



universität
wien

DIPLOMARBEIT

Titel der Diplomarbeit

Grundlagen der Theorie positiv definiter und indefiniter
binärer quadratischer Formen

Verfasserin

Sandra Anna Burda

angestrebter akademischer Grad

Magistra der Naturwissenschaften (Mag. rer. nat.)

Wien, 2015

Studienkennzahl lt. Studienblatt: A 190 406 313

Studienrichtung lt. Studienblatt: Lehramtsstudium UF Mathematik
UF Geschichte, Sozialkunde und Politische Bildung

Betreuer: ao. Univ.-Prof. Dr. Christoph Baxa

Meinen Eltern gewidmet

Inhaltsverzeichnis

1	Einleitung	1
2	Grundlagen und Äquivalenz von binären quadratischen Formen	3
3	Positiv definite binäre quadratische Formen	13
3.1	Äquivalenzklassen positiv definiter binärer quadratischer Formen	19
3.2	Automorphismen positiv definiter binärer quadratischer Formen	25
4	Indefinite binäre quadratische Formen	39
4.1	(Unendliche) Kettenbrüche	42
4.2	Die Abbildung $\mathcal{T}_U(z)$ und die komplexe Zahlenebene	49
4.3	Die Theorie der Kettenbrüche und die Abbildung $\mathcal{T}_U(z)$ in Bezug auf indefinite binäre quadratische Formen	53
4.4	Äquivalenz und Ketten indefiniter binärer quadratischer Formen	63
4.5	Automorphismen indefiniter binärer quadratischer Formen	72
5	Geometrische Interpretation von binären quadratischen Formen	83
5.1	Positiv definite binäre quadratische Formen	85
5.2	Indefinite binäre quadratische Formen	89
5.3	Geometrische Veranschaulichung der Gleichung $f(x, y) = m$	90
Anhang		93
A	Beispiele zur Klassenzahl $h(D)$ für $D < 0$	93
B	Beispiele zur Klassenzahl $h(D)$ für $D > 0$ kein Quadrat	94
C	Abstract	95
Literaturverzeichnis		97
Abbildungsverzeichnis		99
Lebenslauf		101

Kapitel 1

Einleitung

Schon in der Antike war es ein Anliegen vieler Mathematiker nicht bloß alle Lösungen einer Gleichung zu bestimmen, sondern diese in vielerlei Hinsicht zu untersuchen. Dabei wurden an die Gleichung bestimmte Bedingungen gestellt. So sollten u. a. die Lösungen positiv oder die Koeffizienten ganzzahlig sein, um Beispiele zu nennen. Mit solchen Problemen beschäftigte sich schon der Mathematiker *Diophantos von Alexandria* (3. Jh. n. Chr.). Auf ihn geht der Begriff *Diophantische Gleichung* zurück, worunter das Lösen einer Gleichung in den ganzen Zahlen verstanden wird. Im Lauf der Zeit wurde eine große Vielfalt Diophantischer Gleichungen studiert und doch gibt es solche, denen eine größere Bedeutung zugeschrieben wurde und wird. Dazu zählt u. a. die *Pellsche Gleichung* $X^2 - dY^2 = 1$, wobei d im Allgemeinen eine gegebene ganze Zahl ist. Mit der Einschränkung dieser Gleichung auf eine natürliche Zahl d kein Quadrat – sowie der Version $X^2 - dY^2 = N$ (mit $N \in \mathbb{Z}$ gegeben) – haben sich auch die Mathematiker Fermat (1601-1665), Euler (1670-1743) und Lagrange (1736-1813) beschäftigt. Letztendlich gelang es Lagrange um 1766 zu zeigen, dass die Pellsche Gleichung mit den zuvor genannten Voraussetzungen für d unendlich viele ganzzahlige Lösungen besitzt. Insbesondere untersuchten Lagrange (u. a. in Korrespondenz mit Euler) sowie Legendre (1752-1833) eine weitere allgemeinere Diophantische Gleichung, nämlich

$$ax^2 + bxy + cy^2 = m \quad \text{mit} \quad a, b, c, m \in \mathbb{Z}.$$

Die Theorie der *binären quadratischen Formen*, von welcher diese Arbeit handelt, war geboren. Es war jedoch Gauss (1777-1855), der in seinem Werk *Disquisitiones Arithmeticae* die Resultate von Euler und Lagrange vertiefte und die Theorie darüber immens weiterentwickelte. Gauss betrachtete in seinem Werk die Theorie der binären quadratischen Formen u. a. als einen Spezialfall der Theorie der Quadratischen Formen.

Doch was sind Gründe dafür, dass sich zahlreiche Mathematiker und Mathematikerinnen mit gerade diesen Formen auseinandergesetzt haben und dies immer noch tun?

Ein Motiv dafür ist mit Sicherheit die Existenz zahlreicher ungelöster Probleme auf diesem Gebiet. Andere Impulse könnten u. a. durch die folgenden Problemstellungen, mit welchen sich binäre quadratische Formen beschäftigen, ausgelöst worden sein:

- Gibt es für gegebene ganze Zahlen m und $D = b^2 - 4ac$, $D \equiv 0$ oder $1 \pmod{4}$ eine Darstellung von m durch $[m =] f(x, y) = ax^2 + bxy + cy^2$ für die $\text{ggT}(x, y) = 1$ gilt?
- Welche Zahlen m werden durch eine Form dargestellt? Verfügen diese Zahlen über eine spezielle Gestalt?
- Existieren mehrere Darstellungsformen von m und wie sind diese zu bestimmen?
- Können zwei oder mehrere Formen ineinander übergeführt werden? Wenn ja, unter welchen Voraussetzungen ist dies möglich und warum ist dies von Interesse?
- u. v. a. m.¹

Ziel dieser Arbeit ist es jedoch nicht, die oben genannten Probleme vollständig zu lösen. Diesbezüglich bedarf es Kenntnisse über die Klassenkörpertheorie und anderer komplexer Themenbereiche der algebraischen Zahlentheorie. Gedacht ist diese Arbeit als eine Einführung in die Theorie der binären quadratischen Formen und orientiert sich dabei an dem Werk „Zahlentheorie. Eine Einführung“ von Hlawka und Schoißengeier (2. Auflage: 1990)².

Beginnend mit grundlegenden Definitionen und Forderungen an eine binäre quadratische Form ist es in Kapitel 2 unsere Intention zu bestimmen, wann zwei Formen als äquivalent bezeichnet werden und welchen Ertrag eine Äquivalenz liefert. Kapitel 3 und 4 widmen sich zwei Klassen von binären quadratischen Formen. In beiden Kapiteln ist es unser Anliegen, alle Lösungen der Gleichung $m = ax^2 + bxy + cy^2$ zu bestimmen, sofern dies möglich ist. Wir werden hierfür eine Lösungsmethode entwickeln und zeigen, warum es von Wichtigkeit ist, die Automorphismen einer Form zu kennen. Schließlich befassen wir uns in Kapitel 5 mit einer geometrischen Interpretation binärer quadratischer Formen und der Gleichung $m = ax^2 + bxy + cy^2$.

¹(Niven 1976: 132-137, 231-236), (Ribenoim 2009: 119-177), (Weil 1992: 1-3, 18-32, 97-109, 215-225, 330-336, 337-382)

²(Hlawka 1990: 24-29, 79-138)

Kapitel 2

Grundlagen und Äquivalenz von binären quadratischen Formen

In diesem Kapitel sollen die Grundlagen binärer quadratischer Formen sowie deren Äquivalenz untersucht werden. Bevor jedoch eine Definition binärer quadratischer Formen gegeben wird, soll der Überbegriff *Form* und diesbezüglich *quadratische Form* kurz erklärt werden. Bei einer *Form* f handelt es sich um ein homogenes Polynom, also um ein Polynom in mehreren Variablen, wobei alle Terme vom selben Grad sind. Wenn nun von einer *quadratischen Form* f gesprochen wird, so handelt es sich um Terme zweiten Grades, welche sich schreiben lassen als:

$$f(x_1, x_2, \dots, x_n) = \sum_{i,j=1}^n a_{ij}x_i x_j. {}^1$$

Diese Arbeit beschränkt sich auf ganzzahlige Koeffizienten a_{ij} der Form f . Außerdem werden ausschließlich Formen in zwei Variablen betrachtet, welche als *binäre quadratische Formen* bezeichnet werden. Womit wir zu folgender Definition gelangen:

DEFINITION 2.1 Es seien $a, b, c \in \mathbb{Z}$. Dann heißt

$$f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, f(x, y) = ax^2 + bxy + cy^2$$

eine *binäre quadratische Form*. Lassen sich ganze Zahlen (x_0, y_0) mit $f(x_0, y_0) = m$ finden, so sagen wir, dass eine ganze Zahl m *durch f dargestellt wird*. Die Darstellung heißt *eigentlich*, wenn $\text{ggT}(x_0, y_0) = 1$ und *uneigentlich* sonst.

Bei den Abhandlungen von Gauss und Dirichlet findet man stattdessen $f(x, y) = ax^2 + 2bxy + cy^2$. Dies führt im Allgemeinen zu keinem Unterschied, jedoch sollte sich der Leser

¹(Niven 1972: 167f.)

über den daniederliegenden Sinn des Autors informieren. Dahinter stecken die Analogien zu quadratischen Formen im Allgemeinen. Interessant wird die Festlegung auf einen geraden mittleren Koeffizienten $2b$, wenn Körper (oder Ringe) der Charakteristik 2 betrachtet werden.

Bevor wir über die *Äquivalenz* von binären quadratischen Formen sprechen, wollen wir diesbezüglich noch einige Feststellungen treffen. Die Koeffizienten a, b und c sind zu f eindeutig bestimmt, denn

$$a = a \cdot 1^2 + b \cdot 1 \cdot 0 + c \cdot 0^2 = f(1, 0), \quad c = f(0, 1) \quad \text{und} \quad b = f(1, 1) - f(1, 0) - f(0, 1). \quad (1)$$

Somit lässt sich eine binäre quadratische Form f auch schreiben als $f = (a, b, c)$. Außerdem halten wir fest, dass sich $f(x, y) = ax^2 + bxy + cy^2$ mittels Matrizen darstellen lässt:

$$f(x, y) = (x, y) \frac{1}{2} F_f \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{mit} \quad F_f = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}, \quad (2)$$

wovon man sich im Folgenden leicht überzeugen kann:

$$\begin{aligned} f(x, y) &= (x, y) \frac{1}{2} \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \\ &= \left(ax + \frac{b}{2}y, \frac{b}{2}x + cy\right) \begin{pmatrix} x \\ y \end{pmatrix} = ax^2 + bxy + cy^2. \end{aligned}$$

Hierbei ist $\frac{1}{2}F_f$ die einzige symmetrische Matrix, die diese Eigenschaft aufweist. Mithilfe der Matrix F_f können wir die *Diskriminante* von f definieren. Auf diese werden wir im Laufe der Arbeit immer wieder stoßen, da sie uns Klassifizierungen erlaubt.

DEFINITION 2.2 Es sei $f = (a, b, c)$ mit $F_f = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$. Dann bezeichnen wir

$$D_f = -\det F_f = \begin{vmatrix} 2a & b \\ b & 2c \end{vmatrix} = b^2 - 4ac$$

als die *Diskriminante* von f .

Aufgrund dessen, dass für jedes $b \in \mathbb{Z}$ gilt:

$$b^2 \equiv 0 \text{ oder } 1 \pmod{4} \quad \Rightarrow \quad D_f \equiv 0 \text{ oder } 1 \pmod{4}.$$

Diesbezüglich können wir zu jeder Zahl $D \in \mathbb{Z}$ mindestens eine Form mit Diskriminante D

finden und zwar mithilfe der *Grundform* bzw. *Hauptform* zur Diskriminante D :

$$\begin{aligned} f(1, 0, -\frac{D}{4}) &= x^2 - \frac{D}{4}y^2, & \text{falls } D \equiv 0 \pmod{4} \\ f(1, 1, \frac{1-D}{4}) &= x^2 + xy + \frac{1-D}{4}y^2, & \text{falls } D \equiv 1 \pmod{4}. \end{aligned} \quad (3)$$

Eine Form f kann eine Zahl m sowohl eigentlich als auch uneigentlich darstellen, so z. B. gilt für

$$f = x^2 - xy + 2y^2 \quad 16 = 1^2 - 1 \cdot 3 + 2 \cdot 3^2 = 4^2 - 4 \cdot 2 + 2 \cdot 2^2.$$

Somit stellen sich Fragen, wie die folgenden: Für welche (x, y) ist die Gleichung $f(x, y) = m$ lösbar? Welche Formen repräsentieren eine gegebene ganze Zahl m ? Wie viele Darstellungen ein und der selben Zahl gibt es und gibt es einen Weg, all diese zu finden? Zur Beantwortung dieser und anderer Fragen werden die Eigenschaften und Strukturen der Menge der binären quadratischen Formen untersucht.

Dies ist insofern hilfreich, da es einem in der Menge der quadratischen Formen eine Klasseneinteilung ermöglicht. Es wird sich zu einer anfangs kompliziert aussehenden Form eine „schönere“, dazu äquivalente Form finden lassen, welche einem das Suchen der entsprechenden Antwort erleichtern soll.

DEFINITION 2.3 Es sei $L : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ mit $L(x, y) = \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ bijektiv und linear. Dann heißt L eine *ganzzahlige unimodulare*² *Transformation*.

Die Menge dieser Abbildungen ist bekannt als die *General linear group* vom Grad 2 über $\mathbb{Z}$, kurz $GL_2(\mathbb{Z})$. Sie bildet bezüglich der Matrizenmultiplikation eine Gruppe, ist also unter Inversenbildung und Zusammensetzung abgeschlossen.

SATZ 2.1 Eine lineare Transformation $L : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$, $L(x, y) = \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ ist genau dann bijektiv, wenn α, β, γ und $\delta \in \mathbb{Z}$ und $\det L = \pm 1$.

Beweis: ($\Rightarrow$) :

$$\begin{aligned} L(1, 0) &= \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} \in \mathbb{Z}^2 \\ \text{und } L(0, 1) &= \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \beta \\ \delta \end{pmatrix} \in \mathbb{Z}^2. \end{aligned}$$

Da $L \in GL_2(\mathbb{Z})$ existiert L^{-1} , ist ebenfalls linear und bijektiv. Somit ist $\det L^{-1} \in \mathbb{Z}$ und $\det L \in \mathbb{Z}$. Des Weiteren gilt, dass $\det L \cdot \det(L^{-1}) = 1$ woraus $|\det L| = 1$ folgt.

²Anm.: Eine quadratische Matrix heißt *unimodular*, wenn ihre Eintragungen ganzzahlig sind und sie Determinante ± 1 besitzt.

($\Leftarrow$) : L besitzt nur ganzzahlige Einträge und es gilt, dass $|\det L| = 1$. Somit besitzt auch L^{-1} nur ganzzahlige Eintragungen:

$$L^{-1} = \frac{1}{\det L} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}.$$

□

Hieraus erhalten wir, dass sich eine binäre quadratische Form f durch $L \in \text{GL}_2(\mathbb{Z})$ mittels $f \circ L$ wieder in eine binäre quadratische Form überführen lässt und dieselbe(n) Zahl(en) wie f darstellt. Die Umkehrung gilt jedoch nicht. Außerdem führt $L(x, y)$ eigentliche Darstellungen in eigentliche über: Es gilt nämlich $\text{ggT}(x, y) = \text{ggT}(\alpha x + \beta y, \gamma x + \delta y)$ für $L(x, y) \in \text{GL}_2(\mathbb{Z})$ und $(x, y) \neq 0$.³

Wir wollen auch der Menge der eigentlichen Transformationen, das sind jene deren Determinante gleich 1 ist, eine Bezeichnung geben, nämlich *Special linear group* vom Grad 2 über $\mathbb{Z}$, kurz $\text{SL}_2(\mathbb{Z})$. Man kann sich schnell davon überzeugen, dass es sich bei der $\text{SL}_2(\mathbb{Z})$ um eine Untergruppe der $\text{GL}_2(\mathbb{Z})$ handelt, die nicht kommutativ ist.

Solch eine Transformation soll nun genauer betrachtet werden:

Es sei $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$. Wir substituieren x und y in $f(x, y) = ax^2 + bxy + cy^2$ durch

$$\begin{aligned} x' &= \alpha x + \beta y \\ y' &= \gamma x + \delta y. \end{aligned} \quad \text{bzw.} \quad \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \quad (4)$$

Somit geht f in die Form $f'(x', y') = a'x'^2 + b'x'y' + c'y'^2$ über. Doch wie sehen deren Koeffizienten a', b', c' aus?

$$\begin{aligned} a'x'^2 + b'x'y' + c'y'^2 &= a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2 = \\ &= a(\alpha^2 x^2 + 2\alpha x \beta y + \beta^2 y^2) + b(\alpha \gamma x^2 + \beta \gamma \gamma x + \alpha x \delta y + \beta \delta y^2) + c(\gamma^2 x^2 + 2\gamma x \delta y + \delta^2 y^2) = \\ &= x^2(a\alpha^2 + b\alpha\gamma + c\gamma^2) + xy(2a\alpha\beta + b\beta\gamma + b\alpha\delta + 2c\gamma\delta) + y^2(a\beta^2 + b\beta\delta + c\delta^2). \end{aligned}$$

³Angenommen $t|x$ und $t|y$. Dann gilt $t|\alpha x + \beta y$ sowie $t|\gamma x + \delta y$ und wir erhalten

$$\text{ggT}(x, y) \mid \text{ggT}(\alpha x + \beta y, \gamma x + \delta y).$$

Da es sich bei $L(x, y)$ um eine ganzzahlige unimodulare Transformation handelt, gilt aus Symmetriegründen Gleichheit. Somit ergibt sich aus $\text{ggT}(x, y) = 1$, dass auch $\text{ggT}(\alpha x + \beta y, \gamma x + \delta y) = 1$ gilt.

Daraus ergibt sich für a', b', c' das Folgende:

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ c' &= a\beta^2 + b\beta\delta + c\delta^2. \end{aligned} \tag{5}$$

Wenn wir nun also nach jenen $(x, y) \in \mathbb{Z}^2$ suchen, die die Gleichung

$$ax^2 + bxy + cy^2 = m \tag{6}$$

erfüllen, so können wir analog dazu auch die Gleichung

$$a'x'^2 + b'x'y' + c'y'^2 = m \tag{7}$$

lösen. Denn zwischen den Lösungsmengen der Gleichungen (6) und (7) besteht eine Bijektion: Jede Lösung (x', y') von (7) führt mittels Substitution zu einer Lösung $(\alpha x + \beta y, \gamma x + \delta y)$ von (6). Umgekehrt finden wir zu jeder Lösung von (6) mithilfe der inversen Transformation

$$U^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}, \text{ die uns}$$

$$\begin{aligned} x &= \delta x' - \beta y' \\ y &= -\gamma x' + \alpha y' \end{aligned}$$

liefert, eine Lösung zu (7).⁴ Diese Beziehung wird uns bei der Suche nach Lösungen von binären quadratischen Formen hilfreich sein und zudem eine Klasseneinteilung ermöglichen, weswegen wir ihr eine Bezeichnung geben:

DEFINITION 2.4 Zwei binäre quadratische Formen f und g heißen zueinander *äquivalent*⁵, wenn es eine Matrix

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \quad \text{gibt, mit} \quad f \circ U = g.$$

Wir schreiben hierfür $f \sim g$ und sagen f geht durch die Substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ in g über.

SATZ 2.2 Bei der Relation $\sim$ handelt es sich um eine *Äquivalenzrelation*, d. h. sie ist sowohl reflexiv, symmetrisch als auch transitiv.

⁴Zagier 1981: 57ff.

⁵Anm.: In vielerlei Fachliteratur wird zwischen *equivalent* und *properly equivalent*, zu Deutsch *Äquivalenz im weiteren* bzw. *Äquivalenz im engeren Sinne*, unterschieden. Der Unterschied liegt in der Zugehörigkeit der jeweiligen Matrix: *equivalent* im Falle, dass $U \in \text{GL}_2(\mathbb{Z})$ und *properly equivalent* falls U wie in der Definition (2.4) zur $\text{SL}_2(\mathbb{Z})$ gehört.

Beweis: Gegeben seien die binären quadratischen Formen $f(x, y)$, $g(x', y')$, $h(x'', y'')$ sowie die Matrizen $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $V = \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}$, beide aus der $\text{SL}_2(\mathbb{Z})$ sowie die dazugehörige Einheitsmatrix I .

Reflexivität $f \sim f$: $f \circ I = f$ mit der Einheitsmatrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Symmetrie $g \sim f$: Angenommen $f \sim g$, d. h. es gilt $f \circ U = g$. Da $U \in \text{SL}_2(\mathbb{Z})$ existiert $U^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ und ist ebenfalls aus der $\text{SL}_2(\mathbb{Z})$. Somit folgt $f = g \circ U^{-1}$ und damit $g \sim f$.

Transitivität: Gilt $f \sim g$ mit $f \circ U = g$ und $g \sim h$ mit $g \circ V = h$ so folgt daraus, dass auch $f \sim h$. Hierzu nehmen wir an, dass gemäß (4) $f(x, y)$ in $g(x', y')$ überführt und des Weiteren $g(x', y')$ durch

$$\begin{aligned} x'' &= \alpha_1 x' + \beta_1 y' \\ y'' &= \gamma_1 x' + \delta_1 y' \end{aligned} \quad \text{bzw.} \quad \begin{pmatrix} x'' \\ y'' \end{pmatrix} = V \begin{pmatrix} x' \\ y' \end{pmatrix} \quad (8)$$

in $h(x'', y'')$ übergeht. Setzen wir nun (4) in (8) ein, so erhalten wir

$$\begin{aligned} x'' &= \alpha\alpha_1 x + \alpha_1\beta y + \beta_1\gamma x + \beta_1\delta y = (\alpha\alpha_1 + \beta_1\gamma)x + (\alpha_1\beta + \beta_1\delta)y \\ y'' &= \alpha\gamma_1 x + \beta\gamma_1 y + \gamma\delta_1 x + \delta\delta_1 y = (\alpha\gamma_1 + \gamma\delta_1)x + (\beta\gamma_1 + \delta\delta_1)y. \end{aligned}$$

Mittels Matrizenschreibweise können wir dies übersichtlicher schreiben als:

$$\begin{pmatrix} x'' \\ y'' \end{pmatrix} = V \cdot U \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha\alpha_1 + \beta_1\gamma & \alpha_1\beta + \beta_1\delta \\ \alpha\gamma_1 + \gamma\delta_1 & \beta\gamma_1 + \delta\delta_1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

□

Durch den Übergang von f zu $f \circ U$ findet eine Veränderung der Koeffizienten sowohl von f , F_f als auch von D_f statt. Was die Umformung bzgl. f betrifft, so wurde diese bereits auf den Seiten 6f. beschrieben. Dort ist nachzulesen, dass die Koeffizienten durch den Übergang von $f = (a, b, c)$ zu $f \circ U = (a', b', c')$ transformiert werden zu:

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ c' &= a\beta^2 + b\beta\delta + c\delta^2. \end{aligned}$$

Mithilfe der Schreibweise von $f(x, y)$ nach (2) erhalten wir die Koeffizienten für $F_{f \circ U}$, denn

es gilt $F_{f \circ U} = U^t F_f U$:

$$\begin{aligned} f \circ U(x, y) &\stackrel{(2),(4)}{=} (\alpha x + \beta y, \gamma x + \delta y) \frac{1}{2} F_f \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix} = \\ (x, y) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^t \frac{1}{2} F_f \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} &= (x, y) U^t F_f U \begin{pmatrix} x \\ y \end{pmatrix}. \end{aligned}$$

Da es sich bei $\frac{1}{2} F_f$ um eine symmetrische Matrix handelt, liefert $U^t F_f U$ ebenfalls eine symmetrische Matrix und damit gilt die obige Behauptung, dass $F_{f \circ U} = U^t F_f U$.

Interessant und bedeutend ist die Tatsache, dass die zu einer binären quadratischen Form f mit Diskriminante D_f äquivalente Form $f \circ U$ mit $U \in \text{GL}_2(\mathbb{Z})$ ebenfalls die Diskriminante D_f besitzt, d. h.: Wenn $U \in \text{GL}_2(\mathbb{Z})$, so ist $D_f = D_{f \circ U}$.

Dies folgt aus der Definition 2.2 auf Seite 4 und der soeben bewiesenen Behauptung:

$$D_{f \circ U} = -\det F_{f \circ U} = -\det(U^t F_f U) = -(\det U)^2 \det F_f = (\det U)^2 D_f \stackrel{U \in \text{GL}_2(\mathbb{Z})}{=} D_f. \quad (9)$$

Satz 2.2 auf Seite 7 ermöglicht uns die Einteilung aller binären quadratischen Formen in sogenannte *Äquivalenzklassen*. Wir halten also fest, dass sich zwei zueinander äquivalente Formen f und g in der selben Klasse befinden, diese aufgrund der Transitivitätseigenschaft von $\sim$ dieselbe Menge von ganzen Zahlen darstellen und es eine eindeutige Beziehung zwischen den Darstellungen von f und denen von g gibt. Aufgrund dessen genügt die Betrachtung nur eines Repräsentanten von jeder Äquivalenzklasse.⁶ Jedoch stellt sich die Frage, wie man solch einen Repräsentanten findet. Um diese Frage zu beantworten, unterscheiden wir zwischen *definiten*, *indefiniten* sowie *semidefiniten*⁷ binären quadratischen Formen:

DEFINITION 2.5 Eine binäre quadratische Form f heißt

- (i) *positiv definit*, wenn $f(x, y) > 0 \quad \forall (x, y) \in \mathbb{Z}^2 \text{ mit } (x, y) \neq (0, 0)$,
- (ii) *negativ definit*, wenn $f(x, y) < 0 \quad \forall (x, y) \in \mathbb{Z}^2 \text{ mit } (x, y) \neq (0, 0)$,
- (iii) *indefinit*, wenn $\exists (x_1, y_1), (x_2, y_2) \in \mathbb{Z}^2 \text{ mit } f(x_2, y_2) < 0 < f(x_1, y_1)$,
- (iv) *positiv semidefinit*, wenn $\forall (x, y) \in \mathbb{Z}^2: f(x, y) \geq 0 \quad \text{und wenn } \exists (x_0, y_0) \in \mathbb{Z}^2 \text{ mit } f(x_0, y_0) = 0$, wobei $(x_0, y_0) \neq (0, 0)$,

⁶(Niven 1976: 175)

⁷Der semidefinite Fall wird in dieser Arbeit nicht genauer behandelt. Es sei lediglich erwähnt, dass anstelle der Gleichung $f(x, y) = m$ die nach (10) gegebene Gleichung $4af(x, y) = (2ax + by)^2 = 4am$ zu lösen ist. Demnach substituiert man am durch z^2 für ein $z \geq 0$ und löst die Gleichung $2ax + by = \pm 2z$. Das Lösen der Gleichung ist im Fall $\text{ggT}(2a, b) \mid 2z$ immer möglich. Daher besitzt $f(x, y) = m$ entweder keine oder unendlich viele Lösungen.

- (v) *negativ semidefinit*, wenn $\forall(x, y) \in \mathbb{Z}^2: f(x, y) \leq 0$ und wenn $\exists(x_0, y_0) \in \mathbb{Z}^2$ mit $f(x_0, y_0) = 0$, wobei $(x_0, y_0) \neq (0, 0)$.

Die Punkte (ii) und (v) sind insofern zu vernachlässigen, da im Falle dass f positiv definit (bzw. semidefinit) ist, $-f$ negativ definit (bzw. semidefinit) ist und umgekehrt. Ferner gilt, dass $D_{-f} = D_f$. Somit genügt es nur positiv definite, indefinite und positiv semidefinite Formen zu betrachten. Bevor wir uns einem wichtigen Satz widmen sei noch festgehalten, dass für $f = (a, b, c)$ die folgende Formel gilt:

$$4af(x, y) = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 - b^2y^2 + 4acy^2 = (2ax + by)^2 - D_f y^2. \quad (10)$$

Wie bereits erwähnt wurde, wird der Diskriminante D_f einer binären quadratischen Form f eine bedeutende Rolle zu Teil:

SATZ 2.3 Es sei $f = (a, b, c)$ eine binäre quadratische Form. Dann gilt:

- (i) f ist genau dann semidefinit, wenn $D_f = 0$.
- (ii) f ist genau dann positiv definit, wenn $D_f < 0$ und $a > 0$.
- (iii) f ist genau dann indefinit, wenn $D_f > 0$.

Beweis: (i):($\Rightarrow$): Es sei f semidefinit und vorerst $a = 0$. Dann folgt $f(x, 1) = bx + c$. Für $b \neq 0$ hätte f für genügend großes x ein anderes Vorzeichen, als für genügend kleines x und wäre demnach nicht semidefinit. Daraus folgt, dass $b = 0$ und hieraus wiederum $D_f = 0$ gilt.

Ist nun $a = f(1, 0) \neq 0$, dann ist $\forall(x, y) \in \mathbb{Z}^2 0 \leq 4af(x, y) = (2ax + by)^2 - D_f y^2$. Im Besonderen gilt für $x = -b$ und $y = 2a$, dass $0 \leq -D_f 4a^2$. Wäre $D_f < 0$, dann gilt $4af(x, y) = (2ax + by)^2 + |D_f|y^2 = 0$ nur falls $x = y = 0$. Somit ist $D_f = 0$.

($\Leftarrow$): Es sei $D_f = 0$. Ist $a = 0$, dann ist auch $b = 0$ und $\exists(x_0, y_0) \in \mathbb{Z}^2$ mit $f(x_0, y_0) = 0$ und $(x_0, y_0) \neq (0, 0)$, nämlich das Paar $(1, 0)$. Außerdem hat $f(x, y) = cy^2$ konstantes Vorzeichen.

Ist nun $a \neq 0$, so hat $4af(x, y) = (2ax + by)^2$ konstantes Vorzeichen und demnach auch f . Für das Paar $(-b, 2a)$ folgt, dass $f(-b, 2a) = 0$ gilt.

- (ii):($\Rightarrow$): Es sei f positiv definit. Demnach ist $a = f(1, 0) > 0$ und $0 < 4af(-b, 2a) = -D_f 4a^2$. Da $-4a^2 < 0$ folgt $D_f < 0$.

⁸Es gilt auch die Formel $4cf(x, y) = (2cy + bx)^2 - D_f x^2$. (Buchmann 2007: 12.)

($\Leftarrow$): Es sei $a > 0$ und $D_f < 0$. Da $b^2 - 4ac < 0$, ist außerdem $c > 0$. Dann ist

$4af(x, y) = (2ax + by)^2 + |D_f|y^2 = 0$ nur wenn $(x, y) = 0$, was laut Definition jedoch auszuschließen ist.

(iii): Die Behauptung folgt aus (i) und (ii). Denn ist f negativ definit, so ist $-f$ positiv definit. Für $-f$ positiv definit gilt nun

$$D_{-f} < 0 \quad \text{und} \quad -a > 0 \quad \Leftrightarrow \quad D_f < 0 \quad \text{und} \quad a < 0.$$

Wäre nun $D_f < 0$ und $a = 0$, würde sich $b^2 < 0$ ergeben, was jedoch unmöglich ist. $\square$

Bevor wir uns dem nächsten Kapitel widmen, soll noch auf die *Automorphismen von f* eingegangen werden. Der Grund hierfür ist, dass wenn $(x, y) \in \mathbb{Z}^2$ eine Lösung von $f(x, y) = m$ ist und U aus der Menge der Automorphismen von f stammt, so ist auch $U \begin{pmatrix} x \\ y \end{pmatrix}$ Lösung dieser Gleichung.

DEFINITION 2.6 Es sei f eine binäre quadratische Form und $U \in \text{SL}_2(\mathbb{Z})$ so, dass $f \circ U = f$. Dann heißt U ein *Automorphismus von f* . Mit A_f wird die Menge aller Automorphismen von f bezeichnet.

Die Menge A_f hat folgende Eigenschaften:

Sind nämlich U und V zwei Automorphismen von f , so sind dies auch UV und U^{-1}, V^{-1} . Außerdem besitzt A_f noch eine weitere algebraische Eigenschaft, die wir allgemein angeben möchten:

Es sei G eine Gruppe und H_1, H_2 Untergruppen von G . Gibt es ein $x \in G$ mit $H_2 = xH_1x^{-1}$, so heißen H_1 und H_2 *konjugiert in G* .⁹

SATZ 2.4 Es sei f eine binäre quadratische Form und $U \in \text{SL}_2(\mathbb{Z})$. A_f bildet eine Untergruppe von $\text{SL}_2(\mathbb{Z})$ und sie ist zu $A_{f \circ U}$ konjugiert, d. h. es gilt

$$U^{-1}A_fU = A_{f \circ U}.$$

Beweis: 1) A_f ist eine Untergruppe: Zunächst einmal ist $A_f \neq \emptyset$, denn $f \circ I = f$ und somit $I \in A_f$. Es seien $U_1, U_2 \in A_f$, d. h. $f \circ U_1 = f$ und $f \circ U_2 = f$. Aus Letzterem folgt auch $f \circ U_2^{-1} = f$. Insgesamt also gilt

$$(f \circ U_1)U_2^{-1} = f \circ U_2^{-1} = f \quad \text{und somit} \quad U_1U_2^{-1} \in A_f.$$

⁹Dies ist eine Äquivalenzrelation: $H_1 = eH_1e^{-1}$. Für $H_2 = xH_1x^{-1} \Rightarrow H_1 = x^{-1}H_2x$. Ist des Weiteren $H_3 = yH_2y^{-1}$, dann folgt $H_3 = y(xH_1x^{-1})y^{-1} = yxH_1(yx)^{-1}$.

2) $U^{-1}A_fU = A_{f \circ U}$: Es sei $V \in A_{f \circ U}$. Hieraus erhalten wir

$$f \circ UVU^{-1} = (f \circ U)VU^{-1} = f \circ UU^{-1} = f \quad \text{und demnach} \quad UVU^{-1} \in A_f.$$

Dies bedeutet aber auch, dass $V \in U^{-1}A_fU$ und damit $A_{f \circ U} \subseteq U^{-1}A_fU$. Wir erhalten umgekehrt $A_f \subseteq UA_{f \circ U}U^{-1}$, wenn f ersetzt wird durch $f \circ U$ sowie U durch U^{-1} .

□

Ziel der nächsten Kapitel ist es eine Methode anzugeben, wie Lösungen (x, y) der Gleichung $f(x, y) = m$ gefunden werden können. Dazu müssen wir wissen, wann wir zwei Formen f und g als äquivalent bezeichnen können und wie die Automorphismen von f zu bestimmen sind.

Kapitel 3

Positiv definite binäre quadratische Formen

Dieses Kapitel behandelt die positiv definiten binären quadratischen Formen, also jene Formen für die $D_f < 0$ ist. Aufgrund dessen handelt es sich bei D_f um keine Quadratzahl und es gilt $a > 0$. Insbesondere gilt auch $c > 0$, weil $c = f(0, 1)$ ist. Des Weiteren wissen wir, sollte f negativ definit sein, so ist $-f$ positiv definit. Da $\sim$ eine Äquivalenzrelation ist, können wir außerdem das Folgende festhalten:

Ist $U \in \text{SL}_2(\mathbb{Z})$ und f positiv definit, dann ist auch $f \circ U$ positiv definit.

Jedoch wissen wir noch nicht, wie wir solch eine Matrix U finden können. Hierbei sind zwei Matrizen in der $\text{SL}_2(\mathbb{Z})$ von besonderer Relevanz:

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Die $\text{SL}_2(\mathbb{Z})$ wird nämlich von den beiden Matrizen S und T erzeugt, d. h. jede Matrix aus der $\text{SL}_2(\mathbb{Z})$ kann als Produkt der Matrizen S und T und deren Inversen dargestellt werden.¹

PROPOSITION 3.1 Es sei $f = (a, b, c)$ eine binäre quadratische Form. Dann gilt:

$$(i) \quad \forall g \in \mathbb{Z} \quad \text{ist} \quad S^g = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad f \circ S^g = (a, 2ag + b, ag^2 + bg + c).$$

$$(ii) \quad T^2 = -I \quad \text{sowie} \quad f \circ T = (c, -b, a).$$

Beweis: (i): 1) $g \geq 0$ durch Induktion²:

$$g = 0 : \quad S^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

¹Dies wird u. a. durch das Korollar 3.11 gezeigt.

$$g \mapsto g+1: \quad S^{g+1} = S^g \cdot S = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & g+1 \\ 0 & 1 \end{pmatrix}.$$

$$2) \ g < 0: \text{ Da } S^{-g} = \begin{pmatrix} 1 & -g \\ 0 & 1 \end{pmatrix} \text{ folgt, dass } S^g = (S^{-g})^{-1} = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}.$$

3) Wenn wir uns zurückerinnern, so wurde bei (5) die Transformation der Koeffizienten von f durch eine ganzzahlige Matrix U beschrieben. Demnach erhalten wir für $f \circ S^g$ mit $\alpha = 1, \beta = g, \gamma = 0$ und $\delta = 1$:

$$f \circ S^g \stackrel{(5)}{=} (a', b', c') = (a, 2ag + b, ag^2 + bg + c).$$

$$(ii): \ 1) \quad T^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I.$$

2) Auch für $f \circ T$ verwenden wir wieder (5), wobei diesmal $\alpha = 0, \beta = -1, \gamma = 1$ und $\delta = 0$:

$$f \circ T = (c, -b, a).$$

□

Es soll nun ein Weg angegeben werden, um einen Repräsentanten für jede Klasse von positiv definiten binären quadratischen Formen zu finden. Hierbei ist die folgende Definition von Relevanz:

DEFINITION 3.1 Es sei $f = (a, b, c)$ positiv definit. Wir nennen f *reduziert*, wenn

$$|b| \leq a \leq c.$$

Das Ziel ist nun zu zeigen, dass in jeder Klasse mindestens eine reduzierte Form existiert. Für den Beweis des folgenden Lemmas sei noch definiert, was unter der „nächsten ganzen Zahl“ zu einer gegebenen reellen Zahl zu verstehen ist.

DEFINITION 3.2 Es sei $\varrho \in \mathbb{R}$. Dann gibt es $g \in \mathbb{Z}$ und $r \in \mathbb{R}$ mit $-\frac{1}{2} < r \leq \frac{1}{2}$, sodass $\varrho = g + r$. Dazu setzen wir mithilfe der Gaußklammer³

$$g = - \left\lfloor -\varrho + \frac{1}{2} \right\rfloor.$$

²Anm.: Bei den Beweisen durch Vollständige Induktion wird vor dem Induktionsschritt nicht explizit angegeben, dass die Behauptung bereits bis n bewiesen sei. Unter der Abkürzung „I.A.“ sei die Induktionsannahme zu verstehen.

³Für $x \in \mathbb{R}$ sei $\lfloor x \rfloor = \max\{k \in \mathbb{Z} \mid k \leq x\}$ die Gaußklammer von x .

Diese eindeutig bestimmte ganze Zahl g wird als die *nächste ganze Zahl* zu ϱ bezeichnet.

Beispiele: 1.) Es sei $\varrho = 2, 3$. Dann ist die nächste ganze Zahl

$$g = -\lfloor -2, 3 + \frac{1}{2} \rfloor = -\lfloor -1, 8 \rfloor = -(-2) = 2.$$

Für $\varrho = -2, 3$ ergibt sich $g = -2$.

2.) Es sei $\varrho = 3, 5$. Dann ist die nächste ganze Zahl $g = -\lfloor -3, 5 + \frac{1}{2} \rfloor = -\lfloor -3 \rfloor = 3$.

Ist jedoch $\varrho = -3, 5$. So erhalten wir $g = -\lfloor 3, 5 + \frac{1}{2} \rfloor = -\lfloor 4 \rfloor = -4$.

LEMMA 3.2 Es sei $f = (a, b, c)$ positiv definit. Demnach gibt es $\alpha, g \in \mathbb{Z}$, $\alpha \in \{0, 1\}$, sodass

$$f \circ T^\alpha S^g = (a_1, b_1, c_1) \quad \text{und} \quad |b_1| \leq a_1 = \min(a, c) \quad \text{gilt.}$$

Beweis: Falls $a \leq c$ so wähle $\alpha = 0$. Im Fall, dass $a > c$ sei $\alpha = 1$.

Es sei $f \circ T^\alpha = (a', b', c')$.

Nach Proposition 3.1 (ii) ist $a' = \min(a, c)$, denn falls $a \leq c$ so ist $a' = a$ bzw. bei $a > c$ ist $a' = c$. Außerdem gilt $|b'| = |b|$.

Es sei g die nächste ganze Zahl an $-\frac{b'}{2a'}$. Demnach gilt

$$\left| g + \frac{b'}{2a'} \right| \leq \frac{1}{2} \quad \text{bzw.} \quad |2a'g + b'| \leq a'.$$

Es ist

$$(a_1, b_1, c_1) = f \circ T^\alpha S^g \stackrel{\text{Prop. 3.1(i)}}{=} (a', 2a'g + b', a'g^2 + b'g + c').$$

Insgesamt erhalten wir also $a_1 = a'$ und $|b_1| = |b' + 2a'g| \leq a_1 = a' = \min(a, c)$. $\square$

SATZ 3.3 Ist $f = (a, b, c)$ positiv definit, so $\exists g_1, \dots, g_k \in \mathbb{Z}$ und ein $\alpha \in \{0, 1\}$, sodass

$$f \circ U \quad \text{mit} \quad U = T^\alpha S^{g_1} T S^{g_2} \dots T S^{g_k} \quad \text{reduziert ist.}$$

Beweis: Aufgrund von Lemma 3.2 können wir $\alpha_1 \in \{0, 1\}$ und ein $g_1 \in \mathbb{Z}$ wählen, sodass

$$f \circ T^{\alpha_1} S^{g_1} = (a_1, b_1, c_1) \quad \text{mit} \quad |b_1| \leq a_1 = \min(a, c) \quad \text{gilt.}$$

Es sei $a_0 = a$, $b_0 = b$ und $c_0 = c$. Es seien a_j, b_j, c_j für $1 \leq j < n$, $\alpha_j \in \{0, 1\}$ und $g_j \in \mathbb{Z}$ bereits gewählt.

Nach Lemma 3.2 wählen wir nun $\alpha_n \in \{0, 1\}$ und $g_n \in \mathbb{Z}$, sodass mit

$$f \circ T^{\alpha_1} S^{g_1} \dots T^{\alpha_n} S^{g_n} = (a_n, b_n, c_n) \quad \text{auch} \quad |b_n| \leq a_n = \min(a_{n-1}, c_{n-1}) \quad \text{gilt.}$$

Für $n \geq 1$ ist $1 \leq a_n \leq a_{n-1}$, sodass es ein k gibt mit $a_k = a_{k+1}$. Daraus folgt

$$|b_k| \leq a_k = a_{k+1} = \min(a_k, c_k) \leq c_k.$$

Daher ist (a_k, b_k, c_k) reduziert und $U = T^{\alpha_1} S^{g_1} \dots T^{\alpha_k} S^{g_k}$. Für ein $i > 0$ mit $\alpha_i = 0$ können wir $T^{\alpha_i} = I$ einfach weglassen. $\square$

Mithilfe dieses Wissens können wir nun eine zu f äquivalente reduzierte Form finden.

Beispiel: Wir betrachten die Form $f = (5, 14, 11)$ und erhalten dafür

$$D_f = b^2 - 4ac = -24 < 0, \quad \text{also ist } f \text{ positiv definit.}$$

Da $a < c$ folgt nach Lemma 3.2 $\alpha = 0$ und somit

$$f \circ T^0 = f \circ I = (5, 14, 11).$$

Die nächste ganze Zahl zu $-\frac{b'}{2a'} = -\frac{14}{2 \cdot 5} = -\frac{7}{5}$ ist $g_1 = -1$. Nach Präposition 3.1 (i) mit $g_1 = -1$ ergibt sich:

$$f \circ S^{-1} = (5, 4, 2).$$

Diese Form ist aber noch nicht reduziert und somit beginnen wir von vorne.

Diesmal gilt $\alpha = 1$ und daher

$$f \circ S^{-1} T \stackrel{\text{Prop. 3.1(ii)}}{=} (2, -4, 5).$$

Die nächste ganze Zahl zu $-\frac{(-4)}{4}$ ist $g_2 = 1$, also

$$f \circ S^{-1} T S^1 = (2, 0, 3).$$

Diese Form ist nun reduziert, denn es gilt $|b| \leq a \leq c$.

Mithilfe der reduzierten Form einer binären quadratischen Form f können wir noch weitere Eigenschaften von f herausfinden, die uns beim Finden von Lösungen hilfreich sind.

SATZ 3.4 Es sei $f = (a, b, c)$ eine positiv definite reduzierte binäre quadratische Form. Dann gilt:

$$(i) \quad a = \min\{f(x, y) \mid (x, y) \in \mathbb{Z}^2, (x, y) \neq (0, 0)\}.$$

$$(ii) \quad c = \min\{f(x, y) \mid (x, y) \in \mathbb{Z}^2, y \neq 0\}.$$

(iii) $a - |b| + c = \min\{f(x, y) \mid (x, y) \in \mathbb{Z}^2, xy \neq 0\}$.

(iv) $f(x, y) = a$ hat genau die folgenden Lösungen:

(a) falls $|b| \leq a < c$ $(1, 0)$ und $(-1, 0)$,

(b) falls $|b| < a = c$ $(1, 0), (-1, 0), (0, 1)$ und $(0, -1)$,

(c) falls $|b| = a = c$ $(1, 0), (-1, 0), (0, 1), (0, -1), (1, -\operatorname{sgn} b)$ und $(-1, \operatorname{sgn} b)$.

(v) $f(x, y) = a - |b| + c$, $xy \neq 0$ besitzt genau die folgenden Lösungen:

(a) falls $b \neq 0$ $(1, -\operatorname{sgn} b)$ und $(-1, \operatorname{sgn} b)$,

(b) falls $b = 0$ $(1, 1), (-1, 1), (1, -1)$ und $(-1, -1)$.

Beweis: Bevor wir die Punkte (i)-(v) beweisen, behaupten wir zunächst Folgendes:

$$\text{Ist } |xy| > 1 \text{ so folgt } f(x, y) > a - |b| + c. \quad (11)$$

Falls $|x| = |y| > 1$ ergibt sich die Behauptung aus $f(x, y) \geq ax^2 - |b|x^2 + cy^2$.

O.b.d.A. sei nun $|x| > |y|$.⁴ Wir erhalten sodann

$$(*) \quad x^2 = |x|^2 > |x||y| = |xy| \quad \text{und} \quad (**) \quad |xy| = |x||y| > |y|^2 = y^2.$$

Da nach Voraussetzung f reduziert ist gilt $|b| \leq a \leq c \Rightarrow (\diamond) \quad a - |b| \geq 0$. Folglich ist

$$\begin{aligned} f(x, y) &\geq ax^2 - |bxy| + cy^2 \stackrel{(*)}{>} a|xy| - |b||xy| + cy^2 \geq (a - |b|)|xy| + cy^2 \stackrel{(**)}{\underset{(\diamond)}{\geq}} (a - |b| + c)y^2 \\ &\geq a - |b| + c, \quad \text{d. h.} \quad f(x, y) > a - |b| + c. \end{aligned}$$

Für den Fall

$$f(x, y) \leq a - |b| + c, \quad \text{ist dann} \quad |xy| \leq 1.$$

Umgekehrt gilt für $|xy| = 1$, dass

$$f(x, y) \geq ax^2 - |bxy| + cy^2 \stackrel{|x|=1}{\underset{|y|=1}{\geq}} ax^2 - |b||x||y| + cy^2 \geq a - |b| + c.$$

(iii): Für $xy \neq 0$ ist $|xy| \geq 1$ und somit nach obiger Behauptung $f(x, y) \geq a - |b| + c$.

(v): Ist nun

$$f(x, y) [= ax^2 + bxy + cy^2] = a - |b| + c \quad \text{und} \quad xy \neq 0, \quad \text{so ist} \quad |xy| = 1.$$

⁴Sollte der umgekehrte Fall vorliegen, so vertausche man x mit y und a mit c .

Daher ist $-|b| = bxy$ und somit ergibt sich für $b \neq 0$

$$xy = -\frac{|b|}{b} = -\operatorname{sgn} b.$$

Im Fall $b = 0$ erhalten wir aus $f(x, y) = ax^2 + cy^2 = a + c$ die übrigen Lösungen.

- (i): Aus $(\diamond)$ folgt sogleich $c \leq a - |b| + c$ und weil f reduziert ist gilt auch $a[\leq c] \leq a - |b| + c$. Im Fall $f(x, y) < a$ ist also auch $f(x, y) < c$ und $f(x, y) < a - |b| + c$. Demnach ist wegen (11) und (v) $xy = 0$ und wegen (1)⁵ ergibt sich $x = y = 0$, was uns die Behauptung liefert.

- (iv): Es sei

$$f(x, y) = a \quad \text{und anfangs} \quad a - |b| + c > a, \quad \text{also} \quad |b| < c.$$

Es ist aber damit auch $f(x, y) < a - |b| + c$ und somit erneut wegen (11) $xy = 0$.

Für $y = 0$ folgt aus $f(x, 0) = ax^2 = a$, dass $x = \pm 1$.

Im Fall $x = 0$ ergibt sich $f(0, y) = cy^2 = a$. Wegen $c \geq a$ ist $y = \pm 1$ sowie $c = a$. Somit wurden die Punkte (a) und (b) gezeigt.

Falls aber $a - |b| + c = a$ so ist

$$c = |b| = a \quad \text{und} \quad f(x, y) = a - |b| + c.$$

Aufgrund von (va) erhalten wir für

$$\begin{aligned} xy \neq 0 : \quad & xy = -\operatorname{sgn} b, \\ x = 0 : \quad & y = \pm 1, \\ y = 0 : \quad & x = \pm 1. \end{aligned}$$

Dies sind genau die Lösungen von (ivc).

- (ii): Für $|xy| \geq 1$ ist nach der obigen Behauptung (11) $f(x, y) \geq a - |b| + c \geq c$.

Falls $xy = 0$ aber $y \neq 0$, so ergibt sich $f(0, y) = cy^2 \geq c$.

Also ist $c = \min\{f(x, y) \mid (x, y) \in \mathbb{Z}^2, y \neq 0\}$.

□

DEFINITION 3.3 Es sei $f = (a, b, c)$ eine positiv definite reduzierte Form.

- (i) Dann heißt a das *erste Minimum* von f .
(ii) Ist $a < c$, dann heißt c das *zweite Minimum* von f .
(iii) Gilt zudem $a < c < a - |b| + c$, so heißt $a - |b| + c$ das *dritte Minimum* von f .⁶

⁵Es gilt $f(x, y) < a \stackrel{(1)}{=} f(1, 0) \leq c \stackrel{(1)}{=} f(0, 1)$.

⁶Allgemein: Setzt man für eine binäre quadratische Form $f = (a, b, c)$ das *Minimum* von f als

Wir merken an, dass a die kleinste positive Zahl ist, die durch f dargestellt wird. Liegt der Fall vor, dass $a < f(x, y) < c$ erhalten wir wegen Satz 3.4 (ii) $y = 0$ und damit $|x| > 1$. Deswegen ist c die zweitkleinste Zahl, die durch f eigentlich dargestellt wird, wenn $a < c$.

Das dritte Minimum ergibt sich, wenn $c < f(x, y) < a - |b| + c$ gilt. Dann ist wegen Satz 3.4 (iii) $xy = 0$ und $\text{ggT}(x, y) > 1$. Insgesamt ist also $a < c < a - |b| + c$ und somit handelt es sich bei $a - |b| + c$ um die drittkleinste Zahl, die durch f eigentlich dargestellt wird.

Die soeben beschriebenen Minima einer reduzierten Form f können aber auch geometrisch gedeutet werden. Näheres dazu findet sich in Kapitel 5 Abschnitt 5.1.

3.1 Äquivalenzklassen positiv definiter binärer quadratischer Formen

Dieser Abschnitt behandelt Eigenschaften der Äquivalenzklassen und die Einteilung positiv definiter binärer quadratischer Formen in solche Klassen.

THEOREM 3.5 Zu jeder positiv definiten binären quadratischen Form $f = (a, b, c)$ gibt es eine äquivalente reduzierte Form.

Beweis: Mithilfe von Lemma 3.2 und Satz 3.3, welche uns einen Reduktionsalgorithmus erlauben, können wir zu jeder positiv definiten binären quadratischen Form f eine reduzierte Form $f \circ U$ finden. Da die Matrix U ein Produkt der Matrizen $S, T \in \text{SL}_2(\mathbb{Z})$ ist und damit selbst ein Element dieser Gruppe ist, folgt gemäß der Definition 2.4, dass $f \circ U$ äquivalent zu f ist. $\square$

Im Normalfall existiert in einer Äquivalenzklasse positiv definiter Formen nur eine reduzierte Form. Jedoch gibt es die Ausnahme, dass unter bestimmten Bedingungen sogar zwei reduzierte Formen vorliegen, welche aber von spezieller Gestalt sind:

SATZ 3.6 Es seien $f \sim g$ zwei reduzierte positiv definite binäre quadratische Formen und $f = (a, b, c) \neq g$. Dann ist $b \neq 0$ und es ist

$$\begin{array}{ll} \text{entweder} & c = a \quad \text{und} \quad g = (a, -b, a) \\ \text{oder} & a = |b| \quad \text{und} \quad g = (a, -b, c). \end{array}$$

$$\lambda_1 = \inf \{ \sqrt{|f(x, y)|} \mid (x, y) \in \mathbb{Z}^2, (x, y) \neq (0, 0) \},$$

dann erhält man ebenso die in der Definition angeführten Minima einer positiv definiten reduzierten Form. Ebenso ist es möglich, das Minimum einer reduzierten indefiniten Form anzugeben. Dabei handelt es sich um jene absolut kleinste Zahl a , welche in einer der Formen (a, b, c) der entsprechenden Kette (siehe Definition 4.8) auftritt. Somit ist das Minimum der Form $(-19, -40, 2)$ (siehe Beispiel 2.) auf Seite 71) die Zahl 2. (Buchmann 2007: 11f., 94-98, 139)

Beweis: Es sei $g = (a', b', c')$ und $f \circ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = g$ mit $\alpha\delta - \beta\gamma = 1$.

Aufgrund der Äquivalenz dieser beiden Formen stellen f und g dieselbe Menge von Zahlen dar und für $m \in \mathbb{Z}$ haben die Gleichungen $f(x, y) = m$ und $g(x, y) = m$ zudem die selbe Anzahl von Lösungen. Da nach Satz 3.4 (i) a und a' die ersten Minima sind, ist $a = a'$.

1. Fall $c > a$: Es ist nach Satz 3.4 (ii) c die zweitkleinste Zahl, die durch f eigentlich dargestellt wird. Außerdem hat $f(x, y) = a$ nach Satz 3.4 (iva) genau die beiden Lösungen $(-1, 0)$ und $(1, 0)$.

Auch $g(x, y) = a'$ verfügt demnach über genau die zwei Lösungen. Somit gilt wegen Satz 3.4 (ivb) und (ivc) $a' < c'$. Also ist c' die zweitkleinste Zahl, die durch g eigentlich dargestellt wird. Hieraus ergibt sich $c = c'$.

Da f und g auch über dieselbe Diskriminante verfügen und wir bereits $a = a'$ sowie $c = c'$ gezeigt haben, gilt

$$b^2 - 4ac = b'^2 - 4a'c' \Rightarrow |b| = |b'|.$$

Wegen $f = (a, b, c) \neq g$ ergibt sich letztendlich $b' = -b \neq 0$.

Da

$$g(1, 0) = a \stackrel{(5)}{=} a\alpha^2 + b\alpha\gamma + c\gamma^2 = f(\alpha, \gamma) = f(1, 0)$$

erhalten wir wegen Satz 3.4 (iva) $\alpha = \pm 1$ und $\gamma = 0$.

Aufgrund von $\alpha\delta - \beta\gamma = 1$ folgt sodann $\delta = \pm 1$. Da aber $f \neq g$ ist $\beta \neq 0$. Außerdem ist

$$\begin{aligned} c = c' = g(0, 1) &\stackrel{(5); \delta=\pm 1}{=} a\beta^2 + b\beta\delta + c \stackrel{\text{Satz 3.4(iii)}}{\geq} a - |b| + c, \\ \text{also } c &\geq a - |b| + c \\ \text{und damit } |b| &\geq a. \end{aligned}$$

Weil f reduziert ist daher $|b| = a$. Somit ist der Fall $g = (a, -b, c)$ erledigt.

2. Fall $c = a$: Es besitzt $f(x, y) = a$ im Fall $|b| < a$ nach Satz 3.4 (ivb) genau vier bzw. falls $|b| = a$ dann nach (ivc) genau sechs Lösungen.

Da $f \sim g$ gilt für $g(x, y) = a'$ dasselbe.

Wie bereits oben, erhalten wir wegen Satz 3.4 (iv) $c = c'$ und somit $b' = -b \neq 0$.

Dies liefert uns daher für den Fall $c = a$ und $b \neq 0$: $g = (a, -b, a)$.

□

Zu guter Letzt wollen wir noch zeigen, dass für die beiden Formen f und g auch die Umkeh-

rung gilt. Ist $b \neq 0$ und

$$\begin{aligned} c = a : \quad (a, b, a) \circ T &= (a, b, a) \circ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \stackrel{\text{Satz 3.1(ii)}}{=} (a, -b, a). \\ a = |b| : \quad (a, a, c) \circ S^{-1} &= (a, a, c) \circ \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = (a, -a, c) \text{ bzw.} \\ (a, -a, c) \circ S^1 &= (a, a, c) \circ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = (a, a, c). \end{aligned} \quad (12)$$

Wir haben nun eine Möglichkeit gefunden, um zu entscheiden ob f und g äquivalent sind, also ob die Beziehung $f \circ U = g$ gilt und wie sich solch ein $U \in \text{SL}_2(\mathbb{Z})$ finden lässt. Zuerst reduziere man f und g , d. h. man bestimme $U_1, U_2 \in \text{SL}_2(\mathbb{Z})$ derart, dass $f \circ U_1$ und $g \circ U_2$ reduziert sind. In den meisten Fällen ergibt sich daraus, wenn f und g äquivalent sind:

$$f \circ U_1 = g \circ U_2, \quad \text{also} \quad f = g \circ U_2 U_1^{-1}.$$

Es sei denn, dass einer jener Fälle vorliegt, welche im Satz 3.6 betrachtet wurden. Demnach ist

$$f \circ U_1 T = g \circ U_2 \quad \text{bzw.} \quad f \circ U_1 S^{\mp 1} = g \circ U_2.$$

Nun können wir noch eine weitere wichtige Tatsache über die Äquivalenzklassen festhalten.

SATZ 3.7 Es sei $D < 0$. Dann gibt es nur endlich viele Äquivalenzklassen positiv definiter binärer quadratischer Formen mit Diskriminante D .

Beweis: Da es in jeder Äquivalenzklasse mindestens eine reduzierte Form gibt, genügt es zu zeigen, dass es nur endlich viele reduzierte Formen mit Diskriminante D gibt.

Es sei $f = (a, b, c)$ eine reduzierte positiv definite Form und wir setzen $D_f = D$.

Aus

$$\begin{aligned} (*) \quad |b| \leq a \leq c \quad \text{erhalten wir} \quad (**) \quad b^2 \leq ac \\ \Rightarrow \quad |D| = 4ac - b^2 \stackrel{(**)}{\geq} 3ac \stackrel{(*)}{\geq} 3a^2. \end{aligned}$$

Also ist

$$a^2 \leq \frac{|D|}{3} \quad \Rightarrow \quad 1 \leq a \leq \sqrt{\frac{|D|}{3}}.$$

Demnach gilt für b und wegen $(*)$ die Beziehung

$$0 \leq |b| \leq \sqrt{\frac{|D|}{3}}.$$

Da für a und b nur endlich viele Werte in Frage kommen und c durch $D = b^2 - 4ac$ bestimmt

ist, sind auch für c nur endlich viele Werte möglich. $\square$

DEFINITION 3.4 Eine binäre quadratische Form $f = (a, b, c)$ heißt *primitiv*, wenn

$$\text{ggT}(a, b, c) = 1.$$

Beispiele: 1.) $f = (5, 15, 11)$ ist primitiv, denn der $\text{ggT}(5, 15, 11) = 1$.

2.) $f = (6, 9, 12)$ ist nicht primitiv. Es gilt $\text{ggT}(6, 9, 12) = 3 \neq 1$. Jedoch ist die Form

$$f' = \left(\frac{6}{3}, \frac{9}{3}, \frac{12}{3}\right) = (2, 3, 4) \quad \text{primitiv.}$$

PROPOSITION 3.8 ⁷ Ist $f = (a, b, c)$ eine binäre quadratische Form mit Diskriminante D , die nicht primitiv ist, d. h. $\text{ggT}(a, b, c) = g > 1$, so gilt

$$g^2 \mid D \quad \text{und} \quad f' = \left(\frac{a}{g}, \frac{b}{g}, \frac{c}{g}\right) \quad \text{ist primitiv mit Diskriminante} \quad \frac{D}{g^2}.$$

Beweis: Wir wollen zeigen, dass die Form $f' = (\frac{a}{g}, \frac{b}{g}, \frac{c}{g})$ primitiv ist, wobei $f = (a, b, c)$ eine nicht primitive Form mit $\text{ggT}(a, b, c) = g$ ist. Es ist

$$\text{ggT}\left(\frac{a}{g}, \frac{b}{g}, \frac{c}{g}\right) = \frac{1}{g} \text{ggT}(a, b, c) = \frac{1}{g} \cdot g = 1$$

und somit f' primitiv. Für die Diskriminante von f' erhalten wir folglich

$$D' = b'^2 - 4a'c' = \left(\frac{b}{g}\right)^2 - 4\frac{a}{g}\frac{c}{g} = \frac{b^2 - 4ac}{g^2} = \frac{D}{g^2}.$$

$\square$

PROPOSITION 3.9 Ist $f = (a, b, c)$ eine primitive Form und $f \sim g$, so ist auch g primitiv.

Beweis: Ist $(a, b, c) \sim (a', b', c')$ und $t \mid a$, $t \mid b$ und $t \mid c$, dann gilt wegen (5), dass t auch a' , b' und c' teilt. Wir erhalten somit $\text{ggT}(a, b, c) \mid \text{ggT}(a', b', c')$.

Aus Symmetriegründen gilt außerdem $\text{ggT}(a', b', c') \mid \text{ggT}(a, b, c)$, also insgesamt

$$\text{ggT}(a, b, c) = \text{ggT}(a', b', c').$$

$\square$

⁷(Landau 1950: 137)

Es sei nun der Anzahl der Äquivalenzklassen einer binären quadratischen Form ein Name gegeben, wobei die folgende Definition zugleich auch den indefiniten Fall berücksichtigt.

DEFINITION 3.5 Es sei $D_f < 0$ (bzw. $D_f > 0$ kein Quadrat). Die Anzahl positiv definiter (bzw. indefiniter) primitiver binärer quadratischer Formen mit Diskriminante D heißt *Klassenzahl* und wir mit $h(D)$ bezeichnen.

Die Anzahl dieser Äquivalenzklassen ist in beiden Fällen endlich. Diese Endlichkeit wurde für den Fall, dass f eine positiv definite Form ist, bereits mit Satz 3.7 gezeigt. Die Behandlung des indefiniten Falls erfolgt mit Kapitel 4 mit Satz 4.16.

Wir liefern zu der soeben definierten Klassenzahl noch folgende

Bemerkung: Gilt für $b^2 - 4ac = D \not\equiv 0, 1 \pmod{4}$, so folgt daraus: $h(D) = 0$.⁸

Ansonsten ist für $D \equiv 0, 1 \pmod{4}$ die Klassenzahl $h(D) \geq 1$, da zumindest die Grundform bzw. Hauptform (siehe (3)) mit Diskriminante D existiert.

Tatsächlich gibt es auch eine sogenannte *Klassenzahlformel* mit welcher sich $h(D)$ berechnen lässt, nämlich:

$$h(D) = \begin{cases} \frac{\omega \sqrt{|D|}}{2\pi} \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n} & \text{für } D < 0, \\ \frac{\sqrt{D}}{\log \varepsilon} \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) \frac{1}{n} & \text{für } D > 0. \end{cases}$$

Hierbei entspricht $\left(\frac{D}{n}\right)$ dem Kronecker Symbol⁹, ω der Lösungsanzahl der Gleichung¹⁰ $x^2 - Dy^2 = 4$ und

$$\varepsilon = \frac{x_0 + y_0 \sqrt{D}}{2} \quad \text{mit } x_0, y_0 \text{ der kleinsten positiven Lösung von } x^2 - Dy^2 = 4.$$

Die Komplexität der Formel ist ersichtlich und um sie zu beweisen, werden Kenntnisse über Charaktere, L -Reihen und vieles mehr benötigt. Hierfür verweise ich z. B. auf (Zagier 1981: 72-85) oder (Landau 1950: 140-152).

In diesem Gebiet gibt es noch einige offene Probleme zu lösen. Eines dieser Probleme, war jene D zu bestimmen für welche $h(D) = 1$ gilt. So ist nach dem Satz von Stark und Baker $h(D) = 1$ genau für die folgenden D erfüllt:

$$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

⁸(Zagier 1981: 61)

⁹Siehe u. a. (Landau 1950: 51f.)

¹⁰Die Anzahl der Lösungen ist in der Fußnote 19 auf Seite 75 nachzulesen.

Außerdem gilt für $D \rightarrow \infty$, $D \equiv 0, 1 \pmod{4}$, dass $h(D) \rightarrow \infty$.¹¹

Nun wollen wir einige Beispiele zur Bestimmung der Klassenzahl $h(D)$ mithilfe des Satzes 3.7 betrachten.

Beispiele: 1.) $D = -3$: Wenn f reduziert ist, dann gilt $1 \leq a \leq \sqrt{\frac{|D|}{3}}$. Daher ist

$$1 \leq a \leq \sqrt{\frac{3}{3}} = 1, \quad \text{also} \quad a = 1.$$

Aus den Bedingungen $|b| \leq a = 1$, und $b \neq 0 \Rightarrow b = \pm 1$.

Sodann folgt aus $b^2 - 4ac = 1 - 4c \stackrel{!}{=} -3$, dass $c = 1$ ist.

Somit gibt es die zwei reduzierten Formen $(1, 1, 1)$ und $(1, -1, 1)$. Diese sind nach Satz 3.6 äquivalent, weswegen $h(-3) = 1$ ist.

2.) $D = -8$: Ist f reduziert, dann gilt $1 \leq a \leq \sqrt{\frac{8}{3}} < 2$, also $a = 1$ und daher $b^2 - 4c = -8$. Somit gilt $|b| \leq a = 1$. Jedoch ist $b = \pm 1$ nicht möglich, denn sonst wäre $c \notin \mathbb{Z}$. Deshalb ist $b = 0$ und folglich $c = 2$.

Also ist $(1, 0, 2)$ die einzige reduzierten Form und $h(-8) = 1$.

3.) $D = -12$: Ist f reduziert, dann ist wegen $1 \leq a \leq \sqrt{\frac{12}{3}} = 2$ entweder $a = 1$ oder $a = 2$.

-) Für $a = 1$ ergibt sich $b^2 - 4c = -12$. Daraus sowie wegen $|b| \leq a = 1$ folgt $b = 0$. Somit ist $c = 3$ und $(1, 0, 3)$ reduziert.

-) Für $a = 2$ erhalten wir $b^2 - 8c = -12$. Aufgrund dessen und wegen $|b| \leq a = 2$ ist nur $b = \pm 2$ möglich, woraus $c = 2$ folgt.

Somit wäre zwar die Form $(2, \pm 2, 2)$ reduziert, jedoch ist diese nicht primitiv.

Daher erhalten wir insgesamt $h(-12) = 1$.

4.) $D = -39$: Ist f reduziert, dann gilt $1 \leq a \leq \sqrt{\frac{39}{3}} < 4$. Also ist entweder $a = 1$, $a = 2$ oder $a = 3$ möglich. Außerdem ist $b \neq 0$.

-) Für $a = 1$ ist $b^2 - 4c = -39$. Des Weiteren ist $|b| \leq a = 1$ und daher $b = \pm 1$. Daher ist $c = 10$. Wir erhalten die beiden zueinander äquivalenten reduzierten Formen $(1, 1, 10)$ und $(1, -1, 10)$.

-) Ist $a = 2$, dann folgt $b^2 - 8c = -39$. Wegen $|b| \leq a = 2$ ist entweder $b = \pm 1$ oder $b = \pm 2$. Jedoch ist nur $b = \pm 1$ möglich. Daraus folgt $c = 5$ und somit ergeben sich die reduzierten Formen $(2, 1, 5)$ und $(2, -1, 5)$.

¹¹u. a. (Ribenoim 2000: 120-177)

-) Im Fall $a = 3$ ist $b^2 - 12c = -39$ und $|b| \leq a = 3$. Hierbei sind jedoch $b = \pm 1$ und $b = \pm 2$ nicht möglich. Nur im Fall $b = \pm 3$ ist $c = 4 \in \mathbb{Z}$. Demnach erhalten wir die reduzierten Formen $(3, 3, 4)$ und $(3, -3, 4)$, welche zueinander äquivalent sind.

Insgesamt ergibt sich also $h(-39) = 4$.

Im Anhang auf Seite 93 finden sich weitere Beispiele zur Klassenzahl positiv definiter binärer quadratischer Formen.

3.2 Automorphismen positiv definiter binärer quadratischer Formen

Bevor wir endgültig in der Lage sind die Gleichung $f(x, y) = m$ für $m \neq 0$ zu lösen, betrachten wir erneut die Automorphismen von f .

SATZ 3.10¹² Es sei $f = (a, b, c)$ eine positiv definite reduzierte binäre quadratische Form. Dann gilt:

- (i) Für $a < c$ oder $0 < |b| < c$ gilt $A_f = \{I, -I\}$.
- (ii) Für den Fall $0 = |b| < c = a$ ist $A_f = \{I, T, T^2, T^3\}$.
- (iii) Ist $a = b = c$, so ist $A_f = \{R^i \mid 0 \leq i < 6\}$ mit $R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

Beweis: Bevor wir die Punkte (i)-(iii) beweisen, wollen wir uns an gewisse Bestimmungen zurückerinnern. Es sei gemäß Definition 2.6

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in A_f \quad \text{mit} \quad f \circ U = f.$$

Wir wissen außerdem, dass $f(\alpha, \gamma) = a$ gilt. Da

$$U^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \in A_f \quad \text{und} \quad f \circ U^{-1} = f \quad \Rightarrow \quad f(\delta, -\gamma) = a.$$

¹²Aus Satz 3.10 und wegen folgender Eigenschaft:

Es sei G eine Gruppe, $a \in G$ und $\varphi_a : G \rightarrow G$, $\varphi_a(x) = axa^{-1}$.

Dann ist φ_a ein Automorphismus, d. h. ein bijektiver Gruppenhomomorphismus von G auf sich selbst. folgt unmittelbar aufgrund von $A_{f \circ U} = U^{-1}A_fU$:

Ist $f = (a, b, c)$ eine positiv definite binäre quadratische Form, dann ist $A_f = \{I, -I\}$, außer $f \sim (a, 0, a)$, so ist $|A_f| = 4$ bzw. falls $f \sim (a, a, a)$ dann ist $|A_f| = 6$.

Außerdem gilt wegen (5) und

$$(*) : \alpha\delta - \beta\gamma = 1 \quad \Rightarrow \quad \alpha\delta + \beta\gamma = 1 + 2\beta\gamma$$

das Folgende: $[b' =] b = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \stackrel{(*)}{=} 2a\alpha\beta + b + b(2\beta\gamma) + 2c\gamma\delta$.

Damit Gleichheit herrscht muss demnach $a\alpha\beta + b\beta\gamma + c\gamma\delta = 0$ sein. Außerdem ist für $b \neq 0$ zusätzlich $\alpha \neq 0$ oder $\delta \neq 0$, ansonsten wäre nämlich $\beta\gamma = 0$.¹³

(i): 1.) Es sei $a < c$. Aufgrund von Satz 3.4 (iva) sind

$$(\alpha, \gamma), (\delta, -\gamma) \in \{(1, 0), (-1, 0)\}.$$

Daraus folgt $\gamma = 0$ und des Weiteren aus $\alpha\delta - \beta\gamma = 1$, dass $\alpha\delta = 1$ gilt. Wegen $\gamma = 0$ ergibt sich dann aus $a\alpha\beta + b\beta\gamma + c\gamma\delta = 0$: $a\alpha\beta = 0$.

Somit ist insgesamt $\beta = 0$, also $U = \pm I$.

2.) Es sei $a = c$ und $b \neq 0$. Es ist außerdem $f(\beta, \delta) = c$. Nun gilt wegen Satz 3.4 (ivb)

$$(\alpha, \gamma), (\delta, -\gamma), (\beta, \delta) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}.$$

Angenommen $\alpha = 0$, dann folgt $\gamma = \pm 1$ und daher $\delta = 0$. Dies führt aber zu einem Widerspruch: Demnach wäre $\beta = \pm 1$ und somit $b\beta\gamma = 0$ nur für $b = 0$ möglich, was jedoch ausgeschlossen wurde.

Also ist $\alpha = \pm 1$, $\gamma = 0$ und folglich $\delta = \alpha = \pm 1$, $\beta = 0$, weswegen $U = \pm I$ ist.

(ii): Es sei $b = 0$ und $a = c$. Wegen

$$f \circ T = (a, 0, a) \circ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \stackrel{(5)}{=} (a, 0, a) = f \quad \Rightarrow \quad T \in A_f.$$

T hat Ordnung¹⁴ 4 in A_f , d. h. $T^4 = I$. Daher hat A_f mindestens vier Elemente. Aufgrund von Satz 3.4 (ivb) gilt

$$(\alpha, \gamma), (\delta, -\gamma), (\beta, \delta) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}.$$

1.) Für $\alpha = 0$ erhalten wir $\gamma = \pm 1$ und $\delta = 0$. Da $\alpha\delta - \beta\gamma = 1 \Rightarrow \beta\gamma = -1$.

¹³Angenommen $b \neq 0$. Wenn $\alpha = 0$ und $\delta = 0$, so folgt daraus $b\beta\gamma = 0 \Rightarrow \beta = 0$ oder $\gamma = 0$. Daraus ergibt sich, dass entweder $\alpha = \beta = \delta = 0$ oder $\alpha = \gamma = \delta = 0$ ist. Insgesamt wäre aber $\det U = 0$ und damit U nicht Element der A_f .

¹⁴Unter der *Ordnung* eines Gruppenlements g versteht man im Fall einer endlichen Gruppe, die kleinste natürliche Zahl n für die $g^n = e$ gilt, wobei e das neutrale Element der zugehörigen Gruppe sei.

Wir erhalten höchstens zwei Automorphismen, nämlich

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{sowie} \quad -T = T^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

2.) Ist nun $\alpha = \pm 1$, so ist $\gamma = 0$, $\delta = \alpha = \pm 1$ und $\beta = 0$.

Auch hier erhalten wir höchstens zwei Automorphismen und zwar:

$$I = T^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad -I = T^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

(iii): Es sei $a = b = c$ und demnach $f = (a, a, a)$. Da

$$f \circ R = (a, a, a) \circ \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = (a, -a + 2a, a - a + a) = (a, a, a) \Rightarrow R \in A_f.$$

R hat die Ordnung 6 in A_f , denn

$$R^6 = R^3 \cdot R^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = (-I) \cdot (-I) = I.$$

Demnach hat A_f mindestens sechs Elemente. Nun sind wegen Satz 3.4 (ivc)

$$(\alpha, \gamma), (\delta, -\gamma), (\beta, \delta) \in \{(1, 0), (-1, 0), (0, 1), (0, -1), (1, -1), (-1, 1)\}$$

1.) Für $\alpha = 0$ ergibt sich $\gamma = \pm 1$ und $\beta\gamma = -1$. Daher ist $\beta \neq 0$ und $\delta \neq 0$ bzw. $\delta = \pm 1$. Somit erhalten wir höchstens zwei Automorphismen, die von folgender Gestalt sind:

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{und} \quad R^4 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

2.) Ist $\gamma = 0$, so ist $\alpha = \pm 1$ und $\delta = \pm 1$, also $\alpha = \delta$. Aus $a\alpha\beta = 0$ folgt sodann $\beta = 0$, was erneut höchstens zwei Automorphismen liefert, nämlich:

$$I = R^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad -I = R^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

3.) Bleibt noch der Fall $\alpha\gamma \neq 0$. Daraus ergibt sich $\alpha = \pm 1$ und $\gamma = \mp 1$ sowie $\alpha\gamma = -1$.

Angenommen $\delta \neq 0$. Daraus folgt $\delta = \gamma$ und $\alpha\delta = -1$. Nun wäre $\alpha\delta - \beta\gamma = -1 - \beta\gamma = 1$ und demnach $|\beta| = 2$, was jedoch nicht möglich ist. Somit erhalten wir $\delta = 0$ und daraus wiederum $\beta\gamma = -1$. Dies liefert uns höchstens die folgenden zwei Automorphismen:

$$R^5 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{und} \quad R^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

□

Das nächste Korollar macht nochmals die Bedeutung von S und T für die $\text{SL}_2(\mathbb{Z})$ deutlich. Wie bereits zu Beginn dieses Kapitels festgehalten wurde, erzeugen diese beiden Matrizen die $\text{SL}_2(\mathbb{Z})$.

KOROLLAR 3.11 Es sei $U \in \text{SL}_2(\mathbb{Z})$. Dann $\exists g_1, \dots, g_n \in \mathbb{Z}$ und ein $\alpha \in \mathbb{Z}$ mit $0 \leq \alpha < 4$, sodass

$$U = T^\alpha S^{g_1} T S^{g_2} \dots T S^{g_n}.$$

Beweis: Hierzu betrachten wir die reduzierte Form $f = (1, 0, 2)$, welche aufgrund von $D_f = -8$ positiv definit ist. Es ist

$$f \not\sim (a, 0, a) \quad \text{sowie} \quad f \not\sim (a, a, a)$$

und damit nach Satz 3.6 die einzige reduzierte Form in der Äquivalenzklasse von f . Außerdem folgt aus Satz 3.10 (i): $A_f = \{I, -I\}$.

Es sei $g = f \circ U^{-1}$. Aufgrund von Satz 3.3

$$\begin{aligned} \exists g_1, \dots, g_n \in \mathbb{Z} \quad \text{und ein} \quad \alpha \in \{0, 1\} \quad \text{mit} \quad U_1 = T^\alpha S^{g_1} T S^{g_2} \dots T S^{g_n}, \\ \text{sodass} \quad g \circ U_1 = f \circ U^{-1} U_1 \quad \text{reduziert ist.} \end{aligned}$$

Da aber f die einzige reduzierte Form in der Äquivalenzklasse von f ist, erhalten wir

$$f = f \circ U^{-1} U_1 \quad \Rightarrow \quad U^{-1} U_1 \in A_f.$$

Wegen $A_f = \{I, -I\} \quad \Rightarrow \quad U = U_1 \quad \text{oder} \quad U = T^2 U_1 = -U_1.$

□

Bevor wir nun endlich für eine positiv definite binäre quadratische Form f die Gleichung $f(x, y) = m$ lösen können, benötigen wir einen wichtigen Satz, dessen Bedeutung aber nicht nur für definite Formen von Relevanz ist.

SATZ 3.12 Es sei f eine binäre quadratische Form, D_f die Diskriminate von f und

$$f(x, y) = m \quad \text{mit} \quad m \in \mathbb{Z}, \quad m \neq 0.$$

Die Lösungsmenge von $x^2 \equiv D_f \pmod{4|m|}$, $0 \leq x < 2|m|$ sei $\{b_1, \dots, b_k\}$.
Außerdem sei für $1 \leq i \leq k$

$$c_i = \frac{1}{4m} (b_i^2 - D_f) \quad \text{und} \quad f_i = (m, b_i, c_i).$$

Die Nummerierung ist derart zu wählen, dass

$$\begin{aligned} - & f_i \sim f \quad \text{genau für} \quad 1 \leq i \leq t \leq k \quad \text{und} \\ - & U_i = \begin{pmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \quad \text{so, dass} \quad f_i = f \circ U_i. \end{aligned}$$

Die Menge der eigentlichen Lösungen von $f(x, y) = m$ ist dann gegeben durch

$$\left\{ VU_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mid 1 \leq i \leq t, V \in A_f \right\}.$$

Die Anzahl der Lösungen ist dabei gleich $t \cdot |A_f|$ (mit $0 \cdot \infty = 0$).

Beweis: Es sei $f = (a, b, c)$. Der $\text{ggT}(1, 0) = 1$, weswegen die Koordinaten von $VU_i \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ relativ prim sind. Wegen

$$V \in A_f \quad \Rightarrow \quad f \circ VU_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} = f \circ U_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} = f_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} = m.$$

Umgekehrt sei $f(x_0, y_0) = m$ und $\text{ggT}(x_0, y_0) = 1$. Nun $\exists u, v \in \mathbb{Z}$ mit $x_0v - y_0u = 1$.
Für $g \in \mathbb{Z}$ sei demnach

$$W_g = \begin{pmatrix} x_0 & u + gx_0 \\ y_0 & v + gy_0 \end{pmatrix} = \underbrace{\begin{pmatrix} x_0 & u \\ y_0 & v \end{pmatrix}}_{\in \text{SL}_2(\mathbb{Z})} \underbrace{\begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}}_{=S^g \in \text{SL}_2(\mathbb{Z})} \in \text{SL}_2(\mathbb{Z}).$$

Es sei $f \circ W_g = (\bar{a}_g, \bar{b}_g, \bar{c}_g)$. Der mittlere Koeffizient $\bar{b}_g$ hat nach (5) die folgende Gestalt:

$$\begin{aligned} \bar{b}_g &= 2ax_0(u + gx_0) + b \underbrace{(x_0v + gx_0y_0 + uy_0 + gx_0y_0)}_{x_0v + uy_0 + 2gx_0y_0} + 2cy_0(v + gy_0) \\ &= 2ax_0u + b(x_0v + uy_0) + 2cy_0v + 2g \underbrace{(ax_0^2 + bx_0y_0 + cy_0^2)}_{=f(x_0, y_0) = m} \end{aligned}$$

$$= 2ax_0u + b(x_0v + uy_0) + 2cy_0v + 2gm.$$

Somit können wir g derart wählen, dass $0 \leq |\bar{b}_g| < 2|m|$.¹⁵ Da bekanntlich

$$D_f = D_{f \circ W_g} \quad \text{also} \quad [b^2 - 4ac] D_f = \bar{b}_g^2 - 4\bar{a}_g\bar{c}_g [= D_{f \circ W_g}],$$

$$\text{und} \quad (*) \quad f \circ W_g \begin{pmatrix} 1 \\ 0 \end{pmatrix} = f(x_0, y_0) = m$$

$$\Rightarrow \quad \bar{c}_g = \frac{\bar{b}_g^2 - D_f}{4\bar{a}_g} \stackrel{(*)}{=} \frac{\bar{b}_g^2 - D_f}{4m}.$$

Demnach ist $\bar{b}_g^2 \equiv D_f \pmod{4|m|}$ und somit $f \circ W_g = f_i$ mit $1 \leq i \leq k$.

Da $f \circ W_g = f_i \sim f$, gilt $1 \leq i \leq t$. Des Weiteren ergibt sich aus

$$f \circ W_g = f_i = f \circ U_i \quad \Rightarrow \quad f \circ W_g U_i^{-1} = f \quad \text{und daher} \quad W_g U_i^{-1} =: V \in A_f.$$

Also ist

$$W_g = V U_i \quad \text{und} \quad V U_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}.$$

Es bleibt noch zu zeigen, dass die Anzahl der Lösungen gleich $t \cdot |A_f|$ ist. Hierzu müssen die

Lösungen von $V U_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ verschieden sein.

Dies erreichen wir, indem wir den Beweis liefern, dass aus

$$V \in A_f \quad \text{und} \quad V U_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} = U_j \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \Rightarrow \quad V = I \quad \text{sowie} \quad i = j.$$

Aufgrund von

$$U_j^{-1} V U_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \Rightarrow \quad \exists g, h \in \mathbb{Z} \quad \text{mit} \quad U_j^{-1} V U_i = \begin{pmatrix} 1 & g \\ 0 & h \end{pmatrix}$$

Da nun $V U_i, U_j \in \text{SL}_2(\mathbb{Z})$ ist auch $U_j^{-1} V U_i \in \text{SL}_2(\mathbb{Z})$ und daher $h = 1$.

Folglich ist

$$V U_i = U_j \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} \quad \text{also} \quad f \circ V U_i \stackrel{V \in A_f}{=} f \circ U_i = f \circ U_j \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}.$$

¹⁵Hierzu stelle man sich auf der Zahlengerade folgende halboffene Intervalle vor: $[2g|m|, 2(g+1)|m|)$ für eine ganze Zahl g . Wir können nun g so wählen, dass $\bar{b}_g$ im offenen Intervall $(-2|m|, 2|m|)$ liegt und somit $|\bar{b}_g| < 2|m|$ gilt.

Für den mittleren Koeffizienten ergibt sich aus

$$f \circ U_i = f \circ \begin{pmatrix} \alpha_j & \beta_j \\ \gamma_j & \delta_j \end{pmatrix} \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} = f \circ \begin{pmatrix} \alpha_j & \alpha_j g + \beta_j \\ \gamma_j & \gamma_j g + \delta_j \end{pmatrix} \quad \text{wegen (5):}$$

$$b_i = 2a\alpha_j\beta_j + b(\alpha_j\delta_j + \beta_j\gamma_j) + 2c\gamma_j\delta_j + 2gm = b_j + 2gm.$$

Aufgrund dessen und da $0 \leq b_i, b_j < 2|m|$

$$\Rightarrow |2gm| = |b_i - b_j| < 2|m| \quad \text{und somit} \quad g = 0.$$

Insgesamt erhalten wir

$$f_i = f \circ U_i = f \circ U_j = f_j, \quad \text{also} \quad i = j \quad \text{und daher} \quad V = I.$$

□

Es sei noch das Folgende angemerkt:

Ist f eine positiv definite Form und $h(D_f) = 1$, dann ist $t = k$. In diesem Fall gibt es nämlich nur eine Äquivalenzklasse und alle Formen f_i sind zu f äquivalent. Außerdem ist die Gleichung $f(x, y) = m$ für $m > 0$ genau dann eigentlich lösbar, wenn $b^2 \equiv D_f \pmod{4m}$ lösbar ist. Wenn wir die Anzahl der Lösungen von $b^2 \equiv D_f \pmod{4m}$, $0 \leq b < 2m$ mit r bezeichnen, dann ist die

$$\text{Anzahl der eigentlichen Lösungen von } f(x, y) = m \text{ gleich } r \cdot |A_f|.$$

Lösungsmethode:

Wir haben nun eine Strategie entwickelt, um alle eigentlichen Lösungen von $f(x, y) = m$ zu finden:

1. Finde alle Lösungen $\{b_1, \dots, b_k\}$ von $x^2 \equiv D_f \pmod{4|m|}$ mit $0 \leq x < 2|m|$.¹⁶
2. Berechne $c_i = \frac{1}{4m} (b_i^2 - D_f)$ und setze $f_i = (m, b_i, c_i)$ für $1 \leq i \leq k$.
3. Untersuche, welche der Formen f_i mit $0 \leq i \leq t (\leq k)$ zu f äquivalent sind. Für

$$1 \leq i \leq t \quad \text{sei} \quad U_i = \begin{pmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{pmatrix}, \quad \text{sodass} \quad f \circ U_i = f_i$$

4. Suche alle Automorphismen von f .

¹⁶Die Lösungen von $x^2 \equiv D_f \pmod{4|m|}$, $0 \leq x < 2|m|$ heißen die *Minimalwurzeln von f in Bezug auf m* .

5. Die Menge der eigentlichen Lösungen von $f(x, y) = m$ ist dann gegeben durch

$$\left\{ VU_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mid 1 \leq i \leq t, V \in A_f \right\}.$$

Diese Methode der Lösungsfindung soll nun anhand von Beispielen vorgeführt werden:

Beispiele: 1.) Gesucht sind alle Lösungen von $5x^2 + 14xy + 11y^2 = 15$.

Wie wir bereits auf Seite 16 festgestellt haben, ist $D_f = -24$ und

$$(5, 14, 11) \circ S^{-1}TS^1 = (2, 0, 3) \text{ reduziert, mit}$$

$$S^{-1}TS^1 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}.$$

Da $(5, 14, 11) \sim (2, 0, 3)$ genügt es, alle Lösungen von $2x^2 + 3y^2 = 15$ zu bestimmen.

Nach unserer Strategie gilt es jetzt die Kongruenz

$$b'^2 \equiv -24 \pmod{4 \cdot 15}, \quad 0 \leq b' < 2 \cdot 15 = 30 \text{ zu lösen.} \quad (13)$$

Es ist b' gerade, weswegen wir $b' = 2z$ setzen. Wir erhalten sodann

$$4z^2 \equiv -24 \pmod{4 \cdot 15} \Leftrightarrow z^2 \equiv -6 \pmod{15}.$$

Die Lösungen dieser Kongruenz sind $z = 3$ und $z = 12$. Somit ergeben sich für (13) die beiden Lösungen $b'_1 = 6$ und $b'_2 = 24$.

Mithilfe des 2. Schrittes berechnen wir nun c'_1 und c'_2 :

$$c'_1 = \frac{1}{4 \cdot 15}(36 + 24) = 1 \quad c'_2 = \frac{1}{4 \cdot 15}(576 + 24) = 10.$$

Demnach erhalten wir wegen $f_i = (m, b_i, c_i)$

$$f_1 = (15, 6, 1) \quad f_2 = (15, 24, 10).$$

Nach dem dritten Punkt unserer Lösungsmethode untersuchen wir nun, welches f_i zu f äquivalent ist. Um dies zu bestimmen, reduzieren wir f_1 und f_2 gemäß Satz 3.3.

Für f_1 und f_2 erhalten wir demnach:

$$f_1 \circ T = (1, -6, 15), \quad f_1 \circ TS^3 = (1, 0, 6).$$

$$f_2 \circ T = (10, -24, 15), \quad f_2 \circ TS = (10, -4, 1), \quad f_2 \circ TST = (1, 4, 10), \\ f_2 \circ TSTS^{-2} = (1, 0, 6).$$

Keine dieser beiden Formen ist also äquivalent zu f . Nach Satz 3.10 ist $|A_f| = 2$. Da aber weder f_1 noch f_2 äquivalent zu f ist, besitzt f keine Lösung.

- 2.) Gesucht sind alle Lösungen der diophantischen Gleichung $5x^2 + 14xy + 11y^2 = 35$, wobei erneut $D_f = -24$ und $(5, 14, 11) \circ S^{-1}TS^1 = (2, 0, 3)$ reduziert ist, wie oben angegeben. Es wurde bereits erwähnt, dass es genügt alle Lösungen von $2x^2 + 3y^2 = 35$ zu bestimmen.

1. Nach unserer Strategie gilt es jetzt die Kongruenz

$$b'^2 \equiv -24 \pmod{4 \cdot 35}, \quad 0 \leq b' < 2 \cdot 35 = 70 \quad \text{zu lösen.}$$

Es ist b' gerade, weswegen wir $b' = 2z$ setzen:

$$4z^2 \equiv -24 \pmod{4 \cdot 35} \quad \Leftrightarrow \quad z^2 \equiv -6 \pmod{35}.$$

Wir erhalten $z = 8, \quad z = 13, \quad z = 22 \quad \text{und} \quad z = 27 \quad \text{bzw.}$
 $b'_1 = 16, \quad b'_2 = 26, \quad b'_3 = 44 \quad \text{und} \quad b'_4 = 54.$

2. Wir berechnen die zugehörigen c_i 's und f_i 's für $0 \leq i \leq 4$:

$$c'_1 = \frac{1}{4 \cdot 35}(256 + 24) = 2, \quad c'_2 = \frac{1}{4 \cdot 35}(676 + 24) = 5, \\ c'_3 = \frac{1}{4 \cdot 35}(44^2 + 24) = 14, \quad c'_4 = \frac{1}{4 \cdot 35}(54^2 + 24) = 21.$$

$$f_1 = (35, 16, 2) \quad f_2 = (35, 26, 5) \quad f_3 = (35, 44, 14) \quad f_4 = (35, 54, 21).$$

3. Man berechne nun die jeweilige reduzierte Form, um eine eventuelle Äquivalenz feststellen zu können:

$$f_1 \circ TS^4 = (2, 0, 3) \\ f_2 \circ TS^3TS = (2, 0, 3) \\ f_3 \circ TSTS^{-2}TS^{-1} = (2, 0, 3) \\ f_4 \circ TSTS^{-3} = (2, 0, 3).$$

Alle diese Formen sind zu f äquivalent. Nach Satz 3.10 ist $|A_f| = 2$, weswegen es $4 \cdot 2 = 8$ eigentliche Lösungen gibt.

4.+5. Es ist

$$\begin{aligned} f_1 \circ TS^4 &= (2, 0, 3) = (5, 14, 11) \circ \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}, \quad \text{mit} \quad TS^4 = \begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix}. \\ \Rightarrow f_1 &= (5, 14, 11) \circ \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix}}_{=(TS^4)^{-1}} = (5, 14, 11) \circ \begin{pmatrix} -2 & -1 \\ 3 & 1 \end{pmatrix}. \end{aligned}$$

Die zugehörigen Lösungen lauten $(-2, 3)$ und $(2, -3)$.

$$\begin{aligned} f_2 &= (5, 14, 11) \circ \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -3 & -1 \end{pmatrix} = (5, 14, 11) \circ \begin{pmatrix} 4 & +1 \\ -1 & 0 \end{pmatrix} \\ \text{mit den Lösungen} & \quad (4, -1) \quad \text{und} \quad (-4, 1); \end{aligned}$$

$$\begin{aligned} f_3 &= (5, 14, 11) \circ \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} = (5, 14, 11) \circ \begin{pmatrix} -8 & -5 \\ 5 & 3 \end{pmatrix} \\ \text{mit den Lösungen} & \quad (-8, 5) \quad \text{und} \quad (8, -5); \end{aligned}$$

$$\begin{aligned} f_4 &= (5, 14, 11) \circ \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -4 & -3 \\ -1 & -1 \end{pmatrix} = (5, 14, 11) \circ \begin{pmatrix} 6 & 5 \\ -5 & -4 \end{pmatrix} \\ \text{mit den Lösungen} & \quad (6, -5) \quad \text{und} \quad (-6, 5). \end{aligned}$$

Insgesamt haben wir also die gewünschten acht Lösungen erhalten.

Die soeben betrachtete binäre quadratische Form $f = (5, 14, 11)$ stellt die Zahl 35 eigentlich dar, jedoch nicht die Zahl 15. Daher gibt es also nicht bei jeder binären quadratischen Form für jedes $m \in \mathbb{Z}$ eine eigentliche Lösung. Dies ist trivial für den Fall f positiv definit und $m < 0$, da es diesbzgl. keine eigentlichen Lösungen gibt.

Wie bereits im Zuge der Definition 3.3 erwähnt wurde, ist a die kleinste, c die zweitgrößte und $a - |b| + c$ drittgrößte Zahl, welche durch f eigentlich dargestellt werden, wobei f reduziert ist. In diesem Fall ist die zugehörige reduzierte Form gegeben durch $(2, 0, 3)$. Für das obige Beispiele gilt somit bzgl. des ersten Minimums von f :

$$5x^2 + 14xy + 11y^2 = 2 \quad \text{besitzt die eigentlichen Lösungen} \quad (-1, 1) \quad \text{und} \quad (1, -1).^{17}$$

¹⁷Für das zweite Minimum ergeben sich aus $5x^2 + 14xy + 11y^2 = 3$ die eigentlichen Lösungen $(2, -1), (-2, 1)$. Bezüglich dem dritten Minimum erhalten wir für $5x^2 + 14xy + 11y^2 = 5$ die eigentlichen Lösungen $(3, -2)$ und $(-3, 2)$.

Wir können aber noch eine weitere interessante Tatsache festhalten:

Stellt $f = (a, b, c)$ nämlich die Zahlen $m_1, m_2 \in \mathbb{Z}$ dar, so wird auch die Zahl am_1m_2 durch f dargestellt.

Um den entsprechenden Satz 3.13 in Kurzform zu beweisen, bedienen wir uns der folgenden Definition:

DEFINITION 3.6 Es sei $f = (a, b, c)$ eine quadratische Form mit $a \neq 0$. Dann nennt man die Nullstellen

$$w_1(f) = \frac{-b + \sqrt{D_f}}{2a} \quad \text{und} \quad w_2(f) = \frac{-b - \sqrt{D_f}}{2a}$$

des Polynoms $aX^2 + bX + c$ die *erste* bzw. die *zweite* Wurzel von f .

Nun lässt sich die binäre quadratische Form $f = (a, b, c)$ auch schreiben als:

$$\begin{aligned} f(x, y) &= ax^2 + bxy + cy^2 = y^2 \left(a \left(\frac{x}{y} \right)^2 + b \left(\frac{x}{y} \right) + c \right) = y^2 f \left(\frac{x}{y}, 1 \right) = \\ &= y^2 a \underbrace{\left(\left(\frac{x}{y} \right)^2 + \frac{b}{a} \left(\frac{x}{y} \right) + \frac{c}{a} \right)}_{\text{besitzt die Nullstellen } w_1, w_2} \stackrel{\text{Faktorisierung}}{=} y^2 a \left(\frac{x}{y} - w_1(f) \right) \left(\frac{x}{y} - w_2(f) \right) = \\ &= a \cdot y^2 \underbrace{\left(\left(\frac{x}{y} \right)^2 - \frac{x}{y} (w_1(f) + w_2(f)) + w_1(f)w_2(f) \right)}_{=x^2 - xy(w_1(f) + w_2(f)) + y^2 w_1(f)w_2(f)} = \\ &= a(x - yw_1(f))(x - yw_2(f)) \quad \forall y \in \mathbb{Z} \end{aligned}$$

SATZ 3.13 Es sei $f = (a, b, c)$ eine binäre quadratische Form und $x_1, y_1, x_2, y_2 \in \mathbb{Z}$. Für

$$x_3 = ax_1x_2 - cy_1y_2 \quad \text{und} \quad y_3 = a(x_1y_2 + x_2y_1) + by_1y_2, \quad \text{ist dann}$$

$$af(x_1, y_1)f(x_2, y_2) = f(x_3, y_3)$$

Beweis: Es sei $f = (a, b, c)$ und für $w_i(f)$, ($i = 1, 2$) schreiben wir kurz w_i .

Für $a = 0$ ist

$$0 = f(x_3, y_3) = f(-cy_1y_2, by_1y_2) = -b^2cy_1^2y_2^2 + cb^2y_1^2y_2^2.$$

Für $a \neq 0$ ist

$$\begin{aligned} (x_1 - y_1w_1)(x_2 - y_2w_1) &= x_1x_2 - w_1(y_1x_2 + x_1y_2) + y_1y_2w_1^2 = \\ &= x_1x_2 - \frac{c}{a}y_1y_2 - w_1 \left(y_1x_2 + x_1y_2 + \frac{b}{a}y_1y_2 \right) = \frac{x_3}{a} - w_1 \frac{y_3}{a} \end{aligned}$$

Ebenso erhalten wir

$$(x_1 - y_1 w_2)(x_2 - y_2 w_2) = \frac{x_3}{a} - w_2 \frac{y_3}{a}.$$

Somit ist

$$\begin{aligned} af(x_1, y_1)f(x_2, y_2) &= a \cdot a(x_1 - w_1 y_1)(x_1 - w_2 y_1) \cdot a(x_2 - w_1 y_2)(x_2 - w_2 y_2) = \\ &= a^3 \frac{1}{a^2} (x_3 - w_1 y_3)(x_3 - w_2 y_3) = f(x_3, y_3). \end{aligned}$$

□

Der soeben behandelte Satz 3.13 und sein Beweis sind für quadratische Formen hinsichtlich eines weiteren Punktes von Interesse. Gauss definierte in seinem Werk *Disquisitiones Arithmeticae* einen Kompositionsalgorithmus zwischen Äquivalenzklassen von Formen zu einer gegebenen Diskriminante. In Bezug auf binäre quadratische Formen konnte er zeigen, dass deren Äquivalenzklassen eine endliche abelsche Gruppe bilden, wobei eine der Hauptformen (3) als neutrales Element auftritt.

Sind $f_1 = (a_1, b_1, c_1)$ und $f_2 = (a_2, b_2, c_2)$ zwei binäre quadratische Formen mit gleicher Diskriminante D (kein Quadrat) für die $\text{ggT}(a_1, b_1, c_1, a_2, b_2, c_2) = 1$ gilt, dann folgt aus

$$b_1^2 - b_2^2 \equiv 0 \pmod{4}, \quad \text{dass} \quad b_1 \equiv b_2 \pmod{2} \quad \text{ist.}$$

Es lässt sich zeigen, dass für passendes $f_3 = (a_3, b_3, c_3)$

$$f_1(x_1, y_1)f_2(x_2, y_2) = f_3(x_3, y_3) \quad \text{ist mit} \quad D_{f_3} = D$$

$$x_3 = p_1 x_1 x_2 + p_2 x_1 y_2 + p_3 y_1 x_2 + p_4 y_1 y_2$$

$$y_3 = q_1 x_1 x_2 + q_2 x_1 y_2 + q_3 y_1 x_2 + q_4 y_1 y_2$$

$$\text{d. h.} \quad (x_3, y_3) = (x_1 x_2, x_1 y_2, y_1 x_2, y_1 y_2) \begin{pmatrix} p_1 & q_1 \\ p_2 & q_2 \\ p_3 & q_3 \\ p_4 & q_4 \end{pmatrix}.^{18}$$

Stellt nun f_1 die Zahl n_1 und f_2 die Zahl n_2 dar, so wird die Zahl $n_3 = n_1 n_2$ durch f_3 repräsentiert. Die so konstruierte Form f_3 heißt die aus f_1 und f_2 *komponierte* Form und die allgemeine Theorie dazu nennt man *Komposition der Formen*.¹⁹

Doch wie erhält man nun aus den *eigentlichen* Lösungen *alle* Lösungen?

Bekanntlich lässt sich jede ganze Zahl $m \neq 0$ eindeutig als Produkt einer Quadratzahl und

¹⁸Wie die jeweiligen p_i für $i = 1, 2, 3, 4$ zustande kommen ist in (Buell 1989: 55-65) oder in (Hlawka 1990: 86) nachzulesen.

¹⁹Ebd. sowie (Ribenoim 2009: 142ff.) und (Buchmann 2007: 154f.)

einer quadratfreien²⁰ Zahl schreiben, d. h.

$$m = m_0^2 m_1 \quad \text{mit} \quad m_1 \quad \text{quadratfrei und} \quad m_0 > 0.$$

SATZ 3.14 Es sei f eine binäre quadratische Form und für

$$m \in \mathbb{Z}, m \neq 0 \quad \text{sei} \quad m = m_0^2 m_1, \quad \text{wobei} \quad m_1 \quad \text{quadratfrei ist.}$$

Für $d \in \mathbb{Z}^+$ mit $d|m_0$ sei

$$M_d = \left\{ (dx, dy) \left| \text{ggT}(x, y) = 1, f(x, y) = \frac{m}{d^2} \right. \right\}.$$

Die Lösungsmenge von $f(x, y) = m$ ist dann gegeben durch die disjunkte Vereinigung: $\bigcup_{d|m_0} M_d$.

Beweis: Es sei f eine binäre quadratische Form und

$$f(u, v) = m = m_0^2 m_1 \quad \text{und} \quad m_1 \quad \text{quadratfrei sowie} \quad m_0 > 0.$$

Außerdem sei

$$\text{ggT}(u, v) = d \quad \text{woraus} \quad d > 0 \quad \text{und} \quad \text{ggT}\left(\frac{u}{d}, \frac{v}{d}\right) = 1 \quad \text{folgt.}$$

Somit ist

$$f\left(\underbrace{\frac{u}{d}}_x, \underbrace{\frac{v}{d}}_y\right) = \frac{m}{d^2}.$$

Es gilt

$$d^2|m \quad \text{bzw.} \quad d^2|m_0^2 m_1 \quad \Leftrightarrow \quad d|m_0 :$$

Gilt nämlich $d^2|m_0^2 m_1$, dann $\exists l \in \mathbb{Z}$ mit $d^2 l = m_0^2 m_1$.

Da $l \in \mathbb{Z}$, lässt sich dieses auch darstellen als $l = l_0^2 l_1$, wobei l_1 quadratfrei ist. Wir erhalten

$$d^2 l_0^2 l_1 = m_0^2 m_1$$

und wegen der Eindeutigkeit der Darstellung folgt

$$(dl_0)^2 = m_0^2 \quad \text{bzw.} \quad dl_0 = \pm m_0 \quad \text{und somit} \quad d|m_0.$$

Die Umkehrung ist trivial.

Umgekehrt sei nun

$$d|m_0, \quad \text{ggT}(x, y) = 1 \quad \text{und} \quad f(x, y) = \frac{m}{d^2}.$$

²⁰Eine ganze Zahl m heißt *quadratfrei*, wenn jeder Faktor in der Primfaktorzerlegung von m Multiplizität 1 besitzt, d. h. höchstens einmal auftritt.

Demnach ist $f(dx, dy) = m$.

Bleibt noch zu zeigen, dass die Vereinigung dieser Mengen für $d|m_0$ disjunkt ist. Gilt

-) $\text{ggT}(x, y) = \text{ggT}(x', y') = 1$,
-) $d|m_0$ als auch $t|m_0$ und
-) $f(x, y) = \frac{m}{d^2}$ sowie $f(x', y') = \frac{m}{t^2}$,

dann folgt aus $(dx, dy) = (tx', ty')$:

$$d = \text{ggT}(dx, dy) = \text{ggT}(tx', ty') = t.$$

□

Kapitel 4

Indefinite binäre quadratische Formen

Nachdem die positiv definiten binären quadratischen Formen behandelt wurden, ist es an der Zeit, auch den indefiniten Fall zu untersuchen. In diesem Kapitel ist es ebenso unser Ziel zu erkennen, wann zwei indefinite binäre quadratische Form mit der selben Diskriminante äquivalent sind. Auch für Formen mit positiver Diskriminante ist die in Definition 2.4 beschriebene Äquivalenz $\sim$ eine Äquivalenzrelation auf der Menge der indefinten Formen. D. h. es gilt:

$$f \text{ ist indefinit} \Leftrightarrow f \circ U \text{ ist indefinit}.$$

Im Unterschied zu positiv definiten Formen gilt für indefinite nicht nur $D_f > 0$, sondern auch dass die Gleichung $f(x, y) = m$ für $m \in \mathbb{Z}$, sofern sie eine Lösung hat, sogar unendlich viele Lösungen besitzt. Ein weiterer Unterschied zwischen den beiden Fällen besteht darin, dass in jeder Äquivalenzklasse zu einer gegebenen negativen Diskriminante genau eine (mit Ausnahme der Varianten aus Satz 3.6) reduzierte Form liegt. Diese „Eindeutigkeit“ besteht bei indefinten binären quadratischen Formen nicht: In einer Äquivalenzklasse können mehrere „reduzierte“ Formen liegen. Interessant dabei ist jedoch, dass diese eine *Kette*¹ bilden.

Es sollte noch darauf hingewiesen werden, dass im Gegensatz zu positiv definiten Formen nach Definition 2.5 bzw. Satz 2.3 nicht $a > 0$ und $c > 0$ gilt.

Da wir nun Formen betrachten, deren Diskriminante eine positive Zahl ist, soll auch der Fall D_f ein Quadrat betrachtet werden. Ist nämlich D_f ein Quadrat, so besitzt f eine besondere Gestalt, welche einem beim Lösen der Gleichung $f(x, y) = m$ behilflich ist. Außerdem hat die Gleichung $f(x, y) = 0$ auch nicht-triviale Lösungen². Andererseits gilt für D_f kein Quadrat, dass $f(x, y) = 0$ nur die Lösung $x = y = 0$ besitzt, weil $f(X, 1)$ für

¹In zahlreicher Literatur wird dafür auch der Begriff *Zyklus* verwendet.

²D. h. es gibt Lösungen $x, y \neq 0$.

$y \neq 0$ irreduzibel ist.

PROPOSITION 4.1 Es sei f eine binäre quadratische Form. Dann gilt:

$$D_f \text{ ist ein Quadrat} \Leftrightarrow \exists a_1, a_2, a_3, a_4 \in \mathbb{Z} \text{ mit } f(X, Y) = (a_1X + a_2Y)(a_3X + a_4Y).$$

Beweis: ($\Rightarrow$): Es sei $f = (a, b, c)$ eine binäre quadratische Form mit D_f ein Quadrat, also $D_f \in \mathbb{Z}^+$. Dann gilt für die Nullstellen x_1, x_2 von $f(X, 1) = aX^2 + bX + c$

$$x_{1,2} = \frac{-b \pm \sqrt{D_f}}{2a} \in \mathbb{Q}.$$

Da somit $f(X, 1)$ in Linearfaktoren zerfällt, ist $f(X, 1)$ reduzibel in $\mathbb{Q}[X]^3$. Doch führt dies auch zu einer Zerlegungsmöglichkeit in $\mathbb{Z}[X]^4$. Daher $\exists a_1, a_2, a_3, a_4 \in \mathbb{Z}$ mit $f(X, 1) = (a_1X + a_2)(a_3X + a_4)$, woraus die Behauptung folgt.

($\Leftarrow$): Es sei nun umgekehrt

$$f(X, Y) = (a_1X + a_2Y)(a_3X + a_4Y) = \underbrace{a_1a_3}_a X^2 + \underbrace{(a_2a_3 + a_1a_4)}_b XY + \underbrace{a_2a_4}_c Y^2.$$

Daher erhalten wir, wegen

$$D_f = (a_2a_3 + a_1a_4)^2 - 4 \cdot a_1a_3 \cdot a_2a_4 = (a_2a_3)^2 + 2a_1a_2a_3a_4 + (a_1a_4)^2 - 4a_1a_2a_3a_4 = (a_2a_3 - a_1a_4)^2,$$

dass D_f ein Quadrat ist.

□

Ist nun D_f ein Quadrat und es ist die Gleichung

$$f(x, y) = m = (a_1x + a_2y)(a_3x + a_4y), \quad m, a_1, a_2, a_3a_4 \in \mathbb{Z}$$

³Ist R ein kommutativer Ring (mit Einselement), dann bezeichnet $R[X]$ die Menge aller Polynome $f(X) = a_nX^n + \dots + a_0$ mit Koeffizienten in R . Dabei ist $R[X]$ selbst wieder ein kommutativer Ring mit Einselement.

⁴Dies folgt unmittelbar aus dem zugehörigen Lemma von Gauß, welches wir in unserem Fall wie folgt formulieren möchten:

Ist $f(X) \in \mathbb{Z}[X]$ irreduzibel in $\mathbb{Z}[X]$ und $\text{grad } f \geq 1$ dann ist $f(X)$ irreduzibel in $\mathbb{Q}[X]$.

zu lösen, so löst man analog für jeden Teiler d von m das folgende Gleichungssystem:

$$\left. \begin{array}{l} a_1x + a_2y = d \\ a_3x + a_4y = \frac{m}{d} \end{array} \right\} \quad \text{bzw.} \quad = 0 \quad \text{für} \quad m = 0.$$

Für D_f ein Quadrat, sei lediglich der folgende Spezialfall als Beispiel angeführt:

Beispiel: Es sei $f(x, y) = xy$. Dann ist $D_f = 1$ und daher ein Quadrat. Es ist leicht einzusehen, dass jedes $m \in \mathbb{Z}$ durch f darstellbar ist. Zudem erhalten wir für $m, x, y \in \mathbb{Z}$, $m \neq 0$ und $d(m)$ als die Anzahl der positiven Teiler von m , dass es genau $2d(m)$ mögliche Darstellungen von m gibt. Ist $d|m$ (mit $d > 0$), so ist ja $m = (\pm d) \cdot (\pm \frac{m}{d})$.

Wir werden nun den Fall, dass D_f kein Quadrat ist und somit $ac \neq 0$ ist, genauer analysieren.

Einerseits gilt, dass durch die Koeffizienten der binären quadratischen Form $f = (a, b, c)$ deren beiden Wurzeln $w_1(f)$, $w_2(f)$ eindeutig bestimmt sind. Andererseits ist aber auch jede Form $f = (a, b, c)$ mit Diskriminante D_f durch die Angabe *einer* ihrer Wurzeln vollständig charakterisiert und zwar im folgenden Sinne:

Besitzen zwei Formen mit derselben Diskriminante die gleiche erste (oder zweite) Wurzeln, dann sind sie identisch.

PROPOSITION 4.2 Es seien $f = (a, b, c)$ und $g = (a', b', c')$ zwei binäre quadratische Formen mit $D_f = D_g$ kein Quadrat. Gilt

$$w_1(f) = w_1(g), \quad \text{dann ist} \quad f = g.$$

Beweis: Es sei $f = (a, b, c)$, $g = (a', b', c')$ und

$$w_1(f) = w_1(g), \quad \text{also} \quad \frac{-b + \sqrt{D_f}}{2a} = \frac{-b' + \sqrt{D_g}}{2a'}.$$

Daraus folgt

$$a = a' \quad \text{und} \quad b = b'.$$

Des Weiteren gilt $D_f = D_g$, d. h.

$$b^2 - 4ac = b'^2 - 4a'c' \quad \Rightarrow \quad c = c'.$$

Insgesamt erhalten wir also $f = g$. □

Wie bereits zu Beginn des Kapitels erwähnt, gibt es auch im indefiniten Fall zu einer binären quadratischen Form f eine zu ihr äquivalente „reduzierte“ Form. Der Begriff reduziert muss hier aber erneut definiert werden, da er sich von jenem für positiv definite Formen unterscheidet. Für ein besseres Verständnis des Begriffs reduziert im indefiniten Fall, werden wir uns dem Gebiet der Kettenbrüche widmen. Dies ist nicht verwunderlich, besteht doch ein enger Zusammenhang zwischen der Reduktionstheorie indefiniter Formen und Kettenbrüchen.

4.1 (Unendliche) Kettenbrüche

DEFINITION 4.1 Es seien $a_0, a_1, \dots, a_n, c_1, \dots, c_n \in \mathbb{R}$. Ein Bruch von folgender Form

$$a_0 + \frac{c_1}{a_1 + \frac{c_2}{a_2 + \frac{c_3}{\ddots a_{n-1} + \frac{c_n}{a_n}}}} \quad \text{Kurzschreibweise: } a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_n|}{|a_n}$$

wird ein *endlicher Kettenbruch* genannt, wobei jeder Nenner ungleich 0 vorauszusetzen ist. Sind zudem alle $c_i = 1$ und $a_0 \in \mathbb{Z}$, $a_1, \dots, a_n \in \mathbb{N}$, dann heißt der Kettenbruch *regelmäßig* und man schreibt hierfür kurz $[a_0; a_1, \dots, a_n]$.

Wir definieren uns des Weiteren zwei Folgen $(p_i), (q_i)$ für $-2 \leq i \leq n$ und mit $c_0 := 1$:

$$\begin{aligned} p_i &= a_i p_{i-1} + c_i p_{i-2} & \text{für } 0 \leq i \leq n & & p_{-2} &= 0 & p_{-1} &= 1 \\ q_i &= a_i q_{i-1} + c_i q_{i-2} & \text{für } 0 \leq i \leq n & & q_{-2} &= 1 & q_{-1} &= 0. \end{aligned} \quad (14)$$

SATZ 4.3 Es seien $a_0, a_1, \dots, a_n, c_1, \dots, c_n \in \mathbb{R}$, $c_0 = 1$, $0 \leq k \leq n$ und die Folgen $(p_i), (q_i)$ gemäß (14). Dann gilt

$$(i) \quad \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ c_0 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ c_k & 0 \end{pmatrix}.$$

$$(ii) \quad \frac{p_k}{q_k} = a_0 + \frac{c_1|}{|a_1} + \cdots + \frac{c_k|}{|a_k}.$$

Beweis: Wir beweisen beide Teile des Satzes mithilfe von Induktion nach k .

$$(i): \quad k = 0: \quad p_0 \stackrel{(14)}{=} a_0 p_{-1} + c_0 p_{-2} = a_0 \cdot 1 + c_0 \cdot 0 = a_0$$

$$q_0 \stackrel{(14)}{=} a_0 q_{-1} + c_0 q_{-2} = a_0 \cdot 0 + c_0 \cdot 1 = c_0 [= 1]$$

$$\begin{aligned}
& \begin{pmatrix} p_0 & p_{-1} \\ q_0 & q_{-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ c_0 & 0 \end{pmatrix} \\
k \mapsto k+1 : & \begin{pmatrix} p_{k+1} & p_k \\ q_{k+1} & q_k \end{pmatrix} \stackrel{(14)}{=} \begin{pmatrix} p_k a_{k+1} + p_{k-1} c_{k+1} & p_k \\ q_k a_{k+1} + q_{k-1} c_{k+1} & q_k \end{pmatrix} = \\
& = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} \begin{pmatrix} a_{k+1} & 1 \\ c_{k+1} & 0 \end{pmatrix} \stackrel{\text{I.V.}}{=} \begin{pmatrix} a_0 & 1 \\ c_0 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ c_k & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{k+1} & 1 \\ c_{k+1} & 0 \end{pmatrix}.
\end{aligned}$$

(ii): Nach (i) gilt $p_0 = a_0$ und $q_0 = c_0 = 1$. Wir setzen nun

$$\begin{aligned}
(*) \quad a'_k &= a_k + \frac{c_{k+1}}{a_{k+1}}. \\
\Rightarrow \frac{p_{k+1}}{q_{k+1}} &= a_0 + \frac{c_1}{a_1} + \cdots + \frac{c_k}{a_k} + \frac{c_{k+1}}{a_{k+1}} = a_0 + \frac{c_1}{a_1} + \cdots + \frac{c_k}{a'_k} \stackrel{\text{I.V.}}{=} \frac{p'_k}{q'_k}
\end{aligned}$$

wobei $p'_k = a'_k p_{k-1} + c_k q_{k-2}$ und $q'_k = a'_k q_{k-1} + c_k q_{k-2}$ sei.

$$\begin{aligned}
\Rightarrow \frac{p'_k}{q'_k} &= \frac{a'_k p_{k-1} + c_k p_{k-2}}{a'_k q_{k-1} + c_k q_{k-2}} \stackrel{(*)}{=} \frac{(a_k + \frac{c_{k+1}}{a_{k+1}}) p_{k-1} + c_k p_{k-2}}{(a_k + \frac{c_{k+1}}{a_{k+1}}) q_{k-1} + c_k q_{k-2}} = \frac{\overbrace{a_k p_{k-1} + c_k p_{k-2}}^{= p_k} + \frac{c_{k+1}}{a_{k+1}} p_{k-1}}{\underbrace{a_k q_{k-1} + c_k q_{k-2}}_{= q_k} + \frac{c_{k+1}}{a_{k+1}} q_{k-1}} = \\
&= \frac{a_{k+1} p_k + c_{k+1} p_{k-1}}{a_{k+1} q_k + c_{k+1} q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}.
\end{aligned}$$

□

DEFINITION 4.2 Für $\xi \in \mathbb{R} \setminus \mathbb{Q}$ definieren wir den folgenden Kettenbruch:

$$\xi = a_0 + \xi_1^* \quad \text{für } a_0 \in \mathbb{Z} \quad \text{und} \quad 0 \leq \xi_1^* < 1.$$

Für $\xi_1^* = 0$, bricht der Prozess hier ab. Ist $\xi_1^* \neq 0$, dann setzen wir $\xi_1 = \frac{1}{\xi_1^*}$. Es seien a_i und ξ_j für $0 \leq i, j < n$ schon definiert. Es sei

$$\xi_n = a_n + \xi_{n+1}^* \quad \text{für } a_n \in \mathbb{Z} \quad \text{und} \quad 0 \leq \xi_{n+1}^* < 1.$$

Erneut bricht der Prozess für $\xi_{n+1}^* = 0$ hier ab, andernfalls sei $\xi_{n+1} = \frac{1}{\xi_{n+1}^*}$ und damit

$$\xi_n = a_n + \frac{1}{\xi_{n+1}}. \quad (15)$$

Zu guter Letzt setzen wir noch $\xi_0 = \xi$.

Wir erhalten für $n \geq 1$, dass $\xi_n \geq 1$ und somit $a_n \geq 1$ ist. Außerdem ist $a_n = \lfloor \xi_n \rfloor$.

Dann nennt man die zu ξ eindeutig bestimmten Zahlen a_n die *Teilnenner von ξ* . Der Bruch⁵

$$\frac{p_n}{q_n} \quad \text{mit} \quad \begin{array}{lll} p_i = a_i p_{i-1} + p_{i-2} & p_{-2} = 0 & p_{-1} = 1 \\ q_i = a_i q_{i-1} + q_{i-2} & q_{-2} = 1 & q_{-1} = 0. \end{array} \quad (\text{für } n \geq 0) \quad (16)$$

heißt der n -te *Näherungsbruch an ξ* .

Ist nun $\xi \in \mathbb{Q}$, dann bricht das soeben beschriebene Verfahren irgendwann ab, da ja der euklidische Algorithmus einmal abbricht. Anderenfalls erhält man für $\xi \notin \mathbb{Q}$ durch Induktion, dass auch $\xi_n^* \notin \mathbb{Q} \quad \forall n \in \mathbb{N}$. Da aber vor allem $\xi_n^* \neq 0$, bricht dieses Verfahren nicht ab. Insbesondere gelten für p_i, q_i die folgenden Gleichungen⁶:

$$\text{für } i \geq -1 \quad p_{i-1}q_i - p_iq_{i-1} = (-1)^i, \quad (17)$$

$$\text{für } i \geq -1 \quad p_iq_{i-1} - p_{i-1}q_i = (-1)^{i+1}, \quad (18)$$

$$\text{für } i \geq 0 \quad p_{i-2}q_i - p_iq_{i-2} = (-1)^{i-1}a_i. \quad (19)$$

Beweis:

$$\begin{aligned} (17): \quad i = -1: \quad p_{-2}q_{-1} - p_{-1}q_{-2} &\stackrel{(16)}{=} 0 - 1 = 1 = (-1)^{-1} \\ i \mapsto i+1: \quad p_iq_{i+1} - p_{i+1}q_i &\stackrel{(16)}{=} \underbrace{p_i(a_{i+1}q_i + q_{i-1}) - (a_{i+1}p_i + p_{i-1})q_i}_{= p_iq_{i-1} - p_{i-1}q_i} = (-1)^{i+1}. \end{aligned}$$

$$\begin{aligned} (18): \quad p_iq_{i-1} - p_{i-1}q_i &\stackrel{(16)}{=} (a_i p_{i-1} + p_{i-2})q_{i-1} - p_{i-1}(a_i q_{i-1} + q_{i-2}) = p_{i-2}q_{i-1} - p_{i-1}q_{i-2} = \\ &= - \underbrace{(p_{i-1}q_{i-2} - p_{i-2}q_{i-1})}_{(*)}. \end{aligned}$$

Wendet man nun (16) erneut für p_{i-1}, q_{i-1} an, so ergibt sich anstelle von (*):

$-(p_{i-2}q_{i-3} - p_{i-3}q_{i-2})$. Nach mehrmaligen Anwenden dieses Verfahrens, erhält man sodann

$$\begin{aligned} p_iq_{i-1} - p_{i-1}q_i &= (-1)^{i-1}(p_1q_0 - p_0q_1) \stackrel{(16)}{=} (-1)^{i-1} \underbrace{((a_1a_0 + 1) \cdot 1 - a_0 \cdot a_1)}_{=1} = (-1)^{i-1} = \\ &= (-1)^{i+1}. \end{aligned}$$

$$(19): \quad i = 0: \quad p_{-2}q_0 - p_0q_{-2} \stackrel{(16)}{=} 0 - p_0 \stackrel{(16)}{=} -a_0 \cdot 1 - 0 = -1 \cdot a_0 = (-1)^{-1}a_0.$$

⁵Es sei an (14) erinnert, wobei es sich nun um einen regelmäßigen Kettenbruch handelt und daher $c_i = 1$ für $0 \leq i \leq n$ gilt.

⁶(Bundschuh 2002: 222ff.), (Hardy 1958: 149)

$$\begin{aligned}
i \mapsto i+1 : \quad p_{i-1}q_{i+1} - p_{i+1}q_{i-1} &\stackrel{(16)}{=} \underbrace{p_{i-1}(a_{i+1}q_i + q_{i-1}) - (a_{i+1}p_i + p_{i-1})q_{i-1}}_{a_{i+1}(p_{i-1}q_i - p_iq_{i-1})} = \\
&\stackrel{(17)}{=} (-1)^i a_{i+1}.
\end{aligned}$$

□

Beispiel:

$$\begin{aligned}
\xi &= \frac{\sqrt{7}}{3} = \underbrace{0}_{a_0} + \underbrace{\frac{\sqrt{7}}{3}}_{\xi_1^*} \\
\frac{1}{\xi_1^*} = \xi_1 &= \frac{3}{\sqrt{7}} = \frac{3\sqrt{7}}{7} = \frac{\sqrt{63}}{7} = \underbrace{1}_{a_1} + \underbrace{\frac{\sqrt{63}-7}{7}}_{\xi_2^*}, \\
\xi_2 &= \frac{7}{\sqrt{63}-7} = \frac{7(\sqrt{63}+7)}{14} = \frac{\sqrt{63}+7}{2} = \underbrace{7}_{a_2} + \underbrace{\frac{\sqrt{63}-7}{2}}_{\xi_3^*}, \\
\xi_3 &= \frac{2}{\sqrt{63}-7} = \frac{2(\sqrt{63}+7)}{14} = \frac{\sqrt{63}+7}{7} = \underbrace{2}_{a_3} + \underbrace{\frac{\sqrt{63}-7}{7}}_{\xi_4^*=\xi_2^*}, \\
\xi_4 &= \xi_2 = \underbrace{7}_{a_4} + \xi_3^*, \\
\xi_5 &= \xi_3 = \underbrace{2}_{a_5} + \xi_2^*.
\end{aligned}$$

Also ist $\xi_i = \xi_{i+2}$ und $a_i = a_{i+2}$ beides für $i \geq 2$. Der zugehörige Kettenbruch lautet demnach $\xi = [0; 1, \overline{7, 2}]$.

SATZ 4.4 Es sei $\xi \in \mathbb{R} \setminus \mathbb{Q}$ und $n \geq 0$. Dann gilt

$$(i) \quad \xi = [a_0; a_1, \dots, a_{n-1}, \xi_n].$$

$$(ii) \quad \xi = \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}}.$$

Beweis: (i): Der Beweis erfolgt mittels Induktion nach n .

$$\begin{aligned}
n=0 : \quad \xi_0 &\stackrel{(15)}{=} a_0 + \frac{1}{\xi_1} & \xi &= \left[a_0 + \frac{1}{\xi_1} \right] = [a_0; \xi_1] \\
n \mapsto n+1 : \quad \xi_n &\stackrel{(15)}{=} a_n + \frac{1}{\xi_{n+1}} & \xi &\stackrel{I.V.}{=} [a_0; a_1, \dots, \xi_n] = \left[a_0; a_1, \dots, a_{n-1}, a_n + \frac{1}{\xi_{n+1}} \right] = \\
& & &= [a_0; a_1, \dots, a_n, \xi_{n+1}]
\end{aligned}$$

(ii): Es sei nach (16)

$$\begin{aligned} p'_n &= \xi_n p_{n-1} + p_{n-2} & \text{Satz 4.3 (ii)} & \Rightarrow \frac{p'_n}{q'_n} = [a_0; a_1, \dots, a_{n-1}, \xi_n] . \\ q'_n &= \xi_n q_{n-1} + q_{n-2} \end{aligned}$$

Schließlich führt (i) zu der gewünschten Behauptung, denn

$$\begin{aligned} [a_0; a_1, \dots, a_n, \xi_n] &= \left[a_0; a_1, \dots, a_{n-1}, a_n + \frac{1}{\xi_{n+1}} \right] = \frac{p_{n-1} \left(a_n + \frac{1}{\xi_{n+1}} \right) + p_{n-2}}{q_{n-1} \left(a_n + \frac{1}{\xi_{n+1}} \right) + q_{n-2}} = \\ &= \frac{p_n \xi_{n+1} + p_{n-1}}{q_n \xi_{n+1} + q_{n-1}} . \end{aligned}$$

□

SATZ 4.5 (i) Es sei $\xi \in \mathbb{R} \setminus \mathbb{Q}$ mit den Näherungsbrüchen $\frac{p_n}{q_n}$. Dann gilt

$$\lim_{n \rightarrow \infty} \frac{p_n}{q_n} = \xi .$$

(ii) Ist $a_0 \in \mathbb{Z}$, $(a_n)_{n \geq 1}$ eine Folge natürlicher Zahlen und $\frac{p_n}{q_n} = [a_0; a_1, \dots, a_n]$ für $n \geq 0$,
so

$$\exists \lim_{n \rightarrow \infty} \frac{p_n}{q_n} \quad \text{und ist irrational.}$$

Beweis: (i): Für die nach (16) definierten Folgen $(p_i), (q_i)$ gilt

$$q_0 = a_0 \underbrace{q_{-1}}_{=0} + \underbrace{q_{-2}}_{=1} = 1 \quad \text{und somit} \quad q_k \in \mathbb{N} .$$

Außerdem ist $(q_i)_{i \geq 1}$ streng monoton steigend: Aus $q_{i-1} \geq 1$ folgt nämlich

$$q_{i+1} = a_{i+1} q_i + q_{i-1} > a_{i+1} q_i \geq q_i .$$

Es gilt des Weiteren $q_i \geq q_{i-1} + q_{i-2}$ für $i \geq 1$, woraus folgt

$$q_i \geq i \quad \text{für} \quad i \geq 1 .^7 \tag{20}$$

⁷(Bundschuh 2002: 223).

Da nun für $n \geq 0$

$$\begin{aligned} \xi - \frac{p_n}{q_n} &\stackrel{\text{Satz 4.5 (ii)}}{=} \frac{p_n \xi_{n+1} + p_{n-1}}{q_n \xi_{n+1} + q_{n-1}} - \frac{p_n}{q_n} = \frac{(p_n \xi_{n+1} + p_{n-1})q_n - p_n(q_n \xi_{n+1} + q_{n-1})}{(q_n \xi_{n+1} + q_{n-1})q_n} = \\ &= \frac{p_{n-1}q_n - p_n q_{n-1}}{(q_n \xi_{n+1} + q_{n-1})q_n} \stackrel{(17)}{=} \frac{(-1)^n}{(q_n \xi_{n+1} + q_{n-1})q_n} \end{aligned}$$

und wegen

$$\begin{aligned} q_n \xi_{n+1} + q_{n-1} &\stackrel{(15)}{>} q_n a_{n+1} + q_{n-1} = q_{n+1} \quad \text{folgt sodann} \\ \left| \xi - \frac{p_n}{q_n} \right| &< \frac{1}{q_n q_{n+1}} \stackrel{(20)}{\leq} \frac{1}{n(n+1)} \rightarrow 0 \quad (\text{für } n \rightarrow \infty). \end{aligned}$$

Aufgrund dessen gilt $\lim_{n \rightarrow \infty} \frac{p_n}{q_n} = \xi$.

(ii): 1.) Für $n \geq 0$ ist

$$\frac{p_n}{q_n} = \sum_{i=0}^{n-1} \left(\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} \right) + \frac{p_0}{q_0}.$$

Außerdem erhalten wir für

$$\begin{aligned} \sum_{i=1}^{n-1} \underbrace{\left| \frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} \right|}_{= \left| \frac{p_{i+1}q_i - p_i q_{i+1}}{q_{i+1}q_i} \right|} &\stackrel{(18)}{=} \sum_{i=1}^{n-1} \frac{1}{q_i q_{i+1}} \stackrel{(20)}{\leq} \sum_{i=1}^{n-1} \frac{1}{i(i+1)} \stackrel{(*)}{=} 1 - \frac{1}{n}, \\ \text{wobei } (*) &= \sum_{i=1}^{n-1} \left(\frac{1}{i} - \frac{1}{i+1} \right) = \left(1 - \frac{1}{2} \right) + \left(\frac{1}{2} - \frac{1}{3} \right) + \dots + \left(\frac{1}{n-2} - \frac{1}{n-1} \right) + \\ &+ \left(\frac{1}{n-1} - \frac{1}{n} \right) \end{aligned}$$

Da die Reihe $\sum_{i=1}^{n-1} \frac{1}{i(i+1)}$ eine konvergente Majorante⁸ ist folgt, dass die Reihe

$$\sum_{i=0}^{\infty} \left(\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} \right)$$

absolut konvergiert und daher der Grenzwert existiert.

2.) Angenommen $\xi \in \mathbb{Q}$ und es sei

$$\xi := \lim_{n \rightarrow \infty} \frac{p_n}{q_n} = \frac{a}{b} \quad \text{mit} \quad \text{ggT}(a, b) = 1 \quad \text{und} \quad b > 0.$$

⁸Eine konvergenten Majorante ist eine konvergente Reihe $\sum_{i=0}^{\infty} c_k$ mit der Eigenschaft $0 \leq |a_k| \leq c_k$, sodass die Reihe $\sum_{i=0}^{\infty} a_k$ absolut konvergiert, d. h. wiederum $\sum_{i=0}^{\infty} |a_k|$ ist konvergent.

Da die Folge $(q_k)_{k \geq 1}$ streng monoton steigend ist, gibt es ein $n \in \mathbb{N}$ mit $b < q_{2n+1}$.
Nun gilt außerdem

$$\begin{aligned} \left(\frac{p_{2k}}{q_{2k}} \right)_{k \geq 0} & \text{ ist streng monoton steigend,} \\ \left(\frac{p_{2k+1}}{q_{2k+1}} \right)_{k \geq 0} & \text{ ist streng monoton fallend.} \end{aligned}$$

Denn für $k \geq 2$ sind $a_k, q_k, q_{k-2} > 0$ und wegen (19) erhalten wir

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k a_k}{q_{k-2} q_k} \quad \begin{cases} > 0 & \text{für } k \text{ gerade.} \\ < 0 & \text{für } k \text{ ungerade.} \end{cases}$$

Es ist somit

$$\begin{aligned} \frac{p_{2n}}{q_{2n}} &< \sup_{k \geq 0} \frac{p_{2k}}{q_{2k}} = \xi = \inf_{k \geq 0} \frac{p_{2k+1}}{q_{2k+1}} < \frac{p_{2n+1}}{q_{2n+1}} \\ \Rightarrow \quad 0 &< \xi - \frac{p_{2n}}{q_{2n}} = \frac{a}{b} - \frac{p_{2n}}{q_{2n}} < \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} \stackrel{(17)}{=} \frac{1}{q_{2n} q_{2n+1}}. \end{aligned}$$

Daher erhalten wir für diese Ungleichungskette nach Multiplikation mit $bq_{2n} > 0$ und wegen $b < q_{2n+1}$ für ein $n \in \mathbb{N}$

$$0 < aq_{2n} - bp_{2n} < \frac{b}{q_{2n+1}} < 1.$$

Da nun aber $a, b, p_n, q_n \in \mathbb{Z}$ besagt die obige Ungleichungskette, dass zwischen 0 und 1 eine ganze Zahl liegen muss. Das ist aber unmöglich. Aufgrund des Widerspruchs zur Annahme erhalten wir also $\xi \in \mathbb{R} \setminus \mathbb{Q}$. □

DEFINITION 4.3 Es sei $\frac{p_n}{q_n} = [a_0; a_1, \dots, a_n]$ für $n \geq 0$ und $a_0 \in \mathbb{Z}$ sowie $a_1, \dots, a_n \in \mathbb{N}$.
Für

$$[a_0; a_1, \dots] := \lim_{n \rightarrow \infty} \frac{p_n}{q_n} = \lim_{n \rightarrow \infty} a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n}}}}$$

heißt dann $[a_0; a_1, \dots]$ der *unendliche Kettenbruch mit den Teilnennern* $(a_i)_{i \geq 0}$.

Ein unendlicher Kettenbruch heißt des Weiteren *periodisch*, wenn es ganze Zahlen

$$v \geq 0 \quad \text{und} \quad l \geq 1 \quad \text{gibt, mit} \quad a_{n+v+l} = a_{n+v} \quad \text{für alle} \quad n \geq 0,$$

$$\text{d. h.} \quad a_{v+l} = a_v, \quad a_{v+l+1} = a_{v+1} \quad \text{usw.}$$

Wir schreiben hierfür

$$[a_0; a_1, \dots, a_{v-1}, \overline{a_v, a_{v+1}, \dots, a_{v+l-1}}].$$

Dabei nennt man das kleinste solcher v die *Länge der Vorperiode* bzw. das kleinste solcher l die *Länge der Periode*. Der Kettenbruch heißt *reinperiodisch*, wenn $v = 0$ ist.

Es lässt sich zeigen, dass jedes $\xi \in \mathbb{R} \setminus \mathbb{Q}$ sich in eindeutiger Weise in einen Kettenbruch entwickeln lässt. D. h. es gibt genau eine Folge $(a_n)_{n \geq 0}$ ganzer Zahlen, für die $a_n \in \mathbb{N}$ mit $n \geq 1$ und $\xi = [a_0; a_1, \dots]$ gilt.⁹

Insbesondere gilt für $\xi = [a_0; a_1, \dots, a_{v-1}, \overline{a_v, a_{v+1}, \dots, a_{v+l-1}}]$: $\xi_v = \xi_{v+l}$.

Da es uns bzgl. den indefiniten binären quadratischen Formen ein Anliegen ist, zu entscheiden wann zwei Formen äquivalent sind, wollen wir nun die Kettenbruchentwicklung äquivalenter Zahlen betrachten. In dem folgenden Abschnitt 4.2 wird sich zeigen, dass zwei komplexe Zahlen ξ und η äquivalent sind ($\xi \simeq \eta$), wenn es ein $U \in \text{GL}_2(\mathbb{Z})$ gibt mit $\xi = \mathcal{T}_U(\eta)$. Dieser Abschnitt wird uns auch im Kapitel 5 erneut von Hilfe sein.

4.2 Die Abbildung $\mathcal{T}_U(z)$ und die komplexe Zahlenebene

Wir setzen

$$\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\} \quad \text{und} \quad \mathbb{C}^* = \mathbb{C} \setminus \{0\}.$$

Außerdem ordnen wir jeder Matrix

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{mit Eintragungen aus den komplexen Zahlen und} \quad \det U \neq 0$$

die folgende Abbildung zu

$$\mathcal{T}_U : \overline{\mathbb{C}} \rightarrow \overline{\mathbb{C}}, \quad z \mapsto \frac{\alpha z + \beta}{\gamma z + \delta} \tag{21}$$

$$\text{mit} \quad \mathcal{T}_U(\infty) = \frac{\alpha}{\gamma}, \quad \mathcal{T}_U\left(\frac{-\delta}{\gamma}\right) = \infty, \quad \frac{a}{0} = \infty \quad \text{für} \quad a \in \mathbb{C}^* \quad \text{und} \quad (\gamma, \delta) \neq 0$$

Eine solche Abbildung nennt man auch Möbiustransformation. Wir wollen nun über die Abbildung $\mathcal{T}_U$ mehr in Erfahrung bringen.

⁹Siehe hierzu z. B. (Bundschuh 2002: 226).

PROPOSITION 4.6 Es seien $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, V = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$ Matrizen komplexer Zahlen deren Determinante $\neq 0$ ist. Dann gilt:

- (i) $\mathcal{T}_{U \circ V} = \mathcal{T}_U \circ \mathcal{T}_V$.
- (ii) $\mathcal{T}_I = \text{id}_{\overline{\mathbb{C}}}$ die Identität auf $\overline{\mathbb{C}}$.
- (iii) $\mathcal{T}_{U^{-1}} = \mathcal{T}_U^{-1}$.
- (iv) Sind $U, V \in \text{GL}_2(\mathbb{Z})$ und gilt $\mathcal{T}_U = \mathcal{T}_V$, so ist $U = V$ oder $U = -V$.

Beweis: (i) : Es seien U und V wie oben angeführt. Dann ist

$$U \cdot V = \begin{pmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' \end{pmatrix}$$

und deswegen

$$\begin{aligned} \mathcal{T}_{U \circ V}(z) &\stackrel{(21)}{=} \frac{(\alpha\alpha' + \beta\gamma')z + \alpha\beta' + \beta\delta'}{(\gamma\alpha' + \delta\gamma')z + \gamma\beta' + \delta\delta'} = \frac{\frac{\alpha\alpha'z + \beta\gamma'z + \alpha\beta' + \beta\delta'}{\gamma'z + \delta'}}{\frac{\gamma\alpha'z + \delta\gamma'z + \gamma\beta' + \delta\delta'}{\gamma'z + \delta'}} \\ &= \frac{\alpha \frac{\alpha'z + \beta'}{\gamma'z + \delta'} + \beta}{\gamma \frac{\alpha'z + \beta'}{\gamma'z + \delta'} + \delta} = \mathcal{T}_U(\mathcal{T}_V(z)) \quad \text{für } z \in \overline{\mathbb{C}}. \end{aligned}$$

$$(ii) : \text{ Da } I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ folgt } \mathcal{T}_I(z) = \frac{z}{1} = z = \text{id}_{\overline{\mathbb{C}}}.$$

(iii) : Es ist

$$\text{id}_{\overline{\mathbb{C}}} \stackrel{(ii)}{=} \mathcal{T}_I = \mathcal{T}_{UU^{-1}} \stackrel{(i)}{=} \mathcal{T}_U \circ \mathcal{T}_{U^{-1}} \quad \text{sowie} \quad \mathcal{T}_{U^{-1}} \circ \mathcal{T}_U = \text{id}_{\overline{\mathbb{C}}}.$$

(iv) : Es sei zunächst $V = I$. Für alle $z \in \overline{\mathbb{C}}$ folgt wegen $\mathcal{T}_U(z) = \mathcal{T}_I(z) = z$ für alle z :

$$\frac{\alpha z + \beta}{\gamma z + \delta} = z.$$

Daraus ergibt sich

$$\alpha z + \beta = \gamma z^2 + \delta z \quad \Leftrightarrow \quad \gamma z^2 + (\delta - \alpha)z - \beta = 0$$

und somit $\gamma = 0, \beta = 0$ und $\delta = \alpha$.

Da $\alpha^2 = 1$ erhalten wir $U = \pm I$. Es sei nun V beliebig.

Wegen $\mathcal{T}_U = \mathcal{T}_V \Rightarrow \mathcal{T}_{UV^{-1}} = I$.

Somit ist $UV^{-1} = \pm I$ also $U = \pm V$.

□

DEFINITION 4.4 Zwei komplexe Zahlen ξ und η heißen *äquivalent*, wenn

$$\exists U \in \mathrm{GL}_2(\mathbb{Z}) \quad \text{mit} \quad \xi = \mathcal{T}_U(\eta).$$

Die Schreibweise hierfür lautet $\xi \simeq \eta$.

Es ist „ $\simeq$ “ eine Äquivalenzrelation, denn:

- 1.) $\xi \simeq \xi$ folgt aus $U = I$, da $\mathcal{T}_I = \mathrm{id}_{\mathbb{C}} \in \mathbb{C}$.
- 2.) Wenn $\xi = \mathcal{T}_U(\eta)$, dann ist $\eta = \mathcal{T}_{U^{-1}}(\xi)$ und damit $\eta \simeq \xi$.
- 3.) Es sei $\xi \simeq \eta$ und $\eta \simeq \sigma$. Dann ist

$$\xi = \mathcal{T}_U(\eta) = \mathcal{T}_U(\mathcal{T}_V(\sigma)) \stackrel{\text{Prop. 4.6 (i)}}{=} \mathcal{T}_{UV}(\sigma)$$

und wegen $UV \in \mathrm{GL}_2(\mathbb{Z})$ erhalten wir $\xi \simeq \sigma$.

Die nächste Proposition soll nun Aufschluss über die Beziehung zwischen der Abbildung $\mathcal{T}$ und der ersten Wurzel von f , d. h. $w_1(f)$ geben.

PROPOSITION 4.7 Es sei $f = (a, b, c)$ eine binäre quadratische Form, D_f kein Quadrat und $U \in \mathrm{SL}_2(\mathbb{Z})$. Für $i = 1, 2$ ist dann

$$\mathcal{T}_U(w_i(f \circ U)) = w_i(f).$$

Beweis: Es genügt die Behauptung für $U = S$ und $U = T$ zu zeigen, da nach Korollar 3.11 die $\mathrm{SL}_2(\mathbb{Z})$ von den beiden Matrizen S und T erzeugt wird und daher jede Matrix $U \in \mathrm{SL}_2(\mathbb{Z})$ durch S und T darstellbar ist.

- 1.) Es sei $U = S$. Dann ist nach Proposition 3.1 (i) für $g = 1$

$$f \circ S = (a, 2a + b, a + b + c).$$

Außerdem gilt

$$S^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad \text{und daher} \quad (*) \quad \mathcal{T}_{S^{-1}}(w_i(f)) = \frac{1 \cdot w_i(f) - 1}{0 \cdot w_i(f) + 1} = w_i(f) - 1.$$

Es ist somit

$$\begin{aligned} w_i(f \circ S) &= \frac{-(2a+b) \pm \sqrt{D_f}}{2a} = \frac{-b \pm \sqrt{D_f} - 2a}{2a} = w_i(f) - 1 = \\ &\stackrel{(*)}{=} \mathcal{T}_{S^{-1}}(w_i(f)) \quad \text{für } i = 1, 2. \end{aligned}$$

2.) Nun sei $U = T$. Nach Proposition 3.1 (ii) ist $f \circ T = (c, -b, a)$.

Da $T^{-1} = -T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ist sodann

$$(**) \quad \mathcal{T}_{T^{-1}}(w_i(f)) = \frac{0 \cdot w_i(f) + 1}{-1 \cdot w_i(f) + 0} = -\frac{1}{w_i(f)}.$$

Daraus erhalten wir

$$\begin{aligned} w_i(f \circ T) &= \frac{b \pm \sqrt{D_f}}{2c} = \frac{b \pm \sqrt{D_f}}{2c} \cdot \frac{b \mp \sqrt{D_f}}{b \mp \sqrt{D_f}} = \frac{4ac}{2c(b \mp \sqrt{D_f})} = \frac{2a}{b \mp \sqrt{D_f}} = \\ &= -\frac{1}{w_i(f)} \stackrel{(**)}{=} \mathcal{T}_{T^{-1}}(w_i(f)) \quad \text{für } i = 1, 2. \end{aligned}$$

Gilt nun für alle Formen f die Behauptung für U , dann ist sie auch für U^{-1} gültig. Hierzu ersetze man einfach f durch $f \circ U^{-1}$.

Ist die Behauptung außerdem für U und V bewiesen, dann gilt sie auch für UV . Denn

$$w_i(f \circ UV) = \mathcal{T}_{V^{-1}}(w_i(f \circ U)) = \mathcal{T}_{V^{-1}}(\mathcal{T}_{U^{-1}}(w_i(f))) = \mathcal{T}_{(UV)^{-1}}(w_i(f)) \quad \text{für } i = 1, 2.$$

Wie zu Beginn des Beweises angeführt, wird die $\text{SL}_2(\mathbb{Z})$ durch S und T erzeugt, woraus die Behauptung folgt. $\square$

4.3 Die Theorie der Kettenbrüche und die Abbildung $\mathcal{T}_U(z)$ in Bezug auf indefinite binäre quadratische Formen

Nun können wir unser Wissen über die Abbildung $\mathcal{T}_U(z)$ sowie jenes über die Theorie der Kettenbrüche auch auf indefinite binäre quadratische Formen anwenden.

LEMMA 4.8

Ist $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$, $0 \leq \delta \leq \gamma$ und gilt $\begin{cases} \det U = -1 & \text{falls } \delta = 0, \\ \det U = 1 & \text{falls } \delta = \gamma, \end{cases}$

so existiert ein $n \geq 0$ sowie ein endlicher Kettenbruch $[a_0; a_1, \dots, a_n]$ mit

$$U = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}.$$

Es gilt zudem $\forall \xi > 1 \quad \text{ist} \quad \mathcal{T}_U(\xi) = [a_0; a_1, \dots, a_n, \xi]$.

Beweis: Es ist $\gamma > 0$ und wir setzen $\frac{\alpha}{\gamma} = [a_0; a_1, \dots, a_n]$. Wir wählen $n \geq 0$ derart, dass

$$(*) \quad \det U = p_n q_{n-1} - p_{n-1} q_n \stackrel{(18)}{=} (-1)^{n+1}.$$

Da $U \in \text{GL}_2(\mathbb{Z})$, also $\alpha\delta - \beta\gamma = \pm 1$, ergibt sich, dass $\text{ggT}(\alpha, \gamma) = 1$. Wegen $\gamma > 0$ erhalten wir außerdem

$$(\diamond) \quad p_n = \alpha \quad \text{und} \quad q_n = \gamma \quad \Rightarrow \quad (**) \quad p_n \delta - \beta q_n = \det U.$$

Somit erhalten wir durch Gleichsetzen von $(*)$ und $(**)$ das Folgende:

$$\begin{aligned} p_n \delta - \beta q_n = p_n q_{n-1} - p_{n-1} q_n & \Leftrightarrow p_n (\delta - q_{n-1}) - q_n (\beta - p_{n-1}) = 0 \\ & \Rightarrow q_n | \delta - q_{n-1}. \end{aligned}$$

$\delta = 0$: Aufgrund dessen, dass $\gamma > 0$ und wegen $\det U = -1 = -\beta\gamma$ ergibt sich

$$(\diamond\diamond) \quad \beta = \gamma = 1.$$

Für $n = 0$ und wegen (16) sind demnach die Eintragungen von U gegeben durch

$$\begin{aligned} p_0 &= a_0 \stackrel{(\diamond)}{=} \alpha & p_{-1} &= 1 \stackrel{(\infty)}{=} \beta \\ q_0 &= 1 \stackrel{(\diamond)}{=} \gamma & q_{-1} &= 0 = \delta. \end{aligned}$$

$\delta = \gamma$: In diesem Fall ist $\det U = 1$, also $\delta = \gamma = 1$ und somit $\alpha - \beta = 1$. Es sei nun $n = 1$ und $\alpha = [a_0; a_1] = [a_0 - 1; 1]$ (dies ergibt sich aus $a_i = (a_i - 1) + \frac{1}{1}$ für $a_i > 1$)¹⁰, womit wir zu den folgenden Eintragungen von U gelangen

$$\begin{aligned} p_1 &= a_0 \stackrel{(\diamond)}{=} \alpha & p_0 &= a_0 - 1 \\ q_1 &= 1 \stackrel{(\diamond)}{=} \gamma & q_0 &= 1 = \delta. \end{aligned}$$

Wegen $\alpha - \beta = 1$ folgt zuletzt, dass $\beta = p_0$.

$0 < \delta < \gamma$: Aus der angeführten Bedingung folgt nun mittels Subtraktion von q_{n-1} und aufgrund der Tatsache, dass die Folge $(q_n)_{n \geq 1}$ streng monoton steigend ist, das Folgende

$$-q_n \leq -q_{n-1} < \delta - q_{n-1} < \gamma - q_{n-1} \stackrel{(\diamond)}{=} q_n - q_{n-1} \leq q_n.$$

Da nun $q_n | \delta - q_{n-1}$ ist daher

$$\delta = q_{n-1} \quad \Rightarrow \quad \beta = p_{n-1}$$

Die letzte Behauptung folgt unmittelbar aus Satz 4.4. Denn

$$\mathcal{T}_U(\xi) = \frac{p_n \xi + p_{n-1}}{q_n \xi + q_{n-1}} = [a_0; a_1, \dots, a_n, \xi].$$

□

SATZ 4.9 Sind $\xi, \eta \in \mathbb{R} \setminus \mathbb{Q}$ mit $\xi = [a_0; a_1, \dots]$ und $\eta = [b_0; b_1, \dots]$, dann sind die folgenden Aussagen äquivalent:

- (i) $\exists m, n \in \mathbb{N}_0$, sodass $\forall i \geq 0$ gilt: $a_{n+i} = b_{m+i}$ bzw. $\xi_n = \eta_m$.
- (ii) $\xi \simeq \eta$.

Ist $\eta = \mathcal{T}_U(\xi)$ und $U \in \text{GL}_2(\mathbb{Z})$, dann können $m, n \in \mathbb{N}_0$ derart gewählt werden, sodass $\det U = (-1)^{m+n}$.

¹⁰(Bundschuh 2002: 222f.)

Beweis: (i) $\Rightarrow$ (ii): Es seien $\frac{p_k}{q_k}$ die Nherungsbrche von ξ und $\frac{p'_k}{q'_k}$ die Nherungsbrche von η . Nach Satz 4.5 (ii) ist

$$\begin{aligned} \xi &= \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}} = \mathcal{T}_U(\xi_n) & \text{mit} & \quad U = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \\ \text{und} \quad \eta &= \frac{p'_{m-1}\eta_m + p'_{m-2}}{q'_{m-1}\eta_m + q'_{m-2}} = \mathcal{T}_{U'}(\eta_m) & \text{mit} & \quad U' = \begin{pmatrix} p'_{m-1} & p'_{m-2} \\ q'_{m-1} & q'_{m-2} \end{pmatrix}. \end{aligned}$$

Dies bedeutet, dass $\xi \simeq \xi_n$ und $\eta \simeq \eta_m$.

Nach Voraussetzung $\exists m, n \in \mathbb{N}_0$, sodass $\eta_m = \xi_n$. Daher erhalten wir insgesamt

$$\xi \simeq \xi_n = \eta_m \simeq \eta \quad \text{also} \quad \xi \simeq \eta.$$

(i) $\Leftarrow$ (ii): Es sei $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ und $\eta = \mathcal{T}_U(\xi) = \frac{\alpha\xi + \beta}{\gamma\xi + \delta}$. Aufgrund von

$$\mathcal{T}_{-U} = \mathcal{T}_U \quad \text{und} \quad \det(-U) = \det U,$$

knnen wir voraussetzen, dass $\gamma\xi + \delta > 0$. Auerdem sei fr $n \geq 0$

$$U_n = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}.$$

Dann erhalten wir

$$\det U_n = p_{n-1}q_{n-2} - p_{n-2}q_{n-1} \stackrel{(18)}{=} (-1)^n \quad \text{sowie} \quad \xi = \mathcal{T}_{U_n}(\xi_n).$$

Da also $\xi \simeq \xi_n$ und nach Voraussetzung $\xi \simeq \eta$, ergibt sich wegen „ $\simeq$ ist eine quivalenzrelation“:

$$\eta = \mathcal{T}_{U_n}(\xi_n) \quad \text{fr} \quad n \geq 0 \quad (\Rightarrow \quad \eta \simeq \xi_n).$$

Es sei

$$UU_n = \begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix}.$$

Gem der Matrizenmultiplikation erhalten wir fr die Koeffizienten dieser Matrix

$$\begin{aligned} \alpha_n &= \alpha p_{n-1} + \beta q_{n-1} & \beta_n &= \alpha p_{n-2} + \beta q_{n-2} \\ \gamma_n &= \gamma p_{n-1} + \delta q_{n-1} & \delta_n &= \gamma p_{n-2} + \delta q_{n-2}. \end{aligned}$$

Nun lässt sich unter anderem δ_n auch schreiben als

$$(*) \quad \gamma_{n-1} = \gamma p_{n-2} + \delta q_{n-2} = \delta_n .$$

Jetzt liegt es daran zu zeigen, dass wir n so groß wählen können, damit gilt $\gamma_n > \delta_n > 0$. Es ist

$$\begin{aligned} (\diamond) \quad \gamma_n &= \gamma p_{n-1} + \delta q_{n-1} = q_{n-1} \gamma \frac{p_{n-1}}{q_{n-1}} + q_{n-1} \delta - q_{n-1} \gamma \xi + q_{n-1} \gamma \xi = \\ &= q_{n-1} \gamma \left(\frac{p_{n-1}}{q_{n-1}} - \xi \right) + q_{n-1} (\gamma \xi + \delta) . \end{aligned}$$

Nach diesem Schema ergibt sich des Weiteren

$$(\diamond\diamond) \quad \gamma_{n-1} = q_{n-2} \gamma \left(\frac{p_{n-2}}{q_{n-2}} - \xi \right) + q_{n-2} (\gamma \xi + \delta) .$$

Im Beweis zu Satz 4.5 (i) haben wir unter anderem gezeigt, dass

$$\left| \xi - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} \quad \text{für } n \geq 0 . \quad (22)$$

Daher erhalten wir

$$\lim_{n \rightarrow \infty} q_{n-1} \underbrace{\left(\frac{p_{n-1}}{q_{n-1}} - \xi \right)}_{\xrightarrow{n \rightarrow \infty} 0} = 0 .$$

Aufgrund dessen und wegen $(q_k)_{k \geq 1}$ ist streng monoton steigen sowie der obigen Voraussetzung $\gamma \xi + \delta > 0$, gilt insgesamt

$$\lim_{n \rightarrow \infty} \gamma_n = \infty .$$

Wegen $(\diamond)$ und $(\diamond\diamond)$ ist

$$\gamma_n - \delta_n \stackrel{(*)}{=} \gamma_n - \gamma_{n-1} = q_{n-1} \gamma \left(\frac{p_{n-1}}{q_{n-1}} - \xi \right) - q_{n-2} \gamma \left(\frac{p_{n-2}}{q_{n-2}} - \xi \right) + (q_{n-1} - q_{n-2}) (\gamma \xi + \delta) > 0$$

für n genügend groß. Demnach erhalten wir $\gamma_n > \delta_n > 0$. Nach Lemma 4.8 ist

$$\begin{aligned} -) \quad \eta &= \mathcal{T}_U(\xi) = \mathcal{T}_{UU_n}(\xi_n) = [b_0; b_1, \dots, b_{m-1}, \xi_n], \quad \text{also } \eta_m = \xi_n, \quad \text{und} \\ -) \quad \det UU_n &= (-1)^m . \end{aligned}$$

Daher folgt aus

$$\det UU_n = \det U \det U_n = \det U \cdot (-1)^n = (-1)^m, \quad \text{dass}$$

$$\det U = \frac{(-1)^m}{(-1)^n} = (-1)^{m-n} = (-1)^{m+n}.$$

□

Wir wollen nun eine wichtige Definition angeben, welche uns für indefinite Formen von großem Nutzen sein wird.

DEFINITION 4.5 Eine reelle Zahl $\xi \notin \mathbb{Q}$ heißt *quadratische Irrationalzahl*, falls ξ Lösung einer quadratischen Gleichung

$$a\xi^2 + b\xi + c = 0 \quad \text{ist, mit} \quad a, b, c \in \mathbb{Q}.$$

Die andere Nullstelle dieses Polynoms, ist die zu ξ konjugierte Zahl und sei mit ξ' bezeichnet.¹¹

Es lassen sich allerlei interessante und bedeutende Aussagen zu einer quadratischen Irrationalzahl nennen. Zwei davon wären der Satz von Euler und der Satz von Lagrange, welche wir am Ende dieses Abschnitts behandeln werden.

Wir benötigen jedoch für unsere Definition einer indefiniten reduzierten Form, noch einen weiteren Begriff:

DEFINITION 4.6 Eine reelle quadratische Irrationalzahl ξ heißt *reduziert*, wenn

$$\xi > 1 \quad \text{und} \quad -1 < \xi' < 0.$$

Diese Aussagen sind insofern von Interesse, da die erste Wurzel $w_1(f)$ von f (mit Diskriminante $D_f > 0$ kein Quadrat) eine quadratische Irrationalzahl ist.

PROPOSITION 4.10 Es sei $\xi = [a_0; a_1, \dots]$ eine quadratische Irrationalzahl und $f(X) = aX^2 + bX + c \in \mathbb{Z}[X]$ derart gewählt, dass $f(\xi) = 0$. Es seien rekursiv definiert

$$\begin{aligned} A_0 &= a, \\ B_0 &= b, \\ C_0 &= c \end{aligned} \quad \text{und für } n \geq 0 \quad \left\{ \begin{array}{l} A_{n+1} = A_n a_n^2 + B_n a_n + C_n, \\ B_{n+1} = 2A_n a_n + B_n, \\ C_{n+1} = A_n. \end{array} \right. \quad (23)$$

Außerdem sei für $n \geq 0$

$$f_n(X) = A_n X^2 + B_n X + C_n.$$

Dann gelten für $n \geq 0$ die folgenden Punkte:

¹¹Zwar sind hier $a, b, c \in \mathbb{Q}$, jedoch können wir ebenso $a, b, c \in \mathbb{Z}$ verlangen. Außerdem gilt: Ist $\xi \in \mathbb{Q}$, so setzt man $\xi = \xi'$.

- (i) $B_n^2 - 4A_nC_n = b^2 - 4ac =: D.$
- (ii) $f_n(\xi_n) = 0.$
- (iii) $|B_n| \leq \max(|b|, \sqrt{D})$ und $|A_n| \leq \max(|b|, \sqrt{D}).$

Beweis:

$$\begin{aligned}
 \text{(i): } \quad n = 0 : \quad & B_0^2 - 4A_0C_0 \stackrel{(23)}{=} b^2 - 4ac = D \\
 n \mapsto n+1 : \quad & B_{n+1}^2 - 4A_{n+1}C_{n+1} \stackrel{(23)}{=} (2A_n a_n + B_n)^2 - 4(A_n a_n^2 + B_n a_n + C_n)A_n = \\
 & = 4A_n^2 a_n^2 + 4A_n a_n B_n + B_n^2 - 4A_n^2 a_n^2 - 4A_n a_n B_n - 4A_n C_n = \\
 & = B_n^2 - 4A_n C_n.
 \end{aligned}$$

(ii): Mithilfe von $f_n(a_n)$ lassen sich $A_{n+1}, B_{n+1}, C_{n+1}$ auch folgendermaßen beschreiben:

$$(*) \quad A_{n+1} = f_n(a_n), \quad B_{n+1} = f'_n(a_n), \quad C_{n+1} = \frac{1}{2} f''_n(a_n).$$

$$\begin{aligned}
 n = 0 : \quad & f_0(\xi_0) \stackrel{Def. 4.2}{=} f_0(\xi) = 0. \\
 n \mapsto n+1 : \quad & f_{n+1}(\xi_{n+1}) = A_{n+1} \xi_{n+1}^2 + B_{n+1} \xi_{n+1} + C_{n+1} = \\
 & \stackrel{(*)}{=} f_n(a_n) \xi_{n+1}^2 + f'_n(a_n) \xi_{n+1} + \frac{1}{2} f''_n(a_n) = \\
 & = \xi_{n+1}^2 \left(f_n(a_n) + \frac{1}{1!} f'_n(a_n) \frac{1}{\xi_{n+1}} + \frac{1}{2!} f''_n(a_n) \frac{1}{\xi_{n+1}^2} \right) = \\
 & \stackrel{\text{Taylor. Formel}^{12}}{=} \xi_{n+1}^2 f_n \left(a_n + \frac{1}{\xi_{n+1}} \right) \stackrel{(15)}{=} \xi_{n+1}^2 \underbrace{f_n(\xi_n)}_{\stackrel{\text{I.V.}}{=} 0} = 0.
 \end{aligned}$$

(iii): Da nach (ii) $f_n(\xi_n) = 0$, liefert uns folglich die Lösungsformel für die allgemeine qua-

¹²Die Taylorsche Formel besagt das Folgende: Sei $f : I \mapsto \mathbb{R}$ $(n+1)$ -mal stetig differenzierbar und $x_0 \in I$. Dann gilt $\forall x \in I$:

$$\begin{aligned}
 f(x) &= f(x_0) + f'(x_0)(x - x_0) + \frac{f''(x_0)}{2}(x - x_0)^2 + \dots + \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n + R_{n+1}(x) \\
 \text{wobei } R_{n+1} &= \frac{1}{n!} \int_{x_0}^x (x - t)^n \cdot f^{(n+1)}(t) \, dx.
 \end{aligned}$$

dratischen Gleichung

$$(**) \quad \xi_n = \frac{-B_n \pm \overbrace{\sqrt{B_n^2 - 4A_n C_n}}^{(i) \sqrt{D}}}{2A_n} = \frac{-B_n \pm \sqrt{D}}{2A_n}.$$

1. Behauptung:

$$\begin{aligned} n = 0 : \quad |B_0| &= |b| \leq \max(|b|, \sqrt{D}). \\ n \mapsto n+1 : \quad |B_{n+1}| &= |2A_n a_n + B_n| \stackrel{(**)}{=} \left| B_n + a_n \frac{-B_n \pm \sqrt{D}}{\xi_n} \right| = \\ &= \frac{1}{\xi_n} |\xi_n B_n - a_n B_n \pm a_n \sqrt{D}| \leq \frac{1}{\xi_n} B_n (\xi_n - a_n) + \frac{1}{\xi_n} a_n \sqrt{D} \\ &\stackrel{\text{i.V.}}{\leq} \underbrace{\left(\frac{1}{\xi_n} (\xi_n - a_n) + \frac{1}{\xi_n} a_n \right)}_{=1} \max(|b|, \sqrt{D}) = \max(|b|, \sqrt{D}). \end{aligned}$$

2. Behauptung Aus $B_{n+1} = 2A_n a_n + B_n$ folgt

$$2a_n |A_n| = |B_{n+1} - B_n| \stackrel{1. \text{ Beh.}}{\leq} 2 \max(|b|, \sqrt{D}), \quad \text{also} \quad |A_n| \leq \max(|b|, \sqrt{D}).$$

□

Proposition 4.10 (ii) liefert uns eine wichtige Erkenntnis: Nämlich folgt daraus, dass für $n \geq 0$ gilt: ξ_n ist quadratisch irrational.

Zu guter Letzt zeigen wir noch zwei bedeutende Sätze in der Theorie der Kettenbrüche, nämlich jene von Euler und Lagrange, welche sich wie folgt zusammenfassen lassen:

SATZ 4.11 (Satz von Euler/Lagrange) Eine reelle Zahl ξ besitzt genau dann eine periodische Kettenbruchentwicklung, wenn ξ eine quadratische Irrationalzahl ist, d. h.

$\xi \in \mathbb{R} \setminus \mathbb{Q}$ ist Lösung der quadratischen Gleichung $aX^2 + bX + c = 0$ mit $a, b, c \in \mathbb{Z}$, $a \neq 0$.

Beweis: Wir zeigen mit der Hinrichtung den Satz von Euler und folglich mit der Rückrichtung den Satz von Lagrange. Der Beweis von Letzterem ist im Normalfall anspruchsvoller, jedoch haben wir bereits einige Vorbereitungen dafür getroffen.

($\Rightarrow$)¹³: Es sei eine reelle Zahl ξ gegeben, die eine periodische Kettenbruchentwicklung besitzt,

$$\begin{aligned} \text{d. h.} \quad \xi &= [a_0; a_1, \dots, a_{k-1}, \overline{a_k, \dots, a_{k+l-1}}] \stackrel{\text{Satz 4.4 (ii)}}{=} \frac{p_{k-1}\xi_k + p_{k-2}}{q_{k-1}\xi_k + q_{k-2}} \quad \text{für } (k \geq 0) \quad (24) \\ \Rightarrow \quad &\xi(q_{k-1}\xi_k + q_{k-2}) = p_{k-1}\xi_k + p_{k-2} \end{aligned}$$

$$\begin{aligned}
\xi q_{k-1} \xi_k + \xi q_{k-2} &= p_{k-1} \xi_k + p_{k-2} \\
\xi_k (q_{k-1} \xi - p_{k-1}) &= p_{k-2} - \xi q_{k-2} \\
\xi_k &= \frac{p_{k-2} - \xi q_{k-2}}{q_{k-1} \xi - p_{k-1}}.
\end{aligned} \tag{25}$$

Da jedoch $\xi_{k+l} = \xi_k$ gilt nach (24) ebenso

$$\begin{aligned}
\xi &= \frac{p_{k+l-1} \xi_k + p_{k+l-2}}{q_{k+l-1} \xi_k + q_{k+l-2}} \\
\stackrel{(25)}{\Rightarrow} \xi_k &= \frac{p_{k+l-2} - \xi q_{k+l-2}}{q_{k+l-1} \xi - p_{k+l-1}} = \frac{p_{k-2} - \xi q_{k-2}}{q_{k-1} \xi - p_{k-1}} \quad \text{für } k > v \\
\Rightarrow (p_{k+l-2} - \xi q_{k+l-2})(q_{k-1} \xi - p_{k-1}) &= (p_{k-2} - \xi q_{k-2})(q_{k+l-1} \xi - p_{k+l-1}) \\
\Leftrightarrow \dots \Leftrightarrow \xi^2 A_i + \xi B_i + C_i &= 0 \tag{26} \\
\text{mit } A_i &= q_{k-2} q_{k+l-1} - q_{k+l-2} q_{k-1} \\
B_i &= p_{k+l-2} q_{k-1} + p_{k-1} q_{k+l-2} - p_{k-2} q_{k+l-1} - p_{k+l-1} q_{k-2} \\
C_i &= p_{k-2} p_{k+l-1} - p_{k+l-2} p_{k-1}.
\end{aligned}$$

Daher genügt ξ der quadratischen Gleichung (26) und ist nach Definition 4.5 eine quadratische Irrationalzahl.

($\Leftarrow$): Es sei ξ eine quadratische Irrationalzahl, d. h. ξ genügt einem irreduziblem Polynom $f(X) = aX^2 + bX + c$ in $\mathbb{Z}[X]$. Außerdem sei

$$\begin{aligned}
A_0 &= a, B_0 = b, C_0 = c \\
\text{und für } n \geq 0 \quad A_{n+1} &= a_n^2 A_n + B_n a_n + C_n \\
B_{n+1} &= 2A_n a_n + B_n \\
C_{n+1} &= A_n \\
\text{sowie } f_n(X) &= A_n X^2 + B_n X + C_n \quad \text{und} \quad D = B_0^2 - 4A_0 C_0 = b^2 - 4ac.
\end{aligned}$$

Da ξ quadratisch irrational ist, ist folglich $4ac \neq 0$ und D kein Quadrat. Nach Proposition 4.10 sind jedoch die Folgen $(A_n)_{n \geq 1}$ und $(B_n)_{n \geq 1}$ beschränkt¹⁴ und daher ist auch die Menge

$$\{(A_n, B_n) \mid n \geq 1\} \subseteq \mathbb{Z}^2$$

beschränkt und somit endlich. Daraus wiederum ergibt sich, dass es unendlich viele n

¹³(Bundschuh 2002: 228)

¹⁴Es ist auch die Folge $(C_k)_{k \geq 1}$ beschränkt, da $C_{k+1} = A_k$.

mit $A := A_n$, $B := B_n$ gibt. Für eben diese n ist

$$C := C_n = \frac{B^2 - D}{4A} \quad \text{konstant.}$$

Nun gibt es unendlich viele n , für die $A\xi_n^2 + B\xi_n + C = 0$ gilt. Insbesondere gibt es also mindestens zwei ganze Zahlen, welche einander gleich sind. Es folgt sodann, dass es ganze Zahlen

$$k \geq 0 \quad \text{und} \quad l \geq 1 \quad \text{gibt, mit} \quad \xi_k = \xi_{k+l}.$$

Somit ist der Kettenbruch periodisch.

□

Aus dem Satz von Lagrange folgt nun:

SATZ 4.12 Eine reelle Zahl ξ hat genau dann eine reinperiodische Kettenbruchentwicklung, wenn ξ eine reduzierte quadratische Irrationalzahl ist.

Beweis: ($\Rightarrow$): Es sei $\xi = [\overline{a_0; a_1, \dots, a_{l-1}}]$ mit den Näherungsbrüchen $\frac{p_k}{q_k}$.

Da $a_0 = a_l \geq 1$ ist folglich $\xi > 1$. Wegen $\xi = \xi_l$ folgt

$$\xi = \frac{p_{l-1}\xi + p_{l-2}}{q_{l-1}\xi + q_{l-2}}$$

und ξ genügt der quadratischen Gleichung $f(X) = q_{l-1}X^2 + (q_{l-2} - p_{l-1})X - p_{l-2} = 0$. Demnach ist ξ eine quadratische Irrationalzahl. Außerdem gilt wegen

$$f(0) = -p_{l-2} < 0 \quad \text{sowie} \quad f(-1) = q_{l-1} - q_{l-2} + p_{l-1} - p_{l-2} > 0$$

und daher nach dem Spezialfall des Zwischenwertsatzes von Bolzano, dass f zwischen -1 und 0 eine Nullstelle besitzt. Da diese jedoch nicht ξ ist, muss es sich um ξ' handeln. Somit gilt $-1 < \xi' < 0 < 1 < \xi$ und ξ ist nach Definition 4.6 reduziert.

($\Leftarrow$): Es sei $\xi = [a_0; a_1, \dots, a_{v-1}, \overline{a_v, \dots, a_{v+l-1}}]$ und reduziert. Wir nehmen indirekt an, dass für $v \geq 1$ die Beziehung $a_{v-1} \neq a_{v+l-1}$ gelte. Daher ist

$$\begin{aligned} a_{v-1} - \xi_{v-1} &= -\frac{1}{\xi_v} = -\frac{1}{\xi_{v+l}} = a_{v+l-1} - \xi_{v+l-1} \\ \Rightarrow \quad |a_{v-1} - a_{v+l-1}| &= |\xi'_{v-1} - \xi'_{v+l-1}| \stackrel{\xi_n \text{ red.}}{<}^{15} 1, \end{aligned}$$

wobei die letzte Gleichheit auf der Tatsache beruht, dass $x \mapsto x'$ ein Homomor-

¹⁵Da ξ reduziert ist, gilt $\xi_n > 1$ für $n \geq 1$ und ξ_n ist reduziert, denn aus $\xi'_n < 0 \leq a_n - 1$ ergibt sich, dass $\xi'_n - a_n < -1$ ist. Daraus folgt wiederum $\xi'_{n+1} = \frac{1}{\xi'_n - a_n} \in (-1, 0)$.

phismus ist. Aufgrund von $a_n \in \mathbb{N}$ folgt der Widerspruch $a_{v-1} = a_{v+l-1}$ und somit $v = 0$. Also ist $\xi = [\overline{a_0; a_1, \dots, a_{l-1}}]$, d. h. reinperiodisch. $\square$

Bevor wir diesen Abschnitt mit dem nachstehenden Satz endgültig beenden, sei für dessen Beweis noch auf Folgendes hingewiesen:

Sind ξ und η zwei äquivalente quadratische Irrationalzahlen, so haben diese die gleiche Periodenlänge.

Dies erhalten wir aus dem Folgenden:

Sind ξ und η zwei äquivalente quadratische Irrationalzahlen und ist l die Länge der Periode, v die Länge der Vorperiode von ξ und $t \in \mathbb{Z}$ mit $v + tl \geq n$, dann ergibt sich:

$$\begin{aligned} \eta &= [b_0; b_1, \dots, b_{m-1}, a_n, \dots, a_{v+tl-1}, \overline{a_{v+tl}, \dots, a_{v+tl+l-1}}] = \\ &= [b_0; b_1, \dots, b_{m-1}, a_n, \dots, a_{v+tl-1}, \overline{a_v, \dots, a_{v+l-1}}]. \end{aligned}$$

SATZ 4.13 Es seien ξ und η zwei reduzierte Zahlen. Dann sind äquivalent:

- (i) $\exists k \geq 0 : \xi = \eta_k.$
- (ii) $\xi \simeq \eta.$

Für $U \in \text{SL}_2(\mathbb{Z})$ mit $\xi = \mathcal{T}_U(\eta)$ kann k derart gewählt werden, sodass $\det U = (-1)^k$.

Beweis: (i) $\Rightarrow$ (ii): Es seien ξ und η reduziert und somit quadratische Irrationalzahlen.

Außerdem gilt für reduzierte Zahlen, dass für alle $n, m \geq 0$ sowohl ξ_n als auch η_m , d. h. die vollständigen Quotienten der Zahlen, ebenfalls reduziert sind. Die Behauptung folgt dann unmittelbar als ein Spezialfall – es ist ja $\xi = \xi_0$ – aus Satz 4.9.

(ii) $\Rightarrow$ (i): Es sei $\xi = \mathcal{T}_U(\eta)$ für $U \in \text{SL}_2(\mathbb{Z})$. Gemäß Satz 4.9 $\exists m, n \in \mathbb{N}_0$ mit $\xi_n = \eta_m$ sowie $\det U = (-1)^{m+n}$.

Es sei l die Periodenlänge von ξ und $tl \geq n$, wobei t gerade sei. Da ξ und η zwei quadratische Irrationalzahlen sind, besitzen sie die gleiche Periodenlänge (siehe obige Bemerkung). Nun ist ξ nach Voraussetzung reduziert, weswegen wir aus Satz 4.12 folgern, dass

$$\eta = [b_0; b_1, \dots, b_{m-1}, a_n, \dots, a_{tl-1}, \overline{a_0, \dots, a_{l-1}}].$$

Aufgrund dessen, dass auch η reduziert ist, erhalten wir $\eta_{m+tl-n} = \xi$. Somit ist die gesuchte Zahl $k \geq 0$ von der Gestalt $k = m + tl - n$. $\square$

4.4 Äquivalenz und Ketten indefiniter binärer quadratischer Formen

Wir wollen uns nun an der Definition 4.7 für eine reduzierte Form sowie am Beweis des Satzes 4.15 versuchen. Es sei an dieser Stelle an die Definitionen 4.5 und 4.6 erinnert, mithilfe derer das Folgende verständlicher sein sollte:

DEFINITION 4.7 Es sei $f = (a, b, c)$ eine indefinite binäre quadratische Form. Dann heißt die Form

f *reduziert*, wenn $|w_1(f)|$ reduziert ist.

Zwar wurden schon einige Bedingungen und Folgerungen einer reduzierten Form genannt, doch bevor wir uns der Äquivalenz indefiniter binärer quadratischer Formen widmen, sollen wichtige Eigenschaften einer reduzierten Form festgehalten werden.

SATZ 4.14 Es sei $f = (a, b, c)$ eine indefinite binäre quadratische Form und D_f kein Quadrat. Dann sind äquivalent:

- (i) f ist reduziert.
- (ii) $|w_1(f)'| < 1 < |w_1(f)|$ und $w_1(f)w_1(f)' < 0$.
- (iii) $|a + c| + b < 0$ und $ac < 0$.

Beweis: (i) $\Leftrightarrow$ (ii): Es ist $|w_1(f)'| = w_1(f)' \operatorname{sgn} w_1(f)$.

Also ist f genau dann reduziert, wenn

$$0 < -w_1(f)' \operatorname{sgn} w_1(f) < 1 < |w_1(f)|.$$

Dies ist aber äquivalent mit

$$|w_1(f)'| < 1 < |w_1(f)| \quad \text{und} \quad \operatorname{sgn} w_1(f)' \neq \operatorname{sgn} w_1(f), \quad \text{also}$$

$$w_1(f)w_1(f)' < 0.$$

(ii) $\Rightarrow$ (iii):

$$\begin{aligned} w_1(f)w_1(f)' &= \frac{-b + \sqrt{D_f}}{2a} \cdot \frac{-b - \sqrt{D_f}}{2a} = \frac{b^2}{4a^2} - \frac{b\sqrt{D_f}}{4a^2} + \frac{b\sqrt{D_f}}{4a^2} - \frac{D_f}{4a^2} = \\ &= \frac{b^2 - b^2 + 4ac}{4a^2} = \frac{c}{a} \end{aligned}$$

Aufgrund von

$$w_1(f)w_1(f)' < 0 \quad \Rightarrow \quad ac < 0,$$

woraus sich $\sqrt{D_f} = \sqrt{b^2 - 4ac} > b$ ergibt.

Da nun $w_1(f) = \frac{-b + \sqrt{D_f}}{2a}$ erhalten wir insgesamt also

$$\operatorname{sgn} w_1(f) = \operatorname{sgn} a.$$

1.) Wegen

$$|w_1(f)| > 1 \Rightarrow \operatorname{sgn}(1 - w_1(f)) = -\operatorname{sgn} a.$$

Es ist also wegen $|w_1(f)'| < 1$

$$(*) \quad a + b + c = f(1, 1) = a(1 - w_1(f))(1 - w_1(f)') < 0.$$

2.) Außerdem ist

$$\operatorname{sgn}(1 + w_1(f)) = \operatorname{sgn} w_1(f) = \operatorname{sgn} a \quad \text{und} \quad 1 + w_1(f)' > 0$$

und somit

$$(**) \quad -a - c + b = -f(1, -1) = -a(1 + w_1(f))(1 + w_1(f)') < 0$$

Daher erhalten wir insgesamt aus 1.) und 2.) die Behauptung $|a + c| + b < 0$.

(iii) $\Rightarrow$ (ii): Es ist $ac < 0$ und daher

$$\begin{aligned} -) \quad 0 &> \frac{c}{a} = w_1(f)w_1(f)' \quad \text{und} \\ -) \quad \sqrt{D_f} &= \sqrt{b^2 - 4ac} > |b| = -b. \end{aligned}$$

Also gilt

$$|w_1(f)| = \frac{-b + \sqrt{D_f}}{2|a|} > \frac{b + \sqrt{D_f}}{2|a|} = |w_1(f)'|$$

Aus (*) und (**) ergibt sich

$$-a^2(1 - w_1(f))(1 + w_1(f))(1 - w_1(f)')(1 + w_1(f)') = -a^2(1 - w_1(f)^2)(1 - (w_1(f)')^2) > 0.$$

Letztendlich erhalten wir aus

$$1 - w_1(f)^2 < 1 - (w_1(f)')^2 \quad \text{die letzte Behauptung} \quad |w_1(f)| > 1 > |w_1(f)'| = |w_2(f)|.$$

□

Wir haben bereits im Kapitel 3 gezeigt, dass es zu jeder positiv definiten binären quadratischen Form f eine dazu äquivalente reduzierte Form gibt. Diese bedeutende Tatsache

gilt auch für indefinite Formen. Dieser nun folgende Satz wird uns unter anderem auch einen Weg angeben, wie eine zu f äquivalente reduzierte Form gefunden werden kann.

SATZ 4.15 Zu jeder indefiniten binären quadratischen Form f mit D_f kein Quadrat, gibt es eine reduzierte Form g mit $g \sim f$.

Beweis: Die erste Wurzel von f ist eine quadratische Irrationalzahl und besitzt somit nach dem Satz von Euler/Lagrange 4.11 eine periodische Kettenbruchentwicklung, also

$$w_1(f) = [a_0; a_1, \dots, a_{k-1}, \overline{a_k, \dots, a_{k+l-1}}] \stackrel{\text{Satz 4.4 (ii)}}{=} \frac{p_{k-1}w_1(f)_k + p_{k-2}}{q_{k-1}w_1(f)_k + q_{k-2}}$$

Dabei ist $w_1(f)_k$ der k -te vollständige Quotient. Es sei $\eta = (-1)^k w_1(f)_k$.

Für

$$U = \begin{pmatrix} (-1)^k p_{k-1} & p_{k-2} \\ (-1)^k q_{k-1} & q_{k-2} \end{pmatrix} \quad (27)$$

ist $w_1(f) = \mathcal{T}_U(\eta)$. Wegen

$$\det U = (-1)^k \underbrace{(p_{k-1}q_{k-2} - p_{k-2}q_{k-1})}_{\stackrel{(18)}{=} (-1)^k} = (-1)^{2k} = 1 \quad \Rightarrow \quad U \in \text{SL}_2(\mathbb{Z}).$$

Es ist die Kettenbruchentwicklung von $|\eta| = w_1(f)_k$ reinperiodisch, weswegen nach Satz 4.12 $|\eta|$ reduziert ist.

Es sei $g = f \circ U$ und daher $g \sim f$. Aufgrund dessen und wegen Proposition 4.7 ist, erhalten wir

$$|w_1(g)| = |\mathcal{T}_{U^{-1}}(w_1(f))| = |\eta| \quad \Rightarrow \quad g \text{ ist reduziert.}$$

□

Mithilfe dieses Satzes können wir nun eine zu f äquivalente reduzierte Form finden und zwar folgendermaßen:

Beispiele: 1.) Gesucht ist eine zu $f(x, y) = 5x^2 - 3xy - y^2$ äquivalente reduzierte Form. Es ist f indefinit mit $D_f = 29$. Der erste Schritt ist die Vorperiode von $w_1(f)$ zu bestimmen, d. h. wir entwickeln $w_1(f)$ in einen Kettenbruch.

$$\begin{aligned} w_1(f) &= \frac{3 + \sqrt{29}}{10} = 0 + \frac{3 + \sqrt{29}}{10}, \\ w_1(f)_1 &= \frac{10}{3 + \sqrt{29}} = \frac{10(3 - \sqrt{29})}{-20} = \frac{3 - \sqrt{29}}{-2} = \frac{\sqrt{29} - 3}{2} = 1 + \frac{\sqrt{29} - 5}{2}, \\ w_1(f)_2 &= \frac{2}{\sqrt{29} - 5} = \frac{2(\sqrt{29} + 5)}{4} = \frac{\sqrt{29} + 5}{2} = 5 + \frac{\sqrt{29} - 5}{2}, \end{aligned}$$

$$w_1(f)_3 = \frac{2}{\sqrt{29} - 5} = w_1(f)_2$$

und somit ist $w_1(f) = [0; 1, \bar{5}]$.

Für die Länge der Vorperiode erhalten wir $v = 2$. Anschließend bestimmen wir mithilfe von (16) die Koeffizienten jener Matrix (27)

$$U = \begin{pmatrix} (-1)^v p_{v-1} & p_{v-2} \\ (-1)^v q_{v-1} & q_{v-2} \end{pmatrix} = \begin{pmatrix} p_1 & p_0 \\ q_1 & q_0 \end{pmatrix},$$

welche f in eine reduzierte Form überführt.

$$\begin{array}{c|cccc} & 0 & 1 & \dots & a_i \\ \hline 0 & 1 & 0 & 1 & \dots & p_i \\ \hline 1 & 0 & 1 & 1 & \dots & q_i \end{array} \Rightarrow U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \text{SL}_2(\mathbb{Z}),$$

sodass $f \circ U = (1, -5, -1)$ reduziert ist.

- 2.) Es ist die Form $f(x, y) = 17x^2 - 56xy + 46y^2$ zu reduzieren. Es ist $D_f = 8$, D_f kein Quadrat und f indefinit. Wir bestimmen erneut die Vorperiode von $w_1(f)$:

$$\begin{aligned} w_1(f) &= \frac{56 + \sqrt{8}}{34} = \frac{28 + \sqrt{2}}{17} = 1 + \frac{11 + \sqrt{2}}{17}, \\ w_1(f)_1 &= \frac{17}{11 + \sqrt{2}} = \frac{17(11 - \sqrt{2})}{119} = \frac{11 - \sqrt{2}}{7} = 1 + \frac{4 - \sqrt{2}}{7}, \\ w_1(f)_2 &= \frac{7}{4 - \sqrt{2}} = \frac{7(4 + \sqrt{2})}{14} = \frac{4 + \sqrt{2}}{2} = 2 + \frac{\sqrt{2}}{2}, \\ w_1(f)_3 &= \frac{2}{\sqrt{2}} = \frac{2\sqrt{2}}{2} = \sqrt{2} = 1 + \frac{\sqrt{2} - 1}{1}, \\ w_1(f)_4 &= \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{1} = 2 + \frac{\sqrt{2} - 1}{1}, \\ w_1(f)_5 &= \frac{1}{\sqrt{2} - 1} = w_1(f)_4 \end{aligned}$$

und daher erhalten wir $w_1(f) = [1; 1, 2, 1, \bar{2}]$.

Für die Länge der Vorperiode erhalten wir $v = 4$. Anschließend bestimmen wir für jene Matrix

$$U = \begin{pmatrix} (-1)^v p_{v-1} & p_{v-2} \\ (-1)^v q_{v-1} & q_{v-2} \end{pmatrix} = \begin{pmatrix} p_3 & p_2 \\ q_3 & q_2 \end{pmatrix},$$

welche f in eine reduzierte Form überführt, mithilfe von (16) die entsprechenden p_i, q_i :

$$\begin{array}{c|cccccc} & 1 & 1 & 2 & 1 & \dots & a_i \\ \hline 0 & 1 & 1 & 2 & 5 & 7 & \dots & p_i \\ \hline 1 & 0 & 1 & 1 & 3 & 4 & \dots & q_i \end{array} \Rightarrow U = \begin{pmatrix} 7 & 5 \\ 4 & 3 \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$$

und $f \circ U = (1, -2, -1)$ ist reduziert.

Auch im Kapitel zu indefiniten Formen taucht ein Satz auf, welcher uns bereits aus Kapitel 3 vertraut ist (vgl. Satz 3.7).

SATZ 4.16 Ist $D > 0$ und kein Quadrat, so gibt es nur endlich viele Äquivalenzklassen indefiniter binärer quadratischer Formen mit Diskriminante D .

Beweis: Es ist auch dieser Beweis ähnlich zu jenem für Satz 3.7. Demnach genügt es zu zeigen, dass es nur endlich viele reduzierte Form mit Diskriminante D gibt.

Es sei $f = (a, b, c)$ eine indefinite reduzierte Form und wir setzen $D_f = D$. Für eine reduzierte Form gilt nach Satz 4.14, dass $ac < 0$ ist und daher

$$D = b^2 + 4|ac| > b^2 \Rightarrow |b| < \sqrt{D}.$$

Aus

$$D = b^2 + 4|ac| \geq 4|ac|, \quad \text{also} \quad D \geq 4|ac| \Rightarrow |ac| \leq \frac{D}{4}.$$

Somit kommen für die Koeffizienten nur endlich viele Werte in Frage, weswegen es auch nur endlich viele Äquivalenzklassen gibt. $\square$

Bereits zu Beginn des Kapitels 4 wurde erwähnt, dass im indefiniten Fall in einer Äquivalenzklasse mehrere reduzierte Formen liegen können und diese Ketten bilden. Um sie zu finden, ordnen wir jeder indefiniten reduzierten Form f eine periodische Folge $(f_i)_{i \geq 0}$ von Formen zu. Diese Folge besteht gerade aus den zu f äquivalenten Formen.

DEFINITION 4.8 Es sei $f = (a, b, c)$ eine indefinite reduzierte binäre quadratische Form mit $D_f > 0$ kein Quadrat und $|w_1(f)| = [\overline{a_0}; \overline{a_1}, \dots, \overline{a_{l-1}}]$. Wir setzen

$$\begin{aligned} A_0 &= |a|, \\ B_0 &= b, \\ C_0 &= c \operatorname{sgn} a \end{aligned} \quad \text{und für } n \geq 0 \quad \begin{cases} A_{n+1} = a_n^2 A_n + a_n B_n + C_n, \\ B_{n+1} = 2a_n A_n + B_n, \\ C_{n+1} = A_n. \end{cases} \quad (28)$$

Außerdem sei

$$f_n = (A_n \operatorname{sgn} a, (-1)^n B_n, C_n \operatorname{sgn} a). \quad (29)$$

Die Folge $(f_n)_{n \geq 0}$ heißt dann die *Kette von f* .

In Bezug auf die obige Definition stellen wir fest:

$$1.) \quad f_0 \stackrel{(29)}{=} (A_0 \operatorname{sgn} a, (-1)^0 B_0, C_0 \operatorname{sgn} a) = (\underbrace{|a| \operatorname{sgn} a}_{=a}, b, c \underbrace{(\operatorname{sgn} a)^2}_{=1}) = (a, b, c) = f.$$

2.) Für $n \geq 0$ erhalten wir

$$D_{f_n} \stackrel{(28)}{=} (-1)^{2n} B_n^2 - 4A_n C_n (\operatorname{sgn} a)^2 = B_n^2 - 4A_n C_n \stackrel{\text{Prop. 4.10}}{=} \underbrace{b^2 - 4ac}_{=B_0^2 - 4A_0 C_0} = D_f. \quad (30)$$

$$3.) \quad |w_1(f)| \text{ ist Nullstelle von } A_0 X^2 + B_0 X + C_0 = \operatorname{sgn} a (aX^2 + b \cdot \operatorname{sgn} a \cdot X + c).$$

Diese Tatsache folgt aus der Voraussetzung, dass f reduziert ist. Denn für f reduziert liefert uns der Beweis für Satz 4.14, dass das $\operatorname{sgn} w_1(f) = \operatorname{sgn} a$ ist. Aufgrund dessen und weil natürlich $w_1(f)$ eine Nullstelle von $aX^2 + bX + c$ ist, erhalten wir

$$a|w_1(f)|^2 + b \cdot \operatorname{sgn} a \cdot |w_1(f)| + c = a w_1(f)^2 + b w_1(f) + c = 0.$$

Somit ist $|w_1(f)|$ Nullstelle von $A_0 X^2 + B_0 X + C_0$.

4.) Erneut liefert uns die Proposition 4.10 mit dem Punkt (ii) eine wichtige Erkenntnis. Es ist nämlich dort ξ_n und somit auch

$$|w_1(f)|_n \text{ Nullstelle von } A_n X^2 + B_n X + C_n \text{ für } n \geq 0.$$

Da $|w_1(f)|_n$ eine reinperiodische Kettenbruchentwicklung besitzt, ist nach Satz 4.12 $|w_1(f)|_n$ reduziert. Somit liefert uns Satz 4.14, dass auch $A_n X^2 + B_n X + C_n$ reduziert ist. Wir erhalten hieraus, aufgrund des eben genannten Satzes, dass

$$A_n A_{n-1} \stackrel{(28)}{=} A_n C_n < 0, \quad \text{weswegen} \quad \operatorname{sgn} A_n \stackrel{A_0 > 0}{=} (-1)^n.$$

PROPOSITION 4.17 Ist $f = (a, b, c)$ eine indefinite reduzierte binäre quadratische Form mit Diskriminante $D_f > 0$ kein Quadrat und $(f_n)_{n \geq 0}$ die Kette von f , so gilt für $n \geq 0$:

$$(i) \quad |w_1(f)|_n = (-1)^n w_1(f_n) \operatorname{sgn} a.$$

$$(ii) \quad f_n \text{ ist reduziert.}$$

(iii)

$$f_n = f \circ \begin{pmatrix} p_{n-1}(-1)^n & p_{n-2} \operatorname{sgn} a \\ q_{n-1}(-1)^n \operatorname{sgn} a & q_{n-2} \end{pmatrix}.$$

Beweis: (i): Welche der beiden Wurzeln von $A_n X^2 + B_n XY + C_n Y^2$ die größere der beiden ist, hängt vom $\operatorname{sgn} A_n = (-1)^n$ ab. Daher ist $|w_1(f)|_n$ die größere der beiden Wurzeln und es ist

$$\begin{aligned} |w_1(f)|_n &= \frac{-B_n + (-1)^n \sqrt{D_f}}{2A_n} = \frac{(-B_n + (-1)^n \sqrt{D_f})(-1)^n}{2A_n(-1)^n} = \frac{-B_n(-1)^n + \sqrt{D_f}}{2A_n(-1)^n} =^{16} \\ &= (-1)^n w_1(f_n) \operatorname{sgn} a. \end{aligned}$$

(ii): Es ist $|w_1(f)|_n$ reduziert und da nach (i) $|w_1(f)|_n = |w_1(f_n)|$, ist auch $|w_1(f_n)|$ reduziert. Weswegen nach Definition 4.7 f_n reduziert ist.

(iii): Wir setzen

$$V_n = \begin{pmatrix} p_{n-1}(-1)^n & p_{n-2} \operatorname{sgn} a \\ q_{n-1}(-1)^n \operatorname{sgn} a & q_{n-2} \end{pmatrix}.$$

$$\begin{aligned} V_n \in \operatorname{SL}_2(\mathbb{Z}), \quad \text{weil: } \det V_n &= p_{n-1}(-1)^n q_{n-2} - p_{n-2} \operatorname{sgn} a q_{n-1}(-1)^n \operatorname{sgn} a = \\ &= (-1)^n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \stackrel{(18)}{=} (-1)^n (-1)^n = 1. \end{aligned}$$

Es ist zudem

$$|w_1(f)| = \frac{p_{n-1}|w_1(f)|_n + p_{n-2}}{q_{n-1}|w_1(f)|_n + q_{n-2}} \stackrel{(i)}{=} \frac{p_{n-1}(-1)^n w_1(f_n) \operatorname{sgn} a + p_{n-2}}{q_{n-1}(-1)^n w_1(f_n) \operatorname{sgn} a + q_{n-2}}.$$

Da, wie bereits erwähnt, $\operatorname{sgn} w_1(f) = \operatorname{sgn} a$ ergibt sich

$$w_1(f) = \mathcal{T}_{V_n}(w_1(f_n)) \stackrel{\text{Prop. 4.7}}{=} w_1(f_n \circ V_n^{-1})$$

Zu guter Letzt erhalten wir

$$D_f \stackrel{(30)}{=} D_{f_n} \stackrel{(9)}{=} D_{f_n \circ V_n^{-1}} \stackrel{\text{Prop. 4.2}}{\Rightarrow} f = f_n \circ V_n^{-1}.$$

□

Satz 4.18 Für eine indefinite reduzierte binäre quadratische Form f mit $D_f > 0$ kein Quadrat sowie der Kettenbruchentwicklung $|w_1(f)| = [\overline{a_0; a_1, \dots, a_{l-1}}]$ von $|w_1(f)|$ mit Periode l gilt:

(i) Die Folge $(f_n)_{n \geq 0}$ hat Periode $\operatorname{kgV}(2, l)$.

¹⁶Es ist ja $f_n(X, Y) = A_n \operatorname{sgn} a X^2 + (-1)^n B_n XY + C_n \operatorname{sgn} a Y^2$. Daher ist $w_1(f_n) = \frac{-(-1)^n B_n + \sqrt{D_f}}{2A_n \operatorname{sgn} a}$.

- (ii) Die Menge der zu f äquivalenten reduzierten Formen ist gegeben durch

$$\{ f_n \mid 0 \leq n < \text{kgV}(2, l) \}.$$

Beweis: (i): 1. Sind $m, n \in \mathbb{N}_0$ mit

$$n \equiv m \pmod{\text{kgV}(2, l)} \Leftrightarrow \begin{cases} n \equiv m \pmod{2} & \text{und} \\ n \equiv m \pmod{l}, \end{cases}$$

so folgt, dass $2 \mid m - n$ und $l \mid m - n$. Dann gilt

$$|w_1(f)|_n = |w_1(f)|_m \xrightarrow{\text{Prop. 4.17 (i)}} (-1)^n w_1(f_n) \text{sgn } a = (-1)^m w_1(f_m) \text{sgn } a, \text{ bzw.} \\ w_1(f_n) = w_1(f_m).$$

Für die Folge $(f_n)_{n \geq 0}$ gilt (30), weswegen auch $D_{f_n} = D_{f_m}$ gilt. Aufgrund dessen ist nach Proposition 4.2 $f_n = f_m$.

2. Wir gehen nun umgekehrt davon aus, dass $f_n = f_m$ mit $0 \leq m, n < \text{kgV}(2, l)$. Proposition 4.17 liefert uns folglich

$$(-1)^n |w_1(f)|_n = w_1(f_n) \text{sgn } a = w_1(f_m) \text{sgn } a = (-1)^m |w_1(f)|_m.$$

Nun ist $|w_1(f)|_n > 0$ als auch $|w_1(f)|_m > 0$, woraus sich $(-1)^n = (-1)^m$ und $2 \mid m - n$ ergibt. Außerdem gilt wegen $|w_1(f)|_n = |w_1(f)|_m$, dass $l \mid m - n$. Insgesamt erhalten wir also $\text{kgV}(2, l) \mid m - n$ und da nach Voraussetzung $0 \leq m, n < \text{kgV}(2, l)$ gilt, ist somit $m = n$.

- (ii): Wir wissen aufgrund der Proposition 4.17 (ii) und (iii), dass für eine indefinite reduzierte Form f mit ihrer Kette $(f_n)_{n \geq 0}$ auch f_n reduziert und zu f äquivalent ist.

Wir gehen nun umgekehrt davon aus, dass $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ und $f \circ U$ reduziert ist.

Es sei $\lambda = \text{sgn } w_1(f \circ U)$ sowie $V = \begin{pmatrix} \alpha \lambda \text{sgn } a & \beta \text{sgn } a \\ \gamma \lambda & \delta \end{pmatrix}.$

Wir erhalten

$$\det V = \alpha \lambda \text{sgn } a \cdot \delta - \beta \text{sgn } a \cdot \gamma \lambda = \lambda \text{sgn } a \underbrace{(\alpha \delta - \beta \gamma)}_{=1} = \lambda \text{sgn } a.$$

Es ist, wie bereits des Öfteren erwähnt, $\operatorname{sgn} a = \operatorname{sgn} w_1(f)$ und es gilt

$$(*) \quad \lambda \cdot |w_1(f \circ U)| = w_1(f \circ U).$$

Insgesamt folgt daraus

$$|w_1(f)| \stackrel{\text{Prop. 4.7}}{=} \mathcal{T}_U(w_1(f \circ U)) \operatorname{sgn} a \stackrel{(21)}{=} \frac{\alpha w_1(f \circ U) \operatorname{sgn} a + \beta \operatorname{sgn} a}{\gamma w_1(f \circ U) + \delta} \stackrel{(*)}{=} \mathcal{T}_V(|w_1(f \circ U)|).$$

Somit gibt es eine Matrix aus der $\operatorname{GL}_2(\mathbb{Z})$, sodass nach Definition 4.4

$|w_1(f)| \simeq |w_1(f \circ U)|$. Da zudem beide Zahlen reduziert ist, gibt es nach Satz 4.13 ein $n \geq 0$ mit

$$(**) \quad |w_1(f \circ U)| = |w_1(f)|_n \quad \text{und} \quad \det V [= \lambda \operatorname{sgn} a] = (-1)^n.$$

Sodann können wir aus

$$w_1(f \circ U) \stackrel{(*)}{=} \lambda |w_1(f \circ U)| \stackrel{(**)}{=} \lambda |w_1(f)|_n \stackrel{(**)}{=} (-1)^n \operatorname{sgn} a |w_1(f)|_n \stackrel{\text{Prop. 4.17(i)}}{=} w_1(f_n)$$

folgern, dass nach Proposition 4.2 $f_n = f \circ U$ ist.

□

Wir wollen nun dieses Wissen auch anwenden, indem wir zu den angeführten Beispielen deren Kette bestimmen.

Beispiele: 1.) Es ist die Kette von $f = (1, -2, -1)$ gesucht. Es ist $w_1(f) = \frac{2+\sqrt{8}}{2} = [\overline{2}; 2]$. Somit besitzt $w_1(f)$ die Periodenlänge $l = 1$. Nach Satz 4.18 besitzt die Menge $\{f_n \mid 0 \leq n < \operatorname{kgV}(2, 1) = 2\}$ zwei Elemente, weswegen es zu f nur eine einzige äquivalente Form $\neq f$ gibt. Zur Bestimmung dieser bedienen wir uns Definition 4.8:

$$\begin{aligned} A_0 &= |a| = 1 & A_1 &= a_0^2 A_0 + a_0 B_0 + C_0 = 2^2 \cdot 1 - 2 \cdot 2 - 1 = -1 \\ B_0 &= b = -2 & B_1 &= 2a_0 A_0 + B_0 = 2 \cdot 2 \cdot 1 - 2 = 2 \\ C_0 &= c \cdot \operatorname{sgn} a = -1 & C_1 &= A_0 = 1 \end{aligned}$$

Wir erhalten für $f_1 = (A_1 \operatorname{sgn} a, (-1)^1 B_1, C_1 \operatorname{sgn} a) = (-1, -2, 1)$.

2.) Es sei $f = (-19, -40, 2)$. Man bestimme die Kette von f . Es ist $|w_1(f)| = \frac{40+\sqrt{1752}}{38} = [\overline{2}; 6, 2, 20]$, also $l = 4$. Somit besteht die Menge der zu f äquivalenten Formen aus vier Elementen. Wir erhalten

$$A_0 = 19 \qquad A_1 = 2^2 \cdot 19 - 2 \cdot 40 - 2 = -6$$

$$B_0 = -40$$

$$B_1 = 2 \cdot 2 \cdot 19 - 40 = 36$$

$$C_0 = -2$$

$$C_1 = 19$$

$$A_2 = 6^2 \cdot (-6) + 6 \cdot 36 + 19 = 19$$

$$A_3 = 2^2 \cdot 19 + 2 \cdot (-36) - 6 = -2$$

$$B_2 = 2 \cdot 6 \cdot (-6) + 36 = -36$$

$$B_3 = 2 \cdot 2 \cdot 19 - 36 = 40$$

$$C_2 = -6$$

$$C_3 = 19$$

$$f_0 = (-19, -40, 2) \quad f_1 = (6, -36, -19) \quad f_2 = (-19, -36, 6) \quad f_3 = (2, -40, -19).$$

Jede der Formen f_i ($1 \leq i < 4$) ist zu f äquivalent.

Im Anhang auf Seite 94 befinden sich weitere Beispiele mit Diskriminante $D > 0$ kein Quadrat und entsprechender Klassenzahl.

Bemerkung: In dieser Arbeit wurde eine sehr klassische Reduktionsvariante für indefinite Formen vorgestellt, welche auf den Kenntnissen der unendlichen Kettenbrüche beruht. Abseits davon lässt sich eine zu f indefinite reduzierte äquivalente Form auch mittels eines anderen Weges finden. Ähnlich wie im positiv definiten Fall ist hierbei eine Bedingung an b zu stellen.

Aus mehreren Gründen konnte dieses spannende Thema in der vorliegenden Arbeit jedoch nicht behandelt werden. Dennoch möchte ich diesbzgl. sehr gerne auf zwei Werke verweisen: Siehe hierzu (Buchmann 2007: 107-140) sowie (Buell 1989: 21-34).

4.5 Automorphismen indefiniter binärer quadratischer Formen

Damit wir die Gleichung $f(x, y) = m$ auch im indefiniten Fall lösen können, benötigen wir gemäß der Lösungsstrategie auf Seite 31 noch die Automorphismengruppe. Dank Satz 2.4 können wir uns bei der Bestimmung von A_f auf reduzierte Formen beschränken. Für eine binäre quadratische Form f mit D_f kein Quadrat ist nach Proposition 4.2

$$A_f = \{ U \in \mathrm{SL}_2(\mathbb{Z}) \mid w_1(f \circ U) = w_1(f) \}$$

$$\text{bzw. } A_f = \{ U \in \mathrm{SL}_2(\mathbb{Z}) \mid w_1(f) = \mathcal{T}_U(w_1(f)) \}.$$

SATZ 4.19 Für eine primitive binäre quadratische Form $f = (a, b, c)$ und D_f kein Quadrat gilt

$$A_f = \left\{ \left(\begin{pmatrix} \frac{x-by}{2} & -cy \\ ay & \frac{x+by}{2} \end{pmatrix} \right) \middle| (x, y) \in \mathbb{Z}^2, x^2 - D_f y^2 = 4 \right\}.$$

Beweis: ¹⁷ Es sei $f = (a, b, c)$ eine primitive binäre quadratische Form, d. h. $\text{ggT}(a, b, c) = 1$ und D_f kein Quadrat.

($\Rightarrow$): Es sei nun

$$U = \begin{pmatrix} \frac{x-by}{2} & -cy \\ ay & \frac{x+by}{2} \end{pmatrix} \quad \text{und} \quad x^2 - (b^2 - 4ac)y^2 = x^2 - D_f y^2 = 4. \quad (31)$$

Zunächst sind die Koeffizienten der Matrix U ganzzahlig, d. h. es sind auch

$$\frac{x-by}{2}, \frac{x+by}{2} \in \mathbb{Z}.$$

$$\text{Denn } b \equiv D_f \pmod{2} \Rightarrow x \pm by \equiv x + D_f y \equiv x^2 - D_f y^2 \equiv 4 \equiv 0 \pmod{2}.$$

Außerdem ist $U \in \text{SL}_2(\mathbb{Z})$, weil

$$\det U = \frac{x^2 - b^2 y^2}{4} + acy^2 = \frac{x^2 - b^2 y^2 + 4acy^2}{4} = \frac{x^2 - (b^2 - 4ac)y^2}{4} \stackrel{(31)}{=} 1.$$

Es bleibt zu zeigen, dass $f \circ U = f$ ist. Es sei $f \circ U = (A, B, C)$. Mithilfe von (5) ergeben sich für die Transformation die folgenden Koeffizienten

$$\begin{aligned} A &= a \left(\frac{x-by}{2} \right)^2 + b \left(\frac{(x-by) \cdot ay}{2} \right) + ca^2 y^2 = \\ &= \frac{1}{4} (ax^2 - 2abxy + ab^2 y^2 + 2abxy - 2ab^2 y^2 + 4a^2 cy^2) = \frac{1}{4} (ax^2 - ab^2 y^2 + 4a^2 cy^2) = \\ &= \frac{a}{4} (x^2 - y^2(b^2 - 4ac)) \stackrel{(31)}{=} a \\ B &= 2a \left(\frac{x-by}{2} \right) (-cy) + b \left(\frac{x^2 - b^2 y^2 - 4acy^2}{4} \right) + 2c \left(\frac{x+by}{2} \right) ay = \\ &= \frac{1}{4} (-4acxy + 4abcy^2 + bx^2 - b^3 y^2 - 4abcy^2 + 4acxy + 4abcy^2) = \\ &= \frac{1}{4} (4abcy^2 + bx^2 - b^3 y^2) = \frac{b}{4} (x^2 - y^2(b^2 - 4ac)) \stackrel{(31)}{=} b \end{aligned}$$

¹⁷(Landau 1950: 139f.), (Zagier 1981:63ff.)

$$\begin{aligned}
C &= a(-cy)^2 + b(-cy) \left(\frac{x+by}{2} \right) + c \left(\frac{x+by}{2} \right)^2 = \\
&= \frac{1}{4}(4ac^2y^2 - 2bcxy - 2b^2cy^2 + cx^2 + 2bcxy + b^2cy^2) = \frac{c}{4}(x^2 - y^2(b^2 - 4ac)) \stackrel{(31)}{=} c
\end{aligned}$$

Somit ist $f \circ U = f$ und U von obiger Gestalt ein Automorphismus in A_f .

($\Leftarrow$): Es sei umgekehrt

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \quad \text{und} \quad f \circ U = f.$$

Wir erinnern uns zurück an (5):

$$a = a\alpha^2 + b\alpha\gamma + c\gamma^2 \tag{32}$$

$$b = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \tag{33}$$

$$c = a\beta^2 + b\beta\delta + c\delta^2.$$

Aus (33) ergibt sich nach Subtraktion von b

$$\begin{aligned}
0 &= 2(a\alpha\beta + b\beta\gamma + c\gamma\delta) \underbrace{-b\beta\gamma + b\alpha\delta - b}_{\substack{=b(\alpha\delta - \beta\gamma)=b \\ =0}} \quad \text{und daher} \\
0 &= a\alpha\beta + b\beta\gamma + c\gamma\delta
\end{aligned} \tag{34}$$

Da nun einerseits

$$\begin{aligned}
a\beta &\stackrel{(32)}{=} a\alpha^2\beta + b\alpha\beta\gamma + c\beta\gamma^2 = \alpha(a\alpha\beta + b\beta\gamma) + c\beta\gamma^2 \stackrel{(34)}{=} \alpha(-c\gamma\delta) + c\beta\gamma^2 = \\
&= c\gamma(\beta\gamma - \alpha\delta) = -c\gamma
\end{aligned} \tag{35}$$

und andererseits

$$\begin{aligned}
a\delta &\stackrel{(32)}{=} a\alpha^2\delta + b\alpha\gamma\delta + \gamma(c\gamma\delta) \stackrel{(34)}{=} a\alpha^2\delta + \gamma(-a\alpha\beta) + b\alpha\gamma\delta + \gamma(-b\beta\gamma) = \\
&= a\alpha(\alpha\delta - \beta\gamma) + b\gamma(\alpha\delta - \beta\gamma) = a\alpha + b\gamma \\
a(\delta - \alpha) &= b\gamma
\end{aligned} \tag{36}$$

folgt daraus wegen $a, c \neq 0$ ¹⁸, dass $a|c\gamma$ und $a|b\gamma$.

Da nun f primitiv ist erhalten wir

$$(*) \quad a|\gamma \quad \text{somit} \quad \exists y \in \mathbb{Z} : \gamma = ay.$$

¹⁸Da D_f kein Quadrat ist, gilt $a, c \neq 0$.

Nun folgt für (35) $(\diamond) \beta = -cy$ und für (36) $(\diamond\diamond) \delta - \alpha = by$.

Damit haben wir insgesamt

$$\frac{\gamma}{a} = -\frac{\beta}{c} = \frac{\delta - \alpha}{b} = y \in \mathbb{Z}.$$

Zu guter Letzt setzen wir $x = \alpha + \delta$ und erhalten für x^2 :

$$\begin{aligned} x^2 &= (\alpha + \delta)^2 = (\delta - \alpha)^2 + 4\delta\alpha \stackrel{(\diamond\diamond)}{=} b^2y^2 + 4(1 + \beta\gamma) \stackrel{(\diamond)}{=} b^2y^2 + 4(1 - cy \cdot \gamma) = \\ &\stackrel{(*)}{=} b^2y^2 + 4(1 - acy^2) = (b^2 - 4ac)y^2 + 4 = D_f y^2 + 4 \\ x^2 - D_f y^2 &= 4. \end{aligned} \quad ^{19}$$

Daher ergeben sich die ganzzahligen Lösungen

$$\alpha = \frac{x - by}{2} \quad \text{und} \quad \delta = \frac{x + by}{2}.$$

Somit ist U von der gesuchten Gestalt. Es wurde bereits oben gezeigt, dass die $\det U = 1$ ist. $\square$

Mit anderen Worten besagt der Punkt (i) das Folgende:

Die Automorphismengruppe einer primitiven binären quadratischen Form $f = (a, b, c)$ mit D_f kein Quadrat ergibt sich durch jene Matrizen

$$U = \begin{pmatrix} \frac{x - by}{2} & -cy \\ ay & \frac{x + by}{2} \end{pmatrix}$$

für die (x, y) eine Lösung der Pellschen Gleichung $x^2 - D_f y^2 = 4$ ist.

Bei dieser Bijektion, welche zwischen der Lösungsmenge der Pellschen Gleichung und der Automorphismengruppe operiert, handelt es sich um einen Isomorphismus.²⁰

Wir stehen jedoch vor einem Problem: Die Lösungen von $x^2 - D_f y^2 = 4$ sind uns noch unbekannt, was jedoch geändert werden soll. Denn mithilfe der Lösungen lassen sich die

¹⁹Die trivialen Lösungen der Gleichung $x^2 - D_f y^2 = 4$ mit der Bedingung $D_f \equiv 0$ oder $1 \pmod{4}$ sind $(2, 0), (-2, 0)$ und stets vorhanden. Ist $D_f < -4$, so sind dies alle Lösungen. Im Fall $D_f = -4$ existieren des Weiteren $(0, 1), (0, -1)$, daher gibt es vier Lösungen. Für $D_f = -3$ gibt es neben den trivialen Lösungen noch vier weitere, nämlich $(1, 1), (-1, 1), (1, -1), (-1, -1)$, also insgesamt sechs Lösungen. Ist hingegen $D_f > 0$ kein Quadrat, so gibt es unendlich viele Lösungen.

(Landau 1950: 57-64)

²⁰Ein Beweis dazu findet sich u. a. in (Zagier 1981: 63ff.)

Automorphismen von f schnell bestimmen. Im Fall, dass f positiv definit ist, kennen wir Dank Satz 3.4 bereits die Lösungen. Der soeben behandelte Satz liefert dann die zugehörigen Automorphismen.

Daher sei nun f eine indefinite reduzierte Form, $|w_1(f)| = [\overline{a_0; a_1, \dots, a_{l-1}}]$ und $\pi = \text{kgV}(2, l)$. Da nach Satz 4.18

$$[f_0 =] f = f_{\pi n} \quad \forall n \geq 0 \quad (37)$$

ist, ergibt sich aus Proposition 4.17 (iii), dass

$$\begin{pmatrix} p_{\pi n-1} & p_{\pi n-2} \operatorname{sgn} a \\ q_{\pi n-1} \operatorname{sgn} a & q_{\pi n-2} \end{pmatrix} \in A_f.$$

Der nächste Satz zeigt, dass diese Matrizen samt ihren negativen und inversen alle Automorphismen sind.

SATZ 4.20 Für eine indefinite reduzierte Form $f = (a, b, c)$, $|w_1(f)| = [\overline{a_0; a_1, \dots, a_{l-1}}]$ und $\pi = \text{kgV}(2, l)$, wobei l die Periode des Kettenbruchs ist, gilt

$$A_f = \left\{ \epsilon \begin{pmatrix} p_{\pi k-1} & p_{\pi k-2} \operatorname{sgn} a \\ q_{\pi k-1} \operatorname{sgn} a & q_{\pi k-2} \end{pmatrix}^\mu \mid \epsilon, \mu \in \{-1, 1\}, k \geq 0 \right\}.$$

Beweis: Wir können uns auf primitive Formen beschränken:

Denn für $d = \text{ggT}(a, b, c)$ und $g := f \cdot \frac{1}{d}$ ist g primitiv und wegen $w_1(f) = w_1(g)$ ist $A_f = A_g$. ($\Rightarrow$): Es sei nun $U \in A_f$ und somit $\det U = 1$. Wir setzen

$$U_{x,y} = \begin{pmatrix} \frac{x-by}{2} & -cy \\ ay & \frac{x+by}{2} \end{pmatrix} \quad \forall x, y \in \mathbb{Z} \quad \text{mit} \quad x^2 - D_f y^2 = 4. \quad (38)$$

Satz 4.19 liefert uns, dass $\exists x, y \in \mathbb{Z}$ mit $x^2 - D_f y^2 = 4$, weswegen $U_{x,y} = U$ ist. Zudem gilt

$$U_{-x,-y} = -U_{x,y} \quad \text{und} \quad U_{x,-y} = U_{x,y}^{-1} \quad \Rightarrow \quad U_{-x,y} = -U_{x,y}^{-1}.$$

Demnach können wir $(*) \ x, y \geq 0$ voraussetzen.

$y = 0$: In diesem Fall ergibt sich aus (38) und $(*)$, dass $x = 2$ und folglich

$$U = I \stackrel{(16)}{=} \begin{pmatrix} p_{-1} & p_{-2} \operatorname{sgn} a \\ q_{-1} \operatorname{sgn} a & q_{-2} \end{pmatrix}.$$

$y > 0$: Hierfür setzen wir

$$U' = \begin{pmatrix} \frac{x - by}{2} & |c|y \\ |a|y & \frac{x + by}{2} \end{pmatrix}.$$

Nun ist nach Voraussetzung f reduziert und somit $(**) \ ac < 0$, weswegen

$$\begin{aligned} \det U' &= \frac{x^2 - b^2 y^2}{4} - |ac|y^2 = \frac{1}{4}(x^2 - b^2 y^2 - 4|ac|y^2) = \frac{1}{4}(x^2 - y^2(b^2 + 4|ac|)) = \\ &\stackrel{(**)}{=} \frac{1}{4} \underbrace{(x^2 - y^2 D_f)}_{=4} = 1. \end{aligned}$$

Aufgrund von Proposition 4.17 (i) gilt für $f = f_0$, dass $|w_1(f)| = w_1(f) \operatorname{sgn} a$. Wir beachten, dass wegen $(**)$ das $\operatorname{sgn} a \neq \operatorname{sgn} c$ ist und somit $(\diamond) \ |c|y = -cy \operatorname{sgn} a$. Daher gilt des Weiteren

$$\begin{aligned} \mathcal{T}_{U'}(|w_1(f)|) &= \mathcal{T}_{U'}(w_1(f) \operatorname{sgn} a) \stackrel{(21)}{=} \frac{\frac{1}{2}(x - by)w_1(f) \operatorname{sgn} a + |c|y}{\underbrace{|a|yw_1(f) \operatorname{sgn} a + \frac{1}{2}(x + by)}_{=ayw_1(f)}} = \\ &\stackrel{(\diamond)}{=} \frac{\frac{1}{2}(x - by)w_1(f) \operatorname{sgn} a - cy \operatorname{sgn} a}{ayw_1(f) + \frac{1}{2}(x + by)} = \mathcal{T}_U(w_1(f)) \operatorname{sgn} a = \\ &\stackrel{U \in A_f}{=} w_1(f) \operatorname{sgn} a = |w_1(f)|. \end{aligned} \tag{39}$$

Um nun Lemma 4.8 verwenden zu können, gilt es die dafür notwendigen Bedingungen zu schaffen: Es ist zu zeigen, dass $0 \leq \frac{1}{2}(x + by) = |a|y$ gilt.

Es ist wegen

$$\det U' = 1 \quad \text{folglich} \quad \underbrace{4 + 4|ac|y^2}_{\geq 0} = x^2 - b^2 y^2 \geq 0 \quad \text{und daher} \quad \frac{x + by}{2} \geq 0.$$

Da f reduziert ist, gilt nach Satz 4.14 (iii)

$$|a+c|+b < 0 \quad \Leftrightarrow \quad |a+c|-|b| < 0 \quad \Leftrightarrow \quad |a+c| < |b| \quad \stackrel{b \in \mathbb{Z}}{\Rightarrow} (\diamond\diamond) \quad |a+c| \leq |b| - 1.$$

Die Dreiecksungleichung liefert uns:

$$\begin{aligned} |c| &\leq |a| + |a+c| \stackrel{(\diamond\diamond)}{\leq} |a| + |b| - 1 \\ |ac| &\leq a^2 + |ab| - |a| \end{aligned} \tag{40}$$

$$\begin{aligned}
&\Rightarrow \quad x^2 \leq 4 + D_f y^2 \leq 4 + b^2 y^2 + 4|ac|y^2 \stackrel{(40)}{\leq} 4 + b^2 y^2 + 4a^2 y^2 + 4|ab|y^2 - 4|a|y^2 \\
&\quad \stackrel{21}{\leq} 4a^2 y^2 + 4|ab|y^2 + b^2 y^2 = (2|a|y + |b|y)^2 \\
&\stackrel{x \geq 0}{\Rightarrow} \quad x \leq 2|a|y + |b|y \\
&\stackrel{b \leq 0}{\Rightarrow} \quad \frac{x + by}{2} \leq |a|y.
\end{aligned}$$

Nach Lemma 4.8 gibt es ein $n \geq 1$ mit

$$U' = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \quad \text{sowie} \quad |w_1(f)| \stackrel{(39)}{=} \mathcal{T}_{U'}(|w_1(f)|) = [a_0; a_1, \dots, a_{n-1}, |w_1(f)|].$$

Es folgt daraus einerseits, dass $\det U' = (-1)^n$ ist. Jedoch wissen wir bereits, dass $\det U' = 1$ und somit n gerade ist. Andererseits erhalten wir $n = k \cdot l$ für ein $k \geq 0$. Es folgt, dass $l|n$ und da n gerade ist gilt zudem $2|n$. Insgesamt ergibt sich $\pi = \text{kgV}(2, l) | n$ und n lässt sich somit schreiben als πk . Unser U' ist dann von der folgenden Gestalt

$$\begin{aligned}
U' &= \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2}(x - by) & |c|y \\ |a|y & \frac{1}{2}(x + by) \end{pmatrix} = \begin{pmatrix} \frac{1}{2}(x - by) & -c \cdot \text{sgn } a \cdot y \\ a \cdot \text{sgn } a \cdot y & \frac{1}{2}(x + by) \end{pmatrix}. \\
\Rightarrow \quad U &= \begin{pmatrix} \frac{1}{2}(x - by) & -cy \\ ay & \frac{1}{2}(x + by) \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \text{sgn } a \\ q_{n-1} \text{sgn } a & q_{n-2} \end{pmatrix} \quad \text{mit} \quad n = \pi k.
\end{aligned}$$

($\Leftarrow$): ²² Es soll nun gezeigt werden, dass es sich bei

$$V \in \left\{ \epsilon \begin{pmatrix} p_{\pi k-1} & p_{\pi k-2} \text{sgn } a \\ q_{\pi k-1} \text{sgn } a & q_{\pi k-2} \end{pmatrix}^\mu \mid \epsilon, \mu \in \{-1, 1\}, k \geq 0 \right\}$$

um einen Automorphismus handelt. Wir wissen nach Satz 4.18 (ii), dass

$\{f_n \mid 0 \leq n < \text{kgV}(2, l)\}$ die Menge der zu f äquivalenten Formen ist. Außerdem liefert uns dieser Satz mit (i), dass die Folge $(f_n)_{n \geq 0}$ Periode $\text{kgV}(2, l)$ besitzt.

Nun ist $\pi = \text{kgV}(2, l)$ und wir setzen $n = \pi k$ ($k \geq 0$). Dann ist wegen π gerade folglich auch πk gerade. Es ist ja nach (37) $f_0 = f = f_{\pi k} = f_n$. Proposition 4.17 (iii)

²¹Es ist ja $4 + b^2 y^2 + 4a^2 y^2 + 4|ab|y^2 - 4|a|y^2 = \underbrace{b^2 y^2 + 4a^2 y^2 + 4|ab|y^2}_{>0} + \underbrace{4 - 4|a|y^2}_{=4(1-\underbrace{|a|y^2}_{>0}) \leq 0}$.

²²(Mock 2004: 70)

liefert uns sodann

$$\begin{aligned} f = f_n = f \circ \begin{pmatrix} p_{n-1}(-1)^n & p_{n-2} \operatorname{sgn} a \\ q_{n-1}(-1)^n \operatorname{sgn} a & q_{n-2} \end{pmatrix} &= \begin{pmatrix} p_{\pi k-1}(-1)^{\pi k} & p_{\pi k-2} \operatorname{sgn} a \\ q_{\pi k-1}(-1)^{\pi k} \operatorname{sgn} a & q_{\pi k-2} \end{pmatrix} = \\ &= \begin{pmatrix} p_{\pi k-1} & p_{\pi k-2} \operatorname{sgn} a \\ q_{\pi k-1} \operatorname{sgn} a & q_{\pi k-2} \end{pmatrix} \in A_f. \end{aligned}$$

□

Beispiel: Gesucht sind Automorphismen der reduzierten Form $f = (-19, -40, 2)$. Wir bestimmen nun die Näherungsbrüche des entsprechenden Kettenbruchs $|w_1(f)| = [\overline{2; 6, 2, 20}]$:

		2	6	2	20	2	6	2	20	...	a_i
0	1	2	13	28	573	1174	7 617	16 408	335 777	...	p_i
1	0	1	6	13	266	545	3 536	7 617	155 876	...	q_i

Wegen $l = 4$ ist $\pi = \operatorname{kgV}(2, 4) = 4$ und somit

$$U = \begin{pmatrix} p_{\pi k-1} & p_{\pi k-2} \operatorname{sgn} a \\ q_{\pi k-1} \operatorname{sgn} a & q_{\pi k-2} \end{pmatrix} = \begin{pmatrix} p_{4k-1} & -p_{4k-2} \\ -q_{4k-1} & q_{4k-2} \end{pmatrix}.$$

Automorphismen von f sind daher

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 573 & -28 \\ -266 & 13 \end{pmatrix}, \begin{pmatrix} 335 777 & -16 408 \\ -155 876 & 7 617 \end{pmatrix}, \dots$$

Satz 4.21 Es sei $f = (a, b, c)$ eine indefinite reduzierte binäre quadratische Form, $|w_1(f)| = [\overline{a_0; a_1, \dots, a_{l-1}}]$, l die Periode des Kettenbruchs und $\pi = \operatorname{kgV}(2, l)$. Dann gilt:

$$A_f = \left\{ \epsilon \begin{pmatrix} p_{\pi-1} & p_{\pi-2} \operatorname{sgn} a \\ q_{\pi-1} \operatorname{sgn} a & q_{\pi-2} \end{pmatrix}^n \mid \epsilon \in \{-1, 1\}, n \in \mathbb{Z} \right\}.$$

Beweis: Es sei

$$m \in \{l, \pi\}, \quad U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{und} \quad J = \begin{pmatrix} 1 & 0 \\ 0 & \operatorname{sgn} a \end{pmatrix}.$$

Dann ist $J^2 = I$ und es gilt für jede 2×2 Matrix

$$(*) \quad JUJ = \begin{pmatrix} \alpha & \beta \operatorname{sgn} a \\ \gamma \operatorname{sgn} a & \delta \end{pmatrix} \quad \text{sowie} \quad (**) \quad J^{-1} = \frac{1}{\underbrace{\det J}_{= \operatorname{sgn} a}} \begin{pmatrix} \operatorname{sgn} a & 0 \\ 0 & 1 \end{pmatrix} = J$$

Des Weiteren gilt für $\xi = [\overline{a_0; a_1, \dots, a_{k-1}}]$ reduziert mit Näherungsbrüchen $\frac{p_n}{q_n}$, $i \geq -1$ und $k \geq 0$ nach Satz 4.3 auf Seite 42 die folgende Formel

$$\begin{aligned} \begin{pmatrix} p_{lk+i} & p_{lk+i-1} \\ q_{lk+i} & q_{lk+i-1} \end{pmatrix} &= \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{lk-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = {}^{23} \\ &= \begin{pmatrix} p_{l-1} & p_{l-2} \\ q_{l-1} & q_{l-2} \end{pmatrix}^k \begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix}. \end{aligned}$$

Ersetzt man nun in dieser Formel i durch -1 und l durch m so ergibt sich (für $k \geq 0$):

$$V = \begin{pmatrix} p_{mk-1} & p_{mk-2} \\ q_{mk-1} & q_{mk-2} \end{pmatrix} = \begin{pmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{pmatrix}^k \underbrace{\begin{pmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{pmatrix}}_{= I} = \begin{pmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{pmatrix}^k.$$

Daher erhalten wir

$$\begin{aligned} J V J &\stackrel{(*)}{=} \begin{pmatrix} p_{mk-1} & p_{mk-2} \operatorname{sgn} a \\ q_{mk-1} \operatorname{sgn} a & q_{mk-2} \end{pmatrix} \stackrel{(**)}{=} J \begin{pmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{pmatrix}^k J^{-1} = \\ &= \left(J \begin{pmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{pmatrix} J^{-1} \right)^k, \end{aligned}$$

woraus die Behauptung folgt. □

Anhand von einem Beispiel²⁴ soll nun demonstriert werden wie eine Gleichung der Form $f(x, y) = m$, wobei f eine indefinite binäre quadratische Form ist, gelöst werden kann.

Beispiel: 1.) Gesucht sind die Lösungen der Gleichung $5x^2 - 3xy - y^2 = 13$. Es sei $g = (5, -3, -1)$, dann ist $f = g \circ U = (5, -3, -1) \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = (1, -5, -1)$ reduziert und $D_f = 29$.²⁵ Nach unserer Lösungsmethode auf Seite 31 ist die Kongruenz

$$b'^2 \equiv 29 \pmod{4 \cdot 13}, \quad 0 \leq b' < 2 \cdot 13 = 26.$$

$$\begin{aligned} {}^{23} \quad &\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{lk-1} & 1 \\ 1 & 0 \end{pmatrix} = \\ &= \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{l-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{l-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{l-1} & 1 \\ 1 & 0 \end{pmatrix} = \\ &= \left(\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{l-1} & 1 \\ 1 & 0 \end{pmatrix} \right)^k = \begin{pmatrix} p_{l-1} & p_{l-2} \\ q_{l-1} & q_{l-2} \end{pmatrix}^k. \end{aligned}$$

²⁴Das hier angeführte Beispiel ist lösbar in $\mathbb{Z}$. Jedoch gibt es auch den Fall, dass eine Gleichung unlösbar in den ganzen Zahlen ist. Erkennbar ist dies daran, dass keine der mithilfe unserer Lösungsmethode entstandenen Formen nach ihrer Reduktion äquivalent zu der reduzierten Ausgangsform ist.

²⁵Siehe S. 66.

zu lösen. Hierfür erhalten wir die Lösungen $b'_1 = 9$ und $b'_2 = 17$. Daraus ergibt sich

$$\begin{aligned} c'_1 &= \frac{9^2 - 29}{4 \cdot 13} = 1 & c'_2 &= \frac{17^2 - 29}{4 \cdot 13} = 5 \\ f_1 &= (13, 9, 1) & f_2 &= (13, 17, 5). \end{aligned}$$

Diese beiden Formen sollen nun reduziert werden. Hierfür berechnen wir jeweils die erste Wurzel von f_1 und f_2 .

f_1 : Es ist $w_1(f_1) = \frac{-9+\sqrt{29}}{26} = [-1; 1, 6, \bar{5}]$ und somit

$$\begin{array}{c|cccccc} & -1 & 1 & 6 & 5 & \dots & a_i \\ \hline 0 & 1 & -1 & 0 & -1 & -5 & \dots & p_i \\ \hline 1 & 0 & 1 & 1 & 7 & 36 & \dots & q_i \end{array}$$

Da $v = 3$ erhalten wir

$$f_1 \circ \begin{pmatrix} (-1)^3 p_2 & p_1 \\ (-1)^3 q_2 & q_1 \end{pmatrix} = (13, 9, 1) \circ \begin{pmatrix} 1 & 0 \\ -7 & 1 \end{pmatrix} = (-1, -5, 1).$$

Die Form $(-1, -5, 1)$ ist reduziert und zu $(1, -5, -1)$ äquivalent. Außerdem bilden diese beiden Formen eine Kette. Da nach Proposition 4.17 (iii)

$$\begin{aligned} & (-1, -5, 1) \circ \begin{pmatrix} -5 & -1 \\ 1 & 0 \end{pmatrix} = (1, -5, -1) \\ \Rightarrow f_1 \circ U'_1 &= (13, 9, 1) \circ \begin{pmatrix} -5 & -1 \\ 36 & 7 \end{pmatrix} = (1, -5, -1) \\ \Rightarrow U_1 &= \begin{pmatrix} 7 & 1 \\ -36 & -5 \end{pmatrix}. \end{aligned}$$

f_2 : Für $w_1(f_2) = \frac{-17+\sqrt{29}}{26} = [-1; 1, 1, 4, \bar{5}]$ mit $v = 4$ haben wir wegen

$$\begin{array}{c|cccccc} & -1 & 1 & 1 & 4 & 5 & \dots & a_i \\ \hline 0 & 1 & -1 & 0 & -1 & -4 & -21 & \dots & p_i \\ \hline 1 & 0 & 1 & 1 & 2 & 9 & 47 & \dots & q_i \end{array}$$

$$f_2 \circ \begin{pmatrix} (-1)^4 p_3 & p_2 \\ (-1)^4 q_3 & q_2 \end{pmatrix} = (13, 17, 5) \circ \begin{pmatrix} -4 & -1 \\ 9 & 2 \end{pmatrix} = (1, -5, -1).$$

Diese Form entspricht unserer reduzierten Ausgangsform. Es ist

$$\begin{aligned} f_2 \circ U'_2 &= (13, 17, 5) \circ \begin{pmatrix} -4 & -1 \\ 9 & 2 \end{pmatrix} = (1, -5, -1) \\ \Rightarrow U_2 &= \begin{pmatrix} 2 & 1 \\ -9 & -4 \end{pmatrix}. \end{aligned}$$

Da nun $m = 13$ quadratfrei ist, haben alle eigentlichen Lösungen von $x^2 - 5xy - y^2 = 13$ wegen dem 5. Schritt unserer Lösungsmethode die Gestalt

$$A \cdot \begin{pmatrix} 7 \\ -36 \end{pmatrix} \quad \text{und} \quad A \cdot \begin{pmatrix} 2 \\ -9 \end{pmatrix},$$

wobei A ein beliebiger Automorphismus von $(1, -5, -1)$ ist. Demnach erhalten wir z. B. für

$$\begin{aligned} A_0 &= I && \text{die Lösungen} && (7, -36), (2, -9), \\ A_1 &= \begin{pmatrix} 26 & 5 \\ 5 & 1 \end{pmatrix} && \text{die Lösungen} && (2, -1), (7, 1), \\ A_2 &= \begin{pmatrix} 701 & 135 \\ 135 & 26 \end{pmatrix} && \text{die Lösungen} && (47, 9), (187, 36) \end{aligned}$$

Zu guter Letzt wollen wir natürlich noch Lösungen für unsere Ausgangsgleichung $5x^2 - 3xy - y^2 = 13$ finden. Da nun $f = g \circ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = (1, -5, -1)$ erhalten wir für $5x^2 - 3xy - y^2 = 13$ die Lösungen

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 7 \\ -36 \end{pmatrix} &= \begin{pmatrix} 7 \\ -29 \end{pmatrix}, & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ -9 \end{pmatrix} &= \begin{pmatrix} 2 \\ -7 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ -1 \end{pmatrix} &= \begin{pmatrix} 2 \\ 1 \end{pmatrix}, & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 7 \\ 1 \end{pmatrix} &= \begin{pmatrix} 7 \\ 8 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 47 \\ 9 \end{pmatrix} &= \begin{pmatrix} 47 \\ 56 \end{pmatrix}, & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 187 \\ 36 \end{pmatrix} &= \begin{pmatrix} 187 \\ 223 \end{pmatrix}. \end{aligned}$$

Kapitel 5

Geometrische Interpretation von binären quadratischen Formen

Nach Gauss lässt sich jede binäre quadratische Form auch geometrisch interpretieren, nämlich durch ein parallelogrammatisches Gitter. Hierzu wird für eine positiv definite Form (a, b, c) ein Parallelogramm mit den Seitenlängen $\sqrt{a}$ und $\sqrt{c}$ sowie dem eingeschlossenen Winkel φ konstruiert. Der Cosinus von φ ist dann gegeben durch $\cos \varphi = \frac{b}{2\sqrt{ac}}$. Ordnet man diese (kongruenten) Parallelogramme zu einem Parkett an, so entsteht durch dieses allseitige Aneinanderlegen ein sogenanntes *Gitter*.¹ Der Begriff Gitter lässt sich natürlich verallgemeinern:

DEFINITION 5.1 Es seien n linear unabhängige Vektoren $v_1, \dots, v_n$ eines n -dimensionalen Vektorraumes V gegeben. Dann wird ein *Gitter* Γ definiert durch

$$\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n = \langle v_1, \dots, v_n \rangle_{\mathbb{Z}} = \left\{ \sum_{i=1}^n a_i v_i \mid a_i \in \mathbb{Z}, i = 1, \dots, n \right\}.$$

Die Vektoren $v_1, \dots, v_n$ bilden eine $\mathbb{Z}$ -Basis des Gitters Γ . Die Elemente des Gitters heißen *Gitterpunkte*.²

Ein Gitter lässt sich somit auch auffassen als ein System von parallelen Geraden, welches zusätzlich ein System von Punkten definiert: nämlich das System der Schnittpunkte dieser Geraden bzw. der Gitterpunkte.³ Eine Veranschaulichung dessen liefert die Abbildung 5.1. Nun interpretierte Gauss eine binäre quadratische Form f wie folgt:

¹(Fricke 1923: 183f.)

²(Hlawka 1986: 35ff.)

³(Hardy 1958: 28ff.)

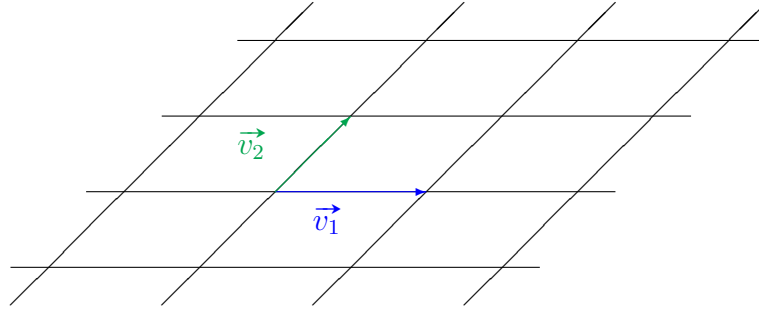


Abbildung 5.1: 2-dimensionales Gitter

Es sei (x, y) jener Eckpunkt des Gitters, welcher nach x -fachen Durchlaufen der Seite $\sqrt{a}$ und nach y -fachen Durchlaufen der Seite $\sqrt{c}$ erreicht wird. Dieser Punkt besitzt vom Ursprung, also dem Punkt $(0, 0)$, nun eine Entfernung, deren Quadrat gleich der binären quadratischen Form $f(x, y) = ax^2 + bxy + cy^2$ ist, d. h.:

Gegeben seien die linear unabhängigen Vektoren

$$p = (p_1, p_2), \quad q = (q_1, q_2) \in \mathbb{R}^2 \quad (41)$$

sowie das Gitter

$$G = \{xp + yq \mid x, y \in \mathbb{Z}\} = p\mathbb{Z} + q\mathbb{Z}.^4 \quad (42)$$

Dann ist das Quadrat der euklidische Norm des Vektors

$$v = xp + yq, \quad x, y \in \mathbb{Z}$$

gegeben durch

$$||v||^2 = (xp_1 + yq_1)^2 + (xp_2 + yq_2)^2 = x^2(p_1^2 + p_2^2) + 2xy(p_1q_1 + p_2q_2) + y^2(q_1^2 + q_2^2).$$

Es seien nun

$$a = p_1^2 + p_2^2, \quad b = 2(p_1q_1 + p_2q_2), \quad c = q_1^2 + q_2^2$$

$$\text{und } f = (a, b, c).$$

Somit ergibt sich

$$||v||^2 = f(x, y).$$

Daher beschreibt $f(x, y)^{\frac{1}{2}}$ den Abstand des Punktes $xp + yq \in G$ vom Ursprung.

⁴ G wird auch als das *Parallelgitter von* f bezeichnet und ist eine Untergruppe des $\mathbb{R}^2$.

Wenn wir also im Gitter G nach einem Vektor der Länge l suchen, dann entspricht dies dem Suchen eines Repräsentanten von l^2 durch f .⁵ Die Diskriminante D_f von f lässt sich nun schreiben als

$$D_f = -4(d(G))^2,$$

wobei $d(G)$ dem Flächeninhalt jenes Parallelogramms entspricht, welches von den Vektoren p und q aufgespannt wird. Anders gesagt versteht sich $d(G)$ als der Absolutbetrag der Determinante derjenigen 2×2 Matrix, deren Spalten die linear unabhängigen Vektoren p und q bilden, d. h.

$$d(G) = \left| \det \begin{pmatrix} p_1 & q_1 \\ p_2 & q_2 \end{pmatrix} \right| = |p_1 q_2 - p_2 q_1|. \quad (43)$$

In diesem Kapitel wollen wir auf den sogenannten *Fundamentbereich* hinarbeiten. Mit Hilfe dessen können geometrische Interpretationen bzgl. der Äquivalenz und Reduktion von binären quadratischen Formen getroffen werden. Wir überlegen uns u. a., wo die erste Wurzel $w_1(f)$ einer positiv definiten reduzierten binären quadratischen Form liegt.

Um dieses Gebiet zu erforschen, erinnern wir uns zurück an den Abschnitt 4.2 auf Seite 49.

5.1 Positiv definite binäre quadratische Formen

Zunächst wollen wir unser Augenmerk auf die geometrische Interpretation positiver definiter binärer quadratischer Formen legen. Bevor wir uns dem Fundamentbereich widmen sei an die drei Minima einer positiv definiten reduzierten Form $f = (a, b, c)$ erinnert, die gemäß Definition 3.3 wie folgt lauten:

erstes Minimum:	a	
zweites Minimum:	c	sofern $a < c$
drittes Minimum:	$a - b + c$	falls $a < c < a - b + c$ gilt.

Wir stellen uns nun, wie schon zu Beginn dieses Kapitels, ein parallelogrammatisches Gitter vor. Da für eine beliebige (also auch für eine nicht reduzierte) positiv definite binäre quadratische Form bekanntlich

$$D_f = b^2 - 4ac < 0 \quad \text{und daher} \quad |b| < 2\sqrt{ac}$$

⁵Des Weiteren entspricht dem Aufsuchen des kürzesten Vektors, welcher $\neq 0$ ist, dem Bestimmen des Minimums von f .

⁶(Buchmann 2007: 17f.)

gilt, gibt es *genau einen* Winkel φ mit

$$\cos \varphi = \frac{b}{2\sqrt{ac}} \quad \text{und} \quad 0 < \varphi < \pi.$$

Daher und weil $\sin^2 \varphi + \cos^2 \varphi = 1$ ergibt sich

$$\sin \varphi = \sqrt{1 - \frac{b^2}{4ac}} = \sqrt{\frac{4ac - b^2}{4ac}} = \sqrt{\frac{-D_f}{4ac}} = \frac{1}{2\sqrt{ac}} \sqrt{-D_f}.$$

Wir betrachten erneut die beiden unabhängigen Vektoren p und q , welche wir bereits bei (41) behandelt haben. Es sei nun

$$p = \sqrt{a}(1, 0) \quad \text{und} \quad q = \sqrt{c}(\cos \varphi, \sin \varphi) = \frac{1}{2\sqrt{a}}(b, \sqrt{-D_f}).$$

Das entsprechende Parallelogramm

$$F = \{ \alpha p + \beta q \mid 0 \leq \alpha, \beta < 1 \}$$

besitzt nach (43) den Flächeninhalt

$$\left| \det \begin{pmatrix} \sqrt{a} & \sqrt{c} \cos \varphi \\ 0 & \sqrt{c} \sin \varphi \end{pmatrix} \right| = \sqrt{a} \sqrt{c} \sin \varphi = \frac{1}{2} \sqrt{-D_f}.$$

Außerdem gilt für das Gitter G laut (42) das Folgende:

$$F \cap G = \{(0, 0)\}, \quad \text{da für } 0 \leq \alpha, \beta < 1 \quad \text{lediglich} \quad \alpha = \beta = 0 \in \mathbb{Z}.$$

Es sei nun f reduziert. Wir legen um den Ursprung die folgenden zwei Kreise:

$$K_1 = \{ (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = a \} \quad \text{mit Radius } r_1 = \sqrt{a}, \quad (44)$$

$$K_2 = \{ (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = c \} \quad \text{mit Radius } r_2 = \sqrt{c}. \quad (45)$$

Diese werden als der *erste* und *zweite Minimumkreis* der reduzierten Form f bezeichnet. Mithilfe von Abbildung 5.2 wird dies auch bildlich veranschaulicht.

In Kapitel 3 haben wir die Eigenschaften reduzierter binärer quadratischer Formen untersucht und konnten mithilfe von Satz 3.4 auch etwas über die Anzahl der Lösungen sagen. Dieses Wissen wollen wir auch hier anwenden:

- 1.) Es sei $a < c$ und daher $K_1 \neq K_2$. Dann enthält K_1 nach Satz 3.4 (iva), mit Ausnahme

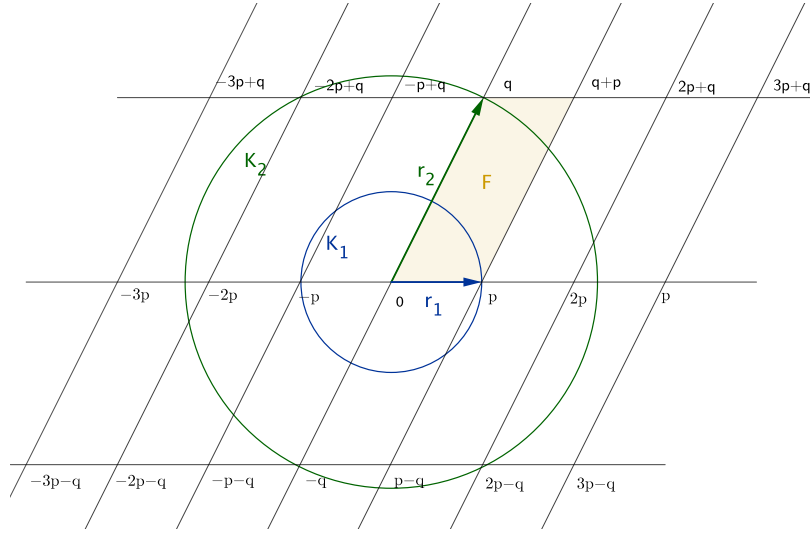


Abbildung 5.2: Minimumkreise einer reduzierten Form

des inneren Punktes $(0,0)$, nur die beiden Punkte $\pm p$ des Gitters G .

Demnach gilt für den zweiten Minimumkreis K_2 mit der Bedingung $c < a - |b| + c$, dass K_2 (ausgenommen der Punkte auf der x -Achse) nur die beiden Punkte $\pm q$ von G enthält.

- 2.) Ist nun $a = c$ und damit $K_1 = K_2$ erhalten wir gemäß Satz 3.4 (ivb), dass auf K_1 die vier Punkte $\pm p$ und $\pm q$ liegen.
- 3.) Gilt neben $a = c$ zusätzlich $|b| = a$, so liegen nach Satz 3.4 (ivc) außerdem die beiden Punkte $p - q \operatorname{sgn} b$ und $-p + q \operatorname{sgn} b$ auf K_1 .

Kommen wir nun zur Betrachtung der ersten Wurzel $w_1(f)$ einer positiv definiten binären quadratischen Form $f = (a, b, c)$ mit Diskriminante $D_f < 0$. Wir setzen

$$w_1(f) = \frac{-b + i\sqrt{|D_f|}}{2a} = x + iy \quad \text{mit} \quad x = -\frac{b}{2a} \quad \text{und} \quad y = \frac{\sqrt{|D_f|}}{2a}. \quad (46)$$

Es ist $y > 0$. Außerdem gilt

$$|x| \leq \frac{1}{2} \Leftrightarrow |b| \leq a \quad \text{sowie} \quad (47)$$

$$x^2 + y^2 = \frac{b^2 - (b^2 - 4ac)}{4a^2} = \frac{c}{a} \geq 1 \Leftrightarrow c \geq a. \quad (48)$$

Wir definieren nun den *Fundamentbereich* der $\mathrm{SL}_2(\mathbb{Z})$ als die Menge

$$F := \{ w \in \mathbb{C} \mid \operatorname{Im} w > 0, \quad |w| \geq 1 \quad \text{und} \quad |\operatorname{Re} w| \leq \frac{1}{2} \} \quad (49)$$

Die Abbildung 5.3 verdeutlicht dies auch grafisch. In dieser wurde der Fundamentbereich eingefärbt.

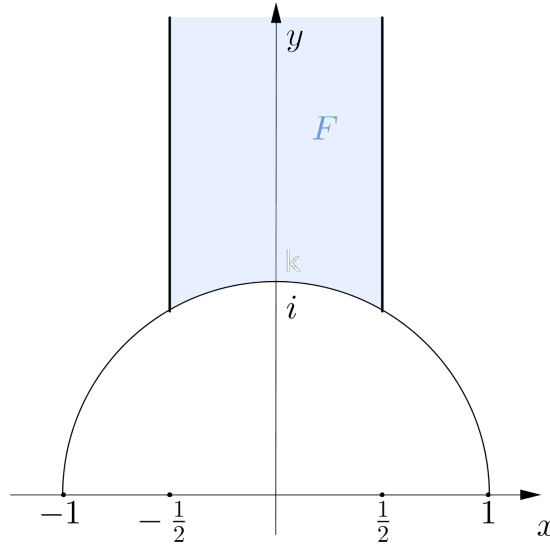


Abbildung 5.3: Fundamentbereich der $\mathrm{SL}_2(\mathbb{Z})$

Die Bedingungen (47) - (49) liefern uns die folgende Proposition:

PROPOSITION 5.1 Es sei f eine positiv definite binäre quadratische Form. Dann gilt:

$$f \text{ ist reduziert} \quad \Leftrightarrow \quad w_1(f) \in F.$$

Außerdem erhalten wir aus Satz 3.3 sowie Proposition 4.7:

$$\exists U \in \mathrm{SL}_2(\mathbb{Z}) \quad \text{mit} \quad \mathcal{T}_U(w_1(f)) \in F.$$

Es lässt sich jedoch noch mehr über eine positiv definite Form f und deren erste Wurzel $w_1(f)$ sagen. Hierzu betrachten wir erneut die Fälle $b = a$ sowie $c = a$ (und $b > 0$):

$$\begin{aligned} 1.) \quad & b = a \quad \Leftrightarrow \quad \operatorname{Re} w_1(f) = -\frac{1}{2} \\ 2.) \quad & c = a \text{ und } b > 0 \quad \Leftrightarrow \quad \operatorname{Re} w_1(f) < 0 \quad \text{und} \quad |w_1(f)| = 1. \end{aligned} \quad (50)$$

ad 1.) Es ist nach (12):

$$f = (a, a, c) \sim (a, -a, c) = f \circ S^{-1}$$

Da des Weitern

$$w_1(f \circ S^{-1}) = w_1(f) + 1 \quad \text{ergibt sich} \quad \operatorname{Re} w_1(f \circ S^{-1}) \stackrel{(46)}{=} -\frac{-a}{2a} = \frac{1}{2}.$$

ad 2.) Aus (12) erhalten wir hier nun:

$$f = (a, b, a) \sim (a, -b, a) = f \circ T.$$

Außerdem ist

$$w_1(f \circ T) = -\frac{1}{w_1(f)} = -\overline{w_1(f)} \quad \text{und daher} \\ \operatorname{Re} w_1(f \circ T) > 0 \quad \text{sowie} \quad |w_1(f \circ T)| \stackrel{(48)}{=} 1.$$

Aus (50) folgt nun:

Jede positiv definite Form f ist mit einer Form g äquivalent, für die gilt:

$$-\frac{1}{2} < \operatorname{Re} w_1(g) \leq \frac{1}{2}, \quad |w_1(g)| \geq 1;$$

$$\text{falls} \quad |w_1(g)| = 1 \quad \Rightarrow \quad \operatorname{Re} w_1(g) \geq 0.$$

$$\stackrel{\text{Satz 3.6}}{\Rightarrow} \quad g \quad \text{ist eindeutig bestimmt.}$$

5.2 Indefinite binäre quadratische Formen

In diesem Abschnitt wollen wir kurz auf die geometrische Charakterisierung einer indefiniten reduzierten Form eingehen. Nach Satz 4.14 gilt für eine reduzierte indefinite Form

$$|w_1(f)| > 1 > |w_2(f)| \quad \text{und} \quad w_1(f)w_2(f) < 0.$$

Dieser Satz lässt sich auch geometrisch veranschaulichen, siehe Abbildung 5.4. Dazu definieren wir den Punkt

$$w(f) := (w_1(f), w_2(f)) = \left(\frac{-b + \sqrt{D}}{2a}, \frac{-b - \sqrt{D_f}}{2a} \right).$$

Die Form f lässt sich sodann für $a \neq 0$ schreiben als

$$f(x, y) = ax^2 + bxy + cy^2 = a \left(x^2 + \frac{b}{a}xy + \frac{c}{a}y^2 \right) = \\ = a \left(x^2 + \frac{b - \sqrt{D} + b + \sqrt{D_f}}{2a}xy + \frac{b^2 - D_f}{4a}y^2 \right)$$

$$= a(x^2 + (-w_1(f) - w_2(f))xy + w_1(f)w_2(f)y^2) = a(x - w_1(f)y)(x - w_2(f)y).$$

In Abbildung 5.4 befinden sich jene Punkte $w(f)$ einer reduzierten Form f in dem dunkler gefärbten Gebiet.^{7 8}

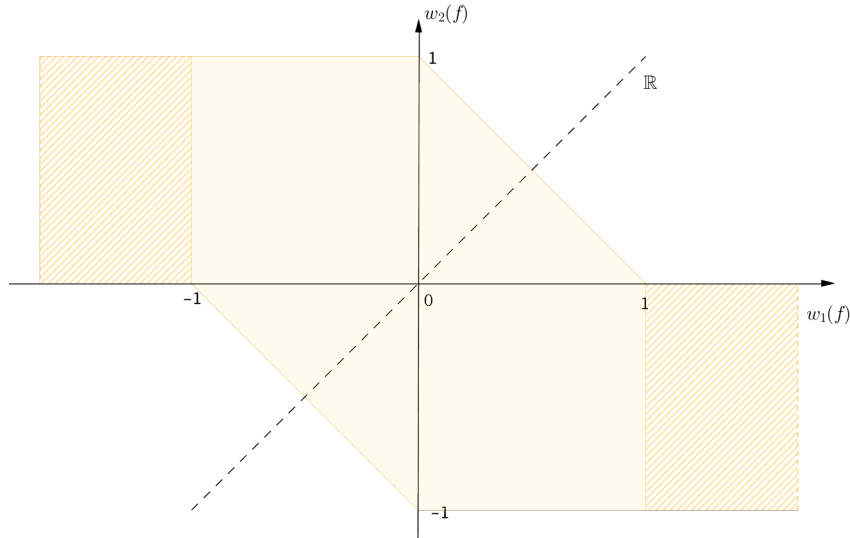


Abbildung 5.4: Punkte reduzierter (und normaler) indefiniten Formen

5.3 Geometrische Veranschaulichung der Gleichung

$$f(x, y) = m$$

Der nun folgende Abschnitt beschäftigt sich mit der geometrischen Orientierung der Gleichung

$$ax^2 + bxy + cy^2 = m. \quad (51)$$

Es sei auch hier $D_f \equiv 0$ oder $1 \pmod{4}$ und D_f kein Quadrat.

Dann gilt im Fall $D_f < 0$, dass durch die Gleichung (51) für

$ma > 0$ eine Ellipse

$m = 0$ ein imaginäres Geradenpaar

⁷Der in Abbildung 5.4 heller gefärbte Teil beinhaltet die Punkte $w(f)$ einer *normalen* Form. Nach (Buchmann 2007: 107) heißt eine indefinite binäre quadratische Form f mit Diskriminante D_f kein Quadrat *normal*, wenn gilt (siehe hierzu auch die Bemerkung auf Seite 72):

$$\begin{aligned} -|a| < b \leq |a| & \quad \text{für } |a| \geq \sqrt{D_f} \\ \sqrt{D_f} - 2|a| < b < \sqrt{D_f} & \quad \text{für } |a| < \sqrt{D_f}. \end{aligned}$$

⁸(Buchmann 2007: 110f.)

$ma < 0$ eine imaginäre Ellipse

dargestellt wird. Handelt es sich bei f um eine indefinite binäre quadratische Form, d. h. es ist $D_f > 0$, so beschreibt die Gleichung (51) im Fall

$m > 0$ oder $m < 0$ eine Hyperbel;⁹
 $m = 0$ ein Geradenpaar, genauer gesagt das Asymptotenpaar
jeder bei $m > 0$ oder $m < 0$ vorkommenden Hyperbel.

Demnach ist auch verständlich, dass eine positiv definite binäre quadratische Form eine endliche Anzahl von ganzen Zahlen darstellt, symbolisiert durch die Gitterpunkte. Wohingegen eine indefinite Form unendliche viele solcher Punkte beinhaltet.¹⁰

Die nun folgenden Beispiele beschreiben Kurven, deren Achsen nicht in Richtung der Koordinatenachsen liegen (erkennbar an dem gemischten Term). Sie entstehen durch Drehung um einen Winkel $\theta \in [0, 2\pi)$ mit der zugehörige Drehmatrix

$$D = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}.$$

Die Rede ist von der sogenannten *Hauptachsentransformation*. Der Winkel θ sowie die Längen der Haupt- und Nebenachsen lassen sich natürlich berechnen. Dabei bedient man sich den algebraischen Kurven zweiter Ordnung, deren Kurvengleichung auch mittels Matrizen beschreibbar ist. Von Interesse dafür ist jene symmetrische Matrix

$$F_f = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix},$$

welche wir bereits auf Seite 4 kennengelernt haben. Um den Kurventyp zu bestimmen, sind die Eigenwerte der Matrix F_f ausschlaggebend. Die zugehörigen Eigenvektoren beschreiben dann die Richtung der Achsen der geneigten Kurven.¹¹

Beispiele: 1.) Es sei die Gleichung $5x^2 + 14xy + 11y^2 = 35$ gegeben. Die zugehörige Ellipse ist der Abbildung 5.5 zu entnehmen. Auf der Kurve sind auch jene Lösungen zu finden, welche wir bereits berechnet haben, siehe Seite 33f.

2.) Gegeben sei die Gleichung $5x^2 - 3xy - y^2 = 13$. Abbildung 5.6 veranschaulicht diese

⁹Hierbei werden x und y als beliebig reelle Koordinaten gedeutet.

¹⁰(Landau 1927: 132)

¹¹Für weitere und genauere Informationen siehe z. B. (Scheid 2009: 116-113), (Burg 2012: 1-54).

Gleichung. Auch in diesem Beispiel wurden die Lösungen, welche auf Seite 82 gegeben sind, eingezeichnet. In Abbildung 5.6(b) wurden die zugehörigen Asymptoten eingezeichnet.

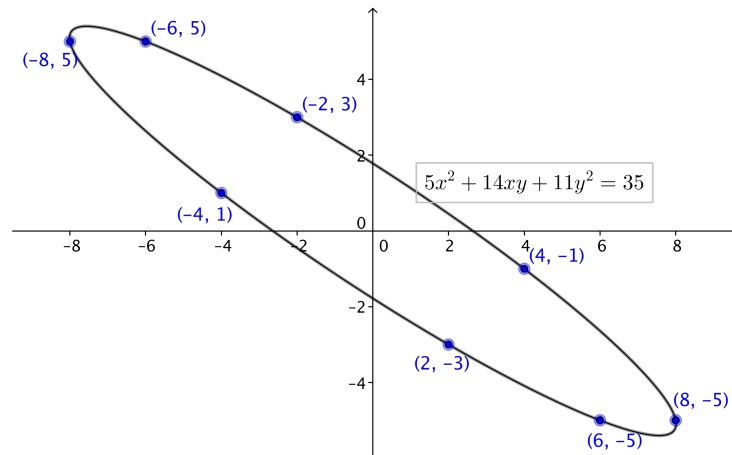


Abbildung 5.5: Geometrische Interpretation der Gleichung $5x^2 + 14xy + 11y^2 = 35$

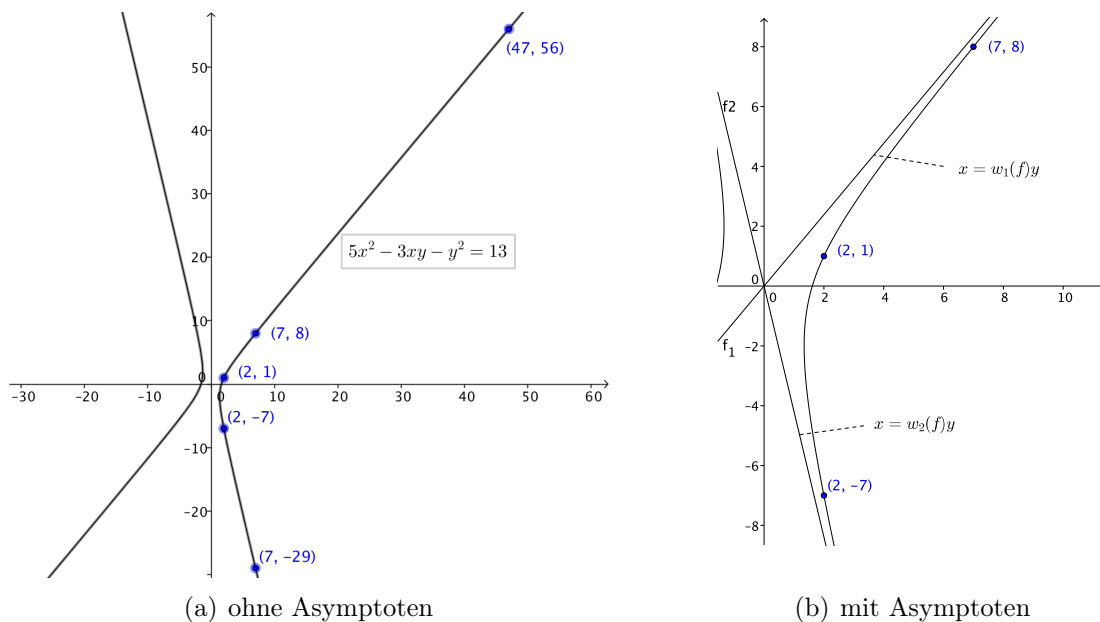


Abbildung 5.6: Geometrische Interpretation der Gleichung $5x^2 - 3xy - y^2 = 13$

Anhang

A Beispiele zur Klassenzahl $h(D)$ für $D < 0$

D	$h(D)$	zugehörige reduzierte Formen	D	$h(D)$	zugehörige reduzierte Formen
-3	1	(1, 1, 1)	-43	1	(1, 1, 11)
-4	1	(1, 0, 1)	-44	3	(1, 0, 11), (3, ± 2 , 4)
-7	1	(1, 1, 2)	-47	5	(1, 1, 12), (2, ± 1 , 6), (3, ± 1 , 4)
-8	1	(1, 0, 2)	-48	2	(1, 0, 12), (3, 0, 4)
-11	1	(1, 1, 3)	-51	2	(1, 1, 13), (3, 3, 5)
-12	1	(1, 0, 3)	-52	2	(1, 0, 13), (2, 2, 7)
-15	2	(1, 1, 4), (2, 1, 2)	-55	4	(1, 1, 14), (2, ± 1 , 7), (4, 3, 4)
-16	1	(1, 0, 4)	-56	4	(1, 0, 14), (2, 0, 7), (3, ± 2 , 5)
-19	1	(1, 1, 5)	-59	3	(1, 1, 15), (3, ± 1 , 5)
-20	2	(1, 0, 5), (2, 2, 3))	-60	2	(1, 0, 15), (3, 0, 5)
-23	3	(1, 1, 6), (2, ± 1 , 3)	-63	4	(1, 1, 16), (2, ± 1 , 8), (4, 1, 4)
-24	2	(1, 0, 6), (2, 0, 3))	-64	2	(1, 0, 16), (4, 4, 5)
-27	1	(1, 1, 7)	-67	1	(1, 1, 17)
-28	1	(1, 0, 7)	-68	4	(1, 0, 17), (2, 2, 9), (3, ± 2 , 6)
-31	3	(1, 1, 8), (2, ± 1 , 4)	-71	7	(1, 1, 18), (2, ± 1 , 9), (3, ± 1 , 6), (4, ± 3 , 5)
-32	2	(1, 0, 8), (3, 2, 3)	-72	2	(1, 0, 18), (2, 0, 9)
-35	2	(1, 1, 9), (3, 1, 3)	-75	2	(1, 1, 19), (3, 3, 7)
-36	2	(1, 0, 9), (2, 2, 5)	-76	3	(1, 0, 19), (4, ± 2 , 5)
-39	4	(1, 1, 10), (2, ± 1 , 5), (3, 3, 4)	-79	5	(1, 1, 20), (2, ± 1 , 10), (4, ± 1 , 5)
-40	2	(1, , 10), (2, 0, 5)	-80	4	(1, 0, 20), (3, ± 2 , 7) , (4, 0, 5)

B Beispiele zur Klassenzahl $h(D)$ für $D > 0$ kein Quadrat

D	$h(D)$	Ketten reduzierter Formen	D	$h(D)$	Ketten reduzierter Formen
5	1	$(1, -1, -1)(-1, -1, 1)$	41	1	$(2, -3, -4)(-4, -5, 1)(1, -5, -4) \sim$ $\sim (-4, -3, 2)(2, -5, -2)(-2, -3, 4) \sim$ $\sim (4, -5, -1)(-1, -5, 4)(4, 3, -2) \sim$ $\sim (-2, -5, 2)$
8	1	$(1, -2, -1)(-1, -2, 1)$	44	2	$(1, -6, -2)(-2, -6, 1);$ $(-1, -6, 2)(2, -6, -1)$
12	2	$(1, -2, -2)(-2, -2, 1);$ $(-1, -2, 2)(2, -2, -1)$	45	2	$(1, -5, -5)(-5, -5, 1);$ $(-1, -5, 5)(5, -5, -1)$
13	1	$(-1, -3, 1)(1, -3, -1)$	48	2	$(1, -6, -3)(-3, -6, 1);$ $(-1, -6, 3)(3, -6, -1)$
17	1	$(1, -3, -2)(-2, -1, 2)(2, -3, -1) \sim$ $\sim (-1, -3, 2)(2, -1, -2)(-2, -3, 1)$	52	1	$(1, -6, -4)(-4, -2, 3)(3, -4, -3) \sim$ $\sim (-3, -2, 4)(4, -6, -1)(-1, -6, 4) \sim$ $\sim (4, -2, -3)(-3, -4, 3)(3, -2, -4) \sim$ $\sim (-5, -6, 1)$
20	1	$(1, -4, -1)(-1, -4, 1)$	53	1	$(1, -7, -1)(-1, -7, 1)$
21	1	$(1, -3, -3)(-3, -3, 1)$	56	2	$(2, -4, -5)(-5, -6, 1)(1, -6, -5) \sim$ $\sim (-5, -4, 2);$ $(-2, -4, 5)(5, -6, -1)(-1, -6, 5) \sim$ $\sim (5, -4, -2)$
24	2	$(1, -4, -2)(-2, -4, 1);$ $(-1, -4, 2)(2, -4, -1)$	57	2	$(3, -3, -4)(-4, -5, 2)(2, -7, -1) \sim$ $\sim (-1, -7, 2)(2, -5, -4)(-4, -3, 3);$ $(-3, -3, 4)(4, -5, -2)(-2, -7, 1) \sim$ $\sim (1, -7, -2)(-2, -5, 4)(4, -3, -3)$
28	2	$(1, -4, -3), (-3, -2, 2), (2, -2, -3) \sim$ $\sim (-3, -4, 1);$ $(-1, -4, 3), (3, -2, -2), (-2, -2, 3) \sim$ $\sim (3, -4, -1)$	60	4	$(1, -6, -6)(-6, -6, 1);$ $(2, -6, -3)(-3, -6, 2);$ $(-1, -6, 6)(6, -6, -1);$ $(-2, -6, 3)(3, -6, -2)$
29	1	$(-1, -5, 1)(1, -5, -1)$			
32	2	$(1, -4, -4)(-4, -4, 1);$ $(-1, -4, 4)(4, -4, -1)$			
33	2	$(1, -5, -2)(-2, -3, 3)(3, -3, -2) \sim$ $\sim (-2, -5, 1);$ $(-1, -5, 2)(2, -3, -3)(-3, -3, 2) \sim$ $\sim (2, -5, -1)$			
37	1	$(1, -5, -3)(-3, -1, 3)(3, -5, -1) \sim$ $\sim (-1, -5, 3)(3, -1, -3)(-3, -5, 1)$			
40	2	$(1, -6, -1)(-1, -6, 1);$ $(2, -4, -3)(-3, -2, 3)(3, -4, -2) \sim$ $\sim (-2, -4, 3)(3, -2, -3)(-3, -4, 2)$			

C Abstract

Diese Arbeit beschäftigt sich mit der Theorie der binären quadratischen Formen, losgelöst von der Theorie der Quadratischen Formen. Ziel ist es, die Gleichung $f(x, y) = ax^2 + bxy + y^2 = m$ für ganzzahlige Koeffizienten in den ganzen Zahlen zu lösen. Diesbezüglich werden die folgenden Fragen behandelt:

Gibt es für gegebene ganze Zahlen m und $D = b^2 - 4ac$, genannt Diskriminante von f , mit $D \equiv 0$ oder $1 \pmod{4}$ eine Darstellung von m durch die Form f ? Welche ganzen Zahlen m werden durch eine Form dargestellt? Existieren mehrere Darstellungsformen von einer ganzen Zahl m ? Wie kann die Äquivalenz zweier oder mehrerer Formen festgestellt werden? u. v. a. m.

Um diese Fragen zu beantworten und tiefere Probleme in der Theorie der binären quadratischen Formen zu lösen, bedarf es Kenntnisse über die Klassenkörpertheorie und anderer komplexer Themenbereiche der algebraischen Zahlentheorie. Darauf wird in dieser Arbeit jedoch verzichtet und der Augenmerk auf eine verständliche Einführung in die Theorie der binären quadratischen Formen gelegt.

Beginnend mit grundlegenden Definitionen und Forderungen an eine binäre quadratische Form ist es in Kapitel 2 die Intention zu bestimmen, wann zwei Formen als äquivalent bezeichnet werden und welchen Ertrag eine Äquivalenz liefert. Kapitel 3 und 4 widmen sich zwei Klassen von binären quadratischen Formen. In beiden Kapiteln ist es ein Anliegen, alle Lösungen der Gleichung $m = ax^2 + bxy + cy^2$ zu bestimmen, sofern dies möglich ist. Um die soeben genannte Gleichung zu lösen, wird eine Lösungsmethode entwickelt und es wird sich die Bedeutung von Automorphismen einer Form zeigen. Schließlich befasst sich Kapitel 5 mit einer geometrischen Interpretation binärer quadratischer Formen und der Gleichung $m = ax^2 + bxy + cy^2$.

Literaturverzeichnis

- [1] Johannes *Buchmann*, Ulrich *Vollmer*, Binary quadratic forms. An algorithmic approach (Berlin/Heidelberg/New York: 2007).
- [2] Duncan A. *Buell*, Binary quadratic forms. Classical theory and modern computations (New York/Berlin/Heidelberg: 1989).
- [3] Peter *Bundschuh*, Einführung in die Zahlentheorie (Berlin/Heidelberg/New York: 2002).
- [4] Klemens *Burg*, Herbert *Haf*, Friedrich *Wille*, Andreas *Meister*, Vektoranalysis. Höhere Mathematik für Ingenieure, Naturwissenschaftler und Mathematiker (Wiesbaden: 2012)
- [5] XCIII. Über die Komposition der binären quadratischen Formen (1893). In: R. *Fricke*, H. *Vermeil*, E. *Bessel-Hagen* (Hrsg.) (Von F. *Klein* mit ergänzenden Zusätzen versehen.), Gesammelte mathematische Abhandlungen. Dritter Band. Elliptische Kurven, insbesondere Modulfunktionen, hyperelliptische und automorphe Funktionen. (Braunschweig/Göttingen: 1923) 283-286.
- [6] Godfrey H. *Hardy*, Edward M. *Wright*, Einführung in die Zahlentheorie. (Original: An introduction to the theory of numbers. (London: 1954)) (Oldenburg/München: 1958).
- [7] Edmund *Hlawka*, Johannes *Schoißengeier*, Rudolf *Taschner*, Geometrische und analytische Zahlentheorie (Wien: 1986).
- [8] Edmund *Hlawka*, Johannes *Schoißengeier*, Zahlentheorie. Eine Einführung (Wien: 1990).
- [9] Edmund *Landau*, Vorlesungen über Zahlentheorie. Aus der elementaren Zahlentheorie (New York: 1950).
- [10] Silvia *Mock*, Eine alternative Sichtweise der Theorie der binären quadratischen Formen. Diplomarbeit, Universität Wien (Wien: 2004).

- [11] Ivan *Niven*, Herbert S. *Zuckermann*, Einführung in die Zahlentheorie I (Original: An Introduction on the Theory of Numbers (u. a. New York: 1972)) (Mannheim/Wien/Zürich: 1976).
- [12] Ivan *Niven*, Herbert S. *Zuckermann*, Einführung in die Zahlentheorie II (Original: An Introduction on the Theory of Numbers (u. a. New York: 1972)) (Mannheim/Wien/Zürich: 1976).
- [13] Paulo *Ribenboim*, Meine Zahlen, meine Freunde. Glanzlichter der Zahlentheorie (Original: My numbers, my friends. Popular Lectures on Number Theory (New York: 2006)) (Heidelberg: 2009).
- [14] Harald *Scheid*, Wolfgang *Schwarz*, Elemente der linearen Algebra und Analysis (Heidelberg: 2009).
- [15] André *Weil*, Zahlentheorie. Ein Gang durch die Geschichte. Von Hammurapi bis Legendre (Original: Number theory: An approach through history; From Hammurapi to Legendre (Boston/Cambridge: 1984)) (Basel: 1992).
- [16] Don B. *Zagier*, Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie (Heidelberg: 1981).

Abbildungsverzeichnis

5.1	2-dimensionales Gitter	84
5.2	Minimumkreise einer reduzierten Form	87
5.3	Fundamentalebene der $SL_2(\mathbb{Z})$	88
5.4	Punkte reduzierter (und normaler) indefiniter Formen	90
5.5	Geometrische Interpretation der Gleichung $5x^2 + 14xy + 11y^2 = 35$	92
5.6	Geometrische Interpretation der Gleichung $5x^2 - 3xy - y^2 = 13$	92

Lebenslauf

Name: Sandra Anna Burda

Geburtsdatum: 05.03.1992

Geburtsort: Sankt Pölten

Staatsbürgerschaft: Österreich

Schulausbildung: 2006-2010: Bundes-Oberstufenrealgymnasium mit
naturwissenschaftlichem Schwerpunkt
Schulring 16, 3100 Sankt Pölten (Abschluss: Matura)
2002-2006: Leopold Figl Hauptschule Atzenbrugg-Heiligeneich
1998-2002: Volksschule Sitzenberg-Reidling

Studium: 2010-2015: Lehramtsstudium (Diplom) UF Mathematik und
UF Geschichte, Sozialkunde und Politische Bildung
31.01.2013: Abschluss des 1. Studienabschnittes
mit Auszeichnung bestanden

Persönliches: seit 2006 freiwillige Lektorin (röm.-kath. Kirche)
seit 1998 Mitglied des Judovereins UJC Rinta-Reidling und
jahrelange Betreuerin der Jugendgruppe im soeben genannten Verein,
Mithelferin bei freiwilligen Veranstaltungen
Interessen: u. a. Musik (Chor, Querflöte), Bücher, Sport und Kochen