Untergruppen der Modulgruppe – Teil 2

Ausarbeitung zum Seminar zur Funktionentheorie II

Vortrag am 04.10.12

Christian Kohl

Nicht immer möchte man, dass eine Funktion auf der oberen Halbebene modular bezüglich der ganzen Modulgruppe ist, sondern lediglich bezüglich einer Untergruppe derselben. Daher werden ausgehend von den Erkenntnissen des Vortrages „Untergruppen der Modulgruppe – Teil 1“ wichtige Untergruppen von Γ untersucht, die sogenannten Kongruenzgruppen. Dies sind jene Untergruppen der Modulgruppe, die eine Hauptkongruenzuntergruppe enthalten. Besonderes Augenmerk wird hierbei auf die Kongruenzgruppen der Stufe 2 gelegt. Im Anschluss erfahren die endlichen Untergruppen der Modulgruppe eine Charakterisierung.

Zunächst müssen indes einige speziellere Ergebnisse über symmetrisch positiv definite Matrizen hergeleitet werden.

In der gesamten Ausarbeitung werden die Bezeichungen wie im Werk [2007] verwendet.

§ 1 Operationen der $\mathrm{GL}_2(\mathbb{R})$

— *Operation der* $\mathrm{GL}_2(\mathbb{R})$ *auf* $\mathbb{H}$ —

(1.1) Satz
Die Gruppe $\mathrm{GL}_2(\mathbb{R})$ operiert auf $\mathbb{H}$ durch

$$M\langle\tau\rangle = \begin{cases} M\tau, & \text{falls } \det(M) > 0 \\ M\overline{\tau}, & \text{falls } \det(M) < 0, \end{cases} \qquad M \in \mathrm{GL}_2(\mathbb{R}),\ \tau \in \mathbb{H}.$$

Beweis

- Wegen
$$\mathrm{Im}(M\tau) = \frac{\det(M)}{|c\tau + d|^2}\,\mathrm{Im}(\tau) \quad \text{für } M \in \mathrm{GL}_2(\mathbb{R}),\ \tau \in \mathbb{H}$$
gilt $\mathrm{Im}(M\langle\tau\rangle) = \frac{\det(M)}{|c\tau+d|^2}\,\mathrm{Im}(\tau) \in \mathbb{H}$ für $M \in \mathrm{GL}_2(\mathbb{R})$, $\tau \in \mathbb{H}$, falls $\det(M) > 0$. Für $\det(M) < 0$ ist $\mathrm{Im}(M\langle\tau\rangle) = \frac{\det(M)}{|c\tau+d|^2}\,\mathrm{Im}(\overline{\tau}) = \frac{|\det(M)|}{|c\tau+d|^2}\,\mathrm{Im}(\tau) \in \mathbb{H}$. Daher gilt für alle $M \in \mathrm{GL}_2(\mathbb{R})$ und $\tau \in \mathbb{H}$, dass $M\langle\tau\rangle \in \mathbb{H}$.
- Offenbar ist E das Einselement.
- Es müssen für $L = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right), M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ die vier verschiedenen Fälle
  (i) $\det(L) > 0$ und $\det(M) > 0$,

(ii) $\det(L) < 0$ und $\det(M) > 0$,

(iii) $\det(L) > 0$ und $\det(M) < 0$,

(iv) $\det(L) < 0$ und $\det(M) < 0$

nachgerechnet werden. Wir wollen uns hier lediglich auf einen beschränken, da die anderen Fälle analog abgehandelt werden können. Sei daher $\det(L) > 0$ und $\det(M) < 0$ und damit auch $\det(LM) < 0$. Dann gilt

$$\begin{aligned} L\langle M\langle\tau\rangle\rangle = L\left\langle \frac{a\overline{\tau}+b}{c\overline{\tau}+d}\right\rangle &= \frac{\alpha\left(\frac{a\overline{\tau}+b}{c\overline{\tau}+d}\right)+\beta}{\gamma\left(\frac{a\overline{\tau}+b}{c\overline{\tau}+d}\right)+\delta} = \frac{\alpha(a\overline{\tau}+b)+\beta(c\overline{\tau}+d)}{\gamma(a\overline{\tau}+b)+\delta(c\overline{\tau}+d)} \\ &= \frac{(\alpha a+\beta c)\overline{\tau}+ab+\beta d}{(\gamma a+\delta c)\overline{\tau}+\gamma b+\delta d} \\ &= \begin{pmatrix}\alpha a+\beta c & ab+\beta d\\ \gamma a+\delta c & \gamma b+\delta d\end{pmatrix}\langle\tau\rangle = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\langle\tau\rangle = (LM)\langle\tau\rangle \end{aligned}$$

Insgesamt gilt also (nach Verifikation aller Fälle):

$$(LM)\langle\tau\rangle = L\langle M\langle\tau\rangle\rangle. \tag{1}$$

Damit folgt die Behauptung. □

— *Eigenschaften symmetrisch positiv definiter* 2×2*-Matrizen und die Operation der* $\mathrm{GL}_2(\mathbb{R})$ *auf* $\mathrm{Pos}_2(\mathbb{R})$ —

(1.2) Definition

(a) Eine reelle 2×2-Matrix

$$S = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathbb{R}^{2\times 2}$$

heißt *positiv definit*, falls für alle $x \in \mathbb{R}^2\backslash\{(0,0)^t\}$ gilt $x^tSx > 0$.

(b) Die Menge der symmetrisch positiv definiten 2×2-Matrizen über $\mathbb{R}$ bezeichnen wir mit $\mathrm{Pos}_2(\mathbb{R})$.

Es gilt:

(1.3) Lemma
S ist genau dann aus $\mathrm{Pos}_2(\mathbb{R})$, wenn

$$S = \begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix} \in \mathbb{R}^{2\times 2}, \quad \det(S) = \alpha\gamma - \beta^2 > 0, \quad \alpha > 0.$$

Beweis
Die Behauptung folgt mit $x = (x_1, x_2)^t$ aus

$$\alpha \cdot x^t S x = \alpha^2 x_1^2 + 2\alpha\beta x_1 x_2 + \alpha\gamma x_2^2 = (\alpha x_1 + \beta x_2)^2 + (\alpha\gamma - \beta^2)x_2^2$$
$$\Leftrightarrow x^t S x = \underbrace{\frac{(\alpha x_1 + \beta x_2)^2}{\alpha}}_{>0,\text{ da }\alpha>0} + \underbrace{\frac{(\alpha\gamma - \beta^2)}{\alpha}}_{>0,\text{ nach Vor.}} x_2^2.$$

Jetzt muss noch für die Hinrichtung gezeigt werden, dass $\alpha \neq 0$ (für Rückrichtung klar): Sei dazu $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{Pos}_2(\mathbb{R})$. Wähle $x = (1,0)^t$. Dann gilt $0 < x^t M x = \alpha$. □

Man setze

$$w : \mathrm{Pos}_2(\mathbb{R}) \longrightarrow \mathbb{H},\ S \mapsto w(S) := \frac{1}{\alpha}\left(-\beta + i\sqrt{\det(S)}\right).$$

Anwenden der pq-Formel liefert die

(1.4) Proposition
Für $S \in \mathrm{Pos}_2(\mathbb{R})$ ist $w = w(S)$ die eindeutig bestimme Lösung $w \in \mathbb{H}$ der Gleichung

$$\alpha w^2 + 2\beta w + \gamma = 0.$$

Bekanntlich operiert die Gruppe $\mathrm{GL}_2(\mathbb{R})$ auf $\mathrm{Pos}_2(\mathbb{R})$ vermöge

$$(M, S) \mapsto M * S := (M^{-1})^t S M^{-1}.$$

Diese Operation ist mit der Operation von $\mathrm{GL}_2(\mathbb{R})$ auf $\mathbb{H}$ gemäß des letzten Abschnittes verträglich:

(1.5) Satz
Für $M \in \mathrm{GL}_2(\mathbb{R})$, $S \in \mathrm{Pos}_2(\mathbb{R})$ und $\tau \in \mathbb{H}$ gilt:

$$w(M * S) = M\langle w(S)\rangle.$$

Beweis
Sei $\tilde{w} = w(M * S)$, $w = w(S)$, $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $M * S = \left(\begin{smallmatrix} \tilde{\alpha} & \tilde{\beta} \\ \tilde{\gamma} & \tilde{\delta} \end{smallmatrix}\right)$. Es gilt:

$$\begin{aligned} &\begin{pmatrix} \tilde{w} & 1 \end{pmatrix} (M^{-1})^t S M^{-1} \begin{pmatrix} \tilde{w} \\ 1 \end{pmatrix} = \begin{pmatrix} \tilde{w} & 1 \end{pmatrix} (M * S) \begin{pmatrix} \tilde{w} \\ 1 \end{pmatrix} = \begin{pmatrix} \tilde{w} & 1 \end{pmatrix} \begin{pmatrix} \tilde{\alpha} & \tilde{\beta} \\ \tilde{\gamma} & \tilde{\delta} \end{pmatrix} \begin{pmatrix} \tilde{w} \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} \tilde{\alpha}\tilde{w} + \tilde{\beta} & \tilde{\beta}\tilde{w} + \tilde{\gamma} \end{pmatrix} \begin{pmatrix} \tilde{w} \\ 1 \end{pmatrix} = \tilde{\alpha}\tilde{w}^2 + \tilde{\beta}\tilde{w} + \tilde{\beta}\tilde{w} + \tilde{\gamma} = \tilde{\alpha}\tilde{w}^2 + 2\tilde{\beta}\tilde{w} + \tilde{\gamma} \overset{(1.4)}{=} 0. \end{aligned}$$

Außerdem gilt mit $M^{-1} = \det(M)^{-1} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$:

$$M^{-1} \begin{pmatrix} \tilde{w} \\ 1 \end{pmatrix} = \det(M)^{-1} \begin{pmatrix} d\tilde{w} - b \\ -c\tilde{w} + a \end{pmatrix} \overset{\tilde{w} \in \mathbb{H}}{=} \frac{-c\tilde{w} + a}{\det(M)} \begin{pmatrix} M^{-1}\langle \tilde{w} \rangle \\ 1 \end{pmatrix}$$

Dann folgt mit $z = M^{-1}\langle \tilde{w} \rangle$:

$$\begin{aligned} 0 &= \begin{pmatrix} \tilde{w} & 1 \end{pmatrix} (M^{-1})^t S M^{-1} \begin{pmatrix} \tilde{w} \\ 1 \end{pmatrix} = \frac{(-c\tilde{w} + a)^2}{\det(M)^2} \begin{pmatrix} z & 1 \end{pmatrix} S \begin{pmatrix} z \\ 1 \end{pmatrix} \\ &= \frac{(-c\tilde{w} + a)^2}{\det(M)^2} \cdot (\alpha z^2 + 2\beta z + \gamma), \end{aligned}$$

also wegen (1.4), dass $z = w$. Also schließt man:

$$z = w \Leftrightarrow M^{-1}\langle \tilde{w} \rangle = w(S) \Leftrightarrow M\langle M^{-1}\langle \tilde{w} \rangle \rangle = M\langle w(S) \rangle.$$

Wegen (1) ergibt sich

$$M\langle M^{-1}\langle \tilde{w} \rangle \rangle \overset{(1)}{=} (MM^{-1})\langle \tilde{w} \rangle = E\langle \tilde{w} \rangle \overset{\tilde{w} \in \mathbb{H}}{=} \tilde{w} \overset{\text{Def.}}{=} w(M * S),$$

also insgesamt die Behauptung. □

§ 2 Kongruenzgruppen

Wir erinnern kurz an die Definition der Hauptkongruenzgruppe:

(2.1) Definition
Für $n \geq 1$ nennt man

$$\Gamma[n] := \{M \in \Gamma | M \equiv E \pmod{n}\}$$

Hauptkongruenzgruppe $\pmod{n}$. Die Zahl n nennt man *Stufe* von $\Gamma[n]$.

(2.2) Definition
Eine Untergruppe Λ von Γ heißt eine *Kongruenzgruppe*, wenn es ein $n \geq 1$ gibt mit $\Gamma[n] \subset \Lambda$. Das kleinste derartige n heißt *Stufe* von Λ.

Wir wissen bereits aus [2007](II, § 3.2, Satz), dass $[\Gamma : \Gamma[n]] < \infty$ gilt. Da für jede Kongruenzgruppe Λ gilt, dass $\Gamma[n] \subset \Lambda$, ist der Index von Λ in Γ kleiner als der von $\Gamma[n]$ in Γ, also insbesondere endlich.

Wir betrachen direkt eine wichtige Klasse von Beispielen und eine erste Anwendung.

— *Die Untergruppen* $\Gamma_0[n]$ *und* $\Gamma^0[n]$ —

(2.3) Definition und Lemma
Die Mengen

$$\Gamma_0[n] := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,\middle|\, c \equiv 0 \pmod{n} \right\}$$

$$\Gamma^0[n] := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,\middle|\, b \equiv 0 \pmod{n} \right\}$$

sind Kongruenzgruppen von Γ und zueinander konjugiert, denn es gilt

$$\Gamma^0[n] = J \cdot \Gamma_0[n] \cdot J^{-1}.$$

Beweis
Für $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), N = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma_0[n]$ gilt

$$MN = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a^2 & a\beta + b\delta \\ c\alpha + d\gamma & d^2 \end{pmatrix} \in \Gamma_0[n],$$

da sowohl $c \equiv 0 \pmod{n}$ als auch $\gamma \equiv 0 \pmod{n}$. Ebenfalls ist M^{-1} in $\Gamma_0[n]$, da

$$M^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \Gamma_0[n],$$

denn mit $c \equiv 0 \pmod{n}$ gilt auch $-c \equiv 0 \pmod{n}$.

Da

$$\begin{aligned} \Gamma[n] :&= \left\{ M \in \Gamma \;\middle|\; M \equiv E \pmod{n} \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; a \equiv d \equiv 1 \pmod{n}, \quad b \equiv c \equiv 0 \pmod{n} \right\}, \end{aligned}$$

gilt $\Gamma[n] \subset \Gamma_0[n]$. Damit ist $\Gamma_0[n]$ eine Kongruenzgruppe. Analog erhält man das Ergebnis für $\Gamma^0[n]$.

Die Konjugationsaussage folgt, da zum einen

$$JMJ^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \in \Gamma^0[n] \qquad \text{für } M \in \Gamma_0[n],$$

zum anderen, weil für $M \in \Gamma^0[n]$ die Matrix

$$L = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

in $\Gamma_0[n]$ liegt und die Gleichung $M = JLJ^{-1}$ erfüllt. □

Bevor wir uns beispielhaft dem Fall $n = 2$ widmen, erinnern wir an zwei Ergebnisse des letzten Vortrages:

(2.4) Satz
Die Faktorgruppe $\Gamma/\Gamma[n]$ ist isomorph zu $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

(2.5) Beispiel
Ein Vertretersystem der Rechtsnebenklassen von $\Gamma[2]$ in Γ ist gegeben durch

$$\begin{pmatrix}1&0\\0&1\end{pmatrix} = E, \quad \begin{pmatrix}1&1\\0&1\end{pmatrix} = T, \quad \begin{pmatrix}1&0\\1&1\end{pmatrix} = -UT,$$
$$\begin{pmatrix}0&-1\\1&0\end{pmatrix} = J, \quad \begin{pmatrix}-1&1\\-1&0\end{pmatrix} = U, \quad \begin{pmatrix}0&-1\\1&-1\end{pmatrix} = U^2.$$

Zudem seien hier noch einmal die Elemente der $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ angegeben:

$$\begin{aligned}\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) &= \left\{ \begin{pmatrix}\overline{1}&\overline{0}\\\overline{0}&\overline{1}\end{pmatrix}, \begin{pmatrix}\overline{1}&\overline{1}\\\overline{0}&\overline{1}\end{pmatrix}, \begin{pmatrix}\overline{1}&\overline{0}\\\overline{1}&\overline{1}\end{pmatrix}, \begin{pmatrix}\overline{0}&\overline{1}\\\overline{1}&\overline{0}\end{pmatrix}, \begin{pmatrix}\overline{1}&\overline{1}\\\overline{1}&\overline{0}\end{pmatrix}, \begin{pmatrix}\overline{0}&\overline{1}\\\overline{1}&\overline{1}\end{pmatrix} \right\} \\ &= \left\{ \quad \overline{E}, \qquad \overline{T}, \qquad \overline{UT}, \qquad \overline{J}, \qquad \overline{U}, \qquad \overline{U^2} \quad \right\}\end{aligned}$$

Daher hat der Isomorphismus aus (2.4) für $n = 2$ die Form:

(2.6) Korollar
Ein Isomorphismus zwischen $\Gamma/\Gamma[2]$ und $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ ist gegeben durch

$$\begin{aligned}&\tau : \Gamma/\Gamma[2] \longrightarrow \mathrm{SL}_2(\mathbb{Z}\ /2\mathbb{Z}), \\ &\Gamma[2]M \mapsto \overline{M} = \Big\{ \ \Gamma[2]E \mapsto \overline{E}, \quad \Gamma[2]T \mapsto \overline{T}, \quad \Gamma[2](-UT) \mapsto \overline{UT} \\ &\qquad\qquad \Gamma[2]J \mapsto \overline{J}, \quad \Gamma[2]U \mapsto \overline{U}, \quad \Gamma[2]U^2 \mapsto \overline{U^2} \Big\}\end{aligned}$$

Wenden wir uns nun dem Fall $n = 2$ zu.

(2.7) Beispiel
Sei $n = 2$. Ein Vertretersystem der Rechtsnebenklassen von Γ modulo $\Gamma_0[2]$ ist gegeben durch E, J und U^2, d. h.

$$\Gamma = \Gamma_0[2] \cup (\Gamma_0[2] \cdot J) \cup (\Gamma_0[2] \cdot U^2).$$

Beweis
Beispiel (2.5) liefert ein Vertretersystem von $\Gamma[2]$ in Γ. Da $\Gamma[2] < \Gamma_0[2]$ und $\Gamma_0[2] < \Gamma$ folgt mit

$$\Gamma = \Gamma[2] \cup (\Gamma[2] \cdot T) \cup (\Gamma[2] \cdot (-UT)) \cup (\Gamma[2] \cdot J) \cup (\Gamma[2] \cdot U) \cup (\Gamma[2] \cdot U^2)$$

insbesondere

$$\Gamma = \Gamma_0[2] \cup (\Gamma_0[2] \cdot T) \cup (\Gamma_0[2] \cdot (-UT)) \cup (\Gamma_0[2] \cdot J) \cup (\Gamma_0[2] \cdot U) \cup (\Gamma_0[2] \cdot U^2).$$

Aus der Algebra ist bekannt, dass zwei Elemente g, h aus einer Faktorgruppe G/H genau dann in derselben Nebenklasse liegen, wenn $gh^{-1} \in H$ gilt. Daher bleibt nun zu prüfen, für welche $M, L \in \{E, T, -UT, J, U, U^2\}$ gilt: $ML^{-1} \in \Gamma_0[2]$. Offensichtlich liegen $\{E, T\}$ in derselben Nebenklasse. Wegen $JU^{-1} = JU^2$ gilt dies auch für $\{J, U\}$. Da der (2,1)-Eintrag von $-UTU$ kongruent zu 0 modulo 2 ist, liegen auch $\{-UT, U^2\}$ in derselben Nebenklasse. Weiteres Ausrechnen zeigt, dass E, J und U^2 ein Vertretersystem der Rechtsnebenklassen von $\Gamma/\Gamma_0[2]$ bilden. Daher gilt

$$\Gamma = \Gamma_0[2] \cup (\Gamma_0[2] \cdot J) \cup (\Gamma_0[2] \cdot U^2).$$ □

Ein Fundamentalbereich lässt sich nun leicht mittels [2007](II, § 3.1, Satz) konstruieren und es ergibt sich:

$$\mathbb{F}(\Gamma_0[2]) = \overline{\mathbb{F}} \cup J\overline{\mathbb{F}} \cup U^2\overline{\mathbb{F}}.$$

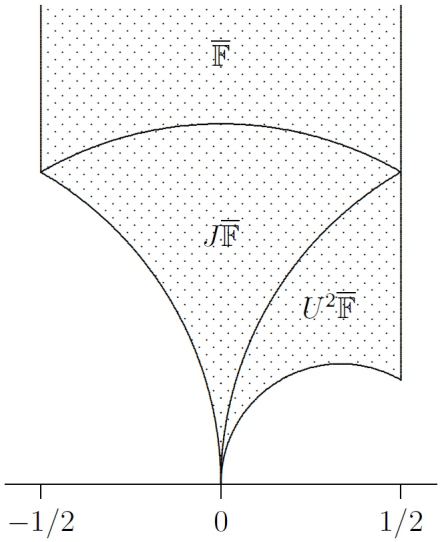

Abbildung 1: Fundamentalbereich von $\Gamma_0[2]$

Nun soll ein Vertretersystem von Rechtsnebenklassen von $\Gamma_0[2]$ modulo $\Gamma[2]$ bestimmt werden. Wegen (2.7) ist der Index von $\Gamma_0[2]$ in Γ gleich 3. Da $\Gamma[2], \Gamma_0[2] < \Gamma$

und $\Gamma[2] \subset \Gamma_0[2]$, folgt mit dem verallgemeinerten Satz von Lagrange:

$$[\Gamma_0[2] : \Gamma[2]] = \frac{[\Gamma : \Gamma[2]]}{[\Gamma : \Gamma_0[2]]} \overset{(2.5),(2.7)}{=} \frac{6}{3} = 2 \tag{2}$$

Da

$$TE^{-1} = T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \notin \Gamma[2],$$

bilden E, T ein solches Vertretersystem. Also gilt $\Gamma_0[2] = \Gamma[2] \cup (\Gamma[2] \cdot T)$.

(2.8) Bemerkungen

(a) Eine ausführliche Diskussion der Gruppen $\Gamma_0[n]$ bzw. $\Gamma^0[n]$ findet man bei [1982], 241–251.

(b) Man kann zeigen

$$[\Gamma : \Gamma_0[n]] = \left[\Gamma : \Gamma^0[n]\right] = n \prod_{p|n} \left(1 + \frac{1}{p}\right)$$

Ein Beweis findet sich bei [1977], 22–26.

(c) Eine Untergruppe Λ von Γ von endlichem Index braucht keine Kongruenzgruppe zu sein. Erste Beispiele wurden gleichzeitig von R. Fricke und G. Pick (Math. Ann. **28**, 99–118 und 119–124 (1887)) angegeben. Weitere Beispiele findet man bei [1983], 77–79, und H. Petersson (J. Reine Angew. Math. **250**, 182-212 (1971); **268/9**, 94-109 (1974)).

(d) $\Gamma_0[n]$ und $\Gamma^0[n]$ sind für $n > 1$ keine Normalteiler.

Beweis

(d) Man betrachte zunächst den Fall $\Gamma_0[n]$: Für $n > 1$ ist sicherlich

$$M = T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0[n].$$

Gülte $\Gamma_0[n] \triangleleft \Gamma$, so müsste insbesondere JMJ^{-1} wieder in $\Gamma_0[n]$ sein. Es gilt aber $JMJ^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right) \notin \Gamma_0[n]$.

Das analoge Ergebnis für $\Gamma^0[2]$ erhält man mit $M = T^t$. □

— *Kongruenzgruppen der Stufe* 2 —

Die Kongruenzgruppen der Stufe 2 sind genau die echten Untergruppen Λ von Γ, die $\Gamma[2]$ enthalten, denn $\Gamma[2] \subset \Lambda$ und $\Gamma = \Gamma[1] \not\subset \Lambda$, wohingegen für die trivialen Untergruppen gilt: $\Gamma[2] \not\subset \{E\}$ und $\Gamma[1] \subseteq \Gamma$ (und somit Γ eine Kongruenzgruppe der Stufe 1 ist).

(2.9) Satz
(a) $\Gamma/\Gamma[2]$ ist isomorph zur Permutationsgruppe S_3.

(b) $\Gamma[2]$ wird erzeugt von den Matrizen $-E, T^2$ und JT^2J^{-1}.

Beweis
(a) Wir wissen nach (2.4) bereits, dass $\Gamma/\Gamma[2] \cong \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ gilt. Sei nun $E := \left\{ \left(\frac{\bar{1}}{\bar{0}}\right), \left(\frac{\bar{0}}{\bar{1}}\right), \left(\frac{\bar{1}}{\bar{1}}\right) \right\} \subset (\mathbb{Z}/2\mathbb{Z})^2$. Um nachzuweisen, dass die $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ via Linksmultiplikation E permutiert, betrachte man die Abbildung

$$\varphi : \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathrm{S}(E),\ M \mapsto (\sigma : E \longrightarrow E,\ e \mapsto Me).$$

Aus der Algebra wissen wir, dass ein Isomorphismus π zwischen $\mathrm{S}(E)$ und S_3 besteht. Durch einfaches Ausrechnen erhält man:

$$\begin{aligned} \pi \circ \varphi : \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) &\longrightarrow S_3, \\ &\left\{ \overline{E} \mapsto \mathrm{id}, \overline{T} \mapsto (2,3), \overline{UT} \mapsto (1,3), \right. \\ &\left. \overline{J} \mapsto (1,2), \overline{U} \mapsto (1,2,3), \overline{U^2} \mapsto (1,3,2) \right\} \end{aligned}$$

Daher ist φ injektiv. Surjektiv ist die Abbildung deshalb, weil die $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ und die S_3 beide Ordnung sechs haben. Die Abbildung ist offensichtlich ein Homomorphismus. Daher sind $\Gamma/\Gamma[2]$ und S_3 isomorph. Mit dem Isomorphismus τ aus (2.6) gilt daher

$$\begin{aligned} \psi := \pi \circ \varphi \circ \tau : \Gamma/\Gamma[2] &\longrightarrow S_3, \\ &\{\Gamma[2]E \mapsto \mathrm{id}, \Gamma[2]T \mapsto (2,3), \Gamma[2](-UT) \mapsto (1,3), \\ &\Gamma[2]J \mapsto (1,2), \Gamma[2]U \mapsto (1,2,3), \Gamma[2]U^2 \mapsto (1,3,2)\}. \end{aligned}$$

(b) Sei $\Lambda := \langle -E, T^2, JT^2J^{-1} \rangle \leq \Gamma[2]$.

„$\subseteq$:“ Klar.

„$\supseteq$:“ Sei $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma[2]$. Iterativ findet man nach endlich vielen Schritten eine Matrix $L \in \Lambda$ mit der gilt:

$$LM = \pm \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}.$$

Da $L \in \Lambda \leq \Gamma[2]$, ist $LM \in \Gamma[2]$ und damit r gerade. Dann ist M aber auch aus Λ, denn es gilt entweder $LM = T^r \in \Lambda$ oder $LM = -E \cdot T^r \in \Lambda$.

Der Algorithmus 1 liefert gerade das gewünschte L. (Beachte: Es gilt entweder $|a| < |c|$ oder $|a| > |c|$, da wegen $M \in \Gamma[2]$ der Eintrag a immer ungerade und c immer gerade ist):

Setze $L = E$ und $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ und $LM = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$.
while $(|\alpha| \neq 1) \wedge (\gamma \neq 0)$ **do**
  if $|\alpha| > |\gamma|$ **then**
    Es existiert eine Matrix $L_i \in \{T^{2m} \mid m \in \mathbb{Z}\}$, so dass $|\alpha| < |\gamma|$, denn

$$\left(T^2\right)^m LM = T^{2m} LM = \begin{pmatrix} 1 & 2m \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha + 2m\gamma & \beta + 2m\delta \\ \gamma & \delta \end{pmatrix}$$

    Setze $L = L_i \cdot L$.
  else
    Es existiert eine Matrix $L_i \in \{\left(JT^2J^{-1}\right)^m \mid m \in \mathbb{Z}\}$, so dass $|\alpha| > |\gamma|$, denn

$$\left(JT^2J^{-1}\right)^m LM = \begin{pmatrix} 1 & 0 \\ -2m & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma - 2m\alpha & \delta - 2m\beta \end{pmatrix}$$

    Setze $L = L_i \cdot L$
  end
end

Algorithm 1: Auffinden eines geeigneten L

Weil $LM \in \Gamma[2]$, reicht die Abbruchbedingung „$(|\alpha| \neq 1)$ und $(\gamma \neq 0)$“ aus, denn aus $\det(LM) = 1$ folgt direkt $\delta = 1$. Außerdem terminiert der Algorithmus, da $a, c < \infty$ und alle Ungleichungen strikt sind. □

Dann folgt auch das

(2.10) Korollar
Die Untergruppen von Γ, die $\Gamma[2]$ enthalten, stehen in Bijektion zu den Untergruppen von $\Gamma/\Gamma[2]$, also von S_3. Die Bijektion ist gegeben durch

$$\begin{aligned}\eta:\ &\{\Lambda \leq \Gamma \mid \Gamma[2] \subseteq \Lambda\} \longrightarrow \mathcal{S} \leq S_3,\\ &\{\Gamma[2] \mapsto \{\mathrm{id}\},\\ &\langle \Gamma[2], \Gamma[2]T\rangle \mapsto \{\mathrm{id}, (2,3)\} = \langle (2,3)\rangle\\ &\langle \Gamma[2], \Gamma[2](-UT)\rangle \mapsto \{\mathrm{id}, (1,3)\} = \langle (1,3)\rangle\\ &\langle \Gamma[2], \Gamma[2]J\rangle \mapsto \{\mathrm{id}, (1,2)\} = \langle (1,2)\rangle\\ &\langle \Gamma[2], \Gamma[2]U, \Gamma[2]U^2\rangle \mapsto \{\mathrm{id}, (1,2,3), (1,3,2)\} = \langle (1,2,3)\rangle\\ &\Gamma \mapsto S_3\}\end{aligned}$$

Die trivialen Untergruppen von S_3 entsprechen damit $\Gamma[2]$ und Γ.

Beweis
Nach Algebra existiert, da $\Gamma[2]$ ein Normalteiler in Γ ist, eine solche, inklusionserhaltende Bijektion. Die Abbildung η leistet das Gewünschte, da die angegebenen Untergruppen der Gruppe Γ durch den Isomorphismus (2.9a) bei elementweiser Anwendung bijektiv auf Untergruppen der S_3 abgebildet werden. Umgekehrt werden von η^{-1} die Elemente einer Untergruppe von S_3 durch (2.9a) auf die entsprechenden Restklassen abgebildet. □

Wie wir im nächsten Theorem beispielhaft feststellen werden, ist die obige Bijektion η nicht nur durch das jeweilige Erzeugnis (z. B. $\langle \Gamma[2], \Gamma[2]J\rangle$), sondern auch direkt durch die Vereinigung (z. B. $\Gamma[2] \cup \Gamma[2]J$) gegeben.

— *Die Theta-Gruppe* Γ_ϑ —

Bevor wir uns den Untergruppen der Ordnung zwei und drei widmen, führen wir eine Defintion und ein Lemma ein.

(2.11) Definition und Lemma
Die Gruppe $\Gamma_\vartheta := \Gamma[2] \cup \Gamma[2]J$ heißt *Theta-Gruppe* und wird erzeugt von den Matrizen J und T^2.

Beweis
Wegen (2.9) kennen wir die Erzeuger von $\Gamma[2]$. Damit bestimmen wir zunächst die Erzeuger von $\langle \Gamma[2], \Gamma[2]J \rangle$:

$$\langle \Gamma[2], \Gamma[2]J \rangle = \langle \underbrace{-E, T^2, JT^2J^{-1}}_{\text{Erzeuger von } \Gamma[2]}, \underbrace{-J, T^2J, JT^2J^{-1}J}_{\text{Erzeuger von } \Gamma[2]J} \rangle.$$

Da mit $J^2 = -E$ auch $-J = J^{-1}$ gilt, ergeben sich als Erzeuger gerade J und T^2. Da leichtes Nachrechnen ergibt, dass Γ_ϑ ebenfalls eine Kongruenzgruppe ist, die die obigen Erzeuger enthält, folgt, dass $\langle \Gamma[2], \Gamma[2]J \rangle \subseteq \Gamma_\vartheta$. Da $\psi(J) = (1,2)$ und $\psi(T^2) = \psi(\overline{T^2}) = \psi(E) = \mathrm{id}$, ψ wie in (2.9a), folgt wegen der Bijektion in (2.10), dass $\Gamma_\vartheta = \langle \Gamma[2], \Gamma[2]J \rangle$. Damit folgt die Behauptung. □

(2.12) Korollar
Die Gruppe S_3 besitzt drei Untergruppen der Ordnung 2. Diese entsprechen den Kongruenzgruppen

$$\Gamma_0[2], \Gamma^0[2] \text{ und } \Gamma_\vartheta.$$

Beweis
Für Γ_ϑ stimmt die Behauptung nach (2.11). Analog erhält man die Ergebnisse $\Gamma_0[2] = \langle \Gamma[2], \Gamma[2]T \rangle$ und $\Gamma^0[2] = \langle \Gamma[2], \Gamma[2](-UT) \rangle$. □

Wir geben nun eine Charakterisierung der Theta-Gruppe.

(2.13) Lemma
Für $M \in \Gamma$ gilt $M \in \Gamma_\vartheta$ genau dann, wenn

$$M \equiv E \pmod 2 \quad \text{oder} \quad M \equiv J \pmod 2. \tag{3}$$

Äquivalent kann man hierfür auch

$$a + b + c + d \equiv 0 \pmod 2 \tag{4}$$

schreiben.

Beweis
Die Äquivalenz von $M \in \Gamma_\vartheta$ und (3) ist nach Definition klar.
Zu zeigen bleibt (3) $\Leftrightarrow$ (4).

„⇒:“ Es gilt:

$$M \equiv E \pmod 2 \Leftrightarrow (a \equiv c \equiv 1 \pmod 2) \text{ und } (b \equiv d \equiv 0 \pmod 2)$$

und

$$M \equiv J \pmod 2 \Leftrightarrow (a \equiv c \equiv 0 \pmod 2) \text{ und } (b \equiv d \equiv 1 \pmod 2)$$

Offenbar erfüllt M dann auch die Gleichung (4).

„⇐:“ Es gelte (4). Da $\Gamma_\vartheta \leq \Gamma = \mathrm{SL}_2(\mathbb{Z})$ ist $\det(M) = 1$ und damit entweder

$$(ad \equiv 1 \pmod 2) \text{ und } ((b \equiv 0 \pmod 2) \text{ oder } (c \equiv 0 \pmod 2)) \quad (5)$$

oder

$$(bc \equiv 1 \pmod 2) \text{ und } ((a \equiv 0 \pmod 2) \text{ oder } (d \equiv 0 \pmod 2)) \quad (6)$$

Falls (5) gilt und gleichzeitig $b \equiv 0 \pmod 2$, so gilt ebenfalls

$$0 \overset{\text{Vor.}}{\equiv} a + b + c + d \equiv 1 + 0 + c + 1 \equiv c \pmod 2.$$

Also ist $M \equiv E \pmod 2$. Analog für $c \equiv 0 \pmod 2$.

Falls (6) gilt und gleichzeitig $a \equiv 0 \pmod 2$, so gilt ebenfalls

$$0 \overset{\text{Vor.}}{\equiv} a + b + c + d \equiv 0 + 1 + 1 + d \equiv d \pmod 2.$$

Also ist $M \equiv J \pmod 2$. Analog für $d \equiv 0 \pmod 2$. □

(2.14) Korollar
Γ_ϑ ist eine Untergruppe von Γ vom Index 3 und es gilt

$$\Gamma = \Gamma_\vartheta \cup (T \cdot \Gamma_\vartheta) \cup (U^2 \cdot \Gamma_\vartheta) = \Gamma_\vartheta \cup (\Gamma_\vartheta \cdot T) \cup (\Gamma_\vartheta \cdot U).$$

Beweis
Nach dem verallgemeinerten Satz von Lagrange gilt wegen $\Gamma_\vartheta, \Gamma_0[2] \leq \Gamma$ und $\Gamma_0[2] \subset \Gamma_\vartheta$:

$$[\Gamma : \Gamma_\vartheta] = \frac{[\Gamma : \Gamma[2]]}{[\Gamma_\vartheta : \Gamma[2]]} = \frac{6}{2} = 3.$$

Aufgrund der in (2.9) gezeigten Isomorphie und der Bijektion in (2.10), können die letzten Behauptungen auch in der $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ nachgerechnet werden. Nach (2.3)

gilt, dass Γ_ϑ in der $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ der Menge $\theta := \left\{ \left(\begin{smallmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{smallmatrix}\right), \left(\begin{smallmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{smallmatrix}\right) \right\} = \{\overline{E}, \overline{J}\}$ entspricht. Dann ist die obige Behauptung aber äquivalent zu

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) &\overset{!}{=} \underbrace{\theta \cup \overline{T}\theta \cup \overline{U^2}\theta}_{=:\,(1)} \\ &\overset{!}{=} \underbrace{\theta \cup \theta\overline{T} \cup \theta\overline{U}}_{=:\,(2)}. \end{aligned}$$

Offensichtlich befinden sich in (1) bereits die Elemente $\{\overline{E}, \overline{J}, \overline{T}, \overline{U^2}\}$ und in (2) bereits die Elemente $\{\overline{E}, \overline{J}, \overline{T}, \overline{U}\}$.

Da gilt

$$\begin{aligned} \overline{T} \cdot \overline{J} &= \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} = \overline{U}, \\ \overline{U^2} \cdot \overline{J} &= \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} = \overline{UT}, \\ \overline{J} \cdot \overline{T} &= \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} = \overline{U^2}, \\ \overline{J} \cdot \overline{U} &= \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} = \overline{UT}, \end{aligned}$$

folgt $(1) = \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) = (2)$. □

Nun können wir mit dem Wissen aus dem ersten Vortrag zu „Untergruppen der Modulgruppe“ einen Fundamentalbereich von Γ_ϑ angeben:

$$\mathbb{F}(\Gamma_\vartheta) := \overline{\mathbb{F}} \cup T\overline{\mathbb{F}} \cup U\overline{\mathbb{F}}.$$

Es existiert ebenfalls ein exakter Fundamentalbereich
$\mathbb{F}_\vartheta := \{\tau = x + iy \in \mathbb{H} \mid |\tau| \geq 1, -1 < x \leq 1, |\tau| > 1 \text{ für } -1 < x < 0\}$.

$\mathbb{F}_\vartheta$ ist ein Fundamentalbereich, da $\mathbb{F}(\Gamma_\vartheta)$ ein Fundamentalbereich ist und man durch Verschieben der Menge $\{\tau = x + iy \mid x > 1 \text{ und } \tau \in \mathbb{F}(\Gamma_\vartheta)\}$ mittels der (in Γ_ϑ befindlichen) Matrix T^2 eine Punktmenge erhält, deren offener Kern mit dem von $\mathbb{F}_\vartheta$ übereinstimmt. Die Punkte auf dem Viertelkreis $\{\tau = x + iy \mid x^2 + y^2 = 1,\ -1 < x < 0,\ 0 < y < 1\}$ werden durch J auf das rechte Kreissegment abgebildet.

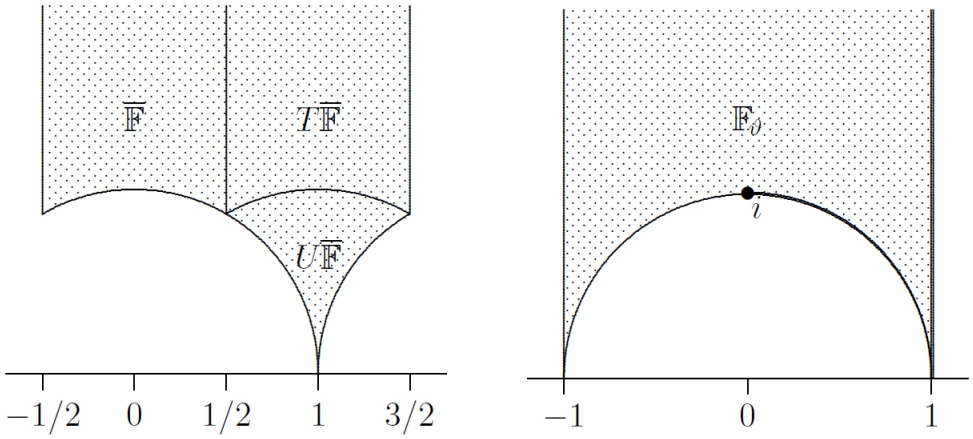

Abbildung 2: Fundamentalbereiche von Γ_ϑ

(2.15) Bemerkungen

(a) Die Benennung der Gruppe Γ_ϑ rührt daher, dass der so genannte *Theta-Nullwert* $\vartheta(\tau) := \vartheta(0;\tau)$ (vgl. [2007](I, § 6.7(1))) sie als „Invarianzgruppe“ besitzt (vgl. Einleitung zu Kapitel III in [2007]).

(b) Die Kongruenzgruppen $\Gamma_0[2], \Gamma^0[2]$ und Γ_ϑ sind konjugiert in Γ. Es gilt nämlich

$$\Gamma^0[2] = J \cdot \Gamma_0[2] \cdot J^{-1}, \quad \Gamma_\vartheta = U \cdot \Gamma_0[2] \cdot U^{-1}$$

(c) Nach [1985](II, § 2.2) ist $\Gamma[2]$ genau die Kommutatorgruppe von $\mathrm{GL}_2(\mathbb{Z})$.

Beweis

(b) Die erste Konjugationsaussage ist bereits in (2.3) gezeigt. Wegen des Isomorphismuses aus (2.9) und wegen (2.10) folgt die zweite Behauptung aus

$$U \cdot \Gamma_0[2] \cdot U^{-1} \mathrel{\widehat{=}} \langle (1,2,3)(2,3)(3,2,1) \rangle = \langle (1,3)(3,2,1) \rangle = \langle (1,2) \rangle \mathrel{\widehat{=}} \Gamma_\vartheta \qquad \square$$

— *Die Gruppe* $\Gamma_N[2]$ —

Wie aus (2.10) ersichtlich, besitzt die S_3 eine weitere Untergruppe A_3 der Ordnung 3 mit Index 2. Mit derselben Methode wie in (2.11), zeigt man, dass die entsprechende Untergruppe von $\Gamma/\Gamma[2]$ die Kongruenzgruppe $\Gamma_N[2] := \Gamma[2] \cup (\Gamma[2] \cdot U) \cup (\Gamma[2] \cdot U^2)$ ist.

(2.16) Proposition
$\Gamma_N[2]$ ist der einzige Normalteiler in Γ vom Index 2. Die Gruppe $\Gamma_N[2]$ wird erzeugt von den Matrizen T^2 und $-U$ und es gilt

$$\Gamma = \Gamma_N[2] \cup \Gamma_N[2] \cdot T. \tag{7}$$

Die Abbildung

$$\chi : \Gamma \longrightarrow \{\pm 1\}, \quad M \mapsto (-1)^{ac+bc+bd},$$

ist ein abelscher Charakter von Γ mit $\mathrm{Kern}(\chi) = \Gamma_N[2]$.

Beweis
Um die Erzeuger von $\Gamma_N[2]$ zu bestimmen, benutze man die Darstellung als Erzeugendensystem aus (2.10):

$$\begin{aligned}\Gamma_N[2] &= \langle \underbrace{-E, T^2, JT^2J^{-1}}_{\text{Erzeuger von } \Gamma[2]}, \underbrace{-U, T^2U, JT^2J^{-1}U}_{\text{Erzeuger von } \Gamma[2]U}, \underbrace{-U^2, T^2U^2, JT^2J^{-1}U^2}_{\text{Erzeuger von } \Gamma[2]U^2} \rangle \\ &= \langle -E, T^2, JT^2J^{-1}, -U \rangle \overset{JT^2J^{-1}=U^{-1}T^2U}{=} \langle -E, T^2, -U \rangle = \langle T^2, -U \rangle,\end{aligned}$$

da $(-U)^3 = -E$.

Nun zeigen wir (7) mittels der Isomorphie aus (2.9) und der Bijektion in (2.10), indem wir die Behauptung in der $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ nachrechnen. Dann entspricht aber $\Gamma_N[2]$ in der $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ der Menge

$$\mathcal{N} = \left\{ \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} \right\} = \left\{ \overline{E}, \overline{U}, \overline{U^2} \right\}.$$

Folglich ist (7) äquivalent zu

$$\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \overset{!}{=} \mathcal{N} \cup (\mathcal{N} \cdot \overline{T}).$$

Offensichtlich sind die Elemente $\overline{E}, \overline{U}, \overline{U^2}$ und $\overline{T}$ bereits in der rechten Menge enthalten. Da

$$\overline{U} \cdot \overline{T} = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \cdot \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} = \overline{UT} \quad \text{und} \quad \overline{U^2} \cdot \overline{T} = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} \cdot \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} = \overline{J},$$

folgt (7).

Damit ist auch sofort klar, dass der Index von $\Gamma_N[2]$ in Γ gleich 2 ist. Aus der Algebra

folgt sofort, dass $\Gamma_N[2]$ ein Normalteiler ist. Zu zeigen bleibt die Eindeutigkeit. Sei dazu Γ^* eine weitere Untergruppe von Γ für die $[\Gamma : \Gamma^*] = 2$ gilt:

„$\subseteq$:“ Diese Inklusion zeigen wir in zwei Schritten. Zunächst folgert man aus $M \in \Gamma$, dass $M^2 \in \Gamma^*$ gilt. Anschließend zeigt man, dass die Erzeuger von $\Gamma_N[2]$ auch in Γ^* liegen.

Sei also $M \in \Gamma$, so dass $M^2 \notin \Gamma^*$ ist. Da $\Gamma^* \leq \Gamma$, ist $M \notin \Gamma^*$ und es gilt insbesondere, dass weder M noch M^2 das neutrale Element ist (denn das liegt ja in Γ^*). Damit gilt $\operatorname{ord}(M) \geq 3$ und $M \neq M^2$. Dann aber existieren mindestens drei disjunkte Rechtsnebenklassen von Γ^* in Γ, nämlich Γ^*, Γ^*M und Γ^*M^2, was allerdings ein Widerspruch zur Annahme ist. Demnach gilt für alle $M \in \Gamma$ auch $M^2 \in \Gamma^*$.

Aus dem gerade Gezeigten folgt, da T, J und U^2 jeweils Elemente in Γ sind, dass

$$T^2 \in \Gamma^*,$$
$$J^2 = -E \in \Gamma^*,$$
$$(U^2)^2 = U^4 = U \in \Gamma^*.$$

Dann befinden sich aber die Erzeuger von $\Gamma_N[2]$ in Γ^*, woraus diese Inklusion $\Gamma_N[2] \subseteq \Gamma^*$ folgt.

„$\supseteq$:“ Angenommen, $\Gamma_N[2] \subsetneqq \Gamma^*$. Dann überträgt sich offenbar die Inklusion auf die Rechtsnebenklassen und es gilt $\Gamma_N[2]T \subsetneqq \Gamma^*T$. Dann gilt mit der disjunkten Zerlegung $\Gamma = \Gamma_N[2] \cup \Gamma_N[2]T$ aber auch $\Gamma^* = \Gamma^*T$, da der Schnitt von Γ^* und Γ^*T nicht leer sein kann. Daraus ergibt sich aber direkt mit $\Gamma = \Gamma^*$ ein Widerspruch zu $[\Gamma : \Gamma^*] = 2$.

Nun soll gezeigt werden, dass χ ein abelscher Charakter ist, also ein Gruppenhomomorphismus in die multiplikative Gruppe der komplexen Zahlen. Beachtet man, dass die Gruppe Γ von den beiden Elementen T und J erzeugt wird, bleibt für die Homomorphieeigenschaft $\chi(ML) = \chi(M) \cdot \chi(L), \quad M, L \in \Gamma$, lediglich

$$\chi(MT) = \chi(M) \cdot \chi(T) \quad \text{und} \quad \chi(MJ) = \chi(M) \cdot \chi(J)$$

zu zeigen. Zunächst stellt man fest:

$$\chi(T) = (-1)^{1\cdot 0+1\cdot 0+1\cdot 1} = -1 = (-1)^{1\cdot 0+(-1)\cdot 1+(-1)\cdot 0} = \chi(J). \tag{8}$$

Dann folgt:

$$\begin{aligned}\chi(MT) &= \chi\left(\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}\right) = (-1)^{ac+c(a+b)+(a+b)(c+d)} \\ &= (-1)^{ac+bc+bd} \cdot (-1)^{ad-bc} \cdot (-1)^{2(ac+bc)} = \chi(M) \cdot (-1) \overset{(8)}{=} \chi(M)\chi(T) \\ \chi(MJ) &= \chi\left(\begin{pmatrix} b & -a \\ d & -c \end{pmatrix}\right) = (-1)^{bd-ad+ac} \\ &= (-1)^{ac+bc+bd} \cdot (-1)^{-ad+bc} \cdot (-1)^{2(-bc)} = \chi(M)(-1) \overset{(8)}{=} \chi(M)\chi(J).\end{aligned}$$

Damit ist χ ein abelscher Charakter.

Zuletzt bestimmen wir noch den Kern von χ. Die Kongruenzgruppe $\Gamma_N[2]$ ist Teilmenge des Kerns von χ, da die Bilder ihre Erzeuger unter χ auf 1 abgebildet werden. Andersherum muss ein Element aus $\Gamma\backslash\Gamma_N[2]$ wegen $\Gamma = \Gamma_N[2] \cup \Gamma_N[2] \cdot T$ in der Nebenklasse $\Gamma_N[2]T$ liegen. Aufgrund der Homomorphieeigenschaft gilt dann aber für $M \in \Gamma_N[2]$:

$$\chi(MT) = \chi(M)\chi(T) = 1 \cdot (-1) = -1.$$

Damit ist $MT \notin \mathrm{Kern}(\chi)$, also gilt $\Gamma\backslash\Gamma_N[2] \not\subset \mathrm{Kern}(\chi)$ und es folgt die Behauptung $\mathrm{Kern}(\chi) = \Gamma_N[2]$. □

§ 3 Endliche Untergruppen von Γ

Betrachten wir zunächst die Elemente $M \in \Gamma$ mit endlicher Ordnung. Für die gilt der

(3.1) Satz
Für $\pm E \neq M \in \Gamma$ sind äquivalent:

(i) M hat die Ordnung $3, 4$ oder 6.

(ii) M hat eine endliche Ordnung.

(iii) $|\mathrm{Spur}(M)| < 2$.

(iv) Es gibt $\tau \in \mathbb{H}$ mit $M\tau = \tau$.

(v) Es gibt $L \in \Gamma$, so dass $L^{-1}ML \in \{\pm J, \pm U, \pm U^2\}$.

Beweis
„(i) $\Rightarrow$ (ii):“ Klar.

„(ii) $\Rightarrow$ (iii):“ Hat M endliche Ordnung, so haben die Eigenwerte von M alle den Betrag 1. Denn dann ist für ein $k \in \mathbb{N}$ die Matrix $M^k = E$ und es gilt für jeden Eigenwert λ von M: $\lambda^k = 1$. Folglich gilt $|\lambda| = 1$.

Das charakteristische Polynom von M, $\chi(M)$, lautet (mit $s := \mathrm{Spur}(M)$ als Abkürzung)

$$\chi(M) = x^2 - \mathrm{Spur}(M)x + \det(M) = x^2 - sx + 1.$$

Also haben die Eigenwerte von M die Form

$$x_{1/2} = \frac{s}{2} \pm \sqrt{\frac{s^2}{4} - 1} = \frac{1}{2}\left(s \pm \sqrt{s^2 - 4}\right). \tag{9}$$

Offenbar wäre mit Blick auf (9) im Falle $s > 2$ ein Eigenwert größer als 1 und im Falle $s < -2$ ein Eigenwert kleiner als -1, was ein Widerspruch zu $|\lambda| = 1$ wäre. Also: $|s| \leq 2$. Zu betrachten bleiben demnach noch die Werte $s = 2$ und $s = -2$. Sei zunächst $s = 2$. Dann folgt aus dem Satz von Cayley-Hamilton

$$M^2 - 2M + E = 0 \Leftrightarrow M^2 = 2M - E. \tag{10}$$

Falls gezeigt werden kann, dass

$$M^n = nM - (n-1)E = M - (n-1)(M-E), \quad n \in \mathbb{N} \tag{11}$$

gilt, dann hätte M wegen $M \neq E$ unendliche Ordnung, was ein Widerspruch zur Voraussetzung wäre.

Den Fall $s = -2$ führt man durch Übergang zu $-M$ auf den ersten Fall zurück, da $\mathrm{Spur}(-M) = 2$ und $-M$ ebenfalls endliche Ordnung besitzt.

Es bleibt also lediglich noch (11) zu zeigen. Wir führen eine Induktion nach n durch:

(IA) $n = 1$: $M^1 = 1 \cdot M - (1-1) \cdot E = M$

(IV) Die Behauptung gelte für ein beliebiges, aber festes $n \in \mathbb{N}$.

(IS) $n \mapsto n+1$:

$$\begin{aligned} M^{n+1} = M \cdot M^n &\overset{\text{(IV)}}{=} M(nM - (n-1)E) = nM^2 - (n-1)M \\ &\overset{(10)}{=} n(2M - E) - (n-1)M = (2n - n + 1)M - nE \\ &= (n+1)M - nE \end{aligned}$$

Mit dem Prinzip der vollständigen Induktion folgt die Behauptung.

„(iii) $\Rightarrow$ (iv):“ Wir zeigen diese Implikation für $M \in \mathrm{SL}_2(\mathbb{R})$. Dann gilt diese insbesondere für $M \in \Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Allgemein gilt für $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$ und $\tau \in \mathbb{C}$ die Gleichung $M\tau = \tau$ genau dann, wenn

$$c\tau^2 + (d-a)\tau - b = 0, \tag{12}$$

denn

$$M\tau = \tau \Leftrightarrow \frac{a\tau + b}{c\tau + d} = \tau \Leftrightarrow a\tau + b = c\tau^2 + d\tau \Leftrightarrow c\tau^2 + (d-a)\tau - b = 0.$$

Speziell für ein $M \in \mathrm{SL}_2(\mathbb{R})$, für welches nach Voraussetzung $|\mathrm{Spur}(M)| < 2$ gilt, darf c nicht 0 sein, denn sonst müsste wegen $M \in \mathrm{SL}_2(\mathbb{R})$ gelten: $a = d = \pm 1$. Dies aber wäre wegen $a + d = \mathrm{Spur}(M) = \pm 2$ ein Widerspruch zur Voraussetzung. Also ist die Gleichung (12) immer quadratisch und die Lösungen sind entweder beide reell oder komplex konjugiert.

Für $M \in \mathrm{SL}_2(\mathbb{R})$ und $\tau \in \mathbb{H} \cup \mathbb{R}$ ist die Gleichung (12) aber dann äquivalent zu

$$\tau = \frac{a-d}{2c} + \frac{i}{2|c|}\sqrt{4 - (\mathrm{Spur}(M))^2}.$$

Denn:

$$\begin{aligned} & c\tau^2 + (d-a)\tau - b = 0 \\ \overset{\tau \in \mathbb{H}\cup\mathbb{R}}{\Leftrightarrow}\ & \tau = \frac{a-d}{2c} + \sqrt{\left(\frac{d-a}{2c}\right)^2 + \frac{b}{c}} \\ & = \frac{a-d}{2c} + \sqrt{\frac{d^2 - 2ad + a^2 + 4bc}{4c^2}} \\ \overset{4(ad-bc)-4=0}{=}\ & \frac{a-d}{2c} + \sqrt{\frac{d^2 + a^2 + 2ad - 4}{4c^2}} \\ & = \frac{a-d}{2c} + \sqrt{\frac{-1}{4c^2}} \cdot \sqrt{4 - (a+d)^2} \\ & = \frac{a-d}{2c} + \frac{i}{2|c|}\sqrt{4 - (\mathrm{Spur}(M))^2} \end{aligned}$$

Dann gibt es aber offenbar genau dann einen Fixpunkt in $\mathbb{H}$, wenn $|\mathrm{Spur}(M)| < 2$ ist.

„(iv) ⇒ (v):“ Es gelte also $M\tau = \tau$ für ein $\tau \in \mathbb{H}$. Nach [2007](II, § 2.3, Korollar A) gilt für dieses dann $\tau = Li$ oder $\tau = L\rho$ für ein $L \in \Gamma$. Somit muss M im Stabilisator von Li oder $L\rho$ liegen, also $M \in \Gamma_{Li}$ oder $M \in \Gamma_{L\rho}$. Da die Fixgruppen konjugiert zueinander sind, gilt $\Gamma_i = L^{-1}\Gamma_{Li}L$ und $\Gamma_\rho = L^{-1}\Gamma_{L\rho}L$. Dann folgt mit [2007](II, § 2.2, Satz (b)) gerade $L^{-1}ML \in \{\pm J\}$ oder $L^{-1}ML \in \{\pm U, \pm U^2\}$, also die Behauptung.

„(v) ⇒ (i):“ Wegen $(L^{-1}ML)^k = L^{-1}M^kL$ hat M dieselbe Ordnung wie $L^{-1}ML$, denn aus $(L^{-1}ML)^k = E$ folgt $E = (L^{-1}ML)^k = L^{-1}M^kL \Leftrightarrow L = M^kL \Leftrightarrow E = M^k$. Nach Voraussetzung gilt $L^{-1}ML \in \{\pm J, \pm U, \pm U^2\}$. Zu bestimmen bleiben also nur noch die Ordnungen dieser Elemente. Ausrechnen zeigt, dass $\mathrm{ord}(U) = \mathrm{ord}(U^2) = 3, \mathrm{ord}(\pm J) = 4$ und $\mathrm{ord}(-U) = \mathrm{ord}(-U^2) = 6$ gilt und somit die Behauptung. □

Zuletzt sollen die endlichen Untergruppen von Γ eine bestechend einfache Charakterisierung erfahren.

(3.2) Satz
Ist Λ eine endliche Untergruppe von Γ, dann ist Λ in Γ konjugiert zu einer der Gruppen

$$\{E\}, \quad \{\pm E\}, \quad \{\pm E, \pm J\}, \quad \{E, U, U^2\} \quad \text{oder} \quad \{\pm E, \pm U \pm U^2\}.$$

Beweis
Es gelten die Bezeichnungen aus § 1. Man definiere sich die Matrix S durch

$$S := \sum_{L \in \Lambda} L^t L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Da S aus einer endlichen Summe symmetrischer Matrizen besteht, reicht es zum Nachweis der Positivdefinitheit mit Blick auf (1.2) aus zu zeigen, dass jeder Summand positiv definit ist. Sei $L = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. Dann ist

$$L^t L = \begin{pmatrix} \alpha^2 + \gamma^2 & \alpha\beta + \gamma\delta \\ \alpha\beta + \gamma\delta & \beta^2 + \delta^2 \end{pmatrix}.$$

Nach (1.3) ist $L^t L$ positiv definit, da $\alpha^2 + \gamma^2 > 0$ und $\det(L^t L) = \det(L^t) \cdot \det(L) = 1 \cdot 1 = 1 > 0$ ist, und somit auch S.

Da für festes $M \in \Lambda$ mit L auch LM ganz Λ durchläuft, folgt

$$M^t S M = M^t \left(\sum_{L \in \Lambda} L^t L \right) M = \sum_{L \in \Lambda} M^t L^t L M = \sum_{L \in \Lambda} (LM)^t (LM) = S. \tag{13}$$

Da wegen (1.3) $a > 0$ und $\det(S) > 0$ ist, liegt $w(S) = \frac{1}{a}\left(-b + i\sqrt{\det(S)}\right)$ in $\mathbb{H}$. Setze $\tau = w(S)$. Dann gilt nach (1.5)

$$\tau = w(S) \overset{(13)}{=} w(M^t S M) \overset{\text{Def.}}{=} w(M^{-1} * S) \overset{(1.5)}{=} M^{-1}\langle w(S)\rangle \underset{\tau \in \mathbb{H}}{\overset{\text{Def.}}{=}} M^{-1}\tau,$$

also $M\tau = \tau$. Demnach liegt M im Stabilisator von τ. Damit ist $\Lambda \subset \Gamma_\tau$ und weil Λ nach Voraussetzung eine Gruppe ist, gilt sogar $\Lambda \leq \Gamma_\tau$. Da die Stabilisatoren konjugiert zueinander sind, also $\Gamma_{M\tau} = M\Gamma_\tau M^{-1}$ gilt, darf man ohne Beschränkung der Allgemeinheit $\tau \in \mathbb{F}$ annehmen. Mit [2007](II, § 2.3) ist dann Λ als Untergruppe von Γ_τ aber konjugiert zu einer der Gruppen

$$\{E\}, \quad \{\pm E\}, \quad \{\pm E, \pm J\}, \quad \{E, U, U^2\} \quad \text{oder} \quad \{\pm E, \pm U \pm U^2\},$$

was gerade der Behauptung entspricht. □

Dann folgt offensichtlich das

(3.3) Korollar
Jede endliche Untergruppe von Γ ist von der Ordnung $1, 2, 3, 4$ oder 6.

Literatur

[1977] R. A. Rankin: *Modular forms and functions*.
Cambridge: Cambridge University Press, 1977.

[1982] H. Petersson: *Modulfunktionen und quadratische Formen*.
Berlin-Heidelberg-New York: Springer-Verlag, 1982.

[1983] H. Maass: *Lectures on modular functions of one complex variable*.
Bombay: Tata Institute, 1964; Überarbeitung, Berlin-Heidelberg-New York: Springer-Verlag, 1983.

[1985] M. Koecher: *Matrices over $\mathbb{Z}$*.
Münster, 1985.

[2007] M. Koecher, A. Krieg: *Elliptische Funktionen und Modulformen*.
2. Auflage, Berlin-Heidelberg-New York: Springer-Verlag, 2007.