RWTH Aachen
Lehrstuhl A für Mathematik

Seminar in Funktionentheorie II
Prof. Dr. A. Krieg

Amal Dajour
Datum: 11. Oktober 2012

Untergruppen der Modulgruppe

Seminar zur Funktionentheorie II

Amal Dajour

Inhaltsverzeichnis

In diesem Vortrag werden Fundamentalbereiche zu Untergruppen der Modulgruppe konstruiert, und einige ihrer Eigenschaften eingeführt. Schließlich werden die Hauptkongruenzgruppen und Kongruenzgruppen als Spezialfälle von Untergruppen der Modulgruppe behandelt.

§ 1 Fundamentalbereiche von Untergruppen

In diesem Abschnitt wird zunächst der Fundamentalbereich einer Untergruppe von SL(2; $\mathbb{R}$) eingeführt. Anschließend werden wir ein Verfahren beschreiben, wie man Fundamentalbereiche zu Untergruppen der Modulgruppe SL(2; $\mathbb{Z}$) konstruieren kann.

— *Einleitung* —

Es bezeichnet $\Gamma = \mathrm{SL}(2;\mathbb{Z})$ die Modulgruppe und Λ eine Untergruppe von Γ.

(1.1) Definition (Fixgruppe)
Für $\tau \in \mathbb{H}$ definieren wir die Fixgruppe von τ

$$\Gamma_\tau := \{M \in \Gamma, M\tau = \tau\}\,. \qquad \diamond$$

(1.2) Definition
$\tau \in \mathbb{H}$ heißt Fixpunkt von Γ, wenn $\Gamma_\tau \neq \{\pm E\}$. $\diamond$

(1.3) Definition
Für $\varepsilon > 0$ nennen wir

$$\mathcal{V}_\varepsilon := \left\{\tau = x + iy \in \mathbb{H}; y \geq \varepsilon, |x| \leq \frac{1}{\varepsilon}\right\}$$

einen **Vertikalstreifen der Höhe** ε in $\mathbb{H}$. $\diamond$

(1.4) Satz
Ist $\varepsilon > 0$, so gibt es nur endlich viele $M \in \Gamma$ mit der Eigenschaft

$$M\mathcal{V}_\varepsilon \cap \mathcal{V}_\varepsilon \neq \emptyset. \qquad \diamond$$

Beweis
Seien $M \in \Gamma$ und $\tau \in \mathcal{V}_\varepsilon$ mit $M\tau \in \mathcal{V}_\varepsilon$. Wir setzen $\tau = x + iy$ mit $x, y \in \mathbb{R}$. Da M invertierbar ist, folgt mit dem Satz (1.1)XI[1]:

$$\mathrm{Im}(M\tau) = \frac{\det M}{|c\tau + d|^2}\mathrm{Im}\tau$$

Mit den Voraussetzungen haben wir $\det M = 1$ und $\mathrm{Im}\tau = y > \varepsilon > 0$, es folgt:

$$\frac{1}{\varepsilon} \geq \frac{1}{\mathrm{Im}\,(M\tau)} = \frac{|c\tau + d|^2}{y} = \frac{(cx+d)^2 + c^2y^2}{y} = \frac{(cx+d)^2}{y} + c^2y \geq c^2y \geq c^2\varepsilon. \quad (*)$$

Also ist

$$|c| \leq \frac{1}{\varepsilon.}$$

Damit gibt es nur endlich viele c für die $M\mathcal{V}_\varepsilon \cap \mathcal{V}_\varepsilon \neq \emptyset$ gelten kann.

- 1. Fall: $c = 0$

  Dann gilt $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ mit a, b, d aus $\mathbb{Z}$. Dies heißt: $\det M = ad = 1$. Daraus folgt $a = d$ mit $a, d \in \{-1, 1\}$. Also ist $M\tau = \frac{\tau+b}{1} = \tau + b$ mit $b \in \mathbb{Z}$. Andererseits für $\tau \in \mathcal{V}_\varepsilon$ haben wir $|\mathrm{Re}(\tau)| \leq \frac{1}{\varepsilon}$. Nun wählen wir $|b| > \frac{2}{\varepsilon}$.
  Es folgt

  $$|\mathrm{Re}\,(M\tau)\,| = |\mathrm{Re}\,(\tau + b)\,| \geq |b| - |\mathrm{Re}\,(\tau)\,| > \frac{1}{\varepsilon}.$$

  Also es gilt

  $$|\mathrm{Re}\,(M\tau)\,| > \frac{1}{\varepsilon}.$$

  Damit gibt es für $c = 0$ nur endlich viele $M \in \Gamma$, die die Behauptung erfüllen.

- 2. Fall: $c \neq 0$.

  Da $c \in \mathbb{Z}$ ist $c \geq 1$ oder $c \leq -1$. Also ist $c^2 \geq 1$. Aus $(*)$ folgt für c:

  $$\frac{1}{\varepsilon} \geq c^2y \geq y,$$

  und damit

  $$\frac{1}{\varepsilon} \geq \frac{(cx+d)^2}{y} + c^2y \geq \frac{(cx+d)^2}{y} \geq \varepsilon\,(cx+d)^2.$$

  So erhalten wir

  $$\frac{1}{\varepsilon^2} \geq (cx+d)^2 = |cx+d|^2, \text{ woraus folgt } \frac{1}{\varepsilon} \geq |cx+d| \geq |d| - |cx|.$$

Also ist

$$|d| \;\leq\; |cx| + \frac{1}{\varepsilon} \;=\; |c||x| + \frac{1}{\varepsilon} \;=\; |c||\mathrm{Re}(\tau)| + \frac{1}{\varepsilon} \;\leq\; \frac{1}{\varepsilon^2} + \frac{1}{\varepsilon},$$

da $|c| \leq \frac{1}{\varepsilon}$ gilt und nach Voraussetzung ist $\mathrm{Re}(\tau) \leq \frac{1}{\varepsilon}$.

Es folgt, dass für d nur endlich Möglichkeiten gibt.
Nach dem Ergänzungs-Lemma XI (2.1) [1] unterscheiden sich zwei Matrizen aus Γ mit der gleichen zweiten Zeile nur um einen Linksseitigen Faktor der Form
$T^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ mit $m \in \mathbb{Z}$.
Dies heißt, dass die Matrizen mit dieser Eigenschaft darstellbar durch die Matrix der Form $T^m M$ sind, mit $m \in \mathbb{Z}$ beliebig, wobei $M \in \Gamma$ fest ist, die gleiche zweite Zeile hat, und erfüllt $M\mathcal{V}_\varepsilon \cap \mathcal{V}_\varepsilon \neq \emptyset$.

Sei nun $T^m M\mathcal{V}_\varepsilon \cap \mathcal{V}_\varepsilon \neq \emptyset$. Dann existiert $x + iy = \tau \in \mathcal{V}_\varepsilon$ mit $T^m M\tau \in \mathcal{V}_\varepsilon$ und $x, y \in \mathbb{R}$. Es gilt:

$$|\mathrm{Re}\,(T^m M\tau)\,| \leq \frac{1}{\varepsilon}.$$

Andererseits ist

$$\begin{aligned}
|\mathrm{Re}\,(M\tau)| &= \left|\mathrm{Re}\left(\frac{a(x+iy)+b}{c(x+iy)+d}\right)\right| \\
&= \left|\mathrm{Re}\left(\frac{(ax+b)+iay}{(cx+d)+icy}\right)\right| \\
&= \left|\mathrm{Re}\left(\frac{((ax+b)+iay)\,(cx+d)-icy)}{((cx+d)+icy)\,(cx+d)-icy)}\right)\right| \\
&= \left|\frac{(ax+b)(cx+d)+acy^2}{(cx+d)^2+c^2y^2}\right| \\
&= \left|\frac{(ax+b)(cx+d)}{(cx+d)^2+c^2y^2} + \frac{acy^2}{(cx+d)^2+c^2y^2}\right| \\
&\leq \left|\frac{(ax+b)(cx+d)}{(cx+d)^2+c^2y^2}\right| + \left|\frac{acy^2}{(cx+d)^2+c^2y^2}\right|
\end{aligned}$$

Da $c^2 \geq 1$, ist $(cx+d)^2 + c^2y^2 \geq c^2y^2 \geq \varepsilon^2 c^2 \geq \varepsilon^2$. Damit folgt, dass

$$\begin{aligned}
|\mathrm{Re}\,(M\tau)| &\leq \left|\frac{(ax+b)(cx+d)}{\varepsilon^2}\right| + \left|\frac{acy^2}{c^2y^2}\right| \\
&= \left|\frac{(ax+b)(cx+d)}{\varepsilon^2}\right| + \left|\frac{a}{c}\right| \\
&\leq \delta
\end{aligned}$$

Wegen $|x| = |\mathrm{Re}(\tau)| \leq \frac{1}{\varepsilon}$, ist $|x|$ beschränkt. Da $\left|\frac{(ax+b)(cx+d)}{\varepsilon^2}\right| + \left|\frac{a}{c}\right|$ ein Polynom 2. Grad ist, ist der Ausdruck auch beschränkt.

Ohne Einschränkung der Allgemeinheit sei $\frac{1}{\varepsilon} \leq \delta$. Wir setzen $\tau' = M\tau$ und wähle $|m| > 2\delta$, dann gilt:

$$\begin{aligned} \left|\mathrm{Re}\left(T^m\tau'\right)\right| &= \left|\mathrm{Re}\left(\frac{\tau'+m}{1}\right)\right| \\ &= \left|\mathrm{Re}\left(\tau'+m\right)\right| \\ &\geq |m| - |\mathrm{Re}\left(\tau\right)| \\ &\geq 2\delta - \delta \\ &\geq \delta \geq \frac{1}{\varepsilon} \end{aligned}$$

Es folgt, dass $T^m\tau' = T^m M\tau \notin \mathcal{V}_\varepsilon$ für alle $\tau \in \mathcal{V}_\varepsilon$ gilt. Demnach gibt es nur endlich viele M, die $M\mathcal{V}_\varepsilon \cap \mathcal{V}_\varepsilon \neq \emptyset$ erfüllen. □

— *Definitionen und Eigenschaften* —

(1.5) Definition (Fundamentalbereiche von Untergruppen)
Sei zunächst Δ eine beliebige Untergruppe von SL(2;$\mathbb{R}$). Eine Teilmenge $\mathcal{F}$ von $\mathbb{H}$ nennt man **Fundamentalbereich** von Δ, wenn gilt:

(FB.0) $\mathcal{F}$ ist (relativ) abgeschlossen in $\mathbb{H}$.

(FB.1) Zu jedem $\tau \in \mathbb{H}$ gibt es $M \in \Delta$ mit $M\tau \in \mathcal{F}$.

(FB.2) Gehören τ und $M\tau$, wobei $M \in \Delta$, zum offenen Kern von $\mathcal{F}$, so gilt $M = \pm E$.◇

Eine Umformulierung dieser Definition ist:

(1.6) Definition (Äquivalente Definition)
Bezeichnet man $M\mathcal{F} := \{M\tau; \tau \in \mathcal{F}\}$ das Bild von $\mathcal{F}$ unter der Transformation $\tau \mapsto M\tau$, so ist ein (relativ) abgeschlossenes $\mathcal{F} \subset \mathbb{H}$ genau dann ein Fundamentalbereich von Δ, wenn gilt:

(FB.1*) $\mathbb{H} = \bigcup_{M\in\Delta} M\mathcal{F}$

(FB.2*) $\overset{\circ}{\mathcal{F}} \cap M\overset{\circ}{\mathcal{F}} \neq \emptyset, M \in \Delta$, so folgt $M = \pm E$ ◇

(1.7) Bemerkung
Sei $\Delta = \Lambda$ eine Untergruppe von Γ. Da Γ abzählbar ist, folgt dass Λ auch abzählbar ist. In diesem Fall folgt aus (FB.1*) und dem Satz von Baire [6], dass jeder Fundamentalbereich innere Punkte besitzt. ◇

(1.8) Bemerkung
Anstelle von dem Begriff **Fundamentalbereich** verwendete man früher auch das Wort **Diskontinuitätsbereich**. R. Dedekind benutzte den Ausdruck **Hauptfeld** dafür (*Ges. Math. Werke I, 174-201*). ◇

— *Konstruktion* —

(1.9) Bezeichnungen

- $\mathbb{F} := \left\{\tau \in \mathbb{H}; -\frac{1}{2} < \mathrm{Re}\tau \leq \frac{1}{2}, |\tau| \geq 1 \text{ und } |\tau| > 1 \text{ für } -\frac{1}{2} < \mathrm{Re}\tau < 0\right\}$ ist der exakte Fundamentalbereich der Modulgruppe Γ.
- $\overline{\mathbb{F}} := \left\{\tau \in \mathbb{H}; |\mathrm{Re}\tau| \leq \frac{1}{2}, |\tau| \geq 1\right\}$.

(Bild) ◇

(1.10) Bemerkung
$\overline{\mathbb{F}}$ ist nach Satz (2.2)[2] ein Fundamentalbereich von Γ nach der Definition (1.5), denn ist $\overline{\mathbb{F}}$ abgeschlossen in $\mathbb{H}$ und (FB.0) und (FB.1) sind erfüllt nach Satz(2.6)XI[1]. ◇

Sei nun Λ' die von Λ und $-E$ erzeugte Untergruppe von Γ und

$$\Gamma = \bigcup_{1 \leq \nu \leq [\Gamma:\Lambda']} \Lambda' M_\nu \qquad (1)$$

eine disjunkte Zerlegung von Γ in Rechtsnebenklassen nach Λ'. So wird Γ in (1) als endliche oder abzählbar unendliche Vereinigung dargestellt, je nachdem ob der Index $[\Gamma : \Lambda'] = \sharp\,(\Gamma/\Lambda')$ endlich ist oder nicht.

Die Repräsentanten M_ν aus (1) sind in Γ eindeutig bestimmt bis auf die Reihenfolge und einen linksseitigen Faktor aus Λ' . Man setzt trotzdem

$$\mathbb{F}(\Lambda) := \bigcup_{1 \leq \nu \leq [\Gamma:\Lambda']} M_\nu \overline{\mathbb{F}}.$$

(1.11) Satz
$\mathbb{F}(\Lambda)$ ist ein Fundamentalbereich von Λ. ◇

Beweis
Sei $\Lambda \neq \{E\}$. Prüfe (FB.0)-(FB.2) aus der Definition (1.5).

- Zu (1):

  Sei $\tau \in \mathbb{H}$ und $\tau \notin \mathbb{F}(\Lambda)$. Sei nun $\varepsilon > 0$ mit

  $$\mathcal{V}_\varepsilon := \left\{ \tau = x + iy \in \mathbb{H};\ \ y \geq \varepsilon,\ \ |x| \leq \frac{1}{\varepsilon} \right\}$$

  der Vertikalstreifen der Höhe ε in $\mathbb{H}$. Wähle ε so, dass $\overline{\mathbb{F}} \subset \mathcal{V}_\varepsilon$ und τ innerer Punkt von $\mathcal{V}_\varepsilon$ ist.

  Vergleich [1]XI §2 muss $\varepsilon \leq \frac{1}{2}\sqrt{3}$ gewählt werden. Nach (1.5) gibt es nur endlich viele $M \in \Gamma$ mit $M\mathcal{V}_\varepsilon \cap \mathcal{V}_\varepsilon \neq \emptyset$. Da $\overline{\mathbb{F}} \subset \mathcal{V}_\varepsilon$ und $\{M_\nu;\ 1 \leq \nu \leq [\Gamma : \Lambda']\} \subset \Gamma$, existieren nur endlich viele ν mit $M_\nu \overline{\mathbb{F}} \cap \mathcal{V}_\varepsilon \neq \emptyset$.

  Andererseits ist $M_\nu \overline{\mathbb{F}}$ abgeschlossen und $\tau \notin M_\nu \overline{\mathbb{F}}$ für alle $1 \leq \nu \leq [\Gamma : \Lambda']$. Also τ kann kein Häufungspunkt in $M_\nu \overline{\mathbb{F}}$ sein. Da aber nur endlich viele ν gibt, so dass $M_\nu \overline{\mathbb{F}} \cap \mathcal{V}_\varepsilon \neq \emptyset$ ist und gleichzeitig τ innerer Punkt von $\mathcal{V}_\varepsilon$ ist, folgt dass τ auch kein Häufungspunkt von $\mathbb{F}(\Lambda)$ ist, und somit ist $\mathbb{F}(\Lambda)$ relativ abgeschlossen in $\mathbb{H}$, da τ beliebig gewählt war.

- Zu (2):

  Zu $\tau \in \mathbb{H}$ wählt man nach Satz(2.6)XI[1] ein $L \in \Gamma$ mit $L\tau \in \mathbb{F}$. Nach (1) gibt es ein $M \in \Lambda$ und ein $1 \leq \nu \leq [\Gamma : \Lambda']$ mit $L^{-1} = \pm M^{-1} M_\nu$. Dies bedeutet $E = \pm M^{-1} M_\nu L$. Es folgt $\pm M = M_\nu L$.

  Da $L\tau \in \mathbb{F}$ ist, ist $M\tau = M_\nu L\tau \in M_\nu \overline{\mathbb{F}} \subseteq \mathbb{F}(\Lambda)$.

- Zu (3):

  Sei $M \in \Lambda$ sowie τ und $M\tau$ innere Punkte von $\mathbb{F}(\Lambda)$ und $\mathcal{U}$ eine offene Umgebung von τ in $\mathbb{F}(\Lambda)$. Nun soll $\mathcal{U}$ gewählt werden, dass $M\mathcal{U}$ genau in $\mathbb{F}(\Lambda)$ liegt. Da die Translation $\tau \to M\tau$ eine Homöomorphismus ist, gilt $M\mathcal{U} \in \mathcal{U}(M\tau)$, wobei $\mathcal{U}(M\tau)$ das System aller Umgebungen von $M\tau$ bezeichnet. Und da $M\tau$ selber ein innere Punkte von $\mathbb{F}(\Lambda)$ ist, kann man nach eventueller Verkleinerung von $\mathcal{U}$ annehmen, dass $M\mathcal{U} = \{Mz; z \in \mathcal{U}\} \subset \mathbb{F}(\Lambda)$ gilt. Da $\mathcal{U} \subset \mathbb{F}(\Lambda) = \bigcup_{1 \leq \nu \leq [\Gamma:\Lambda']} M_\nu \overline{\mathbb{F}}$, hat man

  $$\mathcal{U} = \bigcup_{1 \leq \nu \leq [\Gamma:\Lambda']} \mathcal{U}_\nu \quad \text{mit} \quad \mathcal{U}_\nu := \mathcal{U} \cap M_\nu \overline{\mathbb{F}}.$$

Da $\mathcal{U}_\nu := \mathcal{U} \cap M_\nu \overline{\mathbb{F}}$ abgeschlossen in $\mathcal{U}$ ist, folgt mit dem Satz von Baire [6], dass mindestens eine Menge $\mathcal{U}_\nu$ innere Punkte besitzt.

Sei dies ohne Einschränkung der Allgemeinheit $\mathcal{U}_1$, mit $\overset{\circ}{\mathcal{U}}_1 \neq \emptyset$ und $z \in \overset{\circ}{\mathcal{U}}_1$. Wegen $\mathcal{U}_1 \subset M_1 \overline{\mathbb{F}}$, existiert ein $w \in \overline{\mathbb{F}}$ mit $w := M_1^{-1} z$. Da z ein innerer Punkt von $\mathcal{U}_1$ ist, und die Translation $\tau \mapsto M_1 \tau$ ein Homöomorphismus ist, ist w dann ein innerer Punkt von $\mathbb{F}$. Also es gilt $M_1^{-1} \mathcal{U}_1 \subset \mathbb{F}$.

Weiter gibt es ein ν mit $Mz \in M_\nu \overline{\mathbb{F}}$. Dann ist aber $w' := M_\nu^{-1} M M_1 w = M_\nu^{-1} M z$ ein Punkt von $\overline{\mathbb{F}}$. Indem man w' gegebenenfalls mit J oder T in $\mathbb{F}$ abbildet, wobei J und T die Erzeuger von Γ sind.

Angenommen $w' \notin \mathbb{F}$. Es folgt, dass

$$w \in \overline{\mathbb{F}} \setminus \mathbb{F} = \{\tau \in \mathbb{H} : \mathrm{Re}(\tau) = -\frac{1}{2}, |\tau| \geq 1\} \cup \{\tau \in \mathbb{H} : -\frac{1}{2} < \mathrm{Re}(\tau) < 0, |\tau| = 1\}.$$

Ist $w' \in \{\tau \in \mathbb{H} : \mathrm{Re}(\tau) = -\frac{1}{2}, |\tau| \geq 1\}$, dann kann man w' genau mit $w' \to Tw' = w' + 1$ nach $\mathbb{F}$ abbilden. Damit ist

$$Tw' \in \{\tau \in \mathbb{H} : \mathrm{Re}(\tau) = \frac{1}{2}, |\tau| \geq 1\} \not\subseteq \overset{\circ}{\mathbb{F}}.$$

Da $w \in \overset{\circ}{\mathbb{F}}$ ist, folgt $w \neq Tw'$. Dies ist eine Widerspruch zum Satz(2.6)XI[1]. Analog folgt es für die Matrix J.

Aus dem Satz (2.6)XI[1] folgt, dass

$$w = w' \quad \text{sowie} \quad M_\nu^{-1} M M_1 = \pm E$$

Also

$$M_\nu = \pm M M_1. \qquad (2)$$

Nach Voraussetzung ist $\pm M \in \Lambda'$, folgt $\Lambda' (\pm M M_1) = \Lambda' M_1 = \Lambda' M_\nu$. Da die $\Lambda' M_\nu$ paarweise disjunkt sind, ist dann $M_1 = M_\nu$ und aus (2) ist $\nu = 1$ und $M = \pm E$. □

§ 2 Hauptkongruenzgruppen

In diesem Abschnitt betrachten wir die Hauptkongruenzgruppen und konstruieren ihren zugehörigen Fundamentalbereich.

— *Definitionen und Eigenschaften der Hauptkongruenzgruppen* —

(2.1) Erinnerung
Wir definieren die folgende Menge:
$\mathrm{Mat}(2;\mathbb{Z}) := \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a,b,c,d \in \mathbb{Z} \right\}$. ◇

(2.2) Definition (Kongruenz)
Seien L und $M \in \mathrm{Mat}(2;\mathbb{Z})$ und $n \geq 1$ eine feste natürliche Zahl. $L \equiv M (\mathrm{mod}\ n)$ bezeichnet die **Kongruenz** für L und M, falls eine Matrix $X \in \mathrm{Mat}(2;\mathbb{Z})$ existiert, so dass $L = M + nX$ gilt. ◇

(2.3) Lemma
Es gilt : $LM \equiv L'M' (\mathrm{mod}\ n)$, falls $L \equiv L' (\mathrm{mod}\ n)$ und $M \equiv M' (\mathrm{mod}\ n)$. ◇

Beweis
Seien $L \equiv L' (\mathrm{mod}\ n)$ und $M \equiv M' (\mathrm{mod}\ n)$. Dann gilt

$$L = L' + nX \ \text{ und } \ M = M' + nX' \ \text{ mit } \ X, X' \in \mathrm{Mat}(2;\mathbb{Z})$$

Es folgt, dass

$$\begin{aligned} LM &= (L' + nX)(M' + nX') \\ &= L'M' + nXM' + nL'X' + n^2XX' \\ &= L'M' + n \underbrace{(XM' + L'X' + nXX')}_{:= X'' \in \mathrm{Mat}(2;\mathbb{Z})} \\ &= L'M' + nX''. \end{aligned}$$ □

(2.4) Definition (Hauptkongruenzgruppe)
Sei $n \in \mathbb{N}$. Dann heißt $\Gamma[n] := \{M \in \Gamma; M \equiv E (\mathrm{mod}\ n)\}$ die **Hauptkongruenzgruppe** der **Stufe** n. ◇

Nun betrachten wir die kanonische Projektion

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad x \to \overline{x} := x + n\mathbb{Z},$$

und setzen sie auf 2×2 Matrizen fort

$$\mathrm{Mat}(2;\mathbb{Z}) \to \mathrm{Mat}(2;\mathbb{Z}/n\mathbb{Z}), \qquad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \overline{M} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}.$$

Zunächst zeigen wir, dass für $n \in \mathbb{N}$ die Abbildung $\Phi : \Gamma \to \mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z})$ ein surjektiver Gruppenhomomorphismus ist. Dafür benötigen wir das folgende Lemma.

(2.5) Lemma
Seien $a, b, c \in \mathbb{Z}$, $c \neq 0$ und $\mathrm{ggT}(a, b, c) = 1$. Dann existiert ein $x \in \mathbb{Z}$ mit $\mathrm{ggT}(a + xb, c) = 1$. ◇

Beweis
Sei x das Produkt aller Primzahlen p, die c aber nicht a teilen, das heißt $x = \prod_{p \nmid a, p \mid c} p$, wobei das leere Produkt gleich 1 sei. Angenommen es existiert ein $q \in \mathbb{P}$ mit $q \mid (a + xb)$ und $q \mid c$.

1. Fall: $q \mid a$.

   Dann ist q nicht in der Primfaktorzerlegung von x enthalten. Es folgt $q \nmid x$. Da aber $q \mid (a + xb)$, folgt $q \mid b$. Nach Voraussetzung ist $q \mid c$, was zu einem Widerspruch zu $\mathrm{ggT}(a, b, c) = 1$ führt.

2. Fall: $q \nmid a$.

   Nach Voraussetzung ist $q \mid c$. q ist also in der Primfaktorzerlegung von x enthalten und das heißt $q \mid x$. Da $q \mid (a + xb)$, folgt $q \mid a$.
   Auch das ist ein Widerspruch.

Es folgt, dass $a + xb$ und c teilerfremd sind. □

(2.6) Korollar
Sei $M, L \in \Gamma$. M und L liegen genau dann in derselben Rechtsnebenklassen von $\Gamma[n]$, wenn $M \equiv L \pmod{n}$. ◇

Beweis

- Seien $M, L \in \Gamma$ mit $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ und $M \equiv L \pmod{n}$. Dann existiert eine Matrix $X = \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} \mathrm{Mat}(2; \mathbb{Z})$, so dass $M = \begin{pmatrix} a + nk_1 & b + nk_2 \\ c + nk_3 & d + nk_4 \end{pmatrix}$ mit k_1, k_2, k_3 und $k_4 \in \mathbb{Z}$. Da $\det(L) = ad - bc = 1$, ist $L^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

$$\begin{aligned} L^{-1}M &= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a+nk_1 & b+nk_2 \\ c+nk_3 & d+nk_4 \end{pmatrix} \\ &= \begin{pmatrix} ad-bc+n(dk_1-bk_3) & bd-db+n(dk_2-bk_4) \\ ac-ac+n(ak_3-ck_1) & ad-bc+n(ak_4-ck_2) \end{pmatrix} \\ &= \begin{pmatrix} 1+n(dk_1-bk_3) & 0+n(dk_2-bk_4) \\ 0+n(ak_3-ck_1) & 1+n(ak_4-ck_2) \end{pmatrix} \\ &= E+n\begin{pmatrix} dk_1-bk_3 & dk_2-bk_4 \\ ak_3-ck_1 & ak_4-ck_2 \end{pmatrix} \\ &\equiv E \pmod{n} \end{aligned}$$

Also $L^{-1}M \in \Gamma[n]$. Damit ist $M \in L\Gamma[n]$. Analog folgt auch $L \in \Gamma[n]M$.

- Sei nun $M \in L\Gamma[n]$. Dann existiert eine Matrix $M' \in \Gamma[n]$ und $X \in \mathrm{Mat}\,(2,\mathbb{Z})$ mit

$$\begin{aligned} M &= LM' \\ &= L\,(E+nX) \\ &= L+nLx \\ &\equiv L \pmod{n} \end{aligned}$$

Damit folgt die Behauptung. □

(2.7) Satz
Für $n \in \mathbb{N}$ ist die Abbildung

$$\begin{aligned} \Phi : \Gamma &\to \mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z}) \\ M &\to \overline{M} \end{aligned}$$

ein surjektiver Gruppenhomomorphismus mit Kern $\Gamma[n]$. Damit ist $\Gamma[n]$ ein Normalteiler von endlichem Index in Γ und $\Gamma/\Gamma[n] \cong \mathrm{SL}\,(2;\mathbb{Z}/n\mathbb{Z})$. ◇

Beweis

- Wohldefiniertheit:
  Sei $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, n \in \mathbb{N}$ und $\Phi(M) = \overline{M} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$, mit

$$\det \overline{M} = \overline{a}\overline{d} - \overline{b}\overline{c} \; = \overline{ad-bc} = \overline{\det M} = \overline{1} = 1.$$

  Es folgt $\Phi(\Gamma) \subseteq \mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z})$.

- Gruppenhomomorphismus:

  Seien $L, M \in \Gamma$. Mit Lemma (2.3) gilt: $\Phi(ML) = \overline{ML} = \overline{M} \cdot \overline{L} = \Phi(M)\Phi(L)$. Es folgt, dass Φ ein Gruppenhomomorphismus ist.

  Sei nun $M \in \text{Kern}(\Phi)$. Dies bedeutet, dass $\Phi(M) = \overline{E}$ ist. Das heißt, dass $M = E + nX$, für $X \in \text{Mat}(2;\mathbb{Z})$. Dies ist Äquivalent zu $M \equiv E \pmod{n}$. Es folgt, dass $M \in \Gamma[n]$. Also $\text{Kern}(\Phi) = \Gamma[n]$ und damit ist $\Gamma[n]$ ein Normalteiler in Γ.

- Surjektivität:

  Sei $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}(2;\mathbb{Z})$ mit $\overline{M} \in \text{SL}(2;\mathbb{Z}/n\mathbb{Z})$.

  Ohne Einschränkung der Allgemeinheit sei $c \neq 0$. Dies ist möglich, da man sonst c durch $c + n$ ersetzen kann kann, ohne dass sich $\overline{M}$ ändert.

  Nun ist zu zeigen, dass $\overline{M}$ ein Urbild in Γ besitzt. Wenn $\overline{M} \in \text{SL}(2;\mathbb{Z}/n\mathbb{Z})$ ist, muss gelten, dass $\det(\overline{M}) = \overline{a}\overline{d} - \overline{b}\overline{c} \equiv 1 (\text{mod } n)$.
  Es folgt, dass ein $k \in \mathbb{Z}$ mit $ad - bc - kn = 1$ existiert, woraus $\text{ggT}(d, n, c) = 1$ folgt. Nach Lemma (2.5) gibt es ein $x \in \mathbb{Z}$ so ,dass $\text{ggT}(d + xn, c) = \text{ggT}(m, c) = 1$ mit $m = d + xn$ gilt. Daraus folgt:

$$am - bc = ad - bc + axn = 1 + kn + axn = 1 + n\underbrace{(k + ax)}_{:=s},\ s \in \mathbb{Z}.$$

  Da $\text{ggT}(c, m) = 1$ ist, folgt, dass $k', k'' \in \mathbb{Z}$ existieren, so dass $ck' - k''m = 1$ ist. Hieraus ergibt sich, dass $ck's - k''ms = s$ ist. Nun setze man $k's = \alpha$ und $k''s = \beta$, was bedeutet, dass $c\alpha - m\beta = s$ ist.

  Jetzt betrachten wir die Matrix $L = \begin{pmatrix} a + \beta n & b + \alpha n \\ c & d + xn \end{pmatrix} \in \text{SL}(2;\mathbb{Z}/n\mathbb{Z})$. Da gilt

$$\begin{aligned} \det(L) &= (a + \beta n)(d + xn) - (b + \alpha n)c \\ &= (a + \beta n)m - (b + \alpha n)c \\ &= am + \beta nm - bc - \alpha nc \\ &= am - bc + n(\beta m - \alpha c) \\ &= 1 + ns - ns \\ &= 1. \end{aligned}$$

  Mithin existiert zu $\overline{M} \in \text{SL}(2;\mathbb{Z}/n\mathbb{Z})$ eine Matrix $L \in \Gamma$ mit $\Phi(L) = \overline{L} = \overline{M}$. Damit ist gezeigt, dass Φ surjektiv ist.

Gemäß dem Homomorphiesatz für Gruppen folgt, dass

$$\Gamma/\Gamma[n] \cong \mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z}).$$

Und daraus folgt wiederum, dass $[\Gamma : \Gamma[n]] = \sharp\,\mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z}) < \infty$ ist. □

(2.8) Korollar
$[\Gamma : \Gamma[n]] = \sharp\,\mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z}) = n^3 \prod_{p|n}(1 - \frac{1}{p^2})$ für $n \geq 2$. ◇

Einen Beweis findet man bei H. Maass [4].

Nun betrachten wir die Fixpunkte von $\Gamma[n]$.

(2.9) Proposition
Für $n \geq 2$ besitzt $\Gamma[n]$ keine Fixpunkte, das heißt, aus $M\tau = \tau$ für ein $\tau \in \mathbb{H}$ und $M \in \Gamma[n]$ folgt $M = \pm E$ im Fall $n = 2$ und $M = E$ im Fall $n > 2$. ◇

Beweis
Sei $M \in \Gamma[n]$ mit $M \neq \pm E$ und $M\tau = \tau$. Da $\Gamma[n]$ eine Untergruppe von Γ, folgt dass τ ein Fixpunkt von Γ ist. Aus Korollar(2.8)XI[1] folgt mit einem geeigneten $L \in \Gamma$, dass:

$$\tau = Li \quad \text{oder} \quad \tau = L\rho.$$

Nach Voraussetzung wissen wir, dass $M\tau = \tau$, und damit ergibt sich:

$$MLi = Li \quad \text{oder} \quad ML\rho = \rho.$$

Nun können wir Satz(2.6)XI[1] anwenden und erhalten wir:

$$L^{-1}ML = \pm J \quad \text{oder} \quad L^{-1}ML = \pm U, \pm U^2.$$

Nach Satz (2.7) ist $\Gamma[n]$ ein Normalteiler in Γ. Dies bedeutet, dass für alle $L \in \Gamma$ und $M \in \Gamma[n]$ gilt $L^{-1}ML \in \Gamma[n]$. Also sollen $\pm J$, $\pm U$ oder $\pm U^2$ in $\Gamma[n]$ für $n > 2$ liegen. Dies ist ein Widerspruch zur Annahme, denn es existiert keine Matrizen X, Y, Z aus Mat(2;$\mathbb{Z}$), so dass:

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

$$\pm U = \pm \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} = E + nY \quad \text{oder}$$

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

gilt. Also für $n = 2$ folgt, dass $M = \pm E$. Für $n > 2$ ist $-E \not\equiv_n E$ und $-E \notin \Gamma[n]$, damit folgt $M = E$. □

— *Konstruktion eines Fundamentalbereichs von* $\Gamma[2]$ —

Betrachten wir den Fall $n = 2$ als Beispiel. Nach dem Satz (2.7) wissen wir

$$\Gamma/\Gamma[2] \cong \mathrm{SL}(2;\mathbb{Z})$$

Und mit dem Korollar (2.8) wissen wir auch

$$[\Gamma : \Gamma[2]] = \sharp\mathrm{SL}(2;\mathbb{Z}) = 2^3 \prod_{p|2} \left(1 - \frac{1}{p^2}\right) = 6$$

Das Vertretersystem der Nebenklassen von $\Gamma[2]$ in Γ enthält also genau 6 Elemente. Diese Elemente sind die Repräsentanten jeder Nebenklasse, sie können also nicht in der selben Nebenklasse liegen. Mit Korollar (2.6) genügt es, sechs Matrizen zu bestimmen, so dass immer für jeweils zwei dieser Matrizen L und M nicht kongruent Modulo 2 zu einander sind.

Wir haben

$$\mathrm{SL}(2;\mathbb{Z}/2\mathbb{Z}) = \left\{ \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right) \right\}$$

1 und 0 sind Restklassen. Nun suchen wir die Urbilder der Matrizen aus $\mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z})$ bezüglich Φ:

Für die folgenden Matrizen sieht man sofort, dass sie schon in Γ sind:

$$E = \begin{pmatrix}1&0\\0&1\end{pmatrix}, T = \begin{pmatrix}1&1\\0&1\end{pmatrix}, -UT = \begin{pmatrix}1&0\\1&1\end{pmatrix}$$

und damit Urbilder von sich selbst. Die drei restlichen Matrizen haben eine Determinante, die ungleich 1 ist. Da wir in $\mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z})$ sind, ist $-1 \equiv 1 \pmod 2$. Also folgt:

$$\Phi(J) = \Phi\left(\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right) = \begin{pmatrix}0&1\\1&0\end{pmatrix}$$

$$\Phi(U) = \Phi\left(\begin{pmatrix}-1&1\\-1&0\end{pmatrix}\right) = \begin{pmatrix}1&1\\1&0\end{pmatrix}$$

$$\Phi\left(U^2\right) = \Phi\left(\begin{pmatrix}0&-1\\1&-1\end{pmatrix}\right) = \begin{pmatrix}0&1\\1&1\end{pmatrix}$$

Also das gesuchte Vertretersystem besteht aus den folgenden Matrizen: E, T, J, U, $-UT$ und U^2. Mit dem Satz (1.11) folgt, dass

$$\mathbb{F}(\Gamma[2]) = \overline{\mathbb{F}} \cup J\overline{\mathbb{F}} \cup T\overline{\mathbb{F}} \cup U\overline{\mathbb{F}} \cup (-UT)\,\overline{\mathbb{F}} \cup U^2\overline{\mathbb{F}}$$

ein Fundamentalbereich von $\Gamma[2]$ ist.

- Bestimme $J\overline{\mathbb{F}}$:

  Da $\mathbb{F}$ ein Gebiet ist, ist das Bild von $\mathbb{F}$ unter $\tau \to J\tau = -\frac{1}{\tau}$ auch ein Gebiet. Dann betrachten wir den Rand von $\overline{\mathbb{F}}$. Wir nutzen die Eigenschaft, dass die Orthogonalkreise durch zwei verschiedene Punkte in $\mathbb{H}$ eindeutig bestimmt sind, und bestimmen wir die Bilder von $\rho, \rho^2, \rho+i, \rho^2+i$:

$$J\rho = -\overline{\rho} = \rho^2,$$

$$J\rho^2 = \rho,$$

$$J(\rho+i) = \frac{\rho^2+i}{|\rho+i|^2} = \frac{\rho^2+i}{2+\sqrt{3}},$$

$$J(\rho^2+i) = \frac{1}{\overline{\rho}-i} = \frac{\rho+i}{|\rho+i|^2} = \frac{\rho+i}{2+\sqrt{3}}.$$

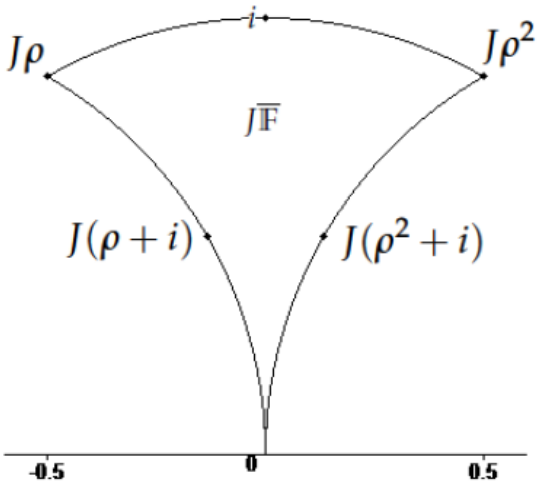

Abbildung 1: $J\overline{\mathbb{F}}$

- Zu $T\overline{\mathbb{F}}$: T verschiebt $\overline{\mathbb{F}}$ um 1 entlang der reellen Achse.

- Zu $U\overline{\mathbb{F}}$: U ist die Hintereinanderausführung von T und J.
- Zu $U^2\overline{\mathbb{F}}$ und $(-UT)\overline{\mathbb{F}}$: $U^2\tau = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\tau$ und $-UT\tau = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\tau$ mit $\tau \in \mathbb{H}$ haben Spitzen in $\mathbb{Q}$ und sind durch drei Orthogonalkreise begrenzt.

  Bestimme die Bilder von ∞, ρ, ρ^2:

$$U^2\infty = \frac{0}{1} = 0, \quad -UT\infty = \frac{1}{1} = 1,$$

$$U^2\rho = \rho, \quad -UT\rho = \frac{\frac{1}{2} + i\frac{\sqrt{3}}{2}}{\frac{3}{2} + i\frac{\sqrt{3}}{2}} = \frac{1}{2} + i\frac{1}{2\sqrt{3}},$$

$$U^2\rho^2 = \frac{-1}{-\frac{3}{2} + i\frac{\sqrt{3}}{2}} = \frac{\frac{3}{2} + i\frac{\sqrt{3}}{2}}{3} = \frac{1}{2} + i\frac{1}{2\sqrt{3}},$$

$$-UT\rho^2 = \frac{-\frac{1}{2} + i\frac{\sqrt{3}}{2}}{\frac{1}{2} + i\frac{\sqrt{3}}{2}} = -\rho^4 = \rho.$$

Insgesamt erhalten wir die folgende Abbildung:

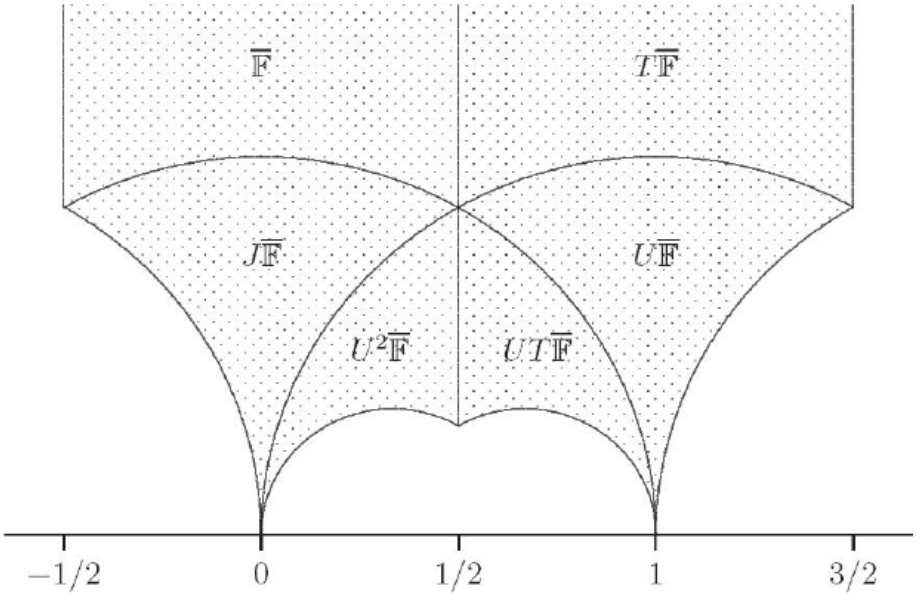

Abbildung 2: Fundamentalbereich von $\Gamma[2]$

§ 3 Literaturverzeichnis

[1] A. Krieg: *Funktionentheorie II*, Vorlesungsskript 2012 RWTH Aachen

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

[3] S. Bosch: *Algebra*, 7. Auflage, Springer-Verlag 2008

[4] H. Maas: *Lectures on modular functions of one complex variable*, §2 Seite 57, Tata Institut, Bombay 1964, Überarbeitung Springer-Verlag, 1983.

[5] H. Petersson: *Modulfunktionen und quadratische Formen*, Springer-Verlag, 1982

[6] B.v. Querenburg: *Mengentheoretische Topologie* §13D, 2. Auflage, Springer-Verlag, Berlin 1979.