Automorphismen von binären quadratischen Formen

ELEMENTE DER MATHEMATIK

Revue de mathématiques élémentaires – Rivista di matematica elementare

Zeitschrift zur Pflege der Mathematik
und zur Förderung des mathematisch-physikalischen Unterrichts

Publiziert mit Unterstützung des Schweizerischen Nationalfonds
zur Förderung der wissenschaftlichen Forschung

El. Math. | Band 23 | Heft 2 | Seiten 25–48 | 10. März 1968

Automorphismen von binären quadratischen Formen

§1. Motivierung

Die Frage, welche ganzen Zahlen durch eine binäre quadratische Form mit ganzen Koeffizienten dargestellt werden, führt nach GAUSS auf die folgenden beiden Probleme:

(I) Zu entscheiden, ob zwei gegebene Formen mit gleicher Diskriminante äquivalent sind.

(II) Alle Substitutionen zu finden, durch welche die eine von zwei gegebenen äquivalenten Formen in die andere übergeht.

Da das Verfahren, mit dem man die Äquivalenz von zwei Formen feststellt, immer auch eine Substitution liefert, die die eine Form in die andere überführt, kann man das Problem (II) modifizieren:

(II′) Wie erhält man aus einer Substitution L, die die Form g in die Form h überführt, alle solchen Substitutionen?

Diese Frage nun lässt sich leicht zurückführen auf die Aufgabe:

(II″) Alle Substitutionen zu finden, durch welche eine Form in sich selbst übergeht.

Diese Substitutionen nennt man Automorphismen der Form.

Die Determinante eines Automorphismus ist ± 1. Eine binäre quadratische Form kann als Norm in einem quadratischen Zahlkörper aufgefasst werden:

$$a x^2 + b x y + c y^2 = a (x - \vartheta y) (x - \vartheta' y) = a N (x - \vartheta y) = a N (x + \vartheta^* y),$$

wobei

$$-\vartheta^* = \vartheta = \frac{-b + \sqrt{b^2 - 4ac}}{2a} = \frac{-b + \sqrt{-D}}{2a}$$

und ϑ' das Konjugium von ϑ bedeutet. Ein Automorphismus der Form ist nun offenbar eine lineare Abbildung φ des quadratischen Körpers auf sich, für die gilt $N(z) = N(\varphi(z))$. Damit führt unser Problem auf das Studium der normerhaltenden linearen Abbildungen des quadratischen Zahlkörpers.

§2. Lineare Abbildungen in einem quadratischen Zahlkörper

(2.1) Sind α' und α von Null verschiedene Elemente eines quadratischen Zahlkörpers K, so gilt

$$N(\alpha') = N(\alpha)$$

genau dann, wenn es ein ε in K gibt mit

$$\alpha' = \varepsilon\,\alpha \quad \text{und} \quad N(\varepsilon) = 1\,.$$

Beweis: Sei $N(\alpha') = N(\alpha)$. In K gibt es genau ein ε mit $\alpha' = \varepsilon\,\alpha$. Dann ist $N(\alpha') = N(\varepsilon\,\alpha) = N(\varepsilon)\,N(\alpha) = N(\alpha)$. Also $N(\varepsilon) = 1$. Die Umkehrung ist trivial.

(2.2) Aus (2.1) sieht man: ist bei einer Abbildung φ von K auf sich die Norm invariant, so gibt es zu jedem $\alpha \in K$ ein $\varepsilon_\alpha \in K$ mit $N(\varepsilon_\alpha) = 1$ und $\varphi(\alpha) = \varepsilon_\alpha \cdot \alpha$. Ist φ eine lineare Abbildung, so genügt es, die Faktoren ε_1 und ε_2 der Basis ϑ_1, ϑ_2 zu kennen:

$$\varphi(\vartheta_1) = \varepsilon_1\,\vartheta_1\,, \quad \varphi(\vartheta_2) = \varepsilon_2\,\vartheta_2\,.$$

Betrachten wir $\varphi\,(\vartheta_1 + \vartheta_2) = \varepsilon_1\,\vartheta_1 + \varepsilon_2\,\vartheta_2$, so ist

$$N\,(\vartheta_1 + \vartheta_2) = N\,(\varepsilon_1\,\vartheta_1 + \varepsilon_2\,\vartheta_2)\,.$$

Hieraus ergibt sich

$$\vartheta_1\,\vartheta_2' + \vartheta_1'\,\vartheta_2 = \varepsilon_1\,\varepsilon_2'\,\vartheta_1\,\vartheta_2' + \varepsilon_1'\,\varepsilon_2\,\vartheta_1'\,\vartheta_2\,. \tag{1}$$

Spur und Norm von $\varepsilon_1\,\varepsilon_2'\,\vartheta_1\,\vartheta_2'$ und $\vartheta_1\,\vartheta_2'$ stimmen also überein. Daraus folgt

$$\varepsilon_1\,\varepsilon_2'\,\vartheta_1\,\vartheta_2' = \begin{cases} \vartheta_1\,\vartheta_2' \\ \vartheta_1'\,\vartheta_2 \end{cases}$$

und zwar ist $\varepsilon_1\,\varepsilon_2'\,\vartheta_1\,\vartheta_2' = \vartheta_1\,\vartheta_2'$ genau dann, wenn $\varepsilon_1 = \varepsilon_2$.

(2.3) Dem linearen Automorphismus φ von K kann eine Matrix

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

mit rationalen Elementen α, β, γ, δ zugeordnet werden; dies soll bedeuten:

$$\varphi(\vartheta_1) = \delta\,\vartheta_1 - \gamma\,\vartheta_2\,, \quad \varphi(\vartheta_2) = -\beta\,\vartheta_1 + \alpha\,\vartheta_2\,.$$

Satz: Es sei φ ein linearer normerhaltender Automorphismus von K und

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

seine Matrix; die Basis ϑ_1, ϑ_2 soll übergehen in $\varepsilon_1\,\vartheta_1$, $\varepsilon_2\,\vartheta_2$. Dann gilt $\det M = \pm 1$, und zwar

$$\begin{vmatrix} \delta & -\gamma \\ -\beta & \alpha \end{vmatrix} = +1 \quad \text{genau dann, wenn} \quad \varepsilon_1 = \varepsilon_2\,;$$

$$\begin{vmatrix} \delta & -\gamma \\ -\beta & \alpha \end{vmatrix} = -1 \quad \text{genau dann, wenn} \quad \varepsilon_1 \neq \varepsilon_2\,.$$

Beweis: a) Es sei $\varepsilon_1 = \varepsilon_2 = \varepsilon$; wir können schreiben:

$$\begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} \vartheta_1 & \vartheta_1' \\ \vartheta_2 & \vartheta_2' \end{pmatrix} = \begin{pmatrix} \varepsilon\,\vartheta_1 & \varepsilon'\,\vartheta_1' \\ \varepsilon\,\vartheta_2 & \varepsilon'\,\vartheta_2' \end{pmatrix}.$$

Also

$$\begin{vmatrix} \delta & -\gamma \\ -\beta & \alpha \end{vmatrix} \cdot \det \begin{pmatrix} \vartheta_1 & \vartheta_1' \\ \vartheta_2 & \vartheta_2' \end{pmatrix} = \varepsilon\,\varepsilon' \det \begin{pmatrix} \vartheta_1 & \vartheta_1' \\ \vartheta_2 & \vartheta_2' \end{pmatrix}.$$

Folglich

$$\alpha\,\delta - \beta\,\gamma = \varepsilon\,\varepsilon' = 1,$$

denn ϑ_1, ϑ_2 bilden eine Basis, also $\vartheta_1\,\vartheta_2' - \vartheta_2\,\vartheta_1' \neq 0$.

b) Sei $\alpha\,\delta - \beta\,\gamma = +1$. Wir schreiben

$$\begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} \vartheta_1 & \vartheta_1' \\ \vartheta_2 & \vartheta_2' \end{pmatrix} = \begin{pmatrix} \varepsilon_1\,\vartheta_1 & \varepsilon_1'\,\vartheta_1' \\ \varepsilon_2\,\vartheta_2 & \varepsilon_2'\,\vartheta_2' \end{pmatrix}$$

und bilden die Determinante

$$\vartheta_1\,\vartheta_2' - \vartheta_1'\,\vartheta_2 = \varepsilon_1\,\varepsilon_2'\,\vartheta_1\,\vartheta_2' - \varepsilon_1'\,\varepsilon_2\,\vartheta_1'\,\vartheta_2. \tag{2}$$

Für jede normerhaltende lineare Abbildung gilt aber die Gleichung (1) aus (2.2):

$$\vartheta_1\,\vartheta_2' + \vartheta_1'\,\vartheta_2 = \varepsilon_1\,\varepsilon_2'\,\vartheta_1\,\vartheta_2' + \varepsilon_1'\,\varepsilon_2\,\vartheta_1'\,\vartheta_2.$$

Addition von (1) und (2) führt auf

$$2\,\vartheta_1\,\vartheta_2' = 2\,\varepsilon_1\,\varepsilon_2'\,\vartheta_1\,\vartheta_2'.$$

Somit $\varepsilon_1 = \varepsilon_2$.

Der Beweis der zweiten Behauptung verläuft vollständig analog.

Wenn im folgenden von linearen Abbildungen die Rede ist, sind stets solche mit positiver Determinante gemeint.

Insbesondere wird uns der Fall interessieren, dass $\vartheta_1 = 1$ und $\vartheta_2 = -\vartheta = \vartheta^*$, wobei

$$\vartheta = \frac{-b + \sqrt{b^2 - 4\,a\,c}}{2\,a}$$

eine Wurzel des Polynoms

$$a\,x^2 + b\,x + c$$

ist (a, b, c ganzrational und $(a, b, c) = 1$). Ist dann

$$\varepsilon = \varepsilon_1 + \varepsilon_2\,\vartheta^*$$

mit rationalen ε_1, ε_2, so findet man

$$\delta - \gamma\,\vartheta^* = \varepsilon_1 + \varepsilon_2\,\vartheta^*$$

$$-\beta + \alpha\,\vartheta^* = \varepsilon_1\,\vartheta^* + \varepsilon_2\,\vartheta^{*2} = -(c/a)\,\varepsilon_2 + (b/a)\,\varepsilon_2\,\vartheta^* + \varepsilon_1\,\vartheta^*,$$

also:

$$\left.\begin{aligned} \delta &= \varepsilon_1 & -\gamma &= \varepsilon_2 \\ -\beta &= -(c/a)\,\varepsilon_2 & \alpha &= \varepsilon_1 + (b/a)\,\varepsilon_2. \end{aligned}\right\} \tag{3}$$

Jeder Zahl $\varepsilon = \varepsilon_1 + \varepsilon_2\,\vartheta^*$ mit $N(\varepsilon) = 1$ ist durch diese Gleichungen eine unimodulare Matrix

$$\begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix} \quad \text{mit} \quad \begin{aligned} \beta &= -(c/a)\,\gamma, \\ \alpha &= \delta - (b/a)\,\gamma \end{aligned}$$

zugeordnet. Umgekehrt bestimmt jede solche Matrix eine Zahl $\delta - \gamma\,\vartheta^*$ der Norm 1.

(2.4) Sind die Elemente einer solchen Matrix ganzrationale Zahlen, so ist die zugehörige Zahl $\varepsilon = \delta - \gamma\,\vartheta^*$ eine ganze Zahl aus K, d.h. eine Einheit.

Beweis: Es ist nur noch zu zeigen, dass die Spur ganz ist:

$$S(\varepsilon) = (\delta - \gamma\,\vartheta^*) + (\delta - \gamma\,\vartheta^{*\prime}) = 2\,\delta - (b/a)\,\gamma = \alpha + \delta\,.$$

(2.5) Einer Einheit $\varepsilon = \varepsilon_1 + \varepsilon_2\,\vartheta^*$ ist offenbar genau dann eine ganzzahlige unimodulare Matrix zugeordnet, wenn ε_1 und ε_2 ganz sind und ε_2 durch a teilbar ist (da $(a, b, c) = 1$).

Behauptung: Falls $D = 4\,a\,c - b^2$ quadratfrei ist, ist jeder Einheit von $K = Q(\sqrt{-D})$ eine ganzzahlige Matrix zugeordnet; in diesem Fall sind also ε_1 und ε_2 ganz und ε_2 durch a teilbar.

Beweis: Weil D quadratfrei ist, ist b ungerade, also $D \equiv -1 \pmod 4$. Die ganzen Zahlen in $Q(\sqrt{-D})$ sind genau die Zahlen $(u + v\sqrt{-D})/2$ mit ganzrationalen u und v und $u \equiv -D\,v \pmod 2$.

In unserer speziellen Basis 1, ϑ^* hat die Zahl $g = (u + v\sqrt{-D})/2$ die Form

$$g = g_1 + g_2\,\vartheta^* = \frac{u + b\,v}{2} - a\,v\,\vartheta^*\,. \tag{4}$$

Ist also g ganz, so sind g_1 und g_2 ganzrational und $a \mid g_2$.

Ist $D = 4\,a\,c - b^2$ nicht quadratfrei, also $D = A^2\,D'$ mit quadratfreiem D', so sind diejenigen Zahlen $(u + v\sqrt{d})/2$ in $Q(\sqrt{-D}) = Q(\sqrt{-D'})$ ganz, für welche gilt:

$$u, v \text{ ganzrational}, \quad u \equiv dv \pmod 2$$

$$d = \begin{cases} -D' & \text{falls} \quad -D' \equiv 1 \pmod 4 \\ -4\,D' & \text{falls} \quad -D' \equiv 2, 3 \pmod 4\,. \end{cases}$$

Bezüglich unserer Basis 1, ϑ^* haben diese die Darstellung

$$g_1 + g_2\,\vartheta^* = \begin{cases} \dfrac{u + (b\,v)/A}{2} - \dfrac{a\,v}{A}\,\vartheta^* & \text{für} \quad -D' \equiv 1 \\ \dfrac{u + (2\,b\,v)/A}{2} - \dfrac{2\,a\,v}{A}\,\vartheta^* & \text{für} \quad -D' \equiv 2, 3\,. \end{cases} \tag{5}$$

Behauptung: Sei $-D' \equiv 1$ (4). g_1 und g_2 sind ganzrational und $a \mid g_2$ genau dann, wenn $A \mid v$.

Beweis: Man sieht sofort, dass $A \mid v$ notwendig ist. Zum Beweis der Umkehrung unterscheiden wir zwei Fälle:

(1) A ungerade. Dann ist

$$u \equiv dv = \frac{b^2 - 4\,a\,c}{A^2}\,v \pmod 2\,, \quad A^2\,u \equiv b^2\,v\,, \quad u \equiv b\,v/A\,.$$

Es ist also $g_1 = (u + b\,v/A)/2$ ganzrational.

(2) A gerade. Dann ist

$$0 \equiv D = 4\,a\,c - b^2 \pmod 2\,,$$

also

$$b^2 \equiv 0\,, \quad b \equiv 0\,.$$

Wegen $A \mid v$ ist auch v gerade, also $u \equiv dv \equiv 0$ (2). Und damit ist wieder

$$u \equiv b\, v/A \pmod 2$$

oder $g_1 = (u + b\, v/A)/2$ ganzrational.

Nun sei $-D' \equiv 2, 3 \pmod 4$. Als notwendig erkennt man jetzt: $A \mid 2\, v$. Dies ist aber auch hinreichend:

a) Wenn $A \mid v$, so ist es trivial.

b) Wenn $A \nmid v$, $A \mid 2\, v$, so ist A gerade, also auch $D = A^2\, D'$ und damit auch b und b $(2\, v/A)$.

u wird als gerade vorausgesetzt, also sind wir fertig.

(2.6) Nun beachten wir, dass in $Q(\sqrt{-D'})$ (D' quadratfrei) eine Zahl $(u + v\sqrt{d})/2$ genau dann eine Einheit mit positiver Norm ist, wenn u, v ganzzahlige Lösungen der Pellschen Gleichung

$$\frac{u^2 - d\, v^2}{4} = 1$$

sind (d definiert wie oben). Für alle Diskriminanten D, deren quadratfreier Kern D' ist, sind wir in ein und demselben quadratischen Zahlkörper $Q(\sqrt{-D'})$. Die obigen Betrachtungen lehren nun, dass genau denjenigen Einheiten $(u + v\sqrt{d})/2$ ganzzahlige Matrizen der gewünschten Art zugeordnet sind, bei denen u und v ganzrationale Lösungen der Pellschen Gleichung $(u^2 + Dv^2)/4 = 1$ sind. Die Matrixelemente $\alpha, \beta, \gamma, \delta$ berechnen sich dann nach den Formeln

$$\begin{aligned} \delta &= (u + b\, v)/2 & -\gamma &= -a\, v \\ -\beta &= c\, v & \alpha &= (u - b\, v)/2 . \end{aligned}$$

Dies folgt aus den Formeln (3), (4) und (5).

§3. Anwendung auf quadratische Formen

Wir betrachten binäre quadratische Formen

$$a\, x^2 + b\, x\, y + c\, y^2$$

mit ganzrationalen Koeffizienten a, b, c. Eine lineare Substitution

$$x = \alpha\, x' + \beta\, y', \quad y = \gamma\, x' + \delta\, y'$$

(wir werden sie als Matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ schreiben) mit ganzrationalen α, β, γ, δ und $\alpha\,\delta - \beta\,\gamma = 1$ führt die Form über in eine äquivalente Form

$$a'\, x'^2 + b'\, x'\, y' + c'\, y'^2 .$$

Ist hierbei $a = a'$, $b = b'$, $c = c'$, so heisst die Substitution ein Automorphismus der Form. Beim Studium der Automorphismen kann man sich auf primitive Formen $a\, x^2 + b\, x\, y + c\, y^2$ beschränken, d.h auf Formen mit $(a, b, c) = 1$. Falls nämlich $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}) = t$ und $\boldsymbol{a} = at$, $\boldsymbol{b} = bt$, $\boldsymbol{c} = ct$, so sind die Automorphismen der imprimitiven Form $\boldsymbol{a}\, x^2 + \boldsymbol{b}\, x\, y + \boldsymbol{c}\, y^2$ durch die der zugehörigen primitiven Form $a\, x^2 + b\, x\, y + c\, y^2$ gegeben.

Nun schreiben wir die Form als Norm in einem quadratischen Zahlkörper:

$$a\,x^2 + b\,x\,y + c\,y^2 = a\,(x - \vartheta\,y)\,(x - \vartheta'\,y) = a\,N\,(x - \vartheta\,y) = a\,N\,(x + \vartheta^*\,y)$$

wobei

$$-\vartheta^* = \vartheta = \frac{-b + \sqrt{b^2 - 4\,a\,c}}{2\,a} = \frac{-b + \sqrt{-D}}{2\,a}.$$

Aus der linearen Algebra ist bekannt, dass einer linearen Substitution

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

der «Koordinaten» eine lineare Abbildung von $K = Q(\sqrt{-D})$ auf sich entspricht, deren Matrix durch

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

gegeben ist. Diese Abbildung führt $N\,(x - \vartheta\,y) = N(x, y)$ über in $N\,(\varepsilon_1\,x - \varepsilon_1\,\vartheta\,y) = \boldsymbol{N}(x, y)$. Ist dabei

$$N(x, y) = \boldsymbol{N}(x, y)$$

für alle x, y und sind $\alpha, \beta, \gamma, \delta$ ganzrational, so ist die Substitution

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

ein Automorphismus von $a\,x^2 + b\,x\,y + c\,y^2$ und umgekehrt. Damit ist die Verbindung zu unseren Überlegungen im § 2 hergestellt, und die Resultate von (2.6) besagen für Automorphismen binärer quadratischer Formen:

Die Substitution

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

ist genau dann ein Automorphismus der primitiven Form

$$a\,x^2 + b\,x\,y + c\,y^2,$$

wenn

$$\alpha = (u - b\,v)/2, \quad \beta = -c\,v,$$
$$\gamma = a\,v, \quad \delta = (u + b\,v)/2,$$

wobei u, v ganzzahlige Lösungen der Pellschen Gleichung

$$\frac{u^2 + D\,v^2}{4} = 1$$

sind.

Dieses Ergebnis wurde von GAUSS durch Rechnung hergeleitet.

P. HAFNER, Zürich

LITERATUR

C. F. GAUSS, *Disquisitiones arithmeticae* (1801) in Werke, Bd. 1, Göttingen 1870 (§ 162, pp. 129–134).

P. G. LEJEUNE DIRICHLET/R. DEDEKIND, *Vorlesungen über Zahlentheorie*, 4. Aufl., Braunschweig 1894 (§ 52, pp. 149–152).

H. HASSE, *Vorlesungen über Zahlentheorie*, Berlin, Göttingen, Heidelberg 1950.