Kongruenzuntergruppen und diskontinuierliche Gruppen

von
Andreas Kinas

Seminar zur Funktionentheorie II

Prof. Dr. Aloys Krieg
Andreas Freh

Lehrstuhl A für Mathematik

RWTH Aachen

WS 2013/14

Vortrag: 13.12.2013

Inhaltsverzeichnis

§1 Repetitorium

Dem Leser dieser Seminararbeit sollte die Theorie zur Geometrie der oberen Halbebene

$$\mathbb{H} := \{\tau \in \mathbb{C};\ \mathrm{Im}(\tau) > 0\} \subset \mathbb{C},$$

zur Modulgruppe

$$\Gamma := \mathrm{SL}_2(\mathbb{Z}) := \{M \in \mathrm{M}_2(\mathbb{Z});\ \det(M) = 1\}$$

und zur speziellen linearen Gruppe

$$\mathrm{SL}_2(\mathbb{R}) := \{M \in \mathrm{M}_2(\mathbb{R});\ \det(M) = 1\}$$

hinreichend bekannt sein. Damit einige Bezeichnungen und Resultate aus der Vorlesung „Funktionentheorie II" ([KA13]) und aus dem Buch [KK98], die für Beweise in dieser Arbeit benötigt werden, nicht nachgeschlagen werden müssen, wiederholen wir diese kurz im Folgenden.

(1.1) Bezeichnung
Für $n \in \mathbb{N}$ sei

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$$

der Restklassenring von $\mathbb{Z}$ modulo $n\mathbb{Z}$.

Sechs Matrizen aus der Modulgruppe werden für diese Arbeit besonders bezeichnet:

- $E := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
- $J := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$
- $T := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$
- $U := \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}$
- $U^2 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$
- $V := -UT = -\begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$

(1.2) Definition
Seien $\tau \in \mathbb{H}$ und Λ eine Untergruppe von Γ. Dann nennt man τ einen *Fixpunkt* von Λ, wenn es eine Matrix $M \in \Lambda$ gibt mit

$$M\tau = \tau$$

und $M \notin \{\pm E\}$.

(1.3) Bemerkung
Sei die Situation aus (1.2) gegeben. Da Λ eine Untergruppe von Γ ist, ist jeder Fixpunkt von Λ auch ein Fixpunkt von Γ. Die Umkehrung gilt im Allgemeinen nicht.

Es sei

$$\mathbb{F} := \left\{ \tau \in \mathbb{H};\ -\frac{1}{2} < \mathrm{Re}(\tau) \leq \frac{1}{2},\ |\tau| \geq 1 \text{ und } |\tau| > 1 \text{ für } -\frac{1}{2} < \mathrm{Re}(\tau) < 0 \right\} \subset \mathbb{C}. \tag{1}$$

Zwei Randpunkte von $\mathbb{F}$ seien hervorgehoben: i und $\rho := \frac{1}{2} + \frac{1}{2} i\sqrt{3}$.

(1.4) Satz
Die Fixpunkte von Γ sind genau die Punkte Mi und $M\rho$ für eine Matrix $M \in \Gamma$.

(1.5) Satz
Gehören τ und $M\tau$ für $M \in \Gamma$ zu $\mathbb{F}$ in (1), so gilt $\tau = M\tau$. Ist $M \notin \{\pm E\}$, so folgt entweder

$$\tau = M\tau = i$$

mit $M \in \{\pm J\}$ oder

$$\tau = M\tau = \rho$$

mit $M \in \left\{\pm U, \pm U^2\right\}$.

(1.6) Satz
Die Automorphismengruppe $\mathrm{Aut}(\mathbb{H})$ operiert transitiv auf $\mathbb{H}$.

(1.7) Satz
Seien

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{R})$$

und $\tau \in \mathbb{H}$ mit $\mathrm{Im}(\tau) \neq 0$. Dann gilt

$$\mathrm{Im}(M\tau) = \tfrac{1}{|c\tau+d|^2}.$$

(1.8) Satz
Jedes Kompaktum von $\mathbb{H}$ ist in einer $\mathbb{H}$-Kreisscheibe mit dem $\mathbb{H}$-Mittelpunkt i der Gestalt

$$\{z \in \mathbb{H};\ |z, i| \leq r\}$$

für eine reelle Zahl $r > 0$ enthalten.

(1.9) Satz
Jeder $\mathbb{H}$-Kreis ist ein euklidischer Kreis in $\mathbb{H}$ und umgekehrt.

Aus (1.9) folgt sofort, dass die durch die $\mathbb{H}$-Metrik induzierte Topologie mit der natürlichen Topologie auf $\mathbb{H}$ übereinstimmt.

§2 Kongruenzuntergruppen

Als grundlegende Referenz für die Abschnitte 2.1 und 2.2 dient [KK98], für den Abschnitt 2.3 dient [SS12].

Ziel dieses Kapitels ist es, ein Vertretersystem der (Rechts- oder Links-) Nebenklassen der Modulgruppe Γ modulo einer Hauptkongruenzgruppe bzw. modulo einer Kongruenzgruppe zu bestimmen. Dieses Vertetersystem kann dann dazu genutzt werden, um Fundamentalbereiche zu Hauptkongruenzgruppen und Kongruenzgruppen von Γ zu konstruieren (vgl. Theorie zu Fundamentalbereichen in [KA13], S. 298-299).

2.1 Hauptkongruenzgruppen

(2.1) Definition
Sei $n \in \mathbb{N}$. Für $M, L \in \mathrm{M}_2(\mathbb{Z})$ wird die *Matrixkongruenz*

$$M \equiv_n L$$

komponentenweise erklärt, das heißt, es gibt eine Matrix $Z \in \mathrm{M}_2(\mathbb{Z})$, sodass

$$M = L + nZ$$

gilt.

Sei $n \in \mathbb{N}$. In $\mathbb{Z}$ kann man aus den beiden Kongruenzen $a \equiv_n a'$ und $b \equiv_n b'$ bereits folgern, dass $ab \equiv_n a'b'$ gilt. Dass diese Tatsache auch über $\mathrm{M}_2(\mathbb{Z})$ erfüllt ist, zeigt das folgende Ergebnis:

(2.2) Lemma
Sei $n \in \mathbb{N}$. Sind $L \equiv_n L^*$ und $M \equiv_n M^*$ für $L, L^*, M, M^* \in \mathrm{M}_2(\mathbb{Z})$ erfüllt, so gilt

$$LM \equiv_n L^* M^*.$$

Beweis:
Wegen $L \equiv_n L^*$ und $M \equiv_n M^*$ für $L, L^*, M, M^* \in \mathrm{M}_2(\mathbb{Z})$ nach Voraussetzung gibt es nach (2.1) Matrizen $Z_1, Z_2 \in \mathrm{M}_2(\mathbb{Z})$, sodass einerseits

$$L = L^* + nZ_1$$

und andererseits

$$M = M^* + nZ_2$$

gilt. Es folgt

$$\begin{aligned} LM &= (L^* + nZ_1)(M^* + nZ_2) \\ &= L^*M^* + L^*nZ_2 + nZ_1M^* + n^2Z_1Z_2 \\ &= L^*M^* + n\left(L^*Z_2 + Z_1M^* + nZ_1Z_2\right) \\ &= L^*M^* + nZ \end{aligned}$$

für $Z := L^*Z_2 + Z_1M^* + nZ_1Z_2 \in \mathrm{M}_2(\mathbb{Z})$ und damit die Behauptung.

□

(2.3) Definition
Sei $n \in \mathbb{N}$. Dann definiert man durch

$$\Gamma[n] := \{M \in \Gamma;\ M \equiv_n E\} \leq \Gamma$$

die *Hauptkongruenzgruppe* (*modulo n*). Dabei wird n die *Stufe* von $\Gamma[n]$ genannt. Insbesondere ist $\Gamma[1] = \Gamma$.

Sei $n \in \mathbb{N}$. Jetzt betrachte man die kanonische Projektion

$$\mathbb{Z} \to \mathbb{Z}_n,\ z \mapsto \overline{z} := z + n\mathbb{Z}$$

und setze diese auf Matrizen des Formats 2 x 2 vermöge

$$\mathrm{M}_2(\mathbb{Z}) \to \mathrm{M}_2(\mathbb{Z}_n),\ M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \overline{M} = \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} \tag{2}$$

fort.

(2.4) Lemma
Seien $a, b \in \mathbb{Z}$ und $c \in \mathbb{Z} \setminus \{0\}$ so, dass $\mathrm{ggT}(a, b, c) = 1$. Dann existiert eine Zahl $x \in \mathbb{Z}$ mit

$$\mathrm{ggT}(a + xb, c) = 1.$$

Beweis:
Sei

$$x := \prod_{p \text{ prim},\, p|c,\, p\nmid a} p \in \mathbb{Z}. \tag{3}$$

Dann ist x wohldefiniert, da es nur endlich viele Primzahlen gibt, die die Zahl c teilen (beachte in (3): Das leere Produkt ist als 1 definiert). Angenommen, es gibt eine Primzahl q mit $q \mid (a + xb)$ und $q \mid c$. Dann unterscheiden wir zwei Fälle:

1. Fall:
Angenommen, es gilt $q \mid a$. Dann gilt per Definition von x, dass $q \nmid x$. Aus $q \mid (a + xb)$, $q \mid a$ und $q \nmid x$ folgt $q \mid b$, ein Widerspruch zur Voraussetzung $\operatorname{ggT}(a, b, c) = 1$.
2. Fall:
Angenommen, es gilt $q \nmid a$. Dann gilt per Definition von x, dass $q \mid x$. Aus $q \mid (a + xb)$ und $q \mid x$ folgt $q \mid a$ als Widerspruch.

Insgesamt folgt nun die Behauptung.

□

(2.5) Satz
Seien $n \in \mathbb{N}$ und die Abbildung

$$\varphi : \Gamma \to \mathrm{SL}_2(\mathbb{Z}_n),\ M \mapsto \overline{M}$$

gegeben (vgl. mit der Abbildung in (2)). Dann ist φ ein surjektiver Gruppenhomomorphismus mit

$$\operatorname{Kern}(\varphi) = \Gamma[n].$$

Es ist $\Gamma[n]$ ein Normalteiler in Γ und für den Index gilt

$$[\Gamma : \Gamma[n]] < \infty.$$

Ferner hat man die Gruppenisomorphie

$$\Gamma/\Gamma[n] \cong \mathrm{SL}_2(\mathbb{Z}_n).$$

Beweis:
Sei

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}).$$

Für eine beliebige Matrix

$$X = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z})$$

gilt

$$\begin{aligned}\det\left(M+nX\right) &= \det\left(\begin{bmatrix} a+nx_1 & b+nx_2 \\ c+nx_3 & d+nx_4 \end{bmatrix}\right)\\ &= (a+nx_1)(d+nx_4)-(b+nx_2)(c+nx_3)\\ &= ad+nax_4+ndx_1+n^2x_1x_4-bc-nbx_3-ncx_2-n^2x_2x_3\\ &= ad-bc+n(ax_4+dx_1+nx_1x_4-bx_3-cx_2-nx_2x_3)\\ &= \det(M)+n\widetilde{x}\end{aligned}$$

für $\widetilde{x} := ax_4+dx_1+nx_1x_4-bx_3-cx_2-nx_2x_3 \in \mathbb{Z}$, also

$$\det\left(\overline{M}\right) = \overline{\det(M)}.$$

Daher ist $\mathrm{Bild}(\varphi) \subseteq \mathrm{SL}_2(\mathbb{Z}_n)$ und φ somit wohldefiniert. Weiterhin ist φ ein Gruppenhomomorphismus, denn nach (2.2) gilt

$$\varphi(M)\varphi(N) = \overline{M}\,\overline{N} = \overline{MN} = \varphi(MN)$$

für alle $M, N \in \Gamma$. Mit (2.1) und (2.3) ist ferner

$$\begin{aligned}\mathrm{Kern}(\varphi) &= \left\{M \in \Gamma;\ \varphi(M) = \overline{E}\right\}\\ &= \{M \in \Gamma;\ \text{es existiert ein } Y \in \mathrm{M}_2(\mathbb{Z}),\ \text{sodass } M = E+nY \text{ ist}\}\\ &= \{M \in \Gamma;\ M \equiv_n E\}\\ &= \Gamma[n].\end{aligned}$$

Da der Kern eines Gruppenhomomorphismus' $H \to H'$ für zwei Gruppen H und H' stets ein Normalteiler in H ist, ist $\Gamma[n]$ ein Normalteiler in Γ. Es sei nun

$$G := \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z})$$

mit $\overline{G} \in \mathrm{SL}_2(\mathbb{Z}_n)$. O.B.d.A. sei $\gamma \neq 0$. Dies ist möglich, da sonst γ durch $\gamma+n$ ersetzt werden kann, ohne dass sich $\overline{G}$ ändert. Wegen

$$\det(G) = \alpha\delta-\beta\gamma \equiv_n 1 \tag{4}$$

gilt $\mathrm{ggT}(\gamma, \delta, n) = 1$. Nach (2.4) existiert eine Zahl $r \in \mathbb{Z}$, sodass

$$\mathrm{ggT}(\gamma, d) = 1$$

mit $d := \delta + rn \in \mathbb{Z}$. Nun gibt es wegen der Kongruenz (4) eine Zahl $g \in \mathbb{Z}$ mit

$$\alpha\delta-\beta\gamma = 1+ng,$$

womit

$$\begin{aligned}\alpha d - \beta\gamma &= \alpha\delta - \beta\gamma + \alpha r n \\ &= 1 + ng + \alpha r n \\ &= 1 + (g + \alpha r)n \\ &= 1 + sn\end{aligned}$$

mit $s := g + \alpha r \in \mathbb{Z}$ erfüllt ist. Wegen $\text{ggT}(\gamma, d) = 1$ findet man ganze Zahlen x und y mit

$$\gamma y - dx = s.$$

Dann gilt

$$M := \begin{bmatrix} \alpha + xn & \beta + yn \\ \gamma & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}),$$

da

$$\begin{aligned}\det(M) &= (\alpha + xn)d - (\beta + yn)\gamma \\ &= \alpha d + dxn - \beta\gamma - \gamma y n \\ &= (\alpha d - \beta\gamma) + n(dx - \gamma y) \\ &= 1 + sn - n(\gamma y - dx) \\ &= 1 + sn - ns \\ &= 1.\end{aligned}$$

Also existiert zu $\overline{G} \in \text{SL}_2(\mathbb{Z}_n)$ eine Matrix $M \in \Gamma$ mit $\varphi(M) = \overline{M} = \overline{G}$, das heißt, φ ist surjektiv. Der Homomorphiesatz für Gruppen liefert nun die Isomorphie

$$\Gamma/\Gamma[n] \cong \text{SL}_2(\mathbb{Z}_n),$$

also insbesondere

$$[\Gamma : \Gamma[n]] = |\text{SL}_2(\mathbb{Z}_n)| < n^4 < \infty$$

mithilfe von (2.7). Insgesamt folgt die Behauptung.

$\square$

Da $\Gamma[n]$ nach (2.5) ein Normalteiler in Γ ist, existiert eine disjunkte Zerlegung von Γ in Nebenklassen von $\Gamma[n]$. Diese ist sogar endlich, da $[\Gamma : \Gamma[n]] < \infty$ ist. Die Matrizen in einer Nebenklasse von $\Gamma[n]$ charakterisieren wir in dem folgenden Resultat:

(2.6) Satz
Sei $n \in \mathbb{N}$. Zwei Matrizen $M, L \in \Gamma$ liegen genau dann in derselben (Links- oder Rechts-) Nebenklasse von $\Gamma[n]$, wenn $M \equiv_n L$ ist.

Beweis:
„$\Rightarrow$“:
Seien $M, L \in \Gamma$ mit

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

und $M \equiv_n L$. Dann gibt es nach (2.1) eine Matrix

$$X = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}),$$

sodass

$$M = L + nX = \begin{bmatrix} a + nx_1 & b + nx_2 \\ c + nx_3 & d + nx_4 \end{bmatrix}.$$

Wegen $L \in \Gamma$ ist $\det(L) = ad - bc = 1 \neq 0$, also existiert die Inverse L^{-1} von L, die mit einer aus der linearen Algebra bekannten Formel die Gestalt

$$L^{-1} = \tfrac{1}{\det(L)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

hat. Damit gilt

$$\begin{aligned} L^{-1}M &= \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a + nx_1 & b + nx_2 \\ c + nx_3 & d + nx_4 \end{bmatrix} \\ &= \begin{bmatrix} ad - bc + n(dx_1 - bx_3) & bd - db + n(dx_2 - bx_4) \\ ac - ac + n(ax_3 - cx_1) & ad - bc + n(ax_4 - cx_2) \end{bmatrix} \\ &= \begin{bmatrix} 1 + n(dx_1 - bx_3) & 0 + n(dx_2 - bx_4) \\ 0 + n(ax_3 - cx_1) & 1 + n(ax_4 - cx_2) \end{bmatrix} \\ &= E + n \begin{bmatrix} dx_1 - bx_3 & dx_2 - bx_4 \\ ax_3 - cx_1 & ax_4 - cx_2 \end{bmatrix} \\ &\equiv_n E. \end{aligned}$$

Es folgt $L^{-1}M \in \Gamma[n]$ und somit $M \in L \cdot \Gamma[n]$. Analog zeigt man, dass $L \in \Gamma[n] \cdot M$.

„$\Leftarrow$“:
Seien $M \in L \cdot \Gamma[n]$ mit $M, L \in \Gamma$. Dann existiert eine Matrix $M' \in \Gamma[n]$ und eine Matrix $X \in \mathrm{M}_2(\mathbb{Z})$, sodass

$$\begin{aligned} M &= LM' \\ &= L(E + nX) \\ &= L + nLX \\ &\equiv_n L. \end{aligned}$$

Analog zeigt man, dass aus $M \in \Gamma[n] \cdot L$ gerade $M \equiv_n L$ folgt.

Insgesamt erhält man die Behauptung.

$\square$

(2.7) Bemerkung
Sei $n \in \mathbb{N} \setminus \{1\}$. Aufgrund der Isomorphie

$$\Gamma/\Gamma[n] \cong \mathrm{SL}_2(\mathbb{Z}_n)$$

aus (2.5) kann der Index $[\Gamma : \Gamma[n]] \in \mathbb{N}$ wie folgt bestimmt werden:

$$[\Gamma : \Gamma[n]] = |\mathrm{SL}_2(\mathbb{Z}_n)| = n^3 \prod_{p \text{ prim}, p|n} \left(1 - \frac{1}{p^2}\right). \tag{5}$$

Auf einen Beweis der zweiten Gleichheit in der Gleichungskette (5) wird in dieser Seminararbeit verzichtet, z. B. findet man einen in [RR77], S. 21-23.

Das nächste Ergebnis macht eine Aussage über die Fixpunkte von $\Gamma[n]$.

(2.8) Satz
Für $n \in \mathbb{N} \setminus \{1\}$ besitzt $\Gamma[n]$ keine Fixpunkte, das heißt, aus $M\tau = \tau$ für ein $\tau \in \mathbb{H}$ und eine Matrix $M \in \Gamma[n]$ folgt
(a) im Falle $n = 2$: $M \in \{\pm E\}$
(b) im Falle $n > 2$: $M = E$

Beweis:
Gilt $M\tau = \tau$ für ein $\tau \in \mathbb{H}$ und eine Matrix $M \in \Gamma[n]$ mit $M \notin \{\pm E\}$, so ist τ nach (1.3) auch Fixpunkt von Γ. Aus (1.4) folgt $\tau = Li$ oder $\tau = L\rho$ mit einer geeigneten Matrix $L \in \Gamma$. Wegen $L \in \Gamma$ ist $\det(L) \neq 0$, also existiert die Inverse L^{-1} von L. Man erhält entweder

$$M\tau = \tau \Leftrightarrow MLi = Li \Leftrightarrow L^{-1}MLi = i$$

oder

$$M\tau = \tau \Leftrightarrow ML\rho = L\rho \Leftrightarrow L^{-1}ML\rho = \rho.$$

Nach Anwendung von (1.5) gilt

$$L^{-1}ML \in \{\pm J\}$$

oder

$$L^{-1}ML \in \left\{\pm U, \pm U^2\right\}.$$

Da $\Gamma[n]$ nach (2.5) ein Normalteiler in Γ ist, gehören die Matrizen $\pm J$, $\pm U$ oder $\pm U^2$ zu $\Gamma[n]$ für $n \geq 2$. Dies ist aber nicht der Fall, denn es existieren für $n \geq 2$ keine Matrizen $X, Y, Z \in \mathrm{M}_2(\mathbb{Z})$, sodass

$$\pm J = \pm \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = E + nX$$

oder

$$\pm U = \pm \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} = E + nY$$

oder

$$\pm U^2 = \pm \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} = E + nZ$$

gilt. Daher folgt $M \in \{\pm E\}$ für $n = 2$ und $M = E$ für $n > 2$, da $M = -E \notin \Gamma[n]$ für $n > 2$. Insgesamt folgt die Behauptung.

□

(2.9) Beispiel
Sei $n = 2 \in \mathbb{N}$. Nach (2.3) ist

$$\Gamma[2] = \{M \in \Gamma;\ M \equiv_2 E\} \lneq \Gamma.$$

Der Index $[\Gamma : \Gamma[2]]$ ergibt sich nach (2.7) zu

$$[\Gamma : \Gamma[2]] = 2^3 \cdot \prod_{p|2} \left(1 - \frac{1}{p^2}\right) = 6,$$

das heißt, ein Vertretersystem von $\Gamma[2]$ in Γ enthält sechs Elemente. An dieser Stelle betrachten wir die folgenden sechs Matrizen aus Γ (vgl. §1): E, T, J, U, U^2 und V. Offensichtlich sind diese Matrizen jeweils paarweise inkongruent modulo 2 (komponentenweise), sodass sie mit (2.6) ein Vertretersystem der Nebenklassen von $\Gamma[2]$ in Γ bilden. Also hat man

$$\Gamma = \Gamma[2] \cup (T \cdot \Gamma[2]) \cup (J \cdot \Gamma[2]) \cup (U \cdot \Gamma[2]) \cup \left(U^2 \cdot \Gamma[2]\right) \cup (V \cdot \Gamma[2]).$$

◇

2.2 Kongruenzgruppen

(2.10) Definition
Eine Untergruppe Λ von Γ heißt *Kongruenzgruppe*, wenn es eine natürliche Zahl n gibt mit $\Gamma[n] \subseteq \Lambda$. Die kleinste natürliche Zahl n mit der Eigenschaft $\Gamma[n] \subseteq \Lambda$ heißt *Stufe* von Λ.

(2.11) Satz
Jede Kongruenzgruppe Λ von Γ hat endlichen Index in Γ.

Beweis:
Da Λ nach Voraussetzung eine Kongruenzgruppe ist, existiert nach (2.10) eine natürliche Zahl n, sodass

$$\Gamma[n] \subseteq \Lambda. \tag{6}$$

Wir wissen bereits, dass es eine endliche Zerlegung von Γ in Rechtsnebenklassen $M_k \in \Gamma[n]$ mit $1 \leq k \leq [\Gamma : \Gamma[n]] < \infty$ gibt (vgl. (2.5)), etwa

$$\Gamma = \bigcup_{1 \leq k \leq [\Gamma:\Gamma[n]]} \Gamma[n] M_k.$$

Wegen der Inklusion (6) gilt $\Gamma[n]M_k \subseteq \Lambda M_k$ für alle k. Es folgt, dass Γ dargestellt werden kann als

$$\Gamma = \bigcup_{1 \leq k \leq [\Gamma:\Gamma[n]]} \Lambda M_k. \tag{7}$$

Die Zerlegung (7) von Γ ist im Allgemeinen nicht disjunkt (außer, wenn $\Gamma[n] = \Lambda$ ist). Somit hat man

$$[\Gamma : \Lambda] \leq [\Gamma : \Gamma[n]] < \infty,$$

was zu zeigen war.

□

(2.12) Beispiel
Sei $n = 2 \in \mathbb{N}$. Betrachte

$$\Gamma_0[2] := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma;\, c \equiv_2 0 \right\} \lneq \Gamma. \tag{8}$$

Wir zeigen, dass $\Gamma_0[2]$ eine echte Untergruppe von Γ ist. Das neutrale Element E (bezüglich Matrixmultiplikation) erfüllt $E \in \Gamma_0[2]$, da $0 \equiv_2 0$ und $\det(E) = 1$. Seien weiter

$$A := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0[2]$$

und

$$A' := \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in \Gamma_0[2].$$

Dann ist

$$B := AA' = \begin{bmatrix} * & * \\ ca' + dc' & * \end{bmatrix} \in \Gamma_0[2],$$

da wegen $c \equiv_2 0$ und $c' \equiv_2 0$ auch $ca' + dc' \equiv_2 0$ und $\det(B) = \det(A)\det(A') = 1$. Wegen $A \in \Gamma_0[2] \subseteq \Gamma$ gilt $\det(A) \neq 0$, also existiert die Inverse A^{-1} von A. Mit der aus der linearen Algebra bekannten Formel für die Inverse einer Matrix vom Format 2 x 2 gilt

$$A^{-1} = \tfrac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in \Gamma_0[2],$$

da wegen $c \equiv_2 0$ gerade $-c \equiv_2 0$ ist und $\det\left(A^{-1}\right) = (\det(A))^{-1} = 1$. Damit ist $\Gamma_0[2]$ eine Untergruppe von Γ. In (8) kann keine Gleichheit gelten, da z. B. $J \in \Gamma$, jedoch klarerweise $J \notin \Gamma_0[2]$ ist.

Ferner gilt $\Gamma[2] \subseteq \Gamma_0[2]$, denn

$$\Gamma[2] = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma;\, a \equiv_2 d \equiv_2 1,\, b \equiv_2 c \equiv_2 0 \right\}.$$

Da $\Gamma[1] = \Gamma \not\subseteq \Gamma_0[2]$ ist, ist nun $\Gamma_0[2]$ gemäß (2.10) eine Kongruenzgruppe von Γ der Stufe 2. Um ein Vertretersystem von Rechtsnebenklassen von Γ modulo $\Gamma_0[2]$ zu bestimmen, beachte man, dass $\Gamma[2]$ eine Untergruppe von $\Gamma_0[2]$ ist. Nach (2.9) gilt insbesondere

$$\Gamma = \Gamma_0[2] \cup (\Gamma_0[2] \cdot T) \cup (\Gamma_0[2] \cdot J) \cup (\Gamma_0[2] \cdot U) \cup \left(\Gamma_0[2] \cdot U^2\right) \cup (\Gamma_0[2] \cdot V)$$

mit den Matrizen E, T, J, U, U^2 und V aus §1. Nun muss verifiziert werden, welche dieser Matrizen dieselben Rechtsnebenklassen von Γ modulo $\Gamma_0[2]$ beschreiben. Dazu prüft man durch einfaches Nachrechnen, für welche Matrizen $M, L \in \left\{E, T, J, U, U^2, V\right\}$ mit $M \neq L$ die Beziehung

$$ML^{-1} \in \Gamma_0[2]$$

gilt. Man erhält, dass $ML^{-1} \notin \Gamma_0[2]$ gilt für $M, L \in \left\{E, J, U^2\right\}$. Somit bilden die Matrizen E, J und U^2 ein Vertretersystem von Rechtsnebenklassen von Γ modulo $\Gamma_0[2]$. Dies bedeutet gerade

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

Man sieht, dass für den Index

$$[\Gamma : \Gamma_0[2]] = 3$$

gilt, dieser also insbesondere endlich ist (vgl. (2.11)).

$\diamond$

(2.13) Satz
Sei $n \in \mathbb{N} \setminus \{1\}$. Dann ist die Untergruppe

$$\Gamma_0[n] := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma;\ c \equiv_n 0 \right\} \lneq \Gamma$$

kein Normalteiler in Γ.

Beweis:
Ein Element M aus $\Gamma_0[n]$ hat etwa die Gestalt

$$M = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} + nZ = \begin{bmatrix} a + nz_1 & b + nz_2 \\ nz_3 & d + nz_4 \end{bmatrix}$$

für eine Matrix

$$Z := \begin{bmatrix} z_1 & z_2 \\ z_3 & z_4 \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}).$$

Wäre $\Gamma_0[n]$ für $n \in \mathbb{N} \setminus \{1\}$ ein Normalteiler in Γ, so würde $NMN^{-1} \in \Gamma_0[n]$ für alle Matrizen $N \in \Gamma$ gelten. Wählt man nun

$$N = J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

und gilt $n \nmid b$, so folgt

$$JMJ^{-1} = \begin{bmatrix} d + nz_4 & -nz_3 \\ -b - nz_2 & a + nz_1 \end{bmatrix} \notin \Gamma_0[n]$$

im Widerspruch zur Annahme. Insgesamt ergibt sich nun die Behauptung.

□

2.3 Beispielklasse von Nicht-Kongruenzgruppen

Eine Untergruppe von Γ von endlichem Index in Γ braucht keine Kongruenzgruppe zu sein. Erste Beispiele für solche Untergruppen wurden 1887 von R. Fricke ([FR87], S. 99-118) und G. Pick ([PG87], S. 119-124) geliefert. In diesem Abschnitt werden wir eine Klasse von Nicht-Kongruenzuntergruppen von Γ konstruieren. Dabei lenken wir unser Augenmerk auf eine Veröffentlichung von I. Reiner ([RI58], S. 142-144) und nutzen außerdem Resultate von H. Frasch ([FH33], S. 229-252), auf deren Beweise aus Platzgründen verzichtet wird.

Zunächst führen wir Ergebnisse aus [FH33] an.

(2.14) Definition
Seien $p > 3$ eine Primzahl, $\alpha \in \mathbb{N}$ eine Primitivwurzel modulo p, das heißt, es gilt

$$\langle \alpha + p\mathbb{Z} \rangle = \left(\mathbb{Z}_p\right)^*,$$

und $\beta \in \mathbb{N}$ mit $\alpha\beta \equiv_p 1$ (beachte: Es ist $\left(\mathbb{Z}_p\right)^*$ als Einheitengruppe eines endlichen Körpers zyklisch und daher die Existenz einer Primitivwurzel garantiert). Es seien weiter

$$V_p := JT^\alpha JT^\beta JT^\alpha = \begin{bmatrix} -\beta & 1-\alpha\beta \\ \alpha\beta - 1 & -\alpha + \alpha(\alpha\beta - 1) \end{bmatrix}$$

und $\lambda, \mu, \nu, \lambda_*, \mu_*, \nu_* \in \mathbb{N}_0$ mit den Eigenschaften $\nu\nu_* \equiv_p 1$, $\mu_* \equiv_p \mu\nu^2 - \nu$ und

$$\lambda_* \equiv_{\frac{p-1}{2}} \lambda + \mathrm{l}_\alpha(\nu),$$

wobei $\alpha^{\mathrm{l}_\alpha(\nu)} \equiv_p \nu$ mit $\mathrm{l}_\alpha(\nu) \in \mathbb{N}_0$. Dann definiert man:
(a) $(\lambda)_p := V_p^\lambda T^p V_p^\lambda$
(b) $(\lambda, \mu)_p := V_p^\lambda T^\mu JT^p J^{-1} T^{-\mu} V_p^{-\lambda}$
(c) $(\lambda, \mu, \nu)_p := V_p^\lambda T^\mu JT^\nu JT^{-\nu_*} J^{-1} T^{-\mu_*} V_p^{-\lambda_*}$

(2.15) Bemerkung
Sei die Situation aus (2.14) gegeben. Ist $\mu \neq 0$, so gilt

$$(\lambda, \mu, 1)_p (\lambda, \mu - 1)_p = 1.$$

(2.16) Satz
Sei die Situation aus (2.14) gegeben. Dann ist $\Gamma[p]$ eine freie Gruppe mit

$$1 + \tfrac{(p-1)p(p+1)}{12}$$

Erzeugern. Diese können so gewählt werden, dass ein Erzeuger T^p ist und die anderen Erzeuger von der Form $(\lambda, \mu, \nu)_p$ mit $\nu \not\equiv_p \pm 1$ und $\nu \not\equiv_p 0$ sind.

Das nächste aufgeführte Ergebnis ist eine Folgerung aus dem Beweis von (2.16).

(2.17) Korollar
Sei die Situation aus (2.14) gegeben. Gilt $(\lambda, \mu, \nu)_p \in \Gamma[p]$, so ist $(\lambda, \mu, \nu)_p$ einer der freien Erzeuger aus (2.16) oder kann als Produkt der freien Erzeuger exklusive T^p geschrieben werden.

Nun kommen wir zur Konstruktion einer Beispielklasse von Nicht-Kongruenzgruppen der Modulgruppe. Wir folgen ab jetzt den Darlegungen aus [RI58].

(2.18) Definition
Seien $p > 3$ eine Primzahl und $s \in \mathbb{N}$. Es bezeichne weiter $\Gamma'[p]$ die Kommutatorgruppe von $\Gamma[p]$. Nach (2.16) ist $\Gamma[p]$ eine freie Gruppe auf endlich vielen, etwa $k \in \mathbb{N}$, Erzeugern. Folglich ist

$$\Delta[p] := \Gamma[p]/\Gamma'[p]$$

eine freie Abelsche Gruppe auf k Erzeugern, das heißt, $\Delta[p]$ ist isomorph zu $\mathbb{Z}^k$ (denn: Es ist $\Delta[p]$ eine endlich erzeugte Abelsche Gruppe ohne Elemente endlicher Ordnung (abgesehen vom Nullelement); die Aussage folgt nun aus dem Hauptsatz über endlich erzeugte Moduln über Hauptidealbereichen). Also ist

$$\Delta[p]/\Delta^s[p] \cong C_s^k$$

eine endliche Gruppe, wobei

$$\Delta^s[p] := \{x^s;\, x \in \Delta[p]\}$$

ist. Ist $\pi : \Gamma[p] \to \Delta[p]$ die kanonische Restklassenabbildung, so sei

$$\Omega(p,s) := \pi^{-1}\left(\Delta^s[p]\right).$$

(2.19) Lemma
Seien $p > 3$ eine Primzahl und $s \in \mathbb{N}$. Dann ist $\Omega(p,s)$ ein Normalteiler und von endlichem Index in Γ.

Beweis:
Es ist $\Delta^s[p]$ ein Normalteiler in $\Delta[p]$. Demnach ist $\Omega(p,s)$ ein Normalteiler in $\Gamma[p]$ als Urbild eines Normalteilers unter einem Homomorphismus. Führt man nun π aus (2.18) und die kanonische Restklassenabbildung von $\Delta[p]$ nach $\Delta^s[p]$ hintereinander aus, so erhält man

$$\Gamma[p]/\Omega(p,s) \cong \Delta[p]/\Delta^s[p].$$

Also ist $\Omega(p,s)$ insbesondere von $\Gamma'[p]$ und $\{x^s;\, x \in \Gamma[p]\}$ erzeugt. Damit ist $\Omega(p,s)$ von endlichem Index in $\Gamma[p]$ und somit auch in Γ. Insgesamt folgt die Behauptung.

□

(2.20) Satz
Seien $p > 3$ eine Primzahl und $s \in \mathbb{N} \setminus \{1\}$ mit $\mathrm{ggT}(p,s) = 1$. Dann enthält $\Omega(p,s)$ keine Hauptkongruenzuntergruppe.

Beweis:
Wir nehmen $\Gamma[m] \subset \Omega(p,s)$ für ein $m \in \mathbb{N}$ an. Da mit Sicherheit $\Gamma[am] \subset \Gamma[m]$ für alle $a \in \mathbb{N} \setminus \{1\}$ ist, können wir weiterhin ohne Einschränkung annehmen, dass wir in der Situation

$$\Gamma\left[p^r st\right] \subset \Omega(p,s)$$

für $r, t \in \mathbb{N}$ mit $\mathrm{ggT}(p,t) = 1$ sind. Setze nun

$$L := \begin{bmatrix} 1 & 0 \\ p & 1 \end{bmatrix} \in \Gamma$$

und

$$R := \begin{bmatrix} 1 & p \\ 0 & 1 \end{bmatrix} \in \Gamma.$$

Weiter seien $q \in \mathbb{Z}$ und

$$A := \begin{bmatrix} a & b \\ c & d \end{bmatrix} := L^q RLR^{st-1} \in \Gamma.$$

Man rechnet leicht nach, dass

$$\frac{b}{p} = p^2(st-1) + st \tag{9}$$

und

$$\tfrac{d-1}{p^2} = q\tfrac{b}{p} + st - 1$$

gilt. Es folgt

$$\mathrm{ggT}\left(\tfrac{b}{p}, pst\right) = 1$$

(denn: Ist v eine Primzahl mit $v \mid pst$, so ist $v = p$ und teilt daher nicht bp^{-1}, da v die Zahl p, aber nicht st teilt, oder es ist $v \neq p$ und v teilt daher nicht bp^{-1}, da v die Zahl st, aber nicht p teilt). Aus diesem Grund kann q so gewählt werden, dass

$$\tfrac{d-1}{p^2} \equiv_{p^r st} 0$$

ist (beachte: Ist

$$u\tfrac{b}{p} \equiv_{p^r st} 1$$

für ein $u \in \mathbb{Z}$, so wähle $q \equiv_{p^r st} u(1-st)$). Letzteres impliziert $d \equiv_{p^r st} 1$ und daher wegen $\det(A) = ad - bc = 1$ auch $a \equiv_{p^r st} 1 + bc$. Setzen wir die Kongruenzen zusammen, so ergibt sich

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv_{p^r st} \begin{bmatrix} 1+bc & b \\ c & 1 \end{bmatrix} =: B.$$

Mit anderen Worten gilt

$$AB^{-1} \in \Gamma\,[p^r st]$$

und somit per Annahme

$$AB^{-1} \in \Omega(p,s).$$

Nun hat man $B = R^{\frac{b}{p}} L^{\frac{c}{p}}$ und daher

$$AB^{-1} = L^q RLR^{st-1} L^{-\frac{c}{p}} R^{-\frac{b}{p}}.$$

Man beachte, dass mit $R, L \in \Gamma[p]$ auch $A \in \Gamma[p]$ ist und somit insbesondere $b, c \in p\mathbb{Z}$ gilt. Zum Abschluss des Beweises zeigen wir gleich die Aussage, dass zu einem Potenzprodukt aus L und R, welches in $\Omega(p,s)$ lebt, die Summe der Exponenten von R ein Vielfaches von s sein muss. Ist diese Aussage bewiesen, so folgt aus $AB^{-1} \in \Omega(p,s)$ gerade

$$1 + (st-1) - \frac{b}{p} = st - \frac{b}{p} \equiv_s 0. \tag{10}$$

Setzen wir Gleichung (9) in (10) ein, so erhalten wir

$$st - \big(p^2(st-1) + st\big) = -p^2(st-1) \equiv_s 0. \tag{11}$$

Die Kongruenz (11) ist ein Widerspruch zur Voraussetzung $\operatorname{ggT}(p,s) = 1$ und im Gegensatz zur Annahme kann $\Omega(p,s)$ folglich keine Kongruenzuntergruppe enthalten. Insgesamt folgt die Behauptung.

Wir zeigen die noch offen stehende Aussage von oben. Nach (2.16) hat die Gruppe $\Gamma[p]$ ein freies Erzeugendensystem, bestehend aus R und einigen Matrizen der Form $(\lambda, \mu, \nu)_p$ (in der Notation von (2.14)). Bemerkung (2.15) ergibt nun

$$L = JT^pJ^{-1} = (0,0)_p = (0,1,1)_p,$$

also taucht R nach (2.17) nicht auf, wenn wir L als Produkt der freien Erzeuger von $\Gamma[p]$ schreiben. Die Elemente von

$$\Omega(p,s) = \langle \Gamma'[p] \cup \{x^s;\, x \in \Gamma[p]\} \rangle$$

haben aber unter den Produkten der freien Erzeuger gerade die Eigenschaft, dass die Exponentensumme an jedem der freien Erzeuger ein Vielfaches der Zahl s ist. Damit folgt die noch zu zeigende Aussage von oben.

□

§3 Diskontinuierliche Gruppen

In diesem Kapitel folgen wir den Darlegungen aus [KK98].

Ziel dieses Kapitels ist es, ein Kriterium zur Verifikation auf Diskontinuität einer Untergruppe von $\mathrm{SL}_2(\mathbb{R})$ zu liefern: Die Äquivalenz zwischen den Eigenschaften „diskret“ und „diskontinuierlich“ (vgl. (3.6)).

(3.1) Definition
Für eine Matrix

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(\mathbb{R})$$

sei der *Matrixbetrag* von M definiert durch

$$|M| := \sqrt{a^2 + b^2 + c^2 + d^2} \in \mathbb{R}_+.$$

Via (3.1) können alle metrischen Begriffe des $\mathbb{R}^4$ auf $\mathrm{M}_2(\mathbb{R})$ übertragen werden.

(3.2) Lemma
Seien $L, M \in \mathrm{M}_2(\mathbb{R})$. Dann gilt

$$|LM| \leq |L||M|.$$

Beweis:
Seien

$$L = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(\mathbb{R})$$

und

$$M = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \in \mathrm{M}_2(\mathbb{R}).$$

Dann gilt

$$LM = \begin{bmatrix} as + bu & at + bv \\ cs + du & ct + dv \end{bmatrix} \in \mathrm{M}_2(\mathbb{R})$$

und mit (3.1)

$$\begin{aligned}|LM|^2 &= (as+bu)^2 + (at+bv)^2 + (cs+du)^2 + (ct+dv)^2 \\ &= a^2s^2 + 2sabu + c^2s^2 + 2scdu + b^2u^2 + d^2u^2 + a^2t^2 + 2tabv + c^2t^2 + 2tcdv + b^2v^2 \\ &\quad + d^2v^2 \\ &= \left(a^2s^2 + a^2t^2 + b^2u^2 + b^2v^2 + c^2s^2 + c^2t^2 + d^2u^2 + d^2v^2\right) + 2sabu + 2scdu + 2tabv \\ &\quad + 2tcdv.\end{aligned}$$

Erneut mit (3.1) hat man sowohl

$$|L|^2 = a^2 + b^2 + c^2 + d^2$$

als auch

$$|M|^2 = s^2 + t^2 + u^2 + v^2$$

und damit

$$\begin{aligned}|L|^2|M|^2 &= \left(a^2+b^2+c^2+d^2\right)\left(s^2+t^2+u^2+v^2\right) \\ &= a^2s^2 + a^2t^2 + a^2u^2 + a^2v^2 + b^2s^2 + b^2t^2 + b^2u^2 + b^2v^2 + c^2s^2 + c^2t^2 + c^2u^2 + c^2v^2 \\ &\quad + d^2s^2 + d^2t^2 + d^2u^2 + d^2v^2 \\ &= \left(a^2s^2 + a^2t^2 + b^2u^2 + b^2v^2 + c^2s^2 + c^2t^2 + d^2u^2 + d^2v^2\right) + a^2u^2 + a^2v^2 + b^2s^2 \\ &\quad + b^2t^2 + c^2u^2 + c^2v^2 + d^2s^2 + d^2t^2.\end{aligned}$$

Die Gültigkeit der Ungleichung

$$|LM| \leq |L||M|$$

ist äquivalent zur Gültigkeit der Ungleichung

$$|LM|^2 \leq |L|^2|M|^2$$

und diese wiederum zur Gültigkeit von

$$2sabu + 2scdu + 2tabv + 2tcdv \leq a^2u^2 + a^2v^2 + b^2s^2 + b^2t^2 + c^2u^2 + c^2v^2 + d^2s^2 + d^2t^2. \quad (12)$$

Eine Äquivalenzumformung der Ungleichung (12) liefert

$$0 \leq a^2u^2 - 2sabu + b^2s^2 + a^2v^2 - 2tabv + b^2t^2 + c^2u^2 - 2scdu + d^2s^2 + c^2v^2 - 2tcdv + d^2t^2,$$

was äquivalent ist zu

$$0 \leq \underbrace{(au-bs)^2}_{\geq 0} + \underbrace{(av-bt)^2}_{\geq 0} + \underbrace{(cu-ds)^2}_{\geq 0} + \underbrace{(cv-dt)^2}_{\geq 0}. \quad (13)$$

Die Ungleichung (13) ist eine wahre mathematische Aussage für alle reelle Zahlen a, b, c, d,

s, t, u und v. Insgesamt folgt die Behauptung.

□

(3.3) Definition
Sei Λ eine Untergruppe von $\mathrm{SL}_2(\mathbb{R})$.
(a) Man nennt Λ *diskret*, wenn Λ eine diskrete Teilmenge von $\mathrm{M}_2(\mathbb{R})$ ist.
(b) Man nennt Λ *diskontinuierlich*, wenn für jedes $\tau \in \mathbb{H}$ und jede Folge $(M_k)_{k\in\mathbb{N}}$ von paarweise verschiedenen Matrizen M_k in Λ die Folge $(M_k\tau)_{k\in\mathbb{N}}$ keinen Häufungspunkt in $\mathbb{H}$ besitzt.

(3.4) Bemerkungen
Sei Λ eine diskontinuierliche Untergruppe von $\mathrm{SL}_2(\mathbb{R})$. Mit (3.3)(b) sind offensichtlich die folgenden Aussagen erfüllt:
(a) Für $\tau \in \mathbb{H}$ ist

$$\mathcal{M} := \{M\tau;\, M \in \Lambda\}$$

diskret in $\mathbb{H}$, das heißt, $\mathcal{M}$ hat als Menge keinen Häufungspunkt in $\mathbb{H}$.
(b) Für $\tau \in \mathbb{H}$ gilt

$$|\{M \in \Lambda;\, M\tau = \tau\}| < \infty.$$

(3.5) Lemma
Seien $\tau \in \mathbb{H}$ und $(L_k)_{k\in\mathbb{N}}$ eine Folge von Matrizen L_k in $\mathrm{SL}_2(\mathbb{R})$ mit

$$\lim_{k\to\infty} L_k\tau = \tau.$$

Dann ist die Folge $(L_k)_{k\in\mathbb{N}}$ beschränkt.

Beweis:
Nach (1.6) wähle eine Matrix $N \in \mathrm{SL}_2(\mathbb{R})$ so, dass $\tau = Ni$ ist. Seien

$$S_k := N^{-1}L_kN \in \mathrm{SL}_2(\mathbb{R})$$

und

$$T_k := J^{-1}S_kJ \in \mathrm{SL}_2(\mathbb{R}).$$

Dabei beachte man: Wegen $N, J \in \mathrm{SL}_2(\mathbb{R})$ gilt $\det(N) = \det(J) \neq 0$, also existieren die Inversen N^{-1} von N und J^{-1} von J. Demnach sind die Definitionen von S_k und T_k wohldefiniert. Nun folgt

$$\lim_{k\to\infty} S_ki = i$$

und

$$\lim_{k\to\infty} T_k i = i.$$

Somit hat man

$$\lim_{k\to\infty} \operatorname{Im}(S_k i) = 1$$

und

$$\lim_{k\to\infty} \operatorname{Im}(T_k i) = 1.$$

Sei etwa

$$S_k = \begin{bmatrix} a_k & b_k \\ c_k & d_k \end{bmatrix} \in \mathrm{SL}_2(\mathbb{R})$$

für $k \in \mathbb{N}$. Per Definition von T_k gilt

$$T_k = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a_k & b_k \\ c_k & d_k \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d_k & -c_k \\ -b_k & a_k \end{bmatrix}. \tag{14}$$

Wegen $S_k, T_k \in \mathrm{SL}_2(\mathbb{R})$ für alle k gilt $\det(S_k) = 1 = \det(T_k)$. Nach (1.7) hat man nun

$$\begin{aligned} 1 &= \lim_{k\to\infty} \operatorname{Im}(S_k i) \\ &= \lim_{k\to\infty} \frac{1}{|c_k i + d_k|^2} \\ &= \frac{1}{\lim\limits_{k\to\infty} c_k^2 + d_k^2} \end{aligned}$$

und mit Gleichung (14) auch

$$\begin{aligned} 1 &= \lim_{k\to\infty} \operatorname{Im}(T_k i) \\ &= \lim_{k\to\infty} \frac{1}{|-b_k i + a_k|^2} \\ &= \frac{1}{\lim\limits_{k\to\infty} (-b_k)^2 + a_k^2} \\ &= \frac{1}{\lim\limits_{k\to\infty} b_k^2 + a_k^2}, \end{aligned}$$

also

$$\lim_{k\to\infty} c_k^2 + d_k^2 = 1$$

und

$$\lim_{k\to\infty} b_k^2 + a_k^2 = 1.$$

Folglich sind die Matrizen S_k beschränkt. Per Definition von S_k und mit (3.2) sind auch die Matrizen L_k beschränkt, was zu zeigen war.

□

Alle Vorbereitungen für den Beweis der Hauptaussage von diesem Kapitel sind nun gemacht.

(3.6) Satz
Sei Λ eine Untergruppe von $\mathrm{SL}_2(\mathbb{R})$. Dann sind folgende Aussagen äquivalent:
(a) Es ist Λ diskret.
(b) Es ist Λ diskontinuierlich.
(c) Für je zwei Kompakta $\mathcal{K}$ und $\mathcal{L}$ von $\mathbb{H}$ gibt es nur endlich viele Matrizen $M \in \Lambda$ mit

$$(M\mathcal{K}) \cap \mathcal{L} \neq \emptyset.$$

Beweis:
Wir zeigen die Äquivalenz der Aussagen (a), (b) und (c) via Ringschlussprinzip.

(a) ⇒ (b):
Angenommen, Λ ist nicht diskontinuierlich. Dann existieren $\tau, \tau^* \in \mathbb{H}$ und eine Folge $(M_k)_{k\in\mathbb{N}}$ von paarweise verschiedenen Matrizen M_k in Λ mit

$$\lim_{k\to\infty} M_k\tau = \tau^*.$$

Es sei

$$N_k := M_k^{-1} M_{k+1} \in \Lambda.$$

Die Definition von N_k ist wohldefiniert: Wegen $M_k \in \Lambda \leq \mathrm{SL}_2(\mathbb{R})$ ist $\det(M_k) \neq 0$ für alle $k \in \mathbb{N}$, also existiert die Inverse M_k^{-1} von M_k. Nun gilt in der invarianten $\mathbb{H}$-Metrik und wegen ihrer Stetigkeit

$$\begin{aligned}\lim_{k\to\infty} |\tau, N_k\tau| &= \lim_{k\to\infty} \left|\tau, M_k^{-1}M_{k+1}\tau\right| \\ &= \lim_{k\to\infty} |M_k\tau, M_{k+1}\tau| \\ &= |\tau^*, \tau^*| \\ &= 0.\end{aligned}$$

Da die $\mathbb{H}$-Topologie mit der gewöhnlichen Topologie übereinstimmt (vgl. (1.9)), folgt

$$\lim_{k\to\infty} N_k\tau = \tau. \tag{15}$$

Nach (3.5) ist die Folge $(N_k)_{k\in\mathbb{N}}$ beschränkt. Da Λ nach Voraussetzung diskret ist, kommen unter den N_k nur endlich viele verschiedene Matrizen vor. Wegen der Identität (15) gibt es also eine Zahl $k_0 \in \mathbb{N}$ mit $N_k\tau = \tau$ für $k \geq k_0$ und $k \in \mathbb{N}$. Damit erhält man

$$M_{k+1}\tau = M_k N_k \tau = M_k\tau = \cdots = M_{k_0}\tau$$

für $k \geq k_0$, also

$$M_k^{-1} M_{k_0}\tau = \tau.$$

Wegen (3.5) und der Diskretheit von Λ gibt es nur endlich viele verschiedene unter den Matrizen $M_k^{-1}M_{k_0}$, also auch nur endlich viele unter den Matrizen M_k im Widerspruch zur Annahme.

(b) ⇒ (c):
Angenommen, es gibt kompakte Teilmengen $\mathcal{K}$ und $\mathcal{L}$ von $\mathbb{H}$ mit

$$(M\mathcal{K}) \cap \mathcal{L} \neq \emptyset$$

für unendlich viele $M \in \Lambda$. Nach (1.8) kann man sowohl $\mathcal{K}$ als auch $\mathcal{L}$ durch eine $\mathbb{H}$-Kreisscheibe

$$K := \{w \in \mathbb{H};\ |w, i| \leq r\}$$

mit einer reellen Zahl $r > 0$ ersetzen. Gilt demnach $w_k \in M_k K \cap K$ für unendlich viele Matrizen $M_k \in \Lambda$, so sind die

$$\tau_k = M_k^{-1} w_k$$

Punkte von K (beachte: Wegen $M_k \in \Lambda \leq \mathrm{SL}_2(\mathbb{R})$ ist $\det(M_k) \neq 0$ für alle k, also existiert die Inverse M_k^{-1} von M_k). Man erhält mit der Dreiecksungleichung sowie mit der Invarianzeigenschaft der $\mathbb{H}$-Metrik

$$|M_k i, i| \leq |M_k i, M_k\tau_k| + |M_k\tau_k, i| = |i, \tau_k| + |w_k, i| \leq r + r = 2r.$$

Dies impliziert, dass die Folge $(M_k i)_{k\in\mathbb{N}}$ einen Häufungspunkt in $\mathbb{H}$ besitzt, ein Widerspruch zur vorausgesetzten Diskontinuität von Λ.

(c) ⇒ (a):
Angenommen, Λ ist nicht diskret. Dann existiert eine Matrix $M \in \mathrm{M}_2(\mathbb{R})$ und eine Folge von paarweise verschiedenen Matrizen $M_k \in \Lambda$ mit komponentenweisem Limes

$$\lim_{k\to\infty} M_k = M.$$

Da $\mathrm{SL}_2(\mathbb{R})$ in $\mathrm{M}_2(\mathbb{R})$ abgeschlossen ist, folgt sofort $M \in \mathrm{SL}_2(\mathbb{R})$. Sei nun $\tau \in \mathbb{H}$. Dann gilt

$$\lim_{k\to\infty} M_k\tau = M\tau =: w.$$

Ist $\mathcal{K} := \{\tau\}$ und $\mathcal{L}$ eine kompakte Umgebung von w in $\mathbb{H}$, so gilt $M_k\tau \in \mathcal{L}$ für alle hinreichend großen Zahlen $k \in \mathbb{N}$, also

$$(M_k\mathcal{K}) \cap \mathcal{L} \neq \emptyset$$

für unendlich viele Zahlen k, ein Widerspruch zur Voraussetzung.

Insgesamt folgt die Behauptung.

□

(3.7) Beispiel
Betrachte

$$\mathcal{D} := \left\{ M = \begin{bmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{bmatrix};\, a,b,c,d \in \mathbb{Z},\ \det(M) = 1 \right\} \lneq \mathrm{SL}_2(\mathbb{R}). \tag{16}$$

Wir zeigen, dass $\mathcal{D}$ eine echte Untergruppe von $\mathrm{SL}_2(\mathbb{R})$ ist. Das neutrale Element E (bezüglich Matrixmultiplikation) erfüllt $E \in \mathcal{D}$, denn man wähle $a = d = 1 \in \mathbb{Z}$ sowie $b = c = 0 \in \mathbb{Z}$ und es ist $\det(E) = 1$. Seien weiter

$$M := \begin{bmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{bmatrix} \in \mathcal{D}$$

und

$$M' := \begin{bmatrix} a' & b'\sqrt{2} \\ c'\sqrt{2} & d' \end{bmatrix} \in \mathcal{D}.$$

Dann ist

$$N := MM' = \begin{bmatrix} aa' + 2bc' & (ab' + bd')\sqrt{2} \\ (ca' + dc')\sqrt{2} & 2b'c + d'd \end{bmatrix} \in \mathcal{D},$$

da $aa' + 2bc' \in \mathbb{Z}$, $ab' + bd' \in \mathbb{Z}$, $ca' + dc' \in \mathbb{Z}$, $2b'c + d'd \in \mathbb{Z}$ und

$$\det(N) = \det(M)\det(M') = 1.$$

Wegen $M \in \mathcal{D}$ gilt $\det(M) \neq 0$, also existiert die Inverse M^{-1} von M. Mit der aus der linearen Algebra bekannten Formel für die Inverse einer Matrix vom Format 2 x 2 gilt

$$M^{-1} = \tfrac{1}{\det(M)} \begin{bmatrix} d & -b\sqrt{2} \\ -c\sqrt{2} & a \end{bmatrix} \in \mathcal{D},$$

da $-b \in \mathbb{Z}$, $-c \in \mathbb{Z}$ sowie $a, d \in \mathbb{Z}$ ohnehin und $\det\left(A^{-1}\right) = (\det(A))^{-1} = 1$. Damit ist $\mathcal{D}$ eine Untergruppe von $\mathrm{SL}_2(\mathbb{R})$. In (16) kann keine Gleichheit gelten, da z. B.

$$P := \begin{bmatrix} -1 & -\sqrt{2} \\ \frac{1}{2}\sqrt{2} & 0 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{R}),$$

aber klarerweise $P \notin \mathcal{D}$ ist.

Desweiteren weisen wir die Diskontinuität von $\mathcal{D}$ nach. Seien $M, M' \in \mathcal{D}$ mit

$$M \neq M' \tag{17}$$

von oben gegeben. Dann gilt

$$M - M' = \begin{bmatrix} a - a' & (b - b')\sqrt{2} \\ (c - c')\sqrt{2} & d - d' \end{bmatrix}.$$

Wegen $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ sind auch $a - a' \in \mathbb{Z}$, $b - b' \in \mathbb{Z}$, $c - c' \in \mathbb{Z}$ und $d - d' \in \mathbb{Z}$. Würden gleichzeitig $a = a'$, $b = b'$, $c = c'$ und $d = d'$ gelten, so würde $M = M'$ folgen, aber die Gleichheit wurde in (17) ausgeschlossen. Das bedeutet, dass mindestens eine der Differenzen $a - a'$, $b - b'$, $c - c'$ oder $d - d'$ – O.B.d.A. sei es die Differenz $a - a'$ – die Bedingung $a - a' \neq 0$ und somit die Ungleichung $|a - a'| \geq 1$ erfüllt. Damit gilt in der Maximumsnorm für Matrizen

$$\begin{aligned} \|M - M'\|_{\max} &= \max\left\{ |a - a'|, |b - b'| \sqrt{2}, |c - c'| \sqrt{2}, |d - d'| \right\} \\ &\geq \max\left\{ |a - a'|, |b - b'|, |c - c'|, |d - d'| \right\} \\ &\geq 1, \end{aligned}$$

was zeigt, dass $\mathcal{D}$ diskret in $\mathrm{SL}_2(\mathbb{R})$ ist. Damit ist $\mathcal{D}$ nach (3.6) diskontinuierlich in $\mathrm{SL}_2(\mathbb{R})$.

◇

(3.8) Beispiel
Betrachte die Untergruppe

$$\mathcal{H}_\alpha := \left\langle J, \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \right\rangle \lneq \mathrm{SL}_2(\mathbb{R})$$

für eine reelle Zahl $\alpha > 0$, die sogenannte *Hecke-Gruppe* (benannt nach dem deutschen Mathematiker Erich Hecke). Hecke zeigte in [HE83], S. 599-616, dass $\mathcal{H}_\alpha$ genau dann diskret in $\mathrm{SL}_2(\mathbb{R})$ ist, wenn

$$\alpha \geq 2$$

oder

$$\alpha = 2\cos\left(\frac{\pi}{q}\right) \tag{18}$$

für $q \in \mathbb{N} \setminus \{1, 2\}$. Wähle z. B. $q = 6$. Mit Gleichung (18) ist $\alpha = \sqrt{3} > 0$, also ist die Gruppe

$$\mathcal{H}_{\sqrt{3}} = \left\langle J, \begin{bmatrix} 1 & \sqrt{3} \\ 0 & 1 \end{bmatrix} \right\rangle$$

diskret in $\mathrm{SL}_2(\mathbb{R})$. Nach (3.6) ist nun $\mathcal{H}_{\sqrt{3}}$ eine diskontinuierliche Untergruppe von $\mathrm{SL}_2(\mathbb{R})$.

$\diamond$

(3.9) Satz
Die Modulgruppe Γ ist eine diskontinuierliche Untergruppe von $\mathrm{SL}_2(\mathbb{R})$. Insbesondere sind alle Untergruppen von Γ diskontinuierlich in $\mathrm{SL}_2(\mathbb{R})$.

Beweis:
Analog zu (3.7) rechnet man die Diskretheit von Γ in $\mathrm{SL}_2(\mathbb{R})$ nach. Nach (3.6) ist Γ dann eine diskontinuierliche Untergruppe von $\mathrm{SL}_2(\mathbb{R})$. Wegen der Diskretheit von Γ in $\mathrm{SL}_2(\mathbb{R})$ ist das neutrale Element (bezüglich Matrixmultiplikation) $E \in \Gamma$ kein Häufungspunkt von Γ. Per Definition enthält jede Untergruppe von Γ ebenfalls dieses neutrale Element E, das kein Häufungspunkt der jeweiligen Untergruppe ist. Folglich ist jede Untergruppe von Γ diskret in $\mathrm{SL}_2(\mathbb{R})$, also nach (3.6) diskontinuierlich in $\mathrm{SL}_2(\mathbb{R})$. Insgesamt folgt nun die Behauptung.

$\square$

Literaturverzeichnis

[FH33] Frasch, H.: *Die Erzeugenden der Hauptkongruenzgruppen zu Primzahlstufen*, Mathematische Annalen, vol. 108, 1933

[FR87] Fricke, R.: *Über die Substitutionsgruppen, welche zu den aus dem Legendre'schen Integralmodul $k^2(\omega)$ gezogenen Wurzeln gehören*, Mathematische Annalen, vol. 28, 1887

[HE83] Hecke, E.: *Mathematische Werke*, Vandenhoek & Ruprecht, Göttingen, 1959

[KA13] Krieg, A.: *Funktionentheorie II*, Skript zur Vorlesung, Lehrstuhl A für Mathematik, RWTH Aachen, Aachen, 2013

[KK98] Koecher, M. und A. Krieg: *Elliptische Funktionen und Modulformen*, Springer-Verlag, Berlin-Heidelberg, 1998

[PG87] Pick, G.: *Über gewissen ganzzahlige lineare Substitutionen, welche sich nicht durch algebraische Congruenzen erklären lassen*, Mathematische Annalen, vol. 28, 1887

[RI58] Reiner, I.: *Normal subgroups of the unimodular group*, J. Math. 2, Illinois, 1958

[RR77] Rankin, R. A.: *Modular Forms and functions*, Cambridge University Press, Cambridge, 1977

[SS12] Schönnenbeck, S.: *Eine Präsentation der Modulgruppe*, Seminarausarbeitung zum Modul „Seminar zur Funktionentheorie II“, Lehrstuhl A für Mathematik, RWTH Aachen, Aachen, 2012