Untergruppen der Modulgruppe

Vortrag zum Seminar zur Funktionentheorie, 13.05.2009 und 17.06.2009

Florian Drescher, Laura Neisius

In diesem Vortrag werden Fundamentalbereiche zu Untergruppen der Modulgruppe konstruiert und deren Eigenschaften erörtert. Es werden die Bezeichnungen aus Vortrag 1-3 übernommen.
$\Gamma = \mathrm{SL}(2;\mathbb{Z})$ bezeichne wieder die Modulgruppe, Λ eine Untergruppe von Γ.

§1 Fundamentalbereiche von Untergruppen

In diesem Abschnitt lernen wir Fundamentalbereiche von Untergruppen und deren Eigenschaften kennen.
Analog zu dem bereits bekannten Fundamentalbereich $\overline{\mathbb{F}}$ der Modulgruppe Γ möchten wir für die Untergruppen Λ von Γ Fundamentalbereiche konstruieren.

— *Allgemeine Definition und Eigenschaften* —

(1.1) Definition (Fundamentalbereiche von Untergruppen)
Sei Δ eine beliebige Untergruppe von $\mathrm{SL}(2;\mathbb{R})$.
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 $M\tau$, $M \in \Delta$, zum offenen Kern von $\mathcal{F}$, so gilt $M = \pm E$.

Eine äquivalente Definition liefert uns das Folgende:
Bezeichnet $M\mathcal{F} := \{M\tau\,;\,\tau \in \mathcal{F}\}$ 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*) $\mathring{\mathcal{F}} \cap M\mathring{\mathcal{F}} \neq \emptyset$, $M \in \Delta \Rightarrow M = \pm E$ ◇

Beweis

(FB.1) $\Rightarrow$ (FB.1*) :

Sei $\tau \in \mathbb{H}$, dann existiert nach Voraussetzung ein $M \in \Delta$ mit $M\tau \in \mathcal{F}$. Nach Definition von $M\mathcal{F}$ gilt somit $\tau = M^{-1}M\tau \in M^{-1}\mathcal{F}$. Da $\tau \in \mathbb{H}$ beliebig ist und $M^{-1} \in \Delta$ folgt $\mathbb{H} = \bigcup_{M\in\Delta} M\mathcal{F}$.

(FB.1) $\Leftarrow$ (FB.1*) :

Nach Voraussetzung existiert für alle $\tau \in \mathbb{H}$ ein $M \in \Delta$ mit $\tau \in M\mathcal{F}$. Es folgt $M^{-1}\tau \in M^{-1}M\mathcal{F} = \mathcal{F}$. Also erfüllt M^{-1} die Bedingung von (FB.1).

(FB.2) $\Leftrightarrow$ (FB.2*) :

Dies erfordert lediglich eine einfache Umformulierung und folgt sofort aus der Definition von $M\mathcal{F}$. □

(1.2) Bemerkung

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

Zum Beweis des nächsten Satzes benötigen wir folgenden Hilfssatz aus der Funktionalanalysis:

(1.3) Hilfssatz (Bairescher Kategoriesatz)

Wird der vollständig metrische Raum E als Vereinigung $E = \bigcup_{n=1} M_n$ abzählbar vieler abgeschlossener Mengen M_n dargestellt, so enthält mindestens ein M_n eine abgeschlossene (erst recht also eine offene) Kugel. ◇

Näheres zu dem Satz von Baire in dieser Form findet man in ([3]).

(1.4) Lemma

Jeder Fundamentalbereich $\mathcal{F}$ von Λ, $\Lambda \subset \Gamma$, besitzt innere Punkte. ◇

Beweis

Ist Λ eine Untergruppe von Γ, so ist $\mathbb{Z}^{2\times 2} \supset \Gamma \supset \Lambda$ und da $\mathbb{Z}$ abzählbar ist, gilt dies auch für $\mathbb{Z}^{2\times 2}$. Insbesondere folgt daraus, dass Λ abzählbar ist.
Mit dem Satz von Baire (auch Kategoriesatz von Baire genannt) und $\overline{\mathbb{H}} = \bigcup_{M\in\Lambda} \overline{M\mathcal{F}}$ ergibt sich, dass mindestens ein $\overline{M\mathcal{F}}$ innere Punkte besitzt und somit besitzt insbesondere $M\mathcal{F}$ innere Punkte.
Betrachtet man nun die Abbildung $\tau \to M^{-1}\tau$ so ist diese, da $M^{-1}\tau = \frac{a\tau+b}{c\tau+d}$ rational, holomorph auf $\mathbb{H} \setminus \{-\frac{d}{c}\}$. Somit besitzt $\mathcal{F}$ innere Punkte aufgrund der Gebietstreue. Dies war die Behauptung. □

— *Konstruktion* —

(1.5) Erinnerung (Der exakte Fundamentalbereich)
Der exakte Fundamentalbereich wurde bereits wie folgt definiert:
$\mathbb{F} := \{\tau \in \mathbb{H}; -\frac{1}{2} < \mathrm{Re}\ \tau \leqslant \frac{1}{2}\ ,\ |\tau| \geqslant 1 \text{ und } |\tau| > 1 \text{ für } -\frac{1}{2} < \mathrm{Re}\ \tau < 0\}$

$\overline{\mathbb{F}} := \{\tau \in \mathbb{H};\ \mathrm{Re}\ \tau \leqslant \frac{1}{2}\ ,\ |\tau| \geqslant 1\}$

$\mathring{\mathbb{F}} := \{\tau \in \mathbb{H};\ \mathrm{Re}\ \tau < \frac{1}{2}\ ,\ |\tau| > 1\}$ ◇

$\overline{\mathbb{F}}$ ist nach ([2] Satz 2.2) ein Fundamentalbereich von Γ im obigen Sinn. Der exakte Fundamentalbereich jedoch nicht, da dieser (FB.0) nicht erfüllt.

Bevor wir zur Konstruktion der Fundamentalbereiche gelangen, sei noch einmal an einige Sätze und Definitionen der Algebra erinnert:

(1.6) Bezeichnung
Sei Λ eine Untergruppe von Γ und Λ' die von Λ und $-E$ erzeugte Untergruppe von Γ. Dann existiert eine disjunkte Zerlegung von Γ in Rechtsnebenklassen der Form

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

mit dem *Index* $[\Gamma : \Lambda'] = \#(\Gamma/\Lambda') \in \mathbb{N} \cup \{\infty\}$
und den *Rechtsnebenklassen* $\Lambda' M_\nu = \{M' M_\nu\ ;\ M' \in \Lambda'\}$ von Λ'.

Hierbei sind die $M_\nu \in \Gamma$ eindeutig bis auf ihre Reihenfolge und einen linksseitigen Faktor aus Λ' bestimmt, da $\Lambda' M' M_\nu = \Lambda' M_\nu$ für alle $M' \in \Lambda'$. ◇

Betrachtet man den Fundamentalbereich $\overline{\mathbb{F}}$ von Γ, so liefert (FB.1*) :

(∗) $\mathbb{H} = \bigcup_{M \in \Gamma} M\overline{\mathbb{F}}$

Da Γ wie in (1) als disjunkte Vereinigung von Rechtsnebenklassen dargestellt werden kann, existiert für alle $M \in \Gamma$ ein M_ν und ein $M' \in \Lambda'$ mit $M' M\nu = M$. Man kann also $(*)$ auch schreiben als $\mathbb{H} = \bigcup_{M' \in \Lambda',\, 1 \leqslant \nu \leqslant [\Gamma:\Lambda']} M' M_\nu \overline{\mathbb{F}} = \bigcup_{M' \in \Lambda'} M' (\bigcup_{M_\nu} M_\nu \overline{\mathbb{F}})$.
Dies liefert eine Idee zur Definition eines Fundamentalbereichs einer Untergruppe Λ von Γ als

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

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

Beweis
Sei $\Lambda \neq \{E\}$, sonst gilt $\mathbb{F}(\Lambda) = \mathbb{H}$, wobei $\mathbb{H}$ (FB.0) - (FB.2) trivialerweise erfüllt.

(FB.0) Sei $\tau \in \mathbb{H} \setminus \mathbb{F}(\Lambda)$, dann existiert ein $\varepsilon > 0$, so dass

$$\mathcal{V}_\varepsilon = \{\tau \in \mathbb{H} \,;\, y \geqslant \varepsilon \,,\, |x| \leqslant \tfrac{1}{\varepsilon}\}$$

Obermenge von $\overline{\mathbb{F}}$ und τ ein innerer Punkt von $\mathcal{V}_\varepsilon$ ist.
Nach ([2] Bemerkung (2.7)) ist $\mathcal{V}_\varepsilon \supset \overline{\mathbb{F}}$ für $\varepsilon \leqslant \frac{\sqrt{3}}{2}$. Mit $\tau = x + iy$ wähle also $\varepsilon = \min\{\frac{\sqrt{3}}{2}, \frac{y}{2}, \frac{1}{2|x|}\}$.
Aus ([2] Satz (2.8)) ist bekannt, dass nur endlich viele $M \in \Gamma$ mit $M\mathcal{V}_\varepsilon \cap \mathcal{V}_\varepsilon \neq \emptyset$ existieren.
Da $\overline{\mathbb{F}} \subset \mathcal{V}_\varepsilon$ und $\{M_\nu \,;\, 1 \leqslant \nu \leqslant [\Gamma : \Lambda']\} \subset \Gamma$, existieren insbesondere nur endlich viele ν_i, $i \in \{1, \ldots, k\}$, mit $M_{\nu_i}\overline{\mathbb{F}} \cap \mathcal{V}_\varepsilon \neq \emptyset$.
Weil die $M_{\nu_i}\overline{\mathbb{F}}$ durch Orthogonalkreise begrenzt werden, sind sie relativ abgeschlossen in $\mathbb{H}$. Die endliche Vereinigung $\bigcup_{i\in\{1,\ldots,k\}} M_{\nu_i}\overline{\mathbb{F}}$ ist ebenso relativ abgeschlossen in $\mathcal{V}_\varepsilon$ und es gilt:

$$\bigcup_{i\in\{1,\ldots,k\}} M_{\nu_i}\overline{\mathbb{F}} \cap \mathcal{V}_\varepsilon = \mathbb{F}(\Lambda) \cap \mathcal{V}_\varepsilon.$$

Somit ist τ kein Häufungspunkt von $\mathbb{F}(\Lambda) \cap \mathcal{V}_\varepsilon$, da $\tau \notin \mathbb{F}(\Lambda)$ und $\mathbb{F}(\Lambda)$ relativ abgeschlossen in $\mathcal{V}_\varepsilon$ ist. Da $\tau \in \mathbb{H}$ beliebig gewählt war, folgt die Behauptung.

(FB.1) Sei $\tau \in \mathbb{H}$, dann existiert ein $L \in \Gamma$ mit $L\tau \in \mathbb{F}$. Für ein $M^{-1} \in \Lambda$ und ein $1 \leqslant \nu \leqslant [\Gamma : \Lambda']$ hat L^{-1} nach (1) die Darstellung

$$\begin{aligned} & L^{-1} = \pm\, M^{-1}M_\nu \\ \iff \quad & E = \pm\, M^{-1}M_\nu L \\ \iff \quad & \pm M = M_\nu L \end{aligned}$$

$\Rightarrow M\tau = (-M)\tau = M_\nu L\tau \in M_\nu\mathbb{F}$, da $L\tau \in \mathbb{F}$. Mit $M_\nu\mathbb{F} \subset \mathbb{F}(\Lambda)$ folgt die Behauptung.

(FB.2) Beweisidee: Unter der Annahme, dass z, Mz mit $M \in \Lambda$ innere Punkte von $\mathbb{F}(\Lambda)$ sind, wählt man geeignete Möbiustransformationen M', M'', so dass $M'z$, $M''Mz$ in $\mathbb{F}$ liegen für welches (FB.2) bereits gezeigt ist.

Dazu: Seien τ, $M\tau$, $M \in \Lambda$ innere Punkte von $\mathbb{F}(\Lambda)$ und $\mathcal{U}$ eine offene Umgebung von τ in $\mathbb{F}(\Lambda)$.
Nun soll $\mathcal{U}$ so gewählt werden, dass $M\mathcal{U}$ genau in $\mathbb{F}(\Lambda)$ liegt. Da $M\tau$ innerer Punkt von $\mathbb{F}(\Lambda)$ ist, existiert ein $\delta > 0$ mit $K_\delta(M\tau) \subset \mathbb{F}(\Lambda)$.

Nach ([4] Lemma (1.3)d)) gilt für $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$:

$$|M\tau' - M\tau| = \frac{1}{|(c\tau+d)(c\tau'+d)|}|\tau' - \tau|$$

Gesucht ist also ein $\varepsilon > 0$, so dass für $|\tau' - \tau| < \varepsilon$, d.h. $\mathcal{U} = K_\varepsilon(\tau)$, $|M\tau' - M\tau| < \delta$ gilt.

Fall 1 : $c = 0$

$$\frac{1}{|(c\tau+d)(c\tau'+d)|}|\tau' - \tau| < \frac{1}{d^2}\,\varepsilon < \delta$$

Wähle also $\varepsilon < d^2\delta$, so dass $K_\varepsilon \subset \mathbb{F}(\Lambda)$.

Fall 2 : $c \neq 0$

$$\frac{1}{\underbrace{|c\tau+d|}_{=:\kappa\in\mathbb{R}_+,\text{ da }\tau\in\mathbb{H}\text{ fest}}|c\tau'+d|}|\tau' - \tau| < \frac{1}{|c\tau'+d|}\frac{\varepsilon}{\kappa} \overset{\tau'=x+iy}{=} \frac{1}{|cx+d+icy|}\frac{\varepsilon}{\kappa} \overset{\triangle\text{ - Ungl.}}{\leqslant} \frac{1}{|cx+d||icy|}\frac{\varepsilon}{\kappa}$$

$$\leqslant \frac{1}{|icy|}\frac{\varepsilon}{\kappa} = \frac{\varepsilon}{|c|y\kappa} < \delta$$

Da $\tau' \in \mathbb{H}$, ist $y > 0$. Wähle also $\varepsilon < \frac{1}{2}|c|y\kappa\delta$, so dass $K_\varepsilon \subset \mathbb{F}(\Lambda)$.

Sei nun $\mathcal{U}_\nu = \mathcal{U} \cap M_\nu\overline{\mathbb{F}}$. Daraus folgt, dass $\mathcal{U} = \bigcup_\nu \mathcal{U}_\nu$, da $\mathcal{U} \subset \mathbb{F}(\Lambda)$ und $\mathbb{F}(\Lambda) = \bigcup_\nu M_\nu\overline{\mathbb{F}}$.
Da $\overline{\mathcal{U}} = \bigcup_\nu \overline{\mathcal{U}_\nu}$ eine kompakte Menge als Vereinigung abzählbar vieler abgeschlossener Mengen ist, hat nach dem Satz von Baire mindestens ein $\overline{\mathcal{U}_\nu}$ innere Punkte, also auch $\mathcal{U}_\nu$.
Sei dies ohne Einschränkung $\mathcal{U}_1$. Es existiert dann ein $z \in \mathring{\mathcal{U}}_1 \subset \mathring{M_1\overline{\mathbb{F}}}$ und $\omega := M_1^{-1}z$ ist dann ein innerer Punkt von $\mathbb{F}$.

Da $\mathbb{F}(\Lambda) = \bigcup_\nu M_\nu\overline{\mathbb{F}}$ existiert ein M_ν mit $Mz = MM_1\omega \in M_\nu\overline{\mathbb{F}}$ und somit liegt $M_\nu^{-1}MM_1\omega =: \omega'$ in $\overline{\mathbb{F}}$. Angenommen $\omega' \notin \mathbb{F}$. Dann ist $\omega' \in \overline{\mathbb{F}} \setminus \mathbb{F}$ mit

$$\overline{\mathbb{F}} \setminus \mathbb{F} = \{\tau \in \mathbb{H}\,;\, \mathrm{Re}\tau = -\frac{1}{2}\,,\, |\,\tau\,| \geqslant 1\}$$
$$\cup\, \{\tau \in \mathbb{H}\,;\, -\frac{1}{2} < \mathrm{Re}\tau < 0\,,\, |\,\tau\,| = 1\} =: \mathcal{G}_1 \cup \mathcal{G}_2$$

Ist $\omega' \in \mathcal{G}_1$, dann kann man ω' genau mit $\omega' \longmapsto T\omega' = \omega' + 1$ nach $\mathbb{F}$ abbilden. Dann ist $T\omega' \in \{\tau \in \mathbb{H}\,;\, \mathrm{Re}\tau = \frac{1}{2}\,,\, |\,\tau\,| \geqslant 1\} \not\subseteq \mathring{\mathbb{F}}$. Nun ist aber $\omega \neq T\omega'$, da $\omega \in \mathring{\mathbb{F}}$.

Dies ist ein Widerspruch zu $\tau, M\tau \in \mathbb{F} \Rightarrow \tau = M\tau$ aus ([1] Satz 2.2). Analog kann man ein $\omega' \in \mathcal{G}_2$ genau mittels J nach

$$\{\tau \in \mathbb{H} \,;\, 0 \leqq \mathrm{Re}\tau \leqq \tfrac{1}{2} \mid \tau \mid = 1\} \subset \mathbb{F}$$

abbilden, wobei $J\omega'$ ebenfalls nicht in $\mathring{\mathbb{F}}$ liegt, was zum selben Widerspruch führt.
Somit muss ω' in $\mathring{\mathbb{F}}$ liegen und ([2] Satz 2.2) liefert dann $\omega = \omega' = M_\nu^{-1} M M_1 \omega$, also

$$\begin{aligned} & M_\nu^{-1} M M_1 = \pm E \\ \Longleftrightarrow \; & \pm M M_1 \quad = M_\nu \qquad\qquad (*) \end{aligned}$$

Nach Vorausetzung ist $\pm M \in \Lambda'$, also $\Lambda'(\pm M M_1) = \Lambda' M_1 = \Lambda' M_\nu$. Somit ist $M_1 = M_\nu$, da die $\Lambda' M_\nu$ paarweise disjunkt sind. Aus $(*)$ folgt dann $M = \pm E$ und somit die Behauptung. □

(1.8) Definition (Spitzen, Spitzenbahn, Fixpunkt)
Die Bilder $M_\nu \infty$ von ∞ sind die *Spitzen* von $\mathbb{F}(\Lambda)$.
Die Bilder $\Lambda M_\nu \infty$, $1 \leqslant \nu \leqslant [\Gamma : \Lambda']$ heißen *Spitzenbahnen* von $\mathbb{F}(\Lambda)$.
Ein $\tau \in \mathbb{H}$ heißt *Fixpunkt* von Λ falls $M \in \Lambda$, $M \neq \pm E$ existiert mit $M\tau = \tau$. ◇

(1.9) Bemerkung
Die Spitzen von $\mathbb{F}(\Lambda)$ sind abhängig von der Wahl der M_ν.
Die Spitzenbahnen jedoch sind eindeutig, da die Zerlegung von Γ in Rechtsnebenklassen aus (1) nur von Λ abhängt, dh.
$\{\Lambda' M_\nu \mid 1 \leqslant \nu \leqslant [\Gamma : \Lambda']\} = \{\Lambda' M'_\nu \mid 1 \leqslant \nu \leqslant [\Gamma : \Lambda']\}$
für unterschiedliche M_ν, M'_ν. ◇

(1.10) Beispiel
Die Spitzenbahn von Γ ist $\mathbb{Q} \cup \{\infty\}$. Dazu sei $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$

1. Fall $c = 0$:
Dann ist $a = d = \pm 1$ wegen $\det(M) = ad - bc = 1$ und es gilt $M\tau = \tau + b \overset{\tau \to \infty}{\longrightarrow} \infty$.

2. Fall $c \neq 0$:
Dann existiert für alle teilerfremden $a, c \in \mathbb{Z}$ eine Matrix $M \in \Gamma$ mit $M = \begin{pmatrix} a & * \\ c & * \end{pmatrix}$.
Dies folgt aus dem erweiterten euklidischen Algorithmus und der Tatsache, dass $ad - cb = 1$. Somit gilt: $M\tau = \frac{a\tau + b}{c\tau + d} \overset{\tau \to \infty}{\longrightarrow} \frac{a}{c} \in \mathbb{Q}$
Also existiert für alle $\frac{a}{c} \in \mathbb{Q}$ eine Matrix $M \in \Gamma$ mit $M\infty = \frac{a}{c}$. ◇

§2 Hauptkongruenzgruppen

In Diesem Kapitel betrachten wir eine spezielle Art von Untergruppen und konstruieren einen zugehörigen Fundamentalbereich.

— *Definition und Bezeichnungen* —

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

In $\mathbb{Z}$ kann man bereits aus $a \equiv a' (\mathrm{mod}\ n)$ und $b \equiv b' (\mathrm{mod}\ n)$ folgern, dass $ab \equiv a'b' (\mathrm{mod}\ n)$ ist. Dass diese Tatsache auch über $\mathrm{Mat}(2\ ;\ \mathbb{Z})$ erhalten bleibt, zeigt folgendes

(2.2) Lemma
Seien L, L', M, $M' \in \mathrm{Mat}(2\ ;\ \mathbb{Z})$ mit $L \equiv L' (\mathrm{mod}\ n)$, $M \equiv M' (\mathrm{mod}\ n)$, so gilt $LM \equiv L'M' (\mathrm{mod}\ n)$. ◇

Beweis
Nach Voraussetzung existieren X_L, $X_M \in \mathrm{Mat}(2\ ;\ \mathbb{Z})$ mit $L = L' + nX_L$ und $M = M' + nX_M$. Es ist also

$$\begin{aligned} LM &= (L' + nX_L)(M' + nX_M) \\ &= L'M' + nL'X_M + nX_LM' + n^2X_LX_M \\ &= L'M' + n(\underbrace{L'X_M + X_LM' + nX_LX_M}_{\in \mathrm{Mat}\ (2\,;\mathbb{Z})}) \end{aligned}$$

Analog zu den Untergruppen $n\mathbb{Z} = \{z \in \mathbb{Z}\ ;\ z \equiv 0\ (\mathrm{mod}\ n)\}$ von $\mathbb{Z}$ als additive Gruppe kann man nun wegen Lemma (2.2) multiplikativ abgeschlossene Teilmengen von Γ definieren. □

(2.3) Definition (Hauptkongruenzgruppe)
Man nennt $\Gamma[n] := \{M \in \Gamma\ ;\ M \equiv E\ (\mathrm{mod}\ n)\}$ die *Hauptkongruenzgruppe*(mod n).
Die Zahl n heißt *Stufe* von $\Gamma[n]$. ◇

— *Eigenschaften der Hauptkongruenzgruppe* —

Dass $\Gamma[n]$ tatsächlich eine Untergruppe von Γ ist, soll nun gezeigt werden.

Die kanonische Projektion $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x} =: x + n\mathbb{Z}$ ist ein surjektiver Gruppenhomomorphismus. Diese kann man auf $\mathrm{Mat}(2\,;\mathbb{Z})$ fortsetzen vermöge

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

Im nächsten Satz soll geklärt werden, ob die Einschränkung $\Gamma \to \mathrm{SL}(2\,;\mathbb{Z}/n\mathbb{Z})$ ebenfalls ein surjektiver Gruppenhomomorphismus ist. Dies würde einige nützliche Eigenschaften von $\Gamma[n]$ und $\Gamma/\Gamma[n]$ liefern. Zuerst benötigen wir jedoch folgendes

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

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

Beweis
Setze $x = \prod_{p \in \mathbb{P},\, p \nmid a,\, p \mid c} p$ also das Produkt aller Primzahlen, die c, aber nicht a teilen. Existieren keine solche Zahlen, zum Beispiel wenn $a = k \cdot c$, $k \in \mathbb{Z}$, setze $x = 1$.
Angenommen es existiert ein $q \in \mathbb{P}$ mit $q \mid (a + xb)$ und $q \mid c$. Damit gilt $\mathrm{ggT}(a + xb, c) = q > 1$.

1. Fall: $q \mid a$.
Dann ist q nicht in der Primfaktorzerlegung von x enthalten, d.h. $q \nmid x$. Da q aber $a + xb$ teilt, muss gelten: $q \mid b$ und $q \mid c$ nach Voraussetzung.
Dies ist ein Widerspruch zu $\mathrm{ggT}(a, b, c) = 1$.

2.Fall: $q \nmid a$.
Nach Voraussetzung gilt $q \mid c$ und somit ist q in der Primzahlzerlegung von x enthalten.
Dies impliziert $q \mid x$ und wegen $q \mid a + xb$ auch $q \mid a$ als Widerspruch. □

Nun also zum angekündigten

(2.5) Satz
Die Abbildung

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

ist ein surjektiver Gruppenhomomorphismus, dessen Kern $\Gamma[n]$ ist. Somit ist $\Gamma[n]$ ein Normalteiler von endlichem Index in Γ und die Faktorgruppe $\Gamma/\Gamma[n]$ ist isomorph zu $\mathrm{SL}(2\,;\,\mathbb{Z}/n\mathbb{Z})$. ◇

Beweis
Wohldefiniertheit:

(i) $\Phi(\Gamma) \subseteq \mathrm{SL}(2\,;\,\mathbb{Z}/n\mathbb{Z})$. Da $\det \overline{M} = \overline{a}\overline{d} - \overline{b}\overline{c} \overset{(\mathrm{mod}\ n)\ \text{in}\ \mathbb{Z}}{=} \overline{ad - bc} = \overline{\det M} = \overline{1}$ ist das Bild von Φ in $\mathrm{SL}(2\,;\,\mathbb{Z}/n\mathbb{Z})$ enthalten.

(ii) Φ Gruppenhomomorphismus:
Lemma (2.2) liefert $\Phi(MN) = \overline{MN} = \overline{M} \cdot \overline{N} = \Phi(M) \cdot \Phi(N)$
Also ist Φ ein Gruppenhomomorphismus mit
$\mathrm{Kern}(\Phi) = \{M \in \Gamma\,;\,\Phi(M) = \overline{E}\} = \{M \in \Gamma\,;\,M \equiv E(\mathrm{mod}\ n)\} = \Gamma[n]$.

Surjektivität:
Sei $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}(2\,;\,\mathbb{Z})$ mit $\overline{K} \in \mathrm{SL}(2\,;\,\mathbb{Z}/n\mathbb{Z})$. Ohne Einschränkung sei $c \neq 0$, sonst kann man c durch $c + n$ ersetzen ohne dass sich $\overline{K}$ ändert. Zu zeigen ist nun, dass dieses $\overline{K}$ ein Urbild in Γ besitzt.
Da $\overline{K} \in \mathrm{SL}(2\,;\,\mathbb{Z}/n\mathbb{Z})$ muss gelten $\det(K) = ad - bc \equiv 1 \pmod{n}$, also existiert ein $k \in \mathbb{Z}$ mit $ad - bc - kn = 1$. Dies impliziert ggT $(d,\ n,\ c) = 1$. Da $c \neq 0$, existiert nach Lemma (2.4) ein $r \in \mathbb{Z}$ mit $\mathrm{ggT}(\underbrace{d + rn}_{=:\delta}, c) = 1$. Man erhält nun:

$$a\delta - bc = ad - bc + arn = 1 + nx + arn = 1 + (\underbrace{x + ar}_{=:s \in \mathbb{Z}})n$$

Wegen ggT $(\delta,\ c) = 1$ gibt es $x', y' \in \mathbb{Z}$ mit $\delta x' - cy' = 1$ und somit auch $x, y \in \mathbb{Z}$ mit $\delta x - cy = s$.

Betrachten wir nun die Matrix $M = \begin{pmatrix} a - xn & b - yn \\ c & d + rn \end{pmatrix} \in \text{Mat}\ (2\ ;\ \mathbb{Z})$

so gilt offensichtlich $\overline{M} = \overline{K}$, und wegen

$$\begin{aligned} \det(M) &= (a - xn)\delta - (b - yn)c \\ &= \underbrace{a\delta - bc}_{=1+ns} - xn\delta + ync \\ &= 1 + sn - n(\underbrace{\delta x - cy}_{=s}) = 1 \end{aligned}$$

liegt M sogar in $\text{SL}(2\ ;\ \mathbb{Z})$ und wir haben unser Urbild zu $\overline{K}$ gefunden, dh. Φ ist surjektiv.

Aus dem Homomorphiesatz für Gruppen folgt nun $\Gamma/\Gamma[n] \simeq \text{SL}(2\ ;\ \mathbb{Z}/n\mathbb{Z})$ und somit $[\Gamma : \Gamma[n]] = \#\ \text{SL}(2\ ;\ \mathbb{Z}/n\mathbb{Z}) < n^4 < \infty$. Also ist der Index von $\Gamma[n]$ in Γ endlich. □

Da $\Gamma[n]$ ein Normalteiler von Γ ist, existiert wie in (1) eine disjunkte Zerlegung von Γ in Nebenklassen von $\Gamma[n]$. Diese ist sogar endlich, da $[\Gamma : \Gamma[n]] < \infty$, wie eben gezeigt. Die Matrizen in einer Nebenklasse von $\Gamma[n]$ charakterisieren wir mit folgendem

(2.6) Lemma
Zwei Matrizen M, $L \in \Gamma$ liegen genau dann in derselben Nebenklasse von $\Gamma[n]$, wenn $M \equiv L(\ \text{mod}\ n)$. ◇

Beweis
Sei $M \equiv L(\ \text{mod}\ n)$, also $M = L + nX$ für ein $X \in \text{Mat}(2\ ;\ \mathbb{Z})$.
Ist $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, dann folgt $M = \begin{pmatrix} a + n\alpha & b + n\beta \\ c + n\gamma & d + n\delta \end{pmatrix}$ mit α, β, γ, $\delta \in \mathbb{Z}$.

Wegen $\det(L) = \det(M) = 1$ kann man folgern, dass

$L^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, $M^{-1} = \begin{pmatrix} d + n\delta & -b - n\beta \\ -c - n\gamma & a + n\alpha \end{pmatrix}$ und es gilt:

$$\begin{aligned} L^{-1}M &= \begin{pmatrix} ad - bc + n(\alpha d - b\gamma) & ab - db + n(d\beta - b\delta) \\ -ac + ac + n(-\alpha c + a\gamma) & ad - bc + n(-c\beta + a\delta) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + n \begin{pmatrix} \alpha d - b\gamma & d\beta - b\delta \\ -\alpha c + a\gamma & -c\beta + a\delta \end{pmatrix} \equiv E \pmod{n} \end{aligned}$$

völlig analog folgert man auch $M^{-1}L \equiv E(\text{mod}\ n)$.

Es gilt also $M^{-1}L$, $L^{-1}M \in \Gamma[n] \Leftrightarrow L \in M\Gamma[n]$ und $M \in L\Gamma[n] \Rightarrow M\Gamma[n] = L\Gamma[n]$, da die Nebenklassen von $\Gamma[n]$ paarweise disjunkt sind. Also liegen M und L in derselben Nebenklasse. Dies war die Behauptung. □

Eine Formel zur Berechnung des Index $[\Gamma : \Gamma[n]]$ liefert der folgende

(2.7) Hilfssatz
$[\Gamma : \Gamma[n]] = \#\,\mathrm{SL}(2\,;\,\mathbb{Z}/n\mathbb{Z}) = n^3 \prod_{p|n}(1 - p^{-2})$ für $n \geqslant 2$. ◇

Einen Beweis hierzu findet man bei *H.Maass* [1983], 63-65, *J. Lehner* [1964], 356 oder *R.A. Rankin* [1977], 21-23.

Bevor wir nun zu einem Beispiel eines Vertretersystems der Nebenklassen kommen, betrachten wir noch die Fixpunkte von $\Gamma[n]$.

(2.8) Satz
Für $n \geqslant 2$ besitzt $\Gamma[n]$ keine Fixpunkte, d.h. aus $M\tau = \tau$ und $M \in \Gamma[n]$ folgt $M = \pm E$ falls $n = 2$ und $M = E$ falls $n > 2$. ◇

Beweis
Sei $M\tau = \tau$ für ein $M \in \Gamma[n]$, $M \neq \pm E$. M ist insbesondere in Γ, also ist τ ein Fixpunkt von Γ. Nach ([2], Satz (2.5)) ist dann für ein $L \in \Gamma$

	$\tau = Li$	oder	$\tau = L\rho$
Es gilt also	$MLi = Li$	oder	$ML\rho = L\rho$
und man folgert	$L^{-1}MLi = i$	oder	$L^{-1}ML\rho = \rho$

Mit ([1] Satz 2.2) folgt aus $L^{-1}MLi = i$, dass $L^{-1}ML = \pm J$ und aus $L^{-1}ML\rho = \rho$, dass $L^{-1}ML = \pm\mathcal{U}, \mathcal{U}^2$.
$\Gamma[n]$ ist ein Normalteiler in Γ, d.h. für alle $L \in \Gamma$, $M \in \Gamma[n]$ gilt $L^{-1}ML \in \Gamma[n]$.
Also müssten $\pm J$, $\pm\mathcal{U}$ oder $\pm\mathcal{U}^2$ in $\Gamma[n]$ liegen. Hierzu müssen die Elemente auf der Nebendiagonalen kongruent 0 modulo n für ein $n \geqslant 2$ sein, was weder bei

$$\pm J = \begin{pmatrix} 0 & \mp 1 \\ \pm 1 & 0 \end{pmatrix}, \pm\mathcal{U} = \begin{pmatrix} \mp 1 & \pm 1 \\ \mp 1 & 0 \end{pmatrix} \text{ noch bei } \pm\mathcal{U}^2 = \begin{pmatrix} 0 & \mp 1 \\ \pm 1 & \mp 1 \end{pmatrix} \text{ der Fall ist.}$$

Dies ist ein Widerspruch zur Annahme.

Für $n = 2$ muss also $M = \pm E$ sein. Ansonsten ist $M = E$, da $-E \notin \Gamma[n]$ für $n > 2$ und $-E \not\equiv E \pmod{n}$. □

Zum Abschluss betrachten wir noch ein

(2.9) Beispiel (Konstruktion eines Fundamentalbereichs von Γ[2])
Aus Satz (2.5) wissen wir, dass

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

Wenn wir also zu jedem $M \in \mathrm{SL}\ (2\,;\,\mathbb{Z}/2\mathbb{Z})$ ein Urbild bezüglich Φ finden, so sind diese Urbilder unser Vertretersystem. Es ist

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

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

sind bereits in Γ enthalten, also offensichtlich Urbilder von sich selbst.

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ und $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

hingegen sind nicht in Γ enthalten, da ihre Determinante -1 ist. Ersetzt man allerdings auf der Nebendiagonalen eine 1 durch -1, so ist diese Matrix sowohl in Γ als auch ein Urbild, da $-1 \equiv 1 \pmod 2$. Zusätzlich kann man noch eine 1 auf der Hauptdiagonalen durch -1 ersetzen, um „ schöne “ Vertreter aus Γ zu erhalten.

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

Insgesamt erhalten wir also das Vertretersystem

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

Der Fundamentalbereich von $\Gamma[2]$ ist also nach Satz (1.7)

$$\begin{array}{rccccc} \overline{\mathbb{F}}(\Gamma[2]) = & \overline{\mathbb{F}} & \cup & T\overline{\mathbb{F}} & \cup & -UT\overline{\mathbb{F}} \\ \cup & J\overline{\mathbb{F}} & \cup & U\overline{\mathbb{F}} & \cup & U^2\overline{\mathbb{F}} \end{array}$$

$J\overline{\mathbb{F}}$ wurde bereits in [1] konstruiert. $T\overline{\mathbb{F}}$ verschiebt $\overline{\mathbb{F}}$ um 1 entlang der reellen Achse und U ist die Hintereinanderausführung von T und J.
Bleiben noch $U^2\overline{\mathbb{F}}$ und $-UT\overline{\mathbb{F}}$. Sowohl U^2 als auch $-UT$ haben Spitzen in $\mathbb{Q}$, werden also durch drei Orthogonalkreise begrenzt.
Da ein Orthogonalkreis durch zwei Punkte festgelegt wird, genügt es, die Bilder von ρ, ρ^2 und ∞ zu betrachten.

$U^2\overline{\mathbb{F}} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\overline{\mathbb{F}}$:

$$U^2\infty = \frac{0}{1} = 0$$
$$U^2\rho = \rho \qquad \text{nach ([1] Satz 2.2)}$$
$$U^2\rho^2 = U^2\langle -\frac{1}{2} + i\frac{\sqrt{3}}{2}\rangle = \frac{-1}{-\frac{3}{2} + i\frac{\sqrt{3}}{2}} = \frac{\frac{3}{2} + i\frac{\sqrt{3}}{2}}{3} = \frac{1}{2} + i\frac{1}{2\sqrt{3}}$$

$-UT\overline{\mathbb{F}} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\overline{\mathbb{F}}$:

$$-UT\infty = \frac{1}{1} = 1$$
$$-UT\rho = -UT\langle\frac{1}{2} + i\frac{\sqrt{3}}{2}\rangle = \frac{\frac{1}{2} + i\frac{\sqrt{3}}{2}}{\frac{3}{2} + i\frac{\sqrt{3}}{2}} = \frac{1}{2} + i\frac{1}{2\sqrt{3}}$$
$$-UT\rho^2 = \frac{-\frac{1}{2} + i\frac{\sqrt{3}}{2}}{\frac{1}{2} + i\frac{\sqrt{3}}{2}} = (-\frac{1}{2} + i\frac{\sqrt{3}}{2})(\frac{1}{2} - i\frac{\sqrt{3}}{2}) = -\rho^4 = \rho \qquad \diamond$$

Insgesamt erhält man also einen Fundamentalbereich von $\Gamma[2]$ wie in Abbildung 1.

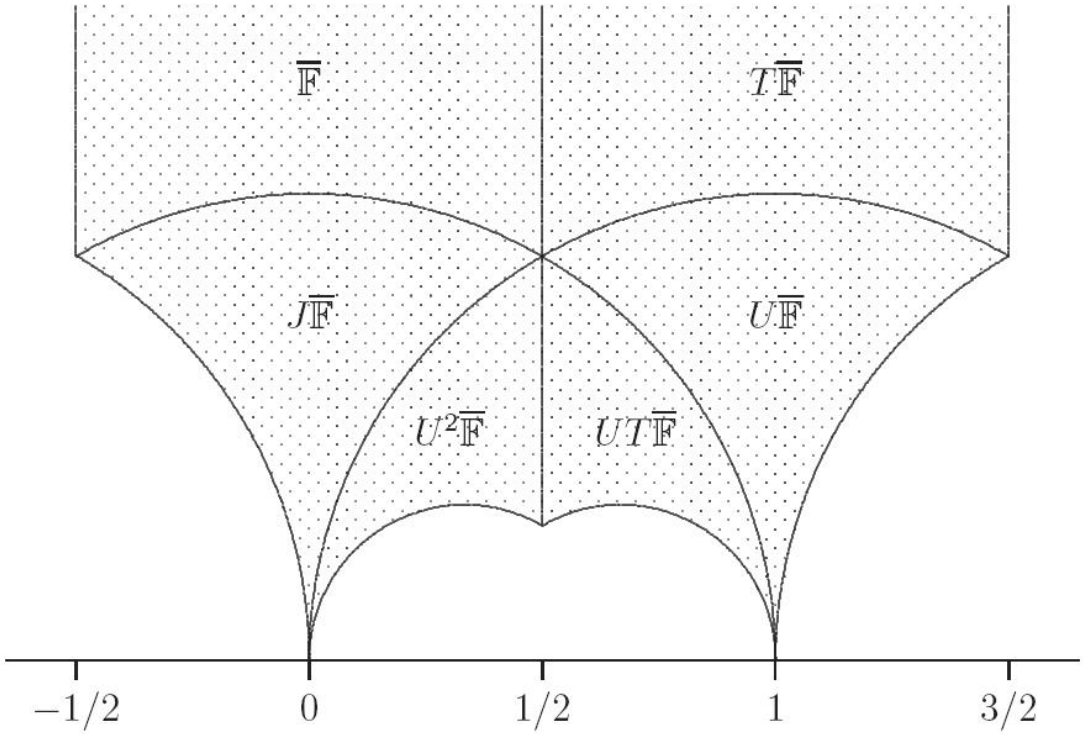

Abbildung 1: Fundamentalbereich von Γ[2]

§3 Kongruenzgruppen

In diesem Abschnitt betrachten wir eine weitere spezielle Art von Untergruppen von Γ, die Kongruenzgruppen.

— *Definition und Zusammenhang mit den Hauptkongruenzgruppen* —

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

(3.2) Lemma
Jede Kongruenzgruppe Λ von Γ hat endlichen Index in Γ. ◇

Beweis
Wir wissen bereits aus (1) und Satz (2.5), dass $\Gamma = \bigcup_{k\in\{1,\dots,j\}} \Gamma[n]M_k$. Weiterhin ist bekannt, dass $\Lambda \supset \Gamma[n]$ und dies impliziert $\Lambda M_k \supset \Gamma[n]M_k \quad \forall k \in \{1,\dots,j\}$.
Daraus folgt, dass Γ dargestellt werden kann als $\Gamma = \bigcup_{k\in\{1,\dots,j\}} \Lambda M_k$. Diese Vereinigung ist im Allgemeinen nicht disjunkt (außer wenn gerade $\Gamma[n] = \Lambda$ gewählt wird). Der Index von Λ in Γ ist somit sogar kleiner als $[\Gamma : \Gamma[n]]$ und damit auf jeden Fall endlich, was die Behauptung war. □

Nun überlegen wir uns, wie eine solche Untergruppe Λ von Γ, die $\Gamma[n]$ enthält, aussehen könnte.

(3.3) Bezeichnung
Eine wichtige Klasse von Beispielen sind die Gruppen

$$\Gamma_0[n] := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,;\, c \equiv 0 \,(\mathrm{mod}\ n) \right\}$$ ◇

Zu prüfen ist, ob $\Gamma_0[n]$ die geforderten Eigenschaften einer Kongruenzuntergruppe von Γ im obigen Sinne erfüllt.

Beweis
Wir beweisen zuerst $\Gamma[n] \subset \Gamma_0[n] \subset \Gamma$.
$\Gamma_0[n]$ ist Obermenge von $\Gamma[n]$, da für alle $M \in \Gamma[n] : M \equiv E(\mathrm{mod}\ n)$ und M insbesondere die von $\Gamma_0[n]$ geforderte Eigenschaft $c \equiv 0(\mathrm{mod}\ n)$ erfüllt.
$\Gamma_0[n] \subset \Gamma$ folgt sofort aus der Definition von $\Gamma_0[n]$.

Nun ist noch zu prüfen, ob $\Gamma_0[n]$ tatsächlich eine Gruppe ist:

(i) $E \in \Gamma[n] \subset \Gamma_0[n]$

(ii) Sei $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0[n]$. Dann ist $M^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, da $\det(M) = 1$.
Da $c \equiv 0 (\mathrm{mod}\ n) \equiv -c$ gilt: $M^{-1} \in \Gamma_0[n]$.

(iii) Sei $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0[n]$ und $L = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0[n]$

$$\Rightarrow ML = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & d\beta + d\delta \end{pmatrix}$$

Da $n \mid c$ und $n \mid \gamma$ gilt: $n \mid c\alpha + d\gamma$. Daraus ergibt sich, dass $ML \in \Gamma_0[n]$.

Mit (i) - (iii) ist $\Gamma_0[n]$ eine Gruppe, was zu zeigen war. □

(3.4) Bezeichnung
Analog zu $\Gamma_0[n]$ definieren wir die Untergruppen

$$\Gamma^0[n] := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,;\, b \equiv 0 \,(\mathrm{mod}\ n) \right\}. \qquad \diamond$$

(3.5) Lemma
$\Gamma^0[n]$ und $\Gamma_0[n]$ sind konjugiert in Γ. Es gilt

$$\Gamma^0[n] = J\,\Gamma_0[n]\,J^{-1} \quad \text{und} \quad \Gamma_0[n] = J^{-1}\,\Gamma_0[n]\,J$$

Beweis
Sei $M \in \Gamma_0[n]$ mit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

$$\begin{aligned} \Rightarrow JMJ^{-1} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \in \Gamma^0[n] \text{ , da } c \equiv 0 \,(\mathrm{mod}\ n) \Rightarrow -c \equiv 0 \,(\mathrm{mod}\ n) \end{aligned}$$

Auf dieselbe Weise folgt $J^{-1}MJ \in \Gamma_0[n]$ für $M \in \Gamma^0[n]$. □

Analog zum Hilfssatz (2.7) wird eine Berechnung des Index $[\Gamma : \Gamma_0[n]]$ gegeben durch folgenden

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

Genaueres hierzu findet man bei *H.Maass* [1983], 63-65, *J. Lehner* [1964], 356 oder *R.A. Rankin* [1977], 21-23.

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

(3.8) Bemerkung
$\Gamma_0[n]$ und $\Gamma^0[n]$ sind für $n > 1$ keine Normalteiler in Γ. ◇

Beweis
Nach Lemma (3.5) gilt für $n > 1$:
$\Gamma^0[n] = J\,\Gamma_0[n]\,J^{-1}$ und somit gilt auch $\Gamma_0[n] = J^{-1}\,\Gamma^0[n]\,J$.
Dies zeigt bereits, dass weder $\Gamma_0[n]$ noch $\Gamma^0[n]$ Normalteiler in Γ ist. □

— *Konstruktion und Struktur* —

Wir wissen bereits Folgendes:
$\Gamma[n] \subset \Gamma_0[n] \subset \Gamma$. $\Gamma[n]$ ist Normalteiler von Γ (und somit auch von $\Gamma_0[n]$). Mit dem zweiten Isomorphiesatz aus der Algebra, ergibt sich:

$$(*)\quad (\Gamma/\Gamma[n])\ /(\Gamma_0[n]\ /\Gamma[n]) \simeq \Gamma/\Gamma_0[n]$$

Damit können wir die Struktur von $\Gamma/\Gamma_0[n]$ untersuchen,
indem wir $(\Gamma/\Gamma[n])\ /(\Gamma_0[n]\ /\Gamma[n])$ betrachten.

Idee:

Wir wissen bereits, dass $\Gamma/\Gamma[n]$ isomorph zu $\mathrm{SL}(2\,;\,\mathbb{Z}/n\mathbb{Z})$ ist. Aus $(*)$ folgt, dass $\Gamma_0[n]\ /\Gamma[n]$ Untergruppe von $\Gamma/\Gamma[n]$ sein muss, und somit isomorph zu einer Untergruppe von $\mathrm{SL}(2\,;\,\mathbb{Z}/n\mathbb{Z})$ ist.

Nun konstruieren wir analog zu $\Phi : \Gamma \to \mathrm{SL}(2\,;\mathbb{Z}/n\mathbb{Z})$ aus Satz (2.5) ein $\Phi_0 : \Gamma_0[n] \to \mathrm{SL}(2\,;\mathbb{Z}/n\mathbb{Z})$ und betrachten $\mathrm{Bild}(\Phi_0)$ und $\mathrm{Kern}(\Phi_0)$.
Dann können wir mit Hilfe des Homomorphiesatzes folgende Aussage treffen:

$$\begin{aligned} & \Gamma_0[n]/\mathrm{Kern}(\Phi_0) \simeq \mathrm{Bild}(\Phi_0) \\ \overset{\text{mit } (*)}{\Rightarrow} \quad & \mathrm{SL}(2\,;\mathbb{Z}/n\mathbb{Z})/\mathrm{Bild}(\Phi_0) \simeq (\Gamma/\Gamma_0[n]) \end{aligned}$$

Sucht man ein Vertretersystem von Nebenklassen von dem $\mathrm{Bild}(\Phi_0)$ in $\mathrm{SL}(2\,;\mathbb{Z}/n\mathbb{Z})$ und findet dann Urbilder bezüglich Φ in Γ, so bilden diese Urbilder ein Vertretersystem der Nebenklassen von $\Gamma_0[n]$ in Γ.

(3.9) Beispiel
Zur Veranschaulichung unserer Idee betrachten wir erneut den Fall $n = 2$:

$$\Gamma_0[2] = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma\,;\, c \equiv 0 \,(\mathrm{mod}\ 2) \right\}$$

$$\Gamma[2] = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma\,;\, M \equiv E \,(\mathrm{mod}\ 2) \right\}$$

$$\begin{aligned} \overset{\text{mit } (*)}{\Rightarrow} \quad & (\Gamma/\Gamma[2])\ /(\Gamma_0[2]\ /\Gamma[2]) \simeq \Gamma/\Gamma_0[2] \\ & \Gamma/\Gamma[2] \simeq \mathrm{SL}(2\,;\underbrace{\mathbb{Z}/2\mathbb{Z}}_{=\mathbb{F}_2}) \end{aligned}$$

$$\Phi_0 : \Gamma_0[2] \to \mathrm{SL}(2\,;\mathbb{F}_2),\ M \mapsto \overline{M}$$

Zur Erinnerung:

$$SL(2;\mathbb{F}_2) = \left\{ \begin{array}{c} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \end{array} \right\}$$

$$\Rightarrow \mathrm{Bild}(\Phi_0) = \left\{ \overbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}^{=E}, \overbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}^{=T} \right\}, \mathrm{Kern}(\Phi_0) = \Gamma[2]$$

$$\overset{\textit{Homomorphiesatz}}{\Rightarrow} \Gamma_0[2]/\Gamma[2] \simeq \mathcal{G} \quad \text{wobei } \mathcal{G} := \mathrm{Bild}(\Phi_0) \subset \mathrm{SL}(2\,;\mathbb{F}_2) \text{ bezeichne.}$$

Da nach obigen Betrachtungen gerade T und E Vertreter von $\Gamma[2]$ in $\Gamma_0[2]$ sind, folgt insbesondere

$$\textbf{(H1)}\quad \Gamma_0[2] = \Gamma[2] \cup \Gamma[2]T$$

und mit $(*)$ gilt: $\Gamma/\Gamma_0[2] \simeq \mathrm{SL}(2\,;\mathbb{F}_2)/\mathcal{G}$.
Betrachtet man nun die Nebenklassen von $\mathcal{G}$ in $\mathrm{SL}(2\,;\mathbb{F}_2)$, so ist eine Nebenklasse natürlich $\mathcal{G}$ selbst.

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\mathcal{G} = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$ ist die zweite Nebenklasse.

Die dritte Nebenklasse muss also $\left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$ sein, diese entspricht genau $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\mathcal{G}$.

Da $E, J \in \Gamma$ können sie als Urbilder von sich selbst gewählt werden.

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

Insgesamt ergibt sich also, dass E, J und U^2 ein Vertretersystem von $\Gamma_0[2]$ in Γ bilden.

$$\Rightarrow \Gamma = \Gamma_0[2] \cup \Gamma_0[2]J \cup \Gamma_0[2]U^2 \qquad \diamond$$

(3.10) Bemerkung
(a) $\Gamma_0[2]$ hat also Index 3 in Γ. Nach (H1) besitzt $\Gamma[2]$ Index 2 in $\Gamma_0[2]$.

(b) Nach (2) gilt $\mathbb{F}(\Gamma_0[2]) = \overline{\mathbb{F}} \cup J\overline{\mathbb{F}} \cup U^2\overline{\mathbb{F}}$ $\diamond$

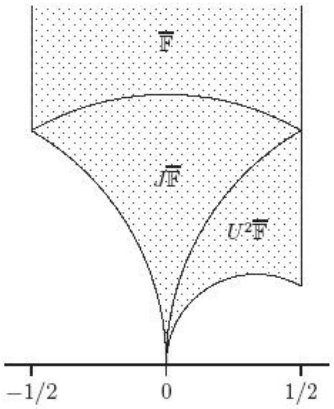

Abbildung 2: Fundamentalbereich $\Gamma_0[2]$

§ 4 Die Kongruenzgruppen der Stufe 2

Im letzten Beispiel haben wir bereits eine Kongruenzgruppe der Stufe 2, nämlich $\Gamma_0[2]$ kennengelernt. Nun möchten wir in diesem Abschnitt alle echten Untergruppen von Γ, die $\Gamma[2]$ enthalten, betrachten.

(4.1) 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
zu a)
Aus Satz (2.5) ist bekannt, dass $\Gamma/\Gamma[2]$ isomorph zu SL(2 ; $\mathbb{Z}/2\mathbb{Z}$) ist.
Bis auf Isomorphie gibt es nur zwei Gruppen der Ordnung 6 :

- C_6, die zyklische Gruppe eines Elements der Ordnung 6
- S_3, welche 3 Elemente der Ordnung 2 und 2 Elemente der Ordnung 3 enthält.

Betrachtet man SL(2 ; $\mathbb{Z}/2\mathbb{Z}$), so haben

$$\text{die Elemente } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ und } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ die Ordnung 2}$$

$$\text{und die Elemente } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ und } \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ die Ordnung 3.}$$

Also ist SL(2 ; $\mathbb{Z}/2\mathbb{Z}$) isomorph zu S_3 und somit auch $\Gamma/\Gamma[2]$.

zu b)
$-E = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ und $JT^2J^{-1} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$ sind offensichtlich Elemente von $\Gamma[2]$. Es bezeichne Λ die von den Matrizen $-E$, T^2 und JT^2J^{-1} erzeugte Untergruppe von $\Gamma[2]$. Nun soll gezeigt werden, dass dann $\Lambda = \Gamma[2]$ gilt.
Sei hierzu $M \in \Gamma[2]$ beliebig. $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv E (\text{mod } 2)$, also sind a, d ungerade und c gerade.

Es sind $(T^2)^m = \begin{pmatrix} 1 & 2m \\ 0 & 1 \end{pmatrix}$ und $(JT^2J^{-1})^m = \begin{pmatrix} 1 & 0 \\ -2m & 1 \end{pmatrix}$

$$\text{also ist} \quad (T^2)^m M = \begin{pmatrix} a+2mc & b+2md \\ c & d \end{pmatrix}$$
$$\text{und} \quad (JT^2J^{-1})^m M = \begin{pmatrix} a & b \\ c-2ma & b-2md \end{pmatrix}$$

Sei ohne Einschränkung $|a| > |c|$ (für $|a| < |c|$ beginne mit dem nächsten Schritt, $|a| = |c|$ ist nicht möglich, da a ungerade und c gerade).
Dann gibt es mit dem euklidischen Alghorithmus ein $m \in \mathbb{Z}$ mit $|a+2mc| < |2c|$. Ist $|c| < |a+2mc|$, so ist $|a+2(m\pm 1)c| < |c|$, ansonsten ist bereits $|a+2mc| < |c|$. Es gibt also ein $m_1 \in \mathbb{Z}$ mit

$$(T^2)^{m_1} M = \begin{pmatrix} a_1 & b_1 \\ c & d \end{pmatrix} =: M_1 \text{ und } |a_1| < |c|.$$

Analog kann man nun ein $k_1 \in \mathbb{Z}$ finden mit

$$(JT^2J^{-1})^{k_1} M_1 = \begin{pmatrix} a_1 & b_1 \\ c-2ka_1 & b_1-2kd \end{pmatrix} =: \begin{pmatrix} a_1 & b_1 \\ c_2 & d_2 \end{pmatrix} =: M_2 \text{ und } |c_2| < |a_1|.$$

Nun lässt sich wieder ein $j \in \mathbb{Z}$ finden mit

$$(T^2)^j M_2 = \begin{pmatrix} a_3 & b_3 \\ c_2 & d_2 \end{pmatrix} \text{ und } |a_3| < |c_2|.$$

Da alle Ungleichunge strikt sind, alle a_i ungerade und alle c_i gerade, muss nach endlich vielen Schritten $|a_s| = 1$ und $|c_{s+1}| = 0$ gelten, d.h. wir haben ein
$L = (JT^2J^{-1})^{k_s}(T^2)^{m_s} \cdot \ldots \cdot (JT^2J^{-1})^{k_1}(T^2)^{m_1} \in \Lambda$ gefunden mit $LM = \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix}$.
Da $LM \in \Gamma[2]$, muss gelten $LM = \begin{pmatrix} \pm 1 & r \\ 0 & \pm 1 \end{pmatrix}$ mit $r \in 2\mathbb{Z}$, da sonst $\det(LM) \neq 1$.

Also ist $LM = \pm T^r \in \Lambda$ und somit $M = L^{-1}(\pm T^r) \in \Lambda$. Da $M \in \Gamma[2]$ beliebig gewählt war, und $\Lambda \subseteq \Gamma[2]$ gilt, folgt die Gleichheit von Λ und $\Gamma[2]$, was zu zeigen war. □

(4.2) Erinnerung
Ist G eine Gruppe, H ein Normalteiler von G, so gilt

$$\{J \leq G \mid J \supseteq H\} \simeq \{\bar{J} \leq G/H\} \text{ vermöge } \pi : J \mapsto \bar{J} \qquad \diamond$$

Da $\Gamma[2]$ ein Normalteiler von Γ ist, stehen somit die Untergruppen von Γ, welche $\Gamma[2]$ enthalten (also genau die Kongruenzgruppen der Stufe 2) in Bijektion zu den Untergruppen von $\Gamma/\Gamma[2]$ und somit auch zu den Untergruppen von $\mathrm{SL}(2\,;\,\mathbb{Z}/2\mathbb{Z})$.

Betrachten wir also die Urbilder der Untergruppen von $\mathrm{SL}(2\,;\,\mathbb{Z}/2\mathbb{Z})$ bezüglich Φ aus Satz (2.5), so erhalten wir ein Vertretersystem von Nebenklassen von $\Gamma[2]$ der entsprechenden Kongruenzgruppe der Stufe 2.

— *Kongruenzgruppen der Stufe 2 mit Index 3* —

$\mathrm{SL}(2\,;\,\mathbb{Z}/2\mathbb{Z})$ enthält drei Untergruppen der Ordnung 2. Diese sind

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \Phi(E)\,,\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \Phi(T)\right\}$$
$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \Phi(E)\,,\ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \Phi(UT)\right\}$$
$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \Phi(E)\,,\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \Phi(J)\right\}$$

Die entsprechenden Kongruenzgruppen von Γ sind also

$$\begin{aligned} \Gamma[2] \cup \Gamma[2]T &= \Gamma_0[2] \\ \Gamma[2] \cup \Gamma[2]UT &= \Gamma^0[2] \\ \Gamma[2] \cup \Gamma[2]J &=: \Gamma_\vartheta \end{aligned}$$

(4.3) Bezeichnung
Γ_ϑ heißt *Theta-Gruppe* mit $\Gamma_\vartheta := \Gamma[2] \cup \Gamma[2]J$. $\diamond$

Genauer charakterisieren wollen wir diese Gruppe mit dem folgenden

(4.4) Korollar

a) Γ_ϑ ist Untergruppe von Γ vom Index 3.

b) $\Gamma = \Gamma_\vartheta \cup \Gamma_\vartheta T \cup \Gamma_\vartheta U$

c) Γ_ϑ wird erzeugt von J und T^2.

d) Sei $M \in \Gamma_\vartheta$ so gilt $M \equiv E (\mathrm{mod}\ 2)$ oder $M \equiv J (\mathrm{mod}\ 2)$.

e) $\mathbb{F}(\Gamma_\vartheta) := \overline{\mathbb{F}} \cup T\overline{\mathbb{F}} \cup U\overline{\mathbb{F}}$ ist ein Fundamentalbereich von Γ_ϑ. ◇

Beweis

zu a)
$\Gamma[2]$ hat in Γ den Index 6 nach Beispiel (2.9) und Γ_ϑ den Index 2.
Der Isomorphiesatz besagt, dass

$$\Gamma/\Gamma_\vartheta[2] \simeq (\Gamma/\Gamma[2])/(\Gamma_\vartheta[2]\ /\ \Gamma[2])$$

und der Satz von Lagrange, dass

$$|\Gamma/\Gamma_\vartheta[2]| = |\Gamma/\Gamma[2]|/|\Gamma_\vartheta[2]\ /\ \Gamma[2]| = \tfrac{6}{2} = 3$$

Also hat Γ_ϑ in Γ den Index 3.

zu b)
$\mathrm{SL}(2\ ;\ \mathbb{Z}/2\mathbb{Z})$ lässt sich als Vereinigung von Rechts- und Linksnebenklassen von $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} =: G_\vartheta$ darstellen:

$$\begin{aligned} \mathrm{SL}(2\ ;\ \mathbb{Z}/2\mathbb{Z}) &= G_\vartheta \cup \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{=\Phi(T)} G_\vartheta \cup \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}}_{=\Phi(U^2)} G_\vartheta \\ &= G_\vartheta \cup G_\vartheta \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{=\Phi(T)} \cup G_\vartheta \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}}_{=\Phi(U)} \end{aligned}$$

Analog zu Beispiel (3.9) folgt also

$$\begin{aligned} \Gamma &= \Gamma_\vartheta \cup T\Gamma_\vartheta \cup U^2\Gamma_\vartheta \\ &= \Gamma_\vartheta \cup \Gamma_\vartheta T \cup \Gamma_\vartheta U \end{aligned}$$

zu c)
$\Gamma[2]$ wir erzeugt von $-E$, T^2 und JT^2J^{-1}, somit wird $\Gamma_\vartheta[2]= \Gamma[2]\cup\Gamma[2]J$ erzeugt von $-E$, T^2, JT^2J^{-1} und J.
T^2 und J genügen als Erzeuger, da $J^2 = -E$ und JT^2J^{-1} im Erzeugnis von diesen beiden Matrizen liegen.

zu d)
Ist $M \in \Gamma_\vartheta$ so gilt mit Bezeichnung (4.3), dass M entweder ein Element aus $\Gamma[2]$ oder ein Element aus $\Gamma[2]J$ ist.
Somit ist $M \equiv E(\mathrm{mod}\ 2)$ oder $M = XJ$, wobei $X \in \Gamma[2]$ ist.
Aus der Multiplikativität der Kongruenz folgt somit die Behauptung.

zu e)
nach b) und Satz (1.7) gilt $\mathbb{F}(\Gamma_\vartheta) := \overline{\mathbb{F}} \cup T\overline{\mathbb{F}} \cup U\overline{\mathbb{F}}$ ist ein Fundamentalbereich von Γ_ϑ. □

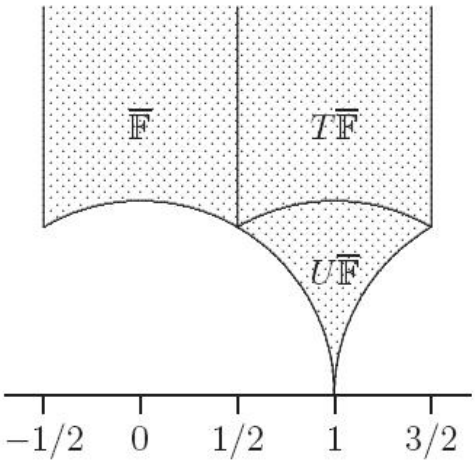

Abbildung 3: Fundamentalbereich von Γ_ϑ

— *Kongruenzgruppe der Stufe 2 mit Index 2* —

Darüber hinaus besitzt SL(2 ; $\mathbb{Z}/2\mathbb{Z}$) mit

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

eine Untergruppe der Ordnung 3. Diese entspricht der Kongruenzgruppe

(4.5) Bezeichnung
$\Gamma_N[2] := \Gamma[2] \cup \Gamma[2]U \cup \Gamma[2]U^2$ ◇

(4.6) Proposition
a) $\Gamma = \Gamma_N[2] \cup \Gamma_N[2]T$

b) Die Gruppe $\Gamma_N[2]$ wird erzeugt von den Matrizen T^2 und $-U$.

c) und es gilt: $\Gamma_N[2]$ ist der einzige Normalteiler in Γ vom Index 2.

d) Die Abbildung $\chi : \Gamma \to \{\pm 1\}$, $M \mapsto (-1)^{ac+bc+bd}$ ist ein *abelscher Charakter* von Γ mit Kern$(\chi) = \Gamma_N[2]$. ◇

Beweis
zu a)
Nach Bezeichnung (4.5) gilt

$$\begin{aligned} & \Gamma_N[2] && = \Gamma[2] \cup \Gamma[2]U \cup \Gamma[2]U^2 \\ \Rightarrow \quad & \Gamma_N[2]T && = \Gamma[2]T \cup \Gamma[2](UT) \cup \Gamma[2](\underbrace{U^2T}_{=J}) \\ \overset{\text{Bsp. (2.9)}}{\Rightarrow} \quad & \Gamma && = \underbrace{\Gamma[2] \cup \Gamma[2]U \cup \Gamma[2]U^2}_{=\Gamma_N[2]} \cup \underbrace{\Gamma[2]T \cup \Gamma[2](UT) \cup \Gamma[2]J}_{=\Gamma_N[2]T} \\ & && = \Gamma_N[2] \cup \Gamma_N[2]T \end{aligned}$$

zu b)
Zu zeigen ist $\Gamma_N[2] = \langle T^2 \, , -U \rangle$:
Nach Satz (4.1) b) wird $\Gamma[2]$ erzeugt von $-E$, T^2 und $JT^2J^{-1} = U^{-1}T^2U$.
Da $\Gamma_N[2] = \Gamma[2] \cup \Gamma[2]U \cup \Gamma[2]U^2$ wird Γ_N erzeugt von $-E$, T^2 , $U^{-1}T^2U$ und U.
Weil $(-U)^3 = -E$, genügen T^2 und $-U$ als Erzeuger.

zu c)
Aus a) folgt, dass $[\Gamma : \Gamma_N[2]] = 2$ und nach Ergebnissen aus der Algebra ist $\Gamma_N[2]$

somit Normalteiler in Γ.
Zu zeigen ist jetzt noch, dass $\Gamma_N[2]$ einziger Normalteiler vom Index 2 in Γ ist:
Sei Γ^* beliebige Untergruppe von Γ vom Index 2.
Angenommen es existiert ein $M \in \Gamma$ mit $M^2 \notin \Gamma^*$ ($\Rightarrow M \notin \Gamma^*$). Dann gilt $M, M^2 \neq E$, d.h. $\text{ord}(M) > 2$, also insbesondere $M \neq M^2$.

Da $M \notin \Gamma^*$, ist $M^2 \notin \Gamma^* M$, d.h. $\Gamma^* M \neq \Gamma^* M^2$. Das heißt, man hat bereits drei disjunkte Nebenklassen gefunden, sodass $\Gamma \supset \Gamma^* \cup \Gamma^* M \cup \Gamma^* M^2$. Daraus folgt bereits, dass $[\Gamma : \Gamma^*] \geqslant 3$, was ein Widerspruch zur Annahme $[\Gamma : \Gamma^*] = 2$ ist.
Somit muss für alle $M \in \Gamma$ gelten, dass $\Gamma M^2 \in \Gamma^*$. Damit liegen auch T^2, $J^2 = -E$, $(U^2)^2 = U$ in Γ^*, woraus sich die Erzeugenden T^2 und $-U$ von $\Gamma_N[2]$ konstruieren lassen. Daraus folgt $\Gamma_N[2] \subseteq \Gamma^*$.
Die Gleichheit ergibt sich aus folgendem Widerspruchsbeweis: Sei $\Gamma_N[2] \subsetneq \Gamma^*$.
Dann gilt $\Gamma^* T \supset \Gamma_N[2]T$ und da $\Gamma = \underbrace{\Gamma_N[2]}_{\subsetneq \Gamma^*} \dot{\cup} \underbrace{\Gamma_N[2]T}_{\subsetneq \Gamma^* T}$ folgt $\Gamma^* \cap \Gamma^* T \neq \emptyset$.
Da zwei Nebenklassen mit nicht leerem Schnitt gleich sein müssen, gilt $\Gamma^* = \Gamma^* T$, woraus mit der Nebenklassenzerlegung von Γ sofort folgt, dass $\Gamma = \Gamma^*$, was ein Widerspruch zur Annahme ist.

zu d) Zuerst prüfen wir, ob χ einen Gruppenhomomorphismus darstellt, dazu ist $\chi(ML) = \chi(M) \cdot \chi(L)$ für alle $L, M \in \Gamma$ zu zeigen:
Da Γ von J und T erzeugt wird, genügt es zu zeigen, dass $\chi(MJ) = \chi(M) \cdot \chi(J)$ und $\chi(MT) = \chi(M) \cdot \chi(T)$ für ein $M \in \Gamma$. Es gilt

$$\chi(T) = \chi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = (-1)^{1\cdot 0+1\cdot 0+1\cdot 1} = -1$$
$$\chi(J) = \chi\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) = (-1)^{1\cdot 0+(-1)\cdot 1+(-1)\cdot 0} = -1$$

Sei nun $M \in \Gamma$ beliebig, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

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

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

Damit ist χ Gruppenhomomorphimus.

Nun wollen wir zeigen, dass $\text{Kern}(\chi) = \Gamma_N[2]$:
Nach b) wird $\Gamma_N[2]$ von T^2 und $-U$ erzeugt. Es gilt:

$$\chi(T^2) = \chi\left(\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\right) = (-1)^{1\cdot 0+2\cdot 0+2\cdot 1} = (-1)^2 = 1$$

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

Wegen $\chi(ML) = \chi(M) \cdot \chi(L)$ ist also $\chi(A) = 1$ für alle $A \in \Gamma_N[2]$.
Somit gilt $\Gamma_N[2] \subset \text{Kern}(\chi)$.
Sei nun $B \in \Gamma \setminus \Gamma_N[2]$, dann liegt B nach a) in $\Gamma_N[2]T$. Daraus folgt, dass B von der Form $B = AT$ für ein $A \in \Gamma_N[2]$.
$\Rightarrow \chi(B) = \chi(AT) = \chi(A) \cdot \chi(T) = 1 \cdot (-1) = -1$
$\Rightarrow B \notin \text{Kern}(\chi)$ und daraus folgt die Behauptung $\text{Kern}(\chi) = \Gamma_N[2]$. □

§ 5 Elemente endlicher Ordnung in Γ

(5.1) Satz
Sei $M \in \Gamma$, $M \neq \pm E$, dann sind äquivalent

(i) M hat Ordnung 3, 4 oder 6

(ii) M hat endliche Ordnung

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

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

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

Beweis
(i)⇒(ii) klar

(ii)⇒(iii) Hat M endliche Ordnung, so existiert ein $n \in \mathbb{N}$ mit $M^n = E$. Ist $\lambda \in \mathbb{C}$ ein Eigenwert von M^n, so ist χ^n ein Eigenwert von M^n. Da E als einzigen Eigenwert $\lambda = 1$ hat, muss also $|\lambda| = 1$ für alle Eigenwerte von M gelten. Das charakteristische Polynom von M ist

$$\chi_M = \lambda^2 - \underbrace{\text{Sp}(M)}_{=:s}\chi + \underbrace{\det(M)}_{=1} \Rightarrow \lambda_{1,2} = \tfrac{1}{2}(s \pm \sqrt{s^2-4})$$

Angenommen $s > 2$, dann gilt

$$\tfrac{1}{2}(s + \sqrt{s^2-4}) > \tfrac{1}{2}(2 + \sqrt{2^2-4}) = 1$$

d.h. ein Eigenwert von M wäre größer als 1.
Wäre andererseits $s < -2$, dann wäre ein Eigenwert kleiner als -1, da

$$\tfrac{1}{2}(s - \sqrt{s^2-4}) < \tfrac{1}{2}(-2 - \sqrt{(-2)^2-4}) = -1$$

Es muss also $|s| \leq 2$ gelten.

Betrachte nun noch $s = \pm 2$:
1.Fall ($s = 2$) : Dann ist $\chi_M = x^2 - 2x + 1$ und da $\chi_M(M) = 0$ nach dem Satz von Cayley-Hamilton gilt also

$$M^2 = 2M - E \qquad (*)$$

Zeige nun $M^n = nM - (n-1)E$ für alle $n \in \mathbb{N}$ mittels vollständiger Induktion.

I.A $n = 1$. $M^1 = 1 \cdot M - 0 \cdot E \qquad \surd$

I.S $M^{n+1} \overset{\text{I.V}}{=} M(nM - (n-1)E) = nM^2 - (n-1)M$
$\overset{(*)}{=} n(2M - E) - (n-1)M = (2n - n + 1)M - nE = (n+1)M - nE \qquad \surd$

Somit gilt $M^n = M + (n-1)(M-E)$. Da $M - E \neq 0$, ist also $M^n \neq M$ für alle $n \geq 2$, d.h. M hat keine endliche Ordnung. Dies ist ein Widerspruch zur Voraussetzung.

2.Fall ($s = -2$) : Ist $\mathrm{Sp}(M) = -2$ und hat M endliche Ordnung n, so ist $\mathrm{Sp}(-M) = 2$ und $-M$ hat ebenfalls endliche Ordnung.
Betrachtet man also $-M$ erhält man den Widerspruch aus dem ersten Fall.

(iii)⇒(iv) Dies ist genau die Folgerung (iii)⇒(i) aus ([2] Satz 1.3)

(iv)⇒(v) Es existiert ein $\tau \in \mathbb{H}$ mit $M\tau = \tau$, also ist τ nach ([2] Korollar 2.5) von der Form Li oder $L\rho$ für ein $L \in \Gamma$.
Also ist $M \in \Gamma_{L_i}$ oder $M \in \Gamma_{L_\rho}$. Nach ([2] Bemerkung 2.4) gilt

$$\begin{aligned} & \Gamma_{L_i} = L\Gamma_i L^{-1} && \text{und} && \Gamma_{L_\rho} = L\Gamma_\rho L^{-1} \\ \Leftrightarrow \quad & L^{-1}\Gamma_{L_i} L = \Gamma_i && \text{und} && L^{-1}\Gamma_{L_\rho} L = \Gamma_\rho \end{aligned}$$

Da $M \in \Gamma_{L_i}$ oder $M \in \Gamma_{L_\rho}$ folgt also mit [1] Satz (2.2)

$$L^{-1}ML \in \Gamma_i = \{\pm J\} \text{ oder } L^{-1}ML \in \Gamma_\rho = \{\pm U\ ,\ \pm U^2\}$$

(v)⇒(i) $L^{-1}ML$ hat dieselbe Ordnung wie M, da aus $M^k = E$ folgt

$$(L^{-1}ML)^k = L^{-1}MLL^{-1}ML \cdot \cdots \cdot L^{-1}ML = L^{-1}M^kL = L^{-1}L = E$$

Nach Voraussetzung ist $L^{-1}ML \in \{\pm J, \pm U\ ,\ \pm U^2\}$ und diese Matrizen sind von der Ordnung 3, 4 oder 6. □

Literaturverzeichnis

[1] *Ein Fundamentalbereich der Modulgruppe* von *Kerstin Küppers*

[2] *Fixpunkte* von *Alexander Hagen*

[3] *Funktionalanalysis - Theorie und Anwendung, 4. Auflage, Teuber Verlag* von *Harro Heuser*

[4] *Die obere Halbebene* $\mathbb{H}$ von *Tom Rihm*

[5] *Elliptische Funktionen und Modulformen, 2. Auflage, Springer Verlag* von *Max Koecher und Alois Krieg*

[6] *Algebra*, 7. Auflage, Springer Verlag von *S. Bosch*