Eine Präsentation der Modulgruppe

Sebastian Schönnenbeck

Seminar zur Funktionentheorie II - WS 2012/13

RWTH Aachen

Lehrstuhl A für Mathematik

Inhaltsverzeichnis

Einleitung **3**

1 Wiederholung: Freie Gruppen und Präsentationen **4**
1.1 Grundlagen 4
1.2 Die universelle Eigenschaft 5
1.3 Präsentationen 6

2 Eine Präsentation der Modulgruppe **10**
2.1 Erzeuger 10
2.2 Die Präsentation 11

3 Eine Klasse von Nicht-Kongruenzuntergruppen **14**
3.1 Zugrunde liegende Ergebnisse von H. Frasch 14
3.2 Eine Klasse normaler Untergruppen 16

Literaturverzeichnis **19**

Einleitung

Ein wesentliches Objekt in der Funktionentheorie ist die Modulgruppe $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, welche durch Möbiustransformationen auf der oberen Halbebene $\mathbb{H}$ operiert. In der Vorlesung haben wir bereits verschiedene Erzeugendensysteme sowie einen Fundamentalbereich der erwähnten Operation bestimmt. Um die Modulgruppe nun aber auch auf gruppentheoretischer Ebene besser in den Griff zu bekommen, ist es von Interesse eine Präsentation von Γ - also Erzeuger und definierende Relationen - zu bestimmen. Dies soll das erste Ziel dieser Ausarbeitung sein. Darüber hinaus beschäftigen wir uns im letzten Kapitel mit einigen (normalen) Untergruppen der Modulgruppe und werden (im Kontrast zu den vorangegangenen Vorträgen) eine Beispielklasse konstruieren, die sämtlich aus Nicht-Kongruenzuntergruppen von Γ besteht.

1 Wiederholung: Freie Gruppen und Präsentationen

1.1 Grundlagen

Wir wiederholen zunächst einige Begriffe aus der Vorlesung „Computeralgebra“ und orientieren uns dabei am Vorlesungsskript von Prof. Dr. G. Nebe aus dem Sommersemester 2010 ([Neb10]).

Definition 1.1.1 *Es sei M eine Menge, sowie M^{-1} eine weitere Menge mit $M \cap M^{-1} = \emptyset$ und einer Bijektion*

$$^{-1} : M \to M^{-1} : a \mapsto a^{-1},$$

deren Umkehrabbildung wir wieder mit $^{-1}$ bezeichnen wollen. Wir definieren nun

$$\mathrm{Seq}(M) := \left\{(a_1, a_2, \ldots, a_n) \;\middle|\; n \in \mathbb{N}_0, a_i \in M \cup M^{-1} \;\forall\; 1 \leq i \leq n\right\},$$

die Menge aller endlichen Folgen (oder Wörter) in Elementen aus $M \cup M^{-1}$.

Bemerkung und Definition 1.1.2 *1. In der Situation von 1.1.1 wird* $\mathrm{Seq}(M)$ *zu einem Monoid durch die Verknüpfung*

$$(a_1, \ldots, a_n)(b_1, \ldots, b_m) := (a_1, \ldots, a_n, b_1, \ldots, b_m),$$

das einfache Aneinanderhängen der Folgen, mit neutralem Element $(\ )$, der leeren Folge.

2. *Auf* $\mathrm{Seq}(M)$ *definieren wir eine Äquivalenzrelation durch $a \sim b$ genau dann, wenn b aus a durch Einfügen und/oder Weglassen endlich vieler Folgenabschnitte der Form (m, m^{-1}), $m \in M \cup M^{-1}$ hervorgeht. Die Äquivalenzklasse von $a \in \mathrm{Seq}(M)$ unter $\sim$ sei mit $[a]$ bezeichnet.*

3. *Die angegebene Verknüpfung, die* $\mathrm{Seq}(M)$ *zu einem Monoid macht, ist verträglich mit* $\sim$*. Anders ausgedrückt, sind* $a, b, a', b' \in \mathrm{Seq}(M)$ *mit* $a \sim a'$ *und* $b \sim b'$ *so ist auch* $ab \sim a'b'$*.*

4. *Die Fortsetzung der obigen Verknüpfungen auf* $\mathrm{F}(M) := \mathrm{Seq}(M)/\sim$ *macht* $\mathrm{F}(M)$ *zu einer Gruppe, der sogenannten freien Gruppe auf* M*.*

Beweis zu (4): Dass die Fortsetzung der Verknüpfung $[a]\,[b] := [ab]\,,\ a, b \in \mathrm{Seq}(M)$ wohldefiniert ist, folgt aus (3). Assoziativität und Einselement erbt F vom Monoid $\mathrm{Seq}(M)$. Zur Existenz von Inversen:

$$[(a_1, \ldots, a_n)]\left[(a_n^{-1}, \ldots, a_1^{-1})\right] = \left[a_1, \ldots, a_n, a_n^{-1}, \ldots, a_1^{-1}\right] = [()]$$

durch sukzessives Anwenden von $[(a, a^{-1})] = [()]$. Also ist

$$[(a_1, \ldots, a_n)]^{-1} = \left[(a_n^{-1}, \ldots, a_1^{-1})\right].$$

□

Beispiel 1.1.3 *Vermöge* $a \leftrightarrow 1$ *ist* $\mathrm{F}(\{a\}) \cong (\mathbb{Z}, +)$*.*

1.2 Die universelle Eigenschaft

Die freien Gruppen sind unter den Gruppen durch gewisse Fortsetzungseigenschaften charakterisiert.

Beispiel 1.2.1 *Es sei* $C_2 \cong G := \{-1, 1\} \leq \mathbb{R}^*$ *die (eindeutige) Untergruppe von Ordnung* 2 *der multiplikativen Gruppe* $\mathbb{R}^* = \mathbb{R} - \{0\}$*. Ist nun* H *eine weitere Gruppe und* $\phi : G \to H$ *ein Homomorphismus, so ist*

$$1 = \phi(1) = \phi((-1)^2) = \phi(-1)^2.$$

$\phi(-1) \in H$ *ist also ein Element von Ordnung* 1 *oder* 2*. Möchte ich also allgemein einen Homomorphismus von* G *in eine andere Gruppe konstruieren, so muss ich unter anderem diese Bedingung an das Bild von* -1 *sicherstellen.*

Sind nun G und H Gruppen und E ein Erzeugendensystem von G, so zeigt das vorangegangene Beispiel, dass sich im Allgemeinen nicht jede Abbildung von E nach H

zu einem Homomorphismus von G nach H fortsetzen lässt. Insbesondere müssen die Bilder der Elemente von E die zwischen den Elementen aus E bestehenden Relationen berücksichtigen. Diese Einschränkungen bestehen bei freien Gruppen nicht, wie der folgende Satz zeigt.

Satz 1.2.2 (Die universelle Eigenschaft) *Ist M eine Menge, G eine Gruppe und $\phi : M \to G$ eine Abbildung, so existiert genau ein Homomorphismus $\Phi : \mathrm{F}(M) \to G$ mit der Eigenschaft $\Phi(m) = \phi(m)\ \forall\ m \in M$.*

Beweis: Wir halten zunächst fest, dass Homomorphismen durch die Bilder eines Erzeugendensystems eindeutig bestimmt sind. Da M ein solches für $\mathrm{F}(M)$ darstellt, ist die Eindeutigkeit (unter der Voraussetzung der Existenz) klar. Zur Existenz: Wir definieren Φ auf die einzig mögliche Art und Weise und zeigen, dass es sich um einen wohldefinierten Homomorphismus handelt. Setze also zunächst zu $m \in M$: $\Phi([m]) = \phi(m)$ und $\Phi([m^{-1}]) = \phi(m)^{-1}$. Dann sind wir gezwungen Φ durch

$$\Phi([(a_1, \ldots, a_n)]) := \Phi([a_1]) \cdot \ldots \cdot \Phi([a_n]),\ a_1, \ldots, a_n \in M \cup M^{-1}$$

zu definieren. Unter dieser Setzung setzt Φ sicherlich ϕ fort. Nach Wahl der $\Phi([m^{-1}]), m \in M$ ändert Einfügen oder Weglassen von Folgenabschnitten der Form $(m, m^{-1}),\ m \in M \cup M^{-1}$ das Bild unter Φ nicht; Φ ist also insbesondere wohldefiniert und nach Konstruktion sicherlich multiplikativ also ein Homomorphismus mit den gewünschten Eigenschaften. □

1.3 Präsentationen

Ist nun M eine Menge, G eine Gruppe und $\Phi : \mathrm{F}(M) \to G$ ein Epimorphismus, so ist nach dem Homomorphiesatz

$$G \cong \mathrm{F}(M)/\mathrm{Ke}(\Phi)$$

wobei $\mathrm{Ke}(\Phi)$ den Kern von Φ - also das Urbild der 1 - bezeichnet. Da wir $\mathrm{F}(M)$ durch die Angabe von M schon vollständig kennen, stellt sich also die Frage, wie wir $\mathrm{Ke}(\Phi)$ möglichst einfach beschreiben können. Dies stellt uns dann eine Beschreibung von G zur Verfügung, die uns möglicherweise neue gruppentheoretische Erkenntnisse liefert.

Beispiel 1.3.1 *Wir betrachten die freie Gruppe auf zwei Elementen $\mathrm{F}(\{a, b\})$ sowie den Homomorphismus $\phi : \mathrm{F}(\{a, b\}) \to S_3$ (S_3 die symmetrische Gruppe auf drei Punkten),*

definiert durch $a \mapsto (1,2),\ b \mapsto (1,2,3)$ *(in der üblichen Zykelschreibweise). Dann gilt*

$$\mathrm{Ke}(\phi) \supset \langle a^2, b^3, aba^{-1}b\rangle,$$

der Kern wird jedoch als Untergruppe nicht von diesen drei Elementen erzeugt (beispielsweise ist $(bab^{-1})^2 \in \mathrm{Ke}(\phi) - \langle a^2, b^3, aba^{-1}b\rangle$*). Der Kern von* ϕ *ist also nicht die kleinste Untergruppe von* $\mathrm{F}(\{a,b\})$*, die* $a^2, b^3, aba^{-1}b$ *enthält, sehr wohl aber der kleinste Normalteiler. An dieser Stelle sei daran erinnert, dass Kerne von Homomorphismen stets Normalteiler sind. Ein Erzeugendensystem als Untergruppe ist beispielsweise (ohne Beweis vgl. [Neb10] Beispiel nach (1.50)) durch*

$$a^2, b^3, (ab)^2, (ba)^2, (ba^{-1})^2, ab^3a^{-1}, (b^{-1}a)^2$$

gegeben.

Das obige Beispiel zeigt, dass es schnell unpraktikabel wird, den Kern des betrachteten Homomorphismus durch ein Untergruppenerzeugendensystem anzugeben. Betrachten wir weiter die herausfaktorisierte Untergruppe als Menge von Relationen (ist b^2 im Kern von ϕ, so können wir dies auch als „$b^2 = 1$ in der Faktorgruppe“ lesen), so gehen insbesondere alle oben genannten Relationen aus den ersten dreien (durch Konjugation und Kombination) hervor. Dies fassen wir konkreter in der folgenden

Definition 1.3.2 *Es sei* G *eine Gruppe und* $R \subset G$ *eine Teilmenge. Wir definieren*

$$\langle R\rangle_{\lhd G} := \bigcap_{N \lhd G, R \subset N} N \lhd G,$$

das Normalteilererzeugnis von R *in* G *(dies hängt insbesondere von* G *ab).*

Im obigen Beispiel ist also

$$\mathrm{Ke}(\phi) = \langle a^2, b^3, aba^{-1}b\rangle_{\lhd \mathrm{F}(\{a,b\})} \neq \langle a^2, b^3, aba^{-1}b\rangle.$$

Diese Kurzschreibweise ermöglicht es uns nun, Präsentationen zu definieren.

Bemerkung und Definition 1.3.3 *Es sei* M *eine Menge und* $R \subset \mathrm{F}(M)$*. Wir setzen*

$$\langle M \mid R\rangle := \mathrm{F}(M)/\langle R\rangle_{\lhd \mathrm{F}(M)}.$$

1. *Haben wir eine Gruppe* G *auf diese Art und Weise geschrieben, so sagen wir, dass* G *durch Erzeuger* (M) *und Relationen* (R) *gegeben ist. Gelegentlich werden*

wir der besseren Lesbarkeit halber anstelle von Elementen aus $\mathrm{F}(M)$ *in* R *formale Gleichsetzungen von Elementen aus* $\mathrm{F}(M)$ *aufnehmen.* $(w_1 = w_2) \in R$ *lesen wir also als* $w_1 w_2^{-1} \in R$*. Beispielsweise ist es einfacher die Aussage von* $(aba^{-1} = b^{-1}) \in R$ *(a konjugiert b auf sein Inverses) zu erfassen, als die Aussage der an sich identischen Relation* $aba^{-1}b \in R$*.*

2. *Ist* G *eine Gruppe und*
$$\phi : \langle M \mid R \rangle \to G$$
ein Isomorphismus, so heißt ϕ *eine Präsentation von* G*. Gelegentlich wird auch* $\langle M \mid R \rangle$ *bereits als Präsentation von* G *bezeichnet.*

3. *Eine Gruppe* G *heißt endlich präsentierbar, falls eine Präsentation von* G *mit endlichen* M *und* R *existiert.*

Wir greifen das vorangegangene Beispiel erneut auf.

Beispiel 1.3.4 $\langle a, b \mid a^2, b^3, aba^{-1} = b^{-1} \rangle$ *ist eine Präsentation von* S_3*. Dies folgert man leicht aus dem nächsten Beispiel, da* $S_3 \cong D_6$ *auch die Symmetriegruppe eines gleichmäßigen Dreiecks ist.*

Proposition 1.3.5 *Jede endliche Gruppe ist endlich präsentierbar. Wähle dazu eine beliebige Menge* M*, welche in Bijektion zu* G *steht (nummeriere die Elemente von* G *beispielsweise durch) und* R *die Multiplikationstafel von* G*.*

Eine recht anschauliche Klasse von Beispielen stellen die Diedergruppen dar:

Beispiel 1.3.6 *Mit* D_{2n} *wollen wir die Symmetriegruppe eines gleichmäßigen* n*-Ecks bezeichnen. Betrachten wir dieses in der üblichen euklidischen Ebene, legen seinen Mittelpunkt in den Ursprung und eine der Ecken in den Punkt* $(0, 1)$*, so zeigt eine geometrische Überlegung:*
$$D_{2n} = \langle S := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, R := \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \rangle$$
Eine Präsentation von D_{2n} *können wir wie folgt angeben:*
$$D_{2n} \cong \langle s, r \mid s^2, r^n, srs = r^{-1} \rangle =: G$$

Beweis: *Wir betrachten* $\phi : \mathrm{F}(\{s, r\}) \to D_{2n}$ *definiert durch* $r \mapsto R, s \mapsto S$*. Dann gilt sicherlich (durch Nachrechnen):*
$$s^2, r^n, (sr)^2 \in \mathrm{Ke}(\phi);$$

folglich ist also

$$\hat{\phi} : \langle s, r \mid s^2, r^n, srs = r^{-1} \rangle \to D_{2n}, s \mapsto S, r \mapsto R$$

wohldefiniert und klarerweise surjektiv, da S und R die Gruppe D_{2n} erzeugen. Weiter ist $N := \langle r \rangle \triangleleft G$ ein Normalteiler (da $srs^{-1} = srs = s^{-1} \in N$) von Ordnung kleiner oder gleich n, sowie $G/N = \langle sN \rangle$ von Ordnung kleiner oder gleich 2 (da $s^2 = 1$). Also ist $|G| \leq 2n$. Da aber $|D_{2n}| = 2n$ und $\hat{\phi}$ surjektiv, folgt bereits $|G| = 2n$ und $\hat{\phi}$ ist somit ein Isomorphismus. Dies war aber gerade die Behauptug. □

2 Eine Präsentation der Modulgruppe

2.1 Erzeuger

Wie üblich bezeichne $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ die Modulgruppe sowie J und T die Matrizen

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

sowie

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Aus der Vorlesung kennen wir bereits das folgende Resultat:

Satz 2.1.1 *J und T sind Erzeuger der Modulgruppe.*

Vergleiche hierzu [KK07] Kapitel II, §2.

Bemerkung und Definition 2.1.2 *Ist G eine Gruppe, so heißt jeder Homomorphismus $\phi : G \to \mathbb{C}^*$ ein abelscher Charakter. Die Menge der abelschen Charaktere der Gruppe G bildet mit der punktweisen Multiplikation selbst eine Gruppe, die wir mit $\hat{G}$ bezeichnen wollen.*

Setzt man

$$U := -TJ = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},$$

so ist $U^3 = I_2$ und man erhält das folgende, bereits aus der Vorlesung bekannte

Korollar 2.1.3 *Γ wird von den Matrizen J und U, welche beide endliche Ordnung haben, erzeugt.*

Diese Aussage findet sich ebenfalls in [KK07] Kapitel II, §2. Im Hinblick auf $\hat{\Gamma}$ können wir also folgern:

Korollar 2.1.4

$$|\hat{\Gamma}| \leq 12$$

Beweis: U und J erzeugen Γ, also legen ihre Bilder einen Homomorphismus eindeutig fest. Ist $\phi \in \hat{\Gamma}$, so ist aus Ordnungsgründen

$$\phi(J) \in \{\pm 1, \pm i\}\,,\ \phi(U) \in \{1, \exp(2\pi i/3), \exp(4\pi i/3)\}\,.$$

Es existieren also höchstens 12 Paare $(\phi(J), \phi(U)),\ \phi \in \hat{\Gamma}$. Damit folgt die Behauptung. □

Wir werden später zeigen, dass jede der 12 Möglichkeiten auch tatsächlich angenommen wird.

2.2 Die Präsentation

Die beiden Erzeuger U und J erfüllen zunächst die Ordnungsrelationen $U^3 = J^4 = 1$. Darüber hinaus ist $J^2 = -I_2$ also insbesondere zentral ($J^2U = UJ^2$). Wir zeigen nun, dass diese drei Relationen alle anderen zwischen J und U herrschenden Relationen implizieren.

Satz 2.2.1

$$\Gamma = \mathrm{SL}_2(\mathbb{Z}) \cong \langle u, j \mid u^3 = j^4 = 1, uj^2 = j^2u \rangle$$

Beweis: U und J erfüllen nach der Vorbemerkung sicherlich die für u und j angegebenen Relationen. Es bleibt also lediglich zu zeigen, dass sich jede andere Relation bereits aus diesen dreien ergibt. Sei dazu

$$I_2 = J^{n_1}U^{m_1} \ldots J^{n_k}U^{m_k},\ n_i, m_i \in \mathbb{Z},\ k \in \mathbb{N}_0.$$

Wir zeigen, dass wir dieses Wort unter Verwendung der bekannten Relationen zum Nullwort reduzieren können. Dazu betrachten wir zunächst die Matrizen

$$UJ = T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, U^2J^3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

und stellen fest, dass jedes endliche Produkt dieser beiden Matrizen ausschließlich nichtnegative Einträge aufweist. Da $A \cdot I_2 \cdot A^{-1} = I_2$ für alle $A \in \Gamma$ können wir nach Konjugation mit U^{m_k} annehmen, dass $m_k = 0$ gilt. Nach Anwenden der Ordnungsrelationen (also dem Streichen aller Potenzen von U^3 und J^4) sind wir also in der Situation

$$I_2 = U^{m_1} J^{n_1} U^{m_2} \dots U^{m_k} J^{n_k},\ k \in \mathbb{N}_0, m_i \in \{1,2\}\,,\ n_i \in \{1,2,3\}\ \forall\ 1 \leq i \leq k.$$

Nun nutzen wir aus, dass J^2 zentral ist, sammeln eine geeignete Potenz von J am Schluss des Produkts und stellen so sicher, dass $n_i = 1$, wann immer $m_i = 1$ und $n_i = 3$, wann immer $m_i = 2$. Zusammengefasst:

$$\begin{aligned} I_2 =& U^{m_1} J^{n_1} U^{m_2} \dots U^{m_k} J^{n_k} J^l,\ k, l \in \mathbb{N}_0, m_1, \dots,\ m_i \in \{1,2\}\ \forall\ 1 \leq i \leq k, \\ & m_i = 1 \Rightarrow n_i = 1, m_i = 2 \Rightarrow n_i = 3 \end{aligned}$$

Nun ist aber $U^{m_1} J^{n_1} U^{m_2} \dots U^{m_k}$ ein Produkt der Matrizen UJ und U^2J^3 besitzt also ausschließlich nichtnegative Einträge (und im Fall $k \neq 0$ einen Nicht-0-Eintrag neben der Diagonalen). Eine solche Matrix ist aber sicher nicht das Inverse einer Potenz von J, es sei denn $k = 0$ und $l \in 4\mathbb{Z}$. Also ist $U^{m_1} J^{n_1} U^{m_2} \dots U^{m_k}$ bereits das Nullwort und J^l lässt sich mit Hilfe der Ordnungsrelation für J ebenfalls zu diesem reduzieren. Folglich haben wir unter Verwendung der gegebenen Relationen das Ausgangswort auf das Nullwort reduziert. Dies impliziert die Behauptung. □

Korollar 2.2.2 *Die Modulgruppe* Γ *ist ein Beispiel für eine unendliche Gruppe, die endlich präsentierbar ist.*

2.2.1 liefert uns nun ein weiteres Resultat, welches in der Vorlesung bereits ohne Beweis angegeben wurde.

Korollar 2.2.3 *Die Gruppe der Modulsubstitutionen ist ein freies Produkt einer* C_2 *und einer* C_3*.*

Beweis: Bekanntlich ist die Gruppe der Modulsubstitutionen isomorph zu $\mathrm{PSL}_2(\mathbb{Z})$. Und damit gilt mit dem soeben bewiesenen Satz:

$$\mathrm{PSL}_2(\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z})/\pm I_2 \cong \Gamma/\langle J^2\rangle \cong \langle u, j \mid u^3, j^4, uj^2 = j^2u\rangle/\langle j^2\rangle \cong \langle u, j | u^3, j^2\rangle$$

Dabei gilt die letzte Isomorphie, da $j^2 = 1$ bereits $j^4 = 1$ und die Zentralität von j^2 impliziert. Letzteres ist aber gerade die Standardpräsentation eines freien Produkts einer C_2 und einer C_3 wie behauptet. □

Auch das bereits erwähnte Resultat zu $\hat{\Gamma}$ folgt nun leicht.

Korollar 2.2.4

$$\hat{\Gamma} \cong C_{12}$$

Beweis: Die Präsentation zeigt, dass jede Wahl von $\phi(U) \in \{1, \exp(2\pi i/3), \exp(4\pi i/3)\}$ und $\phi(J) \in \{\pm 1, \pm i\}$ einen wohldefinierten Homomorphismus $\phi : \Gamma \to \mathbb{C}^*$ liefert, da die zuvor noch nicht berücksichtigte Relation $UJ^2 = J^2U$ in abelschen Gruppen ohnehin stets erfüllt ist. Folglich ist $|\hat{\Gamma}| = 12$. Da weiter die Multiplikation komponentenweise geschieht und $\mathbb{C}^*$ abelsch ist, ist auch $\hat{\Gamma}$ abelsch. Zuletzt ist die Untergruppe $\langle\phi\rangle \leq \hat{\Gamma}$, wobei $\phi(U) = 1, \phi(J) = i$ eine zyklische Gruppe von Ordnung 4 und daher $\hat{\Gamma} \cong C_3 \times C_4 \cong C_{12}$ wie behauptet. □

3 Eine Klasse von Nicht-Kongruenzuntergruppen

In den vorangehenden Vorträgen haben wir die Gruppen

$$\Gamma[n] = \{g \in \Gamma \mid g \equiv I_2 \pmod{n}\}$$

kennengelernt und unter anderem festgestellt, dass jede normale Untergruppe von Γ, die ein $\Gamma[n]$ enthält, endlichen Index haben muss. Einige Zeit stand die Vermutung im Raum, dass auch die Umkehrung dieser Aussage korrekt ist, dass also jede normale Untergruppe von Γ von endlichem Index schon eine Kongruenzuntergruppe ist. Diese Vermutung wurde 1887 von R. Fricke [Fri87] und G. Pick [Pic87] durch explizite Konstruktion eines Gegenbeispiels widerlegt. Im Folgenden wollen wir eine ganze Klasse von normalen Nicht-Kongruenzuntergruppen der Modulgruppe konstruieren. Wir orientieren uns dabei an einer Veröffentlichung von I. Reiner [Rei58] und nutzen darüber hinaus einige Ergebnisse von H. Frasch [Fra33], welche wir aus Platzgründen ohne Beweis angeben werden.

3.1 Zugrunde liegende Ergebnisse von H. Frasch

Wie bereits erwähnt benötigen wir für die folgende Konstruktion einer Klasse von Nicht-Kongruenzgruppen einige Ergebnisse aus [Fra33], welche wir hier ohne Beweis angeben wollen.

Definition 3.1.1 *Es sei $p > 3$ eine Primzahl, $\alpha \in \mathbb{N}$ eine Primitivwurzel modulo p, das heißt*

$$\langle \alpha + p\mathbb{Z} \rangle = (\mathbb{Z}/p\mathbb{Z})^*$$

und $\beta \in \mathbb{N}$ mit $\alpha\beta \equiv 1 \pmod{p}$. Man beachte, dass $(\mathbb{Z}/p\mathbb{Z})^*$ als Einheitengruppe eines endlichen Körpers zyklisch ist und somit stets eine Primitivwurzel existiert.

1. *Wir definieren:*

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

2. *Es seien* $\lambda, \mu, \nu, , \lambda_*, \mu_*, \nu_* \in \mathbb{N}_0$ *mit*

$$\begin{aligned} \nu\nu_* &\equiv -1 && \pmod{p} \\ \mu_* &\equiv \mu\nu^2 - \nu && \pmod{p} \\ \lambda_* &\equiv \lambda + \mathrm{l}_\alpha(\nu) && \pmod{\frac{1}{2}(p-1)}, \end{aligned}$$

wobei

$$\alpha^{\mathrm{l}_\alpha(\nu)} \equiv \nu \pmod{p}.$$

Wir definieren:

$$\begin{aligned} (\lambda)_p &:= V_p^\lambda T^p V_p^\lambda \\ (\lambda, \mu)_p &:= V_p^\lambda T^\mu JT^p J^{-1} T^{-\mu} V_p^{-\lambda} \\ (\lambda, \mu, \nu)_p &:= V_p^\lambda T^\mu JT^\nu JT^{-\nu_*} J^{-1} T^{-\mu_*} V_p^{-\lambda_*} \end{aligned}$$

Bemerkung 3.1.2 *Ist* $\mu \neq 0$*, so gilt*

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

Satz 3.1.3 (H. Frasch) *Ist* $p > 3$ *eine Primzahl, so ist* $\Gamma[p]$ *eine freie Gruppe auf*

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

Erzeugern. Diese können so gewählt werden, dass einer T^p *ist und die anderen von der Form*

$$(\lambda, \mu, \nu)_p, \ \nu \not\equiv -1, 0, 1 \pmod{p}$$

sind.

Ein umfangreicher Beweis dieser Tatsache findet sich in [Fra33].

Korollar 3.1.4 *Ist* $(\lambda, \mu, \nu)_p \in \Gamma[p]$*, so ist* $(\lambda, \mu, \nu)_p$ *einer der freien Erzeuger oder kann als Produkt der freien Erzeuger exklusive* T^p *geschrieben werden.*

Dies ist eine Konsequenz aus dem Beweis des vorangehenden Satzes und wird hier aufgeführt, da wir das Ergebnis im Anschluss noch benötigen.

3.2 Eine Klasse normaler Untergruppen

Wie angekündigt werden wir nun eine Klasse von normalen Untergruppen von Γ konstruieren, bei denen es sich nicht um Kongruenzuntergruppen handelt. Wir folgen dabei dem Vorgehen von [Rei58].

Definition 3.2.1 *Es seien $p > 3$ eine Primzahl und $s \in \mathbb{N}$. $\Gamma'[p]$ bezeichne wie üblich die Kommutatoruntergruppe von $\Gamma[p]$. Nach dem Satz von H. Frasch aus dem vorangegangenen Abschnitt ist $\Gamma[p]$ eine freie Gruppe auf endlich vielen (im Folgenden k) Erzeugern. Folglich ist*

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

eine freie abelsche Gruppe auf k Erzeugern, das heißt isomorph zu $\mathbb{Z}^k$. Dies liegt daran, dass $\Delta[p]$ eine endlich erzeugte abelsche Gruppe ohne Elemente endlicher Ordnung (abgesehen vom Nullelement) ist; der Hauptsatz über endlich erzeugte Moduln über Hauptidealbereichen liefert die Behauptung. Demnach ist

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

eine endliche Gruppe, wobei

$$\Delta^s[p] := \langle x^s \mid x \in \Delta[p] \rangle$$

Ist $\pi : \Gamma[p] \to \Delta[p]$ die kanonische Restklassenabbildung, so definieren wir nun:

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

Lemma 3.2.2 *Sind p, s wie oben, dann ist $\Omega(p,s)$ normal und von endlichem Index in Γ.*

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

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

also ist $\Omega(p,s)$ insbesondere von $\Gamma'[p]$ und $\{x^s \mid x \in \Gamma[p]\}$ erzeugt. Also ist $\Omega(p,s)$ von endlichem Index in $\Gamma[p]$ (und somit auch in Γ) und als charakteristische Untergruppe (das Erzeugendensystem ist invariant unter allen Automorphismen) von $\Gamma[p]$ auch normal in Γ. $\square$

Satz 3.2.3 *Ist $p > 3$ eine Primzahl und $s > 1$ mit $\mathrm{ggT}(p, s) = 1$, so enthält $\Omega(p, s)$ keine Hauptkongruenzuntergruppe.*

Beweis: Wir nehmen an, dass

$$\Gamma[m] \subset \Omega(p, s)$$

für ein $m \in \mathbb{N}$. Da sicherlich

$$\Gamma[a \cdot m] \subset \Gamma[m],$$

können wir ohne Einschränkung annehmen, dass wir in der Situation

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

für ein $r > 0$ und $\mathrm{ggT}(p, t) = 1$ sind. Wir setzen nun

$$L := \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}, \; R := \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}.$$

Weiter sei $q \in \mathbb{Z}$ (wir werden q gleich etwas genauer bestimmen) und setze

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} := L^q R L R^{st-1}.$$

Man rechnet aus:

$$\frac{b}{p} = p^2(st - 1) + st, \; \frac{d-1}{p^2} = q \cdot \frac{b}{p} + st - 1.$$

Also ist $\mathrm{ggT}(\frac{b}{p}, pst) = 1$. (Ist v eine Primzahl, die pst teilt, so ist $v = p$ und teilt daher $\frac{b}{p}$ nicht, da v p, aber nicht st teilt oder $v \neq p$ und v teilt daher $\frac{b}{p}$ nicht, da v st, aber nicht p teilt.) Folglich können wir q so wählen, dass

$$\frac{d-1}{p^2} \equiv 0 \pmod{p^r st}.$$

(Ist $u \cdot \frac{b}{p} \equiv 1 \pmod{p^r st}$, so wähle $q \equiv u(1 - st) \pmod{p^r st}$.) Dies impliziert sicherlich $d \equiv 1 \pmod{p^r st}$ und daher wegen $ad - bc = 1$ auch $a \equiv 1 + bc \pmod{p^r st}$. Wir setzen die Kongruenzen zusammen und erhalten:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 + bc & b \\ c & 1 \end{pmatrix} =: B \pmod{p^r st}$$

Anders ausgedrückt

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

und somit nach Voraussetzung

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

Nun gilt

$$B = R^{b/p} L^{c/p}$$

und daher

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

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

$$1 + (st - 1) - \frac{b}{p} \equiv 0 \pmod{s}$$

Setzen wir also die oben hergeleitete Formel für $\frac{b}{p}$ ein, so ergibt sich

$$st - (p^2(st - 1) + st) \equiv 0 \pmod{s}.$$

Dies ist aber sicher ein Widerspruch zu $\mathrm{ggT}(p, s) = 1$ und im Gegensatz zur Annahme kann $\Omega(p, s)$ somit keine Kongruenzuntergruppe enthalten.

Wir zeigen nun noch die oben offen gelassene Behauptung. Nach dem vorangegangenen Kapitel hat die Gruppe $\Gamma[p]$ ein freies Erzeugendensystem, etwa M, bestehend aus R und einigen Matrizen der Form $(\lambda, \mu, \nu)_p$ (in der Notation des letzten Abschnitts). 3.1.2 ergibt nun

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

nach 3.1.4 taucht R also nicht auf, wenn wir L als Produkt der freien Erzeuger von $\Gamma[p]$ schreiben. Die Elemente von

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

sind aber unter den Produkten der freien Erzeuger gerade dadurch ausgezeichnet, dass die Exponentensumme an jedem der freien Erzeuger ein Vielfaches von s ist. Dies impliziert aber gerade die noch offene Behauptung. □

Bemerkung 3.2.4 *Die ersten konstruierten Nicht-Kongruenzuntergruppen aus [Pic87] und [Fri87] sind gerade die $\Omega(2, s)$ (auch wenn dies hier nicht gezeigt wurde, stellen diese tatsächlich Nicht-Kongruenzgruppen dar).*

Literaturverzeichnis

[Fra33] H. Frasch: *Die Erzeugenden der Hauptkongruenzgruppen zu Primzahlstufen*, Mathematische Annalen, vol. 108 (1933), 229-252

[Fri87] R. Fricke: *Über die Substitutionsgruppen, welche zu den aus dem Legendre'schen Integralmodul $k^2(\omega)$ gezogenen Wurzeln gehören*, Mathematische Annalen, vol. 28 (1887), 99-118

[JS05] J. C. Jantzen, J. Schwermer: *Algebra*, Springer, 2005

[KK07] M. Koecher, A. Krieg: *Elliptische Funktionen und Modulformen*, Springer, 2007

[Kri10] A. Krieg: *Funktionentheorie II*, Vorlesungsskript, RWTH Aachen, 2012

[Neb10] G. Nebe: *Computeralgebra*, Vorlesungsskript, RWTH Aachen, 2010

[Pic87] G. Pick: *Über gewissen ganzzahlige lineare Substitutionen, welche sich nicht durch algebraische Congruenzen erklären lassen*, Mathematische Annalen, vol 28 (1887), 119-124

[Rei58] I. Reiner: *Normal subgroups of the unimodular group*, Illinois, J. Math. 2 (1958), 142-144