Untergruppen der Modulgruppe I

Vortrag zum Seminar zur Höheren Funktionentheorie, 16.04.2008

Hanna Schäfer

Ziel dieses Vortrages ist es, bestimmte Untergruppen der Modulgruppe $\Gamma = \mathrm{SL}(2;\mathbb{Z})$ zu betrachten und deren Fundamentalbereich zu bestimmen. Dafür wird der Fundamentalbereich einer Untergruppe definiert und ein Verfahren angegeben, um diesen zu konstruieren. Im Anschluss daran werden zunächst endliche Untergruppen betrachtet. Schließlich werden die Hauptkongruenzgruppen und Kongruenzgruppen als Spezialfälle von Untergruppen der Modulgruppe genauer untersucht.

§ 1 Fundamentalbereiche von Untergruppen

In diesem Paragrafen wird zunächst der Fundamentalbereich einer Untergruppe von $\mathrm{SL}(2;\mathbb{R})$ definiert. Anschließend wird ein Verfahren zur Konstruktion der Fundamentalbereiche von Untergruppen der Modulgruppe gegeben.

— *Der Fundamentalbereich* —

Sei Δ zunächst eine Untergruppe von $\mathrm{SL}(2;\mathbb{R})$.

(1.1) Definition (Fundamentalbereich)
Eine Teilmenge $\mathcal{F}$ von $\mathbb{H}$ nennt man einen *Fundamentalbereich* von Δ, wenn gilt:

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

(FB.1) Zu jedem $\tau \in \mathbb{H}$ gibt es ein $M \in \Delta$ 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 $M = \pm E$.$\diamond$

Erwähnenswert sind folgende

(1.2) Bemerkungen

a) Bezeichnet man mit $M\mathcal{F} := \{M\tau;\ \tau \in \mathcal{F}\}$ das Bild von $\mathcal{F}$ unter der Transformation $\tau \mapsto M\tau$, so ist eine (relativ) abgeschlossene Teilmenge $\mathcal{F}$ von $\mathbb{H}$ genau dann ein Fundamentalbereich von Δ, wenn gilt:

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

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

b) Ist $\Delta = \Lambda$ eine Untergruppe von $\Gamma = \mathrm{SL}(2;\mathbb{Z})$, so ist Λ abzählbar, da Γ abzählbar ist. In diesem Fall folgt aus (FB.1*) und dem Satz von Baire, dass jeder Fundamentalbereich innere Punkte besitzt:

Die Translation $\tau \mapsto M\tau$ ist für $M \in \Lambda$ ein Homöomorphismus, also eine offene wie auch abgeschlossene Abbildung. Demnach ist das Bild von $\mathcal{F}$ unter der Translation abgeschlossen in $\mathbb{H}$, da $\mathcal{F}$ abgeschlossen ist in $\mathbb{H}$. Nach dem Satz von Baire ist $\mathbb{H}$ ein Raum zweiter Kategorie, der nach (FB.1*) dargestellt werden kann als abzählbare Vereinigung abgeschlossener Mengen. Dann folgt aber, dass mindestens ein $M_0 \in \Lambda$ existiert, so dass $M_0\mathcal{F}$ innere Punkte enthält. Da die Translation, wie schon oben erwähnt, ein Homöomorphismus ist, enthält $\mathcal{F}$ innere Punkte. $\diamond$

Es bezeichne $\mathbb{F}$ die in der Vorlesung zur Höheren Funktionetheorie I, [K] XXVIII § 2, definierte Teilmenge von $\mathbb{H}$, das heißt

$$\mathbb{F} = \left\{ \tau \in \mathbb{H};\ -\frac{1}{2} < \operatorname{Re}\tau \leq \frac{1}{2}, |\tau| \geq 1 \text{ und } |\tau| > 1 \text{ für } -\frac{1}{2} < \operatorname{Re}\tau < 0 \right\}.$$

Im obigen Sinne ist $\overline{\mathbb{F}}$ ein Fundamentalbereich, denn $\overline{\mathbb{F}}$ ist abgeschlossen in $\mathbb{H}$ und (FB.1) und (FB.2) sind erfüllt nach [K] XXVIII Satz 2.6.

— *Die Konstruktion* —

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

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

eine disjunkte Zerlegung von Γ in Rechtsnebenklassen nach Λ'. Damit wird Γ in (1) als endliche oder abzählbar unendliche Vereinigung dargestellt, je nachdem ob der Index $[\Gamma : \Lambda']$ endlich ist oder nicht. Die Repräsentanten M_ν in (1) sind nur bis auf jeweils einen linksseitigen Faktor aus Λ' und bis auf eine Permutation eindeutig bestimmt. Man setzt trotzdem

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

Es gilt der

(1.3) Satz
Die Menge $\mathbb{F}(\Lambda)$ ist ein Fundamentalbereich von Λ. $\diamond$

Beweis
Man prüfe (FB.0)–(FB.2).

(FB.0): Sei $\tau \in \mathbb{H}$ und $\tau \notin \mathbb{F}(\Lambda)$. Für $\varepsilon > 0$ sei

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

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. Damit $\overline{\mathbb{F}} \subset \mathcal{V}_\varepsilon$ gilt, muss $\varepsilon \leq \frac{1}{2}\sqrt{3}$ gewählt werden, vergleiche [K] XXVIII § 2. Nach [K] XXVIII Satz 2.9 gibt es nur endlich viele $M \in \Gamma$ mit $M\mathcal{V}_\varepsilon \cap \mathcal{V}_\varepsilon \neq \emptyset$. Somit gibt es nur endlich viele ν mit $M_\nu\overline{\mathbb{F}} \cap \mathcal{V}_\varepsilon \neq \emptyset$, da ε so gewählt war, dass $\overline{\mathbb{F}} \subset \mathcal{V}_\varepsilon$ gilt. Da $M_\nu\overline{\mathbb{F}}$ für alle $1 \leq \nu \leq [\Gamma : \Lambda']$ abgeschlossen ist und $\tau \notin M_\nu\overline{\mathbb{F}}$ für alle $1 \leq \nu \leq [\Gamma : \Lambda']$ gilt, ist τ kein Häufungspunkt in $M_\nu\overline{\mathbb{F}}$ für jedes $1 \leq \nu \leq [\Gamma : \Lambda']$. Weil es nur endlich viele ν gibt, so dass $M_\nu\overline{\mathbb{F}} \cap \mathcal{V}_\varepsilon \neq \emptyset$ gilt und τ innerer Punkt von $\mathcal{V}_\varepsilon$ ist, folgt damit, dass τ kein Häufungspunkt von $\mathbb{F}(\Lambda)$ ist. Somit ist $\mathbb{F}(\Lambda)$ relativ abgeschlossen in $\mathbb{H}$.

(FB.1): Zu $\tau \in \mathbb{H}$ wähle nach [K] XXVIII Satz 2.6 ein $L \in \Gamma$ mit $L\tau \in \mathbb{F}$. Nach (1) gibt es dann ein $M \in \Lambda$ und ein ν mit $L^{-1} = \pm M^{-1}M_\nu$. Es folgt $\pm M = M_\nu L$ und damit $M\tau = M_\nu \langle L\tau \rangle \in M_\nu\mathbb{F} \subset \mathbb{F}(\Lambda)$.

(FB.2): Seien $M \in \Lambda$ sowie τ und $M\tau$ innere Punkte von $\mathbb{F}(\Lambda)$ und $\mathcal{U}$ eine offene Umgebung von τ in $\mathbb{F}(\Lambda)$. Da die Translation $\tau \mapsto M\tau$ ein Homöomorphismus ist, gilt $M\mathcal{U} \in \mathfrak{U}(M\tau)$, wobei $\mathfrak{U}(M\tau)$ das System aller Umgebungen von $M\tau$ bezeichnet. Nach Voraussetzung ist $M\tau$ selber ein innerer Punkt von $\mathbb{F}(\Lambda)$, also kann man nach eventueller Verkleinerung von $\mathcal{U}$ annehmen, dass $M\mathcal{U} = \{Mz;\ z \in \mathcal{U}\} \subset \mathbb{F}(\Lambda)$ gilt. Man hat

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

Nach dem Satz von Baire ist $\mathcal{U}$ von zweiter Kategorie und es ist $\mathcal{U}_\nu := \mathcal{U} \cap M_\nu\overline{\mathbb{F}}$ abgeschlossen in $\mathcal{U}$, also besitzt mindestens eine Menge $\mathcal{U}_\nu$ innere Punkte. Sei ohne Einschränkung $\overset{\circ}{\mathcal{U}}_1 \neq \emptyset$ und $z \in \overset{\circ}{\mathcal{U}}_1$. Wegen $\mathcal{U}_1 \subset M_1\overline{\mathbb{F}}$ gibt es ein $w \in \overline{\mathbb{F}}$ mit $z = M_1 w$. Da z ein innerer Punkt von $\mathcal{U}_1$ ist und die Translation $\tau \mapsto M_1\tau$ ein Homöomorphismus ist, ist w ein innerer Punkt von $\mathbb{F}$. Es gilt $M\mathcal{U}_1 \subset \mathbb{F}(\Lambda)$, also gibt es ein ν, so dass $Mz \in M_\nu\overline{\mathbb{F}}$. Dann ist aber $w' := M_\nu^{-1}MM_1w = M_\nu^{-1}Mz$ ein Punkt von $\overline{\mathbb{F}}$. Indem man w' gegebenenfalls mit

$$J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{oder} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

in $\mathbb{F}$ abbildet, folgt aus [K] XXVIII Satz 2.6 mit $w' = M_\nu^{-1} M M_1 w$ und $w, w' \in \mathbb{F}$, dass $w = w'$ gilt und $M_\nu^{-1} M M_1 = \pm E$, also $M_\nu = \pm M M_1$. Da $\pm M \in \Lambda'$ gilt, folgt $\nu = 1$ und $M = \pm E$. □

— *Spitzen und Fixpunkte* —

(1.4) Definition (Spitzen, Spitzenbahnen)
Unter *Spitzen* von $\mathbb{F}(\Lambda)$ versteht man die Bilder $M_\nu\infty$ von ∞. Die Mengen $\Lambda M_\nu\infty$ heißen *Spitzenbahnen*. ◇

Erwähnenswert sind die folgenden

(1.5) Bemerkungen

a) Die Definition der Spitzen von $\mathbb{F}(\Lambda)$ ist abhängig von der Wahl der M_ν in (1). Dagegen sind die Spitzenbahnen $\Lambda M_\nu\infty$ durch Λ eindeutig bestimmt, da für verschiedende Repräsentanten M_ν und M'_ν einer Rechtsnebenklasse nach Λ gilt $\Lambda M_\nu = \Lambda M'_\nu$.

b) Mit Hilfe des Ergänzungslemma [K] XXVIII 2.1 bestimmt man $\mathbb{Q} \cup \{\infty\}$ als die Spitzenbahn von Γ:

Es gilt

$$\Gamma\infty = \left\{ M\infty;\ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \right\}$$
$$\subset \left\{ \frac{a}{c};\ c \neq 0, \mathrm{ggT}(a,c) = 1 \right\} \cup \{\infty\} = \mathbb{Q} \cup \{\infty\}.$$

Sei nun $c \neq 0$ und $a/c \in \mathbb{Q}$ mit $\mathrm{ggT}(a,c) = 1$. Dann gibt es nach dem Ergänzungslemma $b, d \in \mathbb{Z}$, so dass

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \text{ und } M\infty = \frac{a}{c},$$

also $a/c \in \Gamma\infty$. Zu ∞ wähle

$$M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma,$$

dann gilt $\infty = M\infty \in \Gamma\infty$. ◇

Ein Analogon zu der Definition eines Fixpunktes von Γ ist die anschließende

(1.6) Definition (Fixpunkt)
Ein Punkt $\tau \in \mathbb{H}$ heißt *Fixpunkt* von Λ, wenn es ein $M \in \Lambda$ gibt mit $M\tau = \tau$ und $M \neq \pm E$. ◇

(1.7) Bemerkungen
(a) Jeder Fixpunkt von Λ ist auch ein Fixpunkt von Γ, denn angenommen τ ist ein Fixpunkt von Λ, so existiert ein $M \in \Lambda$ mit $M\tau = \tau$ und $M \neq \pm E$. Da Λ eine Untergruppe von Γ ist, ist τ somit auch ein Fixpunkt von Γ. Die Umkehrung gilt im Allgemeinen natürlich nicht.

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

§ 2 Endliche Untergruppen

Das Ziel in dieses Paragrafen ist es, endliche Untergruppen der Modulgruppe genauer zu beschreiben und zu bestimmen. Es wird sich herausstellen, dass endliche Untergruppen eine einfache Struktur haben und höchstens von der Ordnung 6 sind. Doch zunächst sollen Matrizen endlicher Ordnung aus Γ genauer untersucht werden. Dazu dient der nächste

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

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

(ii) M hat eine endliche Ordnung.

(iii) Es gilt $|\mathrm{Sp}\, M| < 2$.

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

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

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

$(ii) \Rightarrow (iii)$: Die Matrix M hat endliche Ordnung. Damit ist M, nach [A] Kapitel 9 Korollar (2.3), ähnlich zu einer Diagonalmatrix D, welche die gleichen Eigenwerte wie

M hat. Da sowohl M also auch D die Determinanten 1 haben, haben die Eigenwerte von M den Betrag 1. Das charakteristische Polynom von M hat die Form

$$\chi_M(\lambda) = \lambda^2 - (\operatorname{Sp} M)\lambda + \det M = \lambda^2 - s\lambda + 1,$$

wobei $s := \operatorname{Sp} M$. Daher haben die Eigenwerte von M die Form

$$\lambda_{1,2} = \frac{1}{2}\left(s \pm \sqrt{s^2 - 4}\right).$$

Im Falle $s > 2$ wäre ein Eigenwert größer als 1 und im Falle $s < -2$ wäre ein Eigenwert kleiner als -1. Nach eventuellem Übergang zu $-M$ genügt es also, den Fall $s = 2$ zu betrachten. Nach dem Satz von Cayley-Hamilton gilt $M^2 = 2M - E$, denn $M^2 - sM + E = 0$. Nun zeigt man durch vollständige Induktion nach n, dass

$$M^n = nM - (n-1)E \quad \text{für alle } n \in \mathbb{N} \tag{2}$$

gilt.

(IA): Die Gleichung gilt offensichtlich für $n = 1$.

(IV): Die Behauptung in (2) gelte für ein $n \in \mathbb{N}$.

(IS): Zeige die Behauptung für $n + 1$.

Es gilt

$$\begin{aligned} M^{n+1} &= M^n M \\ &= (nM - (n-1)E)M \\ &= nM^2 - (n-1)M \\ &= n(2M - E) - nM + M \\ &= (n+1)M - nE. \end{aligned}$$

Damit ist die Behauptung in (2) mit Hilfe des Prinzips der vollständigen Induktion gezeigt.

Da $M \neq \pm E$ erfüllt ist, gilt somit, dass M unendliche Ordnung hat. Insgesamt folgt also die Behauptung.

$(iii) \Rightarrow (iv)$: Dieser Teil des Beweises folgt aus [K] XXVIII Proposition 1.8.

$(iv) \Rightarrow (v)$: Nach Voraussetzung gibt es ein $\tau \in \mathbb{H}$ mit $M\tau = \tau$, und da $M \neq \pm E$ gilt, ist τ ein Fixpunkt von Γ. Nach [K] XXVIII Korollar 2.8 sind die einzigen Fixpunkte

von Γ aber gerade Li und $L\rho$ für ein $L \in \Gamma$. Damit gilt $MLi = Li$ oder $ML\rho = L\rho$ und es folgt $L^{-1}MLi = i$ oder $L^{-1}ML\rho = \rho$, also nach [K] XXVIII § 2

$$L^{-1}ML \in \Gamma_i \cup \Gamma_\rho = \{N \in \Gamma;\ Ni = i \text{ oder } N\rho = \rho\} = \left\{\pm E, \pm J, \pm U, \pm U^2\right\}.$$

Aus $L^{-1}ML = \pm E$ folgt $M = \pm E$, aber dies ist aber ein Widerspruch zur Voraussetzung. Damit ist die Behauptung gezeigt.

$(v) \Rightarrow (i)$: Es gilt ord $(\pm U) = 3$, ord $(\pm J) = 4$ und ord $\left(\pm U^2\right) = 6$. Es gelte nun $L^{-1}ML = \pm U$. Dann ergibt sich

$$E = \left(L^{-1}ML\right)^3 = L^{-1}\left(MLL^{-1}\right)^2 ML = L^{-1}M^3L,$$

also ord $M = 3$. Gilt dagegen $L^{-1}ML = \pm J$ beziehungsweise $L^{-1}ML = \pm U^2$, so folgt in analoger Weise ord $M = 4$ beziehungsweise ord $M = 6$. □

Eine wichtige Aussage über die Struktur einer endlichen Untergruppe liefert das folgende

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

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

Beweis
Definiere

$$S := \sum_{L \in \Lambda} L^t L = \begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix}.$$

Für

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

gilt

$$L^t L = \begin{pmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{pmatrix}.$$

Da $a^2 + c^2 > 0$ und $\det(L^t L) = 1$ gilt für $L \in \Lambda$, ist $L^t L$ symmetrisch positiv definit. Somit ist S als endliche Summe von symmetrisch positiv definiten Matrizen symmetrisch positiv definit. Für festes $M \in \Lambda$ durchläuft LM ganz Λ, wenn L ganz Λ durchläuft, also gilt

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

Definiere $\tau := w(S) := \alpha^{-1}(-\beta + i\sqrt{\det S})$. Da $\alpha > 0$ und $\det S > 0$ liegt τ in der oberen Halbebene. Definiert man nun für $N \in \mathrm{GL}(2;\mathbb{R})$ und eine symmetrisch positiv definite Matrix $P \in \mathrm{Mat}(2;\mathbb{R})$ den Operator

$$N * P := \left(N^{-1}\right)^t P N^{-1},$$

so folgt mit [KK] II Satz 1.9 für das beliebig, aber fest gewählte $M \in \Lambda$, dass

$$\tau = w(S) = w\left(M^t S M\right) = w\left(M^{-1} * S\right) = M^{-1}\left\langle w(S)\right\rangle = M^{-1}\tau$$

gilt, also ist $M \in \Gamma_\tau$. Da $M \in \Lambda$ beliebig gewählt war, ist Λ eine Untergruppe von Γ_τ. Nach geeigneter Konjugation in Γ darf man wegen

$$\Gamma_{M\tau} = M\Gamma_\tau M^{-1}$$

ohne Einschränkung $\tau \in \mathbb{F}$ annehmen. Nach [K] XXVIII § 2 gilt

$$\Gamma_i = \{\pm E, \pm J\}, \quad \Gamma_\rho = \left\{\pm E, \pm U, \pm U^2\right\} \quad \text{und} \quad \Gamma_\tau = \{\pm E\}, \text{falls } \tau \in \mathbb{F}, \tau \neq i, \rho.$$

Da Λ eine Untergruppe von Γ_τ ist, ist Λ somit konjugiert zu einer der Gruppen

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

Es folgt

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

§ 3 Hauptkongruenz

In diesem Paragrafen werden die Hauptkongruenzgruppen $\Gamma[n]$ der Modulgruppe Γ eingeführt. Exemplarisch wird die Hauptkongruenzgruppe $\Gamma[2]$ näher betrachtet.

(3.1) Definition (Kongruenz)
Sei $n \geq 1$ eine feste natürliche Zahl. Für $M, L \in \mathrm{Mat}(2;\mathbb{Z})$ wird die *Kongruenz*

$$L \equiv M \pmod{n}$$

komponentenweise erklärt, das heißt, es gibt eine Matrix $X \in \mathrm{Mat}(2;\mathbb{Z})$ mit

$$L = M + nX. \qquad \diamond$$

Es gilt

$$LM \equiv L'M' \pmod{n}, \text{ falls } L \equiv L' \pmod{n} \text{ und } M \equiv M' \pmod{n}, \tag{3}$$

denn ist $L = L' + nX$ für ein $X \in \mathrm{Mat}(2;\mathbb{Z})$ und $M = M' + nY$ für ein $Y \in \mathrm{Mat}(2;\mathbb{Z})$, so folgt

$$\begin{aligned} LM &= (L' + nX)(M' + nY) \\ &= L'M' + nXM' + nL'Y + n^2XY \\ &= L'M' + n(XM' + L'Y + nXY) \\ &= L'M' + nZ \quad \text{für ein } Z \in \mathrm{Mat}(2;\mathbb{Z}). \end{aligned}$$

Man definiert

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

Es gilt $\Gamma[1] = \Gamma$.

Nun betrachtet man die kanonische Projektion

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

und setzt sie auf (2×2)-Matrizen fort:

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

Zum Beweis des nächsten Satzes benötigt man das folgende

(3.2) 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

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

Beweis
Sei x das Produkt aller Primzahlen p, die c, aber nicht a teilen, wobei das leere Produkt gleich 1 sei. Angenommen, es gibt eine Primzahl q mit den Eigenschaften $q \mid (a + xb)$ und $q \mid c$.

1. Fall: Angenommen es gilt $q \mid a$. Nach Definition von x gilt dann $q \nmid x$. Aus $q \mid (a + xb)$ und $q \mid a$ sowie $q \nmid x$ folgt dann aber $q \mid b$. Dies ist ein Widerspruch zur Voraussetzung $\mathrm{ggT}(a, b, c) = 1$.

2. Fall: Angenommen es gilt $q \nmid a$. Dann gilt $q \mid x$ nach Definition von x, und $q \mid (a + xb)$ impliziert $q \mid a$ als Widerspruch.

Daher sind $a + xb$ und c teilerfremd, das heißt $\mathrm{ggT}(a + xb, c) = 1$. □

Damit kommen wir zu dem

(3.3) Satz

Die Abbildung

$$\phi : \Gamma \to \mathrm{SL}(2; \mathbb{Z}/n\mathbb{Z}), \quad M \mapsto \overline{M},$$

ist ein surjektiver Gruppenhomomorphismus, dessen Kern $\Gamma[n]$ ist. Zudem 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

Sei

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}(2; \mathbb{Z}).$$

Für alle

$$X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \in \mathrm{Mat}(2; \mathbb{Z})$$

gilt

$$\begin{aligned} \det M + nX &= \det \begin{pmatrix} a + x_1 n & b + x_2 n \\ c + x_3 n & d + x_4 n \end{pmatrix} \\ &= ad + ndx_1 + nax_4 + n^2 x_1 x_4 - bc - nbx_3 - ncx_2 - n^2 x_2 x_3 \\ &= \det M + n(dx_1 + ax_4 + nx_1 x_4 - bx_3 - cx_2 - nx_2 x_3) \\ &= \det M + nz \quad \text{für ein } z \in \mathbb{Z}, \end{aligned}$$

also gilt $\overline{\det M} = \det \overline{M}$ und das Bild von ϕ ist in $\mathrm{SL}(2; \mathbb{Z}/n\mathbb{Z})$ enthalten. Die Abbildung ϕ ist ein Gruppenhomomorphismus, denn nach (3) gilt

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

für alle $M, N \in \Gamma$. Da

$$\begin{aligned} M \in \mathrm{Kern}\,\phi &\Leftrightarrow \phi(M) = \overline{E} \\ &\Leftrightarrow M = E + nX \quad \text{für ein } X \in \mathrm{Mat}(2; \mathbb{Z}) \\ &\Leftrightarrow M \equiv E \pmod{n} \\ &\Leftrightarrow M \in \Gamma[n] \end{aligned}$$

gilt, folgt $\operatorname{Kern}\phi = \Gamma[n]$. Der Kern eines Gruppenhomomorphismus $\varphi : G \to G'$ ist stets ein Normalteiler in G, also gilt hier, dass $\Gamma[n]$ ein Normalteiler in Γ ist. Sei

$$K := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \operatorname{Mat}(2;\mathbb{Z})$$

mit $\overline{K} \in \mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z})$ und es sei ohne Einschränkung $\gamma \neq 0$, da man sonst γ durch $\gamma + n$ ersetzen kann. Wegen $\alpha\delta - \beta\gamma \equiv 1 \pmod{n}$ gilt $\mathrm{ggT}(\gamma, \delta, n) = 1$. Nach 3.2 existiert ein $r \in \mathbb{Z}$, so dass $\mathrm{ggT}(\gamma, \delta + rn) = \mathrm{ggT}(\gamma, d) = 1$ für $d = \delta + rn$ gilt. Nun hat man

$$\alpha d - \beta\gamma = \alpha\delta - \beta\gamma + \alpha rn = 1 + sn$$

für ein $s \in \mathbb{Z}$. Wegen $\mathrm{ggT}(\gamma, d) = 1$ kann man $x, y \in \mathbb{Z}$ so bestimmen, dass $\gamma y - dx = s$ gilt. Es folgt

$$M := \begin{pmatrix} \alpha + xn & \beta + yn \\ \gamma & \delta + rn \end{pmatrix} \in \mathrm{SL}(2;\mathbb{Z}),$$

da

$$\begin{aligned} \det M &= (\alpha + xn)(\delta + rn) - (\beta + yn) \cdot \gamma \\ &= (\alpha + xn) \cdot d - (\beta + yn) \cdot \gamma \\ &= \alpha d - \beta\gamma + n(xd - y\gamma) \\ &= 1 + sn + n(-s) \\ &= 1, \end{aligned}$$

also existiert zu $\overline{K} \in \mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z})$ ein $M \in \Gamma$ mit $\phi(M) = \overline{M} = \overline{K}$, das heißt, ϕ ist surjektiv. Nach dem Homomorphiesatz für Gruppen ist $\Gamma/\Gamma[n]$ isomorph zu $\operatorname{Bild}\phi = \mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z})$ und es folgt

$$\big[\Gamma : \Gamma[n]\big] = \#\mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z}) < \infty. \qquad \square$$

(3.4) Definition (Hauptkongruenzgruppe, Stufe)
Die Untergruppe $\Gamma[n]$ von Γ heißt *Hauptkongruenzgruppe* $\pmod{n}$, die Zahl n nennt man *Stufe* von $\Gamma[n]$. $\diamond$

Gilt $M \equiv L \pmod{n}$ für $M, L \in \Gamma$, so gibt es ein $X \in \operatorname{Mat}(2;\mathbb{Z})$ mit $M = L + nX$, also $ML^{-1} = E + nXL^{-1}$ und somit $ML^{-1} \equiv E \pmod{n}$. Das heißt, dass M und L in diesem Fall in derselben Nebenklasse modulo $\Gamma[n]$ liegen und man erhält das

(3.5) Korollar
Zwei Matrizen M und L aus Γ liegen genau dann in derselben (Links- oder Rechts-) Nebenklasse von $\Gamma[n]$, wenn $M \equiv L \pmod{n}$ gilt. ◇

Der Index kann mit 3.3 berechnet werden:

$$\big[\Gamma : \Gamma[n]\big] = \#\mathrm{SL}(2;\mathbb{Z}/n\mathbb{Z}) = n^3 \prod_{\substack{p|n \\ p \text{ prim}}} (1 - p^{-2}) \quad \text{für } n \geq 2. \tag{4}$$

Einen Beweis dieser Formel findet man bei [M] S. 63–65, [L] S. 356 und [R] S. 21–23.

Nun folgt eine Aussage über die Fixpunkte in $\Gamma[n]$ in der

(3.6) 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 $M = \pm E$ für $n = 2$ und $M = E$ für $n > 2$. ◇

Beweis
Gilt $M\tau = \tau$ für ein $M \neq \pm E$ aus $\Gamma[n]$, so ist τ ein Fixpunkt von Γ, da $\Gamma[n]$ eine Untergruppe von Γ ist. Mit [K] XXVIII Satz 2.8 schließt man $\tau = Li$ oder $\tau = L\rho$ mit geeignetem $L \in \Gamma$. Da $M\tau = \tau$ nach Voraussetzung gilt, ergibt sich $MLi = Li$ oder $ML\rho = L\rho$, also gilt $L^{-1}MLi = i$ oder $L^{-1}ML\rho = \rho$. Nun kann man [K] XXVIII Satz 2.6 anwenden und erhält $L^{-1}ML = \pm J$ oder $L^{-1}ML = \pm U, \pm U^2$. Da $\Gamma[n]$ nach 3.3 ein Normalteiler von Γ ist, gehören $\pm J, \pm U$ oder $\pm U^2$ zu $\Gamma[n]$ für $n \geq 2$.

Das ist aber nicht der Fall, denn es gibt keine Matrizen $X, Y, Z \in \mathrm{Mat}(2;\mathbb{Z})$, so dass für $n \geq 2$ gilt

$$\begin{aligned}
\pm J &= \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = E + nX, \\
\pm U &= \pm \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} = E + nY \quad \text{oder} \\
\pm U^2 &= \pm \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = E + nZ
\end{aligned}$$

gilt. Daher folgt $M = \pm E$ für $n = 2$ und $M = E$ für $n > 2$, da $M = -E$ für $n > 2$ nicht in $\Gamma[n]$ liegt. □

Nun bestimmt man exemplarisch für den Fall $n = 2$ ein Vertretersystem der Nebenklassen von $\Gamma[2]$ in Γ sowie den Fundamentalbereich von $\Gamma[2]$ in dem folgenden

(3.7) Beispiel
Es sei $n = 2$. Dann gilt

$$\big[\Gamma : \Gamma[2]\big] = \#\mathrm{SL}(2;\mathbb{Z}/2\mathbb{Z}) = 2^3 \prod_{p|2}(1 - p^{-2}) = 6$$

nach (4), das heißt, ein Vertretersystem der Nebenklassen von $\Gamma[2]$ in Γ enthält 6 Elemente. Nach 3.5 genügt es, sechs Matrizen zu bestimmen, so dass immer für jeweils zwei dieser Matrizen L und M die Beziehung

$$M \equiv L \pmod{n}$$

nicht erfüllt ist. Da man in diesem Beispiel einen Fundamentalbereich von $\Gamma[2]$ grafisch darstellen möchte, sollte man hier die Matrizen so wählen, dass der Fundamentalbereich eine übersichtliche Darstellung besitzt. Durch Nachrechnen überprüft man, dass die folgenden Matrizen ein Vertretersystem der Nebenklassen von $\Gamma[2]$ in Γ bilden:

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

$$J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; U = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \; U^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Aus 1.3 folgt damit, dass

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

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

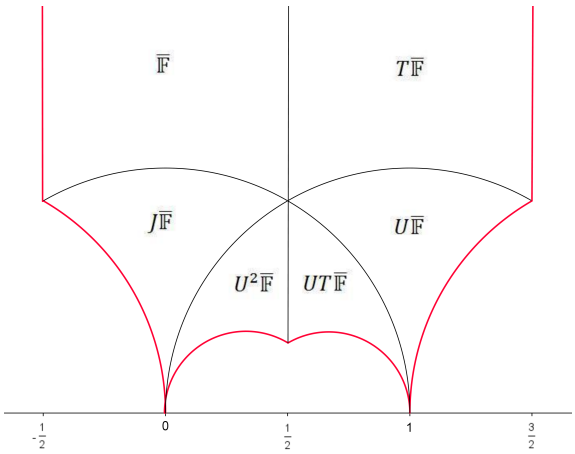

Abbildung 1: Fundamentalbereich von $\Gamma[2]$

Für eine Gruppe, die zu $\Gamma[2]$ äquivalent ist, hat C. F. Gauss bereits um 1808 einen analogen Fundamentalbereich konstruiert, vergleiche [G] S. 100–105. ◇

§ 4 Kongruenzgruppen

Nach der Einführung der Hauptkongruenzgruppen $\Gamma[n]$ in § 3 werden nun Kongruenzgruppen betrachtet. Als Spezialfall wird die Kongruenzgruppe $\Gamma_0[n]$ behandelt. Wie auch in § 3 wird hier der Fall $\Gamma_0[2]$ genauer untersucht.

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

Jede Kongruenzgruppe von Γ hat endlichen Index in Γ, da $\Gamma[n]$ nach 3.3 endlichen Index in Γ hat.

Eine wichtige Klasse von Beispielen sind die Gruppen

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

Man prüft für $M, N \in \Gamma_0[n]$ leicht nach, dass $MN \in \Gamma_0[n]$ und $M^{-1} \in \Gamma_0[n]$ gilt. Für $n = 1$ erhält man $\Gamma_0[1] = \Gamma$. Zudem gilt $\Gamma[n] \subset \Gamma_0[n]$, denn

$$\Gamma[n] = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma;\ a \equiv d \equiv 1 \pmod{n} \text{ und } b \equiv c \equiv 0 \pmod{n} \right\}.$$

Man betrachtet wieder den Fall $n = 2$ in dem folgenden

(4.2) Beispiel
Sei $n = 2$. 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 3.7 gilt somit insbesondere

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

Nun muss überprüft werden, welche dieser Matrizen dieselben Rechtsnebenklassen von Γ modulo $\Gamma_0[2]$ beschreiben. Dazu prüft man durch Nachrechnen, für welche Matrizen $M, L \in \{E, T, -UT, J, U, U^2\}$ die Beziehung

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

gilt. Man erhält, dass $ML^{-1} \notin \Gamma_0[2]$ gilt für $M, L \in \{E, J, U^2\}$. Somit bilden die Matrizen E, J und U^2 ein Vertretersystem von Rechtsnebenklassen von Γ modulo $\Gamma_0[2]$. Nach § 1 (1) gilt also

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

und ein Fundamentalbereich ist nach 1.3 gegeben durch

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

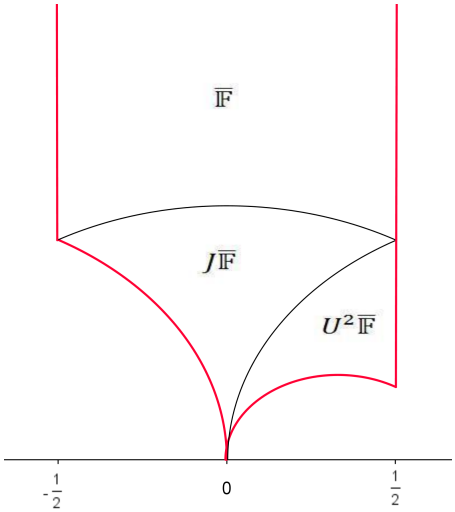

Abbildung 2: Fundamentalbereich von $\Gamma_0[2]$

Da $\Gamma_0[2]$ in Γ den Index 3 und $\Gamma[2]$ in Γ nach 3.7 den Index 6 hat, folgt

$$\big[\Gamma_0[2] : \Gamma[2]\big] = \big[\Gamma : \Gamma[2]\big] / \big[\Gamma : \Gamma_0[2]\big] = 6/3 = 2.$$

Es müssen also zwei Matrizen aus $\Gamma_0[2]$ gefunden werden, die ein Vertretersystem von Rechtsnebenklassen von $\Gamma_0[2]$ modulo $\Gamma[2]$ bilden. Da für E und T gilt

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

bilden E und T dieses Vertretersystem. Daher gilt $\Gamma_0[2] = \Gamma[2] \cup (\Gamma[2] \cdot T)$. ◇

Analog zu $\Gamma_0[n]$ kann man natürlich die Untergruppe

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

definieren. Es gilt $\Gamma^0[n] = J\Gamma_0[n]J^{-1}$, denn ist

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^0[n],$$

so gibt es ein

$$N = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \in \Gamma_0[n]$$

mit $M = JNJ^{-1}$. Ist umgekehrt

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

so ist

$$JMJ^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \in \Gamma^0[n].$$

Eine ausführliche Diskussion der Gruppen $\Gamma_0[n]$ und $\Gamma^0[n]$ findet man unter anderem bei [P] S. 241–251. Mit Hilfe von 3.3 zeigt man, dass

$$\big[\Gamma : \Gamma_0[n]\big] = \big[\Gamma : \Gamma^0[n]\big] = n \prod_{\substack{p|n \\ p \text{ prim}}} (1 + p^{-1}) \quad \text{für } n \geq 2$$

gilt. Einen Beweis dazu findet man in [R] S. 26. Diese und weitere Untergruppen der Modulgruppe werden diskutiert in [KF] Abschnitt 2, [N] Kapitel VIII, [L] Kapitel XI.3 und [R] Kapitel 1.

Zum Abschluss seien noch zwei Bemerkungen geben.

(4.3) Bemerkungen

(a) 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 mal bei [M] S. 77–79 und H. Petersson (J. Reine Angew. Math. **250**, 182–212 (1971); **268/9**, 94–109 (1974)).

(b) Für $n > 1$ sind $\Gamma_0[n]$ und $\Gamma^0[n]$ keine Normalteiler in Γ. Exemplarisch betrachte man den Fall $\Gamma_0[n]$ für $n > 1$. Ein Element aus $\Gamma_0[n]$ hat die Form

$$M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} + nX = \begin{pmatrix} a + nx_1 & b + nx_2 \\ nx_3 & d + nx_4 \end{pmatrix} \text{ mit } X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \in \mathrm{Mat}(2; \mathbb{Z}).$$

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

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

und gilt $n \nmid b$, so folgt

$$JMJ^{-1} = \begin{pmatrix} d + nx_4 & -nx_3 \\ -b - nx_2 & a + nx_1 \end{pmatrix} \notin \Gamma_0[n].$$

Demnach ist $\Gamma_0[n]$ für $n > 1$ kein Normalteiler in Γ. ◇

Literaturverzeichnis

[A] M. Artin: *Algebra*. 1. Aufl., Birkhäuser Verlag AG, Basel 1993.

[D] R. Dedekind: *Gesammelte mathematische Werke I–III*. Braunschweig, 1930–1932; Nachdruck, Chelsea, New York 1969.

[G] C. F. Gauss: *Werke I–XII*. Ges. d. Wiss. Göttingen, Teubner, Leipzig 1863–1933.

[K] A. Krieg: *Höhere Funktionentheorie I*. Vorlesungsskript, RWTH Aachen, Aachen 2007.

[KF] F. Klein, R. Fricke: *Vorlesungen über die Theorie der elliptischen Modulfunktionen I, II*. Teubner, Leipzig 1890, 1892.

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

[L] J. Lehner: *Discontinous groups and automorphic functions*. Math. Surv. Monogr. **VIII**, Amer. Math. Soc., Providence 1964.

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

[N] M. Newman: *Integral matrices*. Academic Press, New York-London 1972.

[P] H. Petersson: *Modulfunktionen und quadratische Formen*. Ergeb. Math. Grenzgeb. **100**, Springer-Verlag, Berlin-Heidelberg-New York 1982.

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