \Longrightarrow \quad x - y \sqsupset 0 \quad \Longrightarrow \quad x \sqsupset y \,.$$

Durch Kontraposition ergibt sich $x \sqsubseteq y \implies x \leq y$.
Aus $(*)$ folgt durch Vertauschung von x und y:

$$x \leq y \implies x \sqsubseteq y\,.$$

Also gilt $x \leq y \iff x \sqsubseteq y$. $\square$

KOROLLAR 3.2. *Die p-adischen Körper $\mathbb{Q}_p$ lassen sich nicht anordnen.*

BEWEIS. Eine Anordnung auf $\mathbb{Q}_p$ induziert eine Anordnung auf $\mathbb{Q}$. Nach Hilfssatz 3.2 ist dies die gewöhnliche Anordnung, also $\frac{1}{1-p^3} < 0$. Wegen

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

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

KOROLLAR 3.3. $\mathbb{R}$ *ist zu keinem der Körper $\mathbb{Q}_p$ isomorph.*

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

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

eine Anordnung auf $\mathbb{Q}_p$, was nach Korollar 3.2 nicht möglich ist. $\square$

DEFINITION 3.7. $x, y \in K^\times$ heißen *quadratgleich*, geschrieben $x \overset{q}{\sim} y$, wenn ein $z \in K^\times$ existiert mit $x = z^2 y$.
$\overset{q}{\sim}$ ist Äquivalenzrelation, $K^\times$ zerfällt in *Quadratklassen*: $\{y \mid y \overset{q}{\sim} x\}$, dargestellt durch Repräsentanten $\{1, \ldots\}$.

Quadratklassen einiger Körper:

Körper	Quadratklassen
$\mathbb{R}$	$\{1, -1\}$
$\mathbb{Q}_p,\ p \neq 2$	$\{1, p, a, ap\}$, $\left(\frac{a}{p}\right) = -1$
$\mathbb{Q}_2$	$\{1, 3, 5, 7, 2, 6, 10, 14\}$

KAPITEL 4

Hilbert-Symbole

Im folgenden sei K stets ein Körper mit einer Charakteristik $\neq 2$.

Untersucht werden soll im folgenden die Gleichung

$$(*) \qquad ax^2 + by^2 = z^2$$

für $a, b \in K^\times$. Ist (x_0, y_0, z_0) eine Lösung von $(*)$, so ist auch $\lambda(x_0, y_0, z_0)$ eine Lösung. Es existiert stets die triviale Lösung $(0, 0, 0)$.

Definition 4.1. Der Ausdruck (a, b) mit

$$(a,b) = (a,b)_K := \begin{cases} 1 & \text{falls } (*) \text{ eine nicht-triviale Lösung besitzt} \\ -1 & \text{sonst} \end{cases}$$

heißt *Hilbert-Symbol*.

Eigenschaften

(A) $(a, b) = (b, a)$ (Symmetrie)
(B) $(a, b) = (a, bc^2)$, $c \in K^\times$.

Beweis. Ist (x_0, y_0, z_0) eine Lösung von $(*)$, so ist (x_0c, y_0, z_0c) eine Lösung von $ax^2 + bc^2y^2 = z^2$. □

(C) $(a, 1) = (a, -a) = (a, 1 - a) = 1$

Beweis. $(0, 1, 1)$, $(1, 1, 0)$, $(1, 1, 1)$ sind jeweils Lösungen. □

Beispiel. (1) Wegen $2(\sqrt{2})^2 - 3 \cdot 1^2 = 1^2$ ist $(2, -3)_{\mathbb{R}} = 1$.
(2) $K = \mathbb{Q}$, $(2, -3)_{\mathbb{Q}} = -1$. Denn:
Annahme: Es gibt eine nicht-triviale Lösung (x_0, y_0, z_0) von $2x^2 - 3y^2 = z^2$. Man kann x_0, y_0 und z_0 als ganzzahlig und teilerfremd annehmen (Multiplikation mit dem Hauptnenner und anschließendes Dividieren durch den größten gemeinsamen Teiler).
Ist $x_0 = 3k$, so folgt $z_0 = 3l$. Aus $2 \cdot 3k^2 - y_0^2 = 3l^2$ ergibt sich, daß auch y_0 durch 3 teilbar ist, im Widerspruch zur Voraussetzung.
Folglich gilt $x_0 \not\equiv 0 \bmod 3$.
Aus $2x_0^2 \equiv z_0^2 \bmod 3$ folgt, daß 2 ein Quadrat in $\mathbb{Z}_3$ ist. Dies ist ein Widerspruch.

Definition 4.2. Sei $a \in K^\times$. Definiere

$$H_a := \{b \in K^\times \mid \exists\, x, y \in K : b = x^2 - ay^2\}$$

Dann gilt $(K^\times)^2 \subseteq H_a \subseteq K^\times$.

Hilfssatz 4.1. *Ist a ein Quadrat, so ist $H_a = K^\times$.*

Beweis. Sei $a = c^2$. Dann ist

$$b = \left(\frac{b+1}{2}\right)^2 - a\left(\frac{b-1}{2c}\right)^2 \in H_a$$

für jedes $b \neq 0$. □

Satz 4.1. *H_a ist eine Untergruppe von $K^\times$. Es gilt*

$$b \in H_a \iff (a, b)_K = 1\,.$$

Beweis. (1) Sei $b = x^2 - ay^2$ und $b' = x_1^2 - ay_1^2$. Dann ist

$$bb' = (xx_1 + ayy_1)^2 - a(xy_1 + yx_1)^2,$$

also ist H_a multiplikativ abgeschlossen. Wegen

$$b^{-1} = \left(\frac{x}{b}\right)^2 - a\left(\frac{y}{b}\right)^2 \in H_a$$

ist H_a auch abgeschlossen gegen Inversenbildung, also eine Untergruppe von $K^\times$.
(2) „ $\Rightarrow$ “: Wegen $ay^2 + b \cdot 1^2 = x^2$ ist $(a, b)_K = 1$.
„ $\Leftarrow$ “: Sei $ax_0^2 + by_0^2 = z_0^2$ nicht-trivial. Ist $y_0 \neq 0$, so ist

$$b = \left(\frac{z_0}{y_0}\right)^2 - a\left(\frac{x_0}{y_0}\right)^2 \in H_a$$

Ist $y_0 = 0$, so ist $x_0 \neq 0$, da sonst die Lösung trivial wäre. Also ist $a = \left(\frac{z_0}{x_0}\right)^2$ ein Quadrat. Nach dem Hilfssatz ist dann $H_a = K^\times$, also $b \in H_a$. □

Wegen der Symmetrie des Hilbert-Symbols gilt

Korollar 4.1. $b \in H_a \iff a \in H_b$.

Korollar 4.2. $(a, b)_K = 1 \quad \Longrightarrow \quad (a, bb')_K = (a, b')_K$

Beweis. Sei $b \in H_a$. Dann gilt, weil H_a eine Gruppe ist,

$$bb' \in H_a \iff b' \in H_a. \quad \square$$

Wegen $(a, -a) = 1$ und $(a, 1-a) = 1,\ a \neq 1$, folgen hieraus die Regeln
(D) $(a, b) = (a, -ab)$.
(E) $(a, b) = \big(a, (1-a)b\big), \quad a \neq 1$.

Die Anwendung der Regeln (A) – (E) zur Umformung von Hilbert-Symbolen zeigt folgendes

Beispiel. $(2, 3)_{\mathbb{Q}} = (2, -6)_{\mathbb{Q}} = (2, 6)_{\mathbb{Q}} = (2, -12)_{\mathbb{Q}} = (2, -3)_{\mathbb{Q}} = -1$.

ZIEL: Wann gilt $(a, bb') = (a, b) \cdot (a, b')$?
Dies hängt vom Index der Untergruppe H_a in $K^\times$ ab.

DEFINITION 4.3. Es sei G eine abelsche Gruppe und U eine Untergruppe von G. Definiere auf G eine Äquivalenzrelation

$$a \sim b \iff a^{-1}b \in U\,.$$

Die *Nebenklassen* aU, $a \in G$, bilden bezüglich

$$aU \cdot bU := abU$$

eine Gruppe, die *Faktorgruppe* G/U.
$(G : U) = |G/U|$ heißt *Index* von U in G.

EIGENSCHAFTEN.
(A) $|G| = (G : U) \cdot |U|$.
(B) Für $U \subseteq V \subseteq G$ gilt $(G : U) = (G : V) \cdot (V : U)$.
(C)

$$(G : U) = 2 \iff G = U \cup cU, c^2 \in U \iff (a, b \notin U \quad \Rightarrow \quad ab \in U)$$

SATZ 4.2. $(K^\times : H_a) \leq 2 \iff (a, bb') = (a, b) \cdot (a, b')$ *für alle* $b, b' \in K^\times$.

BEWEIS. (1) „ $\Rightarrow$ “: Nach Korollar 4.2 gilt die Multiplikativität, falls $(a, b) = 1$ oder $(a, b') = 1$ ist.
Sei also $(a, b) = (a, b') = -1$. Nach Satz 4.1 sind dann $b, b' \notin H_a$, also $bb' \in H_a$, weil der Index ≤ 2 ist. Es folgt

$$(a, bb') = 1 = (-1) \cdot (-1) = (a, b) \cdot (a, b')\,.$$

(2) „ $\Leftarrow$ “: Ist $(K^\times : H_a) > 2$, so gibt es $b, b' \notin H_a$ und $b^{-1}b' \notin H_a$. Dann ist wegen $b^2 \in H_a$

$$bb' = b^2(b^{-1}b') \notin H_a,$$

also

$$(a, b) = (a, b') = (a, bb') = -1.$$

Also gilt die Multiplikativität nicht. $\square$

SATZ 4.3. *In* $\mathbb{Q}_p$, $p \neq 2$, *gilt*

$$(a, bb') = (a, b) \cdot (a, b')\,.$$

BEWEIS. $(\mathbb{Q}_p^\times)^2 \subseteq H_a \subseteq \mathbb{Q}_p^\times$. Da $\mathbb{Q}_p$ in 4 Quadratklassen zerfällt, gilt

$$(\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2) = 4\,.$$

Nach der Indexformel ist $(\mathbb{Q}_p^\times : H_a) \leq 2$, falls $\mathbb{Q}_p^2$ echt in H_a enthalten ist, also ein Element in H_a existiert, das kein Quadrat ist.
FALLUNTERSCHEIDUNG:
1. Fall: Ist a ein Quadrat, so ist nach Hilfssatz 4.1 $H_a = \mathbb{Q}_p^\times$, also

$$(\mathbb{Q}_p^\times : H_a) = 1 \leq 2\,.$$

2. Fall: Sei a kein Quadrat. Es gibt zwei Unterfälle:

(a) $a = p^{2k+1}b$, $|b| = 1$. Dann folgt wegen $(a,-a) = 1$, also $-a \in H_a$

$$-a = p^{2k+1}(-b) \in H_a \setminus (\mathbb{Q}_p^\times)^2 .$$

(b) $a \overset{q}{\sim} b$ (also $b = ax^2$) mit $b \in \mathbb{N}$, $b < p$, $\left(\frac{b}{p}\right) = -1$. Wähle b minimal. Dann ist $\left(\frac{b-1}{p}\right) = 1$.
Jetzt sind nochmals zwei Fälle zu unterscheiden:
(i) Ist $\left(\frac{-1}{p}\right) = 1$, so ist $(a,-b) = (b,-b) = 1$ und

$$\left(\frac{-b}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{b}{p}\right) = -1$$

also $-b \notin H_a \setminus (\mathbb{Q}_p^\times)^2$.
(ii) Ist $\left(\frac{-1}{p}\right) = -1$, so ist $(a, 1-b) = (b, 1-b) = 1$ und

$$\left(\frac{1-b}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b-1}{p}\right) = -1,$$

folglich $1 - b \in H_a \setminus (\mathbb{Q}_p^\times)^2$ Die Behauptung folgt nun aus dem vorangehenden Satz 4.2. $\square$

Für endliche Körper sind die Hilbert-Symbole trivial.

Satz 4.4. *Sei $|K| = q < \infty$, q ungerade. Für alle $a, b \in K^\times$ ist*

$$1 = ax^2 + by^2$$

lösbar, also $(a,b)_K = 1$.

Beweis. Betrachte die Mengen

$$\{ax^2 \mid x \in K\} \qquad \text{und} \qquad \{1 - by^2 \mid y \in K\} .$$

Sie enthalten jeweils $\frac{q+1}{2}$ Elemente:

$$\begin{aligned} ax_1^2 = ax_2^2 \quad &\Longrightarrow \quad x_1 = \pm x_2 \\ 1 - by_1^2 = 1 - by_2^2 \quad &\Longrightarrow \quad y_1 = \pm y_2 . \end{aligned}$$

Sie sind nicht disjunkt, weil sonst $q+1$ Elemente in K existieren würden.
Also gibt es x_0, y_0 mit

$$ax_0^2 = 1 - by_0^2 \quad \Longrightarrow \quad (a,b)_K = 1 . \quad \square$$

Bemerkung. Wegen der Symmetrie der Hilbert-Symbole gilt in Satz 4.3 auch

$$(aa', b) = (a,b)(a',b).$$

Weiterhin gilt Satz 4.3 auch für $p = 2$. Zum Beweis siehe etwa Borewicz, Shafarevich *Zahlentheorie* (Birkhäuser 1966).

Berechnung der Hilbert-Symbole in $\mathbb{Q}_p$:

Zunächst ist wegen (B) und (D)

$$(p,p) \overset{(D)}{=} (p,-p^2) \overset{(C)}{=} (p,-1).$$

Sei $x = p^k a$, $y = p^l b$ mit $|a| = |b| = 1$. Dann ist

$$\begin{aligned}(x,y) &= (x,p)^l \cdot (x,b)\\ &= (p,p)^{kl} \cdot (a,p)^l \cdot (p,b)^k \cdot (a,b)\\ &= (p,-1)^{kl} \cdot (p,a)^l \cdot (p,b)^k \cdot (a,b)\\ &= \big(p, \underbrace{(-1)^{kl} a^l b^k}_{=:c,\ |c|=1}\big) \cdot (a,b)\,.\end{aligned}$$

Ergebnis: (x,y) kann in $\mathbb{Q}_p$ berechnet werden, wenn (p,c) und (a,b) für $|c| = |a| = |b| = 1$ bekannt sind.

Sei $p \neq 2$ und $|a| = 1$, also

$$a = a_0 + a_1 p + a_2 p^2 + \dots, \qquad 0 \leq a_i < p, \quad a_0 \neq 0$$

a_0 ist eindeutig durch a bestimmt, und es ist $|a - a_0| < 1$.

Satz 4.5. *a ist genau dann ein Quadrat in $\mathbb{Q}_p$, wenn $\left(\frac{a_0}{p}\right) = 1$ ist.*

Bemerkung. Für $a \in \mathbb{Z}$ gilt $a \equiv a_0 \bmod p$, also

$$\left(\frac{a}{p}\right) = \left(\frac{a_0}{p}\right)\,.$$

Satz 4.6. *Sei $K = \mathbb{Q}_p$, $p \neq 2$, $|a| = |b| = 1$. Dann ist*

$$(a,b) = 1 \qquad \textit{und} \qquad (p,a) = \left(\frac{a_0}{p}\right)\,.$$

Beweis. (1) $(a,b) = 1$:
Nach Satz 4.4 gilt

$$a x_0^2 + b y_0^2 - 1 \equiv 0 \bmod p, \qquad 0 \leq x_0, y_0 < p$$

Es ist also $x_0 \neq 0$ oder $y_0 \neq 0$. Ohne Beschränkung der Allgemeinheit sei $x_0 \neq 0$.
Betrachte das Polynom

$$f(x) = a x^2 + b y_0^2 - 1, \qquad f'(x) = 2ax$$

Wegen $|f(x_0)| < 1 = |f'(x_0)|^2$ existiert eine Nullstelle von f in $\mathbb{Q}_p$, also ist $(a,b) = 1$.

(2) $(p,a) = \left(\frac{a_0}{p}\right)$:

1. Fall: a ist Quadrat in $\mathbb{Q}_p$, also $\left(\frac{a_0}{p}\right) = 1$. Es folgt

$$(p,a) = (p,1) = 1 = \left(\frac{a_0}{p}\right)$$

2. Fall: a ist kein Quadrat in $\mathbb{Q}_p$, also $\left(\frac{a_0}{p}\right) = -1$.
Wäre $(p,a) = 1$, so wäre $a \in H_p$, also $a = u^2 - pv^2$. Ist $|u| = |p|^k$ und $|v| = |p|^l$, so ist

$$|u^2| = |p|^{2k} \qquad \text{und} \qquad |pv^2| = |p|^{2l+1}\,.$$

Also ist $|u^2| \neq |pv^2|$. Nach dem Dominanzprinzip ist

$$1 = |a| = |u^2 - pv^2| = \max(|u^2|, |pv^2|)\,,$$

also $|u^2| \leq 1$ und $|pv^2| \leq 1$. Es folgt $2k \geq 0$ und $2l+1 \geq 0$, also $k \geq 0$ und $l \geq 0$. Damit ergibt sich

$$a = u^2 - pv^2 \equiv u^2 \bmod p\,,$$

d.h. a Quadrat, im Widerspruch zur Wahl von a. □

Bemerkung. $p = 2$. Sei $|a| = 1$. Zu a existiert ein eindeutiges a_0 mit $0 \leq a_0 < 8$ und $a \equiv a_0 \bmod 8$ oder $|a - a_0| \leq |2|^3$. Die kanonische Darstellung lautet dann

$$a = \underbrace{1 + a_1 2 + a_2 2^2}_{=: a_0 \in \{1,3,5,7\}} + a_3 2^3 + \ldots$$

Satz 4.7. *$K = \mathbb{Q}_2$. Sei $|a| = |b| = 1$. Dann ist*

$$(a,b) = (-1)^{\frac{a_0-1}{2}\frac{b_0-1}{2}} \qquad \textit{und} \qquad (2,a) = (-1)^{\frac{a_0^2-1}{8}}\,.$$

(Für $a, b \in \mathbb{Z}$ können a_0, b_0 wieder durch a, b ersetzt werden.)

Beweis. siehe Borewicz, Shafarevich.

Beispiel. Für welche Primzahlen p existiert eine nicht-triviale Lösung von

$$(**) \qquad 2x^2 - 15y^2 + 14z^2 = 0$$

in $\mathbb{Q}_p$?
$(**)$ ist genau dann nicht-trivial lösbar, wenn $(2x)^2 = 30y^2 - 7\,(2z)^2$ nicht-trivial lösbar ist, d.h. wenn $(30,-7)_p := (30,-7)_{\mathbb{Q}_p} = 1$ ist. Man findet

$$\begin{aligned}
(30,-7)_p &\overset{\text{Satz 4.6}}{=} 1 \text{ für } p > 7\\
(30,-7)_7 &= (30,-1)_7\,(30,7)_7 = \left(\tfrac{30}{7}\right) = 1\\
(30,-7)_5 &= (6,-7)_5\,(5,-7)_5 = \left(\tfrac{-7}{5}\right) = -1\\
(30,-7)_3 &= (3,-7)_3 = \left(\tfrac{-7}{3}\right) = -1\\
(30,-7)_2 &= (2,-7)_2\,(15,-7)_2 = (-1)^{\frac{49-1}{8}}\,(-1)^{\frac{14}{2} - \left(\frac{8}{2}\right)} = 1
\end{aligned}$$

Bemerkung. Hilbert-Symbole in $\mathbb{R}$ lassen sich einfach berechnen. Es gilt

$$(a,b)_{\mathbb{R}} = \begin{cases} 1 & \text{falls } a > 0 \text{ oder } b > 0\\ -1 & \text{falls } a < 0 \text{ und } b < 0\end{cases}$$

Beweis. (1) Sei etwa $a > 0$. Dann ist $(1, 0, \sqrt{a})$ Lösung.
(2) Sei nun $a, b < 0$. Dann ist

$$\underbrace{ax^2 + by^2}_{\leq 0} = \underbrace{z^2}_{\geq 0}\,.$$

Also existiert nur die triviale Lösung $x = y = z = 0$. □

SATZ 4.8. *Es ist* $(a, bb')_{\mathbb{R}} = (a, b)_{\mathbb{R}} \cdot (a, b')_{\mathbb{R}}$.

BEWEIS. (1) Sei $a > 0$: Dann ist $(a, c)_{\mathbb{R}} = 1$ für alle $c \in \mathbb{R}^{\times}$.
(2) Sei $a < 0$: Dann gilt $\operatorname{sgn}(bb') = \operatorname{sgn}(b) \cdot \operatorname{sgn}(b')$. □

BEZEICHNUNGEN: Zur Abkürzung schreiben wir

$$(a, b)_{\mathbb{Q}_p} = (a, b)_p \qquad \text{und} \qquad (a, b)_{\mathbb{R}} = (a, b)_{\infty} .$$

HILBERT benutzte folgende Schreibweise

$$(a, b)_p = \left(\frac{a, b}{p}\right) \qquad \text{und} \qquad (a, b)_{\infty} = \left(\frac{a, b}{\infty}\right) .$$

BEMERKUNG. Für $a, b \in \mathbb{Q} \subseteq \mathbb{Q}_p, \mathbb{R}$ ist $(a, b)_p$ für alle $p \in \mathbb{P} \cup \{\infty\}$ definiert.

KOROLLAR 4.3. *Für $a, b \in \mathbb{Q}^{\times}$ ist $(a, b)_p = 1$ für fast alle $p \in \mathbb{P} \cup \{\infty\}$, d.h. bis auf endlich viele Ausnahmen.*

BEWEIS. Multipliziert man die Ausgangsgleichung $(*)$ mit dem Hauptnenner, so genügt es die Behauptung für $a', b' \in \mathbb{Z}$ zu zeigen.
Ist $p \neq 2, \infty$ und p teilerfremd zu a', b', so ist

$$(a, b)_p = (a', b')_p = 1.$$

Es bleiben nur endlich viele p übrig: $p = 2, \infty$ und die Primteiler von $a'b'$. □

KOROLLAR 4.4 (HILBERTSCHE PRODUKTFORMEL). *Für alle $a, b \in \mathbb{Q}^{\times}$ gilt*

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (a, b)_p = 1.$$

Wegen des obigen Korollars ist dieses Produkt sinnvoll.

BEWEIS. Wegen

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (a, bb')_p = \prod_{p \in \mathbb{P} \cup \{\infty\}} (a, b)_p \cdot \prod_{p \in \mathbb{P} \cup \{\infty\}} (a, b')_p$$

gilt die Produktformel für bb', wenn sie für b und b' gilt.
Zu untersuchen sind also folgende drei Fälle für $q, q' \in \mathbb{P}$:

	a	b
1. Fall	-1	-1
2. Fall	q	-1
3. Fall	q	q'

1. Fall: $a = -1$, $b = -1$: Es ist $(-1, -1)_p = 1$ für $p \in \mathbb{P}$, $p \neq 2$. Also ist

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (-1, -1)_p = (-1, -1)_2 \cdot (-1, -1)_{\infty} \overset{\text{Satz 4.7}}{=} (-1) \cdot (-1) = 1.$$

2. Fall: (a) $a = q = 2$, $b = -1$:

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (2, -1)_p = (2, -1)_2 \cdot (2, -1)_{\infty} = (-1)^{\frac{(-1)^2 - 1}{8}} = 1.$$

(b) $q \neq 2$:

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (q,-1)_p = (q,-1)_2 \cdot (q,-1)_\infty \cdot (q,-1)_q = (-1)^{\frac{q-1}{2}} \cdot 1 \cdot \left(\frac{-1}{q}\right) = 1.$$

Nach dem 1. Ergänzungssatz zum Reziprozitätsgesetz ist $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$.

3. Fall: (a) $q = q'$: $(q,q) \overset{\text{(C)}}{=} (q,-1)$: siehe 2. Fall.
(b) $q < q'$, $q = 2$:

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (2,q')_p = (2,q')_2 \cdot (2,q')_\infty \cdot (2,q')_{q'} = (-1)^{\frac{q'^2-1}{8}} \cdot 1 \cdot \left(\frac{2}{q'}\right) = 1.$$

Nach dem 2. Ergänzungssatz zum Reziprozitätsgesetz ist $\left(\frac{2}{q'}\right) = (-1)^{\frac{q'^2-1}{8}}$.
(c) $2 < q < q'$:

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (q,q')_p = (-1)^{\frac{q-1}{2}\frac{q'-1}{2}} \cdot (q,q')_q \cdot (q,q')_{q'} \overset{\text{Satz 4.6}}{=} (-1)^{\frac{q-1}{2} \cdot \frac{q'-1}{2}} \cdot \left(\frac{q'}{q}\right) \cdot \left(\frac{q}{q'}\right) = 1.$$

Nach dem Reziprozitätsgesetz ist $\left(\frac{q}{q'}\right) \cdot \left(\frac{q'}{q}\right) = (-1)^{\frac{q-1}{2} \cdot \frac{q'-1}{2}}$. $\square$

Bemerkung. Beim Beweis der Produktformel werden im wesentlichen nur die Reziprozitätsgesetze benutzt. Umgekehrt folgen diese aus der Produktformel.

KAPITEL 5

Das Lokal-Global-Prinzip

SATZ 5.1. *Die Gleichung*

$$ax^2 + by^2 + cz^2 = 0, \qquad a, b, c \in \mathbb{Q}$$

ist genau dann nicht-trivial in $\mathbb{Q}$ *lösbar, wenn sie in* $\mathbb{Q}_p$ *für alle* $p \in \mathbb{P} \cup \{\infty\}$ *nicht-trivial lösbar ist.*

BEMERKUNG. HASSE formulierte diesen Satz 1923 für beliebige quadratische Formen. Man spricht auch vom Hasse-Prinzip oder dem Lokal-Global-Prinzip. In diesem Fall sind $\mathbb{Q}$ der globale und $\mathbb{Q}_p$ die lokalen Körper.

Zum Beweis von Satz 5.1 benötigen wir folgendes

LEMMA 5.1. *Es seien* $a, b, c \in \mathbb{N}$, $abc \neq 1$ *und quadratfrei. Existieren nicht-triviale Lösungen von*

$$ax^2 + by^2 - cz^2 \equiv 0 \bmod p$$

für alle Primzahlen $p|abc$, *so gibt es eine nicht-triviale Lösung von*

$$ax^2 + by^2 - cz^2 = 0$$

in $\mathbb{Q}$.

BEWEIS. 1. Besitzt ein zweigliedriger Ausdruck

$$ax^2 + by^2 = 0$$

in einem Körper K eine nicht-triviale Lösung (x_0, y_0), so gibt es eine Zerlegung in Linearfaktoren:
Sei $y_0 \neq 0$. Dann gilt

$$ax^2 + by^2 = a y_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0)\,.$$

Für $p|abc$ gilt also

$$ax^2 + by^2 - cz^2 \equiv (\alpha_p x + \beta_p y + \gamma_p z)(\alpha'_p x + \beta'_p y + \gamma'_p z) \bmod p$$

(Auf der linken Seite steht ein zweigliedriger Ausdruck, weil einer der Koeffizienten $\equiv 0 \bmod p$ ist.)

Das Kongruenzsystem

$$\alpha \equiv \alpha_p \bmod p,$$

wobei p alle Primzahlen durchläuft, die abc teilen, besitzt nach dem Chinesischen Restsatz eine Lösung.
Analog existieren Lösungen der Kongruenzsysteme

$$\beta \equiv \beta_p,\ \gamma \equiv \gamma_p,\ \alpha' \equiv \alpha'_p,\ \beta \equiv \beta'_p,\ \gamma' \equiv \gamma'_p \bmod p\,.$$

Hiermit ist also

$$ax^2 + by^2 - cz^2 \equiv (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z) \bmod p$$

für alle $p|abc$, also

$$ax^2 + by^2 - cz^2 \equiv (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z) \bmod abc\,. \tag{1}$$

2. Durch

$$\begin{array}{lll} 0 & \leq x & < \sqrt{bc} \\ 0 & \leq y & < \sqrt{ac} \\ 0 & \leq z & < \sqrt{ab} \end{array} \tag{2}$$

wird ein Quader im $\mathbb{R}^3$ beschrieben. Sei S die Menge der Punkte $(x, y, z) \in \mathbb{Z}^3$, die den Ungleichungen (2) genügen.

Die Anzahl der $x \in \mathbb{Z}$ mit $0 \leq x < \sqrt{bc}$ ist

$$\begin{cases} \sqrt{bc} & \text{falls } \sqrt{bc} \in \mathbb{Z} \\ \left[\sqrt{bc}\right] + 1 & \text{falls } \sqrt{bc} \notin \mathbb{Z}\,, \end{cases}$$

also stets $\geq \sqrt{bc}$ und $> \sqrt{bc}$, falls $\sqrt{bc} \notin \mathbb{Z}$.
Analog für y und z.

Wegen $abc \neq 1$ und quadratfrei ist $\sqrt{bc}$, $\sqrt{ac}$ oder $\sqrt{ab}$ irrational. Also ist die Anzahl der Punkte aus S

$$|S| > \sqrt{bc}\sqrt{ac}\sqrt{ab} = abc\,.$$

Setzt man die Punkte aus S in $\alpha x + \beta y + \gamma z$ ein, so folgt, da es nur abc Restklassen mod abc gibt, nach dem Schubfachprinzip, daß zwei Punkte $(x_1, y_1, z_1) \neq (x_2, y_2, z_2)$ in S existieren, für die

$$\alpha x_1 + \beta y_1 + \gamma z_1 \equiv \alpha x_2 + \beta y_2 + \gamma z_2 \bmod abc$$

gilt. Setzt man nun $x_0 = x_1 - x_2$, $y_0 = y_1 - y_2$, $z_0 = z_1 - z_2$, so gilt

$$\alpha x_0 + \beta y_0 + \gamma z_0 \equiv 0 \bmod abc$$

und $(x_0, y_0, z_0) \neq (0, 0, 0)$, also nach (1)

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \bmod abc\,. \tag{3}$$

Wegen

$$|x_0| < \sqrt{bc}, \quad |y_0| < \sqrt{ac}, \quad |z_0| < \sqrt{ab}$$

ist

$$-abc < -cz_0^2 \leq ax_0^2 + by_0^2 - cz_0^2 \leq ax_0^2 + by_0^2 < 2abc.$$

Es gibt also nur zwei Fälle:

(a) $ax_0^2 + by_0^2 - cz_0^2 = 0$
(b) $ax_0^2 + by_0^2 - cz_0^2 = abc.$

Im Fall (a) ist (x_0, y_0, z_0) eine nicht-triviale Lösung in $\mathbb{Q}$.
Im Fall (b) folgt

$$a\,(x_0 z_0 + b y_0)^2 + b\,(y_0 z_0 - a x_0)^2 - c\,(z_0^2 + ab)^2 = 0\,.$$

Ist $z_0^2 + ab \neq 0$, so ergibt dies eine nicht-triviale Lösung.
Ist $z_0^2 + ab = 0$, so gilt

$$a\,(b z_0)^2 + b\,(\underbrace{ab}_{\neq 0})^2 - c \cdot 0 = 0,$$

also $(bz_0, ab, 0)$ nicht-triviale Lösung. $\square$

Beweis von Satz 5.1. Sei

$$ax^2 + by^2 + cz^2 = 0, \qquad a, b, c \in \mathbb{Q}$$

nicht-trivial lösbar in $\mathbb{Q}_p$ für alle $p \in \mathbb{P} \cup \{\infty\}$.

Reduktionsschritte:

(1) Man kann $a, b, c \in \mathbb{Z}$ (Sonst multipliziere man die Gleichung mit dem Hauptnenner) und $\neq 0$ (Ist etwa $a = 0$, so ist $(1, 0, 0)$ eine nicht-triviale Lösung) annehmen.

(2) Die Lösbarkeit in $\mathbb{R} = \mathbb{Q}_\infty$ bedeutet, daß a, b, c nicht gleiches Vorzeichen haben. Man kann also ohne Beschränkung der Allgemeinheit $a, b > 0$ und $c < 0$ annehmen, also

$$ax^2 + by^2 - |c| z^2 = 0, \qquad a, b, |c| \in \mathbb{N}$$

(3) Sei p gemeinsamer Teiler von a und b, also

$$a = pa', \quad b = pb'\,.$$

Dann ist

$$pax^2 + pby^2 + pcz^2 = a'(px)^2 + b'(py)^2 + pcz^2\,.$$

Man kann also annehmen: Jede Primzahl p teilt höchstens einen der Koeffizienten.

(4) Ist $ab|c| = 1$,so folgt $a = b = |c| = 1$.
Man hat also die Form

$$x^2 + y^2 - z^2 = 0\,,$$

die die nicht-triviale Lösung $(1, 0, 1)$ besitzt. Diesen Fall kann man daher ausschließen und $ab|c| \neq 1$ voraussetzen.

Mit Lemma 5.1 folgt dann die Lösbarkeit in $\mathbb{Q}$. $\square$

Korollar 5.1. $(a, b)_{\mathbb{Q}} = 1 \iff \forall\, p \in \mathbb{P} \cup \{\infty\} : (a, b)_p = 1$.

Bemerkung. Wegen der Produktformel

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (a, b)_p = 1$$

braucht man in dieser Äquivalenz das Symbol $(a, b)_p$ für ein p nicht zu prüfen, etwa für $p = 2$, da gerade die Berechnung dieses Symbols häufig Schwierigkeiten bereitet.

Wir erhalten

$$\begin{aligned}
& ax^2 + by^2 = cz^2 \text{ nicht-trivial lösbar in } \mathbb{Q} \\
\iff\ & acx^2 + bcy^2 = (cz)^2 \text{ nicht-trivial lösbar in } \mathbb{Q} \\
\iff\ & (ac, bc)_{\mathbb{Q}} = 1 \\
\iff\ & \forall\, p \in \mathbb{P} \cup \{\infty\},\ p \neq 2 : (ac, bc)_p = 1 \\
\iff\ & (ac, bc)_\infty = 1 \text{ und } (ac, bc)_p = 1 \text{ für } p|abc,\ p \neq 2 \\
\iff\ & (ac > 0 \ \vee\ bc > 0) \ \wedge\ (ac, bc)_p = 1 \text{ für } p|abc,\ p \neq 2
\end{aligned}$$

Beispiel. Besitzt die Gleichung

$$37x^2 - 13y^2 = 31z^2$$

eine nicht-triviale Lösung in $\mathbb{Q}$? Dies ist genau dann der Fall, wenn

$$(31 \cdot 37, -13 \cdot 31)_p = 1 \quad \text{für} \quad p \in \{13, 31, 37\}$$

ist. Man findet

$p = 13$:

$$(31 \cdot 37, -13 \cdot 31)_{13} = (31 \cdot 37, 13) = \left(\frac{31 \cdot 37}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1\,.$$

$p = 31$:

$$(31 \cdot 37, -13 \cdot 31)_{31} = (31 \cdot 37, 13 \cdot 37)_{31} = (31, 13 \cdot 37)_{31} = \left(\frac{13 \cdot 37}{31}\right) = \left(\frac{16}{31}\right) = 1\,.$$

$p = 37$:

$$(31 \cdot 37, -13 \cdot 31)_{37} = \left(\frac{-13 \cdot 31}{37}\right) = \left(\frac{4}{37}\right) = 1\,.$$

Damit ist die obige Gleichung nicht-trivial lösbar: Tatsächlich gilt

$$37 \cdot 2^2 - 13 \cdot 3^2 = 31 \cdot 1^2\,.$$

Korollar 5.2. *Eine quadratische Form über $\mathbb{Q}$*

$$q(x, y, z) = ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz$$

besitzt in $\mathbb{Q}$ eine nicht-triviale Nullstelle, wenn q in $\mathbb{Q}_p$ für alle $p \in \mathbb{P} \cup \{\infty\}$ eine nicht-triviale Nullstelle besitzt.

Beweis. Dies folgt, weil sich jede quadratische Form mittels quadratischer Ergänzung auf Diagonalform transformieren läßt. □

Methode:

(A) Sei $a = 0$. Dann gilt

$$2x\,(dy + ez) = -by^2 - cz^2 - 2fyz\,.$$

Wählt man $y, z \in \mathbb{Q}$ so, daß $dy + ez \neq 0$ ist, so kann man $x \in \mathbb{Q}$ berechnen. ($d = e = 0$ bedeutet, daß x nicht in q auftritt. Dann ist aber $(1, 0, 0)$ eine nicht-triviale Lösung.)

(B) Sei $a \neq 0$. Durch quadratische Ergänzung ergibt sich

$$aq = (ax + dy + ez)^2 + By^2 + Cz^2 + 2Fyz.$$

Ist $B = 0$, so erhält man Lösungen wie im Fall (A).
Ist $B \neq 0$, so folgt

$$aBq = B\,(ax + dy + ez)^2 + (By + Fz)^2 + C'z^2\,.$$

Hiermit haben wir die Diagonalform erreicht und können darauf das Lokal-Global-Prinzip anwenden.

Berechnung aller Lösungen, falls eine Lösung bekannt ist:

Betrachte wieder die quadratische Form

$$q(x,y,z) = ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz\,.$$

Sei (x_0, y_0, z_0) eine nicht-triviale Lösung. Transformiere

$$\begin{aligned} x &= x_0 u \\ y &= y_0 u + v \\ z &= z_0 u + w \end{aligned}$$

Dann ist

$$q(x,y,z) = f(x_0 u, y_0 u + v, z_0 u + w) = Q(u,v,w) = Au^2 + Bv^2 + Cw^2 + \cdots$$

Wegen $Q(1,0,0) = q(x_0,y_0,z_0) = 0$ ist der Koeffizient $A = 0$ (Fall (A) bei der Diagonalisierung). Bei vorgegebenen v, w kann man dann u und damit x, y, z berechnen.

Beispiel. Es sei

$$q(x,y,z) = 37x^2 - 13y^2 - 31z^2$$

Eine Lösung ist $(2,3,1)$. Transformiere

$$\begin{aligned} x &= 2u \\ y &= 3u + v \\ z &= u + w \end{aligned}$$

Dann folgt

$$37(2u)^2 - 13(3u+v)^2 - 31(u+w)^2 = -13(6uv + v^2) - 31(2uw + w^2) = 0\,,$$

also

$$(-78v - 62w)u = 13v^2 + 31w^2\,.$$

Wähle v, w beliebig, $-78v - 62w \neq 0$. Dann ist

$$u = \frac{13v^2 + 31w^2}{-78v - 62w}\,,$$

also nach Multiplikation mit dem Nenner

$$\begin{aligned} x &= 2(13v^2 + 31w^2) \\ y &= 3(13v^2 + 31w^2) + v\,(-78v - 62w) \\ z &= (13v^2 + 31w^2) + w\,(-78v - 62w) \end{aligned}$$

Dies ist eine Parameterdarstellung sämtlicher Lösungen.
Der Fall $78v + 62w = 0$ ergibt wieder die Ausgangslösung.
Setzt man z.B. $v = w = 1$, so erhält man die Lösung $(88, -8, -96) = 8(11, -1, -12)$.
(vergleiche GAUSS: Disquisitiones Arithmeticae, Artikel 294-300.)

BEMERKUNG. Um die Lösungen der Gleichung

$$a\mathfrak{x}^2 + b\mathfrak{y}^2 + 2d\mathfrak{x}\mathfrak{y} + 2e\mathfrak{x} + 2f\mathfrak{y} + c = 0\,, \qquad c \in \mathbb{Z} \setminus \{0\}$$

zu finden, subsitutiert man zunächst

$$\mathfrak{x} = \frac{x}{z} \qquad \text{und} \qquad \mathfrak{y} = \frac{y}{z}\,.$$

Multipliziert man nun mit z, so ergibt sich wieder

$$ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz = 0\,,$$

und man kann die oben beschriebene Methode anwenden.

KAPITEL 6

Quadratische Erweiterungen

1. Quadratische Zahlkörper

DEFINITION 6.1. Es sei K ein Körper und $d \in K$ fest gewählt. Definiere auf $L = K \times K$ für $a, b, a', b' \in K$

$$(*) \qquad \begin{aligned} (a,b) + (a',b') &:= (a + a', b + b') \\ (a,b) \cdot (a',b') &:= (aa' + dbb', ab' + ba') \end{aligned}$$

SATZ 6.1. (1) *Bezüglich der Verknüpfungen $(*)$ ist L ein kommutativer Ring.*
(2) *L ist genau dann ein Körper, wenn d kein Quadrat in K ist.*

BEWEIS. (1) Man rechnet leicht nach, daß L ein kommutativer Ring mit dem Einselement $(1,0)$ ist.
(2) Aus

$$(a,b) \cdot (x,y) = (1,0) \qquad \text{folgt} \qquad \begin{aligned} ax + dby &= 1 \\ bx + ay &= 0 \end{aligned}$$

d.h. (a,b) ist in L genau dann invertierbar, wenn die Determinante $a^2 - db^2 \neq 0$ ist.

Ist d ein Quadrat, etwa $d = c^2$, so ist $(c,1)$ nicht invertierbar, also L kein Körper.

Ist d kein Quadrat und $(a,b) \neq (0,0)$, so ist die Determinante $a^2 - db^2 \neq 0$ (aus $a^2 - db^2 = 0$ würde $d = \frac{a^2}{b^2}$ folgen) und damit (a,b) invertierbar, also ist L ein Körper. $\square$

Eigenschaften

(A) Durch $x \cdot (a,b) := (xa, xb)$, $x \in K$, wird L ein Vektorraum über K. Wegen $(a,b) = a\,(1,0) + b\,(0,1)$ bilden $1 = (1,0)$ und $\vartheta = (0,1)$ eine Basis von L über K. In dieser Schreibweise ist $(a,b) = a + b\vartheta$.
Wegen
$$\vartheta^2 = (0,1)\,(0,1) = (d,0) = d\,(1,0) = d$$
schreibt man auch $\alpha = (a,b) = a + b\sqrt{d}$ und $L = K(\sqrt{d})$, $K \subseteq K(\sqrt{d})$.

(B) Die Abbildung
$$K(\sqrt{d}) \to K(\sqrt{d}), \quad \alpha = a + b\sqrt{d} \mapsto \bar{\alpha} = a - b\sqrt{d}$$
heißt *Konjugation*. Es gilt
$$\bar{\bar{\alpha}} = \alpha\,, \qquad \overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}\,, \qquad \overline{\alpha\beta} = \bar{\alpha} \cdot \bar{\beta}\,.$$

(C) Für $\alpha = a + b\sqrt{d} \in K(\sqrt{d})$ heißen

$$\begin{aligned} \mathrm{N}\alpha &= \alpha\bar{\alpha} = a^2 - b^2 d \in K \\ \mathrm{S}\alpha &= \alpha + \bar{\alpha} = 2a \in K \end{aligned}$$

Norm und *Spur* von α. Es gilt

$$\begin{aligned} \mathrm{N}(\alpha\beta) &= \alpha\beta \cdot \overline{\alpha\beta} = \alpha\bar{\alpha} \cdot \beta\bar{\beta} = \mathrm{N}\alpha\,\mathrm{N}\beta \\ \mathrm{S}(\alpha + \beta) &= \mathrm{S}\alpha + \mathrm{S}\beta\,. \end{aligned}$$

Ist d kein Quadrat, so gilt

$$\mathrm{N}\alpha = 0 \iff a^2 - b^2 d = 0 \iff \alpha = 0\,.$$

Division:

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = \frac{1}{\mathrm{N}\beta}\,\alpha\bar{\beta}\,.$$

Speziell:

$$\alpha^{-1} = \frac{\bar{\alpha}}{\alpha\bar{\alpha}} = \frac{1}{\mathrm{N}\alpha}\,\bar{\alpha} = \frac{a - b\sqrt{d}}{a^2 - b^2 d}\,.$$

(D) Jedes Element α ist Nullstelle eines quadratischen Polynoms

$$f_\alpha(t) = t^2 - \mathrm{S}\alpha \cdot t + \mathrm{N}\alpha = (t - \alpha)(t - \bar{\alpha}) \in K[t]\,.$$

Bemerkung. Ist $d = d'c^2$, $c \neq 0$, so ist

$$f : K(\sqrt{d}) \to K(\sqrt{d'})\,, \quad (a, b) \mapsto (a, bc)$$

ein K-Isomorphismus:

$$\begin{aligned} f\big((a,b) \cdot (a',b')\big) &= f(aa' + dbb', ba' + ab') \\ &= (aa' + dbb', cba' + cab') \\ &= (aa' + d'c^2 bb', ab'c + bca') \\ &= (a, bc) \cdot (a', b'c) \\ &= f\big((a,b)\big) \cdot f\big((a',b')\big)\,. \end{aligned}$$

Man kann zeigen, daß zu jeder Quadratklasse bis auf Isomorphie genau eine quadratische Erweiterung existiert. Ist $K = \mathbb{Q}$, so kann man d als quadratfrei voraussetzen:

$$d = \pm p_1 \ldots p_r\,, \qquad p_i \text{ paarweise verschieden}$$

Für $d > 0$ kann man $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$ in $\mathbb{R}$ (*reell-quadratisch*) und für $d < 0$ $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$ in $\mathbb{C}$ (*imaginär-quadratisch*) einbetten.

Definition 6.2. $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ heißt *ganz*, wenn

$$\mathrm{S}\alpha = 2a \in \mathbb{Z} \qquad \text{und} \qquad \mathrm{N}\alpha = a^2 - db^2 \in \mathbb{Z}$$

gilt. Gleichwertig hiermit ist

$$f_\alpha(t) = t^2 - S\alpha \cdot t + N\alpha \in \mathbb{Z}[t]\,.$$

Die Menge aller ganzen Elemente von $\mathbb{Q}(\sqrt{d})$ wird mit $\mathfrak{O}$ bezeichnet.

SATZ 6.2. (1) *Ist $d \equiv 2,3 \bmod 4$, so ist*

$$\mathfrak{O} = \mathbb{Z} + \mathbb{Z}\sqrt{d} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}\,.$$

(2) *Ist $d \equiv 1 \bmod 4$, so ist*

$$\mathfrak{O} = \mathbb{Z} + \mathbb{Z}\,\frac{1+\sqrt{d}}{2}.$$

BEMERKUNG. Der Fall $d \equiv 0 \bmod 4$ kommt nicht vor, da d quadratfrei ist.

BEWEIS. (a) Sei $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Z}$. Dann ist

$$\mathrm{S}\alpha = 2a \in \mathbb{Z}\,, \qquad \text{und} \qquad \mathrm{N}\alpha = a^2 - b^2 d \in \mathbb{Z}\,,$$

also ist α ganz.
Sei $\alpha = a + b\,\frac{1+\sqrt{d}}{2} = a + \frac{b}{2} + \frac{b}{2}\sqrt{d}$ und $d \equiv 1 \bmod 4$. Dann ist

$$\mathrm{S}\alpha = 2a + b \in \mathbb{Z}\,, \qquad \mathrm{N}\alpha = \left(a + \frac{b}{2}\right)^2 - \frac{b^2}{4}d = a^2 + ab + \underbrace{(1-d)}_{=4k}\frac{b^2}{4} \in \mathbb{Z}\,,$$

also ist α ganz.
(b) Sei umgekehrt $\mathrm{S}\alpha = 2a \in \mathbb{Z}$ und $\mathrm{N}\alpha = a^2 - b^2 d \in \mathbb{Z}$.
1. Fall: Ist $a \in \mathbb{Z}$, so ist $b^2 d \in \mathbb{Z}$ und damit $b \in \mathbb{Z}$, weil ein Primteiler des Nenners von b sich nicht gegen die in erster Potenz (quadratfrei) auftretenden Primteiler von d wegheben kann.
2. Fall: Sei $a \notin \mathbb{Z}$, also $a = \frac{2k+1}{2}$. Dann ist auch $b = \frac{2l+1}{2}$ wegen $\mathrm{N}\alpha = a^2 - b^2 d \in \mathbb{Z}$, also

$$(2k+1)^2 - (2l+1)^2 d = 4\mathrm{N}\alpha \in 4\mathbb{Z} \quad (\equiv 0 \bmod 4)\,.$$

Wegen

$$\alpha = a + b\sqrt{d} = \frac{2k+1}{2} + \frac{2l+1}{2}\sqrt{d} = k - l + (2l+1)\frac{1+\sqrt{d}}{2}$$

ist $\alpha \in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$ und damit $d \equiv 1 \bmod 4$
Ist $d \equiv 2,3 \bmod 4$, so tritt nur der erste Fall auf. Daher sind $a, b \in \mathbb{Z}$, also $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$. $\square$

DEFINITION 6.3. Setzt man

$$\omega := \begin{cases} \sqrt{d} & \text{falls } d \equiv 2,3 \bmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{falls } d \equiv 1 \bmod 4 \end{cases}$$

so ist $\mathfrak{O} = \mathbb{Z} + \mathbb{Z}\,\omega$. Man bezeichnet $\{1, \omega\}$ als *Ganzheitsbasis*.

KOROLLAR 6.1. *$\mathfrak{O}$ ist ein Teilring von $\mathbb{Q}(\sqrt{d})$.*

BEWEIS. Es ist

$$\begin{aligned} \omega^2 &= d \in \mathfrak{O} && \text{für } d \equiv 2,3 \bmod 4 \\ \omega^2 &= \omega + \underbrace{\frac{d-1}{4}}_{\in\mathbb{Z}} \in \mathfrak{O} && \text{für } d \equiv 1 \bmod 4 \end{aligned}$$

Wegen

$$(a + b\omega)\,(a' + b'\omega) = aa' + (ab' + a'b)\,\omega + bb'\omega^2 \in \mathfrak{O}$$

ist $\mathfrak{O}$ multiplikativ abgeschlossen. $\square$

BEISPIEL. (1) $\mathbb{Q}(\sqrt{-1})$: $\quad \mathfrak{O} = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$

(2) $\mathbb{Q}(\sqrt{-3})$: $\quad \mathfrak{O} = \mathbb{Z} + \mathbb{Z}\,\dfrac{1+\sqrt{-3}}{2}$

2. Einheiten in $\mathfrak{O}$

VORBEMERKUNG. Ist $\alpha \in \mathfrak{O}$ ein Teiler von $\beta \in \mathfrak{O}$, also $\beta = \alpha\gamma$ für ein $\gamma \in \mathfrak{O}$, so gilt

$$\mathrm{N}\alpha\,\mathrm{N}\gamma = \mathrm{N}\alpha\gamma = \mathrm{N}\beta\,,$$

also ist $\mathrm{N}\alpha$ ein Teiler von $\mathrm{N}\beta$ in $\mathbb{Z}$.

SATZ 6.3. *$\alpha \in \mathfrak{O}$ ist genau dann eine Einheit in $\mathfrak{O}$, wenn $N\alpha = \pm 1$ gilt.*

BEWEIS. Ist $\mathrm{N}\alpha = \pm 1$, so ist $\alpha^{-1} = \frac{\bar\alpha}{\alpha\bar\alpha} = \pm\bar\alpha \in \mathfrak{O}$.
Ist andererseits α eine Einheit in $\mathfrak{O}$, so ist α ein Teiler von 1 in $\mathfrak{O}$, nach der Vorbemerkung also N ein Teiler von 1 in $\mathbb{Z}$. Also ist $\mathrm{N}\alpha = \pm 1$. $\square$

BEMERKUNG. Ist $\alpha \in \mathfrak{O}$, also

$$\alpha = a + b\omega = \begin{cases} a + b\sqrt{d} & \text{falls } d \equiv 2,3 \bmod 4 \\ a + b\,\frac{1+\sqrt{d}}{2} & \text{falls } d \equiv 1 \bmod 4 \end{cases}$$

mit $a, b \in \mathbb{Z}$, so gilt für die Norm

$$\mathrm{N}\alpha = \begin{cases} a^2 - db^2 & \text{falls } d \equiv 2,3 \bmod 4 \\ \left(\frac{2a+b}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 & \text{falls } d \equiv 1 \bmod 4 \end{cases}$$

Im imaginär-quadratischen Fall ($d < 0$) gilt also für die Einheiten ε stets $\mathrm{N}\varepsilon = 1$.

SATZ 6.4. *Ist $d < 0$, so ist die Einheitengruppe E von $\mathfrak{O}$ endlich und zwar*

(1) $E = \{1, -1\}$ *für* $d < -3$ *und* $d = -2$

(2) $E = \{(\sqrt{-1})^k \mid k = 1,2,3,4\}$ *für* $d = -1$

(3) $E = \left\{ \left(\frac{1+\sqrt{-3}}{2}\right)^k \mid k = 1, \dots, 6 \right\}$ *für* $d = -3$.

BEWEIS. (1) Sei $d < -3$, also $d \leq -5$ (d quadratfrei). Ist $d \equiv 2,3 \bmod 4$, so folgt aus

$$a^2 + |d|b^2 = 1$$

$a = \pm 1$ und $b = 0$. Dies gilt auch für $d = -2$.
Ist $d \equiv 1 \bmod 4$, so folgt aus

$$\left(\frac{2a^2+b}{2}\right)^2 = |d|\left(\frac{b}{2}\right)^2 = 1$$

ebenfalls $a = \pm 1$ und $b = 0$.
(2) Ist $d = -1$, so folgt aus

$$\mathrm{N}\varepsilon = a^2 + b^2 = 1$$

$a = \pm 1 \wedge b = 0$ oder $a = 0 \wedge b = \pm 1$.
(3) Ist $d = -3 \equiv 1 \bmod 4$, so gilt

$$\mathrm{N}\varepsilon = \left(\frac{2a+b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2 = 1 \quad \Longrightarrow \quad (2a+b)^2 + 3b^2 = 4\,.$$

1. Fall: Ist $b = 0$, so folgt $a = \pm 1$, also $\varepsilon = \pm 1$.
2. Fall: Ist $b \neq 0$, so ist nur $b = \pm 1$ möglich:
(i): Ist $b = 1$, so folgt

$$(2a+1)^2 + 3 = 4 \quad \Longrightarrow \quad (2a+1)^2 = 1\,,$$

also $a = 0$ oder $a = -1$. Damit ergibt sich

$$\varepsilon = \frac{1+\sqrt{-3}}{2} \quad \text{oder} \quad \varepsilon = \frac{-1+\sqrt{-3}}{2}\,.$$

(ii): Ist $b = -1$, so folgt

$$(2a-1)^2 + 3 = 4 \quad \Longrightarrow \quad (2a-1)^2 = 1\,,$$

also $a = 1$ oder $a = 0$. Damit ergibt sich

$$\varepsilon = \frac{1-\sqrt{-3}}{2} \quad \text{oder} \quad \varepsilon = \frac{-1-\sqrt{-3}}{2}\,. \qquad \square$$

Schwieriger zu beantworten ist die Frage nach den Einheiten in $\mathfrak{O}$ für $d > 0$. Hier ist auch $\mathrm{N}\varepsilon = -1$ möglich.

Hilfssatz 6.1. *Zu jeder reellen Zahl α und zu jeder natürlichen Zahl n gibt es eine rationale Zahl $\frac{x}{y} \in \mathbb{Q}$ mit*

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{yn} \quad \textit{mit } 1 \leq y \leq n\,.$$

Beispiel. Approximiere $\pi = 3{,}1415\ldots$ durch eine rationale Zahl mit einem Nenner ≤ 10:

$$\left|\pi - \frac{31}{10}\right| < \frac{1}{2\cdot 10}\,.$$

Eine bessere Approximation ergibt sich für $n = 7$:

$$\left|\pi - \frac{22}{7}\right| < \frac{1}{790} < \frac{1}{7\cdot 10}\,.$$

Beweis. Bilde zu $k = 0,\ldots,n$

$$r_k = \alpha k - [\alpha k] \in [0,1)$$

Zerlege das Intervall $[0,1)$ in n Teilintervalle

$$\left[0,\frac{1}{n}\right),\left[\frac{1}{n},\frac{2}{n}\right),\ldots,\left[\frac{n-1}{n},1\right)\,.$$

Da es $n+1$ Reste r_k gibt, fallen davon 2 nach dem Schubfachprinzip in das gleiche Teilintervall, etwa $r_k, r_{k'} \in \left[\frac{l}{n},\frac{l+1}{n}\right)$, $k < k'$.

Setze $y = k' - k$. Dann gilt $1 \leq y \leq n$ und $x = [\alpha k'] - [\alpha k]$, und es folgt

$$|r_k - r_{k'}| < \frac{1}{n} \quad \Longrightarrow \quad |\alpha y - x| < \frac{1}{n} \quad \Longrightarrow \quad \left|\alpha - \frac{x}{y}\right| < \frac{1}{yn}. \quad \square$$

Hilfssatz 6.2. *Sei $d > 0$. Zu jedem $n \in \mathbb{N}$ gibt es ein $\alpha \neq 0$ aus $\mathfrak{O}$ mit*

$$|\alpha| < \frac{1}{n}, \qquad |N\alpha| \leq 1 + 2\sqrt{d}\,.$$

Beweis. Nach Hilfssatz 6.1 gibt es $x, y \in \mathbb{Z}$ mit

$$\left|(-\sqrt{d})\, y - x\right| < \frac{1}{n}, \qquad 1 \leq y \leq n\,.$$

Setzt man $\alpha = x + y\sqrt{d}$, so ist $\alpha \neq 0$ und

$$|\alpha| < \frac{1}{n}, \qquad 1 \leq y \leq n\,.$$

Dann ist $\bar{\alpha} = x - y\sqrt{d} = \alpha - 2y\sqrt{d}$, also

$$|\mathrm{N}\alpha| = |\alpha\bar{\alpha}| \leq \frac{1}{n}\left(\frac{1}{n} + 2\sqrt{d}\,n\right) \leq 1 + 2\sqrt{d}\,. \quad \square$$

Hilfssatz 6.3. *Es gibt unendlich viele $\alpha \in \mathfrak{O}$ mit*

$$|\mathrm{N}\alpha| \leq 1 + 2\sqrt{d}\,.$$

Beweis. Sei $n_1 = 1$: Nach Hilfssatz 6.2 gibt es $\alpha_1 \neq 0$ aus $\mathfrak{O}$ mit

$$|\alpha_1| < \frac{1}{n_1}, \quad |\mathrm{N}\alpha_1| \leq 1 + 2\sqrt{d}\,.$$

Wähle n_2 so, daß $\frac{1}{n_2} < |\alpha_1|$ ist. Zu n_2 gibt es dann wieder ein $\alpha_2 \neq 0$ aus $\mathfrak{O}$ mit

$$|\alpha_2| < \frac{1}{n_2}, \qquad |\mathrm{N}\alpha_2| \leq 1 + 2\sqrt{d}$$

usw.
Wegen $|\alpha_1| > |\alpha_2| > |\alpha_3| > \cdots$ sind die α_i alle verschieden. $\square$

Hilfssatz 6.4. *Es gibt in $\mathfrak{O}$ eine Einheit $\varepsilon \neq \pm 1$.*

Beweis. Nach Hilfssatz 6.3 gibt es ein $m \in \mathbb{N}$ mit

$$|\mathrm{N}\alpha| = m$$

für unendlich viele $\alpha \in \mathfrak{O}$. Dann gibt es

$$\alpha = x + y\sqrt{d}\,, \qquad \beta = x' + y'\sqrt{d} \in \mathfrak{O}$$

für die $\alpha \neq \pm\beta$ und

$$x \equiv x' \bmod m\,, \qquad y \equiv y' \bmod m$$

ist. Dann ist

$$\alpha\bar{\beta} = xx' - yy'd + (x'y - xy')\sqrt{d}\,,$$

also

$$\mathrm{N}(\alpha\bar{\beta}) = (xx' - yy'd)^2 - (x'y - xy')^2 d\,.$$

Wegen $x'y - xy' \equiv 0 \bmod m$ und $|\mathrm{N}(\alpha\bar{\beta})| = m^2$ ist $xx' - yy'd$ durch m teilbar.
Also ist

$$\varepsilon = \frac{\alpha\bar{\beta}}{m} = \frac{xx' - yy'd}{m} + \frac{x'y - xy'}{m}\sqrt{d} \in \mathfrak{O}$$

und

$$|\mathrm{N}\varepsilon| = \mathrm{N}\left(\frac{\alpha}{\beta}\right) = 1.$$

Wäre $\varepsilon = \pm 1$, so würde $\alpha = \pm\beta$ folgen, im Widerspruch zur Wahl von α und β. □

Folgerungen

(A) Mit $\varepsilon = x + y\sqrt{d}$ sind auch $\pm x \pm y\sqrt{d}$ Einheiten. Für $\varepsilon \neq \pm 1$ sind $x, y \neq 0$, also gibt es vier verschiedene Einheiten.
Wegen $\mathrm{N}\varepsilon = \varepsilon\bar{\varepsilon} = \pm 1$ verteilen sich diese vier Einheiten auf die Intervalle $(-\infty, -1)$, $(-1, 0)$, $(0, 1)$, $(1, \infty)$.
ε heißt *normiert* , wenn $\varepsilon > 1$ ist. Dann ist $\varepsilon = x + y\sqrt{d}$ mit $2x, 2y \in \mathbb{N}$.

(B) Sei ε normiert. Wegen $\varepsilon < \varepsilon^2 < \varepsilon^3 < \cdots$ gibt es unendlich viele Einheiten.

Hilfssatz 6.5. *Es gibt unter den normierten Einheiten von $\mathfrak{O}$ eine kleinste ε_1. Diese heißt* Grundeinheit.

Beweis. Seien

$$E_1 := \{\varepsilon \in \mathfrak{O} \mid \varepsilon > 1,\, \mathrm{N}\varepsilon = 1\}$$
$$E_{-1} := \{\varepsilon \in \mathfrak{O} \mid \varepsilon > 1,\, \mathrm{N}\varepsilon = -1\}$$

Für $\varepsilon = x + y\sqrt{d}$, $\varepsilon' = x' + y'\sqrt{d} \in E_1$ gilt $x^2 = 1 + dy^2$ bzw. $x'^2 = 1 + y'^2 d$, also

$$(*) \qquad x \le x' \iff y \le y'\,.$$

Aus $\varepsilon \le \varepsilon'$ folgt $x \le x'$ oder $y \le y'$. Aus $(*)$ folgt sogar $x \le x'$ und $y \le y'$.
Wegen $2x \in \mathbb{N}$ existiert ein $\varepsilon_0 \in E_1$ mit minimalem x_0, also $\varepsilon_0 = \min E_1$. Analog existiert $\varepsilon_0' = \min E_{-1}$.
Das kleinere der beiden ist die Grundeinheit. □

Satz 6.5. *Ist ε_1 die Grundeinheit, so besitzt jede Einheit ε die Darstellung*

$$\varepsilon = (-1)^k {\varepsilon_1}^n, \qquad k \in \{0, 1\}, \quad n \in \mathbb{Z}\,.$$

Bemerkung. $\mathfrak{O}$ ist das Produkt der zyklischen Gruppen $\mathfrak{Z}_2$ und $\mathfrak{Z}_\infty$.

Beweis. Sei zunächst ε normiert. Dann gilt

$${\varepsilon_1}^n \le \varepsilon < {\varepsilon_1}^{n+1}$$

für ein $n \in \mathbb{N}$. Hiermit ist

$$1 \le \frac{\varepsilon}{{\varepsilon_1}^n} < \varepsilon_1\,.$$

Wegen der Minimalität von ε_1 ist $\varepsilon = {\varepsilon_1}^n$.

Sei jetzt ε beliebig. Dann ist $\varepsilon_0 = (-1)^k \varepsilon^l$ normiert für geeignetes $k \in \{0,1\}$ und $l \in \{-1,1\}$. Also ist $\varepsilon_0 = {\varepsilon_1}^n$ mit $n \in \mathbb{N}$, und es folgt

$$\varepsilon = (-1)^k {\varepsilon_1}^{ln} = (-1)^k {\varepsilon_1}^{\pm n} . \quad \square$$

Bemerkung. Ist $\mathrm{N}\varepsilon_1 = 1$, so gilt $\mathrm{N}\varepsilon = 1$ für alle Einheiten ε.
Es gibt also nur dann Einheiten ε mit $\mathrm{N}\varepsilon = -1$, wenn $N\varepsilon_1 = -1$ ist.
Berechnung der Grundeinheit:
Für $d \equiv 2, 3 \bmod 4$ sind dies Lösungen von $x^2 - dy^2 = \pm 1$ und für $d \equiv 1 \bmod 4$ Lösungen von $x^2 - dy^2 = \pm 4$ mit $x, y \in \mathbb{N}$.
Verfahren für Computer:
Berechne solange Terme $dy^2 \pm 1$, $y \in \mathbb{N}$, bzw. $dy^2 \pm 4$, bis sich ein Quadrat ergibt.
Ein schnelleres Verfahren erhält man, wenn man Kettenbrüche benutzt.

Beispiel. (1) $d = 5$: Gesucht ist die kleinste Lösung von $5y^2 \pm 4$ Quadrat.
Probiere $y = 1$: Dann ist $5 \cdot 1^2 - 4 = 1^2$. Man erhält

$$\varepsilon_1 = \frac{1 + \sqrt{5}}{2} .$$

(2) $d = 31$: Gesucht ist die kleinste Lösung von $31y^2 \pm 1$ Quadrat.
Probiere $y = 273$: Dann ist $31 \cdot 273^2 + 1 = 1520^2$. Man erhält

$$\varepsilon_1 = 1520 + 273\sqrt{31} .$$

Bemerkung. Es ist nicht allgemein bekannt, für welche d es Einheiten ε mit $\mathrm{N}\varepsilon = -1$ gibt.

Da hierzu Lösungen der Gleichung $x^2 - dy^2 = -1$ bzw. $x^2 - dy = -4$ gesucht werden, ist es notwendig, daß die Gleichung $x^2 - dy^2 = -z^2$ Lösungen in $\mathbb{Q}$ besitzt, d.h. es muß $(d, -1)_{\mathbb{Q}} = 1$ und damit $(d, -1)_p = 1$ für alle Primteiler p von d sein.
So ist zum Beispiel

$$(15, -1)_3 = (3, -1)_3 = \left(\frac{-1}{3}\right) = -1 ,$$

also gibt es in $\mathfrak{O}_{15}$ keine Einheiten mit der Norm -1.
Diese Bedingung ist aber leider nicht hinreichend:

$$d = 34 : \quad (34, -1)_{\mathbb{Q}} = 1, \text{ aber: } 3^2 - 34 \cdot 1^2 = -5^2 .$$

3. Eindeutige Primfaktorzerlegungen

Definition 6.4. Ein Ring R mit 1 heißt *Integritätsbereich* , wenn R nullteilerfrei und kommutativ ist.

In Integritätsbereichen gilt die Kürzungsregel

$$ax = bx \wedge x \neq 0 \quad \Longrightarrow \quad a = b .$$

Sind $a, b \in R$, so heißt a ein Teiler von b, wenn es ein $k \in R$ gibt, so daß $ak = b$ ist (in Zeichen $a|b$).

Definition 6.5. Sei R ein Integritätsbereich.

(1) $p \in R$, $p \neq 0$, heißt *prim*, wenn p keine Einheit, ist und wenn gilt

$$p|ab \quad \Longrightarrow \quad p|a \vee p|b.$$

(2) $q \in R$, $q \neq 0$, heißt *unzerlegbar*, wenn q keine Einheit ist, und wenn gilt

$$q = ab \quad \Longrightarrow \quad a \text{ oder } b \text{ ist eine Einheit}.$$

HILFSSATZ 6.6. *Ist p prim, so ist p unzerlegbar.*

BEWEIS. Sei $p = ab$. Da p prim ist, folgt $p|a$ oder $p|b$. Ohne Beschränkung der Allgemeinheit gelte $p|a$. Also gibt es ein $k \in R$ mit $a = pk$. Es folgt

$$p = ab = (pk)b = p(kb).$$

Mit der Kürzungsregel folgt $1 = kb$, d.h. b ist eine Einheit. □

SATZ 6.6. *Eine Zerlegung $a = p_1 \cdots p_r$ mit p_i prim ist stets eindeutig (bis auf die Reihenfolge und Assoziiertheit).*

BEMERKUNG. Über die Existenz der Produktdarstellung eines Elements wird noch nichts ausgesagt.

BEWEIS. Induktion nach r:
Sei $a = p_1 \cdots p_r = q_1 \cdots q_s$ mit p_i, q_j prim.
Für $r = 1$ ist $p_1 = q_1 \cdots q_s$, also z.B. $p_1 = q_1$, weil p_1 unzerlegbar ist.
Sei $r > 1$: Aus $p_1 | a = q_1 \cdots q_s$ folgt $p_1 | q_j$ für ein j, etwa $p_1 | q_1$, also $p_1 \cdot \ell = q_1$. Weil q_1 unzerlegbar ist, ist ℓ eine Einheit, also sind p_1 und q_1 assoziiert.
Mit der Kürzungsregel folgt $p_2 \cdots p_r = (\ell q_2) \cdots q_s$. Nach Induktion folgt die Behauptung. □

HILFSSATZ 6.7. *Sei d quadratfrei und $\mathfrak{O} = \mathbb{Z} + \mathbb{Z}\,\omega$ die Menge der ganzen Elemente in $\mathbb{Q}(\sqrt{d})$. Besitzt $a \in \mathfrak{O}$ ein Zerlegung $a = b_1 \cdots b_n$ in $\mathfrak{O}$ mit $|\mathrm{N}b_i| \neq$, so gilt $n \leq \log_2 |\mathrm{N}a|$.*

BEWEIS. Es ist

$$|\mathrm{N}a| = |\mathrm{N}b_1| \ldots |\mathrm{N}b_n| \geq 2^n.$$

Logarithmieren liefert die Behauptung. □

SATZ 6.7. *Jedes Element $a \in \mathfrak{O}$, $a \neq 0$, das keine Einheit ist, besitzt eine Zerlegung $a = b_1 \cdots b_n$ mit b_i unzerlegbar.*

BEWEIS. Wegen Hilfssatz 6.7 gibt es eine Zerlegung $a = b_1 \cdots b_n$ mit $|\mathrm{N}b_i| \neq 1$ und maximalem n. Dann sind die b_i unzerlegbar:
Ist etwa $b_1 = c_1c_2$, so hat $a = c_1c_2b_2 \cdot b_n$ genau $n{+}1$ Faktoren. Wegen der Maximalität von n ist daher c_1 oder c_2 eine Einheit. Also ist b_1 unzerlegbar. □

KOROLLAR 6.2. *Ist in $\mathfrak{O}$ jedes unzerlegbare Element prim, so ist $\mathfrak{O}$ ein Ring mit eindeutiger Primfaktorzerlegung.*

KOROLLAR 6.3. *Ist $\mathfrak{O}$ euklidisch, so ist $\mathfrak{O}$ ein Ring mit eindeutiger Primfaktorzerlegung.*

SATZ 6.8. *Für $d \in \{-11, -7, -3, -2, 2, 3, 5\}$ ist $\mathfrak{O}$ euklidisch bezüglich der Gradfunktion $g(a) = |\mathrm{N}a|$.*
(D.h. zu $a, b \in \mathfrak{O}$, $b \neq 0$, gibt es $q, r \in \mathfrak{O}$ mit $a = qb + r$ und $|\mathrm{N}r| < |\mathrm{N}b|$.)

Beweis. Für $a, b \in \mathfrak{O}_d$ bilden wir den Quotienten $\frac{a}{b} = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.
1. Fall: Sei $d \equiv 2, 3 \bmod 4$, also $d \in \{-2, -1, 2, 3\}$.
Wählt man $u, v \in \mathbb{Z}$ mit

$$|x - u| \leq \frac{1}{2} \qquad \text{und} \qquad |y - v| \leq \frac{1}{2},$$

so ergibt sich $a = qb + r$ mit $q = u + v\sqrt{d} \in \mathfrak{O}_d$ und

$$r = \left(\frac{a}{b} - q\right) b = \left((x-u) + (y-v)\sqrt{d}\right) b \in \mathfrak{O}_d .$$

Wegen

$$|\mathrm{N}\left((x-u) + (y-v)\sqrt{d}\right)| \leq \frac{1}{4}|1-d| < 1$$

für $d \in \{-2, -1, 2, 3\}$ ist $|\mathrm{N}r| < |\mathrm{N}b|$.
2. Fall: Sei $d \equiv 1 \bmod 4$, also $d \in \{-11, -7, -3, 5\}$.
Wählt man $u, v \in \mathbb{Z}$ mit

$$\left|y - \frac{v}{2}\right| \leq \frac{1}{4} \qquad \text{und} \qquad \left|x - \frac{v}{2} - u\right| \leq \frac{1}{2},$$

so ergibt sich $a = qb + r$ mit $q = u + v\,\frac{1+\sqrt{d}}{2} \in \mathfrak{O}_d$ und

$$r = \left(\frac{a}{b} - q\right) b = \left(x - u - \frac{v}{2} + \left(y - \frac{v}{2}\right)\right) b \in \mathfrak{O}_d .$$

Wegen

$$\left|\mathrm{N}\left(x - u - \frac{v}{2} + \left(y - \frac{v}{2}\right)\sqrt{d}\right)\right| \leq \frac{1}{4} + \frac{|d|}{16} \leq \frac{15}{16} < 1$$

für $d \in \{-11, -7, -3, 5\}$ ist $|\mathrm{N}r| < |\mathrm{N}b|$. □

Bemerkung. (1) Ist $d < 0$, so gibt es in $\mathfrak{O}$ eindeutige Primfaktorzerlegungen genau für

$$d \in \{-1, -2, -3, -7, -11\} \cup \{-19, -43, -67, -163\} .$$

Diese Vermutung wurde bereits von Gauss aufgestellt, aber erst 1966 von Stark und Baker bewiesen.
Für $d \in \{-19, -43, -67, -163\}$ ist $\mathfrak{O}_d$ Hauptidealring.
(2) Ist $2 \leq d < 100$, so gibt es 60 verschiedene quadratfreie d. Davon haben 38 der entsprechenden $\mathfrak{O}_d$ eindeutige Primfaktorzerlegungen.
Eine offene Frage ist noch: Gibt es endlich oder unendlich viele d mit eindeutiger Primfaktorzerlegung?
Es gibt 21 euklidische $\mathfrak{O}_d$ bezüglich der Norm für $d > 1$. Alle diese d sind kleiner als 100. Bewiesen 1950 von Chatland und Davenport.

Lemma 6.1. *Ist $a \in \mathfrak{O}$ und $|Na| \in \mathbb{P}$, so ist a unzerlegbar.*

Beweis. Ist $a = bc$, so folgt $|\mathrm{N}b| \cdot |\mathrm{N}| = |\mathrm{N}a| \in \mathbb{P}$. Also ist $|\mathrm{N}b| = 1$ oder $|\mathrm{N}c = 1$, d.h. b oder c ist eine Einheit in $\mathfrak{O}$. □

Beispiel. (1) Sei $d = -5$. In $\mathfrak{O} = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ ist die Zerlegung
$$9 = 3 \cdot 3 = (2 + \sqrt{-5})\,(2 - \sqrt{-5})$$
nicht eindeutig, da 3, $2 + \sqrt{-5}$ und $2 - \sqrt{-5}$ unzerlegbar und nicht assoziiert sind.
(2) Sei $d = 6$. In $\mathfrak{O} = \mathbb{Z} + \mathbb{Z}\sqrt{6}$ gilt
$$5 = (1 + \sqrt{6})\,(-1 + \sqrt{6}) = (71 + 29\sqrt{6})\,(-71 + 29\sqrt{6})\,.$$
Nach Lemma 6.1 sind beide Darstellungen unzerlegbar.
Die beiden Darstellungen sind jedoch assoziiert: Wegen
$$(1 + \sqrt{6})\,(49 - 20\sqrt{6}) = -71 + 29\sqrt{6}$$
und
$$\mathrm{N}(49 - 20\sqrt{6}) = 49^2 - 6 \cdot 20^2 = 1$$
ist $49 - 20\sqrt{6}$ eine Einheit. Also sind $1 + \sqrt{6}$ und $-71 + 29\sqrt{6}$ assoziiert.

4. Bewertungen quadratischer Erweiterungen

Es sei E ein Erweiterungskörper von K. Eine Bewertung $|\ |_E$ auf E heißt eine Fortsetzung einer Bewertung $|\ |_K$ auf K, wenn für alle $a \in K$
$$|a|_K = |a|_E$$
gilt.

Satz 6.9. *Es sei K vollständig bezüglich $|\ |_K$, $d \in K$ kein Quadrat in K und $E = K(\sqrt{d})$. Dann ist*
$$|\alpha|_E = \sqrt{|\mathrm{N}\alpha|_K} \in \mathbb{R}_+$$
eine Fortsetzung von $|\ |_K$ auf E.

Beweis. Für $a \in K$ ist $\mathrm{N}a = a^2$, also
$$|a|_E = \sqrt{|a^2|_K} = |a|_K.$$
Es sind noch die Bewertungsaxiome für $|\ |_E$ zu zeigen.
(1) Für $\alpha \in E$ gilt
$$|\alpha|_E = 0 \iff |\mathrm{N}\alpha|_K = 0 \iff \mathrm{N}\alpha = 0 \iff \alpha = 0.$$
(2) Dreiecksungleichung: Wegen
$$|c + d| = |c|\left|1 + \frac{d}{c}\right|, \qquad c \neq 0$$
genügt es,
$$|1 + \alpha|_E \leq 1 + |\alpha|_E\,, \qquad \alpha \in E \setminus K$$
zu zeigen. Es sei
$$f(t) = t^2 + bt + c = (t - \alpha)(t - \bar{\alpha})$$
das Hauptpolynom von α. Das Hauptpolynom von $1 + \alpha$ ist dann
$$g(t) = f(t - 1) = (t - 1)^2 + b(t - 1) + c = t^2 + (b - 2)t + 1 - b + c\,,$$
also ist
$$\mathrm{N}(1 + \alpha) = 1 - b + c.$$

Wegen $\alpha \notin K$ besitzt $f(t)$ keine Nullstelle in K. Nach Satz 2.4 ist dann

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

also

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

(3) Für $\alpha, \beta \in E$ gilt

$$|\alpha\beta|_E = \sqrt{|\mathrm{N}(\alpha\beta)|_K} = \sqrt{|\mathrm{N}\alpha|_K |\mathrm{N}\beta|_K} = |\alpha|_E\,|\beta|_E\,. \quad \square$$

Bemerkung. Für die in Satz 6.9 definierte Bewertung gilt

$$|\alpha|_E = \sqrt{|\mathrm{N}\alpha|_K} = |\bar{\alpha}|_E.$$

Satz 6.10. *Es sei K nicht-archimedisch bewertet und E ein quadratischer Erweiterungskörper von K. Gilt für eine Fortsetzung $|\ |_1 : E \to \mathbb{R}_+$*

$$|\alpha|_1 = |\bar{\alpha}|_1$$

für alle $\alpha \in E$, so ist diese Fortsetzung eindeutig.

Beweis. Es sei $|\ |_2$ eine zweite Bewertung auf E, die $|\ |_K$ fortsetzt, und $\alpha \in E$ mit $|\alpha|_2 \neq |\alpha|_1$, etwa

$$|\alpha|_2 < |\alpha|_1$$

(andernfalls betrachte α^{-1}). Ist wieder

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

das Hauptpolynom von α, so gilt

$$|b|_K = |\alpha + \bar{\alpha}|_1 \leq \max(|\alpha|_1 |\bar{\alpha}|_1) = |\alpha|_1\,.$$

Für $|\ |_2$ folgt dann

$$|\alpha^2|_2 = |\alpha|_2^2 < |\alpha|_1^2 = |\alpha\bar{\alpha}|_1 = |c|_K = |c|_2.$$

Analog ergibt sich

$$|b\alpha|_2 < |c|_2\,.$$

Nach dem Dominanzprinzip ist

$$|f(\alpha)|_2 = |\alpha^2 + b\alpha + c|_2 = |c|_2 \neq 0\,.$$

Dies ist aber ein Widerspruch, denn α ist Nullstelle von $f(t)$. $\square$

Ist K nicht vollständig, so läßt sich die Formel aus Satz 6.9 nicht unmittelbar für die Bewertungsfortsetzung übernehmen. Um Satz 6.9 anwenden zu können, setzt man die Bewertung von K auf die Komplettierung $\hat{K}$ fort. Man hat dann die zwei Fälle zu unterscheiden, ob d ein Quadrat in $\hat{K}$ ist oder nicht. Im ersten Fall läßt sich $K(\sqrt{d})$ in $\hat{K}$, im zweiten in $\hat{K}(\sqrt{d})$ einbetten.

SATZ 6.11. *Es sei* $|\ |_K$ *eine nicht-archimedische Bewertung auf* K *und* $E = K(\sqrt{d})$, d *kein Quadrat in* K. *Dann gilt*

(a) *Ist* d *kein Quadrat in* $\hat{K}$, *so ist*

$$|\ |_E : E \to \mathbb{R}_+, \qquad |\alpha| = \sqrt{|N\alpha|_K}$$

die eindeutige Fortsetzung von $|\ |_K$ *auf* E.

(b) *Ist* d *ein Quadrat in* $\hat{K}$, $d = \vartheta^2$, *so sind*

$$|\ |_1 : E \to \mathbb{R}_+, \qquad |\alpha|_1 = |\alpha|_{\hat{K}} = |a + b\vartheta|_{\hat{K}}$$

$$|\ |_2 : E \to \mathbb{R}_+, \qquad |\alpha|_2 = |\bar{\alpha}|_{\hat{K}} = |a - b\vartheta|_{\hat{K}}$$

zwei Fortsetzungen von $|\ |_K$ *auf* E.

BEWEIS. $|\ |_K$ läßt sich nach Satz 2.1 auf die Komplettierung $\hat{K}$ fortsetzen.
(a)] Es sei $\hat{E} = \hat{K}(\sqrt{d})$. Nach Satz 6.9 besitzt $|\ |_{\hat{K}}$ eine Fortsetzung $|\ |_{\hat{E}}$ mit $|\alpha|_{\hat{E}} = \sqrt{|\mathrm{N}\alpha|_{\hat{K}}}$. Die Restriktion auf E liefert eine Bewertung auf E

$$|\alpha|_E = \sqrt{|a^2 - db^2|_K}.$$

Die Eindeutigkeit folgt aus Satz 6.10.
(b)] Ist $d = \vartheta^2, \vartheta \in \hat{K}$, so erhält man entsprechend der Einbettungen von E in $\hat{K}$

$$a + b\sqrt{d} \mapsto a + b\vartheta \qquad \text{oder} \qquad a + b\sqrt{d} \mapsto a - b\vartheta$$

die angegebenen Bewertungen. Bei Charakteristik $\neq 2$ sind die Bewertungen verschieden: Weil K dicht in $\hat{K}$ liegt, gibt es ein $a \in K$ mit

$$|a - \vartheta|_1 < |2\vartheta|_1 \,.$$

Dann ist nach dem Dominanzprinzip

$$|a + \vartheta|_1 = |a - \vartheta\ + 2\vartheta|_1 = |2\vartheta|_1 \neq |a - \vartheta|_1 = |a + \vartheta|_2 \,. \quad \square$$

BEMERKUNG. Man kann zeigen, daß im Fall (b) nur diese beiden Fortsetzungen existieren. Für $K = \mathbb{Q}$ sind nach dem Satz von OSTROWSKI sämtliche Bewertungen bekannt. Die nicht-archimedischen Bewertungen entsprechen bis auf Äquivalenz der Menge $\mathbb{P}$ der Primzahlen. Durch Satz 6.11 erhält man eine vollständige Übersicht über alle nicht-archimedischen Bewertungen einer quadratischen Erweiterung $E = \mathbb{Q}(\sqrt{d})$.

BEISPIEL. Es sei $E = \mathbb{Q}(\sqrt{-1})$.
Hier gilt

$$-1 \text{ kein Quadrat in } \mathbb{Q}_p \iff p = 2 \vee p \equiv 3 \bmod 4$$
$$-1 \text{ Quadrat in } \mathbb{Q}_2 \iff p \equiv 1 \bmod 4$$

Im ersten Fall ist die Bewertung auf E

$$|a + bi|_E = \sqrt{|a^2 + b^2|_p} \,.$$

Ist $p \equiv 1 \bmod 4$, so ergeben sich zwei Fortsetzungen

$$|a+bi|_1 = |a+b\vartheta|_p\,,$$
$$|a+bi|_2 = |a-b\vartheta|_p\,.$$

Um die Werte auf der rechten Seite zu berechnen, hat man zunächst in $\mathbb{Q}_p$ ein $\vartheta \in \mathbb{Q}_p$ aus der Gleichung

$$\vartheta^2 = -1$$

zu bestimmen. So ist etwa für $p = 5 \equiv 1 \bmod 4$

$$\vartheta = 2 + 5 + 2 \cdot 5^2 + \dots .$$

Für $\alpha = 7 + i$ ist

$$|7+i|_1 = |7 + (2+5+2\cdot 5^2 + \dots)|_5 = 1\,,$$

$$|7+i|_2 = |7 - (2+5+2\cdot 5^2 + \dots)|_5 = \frac{1}{25}\,.$$

Es sei $\mathfrak{P} = \{|\ |_\mathfrak{p}\}$ die Menge der Bewertungen von $E = \mathbb{Q}(\sqrt{d})$. Wir indizieren mit $\mathfrak{p}_p$, falls sie eine p-adische Bewertung fortsetzt.

Satz 6.12. *Es sei $\mathfrak{O} = \{\alpha \in E \mid \mathrm{N}\alpha, \mathrm{S}\alpha \in \mathbb{Z}\}$ der Ring der ganzen Elemente in E und*

$$B_\mathfrak{p} = \{\alpha \in E \mid |\alpha|_\mathfrak{p} \le 1\}$$

die Bewertungsringe der Bewertungen aus $\mathfrak{P}$. Dann ist

$$\mathfrak{O} = \bigcap B_\mathfrak{p},$$

wobei der Durchschnitt über alle Bewertungen aus $\mathfrak{P}$ zu bilden ist.

Beweis. Es sei α aus dem Durchschnitt, also $|\alpha|_\mathfrak{p} \le 1$ für alle Bewertungen $|\ |_\mathfrak{p}$ aus $\mathfrak{P}$. Dann ist auch $\bar{\alpha}$ in dem Durchschnitt. Da dieser ein Teilring von E ist, sind Norm und Spur von α darin enthalten. Weil die Bewertungen aus $\mathfrak{P}$ Fortsetzungen der p-adischen Bewertungen auf $\mathbb{Q}$ sind und $\mathrm{N}\alpha,\ \mathrm{S}\alpha \in \mathbb{Q}$ ist, gilt

$$|\mathrm{N}\alpha|_p \le 1 \ \wedge\ |\mathrm{S}\alpha|_p \le 1$$

für alle $p \in \mathbb{P}$. Das aber bedeutet, daß $\mathrm{N}\alpha$ und $\mathrm{S}\alpha$ keine p-Potenzen im Nenner enthalten und damit ganzzahlig sind. Folglich liegt α in $\mathfrak{O}$.

Sei nun umgekehrt α in $\mathfrak{O}$, also $\mathrm{N}\alpha,\ \mathrm{S}\alpha \in \mathbb{Z}$. Ist d kein Quadrat in $\mathbb{Q}_p$, so ergibt sich sofort

$$|\alpha|_{\mathfrak{p}_p} = \sqrt{|\mathrm{N}\alpha|_p} \le 1\,,$$

weil $\mathrm{N}\alpha$ in $\mathbb{Z}$ liegt. Wir haben daher nur noch solche p zu betrachten, für die d ein Quadrat in $\mathbb{Q}_p$ ist. Wegen $\vartheta^2 = d \in \mathbb{Z}$ ist $\vartheta \in \mathbb{Q}_p$ ganz, also $|a+b\vartheta|_p \le 1$. Es bleibt noch der Fall $d \equiv 1 \bmod 4$, in dem $\omega = \frac{1+\sqrt{d}}{2}$ ist. Diesem Element entspricht $\frac{1+\vartheta}{2}$, das in $\mathbb{Q}_p$ offensichtlich für $p \ne 2$ ganz, für $p = 2$ wegen $\vartheta = 1 + a_1 2 + a_2 2^2 + \cdots$ ebenfalls ganz ist. Alle Elemente $a + b\omega$ aus $\mathfrak{O}$ sind ganz für alle Bewertungen aus $\mathfrak{P}$. $\square$

KOROLLAR 6.4. *Für jedes* $\alpha \in \mathfrak{O}$ *gilt*

$$|\alpha|_{\mathfrak{p}} = 1$$

für fast alle Bewertungen aus $\mathfrak{P}$.

BEWEIS. Es gibt nur endlich viele Primteiler von $\mathrm{N}\alpha$. Ist p kein Teiler von $\mathrm{N}\alpha$, so ist $|\mathrm{N}\alpha|_p = 1$. Mit α liegt auch $\bar{\alpha}$ in $\mathfrak{O}$. Aus

$$1 = |\mathrm{N}\alpha|_p = |\alpha|_{\mathfrak{p}}\, |\bar{\alpha}|_{\mathfrak{p}}$$

für eine Fortsetzung der p-adischen Bewertung folgt dann $|\alpha|_{\mathfrak{p}} = 1$. $\square$

KOROLLAR 6.5. *Für* $\alpha,\ \beta \in \mathfrak{O}$ *gilt*

$$\alpha|\beta \iff |\beta|_{\mathfrak{p}} \le |\alpha|_{\mathfrak{p}}$$

für alle Bewertungen aus $\mathfrak{P}$.

BEWEIS. Es gilt

$$\begin{aligned} \alpha|\beta &\iff \alpha^{-1}\beta \in \mathfrak{O} = \bigcap B_{\mathfrak{p}} \\ &\iff |\alpha^{-1}\beta|_{\mathfrak{p}} \le 1 \text{ für alle } \mathfrak{p} \\ &\iff |\beta|_{\mathfrak{p}} \le |\alpha|_{\mathfrak{p}} \text{ für alle } \mathfrak{p}\,. \quad \square \end{aligned}$$

Die Wertegruppen von $|\ |_{\mathfrak{p}}$ sind diskret:

$$\text{(a)} \qquad |\alpha|_{\mathfrak{p}_p} = \sqrt{|\mathrm{N}\alpha|_p} \in \left\{ \left(\sqrt{|p|_p}\right)^k \,\middle|\, k \in \mathbb{Z} \right\}$$

$$\text{(b)} \qquad |\alpha|_{\mathfrak{p}} = |a + b\vartheta|_p \in \{|p|_p^k \mid k \in \mathbb{Z}\}\,.$$

Gibt es ein $\pi \in K$ mit $|\pi|_{\mathfrak{p}}^2 = |p|_p$, so heißt $\mathfrak{p}$ verzweigt. In diesem Fall vergrößert sich die Wertegruppe (verweigt: 2, $p|d$).

Ist $|\pi|_{\mathfrak{p}} < 1$ erzeugendes Element der Wertegruppe, so definiere

$$\mathrm{ord}_{\mathfrak{P}}\alpha = \begin{cases} k & \text{falls } \alpha \ne 0,\ |\alpha|_{\mathfrak{p}} = |\pi|_{\mathfrak{p}}^k \\ \infty & \text{falls } \alpha = 0 \end{cases}$$

Damit lassen sich Korollar 6.4 und Korollar 6.5 folgendermaßen umformulieren:

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}\alpha = 0 &\text{ für fast alle } \mathfrak{p} \in \mathfrak{P}\,, \\ \alpha|\beta \iff \mathrm{ord}_{\mathfrak{p}}\alpha &\le \mathrm{ord}_{\mathfrak{p}}\beta \text{ für alle } \mathfrak{p} \in \mathfrak{P}\,. \end{aligned}$$

DEFINITION 6.6. (1) Die *Divisorgruppe* $\mathfrak{D}$ ist die freie von $\mathfrak{P}$ erzeugte abelsche Gruppe

$$\mathfrak{D} = \{\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r} \mid \mathfrak{p}_i \in \mathfrak{P},\ k_i \in \mathbb{Z}\}\,.$$

(2) Für $\alpha \in E^\times$ sei

$$(\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}\alpha}$$

der α zugeordnete Divisor.

Die Abbildung

$$E^\times \to \mathfrak{D}\,, \qquad \alpha \mapsto (\alpha)$$

ist ein Homomorphismus, d.h. es ist $(\alpha\beta) = (\alpha)\,(\beta)$. Den Kern bilden die Einheiten, das Bild $\mathfrak{D}_0$ ist im allgemeinen eine Untergruppe von $\mathfrak{D}$ (Hauptdivisoren). Ihren Index in $\mathfrak{D}$ bezeichnet man als *Klassenzahl*.

Beispiel. Es sei $E = \mathbb{Q}(\sqrt{-5})$. Dann gilt

$$-5 \text{ Quadrat in } \mathbb{Q}_p \iff \left(\frac{-5}{p}\right) = 1\,.$$

Damit ergibt sich

$\mathbb{P}$	verzweigt 2	3		verzweigt 5	7
$\mathfrak{P}$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\bar{\mathfrak{p}}_3$	$\mathfrak{p}_5$	$\mathfrak{p}_7$

Man findet

$$\begin{aligned}
(2) &= \mathfrak{p}_2^2\\
(3) &= \mathfrak{p}_3 \cdot \bar{\mathfrak{p}}_3\\
(1+\sqrt{-5}) &= \mathfrak{p}_2 \cdot \mathfrak{p}_3\\
(1-\sqrt{-5}) &= \mathfrak{p}_2 \cdot \bar{\mathfrak{p}}_3\\
6 = 2\cdot 3 &= (1+\sqrt{-5})\,(1-\sqrt{-5})\\
(6) &= \mathfrak{p}_2^2 \cdot \mathfrak{p}_3\bar{\mathfrak{p}}_3 = (\mathfrak{p}_2\mathfrak{p}_3)\,(\mathfrak{p}_2\bar{\mathfrak{p}}_3)
\end{aligned}$$

ANHANG A

Tabelle reell quadratischer Zahlkörper

d	h	ε	$\mathrm{N}(\varepsilon)$	d	h	ε	$\mathrm{N}(\varepsilon)$
2	1	$1+\omega$	-1	53	1	$3+\omega$	-1
3	1	$2+\omega$	$+1$	55	2	$89+12\omega$	$+1$
5	1	ω	-1	57	1	$131+40\omega$	$+1$
6	1	$5+2\omega$	$+1$	58	2	$99+13\omega$	-1
7	1	$8+3\omega$	$+1$	59	1	$530+69\omega$	$+1$
10	2	$3+\omega$	-1	61	1	$17+5\omega$	-1
11	1	$10+3\omega$	$+1$	62	1	$63+8\omega$	$+1$
13	1	$1+\omega$	-1	65	2	$7+2\omega$	-1
14	1	$15+4\omega$	$+1$	66	2	$65+8\omega$	$+1$
15	2	$4+\omega$	$+1$	67	1	$48842+5967\omega$	$+1$
17	1	$3+2\omega$	-1	69	1	$11+3\omega$	$+1$
19	1	$170+39\omega$	$+1$	70	2	$251+30\omega$	$+1$
21	1	$2+\omega$	$+1$	71	1	$3480+413\omega$	$+1$
22	1	$197+42\omega$	$+1$	73	1	$943+250\omega$	-1
23	1	$24+5\omega$	$+1$	74	2	$43+5\omega$	-1
26	2	$5+\omega$	-1	77	1	$4+\omega$	$+1$
29	1	$2+\omega$	-1	78	2	$53+6\omega$	$+1$
30	2	$11+2\omega$	$+1$	79	3	$80+9\omega$	$+1$
31	1	$1520+273\omega$	$+1$	82	4	$9+\omega$	-1
33	1	$19+8\omega$	$+1$	83	1	$82+9\omega$	$+1$
34	2	$35+6\omega$	$+1$	85	2	$4+\omega$	-1
35	2	$6+\omega$	$+1$	86	1	$20405+1122\omega$	$+1$
37	1	$5+2\omega$	-1	87	2	$28+3\omega$	$+1$
38	1	$37+6\omega$	$+1$	89	1	$447+106\omega$	-1
39	2	$25+4\omega$	$+1$	91	2	$1574+165\omega$	$+1$
41	1	$27+10\omega$	-1	93	1	$13+3\omega$	$+1$
42	2	$13+2\omega$	$+1$	94	1	$2143295+221064\omega$	$+1$
43	1	$3482+531\omega$	$+1$	95	2	$39+4\omega$	$+1$
45	1	$24335+3588\omega$	$+1$	97	1	$5035+1138\omega$	-1
47	1	$48+7\omega$	$+1$	101	1	$9+2\omega$	-1
51	2	$50+7\omega$	$+1$				

h = Klassenzahl, ε = Grundeinheit

ANHANG B

Aufgaben und Lösungen

AUFGABE 1. Zeige, daß für $x \in \mathbb{Q}^\times$ gilt:
(a) $|x|_p = 1$ für fast alle Primzahlen $p \in \mathbb{P}$.
(b)

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |x|_p = 1$$

Lösung. Für $x = 1$ oder $x = -1$ sind die Behauptungen offensichtlich richtig. Sei also $x \neq \pm 1$. Dann besitzt x eine Darstellung

$$x = \pm p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$$

mit eindeutig bestimmten Primzahlen p_i und eindeutig bestimmten Exponenten $\alpha_i \in \mathbb{Z} \backslash \{0\}$.

(a) Es ist

$$|x|_p = \begin{cases} \dfrac{1}{p^0} = 1 & \text{falls } p \neq p_i \text{ für alle } i \\ \dfrac{1}{p_i^{\alpha_i}} \neq 1 & \text{falls } p = p_i \end{cases}$$

Also ist $|x|_p \neq 1$ nur für endlich viele Primzahlen p.
(b) Es ist

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |x|_p = \frac{1}{p_1^{\alpha_1}} \cdot \ldots \cdot \frac{1}{p_r^{\alpha_r}} \cdot |x|_\infty = \frac{1}{p_1^{\alpha_1}} \cdot \ldots \cdot \frac{1}{p_r^{\alpha_r}} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} = 1\,.$$

AUFGABE 2. K sei nicht-archimedisch bewertet. Zeige:
Ist $a_1 + \cdots + a_n = 0$, so werden zwei der Summanden gleich bewertet.

Lösung. Ohne Beschränkung der Allgemeinheit sei $\max_{1 \leq i \leq n} |a_i| = |a_1|$. Es folgt

$$|a_1| = |-(a_2 + \cdots + a_n)| = |a_2 + \cdots + a_n| \leq \max_{2 \leq i \leq n} |a_i|^\dagger \leq |a_1|\,.$$

Also gibt es ein a_i, $i \neq 1$, mit $|a_i| = |a_1|$.

---

†Die Bewertung ist nicht-archimedisch

Aufgabe 3. In einem bewerteten Körper K heißt

$$K_r(a) := \{x \in K \mid |x-a| = r\}$$

Kreis mit dem Radius r und dem Zentrum a, und

$$U_r(a) := \{x \in K \mid |x-a| < r\}$$

heißt Kreisscheibe. Zeige für einen nicht-archimedisch bewerteten Körper:

(a) Jeder Punkt $b \in U_r(a)$ ist Zentrum von $K_r(a)$.
(b) Für $y \notin U_r(a)$ ist der Abstand $|y-x|$ von allen Punkten $x \in U_r(a)$ gleich.
(c) Zwei Kreisscheiben sind entweder disjunkt, oder eine ist in der anderen enthalten.

Lösung. (a) Sei $b \in U_r(a)$, beliebig. Zu zeigen ist $K_r(a) = K_r(b)$, also

$$|x-a| = r \iff |x-b| = r\,.$$

Ist $|x-b| = r$, so folgt wegen $|b-a| < r = |x-b|$

$$|x-a| = |(x-b)+(b-a)| = |x-b| = r$$

nach dem Dominanzprinzip.
Analog folgt $|x-a| = r \;\Rightarrow\; |x-b| = r$.

(b) Sei $y \notin U_r(a)$, also $|y-a| \geq r > |x-a|$ für alle $x \in U_r(a)$. Es folgt

$$|y-x| = |(y-a)+(a-x)| = |y-a|$$

nach dem Dominanzprinzip.

(c) Seien

$$U_r(a) = \{x \in K \mid |x-a| < r\} \quad \text{und} \quad U_s(b) = \{x \in K \mid |x-b| < s\}$$

zwei Kreisscheiben mit $r \leq s$.
Ist $U_r(a) \cap U_s(b) \neq \emptyset$, so gibt es ein $x \in K$ mit

$$|x-a| < r \quad \text{und} \quad |x-b| < s\,.$$

Ist nun $y \in U_r(a)$, beliebig, so folgt

$$|y-b| = |(y-a)+(a-x)+(x-b)| \leq \max\{|y-a|,\, |a-x|,\, |x-b|\} < s\,.$$

Also ist $U_r(a) \subseteq U_s(b)$.

Aufgabe 4. (a) Zeige, daß der gewöhnliche Absolutbetrag auf $\mathbb{C}$ der Gleichung

$$(*) \qquad |x+y|^2 + |x-y|^2 = 2 \cdot |x|^2 + 2 \cdot |y|^2$$

genügt.

(b) Zeige, daß es bei nicht-archimedisch bewerteten Körpern K stets $x, y \in K$ gibt, so daß die Gleichung $(*)$ verletzt ist.

Lösung. (a) In $\mathbb{C}$ gilt $|z|^2 = z\overline{z}$. Damit folgt

$$|x+y|^2 + |x-y|^2 = (x+y)(\overline{x+y}) + (x-y)(\overline{x-y}) = 2x\overline{x} + 2y\overline{y} = 2|x|^2 + 2|y|^2 .$$

(b) Sei nun K nicht-archimedisch bewertet. Für $x, y \in K$ mit $x, y \neq 0$ gilt

$$\begin{aligned}|x+y|^2 + |x-y|^2 &\leq \big(\max\{|x|,|y|\}\big)^2 + \big(\max\{|x|,|-y|\}\big)^2 \\ &= 2\big(\max\{|x|,|y|\}\big)^2 < 2|x|^2 + 2|y|^2 .\end{aligned}$$

Aufgabe 5. Ist (a_n) eine Cauchy-Folge in einem bewerteten Körper, die keine Nullfolge ist, so gibt es ein $\varepsilon > 0$ und ein $n_0 \in \mathbb{N}$ mit

$$|a_n| \geq \varepsilon \quad \text{für } n \geq n_0$$

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

$$|a_n| \leq |a_n - a_{n_1}| + |a_{n_1}| < 2\varepsilon .$$

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

Aufgabe 6. Zeige, daß die Folgen
(a) $a_n = 1 + 2 + \cdots + 2^n$
(b) $b_n = 1 \cdot 2 + 2 \cdot 2^2 + \cdots + n \cdot 2^n$
in $\mathbb{Q}$ bezüglich der 2-adischen Bewertung konvergieren. Berechne die Grenzwerte.

Lösung. (a) Es ist

$$a_n = 1 + 2 + \cdots + 2^n = 2^{n+1} - 1 .$$

Es folgt

$$|a_n - (-1)|_2 = |2^{n+1}|_2 = \frac{1}{2^{n+1}} .$$

Also konvergiert (a_n) gegen -1.

(b) Es ist

$$b_n = 1 \cdot 2 + 2 \cdot 2^2 + \cdots + n \cdot 2^n = (n-1)2^{n+1} + 2 .$$

Es folgt

$$|b_n - 2|_2 = |(n-1)2^{n+1}|_2 = |n-1|_2 \cdot |2^{n+1}|_2 \leq 1 \cdot \frac{1}{2^{n+1}} .$$

Also konvergiert (b_n) gegen 2.
Beachte: Bezüglich der 2-adischen Bewertung gilt $|m|_2 \leq 1$ für alle natürlichen Zahlen $m \in \mathbb{N}$.

Aufgabe 7. Es sei K ein vollständiger Körper.
(a) Zeige, daß ein $\varepsilon > 0$ existiert, so daß alle $a \in K$ mit $|1 - a| < \varepsilon$ Quadrate in K sind.
(b) Zeige, daß alle positiven reellen Zahlen Quadrate sind.
(Hinweis: Betrachte das quadratische Polynom $(t+1)^2 - a$, bei Teil (b) zunächst den Fall $0 < a \leq 1$.)

Lösung. Es ist
$$f(t) = (t+1)^2 - a = t^2 + 2t + (1-a)\,.$$
Da K vollständig ist, besitzt $f(t)$ eine Nullstelle, wenn
$$|2|^2 > 4\,|1-a| \quad\Longleftrightarrow\quad |1-a| < \frac{|4|}{4}$$
ist. Also sind alle $a \in K$ mit $|1-a| < \frac{|4|}{4}$ Quadrate in K.

(b) $\mathbb{R}$ ist vollständig bezüglich des gewöhnlichen Absolutbetrages. Sei zunächst $0 < a \leq 1$. Dann ist
$$|1-a| = 1-a < 1\,.$$
Nach (a) ist damit a ein Quadrat in $\mathbb{R}$.

Ist $1 < a$, so folgt $0 < \frac{1}{a} < 1$. Also ist
$$\frac{1}{a} = x^2$$
für ein $x \in \mathbb{R}$. Es folgt
$$a = \frac{1}{x^2} = \left(\frac{1}{x}\right)^2 .$$
Also ist a ein Quadrat in $\mathbb{R}$.

Aufgabe 8. Es sei K ein nicht-archimedisch bewerteter Körper.

(a) Zeige, daß (a_n) eine Cauchy-Folge ist, wenn zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ existiert mit
$$|a_n - a_{n+1}| < \varepsilon$$
für alle $n \geq n_0$.

(b) Zeige, daß eine Reihe $\sum a_n$ konvergiert, wenn K vollständig und $\lim a_n = 0$ ist.

Lösung. Sei $\varepsilon > 0$ und $n_0 \in \mathbb{N}$ mit
$$|a_n - a_{n+1}| < \varepsilon$$
für alle $n \geq n_0$. Seien nun $n, m \geq n_0$ und $m \geq n$, etwa $m = n+k$ mit $k \in \mathbb{N}_0$. Es folgt
$$|a_n - a_m| = |(a_n - a_{n+1}) + \cdots + (a_{n+k-1} - a_{n+k})| \leq \max_{0 \leq i \leq k-1} |a_{n+i} - a_{n+i-1}| < \varepsilon\,.$$
Also ist (a_n) eine Cauchy-Folge.

(b) Sei $\varepsilon > 0$. Dann gibt es ein n_0 mit
$$|a_n| < \varepsilon$$
für alle $n \geq n_0$. Für alle $k \geq n_0$ ist damit
$$\left|\sum_{n=1}^{k+1} a_n - \sum_{n=1}^{k} a_n\right| = |a_{k+1}| < \varepsilon\,.$$
Nach (a) ist damit $\sum a_n$ eine Cauchy-Folge. Da K vollständig ist, ist also $\sum a_n$ konvergent.

Aufgabe 9. Ein Teilring B eines Körpers K heißt ein Bewertungsring, wenn für $x \in K^\times$ stets x oder x^{-1} in B liegt. Zeige:

(a) Ist I eine nicht-leere Teilmenge von B mit

$$x \in B,\, a \in I \quad \Longrightarrow \quad xa \in I\,,$$

so ist I ein Ideal von B.

(b) Die Ideale von B sind durch Inklusion linear geordnet (d.h. für zwei Ideale I_1, I_2 von B gilt $I_1 \subseteq I_2$ oder $I_2 \subseteq I_1$).

Lösung. (a) Zu zeigen ist noch: $(I, +)$ ist eine Untergruppe von $(B, +)$. Zunächst ist $1 \in B$, also auch $-1 \in B$. Ist nun $b \in I$, so folgt also $-b = (-1) \cdot b \in I$. Also ist $a - b \in I$ für $a = 0$ oder $b = 0$.

Sei nun $a, b \in I$ mit $a, b \neq 0$. Weil B ein Bewertungsring ist, folgt

$$a^{-1}b \in B \qquad \text{oder} \qquad b^{-1}a = (a^{-1}b)^{-1} \in B\,.$$

Somit ergibt sich

$$a - b = a(1 - a^{-1}b) = b(b^{-1}a - 1) \in IB \subseteq I\,.$$

Also ist I ein Ideal von B.

(b) Seien I_1, I_2 Ideale von B. Für $I_1 = 0$ oder $I_2 = 0$ ist die Behauptung offensichtlich richtig. Sei also $I_1, I_2 \neq 0$ und etwa $I_1 \not\subseteq I_2$. Dann gibt es es $a \in I_1 \backslash I_2$. Sei $b \in I_2$, $b \neq 0$. Weil B ist Bewertungsring ist, ist

$$a^{-1}b \in B \qquad \text{oder} \qquad b^{-1}a \in B\,.$$

Wäre $b^{-1}a \in B$, so wäre

$$a = b(b^{-1}a) \in I_2 B \subseteq I_2\,,$$

im Widerspruch zur Wahl von a. Also ist $a^{-1}b \in B$ und damit

$$b = a(a^{-1}b) \in I_1 B \subseteq I_2\,.$$

Also ist $I_2 \subseteq I_1$.

Aufgabe 10. Zeige unter Verwendung der geometrischen Reihe, daß in $\mathbb{Q}_p$

$$x = \sum_{i=0}^{\infty} a_i p^i\,, \qquad 0 \leq a_i \leq p-1$$

mit periodischen Koeffizienten (d.h. für ein $t \in \mathbb{N}$ gilt $a_i = a_{i+t}$ für alle i) eine rationale Zahl darstellt.

Berechne speziell $x = 1 + p + p^3 + p^4 + p^6 + p^7 + p^9 + p^{10} + \cdots$

Lösung. Da x die Periode t hat, gilt

$$x = a_0 p^0 + a_1 p^1 + a_2 p^2 + \cdots + a_{t-1}p^{t-1} + a_0 p^t + a_1 p^{t+1} + \cdots$$

und damit

$$\begin{array}{rcll} x & = & a_0\,(p^0 + p^t + p^{2t} + p^{3t} + \cdots) & + \\ & & a_1\,(p^1 + p^{t+1} + p^{2t+1} + p^{3t+1} + \cdots) & + \\ & & a_2\,(p^2 + p^{t+2} + p^{2t+2} + p^{3t+3} + \cdots) & + \\ & & \vdots & + \\ & & a_{t-1}\,(p^{t-1} + p^{2t-1} + p^{3t-1} + \cdots) & \end{array}$$

Faßt man nun zusammen, so ergibt sich

$$x = (a_0 + a_1 p + a_2 p^2 + \cdots + a_{t-1} p^{t-1}) \cdot \sum_{k=0}^{\infty} \left(p^t\right)^k = u \cdot \frac{1}{1-p^t} \in \mathbb{Q}\,.$$

Nebenrechnung: Setzt man $q = p^t$ und

$$s_n = \sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}\,,$$

so folgt

$$\left| s_n - \frac{1}{1-q} \right|_p = \left| \frac{1-q^{n+1}}{1-q} - \frac{1}{1-q} \right|_p = |q^{n+1}|_p \cdot \frac{1}{|1-q|_p} = \frac{1}{\left(p^t\right)^{n+1}} \cdot 1\,,$$

also ist

$$\sum_{k=0}^{\infty} \left(p^t\right)^k = \frac{1}{1-p^t}\,.$$

Speziell für $x = 1 + p + p^3 + p^4 + p^6 + p^7 + p^9 + p^{10} + \cdots$ ist $t = 3$, und es folgt

$$x = (1 + 1 \cdot p + 0 \cdot p^2) \cdot \sum_{k=0}^{\infty} \left(p^3\right)^k = \frac{1+p}{1-p^3}\,.$$

Aufgabe 11. Begründe, daß 7 ein Quadrat in $\mathbb{Q}_3$ ist.
Berechne die Wurzeln von 7

(a) mit dem Newtonschen Verfahren
(b) mit dem Ansatz $x = a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + \cdots$ aus der Gleichung $x^2 = 7$ durch Koeffizientenvergleich (möglich ist $a_0 = 1$ und $a_0 = 2$!)

jeweils bis auf einen Fehler $\leq |3|_3^5$.

Lösung. Wegen $|7|_3 = 1$ liegt 7 im Bewertungsring von $\mathbb{Q}_3$. Ist $\varphi : B \to \mathbb{Z}_3$ der Restklassenhomomorphismus, so gilt $\varphi(7) = 1$. Dies ist ein Quadrat in $\mathbb{Z}_3$. Nach Satz 3.8 ist damit 7 ein Quadrat in $\mathbb{Q}_3$.
Man kann auch das Polynom $f(t) = t^2 - 7$ betrachten. Es ist $f'(t) = 2t$. Mit $4 \in B$ folgt

$$|f(4)|_3 = |9| = |3|_3^2 = \frac{1}{9} < 1 = |2 \cdot 4|_3 = |f'(4)|^2\,.$$

Da $\mathbb{Q}_3$ vollständig ist, besitzt $f(x)$ nach Satz 3.6 eine Nullstelle in $\mathbb{Q}_3$, also ist 7 ein Quadrat in $\mathbb{Q}_3$.
(a) Zu berechnen sind die Wurzeln von $f(t) = t^2 - 7$. Wegen $f'(t) = 2t$ ergibt sich mit dem Startwert $x_1 = 4$

$$\begin{aligned} x_2 &= x_1 - \frac{x_1^2 - 7}{2x_1} &&= 4 - \frac{9}{8} &&= \frac{23}{8} \\ x_3 &= &&= \frac{23}{8} - \frac{81}{16 \cdot 32} &&= \frac{977}{368} \end{aligned}$$

Für den Fehler ergibt sich

$$|x-x_3|_3 \leq \left|\frac{f(x_3)}{f'(x_3)}\right|_3 = \left|\frac{\left(\frac{977}{368}\right)^2-7}{\frac{977}{184}}\right|_3 = \left|\frac{3^8}{2^5\cdot 23\cdot 977}\right|_3 = |3|_3^8 < |3|_3^5\,.$$

Die zweite Wurzel erhält man analog mit dem Startwert $x_1=-4$. Man erhält

$$x_3 = -\frac{977}{368}\,.$$

Für x_3 ist der Fehler $|x-x_3|_3$ wieder $\leq |3|_3^5$.
(b) Der Ansatz $x=\sum_{i=0}^\infty a_i 3^i$ zur Lösung der Gleichung $x^2=7$ führt auf

$$x^2 = \sum_{i=0}^\infty \left(\sum_{k=0}^i a_k a_{i-k}\right) 3^i = 7 = 1\cdot 3^0 + 2\cdot 3^1 + \sum_{i=2}^\infty 0\cdot 3^i\,.$$

Es folgt

$$a_0^2 = 1\,,\quad 2a_0a_1+\varepsilon_0 = 2\,,\quad \sum_{k=0}^i a_k a_{i-k} + \varepsilon_{i-1} = 0 \text{ für } i\geq 2\,,$$

wobei die ε_i jeweils die Überträge sind.
1. Fall: $a_0=1$. Dann ist $a_1=1$. a_2 ergibt sich aus der Gleichung

$$2a_2+1=0 \quad\Longrightarrow\quad a_2=1\,.$$

Als Übertrag erhält man 1. a_3 ergibt sich somit aus der Gleichung

$$2a_3+2a_1a_2+1 = 2a_3+3=0 \quad\Longrightarrow\quad a_3=0\,.$$

Als Übertrag erhält man 1. a_4 ergibt sich somit aus der Gleichung

$$2a_4+a_2^2+1 = 2a_4+2=0 \quad\Longrightarrow\quad a_4=2\,.$$

Als Näherungslösung ergibt sich somit $x_1=1,1102$.
2. Fall: $a_0=2$. Als Übertrag erhält man 1. a_1 ergibt sich somit aus der Gleichung

$$4a_1+1=2 \quad\Longrightarrow\quad a_1=1\,.$$

Als Übertrag erhält man 1. a_2 ergibt sich somit aus der Gleichung

$$4a_2+1+1 = 4a_2+2=0 \quad\Longrightarrow\quad a_2=1\,.$$

Als Übertrag erhält man 2. a_3 ergibt sich somit aus der Gleichung

$$4a_3+2+2 = 4a_3+4=0 \quad\Longrightarrow\quad a_3=2\,.$$

Als Näherungslösung ergibt sich somit $x_2=2,112$.
Den Fehler schätzt man wieder mit der Formel aus der Bemerkung zu Satz 3.6 ab. Man findet

$$|x-x_1|_3 \leq \left|\frac{x_1^2-7}{2x_1}\right|_3 = \left|\frac{175^2-7}{2\cdot 175}\right|_3 = \left|\frac{3^7}{5^2}\right|_3 = |3|_3^7 < |3|_3^5$$

und

$$|x-x_2|_3 \leq \left|\frac{x_2^2-7}{2x_2}\right|_3 = \left|\frac{68^2-7}{2\cdot 68}\right|_3 = \left|\frac{3^5\cdot 19}{2^3\cdot 17}\right|_3 = |3|_3^5\,.$$

AUFGABE 12. Zeige, daß eine rationale Zahl a genau dann ein Quadrat in $\mathbb{Q}$ ist, wenn a ein Quadrat in allen p-adischen Körpern $\mathbb{Q}_p$ und in $\mathbb{R}$ ist. (Betrachte die Primfaktorzerlegung von a.)

Lösung. 1.) Sei a ein Quadrat in $\mathbb{Q}$. Wegen $\mathbb{Q} \subseteq \mathbb{Q}_p$ für alle $p \in \mathbb{P}$ und $\mathbb{Q} \subseteq \mathbb{R}$ ist dann a auch ein Quadrat in allen p-adischen Körpern $\mathbb{Q}_p$ und in $\mathbb{R}$.
2.) Für $a = 0$ ist die Behauptung offensichtlich richtig. Sei also $a \in \mathbb{Q}^\times$. Weil a ein Quadrat in $\mathbb{R}$ ist, besitzt a eine Darstellung

$$a = \prod_{q \in \mathbb{P}} q^{\alpha_q} .$$

Sei nun $p \in \mathbb{P}$ fest gewählt. Dann ist

$$a = p^{\alpha_p} \cdot \prod_{q \in \mathbb{P} \setminus \{p\}} q^{\alpha_q} =: p^{\alpha_q} b .$$

Nach Voraussetzung ist a ein Quadrat in $\mathbb{Q}_p$. Wegen $|b|_p = 1$ ist α_p gerade nach Satz 3.7, also $\alpha_p = 2\beta_p$. Dies gilt für alle $p \in \mathbb{P}$. Es folgt

$$a = \prod_{q \in \mathbb{P}} q^{2\beta_q} \qquad \Longrightarrow \qquad a = \left(\prod_{q \in \mathbb{P}} q^{\beta_q} \right)^2 .$$

Also ist a ein Quadrat in $\mathbb{Q}$.

AUFGABE 13. Berechne für $x = \frac{3}{5}$ zwei Zahlen $a_0, b_0 \in \mathbb{N}$, $a_0 < 41$, $b_0 < 641$, so daß

$$|x - a_0|_{41} < 1 \qquad \text{und} \qquad |x - b_0|_{641} < 1$$

ist.
Stelle hiermit fest, ob x ein Quadrat in $\mathbb{Q}_{41}$ oder $\mathbb{Q}_{641}$ ist.

Lösung. (a) Allgemein gilt für $p \neq 3$, $p \neq 5$ und $a \in \mathbb{N}$:

$$|x - a|_p = \left| \frac{3 - 5a}{5} \right|_p < 1 \iff 5a \equiv 3 \bmod p .$$

1.) Man findet

$$5a_0 \equiv 3 \bmod 41 \iff 5a_0 \equiv 85 \bmod 41 \iff a_0 \equiv 17 \bmod 41 ,$$

also $a_0 = 17 + 41t$. Wegen $0 < a_0 < 41$ folgt $a_0 = 17$.
2.) Man findet

$$5b_0 \equiv 3 \bmod 641 \iff 5b_0 \equiv 1285 \bmod 641 \iff b_0 \equiv 257 \bmod 641 ,$$

also $b_0 = 257 + 641t$. Wegen $0 < b_0 < 641$ folgt $b_0 = 257$.
(b) Allgemein gilt: Ist $|x|_p = 1$ und $0 < c_0 < p$ mit $|x - c_0|_p < 1$, so ist c_0 der erste Koeffizient in der Darstellung

$$x = \sum_{i=0}^{\infty} c_i p^i , \qquad 0 \leq c_i < p .$$

Ist $p \neq 2$, so ist nach Satz 3.8 x genau dann ein Quadrat in $\mathbb{Q}_p$, wenn $\varphi(x)$ ein Quadrat im Restklassenkörper $\mathbb{Z}_p$ ist. Dies ist genau dann der Fall, wenn

$$\left(\frac{c_0}{p}\right) = 1$$

ist. Mit den folgenden Rechenregeln für das Legendre-Symbol

(1) Sind p und q verschiedene ungerade Primzahlen, so gilt
$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, falls $p \equiv 1 \bmod 4$ oder $q \equiv 1 \bmod 4$
$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, falls $p \equiv 3 \bmod 4$ und $q \equiv 3 \bmod 4$

(2) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, falls $p \not| ab$ und $a \equiv b \bmod p$

ergibt sich:

1.)

$$\left(\frac{17}{41}\right) \stackrel{(1)}{=} \left(\frac{41}{17}\right) = \left(\frac{7+2\cdot 17}{17}\right) \stackrel{(2)}{=} \left(\frac{7}{17}\right) \stackrel{(1)}{=} \left(\frac{17}{7}\right) = \left(\frac{3+2\cdot 7}{7}\right) \stackrel{(2)}{=} \left(\frac{3}{7}\right) = -1$$

2.)

$$\begin{aligned} \left(\frac{257}{641}\right) &\stackrel{(1)}{=} \left(\frac{641}{257}\right) = \left(\frac{127+2\cdot 257}{257}\right) \stackrel{(2)}{=} \left(\frac{127}{257}\right) \\ &\stackrel{(1)}{=} \left(\frac{257}{127}\right) = \left(\frac{3+2\cdot 127}{127}\right) \stackrel{(2)}{=} \left(\frac{3}{127}\right) \\ &\stackrel{(1)}{=} -\left(\frac{127}{3}\right) = -\left(\frac{1+42\cdot 3}{3}\right) \stackrel{(2)}{=} -\left(\frac{1}{3}\right) = -1 \end{aligned}$$

Also ist x weder in $\mathbb{Q}_{41}$ noch in $\mathbb{Q}_{641}$ ein Quadrat.

Aufgabe 14. Ermittle mit dem chinesischen Restsatz eine natürliche Zahl, die ein Quadrat in $\mathbb{Q}_2$ und Q_3, aber nicht in $\mathbb{Q}_5$ und $\mathbb{Q}_7$ ist.

Lösung. Beschränkt man sich auf natürliche Zahlen x mit $|x|_2 = |x|_3 = |x|_5 = |x|_7 = 1$, so kann man Satz 3.8 und Satz 3.9 anwenden. Hierzu löst man das Kongruenzensystem

$$\begin{aligned} x &\equiv 1 \bmod 8 \\ x &\equiv 1 \bmod 3 \\ x &\equiv a \bmod 5 \\ x &\equiv b \bmod 7 \end{aligned}$$

wobei a ein quadratischer Nichtrest modulo 5, also $a \in \{2, 3\}$ und b ein quadratischer Nichtrest modulo 7, also $b \in \{3, 5, 6\}$ ist. Wählt man etwa $a = 3$ und $b = 3$, so erhält man

$$x \equiv 1 \bmod 8 \tag{1}$$
$$x \equiv 1 \bmod 3 \tag{2}$$
$$x \equiv 3 \bmod 5 \tag{3}$$
$$x \equiv 3 \bmod 7 \tag{4}$$

Aus der ersten Kongruenz folgt $x = 8t + 1$. Eingesetzt in (2) erhält man

$$8t + 1 \equiv 1 \bmod 3 \iff 8t \equiv 0 \bmod 3 \iff t \equiv 0 \bmod 3$$

und damit $t = 3u$, also $x = 24u + 1$. Eingesetzt in (3) erhält man

$$24u + 1 \equiv 3 \bmod 5 \iff 24u \equiv 2 \bmod 5 \iff 12u \equiv 36 \bmod 5 \iff u \equiv 3 \bmod 5$$

und damit $u = 5v + 3$, also $x = 120v + 73$. Eingesetzt in (4) erhält man

$$120v + 73 \equiv 3 \bmod 7 \iff 120v \equiv 0 \bmod 7 \iff v \equiv 0 \bmod 7$$

und damit $v = 7w$, also $x = 840w + 73$.
Damit ist zum Beispiel $x = 73$ ein Quadrat in $\mathbb{Q}_2$ und $\mathbb{Q}_3$, nicht aber in $\mathbb{Q}_5$ und $\mathbb{Q}_7$.

Aufgabe 15. Für das Hilbertsymbol gelten folgende Rechenregeln:

(A) $(a,b) = (b,a)$
(B) $(a,b) = (a, bc^2)$, $c \in K^\times$
(C) $(a,b) = (a, -ab)$
(D) $(a,b) = \big(a, (1-a)b\big)$, $a \neq 1$

(a) Zeige allein mit den Regeln (A) – (D)

(E) $(a,b) = (a+b, -ab)$, $a + b \neq 0$.

(b) Zeige in $\mathbb{Q}$:

$$(2,3)_{\mathbb{Q}} = (5,-6)_{\mathbb{Q}} = (5,6)_{\mathbb{Q}} = (2,-3)_{\mathbb{Q}}\,.$$

Lösung. (a) Wegen $a + b \neq 0$ ist $ab^{-1} \neq -1$, also $-ab^{-1} \neq 1$. Es folgt

$$\begin{aligned}
(a,b) &= (a, b^{-1}\cdot b^2) &&\overset{(B)}{=} (a, b^{-1}) &&\overset{(A)}{=} (b^{-1}, a)\\
&\overset{(C)}{=} (b^{-1}, -ab^{-1}) &&\overset{(A)}{=} (-ab^{-1}, b^{-1}) &&= (-ab^{-1}, b\cdot b^{-2})\\
&\overset{(B)}{=} (-ab^{-1}, b) &&\overset{(D)}{=} \big(-ab^{-1}, (1-(-ab^{-1}))b\big) &&= (-ab^{-1}, a+b)\\
&\overset{(A)}{=} (a+b, -ab^{-1}) &&\overset{(B)}{=} (a+b, -ab^{-1}\cdot b^2) &&= (a+b, -ab)
\end{aligned}$$

(b) Es ist

$$\begin{aligned}
(2,3) &\overset{(E)}{=} (2+3, -2\cdot 3) &&= (5,-6)\\
&\overset{(D)}{=} \big(5, (1-5)\cdot(-6)\big) &&= (5, 6\cdot 4) &&= (5, 6\cdot 2^2)\\
&\overset{(B)}{=} (5,6) &&= \big(-1+6, -(-1)\cdot 6\big)\\
&\overset{(E)}{=} (-1,6) &&= \big(2+(-3), -2\cdot(-3)\big) &&\overset{(E)}{=} (2,-3)
\end{aligned}$$

Aufgabe 16. Berechne die Hilbert-Symbole

$$\left(-\frac{10}{3}, -\frac{3}{5}\right)_K \tag{1}$$

für $K = \mathbb{Q}_p$ $(p \neq 2)$ und $K = \mathbb{R}$.
Benutze die Produktformel, um (1) auch für $p = 2$ zu berechnen.

Lösung. In $\mathbb{R}$ hat die Gleichung

$$-\frac{10}{3}x^2 - \frac{3}{5}y^2 = z^2$$

nur die triviale Lösung. Daher ist $\left(-\frac{10}{3}, -\frac{3}{5}\right)_{\mathbb{R}} = -1$.
In $\mathbb{Q}_p$ gilt

$$\begin{aligned}
\left(-\frac{10}{3}, -\frac{3}{5}\right)_{\mathbb{Q}_p} &= \left(-\frac{10}{3}\cdot 3^2, -\frac{3}{5}\cdot 5^2\right)_{\mathbb{Q}_p} &&= (-30,-15)_{\mathbb{Q}_p} \\
&= (-2\cdot 15, -15)_{\mathbb{Q}_p} &&= (-2,-15)_{\mathbb{Q}_p} \cdot \underbrace{(15,-15)_{\mathbb{Q}_p}}_{=1} \\
&= (-2,-15)_{\mathbb{Q}_p} &&= (-2,-3\cdot 5)_{\mathbb{Q}_p} \\
&= (-2,-3)_{\mathbb{Q}_p}\cdot(-2,5)_{\mathbb{Q}_p} &&= (-2,3)_{\mathbb{Q}_p}\cdot(-2,-5)_{\mathbb{Q}_p}
\end{aligned}$$

Für $p \neq 2,3,5$ ist $(-2,-3)_{\mathbb{Q}_p} = (-2,5)_{\mathbb{Q}_p} = 1$ nach Satz 4.6. Es folgt

$$\left(-\frac{10}{3}, -\frac{3}{5}\right)_{\mathbb{Q}_p} = 1\,, \qquad p \neq 2,3,5\,.$$

Für $p = 3$ ist $(-2,3)_{\mathbb{Q}_3} = \left(\frac{-2}{3}\right) = \left(\frac{1}{3}\right) = 1$ und $(-2,-5)_{\mathbb{Q}_3} = 1$ nach Satz 4.6. Also ist auch

$$\left(-\frac{10}{3}, -\frac{3}{5}\right)_{\mathbb{Q}_3} = 1\,.$$

Für $p = 5$ ist $(-2,-3)_{\mathbb{Q}_5} = 1$ und $(-2,5)_{\mathbb{Q}_5} = \left(\frac{-2}{5}\right) = \left(\frac{3}{5}\right) = -1$ nach Satz 4.6. Es folgt

$$\left(-\frac{10}{3}, -\frac{3}{5}\right)_{\mathbb{Q}_5} = -1\,.$$

Nach der Produktformel ist mit $a = -\frac{10}{3}$ und $b = -\frac{3}{5}$

$$\prod_{p\in\mathbb{P}\cup\infty} (a,b)_p = (a,b)_2\cdot(a,b)_3\cdot(a,b)_5\cdot(a,b)_\infty = (a,b)_2\cdot 1\cdot(-1)\cdot(-1) = 1$$

und damit $\left(-\frac{10}{3}, -\frac{3}{5}\right)_2 = 1$.

Aufgabe 17. (a) Ein Element $a \neq 0$ ist genau dann in einem Körper K Summe zweier Quadrate, wenn $(a,-1)_K = 1$ ist.
(b) Ist $p \equiv 1 \bmod 4$, so ist in $\mathbb{Q}_p$ jedes Element Summe zweier Quadrate.

Lösung. (a) Mit $H_u = \{v \in K^\times \mid v = x^2 - uy^2\}$ folgt

$$(a,-1)_K = 1 \overset{\text{Satz 4.1}}{\iff} a \in H_{-1} \iff a = x^2 + y^2\,.$$

(b) Für $a = 0$ ist die Aussage offensichtlich richtig. Sei nun $a \neq 0$, also $a = p^k\alpha$ mit $k \in \mathbb{Z}$ und $|\alpha| = 1$. Es folgt

$$(a,-1) = (-1,p^k\alpha) = (-1,p)^k\cdot(-1,\alpha) = (-1,p)^k\cdot 1 = (-1,p)^k$$

nach Satz 4.6. Mit $p = 4n+1$ folgt weiterhin

$$(-1, p) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2n} = 1\,.$$

Insgesamt ist damit $(a, -1) = 1$. Nach (a) ist daher a Summe zweier Quadrate

Aufgabe 18. Jedes Element von $\mathbb{Q}_p$, $p \neq 2$, ist Summe dreier Quadrate.

Lösung. Für $a = 0$ ist die Behauptung offensichtlich richtig. Sei nun $a \neq 0$, also $a = p^k \alpha$ mit $k \in \mathbb{Z}$ und $|\alpha| = 1$.

1. Fall: k ist gerade, also $k = 2n$. Mit Satz 4.6 folgt

$$(a, -1) = (p^{2n}\alpha, -1) = (p, -1)^{2n} \cdot (\alpha, -1) = 1\,.$$

Nach Aufgabe 17 gibt es daher $x, y \in \mathbb{Q}_p$, $(x, y) \neq (0, 0)$ mit

$$a = x^2 + y^2 = x^2 + y^2 + 0^2\,.$$

2. Fall: Sei nun k ungerade, also $k = 2n+1$. Dann ist $|p\alpha| < 1$, also $|p\alpha - 1| = 1$. Nach Satz 4.6 ist daher $(p\alpha - 1, -1) = 1$. Nach Aufgabe 17 gibt es daher $x, y \in \mathbb{Q}_p$, $(x, y) \neq (0, 0)$ mit

$$p\alpha - 1 = x^2 + y^2 \quad \Longrightarrow \quad p\alpha = x^2 + y^2 + 1^2\,.$$

Es folgt

$$a = p^{2n+1} \cdot \alpha = p^{2n} \cdot p\alpha = p^{2n}\left(x^2 + y^2 + 1^2\right) = \left(p^n x\right)^2 + \left(p^n y\right)^2 + \left(p^n\right)^2\,.$$

Aufgabe 19. Es sei $p \in \mathbb{P}$, $p \neq 2$. Zeige für $a, b \in \mathbb{Z}$, die kein Vielfaches von p sind,

$$(pa, pb)_p = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)\,.$$

Lösung. Nach Satz 4.6 ist

$$(p, a)_p = \left(\frac{a}{p}\right), \qquad (p, b)_p = \left(\frac{b}{p}\right), \qquad (a, b)_p = 1\,.$$

Weiterhin ist

$$(p, p)_p = (p, -p^2)_p = (p, -1)_p = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

nach dem ersten Ergänzungssatz zum quadratischen Reziprozitätsgesetz. Insgesamt folgt damit

$$(pa, pb)_p = (p, p)_p \cdot (p, b)_p \cdot (a, p) \cdot (a, b) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)\,.$$

Aufgabe 20. Besitzen die Gleichungen

(a) $3x^2 + 5y^2 - 7z^2 = 0$
(b) $3x^2 - 5y^2 - 7z^2 = 0$

in $\mathbb{Q}$ nicht-triviale Lösungen?

Lösung. Sind $a, b, c \in \mathbb{Z}\backslash\{0\}$, so besitzt die Gleichung $ax^2 + by^2 = cz^2$ genau dann eine nicht-triviale Lösung in $\mathbb{Q}$, wenn die Gleichung $acx^2 + bcy^2 = (cz)^2$ eine nicht-triviale Lösung in $\mathbb{Q}$ besitzt. Dies wiederum ist genau dann der Fall, wenn $(ac, bc)_p = 1$ für alle $p \in \mathbb{P} \cup \{\infty\}$ ist.

(a) Hier ist $a = 3$, $b = 5$, $c = 7$. Also muß $(21, 35)_p$ betrachtet werden. Wegen $21 > 0$ ist $(21, 35)_\infty = 1$. Für $p \neq 2, 3, 5, 7$ ist $(21, 35)_p = 1$ nach Satz 4.6. Für $p = 7$ ist

$$(21, 35)_7 = (7 \cdot 3, 7 \cdot 5)_7 = (-1)^{\frac{7-1}{2}} \cdot \left(\frac{3}{7}\right) \cdot \left(\frac{5}{7}\right) = (-1) \cdot (-1) \cdot (-1) = -1$$

nach Aufgabe 19. Nach Satz 5.1 ist damit die Gleichung

$$3x^2 + 5y^2 - 7z^2 = 0$$

in $\mathbb{Q}$ nur trivial lösbar.

(b) Hier ist $a = 3$, $b = -5$, $c = 7$. Also muß $(21, -35)_p$ betrachtet werden. Wegen $21 > 0$ ist $(21, -35)_\infty = 1$. Für $p \neq 2, 3, 5, 7$ ist $(21, 35)_p = 1$ nach Satz 4.6. Für $p = 7$ ist nach Aufgabe 19

$$(21, -35)_7 = \big(7 \cdot 3, 7 \cdot (-5)\big)_7 = (-1)^{\frac{7-1}{2}} \cdot \left(\frac{3}{7}\right) \cdot \left(\frac{-5}{7}\right) = (-1) \cdot (-1) \cdot 1 = 1\,.$$

Für $p = 5$ ist

$$(21, -35)_5 = \big(21, 5 \cdot (-7)\big)_5 = (21, 5)_p \cdot (21, -7)_5 = (21, 5)_5 \cdot 1 = \left(\frac{21}{5}\right) = \left(\frac{1}{5}\right) = 1\,.$$

Für $p = 3$ ist

$$(21, -35)_3 = (3 \cdot 7, -35)_3 = (3, -35)_3 \cdot (7, -35)_3 = (3, -35)_3 = \left(\frac{-35}{3}\right) = \left(\frac{1}{3}\right) = 1\,.$$

Für $p = 2$ ist

$$(21, -35)_2 = (-1)^{\frac{21-1}{2} \cdot \frac{-35-1}{2}} = 1$$

nach Satz 4.7. Also ist $(21, -35)_p = 1$ für alle $p \in \mathbb{P} \cup \{\infty\}$. Nach Satz 5.1 besitzt damit die Gleichung

$$3x^2 - 5y^2 - 7z^2 = 0$$

nicht-triviale Lösungen in $\mathbb{Q}$.

Aufgabe 21. Für welche $a \in \mathbb{Z}$ besitzt die Gleichung

$$x^2 + 2y^2 = az^2$$

nicht-triviale Lösungen in $\mathbb{Q}$?

Lösung. Zunächst beweisen wir folgendes

Lemma (a) *Sei $p \neq 2$. Dann gilt:*

$$(p, -2)_p = \begin{cases} 1 & \textit{für } p \equiv 1 \bmod 8 \textit{ oder } p \equiv 3 \bmod 8 \\ -1 & \textit{für } p \equiv 5 \bmod 8 \textit{ oder } p \equiv 7 \bmod 8 \end{cases}$$

(b) $(2, -2)_p = 1$.

BEWEIS (a) Es ist

$$(p,-2)_p = (p,-1)_p \cdot (p,2)_p = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}$$

nach den Ergänzungssätzen zum quadratischen Reziprozitätsgesetz. Da p eine ungerade Primzahl, also von der Form $p = 2k+1$ ist, ist $(p,-2)_p = 1$ genau dann, wenn

$$\frac{p-1}{2} + \frac{p^2-1}{8} = k + \frac{k^2+k}{2} = \frac{k\,(k+3)}{2} \in 2\mathbb{Z}$$

also $k\,(k+3) \in 4\mathbb{Z}$ ist. Dies wiederum ist genau dann der Fall, wenn

$$k \equiv 0 \bmod 4 \qquad \text{oder} \qquad k \equiv 1 \bmod 4$$

ist. Eingesetzt erhält man

$$(p,-2)_p = 1 \iff (p \equiv 1 \bmod 8 \vee p \equiv 3 \bmod 8)\,.$$

(b) $(2,-2)_p = \big(2,(-2)\cdot(-2)\big)_p = (2,4)_p = (2,1)_p = 1$. $\square$

Für $a = 0$ ist $(0,0,1)$ eine nicht-triviale Lösung. Sei nun $a \neq 0$. Nach Satz 5.1 besitzt dann die Gleichung $x^2 + 2y^2 = az^2$ genau dann nicht-triviale Lösungen in $\mathbb{Q}$, wenn $(a,-2)_p = 1$ für $p \in \mathbb{P} \cup \{\infty\}$ ist.
Zunächst ist $(a,-2)_\infty = 1 \iff a > 0$.
Sei nun $p \in \mathbb{P} \setminus \{2\}$, beliebig, und $a = p^k\alpha$ mit $|\alpha|_p = 1$ und $k \in \mathbb{N}_0$. Dann ist

$$(a,-2)_p = (p^k\alpha,-2)_p = (p,-2)^k \cdot (\alpha,-2)_p = \left(\frac{-2}{p}\right)^k \cdot 1 = \left(\frac{-2}{p}\right)^k.$$

Ist nun $p \equiv 1 \bmod 8$ oder $p \equiv 3 \bmod 8$, so ist also nach dem Lemma $(a,-2)_p = 1$ für beliebiges $k \in \mathbb{N}_0$. Ist hingegen $p \equiv 5 \bmod 8$ oder $p \equiv 7 \bmod 8$, so ist $(a,-2)_p = 1$ genau dann, wenn k gerade ist.
Damit ergibt sich folgendes: Für $a \in \mathbb{Z} \setminus \{0\}$ gilt

$$(a,-2)_\infty = 1 \qquad \text{und} \qquad (a,-2)_p = 1 \ \text{ für } p \in \mathbb{P} \setminus \{2\}$$

genau dann, wenn $a > 0$ ist und in der Primfaktorzerlegung von a alle Primfaktoren p mit $p \equiv 5 \bmod 8$ oder $p \equiv 7 \bmod 8$ nur in gerader Potenz auftreten. Nach der Produktformel gilt für solches a auch $(a,-2)_2 = 1$.
Für solche a und für $a = 0$ besitzt daher nach Satz 5.1 die Gleichung $x^2 + 2y^2 = az^2$ nicht-triviale Lösungen in $\mathbb{Q}$.

AUFGABE 22. Für welche Primzahlen p ist die Gleichung

$$3x^2 + py^2 = z^2$$

in $\mathbb{Q}$ nicht-trivial lösbar?
Gib die drei kleinsten Primzahlen mit dieser Eigenschaft an.

Lösung. $3x^2 + py^2 = z^2$ ist genau dann in $\mathbb{Q}$ nicht-trivial lösbar, wenn $(3,p)_{\mathbb{Q}} = 1$ ist. Dies wiederum ist genau dann der Fall, wenn $(3,p)_q = 1$ für alle $q \in \mathbb{P} \cup \infty$ ist.
Wegen $3 > 0$ ist $(3,p)_\infty = 1$ für alle Primzahlen p.
1. $q = 2$: Nach Satz 4.7 ist

$$(3,2)_2 = (-1)^{\frac{9-1}{8}} = -1\,,$$

also ist $p = 2$ nicht möglich. Für $p \neq 2$ ist nach Satz 4.7

$$(3,p)_2 = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} = 1 \iff p \equiv 1 \bmod 4\,.$$

Also braucht man nur noch mit $p \equiv 1 \bmod 4$ weiterzurechnen.
2. $q = 3$: Nach Satz 4.6 ist

$$(3,p)_3 = \left(\frac{p}{3}\right) = 1$$

genau dann, wenn p quadratischer Rest modulo 3, also $p \equiv 1 \bmod 3$ ist.
Ergebnis: Ist $3x^2 + py^2 = z^2$ nicht-trivial in $\mathbb{Q}$ lösbar, so ist $p \equiv 1 \bmod 12$.

Dies ist auch hinreichend, denn für $p \equiv 1 \bmod 12$ ist

$$\begin{array}{lclcll}
(3,p)_2 & = & (-1)^{1\cdot 6} & = & 1 & \\
(3,p)_3 & = & \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) & = & 1 & \\
(3,p)_p & = & \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)^{\dagger} & = & 1 & \\
(3,p)_q & = & & = & 1 & \quad q \neq 2,3,p
\end{array}$$

Die drei kleinsten Primzahlen mit dieser Eigenschaft sind 13, 37 und 61.

Aufgabe 23. Die Gleichung

$$x^2 + y^2 + 8xy + 2x - 4y + 1 = 0$$

hat die Lösung $(x_0, y_0) = (1, -2)$. Berechne hiermit sämtliche Lösungen in $\mathbb{Q}$. (Hinweis: Setze $x = \frac{u}{w}$, $y = \frac{v}{w}$.)

Lösung. Substituiert man $x = \frac{u}{w}$ und $y = \frac{v}{w}$, so ergibt sich

$$\frac{u^2}{w^2} + \frac{v^2}{w^2} + 8\,\frac{u}{w}\frac{v}{w} + 2\,\frac{u}{w} - 4\,\frac{v}{w} + 1 = 0\,,$$

also

$$u^2 + v^2 + w^2 + 8uv + 2uw - 4vw = 0\,.$$

Eine Lösung hiervon ist $u_0 = 1$, $v_0 = -2$, $w_0 = 1$.
Um die Gesamtheit aller Lösungen zu finden, transformiert man

$$\begin{array}{lcl}
u & = & u_0 \cdot a \\
v & = & v_0 \cdot a + b \\
w & = & w_0 \cdot a + c
\end{array}
\qquad \text{also} \qquad
\begin{array}{lcl}
u & = & a \\
v & = & -2a + b \\
w & = & a + c
\end{array}$$

Eingesetzt erhält man

$$a^2 + (-2a+b)^2 + (a+c)^2 + 8a\,(-2a+b) + 2a\,(a+c) - 4\,(-2a+b)(a+c) = 0\,,$$

also

(1) $$b^2 + c^2 + 12ac - 4bc = 0 \quad\Longrightarrow\quad 12ac = 4bc - b^2 - c^2\,.$$

Für $c \neq 0$ erhält man

$$a = \frac{4bc - b^2 - c^2}{12c}$$

† Wegen $p \equiv 1 \bmod 12$

und damit

$$u=\frac{4bc-b^2-c^2}{12c}\,,\qquad v=\frac{4bc+2b^2+2c^2}{12c}\,,\qquad w=\frac{4bc-b^2+11c^2}{12c}$$

Rücksubstitution liefert

$$x=\frac{4bc-b^2-c^2}{4bc-b^2+11c^2}\,,\qquad y=\frac{4bc+2b^2+2c^2}{4bc-b^2+11c^2} \tag{2}$$

(Beachte, daß $4bc-b^2+11c^2=0$ in $\mathbb{Q}$ nur die triviale Lösung $b=c=0$ besitzt.)
Für $c=0$ folgt $b=0$ und $a\in\mathbb{Q}$, beliebig, nach (1). Für $a\neq 0$ erhält man hieraus wieder die Lösung $(1,-2)$. Diese ist mit $b=1, c=0$ bereits in (2) enthalten.

Aufgabe 24. Es sei

$$f(x,y)=ax^2+by^2$$

mit $a,b\in\mathbb{Q}^\times$. Eine Zahl $\alpha\in\mathbb{Q}$ heißt durch f darstellbar, wenn $\alpha=f(x,y)$ für ein $(x_0,y_0)\in\mathbb{Q}^2$, $(x_0,y_0)\neq(0,0)$, ist.
Zeige: Sind $\alpha,\beta\in\mathbb{Q}^\times$ durch f darstellbar, so gilt

$$(\alpha\beta,-ab)_{\mathbb{Q}}=1\,.$$

Lösung. Da α und β durch f darstellbar sind, gibt es $u,v,r,s\in\mathbb{Q}$, $(u,v)\neq(0,0)$ und $(r,s)\neq(0,0)$ mit

$$\alpha = au^2+bv^2 \tag{1}$$

$$\beta = ar^2+bs^2 \tag{2}$$

1. Möglichkeit: Aus (1) folgt durch Multiplikation mit b

$$\alpha b\cdot 1^2-abu^2=(bv)^2\,,$$

und aus (2) folgt durch Multiplikation mit b

$$\beta b\cdot 1^2-abr^2=(bs)^2\,.$$

Also ist

$$(\alpha b,-ab)_{\mathbb{Q}}=(\beta b,-ab)_{\mathbb{Q}}=1\,.$$

Mit Korollar 5.2 folgt

$$(\alpha b,-ab)_p=(\beta b,-ab)_p=1$$

für alle $p\in\mathbb{P}\cup\{\infty\}$. Da das Hilbert-Symbol multiplikativ ist für $\mathbb{Q}_p$ und $\mathbb{R}$, folgt

$$(\alpha\beta,-ab)_p\overset{(B)}{=}(b^2\alpha\beta,-ab)_p=(\alpha b,-ab)_p\cdot(\beta b,-ab)_p=1\cdot 1=1$$

für alle $p\in\mathbb{P}\cup\infty$. Nach Korollar 5.2 ist damit

$$(\alpha\beta,-ab)_{\mathbb{Q}}=1\,.$$

2. Möglichkeit: Mit (1) und (2) ergibt sich

$$\begin{aligned}\alpha\beta &= (au^2+bv^2)(ar^2+bs^2)\\ &= a^2u^2r^2+abu^2s^2+abr^2v^2+b^2v^2s^2\\ &= (aur+bvs)^2+(abu^2s^2+abr^2v^2)-2abusrv\\ &= (aur+bvs)^2+ab\,(us-rv)^2\end{aligned}$$

und damit

$$\alpha\beta \cdot 1^2 - ab\,(us - rv)^2 = (aru + bvs)^2\,.$$

Also besitzt die Gleichung $\alpha\beta x^2 - aby^2 = z^2$ eine nicht-triviale Lösung, d.h. es ist $(\alpha\beta, -ab)_K = 1$ für alle Körper K.

Hinweis Alle im folgenden vorkommenden ganzen Zahlen d seien als quadratfrei vorausgesetzt.

Aufgabe 25. Ermittle in $\mathbb{Q}(\sqrt{d})$ für $d < 0$ alle Elemente ε mit $\varepsilon^6 = 1$.

Lösung. Wegen $\varepsilon^6 = 1$ ist ε Nullstelle von $f(t) = t^6 - 1$. In $\mathbb{C}$ besitzt $f(t)$ eine Zerlegung

$$f(t) = (t-1)(t+1)\left(t - \tfrac{-1+\sqrt{-3}}{2}\right)\left(t - \tfrac{-1-\sqrt{-3}}{2}\right)\left(t - \tfrac{1+\sqrt{-3}}{2}\right)\left(t - \tfrac{1-\sqrt{-3}}{2}\right)$$

Sämtliche sechs Nullstellen liegen in $\mathbb{Q}(\sqrt{-3})$, d.h. in $\mathbb{Q}(\sqrt{-3})$ gibt es sechs Elemente ε mit $\varepsilon^6 = 1$.
In $\mathbb{Q}(\sqrt{d})$, $d < 0$, $d \neq -3$, hingegen erfüllen nur $\varepsilon = \pm 1$ die Gleichung $\varepsilon^6 = 1$.

Aufgabe 26. In $\mathbb{Q}(\sqrt{d})$ heißt $\{\omega_1, \omega_2\}$ eine Ganzheitsbasis, wenn

$$\mathfrak{O} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

ist. Sei ω wie in der Vorlesung definiert und

$$\begin{aligned}\omega_1 &= a + b\omega\\ \omega_2 &= c + e\omega\,.\end{aligned}$$

Welche Bedingungen müssen die Koeffizienten a, b, c, e erfüllen, damit $\{\omega_1, \omega_2\}$ eine Ganzheitsbasis ist?
Berechne für $d < 0$ in der Gaußschen Zahlenebene den Flächeninhalt des von ω_1 und ω_2 aufgespannten Parallelogramms.

Lösung. Sei

$$\mathfrak{M} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \quad \text{und} \quad \mathfrak{O} = \mathbb{Z} + \mathbb{Z}\omega\,.$$

1.) Wegen $\mathfrak{M} = \mathfrak{O}$ ist insbesondere $\omega_1, \omega_2 \in \mathfrak{O}$, d.h. es sind $a, b, c, e \in \mathbb{Z}$.
Ist nun $u + v\omega \in \mathfrak{O} = \mathfrak{M}$, beliebig, so gibt es $x, y \in \mathbb{Z}$ mit

$$u + v\omega = x\omega_1 + y\omega_2 = x\,(a + b\omega) + y\,(c + e\omega) = ax + cy + (bx + ey)\,\omega\,.$$

Also müssen $a, b, c, e \in \mathbb{Z}$ so gewählt werden, daß das lineare Gleichungssystem

$$\begin{array}{rcrcl} ax &+& cy &=& u\\ bx &+& ey &=& v\end{array} \tag{1}$$

für alle ganzen Zahlen u, v ganzzahlig lösbar ist. In $\mathbb{Q}$ ist (1) genau dann für alle ganzen Zahlen u, v lösbar, wenn

$$\begin{vmatrix} a & c\\ b & e\end{vmatrix} = ae - bc =: \Delta \neq 0$$

ist. Nach der Cramerschen Regel ist

$$x = \frac{\begin{vmatrix} u & c\\ v & e\end{vmatrix}}{\Delta} = \frac{ue - vc}{\Delta} \quad \text{und} \quad y = \frac{\begin{vmatrix} a & u\\ b & v\end{vmatrix}}{\Delta} = \frac{av - bu}{\Delta}$$

die Lösung von (1). Da x, y stets ganzzahlig sein sollen, erhält man, indem man für $(u, v) = (1, 0)$ und $(u, v) = (0, 1)$ einsetzt:

$$\Delta | a\,, \quad \Delta | b\,, \quad \Delta | c\,, \quad \Delta | e\,,$$

also

$$a = \alpha\Delta\,, \quad b = \beta\Delta\,, \quad c = \gamma\Delta\,, \quad e = \varepsilon\Delta\,.$$

Also geht (1) über in

$$\Delta\,(\alpha x + \gamma y) = u \quad \text{und} \quad \Delta\,(\beta x + \varepsilon y) = v\,,$$

d.h. Δ teilt alle ganzen Zahlen. Dies ist aber nur für $\Delta = \pm 1$ möglich.
Ergebnis: $\{\omega_1, \omega_2\}$ ist genau dann eine Ganzheitsbasis in $\mathbb{Q}(\sqrt{d})$, wenn die Koeffizienten $a, b, c, e \in \mathbb{Z}$ sind und $ae - bc = \pm 1$ ist.

Allgemein: Sind $z_1 = u_1 + v_1 i, z_2 = u_2 + v_2 i \in \mathbb{C}$, so gilt für den Flächeninhalt F des von z_1 und z_2 aufgespannten Parallelogramms

$$F = |u_1 v_2 - v_1 u_2|\,.$$

Sei $\delta := \sqrt{-d}$.
Ist $d \equiv 2, 3 \bmod 4$, so ist $\omega = \sqrt{d} = \delta i$, also

$$\omega_1 = a + b\delta i\,, \quad \omega_2 = c + e\delta i\,.$$

Somit folgt

$$F = |ae\delta - bc\delta| = \delta\,|ae - bc| = \delta \cdot 1 = \sqrt{-d}\,.$$

Ist $d \equiv 1 \bmod 4$, so ist $\omega = \frac{1+\sqrt{d}}{2} = \frac{1}{2} + \frac{\delta}{2} i$, also

$$\omega_1 = \frac{2a+b}{2} + \frac{b\delta}{2} i\,, \qquad \omega_2 = \frac{2c+e}{2} + \frac{e\delta}{2} i\,.$$

Somit folgt

$$F = \left| \frac{2a+b}{2}\,\frac{e\delta}{2} - \frac{2c+e}{2}\,\frac{b\delta}{2} \right| = \frac{\delta}{4}\,|2ae + be - 2bc - be| = \frac{\delta}{2}\,|ae - bc| = \frac{\delta}{2} \cdot 1 = \frac{\sqrt{-d}}{2}\,.$$

Aufgabe 27. (a) Ist d durch eine Primzahl $p \equiv 3 \bmod 4$ teilbar, so gilt

$$\mathrm{N}\varepsilon = 1$$

für alle Einheiten $\varepsilon \in \mathfrak{O}$.

(b) Teste für $d = 2$, 6 und 10, ob ein ganzes Element $\varepsilon \in \mathbb{Q}(\sqrt{d})$ mit $\mathrm{N}\varepsilon = -1$ existiert.

Lösung. (a) Sei $\varepsilon = x + y\omega \in \mathfrak{O}$ eine Einheit. Nach Satz 6.3 ist dann $\mathrm{N}\varepsilon = 1$ oder $\mathrm{N}\varepsilon = -1$. Zu zeigen bleibt also, daß $\mathrm{N}\varepsilon = -1$ nicht auftreten kann, wenn d durch eine Primzahl $p \equiv 3 \bmod 4$ teilbar ist.
1. Fall: $d \not\equiv 1 \bmod 4$. Dann ist $\omega = \sqrt{d}$, also

$$\mathrm{N}\varepsilon = \varepsilon \cdot \bar{\varepsilon} = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2\,.$$

Wäre nun $\mathrm{N}\varepsilon = -1$, so wäre

$$x^2 - dy^2 = -1 \quad \Longrightarrow \quad x^2 \equiv -1 \bmod p\,,$$

d.h. -1 wäre quadratischer Rest modulo p. Wegen $p \equiv 3 \bmod 4$ gilt aber

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1\,.$$

Dies ist ein Widerspruch. Für $d \not\equiv 1 \bmod 4$ gilt daher $\mathrm{N}\varepsilon = 1$ für alle Einheiten $\varepsilon \in \mathfrak{O}$.

2. Fall: $d \equiv 1 \bmod 4$. Dann ist $\omega = \frac{1+\sqrt{d}}{2}$, also

$$\varepsilon = x + y\,\frac{1+\sqrt{d}}{2} = \frac{1}{2}\left(2x + y\,(1+\sqrt{d})\right) = \frac{1}{2}\left((2x+y) + y\sqrt{d}\right).$$

Setzt man $2x + y = z$, so folgt

$$\mathrm{N}\varepsilon = \varepsilon\bar{\varepsilon} = \frac{1}{4}\,(z + y\sqrt{d})(z - y\sqrt{d}) = \frac{1}{4}\,(z^2 - dy^2)\,.$$

Wäre nun $\mathrm{N}\varepsilon = -1$, so wäre

$$z^2 - dy^2 = -4 \quad \Longrightarrow \quad z^2 \equiv -4 \bmod p\,,$$

d.h. -4 wäre quadratischer Rest modulo p. Wegen $p \equiv 3 \bmod 4$ gilt aber

$$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{4}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{2}{p}\right)^2 = -1\,.$$

Dies ist ein Widerspruch. Für $d \equiv 1 \bmod 4$ gilt daher ebenfalls $\mathrm{N}\varepsilon = 1$ für alle Einheiten $\varepsilon \in \mathfrak{O}$.

(b) Wegen $2, 6, 10 \equiv 2 \bmod 4$ ist

$$\mathfrak{O}_d = \mathbb{Z} + \mathbb{Z}\sqrt{d}\,, \qquad d = 2, 6, 10\,.$$

(i) Für $\varepsilon = 1 + \sqrt{2} \in \mathfrak{O}_2$ ist

$$\mathrm{N}\varepsilon = (1+\sqrt{2})(1-\sqrt{2}) = 1 - 2 = -1\,.$$

(ii) Wegen $6 = 2 \cdot 3$ ist nach (a) $\mathrm{N}\varepsilon = 1$ für alle $\varepsilon \in \mathfrak{O}_6$.

(iii) Für $\varepsilon = 3 + \sqrt{10} \in \mathfrak{O}_{10}$ ist

$$\mathrm{N}\varepsilon = (3+\sqrt{10})(3-\sqrt{10}) = 9 - 10 = -1\,.$$

Literatur zur Zahlentheorie

[1] Borevich & Shafarevich: *Zahlentheorie.*
Birkhäuser 1966

[2] Bundschuh: *Einführung in die Zahlentheorie.*
Springer-Verlag 1988

[3] Dickson: *History of the theory of Numbers.*
Chelsea 1971 (Nachdruck von 1920)

[4] Frey: *Elementare Zahlentheorie.*
Vieweg 1984

[5] Gauss: *Untersuchungen über höhere Arithmetik.*
Chelsea 1965 (Disquisitiones Arithmeticae 1801)

[6] Hasse: *Vorlesungen über Zahlentheorie.*
Springer 1950

[7] LeVeque: *Fundamentals of Number theory.*
Addison-Wesley 1977

[8] Niven & Zuckerman: *Einführung in die Zahlentheorie.*
B.I. Wissenschaftsverlag Mannheim/Wien/Zürich 1976

[9] Rosen: *Elementary Number Theory and Applications.*
Wesley 1988

[10] Scheid, H.: *Zahlentheorie.*
B.I. Wissenschaftsverlag Mannheim/Wien/Zürich 1991

[11] Scholz, A. & Schöneberg, B.: *Einführung in die Zahlentheorie.*
Walter de Gruyter 1973

[12] Serre: *Cours d'Arithmetique.*
Hermann 1970

[13] Stark: *An Introduction to Number theory.*
Markham 1970

Index