Der Satz von Hasse-Minkowski

Bachelorarbeit von Charlotte Jergitsch
unter der Aufsicht von Prof. Richard Pink

April 2017

Zusammenfassung

In dieser Arbeit behandeln wir den Beweis des Satzes von Hasse-Minkowski und führen in die dafür benötigten theoretischen Grundlagen ein, insbesondere in die Theorie der p-adischen Zahlen und der quadratischen Formen.

Inhaltsverzeichnis

1 Einleitung **3**

2 Die p-adischen Zahlen **4**
2.1 Konstruktion der p-adischen Zahlen 4
2.2 Die ganzen p-adischen Zahlen 11

3 Das Hilbert-Symbol **15**

4 Quadratische Formen **23**
4.1 Allgemein 23
4.2 Quadratische Formen über $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{Q}_p$ 28

5 Der Satz von Hasse-Minkowski **33**
5.1 Korollare und Erweiterungen 36

1 Einleitung

Der Satz von Hasse-Minkowski behandelt die Frage, wann wir eine rationale Zahl m durch eine quadratische Form $f = \sum_{i,k=1}^{n} a_{i,k} X_i X_k$ mit rationalen Koeffizienten darstellen können. Die Fragestellung klingt harmlos, die Methoden zu deren Lösung sind jedoch komplex. Im Jahr 1921 gelang es Helmut Hasse (1898-1979) in seiner Dissertation [3], die Frage zumindest in der Theorie mit dem Beweis folgenden Satzes zu lösen.

Satz. (Hasse-Minkowski). *Eine quadratische Form f stellt die Null über den rationalen Zahlen $\mathbb{Q}$ genau dann nichttrivial dar, wenn sie die Null über allen p-adischen Körpern $\mathbb{Q}_p$ sowie über den reellen Zahlen $\mathbb{R}$ nichttrivial darstellt.*

Die p-adischen Körper $\mathbb{Q}_p$ waren damals noch eine Neuheit. Zu verdanken sind sie Hasses Lehrer Kurt Hensel (1861-1941). Dieser entwickelte die Theorie der p-adischen Zahlen in seinen Arbeiten zwischen 1899 und 1913 mit der Absicht, ein zahlentheoretisches Werkzeug analog zu den Potenzreihen aus der Funktionentheorie zu schaffen ([7] S.9). Genauer gesagt betrachtete Hensel ganze Zahlen $f \in \mathbb{Z}$ als Funktionen auf dem Raum P der Primzahlen in $\mathbb{Z}$, wobei der Wert von f an $p \in P$ durch

$$f(p) := f \pmod{p}$$

definiert ist. Nun stellt sich die Frage, ob man auf diesen Funktionen f auch höhere Ableitungen sinnvoll definieren kann. Hier erfolgt die Analogie zu den Polynomen $f(Z) \in \mathbb{C}[Z]$ über den komplexen Zahlen bzw. zu den rationalen Funktionen $f(Z) = g(Z)/h(Z) \in \mathbb{C}(Z)$ mit $g, h \in \mathbb{C}[Z]$. Die höheren Ableitungen einer rationalen Funktion an einem Punkt $a \in \mathbb{C}$ mit $h(a) \neq 0$ werden durch die Taylor-Entwicklung

$$f(Z) = \sum_{n=0}^{\infty} a_n (Z-a)^n = a_0 + a_1(Z-a) + a_n(Z-a)^2 + \dots$$

gegeben. Analog dazu kann man eine natürlich Zahl f durch ihre sogenannte p-adische Entwicklung

$$f = a_0 + a_1 p + a_2 p^2 + \dots + a_n p^n$$

darstellen, die man einfach durch Division der Zahl durch Primzahlpotenzen erhält. Zum Beispiel ist die 3-adische Entwicklung der Zahl 46 durch $46 = 1 + 0 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^3$ gegeben. Betrachtet man solche Darstellungen, bei denen die Primzahlpotenzen unbeschränkt groß werden, die Zahl also durch eine Folge von unendlich vielen Koeffizenten definiert ist, so erhält man nach etwas Feinarbeit die p-adischen Zahlen. Die Leserin findet mehr über diese Vorgehensweise in Jürgen Neukirchs *Algebraische Zahlentheorie* [6].

In den ersten zwanzig Jahren nach ihrer Entwicklung bekamen die p-adischen Zahlen nur wenig Aufmerksamkeit geschenkt. Erst durch den Satz von Ostrowski aus dem Jahr 1918 wurde ihre Bedeutung ersichtlich. Der Satz besagt, dass alle möglichen Vervollständigungen von $\mathbb{Q}$ genau durch die reellen Zahlen $\mathbb{R}$ und durch die p-adischen Körper $\mathbb{Q}_p$ gegeben sind (siehe Satz 2.12). Dies änderte die Perspektive auf die rationalen Zahlen grundlegend, welche nun aus topologischer Sicht nicht mehr nur Teilmenge der reellen Zahlen waren, sondern eines Spektrums an topologischen Körpern [8].

Jedoch war nicht nur die Entwicklung der p-adischen Zahlen notwendig, um die Kriterien im Satz von Hasse-Minkowski aufzustellen und zu beweisen, sondern auch maßgebliche Arbeit in der Theorie der quadratischen Formen. Diese wurde von Hermann Minkowski (1864–1909) Ende des 19. Jahrhunderts begründet [5].

In der vorliegenden Arbeit werden wir die theoretischen Grundlagen präsentieren, die für das Verständnis des Satzes von Hasse-Minkowski notwendig sind. Zuerst beschreiben wir die p-adischen Zahlen, dann das Hilbert-Symbol, welches zur Untersuchung quadratischer Formen in drei Variablen dient, und anschließen quadratische Formen im Allgemeinen. Zum krönenden Schluss besprechen wir den Satz von Hasse-Minkowski und dessen Beweis, bei dem die gesamte erarbeitete Theorie zur Anwendung kommt. Dabei haben wir uns dazu entschieden, die p-adischen Zahlen $\mathbb{Q}_p$ als Vervollständigung der rationalen Zahlen $\mathbb{Q}$ einzuführen, da so die Verbindung zwischen den Vervollständigungen von $\mathbb{Q}$ und der Aussage des Satzes von Hasse-Minkowski besser ersichtlich wird. Allerdings gehen wir auch kurz auf die algebraische

Herangehensweise ein, welche die p-adischen ganzen Zahlen als projektiven Limes definiert. Wir setzen vom Leser Grundkenntnisse der Topologie sowie der Algebra, insbesondere über Gruppen, Ringe und Körper, voraus. Indessen führen wir viele elementare Definitionen auf, von denen wir annehmen, dass die Leser sie kennen – einerseits, um deren Erinnerung wachzurufen, andererseits, um Missverständnissen vorzubeugen und die Notation klarzustellen.

Für den Hauptteil der Arbeit haben wir – wo nicht anders angegeben – F. Q. Gouvêas Buch *p-adic Numbers - An Introduction* [2], J.-P. Serres *A Course in Arithmetic* [11] und A. Schmidts *Einführung in die algebraische Zahlentheorie* [9] verwendet. Genauer haben wir uns bei der Konstruktion der p-adischen Zahlen in Kapitel 2 Abschnitt 2.1 dem Titel entsprechend hauptsächlich an F. Q. Gouvêa gehalten, im Abschnitt 2.2 wiederum an A. Schmidt. Im Kapitel 3 über das Hilbert-Symbol und im Kapitel 4 über quadratische Formen sind wir A. Schmidt und J.-P. Serre gleichermaßen gefolgt. Im Beweis des Satzes von Hasse-Minkowski im Kapitel 5 folgten wir hauptsächlich J.-P. Serre.

Ich möchte mich an dieser Stelle bei Prof. Richard Pink und Jennifer-Jayne Jakob für die Betreuung dieser Arbeit und die hilfreichen Verbesserungsvorschläge bedanken.

2 Die p-adischen Zahlen

2.1 Konstruktion der p-adischen Zahlen

Wir erinnern uns erst an die Definitionen des Absolutbetrags und Abstands, um darauf basierend den p-adischen Betrag zu definieren, welcher uns später zu den p-adischen Zahlen führen wird.

Definition 2.1. Ein **Absolutbetrag** (kurz **Betrag**) auf einem Körper $\mathbb{K}$ ist eine Funktion

$$|\ |\colon \mathbb{K} \longrightarrow \mathbb{R}_{\geq 0}$$

mit den Eigenschaften:

1. $|x| = 0 \Leftrightarrow x = 0$ für alle $x \in \mathbb{K}$,
2. $|xy| = |x||y|$ für alle $x, y \in \mathbb{K}$,
3. $|x + y| \leq |x| + |y|$ für alle $x, y \in \mathbb{K}$ (Dreiecksungleichung).

Außerdem bezeichnen wir einen Absolutbetrag als **nichtarchimedisch**, wenn zusätzlich die sogenannte verschärfte Dreiecksungleichung

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

gilt, andernfalls nennen wir ihn **archimedisch**.

Aus 2. folgt insbesondere, dass $|1| = |1||1| = 1$ und $|x^{-1}| = |x^{-1}||x|/|x| = 1/|x|$ ist. Das einfachste Beispiel eines Betrages ist der *triviale Betrag* $|\ |_{tr}$, der sich auf jedem Körper $\mathbb{K}$ definieren lässt, und zwar ist er für $x \in \mathbb{K}$ gegeben als

$$|x|_{tr} = 1 \text{ für } x \neq 0 \text{ und } |0|_{tr} = 0.$$

Definition 2.2. Zu einem Betrag auf $\mathbb{K}$ definieren wir den entsprechenden **Abstand** von zwei Elementen $x, y \in \mathbb{K}$ als

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

Mit dem eben definierten Abstand ist $\mathbb{K}$ ein metrischer Raum, und wir können damit offene Bälle und somit eine Topologie auf dem Körper $\mathbb{K}$ bezüglich des Betrags definieren.

Definition 2.3. Sei $\mathbb{K}$ ein Körper und $|\ |$ ein Betrag auf $\mathbb{K}$. Sei $x \in \mathbb{K}$ und $r \in \mathbb{R}_{>0}$ eine positive reelle Zahl. Dann ist der **offene Ball** mit Radius r und Mittelpunkt x definiert als

$$B(x, r) := \{y \in \mathbb{K} \mid d(x, y) < r\}.$$

Wir können auf $\mathbb{K}$ eine Topologie mit den offenen Bällen als Subbasis definieren, so dass alle offenen Mengen bezüglich dieser Topologie als Vereinigung von beliebig vielen endlichen Schnitten solcher Bälle gebildet werden.

Definition 2.4. Der **Standardbetrag** auf den rationalen Zahlen $\mathbb{Q}$ ist durch

$$|x|_\infty := \begin{cases} x & \text{für } x \geq 0 \\ -x & \text{für } x < 0 \end{cases}$$

definiert. Der Hintergrund der Notation $|\ |_\infty$ wird in den folgenden Seiten noch ersichtlich werden, inzwischen dient sie vor allem zur Unterscheidung von anderen Beträgen.

Definition 2.5. Sei p eine Primzahl in $\mathbb{Z}$. Die **p-adische Bewertung** auf $\mathbb{Q}$ ist die Funktion

$$v_p : \mathbb{Q}^\times \longrightarrow \mathbb{R},$$

wobei $\mathbb{Q}^\times$ die Einheiten in $\mathbb{Q}$ sind, sodass für jede Zahl $r \in \mathbb{Q}^\times$ der Wert $v_p(r)$ als die eindeutige ganze Zahl definiert ist, für die

$$r = p^{v_p(r)} \frac{a}{b} \text{ mit } a, b \in \mathbb{Z},\ ggT(a,b) = 1 \text{ und } p \nmid ab$$

gilt. Wir setzen außerdem $v_p(0) := +\infty$ und erweitern v_p somit auf $\mathbb{Q}$.

Die p-adische Bewertung hat folgende Eigenschaften:

Proposition 2.6. *Für $x, y \in \mathbb{Q}$ gilt $v_p(xy) = v_p(x) + v_p(y)$ und $v_p(x+y) \geq \min(v_p(x), v_p(y))$. Dabei setzen wir für Rechenoperationen mit ∞ die üblichen Regeln voraus, insbesondere $+\infty + (+\infty) = +\infty$.*

Beweis. Ist $xy = 0$, so können wir annehmen, dass $y = 0$ ist, und es gilt

$$v_p(xy) = v_p(0) = +\infty = v_p(x) + v_p(y)$$

und

$$v_p(x+y) = v_p(x) = \min(v_p(x), v_p(y)).$$

Ist $xy \neq 0$, so gilt

$$p^{v_p(xy)} \frac{a_{xy}}{b_{xy}} = xy = p^{v_p(x)} \frac{a_x}{b_x} p^{v_p(y)} \frac{a_y}{b_y} = p^{v_p(x)+v_p(y)} \frac{a_x a_y}{b_x b_y},$$

wobei $p \nmid \frac{a_{xy}}{b_{xy}}$ und $p \nmid \frac{a_x a_y}{b_x b_y}$. Daher ist $v_p(xy) = v_p(x) + v_p(y)$.
Des Weiteren können wir annehmen, dass $\min(v_p(x), v_p(y)) = v_p(x)$ ist. So erhalten wir

$$p^{v_p(x+y)} \frac{a_{x+y}}{b_{x+y}} = x + y = p^{v_p(x)} \frac{a_x}{b_x} + p^{v_p(y)} \frac{a_y}{b_y}$$

$$\Leftrightarrow p^{v_p(x+y)-v_p(x)} \frac{a_{x+y}}{b_{x+y}} = \frac{a_x}{b_x} + p^{v_p(y)-v_p(x)} \frac{a_y}{b_y} = \frac{a_x b_y + p^{v_p(y)-v_p(x)} a_y b_x}{b_x b_y}.$$

Wenn $v_p(y) > v_p(x)$ ist, dann sind auf der rechten Seite weder Zähler noch Nenner durch p teilbar, also muss dasselbe auch für die linke Seite zutreffen. Somit folgt, dass in diesem Fall $v_p(x+y) = v_p(x)$ ist. Ist $v_p(x) = v_p(y)$, so ist es möglich, dass p den Zähler $a_x b_y + a_y b_x$ teilt. In diesem Fall gilt daher, dass $v_p(x+y) \geq v_p(x) = \min(v_p(x), v_p(y))$ ist. □

Definition 2.7. Für $r \in \mathbb{Q}$ definieren wir den **p-adischen Betrag** als

$$|r|_p := \begin{cases} p^{-v_p(r)} & \text{für } r \neq 0 \\ 0 & \text{für } r = 0. \end{cases}$$

Ausgehend von diesem können wir für Zahlen $x, y \in \mathbb{Q}$ den **p-adischen Abstand** festlegen als

$$d_p(x,y) = |x - y|_p.$$

Lemma 2.8. *Der p-adische Betrag ist ein nichtarchimedischer Absolutbetrag. Insbesondere gilt für $x, y \in \mathbb{Q}$, dass $|xy|_p = |x|_p|y|_p$ und $|x+y|_p \leq \max(|x|_p, |y|_p)$ ist.*

Beweis. Für den p-adischen Betrag gilt per Definition, dass $|x|_p = 0 \Leftrightarrow x = 0$ für $x \in \mathbb{Q}$ ist. Für $x, y \in \mathbb{Q}$ mit $x = 0$ gilt $|xy|_p = 0 = |x|_p|y|_p$. Ist $xy \neq 0$, so erhalten wir $|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p$. Aus Definition 2.1 zusammen mit Proposition 2.6 folgt direkt, dass der p-adische Betrag nichtarchimedisch ist. □

Der p-adische Betrag ist auf den ersten Blick sehr unintuitiv. Betrachten wir zum Beispiel die Zahl $\frac{3}{4802} = \frac{3}{2}7^{-4}$. Dann ist der Standardbetrag $|\frac{3}{4802}|_\infty = \frac{3}{4802}$ um vieles kleiner als der 7-adische Betrag $|\frac{3}{4802}|_7 = 7^4 = 2401$. Noch direkter sieht man den Unterschied am Beispiel $|p^n|_\infty = p^n$ und $|p^n|_p = p^{-n}$ für eine Primzahl p.

Definition 2.9. Wir nennen zwei Beträge $|\ |$ und $|\ |'$ auf einem Körper $\mathbb{K}$ **äquivalent**, wenn sie dieselbe Topologie auf $\mathbb{K}$ definieren.

Für den Beweis von Lemma 2.11 über äquivalente Beträge definieren wir noch die Folgenkonvergenz.

Definition 2.10. Sei $|\ |$ ein beliebiger Betrag auf einem Körper $\mathbb{K}$. Man sagt, eine Folge $(x_n)_{n\in\mathbb{N}}$ mit $x_n \in \mathbb{K}$ **konvergiert** gegen den Grenzwert $x \in \mathbb{K}$ bezüglich $|\ |$, wenn für alle $\epsilon > 0$ ein $n_0 \in \mathbb{N}$ existiert, sodass $|x_n - x| < \epsilon$ für alle $n \geq n_0$ ist.

Lemma 2.11. *Seien $|\ |$ und $|\ |'$ zwei Beträge auf einem Körper $\mathbb{K}$. Dann sind folgende Aussagen äquivalent:*

1. *$|\ |$ und $|\ |'$ sind äquivalente Beträge.*
2. *Es gilt $|x| < 1 \Leftrightarrow |x|' < 1$ für alle $x \in \mathbb{K}$.*
3. *Es existiert eine Zahl $\alpha \in \mathbb{R}_{>0}$, sodass $|x|' = |x|^\alpha$ für alle $x \in \mathbb{K}$ gilt.*

Beweis. 1. $\Rightarrow$ 2.: Seien $|\ |$ und $|\ |'$ zwei äquivalente Beträge auf $\mathbb{K}$ und $x \in \mathbb{K}$, sodass $|x| < 1$ ist. Es folgt aus den Definitionen von Konvergenz und Äquivalenz, dass

$$\begin{aligned}
|x| < 1 &\Leftrightarrow \lim_{n\to\infty} |x|^n = 0 \text{ bez. } |\ |_\infty \\
&\Leftrightarrow \forall \epsilon > 0\ \exists n_0 \in \mathbb{N} \text{ sodass } \forall n \geq n_0 \text{ gilt } \left||x|^n - 0\right|_\infty = |x^n| < \epsilon \\
&\Leftrightarrow \forall \epsilon > 0\ \exists n_0 \in \mathbb{N} \text{ sodass } \forall n \geq n_0 \text{ gilt } |x^n - 0| < \epsilon \\
&\Leftrightarrow \lim_{n\to\infty} x^n = 0 \text{ bez. } |\ |.
\end{aligned}$$

Mit derselben Argumentation erhalten wir auch die Äquivalenz $|x|' < 1 \Leftrightarrow \lim_{n\to\infty} x^n = 0$ bez. $|\ |'$. Da $|\ |$ und $|\ |'$ äquivalent sind und somit dieselbe Topologie auf $\mathbb{K}$ induzieren, erhalten wir das Resultat

$$|x| < 1 \Leftrightarrow \lim_{n\to\infty} x^n = 0 \text{ bez. } |\ | \Leftrightarrow \lim_{n\to\infty} x^n = 0 \text{ bez. } |\ |' \Leftrightarrow |x|' < 1.$$

2. $\Rightarrow$ 3.: Nehmen wir an, es existiert kein $x \in \mathbb{K}^\times$ mit der Eigenschaft $|x| < 1$. Dann gibt es auch kein $x \in \mathbb{K}^\times$ mit $|x| > 1$, denn sonst wäre $|x^{-1}| = 1/|x| < 1$. Nach der Annahme in 2. gilt $|x| < 1 \Leftrightarrow |x|' < 1$ und ebenso $|x| > 1 \Leftrightarrow |x|' > 1$. Wenn also kein $x \in \mathbb{K}^\times$ mit der Eigenschaft $|x| < 1$ oder $|x| > 1$ existiert, so müssen beide Beträge gleich dem trivialen Betrag sein, und wir sind fertig. Sonst finden wir ein $x \in \mathbb{K}^\times$ mit $|x| < 1$ und somit nach Annahme $|x|' < 1$. Wir setzen $\alpha := \log(|x|')/\log(|x|)$, sodass $|x|' = |x|^\alpha$ gilt. Nun müssen wir zeigen, dass der Exponent α für alle $y \in \mathbb{K}^\times$ gleich ist.

Sei $y \in \mathbb{K}^\times$, $y \neq x$. Für den Fall $|y|' = |x|' < 1$ erhalten wir nach Annahme und der Argumentation im obigen Absatz

$$|y|' = |x|' \Leftrightarrow |yx^{-1}|' = 1 \Leftrightarrow |yx^{-1}| = 1 \Leftrightarrow |y| = |x|,$$

und somit $|y|^\alpha = |x|^\alpha = |x|' = |y|'$. Für den Fall $|y|' = 1$ erhalten wir ebenso

$$|y|' = 1 \Leftrightarrow |y| = 1,$$

und somit $1 = |y|^\alpha = |y|'$.

Sei nun $|y|' \neq |x|'$ und $|y|' \neq 1$. Sei β die reelle Zahl, sodass $|y|' = |y|^\beta$ gilt. Dann gilt auch für alle ganzen Zahlen n, dass $|y^n|' = |y^n|^\beta$ ist. Folglich können wir annehmen, dass $|y|' < 1$ und somit $|y| < 1$ ist, denn sonst ersetzen wir y einfach durch y^{-1}. Seien nun $n, m \in \mathbb{Z}_{>0}$ beliebig. Es gilt

$$|y^n|' < |x^m|' \Leftrightarrow \left|\frac{y^n}{x^m}\right|' < 1 \Leftrightarrow \left|\frac{y^n}{x^m}\right| < 1 \Leftrightarrow |y^n| < |x^m|.$$

Wenden wir auf die äußeren Ungleichungen den Logarithmus an, so erhalten wir

$$n\log(|y|') < m\log(|x|') \Leftrightarrow n\log(|y|) < m\log(|x|).$$

Außerdem sind $0 < |x|, |x|', |y|, |y|' < 1$. Somit ist deren Logarithmus negativ, und wir erhalten

$$\frac{n}{m} > \frac{\log(|x|')}{\log(|y|')} \Leftrightarrow \frac{n}{m} > \frac{\log(|x|)}{\log(|y|)}, \quad \text{und} \quad \frac{\log(|x|')}{\log(|y|')}, \frac{\log(|x|)}{\log(|y|)} > 0.$$

Da n und m beliebig in $\mathbb{Z}_{>0}$ waren, gilt diese Gleichung für alle positiven rationalen Zahlen $n/m \in \mathbb{Q}_{>0}$. Diese liegen dicht in $\mathbb{R}_{>0}$, daher gilt

$$\frac{\log(|x|')}{\log(|y|')} = \frac{\log(|x|)}{\log(|y|)},$$

und folglich erhalten wir

$$\alpha = \frac{\log(|x|')}{\log(|x|)} = \frac{\log(|y|')}{\log(|y|)} = \beta.$$

Demnach ist $|y|' = |y|^\alpha$ für alle $y \in \mathbb{K}$.
3. $\Rightarrow$ *1.*: Sei nun $|x|' = |x|^\alpha$ für alle $x \in \mathbb{K}$. Es folgt, dass

$$|x - c|' < r \Leftrightarrow |x - c|^\alpha < r \Leftrightarrow |x - c| < r^{1/\alpha}$$

für alle $c \in \mathbb{K}$ gilt. Das heißt, jeder offene Ball bezüglich des einen Betrages ist auch ein offener Ball bezüglich des anderen. Somit definieren beide dieselbe Topologie auf $\mathbb{K}$ und sind äquivalent. □

Nun kommen wir zu dem in der Einleitung schon erwähnten Satz von Ostrowski.

Satz 2.12 (Ostrowski)**.** *Sei* $V = \{p \in \mathbb{N} \mid p \text{ prim}\} \cup \{\infty\}$. *Jeder nichttriviale Betrag auf* $\mathbb{Q}$ *ist äquivalent zu einem der Beträge* $|\ |_v$ *mit* $v \in V$.

Beweis. Wir verweisen den Leser für diesen langen Beweis an [2] S. 46ff. □

Das bedeutet, dass wir nur den Standardbetrag $|\ |_\infty$ und die p-adischen Beträge $|\ |_p$ beachten müssen, wann immer wir nichttriviale Beträge auf $\mathbb{Q}$ untersuchen. Entsprechend wird sich die Relevanz des Satzes von Ostrowski in den folgenden Seiten zeigen, wenn wir die Vervollständigungen von $\mathbb{Q}$ bezüglich der Beträge auf $\mathbb{Q}$ konstruieren. Hierfür benötigen wir noch folgende Definition.

Definition 2.13. Sei $|\ |$ ein beliebiger Betrag auf einem Körper $\mathbb{K}$.

- Eine **Cauchyfolge** bezüglich $|\ |$ in $\mathbb{K}$ ist eine Folge $(x_n)_{n\in\mathbb{N}}$ mit $x_n \in \mathbb{K}$, sodass für alle $\epsilon > 0$ ein $n_0 \in \mathbb{N}$ mit $|x_m - x_n| < \epsilon$ für alle $m, n \geq n_0$ existiert.
- Der Körper $\mathbb{K}$ wird als **vollständig** bezüglich des Betrags $|\ |$ bezeichnet, falls jede Cauchyfolge bezüglich $|\ |$ in $\mathbb{K}$ konvergiert.

Ist $|\ |$ der triviale Betrag auf $\mathbb{Q}$, so sind sowohl die Cauchyfolgen als auch die konvergenten Folgen bezüglich diesem gleich den schließlich stationären Folgen in $\mathbb{Q}$, d.h. die Folgenglieder ändern sich ab einem bestimmten Index nicht mehr. Die rationalen Zahlen sind daher vollständig bezüglich des trivialen Betrages. Aus Definition 2.9 und Lemma 2.11 folgt, dass äquivalente Beträge dieselben Bedingungen für Konvergenz, Cauchyfolgen und Vollständigkeit induzieren. Wenn wir die Vollständigkeit von $\mathbb{Q}$ bezüglich nichttrivialer Beträge erörtern wollen, genügt es somit nach Satz 2.12, nur die Beträge $|\ |_v$ mit $v \in V$ zu betrachten. Allerdings sind nicht alle Cauchyfolgen konvergent in $\mathbb{Q}$ bezüglich $|\ |_v$. Wie man eine solche Folge konstruiert, kann die Leserin in [9] auf S. 157 nachlesen. Demzufolge ist $\mathbb{Q}$ nicht vollständig bezüglich der Beträge $|\ |_v$ mit $v \in V$. Diese Beobachtung führt zu der Frage, ob wir den Körper $\mathbb{Q}$ zu einem vollständigen Körper erweitern können.

Definition 2.14 (Vervollständigung)**.** Sei $\mathbb{K}$ ein Körper und $|\ |$ ein Betrag auf diesem. Dann ist die **Vervollständigung** von $\mathbb{K}$ bezüglich $|\ |$ ein Körper $\mathbb{L}$, sodass gilt:

1. Es gibt eine Einbettung $\mathbb{K} \hookrightarrow \mathbb{L}$.
2. Der Betrag $|\ |$ lässt sich auf $\mathbb{L}$ erweitern, und $\mathbb{L}$ ist vollständig bezüglich dieses Betrages.
3. $\mathbb{K}$ ist dicht in $\mathbb{L}$, d.h. für jedes Element $x \in \mathbb{L}$ existiert eine Folge (x_n) in $\mathbb{K} \subset \mathbb{L}$, sodass (x_n) gegen x konvergiert.

Proposition 2.15. *Existiert eine Vervollständigung $\mathbb{L}$ von $\mathbb{K}$, dann ist $\mathbb{L}$ eindeutig bis auf Isomorphie.*

Beweis. Wir skizzieren hier nur den Beweis. Der Leser kann die Details in [2] auf S. 59, 250f nachverfolgen. Wenn eine weitere Vervollständigung $\mathbb{E}$ von $\mathbb{K}$ existiert, so gibt es nach der Definition einer Vervollständigung eine Einbettung $f\colon \mathbb{K} \hookrightarrow \mathbb{E}$, welche den Betrag der Elemente in $\mathbb{K}$ erhält. Somit ist f stetig, und da der Körper $\mathbb{K}$ dicht in $\mathbb{L}$ liegt, lässt sich f als stetige Funktion zu einer stetigen Abbildung $\tilde{f}\colon \mathbb{L} \longrightarrow \mathbb{E}$ erweitern. Es ist noch zu zeigen, dass $\tilde{f}$ ein Körperhomomorphismus und somit injektiv ist. Auf dieselbe Weise erhalten wir aus der Einbettung $g\colon \mathbb{K} \hookrightarrow \mathbb{L}$ einen Körperhomomorphismus $\tilde{g}\colon \mathbb{E} \longrightarrow \mathbb{L}$. Die Komposition $\tilde{g} \circ \tilde{f}$ bzw. $\tilde{f} \circ \tilde{g}$ erhält den Betrag, ist also stetig, und ist beschränkt auf $\mathbb{Q}$ gleich der Identität. Da $\mathbb{Q}$ dicht in $\mathbb{L}$ und $\mathbb{K}$ liegt, sind $\tilde{g} \circ \tilde{f}$ bzw. $\tilde{f} \circ \tilde{g}$ auch gleich der Identität auf $\mathbb{L}$ bzw. $\mathbb{E}$, und $\mathbb{L}$ und $\mathbb{E}$ sind isomorph. □

Wir definieren nun Konstruktionen, mit denen wir eine Vervollständigung von $\mathbb{Q}$ bezüglich der Beträge $|\ |_v$ mit $v \in V$ erzeugen können.

Definition 2.16. Sei $\mathcal{C}_v = \{(x_n) \mid (x_n)$ ist eine Cauchyfolge bzgl. $|\ |_v\}$, der Ring aller Cauchyfolgen in $\mathbb{Q}$ bezüglich des Betrags $|\ |_v$ für ein $v \in V$ mit komponentenweiser Addition und Multiplikation. Des Weiteren sei $\mathcal{N}_v = \{(x_n) \mid lim_{x\to\infty}|x_n|_v = 0\} \subset \mathcal{C}_v$ das maximale Ideal der Cauchyfolgen, die bezüglich $|\ |_v$ gegen Null konvergieren.

Einen Beweis dafür, dass $\mathcal{C}_v$ ein Ring und $\mathcal{N}_v$ tatsächlich ein maximales Ideal ist, bildet eine Übung in Analysis, welche der Leser in [2] auf S. 53f und S. 249 nachprüfen kann.

Satz 2.17. *Die Vervollständigung von $\mathbb{Q}$ bezüglich des Betrags $|\ |_v$ ist durch den Quotienten*

$$\mathbb{Q}_v := \mathcal{C}_v / \mathcal{N}_v$$

*gegeben. Im Falle $v = \infty$ ist die Vervollständigung $\mathbb{Q}_\infty$ isomorph zu den reellen Zahlen $\mathbb{R}$. Für $v = p$ mit p prim nennen wir $\mathbb{Q}_p$ den **Körper der p-adischen Zahlen**.*

Wir werden den Satz in mehreren Schritten in Form von Lemmas beweisen. Da $\mathcal{N}_v$ ein maximales Ideal ist, sehen wir, dass $\mathbb{Q}_v$ tatsächlich ein Körper ist. Ferner müssen wir die Eigenschaften, die $\mathbb{Q}_v$ nach Definition 2.14 haben muss, verifizieren. Für $\mathbb{Q}_\infty = \mathbb{R}$ erachten wir die Aussage als bewiesen, da $\mathbb{R}$ als die Vervollständigung von $\mathbb{Q}$ bezüglich $|\ |_\infty$ definiert ist und entsprechende Eigenschaften in den meisten Analysisvorlesungen gezeigt werden. Daher fokussieren wir im Folgenden auf die Körper $\mathbb{Q}_p$ mit p prim.

Lemma 2.18. *Es gibt eine Einbettung $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.*

Beweis. Für eine Primzahl p betrachten wir die Abbildung

$$\begin{aligned} \psi\colon \mathbb{Q} &\longrightarrow \mathbb{Q}_p \\ x &\mapsto [(x)], \end{aligned}$$

bei der $x \in \mathbb{Q}$ auf die Äquivalenzklasse der konstanten Folge (x) in $\mathbb{Q}_p$ abgebildet wird. Diese Abbildung ist injektiv: Werden zwei verschiedene Elemente $x \neq y \in \mathbb{Q}$ auf dieselbe Äquivalenzklasse $[(x)] = [(y)] \in \mathbb{Q}_p$ abgebildet, so unterscheiden sich die konstanten Folgen (x) und (y) nur durch die Folge $(z) := (x-y)$, welche bezüglich des Betrags $|\ |_p$ gegen Null konvergiert. Das bedeutet nach Definition 2.10, dass wir für alle $\epsilon > 0$ die Ungleichung $|z-0|_p < \epsilon$ erhalten. Folglich ist $|z|_p = 0$ und somit $z = x - y = 0$. Die Abbildung ψ ist also injektiv. □

Das folgende Lemma ermöglicht uns, den p-adischen Betrag auf den Körper $\mathbb{Q}_p$ zu erweitern.

Lemma 2.19. *Sei für eine Primzahl p eine Cauchyfolge $(x_n) \in \mathcal{C}_p \backslash \mathcal{N}_p$ gegeben. Dann ist die Folge reeller Zahlen $(|x_n|_p)$ schließlich stationär, d.h. es existiert ein Index $n_0 \in \mathbb{N}$, sodass $|x_m|_p = |x_n|_p$ für alle $m, n \geq n_0$ ist.*

Sind außerdem $(x_n), (y_n) \in \mathcal{C}_p \backslash \mathcal{N}_p$ Cauchyfolgen, deren Klassen $[(x_n)]$ und $[(y_n)]$ in $\mathbb{Q}_p$ gleich sind, dann nehmen die Folgen $(|x_n|_p)$ und $(|y_n|_p)$ schließlich denselben stationären Wert an, d.h. es existiert $n_0 \in \mathbb{N}$, sodass $|x_n|_p = |y_n|_p$ für alle $n \geq n_0$ ist.

Beweis. Sei (x_n) eine Cauchyfolge bezüglich $|\ |_p$ für eine Primzahl p, welche nicht gegen Null konvergiert. Folglich existieren eine reelle Zahl c und ein Index $n_1 \in \mathbb{N}$, sodass

$$|x_n|_p \geq c > 0 \text{ für alle } n \geq n_1$$

gilt. Ebenso können wir aufgrund der Cauchyeigenschaft ein $n_2 \in \mathbb{N}$ finden, sodass wir

$$|x_n - x_m|_p < c \text{ für alle } n, m \geq n_2$$

erhalten. Wir setzen nun $n_0 = \max(n_1, n_2)$ und bekommen so für $n, m \geq n_0$ die Ungleichung

$$|x_n - x_m|_p < c \leq \max(|x_n|_p, |x_m|_p).$$

Wir können annehmen, dass $|x_m|_p \geq |x_n|_p$ ist und daher $|x_n - x_m|_p < |x_m|_p$. Außerdem gilt, dass

$$|x_m|_p = |x_n + (x_m - x_n)|_p \leq \max(|x_n|_p, |x_m - x_n|_p) = |x_n|_p,$$

da auf jeden Fall $|x_m - x_n|_p < |x_m|_p$ gelten muss. Somit haben wir die erwünschte Gleichheit $|x_m|_p = |x_n|_p$.

Seien nun (x_n), $(y_n) \in \mathcal{C}_p \backslash \mathcal{N}_p$ Cauchyfolgen, deren Klassen $[|x_n|_p]$ und $[|y_n|_p]$ in $\mathbb{Q}_p$ gleich sind. Das bedeutet, dass wir (x_n) als $(y_n) + (z_n)$ schreiben können, wobei $(z_n) \in \mathcal{N}_p$ eine Nullfolge ist. Nach dem ersten Teil des Lemmas nehmen die Folgenglieder von $(|x_n|_p)$ und $(|y_n|_p)$ für ein ausreichend großes $n \in \mathbb{N}$ jeweils stationäre Werte $\tilde{x}$ und $\tilde{y}$ an. Somit gilt für den Limes

$$\tilde{x} = \lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |y_n + z_n|_p \leq \lim_{n\to\infty} (|y_n|_p + |z_n|_p) = \tilde{y} + \lim_{n\to\infty} |z_n|_p = \tilde{y},$$

und demnach ist $\tilde{x} \leq \tilde{y}$. Ebenso können wir (y_n) als $(x_n) + (\hat{z}_n)$ schreiben, wobei $\hat{z}_n = -z_n$ ist, und nach derselben Argumentation $\tilde{y} \leq \tilde{x}$ erhalten. Folglich ist $\tilde{x} = \tilde{y}$, und die beiden Folgen (x_n) und (y_n) nehmen denselben stationären Wert an. □

Definition 2.20. Sei $x \in \mathbb{Q}_p$ für eine Primzahl p, und sei $(x_n) \in \mathcal{C}_p$ ein Repräsentant von x. Dann definieren wir den p-adischen Betrag auf $\mathbb{Q}_p$ als

$$|x|_p := \lim_{n\to\infty} |x_n|_p.$$

Laut Lemma 2.19 existiert dieser Limes, da die Folge $(|x_n|_p)_{n\in\mathbb{N}}$ schließlich stationär ist, und ist wohldefiniert, da für zwei verschiedene Repräsentanten (x_n) und (y_n) von x die Gleichheit des Limes $\lim_{n\to\infty}|x_n|_p = \lim_{n\to\infty}|y_n|_p$ gilt.

Lemma 2.21. *Die Menge der rationalen Zahlen $\mathbb{Q}$ liegt als Bild der Einbettung $\mathbb{Q}\hookrightarrow\mathbb{Q}_p$ dicht in $\mathbb{Q}_p$.*

Beweis. Es genügt zu zeigen, dass jeder offene Ball um ein Element $x\in\mathbb{Q}_p$ die Äquivalenzklasse einer konstante Folge, also ein Element des Bildes von $\mathbb{Q}$, enthält. Sei $B(x,\epsilon)$ der offene Ball um x mit Radius $\epsilon\in\mathbb{R}_{>0}$, und sei (x_n) eine Cauchyfolge, die x repräsentiert. Sei außerdem $\tilde{\epsilon}\in\mathbb{R}_{>0}$ mit $0<\tilde{\epsilon}<\epsilon$; dann existiert ein $n_0\in\mathbb{N}$, sodass

$$|x_n - x_m|_p < \tilde{\epsilon}$$

für alle $n,m\geq n_0$. Sei $y = x_{n_0}$ und $[(y)]$ die Klasse der entsprechenden konstante Folge in $\mathbb{Q}_p$. Wir zeigen, dass diese im Ball $B(x,\epsilon)$ liegt. Das Element $x-[(y)]\in\mathbb{Q}_p$ wird durch die Folge $(x_n-y)\in\mathcal{C}_p$ dargestellt, und wir erhalten für $n\geq n_0$, dass

$$|(x_n-y)|_p = \lim_{n\to\infty}|x_n-y|_p = \lim_{n\to\infty}|x_n-x_{n_0}|_p \leq \tilde{\epsilon} < \epsilon.$$

Somit liegt die Klasse $[(y)]$ der konstanten Folge (y) im Ball $B(x,\epsilon)$, und wir sind fertig. □

Jetzt müssen wir nur noch überprüfen, dass der Körper der p-adischen Zahlen $\mathbb{Q}_p$ selbst vollständig bezüglich $|\ |_p$ ist.

Lemma 2.22. *Der Körper der p-adischen Zahlen $\mathbb{Q}_p$ ist vollständig bezüglich des p-adischen Betrags $|\ |_p$.*

Beweis. Sei $x=(x_i)_{i\in\mathbb{N}}$ eine Cauchyfolge in $\mathbb{Q}_p$. Dann liegen die Folgenglieder x_i selbst in $\mathbb{Q}_p$ und werden jeweils durch die Cauchyfolge $(x_{i,n})_{n\in\mathbb{N}}$ mit Elementen in $\mathbb{Q}$ repräsentiert. Wir müssen zeigen, dass ein Element $y=[(y_n)_{n\in\mathbb{N}}]\in\mathbb{Q}_p$ existiert, sodass x gegen y konvergiert – das heißt, dass es für alle $\epsilon>0$ einen Index i_0 gibt mit $|x_i-y|_p = \lim_{n\to\infty}|x_{i,n}-y_n|_p<\epsilon$ für alle $i\geq i_0$. Da $\mathbb{Q}$ dicht in $\mathbb{Q}_p$ liegt, finden wir für jeden Index $i\in\mathbb{N}$ und für alle $\epsilon>0$ eine rationale Zahl $y_i\in\mathbb{Q}$, sodass für die Klasse $[(y_i)]$ der konstanten Folge (y_i) der Abstand $|x_i-[(y_i)]|_p<\epsilon$ ist, also $\lim_{n\to\infty}|x_{i,n}-y_i|_p<\epsilon$. Somit erhalten wir für ein beliebiges $\epsilon>0$ eine Folge $(y_i)_{i\in\mathbb{N}}$ von rationalen Zahlen y_i. Diese ist eine Cauchyfolge: Sei $(y_{i,n})_{n\in\mathbb{N}}$ die konstante Folge mit $y_{i,n}=y_i$ für alle n. Dann ist für ausreichend große $i,j\in\mathbb{N}$

$$\begin{aligned}
|y_i-y_j|_p &= \lim_{n\to\infty}|y_{i,n}-y_{j,n}|_p \\
&= \lim_{n\to\infty}|(x_{j,n}-y_{j,n})-(x_{i,n}-y_{i,n})+(x_{i,n}-x_{j,n})|_p \\
&\leq \lim_{n\to\infty}|x_{j,n}-y_{j,n}|_p + \lim_{n\to\infty}|x_{i,n}-y_{i,n}|_p + \lim_{n\to\infty}|x_{i,n}-x_{j,n}|_p \\
&< 3\epsilon,
\end{aligned}$$

wobei die letzte Ungleichung aus der Definition der y_i und aus der Cauchyeigenschaft der Folge $x=(x_i)_{i\in\mathbb{N}}$ folgt. Wir haben also eine Cauchyfolge $(y_i)_{i\in\mathbb{N}}$, welche ein Element $y:=[(y_i)_{i\in\mathbb{N}}]$ in $\mathbb{Q}_p$ darstellt, und zeigen nun, dass die Folge x gegen y konvergiert. Sei $\epsilon>0$ gegeben. Wir zeigen, dass es ein $i_0\in\mathbb{N}$ gibt, sodass $|x_i-y|_p<2\epsilon$ ist. Es gilt

$$\begin{aligned}
|x_i-y|_p &= \lim_{n\to\infty}|x_{i,n}-y_n|_p \\
&= \lim_{n\to\infty}|(x_{i,n}-y_i)+(y_i-y_n)|_p \\
&\leq \lim_{n\to\infty}|x_{i,n}-y_i|_p + \lim_{n\to\infty}|y_i-y_n|_p.
\end{aligned}$$

Aufgrund der Definition von y_i erhalten wir $\lim_{n\to\infty}|x_{i,n}-y_i|_p<\epsilon$. Außerdem ist $(y_i)_{i\in\mathbb{N}}$ eine Cauchyfolge. Demnach gilt für ein ausreichend großes $i_0\in\mathbb{N}$ und $i,n\geq i_0$, dass $|y_i-y_n|_p<\epsilon$ ist, und somit ist für $i\geq i_0$ auch $\lim_{n\to\infty}|y_i-y_n|_p<\epsilon$. Folglich erhalten wir für $i\geq i_0$, dass $|x_i-y|_p<2\epsilon$ ist. Die Cauchyfolge $x=(x_i)_{i\in\mathbb{N}}$ konvergiert somit gegen $y\in\mathbb{Q}_p$. □

Folglich ist $\mathbb{Q}_v$ die Vervollständigung von $\mathbb{Q}$ bezüglich $|\ |_v$ für alle $v\in V$. Nach dem Satz von Ostrowski (2.12) beschreiben die Körper $\mathbb{Q}_v$ bis auf Isomorphie alle nichttrivialen Vervollständigungen von $\mathbb{Q}$.

2.2 Die ganzen p-adischen Zahlen

Im folgenden Abschnitt bezeichnet p wie gehabt immer eine Primzahl. Des Weiteren bezeichnen wir mit $\bar{a} \in \mathbb{Z}/p^n\mathbb{Z}$ die Restklasse des Elements $a \in \mathbb{Z}$ in $\mathbb{Z}/p^n\mathbb{Z}$ mit $n \in \mathbb{N}$.

Definition 2.23. Der **Ring der ganzen p-adischen Zahlen** ist definiert als

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\} = \{x \in \mathbb{Q}_p \mid v_p \geq 0\}.$$

Der p-adische Betrag ist nichtarchimedisch, daher impliziert $|x|_p \leq 1$ und $|y|_p \leq 1$, dass $|x+y|_p \leq 1$ und $|x|_p|y|_p \leq 1$ ist, wodurch wir eine Ringstruktur auf $\mathbb{Z}_p$ erhalten.

Durch die Einbettungen $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{Q}_p$ und aufgrund der Tatsache, dass $v_p(x) \geq 0$ für alle $x \in \mathbb{Z}$ ist, sehen wir, dass $\mathbb{Z}$ in $\mathbb{Z}_p$ enthalten ist.

Lemma 2.24. *Die ganzen Zahlen $\mathbb{Z}$ liegen dicht in $\mathbb{Z}_p$.*

Beweis. Wir zeigen, dass wir jedes Element $a \in \mathbb{Z}_p$ beliebig genau durch ganze Zahlen annähern können, indem wir für jedes $i \in \mathbb{N}$ eine konstante Folge (y_i) mit $y_i \in \mathbb{Z}$ finden, sodass $|a - [(y_i)]|_p \leq p^{-i}$ gilt. Sei $a \in \mathbb{Z}_p$ repräsentiert durch die Folge $(a_n)_{n\in\mathbb{N}}$, und sei $i \in \mathbb{N}$ fixiert. Wir wissen, dass $v_p(a) \geq 0$ und $(a_n)_{n\in\mathbb{N}}$ eine Cauchyfolge ist, und können demnach durch Weglassen endlich vieler Anfangsglieder der Folge annehmen, dass

$$v_p(a_n) \geq 0 \text{ und } v_p(a_n - a_m) \geq i \text{ für alle } n, m \in \mathbb{N}$$

gilt. Wir schreiben jedes Folgenglied als $a_n = c_n/d_n$ mit $c_n \in \mathbb{Z}$ und $d_n \in \mathbb{N}$ mit $p \nmid d_n$. Wir definieren $y_i \in \mathbb{Z}$ als ganze Zahl, sodass $d_1 y_i \equiv c_1 \bmod p^i$ ist. Dies ist wohldefiniert, da $\bar{d}_1$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ liegt. Wir zeigen nun, dass $|a_n - y_i|_p \leq p^{-i}$ ist. Sei $n \in \mathbb{N}$ beliebig. Dann gilt aufgrund der Annahme $v_p(a_n - a_m) \geq i$ für alle $n, m \in \mathbb{N}$, dass

$$a_n - a_1 = \frac{c_n}{d_n} - \frac{c_1}{d_1} = p^i \frac{c}{d} \text{ für ein } c \in \mathbb{Z},\ d \in \mathbb{N} \text{ und } p \nmid d$$

ist. Wir multiplizieren mit den Nennern und erhalten $d(c_n d_1 - c_1 d_n) = p^i c d_1 d_n$. Da $p \nmid d$ gilt, erhalten wir $p^i \mid (c_n d_1 - c_1 d_n)$. Aufgrund der Definition von y_i gilt ebenso $p^i \mid (c_n d_1 - d_1 y_i d_n)$. Die Primzahl p teilt d_1 ebenfalls nicht, daher erhalten wir $p^i \mid (c_n - y_i d_n)$. Somit existiert ein $b \in \mathbb{Z}$, sodass $p^i b = (c_n - y_i d_n)$ und $p^i b/d_n = (c_n/d_n - y_i) = a_n - y_i$. Daher ist $|a_n - y_i|_p \leq p^{-i}$, und da $n \in \mathbb{N}$ beliebig gewählt war, gilt das für alle n. Somit ist für die konstante Folge (y_i) der Abstand $|a - [(y_i)]|_p = \lim_{n\to\infty} |a_n - y_i|_p \leq p^{-i}$ für beliebig große $i \in \mathbb{N}$. Wir können folglich das Element $a \in \mathbb{Z}_p$ beliebig genau durch ganze Zahlen $y_i \in \mathbb{Z}$ approximieren. □

Lemma 2.25. *Die Inklusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ induziert einen natürlichen Isomorphismus*

$$\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_p/p^n\mathbb{Z}_p.$$

Beweis. Ein Element $a \in \mathbb{Z}_p$ liegt genau dann in $p^n\mathbb{Z}_p$, wenn $v_p(a) \geq n$ ist. Daher wird eine ganze Zahl a dann auf die Null in $\mathbb{Z}_p/p^n\mathbb{Z}_p$ abgebildet, wenn sie in $p^n\mathbb{Z}$ liegt. Die obige Abbildung ist also injektiv. Sei nun $\bar{a} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$, und sei a ein Repräsentant von $\bar{a}$ in $\mathbb{Z}_p$. Da die ganzen Zahlen $\mathbb{Z}$ nach Lemma 2.24 dicht in $\mathbb{Z}_p$ liegen, können wir ein $a_n \in \mathbb{Z}$ mit konstanter Folge (a_n) finden, sodass $|a - [(a_n)]|_p \leq p^{-n}$ ist, beziehungsweise gilt $v_p(a - [(a_n)]) \geq n$. Somit ist $[(a_n)]$ ebenfalls ein Repräsentant des Elements $\bar{a}$ in $\mathbb{Z}_p/p^n\mathbb{Z}_p$, und a_n ist ein Urbild dessen in $\mathbb{Z}/p^n\mathbb{Z}$. □

Durch dieses Lemma ergibt es Sinn, p-adische ganze Zahlen modulo einer Primzahlpotenz als Elemente von $\mathbb{Z}/p^n\mathbb{Z}$ zu betrachten.

Exkurs: Die p-adischen ganzen Zahlen als projektiver Limes
Sei $\mathbb{Z}/p^n\mathbb{Z}$ der Ring ganzer Zahlen modulo p^n für $n \in \mathbb{N}$. Wir erhalten Homomorphismen

$$\begin{aligned} \phi_n \colon \mathbb{Z}/p^n\mathbb{Z} &\longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z} \\ a \pmod{p^n} &\mapsto a \pmod{p^{n-1}}, \end{aligned}$$

und dadurch ein System

$$\cdots \to \mathbb{Z}/p^{n-1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} \to \cdots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

Der *projektive Limes* $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ ist definiert als der Ring, dessen Elemente Folgen $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ sind, welche die *Kompatibilitätsbedingung* erfüllen – das bedeutet

$$a_{n+1} \equiv a_n \pmod{p^n} \quad \text{für alle } n \in \mathbb{N}.$$

Mit der Addition $(a_n) + (b_n) = (a_n + b_n)$ und der Multiplikation $(a_n) \cdot (b_n) = (a_n \cdot b_n)$ hat der projektive Limes eine Ringstruktur. Durch Lemma 2.25 ergibt es Sinn, Elemente $a \in \mathbb{Z}_p$ modulo einer Primzahlpotenz zu betrachten, und wir können jedem Element $a \in \mathbb{Z}_p$ eine Folge $(a_n)_{n\in\mathbb{N}}$ zuordnen, sodass $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ die Restklassen von a modulo p^n sind. Diese erfüllen die Kompatibilitätsbedingung, da

$$a_{n+1} \pmod{p^n} = (a \pmod{p^{n+1}}) \pmod{p^n} = a \pmod{p^n} = a_n$$

gilt. Die Folge $(a_n)_{n\in\mathbb{N}}$ ist somit in $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ enthalten. Die Restklassenfolgen der Elemente $a \in \mathbb{Z}_p$ entsprechen sogar genau den Elementen in $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, wie folgender Satz zeigt.

Satz 2.26. *In der oben beschriebenen Weise können wir jeder p-adischen ganzen Zahl $a \in \mathbb{Z}_p$ die Folge ihrer Restklassen modulo p^n im projektiven Limes $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ zuordnen und erhalten somit einen Isomorphismus*

$$\Phi \colon \mathbb{Z}_p \xrightarrow{\sim} \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

Beweis. Es gilt $\Phi(a+b) = (a_n + b_n)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = \Phi(a) + \Phi(b)$ und $\Phi(a \cdot b) = (a_n \cdot b_n)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = \Phi(a) \cdot \Phi(b)$ für alle $a, b \in \mathbb{Z}_p$. Die Abbildung ist somit ein Homomorphismus. Ist $\Phi(a) = \Phi(b)$ für $a, b \in \mathbb{Z}_p$, so gilt für alle $n \in \mathbb{N}$, dass

$$\begin{aligned} & a \pmod{p^n} = b \pmod{p^n} \\ \Leftrightarrow\ & a - b \equiv 0 \pmod{p^n} \\ \Leftrightarrow\ & |a - b|_p \leq p^{-n}. \end{aligned}$$

Daher ist $a - b = 0$ in $\mathbb{Z}_p$, und Φ ist injektiv. Sei nun $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in \mathbb{Z}/p^n\mathbb{Z}$. Wir wählen einen Repräsentanten $A_n \in \mathbb{Z}$ für jedes a_n. Sei $\epsilon > 0$ gegeben, und $n_0 \in \mathbb{N}$, sodass $p^{-n_0} < \epsilon$ ist. Aufgrund der Kompatibilitätsbedingung gilt für alle $n, m \geq n_0 \in \mathbb{N}$, dass $A_n \equiv A_m$ modulo p^{n_0} ist. Somit erhalten wir $|A_n - A_m|_p \leq p^{-n_0} < \epsilon$. Die Folge $(A_n)_{n\in\mathbb{N}}$ ist demnach eine p-adische Cauchyfolge und stellt ein Element $a \in \mathbb{Z}_p$ dar. Die Restklassen von a modulo p^n stimmen mit den a_n überein, somit ist $\Phi(a) = (a_n)_{n\in\mathbb{N}}$, und die Surjektivität von Φ ist bewiesen. □

Die Konstruktion über den projektiven Limes ist somit ein alternativer Weg, um die p-adischen ganzen Zahlen aufzubauen. Den Körper der p-adischen Zahlen $\mathbb{Q}_p$ erhält man aus $\mathbb{Z}_p$ als Erweiterung $\mathbb{Z}_p[p^{-1}]$ oder als Quotientenkörper des Integritätsbereichs $\mathbb{Z}_p$, wie aus Lemma 2.29 unten hervorgeht.

Wir ergründen nun weitere Eigenschaften der p-adischen Zahlen $\mathbb{Q}_p$ in Bezug auf die p-adischen ganzen Zahlen $\mathbb{Z}_p$, insbesondere deren Einheiten und Quadrate.

Lemma 2.27. *Ein Element $u \in \mathbb{Q}_p$ ist genau dann eine Einheit in $\mathbb{Z}_p$, wenn $v_p(u) = 0$ bzw. $|u|_p = 1$ gilt.*

Beweis. Sei $u \in \mathbb{Q}_p$ mit $|u|_p = 1$. Dann gilt $|u^{-1}|_p = 1/|u|_p = 1$, und sowohl u als u^{-1} liegen in Z_p. Folglich ist u ist eine Einheit in $\mathbb{Z}_p$. Sei umgekehrt $u \in \mathbb{Q}_p$ eine Einheit in $\mathbb{Z}_p$. Dann gibt es ein $v \in \mathbb{Z}_p^\times$, sodass $uv = 1$ und $|u|_p|v|_p = 1$ ist. Da u und v in $\mathbb{Z}_p$ liegen, gilt $|u|_p, |v|_p \leq 1$ und folglich $|u|_p = 1$. □

Korollar 2.28. *Ein Element $u \in \mathbb{Z}_p$ ist genau dann eine Einheit in $\mathbb{Z}_p$, wenn seine Restklasse $\bar{u} \in \mathbb{Z}/p\mathbb{Z}$ ungleich 0 ist.*

Beweis. Es gilt für $u \in \mathbb{Z}_p$, dass $u \in \mathbb{Z}_p^\times \Leftrightarrow v_p(u) = 0 \Leftrightarrow \bar{u} \in (Z_p/pZ_p)^\times \Leftrightarrow \bar{u} \neq 0$ ist. □

Lemma 2.29. *Wir können jedes Element $x \in \mathbb{Q}_p^\times$ eindeutig als*

$$x = p^n u$$

mit $u \in \mathbb{Z}_p^\times$ und $n \in \mathbb{Z}$ schreiben.

Beweis. Sei $x \in \mathbb{Q}_p$ und $v_p(x) = n$ für ein $n \in \mathbb{Z}$. Dann ist $v_p(p^{-n}x) = 0$, sodass nach Lemma 2.27 $p^{-n}x \in \mathbb{Z}_p^\times$ gilt, und $x = p^n u$ für $u := p^{-n}x$ ist. Sei umgekehrt $x = p^n u$ für ein $n \in \mathbb{Z}$ und $u \in \mathbb{Z}_p^\times$, so ist $n = v_p(x)$ und $u = p^{-n}x$. Die Darstellung ist somit eindeutig. □

Durch die Darstellung $x = p^n u$ der Elemente in $\mathbb{Q}_p$ reduzieren sich Fragen zu deren Eigenschaften auf die Untersuchung der Primzahlpotenzen p^n und der p-adischen Einheiten u. Wir werden diese Darstellung nun ausnutzen, um die Quadrate in $\mathbb{Q}_p$ in Satz 2.36 zu bestimmen. Dafür führen wir zuerst das Legendre-Symbol ein und untersuchen seine Eigenschaften.

Definition 2.30 (Quadratischer Rest)**.** Eine ganze Zahl $a \in \mathbb{Z}$ heißt **quadratischer Rest** modulo p, wenn $p \nmid a$ und das Bild von a in $(\mathbb{Z}/p\mathbb{Z})^\times$ ein Quadrat in $(\mathbb{Z}/p\mathbb{Z})^\times$ ist. Wenn $p \nmid a$ gilt, jedoch a kein quadratischer Rest ist, so nennt man a **quadratischer Nichtrest**.

Es sei hier angemerkt, dass es keinen quadratischen Nichtrest modulo 2 gibt, da $(\mathbb{Z}/2\mathbb{Z})^\times$ nur das Element $\bar{1}$ enthält, welches ein Quadrat ist. Basierend auf obiger Definition können wir das Legendre-Symbol für ganze Zahlen einführen.

Definition 2.31. Das **Legendre-Symbol** $\left(\frac{a}{p}\right)$ für Zahlen $a \in \mathbb{Z}$ ist folgendermaßen definiert:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{falls } a \text{ quadratischer Rest modulo } p, \\ 0 & \text{falls } p|a, \\ -1 & \text{falls } a \text{ quadratischer Nichtrest modulo } p \text{ ist.} \end{cases}$$

Wir können das Legendre-Symbol auf $u \in \mathbb{Z}_p$ erweitern, indem wir durch Satz 2.25 den Ausdruck $\left(\frac{u}{p}\right)$ als das Legendre-Symbol der Restklasse von u modulo p in $\mathbb{Z}/p\mathbb{Z}$ betrachten. Eine wichtige Eigenschaft des Legendre-Symbols ist dessen Multiplikativität, die wir im Lemma 2.34 zeigen werden. Der Beweis des Lemmas verwendet *primitive Wurzeln*, welche wir hier kurz einführen wollen.

Definition 2.32. Ein Element a der Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ mit Ordnung $\mathrm{ord}(a) = p - 1$ heißt **primitive Wurzel modulo** p. Wir nennen eine Zahl $g \in \mathbb{Z}$ primitive Wurzel modulo p, wenn ihre Restklasse $\bar{g} \in (\mathbb{Z}/p\mathbb{Z})^\times$ eine primitive Wurzel ist.

Eine primitive Wurzel erzeugt aufgrund ihrer Ordnung die Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ durch Multiplikation, da $(\mathbb{Z}/p\mathbb{Z})^\times$ genau $p - 1$ Elemente enthält. Die Existenz primitiver Wurzeln wird in einer einführenden Algebravorlesung gezeigt und kann sonst in [9] auf S.18 nachgelesen werden – wir setzen sie hier demnach voraus. Mit folgender Eigenschaft primitiver Wurzeln ist die Multiplikativität des Legendre-Symbols in Lemma 2.34 fast schon bewiesen.

Lemma 2.33. *Sei q eine Primzahl ungleich 2. Für $g \in \mathbb{Z}$ eine primitive Wurzel modulo q und $k \in \mathbb{N}$ gilt*

$$\left(\frac{g^k}{q}\right) = (-1)^k.$$

Das heißt, die Potenz g^k einer primitven Wurzel ist genau dann ein quadratischer Rest, wenn k gerade ist.

Beweis. Ist k gerade, gilt $\bar{g}^k = (\bar{g}^{k/2})^2$, und $\bar{g}^k$ ist somit ein quadratischer Rest. Sei umgekehrt $\bar{g}^k = \bar{h}^2$ in $(\mathbb{Z}/q\mathbb{Z})^\times$. Da $\bar{g}$ eine primitive Wurzel ist, gilt außerdem, dass $\bar{h} = \bar{g}^n$ für ein $n \in \mathbb{N}$ ist. Daraus erhalten wir $\bar{g}^k = \bar{g}^{2n}$ und $\bar{g}^{k-2n} = \bar{1}$. Das bedeutet, dass die Ordnung $\mathrm{ord}(\bar{g})$ des Elements $\bar{g}$ die Potenz $k - 2n$ teilt. Allerdings ist die Ordnung $\mathrm{ord}(\bar{g}) = q - 1$, also gerade, und somit ist auch k gerade. □

Lemma 2.34. *Es gilt*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

für p prim und $a, b \in \mathbb{Z}_p$.

Beweis. Es gilt $p|ab$ genau dann, wenn $p|a$ oder $p|b$ erfüllt ist. Also ist die linke Seite genau dann gleich Null, wenn es die rechte Seite ist. Die beweist sogleich die Aussage für $p = 2$, da das Legendre-Symbol in diesem Fall nicht den Wert -1 annehmen kann.
Es gelte nun $p \neq 2$ und $p \nmid ab$. Sei g eine primitive Wurzel modulo p, so dass die Klasse $\bar{g}$ von g in $(\mathbb{Z}/p\mathbb{Z})^\times$ alle anderen Elemente in $(\mathbb{Z}/p\mathbb{Z})^\times$ durch Multiplikation erzeugt. Da a und b nicht durch p teilbar sind, können wir ihre Klassen in $\mathbb{Z}/p\mathbb{Z}$ als $\bar{a} = \bar{g}^r$ und $\bar{b} = \bar{g}^s$ mit $r, s \in \mathbb{N}$ schreiben. Wir erhalten aus Lemma 2.33 somit

$$\left(\frac{ab}{p}\right) = \left(\frac{g^{r+s}}{p}\right) = (-1)^{r+s} = (-1)^r(-1)^s = \left(\frac{g^r}{p}\right)\left(\frac{g^s}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

und die Behauptung ist bewiesen. □

Um die Quadrate in $\mathbb{Q}_p$ zu finden, benötigen wir noch Hensels Lemma.

Satz 2.35 (Hensels Lemma)**.** *Sei $f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_lX^l$ ein Polynom mit Koeffizienten in $\mathbb{Z}_p$ und $f'(X)$ die formale Ableitung $f'(X) = a_1 + 2a_2X + \ldots + la_lX^{l-1}$ von $f(X)$. Nehmen wir an, es existiert für $m \geq 1$ eine p-adische ganze Zahl $x_0 \in \mathbb{Z}_p$, sodass*

$$f(x_0) \equiv 0 \ (mod\ p^m) \text{ und } v_p(f'(x_0)) = k \text{ mit } 2k < m$$

ist. Dann können wir eine p-adische ganze Zahl $x \in \mathbb{Z}_p$ finden, sodass $f(x) = 0$ und $x \equiv x_0 \ (mod\ p^{m-k})$ ist.

Beweis. Dieser Satz wird in [9] auf S. 167 bewiesen. □

Nun haben wir das nötige Werkzeug, um die Quadrate in $\mathbb{Q}_p$ zu bestimmen.

Satz 2.36. *Sei $x = p^n u \in \mathbb{Q}_p$ mit $u \in \mathbb{Z}_p^\times$. Das Element x ist genau dann ein Quadrat in $\mathbb{Q}_p$, wenn*

$$2|n \text{ und } \begin{cases} \left(\frac{u}{p}\right) = 1 & \text{für } p \neq 2, \\ u \equiv 1 \pmod 8 & \text{für } p = 2. \end{cases}$$

Beweis. Sei $x = p^n u$ in $\mathbb{Q}_p$ mit $u \in \mathbb{Z}_p^\times$. Ist x ein Quadrat mit Quadratwurzel $y \in \mathbb{Q}_p$, dann gilt $n = v_p(x) = v_p(y \cdot y) = 2v_p(y)$, und n ist notwendigerweise gerade. Ist ein solches n gegeben, so ist x genau dann ein Quadrat, wenn u eines ist. Da $u \in \mathbb{Z}_p^\times$ ist, haben wir $p \nmid u$, und für eine Quadratwurzel v gilt somit ebenfalls $p \nmid v$ und $v \in \mathbb{Z}_p^\times$.
Ist $p \neq 2$ und u hat eine Quadratwurzel v in $\mathbb{Z}_p^\times$, dann ist u quadratischer Rest modulo p. Sei umgekehrt u ein quadratischer Rest modulo p, dann hat das Polynom $f(X) = X^2 - u$ modulo p eine Nullstelle

$y \in (\mathbb{Z}/p\mathbb{Z})^\times$, und die Ableitung ist $f'(y) = 2y \neq 0$ modulo p. Nach Satz 2.35 gibt es eine Lösung $v \in \mathbb{Z}_p$, und u ist ein Quadrat in $\mathbb{Z}_p$. Ist n gerade, dann ist auch $x = p^n u$ ein Quadrat in $\mathbb{Q}_p$.

Sei nun $p = 2$ und $u = v^2 \in \mathbb{Z}_2^\times$ ein Quadrat, so gilt $v \in \mathbb{Z}_2^\times$. Daraus folgt $2 \nmid u$ und $2 \nmid v$, und wir können $u = 1 + 2x$ und $v = 1 + 2y$ mit $x, y \in \mathbb{Z}_2$ schreiben. Aus $u = v^2$ erhalten wir

$$\begin{aligned} & 1 + 2x = (1 + 2y)^2 = 1 + 4y + 4y^2 = 1 + 4y(1 + y) \\ \Leftrightarrow\ & x = 2y(1 + y). \end{aligned}$$

Da entweder $2 \mid y$ oder $2 \mid (1 + y)$ gilt, erhalten wir $4 \mid x$ und folglich $u = 1 + 2x \equiv 1 \pmod 8$.

Ist umgekehrt $u \equiv 1 \pmod 8$, dann ist 3 eine Nullstelle des Polynoms $f(X) = X^2 - u$ modulo $2^3 = 8$, denn $3^2 - u \equiv 1 - 1 = 0 \pmod 8$. Für die Ableitung gilt außerdem, dass $v_2(f'(3)) = v_2(6) = 1$ und $2 \cdot 1 < 3$. Aus Satz 2.35 folgt, dass ein $x_0 \in \mathbb{Z}_p$ mit $f(x_0) = 0$ existiert. Entsprechend ist $u = x_0^2$ ein Quadrat. □

Korollar 2.37. *Die Untergruppe der Quadrate $\mathbb{Q}_p^{\times 2} \subset \mathbb{Q}_p^\times$ ist offen in $\mathbb{Q}_p^\times$. Außerdem gibt es für jedes $x \in \mathbb{Q}_p^\times$ ein $\epsilon > 0$, sodass*

$$|y - x|_p < \epsilon \Rightarrow \frac{y}{x} \in \mathbb{Q}_p^{\times 2}$$

für jedes $y \in \mathbb{Q}_p$ gilt.

Beweis. Die erste Aussage ergibt sich folgendermaßen aus Satz 2.36. Für $p \neq 2$ ist eine Einheit $u \in \mathbb{Z}_p^\times$ genau dann ein Quadrat, wenn $u \equiv v^2 \pmod p$ für ein $v \in \mathbb{Z}_p^\times$ ist. Der offene Ball $B(u, 1) = u + p\mathbb{Z}_p$ in $\mathbb{Z}_p^\times$ ist demnach in $\mathbb{Q}_p^{\times 2}$ enthalten, und somit hat auch ein Element $x = p^n u \in \mathbb{Q}_p^{\times 2}$ eine offene Umgebung $x + p^{n+1}\mathbb{Z}_p$ in $\mathbb{Q}_p^\times$, welche ebenfalls in $\mathbb{Q}_p^{\times 2}$ liegt. Für $p = 2$ ist $u \in \mathbb{Z}_p^\times$ genau dann ein Quadrat, wenn $u \equiv 1 \pmod{p^3}$ gilt. Folglich ist der offene Ball $B(u, p^{-2}) = u + p^3\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ in $\mathbb{Q}_p^{\times 2}$ enhalten, und $x = p^n u \in \mathbb{Q}_p^{\times 2}$ hat eine offene Umgebung $x + p^{n+3}\mathbb{Z}_p \subset \mathbb{Q}_p^\times$, welche in $\mathbb{Q}_p^{\times 2}$ liegt. Die Menge der Quadrate $\mathbb{Q}_p^{\times 2}$ ist somit offen in $\mathbb{Q}_p^\times$ für alle Primzahlen p.

Da $1 \in \mathbb{Q}_p^{\times 2}$ und $\mathbb{Q}_p^{\times 2} \subset \mathbb{Q}_p^\times$ offen ist, existiert ein $\epsilon' > 0$, sodass der offene Ball $B(1, \epsilon')$ in $\mathbb{Q}_p^{\times 2}$ liegt. Wir setzen nun für $x \in \mathbb{Q}_p^\times$ den Wert $\epsilon := |x|_p \epsilon' > 0$. Dann gilt für $y \in \mathbb{Q}_p$ mit $|y - x|_p < \epsilon$, dass

$$\left|\frac{y}{x} - 1\right|_p = |x|_p^{-1}|y - x|_p < |x|_p^{-1}\epsilon = \epsilon'.$$

Wir erhalten $\frac{y}{x} \in B(1, \epsilon')$ und folglich $\frac{y}{x} \in \mathbb{Q}_p^{\times 2}$.

□

3 Das Hilbert-Symbol

Wir beschreiben nun das Hilbert-Symbol, welches der Untersuchung der Lösungen quadratischer Formen in drei Variablen dient. Im gesamten Abschnitt bezeichne $\mathbb{Q}_v$ mit $v \in V = \{p \in \mathbb{N} \mid p \text{ prim}\} \cup \{\infty\}$ wieder den Körper der reellen Zahlen $\mathbb{R} = \mathbb{Q}_\infty$ oder einen der Körper der p-adischen Zahlen $\mathbb{Q}_p$ für eine Primzahl p.

Definition 3.1 (Hilbert-Symbol)**.** Das Hilbert-Symbol $(a, b)_v$ für Zahlen $a, b \in \mathbb{Q}_v^\times$ ist folgendermaßen definiert:

$$\begin{aligned} &(a, b)_v = +1, \text{ wenn } Z^2 - aX^2 - bY^2 = 0 \text{ eine Lösung } (z, x, y) \neq (0, 0, 0) \text{ in } \mathbb{Q}_v^3 \text{ hat.} \\ &(a, b)_v = -1, \text{ wenn eine solche Lösung nicht existiert.} \end{aligned}$$

Der Wert von $(a, b)_v$ ändert sich nicht, wenn man a oder b mit einem Quadrat multipliziert, da die Variablen quadratische Faktoren absorbieren können. Daher definiert das Hilbert-Symbol eine Abbildung $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2} \times \mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2} \to \{\pm 1\}$. Wir untersuchen nun einige Eigenschaften des Hilbert-Symbols.

Definition 3.2. Für $b \in \mathbb{Q}_v^\times$ definieren wir die **Normgruppe** von b in $\mathbb{Q}_v^\times$ als

$$N_b := \{a \in \mathbb{Q}_v^\times \mid a = r^2 - bs^2 \text{ mit } r, s \in \mathbb{Q}_v\}.$$

Proposition 3.3. *Die Normgruppe N_b für $b \in \mathbb{Q}_v^\times$ ist eine Untergruppe von $\mathbb{Q}_v^\times$. Ist b ein Quadrat in $\mathbb{Q}_v^\times$, dann gilt $N_b = \mathbb{Q}_v^\times$.*

Beweis. Seien $a = r^2 - bs^2$ und $\tilde{a} = \tilde{r}^2 - b\tilde{s}^2$ in N_b. Dann ist

$$\begin{aligned} a\tilde{a} &= (r^2 - bs^2)(\tilde{r}^2 - b\tilde{s}^2) \\ &= (r\tilde{r})^2 - b(r\tilde{s})^2 - b(\tilde{r}s)^2 + (bs\tilde{s})^2 + 2brs\tilde{r}\tilde{s} - 2brs\tilde{r}\tilde{s} \\ &= (r\tilde{r} - bs\tilde{s})^2 - b(r\tilde{s} - \tilde{r}s)^2 \in N_b. \end{aligned}$$

Außerdem ist a^{-1} durch

$$\frac{1}{r^2 - bs^2} = \frac{r^2 - bs^2}{(r^2 - bs^2)^2} = \left(\frac{r}{r^2 - bs^2}\right)^2 - b\left(\frac{s}{r^2 - bs^2}\right)^2 \in N_b$$

gegeben. Mit $1 = 1^2 - b0^2$ enthält N_b auch das neutrale Element von $\mathbb{Q}_v^\times$ und ist somit eine Untergruppe.

Ist $b = c^2$ ein Quadrat in $\mathbb{Q}_v^\times$, so können wir jedes $a \in \mathbb{Q}_v^\times$ als

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

schreiben. Demnach gilt $N_b = \mathbb{Q}_v^\times$, wenn b ein Quadrat ist. □

Proposition 3.4. *Seien $a, b \in \mathbb{Q}_v^\times$, dann gilt $(a,b)_v = 1$ genau dann, wenn a in der Normgruppe N_b liegt – das heißt, genau dann, wenn a in der Form $r^2 - bs^2$ mit $r, s \in \mathbb{Q}_v$ geschrieben werden kann.*

Beweis. Sei zuerst $b = c^2$ ein Quadrat. Dann hat die Gleichung $Z^2 - aX^2 - c^2Y^2 = 0$ als Lösung $(c, 0, 1)$ für alle $a \in \mathbb{Q}_v^\times$, und somit ist $(a,b)_v = 1$ für alle a. Ebenso gilt $N_b = \mathbb{Q}_v^\times$ und somit liegen alle $a \in \mathbb{Q}_v^\times$ auch in N_b.

Sei nun b kein Quadrat und $(a,b)_v = 1$. Dann hat die Gleichung $Z^2 - aX^2 - bY^2 = 0$ eine Lösung $(z, x, y) \neq (0,0,0)$ in $(\mathbb{Q}_v)^3$. Falls $x = 0$ ist, dann ist b im Widerspruch zur Annahme ein Quadrat $b = (z/y)^2$. Es gilt daher $x \neq 0$, und so können wir a als $a = (z/x)^2 - b(y/x)^2$ schreiben.

Sei nun umgekehrt $a = r^2 - bs^2$ mit $r, s \in \mathbb{Q}_v$. Dann hat die Gleichung $Z^2 - aX^2 - bY^2 = 0$ die Lösung $(r, 1, s) \in (\mathbb{Q}_v)^3$. Somit ist $(a,b)_v = 1$. □

Proposition 3.5. *Das Hilbert-Symbol hat folgende Eigenschaften für alle $a, b, c \in \mathbb{Q}_v^\times$:*

1. $(a,b)_v = (b,a)_v$ *und* $(a,b^2)_v = 1$,
2. $(a,-a)_v = 1$ *und für* $a \neq 1$ *gilt* $(a,1-a)_v = 1$,
3. *wenn* $(a,bc)_v = 1$, *dann gilt* $(a,b)_v = (a,c)_v$,
4. $(a,b)_v = (a,-ab)_v = (a,(1-a)b)_v$,
5. $(a,1)_v = 1$ *und* $(a,a)_v = (a,-1)_v$,

Beweis. 1.: Die Eigenschaft $(a,b)_v = (b,a)_v$ folgt aus der Austauschbarkeit der Variablen. Des Weiteren hat die Gleichung $Z^2 - aX^2 - b^2Y^2 = 0$ wie im Beweis von Proposition 3.4 als Lösung $(b, 0, 1)$, und somit gilt $(a,b^2)_v = 1$.

2.: Die Gleichung $Z^2 - aX^2 + aY^2 = 0$ hat als Lösung $(0, 1, 1)$, daher ist $(a,-a)_v = 1$. Für $a \neq 1$ hat die Gleichung $Z^2 - aX^2 - (1-a)Y^2 = 0$ als Lösung $(1, 1, 1)$, somit ist auch $(a, 1-a)_v = 1$.

3.: Sei $(a,bc)_v = 1$. Dann liegt bc nach Proposition 3.4 in N_a. Ist $(a,b)_v = 1$ und somit b in N_a, so ist $c = b^{-1}(bc)$ ebenfalls in N_a und $(a,c)_v = 1$. Ebenso impliziert $(a,c)_v = 1$, dass c und folglich $b = c^{-1}(bc)$ in N_a liegen, und somit $(a,b)_v = 1$ ist. Damit folgt aus $(a,bc)_v = 1$, dass $(a,b)_v = (a,c)_v$ ist.

4. Ist $(a,b)_v = 1$, so gilt $(a,b)_v = (a,b(-a)^2)_v = (a,-ab(-a))_v = 1$, da die Variablen der Gleichung $Z^2 - aX^2 - bY^2 = 0$ quadratische Faktoren absorbieren. Aus 2. und 3. erhalten wir $(a,-ab)_v = (a,-a)_v = 1$. Sei umgekehrt $(a,-ab)_v = 1$. Dann gilt nach 3., dass $(a,b)_v = (a,-a)_v = 1$ ist, und somit gilt

$(a,b)_v = (a,-ab)_v$. Ist $(a,b)_v = 1$, so gilt auch $(a,b(1-a)^2)_v = 1$ und nach 2. und 3. somit $(a,b(1-a))_v = (a,1-a)_v = 1$. Sei umgekehrt $(a,(1-a)b)_v = 1$. Dann folgt ebenso $(a,b)_v = (a,1-a)_v = 1$, und somit ist $(a,b)_v = (a,(1-a)b)_v$.

5.: Die Gleichung $Z^2 - aX^2 - Y^2 = 0$ hat als Lösung $(1,0,1)$, also ist $(a,1)_v = 1$. Aus 2. wissen wir, dass $(a,-a)_v = 1$ ist, und zusammen mit 3. ergibt das $(a,a)_v = (a,-1)_v$. □

Wir werden nun genaue Formeln für den Wert von $(a,b)_v$ über den Körpern $\mathbb{Q}_v$ herleiten. Aus diesen wird auch folgen, dass das Hilbert-Symbol eine bimultiplikative Abbildung ist, d.h. es hat die nützliche Eigenschaft, dass $(a,bc)_v = (a,b)_v(a,c)_v$ gilt. Wir müssen dafür das Hilbert-Symbol für alle möglichen Kombinationen von Elementen $a,b \in \mathbb{Q}_v$ ausrechnen. Da das Hilbert-Symbol eine Abbildung $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2} \times \mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2} \to \{\pm 1\}$ definiert, ist es ausreichend, wenn wir das Symbol nur auf den Äquivalenzklassen in $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$ berechnen. Diese sind folgendermaßen gegeben.

Lemma 3.6. *1. Die Gruppe $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ hat Ordnung 2 und wird durch die Repräsentanten $\{1,-1\}$ beschrieben.*

2. Für $p \neq 2$ hat die Gruppe $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ Ordnung 4. Die Elemente werden durch die Repräsentanten

$$\{1,u,p,pu\}$$

gegeben, wobei $u \in \mathbb{Z}_p^\times$ ein beliebiger quadratischer Nichtrest ist.

3. Für $p = 2$ hat die Gruppe $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ Ordnung 8. Die Elemente werden durch die Repräsentanten

$$\{\pm 1, \pm 5, \pm 2, \pm 10\}$$

gegeben.

Beweis. 1.: Für alle Zahlen $a \in \mathbb{R}^\times$ gilt, dass entweder $a \cdot 1 \in \mathbb{R}^{\times 2}$ oder $a \cdot (-1) \in \mathbb{R}^{\times 2}$, also sind durch $\{1,-1\}$ Repräsentanten gegeben.

2.: Auch hier ist zu zeigen, dass für alle $a \in \mathbb{Q}_p^\times$ und einen beliebig gewählten quadratischen Nichtrest $u \in \mathbb{Z}_p^\times$ genau ein Repräsentant $x \in \{1,u,p,pu\}$ die Bedingung $a = xq$ für ein Quadrat $q \in \mathbb{Q}_p^{\times 2}$ erfüllt, also dass $ax^{-1} \in \mathbb{Q}_p^{\times 2}$ ist. Sei nun $a = p^n v \in \mathbb{Q}_p^\times$ mit $v \in \mathbb{Z}_p^\times$, und sei $u \in \mathbb{Z}_p^\times$ ein quadratischer Nichtrest. Aus Satz 2.36 wissen wir, dass $a = p^n v$ genau dann ein Quadrat ist, wenn $2 | v_p(a)$ und $\left(\frac{v}{p}\right) = 1$ gilt. Ist $a = p^n v$ ein Quadrat, so ist es nach Multiplikation mit p oder dem quadratischen Nichtrest u kein Quadrat mehr, daher gilt $a \cdot 1 \in \mathbb{Q}_p^{\times 2}$ mit 1 als einzig möglichen Repräsentanten. Ist a kein Quadrat, jedoch gilt $2 \mid n$, dann ist v quadratischer Nichtrest. Somit gilt $\left(\frac{vu^{-1}}{p}\right) = \left(\frac{v}{p}\right)\left(\frac{u^{-1}}{p}\right) = (-1)^2 = 1$ und $a \cdot u^{-1} \in \mathbb{Q}_p^{\times 2}$. Ist a kein Quadrat, jedoch v ein quadratischer Rest, so gilt $2 \nmid v_p(a)$. Folglich ist $a \cdot p^{-1} \in \mathbb{Q}_p^{\times 2}$. Für a mit $2 \nmid v_p(a)$ und v quadratischer Nichtrest gilt demnach $a \cdot (pu)^{-1} \in \mathbb{Q}_p^{\times 2}$. Somit wird durch $\{1,u,p,up\}$ ein vollständiges Repräsentantensystem gegeben.

3.: Hier ist Ähnliches wie für 2. zu zeigen. Allein die Bedingung für Quadrate ändert sich: Ein Element $a = p^n v \in \mathbb{Q}_2^\times$ mit $v \in \mathbb{Z}_2^\times$ und $p = 2$ ist nach Satz 2.36 genau dann ein Quadrat, wenn $2 \mid n$ und $v \equiv 1 \pmod 8$ ist. Sei nun $a = p^n v$ mit $v \in \mathbb{Z}_2^\times$ gegeben. Aufgrund $2 \nmid v$ müssen wir für v nur vier verschiedene Fälle beachten:

- $v \equiv 1 \pmod 8$: Dann ist $v \cdot 1 \equiv 1 \pmod 8$.
- $v \equiv 3 \pmod 8$: Dann ist $v \cdot (-5) \equiv v \cdot (-5)^{-1} \equiv -15 \equiv 1 \pmod 8$.
- $v \equiv 5 \pmod 8$: Dann ist $v \cdot 5 \equiv v \cdot 5^{-1} \equiv 25 \equiv 1 \pmod 8$.
- $v \equiv 7 \pmod 8$: Dann ist $v \cdot (-1) \equiv 1 \pmod 8$.

Gilt auch $2 \nmid n$, müssen wir a zusätzlich mit 2^{-1} multiplizieren. Das bedeutet, dass wir insgesamt 8 verschiedene Fälle haben, die alle durch das Repräsentantensystem $\{\pm 1, \pm 5, \pm 2, \pm 10\}$ dargestellt werden. □

Durch Lemma 3.6 wird der Rechenaufwand für die Fälle $\mathbb{R}$, $\mathbb{Q}_2$ und $\mathbb{Q}_p$ mit $p \neq 2$ schon erheblich auf $4 + 16 + 64$ Werte verringert. Durch die Eigenschaft $(a,b)_v = (b,a)_v$ des Hilbert-Symbols reduziert sich der Aufwand abermals. Folgendes Lemma wird uns helfen, im Satz 3.8 die Werte des Hilbert-Symbols zu berechnen.

Lemma 3.7. *Der Körper $\mathbb{Z}/p\mathbb{Z}$ enthält genau $\frac{p+1}{2}$ Quadrate.*

Beweis. Sei $\bar{g} \in (\mathbb{Z}/p\mathbb{Z})^\times$ eine primitive Wurzel modulo p. Das Element $\bar{g}$ generiert demnach alle Elemente in $(\mathbb{Z}/p\mathbb{Z})^\times$. Gleichzeitig wissen wir aus Lemma 2.33, dass für ein $k \in \mathbb{N}$ das Element $\bar{g}^k$ genau dann ein Quadrat in $(\mathbb{Z}/p\mathbb{Z})^\times$ ist, wenn k gerade ist. Die Ordnung von $\bar{g}$ ist $p-1$, daher gibt es $(p-1)/2$ Quadrate in $(\mathbb{Z}/p\mathbb{Z})^\times$. In $\mathbb{Z}/p\mathbb{Z}$ ist außerdem die Null auch ein Quadrat, somit gibt es dort $(p+1)/2$ Quadrate. □

Satz 3.8. *Die Werte des Hilbert-Symbols sind folgendermaßen gegeben.*

1. *Über dem Körper $\mathbb{R}$ gilt*

$$(1,-1)_\infty = (-1,1)_\infty = (1,1)_\infty = 1 \text{ und } (-1,-1)_\infty = -1.$$

   Das Hilbertsymbol $(a,b)_\infty$ ist also genau dann gleich 1, wenn mindestens einer der beiden Koeffizienten a oder b positiv ist.

2. *Über dem Körper $\mathbb{Q}_p$ mit $p \neq 2$ und $u, v \in \mathbb{Z}_p^\times$ gilt*

$$(p,p)_p = (-1)^{\frac{p-1}{2}}, \quad (p,u)_p = \left(\frac{u}{p}\right), \quad (u,v)_p = 1.$$

3. *Über dem Körper $\mathbb{Q}_2$ und $u, v \in \mathbb{Z}_2^\times$ gilt*

$$(2,2)_2 = 1, \quad (2,u)_2 = (-1)^{\frac{u^2-1}{8}}, \quad (u,v)_2 = (-1)^{\frac{u-1}{2}\frac{v-1}{2}},$$

   wobei wir hier mit $(-1)^a$ für $a \in \mathbb{Z}_2$ den Ausdruck $(-1)^{a \bmod 2}$ bezeichnen.

Insbesondere ist das Hilbert-Symbol bimultiplikativ, woraus sich auch die restlichen Werte über $\mathbb{Q}_p$ mit p prim ergeben.

Beweis. Wir werden hier 1. und 2. beweisen, indem wir das Hilbert-Symbol für alle möglichen Kombinationen von Elementen berechnen. Die Bimultiplikativität des Hilbert-Symbols ergibt sich dann direkt aus den berechneten Resultaten. Der Beweis von 3. ist vor allem eine Anwendung von Proposition 3.5 und kann in [9] auf S. 174 nachgelesen werden. Dort werden abermals alle Werte einzeln ausgerechnet, sodass sich auch hier die Bimultiplikativität direkt ergibt.

1.: Alle Quadrate in $\mathbb{R}$ sind positiv. Daher hat die Gleichung $Z^2 - aX^2 - bY^2 = 0$ mit Koeffizienten in $\mathbb{R}^\times$ genau dann eine nichttriviale Lösung in $\mathbb{R}^3$, wenn a, b oder beide strikt positiv sind, da die Summe der linken Seite der Gleichung sonst nicht Null ergeben kann. Daher gilt $(1,-1)_\infty = (-1,1)_\infty = (1,1)_\infty = 1$ und $(-1,-1)_\infty = -1$.

2.: Betrachten wir nun $\mathbb{Q}_p$ mit $p \neq 2$. Es folgt aus Satz 2.36, dass ein quadratischen Rest $u \in \mathbb{Z}_p^\times$ ein Quadrat ist. Daraus folgt nach Proposition 3.5, dass $(a,u)_p = 1$ für alle $a \in \mathbb{Q}_p^\times$ gilt. Somit sind die Fälle $(p,u)_p = 1 = \left(\frac{u}{p}\right)$, $(u,v)_p = 1$ und $(pu,u)_p = 1 = \left(\frac{u}{p}\right) \cdot 1 = (p,u)_p(u,u)_p$ für alle $v \in \mathbb{Z}_p^\times$ und für u ein quadratischer Rest geklärt.

Wir berechnen nun den Wert von $(p,u)_p$ für $u \in Z_p^\times$ ein quadratischer Nichtrest. Betrachten wir die Gleichung

$$Z^2 - pX^2 - uY^2 = 0.$$

Nehmen wir $(p,u)_p = 1$ an, dass also diese Gleichung eine nichttriviale Lösung $(z,x,y) \in \mathbb{Q}_p^3$ hat. Dann können wir durch Multiplizieren der Gleichung mit der Primzahlpotenz p^{-k} mit $k := \min(v_p(z), v_p(x), v_p(y))$ erreichen, dass x, y und z in $\mathbb{Z}_p$ liegen und nicht alle durch p teilbar sind. Wir zeigen nun durch Widerspruch, dass nur x durch p teilbar ist. Wenn y durch p teilbar ist, so muss auch z durch p teilbar sein, und in Folge ist px^2 durch p^2 teilbar. Das bedeutet, dass x ebenfalls durch p teilbar ist – ein Widerspruch zu unserer Wahl von k. Sei nun z durch p teilbar. Durch analoge Argumentation ist

ebenso y und somit auch x durch p teilbar, und wir erhalten denselben Widerspruch. Demnach gilt, dass $y, z \in \mathbb{Z}_p^\times$ und $x \in \mathbb{Z}_p$ ist, und wir können die Gleichung sinnvoll modulo p betrachten. Wir erhalten

$$z^2 - uy^2 \equiv 0 \pmod{p},$$

also ist $u \equiv z^2/y^2 \pmod{p}$ ein quadratischer Rest modulo p. Dies widerspricht unserer Wahl von u. Somit kann nicht $(p,u)_p = 1$ gelten, und wir erhalten $(p,u)_p = -1 = \left(\frac{u}{p}\right)$. Zusammen mit dem vorherigen Resultat gilt folglich für alle $u \in \mathbb{Z}_p^\times$, dass $(p,u)_p = \left(\frac{u}{p}\right)$.

Sei wieder $u \in \mathbb{Z}_p^\times$ ein quadratischer Nichtrest. Wir berechnen nun $(u,u)_p$ und $(pu,v)_p$ für $v \in \mathbb{Z}_p^\times$. Dafür betrachten wir die Gleichung

$$u^{-1} - X^2 - Y^2 = 0.$$

Da die Funktionen $Y \mapsto Y^2$ und $X \mapsto u^{-1} - X^2$ modulo p nach Lemma 3.7 jeweils $(p+1)/2$ verschiedene Werte in $\mathbb{Z}/p\mathbb{Z}$ annehmen und $\mathbb{Z}/p\mathbb{Z}$ nur p verschiedene Elemente hat, muss es eine Lösung $(x,y) \in (\mathbb{Z}_p)^2$ der Gleichung modulo p geben. Wir haben also $x^2 + y^2 \equiv u^{-1} \pmod{p}$. Da u nicht durch p teilbar ist, gilt das ohne Beschränkung der Allgemeinheit auch für x. Wir definieren das Polynom $f(X) = u^{-1} - X^2 - y^2$. Da x eine Lösung modulo p und außerdem $f'(x) = 2x \not\equiv 0 \pmod{p}$ ist, können wir Satz 2.35 anwenden und erhalten eine Lösung $x_0 \in \mathbb{Z}_p$ des Polynoms. Wir multiplizieren das Polynom mit u und erhalten $0 = 1 - ux_0^2 - uy^2$. Folglich hat die Gleichung $Z^2 - uX^2 - uY^2 = 0$ eine nichttriviale Lösung $(1, x_0, y) \in (\mathbb{Q}_p)^3$, und es gilt $(u,u)_p = 1$. Aus $1 = (u,u)_p = (up^2, u)_p$ folgt mit Proposition 3.5 (3.), dass $(pu,u)_p = (p,u)_p = -1$ ist, da u quadratischer Nichtrest ist. Das heißt, für beliebige $v \in \mathbb{Z}_p^\times$ gilt $(pu,v)_p = \left(\frac{v}{p}\right) = (p,v)_p(u,v)_p$.

Aus den bisherigen Resultaten und Proposition 3.5 (3.) können wir des Weiteren schließen, dass $(p,p)_p = (p,-1)_p = \left(\frac{-1}{p}\right)$, da -1 in $\mathbb{Z}_p^\times$ liegt. Wir wissen, dass eine primitive Wurzel $\bar{g}$ die Eigenschaft $\bar{g}^{p-1} = 1$ hat. Da ebenso $(-1)^2 = 1$ gilt und $p-1$ als Ordnung von g minimal ist, erhalten wir $\bar{g}^{(p-1)/2} = -1$ und somit $(p,p)_p = \left(\frac{\bar{g}^{\frac{p-1}{2}}}{p}\right) = (-1)^{\frac{p-1}{2}}$. Aus Proposition 3.5 (4.) folgt $(p,pu)_p = (p,-p^2u)_p = (p,-u)_p = \left(\frac{-u}{p}\right) = (p,p)_p(p,u)_p$. Analog erhalten wir mit Proposition 3.5 (5.) das Resultat $(pu,pu)_p = (pu,-1)_p = \left(\frac{-1}{p}\right)$, da -1 ein Einheit in $\mathbb{Z}_p^\times$ ist. Dies zeigt die Werte des Hilbert-Symbols für $p \neq 2$. □

Aus diesem Satz erhalten wir folgendes Korollar.

Korollar 3.9. *Das Hilbert-Symbol ist eine nichtausgeartete bimultiplikative Abbildung auf* $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2} \times \mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$.

Beweis. Die Bimultiplikativität haben wir schon mit Satz 3.8 bewiesen. Es ist noch zu zeigen, dass ein Element $a \in \mathbb{Q}_v^\times$ mit der Eigenschaft $(a,b)_v = 1$ für alle $b \in \mathbb{Q}_v^\times$ in $\mathbb{Q}_v^{\times 2}$ liegt. Dies folgt ebenfalls aus den errechneten Werten aus Satz 3.8. Gilt über $\mathbb{R}$ für ein $a \in \mathbb{R}^\times$, dass $(1,a)_\infty = (-1,a)_\infty = 1$ ist, so folgt $a \equiv 1 \pmod{\mathbb{R}^{\times 2}}$, und a ist ein Quadrat. Sei nun $a \in \mathbb{Q}_p^\times$ mit $p \neq 2$ prim, sodass a die Relationen $(a,p)_p = (a,u)_p = 1$ für einen quadratischen Nichtrest u erfüllt. Gilt $a \equiv u$, so folgt $(a,p)_p = (u,p)_p = (\frac{u}{p}) = 1$, im Widerspruch zu der Wahl von u. Gilt $a \equiv p$, so folgt aus $(u,a)_p = (u,p)_p = (\frac{u}{p}) = 1$ gleichfalls ein Widerspruch. Somit kann auch dieser Fall nicht vorkommen. Gilt $a \equiv pu$, so erhalten wir $(pu,u)_p = (p,u)_p(u,u)_p = 1$. Aus $(u,u)_p = 1$ folgt $(p,u)_p = 1$, was wieder der Wahl von u als quadratischer Nichtrest widerspricht. Somit kann dieser Fall auch nicht vorkommen. Daher muss $a \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$ gelten, und folglich ist a ein Quadrat.

Der Beweis über $\mathbb{Q}_2$ geht analog zu $\mathbb{Q}_p$. □

Der Körper der rationalen Zahlen $\mathbb{Q}$ ist in den Körpern $\mathbb{Q}_v$ mit $v \in V$ als Unterkörper enthalten. Für Zahlen $a, b \in \mathbb{Q}^\times$ können wir daher das Hilbert-Symbol $(a,b)_v$ ihrer jeweiligen Bilder in $\mathbb{Q}_v$ betrachten. Eine bemerkenswerte Eigenschaft des Hilbertsymbols für Elemente in $\mathbb{Q}$ ist die Produktformel, welche wir in Satz 3.11 beweisen. Ein Teil des Beweises basiert auf dem Quadratischen Reziprozitätsgesetz, welches wir hier vorstellen.

Lemma 3.10 (Quadratisches Reziprozitätsgesetz). *Seien $p, q > 2$ zwei Primzahlen. Dann gilt*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Für die Primzahl 2 gilt

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Beweis. Einen Beweis findet der Leser in [9] auf S. 24ff. □

Satz 3.11 (Produktformel des Hilbert-Symbols). *Seien $a, b \in \mathbb{Q}^\times$. Dann gilt $(a,b)_v = 1$ für fast alle $v \in V$, außerdem gilt die Produktformel*

$$\prod_{v \in V} (a,b)_v = 1.$$

Beweis. Da das Hilbert-Symbol invariant bleibt, wenn wir a oder b mit Quadraten multiplizieren, können wir annehmen, dass a und b beide quadratfrei sind und in $\mathbb{Z}$ liegen. Ganze Zahlen haben endlich viele Primteiler, daher gilt für fast alle Primzahlen p, dass $p \nmid ab$ und somit $a, b \in \mathbb{Z}_p^\times$ ist. Nach Satz 3.8 folgt daher $(a,b)_v = 1$ für fast alle $v \in V$.

Wir beweisen nun die Produktformel. Aufgrund der Bimultiplikativität und Symmetrie des Hilbert-Symbols müssen wir uns nur auf die Fälle der Tupel $(a,b) = (-1,-1), (-1,p)$ oder (p,q) für Primzahlen p und q konzentrieren, da alle ganzen Zahlen durch Multiplikation von Primzahlen und -1 erzeugt werden. Durch die speziellen Eigenschaften der Primzahl 2 ergeben sich daraus sechs Fälle.

1. Sei $(a,b) = (-1,-1)$. Es gilt $(-1,-1)_\infty = -1$, $(-1,-1)_p = 1$ für $2 \nmid p$ und $(-1,-1)_2 = -1$.

2. Sei $(a,b) = (-1,p)$ mit $p \neq 2$ eine Primzahl. Es gilt $(-1,p)_\infty = 1$, $(-1,p)_q = 1$ für q nicht gleich p oder 2, $(-1,p)_p = (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ und $(-1,p)_2 = (-1)^{\frac{p-1}{2}}$.

3. Sei $(a,b) = (-1,2)$. Die Gleichung $Z^2 - (-1)X^2 - 2Y^2 = 0$ hat als Lösung $(1,1,1)$, und daher gilt $(-1,2)_v = 1$ für alle $v \in V$.

4. Sei $(a,b) = (p,q)$ mit $p, q \neq 2$ Primzahlen. Es gilt $(p,q)_\infty = 1$, $(p,q)_r = 1$ für $r \neq 2, p$ oder q, $(p,q)_\infty = 1$, $(p,q)_q = (\frac{p}{q})$, $(p,q)_p = (\frac{q}{p})$ und $(p,q)_2 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Mit dem Quadratischen Reziprozitätsgesetz erhalten wir

$$\begin{aligned}(p,q)_q (p,q)_p (p,q)_2 &= \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1.\end{aligned}$$

5. Sei $(a,b) = (2,p)$ mit $p \neq 2$ eine Primzahl. Es gilt $(2,p)_\infty = 1$, $(2,p)_q = 1$ für $q \neq 2$ oder p, $(2,p)_p = (\frac{2}{p})$ und $(2,p)_2 = (-1)^{\frac{p^2-1}{8}}$. Aus dem Quadratischen Reziprozitätsgesetz folgt

$$(2,p)_p (2,p)_2 = (\frac{2}{p})(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p^2-1}{8}}(-1)^{\frac{p^2-1}{8}} = 1.$$

6. Sei $(a,b) = (2,2)$. Es gilt $(2,2)_v = 1$ für alle $v \in V$.

In jedem der sechs Fälle erhalten wir, dass das Produkt $\prod_{v \in V}(a,b)_v = 1$ ist. □

Es folgen nun drei Lemmas, die dazu dienen, Satz 3.15 zu beweisen. Jenen werden wir im Beweis des Satzes von Hasse-Minkowski verwenden. Auch der Chinesische Restsatz und die simultane Approximation werden uns wieder begegnen.

Lemma 3.12 (Chinesischer Restsatz). *Seien $a_1, \dots, a_k \in \mathbb{Z}$ und seien $m_1, \dots, m_k \in \mathbb{Z}_{>1}$ paarweise teilerfremd. Dann gibt es ein $x \in \mathbb{Z}$, sodass*

$$\begin{array}{rcl} x & \equiv a_1 & \mod m_1 \\ x & \equiv a_2 & \mod m_2 \\ & \vdots & \vdots \\ x & \equiv a_k & \mod m_k \end{array}$$

und $x \mod m_1 m_2 \cdots m_k$ eindeutig ist.

Beweis. Dies ist ein Satz der elementaren Algebra. Ein Beweis ist in [9] auf S.9 zu finden. □

Lemma 3.13 (Satz von Dirichlet). *Seien a und m zwei teilerfremde ganze Zahlen in $\mathbb{Z}_{\geq 1}$. Dann gibt es unendlich viele Primzahlen p, sodass $p \equiv a \mod m$.*

Beweis. Der Beweis dieses Satzes erfordert Methoden, deren Einführung eine weitere Bachelorarbeit füllen würden. Die neugierige Leserin verweisen wir daher an [9] Kapitel 8 oder an [11] Kapitel 6. □

Lemma 3.14 (Simultane Approximation). *Seien $v_1, \dots, v_n$ paarweise verschiedene Elemente in V, und $x_i \in \mathbb{Q}_{v_i}$ beliebige dazugehörige Zahlen. Dann gibt es eine Folge $(a_k)_{k \in \mathbb{N}}$ rationaler Zahlen, die für alle $i \in \{1, \dots, n\}$ gegen x_i in $\mathbb{Q}_{v_i}$ konvergiert.*

Beweis. Seien $p_1, \dots, p_n$ paarweise verschiedene Primzahlen, $x_i \in \mathbb{Q}_{p_i}$ beliebig, und $x_\infty \in \mathbb{R}$. Wir müssen zeigen, dass für ein beliebiges $N \in \mathbb{N}$ ein $x \in \mathbb{Q}$ existiert, sodass

$$|x - x_\infty|_\infty \leq p^{-N} \text{ und } |x - x_i|_{p_i} \leq p^{-N}$$

für alle i erfüllt ist. Durch Multiplikation aller x_i und x_∞ mit einer entsprechenden natürlichen Zahl können wir annehmen, dass $x_i \in Z_{p_i}$ für $i = 1, \dots, n$ gilt. Wir fixieren $N \in \mathbb{N}$. Nach dem Chinesischen Restsatz existiert ein $x_0 \in \mathbb{Z}$, welches das System von Kongruenzen $x \equiv x_i \pmod{p_i^N}$ erfüllt. Aus den Kongruenzen folgt, dass $|x_0 - x_i|_{p_i} \leq p^{-N}$ gilt. Wir definieren die ganze Zahl $m := p_1^N \cdots p_n^N$ und wählen ein $r \in \mathbb{N}$ teilerfremd zu m ausreichend groß, sodass $|m/r|_\infty \leq p^{-N}$. Wir möchten eine ganze Zahl $a \in \mathbb{Z}$ finden, sodass die Ungleichung

$$\left|x_0 - \frac{am}{r} - x_\infty\right|_\infty \leq p^{-N}$$

erfüllt ist. Existiert ein solches a, so gilt für $x := x_0 - \frac{am}{r}$ die gewünschte Ungleichung $|x - x_\infty|_\infty \leq p^{-N}$. Da r teilerfremd zu m ist, gilt ebenso $|am/r|_{p_i} \leq p^{-N}$. Demnach erhalten wir mit der verschärften Dreiecksungleichung ebenso

$$|x - x_i|_{p_i} = \left|x_0 - \frac{am}{r} - x_i\right|_{p_i} \leq \max(|x_0 - x_i|_{p_i}, \left|\frac{am}{r}\right|_{p_i}) = p^{-N}.$$

Wir definieren a als eine ganze Zahl, sodass $|\frac{r}{m}(x_0 - x_\infty) - a|_\infty \leq 1$ ist. Zum Beispiel erfüllt dies $a := \lceil \frac{r}{m}(x_0 - x_\infty) \rceil$, wenn $\frac{r}{m}(x_0 - x_\infty) \leq 0$ ist, und $a := \lfloor \frac{r}{m}(x_0 - x_\infty) \rfloor$, wenn $\frac{r}{m}(x_0 - x_\infty) \geq 0$ ist. Somit gilt

$$\left|x_0 - \frac{am}{r} - x_\infty\right|_\infty = \left|\frac{m}{r}\right|_\infty \left|\frac{r}{m}(x_0 - x_\infty) - a\right|_\infty \leq p^{-N},$$

wie gewünscht. Da wir ein entsprechendes $x =: a_N$ für alle $N \in \mathbb{N}$ finden können, erhalten wir eine Folge rationaler Zahlen $(a_n)_{n \in \mathbb{N}}$, die gegen die Elemente $x_i \in \mathbb{Q}_{p_i}$ mit $i = 1, \dots, n$ und $x_\infty \in \mathbb{R}$ konvergiert. □

Satz 3.15. *Seien $a_1, \dots a_n$ rationale Zahlen in $\mathbb{Q}^\times$, und seien $\epsilon_{i,v} \in \{\pm 1\}$ für $i = 1, \dots, n$ und $v \in V$. Es existiert genau dann ein $x \in \mathbb{Q}^\times$ mit der Eigenschaft, dass $(a_i, x)_v = \epsilon_{i,v}$ für alle $i = 1, \dots, n$ und $v \in V$, wenn folgende drei Bedingungen erfüllt sind:*

1. *Fast alle $\epsilon_{i,v}$ sind gleich 1.*
2. *Für alle $i = 1, \dots, n$ gilt $\prod_{v \in V} \epsilon_{i,v} = 1$.*

3. Für alle $v \in V$ existiert ein $x_v \in \mathbb{Q}_v^\times$, sodass $(a_i, x_v)_v = \epsilon_{i,v}$ für alle $i = 1, \ldots, n$.

Beweis. Angenommen es existiert ein $x \in \mathbb{Q}^\times$, sodass $(a_i, x)_v = \epsilon_{i,v}$ für alle $i = 1, \ldots, n$ und $v \in V$. Dann folgen die erste und zweite Bedingung aus Satz 3.11. Die dritte Bedingung ist erfüllt, indem wir einfach $x_v = x$ setzen.

Seien umgekehrt $\epsilon_{i,v} \in \{\pm 1\}$ mit $i = 1, \ldots, n$ und $v \in V$ gegeben, sodass sie die Bedingungen 1.-3. erfüllen. Wir können die a_i mit einer geeigneten Quadratzahl multiplizieren ohne das Hilbert-Symbol zu verändern, und daher die a_i als ganze Zahlen annehmen. Wir definieren die endlichen Mengen $S := \{\text{alle Primteiler der } a_i\} \cup \{2, \infty\}$ und $T := \{v \in V | \epsilon_{i,v} = -1 \text{ für mindestens ein } i\}$. Die Menge T ist aufgrund der ersten Bedingung im Satz endlich.

Wir nehmen zuerst an, dass $S \cap T = \emptyset$ ist. Wir definieren zwei ganze Zahlen

$$m := 8 \prod_{\ell \in S, \ell \neq 2, \infty} \ell \quad \text{und} \quad a := \prod_{\ell \in T, \ell \neq \infty} \ell.$$

Aufgrund $S \cap T = \emptyset$ gilt auch $2 \nmid a$, und a und m sind teilerfremd. Wir wenden Lemma 3.13 an, wonach unendlich viele Primzahlen p existieren, sodass $p \equiv a \pmod{m}$ gilt. Da S und T nur endlich viele Primzahlen enthalten, existiert ein $p \notin S \cup T$ mit $p \equiv a \pmod{m}$. Wir werden nun zeigen, dass das Element $x := ap \in \mathbb{Z}$ die Bedingung $(a_i, x)_v = \epsilon_{i,v}$ für alle $i = 1, \ldots, n$ und $v \in V$ erfüllt.

Liegt $v \in S$, so gilt wegen der Annahme $S \cap T = \emptyset$ und der Definition von T, dass $\epsilon_{i,v} = 1$ für alle i ist. Das heißt, wir müssen $(a_i, x)_v = 1$ für alle $i = 1, \ldots, n$ zeigen. Ist $v = \infty$, so folgt dies aus $x > 0$. Sei nun $v = q$ eine Primzahl. Aus der Konstruktion von x folgt $x = ap \equiv a^2 \pmod{m}$. Da q und 8 die Zahl m teilen, ist x ein Quadrat modulo q für $q \neq 2$ und ein Quadrat modulo 8 für $q = 2$. Außerdem gilt $q \nmid x$, und demnach ist x eine q-adische Einheit. Nach Satz 2.36 ist x somit ein Quadrat in $\mathbb{Q}_q$. Folglich gilt $(a_i, x)_q = 1$ für alle i.

Ist hingegen $v = q \notin S$, folgt aus der Definition von S, dass alle a_i q-adische Einheiten sind. Außerdem ist $2 \in S$ und daher $q \neq 2$. Nach der Wertetabelle in Satz 3.8 und der Bimultiplikativität des Hilbert-Symbols erhalten wir für jedes $b = q^{v_q(b)} u \in Q_q^\times$ die Gleichung

$$(a_i, b)_q = (a_i, q^{v_q(b)} u)_q = (a_i, q)_q^{v_q(b)} = \left(\frac{a_i}{q}\right)^{v_q(b)}.$$

Gilt auch $q \notin T$ und $q \neq p$, so gilt $q \nmid x$. Somit ist $v_q(x) = 0$ und $(a_i, x)_q = 1 = \epsilon_{i,q}$ für alle i.
Liegt $q \in T$, so gilt aufgrund der Konstruktion von $x = ap$, dass $v_q(x) = 1$ ist. Wir müssen also zeigen, dass $(a_i, x)_q = \left(\frac{a_i}{q}\right) = \epsilon_{i,q}$ gilt. Nach der dritten Bedingung im Satz existiert ein $x_q \in \mathbb{Q}_q^\times$ mit $(a_i, x_q)_q = \epsilon_{i,q}$ für alle i. Da $q \in T$ liegt, gilt für mindestens einen Index j, dass $\epsilon_{j,q} = -1$ ist. Wir wenden die obige Formel auf $(a_j, x_q)_q$ an und sehen, dass $\left(\frac{a_j}{q}\right)^{v_q(x_q)} = -1$ ist, also dass $v_q(x_q)$ ungerade ist. Daraus folgt

$$\epsilon_{i,q} = (a_i, x_q)_q = \left(\frac{a_i}{q}\right)^{v_q(x_q)} = \left(\frac{a_i}{q}\right) = (a_i, x)_q$$

für $i = 1, \ldots, n$.

Es bleibt nur noch der Fall $v = p$ zu zeigen. Aus der zweiten Bedingung im Satz erhalten wir, dass $\prod_{v \in V} \epsilon_{i,v} = 1$ für alle $i = 1, \ldots, n$ gilt. Da $p \nmid a, a_i$ gilt, folgt $a, a_i \in \mathbb{Z}_q^\times$ und $(a_i, x)_p = (a_i, ap)_p = (a_i, a)_p (a_i, p)_p = (a_i, p)_p$. Da wir für $v \neq p$ schon $(a_i, x)_v = \epsilon_{i,v}$ gezeigt haben, ergibt sich in Kombination mit der Produktformel für das Hilbert-Symbol zusammen mit der zweiten Bedingung im Satz

$$(a_i, p)_p = \frac{1}{\prod_{v \neq p} (a_i, p)_v} = \frac{1}{\prod_{v \neq p} \epsilon_{i,v}} = \epsilon_{i,p}.$$

Somit haben wir die Aussage für den Spezialfall $S \cap T = \emptyset$ gezeigt. Der allgemeine Fall kann wie folgt auf den Spezialfall zurückgeführt werden. Nach der dritten Bedingung im Satz existiert für jedes $v \in V$ ein $x_v \in \mathbb{Q}_v^\times$, sodass $(a_i, x_v)_v = \epsilon_{i,v}$ für alle i gilt. Da S eine endliche Menge ist, können wir die Elemente

x_v mit $v \in S$ mittels der simultanen Approximation aus Satz 3.14 durch eine Folge rationaler Zahlen gleichzeitig annähern. Das bedeutet, für beliebiges $\epsilon > 0$ existiert ein $y \in \mathbb{Q}$, sodass für alle x_v mit $v \in S$ die Ungleichung

$$|y - x_v|_v < \epsilon$$

gilt. Wählen wir ϵ ausreichend klein, erhalten wir aus Korollar 2.37, dass y/x_v ein Quadrat in $\mathbb{Q}_v^\times$ ist. Daraus folgt insbesondere, dass $(a_i, x_v)_v = (a_i, x_v \frac{y}{x_v})_v = (a_i, y)_v$ für alle $v \in S$ und $i = 1, \ldots, n$ gilt. Wir ändern nun die Vorgaben ab und setzen $\tilde{\epsilon}_{i,v} := \epsilon_{i,v}(a_i, y)_v$ für alle $v \in V$ und $i = 1, \ldots, n$. Für die neuen Werte gilt $\tilde{\epsilon}_{i,v} = 1$ für alle $v \in S$, und somit erhalten wir wieder den Spezialfall $S \cap T = \emptyset$. Auf diese Weise finden wir ein $\tilde{x} \in \mathbb{Q}^\times$ mit $(a_i, \tilde{x})_v = \tilde{\epsilon}_{i,v}$ für alle $v \in V$ und alle i. Wir definieren nun ein Element $x := \tilde{x}y \in \mathbb{Q}^\times$ und zeigen, dass es für unsere ursprünglichen Werte $\epsilon_{i,v}$ die Bedingung $(a_i, x)_v = \epsilon_{i,v}$ erfüllt. Es gilt

$$(a_i, x)_v = (a_i, \tilde{x}y)_v = (a_i, \tilde{x})_v (a_i, y)_v = \tilde{\epsilon}_{i,v}(a_i, y)_v = \frac{\tilde{\epsilon}_{i,v}}{(a_i, y)_v} = \epsilon_{i,v}$$

und somit $(a_i, x)_v = \epsilon_{i,v}$ für alle $v \in V$ und $i = 1, \ldots, n$. □

4 Quadratische Formen

In diesem Abschnitt entwickeln wir die Theorie der quadratischen Formen. Eine solche Form kann zum Beispiel durch ein Polynom $f(X) = aX_1^2 + bX_1X_2 + cX_3^2$ mit Koeffizienten in einem Körper k und $X = (X_1, X_2, X_3)$ in einem Vektorraum $M \cong k^3$ dargestellt werden.

4.1 Allgemein

Definition 4.1. Sei M ein Vektorraum über einem Körper k der Charakteristik $\mathrm{char}(k) \neq 2$. Dann ist eine **quadratische Form** auf M eine Funktion $Q\colon M \to k$ mit den Eigenschaften:

1. $Q(ax) = a^2 Q(x)$ für $a \in k$ und $x \in M$,
2. Die Abbildung $(x, y) \mapsto \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$ ist bilinear.

Wir nennen das Paar (M, Q) einen **quadratischen Raum**. Da wir an den Fällen interessiert sind, in denen der Raum M ein endlich-dimensionaler Vektorraum über einem der Körper $\mathbb{Q}$ oder $\mathbb{Q}_v$ ist, beschränken wir unsere Ausführungen im Folgenden auf quadratische Formen auf endlich-dimensionalen Vektorräumen. Anhand Punkt 2 in der Definition 4.1 können wir die mit $\mathbb{Q}$ assoziierte symmetrische Bilinearform als

$$[x, y] := \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$$

definieren. Es gilt $Q(x) = [x, x]$, und somit gibt es eine Bijektion zwischen den quadratischen Formen auf M und symmetrischen Bilinearformen auf $M \times M$. Sind zwei quadratische Räume (M, Q) und (M', Q') gegeben, so definieren wir einen **Morphismus** von (M, Q) nach (M', Q') als eine lineare Abbildung $\phi : M \to M'$ mit der zusätzlichen Eigenschaft, dass $Q' \circ \phi = Q$, also $[\phi(x), \phi(y)] = [x, y]$ gilt. Ist ϕ ein Isomorphismus von M nach M', so sprechen wir von einem **Isomorphismus** von (M, Q) nach (M', Q').

Definition 4.2. Sei $(e_i)_{i=1}^n$ eine Basis des k-Vektorraums M. Dann wird die **Darstellungsmatrix** $A = (a_{ij})$ **von** Q bezüglich dieser Basis durch die Einträge $a_{ij} = [e_i, e_j]$ definiert. Die Matrix A ist symmetrisch, da auch die Bilinearform symmetrisch ist. Somit erhalten wir den Wert von Q an $x \in M$ bezüglich der gegebenen Basis als

$$f_Q(x) := \sum_{i,j} a_{ij} x_i x_j = x^t A x,$$

wobei x^t die Transposition des Vektors x ist. Wir nennen $f_Q(X) = \sum_{i,j} a_{ij} X_i X_j$ mit einer Variablen $X = (X_1, \ldots, X_n)$ eine **Darstellung** von Q bezüglich der Basis $(e_i)_{i=1}^n$.

Wenn wir mit Hilfe einer invertierbaren Matrix B einen Basiswechsel vollziehen, dann ist die Matrix A' von Q bezüglich der neuen Basis gleich $A' := B \cdot A \cdot B^t$. Daraus folgt, dass $\det(A') = \det(A) \cdot \det(B)^2$ ist, und somit, dass $\det(A)$ ist bis auf Multiplikation mit einem Element in $k^{\times 2}$ durch Q bestimmt. Der Wert von $\det(A)$ modulo $k^{\times 2}$ ist daher invariant unter Basiswechsel, und wir nennen ihn die **Diskriminante** $\mathrm{d}(Q) := \det(A) \pmod{k^{\times 2}}$ von Q.

Definition 4.3. Sei (M, Q) ein quadratischer Raum über k. Zwei Elemente $x, y \in M$ heißen **orthogonal**, falls $[x, y] = 0$ gilt. Wir bezeichnen die Menge aller Elemente, die orthogonal zu einer Untermenge H von M sind, als das **orthogonale Komplement** $H^\perp$ von H. Das orthogonale Komplement $M^\perp$ des Vektorraums M wird auch als **Kern** $\ker(Q)$ der quadratischen Form Q bezeichnet. Darüber hinaus nennen wir zwei Unterräume M_1 und M_2 von M **orthogonal**, wenn $M_1 \subset M_2^\perp$ (und somit $M_2 \subset M_1^\perp$) ist.

Definition 4.4. Wir bezeichnen eine Basis $(e_i)_{i=1}^n$ eines quadratischen Moduls (M, Q) als **orthogonale Basis**, wenn ihre Elemente paarweise orthogonal sind. In diesem Fall können wir M als die direkte Summe $M = ke_1 \oplus \ldots \oplus ke_n \cong k^n$ schreiben, und die Matrix A von Q bezüglich dieser Basis nimmt eine diagonale Form an:

$$\begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & a_n \end{pmatrix}$$

Wir erhalten folglich die Darstellung $f_Q(X) = a_1 X_1^2 + \ldots + a_n X_n^2$ bezüglich dieser orthogonalen Basis.

Satz 4.5. *Für jeden quadratischen Raum (M, Q) existiert eine orthogonale Basis. Somit hat jede quadratische Form Q eine Darstellung der Form $f_Q(X) = a_1 X_1^2 + \ldots + a_n X_n^2$ mit $a_i \in k$.*

Beweis. Wir beweisen den Satz durch eine Induktion nach der Dimension $\dim(M) =: n$ des Vektorraums M. Die Induktionsverankerung durch $n = 0$ ist trivial. Sei also $n > 0$ und nehmen wir an, dass jeder quadratische Raum mit Dimension $< n$ eine orthogonale Basis hat. Gilt $Q(x) = 0$ für alle $x \in M$, so ist jede Basis $(e_i)_{i=1}^n$ von M orthogonal, denn es gilt $[e_i, e_j] = 0$ für alle $i, j \in \{1, \ldots, n\}$. Sonst wählen wir ein Element $e_n \in M$ sodass $Q(e_n) = [e_n, e_n] \neq 0$. Das orthogonale Komplement H von ke_n bestehend aus Vektoren $x \in M$ mit $[e_n, x] = 0$ ist ein $(n-1)$-dimensionaler Unterraum, und wir können $M = H \oplus ke_n$ schreiben. Der Raum H hat nach Induktionsannahme eine orthogonale Basis $(e_i)_{i=1}^{n-1}$. Da e_n orthogonal zu allen $e_1, \ldots, e_{n-1}$ ist, ergibt die Basis $(e_1, \ldots, e_n)$ eine orthogonale Basis von M.

Aus Definition 4.4 folgt, dass somit jede quadratische Form Q eine Darstellung der Form $f_Q(X) = a_1 X_1^2 + \ldots + a_n X_n^2$ mit $a_i \in k$ besitzt. □

Definition 4.6. Wir bezeichnen eine quadratische Form Q als **ausgeartet**, wenn ihr Kern $\ker(Q)$ ungleich Null ist. Gilt jedoch $ker(Q) = 0$, so nennen wir Q **nichtausgeartet**.

Proposition 4.7. *Eine quadratische Form Q auf M ist genau dann ausgeartet, wenn für die zugehörige Diskriminante $\mathrm{d}(Q) = 0$ gilt.*

Beweis. Sei Q ausgeartet und $(e_i)_{i=1}^n$ eine orthogonale Basis von M, sodass $e_n \in M^\perp$ und somit $[e_n, e_n] = 0$ ist. Die Matrix A von Q bezüglich dieser Basis ist diagonal mit Diagonaleinträgen $a_{ii} = [e_i, e_i]$ für $i = 1, \ldots, n$. Demnach erhalten wir $\det(A) = 0$ und $\mathrm{d}(Q) = 0$. Ist hingegen $\mathrm{d}(Q) = 0$, so gilt für die Matrix A bezüglich einer orthogonalen Basis $(e_i)_{i=1}^n$, dass $\det(A) = 0$ ist. Demnach ist einer der Diagonaleinträge $a_{ii} = [e_i, e_i] = 0$. Daraus folgt $Q(e_i) = 0$ und somit für alle $x = (x_1, \ldots, x_n)^t \in M$, dass

$$\begin{aligned} [e_i, x] &= \frac{1}{2}\left(Q(x + e_i) - Q(x) - Q(e_i)\right) \\ &= \frac{1}{2}\left((x_1, \ldots, x_i + 1, \ldots, x_n)^t A (x_1, \ldots, x_i + 1, \ldots, x_n) - Q(x)\right) \\ &= \frac{1}{2}\left(Q(x) - Q(x)\right) = 0 \end{aligned}$$

gilt. Der letzte Schritt folgt daraus, dass $a_{ii} = 0$ ist, und daher der i-te Eintrag von x irrelevant ist. Die Form Q ist folglich ausgeartet. □

Eine Konsequenz daraus ist, dass die Diskriminante $\mathrm{d}(Q) \neq 0$ einer nichtausgearteten Form Q als Element in $k^\times/k^{\times 2}$ ausgedrückt werden kann.

Definition 4.8. Der **Rang** $\mathrm{Rg}(Q)$ einer quadratischen Form Q auf M ist der Rang der zugehörigen Matrix A.

Ist Q nicht ausgeartet, gilt also $\mathrm{Rg}(Q) = \dim(M)$. Da wir nach Definition 4.4 und Satz 4.5 für den Vektorraum $M \cong k^n$ erhalten, werden wir von nun an nur noch quadratische Formen über k^n betrachten.

Definition 4.9 (Äquivalenz)**.** Wir nennen zwei quadratische Formen Q und Q' bzw. deren Darstellungen f und f' bezüglich einer gegebenen Basis **äquivalent**, wenn die jeweiligen Räume (k^n, Q) und $(k^{n'}, Q')$ isomorph sind. Das heißt, es gibt einen Isomorphismus $\phi : k^n \to k^{n'}$, sodass $Q' \circ \phi = Q$ (und somit $n = n'$) gilt. Wir schreiben $Q \sim Q'$ bzw. $f \sim f'$.

Beispiel 4.10. Seien f und g Darstellungen quadratischer Formen bezüglich derselben Basis.

1. $f(X) = X_1^2 - X_2^2 = (X_1 - X_2)(X_1 + X_2)$ ist äquivalent zu $g(X) = X_1X_2$ durch
$$f(X) = g\left(\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} X_1 \\ X_2 \end{pmatrix}\right).$$
2. Für alle $a, b \in k$ gilt $f(X) := aX_1^2 \sim bX_1^2 =: g(X)$ genau dann, wenn ein $c \in k^\times$ existiert, sodass $a = bc^2$ ist:
$$f(X) = aX_1^2 = bc^2X_1^2 = g(cX).$$
3. Sei f eine Form von Rang n und $a \in k^\times$ ein Skalar. Dann ist $a^2f \sim f$ durch $a^2f(X) = f((a \cdot I_n) \cdot X)$, wobei I_n die $(n \times n)$-Identitätsmatrix über k bezeichnet.

Ein Isomorphismus $\phi : k^n \to k^n$ zweier äquivalenter quadratischer Formen Q und Q' auf n Variablen ist einfach ein Basiswechsel. Somit gilt auch für die zu den Formen gehörigen Diskriminanten $\mathrm{d}(Q)$ und $\mathrm{d}(Q')$, dass $\mathrm{d}(Q) = \mathrm{d}(Q')$ in $k^\times/k^{\times 2}$ oder $\mathrm{d}(Q) = \mathrm{d}(Q') = 0$ ist.

Sei nun $f(X) = \sum_{i=1}^n a_{ii}X_i^2 + 2\sum_{i<j} a_{ij}X_iX_j$ die Darstellung einer quadratischen Form in n Variablen über k, wobei wir durch Basiswechsel $a_{ij} = a_{ji}$ für $i < j$ setzen können, sodass die dazugehörige Matrix $A = (a_{ij})_{i,j=1}^n$ symmetrisch ist. Der entsprechende quadratische Raum ist das Tupel (k^n, f). Wir unterscheiden im Folgenden in der Bezeichnung nicht mehr zwischen einer quadratischen Form und deren Darstellung bezüglich einer Basis.

Definition 4.11. Wir sagen, dass eine quadratische Form f ein **Element a in k darstellt**, wenn es ein $x \neq 0$ in k^n gibt, sodass $f(x) = a$ ist. Gilt $f(x) = 0$ nur für $x = 0$, so sagen wir, dass f die Null nur **auf triviale Weise darstellt**.

Aus Definition 4.9 geht hervor, dass f genau dann ein Element $a \in k$ auf nichttriviale Weise darstellt, wenn das auch für alle äquivalenten Formen von f gilt.

Definition 4.12. Wir nennen eine quadratische Form f **isotrop**, wenn es ein $x \in k^n$ mit $x \neq 0$ gibt, sodass $f(x) = 0$ ist. Das heißt, die Form f stellt die Null nichttrivial dar.

Für eine ausgeartete quadratische Form geschrieben als $f(X) = a_1X_1^2 + \ldots + a_nX_n^2$ ist mindestens einer der Koeffizienten, sagen wir a_n, gleich Null. Somit existiert eine Nullstelle $x := (0, \ldots, 0, 1) \in k^n$ mit $f(x) = 0$. Das bedeutet, dass jede ausgeartete quadratische Form isotrop ist. Daher werden wir uns im restlichen Abschnitt vor allem auf nichtausgeartete Formen beziehen, um herauszufinden, unter welchen Umständen diese isotrop sind.

Proposition 4.13. *Eine nichtausgeartete quadratische Form $f = a_1X_1^2$ von Rang 1 ist nicht isotrop.*

Beweis. Es gilt $f(X) = 0 \Leftrightarrow a_1X_1^2 = 0 \Leftrightarrow X_1^2 = 0 \Leftrightarrow X_1 = 0$. Die Form f stellt die Null also nur auf triviale Weise dar. □

Satz 4.14. *Sei f eine nichtausgeartete quadratische Form, welche isotrop ist. Dann stellt f jedes Element in k dar.*

Beweis. Sei $f(X) = a_1X_1^2 + \ldots + a_nX_n^2$ mit $a_1, \ldots, a_n \in k^\times$ und a ein beliebiges Element in k. Nach Annahme existiert ein $x = (x_1, \ldots, x_n) \in k^n, x \neq 0$, sodass $f(x) = a_1x_1^2 + \ldots + a_nx_n^2 = 0$ ist. Nach eventueller Umnummerierung können wir annehmen, dass $x_1 \neq 0$ gilt. Für ein beliebiges $t \in k$ definieren wir basierend auf x ein neues Element $y = (y_1, \ldots, y_n) \in k^n$ mit $y \neq 0$ als $y_1 := x_1(1+t)$ und $y_i := x_i(1-t)$ für $i \geq 2$. Wir erhalten

$$\begin{aligned} f(y) &= a_1y_1^2 + \ldots + a_ny_n^2 \\ &= a_1x_1^2(1 + 2t + t^2) + a_2x_2^2(1 - 2t + t^2) \ldots + a_nx_n^2(1 - 2t + t^2) \\ &= (1 + t^2)(a_1x_1^2 + \ldots + a_nx_n^2) + 2t(a_1x_1^2 - (a_2x_2^2 + \ldots + a_nx_n^2)) \\ &= 2t(a_1x_1^2 - (-a_1x_1^2)) \\ &= 4ta_1x_1^2. \end{aligned}$$

Wir setzen $t = a/4a_1x_1^2$ und erhalten somit $f(y) = a$. □

Wir definieren nun eine Verknüpfung der quadratischen Formen. Seien $f(X_1, X_2, \ldots, X_n)$ und $g(X_1, X_2, \ldots, X_m)$ zwei quadratische Formen. Dann definieren wir

$$\begin{aligned} f \dot{+} g &:= f(X_1, X_2, \ldots, X_n) + g(X_{n+1}, X_{n+2}, \ldots, X_{n+m}) \\ f \dot{-} g &:= f(X_1, X_2, \ldots, X_n) - g(X_{n+1}, X_{n+2}, \ldots, X_{n+m}) \end{aligned}$$

als quadratische Formen in $n + m$ Variablen. Somit erhalten wir aus Satz 4.14 folgendes Korollar.

Korollar 4.15. *Seien g und h zwei nichtausgeartete quadratische Formen, deren Rang ≥ 1 ist, und sei $f = g \dot{-} h$. Dann sind folgende Eigenschaften äquivalent:*

1. *Die Form f ist isotrop.*
2. *Es existiert ein Element a in $k^\times$, welches sowohl von g als auch von h dargestellt wird.*
3. *Es existiert ein Element a in $k^\times$, sodass $g \dot{-} aZ^2$ und $h \dot{-} aZ^2$ beide isotrop sind, wobei Z eine weitere Variable über k ist.*

Beweis. 1. $\Rightarrow$ 2.: Sei $f(X) = g(X_1, \ldots, X_r) - h(X_{r+1}, \ldots, X_n)$ isotrop. Dann existiert ein $x \in k^n$ mit $x \neq 0$, sodass $f(x) = g(x_1, \ldots, x_r) - h(x_{r+1}, \ldots, x_n) = 0$ und somit $g(x_1, \ldots, x_r) = h(x_{r+1}, \ldots, x_n) =: a \in k$ ist. Gilt $a \neq 0$, so ist 2. erfüllt. Ist hingegen $a = 0$, so stellt zumindest eine der beiden Formen g und h die Null nichttrivial dar, sagen wir g. Nach Satz 4.14 stellt g alle $b \in k$ dar, und somit auch alle Werte in $k^\times$, die von h dargestellt werden. Somit existiert ein $b \in k^\times$, das sowohl von g als auch von h dargestellt wird.
2. $\Rightarrow$ 3.: Sei $a \in k^\times$ ein Element, das von g und h dargestellt wird. Das heißt, es existiert ein $x \in k^r$, sodass $g(x) = a$ ist. Folglich gilt $g(x) - a1^2 = 0$, und wir erhalten eine quadratische Form $\tilde{g} = g \dot{-} aZ^2$, welche isotrop ist. Analog erhalten wir eine isotrope Form $\tilde{h} = h \dot{-} aZ^2$.
3. $\Rightarrow$ 1.: Sei a in $k^\times$, sodass $g \dot{-} aZ^2$ und $h \dot{-} aZ^2$ beide isotrop sind. Es gibt für g also ein Element $(x, z) = (x_1, \ldots, x_r, z) \in k^{r+1}$, sodass $g(x) - az^2 = 0$ ist. Gilt $z = 0$, so ist g isotrop. Sonst ist $(x_1/z, \ldots, x_r/z, 1)$ ebenfalls eine Nullstelle von $g \dot{-} aZ^2$, und es gilt $g(x_1/z, \ldots, x_r/z) = a$. Wir gehen analog für $h \dot{-} aZ^2$ vor und erhalten ebenso entweder eine Nullstelle $(x_{r+1}, \ldots, x_n, 0) \in k^{n-r+1}$, sodass h isotrop ist, oder ein Element $(x_{r+1}/\tilde{z}, \ldots, x_n/\tilde{z}, 1) \in k^{n-r+1}$, sodass $h((x_{r+1}/\tilde{z}, \ldots, x_n/\tilde{z}) = a$ ist. Nun zeigen wir, dass in allen diese Fällen f isotrop ist. Sind g und h beide isotrop, so folgt daraus direkt, dass $f = g \dot{-} h$ auch isotrop ist. Wenn hingegen nur g und nicht h isotrop ist, dann stellt g nach Satz 4.14 alle Elemente in $k^\times$ dar, also auch alle, die von h dargestellt werden. Somit ist $f = g \dot{-} h$ auch in diesem Fall isotrop. Gilt für g als auch h, dass sie nicht isotrop sind, dann stellen beide das Element $a \in k^\times$ dar. So ist auch in diesem Fall $f(x_1/z, \ldots, x_r/z, x_{r+1}/\tilde{z}, \ldots, x_n/\tilde{z}) = a - a = 0$ und f isotrop. □

Satz 4.16. *Sei $f = a_1X_1^2 + \ldots + a_nX_n^2$ eine quadratische Form in n Variablen, welche das Element $a \in k^\times$ darstellt. Dann ist f äquivalent zu einer Form*

$$aX_1^2 + g(X_2, \ldots, X_n),$$

wobei g eine quadratische Form in $n-1$ Variablen ist.

Beweis. Die Idee des Beweises ist, dass wir ausgehend von einem Vektor $y = (y_1, \ldots, y_n) \in k^n \backslash \{0\}$ mit $f(y) = a$ eine invertierbare Matrix S mit diesem Vektor als erste Spalte bilden können, und aus dieser Matrix die zu f äquivalente Form $f'(X) := f(SX) = f(y)X_1^2 + h(X_1, \ldots, X_n)$ erhalten, wobei die Form h sich aus den restlichen Termen von $f(SX)$ ergibt. Die Form f' hat folglich das Element a als Koeffizient für X_1^2. Durch eine Substitution kann man die Mischterme X_1X_i mit $i \neq 1$ entfernen und erhält somit eine quadratische Form $f''(X) := aX_1^2 + g(X_2, \ldots, X_n) \sim f$, wobei g eine quadratische Form in $n-1$ Variablen ist. Die Details dieses Spiels mit Matrizen kann die Leserin in [9] auf S. 183 nachlesen. □

Satz 4.17. *Seien f, f' auf k^n und g auf k^r quadratische Formen. Ist $f \sim f'$, so gilt $f \dot{+} g \sim f' \dot{+} g$.*

Beweis. Sei A die $n \times n-$Matrix, sodass $f(X) = f'(AX)$ gilt. Sei I_r die $(r \times r)$-Identitätsmatrix. Wir definieren eine neue Matrix

$$B := \begin{pmatrix} A & 0 \\ 0 & I_r \end{pmatrix}.$$

Dann gilt $(f \dot{+} g)(X) = (f' \dot{+} g)(BX)$, und daher ist $f \dot{+} g \sim f' \dot{+} g$. □

Definition 4.18. Seien $f(X) = a_1X_1^2 + \ldots + a_nX_n^2$ und $g(X) = b_1X_1^2 + \ldots + b_nX_n^2$ quadratische Formen. Man nennt f und g **benachbart**, wenn sie die folgende Bedingung erfüllen:

- Es gibt zwei Indizes $i \neq \ell$, sodass $a_j = b_j$ für alle $j \notin \{i, \ell\}$ und $a_iX_i^2 + a_\ell X_\ell^2 \sim b_iX_i^2 + b_\ell X_\ell^2$ gilt.

Sind f und g vom Rang 1, so bezeichnen wir sie als benachbart, wenn $a_1X_1^2 \sim b_1X_1^2$ ist.

Benachbarte Formen sind äquivalent zueinander. Umgekehrt gilt folgender Satz:

Satz 4.19 (Witt'scher Kettenäquivalenzsatz)**.** *Sind f und g zwei äquivalente quadratische Formen, so existiert eine Kette $f_0, \ldots, f_m$ von quadratischen Formen, sodass*

1. *$f_0 = f$ und $f_m = g$,*
2. *f_i und f_{i+1} sind benachbart für alle $i = 0, \ldots, m-1$.*

Beweis. Da wir diesen Satz nur für einen Schritt im Beweis von Satz 4.23 brauchen und der Beweis selber nicht sonderlich erleuchtend ist, skizzieren wir ihn hier nur und verweisen den Leser für Details auf [9] S. 187. Existiert eine Kette von $f(X) = a_1X_1^2 + \ldots + a_nX_n^2$ nach $g(X) = b_1X_1^2 + \ldots + b_nX_n^2$ wie im Satz beschrieben, so nennen wir f und g *kettenäquivalent* und schreiben $f \approx g$. Der Beweis dieses Satzes beruht auf Induktion über den Rang n der Formen f und g, wobei wir diese ohne Beschränkung der Allgemeinheit als nichtausgeartet annehmen können. Für $n = 1, 2$ folgt die Aussage direkt aus Definition 4.18. Für $n \geq 3$ folgt aus der Äquivalenz von f und g, dass f den ersten Koeffizienten b_1 von g darstellt. Unter den zu f kettenäquivalenten Formen können wir damit eine Form $f' := c_1X_1^2 + \ldots + c_nX_n^2$ mit minimalem $r \leq n$ finden, sodass $c_1X_1^2 + \ldots + c_rX_r^2$ auch b_1 darstellt. Durch einen Widerspruchsbeweis ergibt sich $r = 1$ und somit $c_1X_1^2 \sim b_1X_1^2$. Daraus folgt $f' = c_1X_1^2 + c_2X_2^2 + \ldots + c_nX_n^2 \approx b_1X_1^2 + c_2X_2^2 + \ldots + c_nX_n^2 =: g'$, und nach Induktionsannahme erhalten wir $c_2X_2^2 + \ldots + c_nX_n^2 \approx b_2X_2^2 + \ldots + b_nX_n^2$. Daraus folgt $f \approx f' \approx g' \approx g$. □

4.2 Quadratische Formen über $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{Q}_p$

Der Satz von Hasse-Minkowski dient dem besseren Verständnis quadratischer Formen über $\mathbb{Q}$ durch solche über den Körpern $\mathbb{Q}_v$. Dies ist nur hilfreich, wenn wir über letztere Aussagen treffen können. Diese werden wir in diesem Abschnitt besprechen. Über die Darstellung von Formen über $\mathbb{Q}$ und $\mathbb{R}$ können wir davor noch folgende Aussage treffen.

Definition 4.20. Wir bezeichnen eine Zahl $a \in \mathbb{Z}$ als **quadratfrei**, wenn a nicht durch ein Quadrat ungleich 1 in $\mathbb{Z}$ teilbar ist – das heißt, wenn $a \neq 0$ ist und ihre Primfaktorisierung $a = p_1 p_2 \cdots p_k$ mit $p_1, \ldots, p_k$ prim keine Primzahl mehrfach enthält.

Proposition 4.21.
- *Jede nichtausgeartete quadratische Form f über $\mathbb{Q}$ von Rang n ist äquivalent zu einer Form $\tilde{f}(X) = b_1 X_1^2 + \ldots + b_n X_n^2$ mit $b_1, \ldots, b_n \in \mathbb{Z}\backslash\{0\}$ quadratfreie ganze Zahlen.*
- *Jede nichtausgeartete quadratische Form f über $\mathbb{R}$ von Rang n ist äquivalent zu einer Form $\tilde{f}(X) = b_1 X_1^2 + \ldots + b_n X_n^2$ mit $b_1, \ldots, b_n \in \{\pm 1\}$.*

Beweis. Sei f eine nichtausgeartete quadratische Form vom Rang n über $\mathbb{Q}$. Aus Satz 4.5 und Proposition 4.7 folgt die Äquivalenz von f zu einer Form der Gestalt $f'(X) = a_1 X_1^2 + \ldots + a_n X_n^2$ mit $a_1, \ldots, a_n \in \mathbb{Q}^\times$. Wir schreiben die Koeffizienten als $a_i = r_i/s_i$ für $i = 1, \ldots, n$, wobei r_i und $s_i \in \mathbb{Z}$ keine gemeinsamen Teiler besitzen. Wir multiplizieren f' mit $k := \prod_{i=1}^n s_i^2$ und erhalten die Form $g := kf'$ mit ganzzahligen Koeffizienten $\tilde{a}_i \in \mathbb{Z}$. Da k ein Quadrat ist, gilt auch $g \sim f'$ (siehe Beispiel 4.10 (3.)). Nun können wir die Koeffizienten von g als $\tilde{a}_i = b_i c_i^2$ mit $b_i, c_i \in \mathbb{Z}$ schreiben, wobei b_i für alle i quadratfrei ist. Nach Beispiel 4.10 (2.) gilt für alle i, dass $\tilde{a}_i X_i^2 \sim b_i X_i^2$ und demnach $g(X) = \tilde{a}_1 X_1^2 + \ldots + \tilde{a}_n X_n^2 \sim b_1 X_1^2 + \ldots + b_n X_n^2 =: \tilde{f}(X)$ ist. Die Form $\tilde{f}$ hat quadratfreie ganzzahlige Koeffizienten, und es gilt $f \sim \tilde{f}$.

Sei nun $f \sim a_1 X_1^2 + \ldots + a_n X_n^2$ eine nichtausgeartete quadratische Form über $\mathbb{R}$. Da alle positiven Zahlen in $\mathbb{R}$ Quadrate sind, können wir jede reelle Zahl als Produkt von ± 1 und einem Quadrat und somit alle Koeffizienten als $a_i = \pm c_i^2$ schreiben. Analog zum ersten Teil des Beweises können wir den quadratischen Faktor c_i^2 für alle i herausdividieren und erhalten eine zu f äquivalente Form $\tilde{f}(X) := \pm X_1^2 \pm \ldots \pm X_n^2$. □

Wir betrachten nun nichtausgeartete quadratische Formen f über den reellen Zahlen $\mathbb{R}$ bzw. den p-adischen Körpern $\mathbb{Q}_p$ und arbeiten einige Kriterien aus, welche Einblick geben, wann eine solche Form isotrop über dem jeweiligen Körper ist. Im restlichen Abschnitt sei daher mit einer quadratischen Form immer eine *nichtausgeartete* quadratische Form gemeint. Wir beginnen damit, Invarianten der quadratischen Formen über $\mathbb{R}$ und dann über $\mathbb{Q}_p$ auszuarbeiten.

Sei f eine quadratische Form von Rang n über den reellen Zahlen $\mathbb{R}$. Wir wissen aus Proposition 4.21, dass f äquivalent ist zu

$$a_1 X_1^2 + \ldots + a_n X_n^2$$

mit $a_i \in \{\pm 1\}$. Daher können wir f als

$$X_1^2 + \ldots + X_r^2 - Y_1^2 - \ldots - Y_s^2$$

schreiben, wobei r und s ganze Zahlen sind, sodass $r + s = n$ ist. Das Tupel (r, s) wird durch f eindeutig bis auf Vertauschen von r und s bestimmt. Einen Beweis zur Eindeutigkeit findet der Leser in [9] auf S. 189f. Das Tupel (r, s) ist also eine Invariante der Äquivalenzklasse von f und wird als die **Signatur** von f bezeichnet. Außerdem bezeichnen wir f als **definit**, wenn entweder r oder $s = 0$ ist. In diesem Fall ist f nicht isotrop, da die Summe von Quadraten ungleich Null in $\mathbb{R}$ nicht Null ergeben kann. Ansonsten sind $r, s \geq 1$, und wir nennen f **indefinit**. Jede indefinite Form ist isotrop – man wähle zum Beispiel $X_1 = 1 = Y_1$ und 0 für alle anderen Variablen – und stellt somit nach Satz 4.14 jedes Element in $\mathbb{R}$ dar.

Sei wieder $V = \{p \in \mathbb{Z} |\ p \text{ prim}\} \cup \{\infty\}$. Wie wir in Abschnitt 4.1 herausgearbeitet haben, ist die *Diskriminante* einer quadratischen Form eine Invariante ihrer Äquivalenzklasse. Ist $f(X) \sim a_1 X_1^2 + \ldots + a_n X_n^2$ eine Form über $\mathbb{Q}_v$, so bezeichnen wir ihre Diskriminante als $\mathrm{d}_v(f)$ und können diese schreiben als

$$\mathrm{d}_v(f) = a_1 \cdots a_n \text{ modulo } \mathbb{Q}_v^{\times 2}.$$

Ist die Signatur einer Form f über $\mathbb{R}$ durch (r,s) gegeben, so gilt $f \sim X_1^2 + \ldots + X_r^2 - Y_1^2 - \ldots - Y_s^2$ und für die Diskriminante folglich $\mathrm{d}_\infty(f) = (-1)^s$.

Eine weitere Invariante quadratischer Formen über $\mathbb{Q}_v$ ist die sogenannte Hasse-Invariante.

Definition 4.22. Sei $(a,b)_v \in \{\pm 1\}$ das Hilbert-Symbol über $\mathbb{Q}_v$. Wir definieren die **Hasse-Invariante** einer quadratischen Form $f \sim a_1X_1^2 + \ldots + a_nX_n^2$ über $\mathbb{Q}_v$ als

$$\epsilon_v(f) := \prod_{i<j} (a_i, a_j)_v.$$

Satz 4.23. *Die Hasse-Invariante ist tatsächlich eine Invariante einer Äquivalenzklasse quadratischer Formen über $\mathbb{Q}_v$ und wohldefiniert. Das heißt, zwei äquivalente quadratische Formen $f(X) \sim a_1X_1^2 + \ldots + a_nX_n^2$ und $g(X) \sim b_1X_1^2 + \ldots + b_nX_n^2$ über $\mathbb{Q}_v$ für ein $v \in V$ haben dieselbe Hasse-Invariante $\epsilon_v(f) = \epsilon_v(g)$.*

Beweis. Seien f und g zwei äquivalente quadratische Formen über $\mathbb{Q}_v$ von Rang n. Ist $n = 1$, so erhalten wir als Hasse-Invariante für beide Formen ein leeres Produkt, welches per Konvention gleich 1 ist. Wenn $n = 2$ ist, gilt für die Form f die Bedingung $\epsilon_v(f) = (a_1, a_2)_v = 1$ genau dann, wenn die Gleichung $Z^2 - a_1X^2 - a_2Y^2 = 0$ eine nichttriviale Lösung über $\mathbb{Q}_v$ hat – das heißt, genau dann, wenn die Form $Z^2 \dot{-} f$ isotrop ist. Da $f \sim g$ ist, gilt nach Satz 4.17, dass $Z^2 \dot{-} f \sim Z^2 \dot{-} g$ ist. Folglich ist $Z^2 \dot{-} g = Z^2 - b_1X^2 - b_2Y^2 = 0$ ebenfalls isotrop. Das ist genau dann der Fall, wenn $\epsilon_v(g) = (b_1, b_2) = 1$ ist. Somit haben wir für $n = 2$ gezeigt, dass $\epsilon_v(f) = \epsilon_v(g)$ ist.

Wir beweisen die restlichen Fälle $n \geq 3$ durch eine Induktion über n. Die Induktionsverankerung ist durch den Fall $n = 2$ gegeben. Sei nun der Rang der Formen f und g gleich $n \geq 3$ und die Hasse-Invariante für alle äquivalenten Formen von Rang $< n$ gleich. Die Formen f und g sind äquivalent und daher nach Satz 4.19 durch eine Kette benachbarter Formen $f = f_0, \ldots, f_m = g$ verbunden. Es genügt daher zu zeigen, das die Hasse-Invariante für zwei benachbarte Formen f und g gleich ist. Seien also f und g benachbarte Formen. Wir können nach Permutation der Indizes annehmen, dass $a_i = b_i$ für alle $i \geq 3$ und $f' := a_1Y^2 + a_2Z^2 \sim b_1\tilde{Y}^2 + b_2\tilde{Z}^2 =: g'$ gilt. Nach Induktionsannahme ist $\epsilon_v(f') = \epsilon_v(g')$ und daher $(a_1, a_2)_v = (b_1, b_2)_v$. Aus $f' \sim g'$ und somit $\mathrm{d}_v(f') = \mathrm{d}_v(g')$ in $\mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}$ folgt außerdem, dass $a_1a_2 = b_1b_2c^2$ für ein $c \in \mathbb{Q}_v^\times$ ist. Folglich erhalten wir

$$\begin{aligned}
\epsilon_v(f) = \prod_{i<j} (a_i, a_j)_v &= (a_1, a_2)_v (a_1, a_3 \cdots a_n)_v (a_2, a_3 \cdots a_n)_v \prod_{3 \leq i < j} (a_i, a_j)_v \\
&= (a_1, a_2)_v (a_1a_2, a_3 \cdots a_n)_v \prod_{3 \leq i < j} (a_i, a_j)_v \\
&= (b_1, b_2)_v (b_1b_2, b_3 \cdots b_n)_v \prod_{3 \leq i < j} (b_i, b_j)_v \\
&= \prod_{i<j} (b_i, b_j)_v = \epsilon_v(g),
\end{aligned}$$

und die Behauptung ist bewiesen. □

Da jede Form f über $\mathbb{R}$ zu einer Form mit Koeffizienten in $\{\pm 1\}$ äquivalent ist, folgt aus Satz 4.23, dass für jede quadratische Form über den reellen Zahlen die Hasse-Invariante von der Form $\epsilon_\infty(f) = \prod(\pm 1, \pm 1)_\infty$ ist. Wir erinnern uns, dass nach Satz 3.8 für das Hilbert-Symbol $(1,1)_\infty = (1,-1)_\infty = (-1,1)_\infty = 1$ und $(-1,-1)_\infty = -1$ gilt. Daraus folgt, dass die Diskriminante und die Hasse-Invariante für quadratische Formen f über $\mathbb{R}$ folgende Werte annehmen:

$$\mathrm{d}_\infty(f) = (-1)^s = \begin{cases} 1 & \text{für } s \equiv 0 \pmod 2 \\ -1 & \text{für } s \equiv 1 \pmod 2 \end{cases}$$

$$\epsilon_\infty(f) = (-1)^{s(s-1)/2} = \begin{cases} 1 & \text{für } s \equiv 0,1 \pmod 4 \\ -1 & \text{für } s \equiv 2,3 \pmod 4. \end{cases}$$

Wir kennen die Werte von $\mathrm{d}_\infty(f)$ und $\epsilon_\infty(f)$ somit genau dann, wenn wir den Wert von s modulo 4 kennen. Wenn der Rang der Form f also ≤ 3 ist, können wir von den beiden Invarianten direkt f selbst (bis auf Äquivalenz) bestimmen.

Beispiel 4.24. Sei f eine quadratische Form über $\mathbb{R}$ von Rang $n = 3$ mit Diskriminante $\mathrm{d}_\infty(f) = 1$ und Hasse-Invariante $\epsilon_\infty(f) = -1$. Somit gilt $s \equiv 0 \pmod 2$ und $s \equiv 2, 3 \pmod 4$. Da der Rang $n \leq 4$ ist, folgt daraus, dass $s = 2$ und $f \sim X_1^2 - X_2^2 - X_3^2$ ist.

Wir untersuchen nun, wann eine quadratische Form f über $\mathbb{Q}_p$ für p prim isotrop ist. Dafür lassen sich Bedingungen aus den beiden Invarianten

$$\begin{aligned} \mathrm{d}_p(f) &= a_1 \cdots a_n \mod \mathbb{Q}_p^{\times 2} \\ \epsilon_p(f) &= \prod_{i<j} (a_i, a_j)_p \end{aligned}$$

der Äquivalenzklasse von f ableiten, welche wir in Satz 4.26 zeigen werden. Dafür benötigen wir folgendes Lemma, welches wir aus Korollar 3.9 erhalten.

Lemma 4.25. *Seien $a, a' \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ für eine Primzahl p und $\eta, \eta' \in \{\pm 1\}$. Wir definieren $H_a^\eta := \{b \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \mid (a,b)_p = \eta\}$ und setzen $r := 2$ für $p \neq 2$ und $r := 3$ für $p = 2$. Dann gilt Folgendes:*

1. *Die Menge H_1^1 hat $|\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}| = 2^r$ Elemente, und es gilt $H_1^{-1} = \emptyset$.*
2. *Für $a \neq 1$ hat H_a^η genau 2^{r-1} Elemente.*
3. *Sind H_a^η und $H_{a'}^{\eta'}$ nichtleer, dann gilt*

$$H_a^\eta \cap H_{a'}^{\eta'} = \emptyset \Leftrightarrow a = a' \text{ und } \eta = -\eta'.$$

Beweis. 1. Dies folgt direkt aus Proposition 3.5 (5.) und Lemma 3.6.

2. Für alle Elemente $x \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ gilt $x^2 = 1$. Wir können daher $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ als Vektorraum über $\mathbb{Z}/2\mathbb{Z}$ mit der Skalarmultiplikation $k \cdot x = x^k$ für $k \in \mathbb{Z}/2\mathbb{Z}$ betrachten. Nach Lemma 3.6 enthält dieser genau 2^r Elemente mit $r = 2$ für $p \neq 2$ und $r = 3$ für $p = 2$. Für $a \neq 1$ definieren wir den Homomorphismus

$$\begin{aligned} H_a : \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} &\longrightarrow \{\pm 1\} \\ b &\mapsto (a,b)_p \end{aligned}$$

Da a kein Quadrat ist, muss H_a surjektiv sein. Der Kern H_a^1 hat daher 2^{r-1} Elemente – ebenso sein Komplement H_a^{-1}.

3. Seien nach Annahme $H_a^\eta, H_{a'}^{\eta'} \neq \emptyset$, mit $H_a^\eta \cap H_{a'}^{\eta'} = \emptyset$. Ist $a = 1$, so folgt aus $H_a^\eta \neq \emptyset$ und 1., dass $H_a^\eta = \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ und somit $H_{a'}^{\eta'} = \emptyset$ ist – ein Widerspruch zur Annahme. Analoges gilt für $a' = 1$, somit können wir $a, a' \neq 1$ annehmen. Es folgt aus 2., dass H_a^η und $H_{a'}^{\eta'}$ jeweils 2^{r-1} Elemente enthalten. Demnach gilt $H_a^\eta \cup H_{a'}^{\eta'} = \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$. Unter Betrachtung des obigen Homomorphismus folgt somit $H_a^\eta = H_{a'}^{-\eta'}$. Gilt $\eta = \eta'$, so erhalten wir daraus $H_a^\eta \cap H_{a'}^{\eta'} = H_a^\eta \cap H_{a'}^\eta = \emptyset$. Aus 2. folgt ebenso $H_a^{-\eta} \cap H_{a'}^{-\eta} = \emptyset$, und somit gilt auch $H_a^1 \cap H_{a'}^1 = \emptyset$. Allerdings enthalten beide Mengen das Element 1, wir erhalten also einen Widerspruch. Somit gilt $\eta = -\eta'$ und $H_a^1 = H_{a'}^1$. Daraus folgt

$$\begin{aligned} &(x,a)_p = (x,a')_p \text{ für alle } x \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \\ \Leftrightarrow\ &(x, aa')_p = 1 \text{ für alle } x \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \end{aligned}$$

Aus Korollar 3.9 erhalten wir, dass $aa' = 1$ und somit $a = a'$ in $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ ist.
Sei umgekehrt $a = a'$ und $\eta = -\eta'$. Dann folgt direkt aus 2., dass $H_a^\eta \cap H_{a'}^{\eta'} = H_a^\eta \cap H_a^{-\eta} = \emptyset$.

□

Satz 4.26. *Sei nun $f(X) = a_1X_1^2 + \ldots + a_nX_n^2$ eine quadratische Form vom Rang n über $\mathbb{Q}_p$, und seien $d := \mathrm{d}_p(f)$ in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ und $\epsilon := \epsilon_p(f)$ die beiden Invarianten. Die Form f ist genau dann isotrop, wenn eine der folgenden Bedingungen zutrifft:*

1. *$n = 2$ und $d = -1$,*
2. *$n = 3$ und $(-1, -d)_p = \epsilon$,*
3. *$n = 4$ und entweder $d \neq 1$ oder $d = 1$ und $\epsilon = (-1, -1)_p$,*
4. *$n \geq 5$.*

Das bedeutet insbesondere, dass alle quadratischen Formen über $\mathbb{Q}_p$ vom Rang ≥ 5 die Null darstellen.

Bevor wir diesen Satz beweisen, schließen wir daraus noch folgendes Korollar.

Korollar 4.27. *Seien f, d und ϵ wie in Satz 4.26, und sei a ein Element in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$. Die Form f stellt a genau dann dar, wenn:*

1. *$n = 1$ und $d = a$,*
2. *$n = 2$ und $(a, -d)_p = \epsilon$,*
3. *$n = 3$ und entweder $a \neq -d$ oder $a = -d$ und $(-1, -d)_p = \epsilon$,*
4. *$n \geq 4$.*

Beweis Korollar 4.27. Sei $a \in \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$. Dann stellt $f(X) = a_1X_1^2 + \ldots + a_nX_n^2$ genau dann a dar, wenn die Form $f_a = f \dot{-} aZ^2$ isotrop ist. Für f_a gilt

$$\mathrm{d}_p(f_a) = -ad \text{ und } \epsilon_p(f_a) = (-a, d)_p\epsilon_p(f).$$

Ersteres folgt direkt. Die zweite Gleichung folgt aus

$$\epsilon_p(f_a) = \prod_{i<j}(a_i, a_j)_p \prod_i (a_i, -a)_p = \epsilon_p(f)(a_1 \cdots a_n, -a)_p = \epsilon_p(f)(-a, d)_p.$$

Zusammen mit Satz 4.26 folgen daraus die gegebenen Fälle.

$n = 1$: Die Form $f = a_1X_1^2$ stellt a genau dann dar, wenn für $\mathrm{d}_p(f_a) = -1$ gilt. Somit erhalten wir für f, dass die Bedingung $d = a$ notwendig und ausreichend ist.

$n = 2$: Die Form $f = a_1X_1^2 + a_2X_2^2$ stellt a genau dann dar, wenn $(-1, -\mathrm{d}_p(f_a))_p = \epsilon_p(f_a)$, also genau dann, wenn

$$\begin{aligned} & (-1, ad)_p = (-a, d)_p\epsilon \\ \Leftrightarrow\ & (-1, ad)_p(-a, d)_p = \epsilon \\ \Leftrightarrow\ & (-1, d)_p(-1, a)_p(-a, d)_p = (-1, a)_p(a, d)_p = (a, -d)_p = \epsilon \end{aligned}$$

gilt, und der Fall ist bewiesen.

$n = 3$: Dieser Fall folgt der selben Argumentation wie die Fälle $n = 1$ und $n = 2$.

$n \geq 4$: Die Form $f = a_1X_1^2 + \ldots + a_nX_n^2$ stellt a genau dann dar, wenn f_a isotrop ist. Da f_a Rang ≥ 5 hat, folgt das Resultat direkt aus Satz 4.26. □

Die Aussage von Satz 4.26 für $n = 3$ – beziehungsweise die von Korollar 4.27 für $n = 2$ – trifft auch auf Formen über $\mathbb{R}$ zu. Der Beweis erfolgt analog wie der über $\mathbb{Q}_p$.

Beweis Satz 4.26. $n = 2$: Die Form $f(X) = a_1X_1^2 + a_2X_2^2$ ist genau dann isotrop, wenn $-a_1/a_2$ ein Quadrat ist. Es gilt in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, dass $d = a_1a_2 = a_1/a_2 = (-1)(-a_1/a_2) = -1$.

$n = 3$: Die Form $f(X) = a_1X_1^2 + a_2X_2^2 + a_3X_3^2$ ist genau dann isotrop, wenn die Form

$$f'(X) := \frac{1}{a_1}f(X) = X_1^2 + \frac{a_2}{a_1}X_2^2 + \frac{a_3}{a_1}X_3^2$$

isotrop ist. Die Form f' wiederum ist genau dann isotrop, wenn für das Hilbert-Symbol $(-a_2/a_1, -a_3/a_1)_p = (-a_1a_2, -a_1a_3)_p = 1$ gilt. Wenn wir den Ausdruck $(-a_1a_2, -a_1a_3)_p$ erweitern, erhalten wir durch Anwendung von Proposition 3.5, insbesondere von 5., und der Bilinearität des Hilbert-Symbols, dass

$$\begin{aligned}(-a_1a_2, -a_1a_3)_p &= (-1,-1)_p(-1,a_1)_p(-1,a_2)_p(-1,a_3)_p(-1,a_1)_p(a_1,a_1)_p(a_1,a_2)_p(a_1,a_3)_p(a_2,a_3)_p\\ &= (-1, -a_1a_2a_3)_p(-1,a_1)_p(a_1,a_1)_p\epsilon_p(f)\\ &= (-1, -\mathrm{d}_p(f))_p\epsilon_p(f).\end{aligned}$$

Demnach gilt $(-a_1a_2, -a_1a_3)_p = 1$ genau dann, wenn $(-1,-d)_p = \epsilon$ ist.

$n = 4$: Die Form $f(X) = a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2$ ist nach Korollar 4.15 genau dann isotrop, wenn die beiden Formen $g(X) := a_1X_1^2 + a_2X_2^2$ und $h(X) := -a_3X_3^2 - a_4X_4^2$ ein gemeinsames Element $x \in \mathbb{Q}_p^\times$ darstellen. Da wir diesen Satz schon für den Fall $n = 3$ bewiesen haben, welcher für den Fall $n = 2$ im Korollar 4.27 verwendet wird, können wir das Korollar hier auf g und h anwenden. Die Form f ist demnach genau dann isotrop, wenn für ein $x \in \mathbb{Q}_p^\times$ gilt, dass $(x, -\mathrm{d}_p(g))_p = \epsilon_p(g)$ und $(x, -\mathrm{d}_p(h))_p = \epsilon_p(f)$, also genau dann, wenn

$$(x, -a_1a_2)_p = (a_1,a_2)_p \text{ und } (x, -a_3a_4)_p = (-a_3,-a_4)_p.$$

Sei A die Menge der Elemente in $\mathbb{Q}_p^\times$, welche die erste Bedingung erfüllen, und B die Menge der Elemente, welche die zweite Bedingung erfüllen. Dann ist f genau dann isotrop, wenn $A \cap B \neq \emptyset$ ist. Der umgekehrte Fall, und zwar $A \cap B = \emptyset$, gilt nach Lemma 4.25 genau dann, wenn

$$a_1a_2 = a_3a_4 \text{ und } (a_1,a_2)_p = -(-a_3,-a_4)_p.$$

Ersteres impliziert, dass $d = (a_1a_2)^2 = 1$. Ist dies der Fall, folgt daraus unter Verwendung von $(a,a)_p = (-1,a)_p$, dass

$$\begin{aligned}\epsilon &= (a_1,a_2)_p(a_1,a_3a_4)_p(a_2,a_3a_4)_p(a_3,a_4)_p\\ &= (a_1,a_2)_p(a_3,a_4)_p(a_3a_4,a_3a_4)_p\\ &= (a_1,a_2)_p(a_3,a_4)_p(-1,a_3a_4)_p\\ &= (a_1,a_2)_p(a_3,a_4)_p(-1,-a_3a_4)_p(-1,-1)_p\\ &= (a_1,a_2)_p(a_3,a_4)_p(-1,a_4)_p(-1,-a_3)_p(-1,-1)_p\\ &= (a_1,a_2)_p(-a_3,-a_4)_p(-1,-1)_p\end{aligned}$$

gilt. Die zweite Bedingung $(a_1,a_2)_p = -(-a_3,-a_4)_p$ ist demnach zu $\epsilon = -(-1,-1)_p$ äquivalent. Damit f isotrop ist und dadurch $A \cap B \neq \emptyset$, dürfen nicht beide Bedingungen gleichzeitig erfüllt sein. Somit ist f genau dann isotrop, wenn $d \neq 1$ gilt, oder $d = 1$ und $\epsilon = (-1,-1)_p$.

$n \geq 5$: Wenn wir für $n = 5$ zeigen können, dass alle quadratischen Formen über $\mathbb{Q}_p$ von Rang 5 isotrop sind, so impliziert dies automatisch, dass alle Formen von Rang ≥ 5 auch isotrop sind, denn wir können für eine Form $f(X) = a_1X_1^2 + \ldots + a_nX_n^2$ einfach eine nichttriviale Lösung $(x_1,\ldots,x_5,0,\ldots,0) \in (\mathbb{Q}_p)^n$ finden. Sei somit $f(X) = a_1X_1^2 + \ldots + a_5X_5^2$ eine Form von Rang 5.

Nach Lemma 4.25 existieren für ein gegebenes $a \in \mathbb{Q}_p^\times$ genau 2^{r-1} verschiedene Elemente b modulo $\mathbb{Q}_p^{\times 2}$, sodass die Gleichung $Z^2 - aX^2 - bY^2 = 0$ eine Lösung hat. Demnach stellt die Form $\tilde{Z}^2 - a\tilde{X}^2$ und folglich jede beliebige quadratische Form von Rang 2 über $Q_p^\times/\mathbb{Q}_p^{\times 2}$ genau 2^{r-1} und somit mindestens 2 verschiedene Elemente dar. Dasselbe gilt für alle Formen von Rang ≥ 2. Folglich stellt f ein $a \neq d \in \mathbb{Q}_p^\times$ dar. Mit Satz 4.16 erhalten wir die Äquivalenz

$$f \sim aX^2 \dot{+} g,$$

wobei g von Rang 4 ist. Aufgrund der Invarianz der Diskriminante gilt $\mathrm{d}_p(g) = d/a$, sie ist also ungleich 1. Da wir den Fall $n = 4$ für diesen Satz schon bewiesen haben, können wir folgern, dass g aufgrund $\mathrm{d}_p(g) \neq 1$ isotrop ist. Folglich ist auch f isotrop. Der Beweis von Satz 4.26 ist somit vollständig. □

5 Der Satz von Hasse-Minkowski

Nun kommen wir zum Höhepunkt dieser Arbeit. In diesem Abschnitt ergründen wir, wann eine quadratische Form f über den rationalen Zahlen $\mathbb{Q}$ die Null nichttrivial darstellt. Sei V wieder die Menge $\{p \in \mathbb{Z} |\ p \text{ prim}\} \cup \{\infty\}$, sei $\mathbb{Q}_\infty = \mathbb{R}$, und sei p immer eine Primzahl. Alle quadratischen Formen in diesem Abschnitt werden als *nichtausgeartet* und mit *Koeffizienten in* $\mathbb{Q}$ angenommen.

Sei

$$f \sim a_1 X_1^2 + \ldots + a_n X_n^2$$

mit $a_i \in \mathbb{Q}$ eine solche quadratische Form. Wir können f durch die Injektion $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$ als quadratische Form f_v in Q_v betrachten und ihre Eigenschaften über diesen Körpern ebenfalls analysieren. Die Invarianten von f_v bezeichnen wir als $\mathrm{d}_v(f) := \mathrm{d}_v(f_v)$ und $\epsilon_v(f) := \epsilon_v(f_v)$. Durch die Produktformel vom Satz 3.11 erhalten wir die Relation

$$\prod_{v \in V} \epsilon_v(f) = 1.$$

Die Diskriminante von f über $\mathbb{Q}$ bezeichnen wir ohne Index mit $\mathrm{d}(f) \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$. Die Signatur (r, s) der reellen quadratischen Form f_∞ ist ebenso eine Invariante von f.

Nun kommen wir zum Hauptsatz dieser Arbeit.

Satz 5.1 (Hasse-Minkowski)**.** *Sei f eine nichtausgeartete quadratische Form über $\mathbb{Q}$. Die Form f ist genau dann isotrop, wenn die Form f_v für alle $v \in V$ isotrop ist.*

Beweis. Es ist klar, dass f_v für alle $v \in V$ die Null nichttrivial darstellt, wenn dies auch für f der Fall ist. Umgekehrt werden wir für den Beweis eine Fallunterscheidung für den Rang n von f machen. Wir schreiben f als

$$f = a_1 X_1^2 + \ldots + a_n X_n^2$$

mit $a_i \in \mathbb{Q}^\times$. Wir können außerdem ohne Beschränkung der Allgemeinheit annehmen, dass $a_1 = 1$ ist, da wir sonst f durch $1/a_1 f$ ersetzen können, und f genau isotrop ist, wenn das für $1/a_1 f$ der Fall ist. Wie in Proposition 4.13 besprochen, stellt eine Form f mit Rang $n = 1$ die Null nur auf triviale Weise dar. Wir beginnen daher mit dem Fall $n = 2$.

- $n = 2$
  Wir schreiben $f = X_1^2 - aX_2^2$. Da f_∞ die Null darstellt, ist f_∞ indefinit nach unserer Argumentation in Abschnitt 4.2. Daher können nicht alle Koeffizienten von f dasselbe Vorzeichen haben, und es muss $a > 0$ gelten. Wir können den Zähler und den Nenner der rationalen Zahl a in ihre Primfaktoren zerlegen und a als

  $$a = \prod_p p^{v_p(a)}$$

  schreiben. Die Form $f_p = X_1^2 - aX_2^2$ stellt für jede Primzahl p die Null dar. Das bedeutet, für jede Primzahl p existieren $x_{1,p}, x_{2,p} \in \mathbb{Q}_p$, sodass $x_{1,p}^2 - a x_{2,p}^2 = 0$ gilt. Die Zahl a ist daher ein Quadrat $a = x_{1,p}^2 / x_{2,p}^2$ in $\mathbb{Q}_p$, und nach Satz 2.36 ist $v_p(a)$ somit gerade für alle p. Folglich ist a auch ein Quadrat in $\mathbb{Q}$, und f stellt am Punkt $(X_1, X_2) = (\sqrt{a}, 1)$ die Null dar.

- $n = 3$
  Wir schreiben $f = X_1^2 - aX_2^2 - bX_3^2$. Laut Proposition 4.21 können wir a und b als quadratfreie ganze Zahlen annehmen, und des Weiteren können wir davon ausgehen, dass $|a|_\infty \leq |b|_\infty$ ist. Wir werden mit Induktion über $s = |a|_\infty + |b|_\infty$ argumentieren. Für die Induktionsverankerung $s = 2$ gilt $|a|_\infty = |b|_\infty = 1$ und

  $$f = X_1^2 \pm X_2^2 \pm X_3^2.$$

Da f_∞ die Null darstellt, muss f_∞ indefinit sein. Der Fall $f = X_1^2+X_2^2+X_3^2$ ist somit ausgeschlossen. In den anderen Fällen stellt f in $\mathbb{Q}$ die Null dar, zum Beispiel $f = X_1^2 + X_2^2 - X_3^2$ am Punkt $(1,0,1) \in \mathbb{Q}^3$.

Wenn $s \geq 3$ ist, dann ist $|b|_\infty \geq 2$. Wir werden die Isotropie von f auf die einer Form $\tilde{f} = X_1^2 - aX_2^2 - \tilde{b}X_3^2$ zurückführen, bei der $|\tilde{b}|_\infty < |b|_\infty$ gilt und somit die Induktionshypothese greift.

Wir notieren die Primzahlzerlegung

$$b = \pm p_1 \cdots p_m.$$

Die Zahl b ist quadratfrei, daher sind alle p_i paarweise verschieden. Wir zeigen nun, dass a ein Quadrat modulo p_i für alle $i = 1, \ldots, m$ ist. Sei $p = p_i$ für ein $i \in \{1, \ldots, m\}$. Ist $a \equiv 0 \pmod{p}$, dann ist a ein Quadrat modulo p, und wir sind fertig. Ansonsten ist a nach Korollar 2.28 eine Einheit in $\mathbb{Z}_p$. Nach unserer Annahme im Satz gibt es $x = (x_1, x_2, x_3) \in (\mathbb{Q}_p)^3$, sodass $x_1^2 - ax_2^2 - bx_3^2 = 0$ ist. Wir können nach Lemma 2.29 jedes x_i als $x_i = p^{n_i}u_i$ schreiben, wobei $n_i \in \mathbb{Z}$ und $u_i \in Z_p^\times$ ist. Sei $h := \min(n_1, n_2, n_3)$ und $y := p^{-h}x$. Das neue Element y ist ebenfalls eine Nullstelle von f_p, allerdings ist (y_1, y_2, y_3) in $(\mathbb{Z}_p)^3$, und für mindestens ein $j \in \{1,2,3\}$ gilt $y_j \in \mathbb{Z}_p^\times$. Wir haben nun die Gleichung $y_1^2 - ay_2^2 - by_3^2 = 0$ und wissen, dass $b \equiv 0 \pmod{p}$ ist. Daher gilt $y_1^2 - ay_2^2 \equiv 0 \pmod{p}$. Wir zeigen nun, dass $y_1, y_2 \not\equiv 0 \pmod{p}$ sind, und daher a ein Quadrat modulo p ist. Angenommen $y_2 \equiv 0 \pmod{p}$. Dann ist auch $y_1 \equiv 0 \pmod{p}$, und $0 = y_1^2 - ay_2^2 - by_3^2 \equiv by_3^2 \pmod{p^2}$. Da $v_p(b) = 1$ ist, muss daher p auch y_3^2 und somit y_3 teilen. Es gilt also auch $y_3^2 \equiv 0 \pmod{p}$ und somit $y_3 \notin \mathbb{Z}_p^\times$, im Widerspruch zur Definition von y. Somit gilt $y_2 \not\equiv 0 \pmod{p}$, und da in der Gleichung $y_1^2 - ay_2^2 \equiv 0 \pmod{p}$ auch $a \not\equiv 0 \pmod{p}$ ist, gilt ebenso $y_1 \not\equiv 0 \pmod{p}$. Wir können folglich a als Quadrat $a \equiv y_1^2/y_2^2 \pmod{p}$ schreiben. Dies gilt für alle $p_i, i \in \{1, \ldots, m\}$, folglich ist a ein Quadrat in $\prod_{i=1}^m \mathbb{Z}/p_i\mathbb{Z}$. Nach dem Chinesischen Restsatz (Lemma 3.12) gilt $\prod_{i=1}^m \mathbb{Z}/p_i\mathbb{Z} \cong \mathbb{Z}/b\mathbb{Z}$, und somit ist a auch ein Quadrat modulo b.

Da a ein Quadrat modulo b ist, gibt es zwei ganze Zahlen $q, c \in \mathbb{Z}$, sodass

$$q^2 = a + bc.$$

Wir können q in $\{0, 1, \ldots, |b-1|_\infty\}$ wählen, da wir dadurch entstehende Differenzen durch die Wahl von c ausgleichen können. Ist $q > |b/2|_\infty$, so gilt $k := |b|_\infty - q < |b/2|_\infty$ und

$$q^2 = (|b|_\infty - k)^2 = |b|_\infty^2 - 2|b|_\infty k + k^2 \equiv k^2 \pmod{b}.$$

Wir können also q durch k ersetzen, wenn wir c entsprechend anpassen. Somit können wir ohne Beschränkung der Allgemeinheit q so wählen, dass $|q|_\infty \leq |b/2|_\infty$ ist. Wir erhalten $bc = q^2 - a = q^2 - a \cdot 1^2$ mit $1, q \in \mathbb{Z} \subset \mathbb{Q}_v$ für alle $v \in V$. Somit liegt bc in der Normgruppe N_a bezüglich $\mathbb{Q}_v$. Nach Proposition 3.4 folgt, dass das Hilbertsymbol $(a, bc)_v = 1$ für alle $v \in V$ ist. Von Proposition 3.5 wissen wir, dass $1 = (a, bc)_v = (a, b)_v (a, c)_v$ gilt. Das heißt, $f = X_1^2 - aX_2^2 - bX_3^2$ stellt die Null genau dann über $\mathbb{Q}_v$ dar, wenn $f' = X_1^2 - aX_2^2 - cX_3^2$ auch die Null darstellt. Insbesondere folgt daraus, dass f'_v für alle $v \in V$ die Null darstellt. Außerdem ist

$$|c|_\infty = |\frac{q^2 - a}{b}|_\infty \leq \frac{|q^2|_\infty + |a|_\infty}{|b|_\infty} < |b|_\infty,$$

da $|q|_\infty \leq |b/2|_\infty$, $|a|_\infty \leq |b|_\infty$ und $|b|_\infty \geq 2$ ist. Des Weiteren können wir $c = \tilde{b}d^2$ schreiben, wobei $\tilde{b}$ und d ganze Zahlen sind, $\tilde{b}$ quadratfrei und $|\tilde{b}|_\infty < |b|_\infty$ ist. Folglich können wir die Induktionshypothese auf die Form $\tilde{f} = X_1^2 - aX_2^2 - \tilde{b}X_3^2$ anwenden, welche äquivalent zu f' ist. Die Form f' stellt daher die Null dar, und somit auch f.

- $n = 4$
  Wir schreiben $f = (aX_1^2 + bX_2^2) - (cX_3^2 + dX_4^2) = g \dot{-} h$. Für $v \in V$ ist f_v isotrop über $\mathbb{Q}_v$. Nach

Korollar 4.15 ist dies äquivalent dazu, dass für alle $v \in V$ ein Element $z_v \in \mathbb{Q}_v$ existiert, welches von der Form g_v als auch von h_v dargestellt wird. Darauf können wir nun die Bedingungen von Korollar 4.27 für $n = 2$ anwenden, und sehen, dass

$$(z_v, -ab)_v = (a, b)_v =: \epsilon_{1,v} \text{ und } (z_v, -cd)_v = (c, d)_v =: \epsilon_{2,v}$$

gilt. Dank Satz 3.11 wissen wir, dass $\prod_{v \in V} \epsilon_{1,v} = 1 = \prod_{v \in V} \epsilon_{2,v}$ gilt, und dass für fast alle v die Werte $\epsilon_{1,v}$ und $\epsilon_{2,v}$ gleich 1 sind. Damit sind alle drei Bedingungen von Satz 3.15 erfüllt, sodass ein $z \in \mathbb{Q}^\times$ existiert mit der Eigenschaft

$$(z, -ab)_v = (a, b)_v \text{ und } (z, -cd)_v = (c, d)_v \text{ für alle } v \in V.$$

Wir wenden hier Korollar 4.27 für $n = 3$ abermals an, und erhalten, dass die Form $g_v(X) = aX_1^2 + bX_2^2$ das Element $z \in \mathbb{Q}^\times$ darstellt. Daraus folgt, dass die Form $\tilde{g}_v(X) := aX_1^2 + bX_2^2 - zZ^2$ isotrop in $\mathbb{Q}_v$ für alle $v \in V$ ist. Nach dem obigen Beweis für den Rang $n = 3$ ist diese Form auch in $\mathbb{Q}$ isotrop, und $g(X) = aX_1^2 + bX_2^2$ stellt z über $\mathbb{Q}$ dar. Wir wenden dasselbe Argument auf die Form $h_v(X) = cX_3^2 + dX_4^2$ an und erhalten gleichfalls, dass $h(X) = cX_3^2 + dX_4^2$ das Element z über $\mathbb{Q}$ darstellt. Nach Korollar 4.15 ist somit $f = g \dot{-} h$ isotrop.

- $n \geq 5$
  Wir schreiben f in der Form

$$f = (a_1X_1^2 + a_2X_2^2) - (a_3X_3^2 + \ldots + a_nX_n^2) = g \dot{-} h,$$

wobei wir ohne Beschränkung der Allgemeinheit annehmen können, dass $a_i \in \mathbb{Z}$ gilt. Wir führen eine Induktion nach dem Rang n durch. Die Induktionsverankerung ist durch den eben bewiesenen Fall $n = 4$ gegeben. Die Form f_v stellt die Null dar, daher gibt es ein Element $z_v \in \mathbb{Q}_v$, welches sowohl von g_v als auch h_v dargestellt wird. Wir werden nun ein Element $z \in \mathbb{Q}$ finden, welches ebenfalls von g_v und h_v für alle $v \in V$ dargestellt wird. Sei $x_v = (x_1^v, \ldots, x_n^v) \in (\mathbb{Q}_v)^n$, sodass

$$a_1(x_1^v)^2 + a_2(x_2^v)^2 = z_v = a_3(x_3^v)^2 + \ldots + a_n(x_n^v)^2.$$

Sei $S := \{2, \infty\} \cup \{p \text{ prim} \mid p \text{ teilt mindestens ein } a_i \text{ mit } i = 3, \ldots, n\}$ eine endliche Untermenge von V. Durch die simultane Approximation aus Satz 3.14 können wir x_1^s und x_2^s simultan für alle $s \in S$ durch rationale Zahlen approximieren. Somit finden wir $z_1, z_2 \in \mathbb{Q}$, sodass $a_1(z_1)^2 + a_2(z_2)^2 = z$ für alle s beliebig nahe bei z_s liegt. Nach Korollar 2.37 gilt dann, dass $z/z_s \in \mathbb{Q}_s^{\times 2}$ ist. Sei $c_s \in \mathbb{Q}_s^\times$ eine Wurzel von z/z_s. Folglich wird $z = z_s c_s^2$ ebenfalls über $\mathbb{Q}_s$ durch die Form $h_s(X) = a_3(X_3)^2 + \ldots + a_n(X_n)^2$ dargestellt, und zwar an der Stelle $(x_3^s c_s, \ldots, x_n^s c_s)$.

Aus der Konstruktion der Zahl z folgt, dass sie von g über $\mathbb{Q}$ dargestellt wird. Nun müssen wir noch zeigen, dass z auch für alle restlichen $v \notin S$ von h_v und folglich auch über $\mathbb{Q}$ dargestellt wird. Für $n \geq 6$ ist der Rang von h größer als 4, somit stellt h_v nach Korollar 4.27 die Zahl z dar. Sei also $n = 5$. Für $v \notin S$ sind die Koeffizienten $-a_3, -a_4, -a_5$ der Form h_v in $\mathbb{Z}_v^\times$, da für sie $v_v(a_i) = 0$ gilt. Folglich werden sie modulo $\mathbb{Q}_v^{\times 2}$ durch einen quadratischen Nichtrest u oder durch 1 repräsentiert (siehe Beweis von Lemma 3.6). Aus Satz 3.8 erhalten wir die Werte des Hilbert-Symbols und somit

$$\epsilon_v(h) = (-a_3, -a_4)_v(-a_3, -a_5)_v(-a_4, -a_5)_v = 1 \cdot 1 \cdot 1 = 1.$$

Ebenso liegt $d_v(h) = -a_3a_4a_5$ in $\mathbb{Z}_v^\times$, und wir erhalten aus demselben Satz 3.8, dass $(-1, -d_v(h))_v = 1 = \epsilon_v(h)$ gilt. Nach Korollar 4.27 für $n = 5$ stellt h_v demnach die rationale Zahl z für alle $v \notin S$ dar. Somit stellt h_v für alle $v \in V$ die Zahl $z \in \mathbb{Q}$ dar, und $\tilde{h} = h \dot{-} zZ^2$ ist über $\mathbb{Q}_v$ isotrop. Die Form $\tilde{h}$ hat Rang $n - 1$, und nach unserer Induktionsannahme ist $\tilde{h}$ auch über $\mathbb{Q}$ isotrop. Damit stellt h über $\mathbb{Q}$ das Element z dar. Ebenso ist die Form $\tilde{g} = g \dot{-} zZ^2$ für alle v über $\mathbb{Q}_v$ isotrop. Sie hat Rang 3, somit ist sie, da wir den Satz für $n = 3$ schon gezeigt haben, auch über $\mathbb{Q}$ isotrop. Es stellen folglich sowohl h als auch g über $\mathbb{Q}$ das Element z dar, und demzufolge ist $f = g \dot{-} h$ isotrop.

□

5.1 Korollare und Erweiterungen

Korollar 5.2. *Sei $a \in \mathbb{Q}$ eine rationale Zahl. Dann stellt eine quadratische Form f die Zahl a genau dann über $\mathbb{Q}$ dar, wenn sie diese für alle $v \in V$ über $\mathbb{Q}_v$ darstellt.*

Beweis. Sei f eine quadratische Form über $\mathbb{Q}$ vom Rang n. Stellt die Form f die Zahl a über $\mathbb{Q}$ dar, so ist dies auch für f_v für jedes $v \in V$ der Fall. Stellt umgekehrt f_v für jedes $v \in V$ die Zahl a dar, so sind die Formen $f_v - aZ^2$ über $\mathbb{Q}_v$ isotrop. Nach dem Satz von Hasse-Minkowski ist somit auch $f - aZ^2$ über $\mathbb{Q}$ isotrop, das heißt, es gibt einen Vektor $(x, z) := (x_1, \ldots, x_n, z) \in \mathbb{Q}^{n+1} \backslash \{0\}$, sodass $f(x) - az^2 = 0$ gilt. Ist $z \neq 0$, so stellt f an der Stelle $(x_1/z, \ldots, x_n/z)$ das Element a dar. Gilt hingegen $z = 0$, so ist f isotrop und stellt nach Satz 4.14 alle Elemente in $\mathbb{Q}$ und somit auch a dar. □

Korollar 5.3. *Eine quadratische Form f von Rang ≥ 5 stellt die Null über $\mathbb{Q}$ genau dann dar, wenn sie indefinit ist.*

Beweis. Sei f eine indefinite quadratische Form über $\mathbb{Q}$. Aus Satz 4.26 folgt, dass f für alle Primzahlen p über $\mathbb{Q}_p$ die Null darstellt, und aus der Indefinitheit folgt, dass f die Null über den reellen Zahlen darstellt. Aus dem Satz von Hasse-Minkowski folgt das Resultat.
Umgekehrt kann eine Form f nur dann über $\mathbb{Q}$ die Null darstellen, wenn sie indefinit ist. □

Korollar 5.4. *Sei f eine quadratische Form über $\mathbb{Q}$ von Rang n. Angenommen, es ist $n = 3$, oder es gilt $n = 4$ und $d(f) = 1$, und f stellt die Null über $\mathbb{Q}_v$ für alle $v \in V$ bis auf ein $v_0 \in V$ auf nichttriviale Weise dar. Dann ist f isotrop über $\mathbb{Q}$.*

Beweis. Sei f eine quadratische Form über $\mathbb{Q}$ von Rang n, welche die Null über $\mathbb{Q}_v$ für alle $v \in V$ bis auf ein v_0 nichttrivial darstellt. Ist $n = 3$, so folgt aus Satz 4.26, dass für alle $v \neq v_0$ die Gleichung $(-1, -\mathrm{d}(f))_v = \epsilon_v(f)$ gilt. Aus der Produktformel in Satz 3.11 folgt für den fehlenden Index v_0, dass

$$(-1, -\mathrm{d}(f))_{v_0} = \prod_{v \in V, v \neq v_0} (-1, -\mathrm{d}(f))_v = \prod_{v \in V, v \neq v_0} \epsilon_v(f) = \epsilon_{v_0}(f).$$

Nach Satz 4.26 ist auch f_{v_0} isotrop, und mit dem Satz von Hasse-Minkowski folgt auch, dass f isotrop ist.

Ist $n = 4$ und gilt $\mathrm{d}(f) \neq 1$, so ist nach Satz 4.26 die Form f_{v_0} und folglich auch die Form f isotrop. Ist hingegen $\mathrm{d}(f) = 1$, so müssen wir nach Satz 4.26 zeigen, dass $(-1, -1)_{v_0} = \epsilon_{v_0}(f)$ gilt. Dies folgt analog zum Fall $n = 3$ aus der Produktformel des Hilbert-Symbols. Dadurch gilt auch hier, dass f_v und somit f isotrop ist. □

Natürlich ist der Satz von Hasse-Minkowski zur Untersuchung quadratischer Formen über $\mathbb{Q}$ nur dann nützlich, wenn wir Aussagen über deren Isotropie über den Körpern $\mathbb{Q}_v$ machen können. Durch das Hilbert-Symbol und die Kriterien in Satz 4.26 haben wir dafür sehr gute Werkzeuge zur Verfügung. Wir illustrieren eine konkrete Anwendung des Satzes von Hasse-Minkowski an einem Beispiel.

Beispiel 5.5. Betrachten wir die Form $f(X) = X^2 - 2Y^2 - 7Z^2$. Für $v \in V$ ist f_v genau dann isotrop, wenn das Hilbert-Symbol $(2, 7)_v = 1$ ist. Da f indefinit ist, erübrigt sich der Fall $v = \infty$. Aus Satz 3.8 erhalten wir $(2, 7)_p = 1$ für $p \neq 2, 7$, sowie $(2, 7)_2 = (-1)^{\frac{7^2-1}{8}} = (-1)^{\frac{48}{8}} = 1$. Nach Korollar 5.4 müssen wir den Wert von $(2, 7)_7$ nicht mehr berechnen, da wir schon für alle bis auf ein $v \in V$ gezeigt haben, dass f_v isotrop über $\mathbb{Q}_v$ ist, und sich der letzte Fall somit automatisch ergibt. Daher sind die Formen f_v für alle $v \in V$ isotrop, und es existiert eine nichttriviale Nullstelle über $\mathbb{Q}$ für die Form f. Leider ist der Satz von Hasse Minkowski nicht konstruktiv, aber in diesem Fall findet man noch leicht selbst eine Nullstelle – zum Beispiel erfüllt $(x, y, z) := (3, 1, 1)$ die Bedingung.

Der Satz von Hasse-Minkowski kann erweitert werden, sodass er für quadratische Formen über beliebigen Zahlkörpern, d.h. über endlichen Körpererweiterungen von $\mathbb{Q}$, gilt. Die Formulierung lautet dann folgendermaßen.

Satz 5.6. *Sei f eine quadratische Form über einem Zahlkörper $\mathbb{K}$. Dann ist f genau dann über $\mathbb{K}$ isotrop, wenn f über alle Vervollständigungen von $\mathbb{K}$ isotrop ist.*

Der Beweis dieser Version des Satzes geht allerdings über das Ausmaß dieser Arbeit hinaus.

Der Satz von Hasse-Minkowksi kann jedoch nicht auf Formen vom Grad ≥ 3 ausgeweitet werden. So hat zum Beispiel der norwegische Mathematiker Ernst Sejersted Selmer in einer Arbeit von 1951 bewiesen, dass die Gleichung $3X^3 + 4Y^3 + 5Z^3 = 0$ zwar eine nichttriviale Lösung in allen $\mathbb{Q}_v$ hat, aber nicht in $\mathbb{Q}$ (siehe [10] S. 205).

Literatur

[1] H. Cohen. *Number Theory Volume I: Tools and Diophantine Equations*. Springer-Verlag, 2007.

[2] F. Q. Gouvêa. *p-adic Numbers - An Introduction*. Springer-Verlag, 1997.

[3] H. Hasse. *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen*. Journal für reine und angewandte Mathematik, Bd. 152, 1923. Abgerufen von http://gdz.sub.uni-goettingen.de/dms/load/img/?PID=GDZPPN002169037 am 3. Oktober 2016.

[4] H. Hasse. *Festschrift im Gedenken an Hensel*, erschienen in H. Pieper. *Zahlen aus Primzahlen - Eine Einführung in die Zahlentheorie*. Deutscher Verlag der Wissenschaften, 1984.

[5] M. Kneser. *Quadratische Formen*. Springer-Verlag, 2002.

[6] J. Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, 1992.

[7] H. Pieper. *Zahlen aus Primzahlen - Eine Einführung in die Zahlentheorie*. Deutscher Verlag der Wissenschaften, 1984.

[8] M. Ram Murty. *Introduction to p-adic Analytic Number Theory*. American Mathematical Society and International Press, 2002.

[9] A. Schmidt. *Einführung in die algebraische Zahlentheorie*. Springer-Verlag, 2007.

[10] E. Selmer, *The Diophantine equation ax3 + by3 + cz3 = 0*, Acta Mathematica 85, 1951, 203–362. Abgerufen von http://projecteuclid.org/euclid.acta/1485888630 am 3. April 2017.

[11] J.-P. Serre. *A Course in Arithmetic*. Springer-Verlag, 1973.