JOURNAL OF NUMBER THEORY 7, 49–70 (1975)

Über die gruppentheoretische Struktur der Relationen zwischen Relativnormabbildungen in endlichen Galoisschen Körpererweiterungen

HANS PETER REHM

Mathematical Institute II, University of Karlsruhe, 75 Karlsruhe 1, Englerstraße 2, Germany

Communicated by H. W. Leopoldt

Received April 23, 1972

We define and study the module (over rational integers) of relative norms in galois field extensions in a purely group theoretical manner. We can compute a basis of this module from the lattice of subgroups by means of the Möbius function. Its rank is the number of noncyclic subgroups. The module depends functorially on the group. The module of a factor group is naturally imbedded in the module of the group. We prove some other structure results of this type.

A norm relation relates those subfields which have nonzero coefficient in this relation, the other fields being eliminated.

Using deep group theoretical results by Zassenhaus and Suzuki we can give an explicit description of all those groups for which the trivial subgroup is eliminated in any norm relation. (This means for example that we know the group types of all those galois number fields in which norm relations do not yield an estimate of the divisor class group exponent by means of similar exponents of subfields.) The list is somewhat unexpected, it includes special linear groups of dimension 2 over galois fields of Fermat prime characteristic and certain metacyclic groups.

0. EINLEITUNG UND ÜBERBLICK

0.1. *Galoistheoretische Einführung des Normrelatorenmoduls*

Ich verwende die folgenden Bezeichnungen und Festlegungen:

$\mathbf{Z}$: Ring der ganzrationalen Zahlen.

G: endliche Gruppe; E die Gruppe mit nur einem Element.

$n = |G| =$ Ordnung von G.

$\mathbf{Z}[G]$: Gruppenring von G über $\mathbf{Z}$.

Jeder Untergruppe $U \leqslant G$ ordnen wir das fogende Element $\underline{U} \in \mathbf{Z}[G]$ zu

$$\underline{U} = \sum_{h \in U} h. \tag{1}$$

K/k: galoissche Körpererweiterung mit Galoisgruppe G.

$K^\times$: Multiplikativgruppe von K.

$L \mapsto L'$: der durch den Fundamentalsatz der Galoistheorie gegebene Verbandsantiisomorphismus

$$\Lambda = \{L; k \leqslant L \leqslant K\} \to \Gamma := \{U; U \leqslant G\}$$

des Zwischenkörperverbands Λ mit dem Untergruppenverband Γ.

$\Delta = \{U; U \leqslant G,\ U \text{ zyklisch}\}$; $\Delta' = \Gamma \backslash \Delta$. Wenn die Bezugnahme auf G nötig ist, schreibe ich auch $\Delta(G)$, etc. $\varnothing$ = Leere Menge.

Ferner verwende ich die üblichen Bezeichnungen aus der Gruppentheorie und Algebra. $\mathbf{Z}[G]$ operiert galoissch auf $K^\times$; wir schreiben diese Operation exponentiell.

Die *Relativnormfunktion*

$$N_{K/L} : K^\times \to L^\times$$

ist dann gegeben durch

$$x \mapsto N_{K/L}x = \prod_{h \in L'} x^h = x^{\underline{L'}}. \tag{2}$$

Ein *Normrelator* von K/k ist ein Vektor $\alpha = (\alpha_U)_{U \leqslant G} \in \mathbf{Z}^\Gamma$, der (für alle $x \in K^\times$) die folgende Gleichung erfüllt:

$$1 = \prod_{L \in \Lambda} (N_{K/L}x)^{\alpha_{L'}} \tag{3}$$

Die Menge aller Normrelatoren von K/k bilden einen $\mathbf{Z}$-Modul, den *Normrelatorenmodul* von K/k.

Der Annulator von $K^\times$ (als $\mathbf{Z}[G]$-Modul) ist das folgende zweiseitige Ideal von $\mathbf{Z}[G]$

$$\operatorname{Ann} K^\times = \{u \in \mathbf{Z}[G]; x^u = 1 \text{ für alle } x \in K^\times\}.$$

Gleichung (3) ist genau dann richtig, wenn in $\mathbf{Z}[G]$ die Kongruenz

$$0 \equiv \sum_{U \in \Gamma} \alpha_U \underline{U} \bmod \operatorname{Ann} K^\times \tag{4}$$

erfüllt ist. (Diese Betrachung gilt auch für andere $\mathbf{Z}[G]$-Moduln als $K^\times$.)

Der Satz von Artin [2, Theorem 5] über die multiplikative Unabhängigkeit von Automorphismen sagt genau aus, daß für Körper mit

unendlich vielen Elementen Ann $K^\times = 0$ ist. (Endliche Körper sind für die zu entwickelnde Theorie wegen der zyklischen Galoisgruppen sowieso uninteressant.)

In Körpern mit unendlich vielen Elementen sind also sämtliche Normrelatoren $\alpha = (\alpha_U)$ gegeben als die ganzzahligen Lösungen der Gleichungen in $\mathbf{Z}[G]$

$$0 = \sum_{U \in \Gamma} \alpha_U \underline{U}, \tag{5}$$

$\mathbf{U}(G) = \{\alpha = (\alpha_U);\ \alpha_U \in \mathbf{Z},\ \alpha \text{ erfüllt } (5)\}$ heißt *Normrelatorenmodul* von G. Seiner Untersuchung dient diese Arbeit.

Im Abschnitt 1 interessieren wir uns für die Abhängigkeit von $\mathbf{U}(G)$ von G. Die algebraische Struktur wird durch den Basissatz (Satz 1) völlig aufgeklärt: $\mathbf{U}(G)$ ist ein freier $\mathbf{Z}$-Modul, dessen Rang gleich der Anzahl der nichtzyklischen Untergruppen von G ist; es wird sogar eine explizite Formel zur Berechnung einer Basis aus dem Untergruppenverband angegeben.

$\mathbf{U}$ erweist sich als kovarianter Funktor (Satz 2). Der Normschachtelungssatz hat seine Entsprechung in einer natürlichen Einbettung des Normrelatorenmoduls der Faktorgruppen ($\mathbf{U}$ verhält sich also kontravariant funktoriell auf den Gruppen mit surjektiven Homomorphismen) (Satz 4). Der Aufbau des Moduls bei Gruppenerweiterungen aus den Faktoren hängt im allgemeinen unübersichtlich von der speziellen Erweiterung ab. Eine brauchbare Aussage ist aber im Falle eines direkten Produkts bei teilerfremden Ordnungen der Faktoren möglich (Satz 3).

Im Brennpunkt des Interesses stehen aber in dieser Arbeit spezifische Fragen im Hinblick auf galoistheoretische Anwendungen. Obwohl später von diesen Anwendungen nicht weiter geredet wird, bilden sie doch die Richtschnur der Untersuchung.

0.2. *Bemerkungen zur zahlentheoretischen Anwendung*

G operiert, auch abgesehen vom $K^\times$, auf geeigneten, den Körpern funktoriell zugeordneten Gruppen. Ist K ein algebraischer Zahlkörper, so gilt dies z. B. für

$\mathbf{D}_K$: Divisorengruppe von K, $\mathbf{H}_K$: Gruppe der Hauptdivisoren von K, $\mathbf{C}_K$: Divisorenklassengruppe von K, $\mathbf{J}_K$: Idelgruppe von K, etc.

Den Zahlentheoretiker interessiert die endliche Gruppe $\mathbf{C}_K$ besonders; wir wollen sie etwas näher ins Auge fassen (und überlassen es dem Leser, entsprechende Anwendungsmöglichkeiten auf die anderen Gruppen oder gar einen abstrakten Rahmen mit G-Moduln zu entwerfen).

Für $\alpha \in \mathbf{U}(G)$ und $x \in \mathbf{C}_K$ gewinnen wir aus (3)

$$x^{-\alpha_E} = \prod_{\substack{L \in \Lambda \\ L \neq K}} (N_{K/L}x)^{\alpha_{L'}}. \tag{6}$$

Es ist aber $N_{K/L}x = x^{L'}$ Element des natürlichen homomorphen Bildes der Divisorenklassengruppe von L in $\mathbf{C}_K$. (Man faßt wie üblich $N_{K/L}\mathbf{D}_K$ und $N_{K/L}\mathbf{H}_K$ als Untergruppen von $\mathbf{D}_L$ und $\mathbf{H}_L$ auf.) Auf diese Weise bedeutet (6), grob gesprochen, eine Beschränkung von $\mathbf{C}_K$ durch die $\mathbf{C}_L$. Für die Exponenten e_L der Divisorenklassengruppen $\mathbf{C}_L$ folgt direkt aus (6)

LEMMA 1. *Ist* $\alpha \in \mathbf{U}(G)$, *so ist* e_K *ein Teiler von*

$$\alpha_E \cdot \mathrm{kgV}\{e_L\,;\, k \leqslant L < K, \alpha_{L'} \neq 0\}.$$

(kgV bedeutet: kleinstes gemeinsames Vielfaches.)

Dies legt folgende Begriffserklärungen und Fragestellungen nahe: In $\alpha \in \mathbf{U}(G)$ nennen wir diejenigen $U \in \Gamma$ *eliminiert*, für die $\alpha_U = 0$ ist. Eine Menge M von Untergruppen heißt *nichttrivial eliminierbar*, wenn es ein $\alpha \in \mathbf{U}(G)$ mit $\alpha_U = 0$ für all $U \in M$, aber $\alpha_E \neq 0$ gibt. α_E fungiert als wichtige *Abschätzkonstante*, über deren Natur man möglichst viel wissen möchte. Galoistheoretisch ist also besonders das *Eliminationsproblem* für $\mathbf{U}(G)$ von Belang: Welche Untergruppenmengen von G sind nichttrivial eliminierbar? Welches sind dabei jeweils die bestmöglichen "Abschätzkonstanten" α_E? Für welche Gruppen gibt es keine nichttrivial eliminierbaren Untergruppenmengen?

Rechnerischer Behandlung zugänglich gemacht wird das Problem durch Einführung des einer Untergruppenmenge M zugeordneten *Eliminativmoduls* $\mathbf{E}(M)$:

$$\mathbf{E}(M) := \{\alpha \in \mathbf{U}(G);\ \alpha_U = 0 \text{ für alle } U \in M\}.$$

In 2.1 wird ein Verfahren angegeben, wie bei gegebener Gruppe G und Menge M eine Basis von $\mathbf{E}(M)$ ausgerechnet werden kann. Dies erlaubt eine vollständige Behandlung des Eliminationsproblems bei vorgegebener Gruppe mit angemessenem Rechenaufwand. In 3.2 werden, gestützt auf die in 1 und 2 entwickelte Theorie und tiefliegende gruppentheoretische Arbeiten von M. Suzuki und H. Zassenhaus, sämtliche Gruppen ohne nichttrivial eliminierbare Untergruppenmengen explizit aufgestellt (Satz 5). Ein kurioses Faktum ist dabei das Auftreten von speziellen linearen Gruppen $SL(2, p)$ zu Fermatprimzahlen (d.h. solchen der Form $p = 2^n + 1$) im nichtauflösbaren Fall.

Vielleicht wirkt zum Abschluß der zahlentheoretischen Bemerkungen das einfachste nichttriviale Beispiel illustrativ: Sei k der Körper der rationalen Zahlen, K/k habe die alternierende Gruppe $G = A_4$ der geraden Permutationen von 4 Elementen zur Galoisgruppe. Der Untergruppenverband hat folgende Gestalt: V ist ein nichtzyklischer Normalteiler der Ordnung 4, dessen 3 Untergruppen der Ordnung 2 (sie sind in G konjugiert) B_1, B_2, B_3 seien. Weiter enthält A_4 noch 4 konjugierte zyklische Untergruppen C_1,..., C_4 der Ordnung 3. (Seihe Fig. 1.) $\mathbf{U}(G)$ hat nach Satz 1 den Rang 2; die Basismatrix ist

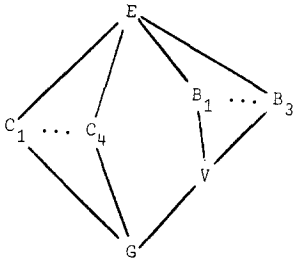

FIGURE 1

	G	V	B_1	B_2	B_3	C_1	C_2	C_3	C_4	E
γ^G	1	0	−1	−1	−1	−1	−1	−1	−1	6
γ^V	0	1	−1	−1	−1	0	0	0	0	2

Es gibt genau 3 maximale nichttrivial eliminierbare Mengen, nämlich

$M_1 = \{G, C_1, ..., C_4\}$, $\mathbf{E}(M_1) = \mathbf{Z} \cdot \gamma^V$, Abschätzkonstante: 2,
$M_2 = \{V\}$, $\mathbf{E}(M_2) = \mathbf{Z} \cdot \gamma^G$, Abschätzkonstante: 6,
$M_3 = \{B_1, B_2, B_3\}$, $\mathbf{E}(M_3) = \mathbf{Z}(\gamma^G - \gamma^V)$, Abschätzkonstante: 4.

Galoistheoretisch ist dabei M_3 am interessantesten, da die "großen" zu B_1, B_2, B_3 gehörigen Körper eliminiert sind. Beachtet man noch, daß konjugierte Körper isomorphe Klassengruppen haben, so findet man.

Bezeichnet e_H den Exponenten der Divisorenklassengruppe des galoistheoretisch zu H gehörigen Körpers, so ist im vorliegenden Beispiel e_E (der Exponent zu K) ein Teiler von $4 \cdot \mathrm{kgV}\{e_{C_1}, e_V\}$.

Sollten darüber hinaus die Klassenzahlen der Körper zu C_1 und V beide 1 *sein, so ist die Klassengruppe von K eine* 2*-Gruppe mit höchstens Exponent* 4.

Aus den Klassengruppenexponenten von zwei Körpern der Grade 3

und 4 ergibt sich demnach eine Abschätzung für den Klassengruppenexponenten eines Körpers 12. Grades.

Ähnliche, im Rahmen dieser $\mathbf{U}(G)$ Methode vollständige Resultate lassen sich für jede konkret gegebene endliche Galoisgruppe gewinnen, wobei die Rechnung ohne weiteres einem Automaten zugewiesen werden könnte. Da über Klassengruppen nichtabelscher Körper kaum gute Abschätzungen nach oben bekannt sind, mag diese Methode auch für praktische Rechnungen in Zahlkörpern von Nutzen sein.

0.3. *Eine geschichtliche Bemerkung*

Ihrer Motivierung nach stellt die Arbeit einen Versuch dar, Aufschluß zu suchen, wie die Galoisgruppenstruktur die Freiheit gewisser (vorzugsweise zahlentheoretischer) "Invarianten" in sämtliche Zwischenkörpern einschränkt. In dieser Hinsicht ist sie in einer Linie zu sehen mit Artins Arbeiten über Relationen von ζ-Funktionen. (Artin [1], siehe auch R. Brauer [4]). Im Gegensatz zu den Artinschen liegen die hier betrachteten Relationen auf der Hand; dafür interessiert uns deren spezifisch galoistheoretische Struktur in Abhängigkeit von der Gruppenstruktur. Hierbei treten andersartige Fragen in den Vordergrund. Ich glaube, daß die vorliegende Arbeit die Fragen soweit aufschließt, daß man einen gewissen Eindruck bekommt, was und was nicht auf dem hier eingeschlagenen Wege erzielt werden kann.

Ich danke Herrn Professor Leopoldt für sein förderndes Interesse an dieser Arbeit; ihm verdanke ich die Anregung, Normrelationen systematisch zu untersuchen.

1. Der Normrelatorenmodul $\mathbf{U}(G)$

Die in 0.1 eingeführten Begriffe und Bezeichnungen werden in der ganzen Arbeit weiterverwendet.

1.1. *Der Basissatz*

Satz 1. *μ sei die Möbiussche zahlentheoretische Funktion ($\mu(1) = 1$, $\mu(p_1 \cdots p_r) = (-1)^r$, falls die Primzahlen $p_1, \ldots, p_r$ alle verschieden, sonst $\mu(p_1 \cdots p_r) = 0$). Dann bilden die Vektoren*

$$\gamma^H, \qquad H \leqslant G, \qquad H \text{ nicht zyklisch},$$

eine Basis des freien $\mathbf{Z}$-Moduls $\mathbf{U}(G)$, wenn die Komponenten $\gamma_U{}^H$ von γ^H

wie folgt erklärt werden:

$$\gamma_U{}^H = \begin{cases} 1 & \text{für} \quad U = H, \\ -\sum\limits_{\substack{V \\ H \geqslant V \geqslant U \\ V \text{ zyklisch}}} \mu(V\colon U) & \text{für} \quad U \neq H. \end{cases} \tag{7}$$

(*Die Summe ist leer, wenn* $U \not\leqslant H$ *ist, oder wenn* U *nichtzyklisch ist. Ihr Wert ist dann* 0. *Das System der* γ^H *ist genau dann leer, wenn* G *zyklisch ist. Genau dann ist* $\mathbf{U}(G) = 0$.) *Jedes* $\alpha = (\alpha_U) \in \mathbf{U}(G)$ *schreibt sich in eindeutiger Basisdarstellung als*

$$\alpha = \sum_{\substack{H \leqslant G \\ H \text{ nicht-} \\ \text{zyklisch}}} \alpha_H \gamma^H. \tag{8}$$

Beweis. Durch Zufügen von 0-Komponenten kann man in natürlicher Weise $\mathbf{U}(H)$ für eine Untergruppe $H \leqslant G$ als Teilmodul von $\mathbf{U}(G)$ auffassen. Demnach teicht der Beweis von $\gamma^G \in \mathbf{U}(G)$ auch für $\gamma^H \in \mathbf{U}(G)$ hin.

Dazu zeigen wir zunächst, daß die in (7) erklärten $\gamma_Z{}^G$ fur $Z \in \Delta$ der rekursiven Bestimmungsgleichung

$$\gamma_Z{}^G = -1 - \sum_{\substack{Y > Z \\ Y \in \Delta}} \gamma_Y{}^G \tag{9}$$

genügen. Ist Z maximal in Δ (der Menge der zyklischen Untergruppen), so ist (9) evident ($\mu(1) = 1$, leere Summe). Ist $X, Z \in \Delta$ und durchläuft Y die Untergruppen $X \geqslant Y \geqslant Z$, so durchläuft $(X\colon Y)$ genau alle Teiler von $|X|$, die Vielfache von $|Z|$ sind. Daher ist bekanntlich (Summenformel für μ):

$$\sum_{\substack{Y \\ X \geqslant Y \geqslant Z}} \mu(X\colon Y) = 0, \qquad \text{falls} \quad X \neq Z.$$

Damit und mit einer Induktionshypothese berechnet man (zu summieren ist über $X, Y \in \Delta$ unter den angegebenen Einschränkungen, Z fest)

$$\begin{aligned} -1 - \sum_{Y > Z} \gamma_Y{}^G &= -1 + \sum_{Y > Z} \sum_{X \geqslant Y} \mu(X\colon Y) \\ &= -1 + \sum_{X \geqslant Y > Z} \mu(X\colon Y) - \sum_{\substack{X \geqslant Y \geqslant Z \\ X > Z}} \mu(X\colon Y) \\ &= -1 - \sum_{X > Z} \mu(X\colon Z) = \gamma_Z{}^G. \end{aligned}$$

Das beweist (9). Mit Hilfe von (9) prüft man leicht, daß $\gamma^G \in \mathbf{U}(G)$ ist, wenn man folgendes bemerkt:

LEMMA 2. *$\beta \in \mathbf{Z}^\Gamma$ ist genau dann in $\mathbf{U}(G)$, wenn für alle $Z \in \Delta$ gilt:*

$$\sum_{\substack{Y \in \Gamma \\ Y \geqslant Z}} \beta_Y = 0. \tag{10}$$

(Ist nämlich Z erzeugt von $g \in G$, dann stimmt die linke Seite von (10) überein mit dem Koeffizienten von g in $\sum_{U \leqslant G} \beta_U \underline{U}$.)

Nachdem wir $\gamma^H \in \mathbf{U}(G)$ bewiesen haben, und die Freiheit der γ^H über $\mathbf{Z}$ trivial ist, reicht der Beweis von (8) zum Nachweis der Basiseigenschaft.

Wir sahen $\gamma^H \in \mathbf{U}(G)$, also für $\alpha = (\alpha_U) \in \mathbf{U}(G)$ auch

$$\beta := \alpha - \sum_{\substack{H \leqslant G \\ H \in \Delta'}} \alpha_H \gamma^H \in \mathbf{U}(G),$$

und es ist $\beta_H = 0$ für alle $H \in \Delta'$ (die nichtzyklischen Untergruppen). Es bleibt also zu zeigen, daß für so ein β notwendig $\beta = 0$ ist, d.h. auch für die zyklischen Z $\beta_Z = 0$ wird. Dies folgt rekursiv aus (10): Ist Z maximal in Δ, so bleibt in (10) nur $\beta_Z = 0$ stehen. Nach Entfernung dieser maximalen aus Δ bleibt für die im Rest maximalen Gruppen wiederum jeweils nur ein Glied links stehen, das damit notwendig verschwindet. Diesen Prozess kann man fortsetzen bis ganz Δ erschöpft ist. Die Überlegung zeigt auch, daß für zyklische G $\mathbf{U}(G) = 0$ ist. Das beendet den Beweis.

1.2. $\mathbf{U}(G)$ *als Funktion von G*

Wir betrachten nun $\mathbf{U}(G)$ in Abhängigkeit von G. Man kann aus zwei geeigneten zyklischen Gruppen ein semidirektes Produkt mit nichtzyklischen Untergruppen beliebig großer Anzahl aufbauen. Demnach hängt $\mathbf{U}(G)$ nicht nur von den Moduln der Gruppen einer Kompositionsreihe von G, sondern auch sehr unübersichtlich von der speziellen Erweiterung ab. Bei homomorpher Vergröberung jedoch verhält sich $\mathbf{U}$ vernünftig.

SATZ 2. *$\mathbf{U}$ ist ein kovarianter Funktor von der Kategorie der endlichen Gruppen in die Kategorie der endlich erzeugbaren $\mathbf{Z}$-Moduln, wenn für zwei Gruppen G, G' und $\phi \in \mathrm{Hom}(G, G')$*

$$\mathbf{U}\phi\colon \mathbf{U}(G) \to \mathbf{U}(G')$$

wie folgt erklärt wird:

Für $\alpha \in \mathbf{U}(G)$ *und* $U' \leqslant G'$ *sei*

$$(\mathbf{U}\phi(\alpha))_{U'} = \sum_{\substack{U \leqslant G \\ \phi U = U'}} \alpha_U \mid U \cap \operatorname{Kern} \phi \mid. \tag{11}$$

Speziell ist für γ^H *aus* (7)

$$\mathbf{U}\phi(\gamma^H) = \mid \operatorname{Kern} \phi \cap H \mid \cdot \gamma^{\phi H}, \tag{12}$$

worin für zyklische ϕH $\gamma^{\phi H} = 0$ *zu setzen ist.*

Beweis. ϕ hat eine wohlbestimmte, mit den Einbettunger der Gruppen in ihre Gruppenringe verträgliche $\mathbf{Z}$-lineare Fortsetzung zu einem Homomorphismus $\bar{\phi}$: $\mathbf{Z}[G] \to \mathbf{Z}[G']$ der Gruppenringe.

Anwendung von $\bar{\phi}$ auf die Gleichung (5) aus 0.1 ergibt

$$0 = \bar{\phi}(0) = \bar{\phi}\left(\sum_{U \leqslant G} \alpha_U \underline{U}\right) = \sum_{U \leqslant G} \alpha_U \bar{\phi}(\underline{U}).$$

Wir berechnen $\bar{\phi}(\underline{U}) = \sum_{h \in U} \phi(h)$.

Hierin ist $\phi(h) = \phi(h')$, genau wenn $h^{-1}h' \in \operatorname{Kern} \phi \cap U$. Daher ist

$$\bar{\phi}(\underline{U}) = \mid \operatorname{Kern} \phi \cap U \mid \underline{\phi U}$$

$$\sum_{U \leqslant G} \alpha_U \mid \operatorname{Kern} \phi \cap U \mid \underline{\phi U} = 0.$$

Fassen wir die U's, die ein und dasselbe Bild $U' = \phi U$ haben, zusammen, so finden wir

$$\sum_{U' \leqslant G'} \left(\sum_{\substack{U \leqslant G \\ U' = \phi U}} \alpha_U \mid \operatorname{Kern} \phi \cap U \mid \right) \underline{U'} = 0.$$

Dies zeigt nach Lemma 2 $\mathbf{U}\phi(\alpha) \in \mathbf{U}(G')$. Daß $\mathbf{U}\phi$ $\mathbf{Z}$-linear ist, bestätigt man durch elementare Rechnung.

Nunmehr kommen wir zur eigentlichen Funktoreigenschaft $\mathbf{U}\psi \circ \mathbf{U}\phi = \mathbf{U}(\psi \circ \phi)$. ($\circ$ bedeutet Komposition von Abbildungen durch Hintereinanderschalten, und ψ sei ein weiterer Gruppenhomomorphismus $G' \to G''$.)

Wir beweisen also für alle $U'' \leqslant G''$ und alle $\alpha \in \mathbf{U}(G)$

$$(\mathbf{U}(\psi \circ \phi)(\alpha))_{U''} = ((\mathbf{U}\psi \circ \mathbf{U}\phi)(\alpha))_{U''}.$$

Nach Definition gilt:

$$(\mathbf{U}(\psi \circ \phi)(\alpha))_{U''} = \sum_{\substack{U \leqslant G \\ U'' = (\psi\phi)U}} \alpha_U \mid U \cap \operatorname{Kern} \psi\phi \mid$$

und

$$((\mathbf{U}\psi \circ \mathbf{U}\phi)(\alpha))_{U''} = \sum_{\substack{U' \leqslant G' \\ U''=\psi U'}} \left(\sum_{\substack{U \leqslant G \\ U'=\phi U}} \alpha_U \mid U \cap \operatorname{Kern} \phi \mid \right) \mid U' \cap \operatorname{Kern} \psi \mid$$

$$= \sum_{\substack{U \leqslant G \\ U''=(\psi \cdot \phi) U}} \alpha_U \mid U \cap \operatorname{Kern} \phi \mid\mid \phi U \cap \operatorname{Kern} \psi \mid$$

denn $U \mapsto (\phi U, U)$ bezieht die Summationsmengen der letzten und vorletzten Zeile bijektiv aufeinander.

Der Beweis ist damit reduziert auf den elementarengruppentheoretischen Hilfssatz, den ich als bekannt annehme: Sind $\phi\colon G \to G'$ und $\psi\colon G' \to G''$ Gruppenhomomorphismen und ist $U \leqslant G$, so gilt:

$$\mid U \cap \operatorname{Kern} \phi \mid \cdot \mid \phi U \cap \operatorname{Kern} \psi \mid = \mid U \cap \operatorname{Kern} \psi \circ \phi \mid.$$

Zum Beweis von (12) beachte man schließlich, daß es ausreicht, $(\mathbf{U}\phi(\gamma^H))_{U'} = \mid \operatorname{Kern} \phi \cap H \mid \gamma_{U'}^{\phi H}$ für nichtzyklische U' nachzuweisen und daß man sich infolge der Inklusion $H \leqslant G$ sogar auf $G = H$ beschränken kann.

$\mathbf{U}$ ist offensichtlich nicht exakt, es gilt aber: Ist ϕ momomorph, so ist $\mathbf{U}\phi$ momomorph. Ist ϕ epimorph, so ist zwar $\mathbf{U}\phi$ im allgemeinen nicht epimorph, aber $\mathbf{U}\phi(\mathbf{U}(G))$ hat endlichen Index in $\mathbf{U}(\phi G)$.

Aus (11) entnimmt man: Ist Kern ϕ eine p-Gruppe, so ist $(\mathbf{U}\phi(\alpha))_E \equiv \alpha_E \bmod p$. Das ergibt zusammen mit (12): *Hat G eine nichttriviale p-Gruppe als Normalteiler, dann ist p ein Teiler von $\gamma_E{}^G$.*

SATZ 3. *Eine endliche Gruppe G sei das direkte Produkt ihrer Untergruppen H und K. Der größte gemeinsame Teiler der Ordnungen $\mid H \mid$ und $\mid K \mid$ sei* 1; *H oder K sei nicht zyklisch. Für zyklische Untergruppen Z von G setze man*

$$\gamma_T{}^Z := -\sum_{\substack{X \\ Z \geqslant X \geqslant T}} \mu(X\colon T) = \begin{cases} -1 & Z = T \\ 0 & \textit{sonst} \end{cases}$$

(beachte: $\gamma^Z \notin \mathbf{U}(G)$). Ist dann U eine zyklische Untergruppe, V eine nichtzyklische Untergruppe von G, so gilt:

$$-\gamma_U{}^V = \gamma_{H \cap U}^{H \cap V} \gamma_{K \cap U}^{K \cap V}. \tag{13}$$

Beweis. $U \mapsto (H \cap U, K \cap U)$ vermittelt wegen $U = (H \cap U) \times (K \cap U)$ (dies wäre ohne die Teilbarkeitsvoraussetzung nicht richtig) eine bijektive Abbildung von der Menge aller Untergruppen von G auf das kartesische Produkt der entsprechenden Mengen von H und K, webei U genau dann

zyklisch ist, wenn $H \cap U$ und $K \cap U$ beide zyklisch sind. Für nichtzyklische V können wir ohne Einschränkung $V = G$, also $H \cap V = H$, $K \cap V = K$ und H nichtzyklisch annehmen und haben dann zu beweisen:

$$-\gamma_U{}^G = \gamma_{H\cap U}^H \cdot \gamma_{K\cap U}^K .$$

Für $U \in \Delta(G)$ erhält man, das zu Anfang des Beweises Gesagte und die schwache Multiplikativität von μ ausnützend, wegen

$$Z/U \simeq (Z \cap H)/(U \cap H) \times (Z \cap K)/(U \cap K)$$

nach kurzer Rechnung die Behauptung.

Zur Motivierung des folgenden Satzes betrachten wir (3) in der Einleitung. Sei zusätzlich M ein Erweiterungskörper von K, der über k galoissch ist, mit Galoisgruppe $\tilde{G}$, $\tilde{N}$ die Fixgruppe von K; die Galoisgruppe G von K/k ist dann isomorph zu $\tilde{G}/\tilde{N}$. Zu den Zwischenkörpern L von K/k gehören in $\tilde{G}$ galoistheoretisch diejenigen Untergruppen, die $\tilde{N}$ enthalten. Wenden wir die Normschachtelungsformel

$$N_{M/L}(y) = N_{K/L}(N_{M/K}(y))$$

auf (3) mit $x = N_{M/K}(y)$ an, so sehen wir für alle $y \in M^\times$

$$1 = \prod_{L\in\Lambda} (N_{M/L}(y))^{\alpha_{L'}} \tag{14}$$

wobei $L \to L'$ die Galoiszuordnung der Zwischenkörper von K/k zu den Untergruppen von G angibt. Deutet man dies durch Zufügen vom 0-Exponenten in $\tilde{G}$, so liegt folgender Satz nahe:

SATZ 4. *Sei $\tilde{N}$ ein Normalteiler der endlichen Gruppe $\tilde{G}$ und ϕ der kanonische Epimorphismus*

$$\phi\colon \tilde{G} \to \tilde{G}/\tilde{N} =: G.$$

Dann definiert die folgende Gleichung (15), *angewendet auf alle $\alpha \in \mathbf{U}(G)$ eine natürliche Einbettung*

$$\begin{gathered} \iota\colon \mathbf{U}(G) \to \mathbf{U}(\tilde{G}) \\ (\iota\alpha)_{\tilde{U}} := \begin{cases} \alpha_{\phi\tilde{U}} & \text{falls } \tilde{U} \geqslant \tilde{N} \\ 0 & \text{sonst.} \end{cases} \end{gathered} \tag{15}$$

Beweis. Wir haben nur $\iota\alpha \in \mathbf{U}(G)$ nachzuweisen; daß dann (15) ein $\mathbf{Z}$-Modul-Monomorphismus ist, ist klar.

Wir stellen $\tilde{G}$ als Galoisgruppe einer Körpererweiterung M/k (etwa durch Permutation von Unbestimmten) dar. Bezeichne K den Fixkörper von $\tilde{N}$, G seine Galoisgruppe über k. Ausgehend von $\alpha \in \mathbf{U}(G)$ erhalten wir aus (3) wie oben die generelle Normrelation (14). Wegen Ann $M^\times = 0$ (siehe 0.1) zeigt dies, daß $\iota\alpha \in \mathbf{U}(\tilde{G})$ ist.

ι aus Satz 4 und $\mathbf{U}\phi$ aus Satz 2 komponieren sich wie folgt:

$$U\phi(\iota(\alpha)) = |\operatorname{Kern}\phi| \cdot \alpha.$$

2. Elimination von Untergruppen

2.1. *Rechnerische Bestimmung einer Basis des Eliminativmoduls* $\mathbf{E}(M)$

Offensichtlich ist der $\mathbf{Z}$-Modul aller ganzzahligen Lösungsvektoren

$$(\alpha_H), \qquad H \in \Delta'$$

des linear-homogen-diophantischen Gleichungssystems

$$\sum_{H \in \Delta'} \alpha_{HY} \gamma_V^H = 0, \qquad V \in M, \tag{16}$$

vermöge $(\alpha_H) \mapsto \sum_{H \in \Delta'} \alpha_H \gamma^H$ isomorph zu $\mathbf{E}(M)$.

Es ist wohlbekannt, wie Gleichung (16) durch Verfahren der linearen Algebra aufgelöst werden kann. Speziell gilt

Lemma 3. *Ist B die Matrix der γ_V^H in* (16), *so gilt für die Ränge*

$$\operatorname{rg} \mathbf{E}(M) = \operatorname{rg} \mathbf{U}(G) - \operatorname{rg} B.$$

Ein Programm, das aus dem Untergruppenverband eine Liste maximaler nichttrivial eliminierbarer Mengen nebst Basen der Eliminativmoduln berechnet, ist im Rahmen einer Karslruher Diplomarbeit von W. Happle geschrieben worden.

2.2. *Abschätzkonstanten*

Für eine feste Untergruppe U von G ist $\{\beta_U ; \beta \in \mathbf{E}(M)\}$ ein Ideal von $\mathbf{Z}$; daher ist jedes vorkommende β_U Vielfaches des kleinsten positiven darunter; dieses wird mit $k_U(M)$ bezeichnet. $k_U(M)$ kann als der größte gemeinsame Teiler aller $\alpha_U{}^\lambda$ gefunden werden, wenn $\{\alpha^\lambda ; \lambda = 1,\ldots,f\}$ eine Basis von $\mathbf{E}(M)$ ist.

Nach 0.2 verdienen die Zahlen $k_E(M)$ besonderes Interesse.

2.3. *Eine Bedingung für* $\gamma_E{}^G = 0$

LEMMA 4. *D sei der Durchschnitt der maximalen unter den zyklischen Untergruppen quadratfreier Ordnung von G. Ist dann* $D \neq E$, *so gilt*

$$\gamma_E{}^G = 0 \qquad (\gamma_E{}^G \text{ aus Satz 1}).$$

Beweis. Ausgehend von $\underline{B}_1$, der Menge der maximalen unter den zyklischen Untergruppen quadratfreier Ordnung, sei $\underline{B}_i$ die Menge der Durchschnitte von je i verschiedenen Untergruppen aus $\underline{B}_1$; für zu große i sei $\underline{B}_i$ leer. Wir erklären f und B_i durch

$$f := \min\{i;\ \underline{B}_i = \{D\}\},$$

$$B_i = \underline{B}_i \Big\backslash \bigcup_{j>i} \underline{B}_j .$$

Es ist dann $B_1 = \underline{B}_1$. Für $Z \in \Delta^E$ (Menge der zyklischen Untergruppen quadratfreier Ordnung) sei die "Tiefe" $t(Z)$ das kleinste i, derart daß für wenigstens ein $N \in B_i Z \leqslant N$ ist. Eigenschaften der Funktion $t(Z)$:

(a) $t: \Delta^E \to \{1, 2, ..., f\}$

(b) Aus $Z \leqslant Z'$ folgt $t(Z) \geqslant t(Z')$.

(c) Ist $N \in B_i$, so ist $t(N) = i$.

(d) Ist $Z \leqslant M \cap N$, $M \in B_i$, $N \in B_k$, $i \leqslant k$ und $M \not\leqslant N$, so folgt $t(Z) > k$.

(e) Zu jedem Z mit $t(Z) = i$ gibt es ein und nur ein $M = M(Z) \in B_i$ mit $Z \leqslant M$.

(a) und (b) sind klar. In (c) führt die Hypothese $t(N) = k > i$ wie folgt auf einen Widerspruch: Für geeignete verschiedene $N_1, ..., N_k \in B_1$ ist dann $N < N_1 \cap \cdots \cap N_k$ notwendig echt, da $B_i \cap \underline{B}_k$ leer ist. Andererseits ist $N = N_1' \cap \cdots \cap N_i'$ für geeignete $N_1', ..., N_i' \in B_1$. In der Darstellung $N = N_1 \cap \cdots \cap N_k \cap N_1' \cap \cdots \cap N_i'$ lasse man diejenigen N_j' weg, die unter den $N_1, ..., N_k$ schon vorkommen; mindestens eines wird dann nicht weggelassen. Dies zeigt $N \in \underline{B}_s$ für $s > i$, was mit $N \in B_i$ unvereinbar ist.

In (d) genügt wegen (b) der Beweis von $t(M \cap N) > k$. Aus $M \not\geqslant N$ folgt $M \cap N \in B_s$ für ein $s > k$, also nach (c) $t(M \cap N) = s > k$. Haben schließlich die Gruppen M und M' die Eigenschaften, die in (e) für M vorausgesetzt wurden, so ergäbe $M \neq M'$ nach (b) und (d) den Widerspruch $t(Z) \geqslant t(M \cap M') > i$.

Nunmehr beweist man Satz 7 durch eine rekursive Rechnung.

Man bildet mit Unbestimmten X_V ($V \in \Delta^E$) für $1 \leqslant \lambda < f$:

$$s_1 = \sum_{M \in B_1} \sum_{V \leqslant M} X_V,$$

$$s_{\lambda+1} = s_\lambda - \sum_{M \in B_{\lambda+1}} (d(M, \lambda) - 1) \sum_{V \leqslant M} X_V;$$

die Koeffizienten $d(M, \lambda)$ in $s_{\lambda+1}$ sind wie folgt aus s_λ zu bestimmen:

$$s_\lambda = \sum_{V \in \Delta^E} d(V, \lambda) X_V.$$

Kernbehauptung. Ist $t(V) \leqslant \lambda \leqslant f$, so ist $d(V, \lambda) = 1$. Für $\lambda = 1$ ist dies klar nach (e). Für $1 \leqslant \lambda < f$ sei die Kernbehauptung erwiesen. Falls $t(V) \leqslant \lambda$, so it für alle $M \in B_{\lambda+1}$ nach (b) und (c) $V \nleqslant M$, daher $1 = d(V, \lambda) = d(V, \lambda + 1)$. Für den Fall $t(V) = \lambda + 1$ (Induktionsschritt) brauchen wir die Aussage: Aus $t(V) = \lambda + 1$ folgt für das $M = M(V) \in B_{\lambda+1}$ aus (e) $d(V, \lambda) = d(M, \lambda)$. Hierzu zeigt man für i mit $1 \leqslant i \leqslant \lambda$ und $M' \in B_i$, daß die Eigenschaft $V \leqslant M'$ mit $M \leqslant M'$ gleichbedeutend ist. Wäre nämlich $V \leqslant M'$, aber $M \nleqslant M'$, so ergäbe sich nach (d) $\lambda + 1 = t(V) \geqslant t(M \cap M') > t(M) = \lambda + 1$.

Der Induktionsschritt wird nunmehr klar vermöge der Definition von $s_{\lambda+1}$ und $d(V, \lambda + 1)$.

$$d(V, \lambda + 1) = d(V, \lambda) - (d(M, \lambda) - 1) = 1.$$

Als Ziel dieser Erörterung gewinnt man aus der Kernbehauptung nach (a):

$$s_f = \sum_{V \in \Delta^E} X_V.$$

Es enstehe nun s_λ' aus s_λ durch Einsetzen von $\mu(V: E)$ für X_V (μ ist die Möbiusfunktion). Aus unserer letzten Gleichung ersieht man $\gamma_E{}^G = -s_1$. (Da sich die $d(M, \lambda)$ für $\lambda = 1, 2, \ldots$ der Reihe nach direkt berechnen lassen, ist damit auch im Falle $D = E$ eine andersartige Berechnungsmöglichkeit für $\gamma_E{}^G$ aufgefunden, die z.B. zeigt, daß $\gamma_E{}^G$ nur von derjenigen Untergruppe von G abhängt, die durch alle Elemente von Primzahlordnung erzeugt wird.)

Ist nun sogar $D \neq E$, so ist für $\lambda \in \{1, \ldots, f\}$ $E \notin B_\lambda$; für $M \in B_\lambda$ ist daher $\sum_{V \leqslant M} \mu(V: E) = 0$, es werden der Reihe nach

$$s_1' = 0, \qquad s_2' = 0, \ldots, s_f' = 0 = \gamma_E{}^G,$$

Bemerkung. Das Verfahren dieses Beweises führt ohne weitere Ändererung zur Berechnung von $\gamma_U{}^G$ (U zyklisch), wenn man E durch U

ersetzt, statt Δ^E die Menge Δ^U derjenigen zyklischen Untergruppen von G nimmt, in denen U quadratfreien Index hat und D den Durchschnitt der maximalen Elemente von Δ^U bedeutet. Insbesondere ist im Falle von $D \neq U$ dann $\gamma_U{}^G = 0$.

3. Die Gruppen ohne Nichttriviale Elimination

In diesem Abschnitt werden alle Gruppen bestimmt, in denen alle Abschätzkonstanten α_E verschwinden. Hierzu ist hinreichend und notwendig $\gamma_E{}^H = 0$ für alle $H \in \Delta'$, d.h. $k_E(\varnothing) = 0$. Für $k_E(\varnothing)$ schreibe ich auch $k(G)$: Das ist die bestmögliche Abschätzkonstante durch irgendwelche Untergruppen.

3.1. *Vorbereitungen*

Ist G eine p-Gruppe (p Primzahl), $G \neq E$ und a die Anzahl der Untergruppen der Ordnung p. Dann ist nach Satz 1 $\gamma_E{}^G = a - 1$. Daher ist für $k_E(\varnothing) = 0$ notwendig und hinreichend, daß G genau eine Untergruppe der Ordnung p enthält, d.h. daß G zyklisch oder (ein nur im Falle $p = 2$ auftretender Sonderfall) eine verallgemeinerte Quaternionengruppe ist (siehe etwa Zassenhaus [9]). Diese Gruppen nenne ich im folgenden "fastzyklische p-Gruppen."

Wir formulieren nun die Bedingung $D \neq E$ aus Lemma 4 um.

Lemma 5. *"$D \neq E$" ist gleichbedeutend mit der Aussage: "eine p-Sylowgruppe S von G ist fastzyklisch und der Durchschnitt ihrer Konjugierten ist nichttrivial. Ist Z die zyklische Untergruppe von S der Ordnung p, so enthält der Zentralisator von Z in G alle weiteren Elemente von Primzahlordnung in G."*

Beweis. Ist $D \neq E$ und Z eine Untergruppe der Ordnung p von D, so ist nach Definition von D Z die einzige Untergruppe der Ordnung p von G (ansonsten gäbe es eine maximale zyklische Untergruppe quadratfreier Ordnung, die eine andere derartige Gruppe, also Z, nicht enthielte). Hieraus folgen die Aussagen über S, eine Z enthaltende p-Sylowgruppe von G. Würde nun eine Untergruppe U von Primzahlordnung durch Z nicht zentralisiert, so wäre wiederum Z in den maximalen zyklischen Untergruppen quadratfreier Ordnung, die U enthalten, nicht enthalten.

Umgekehrt sei Z die Untergruppe der Ordnung p von S. Z ist die einzige Untergruppe der Ordnung p in G, und nach der Voraussetzung ist $Z \leqslant D$ klar.

Als Ergänzung zu Lemma 4 können wir beweisen (ohne es später zu brauchen)

LEMMA 6. *Für eine nilpotente Gruppe G ist $\gamma_E{}^G = 0$ und $D \neq E$ gleichbedeutend.*

Beweis. Wegen Lemma 4 haben wir nur zu zeigen, daß aus $\gamma_E{}^G = 0$ $D \neq E$ folgt. Eine nilpotente Gruppe ist das direkte Produkt ihrer Sylowgruppen. Nach Satz 3 ist $\gamma_E{}^G$ bis auf das Vorzeichen das Produkt der $\gamma_E{}^S$ für die Sylowgruppen S von G. Demnach verschwindet mindestens ein $\gamma_E{}^S$, S ist fastzyklisch. Da die anderen Sylowgruppen im Zentralisator von S liegen, folgt nach Lemma 5 $D \neq E$. Der bequemen Handhabung halber formuliere ich noch eine Spezialisierung von Lemma 5.

LEMMA 7. *G enthalte genau eine Untergruppe Z der Ordnung 2. Dann ist $k(G) = 0$ gleichbedeutend mit $\gamma_E{}^H = 0$ für alle Untergruppen H ungerader Ordnung in Δ.*

Beweis. Enthält G genau eine Untergruppe der Ordnung 2, so hat auch jede Untergruppe H gerader Ordnung diese Eigenschaft. Nach Lemma 5 ist für alle diese Gruppen $D \neq E$, also nach Lemma 4 auch $\gamma_E{}^H = 0$. Dies beweist die Behauptung.

3.2. *Bestimmung der Gruppen ohne nichttriviale Elimination*

Sei G eine Gruppe mit $k(G) = 0$. Dies hat für jedes $H \in \Delta'$ die Folge $\gamma_E{}^H = 0$. Demnach kann in G keine nichtzyklische Untergruppe der Ordnung p^2 enthalten sein, d.h. alle abelschen Untergruppen sind zyklisch. (Es ist wohlbekannt und leicht zu beweisen, daß die Sylowgruppen einer solchen Gruppe fastzyklisch sind, siehe Zassenhaus [9]. Eine Bestimmung aller Gruppen mit dieser Eigenschaft ist in tiefliegenden Ergebnissen von Zassenhaus [8] und Suzuki [7] enthalten.)

Wir werden zur Bequemlichkeit des Lesers die relevanten Ergebnisse von Zassenhaus und Suzuki genau angeben und dann aus ihrer Aufzählung die Gruppen mit $k(G) = 0$ heraussuchen.

Zassenhaus [8, Satz 7]: Eine endliche Gruppe, deren 2-Sylowgruppen eine zyklische Untergruppe höchstens vom Index 2 enthält, während die übrigen Sylowgruppen zyklisch sind, kann in erzeugenden und definierenden Relationen in einer der Formen (A)–(E) angegeben werden ($[\cdots]$ bezeichnet gruppentheoretische Erzeugung).

(A) $G = [a, b]$ mit

(1) $a^m = 1$, $b^n = a^t$, $bab^{-1} = a^r$;

(2) $\mathrm{ggT}\{r - 1, m\} = r_0 > 0$, $r_0 t = m > 0$;

(3) $r^i \not\equiv 1 \bmod m$ für $1 \leqslant i < n$, $r^n \equiv 1 \bmod m$;

(4) $\mathrm{ggT}\{n, t\} = 1$.

(B) $G = [a, b, c]$ mit (A)(1)–(A)(4), dazu

(1a) $cac^{-1} = a^f, cbc^{-1} = b^f$;

(5) $f^2 \equiv 1 \bmod m, f \equiv 1 \bmod n$;

(α) $c^2 = 1$ oder

(β) $n \equiv 0 \bmod 2$ und $c^2 = b^{r_0 \cdot n/2}$.

(C) $G = [a, b, d, e]$ mit (A)(1)–(A)(4), dazu

(6) $n \equiv m \equiv 1 \bmod 2$;

(7) $e^2 = d^2 = (de)^2$; und

(α) $d^2 = 1$ oder

(β) $d^4 = 1$, ferner

(6a) $n \not\equiv 0 \bmod 3$, $m \equiv 0 \bmod 3$; und

(1b) $ada^{-1} = e, aea^{-1} = de, bd = db, be = eb$.

(D) Genau wie (C), aber statt (6a) nun (6b) und statt (1b) nun (1c):

(6b) $n \equiv 0 \bmod 3$;

(1c) $ad = da, ae = ea, bdb^{-1} = e, beb^{-1} = de$.

(E) $G = [a, b, c, d, e]$ wie in (C), zusätzlich

(7a) $c^2 = d, (ce)^2 = 1$;

(1a) $cac^{-1} = a^f, cbc^{-1} = b^f$;

(5) $f^2 \equiv 1 \bmod m, f \equiv 1 \bmod n$;

(5a) $f \equiv -1 \bmod 3$.

(A) umfaßt genau die (im Sinn von Zassenhaus) metazyklischen Gruppen, das sind die Gruppen, bei denen Kommutator- und Faktorkommutatorgruppe zyklisch sind. Statt [a], das Erzeugnis von Kommutator und Zentrum, zu verwenden, ist es von Nutzen, bei der Erzeugung von der Kommutatorgruppe $[g]$ auszugehen. Dann gewinnt (A) die Gestalt

(A′) $$G = [g, h]$$

mit $g^M = h^N = 1$, $hgh^{-1} = g^R$, wobei die nichtnegativen ganzen Zahlen M, N, R den folgenden Bedingungen genügen müssen:

$$\mathrm{ggT}\{M, N(R-1)\} = 1, R^N \equiv 1 \bmod M.$$

(ggT ist der größte gemeinsame Teiler.)

M, N sind dann dem Isomorphietyp von G invariant zugeordnet, während die Klasse R mod M von der Wahl von g, h abhängt. Invariant ist aber die von R in der Gruppe der primen Restklassen mod M erzeugte Untergruppe. Ist deren Ordnung L, und $N = LS$, so ist S die Ordnung des Zentrums. Wir zitieren weiter Suzuki [7, Theorem E]: In einer nicht auflösbaren Gruppe sind genau dann alle abelschen Untergruppen zyklisch, wenn sie isomorph zu einer der unter (a) und (b) genannten Gruppe ist (SL bedeutet wie üblich spezielle lineare Gruppe).

(a) $\mathrm{SL}(2, p) \times G$, G metazyklisch, d.h. wie in (A'), dazu

$$\mathrm{ggT}\{|\,\mathrm{SL}(2, p)|, |\,G\,|\} = 1$$

und p ungerade Primzahl.

(b) $[\mathrm{SL}(2, p) \times G, c]$ Erweiterung vom Grad 2 einer der in (a) genannten Gruppen mit zusätzlich

$$c^4 = 1, \qquad cgc^{-1} = g^{-1}, \qquad ch = hc$$

und $cuc^{-1} = \theta(u)$ für alle $u \in \mathrm{SL}(2, p)$. θ ist dabei der Automorphismus von $\mathrm{SL}(2, p)$, der durch Konjugation mit

$$\begin{pmatrix} 0 & -1 \\ \omega & 0 \end{pmatrix}$$

induziert wird; hierin ist ω eine Erzeugende der Multiplikativgruppe des Körpers mit p Elementen. c^2 ist im Zentrum von $\mathrm{SL}(2, p)$ und es ist $c^2 \neq 1$.

Es ist nun unsere Aufgabe, aus dieser Aufstellung die Gruppen mit $k(G) = 0$ auszuwählen. Wir beginnen mit Fall (A).

LEMMA 8. *Sei G metazyklisch, erzeugt wie in* (A'), *und K das Produkt aller Primzahlen, die N teilen. Dann ist $k(G) = 0$ genau dann, wenn $S \equiv 0 \bmod K$ ist.*

Beweis. $S \not\equiv 0 \bmod K$ ist gleichbedeutend damit, daß die maximale Untergruppe quadratfreier Ordnung von $[h]$ im Zentrum von G enthalten ist. Daher gibt es nur eine maximale zyklische Untergruppe quadratfreier Ordnung in G. Da sich diese Eigenschaft auf jede Untergruppe von G vererbt, folgt daraus nach Lemma 4 $k(G) = 0$.

Ist hingegen $S \not\equiv 0 \bmod K$, dan gibt es eine Primzahl p mit $p \mid K$, $p \nmid |\,S\,|$. Es gibt dann auch einen Primteiler q von M, so daß

$$H = [g^{M/q}, h^{N/p}]$$

nicht abelsch ist. (Man beachte, daß $h^{N/p}$ nicht im Zentrum von G ist, und daß L, die Ordnung von R, zu M prim ist.) H enthält genau eine Untergruppe der Ordnung q und q_H konjugierte Untergruppen der Ordnung p. Dies zeigt $\gamma_E{}^H = q \neq 0$. (Es sei noch bemerkt, daß $S \equiv 0 \bmod K$ mit $R^{N/p} \equiv 1 \bmod M$ gleichbedeutend ist.)

LEMMA 9. *$k(\mathrm{SL}(2,p)) = 0$ ist gleichbedeutend mit $p = 2^x + 1$ für eine natürliche Zahl $x \geqslant 1$; d.h. p ist Fermat-Primzahl.*

Beweis. Man bestimmt leicht $\gamma_E{}^G = 0$ für $p = 3$ und kann daher wieterhin $p > 3$ annehmen. Da $\mathrm{SL}(2,p)$ genau ein Element der Ordnung 2 enthält (dieses erzeugt das Zentrum Z) gilt nach Lemma 7: $k(\mathrm{SL}(2,p)) = 0$ ist gleichbedeutend mit $\gamma_E{}^H = 0$ für alle Untergruppen H ungerader Ordnung. Mann kann wegen

$$\mathrm{SL}(2,p)/Z \simeq \mathrm{PSL}(2,p) \qquad \text{und} \qquad H \simeq HZ/Z.$$

H als Untergruppe von $\mathrm{PSL}(2,p)$ annehmen (PSL ist die projektive spezielle lineare Gruppe). Gierster [5] hat alle Untergruppen von $\mathrm{PSL}(2,p)$ bestimmt. Aus seiner Arbeit entnimmt man, daß Untergruppen ungerader Ordnung durch einen inneren Automorphismus in Untergruppen der Gruppe U/Z übergehen, wobei U aus allen Matrizen der Form

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \qquad a \neq 0$$

besteht. U ist metazyklisch mit $M = p$, $N = p - 1$, $S = 2$ als Invarianten und hat dasselbe Zentrum wie $\mathrm{SL}(2,p)$. Eine erneute Anwendung von Lemma 7 zeigt nun, daß $k(\mathrm{SL}(2,p)) = 0$ mit $k(U) = 0$ gleichbedeutend ist. Nach Lemma 8 gilt aber $k(U) = 0$ genau dann, wenn $2 \equiv 0 \bmod K$, also $K = 2$ ist. Es folgt die Behauptung.

LEMMA 10. *Von den im Zassenhausschen Satz genannten Gruppen haben die folgenden keine zyklischen oder verallgemeinerte Quaternionengruppen als 2-Sylowgruppen*: ((Cα), (Dα), (Eα) *und* (Eβ).

Beweis. Im Falle (Cα), (Dα), (Eα) bilden $[d, e]$ Kleinsche Vierergruppen. Im Fall (E) enthält die Untergruppe $[c, d, e]$ der Ordnung 16 zwei verschiedene Elemente der Ordnung 2, z.B. d^2 und ce.

LEMMA 11. *Sei G eine Erweiterung einer Quaternionengruppe mit einer metazyklischen Gruppe H ungerader Ordnung. Dann ist $k(G) = 0$ genau dann, wenn $k(H) = 0$ ist.*

Beweis. Wegen Lemma 7 kommt es nur auf die Untergruppen

ungerader Ordnung an. Diese lassen sich aber nach Halls Sätzen über auflösbare Gruppen (Hall [6]) durch innere Automorphismen in Untergruppen von H überführen. Die Behauptung ist danach evident.

Lemma 11 erledigt die Fälle (Cβ) und (Dβ). (B) enthält Erweiterungen metazyklischer Gruppen mit einer zyklischen Gruppe der Ordnung 2. Sie werden im Lemma 12 betrachtet.

LEMMA 12. *Eine der unter* (B) *genannten Gruppen G mit nichtzyklischer 2-Sylowgruppe hat genau dann $k(G) = 0$, wenn G eine Erzeugung $G = [g, h, u]$ mit $[g, h]$ wie in* (A'), $k([g, h]) = 0$ *und den weiteren definierenden Relationen hat*

$$u^2 = h^{N/2}, \qquad ugu^{-1} = g^f, \qquad uhu^{-1} = h^f,$$

wobei $N \equiv 0 \bmod 4$, $f^2 \equiv 1 \bmod MN$, $R^f \equiv R \bmod M$ *ist.*

Beweis. Ist $k(G) = 0$, so hat unser G eine verallgemeinerte Quaternionengruppe als 2-Sylowgruppe. Daher ist $MN \equiv 0 \bmod 4$, und es muß Fall β vorliegen, was $N \equiv 0 \bmod 2$, also $N \equiv 0 \bmod 4$ nach sich zieht. Das einzige Element der Ordnung 2 in G ist $h^{N/2}$; es folgt $u^2 = h^{N/2}$ für ein geignetes $u \in [g, h]$. u^2 operiert durch Konjugation trivial auf $[g, h]$, daher die erste Kongruenz für 1. $R^f \equiv R \bmod M$ ist gleichbedeutend mit $f \equiv 1 \bmod n$.

Umgekehrt schließt man aus der angegebenen Gestalt von G, daß $k(G) = 0$ ist: u^2 ist das einzige Element der Ordnung 2, und man argumentiert wie im Beweis zu Lemma 11.

LEMMA 13. *Es ist für die in Suzukis Satz angegebenen Gruppen genau dann $k = 0$, wenn zugleich $k(G) = 0$ für die metazyklische Untergruppe G und $k(\mathrm{SL}(2, p)) = 0$ ist.*

Beweis. Fall (a) wird durch Satz 3 erledigt. Im Fall (b) ist c^2 das einzige Element der Ordnung 2, während Untergruppen ungerader Ordnung schon in $G \times \mathrm{SL}(2, p)$ enthalten sein müssen. Dies reduziert nach Lemma 7 die Frage auf den Fall (a). Ausfürlich zusammengestellt erhält man also

SATZ 5. *Eine endliche Gruppe H erfüllt genau dann $k(H) = 0$, wenn sie isomorph zu einer der unter* (I)–(IV) *durch Erzeugende und definierende Relationen angegebenen Gruppen ist*:

(I) $G = [g, h]$, $g^M = h^N = 1$, $hgh^{-1} = g^R$, *wobei die natürlichen Zahlen M, N, R den Nebenbedingungen* $\mathrm{ggT}\{M, N(R-1)\} = 1$ *und* $R^{N/K} \equiv 1 \bmod M$ *genügen. (K ist das Produkt aller Primzahlen, die N teilen.)*

(II) $[G, u]$, G *wie* (I), *dazu* $N \equiv 0 \bmod 4$ *und* $u^2 = h^{N/2}$, $ugu^{-1} = g^f$, $uhu^{-1} = h^f$, *mit* $f^2 \equiv 1 \bmod MN$ *und* $R^f \equiv R \bmod M$.

(III) $[G, d, e]$, G *wie in* (I), *dazu* $M \equiv N \equiv 1 \bmod 2$, $[d, e]$ *Quaternionengruppe mit den üblichen Relationen* $d^4 = 1$, $d^2 = (de)^2 = e^2$, *und entweder*

(i) $N \equiv 0 \bmod 3$ *und* $gd = dg$, $ge = eg$, $hdh^{-1} = e$, $heh^{-1} = de$, *oder*

(ii) $M \equiv 0 \bmod 3$ und $gdg^{-1} = e$, $geg^{-1} = e$, $hd = dh$, $he = eh$.

(IV) $G \times \mathrm{SL}(2, p)$, G *wie in* (I), p *Primzahl der Form* $p = 2^x + 1$ *mit einer ganzen Zahl* $x \geqslant 2$, *ferner* $\mathrm{ggT}\{NM, p(p^2 - 1)\} = 1$.

(V) $[G \times \mathrm{SL}(2, p), c]$, $G \times \mathrm{SL}(2, p)$ *wie in* (IV), *dazu*

$$c^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad cgc^{-1} = g^{-1}, \qquad ch = hc,$$

$cuc^{-1} = \theta(u)$ *für alle* $u \in \mathrm{SL}(2, p)$. θ *ist wie folgt erklärt: Sei* ω *eine Erzeugende der Multiplikativgruppe des Körpers mit* p *Elementen. Dann ist* θ *Automorphismus von* $\mathrm{SL}(2, p)$. *der durch*

$$\theta: \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ -\omega & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \to \begin{pmatrix} 0 & \omega^{-1} \\ -\omega & 0 \end{pmatrix}$$

angegeben ist.

Diese Gruppen lassen sich wie folgt charakterisieren: (I) Metazyklische Gruppen, in denen alle Untergruppen von Primzahlordnung normal sind. (II) Erweiterungen von Gruppen der Art (I) vom Grad 2 mit verallgemeinerten Quaternionengruppen als 2-Sylowgruppen. (III) Erweiterungen von Quaternionengruppen mit Gruppen ungerader Ordnung der Art (I). Die Gruppen (I)–(III) sind auflösbar, die Gruppen (IV) und (V) nicht auflösbar.

REFERENZEN

1. E. ARTIN, Über eine neue Art von L-Reihen, *Hamb. Abh.* (1923), 89–108.
2. E. ARTIN, Linear mappings and the existence of a normal basis, "Volume for Courant's 60th Birthday," pp. 1–5, Interscience, New York, 1948.
3. E. ARTIN, "Galoissche Theorie," *Leipzig*, 1959.
4. R. BRAUER, Beziehungen zwischen den Klassenzahlen von Teilkörpern eines galoisschen Körpers. *Math. Nachrichten* **4** (1951), 158–174.
5. J. GIERSTER, Die Untergruppen der Galois'schen Gruppe der Modulargleichungen für den Fall eines primzahligen Transformationsgrades, *Math. Ann.* **18** (1882), 319–365.

6. PH. HALL, A note on soluble groups, *J. London Math. Soc.* **3** (1928), 98–105.
7. M. SUZUKI, On finite groups with cyclic Sylow subgroups for all odd primes, *Amer. J. Math.* **77** (1955), 657–691.
8. H. ZASSENHAUS, Über endliche Fastkörper, *Hamb. Abh.* **11** (1936), 187–220.
9. H. ZASSENHAUS, "Gruppentheorie," *B. C. Teubner, Leipzig und Berlin,* 1937.