

# 8 Ganzzahlige quadratische Formen

## 8.1 Grundbegriffe und Bezeichnungen

**Problem:** Man diskutiert die diophantische Gleichung

$$k = ax^2 + bxy + cy^2 \quad (*)$$

Gegeben sind  $a, b, c, k \in \mathbb{Z}$ , gesucht ist ein  $\underline{x} = (x, y) \in \mathbb{Z}^2$ , für die (\*) gilt.

Gegeben  $Q = aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]$ ,  $a, b, c \neq 0$ , mit Kurzbezeichnung  $Q = [a, b, c]$ . Dieses  $Q$  heißt ganzzahlige binäre (wegen den 2 Variablen) quadratische (grad  $q = 2$ ) Form.

Nun betrachtet man  $Q$  als Abbildung  $\mathbb{Z}^2 \rightarrow \mathbb{Z}$ ,  $\underline{x} = (x, y) \mapsto Q(\underline{x})$ .

**Definition**

- (1)  $\underline{x}$  primitiv  $\iff \text{ggT}(x, y) = 1$
- (2)  $Q$  primitiv  $\iff \text{ggT}(a, b, c) = 1$
- (3)  $Q$  stellt  $k \in \mathbb{Z}$ ,  $k \neq 0$  (primitiv) da  $\iff \exists \underline{x} \in \mathbb{Z}^2$  ( $\underline{x}$  primitiv), mit  $Q(\underline{x}) = k$

**Problem:** Welche Formen stellen welche Zahlen dar?  $Q(\mathbb{Z}^2) = ?$

Falls  $k \in Q(\mathbb{Z}^2)$ , welche weiteren  $\underline{x}'$  erzeugen  $k = Q(\underline{x}')$ ?  $Q^{-1}(\{k\}) = ?$

**Bemerkung:** (1)  $z \in \mathbb{Z}$ , so  $Q(z \cdot \underline{x}) = z^2 \cdot Q(\underline{x})$

- (2) Mit  $Q$  ist auch  $mQ$  eine Quadratische Form ( $m \in \mathbb{Z}$ ,  $m \neq 0$ )

Wegen (1) genügt es meist, primitive Darstellungen zu betrachten.

Aus der Linearen Algebra ist über reelle Quadriken bekannt: Es gibt Darstellungsmatrizen  $A_Q = \mathbb{R}^{2 \times 2}$  mit  $Q(\underline{x}) = \underline{x} A_Q \underline{x}^\top$ , wobei

$$A_Q = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

**Idee** (Gauß?) Wegen  $\mathbb{Z}^2 U = \mathbb{Z}^2$  für  $U \in GL_2(\mathbb{Z})$  gilt  $Q(\mathbb{Z}^2) = Q \cdot (\mathbb{Z}^2 U)$ .  $Q(\underline{x}U) = \underline{x}U \cdot A_Q \cdot (\underline{x}U)^\top = \underline{x}(U A_Q U^\top) \underline{x}^\top$

**Definition**

- (1) Zu  $Q$  sei  $U \cdot Q$  die Quadratische Form mit Darstellungsmatrix  $U A_Q U^\top$
- (2)  $Q$  und  $Q'$  heißen (eigentlich) äquivalent ( $Q \sim Q'$  bzw.  $Q \approx Q'$ )  $\iff \exists U \in GL_2(\mathbb{Z})$  (bzw.  $\exists I \in SL_2(\mathbb{Z})$ , wobei  $SL_2(\mathbb{Z}) = \{U \in \mathbb{Z}^{2 \times 2} \mid \det U = 1\}$ ) mit  $Q' = U \cdot Q$ .

$\sim, \approx$  unterscheiden sich wenig, sozusagen höchstens um eine Matrix  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .

**Bemerkung:** (1)  $1_2 \cdot Q = Q$ ,  $U, V \in GL_2(\mathbb{Z})$ .  $(UV) \cdot Q = U \cdot (V \cdot Q)$ .

„ $GL_2(\mathbb{Z})$  bzw.  $SL_2(\mathbb{Z})$  operiert auf der Menge der Quadratischen Formen“

(2)  $\sim, \approx$  sind Äquivalenzrelationen

(3) Äquivalente Formen stellen die selben Zahlen dar.

**Beweis**

(1)  $UV \cdot Q: UV A_Q (UV)^T = U(V A_Q V^T) U^T : U \cdot (V \cdot Q)$ .

Folgt  $Q' = U \cdot Q$ , so  $U^{-1} \cdot Q' = U^{-1} \cdot (U \cdot Q) = (U^{-1} U) \cdot Q = 1_2 \cdot Q = Q$ .

Also ist  $\sim$  symmetrisch:  $Q \sim Q$ .

Transitivität:  $Q \sim Q'$ ,  $Q' = U \cdot Q$  und  $Q' \sim Q''$ ,  $Q'' = V \cdot Q'$ , mit  $U, V \in GL_2(\mathbb{Z})$ , so ist  $Q'' = V \cdot (U \cdot Q) = (VU) \cdot Q \implies Q'' \sim Q$  ■

## 8.2 Die Diskriminante

Sei  $Q = [a, b, c]$  eine Quadratische Form.

**Definition**

$\Delta = -4 \cdot \det A_Q = b^2 - 4ac = \text{dis}(Q) \in \mathbb{Z}$  heißt Diskriminante von  $Q$ .

Bemerkung aus der Linearen Algebra:  $\mathcal{V} = \mathcal{V}_{Q-k}(\mathbb{R}) = \{\underline{x} \in \mathbb{R}^2 \mid Q(\underline{x}) = k\}$  ist reelle Quadrik, abgesehen von ausgearteten Fällen gilt:  $\Delta < 0$ :  $\mathcal{V}$  Ellipse,  $\Delta > 0$ ,  $\mathcal{V}$  Hyperbel.

**Beispiel**

$X^2 + 5Y^2$  Ellipse:  $\Delta = 0 - 4 \cdot 5 = -20 < 0$

$X^2 - 2Y^2$  Hyperbel:  $\Delta = 0 - 4 \cdot (-2) = 8 > 0$

**Problem:** Welche  $(x, y) \in \mathbb{Z}^2$  (Gitterpunkte) liegen auf  $\mathcal{V}$ .

**Satz 8.1 (Diskriminantensatz)**

Sei  $Q$  eine Quadratische Form.

(1) Ist  $Q \sim Q'$ , so gilt  $\text{dis}(Q) = \text{dis}(Q')$ .

(2) Ist  $\Delta = \text{dis } Q$  ein Quadrat in  $\mathbb{Z} \iff$  „ $Q$  zerfällt über  $\mathbb{Z}$ “, also  $\exists u, v, w, z \in \mathbb{Z}$  mit  $Q = (uX + vY)(wX + zY)$

(3) Ist  $\text{dis } Q \neq 0$ , so gilt

$$Q \text{ definit} \iff \text{dis } Q < 0$$

$$Q \text{ indefinit} \iff \text{dis } Q > 0$$

(4)  $0 \neq d \in \mathbb{Z}$  ist Diskriminante  $\iff d \equiv 0, 1 \pmod{4}$

Anwendung:  $\Delta = \text{dis } Q$  sei ein Quadrat  $Q(\underline{x}) = k \neq 0 \iff \exists d \in \mathbb{Z}, dk: ux + vy = d, wx + zy = \frac{k}{d}$ . Die Frage nach den darstellbaren  $k$  läuft zurück auf a) Bestimmung aller Teiler von  $k$ , b) Diskussion eines ganzzahligen LSG.

Ab jetzt interessieren nur noch nichtquadratische Diskriminanten.

### Beweis

$$(4) \delta = \text{dis } Q = b^2 - 4ac \equiv b^2 \equiv 0, 1 \pmod{4}.$$

$$d \equiv 0 \pmod{4}: Q = [1, 0, -\frac{d}{4}]$$

$$d \equiv 1 \pmod{4}: Q = [1, 1, -\frac{1-d}{4}]$$

Für diese Formen gilt  $\text{dis } Q = d \equiv \Delta$ . Diese Form heißt „Hauptform“ der Diskriminante.

$$(1) \det U A_Q A^T = \det U \cdot \det U^T \cdot \det A_Q = (\det U)^2 \cdot \det A_Q = \det A_Q \implies \text{Behauptung.}$$

(2) (Skizze)

„ $\Leftarrow$ “ Nachrechnen

„ $\Rightarrow$ “  $\Delta = \text{dis } Q = q^2$ . Sei  $t = \text{ggT}(a, \frac{b-a}{2})$ , dann (Übung):

$$Q = \left(\frac{a}{t}X + \frac{b-q}{2t}Y\right)\left(tX + \frac{b+q}{2\frac{a}{t}}Y\right)$$

$$(3) a = 0 \implies \Delta > 0, Q = bXY + cY^2 = (bX + cY)Y \text{ indefinit}$$

$$a \neq 0: aQ = (aX + bY)^2 - \frac{1}{4}\Delta Y^2. \text{ Offensichtlich: } \Delta < 0: \text{definit, } \Delta > 0: \text{indefinit} \quad \blacksquare$$

<+++>

## 8.3 Darstellung von Zahlen durch QFen

Vor.  $Q$  QF,  $\text{dis } Q = \Delta$  sei kein Quadrat.

$U.Q$  QF mit Matrix  $U A_Q U^T, U \in GL_2(\mathbb{Z})$

$$U = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \Rightarrow U.Q = [Q(r, s), 2rU \cdot a + (rv + su)b + 2sv \cdot c, Q(u, v)]$$

Spezialfälle:

$$Q' = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \cdot Q = [a, t \cdot 2a + b, at^2 + bt + c]$$

$$Q' = \begin{pmatrix} \cdot & 1 \\ -1 & t \end{pmatrix} \cdot Q = [c, -b + 2ct, ct^2 - bt + a]$$

$$Q' = \begin{pmatrix} \cdot & 1 \\ -1 & \cdot \end{pmatrix} \cdot Q = [c, -b, a]$$

$$Q' = \begin{pmatrix} 1 & \cdot \\ 1 & 1 \end{pmatrix} \cdot Q = [a, 2a + b, a + b + c]$$

Wunsch:

Algorithmus der feststellt, ob  $Q$   $k$  darstellt oder nicht.

**Satz 8.2 (1. Darstellungssatz)**

$Q$  stellt  $0 \neq k \in \mathbb{Z}$  genau dann primitiv dar, wenn:  $\exists Q' = [k, l, m]$  mit  $Q' \approx Q \wedge -|k| < l \leq |k|$ .

Hat man also einen Algorithmus, der feststellt, ob  $Q \approx Q' \vee Q \not\approx Q'$ , so hat man einfach  $2k$  Formen zu testen (auf Äquivalenz zu  $Q$ ). ( $m = \frac{l^2 - \Delta}{4k}$ )

Spezialfall:

$k = 1, Q$  stellt 1 dar  $\Leftrightarrow Q \approx [1, 0, \frac{-\Delta}{4}]$  (für  $\Delta \equiv 0 \pmod{4}$ )

–HIER FEHLT NOCH EINE ZEILE, WELCHE NICHT RICHTIG KOPIERT WURDE –

$Q \approx [1, 1, \frac{1-\Delta}{4}]$  (für  $\Delta \equiv 1 \pmod{4}$ ).

Ergebnis: Genau die zur Hauptform äquivalenten Formen stellen 1 dar.

**Beweis**

„ $\Leftarrow$ “:  $Q'(1, 0) = k$ . Hat man  $Q' \approx Q \Rightarrow Q$  stellt  $k$  dar

„ $\Rightarrow$ “:  $k = Q(x, y), \text{ggT}(x, y) = 1$ . LinKomSatz liefert  $u, v \in \mathbb{Z}$  mit  $xv - yu = 1 \Rightarrow U := \begin{pmatrix} x & y \\ u & v \end{pmatrix} \in \text{Sl}_2(\mathbb{Z})$

$$Q_1 := U.Q = [\underbrace{Q(x, y)}_{=k}, l', \text{irgendwas}], l := l' \bmod 2|k|, \exists t : l = l' + 2tk \Rightarrow Q' = \begin{pmatrix} 1 & \cdot \\ t & 1 \end{pmatrix} . Q_1$$

wie verlangt. ■

**Satz 8.3 (2. Darstellungssatz)**

Sei  $k \in \mathbb{Z}, k \neq 0$ . Genau dann gibt es eine Form  $Q$  mit  $\text{dis } Q = \Delta$ , die  $k$  primitiv darstellt, wenn die Kongruenz  $l^2 \equiv \Delta \pmod{4k}$  so lösbar ist, dass  $\text{ggT}(k, l, \frac{l^2 - \Delta}{4k}) = 1$ .

**Beweis**

„ $\Leftarrow$ “: Einfach, die Form  $[k, l, \frac{l^2 - \Delta}{4k}]$  tut es

„ $\Rightarrow$ “:  $k$  so darstellbar  $Q \approx Q' = [k, l, \frac{l^2 - \Delta}{4k}]$  nach 1. Darstellungssatz (für (mindestens) ein  $l$ )  
 $\Rightarrow \frac{l^2 - \Delta}{4k} \in \mathbb{Z} \Rightarrow l^2 \equiv \Delta \pmod{4k}$  [ggT stimmt auch] ■

Spezialfälle:

Sei  $k = p \in \mathbb{P}$

- $p \nmid \Delta, p \neq 2$  :  $p$  so darstellbar  $\Leftrightarrow (\frac{\Delta}{p}) = 1$
- $p \mid \Delta, p \neq 2$  :  $p$  so darstellbar  $\Leftrightarrow v_p(\Delta) = 1$
- $p = 2 \mid \Delta$  : 2 so darstellbar  $\Leftrightarrow \Delta \equiv 8, 12 \pmod{16}$

Zu den Spezialfällen

- $p \nmid \Delta : \left(\frac{\Delta}{p}\right) = 1$  lösbar,  $l_1^2 \equiv \Delta \pmod{p} \Leftrightarrow l_1^2 \equiv \Delta \pmod{4p} \rightsquigarrow ChRs$
- $2 \neq p \mid \Delta$ : Löse  $l \equiv 0 \equiv \Delta \pmod{p(*)}$ ,  $l^2 \equiv \Delta \pmod{4} \Rightarrow l^2 \equiv \Delta \pmod{4p}$   
 $\text{ggT}(\underbrace{p, l}_{\text{ggT}=p}, \frac{l^2 - \Delta}{4p}) = 1 \Leftrightarrow p \nmid \frac{l^2 - \Delta}{4p} \Leftrightarrow p^2 \nmid l^2 - \Delta \Leftrightarrow p^2 \nmid \Delta$ , da  $p^2 \mid l^2$  nach (\*). ( $\Rightarrow v_p(\Delta) = 1$ )
- $p = 2 \mid \Delta$ : Ü.

**Definition**

Die Klassenzahl  $h(\Delta)$  ist die Anzahl der Klassen eigentlich äquivalenter Formen mit Diskriminante  $\Delta$ . „Schöne Resultate“, falls  $h(\Delta) = 1$ .

$\Rightarrow$  Alle Formen der Diskriminante  $\Delta$  stellen  $k$  dar  $\Leftrightarrow$  Bed. 2. DarstSatz.

Später.  $h(-4) = 1, Q = [1, 0, 1]$  Ergebnis:  $2 \neq p \in \mathbb{P}$  wird durch  $Q = x^2 + y^2$  dargestellt  $\Leftrightarrow 1 = \left(\frac{-4}{p}\right) = \frac{-1}{p} = (-1)^{\frac{p-1}{2}} \Leftrightarrow p \equiv 1 \pmod{4}$  Andere Beispiele, etwa  $\Delta = -164$  (Klassenzahl 1, betragsmäßig größte negative Zahl. Im positiven unbekannt)

## 8.4 Reduktion der definiten Formen

Sei  $\Delta < 0$  [und damit „Nicht-Quadrat“],  $\Delta = b^2 - 4ac \Rightarrow ac > 0$ . Ohne Einschränkung positiv definit, d.h.  $a > 0, c > 0$ .

**Definition (Gauß)**

$Q$  (mit Diskr  $\Delta$ ) heißt reduziert  $\Leftrightarrow |b| \leq a \leq c$

In dieser Vorlesung:

$Q$  heißt vollreduziert  $\Leftrightarrow Q$  ist reduziert und falls  $(c = 0 \wedge b \neq 0) \vee (|b| = a)$  auch noch  $b > 0$  ist.

Idee (Gauß):

Setzte  $|Q| := a + |b|$ . Versuche  $Q' \approx Q$  zu finden mit  $|Q'| < |Q|$ . Das geht, solange  $Q$  nicht reduziert ist.

Fall I:  $a > c, Q' := \begin{pmatrix} \cdot & 1 \\ -1 & \cdot \end{pmatrix}, Q = [\underbrace{c}_{-a'}, \underbrace{-b}_{b'}, \underbrace{a}_{c'}]. |Q'| = a' + |b'| = |b| + c < |b| + a = |Q|$

Fall II:  $a \leq c, |b| > a$  (da  $Q$  nicht-reduziert) Division von  $b$  mit Rest durch  $2a$ :  $\exists t \in \mathbb{Z} : b = b' - 2ta, -a < b' \leq a$ .  $Q' = \begin{pmatrix} 1 & \cdot \\ t & 1 \end{pmatrix} \cdot Q = [a, \underbrace{b + 2ta}_{b'}, c']$ .  $|Q'| = |b'| + a \leq a + \underbrace{|a|}_{=a \text{ (da } -a \leq a)}$

Dies ergibt Vollreduktionsalgorithmus  $red(Q)$ , der  $\tilde{Q}$  berechnet mit  $\tilde{Q} \approx Q \wedge \tilde{Q}$  vollreduziert. Wiederholte Anwendung von  $Q := Q'$  aus Fall I,II endet nach endlich vielen Schritten mit reduziertem  $Q_1 \approx Q$ . Falls  $Q_1$  vollreduziert, so  $\tilde{Q} := Q_1$ .

Falls  $Q_1$  nicht vollreduziert, so 2 Fälle für  $Q_1 = [a, b, c]$

- $c = a$ , aber  $b < 0 : \tilde{Q} := \begin{pmatrix} \cdot & 1 \\ -1 & \cdot \end{pmatrix} \cdot Q_1 = [a, -b, a]$ , jetzt  $-b > 0$
- $|b| = a$ , also  $b = -a < 0$ .  $\tilde{Q} = \begin{pmatrix} 1 & \cdot \\ 1 & 1 \end{pmatrix} \cdot [a, -a, c] = [a, a, c], c' = a + b + c = c$  ist

vollreduziert ( $b' = a > 0$ ).

Ziel: 2 vollreduzierte Formen der Disk  $\Delta$  sind äquivalent  $\Leftrightarrow$  sie sind gleich. Es folgt:

$Q \approx Q' \Leftrightarrow \text{red } Q = \text{red } Q'$ . Daher gibt es einen Algorithmus, der entscheidet, ob  $Q \approx Q' \vee Q \not\approx Q'$

Hilfsatz:

$Q = [a, b, c]$  sei reduziert. Dann:

(i)  $a = \min Q(\mathbb{Z}^2 \setminus 0)$

(ii) Für  $a < c$  ist  $Q^{-1}(\{a\}) = \{\pm(1, 0)\}$  (klar:  $Q(\underline{x}) = Q(-\underline{x})$ )

Für  $0 \leq b < a = c$  ist  $Q^{-1}(\{a\}) = \{\pm(1, 0), \pm(0, 1)\}$ . (Für  $|b| = a = c$  (=1, da  $Q$  primitiv)

$Q[1, \pm 1, 1] = x^2 \pm xy + y^2 \Rightarrow \#Q^{-1}\{a\} = 6$ )

$|b| \leq a \leq c$

(\*)  $Q(x, y) = ax^2 + bxy + cy^2 \stackrel{(1)}{\geq} ax^2 - |bxy| - ay^2 \geq a(|x| - |y|)^2 + (2a - |b|)|xy| \geq a(\underbrace{(|x| - |y|)^2 + |xy|}_{\in \mathbb{Z}, \neq 0, \text{ wenn } (x, y) \neq 0, \text{ also } \geq 1}) \stackrel{(4)}{\geq} a.$

Erinnerung:

$Q = [a, b, c]$  reduziert  $\Leftrightarrow |b| \leq a \leq c$

Vollreduziert: Falls  $a = c \wedge b \neq 0 \vee a = c = |b|$ , so  $b > 0 \leadsto$  Vollreduktionsalgorithmus red.

Sei  $Q(x, y) = a \Rightarrow$  in (\*) überall „ $c$ “

$a < c \Rightarrow y = 0$  (sonst bei (1)  $>$ )

„ $=$ “ bei (4)  $\Rightarrow (|x| - |y|)^2 + |xy| = 1 \Rightarrow (x, y) \in M = \{\pm(1, 0), \pm(0, 1), (\pm 1, \pm 1)\}$

Fall I:  $Q^{-1}(a) = \{\pm(1, 0)\}, \#Q^{-1}(a) = 2$

Fall II:  $a = c$ , aber  $|b| < a \Rightarrow 2a - |b| > a \Rightarrow$  „ $=$ “ nur für  $|xy| = 0$ .  $Q^{-1}(a) = \{\pm(1, 0), \pm(0, 1)\}$

Fall III:  $a = c = |b|$ , etwa  $b > 0$ , so  $x^2 + xy + y^2 = 1$  von  $(\pm 1, \pm 1)$  in  $M$  nur  $\pm(1, -1)$  [dazu noch  $\pm(1, 0), \pm(0, 1)$ ]  $\Rightarrow \#Q^{-1}(a) = 6$

Folgerung: Sei  $Q, Q'$  vollständig reduziert und  $Q \approx Q'$ , so ist  $Q = Q'$ .

**Beweis**

$a = \min(Q(\mathbb{Z}^2 \setminus 0)) = \min(Q'(\mathbb{Z}^2 \setminus 0)) = a'$ .

Fall I:  $a < c \wedge U = \begin{pmatrix} r & s \\ u & v \end{pmatrix}$  mit  $U \cdot Q = Q'$ .  $a = Q(1, 0) = Q'(1, 0) = Q((1, 0)U) = Q(r, s) \Rightarrow$

$(r, s) = \pm(1, 0) \Rightarrow s = 0, \pm U = \begin{pmatrix} 1 & 0 \\ 0(?) & 1 \end{pmatrix} = U.$

$Q' = (a, b + 2au, *(?)), |b| \leq a, Q'$  red.  $|b'| = |b + 2au| < a$ . Wegen  $|b| < a \Rightarrow U = 0, \pm U = \begin{pmatrix} 1 & \cdot \\ \cdot & 1 \end{pmatrix} \Rightarrow Q = Q'$

Fall II:  $a = c, |b| \neq a$ .  $\#Q^{-1}(a) = 4 \Rightarrow$  II liegt auch für  $Q'$  vor  $\Rightarrow a = a' = c' \Rightarrow b^2 = b'^2 \Rightarrow b' = \pm b$ , aber nur  $b$  möglich, da  $Q'$  vollständig reduziert  $\Rightarrow Q' = Q$ .

Fall III:  $a = c = |b| = b \Rightarrow$  Fall II auch für  $Q' \Rightarrow a = a' = c' = b'$  ■

**Satz 8.4 (Hauptsatz über definite QFen)**

Sei  $\Delta \in \mathbb{Z}, \Delta \equiv 0, 1 \pmod{4}, \Delta < 0$ .

- (i) Zwei Formen  $Q, Q'$  mit Diskriminante  $\Delta$  sind genau dann eigentlich äquivalent, wenn  $\text{red}(Q) = \text{red}(Q')$  (mit VollredAlgo red)
- (ii) Die vollreduzierten Formen der Diskriminanten  $\Delta$  bilden ein volles Vertretersystem aller eigentlichen Formenklassen, insbesondere ist die Klasse zu  $U$   $h(\Delta)$  endlich.

**Beweis**

- (i)  $\exists U, U'$  mit  $\text{red } Q = U \cdot Q, \text{red } Q' = U' \cdot Q' (U, U' \in \text{Sl}_2(\mathbb{Z}))$  können in red berechnet werden. Multipliziere die Matrizen bei den Reduktionsschritten,  $Q \approx \text{red } Q, Q' \approx \text{red } Q'$ .  
 $Q \approx Q' \Leftrightarrow \text{red } Q \approx \text{red } Q' \stackrel{\text{Folgerung}}{\Leftrightarrow} \text{red}(Q) = \text{red}(Q')$ .
- (ii)  $Q$  reduziert  $\Leftrightarrow |b| \leq a \leq c \Rightarrow b^2 \leq ac \Rightarrow |\Delta| = -\Delta = -b^2 + 4ac \geq -b^2 + 4b^2 = 3b^2$ .  
 Abschätzung:  $|b| \leq \sqrt{\frac{|\Delta|}{3}} \Rightarrow$  Nur endlich viele reduzierte  $Q$ s.  
 Dies ergibt Algorithmus zur Bestimmung von  $h(\Delta)$ :  $h(\Delta) = \#$  vollreduzierten Formen zu  $\Delta$ . Reduzierte Form  $Q = [a, b, c] \Leftrightarrow |b| \leq \sqrt{\frac{|\Delta|}{3}}, \equiv \Delta \pmod{2}$ , da  $b^2 \equiv \Delta \pmod{4}$ .  
 $|b| \leq a \leq c \leq ac = \frac{b^2 - \Delta}{4}$ . Stelle alle diese  $(a, b, c)$  auf, streiche die nicht vollreduzierten. ■

**Satz 8.5 (Heegner/Stark (1969))**

Für  $\Delta < 0$  gilt:  $h(\Delta) = 1 \Leftrightarrow \Delta \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}$

Beweis im Netz!

**Satz 8.6 (Siegel)**

Für negative Diskriminanten  $\Delta$  gilt  $\lim_{|\Delta| \rightarrow \infty} h(\Delta) = \infty$

( $\Rightarrow$  Für jedes feste  $\hat{h} \in \mathbb{N}$  gibt es  $\infty$  viele  $\Delta$  mit  $h(\Delta) = \hat{h}$ .)

Gauß definiert eine Verknüpfung (Komposition) zweier Formen  $Q_1, Q_2 \Rightarrow Cl(\Delta) =$  Menge aller Formenklassen wird (endliche abelsche Gruppe „Klassengruppe“ genannt.

$\leadsto$  viele Vermutungen, wenige Sätze bis heute Gaußsche Geschlechtertheorie ersetzt  $h(\Delta) = 1$  durch etwas schwächere Bedingung.

**8.5 Reduktion indefiniter Formen**

Vor:  $Q = [a, b, c], \Delta = b^2 - 4ac > 0, \sqrt{\Delta} \notin \mathbb{Q}$  ( $\Delta$  kein Quadrat in  $\mathbb{Z}$ ) [aber  $a, c \neq 0$ ]

Ärger: Theorie viel komplizierter als bei  $\Delta < 0$

**Definition**

- (i)  $Q$  heißt halbreduziert  $\Leftrightarrow \sqrt{\Delta} - |2a| < b < \sqrt{\Delta}$
- (ii)  $Q$  heißt reduziert  $\Leftrightarrow 0 < b < \sqrt{\Delta} \wedge \sqrt{\Delta} - b < |2a| < \sqrt{\Delta} + b$

**Satz 8.7 (Reduktionsungleichungen)**

Für eine reduzierte Form  $Q = [a, b, c]$  gilt:

$$ac < 0$$

$$0 \stackrel{(1)}{<} b \stackrel{(2)}{<} \sqrt{\Delta}$$

$$\sqrt{\Delta} - b \stackrel{(3)}{<} |2a| \stackrel{(5)}{<} \sqrt{\Delta} + b$$

$$\sqrt{\Delta} - b \stackrel{(4)}{<} |2c| \stackrel{(6)}{<} \sqrt{\Delta} + b$$

$Q$  ist genau dann reduziert, wenn (2), (3), (4) gelten.

**Beweis**

Abschätzen  $\leadsto$  Netz ■

**Folgerung 8.8 (Reduktionskriterium)**

Sei  $Q$  halbreduziert. Dann ist  $Q$  reduziert, wenn eine der folgenden Ungleichungen gilt:

- (i)  $|a| \leq |c|$
- (ii)  $\sqrt{\Delta} - b < |2c|$

**Beweis**

(2), (3) ok bei halbreduzierten Formen

(ii) fordert (4)

(i) Bei  $|a| \leq |c| : (3) \Rightarrow (4)$  ■

**Bemerkung:** Zu  $Q = [a, b, c] \exists! t \in \mathbb{Z}$  mit  $Q' = \begin{pmatrix} \cdot & 1 \\ -1 & t \end{pmatrix} \cdot Q$  halbreduziert, denn  $Q' = [\underbrace{c}_{=a'}, \underbrace{-b+2ct}_{=b'}, ct^2 - bt + c]$ .

Zu erreichen.  $\sqrt{\Delta} - \underbrace{|2a'|}_{|2c|} < b' < \sqrt{\Delta} \exists! t$ , so dass das stimmt.

Benennungen:

- (i)  $Q' = [a', b', c']$  heißt rechter (linker) Nachbar von  $Q = [a, b, c]$ , wenn gilt:  $b+b' \equiv 0 \pmod{2c}$  und  $a' = c$  ( $a = c'$ ) und  $Q'$  halbreduziert.
- (ii)  $T =: T_Q$  aus Bew (oder Bem?) heie Nachbarmatrix (also  $Q' = T_Q \cdot Q$ )

Leicht zu sehen: Jede QF hat je genau einen reduzierten rechten bzw. linken Nachbarn.



Reduktionsalgorithmus:

Wiederhole das Bilden des rechten Nachbars so lange, bis reduzierte Form erreicht ist.

Wieso terminiert? Ist  $Q' = [c, -b+2ct, c']$  nicht-reduziert, so muss (i) im Reduktionskriterium nicht vorliegen, d.h.  $|a'| = |c| > |c'|$  (für  $Q'$ ). Der Koeffizient  $|c|$  kann nicht unendlich oft verkleinert werden.

**Satz 8.9 (Nachbarreduktionssatz)**

- (i) Ist  $Q = [a, b, c]$  reduziert, so ist auch der rechte Nachbar  $Q'$  von  $Q$  reduziert und es ist  $\text{sign}(a) = -\text{sign}(a')$
- (ii) Es gibt nur endlich viele reduzierte Formen.

**Beweis**

- (i) Abschätzen  $\leadsto$  mühsam
- (ii) Klar. Nur endlich viele  $b$  zu  $\Delta$ . Nur endlich viele  $a, c$  laut Ungleichungen zu  $B \Rightarrow$  Algorithmus zur Aufstellung aller reduzierten Formen. ■

$\Delta = -1$  bzw  $\Delta = -4m, m \in \mathbb{N}, qf, 2 \nmid m$ . Dann: Formen zu  $\Delta$  stellen  $p \in \mathbb{P}$  dar mit  $p \mid m$  kann zur Faktorisierung von  $m$  ausgenutzt werden. Hierzu schneller, hochgezüchteter Algorithmus von Shanks:

WH:  $Q$  indefinit,  $\Delta > 0, \sqrt{\Delta} \notin \mathbb{Q}$

1.  $Q = [a, b, c]$  halbreduziert  $\Leftrightarrow 0 < b < \sqrt{\Delta}, \sqrt{\Delta} - b < |2a| < \sqrt{\Delta} + b$ . Rechter (halbreduzierter) Nachbar von  $Q$  ist  $Q' = [a', b', c'], Q' = \begin{pmatrix} \cdot & 1 \\ -1 & t \end{pmatrix} \cdot Q, t$  mit  $\sqrt{\Delta} - |2c| < -bt2ct < \sqrt{\Delta}$ .  
Also  $t = \text{sign}(c) \cdot \lfloor \frac{\sqrt{\Delta}+b}{|2c|} \rfloor$ .

Algorithmus: Wiederholtes Nachbarbilden ergibt (irgendwann) reduzierte Form.

Sei  $Q = Q_0$  reduziert.  $Q_{j+1} = Q'_j (j \geq 0)$ . Da es nur endlich viele reduzierte Formen gibt, muss vorkommen:  $\exists k, l \in \mathbb{N}, l > 0$  mit  $Q_k = Q_{k+l}$ .

Der reduzierte linke Nachbar ist  $Q_{k-1} = Q_{kl-1}$  (da eindeutig bestimmt, usw gibt  $Q_0 = Q_l$  (mit  $l > 0$ )). Ist hier  $l$  minimal, so  $2 \mid l$  (wegen  $\text{sign}(a') = -\text{sign}(a)$ ), und  $Q_0, \dots, Q_{l-1}$  sind alle verschieden.

Benennung:

$\zeta(Q) = [Q_0, Q_1, \dots, Q_{l-1}]$  heißt Zyklus von  $Q$  ( $Q$  reduziert)

Klar: Die Menge der reduzierten Formen zerfällt disjunkt in Zyklen.

**Satz 8.10 (Satz von Mertens)**

Sei  $U \in \text{Sl}_2(\mathbb{Z}), U \neq \pm 1_2$ . Die Formen  $Q$  und  $\tilde{Q} := U \cdot Q$  seien reduziert. Dann ist eine der Matrizen  $\pm U, \pm U^{-1}$  ein Produkt von Nachbarmatrizen aufeinanderfolgender rechter Nachbarn. Insbesondere sind  $Q$  und  $\tilde{Q}$  im selben Zyklus.

**Folgerung 8.11**

Für 2 definite QFen  $Q_1, Q_2$  sei  $\Delta > 0$  usw (<- kein Quadrat) und es gilt:  
 $Q_1 \approx Q_2 \Leftrightarrow \text{red}(Q_2)$  ist im Zyklus  $\zeta(\text{red}(Q_1)) \Leftrightarrow \zeta(\text{red}(Q_2)) = \zeta(\text{red}(Q_1))$ .

Klar:

1. Es gibt einen Algorithmus, der entscheidet, ob  $Q_1 \approx Q_2$  oder nicht
2. Die Zyklen entsprechen den Formklassen zu  $\Delta \Rightarrow$  ist Algorithmus, der  $h(\Delta)$  berechnet (stelle alle reduzierten Formen auf, berechne Zyklen!).

Zum Beweis des Satzes von Merteus: Viele mühsame Abschätzungen.

$$U \cdot Q = (-U) \cdot Q, \text{ da } U = \begin{pmatrix} r & s \\ u & v \end{pmatrix}, -U = \begin{pmatrix} -r & -s \\ -u & -v \end{pmatrix}, 1 = \det U = rv - us. U^{-1} = \begin{pmatrix} v & -s \\ -u & r \end{pmatrix}, -U^{-1} = \begin{pmatrix} -v & s \\ u & -r \end{pmatrix}.$$

Die richtige Wahl entscheidet sich für passende positive Vorzeichen.

Ohne Einschränkung  $r > 0, v > 0$ , setze  $U' = UT_Q^{-1} = \begin{pmatrix} r' & s' \\ u' & v' \end{pmatrix}$ . Man zeigt:  $IU, IU^{-1}$  keine Nachbarmatrix  $\neq \pm 1 \Rightarrow 0 < r' < r$   
 Induktionshypothese für  $U', Q' \Rightarrow$  Behauptung.

Über  $h(\Delta)$  und Struktur der Klassengruppe bei  $\Delta > 0$  „fast“ keine allgemeine Sätze bekannt.  
 Unbekannt z.B: existieren unendlich viele  $\Delta$  mit  $h(\Delta) = 1$ ?

## 8.6 Automorphismengruppen

**Definition**

- (i)  $U \in Sl_2(\mathbb{Z})$  heißt eigentlicher Automorphismus der QF  $Q = [a, b, c] : \Leftrightarrow U \cdot Q = Q$ .
- (ii)  $\text{Aut}_+(Q) = \{U \in Sl_2(\mathbb{Z}) : U \cdot Q = Q\}$  (ist UGR von  $Sl_2(\mathbb{Z}) \leadsto$  Untergruppenkriterium) heißt eigentliche Automorphismengruppe von  $Q$ .

**Beweis**

- (i)  $\Delta > 0 \Rightarrow \text{Aut}_+(Q)$  abelsch und  $\#\text{Aut}(Q) = \infty. Q(\Delta) = k, U \in \text{Aut}_+(Q) \Rightarrow k = U \cdot Q(\underline{x}) = Q(\underline{x}U)$ . Mit  $\underline{x}$  stellt auch  $\underline{x}U$  die Zahl  $k$  dar  $\Rightarrow$  existieren unendlich viele  $\underline{y} \in \mathbb{Z}^2 : Q(\underline{y}) = k$ .  
 Man kann zeigen: Es gibt  $\underline{x}_1, \dots, \underline{x}_l, l \in \mathbb{N}_+$ , so dass  $\{\underline{x} | Q(\underline{x}) = k\} = \underline{x}_1 G \dot{\cup} \dots \dot{\cup} \underline{x}_l G$  mit  $G = \text{Aut}_+(Q)$  (falls  $k$  überhaupt darstellbar) ■

**Definition**

$[Q_0, \dots, Q_{2l-1}] = \zeta(Q), Q = Q_0$  reduziert. Die Matrix  $-T_Q, T_Q =: R$  heißt Doppelnachbarmatrix zu  $Q$  ( $Q'$  rechter Nachbar).  $B : R_{2l-2} \cdot \dots \cdot R_2 \dot{R}_0$  heißt Grundmatrix zu  $Q$ .

Klar nach Definition:  $B \cdot Q = Q$ , d.h.  $B \in \text{Aut}_+(Q)$ . Betrachte  $V \in \text{Aut}_+(Q)$ , so  $\pm V, \pm V^{-1}$  (eines davon) nach Satz von Mertes ein Produkt von Nachbarmatrizen.

$\Rightarrow$  Eine dieser Matrizen ist Potenz von  $B$ ! [würde sonst irgendwo mitten im Zyklus stehenbleiben]

**Satz 8.12**

$\text{Aut}_+(Q) = \{\pm B^m \mid m \in \mathbb{Z}\}$  ist sogar abelsch.

Wieso unendlich? Man zeigt leicht:  $R$  hat alle Koeffizienten  $> 0 \Rightarrow B$  auch  $\Rightarrow$  Alle Matrizen  $\pm B^m$  sind verschieden.

Es gibt auch Aussagen für nicht-reduziertes  $Q$ . Ist  $Q' = V.Q$ ,  $V \in \text{Sl}_2(\mathbb{Z})$ , so ist die Abbildung  $\phi : \text{Aut}_+(Q) \rightarrow \text{Aut}_+(Q'), U \mapsto VUV^{-1} =: \phi(U)$  ein Isomorphismus von Gruppen.

Moderne Theorie: Theorie der QFen zu  $\Delta$  weitgehend äquivalent zur algZT in quadratischem „Zahlkörper“  $K = \mathbb{Q}(\sqrt{\Delta})$ . Norm  $n(a + b\sqrt{\Delta}) = (a + b\sqrt{\Delta})(a - b\sqrt{\Delta}) = a^2 - b^2\Delta$  ist QF für  $a, b$ .