PROF. WILHELM ZINK

Ausgewählte Kapitel der Algebra und Zahlentheorie

Skript zur Vorlesung im Sommersemester 2006

HUMBOLDT-UNIVERSITÄT ZU BERLIN
INSTITUT FÜR MATHEMATIK

Beschreibung. Skript zu der Vorlesung *Ausgewählte Kapitel der Algebra und Zahlentheorie* (SS 2006) bei Prof. Zink an der Humboldt Universität zu Berlin.

Achtung. Dieses Skript ist unvollständig und enthält mit Sicherheit Fehler. Insbesondere enthält es nicht alle Beweise. Es ist nur als Ergänzung zur Vorlesung gedacht.

Beweise. Sätze, bei denen der Beweis angedeutet ist (*Beweis.* □), wurden in der Vorlesung bewiesen.

Fehler. Fehler an stamp@mathematik.hu-berlin.de senden.

Web. http://www.mathematik.hu-berlin.de/~zyska/akaz06.pdf

Letzte Änderung: 29. März 2007
Dieses Skript wurde mit Hilfe von KOMA-Script und LaTeX gesetzt.

Inhaltsverzeichnis

1 Binäre quadratische Formen

1. Vorlesung
18.04.2006

Natürliche Zahlen	$\mathbb{N}$
Ganze Zahlen	$\mathbb{Z}$
Rationale Zahlen	$\mathbb{Q}$
Reelle Zahlen	$\mathbb{R}$
komplexe Zahlen	$\mathbb{C}$
p-adische Zahlen	$\mathbb{Q}_p$

Die Zahlbereiche

Problemstellung. Seinen $a, b, c, m \in \mathbb{Z}$. Betrachte

$$ax^2 + bxy + cy^2 = m$$

z.B.

$$x^2 + 3xy + 2y^2 = 7$$

(i) Wann ist eine solche Gleichung *ganzzahlig* lösbar?
- Geometrie: Ellipse oder Hyperbel
- Arithmetik!

(ii) Wie kann man ganzzahlige Lösungen konstruieren? Problem der arithmetischen Geometrie.

Betrachte Gleichungen

$$x^2 + y^2 = m$$

mit $m \in \mathbb{Z}, m \geq 0$. Geometrisch ist dies ein Kreis mit Radius $\sqrt{m}$. Wann gibt es auf einem solchen Kreis Punkte mit ganzzahligen Koordinaten?

1.1 Beispiele.

$$5 = 2^2 + 1^2$$
$$10 = 3^2 + 1^2$$
$$64 = 7^2 + 4^2$$

für $m = M^2$:

$$M^2 = M^2 + 0^2$$

1.2 Gegenbeispiele (Nichtexistenz von Lösungen)**.**

$$m = 3, 19, 154$$

Konstruktiv: Sei $m = x^2 + y^2$ eine Lösung, o.B.d.A. $0 \leq x \leq y$.

$$\Rightarrow \quad 2x^2 \leq m$$
$$\Rightarrow \quad x \leq \left\lfloor \sqrt{\frac{m}{2}} \right\rfloor$$

Also teste

$$m - x^2 = y^2$$

für $x = 0, \ldots, \left\lfloor \sqrt{\frac{m}{2}} \right\rfloor$.

- $m = 19, \left\lfloor \sqrt{\frac{19}{2}} \right\rfloor = 3$ für $x = 0, 1, 2$ ist kein Quadrat also Fehlanzeige.
- $m = 154, \left\lfloor \sqrt{\frac{154}{2}} \right\rfloor = 8, 154 - x^2$ für $x = 0, \ldots, 8$ testen

1	***2***	*3*	**4**
5	6	*7*	**8**
9	**10**	*11*	12
13	14	15	**16**
17	**18**	*19*	**20**
21	22	*23*	24
25	**26**	27	28
29	30	*31*	**32**
33	**34**	35	**36**
37	38	39	**40**

Für $m \leq 40$. Die guten sind fett, die Primzahlen kursiv.

1.3 Lemma. *Wenn $m \equiv 3 \bmod 4$, dann ist m immer schlecht.*

Beweis. Wenn eine Kongruenz nicht realisierbar ist, dann ist erst recht die Gleichung nicht realisierbar:

$$m = x^2 + y^2 \quad \Rightarrow \quad m \equiv x^2 + y^2 \mod 4$$

Test für $x, y \equiv 0,1,2,3 \bmod 4$, also für $x^2, y^2 \equiv 0,1,0,1 \bmod 4$:

$$x^2 + y^2 \equiv \begin{cases} 0+0 \\ 0+1 \\ 1+1 \end{cases} \equiv \begin{cases} 0 \\ 1 \\ 2 \end{cases} \mod 4$$

Die Restklasse 3 kommt nicht vor. □

1.4 Reduktion. Sei $m \equiv 0 \bmod 4$. Modulo 4 ist die einzige Lösung: $0 = 0 + 0$.
D.h.: Wenn $m = x^2 + y^2$ lösbar ist, dann müssen sowohl x wie y gerade sein:

$$\frac{m}{4} = \left(\frac{m}{2}\right)^2 + \left(\frac{y}{2}\right)^2$$

Damit haben wir unser Problem auf die Frage

$$\frac{m}{4} = a^2 + b^2$$

reduziert.
Man kann so lange reduzieren, bis man ein m erhält, das nicht mehr durch 4 teilbar ist. Die interessanten Fälle sind:

$$m \equiv \begin{cases} 1 \\ 2 \end{cases} \mod 4$$

1.1 Primzahlen m

Wir interessieren uns zunächst für den Fall, in dem $m = p$ Primzahl ist.

- Ausnahme: $p = 2 = 1^2 + 1^2$.
- Ungerade Primzahlen $p \neq 2$:

$$\begin{aligned} p &\equiv 1 \pmod 4 \\ p &\equiv 3 \pmod 4 \quad \text{schlecht} \end{aligned}$$

1.5 Satz. *Sei $m = p$ Primzahl $\neq 2$. Dann ist p gut gdw. $p \equiv 1\ (4)$.*

Beweis. Wenn p gut $\Rightarrow p \equiv 1\ (4)$. Zu zeigen: Jede Primzahl $p \equiv 1\ (4)$ ist gut. □

Zwei Bemerkungen:

1.6 Lemma (Eine triviale Bemerkung)**.** *Wenn m_1 und m_2 beide gut sind, dann ist auch $m_1 \cdot m_2$ gut.*

Beweis. □

Interpretation. Vom Standpunkt der komplexen Zahlen:

$$\begin{aligned} z = u + \mathrm{i}v \quad &\Rightarrow \quad |z|^2 = z \cdot \bar{z} = u^2 + v^2 \\ w = a + \mathrm{i}b \quad &\Rightarrow \quad |w|^2 = w \cdot \bar{w} = a^2 + b^2 \end{aligned}$$

Damit:

$$(u^2 + v^2)(a^2 + b^2) = |z|^2 + |w|^2 = |z \cdot w|^2 = x^2 + y^2$$

mit $x = \mathrm{Re}(zw), y = \mathrm{Im}(zw)$.

1.7 Lemma (Eine nichttriviale Bemerkung)**.** *Es sei p eine Primzahl $\neq 2$.*

(i) Der Restklassenring $\mathbb{Z}/p\mathbb{Z}$ ist in diesem Fall ein Körper, d.h. jede Restklasse $[a] \neq [0]$ hat ein Inverses.

(ii) $(\mathbb{Z}/p\mathbb{Z})^\times$ ist Gruppe mit $p - 1$ Elementen.

Behauptung: Diese Gruppe ist immer zyklisch, d.h. es existiert eine Restklasse $[x]$, so dass sämtliche Restklassen $\neq [0]$ als Potenzen von $[x]$ realisierbar sind.

Definition (Primitivwurzel)**.** *Mann nennt dann x eine* ***Primitivwurzel*** $\bmod p$.

Beispiel. (i) $p = 5, x = 2$:

$$x^1 \equiv 2 \qquad x^2 \equiv 4 \qquad x^3 \equiv 3 \qquad x^4 \equiv 1 \mod 5$$

(ii) $p = 7, x = 3$:

$$x^1 \equiv 3 \quad x^2 \equiv 2 \quad x^3 \equiv 6 \quad x^4 \equiv 4 \quad x^5 \equiv 5 \quad x^6 \equiv 1 \mod 5$$

Sei p gegeben. Finde Formel für eine Primitivwurzel mod$p$. Emil ARTIN: Gibt es unendlich viele Primzahlen p, für welche die 2 eine Primitivwurzel ist?

Folgerung. *Es sei x eine Primitivwurzel* mod$p$*. Dann ist*

$$x^{\frac{p-1}{2}} \equiv -1 \mod p$$

Beweis. □

Folgerung. *Wenn $p \equiv 1$ (4) dann ist die Kongruenz*

$$z^2 \equiv -1 \mod p \tag{1.1}$$

lösbar mit $z = x^{\frac{p-1}{4}}$, wobei x eine Primitivwurzel mod$p$ *ist.*

Beweis. □

Folgerung. *Wenn $p \equiv 1$ (4) dann existiert ein Vielfaches $M \cdot p$, so dass*

$$M \cdot p = z^2 + 1 = z^2 + 1^2$$

und

$$M \leq \frac{p-1}{4}$$

Beweis. □

Beispiel. $p = 881, M \leq 220$:

$$170 \cdot 881 = 387^2 + 1^2$$

1.8 Satz (Abstiegsargument von FERMAT[1])**.** *Sei*

$$Mp = a^2 + b^2$$

mit $M < p$. Wenn $M > 1$, dann existiert $M > r \geq 1$, so dass auch

$$rp = x^2 + y^2$$

Deswegen muss dann auch p selbst eine gute Zahl sein.

Beweis. □

2. Vorlesung
25.04.2006

[1] Pierre de FERMAT (1607 oder 1608 – 1665), Jurist, Toulouse

Zusammenfassung. Gegeben sei eine Primzahl $p \equiv 1 \bmod 4$. Suche $p = x^2 + y^2$. Es gilt:

$$x^2 \equiv -1 \mod p \quad \text{und} \quad Mp = x^2 + 1$$

ist lösbar. Wegen das Abstiegsarguments ist dann auch:

$$p = a^2 + b^2$$

Zum Beispiel für $p = 881$:

$$\begin{aligned} 170 \cdot 881 &\equiv 387^2 + 1^2 \\ 47 &\equiv 387 \quad (170) \\ 1 &\equiv 1 \quad (170) \end{aligned}$$

damit

$$47^2 + 1^2 \equiv 387^2 + 1^2 \equiv 0 \quad (170)$$

Also:

$$\begin{aligned} 47^2 + 1^2 &= 170 \cdot 13 \\ 387^2 + 1^2 &= 170 \cdot 881 \end{aligned}$$

und

$$\begin{aligned} & (47^2 + 1^2)(387^2 + 1^2) = 170^2 \cdot 13 \cdot 881 \\ \Leftrightarrow \quad & 18\,190^2 + 340^2 = 170^2 \cdot 13 \cdot 881 \end{aligned}$$

Diese Gleichung muss durch 170^2 teilbar sein:

$$\begin{aligned} & \left(\frac{18\,190}{170}\right)^2 + \left(\frac{340}{170}\right)^2 = 13 \cdot 881 \\ \Leftrightarrow \quad & 107^2 + 2^2 = 13 \cdot 881 \end{aligned}$$

mit $M = 13$ des Abstiegsargument. Dies muss noch iteriert werden, um schließlich von $M = 13$ auf $M = 1$ zu kommen.

In der Praxis ist das Abstiegsargument viel zu schwerfällig (es ist nur Hilfsmittel zum Beweis), sondern man verfährt wie folgt: $881 \equiv 1$ (4) bedeutet 881 ist Summe von 2 Quadraten:

$$881 = x^2 + y^2 \quad \text{mit} \quad x \leq \left\lfloor \sqrt{\frac{881}{2}} \right\rfloor = 20$$

Probiere daher $881 - x^2$ für $x = 1, \ldots, 20$. Man erhält:

$$881 = 16^2 + 25^2$$

Ergebnis. Für Primzahlen erhält man also:

$$\begin{aligned} p &= 2 = 1^2 + 1^2 \\ p &\equiv 3 \quad (4) \quad \text{schlecht} \\ p &\equiv 1 \quad (4) \quad \text{gut} \end{aligned}$$

1.2 Allgemeine Zahlen m

Jede Zahl m ist eindeutiges Produkt von Primzahlpotenzen zugeordnet:

$$\begin{aligned} m &= \prod_{i=1}^{r} p_i^{\nu_i} = p_1^{\nu_1} \cdot \cdots \cdot p_r^{\nu_r} \\ &= \prod p_j^{2\nu_j+1} \cdot \prod p_k^{2\nu_k} = p_{j_1} \cdot \cdots \cdot p_{j_l} M^2 \end{aligned}$$

Idee: Jede natürliche Zahl m schreibt sich eindeutig:

$$m = \underbrace{\text{Produkt verschiedener Primzahlen}}_{\text{ist leer, wenn } m \text{ selbst Quadrat ist}} \cdot \text{Quadrat}$$

In m treten r verschiedene Primzahlen auf. Wenn die entsprechende Potenz gerade ist, dann wird der Primfaktor von M^2 verschluckt.

Beispiel.

$$\begin{aligned} m &= 252\,000 = 2^5 \cdot 3^2 \cdot 5^3 \cdot 7 \\ &= (2 \cdot 5 \cdot 7) \cdot 2^4 \cdot 3^2 \cdot 5^2 \\ &= (2 \cdot 5 \cdot 7)(2^2 \cdot 3 \cdot 5)^2 \end{aligned}$$

1.9 Satz. *Die Primfaktoren p, welche in m mit ungerader Potenz aufgehen, seien höchstens $p \equiv 2$ bzw. $p \equiv 1$ (4). Dann ist m Summe von 2 Quadraten.*

Beweis. □

Weiteres Ziel. Das Ergebnis 1.9 ist vollständig.

2 Der Gaußsche Zahlenring

2.1 Die komplexen Zahlen

2.1 Die komplexen Zahlen $\mathbb{C}$ als Restklassenring $\mathbb{R}[X]$.

- $\mathbb{R}[X]$ = Ring der Polynome mit reellen Koeffizienten
- deg = Gradfunktion
- $(\mathbb{R}[X], \deg)$ ist ein euklidischer Ring , d.h. es gibt eine Division mit Rest: Seien $\alpha, \beta \in \mathbb{R}[X]$ mit $\beta \neq 0$ und

$$\alpha = \sum a_i X^i$$

dann finde eindeutige $q, r \in \mathbb{R}[X]$, so dass

$$\alpha = q\beta + r \quad \text{und} \quad \begin{cases} r = 0 & \text{oder} \\ \deg(r) < \deg(\beta) \end{cases}$$

Allgemeine Konsequenz. Euklidscher Ring ⇒ Hauptidealring ⇒ Faktorieller Ring

Konkret. Jedes Polynom schreibt sich eindeutig bis auf konstante Faktoren als Produkt von irreduziblen Polynomen.

Das Polynom $X^2 + 1 \in \mathbb{R}[X]$ ist irreduzibel. D.h. $(X^2 + 1)$, das von $X^2 + 1$ erzeugte Hauptideal, ist Maximalideal und der Restklassenring

$$\mathbb{R}[X] \Big/ \left(X^2 + 1\right) =: \mathbb{C}$$

ist ein Körper. Die Elemente von $\mathbb{C}$ sind die Restklassen:

$$\alpha \sim \beta \quad \Leftrightarrow \alpha - \beta \text{ teilbar durch } X^2 + 1$$

Die Division mit Rest durch $X^2 + 1$ (deg = 2) bedeutet: in jeder Restklasse findet man einen Repräsentanten der Form $a + bX$ mit $a, b \in \mathbb{R}$. Setzen:

$$\begin{aligned} 1 &\in \mathbb{C} \quad \text{Restklasse des „Polynoms“ } 1 \\ \mathrm{i} &\in \mathbb{C} \quad \text{Restklasse des Polynoms } X \end{aligned}$$

Es gibt also die Relation

$$\mathrm{i}^2 + 1 = [0] = 0$$

Nicht ganz präzise sagt man: Komplexe Zahlen sind

$$z = a + b\mathrm{i} \quad \text{mit } a, b \in \mathbb{R}$$

und der Relation

$$\mathrm{i}^2 + 1 = 0$$

Komplexe Konjugation. Definiert durch

$$z = a + b\mathrm{i} \in \mathbb{C} \mapsto \overline{z} = a - b\mathrm{i} \in \mathbb{C}$$

Sie ist verträglich mit der Addition und Multiplikation:

$$\overline{z + w} = \overline{z} + \overline{w}$$
$$\overline{zw} = \overline{z}\,\overline{w}$$

Wir machen aus $\mathbb{C}$ einen euklidischen Vektorraum: $\mathbb{R} \times \mathbb{C} \to \mathbb{C}$, $\mathbb{R}$ sind die Skalare, $\mathbb{C}$ die Vektoren, d.h. $\mathbb{C}$ ist $\mathbb{R}$-Vektorraum.

Skalarprodukt. $\langle z, w \rangle := \mathrm{Re}(z\overline{w}) \in \mathbb{R}$ mit $z, w \in \mathbb{C}$.

Damit ist $(\mathbb{C}, \langle \circ, \circ \rangle)$ ein euklidischer Vektorraum mit der *Orthonormalbasis* $\{1, \mathrm{i}\}$. $\mathbb{C}$ ist ein 2-dimensionaler $\mathbb{R}$-Vektorraum.

Norm. Für $z = a + b\mathrm{i} \in \mathbb{C}$:

$$\|z\| := \sqrt{\langle z, z \rangle} = \sqrt{\mathrm{Re}\, z\overline{z}} = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2} \in \mathbb{R}$$

Minkowski-Ungleichung.

$$\|z + w\| \leq \|z\| + \|w\|$$
$$\|z - w\| \geq |\|z\| - \|w\||$$

$\mathbb{C}$ ist nicht nur Vektorrraum, sondern wir haben in $\mathbb{C}$ noch die Multiplikation $z \cdot w$. Es gilt:

$$\|zw\| = \|z\|\,\|w\|$$

Betrachte den Einheitskreis $\mathbb{C}^1 := \{z \in \mathbb{C} : \|z\| = 1\}$. Dann gilt für $z \in C^1$, d.h. $a^2 + b^2 = 1$:

$$z = a + b\mathrm{i} = \cos\theta + \sin\theta \cdot \mathrm{i}$$

mit eindeutig bestimmten $\theta \in [0, 2\pi)$. Beachte hier, das $(\mathbb{C}, \langle , \rangle)$ ein euklidischer Raum mit der ON-Basis $\{1, \mathrm{i}\}$ ist. Deswegen gilt für den Winkel θ zwischen z und 1:

$$\cos\theta = \frac{\langle z, 1 \rangle}{\|z\|\,\|1\|} = \mathrm{Re}(z)$$
$$\theta = \arccos \mathrm{Re}(z)$$

Polarkoordinaten. Sei $z \neq 0$.

$$z = \underbrace{\|z\|}_{\in \mathbb{R}} \cdot \underbrace{\frac{z}{\|z\|}}_{\in \mathbb{C}^1} = r(\cos\theta + \mathrm{i}\sin\theta)$$

$r := \|z\|$ und $\theta \in [0,2\pi)$ sind die Polarkoordinaten von z.

Die Multiplikation von komplexen Zahlen schreibt sich bequem, wenn man Polarkoordinaten benutzt:

$$\begin{aligned} z &= r(\cos\theta + \mathrm{i}\sin\theta) \\ w &= s(\cos\psi + \mathrm{i}\sin\psi) \\ zw &= rs\,(\cos(\theta+\psi) + \mathrm{i}\sin(\theta+\psi)) \end{aligned}$$

In $\mathbb{C}^1$ entspricht die Multiplikation der Addition der Winkel modulo 2π.

Beispiel (Die n-ten Einheitswurzeln in $\mathbb{C}$, e^z). Finde z mit $z^n = 1$:

$$\begin{aligned} & z^n = 1 \\ \Rightarrow \quad & \|z\| = 1 \text{ und } z = \cos\theta + \mathrm{i}\sin\theta \\ \Rightarrow \quad & n\cdot\theta = \text{Vielfaches von } 2\pi \\ \Rightarrow \quad & \theta = \frac{2\pi k}{n} \text{ für } k = 0,\ldots,n-1 \end{aligned}$$

Satz. *In $\mathbb{C}$ gibt es genau n n-te Einheitswurzeln. Alle Lösungen haben die Form*

$$z = \cos\theta + \mathrm{i}\sin\theta \quad \textit{mit} \quad \theta = \frac{k\cdot 2\pi}{n}, k = 0,\ldots,n-1$$

Die Gruppe $(\mu_n, \cdot)$ der n-ten Einheitswurzeln ist isomorph zu $(\mathbb{Z}/n\mathbb{Z}, +)$:

$$[k] \mapsto z_k := \cos\frac{k\cdot 2\pi}{n} + \mathrm{i}\sin\frac{k\cdot 2\pi}{n} \qquad z_{k_1+k_2} = z_{k_1}\cdot z_{k_2}$$

Auch $\mathrm{e}^z = \sum_{n=0}^{\infty}\frac{z^n}{n!}$ ist eine wohldefinierte komplexe Zahl (Real- und Imaginärteil).

2.2 Gaußsche Zahlenring

2.2 Definition (Der Gaußsche Zahlenring)**.** *Wir betrachten in $\mathbb{C}$ die Teilmenge der* ***Gaußschen Zahlen***

$$\mathcal{O} = \{z = a + b\mathrm{i} : a, b \in \mathbb{Z}\}$$

Anschaulich ist $\mathcal{O}$ ein Gitter in $\mathbb{C}$.

$\mathcal{O}$ ist ein Ring, d.h. abgeschlossen bezüglich $+$ und $\cdot$. Aber in $\mathcal{O}$ können wir im allgemeinen nicht dividieren. $\mathcal{O}$ ist ein Ring, aber kein Körper.
Wir definieren auf $\mathcal{O}$ die „Norm“:

$$z = a + b\mathrm{i} \in \mathcal{O} \mapsto N(z) := \|z\|^2 = z\bar{z} = a^2 + b^2$$

Die Normen von Gaußschen Zahlen sind genau die Summen von zwei Quadratzahlen. Es gilt:

$$N(zw) = N(z)N(w)$$

2.3 Satz. *Der Gaußsche Zahlenring $(\mathcal{O}, N)$ versehen mit der Normfunktion ist ein euklidischer Ring, d.h. es existiert eine Division mit Rest: Sei $\alpha, \beta \in \mathcal{O}, \beta \neq 0$, dann finde $q, r \in \mathcal{O}$, so dass*

$$\alpha = q\beta + r \quad \textit{mit} \quad N(r) < N(\beta) \textit{ oder } r = 0$$

Beweis. □

Beispiel. Für $z = 6 + 13\mathrm{i}$ und $w = 7 + 3\mathrm{i}$:

$$\begin{aligned}\frac{z}{w} &= \frac{6 + 13\mathrm{i}}{7 + 3\mathrm{i}} = \frac{(6 + 13\mathrm{i})(7 - 3\mathrm{i})}{58} \\ &= \frac{81}{58} + \frac{73}{58}\mathrm{i}\end{aligned}$$

mit der nächstgelegenen Gaußschen Zahl $q = 1 + \mathrm{i}$ ($\frac{81}{58}$ und $\frac{73}{58} \leq 1\frac{1}{2}$):

$$\begin{aligned}z &= qw + r \\ 6 + 13\mathrm{i} &= (1 + \mathrm{i})(7 + 3\mathrm{i}) + (2 + 3\mathrm{i})\end{aligned}$$

erhält man $r = 2 + 3\mathrm{i}$ und $N(w) = 58 > N(r) = 13$.

2.4 Folgerung. *Der Gaußsche Zahlenring $\mathcal{O}$ ist ein faktorieller Ring, d.h. jede Gaußsche Zahl schreibt sich eindeutig bis auf Einheiten als Produkt Gaußscher Primzahlen.*

Beweis. □

Division mit Rest anschaulich. Seien z, w gegeben, $w \neq 0$. Bilde $\frac{z}{w} \in \mathbb{C}$. $\frac{z}{w}$ ist i.A. kein Gitterpunkt. Wir nehmen für q den nächstgelegenen Gitterpunkt mit $N(q) < N(w)$.

$$z = qw + r \qquad\qquad N(r) < N(w)$$

3. Vorlesung
02.05.2006

Definition.

$$\begin{aligned}r\textit{-Primzahl} &:= \textit{Primzahl in } \mathbb{Z} \\ g\textit{-Primzahl} &:= \textit{Primzahl in } \mathcal{O}\end{aligned}$$

2.5 Satz (Einheiten in $\mathcal{O}$)**.** *Eine Zahl $z \in \mathcal{O}$ ist Einheit genau dann, wenn $N(z) = 1$ ist. Also gibt es in $\mathcal{O}$ genau 4 Einheiten:*

$$\mathcal{O}^\times = \{\pm 1, \pm \mathrm{i}\}$$

Beweis. □

Bemerkung. In $\mathbb{Z}$ gilt: $\mathbb{Z}^\times = \{\pm 1\}$. Vier Einheiten bedeuten: Zu jedem $\alpha \in \mathcal{O}, \neq 0$ gibt es genau vier zu α assoziierte Zahlen $\alpha_1 = \alpha, \ldots, \alpha_4$ mit

$$\alpha_i \mid \alpha \quad \text{und} \quad \alpha \mid \alpha_i$$

Und zwar $1 \cdot \alpha$, $-1 \cdot \alpha$, $\mathrm{i} \cdot \alpha$ und $-\mathrm{i} \cdot \alpha$.
Anschaulich:

$\mathbb{Z}$: je ein VertreterVertreter links und rechts der 0
$\mathbb{Z} + \mathrm{i}\mathbb{Z}$: je ein Vetreter in jedem Quadranten

Beispiel.

$\alpha = 20 + 31\mathrm{i}$	Quadrant I
$-\alpha = -20 - 31\mathrm{i}$	Quadrant III
$\mathrm{i}\alpha = -31 + 20\mathrm{i}$	Quadrant II
$-\mathrm{i}\alpha = 31 - 20\mathrm{i}$	Quadrant IV

2.3 Klassifizierung der g-Primzahlen

Unser Ausgangspunkt ist folgender Satz:

2.6 Satz.

(i) Zu jeder r-Primzahl p muss es eine g-Primzahl π mit $\pi \mid p$ geben.

(ii) Ist π eine g-Primzahl, dann existiert genau eine r-Primzahl p mit der Eigenschaft $\pi \mid p$.

Beweis. □

Strategie. Betrachte alle r-Primzahlen und zerlege sie in ein Produkt von g-Primzahlen. Dann sind alle g-Primzahlen bekannt. Für verschiedene p bekommen wir verschiedene g-Primzahlen.

2.7 Satz (Der Fall $p = 2$)**.** *Offensichtlich gilt:*

$$2 = (-\mathrm{i})(1 + \mathrm{i})^2$$

Behauptung: $1 + \mathrm{i}$ *ist eine g-Primzahl und die einzige (bis auf Assoziierte) g-Primzahl, welche* 2 *teilt.*

2.8 Satz (Kriterium)**.** *Es sei $\alpha \in \mathcal{O}$ eine Gauß-Zahl mit der Eigenschaft, dass $N(\alpha)$ eine r-Primzahl ist. Dann muss α eine g-Primzahl sein.*

Beweis. □

2.9 Satz. *Sei p eine r-Primzahl, $p \neq 2$. Dann können nur folgende Fälle eintreten:*

(i) unser p ist sogar eine g-Primzahl

(ii) $p = \pi_1\pi_2$ ist das Produkt von zwei g-Primzahlen mit der Eigenschaft

$$N(\pi_1) = N(\pi_2) = p$$

Die beiden Primfaktoren sind in diesem Fall echt verschieden.

Beweis. □

2.10 Satz. *Sei $p \neq 2$ eine r-Primzahl.*

(i) Wenn $p \equiv 3 \mod 4$, dann ist p auch g-Primzahl.

(ii) Wenn $p \equiv 1 \mod 4$, dann zerlegt sich p in 2 echt verschiedene g-Primzahlen.

Beweis. □

2.11 Satz (Klassifikation der g-Primzahlen)**.** *Zu jeder g-Primzahl π existiert genau eine r-Primzahl p mit $\pi \mid p$.*

(i) $p = 2$. Es gibt bis auf Assoziierte genau ein $\pi \mid 2$, $\pi = 1 + i$.

(ii) $p \equiv 1 \ (4)$. Es gibt genau 2 g-Primzahlen π_1, π_2, welche p teilen. Wir erhalten π_1, π_2 aus einer Zerlegung $p = x^2 + y^2$ mit

$$\pi_1 = x + \mathrm{i}y$$
$$\pi_2 = y + \mathrm{i}x$$

Wir erhalten genau einen Repräsentanten im Quadranten I.

(iii) $p \equiv 3 \ (4)$. Dann ist p g-Primzahl.

Frage. Was sind die Konsequenzen für unser Problem $m = x^2 + y^2$?

2.12 Folgerung. *Sei $m = p$ Primzahl mit $p \equiv 1 \ (4)$. Dann ist die Zerlegung $p = x^2 + y^2$ bis auf Reihenfolge eindeutig.*

Beweis. □

2.13 Hauptsatz. *Sei $m \in \mathbb{N}$. Dann ist m Summe von 2 Quadraten genau dann, wenn für alle Primzahlen $p \equiv 3 \mod 4$ der p-Exponent gerade ist.*

2.14 Satz. *(i) Seien $m, n \in \mathbb{N}$ und sei $m^2 \cdot n$ Summe von 2 Quadraten. Dann ist auch n bereits Summe von 2 Quadraten.*

(ii) Sei $m \in \mathbb{N}$ uns sei $m = r_1^2 + r_2^2$ die Summe von 2 Quadraten rationaler Zahlen. Dann ist m auch darstellbar als Summe von Quadraten ganzer Zahlen.

Beweis. □

2.4 Aufgaben

2.1 Zerlege $\alpha = 21 + 121\mathrm{i}$ in ein Produkt von g-Primzahlen.

2.2 Es sei $p \equiv 3 \bmod 4$. Zeigen Sie, dass dann der Faktorring $\mathcal{O}/p\mathcal{O}$ ein Körper mit p^2 Elementen ist.

2.3 Sei R ein kommutativer Ring mit der Einheitengruppe $R^\times$. Es sei G eine endliche Untergruppe von $R^\times$. Zeigen Sie:

a) Wenn $G \neq \{1\}$, dann ist $\sum_{u \in G} u = 0_R$.

b) Gegeben sei ein regelmäßiges n-Eck in $\mathbb{C}$. Wie kann man den Mittelpunkt dieses n-Ecks berechnen?

3 Geometrische Veranschaulichung unseres Problems

4. Vorlesung
09.05.2006

Seien $a, b, c \in \mathbb{Z}$ und $f(x, y) = ax^2 + bxy + cy^2$. Welche Lösungen $(x, y) \in \mathbb{Z}^2$ kann eine Gleichung

$$f(x, y) = m$$

für $m \in \mathbb{Z}$ haben? $f(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ ist unsere quadratische Form. $A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ ist symmetrisch. Wir wollen die Hauptachsentransformation ausführen.

3.1 Eigenwerte. Dazu brauchen wir die Eigenwerte:

$$\begin{aligned} \chi_A(x) &= X^2 - (a + c)X + \det A = X^2 - (a + c)X + \left(ac - \frac{b^2}{4}\right) \\ &= (X - \lambda_1)(X - \lambda_2) \\ \lambda_{1,2} &= \frac{a + c}{2} \pm \sqrt{(a + c)^2 - 4 \det A} = \frac{a + c}{2} \pm \sqrt{(a + c)^2 + b^2 - 4ac} \\ &= \frac{a + c}{2} \pm \sqrt{(a - c)^2 + b^2} \end{aligned}$$

Wir sehen, dass beide Eigenwerte reell sind, und wir sehen:

$$\begin{aligned} \lambda_1 + \lambda_2 &= a + c \\ \lambda_1 \lambda_2 &= \det A = ac - \frac{b^2}{4} \end{aligned}$$

Allgemein heißt das: für Polynome n-ten Grades bekommt man die Koeffizienten als elementarsymmetrische Funktionen in den Nullstellen des Polynoms. Idee: $(X - \lambda_1) \cdot \cdots \cdot (X - \lambda_n)$ ausmultiplizieren.

3.2 Erinnerung. Sei $A \in \mathbb{R}^{n \times n}$ eine symmetrische Matrix. Dann besitzt der euklidische Vektorraum $(\mathbb{R}^{n \times 1}, \langle \circ, \circ \rangle_S)$, $\langle v, w \rangle_S = v^t \cdot w$ eine Orthonormal-Basis, welche aus Eigenvektoren der Matrix A besteht.

Sei also $(b_1, \ldots, b_n)$ eine solche Basis, und sei $Ab_i = \lambda_i b_i$, dann bilde die Matrix $P = (b_1, \ldots, b_n)$, mit den Vektoren b_i als Spaltenvektoren. Dann gilt:

(i) $(b_1, \ldots, b_n)$ ist ON-Basis $\Leftrightarrow$ P ist Orthogonalmatrix: $P^t P = I_n, P^t = P^{-1}$

(ii) $P^{-1}AP$ ist diagonal mit den Eigenwerten als Einträgen (Reihenfolge!)

$$P^{-1}AP = P^{\mathrm{t}}AP = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

Wir können die Matrix P als Hauptachsentransformation interpretieren.

$P^{\mathrm{t}}P = I_n \Leftrightarrow$ in unserer Standardmetrik erhält die Transformation $\mathbb{R}^{n\times 1} \xrightarrow{P} \mathbb{R}^{n\times 1}$ Längen und Winkel.

Lemma. *Wir betrachten die Quadrik*

$$\Phi_m := \left\{ v \in \mathbb{R}^{n\times 1} : v^{\mathrm{t}} \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} v = m \right\}$$

und die Ausgangsquadrik

$$\Psi_m := \left\{ v \in \mathbb{R}^{n\times 1} : v^{\mathrm{t}} A v = m \right\}$$

Dann führt P genau die Quadrik Φ_m in die Quadrik Ψ_m über.

$$\Phi_m \underset{P^{\mathrm{t}}}{\overset{P}{\longleftrightarrow}} \Psi_m$$

Beweis. □

Uns interessieren ganzzahlige Lösungen von Ψ_m, d.h. wir suchen:

$$\begin{array}{ll} \Psi_m \cap \mathbb{Z}^{n\times 1} & \text{(ganzzahlige Koordinaten)} \\ \quad \downarrow & \\ \Phi_m \cap P^{\mathrm{t}} \cdot \mathbb{Z}^{n\times 1} & \end{array}$$

$\Gamma := P^{\mathrm{t}} \cdot \mathbb{Z}^{n\times 1}$ ist wieder ein Gitter.

Wir untersuchen $n = 2$:

(i) $\Psi_m \cap \mathbb{Z}^{2\times 1}$, $\begin{pmatrix} x & y \end{pmatrix} A \begin{pmatrix} x \\ y \end{pmatrix} = m$

(ii) $\Phi_m \cap \Gamma$ ist das transformierte Problem.

Wir suchen nur nach solchen Lösungen, welche gleichzeitig Gitterpunkte sind.

- Φ_m ist unsere Normalform
- Γ ist ein gedrehtes Gitter

Wei es zwischen (i) und (ii) eine Bijektion gibt, haben wir in jedem Fall gleich viele Lösungen. Um uns einen Eindruck von der Menge der Lösungen zu verschaffen, betrachten wir (ii).

Konkret: Normalform Φ_m für $m \neq 0$:

$$\lambda_1 x^2 + \lambda_2 y^2 = m \tag{3.1}$$

wobei λ_1 und λ_2 Eigenwerte von A sind.

$$A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & a \end{pmatrix} \quad \longleftrightarrow \quad \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

Fallunterscheidung. Wir unterscheiden nach $\operatorname{sgn} \det A$:

(i) $\det A = \lambda_1 \lambda_2 > 0$. D.h. beide Eigenwerte haben dasselbe Vorzeichen. Unsere Gleichung (3.1) ist nur lösbar, wenn

$$\operatorname{sgn}(m) = \operatorname{sgn}(\lambda_i)$$

Was bedeutet das für Ψ_m?

$$\det(A) = ac - \frac{b^2}{4} > 0$$

Also:

$$\operatorname{sgn}(a) = \operatorname{sgn}(c)$$

Außerdem gilt:

$$a + c = \lambda_1 + \lambda_2$$

$\lambda_1, \lambda_2, a, c$ haben alle dasselbe Vorzeichen, und die Gleichung ist nur lösbar, wenn die rechte Seite m auch dieses Vorzeichen hat.

Auswahl der Lösungen: Aus der Normalform (3.1) und $\operatorname{sgn}(\lambda_i) = \operatorname{sgn}(m)$ erhält man:

$$\frac{x^2}{\sqrt{\frac{m}{\lambda_1}}} + \frac{y^2}{\sqrt{\frac{m}{\lambda_2}}} = 1$$

und mit $l = \sqrt{\frac{m}{\lambda_1}}, k = \sqrt{\frac{m}{\lambda_2}}$ erhält man Φ_m als Ellipse:

$$\frac{x^2}{k^2} + \frac{y^2}{l^2} = 1$$

Uns interessieren nur diejenigen Lösungen, welche auf dem gedrehten Gitter $\Gamma = P^{\mathrm{t}} \mathbb{Z}^{2\times 1}$ liegen.

Resultat. $\det A > 0$: Wir können nur Lösungen erwarten, wenn die Vorzeichenbedingung gilt, und wir können höchstens endlich viele Lösungen erwarten.

(ii) $\det(A) = \lambda_1\lambda_2 < 0$. D.h. $\operatorname{sgn}(\lambda_1) \neq \operatorname{sgn}(\lambda_2)$. Jetzt gibt es für die Normalform Φ_m (3.1) keine Einschränkungen mehr für die rechte Seite m. O.B.d.A. :

$$\operatorname{sgn}(\lambda_1) = \operatorname{sgn}(m)$$

Dann können wir Φ_m in der Standardform schreiben

$$\frac{x^2}{\sqrt{\frac{m}{\lambda_1}}} - \frac{y^2}{\sqrt{\frac{m}{-\lambda_2}}} = 1$$

Φ_m ist also Hyperbel:

$$\frac{x^2}{k^2} - \frac{y^2}{l^2} = 1$$

Suche $\Phi_m \cap \Gamma$: In diesem Fall ist es möglich, dass sogar der Durchschnitt $\Phi_m \cap \Gamma$ unendlich viele Punkte hat.
Resultat. Für $\det A < 0$: Es kann für jede rechte Seite m Lösungen geben, und vielleicht sogar unendlich viele Lösungen.

(iii) Sonderfall $\det(A) = ac - \frac{b^2}{4} = 0$. D.h.

$$ac = \frac{b^2}{4}$$

O.B.d.A. $a \neq 0$ (sonst: $b = 0, f(x,y) = cy^2$), also $c = \frac{b^2}{4a}$ und

$$\begin{aligned} & f(x,y) = a^{-1}\left(ax + \frac{b}{2}y\right)^2 = m \\ \Leftrightarrow \quad & \left(ax + \frac{b}{2}y\right)^2 = am \end{aligned}$$

Ein Lösung kann es nur geben, wenn

$$am = n^2$$

das Quadrat einer natürlichen Zahl n ist, und wenn die linearen Gleichungen

$$ax + \frac{b}{2}y = \pm n$$

erfüllt sind. Aus $ac = \left(\frac{b}{2}\right)^2$ folgt $2 \mid b$. Dies führt zu einer ganzzahligen linearen Gleichung.

Beispiel. Für $f(x,y) = x^2 + xy + y^2$ ist

$$A_f = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$$

mit den Eigenwerten $\lambda_1 = \frac{1}{2}$, $\lambda_2 = \frac{1}{2}$ und den auf Länge 1 normierten Eigenvektoren

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

Die zugehörige orthogonale Transfomation ist

$$P = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \qquad P^{\mathrm{t}} A_f P = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{3}{2} \end{pmatrix}$$

oder

$$P = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{mit} \quad \theta = -45^\circ$$

P ist anschaulich die Drehung um $\mathbb{R}^2$ um den Winkel -45°.
Sei $m = 2$. Lösungsmenge Φ_2, d.h. im Gitter $\mathbb{Z}^2$:

$$x^2 + xy + y^2 = 2$$

Lösungmenge Φ_2:

$$\begin{aligned} & \frac{1}{2}x^2 + \frac{3}{2}y^2 = 2 \\ \Leftrightarrow \quad & \frac{x^2}{2^2} + \frac{y^2}{\left(2\sqrt{\frac{1}{3}}\right)^2} = 1 \end{aligned}$$

Es ist $2\sqrt{\frac{1}{3}} \approx 1{,}15$.

3.1 Aufgaben

3.1 $f(x,y) = x^2 + 5xy + y^2 = 1$, $A_f = \begin{pmatrix} 1 & \frac{5}{2} \\ \frac{5}{2} & 1 \end{pmatrix}$, $\det A = 1 - \frac{25}{4} < 0 \Rightarrow$ Hyperbel.

4 Eine Lösungsstrategie

4.1 Definition (Unimodulare Transformation)**.** *Eine ganzzahlige* ***unimodulare Transformation*** *L des Raumes $\mathbb{R}^2$ (allgemein $\mathbb{R}^n$) ist eine lineare Selbstabbildung, welche das Gitter $\mathbb{Z}^2$ (allgemein $\mathbb{Z}^n$) auf sich abbildet.*

Lemma. *Mit $L(x,y) = (x,y) \cdot A$ ist dies äquivalent zu $A \in \mathbb{Z}^{2\times 2}$ und* $\det A = \pm 1$.

Beweis. □

Lemma. *Alle Einträge von A aus $\mathbb{Z}$ und* $\det A = \pm 1$ *ist auch im allgemeinen Fall notwendig und hinreichend.*

Definition und Satz (Unimodulare Gruppe)**.** *Die unimodularen Transformationen bilden bezüglich Matrizenmultiplikation eine Gruppe, die so genannte* ***unimodulare Gruppe*** $\mathrm{GL}_2(\mathbb{Z})$ *(bzw.* $\mathrm{GL}_n(\mathbb{Z})$*).*

Beispiel. Wie beschafft man sich konkret Elemente aus der Gruppe $\mathrm{GL}_2(\mathbb{Z})$? Es gilt:

$$\alpha\delta - \beta\gamma = \pm 1$$

D.h. alle Einträge aus einer beliebig gewählten Zeile oder Spalte müssen immer ggT = 1 haben. Wähle irgendein Paar α, β mit $\mathrm{ggT}(\alpha,\beta) = 1$. Bilde

$$\begin{pmatrix} \alpha & \beta \\ -\gamma & \alpha \end{pmatrix}$$

und finde x und y mit

$$x\alpha + y\beta = 1$$

$$\begin{pmatrix} \alpha & \leftrightarrow & \beta \\ \updownarrow & & \updownarrow \\ \gamma & \leftrightarrow & \delta \end{pmatrix}$$

ggT = 1

4.2 Definition. $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{GL}_2(\mathbb{Z})$ *sind die Matrizen mit* $\det = 1$. *Sie bilden eine Gruppe, die* ***spezielle lineare Gruppe****.*

5. Vorlesung
16.05.2006

4.3 Definition. *(i) Es sei* BQF *die Menge der binären quadratischen Formen.*

(ii) Für $f(x,y) = ax^2 + bxy + cy^2$ schreiben wir als Abkürzung $f = (a,b,c)$.

(iii) Sei $M \in \mathrm{GL}_2(\mathbb{Z})$. Setze für $M \circ f$:

$$(M \circ f)(x,y) := f((x,y) \cdot M)$$

Lemma. *Aus der der Funktion $f(x,y)$ können die Koeffizienten rekonstruiert werden:*

$$f(1,0) = a \qquad f(1,1) - f(1,0) - f(0,1) = b \qquad f(0,1) = c$$

Lemma. *Sei* $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$. *Die Koeffizienten der neuen Form* $Mf \in \mathrm{BQF}$ *sind:*

$$\begin{aligned} a_{Mf} &= f(\alpha, \beta) \\ b_{Mf} &= f(\alpha + \beta, \gamma + \delta) - f(\alpha, \beta) - f(\gamma, \delta) \\ c_{Mf} &= f(\gamma, \delta) \end{aligned}$$

Beweis. □

Die Transformationen $M \in \mathrm{GL}_2(\mathbb{Z})$ leisten für unser Problem das Folgende:

4.4 Satz. *Betrachte*

$$\begin{aligned} S_{\mathbb{Z}}(f, m) &:= \left\{(x, y) \in \mathbb{Z}^2 : f(x, y) = m\right\} \\ S_{\mathbb{Z}}(Mf, m) &= \left\{(x, y) \in \mathbb{Z}^2 : (Mf)(x, y) = m\right\} \end{aligned}$$

Dann können wir Lösungsmengen vermittels M *ineinander überführen:*

$$\begin{aligned} S_{\mathbb{Z}}(f, m) &= S_{\mathbb{Z}}(Mf, m) \circ M \\ (x, y) \cdot M &\leftrightarrow (x, y) \end{aligned}$$

Beweis. □

Wir betrachten nur Matrizen $M \in \mathrm{GL}_2(\mathbb{Z})$ um zu garantieren, dass bei der Transformation ganzzahlige Lösungen in ganzzahlige übergehen.

Strategie. Gehe von $f(x, y) = m$ in eine äquivalente Gleichung $(Mf)(x, y) = m$ über, welche sich leichter lösen lässt.

4.5 Satz. *Auf* BQF *existiert eine Äquivalenzrelation. Seien* $f, g \in \mathrm{BQF}$*:*

$$f \sim g :\Leftrightarrow \exists M \in \mathrm{GL}_2(\mathbb{Z}) : g = Mf$$

Beweis. □

Bemerkung. Eine Äquivalenzrelation entsteht immer dann, wenn eine Gruppe G auf einer Menge S operiert:

$$\begin{aligned} G \times S &\to S \\ (g, s) &\mapsto g \circ s \end{aligned}$$

Damit eine Äquivalenzrelation entsteht, braucht man folgende Eigenschaften:

$$1_G \circ s = s \tag{E1}$$

$$g_1 \circ (g_2 \circ s) = (g_1 g_2) \circ s \tag{E2}$$

Wie entsteht die Äquivalenzrelation? Allgemein:

$$s_1 \sim s_2 : \Leftrightarrow \exists g \in G : s_2 = g \circ s_1$$

Nachweis der Äquivalenzeigenschaften:

(i) *Reflexivität $s \sim s$:* Nimm $g = 1_G$.

(ii) *Symmetrie $s_1 \sim s_2 \Rightarrow s_2 \sim s_1$: $s_2 = g \circ s_2 \Leftrightarrow g^{-1} \circ s_2 = s_1$*

(iii) *Transitivität $s_1 \sim s_2, s_2 \sim s_3 \Rightarrow s_1 \sim s_3$:* Also $s_2 = g \circ s_1$ und $s_3 = h \circ s_2$. Dann ist $s_3 = h \circ (g \circ s_1) = (hg) \circ s_1$.

Der konkrete Fall ergibt auf BQF eine Äquivalenzrelation. Alle Formen aus derselben Äquivalenzklasse haben äquivalente Lösungsmengen.

Definition (1-Äquivalenz)**.** *In Satz 4.5 könnte man auch die Gruppe $G = \mathrm{SL}_2(\mathbb{Z})$ betrachten. Dann sprechen wir von **1-Äquivalenz**.*

4.6 Satz. *Sei $A_f = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ die Matrix zu $f(x,y) = (a,b,c) = ax^2 + bxy + cy^2$. Dann gilt:*

$$A_{Mf} = MA_fM^{\mathrm{t}}$$

Beweis. □

Folgerung. *Wenn $f \sim g \in$ BQF, dann ist $\det A_f = \det A_g$.*

Beweis. □

Die Umkehrung gilt im Allgemeinen nicht. Zwei Sonderfälle, bei denen die Umkehrung gilt:

(i) $f(x,y) = (1,0,1) = x^2 + y^2$ mit $A_f = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ und $\det A_f = 1$. Wenn $\det A_g = 1$, dann ist $g \sim f$.

(ii) $f(x,y) = (1,1,1) = x^2 + xy + y^2$ mit $A_f = \left(\begin{smallmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{smallmatrix}\right)$ und $\det A_f = \frac{3}{4}$. Wenn $\det A_g = \frac{3}{4}$, dann ist $g \sim f$.

Definition (Diskriminante, eigentliche Lösung)**.**

*(i) Man nennt $D_f := -4 \det A_f$ die **Diskriminante** von f. Für $A_f = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ ist $D_f = b^2 - 4ac$.*

*(ii) Als **eigentliche Lösung** von $f(x,y) = m$ bezeichnet man eine Lösung (x_0, y_0) mit $\mathrm{ggT}(x_0, y_0) = 1$.*

4.7 Satz. *Sei $f = (a,b,c) \in$ BQF. Dann ist folgendes äquivalent:*

(i) $f(x,y) = m$ besitzt eine eigentliche Lösung.

(ii) f ist äquivalent zu einer Form g von Typ $g = (m, \beta, \gamma)$.

Beweis. □

Definition (quadratischer Rest)**.** *Eine ganze Zahl r heißt **quadratischer Rest** modulo m, falls die Kongruenz $r \equiv x^2 \bmod m$ lösbar ist.*

4.8 Folgerung. *Wenn $f(x, y) = m$ eine eigentliche Lösung hat, dann ist*

$$D_f \equiv x^2 \mod |4m|$$

lösbar. D.h. D_f ist dann ein quadratischer Rest (modulo $|4m|$).

Beweis. □

Anwendung. Betrachte wieder $x^2 + y^2 = m$. Wann hat die Gleichung Lösungen?

$$f(x, y) = (1,0,1) = x^2 + y^2 \qquad D_f = -4 \det A_f = -4$$

Also notwendige Bedingung: $-4 \equiv x^2 \bmod 4m$. Also:

$$x = 2y \quad \text{und} \quad -1 \equiv y^2 \mod m$$

Für welche Moduln m ist -1 ein quadratischer Rest?

4.9 Satz. *Sei $m = p_1^{\nu_1} \cdots p_r^{\nu_r}$. Dann ist $D = x^2 \bmod m$ lösbar gdw. $D \equiv x_1^2 \bmod p_i^{\nu_i}$ Lösungen x_i für alle $i = 1, \ldots, r$ hat.*

Beweis. □

Anwendung. $-1 \equiv y^2 \bmod m$ ist lösbar gdw. $-1 \equiv y^2 \bmod p_i^{\nu_i}$ für alle Primteiler von m. Dies ist äquivalent zu

$$-1 \equiv y^2 \mod p \text{ lösbar} \quad \Leftrightarrow \quad \text{lösbar für } p \equiv 1 \mod 4$$

$m = x^2 + y^2$ hat nur dann eigentliche Lösungen, wenn für alle Primteiler $p \neq 2$ von m $p \equiv 1\ (4)$ gilt.

6. Vorlesung
23.05.2006

Beispiel. Sei $f = (1,3,2) = x^2 + 3xy + 2y^2$ und $M = \left(\begin{smallmatrix} 5 & 4 \\ 4 & 3 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$. Was ist $M \circ f = (\alpha, \beta, \gamma)$? Drei Möglichkeiten der Berechnung:

(i) direkt ausrechnen:

$$\begin{aligned}(Mf)(x, y) &= f((x, y)M) = f(5x + 4y, 4x + 3y) \\ &= (5x + 4y)^2 + 3(5x + 4y)(4x + 3y) + 2(4x + 3y) \\ &= \cdots = 117x^2 + 181xy + 70y^2\end{aligned}$$

(ii) Koeffizienten berechnen:

$$\alpha = f(Z_1(M)) = f(5,4) = 5^2 + 3 \cdot 20 + 2 \cdot 16 = 117$$
$$\gamma = f(Z_2(M)) = f(4,3) = 4^2 + 3 \cdot 12 + 2 \cdot 9 = 70$$
$$\beta = f(Z_1(M) + Z_2(M)) - f(Z_1(M)) - f(Z_2(M)) = f(9,7) - 117 - 70 = 181$$

(iii) Über die zugehörige Matrix $f \mapsto A_f = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$:

$$A_{Mf} = MA_fM^{\mathrm{t}} = \begin{pmatrix} 5 & 4 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & \frac{3}{2} \\ \frac{3}{2} & 2 \end{pmatrix} \begin{pmatrix} 5 & 4 \\ 4 & 3 \end{pmatrix} = \cdots = \begin{pmatrix} 117 & \frac{181}{2} \\ \frac{181}{2} & 70 \end{pmatrix}$$

Ergebnis: $Mf = (117,181,70)$. Für die Diskriminante $D = b^2 - 4ac$ gilt:

$$D_f = 9 - 8 = 1 = 181^2 - 4 \cdot 117 = D_{Mf}$$

4.1 Veranschaulichung der Transformationen aus $\mathrm{GL}_2(\mathbb{Z})$ in $\mathbb{R}^2$

Resultat in $\mathbb{R}^{n\times 1}$. Seien $b_1, \ldots, b_n$ Spaltenvektoren, die eine Basis bilden. Dazu gehört das Parallelotop:

$$P(b_1, \ldots, b_n) = \left\{ \sum_{i=1}^{n} \lambda_i b_i : 0 \le \lambda_i \le 1 \right\}$$

Es gilt:

$$\mathrm{vol}\, P(b_1, \ldots, b_n) = |\det(b_1, \ldots, b_n)|$$

$\mathrm{vol}\, P$ ist als Vergleichszahl zum Volumen des Einheitswürfel $P_0 = P(e_1, \ldots, e_n)$, aufgespannt von den Einheitsvektoren, zu verstehen.

In $\mathbb{R}^{2\times 1}$. Sei $B = (b_1, b_2) \in \mathrm{GL}_2(\mathbb{Z})$. Dann ist $|\det B| = 1$, also $\mathrm{vol}\, P(b_1, b_2) = 1$.

Pflasterung. Sei $P_0 = P(e_1, e_2)$ der Einheitswürfel. Man erhält die Pflasterung:

$$\mathbb{R}^2 = \bigcup_{\gamma \in \mathbb{Z}^2} (\gamma + P_0)$$

Wir wenden hierauf $B \in \mathrm{GL}_2(\mathbb{Z})$ an. Da $\det B \neq 0$, ist die Transformation bijektiv. Mit $P_1 = B(P_0)$:

$$\mathbb{R}^2 = \bigcup_{\gamma' \in \mathbb{Z}^2} (B(\gamma) + P_1)$$

B ist ganzzahlig, also ist $B(\mathbb{Z}^2) = \Gamma \subseteq \mathbb{Z}^2$. Deswegen:

$$\mathbb{R}^2 = \bigcup_{\gamma' \in \Gamma = B(\mathbb{Z}^2)} (\gamma' + P_1)$$

Das Volumen von P_1 ist ebenfalls 1. Wir brauchen als Ansatzpunkt für unsere Pflastersteine sämtliche Elemente aus $\mathbb{Z}^2$. Daher:

$$\Gamma = \mathbb{Z}^2$$

Man kann zeigen:

Satz. Es sei (b_1, b_2) Basis von $\mathbb{R}^2$ mit ganzzahligen Koordinaten, d.h. $B = (b_1, b_2) \in \mathbb{Z}^{2\times 2} \cap \mathrm{GL}_2(\mathbb{Q})$, $P_1 = B(P_0)$ und $\Gamma = B(\mathbb{Z}^2)$. Dann ist

$$(\mathbb{Z}^2 : \Gamma) = \frac{\mathrm{vol}\, P_1}{\mathrm{vol}\, P_0} = \mathrm{vol}\, P_1 = |\det B|$$

wobei $(\mathbb{Z}^2 : \Gamma)$ den Index der Untergruppe Γ in der additiven Gruppe $\mathbb{Z}^2$ bezeichnet.

4.2 Konstruktion von Matrizen aus $\mathrm{GL}_2(\mathbb{Z})$

Wie stellt man Matrizen aus $\mathrm{GL}_2(\mathbb{Z})$ her? Es gilt:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \quad \Rightarrow \quad \mathrm{ggT}(a, b) = 1$$

Beginne mit einem Zahlenpaar $1 = xa + yb$ realisierbar, also ist $\left(\begin{smallmatrix} a & b \\ -y & x \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Beispiel. Konkret: (31,13). Nutze die erweiterte Ping-Pong-Methode, suche zuerst $[13]_{31}^{-1}$:

$$\begin{pmatrix} 31 & 13 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 5 & 13 \\ -2 & 1 \end{pmatrix} \sim \begin{pmatrix} 5 & -2 \\ -2 & 7 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 \\ 12 & 7 \end{pmatrix}$$

Also ist $12 \cdot 13 \equiv 1 \bmod 31$ und aus $1 = 12 \cdot 13 + 31x$ erhält man $x = -5$. Damit ist $\left(\begin{smallmatrix} 31 & 13 \\ -12 & -5 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Frage. Wie findet man *alle* Matrizen $\left(\begin{smallmatrix} 31 & 13 \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ oder $\in \mathrm{GL}_2(\mathbb{Z})$?

Eine zweite Möglichkeit. Beginne mit $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ und wende darauf Zeilen- bzw. Spaltenoperationen an, welche ganzzahlig invertierbar sind. Möglichkeiten[1]

(i) Zeilen- und Spaltenaddtion. Für $n \in \mathbb{Z}$:

$$Z_1 \longrightarrow Z_1 + nZ_2$$
$$S_1 \longrightarrow S_1 + nS_2$$

[1] Z_i und S_i sind Zeile i und Spalte i.

(ii) Vertauschung von Zeilen oder Spalten

(iii) Ersetzte Z_i bzw. S_i durch nZ_i bzw. nS_i. Es ist nur $n = \pm 1$ erlaubt.

Beispiel.

$$\begin{pmatrix}1&0\\0&1\end{pmatrix} \overset{\text{a)}}{\sim} \begin{pmatrix}1&5\\0&1\end{pmatrix} \overset{\text{a)}}{\sim} \begin{pmatrix}11&5\\2&1\end{pmatrix} \overset{\text{b)}}{\sim} \begin{pmatrix}2&1\\11&5\end{pmatrix} \overset{\text{a)}}{\sim} \begin{pmatrix}2&3\\11&16\end{pmatrix} \dots$$

Möglichkeiten zur Berechnung von MAM^{t}. Sei $\mathrm{GL}_2(\mathbb{Z}) \ni M = Z(I)$ erzeugt durch eine Folge von Zeilenoperationen Z. Dann ist $M^{\mathrm{t}} = S(I)$ erzeugt durch eine entsprechende Folge von Spaltenoperationen S. Daher:

$$\begin{aligned} MAM^{\mathrm{t}} &= Z(I) \cdot A \cdot S(I) = Z(A) \cdot S(I) \\ &= S(Z(A)) = Z(S(A)) \end{aligned}$$

Beispiel. Sei $f = (a,b,c)$.

(i) Für $M = \left(\begin{smallmatrix}1&0\\n&1\end{smallmatrix}\right)$:

$$\begin{aligned} \begin{pmatrix}1&0\\n&1\end{pmatrix}\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix}\begin{pmatrix}1&n\\0&1\end{pmatrix} &= \begin{pmatrix}a&\frac{b}{2}\\na+\frac{b}{2}&n\frac{b}{2}+c\end{pmatrix}\begin{pmatrix}1&n\\0&1\end{pmatrix} \\ &= \begin{pmatrix}a&na+\frac{b}{2}\\na+\frac{b}{2}&n^2a+nb+c\end{pmatrix} \end{aligned}$$

Dann ist also $Mf = (a, 2na+b, n^2a+nb+c)$.

(ii) Für $M = \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$, erzeugt durch 2 Zeilenoperationen (Vertauschen und 1 Zeile mit -1 multiplizieren).

$$\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix} \sim \begin{pmatrix}c&\frac{b}{2}\\\frac{b}{2}&a\end{pmatrix} \sim \begin{pmatrix}c&-\frac{b}{2}\\-\frac{b}{2}&a\end{pmatrix}$$

Also ist $Mf = (c, -b, a)$.

4.10 Satz (Kriterium von LEGENDRE[2])**.** *Wenn $f(x,y) = m$ eine eigentliche Lösung hat, dann muss die Diskriminante $D_f \equiv X^2 \mod 4m$ sein.*

4.11 Anwendung. Zwei Anwendungen des LEGENDRE-Kriteriums:

(i) Sei $f = (1,0,1)$, $D_f = -4$ und $x^2 + y^2 = m$ eigentlich lösbar. Dann gilt:

$$\begin{aligned} & & -4 &\equiv x^2 \mod 4m \\ \text{mit } x = 2y: \quad &\Leftrightarrow & -1 &\equiv y^2 \mod m \\ \text{mit Chin. Restsatz:} \quad &\Leftrightarrow & -1 &\equiv y^2 \mod p^{\nu_p(m)} \mod p \quad \forall p \mid m \\ \text{mit Lemma:} \quad &\Leftrightarrow & -1 &\equiv y^2 \mod p \quad \forall p \mid m \\ \text{mit Vortrag quadr. Rest:} \quad &\Leftrightarrow & p &\equiv 1 \mod 4 \quad \text{oder} \quad p = 2, \nu_2(m) = 1 \end{aligned}$$

[2] Adrian-Marie LEGENDRE, 1752 – 1833, Professor an der École Normale, Paris

(ii) Sei $f = (1,1,1)$, $D_f = -3$ und $x^2 + xy + y^2 = m$ eigentlich lösbar. Dann folgt:

$$\begin{aligned} & & -3 \equiv x^2 \mod 4m \text{ lösbar} \\ m \text{ ungerade, chin. Restsatz:} \quad & \Leftrightarrow & -3 \equiv x^2 \mod m \text{ lösbar} \\ & \Leftrightarrow & -3 \equiv x^2 \mod p^{\nu_p(m)} \text{ lösbar für alle } p \\ \text{quadratischer Rest:} \quad & \Leftrightarrow & -3 \equiv x^2 \mod p \text{ lösbar für alle } p \mid m \end{aligned}$$

$\Leftrightarrow$ Die Primteiler von p haben alle die Eigenschaft $p \equiv 1 \bmod 3$.

Lemma. *Sei $p \neq 2$ eine Primzahl $p \nmid \Delta$. Dann ist $\Delta \equiv X^2 \mod p^\nu$ für $\nu \geq 1$ lösbar gdw. $\Delta \equiv X^2 \mod p$ lösbar ist.*

Beweis. □

Vorhin hatten wir:

$$-1 \equiv y^2 \mod p^{\nu_p(m)} \quad \Leftrightarrow \quad -1 \equiv y^2 \mod p \quad \Leftrightarrow \quad p \equiv 1 \mod 4$$

Ergebnis. Wenn $x^2 + y^2 = m$ eine eigentliche Lösung hat, dann folgt: Die Primteiler von m sind alle $\equiv 1 \bmod 4$ und $\nu_2(m) \leq 1$.

Mit dem Ring $\mathcal{O}$der Gauß-Zahlen kann man auch die Umkehrung beweisen.

7. Vorlesung
30.05.2006

Wir betrachten

$$x^2 + y^2 = m \tag{4.1}$$

Nach dem Legendre-Kriterium gilt: Wenn (4.1) eine eigentliche Lösung hat, dann ist

$$p \equiv 1 \bmod 4 \forall p \mid m \text{ und eventuell } \nu_2(m) = 1 \tag{4.2}$$

4.12 Satz. *Es gilt auch die Umkehrung, d.h. wenn* (4.2) *erfüllt ist, dann besitzt* (4.1) *eine eigentliche Lösung.*

Beweis. □

Beispiel. Sei $x^2 + y^2 = 17^2$. Da $17 \equiv 1 \ (4)$ ist, muss eine primitive Lösung existieren. Es ist $17 = 4^1 + 1^2$, d.h. $\pi_{17} = 4 + \mathrm{i}$ und $\overline{\pi_{17}} = 4 - \mathrm{i}$ sind die beiden Primteiler von 17 im Ring $\mathcal{O}$. Bilde

$$y = \pi_{17}^3 = (4 + \mathrm{i})^3 = 52 + 47\mathrm{i}$$

Damit erhält man eine primitive Lösung:

$$17^3 = 52^2 + 47^2$$

Eine nichtprimitive Lösung folgt direkt aus $17 = 4^2 + 1^2$:

$$17^3 = 17 \cdot 17^2 = (4 \cdot 17)^2 + 17^2$$

Bemerkung (Zurückführung auf primitive Lösungen). Ist $f(x,y) = m$ und (x_0, y_0) eine Lösung mit $\mathrm{ggT}(x_0, y_0) = d$, dann muss d^2 m teilen und es gilt

$$f\left(\frac{x_0}{d}, \frac{y_0}{d}\right) = \frac{m}{d^2}$$

Also ist $\left(\frac{x_0}{d}, \frac{y_0}{d}\right)$ eine primitive Lösung der Gleichung $f(x,y) = \frac{m}{d^2}$.

4.13 Hauptsatz. *Sei $f = (a,b,c) \in \mathrm{BQF}$ und $m \neq 0 \in \mathbb{Z}$. Um die eigentlichen Lösungen von $f(x,y) = m$ zu bestimmen, muss man folgende Daten betrachten:*

(i) Die Menge $\{\beta_1, \ldots, \beta_k\}$ aller Lösungen der Kongruenz

$$D_f \equiv x^2 \mod 4m$$

im Bereich $\{0,1,2,\ldots,2|m|-1\}$.

(ii) Zu jedem β_i, $i = 1, \ldots, k$, bilde

$$\gamma_i = \frac{1}{4m}\left(\beta_i^2 - D_f\right)$$

und betrachte die Formen $f_i = (m, \beta_i, \gamma_i)$. (Diese haben alla die Diskriminante D_f.)

(iii) Prüfe, welche der der Formen f_i tatsächlich zu f 1-äquivalent sind, und finde gegebenenfalls $U_i \in \mathrm{SL}_2(\mathbb{Z})$, so dass $f_i = U_i \circ f$ ist. (O.B.d.A. : $f_1, \ldots, f_t \sim f$, $f_{t+1}, \ldots, f_k \nsim f$)

(iv) Bestimme die Automorphismengruppe

$$\mathrm{Aut}\, f := \{U \in \mathrm{SL}_2(\mathbb{Z}) : U \circ f = f\}$$

Wenn diese Daten bekannt sind, dann gilt: Sämtliche eigentliche Lösungen von $f(x,y) = m$ sind gegeben in der Form

$$(1,0) \cdot U_i U \text{ für } i = 1, \ldots, t \text{ und für alle } U \in \mathrm{Aut}\, f$$

D.h. als erste Zeile der Matrix $U_i U$.

Beweis. □

4.3 Aufgaben

4.1 Schreibe einige unimodulare Matrizen auf, und stelle fest, dass sie das Normalgitter $\mathbb{Z}^2$ in sich überführen.

4.2 Aktion einer Gruppe G auf Menge S.

a) $S = \mathbb{R}^{m\times n}$, $G = \mathrm{GL}_m(\mathbb{R})$

$$G \times S \to S$$
$$(A, M) \mapsto A \cdot M$$

Die zugehörige Äquivalenz ist die Zeilenäquivalenz[3].

b) $S = \mathbb{R}^{m\times n}$, $G = \mathrm{GL}_n(\mathbb{R})$. Operation:

$$(A, M) \mapsto M \cdot A^{-1}$$

Die zugehörige Äquivalenzrelation ist die Spaltenäquivalenz.

4.3 Berechne $M \circ f$ für

a) $f = (1,2,1)$, $M = \left(\begin{smallmatrix} 3 & 4 \\ 5 & 7 \end{smallmatrix}\right)$

b) $f = (3,1,4)$, $M = \left(\begin{smallmatrix} 7 & 15 \\ 1 & 2 \end{smallmatrix}\right)$

Zwei Methoden, um die Koeffizienten von $M \circ f$ zu bestimmen. $A_{M\circ f} = MA_f M^{\mathrm{t}}$.

4.4 Sei $f = (1,0,1)$. $x^2 + y^2 = 17$ ist eigenlich lösbar mit $x = 4$ und $y = 1$. Man finde $g = (17, \beta, \gamma)$ mit $f \sim g$.

4.5 Zu gegebener 1. Zeile (a, b) bestimme man alle Matrizen $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$.

4.6 Für $B = (b_1, b_2) \in \mathrm{GL}_2(\mathbb{Z})$ sei $P = P(b_1, b_2)$ das zugehörige Parallelogramm. Dann liegt im Inneren von P kein Punkt aus $\mathbb{Z}^2$.

4.7 Was sagen unsere Kriterien über die Lösbarkeit von $x^2 + xy + y^2 = m$ für ungerades $m > 1$? *Hinweis:* Zurückführung auf quadratische Rest mod p.

[3] wenn die Matrizen durch eine Folge elementarer Zeilenoperationen hervorgehen

5 Reduktionstheorie und geometrische Veranschaulichung

In der Reduktionstheorie wird folgende Frage behandelt: Gegeben seien zwei Formen $f = (\alpha, \beta, \gamma)$ und $h = (\alpha', \beta', \gamma')$ mit derselben Diskriminante $D_f = D_h$. Wie können wir entscheiden, ob die Formen tatsächlich äquivalent sind und wie finden wir gegebenenfalls eine Matrix $M \in \mathrm{SL}_2(\mathbb{Z})$, so dass $h = M \circ f$ ist?

5.1 Satz. *Jede* BQF $f = (a, b, c)$ *ist 1-äquivalent zu einer Form* $h = (a', b', c')$ *mit der Nebenbedingung*

$$|b'| \leq |a'| \leq |c'|$$

Beweis. □

Beispiel. Für $f = (28{,}75{,}31)$.

$$(28{,}75{,}31) \xrightarrow[\leq a=28, n=-1 \text{ tut das}]{2na+b=n56+57} (28{,}19{,}-16) \xrightarrow{T} (-16{,}-19{,}28)$$

$$(-16{,}-19{,}28) \xrightarrow[\leq |a|=16, n=-1 \text{ ist gut}]{2na+b=-32n-19} (-16{,}13{,}31) \quad \text{Test: } |a| > |c| \Rightarrow \text{nein! Stop.}$$

8. Vorlesung
06.06.2006

5.2 Folgerung. *Zu gegebener Diskriminante* D *gibt es nur endlich viele nichtäquivalente Formen* f *mit* $D_f = D$.

Beweis. □

5.3 Folgerung. *Alle positiv definiten Formen mit Diskriminante* $D = -3$ *bzw.* $D = -4$ *sind äquivalent zu* $f = (1{,}1{,}1)$ *bzw.* $f = (1{,}0{,}1)$.

Beweis. □

5.4 Satz. *Betrachte* $f(x, y) = x^2 + xy + y^2 = m$ *mit ungeradem* $m \geq 1$. *Dann existiert eine eigentliche Lösung gdw.* $\nu_3(m) \leq 1$ *und für Primzahlen* $p \neq 2{,}3$ *und* $p \mid m$ *gilt* $p \equiv 1 \bmod 3$.

Beweis. □

Beispiel. Sei $f(x,y) = x^2 = xy + y^2 = 273 = 3 \cdot 7 \cdot 13$. Das Kriterium ist erfüllt, also muss eine eigentliche Lösung existieren. Suche Lösung x für $-3 \equiv x^2 \bmod 4m$. Löse:

$$\begin{aligned} -3 &\equiv x_1^2 \mod 4 && \Rightarrow \quad x_1 = 1 \\ -3 &\equiv x_2^2 \mod 3 && \Rightarrow \quad x_1 = 0 \\ -3 &\equiv x_2^2 \mod 7 && \Rightarrow \quad x_1 = 2 \\ -3 &\equiv x_2^2 \mod 13 && \Rightarrow \quad x_1 = 6 \end{aligned}$$

Danach finde x, so dass:

$$x \equiv \begin{cases} 1 \mod 4 \\ 0 \mod 3 \\ 2 \mod 7 \\ 6 \mod 13 \end{cases}$$

Dies ist erfüllt für $x = 513$. D.h. $-3 \equiv 513^2 \bmod 4 \cdot 273$, also $g = (273,513,\frac{x^2-D}{4m} = 241)$. g hat daher $D_g = -3$ und ist deshalb äquivalent zu $f = (1,1,1)$.
Explizites Herstellen der Äquivalenz:

$$(273,513,241) \xrightarrow{\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)} (273,-33,1) \xrightarrow{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)} (1,33,273) \xrightarrow{\left(\begin{smallmatrix} 1 & 0 \\ -16 & 1 \end{smallmatrix}\right)} (1,1,1)$$

Für $M = \left(\begin{smallmatrix} 1 & 0 \\ -16 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$ ist also

$$M \circ (273,513,241) = (1,1,1) \qquad (273,512,241) = M^{-1} \circ (1,1,1)$$

und die erste Zeile von M^{-1} ist unsere Lösung:

$$M^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 16 & 1 \end{pmatrix} = \begin{pmatrix} 16 & 1 \\ 15 & 1 \end{pmatrix}$$

Also ist eine Lösung: $(16,1)$. Test: $16^2 + 16 + 1 = 273$.

$$(273,512,241)(x,y) = \left(M^{-1} \circ (1,1,1)\right)(x,y) = (1,1,1)\left((x,y)M^{-1}\right) = 273$$

hat offensichtlich die Lösung $(x,y) = (1,0)$. Also ist $(x',y') = (1,0)M^{-1}$, die erste Zeile von M^{-1}, eine Lösung von $(1,1,1)(x',y') = 273$.

Zerlege $ax^2 + bxy + cy^2$ in Linearfaktoren. Betrachte $ax^2 + bx + c = 0$ für $y = 1$. Dies hat die Lösungen:

$$w(f) := w = \frac{-b + \sqrt{D}}{2a} \qquad w' = \frac{-b - \sqrt{D}}{2a}$$

Wenn D kein Quadrat ist, dann sind w und w' zueinander konjugierte quadratische Irrationalitäten. (D ein Quadrat ist ein Sonderfall, wo man auf lineare Gleichungen reduzieren kann.) Ist $D = b^2 - 4ac$ keine Quadrat, ist $ac \neq 0$, also a und c beide $\neq 0$.

Normierung von w, w':

(i) Wenn $D > 0$, dann soll $\sqrt{D} > 0$ gemeint sein.

(ii) Wenn $D < 0$, dann soll $\sqrt{D} = \mathrm{i}\sqrt{|D|}$ positiven Imaginärteil haben.

Nach Konstruktion ist $ax^2 + bx + c = a(x - w)(x - w')$, also

$$ax^2 + bxy + cy = a(x - yw)(x - yw')$$

Weitere Behandlung mit Hilfe von quadratischen Zahlkörpern (kommt später).

Frage. Betrachte:

$$\begin{array}{ccc} f = (a,b,c) & \longmapsto & w(f) \in \text{ quadr. Irrationalität} \\ \Big\downarrow{\scriptstyle M} & & \Big\downarrow{\scriptstyle ?} \\ M \circ f & \longmapsto & w\,(M \circ f) \end{array}$$

Der Zusammenhang zwischen $w\,(M \circ f)$ und $w(f)$ wird in 5.5 aufgeklärt.

Definition ($*$-Operation[1]). *Sei* $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$, $z \in \mathbb{C}$*:*

$$\begin{aligned} \mathrm{GL}_2(\mathbb{R}) \times \mathbb{C} &\to \mathbb{C} \\ (A, z) &\mapsto A * z := \frac{az + b}{cz + d} \end{aligned}$$

Um die Operation $*$ überall zu definieren, betrachte $\overline{\mathbb{C}} := \mathbb{C} \cup \infty$. Setze:

$$\begin{aligned} A * z &:= \infty \quad \textit{falls } cz + d = 0 \\ A * \infty &:= \frac{a}{c} \quad \left(= \frac{a\infty + b}{c\infty + d} = \frac{a + b/\infty}{c + d/\infty}\right) \end{aligned}$$

Folgerung (Eigenschaften)**.** *Es gelten die Eigenschaften:*

$$A' * (A * z) = (A'A) * z$$

insbesondere $(A^{-1}) * (A * z) = z$*.*

5.5 Satz. *Sei* $f = (a,b,c) \in \mathrm{BQF}$*,* D_f *kein Quadrat (d.h.* $a, c \neq 0$*) und* $U = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$*. Dann gilt:*

$$w(U \circ f) = U^* * w(f)$$

[1] heißt auch MÖBIUS-Transformation für $A \in \mathrm{GL}_2(\mathbb{C})$

wobei $U^* := (U^{-1})^{\mathrm{t}} = (U^{\mathrm{t}})^{-1}$ *das transponierte Inverse von* U *ist. (Da* $\det U = 1$*, ist* $U^* = \left(\begin{smallmatrix} \delta & -\gamma \\ -\beta & \alpha \end{smallmatrix}\right)$*, die Kofaktormatrix.)*
Das folgende Diagramm kommutiert also:

$$\begin{array}{ccc} f = (a,b,c) & \longmapsto & w(f) = \frac{-b+\sqrt{D}}{2a} \\ {\scriptstyle U\in \mathrm{SL}_2(\mathbb{Z})}\downarrow & \circlearrowleft & \downarrow{\scriptstyle U^**} \\ U \circ f & \longmapsto & w\,(U \circ f) \end{array}$$

Der Beweis erfolgt durch Zurückführung der Behauptung auf zwei Spezialfälle:

Lemma (Spezialfall 1)**.** *Sei für alle* f*:*

$$w(U_1 f) = U_1^* * w(f) \qquad\qquad w(U_2 f) = U_2^* * w(f)$$

Dann gilt auch:

$$w(U_1 U_2 f) = (U_1 U_2)^* * w(f) \qquad\qquad w(U_1^{-1} f) = (U_1^{-1})^* * w(f)$$

Beweis. □

Lemma (Spezialfall 2)**.** *Jedes Element* $A \in \mathrm{SL}_2(\mathbb{Z})$ *lässt sich schreiben als Produkt von positiven und negativen Potenzen der Matrizen* $\mathscr{A} := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *und* $\mathscr{B} := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$*.*
Kurz: Die Gruppe $\mathrm{SL}_2(\mathbb{Z})$ *ist durch die angegebenen Matrizen erzeugt:*

$$\mathrm{SL}_2(\mathbb{Z}) = (\mathscr{A}, \mathscr{B})$$

Vorsicht: $\mathrm{SL}_2(\mathbb{Z})$ ist nicht kommutativ, d.h. $ABA \neq A^2B$, aber es gilt für alle $n \in \mathbb{Z}$:

$$\mathscr{A}^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \qquad\qquad \mathscr{B}^4 = I_2$$

Beweis. □

9. Vorlesung
13.06.2006

Beweis von Satz 5.5. Es genügt den Satz für $U = \mathscr{A}$ und $U = \mathscr{B}$ zu beweisen. □

5.6 Satz. *Sei* $f = (a,b,c) \in \mathrm{BQF}$*,* $U \in \mathrm{SL}_2(\mathbb{Z})$ *und* $\hat{f} = (\hat{a},\hat{b},\hat{c}) = U \circ f$*. d ist gdw Teiler von* (a,b,c)*, wenn er auch gemeinsamer Teiler von* $(\hat{a},\hat{b},\hat{c})$ *ist.*

Beweis. □

Folgerung (Ergebnis)**.** *Es gilt auch* $\mathrm{ggT}(a,b,c) = \mathrm{ggT}(\hat{a},\hat{b},\hat{c})$*.*

Also bleiben bei $f \mapsto U \circ f$ die Diskriminante D und der ggT $= d$ invariant. Im weiteren beschränken wir uns auf den Fall $d = 1$.

Definition (primitive Form, BQF_0)**.** *Dann nennt man die Form (a,b,c) primitiv und bezeichnet die primitiven Formen mit $\mathrm{BQF}_0 \subset \mathrm{BQF}$. Zwei Teilfälle:*

(i) BQF_0^+*: positiv definite Formen ($D<0, a>0$). Das sind Formen, welche nur Werte $m \geq 0$ annehmen.*

(ii) BQF_0^-*: indefinite Formen ($D>0$, kein Quadrat). Nehmen sowohl positive, wie negative Werte an.*

5.1 Klassifizierung der Formen durch die Punkte eines Modulraumes

Sei $\mathbb{H}$ die obere Halbebene von $\mathbb{C}$, mit $\mathrm{Im}>0$, und $\mathbb{H}_q$ die quadratischen Irrationalitäten in $\mathbb{H}$.

$$\mathbb{C} \supset \mathbb{H} \supset \mathbb{H}_q$$

Definition ($\mathbb{H}_q$)**.** *$w \in \mathbb{H}_q$ gdw. w ist Nullstelle einer quadratischen Gleichung mit Koeffizienten in $\mathbb{Q}$:*

$$(X-w)(X-\overline{w}) \in \mathbb{Q}[X]$$

Lemma. *$w \in \mathbb{H}_q$ gdw.* $\mathrm{Re}(w) \in \mathbb{Q}$ *und* $|w|^2 \in \mathbb{Q}$.

Satz (Bijektion für BQF_0^+)**.** *Dann bekommen wir eine Bijektion*

$$\begin{aligned} \mathrm{BQF}_0^+ &\longleftrightarrow \mathbb{H}_q \\ f &\longmapsto w(f) = \frac{-b+\sqrt{D}}{2a} \\ f \sim (1, -w-\overline{w}, w\overline{w}) &\longmapsto w \end{aligned}$$

mit $a = \mathrm{kgV}(\mathrm{Nenner}(w+\overline{w}), \mathrm{Nenner}(w\overline{w}))$ *und* $f = (a, -a(w+\overline{w}), aw\overline{w})$.

Beweis. □

Beispiel. Für $w = -\frac{15}{4} + \frac{\sqrt{3}}{4}\mathrm{i} \in \mathbb{H}_q$: Es ist

$$w+\overline{w} = -\frac{15}{2} \qquad\qquad w\overline{w} = \left(\frac{15}{2}\right)^2 + \frac{3}{16} = \frac{228}{16} = \frac{57}{4}$$

Mit der obigen Bijektion

$$w \mapsto (1, -w-\overline{w}, w\overline{w}) = (1, \frac{15}{2}, \frac{57}{4}) \sim (4{,}30{,}57)$$

erhält man $f = 4x^2 + 30xy + 57y^2$ als zugehörige Form mit $D_f = b^2 - 4ac = 900 - 16 \cdot 57 = -12$.

Betrachte die indefinite Formen mit $D > 0$, $\sqrt{D} \in \mathbb{R}$.

Definition ($\mathbb{R}_q^2$)**.** *Betrachte*

$$\mathbb{R}_q^2 := \left\{ (x,y) \in \mathbb{R}^2 : \begin{array}{c} \text{die Koordinaten } x,y \text{ sind Nullstellen} \\ \text{von quadratischen Polynomen über } \mathbb{Q} \end{array} \right\}$$

d.h. $(x,y) = (w,w')$*, wobei* $w + w' \in \mathbb{Q}$, $ww' \in \mathbb{Q}$ *(äquivalent:* $w - w' \in \sqrt{\mathbb{Q}} \setminus \mathbb{Q}$*).* w, w' *sollen irrational sein. (*w' *ist die zweite Nullstelle.)*

5.7 Satz (Bijektion für BQF_0^-)**.** *Man erhält die Bijektion*

$$\begin{aligned} \mathrm{BQF}_0^- &\longleftrightarrow \mathbb{R}_q^2 \\ f &\longmapsto (w(f), w'(f)) = \left(\frac{-b+\sqrt{D}}{2a}, \frac{-b-\sqrt{D}}{2a} \right) \\ f \sim (1, -w-w', ww') &\longmapsfrom (w,w') \end{aligned}$$

Bei $(w,w') \mapsto f$ *ist auf die Reihenfolge zu achten! Es ist*

$$f = (a, -a(w+w'), aww')$$

mit $|a| = \mathrm{kgV}(\mathrm{Nenner}(w+w'), \mathrm{Nenner}(ww'))$ *und* $\mathrm{sgn}(a) = \mathrm{sgn}(w-w')$.

Beweis. □

Lemma. *Die Bijektionen*

$$\begin{aligned} \mathrm{BQF}_0^+ &\longleftrightarrow \mathbb{H}_q \\ \mathrm{BQF}_0^- &\longleftrightarrow \mathbb{R}_q^2 \end{aligned}$$

sind verträglich mit den jeweiligen Aktionen der Gruppe $\mathrm{SL}_2(\mathbb{Z})$*. D.h.*

$$\begin{aligned} w(U \circ f) &= U^* * w(f) \\ (w,w')(U \circ f) &= (U^* * w(f), U^* * w'(f)) \end{aligned}$$

Definition (Klassenzahl $h(D)$)**.** *Sei* D *eine vorgegebene Diskriminante,* D *kein Quadrat. Dann ist die* ***Klassenzahl*** *von* D

$$h(D) := \begin{cases} \#\left[\mathrm{SL}_2(\mathbb{Z}) \setminus \mathrm{BQF}_0^+(D)\right] & \text{falls } D < 0 \\ \#\left[\mathrm{SL}_2(\mathbb{Z}) \setminus \mathrm{BQF}_0^-(D)\right] & \text{falls } D > 0 \end{cases}$$

wobei $BQF_0^{\pm}(D) = \left\{ f \in \mathrm{BQF}_0^{\pm} : D_f = D \right\}$.

Mit $\left[\mathrm{SL}_2(\mathbb{Z}) \setminus \mathrm{BQF}_0^{\pm}(D)\right]$ sind Äquivalenzklassen gemeint. # zählt die Äquivalenzklassen ($f, g \in \mathrm{BQF}$):

$$f \sim g \quad \Leftrightarrow \quad \exists U \in \mathrm{SL}_2(\mathbb{Z}) : g = U \circ f$$

Folgerung. *$h(D)$ ist immer endlich.*

Beweis. In jeder Äquivalenzklasse gibt es Formen mit der Nebenbedingung

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

Bei fixiertem D gibt es nur endlich viele Möglichkeiten. □

Beispiel. $h(-4) = h(-3) = 1$.

Eine wichtige Zusatzbemerkung:

Satz. *Wenn $h(D_f) = 1$ ist, dann ist das Legendre-Kriterium 4.10 für die Lösbarkeit von $f(x,y) = m$ nicht nur notwendig, sonder auch hinreichend.*

Jetzt geht es weiter mit dem positiv definiten Fall ($D < 0, a > 0, c > 0$).

Definition (reduzierte Form)**.** *Nenne $f = (a,b,c)$* ***reduziert****, falls $|b| \leq |a| \leq |c|$. ($|a| = a$, $|c| = c$.)*

Was bedeutet das für $w = \frac{-b+\sqrt{D}}{2a}$?

Folgerung. *Ist f reduziert, dann liegt $w = w(f) \in \mathbb{H}_q$ in dem* ***Fundamentalbereich*** *$\mathscr{F}$,*

$$\mathscr{F} := \left\{ w \in \mathbb{H}_q : \mathrm{Re}(w) \in \left[-\frac{1}{2}, \frac{1}{2} \right], |w| \geq 1 \right\}$$

Beweis. □

Wir hatten das Problem: *In der Äquivalenzklasse von Formen f befindet sich eine Form $U \circ f$, welche reduziert ist.* Äquivalent dazu ist:

Satz. *Sei $w \in \mathbb{H}$. Dann existiert immer eine Matrix $U \in \mathrm{SL}_2(\mathbb{Z})$ mit $U * w \in \mathscr{F}$.*

Beweis. □

10. Vorlesung
20.06.2006

Seien f und g zwei BQF. Entscheide, ob $f \sim g$, d.h. ob $U \in \mathrm{SL}_2(\mathbb{Z})$ existiert, so dass

$$g = U \circ f \qquad\qquad g(x,y) = f((x,y) \circ U)$$

Äquivalente Formen haben den selben Wertebereich (in $\mathbb{Z}$):

$$f(x,y) = m = g(x,y)$$

Als notwendige Bedingung hat man: Wenn $f \sim g$, dann sind die Diskriminante und die Teiler invariant, d.h.

$$D_f = D_g \qquad\qquad d(f) = d(g)$$

mit

Definition ($d(f)$)**.** $d(f) := \mathrm{ggT}(a,b,c)$*, falls* $f = (a,b,c)$ *ist.*

O.B.d.A. sei $d(f) = 1$, betrachte nur positiv definite Formen ($D > 0$, $a > 0$):

$$f = (a,b,c) \in \mathrm{BQF}_0^+ \mapsto w_f = \frac{-b + \sqrt{D}}{2a} \in \mathbb{H}$$

f reduziert bedeutet: $|b| \le a \le c \Leftrightarrow$ Wurzel $w_f \in \mathscr{F}$ (d.h. $\mathrm{Re}(w_f) \in \left[-\frac{1}{2}, \frac{1}{2}\right]$ und $\left|w_f\right| \ge 1$).

$$\begin{array}{ccc} f & \overset{S\,T}{\longmapsto} & \text{reduzierte Form } \hat{f} \\ \downarrow & & \updownarrow \\ w_f & \longmapsto & w_{\hat{f}} \in \mathscr{F} \end{array}$$

Ist $U \in \mathrm{SL}_2(\mathbb{Z})$ mit der Kofaktormatirx $U^* = (U^{-1})^t$, so gilt:

$$z = U * w_f \quad \Rightarrow \quad g = U^* \circ f \text{ hat } w_g = z$$

Transport. Es gibt zwei Operationen:

(i) Translation um 1:

$$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) * z = z + 1$$

(ii) Spiegelung an der imaginären Achse und Längenänderung (entfällt, wenn $|z| = 1$):

$$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) * z = -\frac{1}{z} = -\frac{\overline{z}}{|z|^2}$$

Frage. Ist $f \sim g$? Nimm w_f, w_g und transportiere sie nach $\mathscr{F}$.

Ziel. $f \sim g$ gdw. die nach $\mathscr{F}$ transportierten Wurzeln gleich sind.

Der Bereich $\mathscr{F}$ ist dafür etwas zu groß. Wir müssen vom Rand von $\mathscr{F}$ die „Hälfte“ entfernen, d.h. betrachte nur $\mathscr{F}_0$ (siehe lezte Abbildung):

$$\mathscr{F}_0 := \mathscr{F} \setminus \left(\left\{ z \in \mathscr{F} : \mathrm{Re}(z) = \frac{1}{2} \right\} \cup \left\{ z \in \mathscr{F} : |z| = 1 \wedge \mathrm{Re}(z) \in \left[0, \frac{1}{2}\right] \right\} \right)$$

$f = (a,b,c)$ mit $w_f \in \mathscr{F}$ bedeutet:

$$|b| \le a \le c$$

$w_f \in \mathscr{F}_0$ bedeutet (beachte $\left|w_f\right|^2 = \frac{c}{a}$):

$$-a < b \le a < c \quad \text{oder} \quad 0 \le b \le a = c$$

Definition (kongurent)**.** *Zwei komplexex Zahlen z, z' sind* ***kongruent*** *modulo* $\mathrm{SL}_2(\mathbb{Z})$*, falls $U \in \mathrm{SL}_2(\mathbb{Z})$ existiert, so dass $z' = U * z$.*

5.8 Satz (Eindeutigkeitssatz)**.** *Seien $z \neq z' \in \mathscr{F}$ komplexe Zahlen, welche kongruent modulo* $\mathrm{SL}_2(\mathbb{Z})$ *sind. Dann gibt es nur zwei Möglichkeiten:*

(i) $\mathrm{Re}(z) = \pm\frac{1}{2}$, $z = z' \pm 1$.

(ii) $|z| = 1$, $z' = -\frac{1}{z} = -\overline{z}$.

Beweis. □

5.9 Endergebnis im positiv definiten Fall. Seien $f, g \in \mathrm{BQF}_0^+$ mit $D_f = D_g = D$. Finde Transformationen von f und g, bzw. von w_f und w_g, so dass

$$U_1 \circ f, U_2 \circ g \in \begin{cases} -a < b \leq a < c \\ 0 \leq b \leq a = c \end{cases} \tag{5.1}$$

bzw.

$$w_{U_1 f} = U_1^* * w_f, w_{U_2 g} = U_2^* * w_g \in \mathscr{F}_0$$

Dann gilt $f \sim g$ gdw.

$$U_1 \circ f = U_2 \circ g \quad \text{bzw.} \quad U_1^* * w_f = U_2^* * w_g$$

Damit gilt auch:

$$f = U_1^{-1} U_2 g \qquad\qquad g = U_2^{-1} U_1 f$$

5.2 Geometrische Veranschaulichung

Sei $f \in \mathrm{BQF}_0^+$. O.B.d.A. sei f reduziert, d.h. (a, b, c) genügen (5.1) bzw. $w_f \in \mathscr{F}_0$. Man hat in diesem Fall als Nullstellen von $ax^2 + bx + c$:

$$w = w_f = \frac{-b + \sqrt{D}}{2a} \qquad\qquad w' = \overline{w} = \frac{-b - \sqrt{D}}{2a}$$

mit $D = b^2 - 4ac$. Untersuche

$$ax^2 + bxy + cy^2 = m \tag{5.2}$$

Mit $\hat{w} = -w' = \frac{b+\sqrt{D}}{2a}$ und $\hat{w}' = -w = \frac{b-\sqrt{D}}{2a} \in \mathbb{H}$ ist dies

$$\begin{aligned} ax^2 + bxy + cy^2 &= a(x - wy)(x - w'y) = a(x - \hat{w}y)(x + \hat{w}'y) \\ &= a\,|x + \hat{w}y|^2 \end{aligned}$$

Damit schreibt sich (5.2) als:

$$|x + \hat{w}y| = \sqrt{\frac{m}{a}}$$

D.h. die Lösungen $(x, y) \in \mathbb{Z}^2$ unserer Gleichung (5.1) entsprechen den Gitterpunkten $x + \hat{w}y$ auf dem Kreis mit dem Radius $r = \sqrt{\frac{m}{a}}$. Wir müssen das Gitter ansehen, welches von 1 und $\hat{w}$ erzeugt wird.

Nach Voraussetzung ist $w \in \mathscr{F}$ und $\hat{w} = -\overline{w} \in \mathscr{F}$ die Spiegelung an der imaginären Achse.

Wenn wir die Gleichung lösen wollen, dann kommen nur Kreise um den Nullpunkt in Frage, auf denen sich Gitterpunkte aus $\mathbb{Z} + \hat{w}\mathbb{Z}$ befinden. Welches sind die kleinsmöglichen Kreise?

Wir betrachten nacheinander die Kreise um den Nullpunkt auf dem die Gitterpunkte

$$1 = 1 + 0 \cdot \hat{w} \qquad \hat{w} = 0 + 1 \cdot \hat{w} \qquad 1 + \hat{w} \qquad 1 - \hat{w}$$

liegen. Die Radien dieser Kreise sind:

$$r = 1 \quad r = |\hat{w}| = \sqrt{\frac{c}{a}} \quad r = |1 + \hat{w}| = \sqrt{\frac{a + b + c}{a}} \quad r = |1 - \hat{w}| = \sqrt{\frac{a - b + c}{a}}$$

(i) Kleinster Kreis hat Radius 1. Darauf befindet sich der Gitterpunkt $1 + \hat{w} \cdot 0 = 1$.

(ii) Nächste Möglichkeit: Kreis hat Radius $|\hat{w}| = |w| = \sqrt{\frac{c}{a}}$. (Also Werte a, c, $a + c - |b|$.)

(iii) 3. Möglichkeit: Der Kreis durch $1 + \hat{w}$ oder $1 - \hat{w}$.

Resultat. Die kleinstmöglichen Werte $f(x, y) = ax^2 + bxy + cy^2 = m \neq 0$, die wir mit einer *reduzierten* Form realisieren können sind

$$m = a \qquad m = c \qquad m = a + c - |b|$$

Für eine beliebige Form g: Wandle g in eine reduzierte Form f um. g und f nehmen dieselben Werte an. Die kleinstmöglichen Werte ergeben sich aus den Koeffizienten von f.

5.3 Kettenbrüche

Um die Frage nach $f \sim g$ für indefinite Formen zu behandeln, braucht man Kettenbrüche (KBE), oder als Variante die Minus-Kettenbruchentwicklung ($^-$KBE) einer reelen Zahl.

Für die KBE sind für alle i die $a_i \geq 1$:

$$[a_0, a_1, a_2, \dots] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}$$

Die ¯KBE mit der Vereinbarung $a_i \geq 2 \forall i > 0$:

$$[\![a_0, a_1, a_2, \dots]\!] := a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \dots}}$$

d.h.: die ¯KBE ist immer unendlich. Eine ganze Zahl $n \in \mathbb{Z}$ hat die ¯KBE:

$$n = [\![n+1, 2, 2, \overline{2}, \dots]\!] = n + 1 - \cfrac{1}{2 - \cfrac{1}{2 - \dots}} = (n+1) - 1$$

($\overline{2}$ soll dabei die Periode andeuten, d.h. alle folgenden $a_i = 2$.)

Folgerung. *Die Zahlen α sind rational, d.h. $\in \mathbb{Q}$, gdw. die ¯KBE von α endet:*

$$\alpha = [\![\dots, 2, \overline{2}, \dots]\!]$$

Uns interessieren nur irrationale Zahlen, d.h. Entartungen dieser Art kommen nicht vor.

Beispiel. Für $\sqrt{2}$:

$$\begin{aligned}\sqrt{2} = \left[1, 2, \overline{2}, \dots\right] &= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \dots}} \\ = [\![2, 2, 4, \overline{2,4}, \dots]\!] &= 2 - \cfrac{1}{2 - \cfrac{1}{4 - \dots}}\end{aligned}$$

D.h. bei ¯KBE muss man aufrunden.

Lemma. *Die Berechnung der Kettenbruchentwicklung von ξ erfolgt nach folgendem Algorithmus:*

(i) KBE*: Sei $\xi_0 := \xi$, $\xi_{i+1} := \frac{1}{\xi_i - \lfloor \xi_i \rfloor}$ und $a_i := \lfloor \xi_i \rfloor$. Dann ist $\xi = [a_0, a_1, \dots]$.*

(ii) ¯KBE*: Sei $\xi_0 := \xi$, $\xi_{i+1} := \frac{1}{\lceil \xi_i \rceil - \xi_i}$ und $a_i := \lceil \xi_i \rceil$. Dann ist $\xi = [\![a_0, a_1, \dots]\!]$.*

Dabei ist $\lfloor \xi \rfloor = \max\{k \in \mathbb{N} : k \leq \xi\}$ und $\lceil \xi \rceil = \min\{k \in \mathbb{N} : k \geq \xi\}$, d.h. ξ ab- bzw. aufgerundet.

Literatur. Weiterführende Literatur zu diesem Kapitel findet man in [Gau81], [Zag81] und [HS90].

5.4 Aufgaben

5.1 Finden Sie die zu $f = (48,89,17)$ äquivalente Form $h = (a,b,c)$ mit $|b| \leq |a| \leq |c|$ und geben Sie die Transformationsmatrix M, $Mf = h$, an.

5.2 Finden Sie eine eigentliche Lösung der Gleichung $x^2 + y^2 = 274625$.

5.3 Finden Sie eine eigentliche Lösung der Gleichung $x^2 + xy + y^2 = 133$. *Hinweis:* Wenden Sie den Hauptsatz an.

5.4 Die Formen $(1,1,1)$ und $(1,-1,1)$ sind zueinander äquivalent.

5.5 Betrachte $f = (a,b,c) \mapsto D = b^2 - 4ac$. D ist ein Quadrat gdw. vier ganze Zahlen $a_1, \ldots, a_4$ existieren, so dass

$$ax^2 + bxy + cy^2 = (a_1x + a_2y)(a_3x + a_4y)$$

Die Lösung von $f(x,y) = m$ ist in diesem Fall äquivalent zur Lösung der Gleichungssysteme

$$a_1x + a_2y = d \qquad\qquad a_3x + a_4y = \frac{m}{d}$$

für alle Teiler $d \mid m$.

5.6 Wenn D eine Diskriminante ist, dann ist

$$D \equiv \begin{cases} 0 \\ 1 \end{cases} \mod 4$$

Umgekehrt ist so ein D stets Diskriminante einer Form. Hauptform:

$$f = \begin{cases} (1,0,-\frac{D}{4}) & \text{falls } D \equiv 0 \mod 4 \\ (1,1,\frac{1-D}{4}) & \text{falls } D \equiv 1 \mod 4 \end{cases}$$

5.7 Überprüfe die KBE und $^-$KBE von $\sqrt{2} = \left[1,\overline{2}\right] = [\![2,\overline{2,4}]\!]$.

6 Kettenbrüche und Anwendungen auf das Äquivalenzproblem in BQF^-

11. Vorlesung
27.06.2006

6.1 Kettenbrüche

Siehe auch Abschnitt 5.3 für Kettenbrüche.

6.1 Definition (Minuskettenbruch $^-$KBE)**.** *Für $\xi \in \mathbb{R}$:*

$$\xi = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \dots}}$$

Notation: $^-$KBE *und* $[\![\cdot \cdots]\!]$, $\xi = [\![a_0, a_1, a_2, \dots]\!]$.

Berechne mit reeler Zahl ξ:

(i) Bilde

$$\lceil \xi \rceil := \lfloor \xi \rfloor + 1 = \begin{cases} \xi \text{ aufgerundet} & \text{wenn } \xi \notin \mathbb{Z} \\ \xi + 1 & \text{wenn } \xi \in \mathbb{Z} \end{cases}$$

(ii) Bilde Ableitungen: $\xi_0 := \xi$, $a_0 := \lceil \xi \rceil$. Wenn ξ_i und $a_i := \lceil \xi_i \rceil$ schon gegeben sind, dann bilde

$$\xi_{i+1} := \frac{1}{a_i - \xi_i} \qquad\qquad a_{i+1} := \lceil \xi_{i+1} \rceil$$

(iii) Daraus ergibt sich induktiv: $\xi = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \dots}}$ mit $a_i = \lceil \xi_i \rceil$:

$$\begin{aligned} & \xi_{i+1} = \frac{1}{a_i - \xi_i} \\ \Leftrightarrow \quad & \xi_i = a_i - \frac{1}{\xi_{i+1}} = \begin{pmatrix} a_i & -1 \\ 1 & 0 \end{pmatrix} * \xi_{i+1} \end{aligned}$$

(iv) Durch Iteration folgt:

$$\begin{aligned}\xi &= \begin{pmatrix} a_0 & -1 \\ 1 & 0 \end{pmatrix} * \xi_1 \\ &= \begin{pmatrix} a_0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & -1 \\ 1 & 0 \end{pmatrix} * \xi_2 \\ &= \begin{pmatrix} a_0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_2 & -1 \\ 1 & 0 \end{pmatrix} * \xi_3 \\ &= \dots\end{aligned}$$

Bemerkung. Es gilt $\xi = [\![a_0, \dots, a_i, \xi_{i+1}]\!]$ für alle $i \geq -1$. Dies ergibt sich induktiv aus $\xi = \xi_0$ und $\xi_i = a_i - \frac{1}{\xi_{i+1}}$. Die ξ_i werden als **vollständige Quotienten** von ξ bezeichnet.

Folgerung. *Es ist:*

$$\xi = \begin{pmatrix} a_0 & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & -1 \\ 1 & 0 \end{pmatrix} * \xi_{n+1}$$

6.2 Lemma (Berechnung der Näherungsbrüche)**.** *Der Näherungsbruch*

$$[\![a_0, \dots, a_n]\!] = \frac{p_n}{q_n}$$

ist eine rationale Zahl. Setze:

$$\begin{pmatrix} p_0 & p_{-1} \\ q_0 & q_{-1} \end{pmatrix} := \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}$$

mit $\frac{p_{-1}}{q_{-1}} = \infty$ *und* $\frac{p_0}{q_0} = a_0$*. Dann gilt allgemein für alle* $n \geq 1$*:*

$$\begin{pmatrix} p_n \\ q_n \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}\begin{pmatrix} a_n \\ -1 \end{pmatrix}$$

und dies ist äquivalent zu

$$\frac{p_n}{q_n} = \begin{pmatrix} p_{n-1} & -p_{n-2} \\ q_{n-1} & -q_{n-2} \end{pmatrix} * a_n$$

Beweis. □

Bemerkung (Konjugation einer Gleichung). Sei $A = A_0 \cdot A_1 \cdot \cdots A_n$ und B invertierbar. Dann ist

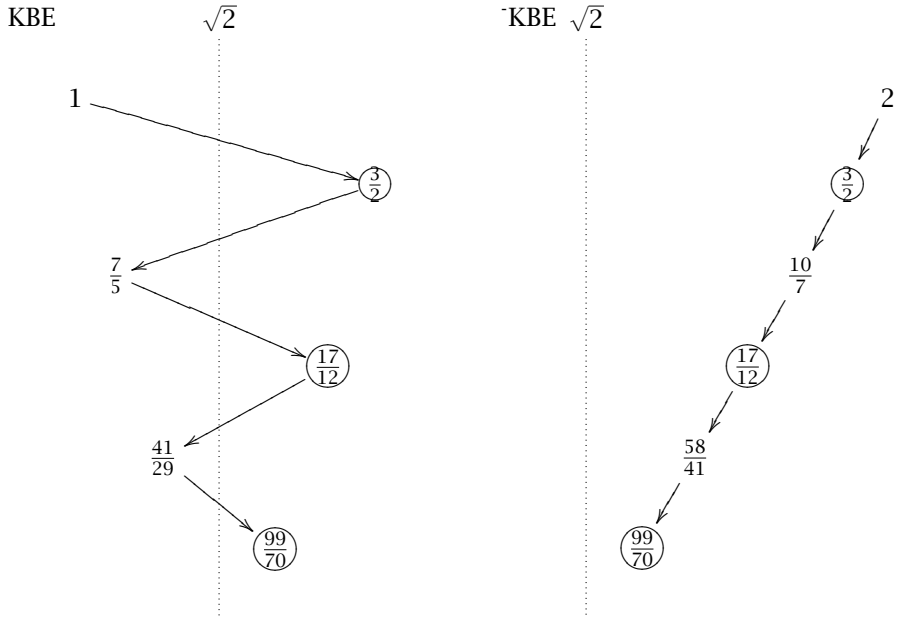
$$\begin{aligned} BAB^{-1} &= B(A_0 \cdots A_n)B^{-1} \\ &= (BA_0B^{-1}) \cdots (BA_nB^{-1})\end{aligned}$$

Folgerung. *Die Näherungsbrüche werden ständig kleiner:*

$$\frac{q_{n-1}}{q_{n-1}} > \frac{p_n}{q_n}$$

Beweis. □

Beispiel. $\sqrt{2} = \left[1, \overline{2}\right] = [\![2, \overline{2,4}]\!]$. Wir bilden Näherungsbrüche:



6.3 Lemma (Abschätzung für ¯KBE)**.** *Für die* ¯KBE *sind außer* $a_0 = \lceil \xi \rceil$ *alle weiteren* $a_i \geq 2$*. Die Nenner* q_i *sind echt wachsend, und außer* $q_{-1} = 0$ *sind alle Nenner positiv.*

Beweis. □

6.4 Bemerkung. Ist $a \in \mathbb{Z}$, dann ist die ¯KBE $a = [\![a+1, \overline{2}]\!]$. Für den Näherungsbruch gilt:

$$\frac{p_n}{q_n} = a + \frac{1}{n+1} \qquad \lim_{n\to\infty}\left(a + \frac{1}{n+1}\right) = a$$

Daraus folgt:

$$\xi \in \mathbb{Q} \quad \Leftrightarrow \quad \xi = [\![\ldots, \overline{2}]\!]$$

(d.h. die ¯KBE von ξ endet auf …,2,2,2….)

6.2 Reduzierte Formen

6.5 Lemma. *Sei $f_i = (\alpha_i, \beta_i, \gamma_i) \in \mathrm{BQF}$ mit $D = \beta_i^2 - 4\alpha_i\gamma_i$. Setze*

$$\xi_i = w_{f_i}^{\surd} = \frac{\beta_i + \sqrt{D}}{2\alpha_i} \qquad\qquad a_i = \lfloor \xi_i \rfloor$$

wobei $w_{f_i}^{\surd}, {w'}_{f_i}^{\surd}$ die Wurzeln von $\alpha_i X^2 - \beta_i X + \gamma_i$ sind. Sei $\xi_{i+1} = \frac{1}{a_i - \xi_i}$ die Ableitung von ξ_i. Dann ist $\xi_{i+1} = w_{f_{i+1}}^{\surd}$ für $f_{i+1} = (\alpha_{i+1}, \beta_{i+1}, \gamma_{i+1})$ mit

$$f_{i+1} = \begin{pmatrix} a_i & -1 \\ 1 & 0 \end{pmatrix} f_i$$

Dies bedeutet explizit:

$$(\alpha_{i+1}, \beta_{i+1}, \gamma_{i+1}) = (a_i^2\alpha_i - a_i\beta_i + \gamma_i, 2a_i\alpha_i - \beta_i, \alpha_i)$$

$$\begin{array}{ccc} f_i & \longleftrightarrow & \xi_i = w_{f_i}^{\surd} \\ \Big\downarrow {\scriptstyle \left(\begin{smallmatrix} a_i & -1 \\ 1 & 0 \end{smallmatrix}\right)} & & \Big\downarrow {\scriptstyle \frac{1}{a_i - \xi_i}} \\ f_{i+1} & \longleftrightarrow & \xi_{i+1} \end{array}$$

Beweis. □

6.6 Definition und Satz (reduziert)**.** *Sei $(\alpha, \beta, \gamma) = f \in \mathrm{BQF}^-$ und D_f kein Quadrat. Wir nennen dieses Tripel **reduziert**, falls folgende äquivalente Eigenschaften gelten:*

(i) $\alpha > 0$, $\gamma > 0$ *und* $\beta > \alpha + \gamma$

(ii) $w_f^{\surd}$ *genügt:*

$$0 < {w'}_f^{\surd} < 1 < w_f^{\surd}$$

(iii) w_f *genügt:*

$$0 > w_f > -1 > {w'}_f$$

Beweis. □

12. Vorlesung
04.07.2006

Gegeben: Zwei Formen f und g mit denselben D und $d(f) = d(g)$ o.B.d.A. $= 1$. Entscheide, ob $f \sim g$ und finde gegebenenfalls $U \in \mathrm{SL}_2(\mathbb{Z})$ mit $g = U \circ f$. Zu $f = (\alpha, \beta, \gamma)$ gehört $w_f = \frac{-\beta + \sqrt{D}}{2\alpha}$ (Nullstellen von $\alpha X^2 + \beta X + \gamma$) und die duale Wurzel $w_f^{\surd} = \frac{\beta + \sqrt{D}}{2\alpha}$ (Nullstellen von $\alpha X^2 - \beta X + \gamma$). Offensichtlich sind w_f

und $w_f^{\surd}$ quadratische Irrationalitäten (Nullstellen eines irreduziblen Polynoms mit Koeffizenten in $\mathbb{Z}$).

Sei ξ eine quadratische Irrationalität. Dann bezeichne ξ' immer die zweite Nullstelle, die zu ξ konjugierte Zahl (wenn ξ eine komplexe quadratische Irrationalität ist, dann ist $\xi' = \overline{\xi}$). Ist $D > 0$, so sind $w_f, w_f^{\surd} \in \mathbb{R}$.

Wir veranschaulichen eine quadratische Irrationalität ξ durch den Punkt $(\xi, \xi') \in \mathbb{R}^2$.

$$\mathrm{BQF}^- \ni f \mapsto \begin{cases} P_f = (w_f, w_f') \\ P_f^{\surd} = (w_f^{\surd}, w'^{\surd}_f) \end{cases} \in \mathbb{R}^2$$

$P_f \leftrightarrow P_f^{\surd}$ entspricht $(x, y) \mapsto (-y, -x)$, der Spiegelung an der Diagonalen $x = -y$.

Aus technischen Gründen bevorzugen wir $P_f^{\surd}$ als den zu f gehörenden Punkt. Was passiert, wenn wir zu einer äquivalenten Form übergehen?

Definition. *Sei* $U \in \mathrm{SL}_2(\mathbb{Z})$, $P = (x, y) \in \mathbb{R}^2$.

$$U * P := (U * x, U * y) \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} * x := \frac{ax + b}{cx + d}$$

Die Frage hat folgende Antwort:

$$\begin{array}{ccccc} f & \longmapsto & P_f & \longmapsto & P_f^{\surd} \\ \downarrow & & \downarrow & & \downarrow \\ U \circ f & \longmapsto & P_{U\circ f} = U^* * P_f & \longmapsto & P^{\surd}_{U\circ f} = U^{\surd} * P_f^{\surd} \end{array}$$

Dabei ist mit $i := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ und $s = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ (es gilt $i^2 = -I_2$, $s^2 = I_2$ und $s = s^{-1}$):

$$U^* = (U^{-1})^{\mathrm{t}} = i \cdot U \cdot i^{-1}$$
$$U^{\surd} = s \cdot U \cdot s^{-1}$$

und

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & c \\ b & a \end{pmatrix} = U^{\surd}$$

Es sei $\mathscr{R}$ der Bereich der reduzierten Formen, und es sei $\mathscr{F} \subset \mathbb{R}^2$ der Bereich aller (x, y) mit $0 < y < 1 < x$. Es gilt (wegen 6.6):

$$f \in \mathscr{R} \quad \Leftrightarrow \quad P_f^{\surd} \in \mathscr{F}$$

Definition. *Definiere folgende Äquivalenzrealtionen:*

(i) $f \sim g$ *falls* $U \in \mathrm{SL}_2(\mathbb{Z})$ *existiert mit* $g = U \circ f$, $[f]$ *seien die Äquivalenzklassen von* f.

(ii) $P \sim Q$ *falls* $U \in \mathrm{SL}_2(\mathbb{Z})$ *existiert mit* $Q = U * P$, $[P]$ *seien die Äquivalenzklassen von* P.

Folgerung. *Es folgt:*

$$[f] \cap \mathscr{R} \leftrightarrow [P_f^{\surd}] \cap \mathscr{F}$$

$$\text{reduzierte Formen äquivalent zu } f \;\hat{=}\; \text{Punkte aus } \mathscr{F}, \text{ welche zu } P_f^{\surd} \text{ äquivalent sind}$$

Beweis. □

Siehe dazu auch den Anhang A *Tabellen: Reduzierte Formen.*

6.7 Satz (Hauptergebnisse)**.**

(i) quadratische Irrationalitäten $(\xi, \xi') \in \mathscr{F} \Leftrightarrow$ *-*KBE *von* ξ *ist rein periodisch*

$$\xi = [\![\overline{a_0, a_1, \ldots, a_{e-1}}]\!]$$

mit der Periode e $(\Rightarrow a_0 = \lceil \xi \rceil \geq 2 \Rightarrow \xi > 1)$.

Bemerkung: Ein entsprechender Satz für die KBE*:*

$$(\xi, \xi') \in \mathscr{F}' \quad \Leftrightarrow \quad \text{KBE } \textit{von } \xi \textit{ reinperiodisch}$$

Folgerung: $f \in \mathscr{R} \Leftrightarrow P_f^{\surd} \in \mathscr{F} \Leftrightarrow w_f^{\surd} = \xi$ *hat rein periodische -*KBE*.*

(ii) Betrachte irgendein f *und die zugehöre quadratische Irrationalität* $\xi = w_f^{\surd}$*. Die -*KBE *von* ξ *wird periodisch, d.h. wir haben:*

$$\xi = [\![\underbrace{a_0, \ldots, a_{n-1}}_{\textit{Vorperiode}}, \underbrace{\overline{a_n, \ldots, a_{n+e-1}}}_{\textit{Periode}}]\!]$$

Dann gilt für die Äquivalenzklasse des Punktes $P = (\xi, \xi') = P_f^{\surd}$*:*

$$\begin{aligned} [P] \cap \mathscr{F} &= \{(\xi_n, \xi_n'), \ldots, (\xi_{n+e-1}, \xi_{n+e-1}')\} \quad e \textit{ Punkte} \\ \xi_n &= [\![a_n, \ldots, a_{n+e-1}, a_n, \ldots]\!] \\ \xi_{n+1} &= [\![a_{n+1}, \ldots]\!] \\ &\vdots \\ \xi_{n+e} &= \xi_n \end{aligned}$$

wobei e *die Periodenlänge ist.*

Entsprechend haben wir

$$[f] \cap \mathscr{R} = \{f_n, \ldots, f_{n+e-1}\}$$

wobei $P_{f_i}^{\surd} = (\xi_i, \xi_i')$ *ist.*

Beachte: In jeder Äquivalenzklasse gibt es reduzierte Formen, und zwar nur endlich viele.

(iii) Es seien f, g *zwei Formen mit* $w_f^{\surd} = \xi, w_g^{\surd} = \eta$ *quadratische Irrationalitäten. Dann ist folgendes äquivalent:*

a) $f \sim g$
b) $[f] \sim [g]$
c) $[f] \cap \mathscr{R} = [g] \cap \mathscr{R}$
d) $[P_f^{\surd}] \cap \mathscr{F} = [P_g^{\surd}] \cap \mathscr{F}$
e) Es gibt vollständige Quotienten ξ_n *von* ξ *und* η_m *von* η*, so dass* $\xi_n = \eta_m$ *ist.*

Beweis. □

13. Vorlesung
11.07.2006

Sei $f = (a,b,c) \in \mathrm{BQF}^-$, $D = b^2 - 4ac > 0$ mit $\mathrm{ggT}(a,b,c) = 1$. Die Äquivalenzklasse von f ist $[f] = \{U \circ f : U \in \mathrm{SL}_2(\mathbb{Z})\}$. In jeder Äquivalenzklasse befindet sich mindestens eine reduzierte Form, d.h. $a, c > 0$ und $b > a + c$.

$$f \mapsto P_f^{\surd} = (w_f^{\surd}, w_f^{\surd\prime}) = \left(\frac{b+\sqrt{D}}{2a}, \frac{b-\sqrt{D}}{2a}\right)$$

$$\mathscr{R} \ni f \Leftrightarrow P_f^{\surd} \in \mathscr{F}$$

Für beliebige f gibt $\#[f] \cap \mathscr{R}$ die Länge der Periode in der $^-$KBE von $\xi = w_f^{\surd}$ an.

Beispiel. Die Grundform f zu D ist

$$f = \begin{cases} (1,0,-\frac{D}{4}) & D \equiv 0 \bmod 4 \\ (1,1,-\frac{D-1}{4}) & D \equiv 1 \bmod 4 \end{cases}$$

$\#[f] \cap \mathscr{R}$ ist die Länge der $^-$KBE-Periode von $w_f^{\surd} = \frac{\sqrt{D}}{2}$ bzw. $= \frac{1+\sqrt{D}}{2}$.

6.3 Die Klassenzahl $h(D)$

Wir wollen die Klassenzahl $h(D)$ bestimmen.

$$h(D) = \begin{matrix}\text{Zahl der verschiedenen Äquivalenzklassen } [f] \\ \text{zu gegebener Diskriminate } D\end{matrix}$$

Um $h(D)$ zu berechnen, genügt es sich auf reduzierte Formen zu beschränken. Aufstellung der reduzierten Formen $f = (a,b,c)$ zu gegebenem D, d.h. $a > 0$, $c > 0$ und $b > a + c$. Setze $k = b - 2a$, dann ist

$$D - k^2 = b^2 - 4ac - (b-2a)^2 = 4a(b-c-a) > 0$$

Also $D - k^2 > 0$ und immer durch 4 teilbar.

Algorithmus (Finde Reduzierte Formen zu D).

(i) Finde alle k mit

$$k^2 < D \qquad \text{und} \qquad 4 \mid D - k^2$$

(ii) Sei ein k gefunden. Dann betrachte alle $a \geq 1$, so dass

$$a \mid \frac{D-k^2}{4}$$

(iii) Zusatzbedingung: Wir brauchen

$$k + 2a > \sqrt{D}$$

(Da $k + 2a = (b-2a) + 2a = b > \sqrt{D} \Leftrightarrow b^2 > D = b^2 - 4ac$.)

Aus den zulässigen Paaren (k,a) ergeben sich alle reduzierten Formen:

$$(k,a) \mapsto (a, k+2a, \underbrace{k + a - \frac{D-k^2}{4a}}_{c})$$

Der Wert von c wird erzwungen, weil die Form die Diskriminante D haben soll. Wenn sich dabei nicht primitive Formen ergeben, dann weglassen.

Algorithmus (Bestimmung der Klassenzahl von D). Aus der Liste der reduzierten Formen f mit Diskriminante D wird die Klassenzahl bestimmt, indem man feststellt, wie viele dieser Formen jeweils äquivalent sind:

$$f = (a,b,c) \text{ reduziert } \mapsto w_f^{\surd} = \frac{b + \sqrt{D}}{2a} \in \mathscr{F}$$

$w_f^{\surd} = [\![\overline{a_0, \ldots, a_{e-1}}]\!]$ ist rein periodisch. e gibt die Anzahl $\#[f] \cap \mathscr{R}$ an. Dann sind

$$\begin{pmatrix} a_0 & -1 \\ 1 & 0 \end{pmatrix} \circ f, \begin{pmatrix} a_1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & -1 \\ 1 & 0 \end{pmatrix} \circ f, \ldots,$$

die zu f äquivalenten Formen.

Wenn damit die aufgestellte List noch nicht erschöpft ist, dann wähle ein f aus dem Komplement und wiederhole das Verfahren.

Im Anhang A *Tabellen: Reduzierte Formen* findet man die Klassenzahl für alle $D < 30$ in Tabelle A.2.

Beobachtung. (i) Im positiv definiten Fall $f = (a, b, c)$, $a > 0$ und $D < 0$ haben wir $\mathscr{F}$ als Fundamentalbereich. In $\mathscr{F}$ hat jede Äquivalenzklasse genau einen Vertreter:

$$\#[f] \cap \mathscr{F} = 1$$

(ii) Indefiniter Fall: Jede Äquivalenzklasse $[f]$ hat Vertreter f_i, so dass $P_{f_i}^{\surd} = (w_{f_i}^{\surd}, w_{f_i}^{\surd}) \in \mathscr{F}$. Die Zahl der Vertreter kann groß werden, sie entspricht der Periodenlänge in der ¯KBE von $w_f^{\surd}$.

Eindruck. (i) Im definiten Fall sind die einzelnen Äquivalenzklassen kleiner, und $h(D) \to \infty$ ist größer.

(ii) Im indefiniten Fall, $D > 0$. Vermutung: $h(D) = 1$ für unendlich viele D. Test mit dem Computer für $D = p \equiv 1 \bmod 4$. Dann ist in 80% der gegebenen Fälle $h(D) = 1$.

6.4 Weitere Sätze

Weitere tiefergehende Sätze über die Klassenzahl positiv definiter Formen sind:

6.8 Satz (Heilbronn und Siegel)**.** *Mit $D \to -\infty$ geht $h(D) \to +\infty$, d.h. die Klassenzahl wird beliebig groß.*

6.9 Satz (Heegner, Stark und Baker)**.** *Es gibt genau 13 negative Werte D mit $h(D) = 1$, nämlich:*

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

6.5 Aufgaben

6.1 Berechne die ¯KBE von $\sqrt{3}$.

6.2 Bereche Grundform und die reduzierten Formen von $f = (20, -12, -9)$.

6.3 Vervollständigen Sie die Tabelle A.1 für die Fälle $D = 28, 29$.

6.4 Entscheiden Sie, ob die Formen $f = (1,0,-5)$, $g = (1,10,20)$ äquivalent sind, und finden Sie gegebenenfalls $U \in \mathrm{SL}_2(\mathbb{Z})$, welche zwischen f und g vermittelt.

6.5 Zwischen KBE und ¯KBE besteht folgender Zusammenhang:

$$\begin{aligned}\xi &= [a_0, a_1, a_2, \dots] \\ &= [\![a_0 + 1, 2^{a_1-1}, a_2 + 2, 2^{a_3-1}, a_4 + 2, \dots]\!]\end{aligned}$$

7 Die Automorphismengruppe einer BQF

Sei $f = (a,b,c)$. Die Automorphismengruppe

$$\mathrm{Aut}(f) = \{U \in \mathrm{SL}_2(\mathbb{Z}) : U \circ f = f\}$$

ist eine Untergruppe (Hauptsatz 4.13).
Die Diskriminante $D = b^2 - 4ac$ sei keine Quadratzahl. Dann ist

$$K = \mathbb{Q}(\sqrt{D}) = \left\{a + b\sqrt{D} : a,b \in \mathbb{Q}\right\}$$

ein Körper mit $\dim_{\mathbb{Q}}(K) = 2$, also ein **quadratischer** Körper. Alle Zahlen aus K sind entweder in $\mathbb{Q}$ oder es sind quadratische Irrationalitäten. Dabei ist

K reell quadratisch für $D > 0$
K imaginär quadratisch für $D < 0$

Definition (Gitter m_f)**.** *Zu $f = (a,b,c)$ gehört ein Gitter $m_f \subset K$, nämlich*[1]

$$m_f = \mathbb{Z} \cdot 1 + \mathbb{Z} w_f^{\surd}$$

($\mathbb{Q} \cdot 1 + \mathbb{Q} w_f^{\surd} = K$, weil $\dim_{\mathbb{Q}} K = 2$.)

7.1 Satz.

(i) Sei $f_0 = \left(1,0,-\frac{D}{4}\right)$ bzw. $\left(1,1,\frac{1-D}{4}\right)$ die Grundform zur Diskriminante D. Dann ist das Gitter m_{f_D} sogar ein Ring (abgeschlossen bezüglich Multiplikation). Wir bezeichnen diesen Ring mit $\mathcal{O}_D$.

(ii) Für alle f mit Diskriminante $D(f) = D$ gilt immer:

$$\mathcal{O}_D \cdot m_f \subseteq m_f$$

*d.h. m_f ist stets ein **Modul**[2] über dem Ring $\mathcal{O}_D$.*

(iii) Es gilt sogar

$$\mathcal{O}_D = \left\{x \in K : x \cdot m_f \subseteq m_f\right\}$$

*(der **Multiplikator** von m_f).*

[1] $w_f^{\surd}$ war vorher $\hat{w}(f) = -w'(f) = \frac{b+\sqrt{D}}{2a}$
[2] naiv: $\mathcal{O}_D$-Vektorraum, mit Skalaren aus $\mathcal{O}_D$.

Beweis. □

Explizite Bestimmung des Ringes $\mathcal{O}_D$.

$$\mathcal{O}_D = \begin{cases} \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\frac{\sqrt{D}}{2} & \text{falls } D \equiv 0 \pmod 4 \\ \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\frac{1+\sqrt{D}}{2} & \text{falls } D \equiv 1 \pmod 4 \end{cases}$$

Das heißt $\lambda \in \mathcal{O}_D$ genau dann, wenn $\lambda = \frac{x+y\sqrt{D}}{2}$, mit $x, y \in \mathbb{Z}$ und $x \equiv yD \pmod 2$.

7.2 Satz. *Die Abbildung*

$$\lambda \in \mathcal{O}_D \mapsto U_\lambda \in \mathbb{Z}^{2\times 2} \qquad\qquad \begin{pmatrix} 1 \\ w_f^{\surd} \end{pmatrix} \cdot \lambda = U_\lambda \cdot \begin{pmatrix} 1 \\ w_f^{\surd} \end{pmatrix}$$

ist ein Homomorphismus (d.h. verträglich mit $+$ und $\cdot$) vom Ring $\mathcal{O}_D$ in den Ring $\mathbb{Z}^{2\times 2}$.

Beweis. □

Definition (Norm)**.** *Sei $\lambda \in K$, dann definiere die Norm von λ in $\mathbb{Q}$*

$$N(\lambda) := \lambda\lambda'$$

als das Produkt von λ und seiner konjugierten Zahl.

$(X-\lambda)(X-\lambda')$ ist ein Polynom mit Koeffizienten in $\mathbb{Q}$. Für $\lambda, \tau \in K$ gilt:

$$N(\lambda\tau) = N(\lambda)\cdot N(\tau)$$

7.3 Satz. *Betrachte die obige Abbildung $\lambda \in \mathcal{O}_D \mapsto U_\lambda \in \mathbb{Z}^{2\times 2}$. Dann gilt:*

$$(U_\lambda \circ f)(x, y) = N(\lambda)\cdot f(x, y)$$

und

$$N(\lambda) = \det(U_\lambda)$$

Beweis. □

Folgerung. *Es gilt*

$$U_\lambda \in \mathrm{Aut}(f) \quad\Leftrightarrow\quad U_\lambda \circ f = f \quad\Leftrightarrow\quad N(\lambda) = 1$$

d.h. $\frac{x^2-y^2D}{4} = 1$, d.h. $\lambda = \frac{x+y\sqrt{D}}{2}$, wobei die ganzzahligen Koordinaten x, y der ***Pellschen Gleichung*** *$x^2 - y^2D = 4$ genügen.*
Das ist tatsächlich die gesamte Automorphismenguppe, d.h. jedes $U \in \mathrm{Aut}(f)$ hat die Form $U = U_\lambda$ für geeignetes $\lambda = \frac{x+y\sqrt{D}}{2}$.

A Tabellen: Reduzierte Formen

A.1 Reduzierte Formen mit positiver Diskriminante

A.1 Anwendung. Aufstellung *aller* reduzierten Formen $f = (a, b, c)$ für positive Diskriminante $D > 0$. Wir fordern: $a > 0, c > 0$ und $b > a + c$. Setze $k = b - 2a$. Dann ist

$$D - k^2 = b^2 - 4ac - (b - 2a)^2 = 4a(b - c - a) > 0.$$

Daraus ergibt sich folgender Algorithmus zum Aufstellen der reduzierten Formen ($D > 0$ ist fixiert.)

(i) Finde alle $k \in \mathbb{Z}$, sodass $D - k^2$ positiv und durch 4 teilbar ist. (Wegen $|k| < \sqrt{D}$ gibt es nur endlich viele.)

(ii) Sei ein k aus 1. fixiert. Dann betrachte dann alle $a \geq 1$, welche $\frac{1}{4}(D - k^2)$ teilen.

(iii) Aus der bisher gewonnenen Liste von Paaren (k, a) streiche alle Paare mit $k + 2a \leq \sqrt{D}$.

(iv) Zu den übrig bleibenden Paaren (k, a) bilde die Formen

$$f = \left(a, k + 2a,\ k + a - \frac{D - k^2}{4a}\right).$$

Dies sind dann alle reduzierten Formen mit der Diskriminante D.

Bemerkung: Darunter können sich Formen befinden mit ggT $(a, b, c) \neq 1$. Diese Formen kann man weglassen.

A.2 Reduzierte Formen und Klassenzahl $h(D)$

Bisher haben wir nur die reduzierten Formen betrachtet, welche zur Grundform $f_D = (1,0,-\frac{D}{4})$ oder $f_D = (1,1,\frac{1-D}{4})$ äquivalent sind.

Zur Bestimmung der Klassenzahl $h(D)$ genügt es reduzierte Formen zu betrachten, denn für jede Äquivalenzklasse $[f]$ von Formen ist

$$[f] \cap \mathscr{R} \neq \emptyset$$

($\mathscr{R}$ = Menge der reduzierten Formen).

D	Grundform f	reduzierte Form, d.h. die Periode	$w_f^{\surd} = \frac{\beta+\sqrt{D}}{2\alpha}$	-KBE	Perioden-länge
5	$(1,1,-1)$	$f_1 = (1,3,1)$	$\frac{1}{2}(1+\sqrt{5})$	$= [\![2,\overline{3}]\!]$	1
8	$(1,0,-2)$	$f_1 = (2,4,1)$ $f_2 = (1,4,2)$	$\frac{1}{2}\sqrt{8}$	$= [\![2,\overline{2,4}]\!]$	2
12	$(1,0,-3)$	$f_1 = (1,4,1)$	$\frac{1}{2}\sqrt{12}$	$= [\![2,\overline{4}]\!]$	1
13	$(1,1-3)$	$f_1 = (3,5,1)$ $f_2 = (3,7,3)$ $f_3 = (1,5,3)$	$\frac{1}{2}(1+\sqrt{13})$	$= [\![3,\overline{2,2,5}]\!]$	3
17	$(1,1,-4)$	$f_1 = (2,5,1)$ $f_2 = (4,7,2)$ $f_3 = (4,9,4)$ $f_4 = (2,7,4)$ $f_5 = (1,5,2)$	$\frac{1}{2}(1+\sqrt{17})$	$= [\![3,\overline{3,2,2,3,5}]\!]$	5
20	$(1,0,-5)$	$f_1 = (4\ 6\ 1)$ $f_2 = (5,10,4)$ $f_3 = (4,10,5)$ $f_4 = (1,6,4)$	$\frac{1}{2}\sqrt{20}$	$= [\![3,\overline{2,2,2,6}]\!]$	4
21	$(1,1-5)$	$f_1 = (1,5,1)$	$\frac{1}{2}(1+\sqrt{21})$	$= [\![3,\overline{5}]\!]$	1
24	$(1,0,-6)$	$f_1 = (3,6,1)$ $f_2 = (1,6,3)$	$\frac{1}{2}\sqrt{24}$	$= [\![3,\overline{2,6}]\!]$	2
28	$(1,0-7)$	$f_1 = (2,6,1)$	$\frac{1}{2}\sqrt{28}$	$= [\![3,\overline{3,6}]\!]$	2
29	$(1,1,-7)$	$f_1 = (5,7,1)$	$\frac{1}{2}(1+\sqrt{29})$	$= [\![4,\overline{2,2,2,2,7}]\!]$	5

Tabelle A.1: Die Grundformen und ihre Periode für positive Diskriminanten $D < 30$. Weil D kein Quadrat sein darf (Sonderfall) und weil $D \equiv 0,1 \bmod 4$, kommen nur 10 Werte in Frage.

D	k	$\frac{D-k^2}{4}$	a	Zulässige Paare (k,a)	Formen $(a,k+2a,k+a-\frac{D-k^2}{4a})$	$w_f^{\surd} = $ KBE	$h(D)$
5	±1	1	1	(1,1)	(1,3,1)		1
8	0	2	1,2	(0,2), (2,1)	(2,4,1), (1,4,2)		1
	±2	1	1				
12	0	3	1,3	(0,3), (2,1), (2,2)	(3,6,2), (1,4,1)		2
	±2	2	1,2		(2,6,3)		
13	±1	3	1,3	(−1,3), (1,3), (3,1)	(3,5,1), (3,7,3)		1
	±3	1	1		(1,5,3)		
17	±1	4	1, 2, 4	(−1,4), (1,2), (1,4)	(4,7,2), (2,5,1)		1
	±3	2	1, 2	(3,1), (3,2)	(4,9,4)		
					(1,5,2), (2,7,4)		
20	0	5	1, 5	(0,5), (−2,4), (2,2)	(5,10,4), (4,6,1)		1
	±2	4	1, 2, 4	(2,4), (4,1)	(2,6,2)		
	±4	1	1		(4,10,5), (1,6,4)		
21	±1	5	1, 5	(−1,5), (1,5)	(5,9,3), (5,11,5)	$\frac{9+\sqrt{21}}{10} = [\![2,\overline{2,3}]\!]$	2
	±3	3	1, 3	(3,1), (3,3)	(1,5,1), (3,9,5)		
24	0	6	1, 2, 3, 6	(0,3), (0,6)	(3,6,1), (6,12,5)	$\frac{12+\sqrt{24}}{12} = [\![2,\overline{2,4,2}]\!]$	2
	±2	5	1, 5	(−2,5), (2,5)	(5,8,2), (5,12,6)		
	±4	2	1, 2	(4,1), (4,2)	(1,6,3); (2,8,5)		
28	0	7	1, 7	(0,7), (−2,6), (2,2)	(7,14,6), (6,10,3)	$\frac{14+\sqrt{28}}{14} = [\![2,\overline{2,3,32}]\!]$	2
	±2	6	1, 2, 3, 6	(2,3), (2,6)	(2,6,1), (3,8,3), (6,14,7)		
	±4	3	1, 3	(4,1), (4,3)	(1,6,2), (3,10,6)		
29	±1	7	1, 7	(−1,7), (1,7)	(7,13,5), (7,15,7)		1
	±3	5	1, 5	(−3,5), (3,5)	(5,7,1), (5,13,7)		
	±5	1	1	(5,1)	(1,7,5)		

Tabelle A.2: Berechnung der Klassenzahl für $D > 0$. Auffinden aller reduzierten Formen zu gegebenem D. Die Klassenzahl h(D) ist die Anzahl der *verschiedenen* Zykel reduzierter Formen welche zu fixiertem D gehören. In Tabelle A.1 erschien immer nur ein Zyklus, nämlich der welcher sich aus der Grundform ergibt.

B Seminarvorträge

1. Zyklische Gruppen [Isc92]
2. Zur Existenz der Primitivwurzeln [Sil05, Kapitel 20 und 21]
3. Mersenne-Zahlen und perfekte Zahlen [Sil05]
4. Kettenbrüche [SF06, I8 und I9]
5. 6 Beweise für die Unendlichkeit der Primzahlfolge [AZ04]
6. Quadratisches Reziprozitätsgesetz [Sil05, §22-24], [Isc92]
7. Primfaktorzerlegung
8. Das Bertrandsche Postulat [AZ04]
9. Minkoskischer Gittersatz und Anwendung auf Quadratsummen [SF06]
10. Eisenstein-Zahlen und der Fermat'sche Satz [AZ04]
11. Zahlentheoretische Funktionen und Möbius'sche Umkehrformel [SF06]

Literaturverzeichnis

Weiterführende Literatur zur Vorlesung ([Gau81], [Zag81], [HS90]) und zum Seminar ([Sil05], [SF06], [Isc92], [AZ04], [BSK66]):

[AZ04] AIGNER, MARTIN und GÜNTER ZIEGLER: *Das Buch der Beweise*. Springer Verlag, 2te Auflage, 2004. ISBN: 978-3-540-40185-8.

[BSK66] BOREVIC, ZENON I., IGOR R. SAFAREVIC und HELMUT KOCH: *Zahlentheorie*. Birkhäuser, 1966. ASIN: B0000BQ6TP.

[Gau81] GAUSS, CARL FRIEDRICH: *Untersuchungen über höhere Arithmetik*. AMS Chelsea Publishing, 1965, reprint: 1981. ISBN: 978-0-8284-0191-3.

[HS90] HLAWKA, EDMUND und JOHANNES SCHOISSENGEIER: *Zahlentheorie. Eine Einführung*. Manz Verlag, Wien, 1990. ISBN: 3-214-00005-5.

[Isc92] ISCHEBECK, FRIEDRICH: *Einladung zur Zahlentheorie*. Spektrum Akademischer Verlag, 1992. ISBN: 3860254316.

[SF06] SCHEID, HARALD und ANDREAS FROMMER: *Zahlentheorie*. Spektrum Akademischer Verlag, 4te Auflage, Oktober 2006. ISBN: 978-3827416926.

[Sil05] SILVERMAN, JOSEPH: *A friendly Introduction to Number Theory*. Prentice Hall, 3te Auflage, 2005. ISBN: 0131861379.

[Zag81] ZAGIER, DON BERNARD: *Zeta-Funktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie*. Springer, Berlin, 1981. ISBN: 978-3-540-10603-6.

Index