Math. Zeitschr. 106, 293–311 (1968)

Freie Präsentierungen endlicher Gruppen und zugehörige Darstellungen

MANUEL OJANGUREN

1. Einleitung

Eine Präsentierung $G=F/R$ der Gruppe G als Quotient einer freien Gruppe F gibt in bekannter Weise Anlaß zu einer Darstellung von G durch Automorphismen der Abelsch gemachten Relationengruppe $R_0=R/[R,R]$: man ordnet dem Element $\xi=xR$ von G, $x\in F$, die Abbildung zu, welche das Element $r[R,R]$ von R_0, $r\in R$, in $xrx^{-1}[R,R]$ überführt. Die freie Abelsche Gruppe R_0, die additiv geschrieben sei, wird dadurch zu einem G-Modul; anders ausgedrückt: es liegt eine ganzzahlige Darstellung von G vor, deren Grad gleich dem Rang N von R ist. Die vorliegende Arbeit handelt von einigen Eigenschaften dieser Darstellung von G. Im folgenden soll F stets frei und nicht-Abelsch sein, also $n\geqq 2$ freie Erzeugende besitzen.

Zunächst erinnern wir an die Arbeit von Auslander und Lyndon [1], in welcher folgende bemerkenswerte Aussagen über den genannten G-Modul R_0 gemacht werden:

(A) *G operiert treu in R_0, d.h. aus $\xi r_0=r_0$ für alle $r_0\in R_0$ folgt $\xi=1$.*

(B) *Der bezüglich G invariante Teilmodul R_0^G von R_0 ist genau dann von 0 verschieden, wenn G endlich ist.*

In der vorliegenden Arbeit werden, für den Fall einer endlichen Gruppe G der Ordnung g, diese Resultate von Auslander und Lyndon neu bewiesen und verschärft (§ 3 und 4). Wir zeigen insbesondere:

(A′) *$R_0\otimes C\cong C\oplus CG\oplus\cdots\oplus CG$ wobei C der triviale G-Modul der komplexen Zahlen ist, CG die komplexe Gruppenalgebra von G, in üblicher Weise als G-Modul aufgefaßt, und wobei die Anzahl der Summanden rechts gleich n ist (also $\geqq 2$).*

(B′) *R_0^G ist eine freie Abelsche Gruppe vom gleichen Rang wie F.*

Aus (A′) folgt, daß die Gruppe G in $R_0\otimes C$, also auch in R_0, treu operiert. Aus (B′), daß $R_0^G\neq 0$ ist.

Unsere Methoden benutzen die Interpretation von G als Deckbewegungsgruppe einer regulären Überlagerung P^* eines 1-dimensionalen Komplexes P mit der Fundamentalgruppe F; einige „geometrische“ Vorbereitungen finden sich in § 2. Wir verwenden im besonderen einfache Beziehungen betreffend die Bettischen Zahlen von P und P^* (aus denen sich übrigens die Schreiersche Formel für den Rang N von R, $N=1+g(n-1)$ besonders elegant ergibt – unsere Betrachtungen sind in einem gewissen Sinne Verallgemeinerungen dieser Formel).

In § 3 liefert eine Anwendung von (A′) den folgenden Satz:

(C) *Falls die endliche Gruppe G durch n ihrer Elemente erzeugt werden kann, so ist die dritte ganzzahlige Homologiegruppe $H_3(G)$ von G durch $2n-1+g(n-1)^2$ Elemente (oder weniger) erzeugbar.*

In § 5 wird untersucht, ob sich der G-Modul R_0 selbst in ähnlicher Weise zerlegen läßt wie $R_0 \otimes C$; wir zeigen, daß die zu (A′) analoge Isomorphie

$$R_0 \cong Z \oplus ZG \oplus \cdots \oplus ZG$$

genau dann besteht, wenn G eine zyklische Gruppe ist.

In § 6 wird eine Basis der Abelschen Gruppe R_0^G konstruiert und, mit Hilfe dieser Basis, folgendes bewiesen:

(D) *Falls F/R endlich ist, ist das Zentrum von $F/[R,R]$ eine freie Abelsche Gruppe vom gleichen Rang wie F, die mit dem Bild der Verlagerung von F in R_0 übereinstimmt.*

(E) *Ist F eine freie Gruppe mit $n \geqq 2$ Erzeugenden und R ein beliebiger Normalteiler von F, so gibt es keine Untergruppe X von F derart, daß*

$$[F,X]=[R,R]$$

ist, ausgenommen in den Fällen $R=F$ oder $R=1$.

Die meisten Resultate dieser Arbeit sind ohne Beweise in einer Comptes Rendus-Note[1] angekündigt worden.

2. Überlagerung

In diesem und in den folgenden Abschnitten habe F einen endlichen Rang $n \geqq 1$ und G die Ordnung g.

Man kann F als Fundamentalgruppe eines 1-dimensionalen Polyeders P auffassen: dem Normalteiler R von F entspricht eine reguläre Überlagerung P^* über P, deren Deckbewegungsgruppe isomorph zu G ist. Die Fundamentalgruppe von P^* ist isomorph zu R. Hat P α_0 Ecken und α_1 Kanten, so ist [11, S. 170]

$$n=1+\alpha_1-\alpha_0;$$

P^* hat $g\alpha_0$ Ecken und $g\alpha_1$ Kanten, und deswegen ist der Rang N seiner Fundamentalgruppe durch die Schreiersche Formel [2]

$$N=1+g\alpha_1-g\alpha_0=1+g(n-1)$$

gegeben.

Die erste Homologiegruppe $H_1(P^*, A)$ mit Koeffizienten in einem trivialen G-Modul A ist isomorph zur abelschen Gruppe $A \otimes R_0$. Die Decktransformationen induzieren in $H_1(P^*, A)$ Automorphismen, welche H_1 zu einem G-Modul machen. Wir wollen sehen, wie das geschieht. Es sei b der Basispunkt von P und b^* ein über b liegender Punkt der als Basispunkt von P^* gewählt wird. Es sei r ein beliebiges Element aus der Fundamentalgruppe $\Pi(P^*, b^*)=R$ von P^*, u^* ein zur Homotopieklasse r gehöriger Weg von P^* und u seine

[1] Ojanguren, M.: C. R. Acad. Sci. Paris **264**, 60–61 (1967).

Projektion in P. Ferner sei x ein Element aus der Fundamentalgruppe $\Pi(P,b)=F$, $\bar{x}$ seine Projektion in $F/R=G$, w ein zur Homotopieklasse x gehöriger Weg von P und w^* die in b^* beginnende Überlagerung von w. Die zu $\bar{x}$ gehörige Decktransformation $D_{\bar{x}}$ bildet u^* in einen geschlossenen Weg $D_{\bar{x}}(u^*)$ ab, der im Endpunkt $D_{\bar{x}}(b^*)$ von w^* beginnt. Die (ganzzahlige) Homologieklasse von $D_{\bar{x}}(u^*)$ ist offenbar dieselbe wie diejenige von $w^* D_{\bar{x}}(u^*)(w^*)^{-1}$. Dieser Weg ist eine Überlagerung von wuw^{-1} und liegt deswegen in der Homotopieklasse xrx^{-1} von $\Pi(P^*,b^*)$. Die Homologieklasse von xrx^{-1} ist aber die Klasse von xrx^{-1} modulo $[R,R]$, also sind $H_1(P^*,Z)$ und R_0 auch als G-Moduln isomorph, falls die G-Modul-Struktur von R_0 wie im §1 erklärt wird. Daraus folgt, daß auch $H_1(P^*,A)$ und $A\otimes R_0$ zueinander isomorphe G-Moduln sind, falls

$$\xi(a\otimes r_0)=a\otimes\xi r_0 \tag{1}$$

für alle $\xi\in G$, und $r_0\in R$ gesetzt wird.

Wir wollen jetzt ein spezielles Paar (P,P^*) konstruieren. Das Polyeder P bestehe einfach aus einer Ecke E und aus n orientierten Schleifen

$$\varepsilon_1,\ldots,\varepsilon_n$$

mit Anfangs- und Endpunkten in E, welche die Erzeugenden

$$e_1,\ldots,e_n$$

der Fundamentalgruppe F repräsentieren. Im folgenden bezeichnen wir mit ε_i sowohl den orientierten Weg als auch die ihm entsprechende 1-dimensionale orientierte Zelle. Der in entgegengesetzter Richtung durchlaufene Weg wird mit ε_i^{-1} bezeichnet. Die Überlagerung P^* von P hat g 0-dimensionale Zellen und ng 1-dimensionale Zellen. Wir identifizieren die Ecken von P^* mit den Elementen $\xi_1,\ldots,\xi_g\in G$ und die 1-Zellen von P^* mit den Produkten

$$\xi_1\varepsilon_1,\xi_1\varepsilon_2,\ldots,\xi_g\varepsilon_n$$

so, daß der 1-Zelle, welche in der ξ_i entsprechenden Ecke beginnt und ε_j überlagert, das Produkt $\xi_i\varepsilon_j$ zugeordnet ist und daß diese Zelle in der $\xi_i\bar{e}_j$ entsprechenden Ecke endet. (Hier und in der Folge bezeichnen wir die kanonischen Projektionen von F und F_0 in G mit einem Querstrich.) Die $\xi\in G$ entsprechende Decktransformation von P^* bildet die Ecke ξ_i in die Ecke $\xi\xi_i$ und die 1-Zelle $\xi_i\varepsilon_j$ auf die 1-Zelle $\xi\xi_i\varepsilon_j$ ab. Der G-Modul L^0 der 0-Ketten von P^* ist also zum ganzzahligen Gruppenring ZG isomorph und soll mit ihm identifiziert werden, während der G-Modul L der 1-Ketten frei erzeugt wird durch $\varepsilon_1,\ldots,\varepsilon_n$. Die Randbildung

$$\partial\colon\ L\to L^0 \tag{2}$$

ist offenbar durch

$$\partial\xi\varepsilon_i=\xi(\bar{e}_i-1)\in ZG \tag{3}$$

gegeben. Jedem Element $x=e_{i_1}^{\pm1}\ldots e_{i_m}^{\pm1}\in F$ ordnen wir einen geschlossenen Weg $w(x)=\varepsilon_{i_1}^{\pm1}\ldots\varepsilon_{i_m}^{\pm1}$ zu, und diesem Weg einen ihn überlagernden Weg $w^*(x)$ in P^* mit Anfangspunkt in der Ecke $\xi_1=1$. $w^*(x)$ entspricht in natürlicher Weise eine 1-dimensionale Kette $dx\in L$. Man sieht sofort, daß die folgenden Beziehungen gelten:

$$de_i = \varepsilon_i, \tag{4}$$

$$d(xy) = dx + \bar{x}\,dy. \tag{5}$$

Die so erhaltene Abbildung

$$d\colon F \to L$$

definiert einen Homomorphismus von R in L, denn es ist

$$d(r_1 r_2) = dr_1 + dr_2 \qquad r_1, r_2 \in R \tag{6}$$

wie man aus (5) sieht. Weiter gilt

$$d[r_1, r_2] = 0 \qquad r_1, r_2 \in R. \tag{7}$$

Also induziert d einen ebenfalls mit d bezeichneten Homomorphismus von R_0 in L. d ist sogar ein G-Homomorphismus, denn

$$d(x r x^{-1}) = dx + \bar{x}\,dr + \bar{x}\bar{r}\,d(x^{-1}) = dx + \bar{x}\,dr - \bar{x}\bar{r}\bar{x}^{-1}\,dx = \bar{x}\,dr \tag{8}$$

also

$$d(\bar{x} r_0) = \bar{x}\,dr_0 \qquad \text{für alle } r_0 \in R_0,\ \bar{x} \in G. \tag{9}$$

Weil die geschlossenen Wege in P^* genau diejenigen sind, deren Projektionen zu einer Homotopieklasse $r \in R$ gehören, fällt der Teilmodul der Zyklen von L mit $d(R_0)$ zusammen. Andererseits ist das Bild $\partial(L)$ von L wegen (3) einfach das Augmentierungsideal IG von ZG.

Aus dieser ganzen Betrachtung erhalten wir:

Lemma 2.1. *Zu einer gegebenen freien Präsentierung F/R von G gibt es ein 1-dimensionales Polyeder P und eine reguläre Überlagerung P^* von P so, daß die Deckbewegungsgruppe von P^* über P isomorph zu G ist und daß die G-Modul-Isomorphie*

$$H_1(P^*, Z) \cong R_0 \tag{10}$$

gilt.

Lemma 2.2. *Zu einer gegebenen freien Präsentierung F/R von G gibt es einen freien G-Modul L und zwei G-Homomorphismen d und ∂ so, daß die Sequenz*

$$0 \to R_0 \xrightarrow{d} L \xrightarrow{\partial} IG \to 0 \tag{11}$$

exakt ist.

3. Die Darstellung von G in $SL(N, Z)$

Weil R eine freie Gruppe vom Range $N = 1 + g(n-1)$ ist, so ist R_0 eine freie abelsche Gruppe, ebenfalls vom Range N, und besitzt also eine Basis

$$r_1, \ldots, r_N.$$

Das Operieren eines Elementes $\xi \in G$ auf R_0 kann durch

$$\xi r_i = \sum_j A_{ij}(\xi)\, r_j, \tag{12}$$

d.h. durch eine ganzzahlige Matrix $A(\xi) = (A_{ij}(\xi))$, beschrieben werden. Wegen

$$(\xi\eta)\, r = \sum_j \xi A_{ij}(\eta)\, r_j = \sum_{j,k} A_{ij}(\eta)\, A_{jk}(\xi)\, r_k \tag{13}$$

liefert die Zuordnung

$$\mathfrak{R}:\ \xi \to A(\xi^{-1}) \tag{14}$$

eine Darstellung von G in $SL(N, Z) \subset SL(N, C)$.

Lemma 3.1. *Die Spur* $\operatorname{Sp} A(\xi)$ *von* $A(\xi)$ *ist gleich* 1, *wenn* $\xi \neq 1$ *und gleich* N, *wenn* $\xi = 1$.

Beweis. Der Fall $\xi = 1$ ist trivial. Es sei also $\xi \neq 1$. Die zu ξ gehörige Decktransformation induziert in $H_0(P^*, Z) \cong Z$ die Identität und in $H_1(P^*, Z)$ einen Automorphismus, der auf Grund von (10) und (12) gerade durch $A(\xi)$ beschrieben wird. Weil diese Decktransformation keine Fixpunkte hat, folgt aus der Hopfschen Spurformel:

$$\operatorname{Sp} A(\xi) - 1 = 0, \quad \text{d.h.} \quad \operatorname{Sp} A(\xi) = 1.$$

Satz 3.1. *Die Darstellung* $\mathfrak{R}$ *ist als komplexe Darstellung aufgefaßt (d.h. als Darstellung von* G *in* $SL(N, C)$*), äquivalent zur Summe einer identischen* 1-*dimensionalen Darstellung und* $n-1$ *regulären Darstellungen von* G.

Beweis. χ sei der Charakter einer irreduziblen m-dimensionalen Darstellung von G. Aus Lemma 3.1 folgt

$$\frac{1}{g} \sum_{\xi \in G} \operatorname{Sp} A(\xi)\, \chi(\xi) = \frac{1}{g}\Big[N\chi(1) - \chi(1) + \sum_{\xi \in G} \chi(\xi)\Big].$$

Ist nun χ nicht trivial, so ist $\sum_{\xi \in G} \chi(\xi) = 0$ und $\chi(1) = m$, also

$$\frac{1}{g} \sum_{\xi \in G} \operatorname{Sp} A(\xi)\, \chi(\xi) = \frac{1}{g}\, m(N-1) = m(n-1).$$

Falls χ trivial ist, d.h. $\chi(\xi) = 1$ für alle $\xi \in G$, erhalten wir

$$\frac{1}{g} \sum_{\xi \in G} \operatorname{Sp} A(\xi)\, \chi(\xi) = \frac{1}{g} \sum_{\xi \in G} \operatorname{Sp} A(\xi) = \frac{1}{g}(g - 1 + N) = n.$$

Jede m-dimensionale irreduzible Darstellung kommt aber in der regulären Darstellung genau m-mal vor, d.h. $\mathfrak{R}$ besteht aus $n-1$ regulären Darstellungen und aus einer trivialen 1-dimensionalen Darstellung.

Korollar 3.1. *Es gilt*

$$R_0 \otimes C \cong C \oplus CG \oplus \cdots \oplus CG. \tag{15}$$

Korollar 3.2. *Ist der Rang* n *von* $F \geqq 2$, *so ist* $\mathfrak{R}$ *treu, d.h.* G *operiert treu in* R_0 *(vgl.* § 1, (A')*).*

Als Anwendung vom Satz 3.1 beweisen wir den folgenden Satz über die dritte Homologiegruppe einer endlichen Gruppe.

Satz 3.2. *Wenn die endliche Gruppe* G *durch* n *ihrer Elemente erzeugt werden kann, so kann* $H_3(G, Z)$ *durch weniger als*

$$2n + g(n-1)^2$$

Elemente erzeugt werden.

Beweis. Auf Grund von Lemma 2.2 und mit derselben Bezeichnung gibt es eine lange exakte Sequenz in der modifizierten Cohomologie $\hat{H}$ von G [10, 12]

$$\to \hat{H}^n(G, L) \to \hat{H}^n(G, IG) \to \hat{H}^{n+1}(G, R_0) \to \hat{H}^{n+1}(G, L) \to$$

aus welcher wir die Isomorphie

$$\hat{H}^n(G, IG) \cong \hat{H}^{n+1}(G, R_0) \tag{16}$$

ablesen können; denn L ist frei und somit $\hat{H}^n(G, L) = \hat{H}^{n+1}(G, L) = 0$.

Analog folgt aus der exakten Sequenz

$$0 \to IG \to ZG \to Z \to 0$$

$$\hat{H}^{n+1}(G, IG) \cong \hat{H}^{n-1}(G, Z). \tag{17}$$

(16) und (17) zusammen ergeben die Formel (vgl. [8], S. 273)

$$\hat{H}^{n+1}(G, R_0) \cong \hat{H}^{n-1}(G, Z). \tag{18}$$

Für die gewöhnliche Homologie von G entnimmt man daraus die Beziehung

$$H_3(G, Z) \cong H_1(G, R_0).$$

Um die Anzahl der Erzeugenden von $H_1(G, R_0)$ abzuschätzen, konstruieren wir eine freie Auflösung von Z:

$$\cdots \to L \xrightarrow{\partial_1} ZG \xrightarrow{\partial_0} Z \to 0. \tag{19}$$

L ist jetzt der freie rechts G-Modul über $\varepsilon_1, \ldots, \varepsilon_n$. Der Homomorphismus ∂_1 ist, wie vorher ∂, durch

$$\partial_1 \varepsilon_i = \bar{e}_i - 1$$

definiert und ∂_0 ist die evidente Projektion von ZG auf $Z \cong ZG/IG$. Alle anderen Bezeichnungen sind die gleichen wie in § 2.

Aus (19) folgt, durch Tensorieren mit R_0

$$\cdots \to L \otimes_G R_0 \to ZG \otimes_G R_0 \to Z \otimes_G R_0 \to 0. \tag{20}$$

Man kann jedes Element von $L \otimes R_0$ als Summe

$$\sum_{i,j} c_{ij} \varepsilon_i \otimes r_j, \qquad c_{ij} \in Z \tag{21}$$

darstellen, denn

$$\varepsilon_i \xi \otimes r_j = \varepsilon_i \otimes \xi r_j = \sum_{i,j} \varepsilon_i \otimes A_{jk}(\xi)\, r_k, \qquad (\xi \in G).$$

Die Summe (21) ist ein 1-dimensionaler Zyklus, also ein Element aus

$$\operatorname{Ker}(L \otimes R_0 \to ZG \otimes R_0)$$

wenn

$$\sum_{i,j} c_{ij}(\bar{e}_i - 1) \otimes r_j = 0,$$

d.h. wenn

$$\sum_{i,j,k} c_{ij}\big(A_{jk}(\bar{e}_i) - \delta_{jk}\big)\, r_k = 0 \tag{22}$$

ist. ($\delta_{jk}=0$ oder 1 je nachdem $j \neq k$ oder $j=k$.) Weil die r_k eine Basis der abelschen Gruppe R_0 bilden, folgt aus (22)

$$\sum_{i,j} c_{ij}\big(A_{jk}(\bar{e}_i)-\delta_{jk}\big)=0 \qquad \text{für alle } k=1,\dots,N. \tag{23}$$

Die ganzen Zahlen c_{ij} müssen somit ein Gleichungssystem mit nN Unbekannten und N Gleichungen befriedigen. Durch geeignete Anordnung der c_{ij} kann man die Matrix dieses Systems wie folgt schreiben:

$$\mathfrak{P}=\big(A^*(\bar{e}_1)-E,\dots,A^*(\bar{e}_n)-E\big);$$

dabei ist A^* die Transponierte von A und E die Einheitsmatrix.

Hilfssatz. *Der Rang von $\mathfrak{P}$ ist $(n-1)(g-1)$.*

Aus diesem Hilfssatz folgt sofort, daß der Lösungsraum des Systems (23) die Dimension

$$nN-(n-1)(g-1)=2n-1+g(n-1)^2$$

hat, d.h., daß es höchstens $2n-1+g(n-1)^2$ unabhängige 1-dimensionale Zyklen gibt. $H_1(G,R_0)$ kann also durch $2n-1+g(n-1)^2$ Elemente erzeugt werden, und damit ist 3.2 bewiesen.

Beweis des Hilfssatzes. Nach den Resultaten von § 2 ist auch die durch

$$\xi \to A^*(\xi) \tag{24}$$

definierte Darstellung von G äquivalent zur Summe einer 1-dimensionalen trivialen Darstellung und $n-1$ regulären Darstellungen von G. Die Matrizen $A^*(\xi)$ sind also äquivalent zu den Matrizen

$$\mathfrak{Q}(\xi)=\begin{pmatrix} 1 & & & \\ & B(\xi) & & \\ & & \ddots & \\ & & & B(\xi)\end{pmatrix},$$

wobei $B(\xi)$ die Matrix der regulären Darstellung ist. Infolgedessen ist $\mathfrak{P}$ äquivalent zu einer Matrix

$$\big(\mathfrak{Q}(\bar{e}_1)-E,\dots,\mathfrak{Q}(\bar{e}_n)-E\big).$$

Der Rang dieser Matrix ist, offensichtlich, $n-1$ mal größer als der Rang von

$$B_0=\big(B(\bar{e}_1)-E,\dots,B(\bar{e}_n)-E\big).$$

Um den Rang von B_0 zu bestimmen, betrachten wir einen Vektor

$$x=(x,\dots,x_g)$$

und das Gleichungssystem

$$xB_0=0. \tag{25}$$

Dieses System hat g Unbekannte und ng Gleichungen, die wie folgt geschrieben werden können:

$$\begin{aligned} &x_1 = x_{\sigma_1(1)}, \ldots, x_g = x_{\sigma_1(g)} \\ &x_1 = x_{\sigma_2(1)}, \ldots, x_g = x_{\sigma_2(g)} \\ &\cdots\cdots\cdots\cdots \\ &x_1 = x_{\sigma_n(1)}, \ldots, x_g = x_{\sigma_n(g)}. \end{aligned} \tag{26}$$

Die σ_i sind dabei diejenigen Permutationen der Indizes $1, \ldots, g$ welche in G der Multiplikation mit $\bar{e}_i$ entsprechen. Weil die Elemente $\bar{e}_1, \ldots, \bar{e}_n$ die ganze Gruppe G erzeugen, wird von den σ_i eine transitive Permutationsgruppe erzeugt, und aus (26) folgt

$$x_1 = x_2 = \cdots = x_g.$$

Der Lösungsraum des Systems (25) ist deshalb 1-dimensional und B_0 hat den Rang $g-1$, also $\mathfrak{P}$ den Rang $(n-1)(g-1)$.

Bemerkung. Im Falle einer zyklischen Gruppe gibt Satz 6.5 für die Anzahl der Erzeugenden von $H_3(G)$ die richtige Schranke $(=1)$ an.

4. Der invariante Teil von R_0

U sei eine beliebige Untergruppe von G. Wir bezeichnen mit R_0^U die Gesamtheit der Elemente aus R_0, die invariant sind bezüglich U, d.h. die Elemente $r_0 \in R_0$, für welche

$$\xi r_0 = r_0 \qquad \text{für alle } \xi \in U.$$

Satz 4.1. *Hat U den Index j in G, so ist R_0^U eine freie abelsche Gruppe vom Range*

$$1 + j(n-1).$$

Als abelsche Gruppe ist R_0^U ein direkter Faktor von R_0.

Beweis. Die erste rationale Homologiegruppe von P^* ist

$$H_1(P^*, Q) \cong Q \otimes R_0. \tag{27}$$

Jedem von 1 verschiedenen Element $\xi \in U$ entspricht eine fixpunktfreie Abbildung von P^* in sich, welche in $Q \otimes R_0$ den Automorphismus

$$1 \otimes \xi\colon\ q \otimes r_0 \to q \otimes \xi r_0 \qquad q \in Q,\ r_0 \in R_0 \tag{28}$$

induziert. Nach Eckmann [3] ist der Rang des invarianten Teils $H_1(P^*, Q)^U$ von $H_1(P^*, Q)$ (also der Rang von $(Q \otimes R_0)^U$) durch die Formel

$$\frac{1}{u} \sum_{\xi \in U} \operatorname{Sp} A(\xi) \tag{29}$$

gegeben; u ist dabei die Ordnung von U. Aus Lemma 3.1 folgt sofort

$$\operatorname{Rang}(Q \otimes R_0)^U = 1 + j(n-1), \tag{30}$$

wobei $j=g/u$ der Index von U in G ist. Wegen (28) gilt aber

$$(Q\otimes R_0)^U=Q\otimes R_0^U$$

und daher

$$\operatorname{Rang} R_0^U=\operatorname{Rang} Q\otimes R_0^U=1+j(n-1).$$

Aus dem Fundamentalsatz über die freien abelschen Gruppen folgt, daß es eine Basis

$$r_1, \ldots, r_N$$

von R_0 und natürliche Zahlen $\lambda_1, \ldots, \lambda_m$ gibt, derart daß

$$\lambda_1 r_1, \ldots, \lambda_m r_m$$

eine Basis von R_0^U ist. Mit $\lambda_i r_i$ ist aber auch r_i invariant, also sind alle $\lambda_i=1$ und R_0^U ist ein direkter Faktor von R_0.

Korollar 4.1. *R_0^G, der unter G invariante Teil von R_0, hat den Rang $n\geqq 1$ und ist also $\neq 0$ (vgl. §1, (B')).*

Korollar 4.2. *R_0^U ist genau dann ein Teilmodul von R_0, wenn U ein Normalteiler von G ist.*

Beweis. a) U sei ein Normalteiler von G, r_0 ein Element aus R_0^U und ξ ein Element aus G. Für alle $\eta\in U$ gilt

$$\eta(\xi r_0)=\xi(\xi^{-1}\eta\xi)r_0=\xi r_0 \tag{31}$$

also $\xi r_0\in R_0^U$; da dies für beliebige $r_0\in R_0$ und $\xi\in G$ gilt, ist R_0^U ein Teilmodul von R_0.

b) Ist R_0^U ein Teilmodul von R_0, so ist $\xi r_0\in R_0^U$ für alle $r_0\in R_0^U$ und alle $\xi\in G$, also $\eta\xi r_0=\xi r_0$, d.h.

$$\xi^{-1}\eta\xi r_0=r_0 \qquad \text{für alle } \xi\in G, \eta\in U, r_0\in R_0^U. \tag{32}$$

Sei nun V der von U erzeugte Normalteiler von G. Aus (32) folgt, daß alle bezüglich U invarianten Elemente von R_0 auch bezüglich V invariant sind, was $R_0^V=R_0^U$ und insbesondere

$$\operatorname{Rang} R_0^U=\operatorname{Rang} R_0^V \tag{33}$$

nach sich zieht. Aus (33) und aus Satz 4.1 folgt, daß V und U den gleichen Index haben, also gleich sind.

5. Über die Zerlegbarkeit von R_0

Man kann sich fragen, ob die Zerlegung der Darstellung $\mathfrak{R}$ auch mit Hilfe ganzzahliger unimodularer Transformationen realisierbar ist, d.h. ob es möglich ist, R_0 als Summe

$$R_0\cong Z\oplus ZG\oplus\cdots\oplus ZG \tag{34}$$

darzustellen, wobei Z der triviale G-Modul der ganzen Zahlen und ZG der ganzzahlige Gruppenring ist. Die Antwort ist im allgemeinen negativ:

Satz 5.1. *Ist R_0 als Summe*

$$R_0 \cong Z \oplus ZG \oplus \cdots \oplus ZG$$

darstellbar, so ist G eine zyklische Gruppe.

Es scheint sogar plausibel zu sein, daß eine Zerlegung von R_0 in einer Summe

$$R_0 = S_0 \oplus T_0$$

mit einem freien G-Modul T_0 nur dann möglich ist, wenn G mit weniger als n Elementen erzeugbar ist. Man kann jedenfalls den folgenden Satz beweisen:

Satz 5.2. *Falls G nilpotent ist und R_0 in eine Summe*

$$R_0 = S_0 \oplus T_0 \tag{35}$$

zerfällt, wobei T_0 ein freier G-Modul vom Range k ist, so kann die Gruppe G durch $n-k$ ihrer Elemente erzeugt werden.

Wir beweisen zunächst den folgenden Satz:

Satz 5.3. *Zerfällt R_0 in eine Summe*

$$R_0 = S_0 \oplus T_0,$$

wobei T_0 ein freier G-Modul vom Range k ist, so kann die Gruppe $G/[G, G]$ durch $n-k$ ihrer Elemente erzeugt werden.

Beweis. Wir betrachten die exakte Sequenz (11) und fassen R_0 als Teilmodul von L auf. L wird von den Elementen

$$\varepsilon_1, \ldots, \varepsilon_n$$

erzeugt und L^G, der invariante Teil von L, wird durch

$$\sum_{\xi \in G} \xi \varepsilon_1, \ldots, \sum_{\xi \in G} \xi \varepsilon_n \tag{36}$$

erzeugt. In der Folge schreiben wir Γ für die Summe $\sum_{\xi \in G} \xi$. L^G ist in R_0 enthalten, weil die Elemente $\Gamma \varepsilon_i$, die bei der Abbildung $\partial: L \to IG$ in $\Gamma(\bar{e}_i - 1) = \Gamma - \Gamma = 0$ übergehen, im Kern von ∂, also in R_0 liegen. Es ist also

$$R_0^G = L^G. \tag{37}$$

Der freie G-Modul T_0 sei von den k Elementen

$$t_1, \ldots, t_k$$

frei erzeugt; T_0^G wird also, analog wie L^G, durch

$$\Gamma t_1, \ldots, \Gamma t_k \tag{38}$$

erzeugt. Aus (35) folgt

$$R_0^G = S_0^G \oplus T_0^G \tag{39}$$

und aus (37)

$$L^G = S_0^G \oplus T_0^G. \tag{40}$$

L^G ist eine freie abelsche Gruppe mit den freien Erzeugenden (36); S_0^G und T_0^G sind ebenfalls freie abelsche Gruppen. Weil T_0^G den Rang k hat, gibt es eine Basis

$$s_1, \dots, s_{n-k}$$

von S_0^G und eine unimodulare Transformation

$$\begin{aligned} \Gamma t_i &= \sum_j a_{ij} \Gamma \varepsilon_j \qquad i=1,\dots,k \\ s_i &= \sum_j b_{ij} \Gamma \varepsilon_j \qquad i=1,\dots,n-k, \end{aligned} \tag{41}$$

welche die Basis (36) von L^G in die Basis

$$\Gamma t_1, \dots, \Gamma t_k, s_1, \dots, s_{n-k} \tag{42}$$

überführt. Da T_0 ein Teilmodul von L ist, kann man schreiben

$$t_i = \sum_j c_{ij} \varepsilon_j$$

mit $c_{ij} \in ZG$, oder auch

$$t_i = \sum_j c'_{ij} \varepsilon_j + \sum_j \gamma_{ij} \varepsilon_j \tag{43}$$

mit $c'_{ij} \in Z$ und $\gamma_{ij} \in IG$. Durch Multiplikation mit Γ und Vergleich mit (41) erhält man aus (43)

$$c'_{ij} = a_{ij}. \tag{44}$$

Betrachten wir jetzt die Basistransformation

$$\begin{aligned} \tau_i &= \sum_j a_{ij} \varepsilon_j \qquad i=1,\dots,k \\ \sigma_i &= \sum_j b_{ij} \varepsilon_j \qquad i=1,\dots,n-k \end{aligned} \tag{45}$$

in L, und die Sequenz

$$S_0 \oplus T_0 \xrightarrow{d} L \xrightarrow{\partial} IG \xrightarrow{p} IG/(IG)^2, \tag{46}$$

wobei p die natürliche Projektion von IG auf $IG/(IG)^2$ ist. Aus (43) und (44) ergibt sich

$$\tau_i = t_i - \sum_j \gamma_{ij} \varepsilon_j$$

und aus Lemma 2.2 folgt $\partial t_i = 0$, d.h., es ist

$$\partial \tau_i = -\sum_j \gamma_{ij} (\bar{e}_j - 1) \in (IG)^2$$

und somit

$$p \partial \tau_i = 0.$$

$IG/(IG)^2$ wird also durch die $n-k$ Bilder der σ_i erzeugt, und aus der bekannten Isomorphie [13]

$$IG/(IG)^2 \cong G/[G, G]$$

folgt, daß die abelsch gemachte Gruppe G durch $n-k$ Elemente erzeugt wird.

Satz 5.2 ist eine unmittelbare Folgerung aus Satz 5.3 und aus

Satz 5.4. *Ist G eine endliche nilpotente Gruppe und kann man $G/[G, G]$ mit k Elementen erzeugen, so kann man auch G mit k Elementen erzeugen.*

Beweis. Es sei m die kleinstmögliche Anzahl Erzeugender von G. Es genügt zu zeigen, daß $G/[G, G]$ mindestens m Erzeugende hat. Nach [6, Theorem 3.5] kann man die m Erzeugenden $a_1, \ldots, a_m$ von G so wählen, daß ihre Bilder in $G/[G, G]$ eine kanonische Basis der Abelsch gemachten Gruppe bilden. Falls diese weniger als m Erzeugende hat, liegt eines der a_i, z.B. a_1, in $[G, G]$ und nach [6, Lemma 5.9], da G nilpotent ist, wird G schon durch $a_2, \ldots, a_m$ erzeugt, was der Voraussetzung über m widerspricht.

Beweis des Satzes 5.1. Mit Hilfe einfacher homologischer Methoden kann man den Satz 5.1 folgendermaßen verschärfen:

Satz 5.5. *Ist R_0 in eine Summe*

$$R_0 = Z \oplus T_0$$

zerlegbar, wobei der G-Modul T_0 die Bedingung

$$\hat{H}^2(G, T_0) = 0 \tag{47}$$

erfüllt, so ist G zyklisch.

($\hat{H}$ ist wieder, wie in § 3, der modifizierte Cohomologiefunktor.)

Zum Beweis benötigen wir folgendes Lemma:

Lemma 5.1. *Ist G eine endliche Gruppe, für die*

$$\hat{H}^0(G, Z) = \hat{H}^2(G, Z) \tag{48}$$

gilt, so ist G zyklisch.

Korollar. *Hat G die Periode 2, so ist G zyklisch.*

Beweis des Lemmas. Es gilt [12, S. 36]

$$\hat{H}^0(G, Z) \cong Z_g \quad \text{und} \quad \hat{H}^2(G, Z) \cong G/[G, G].$$

Daraus folgt

$$Z_g \cong G/[G, G],$$

also, da g die Ordnung von G ist,

$$[G, G] = 1 \quad \text{und} \quad G \cong Z_g.$$

Beweis des Satzes 5.5. Ist

$$R_0 = Z \oplus T_0 \quad \text{und} \quad \hat{H}^2(G, T_0) = 0,$$

so folgt aus (18) für $n = 1$,

$$\hat{H}^2(G, Z \oplus T_0) = \hat{H}^2(G, Z) \cong \hat{H}^0(G, Z)$$

und nach Lemma 5.1 muß G zyklisch sein.

Wir beweisen jetzt die Umkehrung des Satzes 5.1.

Satz 5.6. *Ist G zyklisch, so ist*

$$R_0 \cong Z \oplus ZG \oplus \cdots \oplus ZG.$$

Beweis. Wir wählen in F eine neue Basis $a_1, \ldots, a_n$ derart, daß

$$a_1^g, a_2, \ldots, a_n \in R.$$

Das ist sicher möglich, weil es eine solche Basis in $F/[F, F]$ gibt (Fundamentalsatz der Abelschen Gruppen) und weil jede Basistransformation von $F/[F, F]$ durch (mindestens) eine Basistransformation von F induziert wird. Mit Hilfe dieser neuen Basis konstruieren wir, nach der Methode von Schreier, eine Basis von R (vgl. [4], Ch. 7, S. 91). Als Repräsentanten der Elemente von G nehmen wir das „Schreier-System"

$$1, a_1, a_1^2, \ldots, a_1^{g-1}.$$

Ist für alle $x \in F$ $\Phi(x)$ der Vertreter von $\bar{x}$, so bilden die von 1 verschiedenen Elemente der Form

$$a_1^h a_j \Phi(a_1^h a_j)^{-1} \qquad h = 0, 1, \ldots, g-1; j = 1, \ldots, n$$

eine Basis von R. Wir haben also die Basis

$$\begin{array}{l} a_1^g \\ a_2, a_1 a_2 a_1^{-1}, \ldots, a_1^{g-1} a_2 a_1^{1-g} \\ \cdots\cdots\cdots\cdots\cdots \\ a_n, a_1 a_n a_1^{-1}, \ldots, a_1^{g-1} a_n a_1^{1-g}. \end{array}$$

Die Konjugation mit a_1 führt a_1^g in sich selbst über und bewirkt eine zyklische Vertauschung der Elemente der anderen Zeilen; also erzeugt das Bild von a_1 in R_0 einen direkten Summanden $\cong Z$ und das Bild von a_i, $i \geqq 2$, einen direkten Summanden $\cong ZG$. Damit ist der Satz bewiesen.

6. Weitere Eigenschaften der Präsentierung F/R

Aus dem Satz 4.1 und aus dem Fundamentalsatz über freie abelsche Gruppen folgt, daß es eine Basis

$$t_1, \ldots, t_n, r_{n+1}, \ldots, r_N \tag{49}$$

der abelschen Gruppe R_0 gibt, so daß

$$t_1, \ldots, t_n \tag{50}$$

eine Basis von R_0^G ist. Im Hinblick auf einige Anwendungen soll jetzt hier eine solche Basis explizit konstruiert werden.

Die freie Gruppe F sei durch

$$e_1, \ldots, e_n$$

erzeugt. Nach dem Beweis des Schreierschen Satzes über freie Gruppen (vgl. z. B. [4], S. 94) kann man ein System

$$x_1, \dots, x_g \tag{51}$$

von Repräsentanten der Klassen xR konstruieren, derart, daß R genau durch die von 1 verschiedenen Elemente

$$t_{ij} = x_i e_j \Phi(x_i e_j)^{-1} \qquad i=1,\dots,g, j=1,\dots,n \tag{52}$$

frei erzeugt wird. $\Phi(x)$ ist hier der Repräsentant der Klasse xR. Setzen wir jetzt

$$t_j^* = t_{1j} t_{2j} \dots t_{gj} \qquad j=1,\dots,n. \tag{53}$$

Offensichtlich ist

$$t_j^* \equiv e_j^g \qquad \text{modulo } [F,F] \tag{54}$$

also

$$t_j^* \neq 1 \qquad \text{für alle } j.$$

Bei festem j sind also nicht alle $t_{ij}=1$, und man kann in der aus den t_{ij} gebildeten Basis n Elemente $t_{i_1 1}, \dots, t_{i_n n}$ durch $t_1^*, \dots, t_n^*$ ersetzen. Damit erhalten wir eine neue Basis von R:

$$t_1^*, \dots, t_n^*, r_{n+1}^*, \dots, r_N^*. \tag{55}$$

Für alle t_j^* und alle $x \in F$ gilt

$$x t_j^* x^{-1} \equiv t_j^* \qquad \text{modulo } [R,R]; \tag{56}$$

in der Tat:

$$\begin{aligned} x t_j^* x^{-1} &= x \prod_{i=1}^{g} x_i e_j \Phi(x_i e_j)^{-1} x^{-1} = \prod_{i=1}^{g} x x_i e_j \Phi(x_i e_j)^{-1} x^{-1} \\ &= \prod_{i=1}^{g} x x_i \Phi(x x_i)^{-1} \Phi(x x_i) e_j \Phi(\Phi(x x_i) e_j)^{-1} \Phi(x x_i e_j) \Phi(x_i e_j)^{-1} x^{-1} \\ &\equiv ABC \qquad \text{modulo } [R,R], \end{aligned}$$

wobei

$$A = \prod_{i=1}^{g} x x_i \Phi(x x_i)^{-1}$$

$$B = \prod_{i=1}^{g} \Phi(x x_i) e_j \Phi(\Phi(x x_i) e_j)^{-1}$$

$$C = \prod_{i=1}^{g} \Phi(x x_i e_j) \Phi(x_i e_j)^{-1} x^{-1}.$$

Mit x_i durchläuft auch $\Phi(x x_i)$ das ganze System (51) und daher ist

$$B \equiv t_j^* \quad \text{und} \quad A \equiv C^{-1} \qquad \text{modulo } [R,R],$$

also

$$x t_j^* x^{-1} \equiv ABC \equiv t_j^* \qquad \text{modulo } [R,R].$$

Die kanonischen Bilder t_j der t_j^* in $R/[R,R]$ erzeugen einen direkten Faktor von R_0, welcher den Rang n hat und, wegen (56), invariant ist bezüglich G, also mit R_0^G übereinstimmt. Damit ist gezeigt, daß die kanonischen Bilder der (55) eine Basis der gewünschten Art (49) bilden.

Aus der Konstruktion der t_j und aus der Definition der Verlagerung folgt sofort der

Satz 6.1. *R_0^G ist das Bild der Verlagerung von F in R_0.*

Eine unmittelbare Folgerung dieses Satzes ist

Satz 6.2. *Das Zentrum von $F/[R,R]$ ist das Bild der Verlagerung von $F/[R,R]$ in $R/[R,R]$.*

Beweis (vgl. [1, Th. 1, Cor.]). Es sei z im Zentrum von $F/[R,R]$. Für alle $x \in F/[R,R]$ gilt

$$z x z^{-1} x^{-1} = 1 \tag{57}$$

und insbesondere

$$z r_0 z^{-1} r_0^{-1} = 1 \qquad \text{für alle } r_0 \in R_0,$$

was gleichbedeutend ist mit

$$\bar{z} r_0 = r_0 \qquad \text{für alle } r_0 \in R_0.$$

Nach Korollar 3.2 muß, in diesem Fall, $\bar{z} = 1$ sein, d.h. $z \in R/[R,R]$. Das Zentrum von $F/[R,R]$ liegt also in R_0. Aus (57) folgt sofort, daß R_0^G mit ihm übereinstimmt und daraus mit Satz 6.1 die Behauptung.

Aus Satz A von §1 und aus Korollar 4.1 erhält man noch:

Satz 6.3. *Das Zentrum von $F/[R,R]$ ist trivial, wenn F/R unendlich ist. Es ist eine freie abelsche Gruppe vom gleichen Rang wie F, wenn F/R endlich ist.*

Wir wollen jetzt einen Satz über Kommutatorgruppen freier Gruppen beweisen.

Satz 6.4. *Ist F eine freie Gruppe mit $n \geqq 2$ Erzeugenden und R ein beliebiger Normalteiler von F (eventuell also von unendlichem Index), so gibt es keine Untergruppe X von F derart, daß*

$$[F, X] = [R, R],$$

außer wenn $R = F$ oder $R = 1$ ist.

Beweis. Wenn $[F,X] = [R,R]$ ist, so muß $X/[F,X] = X/[R,R]$ im Zentrum von $F/[R,R]$ liegen. Ist F/R unendlich, so ist das Zentrum von $F/[R,R]$ die triviale Gruppe (Satz 6.3) und somit

$$X/[F,X] = 1$$

oder

$$X = [F, X]. \tag{58}$$

Wiederholte Anwendung von (58) hat die Gleichungen

$$X = [F, X] = [F, [F, X]] = \cdots = [F, \cdots [F, X] \ldots]$$

zur Folge. Diese zeigen, daß X in allen Kommutatorgruppen

$$[F,[F,\dots[F,F]\dots]]$$

enthalten ist. Der Durchschnitt dieser Kommutatorgruppen ist aber $=1$ (Magnus [5]), also sind auch X und $R=1$. Wir nehmen jetzt an, $F/R=G$ habe die endliche Ordnung g. (Die Bezeichnungen sind die gleichen wie in den vorhergehenden Abschnitten.) Nach einem bekannten Satz (vgl. z.B. [6], S. 140, Theorem 3.5) ist es möglich, eine Basis

$$e_1,\dots,e_n$$

von F so zu wählen, daß R von gewissen Elementen

$$e_1^{d_1}c_1,\dots,e_n^{d_n}c_n,c_{n+1},\dots$$

erzeugt wird, wobei die d_i natürliche Zahlen sind und die c_i in der Kommutatorgruppe von F liegen. Die d_i können sogar so gewählt werden, daß d_i immer ein Teiler von d_{i+1} ist. Es sei nun T das Urbild von R_0^G in F, d.h. T ist die von den t_j^* und $[R,R]$ erzeugte Untergruppe von F. Wie vorher ist $X/[R,R]$ im Zentrum von $F/[R,R]$ enthalten, also ist

$$X\subset T$$

und somit

$$[F,X]\subset[F,T]\subset[R,R];$$

folglich gilt

$$[F,T]=[R,R]. \tag{59}$$

Es sei jetzt x ein beliebiges Element aus F und t ein beliebiges Element aus T. Man kann schreiben

$$x\equiv e_1^{p_1}\dots e_n^{p_n} \qquad \text{modulo } [F,F] \tag{60}$$

und wegen (54),

$$t\equiv e_1^{g_1}\dots e_n^{g_n} \qquad \text{modulo } [F,F], \tag{61}$$

wobei alle g_i durch g teilbar sind. Aus (60) und (61) folgt leicht, daß

$$[x,t]\equiv\prod_{i<j}[e_i,e_j]^{gk_{ij}} \qquad \text{modulo } [F,[F,F]], \tag{62}$$

für gewisse ganze Zahlen k_{ij}; damit ist jedes Element aus $[X,T]$ zu einem solchen Produkt kongruent modulo $[F,[F,F]]$. Es ist jetzt leicht zu zeigen, daß (59) nicht möglich ist, falls $n\geqq 3$ ($n=$Anzahl der Erzeugenden von F) vorausgesetzt wird. Wir betrachten in R die drei Elemente

$$e_1^{d_1}c_1,\quad e_2^{d_2}c_2,\quad e_3^{d_3}c_3.$$

Es gilt

$$\begin{aligned}
[e_1^{d_1}c_1,\ e_2^{d_2}c_2]&\equiv[e_1,\ e_2]^{d_1d_2} && \text{modulo } [F,[F,F]]\\
[e_1^{d_1}c_1,\ e_3^{d_3}c_3]&\equiv[e_1,\ e_3]^{d_1d_3} && \text{modulo } [F,[F,F]]\\
[e_2^{d_2}c_2,e_3^{d_3}c_3]&\equiv[e_2,e_3]^{d_2d_3} && \text{modulo } [F,[F,F]].
\end{aligned} \tag{63}$$

Wenn wirklich $[F,T]=[R,R]$ wäre, so könnte man die linke Seite dieser Kongruenzen durch ein Produkt der Form (62) darstellen. Die Klassen modulo $[F,[F,F]]$ aller Kommutatoren $[e_i,e_j]$ mit $i<j$ bilden, nach einem Satz von Witt [7], eine Basis der freien abelschen Gruppe $[F,F]/[F,[F,F]]$. Folglich sind die rechten Seiten von (63) nur dann als Produkte der $[e_i,e_j]^{g k_{ij}}$ darstellbar, wenn die Exponenten $d_i d_j$ $(i,j=1,2,3)$ durch g teilbar sind. Es müßte somit g^3 die Zahl $(d_1 d_2 d_3)^2$ teilen. Das Produkt $d_1 d_2 \dots d_n$ gibt aber gerade die Ordnung von $G/[G,G]$ an; diese ist ein Teiler von g. Es müßte also g^3 ein Teiler von g^2 sein, was für $g \neq 1$, d.h. $F \neq R$ unmöglich ist.

Betrachten wir jetzt den Fall $n=2$. Die gleiche Überlegung wie im Falle $n \geqq 3$ zeigt, daß G eine abelsche Gruppe der Ordnung g ist; d.h., G besitzt eine Präsentierung

$$\{e_1, e_2; e_1^{d_1}, e_2^{d_2}, [e_1, e_2]\}$$

die für $g>1$ folgende Bedingungen erfüllt:

$$d_1 \mid d_2, \qquad d_1 d_2 = g, \qquad 1 \leqq d_1 < g. \tag{64}$$

Wir setzen $[F,F]=F_2$ und $F_{m+1}=[F,F_m]$ für $m \geqq 2$. F_2/F_3 ist frei erzeugt durch $[e_1,e_2]\,F_3$ und F_3/F_4 durch

$$[[e_1,e_2],e_1]\,F_4 \quad \text{und} \quad [[e_1,e_2]\,e_2]\,F_4 \qquad ([4], \text{S.}\,167).$$

Der Kürze halber bezeichnen wir $[e_1,e_2]$ einfach mit e_{12}. Für jedes Element x aus F gilt bekanntlich ([7] oder [4, S. 167])

$$x \equiv e_1^{p_1} e_2^{p_2} e_{12}^{p_{12}} \qquad \text{modulo } F_3 \tag{65}$$

mit eindeutig bestimmten p_1, p_2, p_{12}. Aus der Definition der t_{ij} und der t_j^* sieht man leicht, daß nicht nur (54) gilt, sondern sogar

$$t_j^* \equiv e_j^g \qquad \text{modulo } [R,R]. \tag{66}$$

Die Untergruppe T ist deshalb durch die e_j^g und $[R,R]$ erzeugt. Jedes Element r aus R erfüllt eine Kongruenz der Form

$$r \equiv e_1^{d_1 k_1} e_2^{d_2 k_2} \qquad \text{modulo } [F,F]. \tag{67}$$

Also gilt für ein Element y aus $[R,R]$:

$$\begin{aligned} y &\equiv \prod_i [e_1^{d_1 k_{1i}} e_2^{d_2 k_{2i}}, e_1^{d_1 h_{1i}} e_2^{d_2 h_{2i}}] \\ &\equiv \prod_i [e_1, e_2]^{g(k_{1i} h_{2i} - k_{2i} h_{1i})} \qquad \text{modulo } F_3, \end{aligned} \tag{68}$$

wie man leicht aus den Identitäten

$$[AB, C] = [B, C]\,[[B, C], A]\,[A, C], \tag{69}$$

$$[A, BC] = [A, B]\,[A, C]\,[[A, C], B] \tag{70}$$

schließen kann. Aus (66) und (68) ergibt sich für jedes $t \in T$,

$$t \equiv e_1^{g_1} e_2^{g_2} e_{12}^{g_{12}} \qquad \text{modulo } F_3, \tag{71}$$

wobei g_1, g_2, g_{12} Vielfache von g sind. Aus (65) und aus (71) folgt weiter, mit Hilfe der Identitäten (69) und (70),

$$\begin{aligned}[x,t] &\equiv [e_1^{p_1} e_2^{p_2} e_{12}^{p_{12}}, e_1^{g_1} e_2^{g_2} e_{12}^{g_{12}}] \\ &\equiv e_{12}^a [e_{12}, e_1]^b [e_{12}, e_2]^c \qquad \text{modulo } F_4\end{aligned} \tag{72}$$

mit

$$\begin{aligned} a &= p_1 g_2 - p_2 g_1 \\ b &= p_{12} g_1 - p_1 g_{12} + p_1 g_2 g_1 - p_1 p_2 g_1 + \tfrac{1}{2} p_1 g_2 (g_2 - 1) + \tfrac{1}{2} g_2 p_1 (p_1 - 1) \\ c &= p_{12} g_2 - p_2 g_{12} - \tfrac{1}{2} p_2 g_1 (g_1 - 1) - \tfrac{1}{2} g_1 p_2 (p_2 - 1). \end{aligned} \tag{73}$$

Wir wollen jetzt zeigen, daß das Element $[e_{12}, e_1^{d_1}]$ von $[R, R]$ in $[F, T]$ nicht enthalten ist, d.h. daß es nicht zu einem Produkt

$$\begin{aligned}\prod_i [x_i, t_i] &= \prod_i [e_1^{p_{1i}} e_2^{p_{2i}} e_{12}^{p_{12i}}, e_1^{g_{1i}} e_2^{g_{2i}} e_{12}^{g_{12i}}] \\ &\equiv \prod_i e_{12}^{a_i} [e_{12}, e_1]^{b_i} e_{12}, e_2^{c_i}\end{aligned} \tag{74}$$

modulo F_4 kongruent ist. (Die a_i, b_i, c_i sind, mutatis mutandis, durch die (73) gegeben.) Es ist

$$[e_{12}, e_1^{d_1}] \equiv [e_{12}, e_1]^{d_1} \qquad \text{modulo } F_4$$

und für jedes Element $z \in F$ gilt eine Kongruenz der Form

$$z \equiv e_1^{q_1} e_2^{q_2} e_{12}^{q_{12}} [e_{12}, e_1]^{m_1} [e_{12}, e_2]^{m_2} \qquad \text{modulo } F_4, \tag{75}$$

wobei die Exponenten eindeutig bestimmt sind (vgl. z.B. [4, S. 167]). Wäre also

$$[e_{12}, e_1]^{d_1} \equiv \prod_i e_{12}^{a_i} [e_{12}, e_1]^{b_i} [e_{12}, e_2]^{c_i} \qquad \text{modulo } F_4,$$

so müßte

$$\sum_i a_i = 0, \qquad \sum_i b_i = d_1, \qquad \sum_i c_i = 0$$

und insbesondere, wegen (73)

$$\sum_i (p_{1i} g_{2i} - p_{2i} g_{1i}) = 0, \tag{76}$$

$$\sum_i \tfrac{1}{2} p_{1i} g_{2i} (g_{2i} - 1) \equiv d_1 \qquad \text{modulo } g, \tag{77}$$

$$\sum_i \tfrac{1}{2} p_{2i} g_{1i} (g_{1i} - 1) \equiv 0 \qquad \text{modulo } g \tag{78}$$

sein. Für ein ungerades g erhielte man aus (77)

$$d_1 \equiv 0 \qquad \text{modulo } g,$$

was den Voraussetzungen (64) widerspräche. Wäre aber $g = 2h$, so ergäben die Kongruenzen (77) und (78)

$$\sum_i p_{1i} h_{2i} (2h_{2i} - 1) \equiv d_1 \qquad \text{modulo } g, \tag{79}$$

$$\sum_i p_{2i} h_{1i} (2h_{1i} - 1) \equiv 0 \qquad \text{modulo } g \tag{80}$$

mit $2h_{1i}=g_{1i}$, $2h_{2i}=g_{2i}$. Aus (79) und (80) würde, durch Subtraktion und Berücksichtigung von (76),

$$\sum_i 2(p_{1i}h_{2i}^2 - p_{2i}h_{1i}^2) \equiv d_1 \qquad \text{modulo } g$$

folgen. Dies ergäbe wieder den Widerspruch

$$d_1 \equiv 0 \qquad \text{modulo } g.$$

Damit ist gezeigt, daß es ein Element aus $[R, R]$ gibt, das nicht in $[F, T]$ liegt. Satz 6.4 ist somit bewiesen.

Bemerkung. Als Spezialfall von Satz 6.4 erhalten wir:

$$F_m \neq [R, R] \qquad \text{falls } F \neq R.$$

Dies ist im folgenden Resultat von Neumann [9] enthalten:

$$F_m \not\subset [R, R] \qquad \text{falls } F \neq R.$$

Literatur

1. Auslander, M., and R. C. Lyndon: Commutator subgroups of free groups. Amer. J. Math. **77**, 929–931 (1955).
2. Schreier, O.: Die Untergruppen der freien Gruppen. Abh. Math. Sem. Univ. Hamburg **5**, 161–183 (1927).
3. Eckmann, B.: Coverings and Betti numbers. Bull. Amer. Math. Soc. **55**, 95–101 (1949).
4. Hall, M.: The theory of groups. New York: Macmillan Co. 1959.
5. Magnus, W.: Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring. Math. Ann. **111**, 259–280 (1935).
6. –, A. Karras, and D. Solitar: Combinatorial group theory. New York-Sidney-London: Interscience 1966.
7. Witt, E.: Treue Darstellung Liescher Ringe. J. reine angew. Math. **177**, 152–160 (1937).
8. MacLane, S.: Homology. Berlin-Göttingen-Heidelberg: Springer 1963.
9. Neumann, B. H.: On a theorem of Auslander and Lyndon. Arch. Math. **13**, 4–9 (1962).
10. Cartan, H., and S. Eilenberg: Homological algebra. Princeton: Princeton Univ. Press 1956.
11. Seifert, H., and W. Threlfall: Lehrbuch der Topologie. Leipzig u. Berlin: Teubner 1934.
12. Lang, S.: Rapport sur la cohomologie des groupes. New York-Amsterdam: Benjamin 1966.
13. Hopf, H.: Fundamentalgruppe und zweite Bettische Gruppe. Comm. Math. Helv. **14**, 237–309 (1942).

Dr. Manuel Ojanguren
Forschungsinstitut für Mathematik
der Eidgenössischen Technischen Hochschule
CH 8006 Zürich

(Eingegangen am 20. Oktober 1967)