MATH. SCAND. 16 (1965), 148–158

MAXIMAL-FASTPERIODIZITÄT VON GRUPPEN I

W. FLUCH

Einleitung.

Will man die Theorie der fastautomorphe Funktionen auf höhere Modulgruppen übertragen, so ist es interessant zu wissen, ob es überhaupt fastperiodische Funktionen auf diesen Gruppen gibt. Für die gewöhnliche (= elliptische) Modulgruppe ist diese Frage erledigt durch die Existenz von treuen unitären 2-dim. Darstellungen, das heißt sie ist maximal-fastperiodisch (max.-f.p.) (daher auch ihre Untergruppen $\Gamma(n)$; speziell also alle freien Gruppen F_m). Die Maximal-fastperiodizität (Max.-f.p.) der Hilbert'schen und der Siegel'schen Modulgruppe ergibt sich im Folgenden in Satz 1.

Sei nämlich Γ_n der Ring der ganzen Zahlen eines algebraischen Zahlkörpers K_n, so wird bewiesen, daß die Gruppe $\mathfrak{M}_k(\Gamma_n)$, der $k \times k$-Matrizen mit Determinante 1 und Koeffizienten aus Γ_n, max.-f.p. ist. Dabei ist es möglich, ein System von Normalteilern $G_\mathfrak{p}$ mit endlichem Index und Durchschnitt $\bigcap G_\mathfrak{p} = 1$ zu finden. Dann wird die Max.-f.p. einiger Gruppen aufgezeigt, für welche ein Normalteilersystem mit den eben angegebenen Eigenschaften nicht unmittelbar ersichtlich ist. In einigen Fällen können wir auf Grund von Satz 1 auf die Max.-f.p. der Faktorgruppen bei Kongruenzmoduln schließen, und damit auf die der Gruppe selbst. In der Arbeit werden Beispiele von max.-f.p. Gruppen mit unendlich vielen Erzeugenden und Relationen und sogar solche Gruppen mit endlich vielen Erzeugenden und unendlich vielen Relationen gegeben. Sämtliche bisher bekannten minimal-f.p. Gruppen sind einfache Gruppen. Wir zeigen jedoch, daß die Gruppe $\mathfrak{M}_2(R[x])$, welche unendlich viele Normalteiler besitzt, min.-f.p. ist. Weiter geben wir ein Beispiel einer diskreten max.-f.p. Gruppe, welche keine treue endliche unitäre Darstellung besitzt. Lemma 3 und 4 haben als Aussagen über endliche unitäre Matrizen selbständiges Interesse. Besondere Beachtung verdient Satz 7.

1. Unimodulare Gruppen.

Wir wiederholen kurz die Definition von Max.-f.p. Sei G_0 der Normalteiler der Gruppe G, bestehend aus allen Elementen $a \in G$ mit $D(a) = 1$

Eingegangen am 6. März 1964.

für jede endliche unitäre Darstellung D von G. Dann heißt G max.-f.p., falls $G_0 = 1$.

Satz 1. *Die Gruppe* $\mathfrak{M}_k(\Gamma_n)$, *der* $k \times k$-*Matrizen mit Elementen aus dem Ring* Γ_n *und der Determinante* 1, *ist* max.-f.p.

Bemerkung. Da jede Untergruppe einer max.-f.p. Gruppe wieder max.-f.p. ist, so ist die in der Arbeit gegebene Formulierung (der Sätze 1, 2, 3, 4, 9, 10) als Kurzform der folgenden aufzufassen:

»Jede Matrizen-Gruppe, bestehend aus Matrizen mit Determinante 1 und Koeffizienten aus dem Ring ..., ist max.-f.p.«

Ist G_1 der Durchschnitt aller Normalteiler N von G mit endlichem Index, so gilt folgendes Lemma (vgl. Neumann–Wigner [4]):

Lemma 0. *Es gilt stets* $G_0 \subseteqq G_1$.

Beweis des Satzes 1. Es sei $\mathfrak{p} \in K_n$ ein beliebiges Primideal. Wir bilden die Modulgruppe G_A von $\mathfrak{M}_k(\Gamma_n) \equiv G_A \pmod{\mathfrak{p}}$. Da G_A eine (endliche) Gruppe ist, bilden die Matrizen $M \in \mathfrak{M}_k(\Gamma_n)$ mit $M \equiv E \pmod{\mathfrak{p}}$, wobei E die Einheitsmatrix, einen Normalteiler $G_{\mathfrak{p}}$ von endlichem Index A mit $\mathfrak{M}_k(\Gamma_n)/G_{\mathfrak{p}} \cong G_A$. Dabei ist $A = (N\mathfrak{p})^{k^2-1} \cdot (1 - N_{\mathfrak{e}}{}^{-2}) \dots (1 - N_{\mathfrak{e}}{}^{-k})$. (Der genaue Wert ist natürlich hier unwesentlich.) Wir wählen eine beliebige Matrix $M \in G_1$. Für diese muß dann gelten:

$$M \equiv E \pmod{\mathfrak{p}}$$

für jedes Primideal aus K_n. Nach dem Fundamentalsatz der Idealtheorie folgt aber

$$M = E\,.$$

Damit ist $G_1 = 1$, also erst recht $G_0 = 1$.

Spezialfälle: (1) $K_n = R$, Körper der rationalen Zahlen. $\mathfrak{M}_k(\Gamma)$ ist die unimodulare Gruppe mit ganz rat. Koeffizienten; sie enthält für $k = 2m$ als Untergruppe die Siegel'sche Modulgruppe.

(2) K_n = total reeller algebraischer Zahlkörper, und $k = 2$. Die Gruppe $\mathfrak{M}_2(\Gamma_n)$ ist isomorph zur Hilbert'schen Modulgruppe.

Aus einem Satz von Balcerzyk–Mycielski [1] folgt die *Maximalfastperiodizität des freien Produktes*

$$G = \prod_{t \in T}{}^{*} G_t$$

einer beliebigen Menge T (mit Mächtigkeit $\leqq 2^{\aleph_0}$) *von Gruppen* G_t *der Gestalt*:

Zyklische Gruppen Z_n, Diedergruppen D_{2n}, Tetraedergruppe A_4, Oktaedergruppe S_4, Ikosaedergruppe A_5.

Dabei darf $n = \infty$ sein und jede dieser Gruppen mehrmals als Faktor auftreten.

Im Spezialfall $G = Z_2 * Z_3$ bzw. $F_n = Z_\infty * \ldots * Z_\infty$ erhalten wir die in der Einleitung zitierten Gruppen aufs Neue.

Wir beweisen folgendes Lemma, auf welches sich die folgenden Beweise stützen werden.

Lemma 1. *Ist N ein Normalteiler von G mit* max.-f.p. *Faktorgruppe, dann ist $G_0 \subseteq N$. Weiter ist G_0 selbst der Durchschnitt über alle solche Normalteiler.*

Beweis. Da G/N max.-f.p. ist, so gibt es zu je zwei Elementen a_j, a_k aus zwei verschiedenen Restklassen von $G = \bigcup_i Na_i$ eine endliche unitäre Darstellung D, so daß sie getrennt werden, das heißt $D(a_j) \neq D(a_k)$. Alle von 1 nicht trennbaren Elemente liegen daher in einer Restklasse, somit in N, also $G_0 \subseteq N$. Nach Definition von G_0 ist G/G_0 max.-f.p. Faktorgruppe, und G_0 ist daher selbst ein Normalteiler N_1. Somit $\bigcap N \subseteq G_0$; wegen $G_0 \subseteq N$ folgt dann aber $\bigcap N = G_0$.

Bemerkung. Zur Untersuchung einer Gruppe G auf Max.-f.p. stehen uns also jedenfalls Normalteilersysteme a) mit endlichen, b) mit treu unitär darstellbaren, c) mit max.-f.p. Faktorgruppen zur Verfügung.

Sei Γ der Ring der ganz rationalen Zahlen und $\Gamma[x]$ der Polynomring über Γ. Dann gilt folgender Satz:

Satz 2. *Die Gruppe $\mathfrak{M}_k(\Gamma[x])$, der $k \times k$-Matrizen mit Determinante* 1 *und Koeffizienten aus $\Gamma[x]$, ist* max.-f.p.

Wir geben für diesen Satz zwei Beweise.

Erster Beweis. Wir bilden mittels $p(x) \in \Gamma[x]$, welches irreduzibel sei und ersten Koeffizienten $a_0 = 1$ habe, die Modulgruppe $\mathfrak{M}_{p(x)}$:

$$\mathfrak{M}_k(\Gamma[x]) \equiv \mathfrak{M}_{p(x)} \mod p(x) .$$

Für diese (unendliche) Gruppe gilt nun folgendes Lemma:

Lemma 2. *Die Gruppe $\mathfrak{M}_{p(x)}$ ist isomorph einer Untergruppe von $\mathfrak{M}_k(\Gamma_n)$, wobei K_n der durch $p(x) = 0$ definierte algebraische Zahlkörper ist.*

Beweis des Lemmas. Sei α definiert durch $p(\alpha) = 0$, so ist α nach den Voraussetzungen über $p(x)$ eine ganz algebraische Zahl. Jedes Element $m(x)$ von $M(x) \in \mathfrak{M}_k(\Gamma[x])$ ist aber ein ganz rationales Polynom in x, das heißt aus $\Gamma[x]$, somit jedes Element $\tilde{m}$ von $\tilde{M} \in \mathfrak{M}_{p(x)}$ ganz rationales

Polynom in α. Daher ist $\tilde{m}$ ganz algebraisch $\in R(\alpha)=K_n$ und da $\mathfrak{M}_{p(x)}$ eine Gruppe, ist $\mathfrak{M}_{p(x)}$ isomorph einer Untergruppe von $\mathfrak{M}_k(\Gamma_n)$.

Um den Beweis von Satz 2 zu beenden, wählen wir jetzt irgendwelche unendlich viele $p(x)$ mit oben angegebenen Eigenschaften. Zu jedem $p(x)$ gehört dann ein Normalteiler $G_{p(x)}$, so daß

$$\mathfrak{M}_k(\Gamma[x])/G_{p(x)} \cong \mathfrak{M}_{p(x)}$$

wird. Aus Lemma 2 und dem Satz 1 folgt, daß $\mathfrak{M}_{p(x)}$ max.-f.p. ist. Wir wollen jetzt noch zeigen, daß stets $\bigcap G_{p(x)}=1$ für unendlich viele $p(x)$. Sei $M(x) \in \bigcap G_{p(x)}$, das heißt $M(x) \equiv E \bmod p(x)$ für unendlich viele $p(x)$. Jedes Element $a(x)$ der Matrix $M(x)-E$ hat aber eine eindeutige Zerlegung in Primpolynome, insbesondere jedes $a(x) \neq 0$ nur endlich viele Primpolynome als Teiler (endlicher Grad), so daß aus $a(x) \equiv 0 \bmod p(x)$ für unendliche viele $p(x)$ notwendig folgt

$$a(x) = 0, \qquad \text{also} \qquad M(x)-E = 0\,.$$

Nach Lemma 1 ist aber $G_0 \subseteqq G_{p(x)}$, also erst recht $G_0=1$.

Man könnte sich bei diesem Beweis auf die Polynome $p(x)=x-\alpha$, $\alpha \in \Gamma$, beschränken.

Zweiter Beweis. Wir bilden zu jeder Primzahl $p \in \Gamma$ die Modulargruppe $\mathfrak{M}_p(x)$

$$\mathfrak{M}_k(\Gamma[x]) \equiv \mathfrak{M}_p(x) \mod p\,.$$

$\mathfrak{M}_p(x)$ ist wieder eine unendliche Gruppe; wir behaupten jedoch

Lemma 2a. *Die Modulargruppe* $\mathfrak{M}_p(x)$ *ist* max.-f.p.

Beweis des Lemmas. Sei $\pi(x) \in \Gamma[x] \bmod p$ irreduzibel über $\mathrm{GF}[p]$ und vom Grade n. Wir bilden $\mathfrak{M}_p(x) \equiv \mathfrak{M}_p(\alpha) \bmod \pi(x)$. Jede Matrix $M \in \mathfrak{M}_p(\alpha)$, wo $\pi(\alpha)=0$, besteht aus Elementen

$$m = m_0+m_1\alpha+\ldots+m_{n-1}\alpha^{n-1}$$

mit $m_i \in \mathrm{GF}[p]$, das heißt $m \in \mathrm{GF}[p^n]$. Somit ist $\mathfrak{M}_p(\alpha)$ endliche Gruppe. Den zu $\pi(x)$ gehörenden Normalteiler bezeichnen wir mit $G_{\pi(x)}$ und wählen $M(x) \in \bigcap G_{\pi(x)}$, das heißt $M(x) \equiv E \bmod \pi(x)$. Wie beim ersten Beweis folgt $M(x)=E$, also $\mathfrak{M}_p(x)$ max.-f.p.

Nun können wir den zweiten Beweis leicht zu Ende führen. Ist nämlich G_p der Normalteiler zur Primzahl p, so daß

$$\mathfrak{M}_k(\Gamma[x])/G_p \cong \mathfrak{M}_p(x)$$

wird und $M(x) \in \bigcap G_p$, so folgt aus $M(x) \equiv E \bmod p$, daß $M(x)=E$ das heißt $G_0=1$. Wegen der Max.-f.p. der Gruppen $\mathfrak{M}_p(x)$ folgt daraus die Behauptung des Satzes.

BEMERKUNG. Für jedes $k \geqq 2$ hat $\mathfrak{M}_k(\Gamma[x])$ unendlich viele Erzeugende und Relationen. $\mathfrak{M}_2(\Gamma[x])$ enthält die sogenannten Hecke-gruppen

$$\mathfrak{Y}(x) = \left\{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right\}$$

als Untergruppen.

Eine leichte Verallgemeinerung von Satz 2 gibt uns der Satz 3, bei dessen Beweis wir uns nun kürzer fassen können.

SATZ 3. *Die Gruppe* $\mathfrak{M}_k(\Gamma_n[x])$, *der* $k \times k$-*Matrizen mit Determinante* 1 *und Koeffizienten aus* $\Gamma_n[x]$, *ist* max.-f.p.

BEWEIS (analog wie bei Satz 2). Man wähle unendlich viele irreduzible $p(x) \in \Gamma_n[x]$ mit $a_0 = 1$. Dann ist α, mit $p(\alpha) = 0$, ganz algebraische Zahl und daher die Modulargruppe $\mathfrak{M}_{p(x)}$, welche durch

$$\mathfrak{M}_k(\Gamma_n[x]) \equiv \mathfrak{M}_{p(x)} \mod p(x)$$

definiert ist, isomorph einer Untergruppe von $\mathfrak{M}_k(\hat{\Gamma})$; dabei ist $\hat{\Gamma}$ der Ring der ganzen Zahlen des Körpers $\hat{K} = K_n(\alpha)$. Speziell wird für die Polynome $p(x) = x - \alpha$, $\alpha \in \Gamma_n$, die Modulargruppe $\mathfrak{M}_{p(x)}$ isomorph einer Untergruppe von $\mathfrak{M}_k(\Gamma_n)$. Da im Polynomring $\Gamma_n[x]$ eindeutige Zerlegung in Primpolynome herrscht, läßt sich der Beweis leicht beenden.

Wir benützen nun Satz 3, um mittels Induktion dieselbe Aussage für die Gruppe $\mathfrak{M}_k(\Gamma_n[x_1 \ldots x_m])$ zu beweisen.

SATZ 4. *Die Gruppe* $\mathfrak{M}_k(\Gamma_n[x_1 \ldots x_m])$, *der* $k \times k$-*Matrizen mit Determinante* 1 *und Koeffizienten aus dem Polynomring* $\Gamma_n[x_1 \ldots x_m]$ *ist* max.-f.p.

BEWEIS. Mittels vollständiger Induktion nach m. Für $m = 1$ ist Satz 4 mit Satz 3 identisch, also bewiesen. Nun sei er bereits für $m - 1$ richtig! Wir wählen unendlich viele (irreduzible) Polynome

$$p(x_1, \ldots, x_m) = x_m - p_1(x_1, \ldots, x_{m-1}),$$

mit $p_1(x_1 \ldots x_{m-1}) \in \Gamma_n[x_1 \ldots x_{m-1}]$. Als Modulargruppe erhalten wir

$$\mathfrak{M}_k(\Gamma_n[x_1 \ldots x_m]) \equiv \mathfrak{M}_{p(x_1 \ldots x_m)} \quad \mod \quad p(x_1, \ldots, x_m).$$

$\mathfrak{M}_{p(x_1 \ldots x_m)}$ ist also wegen unserer Wahl von $p(x_1, \ldots, x_m)$ isomorph einer Untergruppe von $\mathfrak{M}_k(\Gamma_n[x_1, \ldots, x_{m-1}])$ das heißt aber max.-f.p. nach Induktionsvoraussetzung. Für die zugehörigen Normalteiler $G_{p(x_1, \ldots, x_m)}$ gilt aber

$$\bigcap G_{p(x_1,\ldots,x_m)} = 1 \,,$$

da aus $M(x_1 \ldots x_m) \equiv E \bmod p(x_1,\ldots,x_m)$ für unendlich viele $p(x_1,\ldots,x_m)$, folgt

$$M(x_1,\ldots,x_m) = E$$

(ZPE-Satz im Polynomring $\Gamma_n[x_1 \ldots x_m]$). Nach Lemma 1 folgt $G_0 = 1$.

2. Beispiel einer nichteinfachen minimal-f.p. Gruppe.

Wir wollen selbstredend von den direkten Produkten einfacher Gruppen absehen und geben ein Beispiel einer min.-f.p. Gruppe mit unendlich vielen Normalteilern.

R sei der Körper der rationalen Zahlen und $R[x]$ der Polynomring über R. Dann gilt folgender Satz.

Satz 5. *Die Gruppe* $\mathfrak{M}_2(R[x])$, *der* 2×2-*Matrizen mit Determinante* 1 *und Elementen aus* $R[x]$, *ist* min.-f.p. *Die Gruppe hat unendlich viele Normalteiler.*

Beweis. Die Gruppe wird erzeugt von den Elementen

$$\left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & b(x) \\ 0 & 1 \end{pmatrix} \right\}$$

wobei die $b(x) \in R[x]$ ein Erzeugendensystem der additiven Gruppe der Polynome aus $R[x]$ bilden sollen. Die Elemente

$$V_n = \begin{pmatrix} n & 0 \\ 0 & n^{-1} \end{pmatrix}, \qquad n = \text{natürliche Zahl}\,,$$

liegen in $\mathfrak{M}_2(R[x])$. Bezeichnen wir mit S_b das Element

$$S_b = \begin{pmatrix} 1 & b(x) \\ 0 & 1 \end{pmatrix}, \qquad \text{so gilt} \qquad V_n S_b V_n^{-1} = S_b^{n^2} .$$

Daraus folgt nun (siehe Neumann-Wigner [4, Lemma 1]), daß für jede endliche unitäre Darstellung $D(S_b) = E$, also $S_b \in G_0$. Mit

$$T_b = \begin{pmatrix} 1 & 0 \\ b(x) & 1 \end{pmatrix} \qquad \text{gilt} \qquad V_n^{-1} T_b V_n = T_b^{n^2} ,$$

und daher $D(T_b) = E$. Insbesondere ist

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in G_0 .$$

Also sind sämtliche Erzeugende von $\mathfrak{M}_2(R[x])$ in G_0; das bedeutet aber gerade $G_0 = \mathfrak{M}_2(R[x])$. Mit den unendliche vielen irreduziblen Polynomen $p(x) \in \Gamma[x]$ können wir unendlich viele (nicht isomorphe) Modulargruppen bilden:

$$\mathfrak{M}_2(R[x]) \equiv \mathfrak{M}_{p(x)} \mod p(x) .$$

Wir erhalten also unendlich viele verschiedene Normalteiler. Alle Faktorgruppen sind natürlich min.-f.p.

Der Satz läßt sich auf Körper erweitern, die den rationalen Zahlkörper enthalten, und von der Dimension 2 auf beliebige Dimension $n \geqq 2$.

Um den nächsten Satz beweisen zu können, benötigen wir ein Lemma, aus welchem sich sofort das oben zitierte Neumann–Wigner'sche Lemma ergibt.

LEMMA 3. *Jede endliche unitäre Matrix U, welche mit einer Potenz $\geqq 2$ von sich selbst konjugiert ist, hat endliche Ordnung, mit anderen Worten, gibt es eine invertierbare Matrix V, so daß $VUV^{-1} = U^t$, mit $|t| \geqq 2$, t ganzrational, dann folgt $U^m = 1$ für eine natürliche Zahl m.*

BEMERKUNG. Allgemein lautet dieses Lemma offenbar so: Gibt es zu einer endlichen Matrix U eine invertierbare Matrix V, so daß $VUV^{-1} = U^t$, mit $|t| \geqq 2$, dann sind die Eigenwerte von U lauter Einheitswurzeln. Beweis wie unten.

BEWEIS VON LEMMA 3. Wir setzen $V_k = V^k$, $k = 1, 2, 3, \ldots.$ Aus $VUV^{-1} = U^t$ folgt sofort $V_k U V_k^{-1} = U^{t^k}$ für jedes natürliche k. Die Dimension der Matrizen sei n und $\alpha_1, \ldots, \alpha_n$ seien die Eigenwerte der Matrix U. Nun hat $V_k U V_k^{-1}$ dieselben Eigenwerte wie U, während U^{t^k} die Eigenwerte $\alpha_1^{t^k}, \ldots, \alpha_n^{t^k}$ hat; diese müssen also eine Permutation der α_i sein. Da wir aber für k unendlich viele Möglichkeiten haben, so gibt es für jedes $i = 1, 2, \ldots, n$ zwei verschiedene k mit $\alpha_i^{t^{k_i'}} = \alpha_i^{t^{k_i''}}$, das heißt $\alpha_i^{t^{k_i'-k_i''}} = 1$. Jedes α_i ist also Einheitswurzel, somit $U^m = 1$ für geeignetes m.

Der Fall $t = 0$ ist trivial. Im Falle $|t| = 1$ ist das Lemma offensichtlich falsch; für $t = 1$ wähle man Diagonalmatrizen, für $t = -1$

$$V = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

mit λ transzendent und $|\lambda| = 1$.

KOROLLAR. *Jede Gruppe, welche ein Element von unendlich hoher Ordnung hat, das mit einer Potenz $\geqq 2$ von sich in ein und derselben Klasse konjugierter Elemente liegt, besitzt keine treue endliche unitäre Darstellung.*

Das Korollar gilt insbesondere für die Gruppen $G=\{a,b\}$ mit der einzigen Relation $bab^{-1}=a^n$, $n \geqq 2$. Also gilt (für die letzte Behauptung siehe Satz 1).

SATZ 6. *Es gibt Gruppen mit zwei Erzeugenden und einer einzigen Relation, welche keine treue endliche unitäre Darstellung besitzen. Im Gegensatz dazu ist die freie Gruppe mit zwei Erzeugenden treu unitär darstellbar durch* 2×2*-Matrizen.*

LEMMA 4. *Seien* U, U_2 *zwei unitäre* $n \times n$*-Matrizen, welche mit* $K = U_1 U_2 U_1^{-1} U_2^{-m}$, $m \geqq 1$, *vertauschbar sind. Dann hat* K *endliche Ordnung, und für* $m \geqq 2$ *auch* U_2.

BEWEIS. Wir bezeichnen den n-dimensionalen Vektorraum, in dem die Matrizen wirken, mit $\mathfrak{W}$; mit α einen Eigenwert von K und mit $\mathfrak{W}_\alpha$ den Teilraum von $\mathfrak{W}$, definiert durch

$$\mathfrak{W}_\alpha = \{x \mid Kx = \alpha x\}.$$

Wegen $KU_1 = U_1 K$, $KU_2 = U_2 K$ gilt

$$U_1(\mathfrak{W}_\alpha) \subseteqq \mathfrak{W}_\alpha \qquad \text{und} \qquad U_2(\mathfrak{W}_\alpha) \subseteqq \mathfrak{W}_\alpha .$$

In $\mathfrak{W}_\alpha$ ist aber $K = \alpha \cdot 1$, das heißt $U_1 U_2 U_1^{-1} = \alpha U_2^m$.

Zuerst sei $m=1$. Dann haben U_2 und αU_2 als Transformationen von $\mathfrak{W}_\alpha$ dieselben Eigenwerte: $\lambda, \alpha\lambda, \alpha^2\lambda, \ldots, \lambda \neq 0$. Wegen $\dim(\mathfrak{W}_\alpha) \leqq n$ muß $\lambda\alpha^{k'} = \lambda\alpha^{k''}$ sein, für zwei verschiedene k. Somit $\alpha^{k'-k''}=1$; jeder Eigenwert von K ist Einheitswurzel und $K^s = 1$, mit geeignetem s.

Im Falle $m \geqq 2$ folgt, daß U_2 und αU_2^m dieselben Eigenwerte haben. Somit sind $\lambda, \alpha\lambda^m, \alpha^2\lambda^{m^2}, \alpha^3\lambda^{m^3}, \ldots, \lambda \neq 0$, die Eigenwerte von U_2. Wir setzen

$$U_2 = \sigma W, \qquad \sigma = \alpha^{-1/(m-1)} .$$

Dann ist W unitär, weil $|\alpha| = 1$, und $U_1 W U_1^{-1} = W^m$. Nach Lemma 3 ist jeder Eigenwert von W Einheitswurzel, also $\lambda = \sigma\mu$, wobei μ eine Einheitswurzel ist. Wegen $\dim(\mathfrak{W}_\alpha) \leqq n$ gibt es zwei ganze Zahlen $k_1 < k_2$ für welche $\alpha^{k_1}\lambda^{m^{k_1}} = \alpha^{k_2}\lambda^{m^{k_2}}$. Also ist

$$\alpha^{(m^{k_1}-m^{k_2})/(m-1)-(k_1-k_2)} = \mu^{m^{k_1}-m^{k_2}} .$$

Da

$$\frac{m^{k_1}-m^{k_2}}{m-1} = m^{k_1-1} + \ldots + m^{k_2} > k_1 - k_2, \qquad m \geqq 2 ,$$

ist α Einheitswurzel.

Im Falle $m=0$ ist das Lemma offenbar falsch (vgl. Lemma 3), und für $K=1$ ist es in Lemma 3 enthalten.

Mit Lemma 4 ist bewiesen, daß die Gruppen $G=\{a,b\}$ mit den Relationen

$$ac = ca, \qquad bc = cb, \qquad c = aba^{-1}b^{-n},$$

$n \geqq 1$, nicht treu unitär darstellbar sind durch endliche Matrizen.

Wir beweisen nun den folgenden, weitergehenden Satz.

Satz 7. *Es gibt Gruppen mit endlich vielen Erzeugenden und Relationen, welche* min.-f.p. *sind, das heißt deren sämtliche beschränkte, endliche Darstellungen trivial sind.*

Beweis. Wir zeigen, daß die (unendliche) Gruppe $G=\{a,b,c,d\}$ mit den Relationen

$$a^{-1}ba = b^2, \qquad b^{-1}cb = c^2, \qquad c^{-1}dc = d^2, \qquad d^{-1}ad = a^2$$

min.-f.p. ist. Nach Lemma 3 hat nämlich bei jeder endlichen unitären Darstellung von G das Element $\bar{a}=D(a)$ endliche Ordnung α; analog haben die Elemente $\bar{b}$, $\bar{c}$, $\bar{d}$ endliche Ordnungen β, γ, δ. Daraus folgt nun (siehe [2]), daß $\alpha=\beta=\gamma=\delta=1$. Damit ist die dargestellte Gruppe stets 1, also G min.-f.p.

Es ist interessant zu bemerken, daß die ähnlich definierte (unendliche) Gruppe $G=\{a,b,c\}$ mit

$$a^{-1}ba = b^{-1}, \qquad b^{-1}cb = c^{-1}, \qquad c^{-1}ac = a^{-1}$$

treu unitär darstellbar ist. (In diesem Falle $t=-1$ ist Lemma 3 ja auch falsch). Zum Beweis der Behauptung wähle man drei Darstellungen

$$D_1(a) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad D_1(b) = \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}, \qquad D_1(c) = E$$

mit $|\beta|=1$ transzendent; analog sind D_2, D_3 mit $D_2(b)=D_3(a)=E$ und $|\alpha|=|\gamma|=1$ ebenfalls transzendent. Die unitäre Darstellung

$$D(x) = D_1(x) \oplus D_2(x) \oplus D_3(x)$$

ist treu, wie man an der Normalform der Elemente $x \in G$ sieht.

Eine teilweise Verschärfung von Satz 7, welche jedoch nicht in den Rahmen dieser Arbeit gehört, erhalten wir so (weiter-gehende Resultate in meiner Arbeit: »Über die Nichtlinearität einer gewissen Gruppe«, welche demnächst erscheint, und [4]):

Satz 8. *Es gibt Gruppen mit endlich vielen Erzeugenden, welche keine (nichttriviale) endliche Darstellung besitzen.*

Beim Beweis stützen wir uns auf folgendes

Lemma 5. *Es gibt eine einfache, unendliche, periodische Gruppe F vom Exponent* 73 *mit endlich vielen Erzeugenden.*

Beweis. Siehe [3, Seite 71ff].

Andererseits folgern wir aus den Burnside-Kriterium über periodische Matrizengruppen, daß bei jeder endlichen Darstellung von F die (treu) dargestellte Gruppe endlich ist. Wegen der Einfachheit von F also stets gleich 1. Es ist jedoch nicht bekannt, ob die Gruppe F auch endlich viele Relationen besitzt.

Wir gehen nun über zur Untersuchung der Gruppe $\mathfrak{M}_2(\Gamma_{(p)})$. Mit $\Gamma_{(p)}$ bezeichnen wir den Ring der p-rationalen Zahlen, das heißt die Menge der rationalen Zahlen

$$a = \sum_{\nu=-n}^{n} a_\nu p^\nu, \qquad 0 \leqq a_\nu \leqq p-1 \;,$$

wobei p eine Primzahl sein soll. Dann ist $\mathfrak{M}_2(\Gamma_{(p)})$ die Gruppe der 2×2-Matrizen mit Determinante 1 und Elementen aus $\Gamma_{(p)}$.

Satz 9. *Die Gruppe* $\mathfrak{M}_2(\Gamma_{(p)})$ *ist* max.-f.p. *Die Gruppe besitzt jedoch keine treue, endliche, unitäre Darstellung.*

Beweis. Der zweite Teil der Aussage folgt sofort aus dem Korollar. Die beiden Matrizen

$$V = \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

liegen nämlich in $\mathfrak{M}_2(\Gamma_{(p)})$, S hat unendliche Ordnung, und es gilt

$$VSV^{-1} = S^{p^2}, \qquad \text{also} \quad t = p^2 > 2 \;.$$

Wir bilden nun mit den Zahlen $N_m = p^{2m} - 1$, $m = 1, 2, 3, \ldots$, die Modulargruppen

$$\mathfrak{M}_2(\Gamma_p) \equiv G_m \mod N_m \,.$$

Diese sind endliche Gruppen, da wegen $p^{-1} \equiv p^{2m-1} \bmod N_m$ jede Zahl $a \in \Gamma_p$ einer ganz rationalen Zahl $(\bmod N_m)$ kongruent ist. Für eine Matrix M aus dem Durchschnitt der zugehörigen Normalteiler aber muß $M \equiv E \bmod N_m$, $m = 1, 2, 3, \ldots$, gelten. Wegen $N_m \to \infty$ für $m \to \infty$ ist also $M = E$.

Zum Schluß deuten wir noch den Beweis eines Satzes an, der eine Art Verallgemeinerung des vorherigen darstellt.

Satz 10. *Die Gruppe* $\mathfrak{M}_k(\Gamma_n[x, x^{-1}])$, *der* $k \times k$-*Matrizen mit Determinante* 1 *und Elementen aus dem Polynomring* $\Gamma_n[x, x^{-1}]$ *ist* max.-f.p.

Beweis. Man wähle unendlich viele verschiedene irreduzible Polynome $p(x) \in \Gamma[x]$, so daß α mit $p(\alpha)=0$ eine »Einheit« ist, und also α und α^{-1} ganz-algebraische Zahlen sind. Die mittels $p(x)$ gewonnene Modulargruppe,

$$\mathfrak{M}_k(\Gamma[x,x^{-1}]) \equiv \mathfrak{M}_{p(x)} \quad \bmod p(x)\,,$$

ist daher isomorph einer Untergruppe von $\mathfrak{M}_k(\hat{\Gamma}_n)$, wobei $\hat{\Gamma}$ der Ring der ganzen Zahlen des Körpers $\hat{K}_n = K_n(\alpha)$ ist. Der Durchschnitt der zugehörigen Normalteiler ist notwendig 1, da wir unendlich viele verschiedene $p(x)$ zur Verfügung haben.

Folgerung. Es gibt Gruppen mit endlich vielen Erzeugenden und unendlich vielen Relationen, welche max.-f.p. sind.

Zum Beweis dieser Behauptung bemerken wir, daß die Gruppe

$$N = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

Untergruppe von $\mathfrak{M}_2(\Gamma[x,x^{-1}])$ ist. Sie besitzt aber, wie in [5] bewiesen, unendlich viele definierende Relationen.

LITERATUR

1. S. Balcerzyk and J. Mycielski, *On faithful representations of free products of groups*, Fund. Math. 50 (1961/62), 63–71.
2. G. Higman, *A finitely generated infinite simple group*, J. London Math. Soc. 26 (1951), 61–64.
3. B. H. Neumann, *Lectures on topics in the theory of infinite groups*, Bombay, 1960.
4. J. v. Neumann and E. P. Wigner, *Minimally almost periodic groups*, Ann. of Math. 41 (1940), 746–750.
5. V. L. Nisnewitsch, *Über Gruppen, die durch Matrizen über einem kommutativen Feld isomorph darstellbar sind*, Rec. Math. [Mat. Sbornik] N. S. 8 (50) (1940), 395–403. (Russisch, Resumé in Deutsch.)

UNIVERSITÄT GÖTTINGEN, DEUTSCHLAND