Die endlichen einstufig nichtnilpotenten Gruppen.

Dem Andenken von Tibor Szele gewidmet.

Von LADISLAUS RÉDEI in Szeged.

§. 1. Einleitung.

„Gruppe" soll stets eine endliche Gruppe bedeuten. Isomorphe Gruppen werden oft als gleich angesehen. *Nilpotent* nennen wir eine Gruppe, wenn sie das direkte Produkt ihrer Sylowgruppen ist (einige Verfasser nennen sie spezielle Gruppen). *Einstufig nichtnilpotent* nennen wir jede nichtnilpotente Gruppe mit lauter nilpotenten echten Untergruppen. *Einstufig nichtabelsch* nennen wir jede nichtabelsche Gruppe mit lauter Abelschen echten Untergruppen. Diesen Gruppen ist eine große Bedeutung beizumessen. da jede nichtnilpotente Gruppe bzw. jede nichtabelsche Gruppe mindestens eine einstufig nichtnilpotente bzw. einstufig nichtabelsche Untergruppe enthält.

Die einstufig nichtabelschen Gruppen haben zuerst MILLER und MORENO [2], dann SCHMIDT [6] untersucht, endlich habe ich [3] sie vollständig bestimmt. Unter ihnen waren diejenigen, die nilpotent (also p-Gruppen) sind, schon seit längerem bekannt und werden im folgenden außer Acht bleiben. Die nichtnilpotenten einstufig nichtabelschen Gruppen bilden freilich einen Spezialfall aller einstufig nichtnilpotenten Gruppen.

Die letzteren Gruppen hat zuerst SCHMIDT [6] untersucht, dann hat sie GOLFAND [1] erforscht, jedoch blieben dabei einige Fragen unbeantwortet. Der Zweck meiner Arbeit ist diese Gruppen vollständig anzugeben, was ich wegen ihrer Wichtigkeit für eine dankbare Aufgabe halte.[1])

In einer früheren Arbeit [4] bekam ich mit Anwendung der einstufig nichtabelschen Gruppen, daß mit Ausnahme der Ikosaedergruppe jede nichtzyklische einfache Gruppe von gerader Ordnung mindestens eine nichtabelsche zweitmaximale Untergruppe enthält. Es ist zu hoffen, daß sich auf Grund der Resultate der vorliegenden Arbeit ein entsprechender Satz gewinnen läßt.

---

[1]) Es werde bemerkt, daß der Beweis in der zitierten Arbeit von GOLFAND [1] teils nur skizziert ist. Herr GOLFAND teilte mir in einem freundlichen Briefe mit. daß auf diesen Gegenstand in einer weiteren Publikation zurückzukommen nicht in seiner Absicht liegt.

Es ist klar, daß sich jede einstufig nichtnilpotente Gruppe durch zwei Elemente erzeugen läßt, und zwar sind hierzu irgendzwei nichtvertauschbare Elemente von relativ primer Ordnung geeignet. Wir werden sie in zwei Formen, nämlich sowohl durch zwei Erzeugende als auch durch die Produktregel der Elemente angeben.

Einige durchgängige Bezeichnungen:

p, q verschiedene Primzahlen.

$O(\ldots)$ die Ordnung (d. h. Anzahl der Elemente) einer endlichen Struktur (die bei uns stets eine Gruppe oder ein Körper sein wird).

$o(\ldots)$ die Ordnung eines Gruppenelementes (stets nur in einer multiplikativen Gruppe, die aber auch die Gruppe der von 0 verschiedenen Elemente eines endlichen Körpers sein kann). Insbesondere sei

$$u = o(p(\mathrm{mod}\, q)) \tag{1}$$

die *Ordnung von p mod q*, d. h. die kleinste natürliche Zahl u mit

$$p^u \equiv 1 (\mathrm{mod}\, q). \tag{2}$$

Mit anderen Worten ist u die Ordnung der Restklasse p mod q in der (multiplikativen) Gruppe der aus den zu q primen ganzen Zahlen gebildeten Restklassen mod q.

$\mathfrak{G}', \mathfrak{G}'', \mathfrak{G}'''$ die erste, zweite, dritte Kommutatorgruppe einer Gruppe $\mathfrak{G}$.

1 wird immer das Einselement bezeichnen auch in verschiedenen Strukturen, woraus kein Mißverständnis entstehen wird.

Satz 1. (SCHMIDT [6] und GOLFAND [1].) *Für jede einstufig nichtnilpotente Gruppe $\mathfrak{G}$ ist $O(\mathfrak{G})$ durch genau zwei Primzahlen p, q teilbar. Die Kommutatorgruppe $\mathfrak{G}'$ ist die Einzige normale Sylowgruppe von $\mathfrak{G}$. Stets wähle man die Bezeichnung so, daß diese die p-Sylowgruppe ist. Die q-Sylowgruppen sind zyklisch. Es ist*

$$O(\mathfrak{G}'/\mathfrak{G}'') = p^u \tag{3}$$

(also nach (1) *durch p, q eindeutig bestimmt). Ferner gilt*

$$\mathfrak{G}''' = 1. \tag{4}$$

Dann und nur dann ist $\mathfrak{G}'' = 1$, wenn $\mathfrak{G}$ sogar einstufig nichtabelsch ist. Stets liegt $\mathfrak{G}''$ im Zentrum von $\mathfrak{G}$. Es ist $\mathfrak{G}/\mathfrak{G}'$ eine zyklische q-Gruppe, ferner sind $\mathfrak{G}'/\mathfrak{G}''$, $\mathfrak{G}''$ elementare Abelsche p-Gruppen. $\mathfrak{G}/\mathfrak{G}''$ ist einstufig nichtabelsch.

In den unten folgenden Sätzen werden wir die einstufig nichtnilpotenten Gruppen genau bestimmen. Das wird nur im Besitz der genauen Kenntnis des Spezialfalls der nichtnilpotenten einstufig nichtabelschen Gruppen möglich, weshalb wir zuerst die diesbezüglichen Resultate zusammenstellen werden.

Bevor wir das tun, betrachten wir zunächst eine beliebige einstufig nichtnilpotente Gruppe $\mathfrak{G}$. Dieser sind nach Satz 1 die Primzahlen p, q (in dieser Reihenfolge) eindeutig zugeordnet. Freilich ist dann $\mathfrak{G}$ auch die Ordnung der q-Sylowgruppen von $\mathfrak{G}$ eindeutig zugeordnet, die wir im folgenden stets in der Form q^v $(v \geqq 1)$ annehmen. Hierfür gilt übrigens nach Satz 1 auch

$$O(\mathfrak{G}/\mathfrak{G}') = q^v. \tag{5}$$

Wir nennen die Zahlen p, q^v die *Invarianten der einstufig nichtnilpotenten Gruppe* $\mathfrak{G}$. Diese Invarianten sind in dem Sinne unabhängig, daß es für beliebige p, q^v mindestens ein $\mathfrak{G}$ gibt, und zwar nach den bekannten früheren Resultaten genau ein solches $\mathfrak{G}$, das einstufig nichtabelsch ist (innerhalb letzterer Gruppen sind also die Invarianten p, q^v „charakteristisch"). Es ist sehr auffällig, daß es nach GOLFAND [1] weitere $\mathfrak{G}$ mit den gegebenen Invarianten p, q^v dann und nur dann gibt, wenn u gerade ist; dabei sind aber auch diese Gruppen aus einer unter ihnen leicht ableitbar (s. unten). Hiernach sind die Invarianten p, q^v für unsere Gruppen in allen Fällen in großem Maße ausschlaggebend.

Weitere durchgängige Bezeichnungen:

K der endliche Körper mit

$$O(\mathsf{K}) = p^u. \tag{6}$$

K^* die „Gruppe von K" d. h. die multiplikative Gruppe der von 0 verschiedenen Elemente von K. Dann gilt

$$O(\mathsf{K}^*) = p^u - 1, \tag{7}$$

ferner ist K^* zyklisch.

K_0 der Primkörper von K. Die Elemente von K_0 bezeichnen wir üblicherweise mit den ganzen rationalen Zahlen, die nur mod p in Betracht kommen.

ω ein festgewähltes Element q-ter Ordnung von K^*:

$$o(\omega) = q \qquad (\omega \in \mathsf{K}). \tag{8}$$

Wegen (1) ist ω vom u-ten Grade, d. h. ein erzeugendes Element von K:

$$\mathsf{K} = \mathsf{K}_0(\omega). \tag{9}$$

Satz 2. (RÉDEI [3].) *Zu beliebigen Invarianten p, q^v gehört eine einzige einstufig nichtabelsche Gruppe $\mathfrak{G}$. Für diese gilt*

$$O(\mathfrak{G}) = p^u q^v. \tag{10}$$

Es lassen sich die Elemente der p-Sylowgruppe (d. h. der Kommutatorgruppe $\mathfrak{G}'$) von $\mathfrak{G}$ mit $P_\alpha (\alpha \in \mathsf{K}, P_0 = 1)$ und ein Element q^v-ter Ordnung von $\mathfrak{G}$ mit Q bezeichnen so, daß in $\mathfrak{G}$ das Produkt zweier beliebiger Elemente sich nach der Regel

$$P_\alpha Q^a \cdot P_\beta Q^b = P_{\alpha+\omega^a\beta} Q^{a+b} \qquad (\alpha, \beta \in \mathsf{K};\ a, b = 0, \ldots, q^v - 1) \tag{11}$$

berechnet. (Aus (11) *folgt* $P_\alpha P_\beta = P_{\alpha+\beta}$, $P_\alpha^p = P_{p\alpha} = P_0 = 1$, *also daß* $\mathfrak{S}'$ *eine elementare Abelsche p-Gruppe ist. Aus* (8) *und* (11) *folgt, daß durch* Q^q *das Zentrum erzeugt wird. Es folgt aus dem Satz auch, daß zu den verschiedenen* ω *lauter isomorphe* $\mathfrak{S}$ *gehören.)*

Wohl ist dieser Satz von unübertreffbarer Eleganz, doch ist oft (so auch zu unseren späteren Zwecken) nützlich, daß man die darin beschriebene Gruppe auch in anderer Form (nämlich mit Hilfe von zwei Erzeugenden) angibt.

Wir schicken noch die folgenden *durchgängigen Bezeichnungen* voran:

$\psi(x)$ das ω zugehörige (irreduzible) Hauptpolynom im Polynomring $K_0[x]$. (Unter einem Hauptpolynom verstehen wir im allgemeinen ein Polynom mit dem Anfangskoeffizienten 1.) Wegen (6) und (9) ist $\psi(x)$ vom u-ten Grade. Wir setzen

$$\psi(x) = x^u + e_{u-1}x^{u-1} + \cdots + e_0 = \sum_{i=-\infty}^{\infty} e_i x^i \tag{12}$$
$$(e_u = 1; \quad e_i = 0 \quad \text{für} \quad i < 0 \quad \text{oder} \quad i > u),$$

wobei die e_i ganze Zahlen sind, die nur mod p in Betracht kommen. Wir wählen sie stets so, daß

$$0 \leqq e_i \leqq p-1 \qquad (i = 0, \ldots, u-1) \tag{13}$$

gilt. Da nach der Definition

$$\psi(\omega) = 0 \tag{14}$$

ist, so folgt aus (8)

$$\psi(x) \Big| \frac{x^q - 1}{x - 1} \quad (\text{in } K_0[x]). \tag{15}$$

Freilich läßt sich $\psi(x)$ auch als ein mod p irreduzibles Hauptpolynom und Teiler mod p der rechten Seite von (15) definieren. (Durch die den sämtlichen ω zugehörigen $\psi(x)$ werden nämlich alle möglichen Fälle erschöpft.)

Satz. 2′. (RÉDEI [3].) *Die im Satz 2 beschriebene Gruppe* $\mathfrak{S}$ *läßt sich auch durch die Gleichungen*

$$A_0^p = \cdots A_{u-1}^p = 1, \tag{16}$$

$$Q^{q^v} = 1, \tag{17}$$

$$A_i A_k = A_k A_i \qquad (0 \leqq i < k \leqq u-1), \tag{18}$$

$$Q A_i Q^{-1} = A_{i+1} \qquad (0 \leqq i \leqq u-2), \tag{19}$$

$$Q A_{u-1} Q^{-1} = A_0^{-e_0} \cdots A_{u-1}^{-e_{u-1}} \tag{20}$$

definieren. Und zwar kann der Übergang von der einen zur anderen Darstellung von $\mathfrak{S}$ *durch*

$$P_{\omega^i} = A_i \qquad (i = 0, \ldots, u-1) \tag{21}$$

vermittelt werden. (Man sieht aus (16) *bis* (20), *daß* A_0, Q *Erzeugende von* $\mathfrak{S}$ *sind.)*

Mit $\{\ldots\}$ bezeichnen wir die durch die eingeklammerten Elemente erzeugte Gruppe.

Satz 3. *Zu den Invarianten* p, q^v *gehört außer der im Satz* 2 *angegebenen Gruppe dann und nur dann mindestens eine weitere einstufig nichtnilpotente Gruppe* $\mathfrak{S}$, *wenn* $2|u$ *d. h.*

$$u = 2t \qquad (t \text{ ganz}) \tag{22}$$

ist. Unter diesen $\mathfrak{S}$ *gibt es ein einziges mit der maximalen Ordnung*

$$O(\mathfrak{S}) = p^{u+t}q^v \left(= p^{\frac{3u}{2}} q^v = p^{3t} q^v\right). \tag{23}$$

Dieses $\mathfrak{S}$ *läßt sich durch die Gleichungen*

$$A_0^p = \cdots = A_{u-1}^p = C \tag{24}$$

$$B_1^p = \cdots = B_{u-1}^p = 1, \tag{25}$$

$$Q^{q^v} = 1, \tag{26}$$

$$B_i = \prod_{k=1}^{i-1} B_k^{e_{i+k}-e_{i-k}} \qquad (t+1 \leqq i \leqq u-1), \tag{27}$$

$$A_k A_i = A_i A_k B_{k-i} \qquad (0 \leqq i < k \leqq u-1), \tag{28}$$

$$Q A_i Q^{-1} = A_{i+1} \qquad (0 \leqq i \leqq u-2), \tag{29}$$

$$Q A_{u-1} Q^{-1} = A_0^{-e_0} \cdots A_{u-1}^{-e_{u-1}}, \tag{30}$$

$$C = 1 \text{ (für } p \neq 2) \quad \text{bzw.} \quad C = B_1^{e_t - 1} B_2^{e_t - 2} \; B_t^{e_0} \text{ (für } p = 2) \tag{31}$$

und durch die Zusatzbedingung definieren, daß alle B_i *ins Zentrum gehören. Die Faktorgruppen von diesem* $\mathfrak{S}$ *nach den Untergruppen von* $\{B_1, \ldots, B_t\}$ *sind bis auf Isomorphie die zu den Invarianten* p, q^v *gehörenden sämtlichen einstufig nichtnilpotenten Gruppen. (Für das obige* $\mathfrak{S}$ *mit* (23) *folgt trivial* $\mathfrak{S} = \{A_0, Q\}$, $\mathfrak{S}' = \{A_0, \ldots, A_{u-1}\}$ *mit* $O(\mathfrak{S}') = p^{u+t}$, $\mathfrak{S}'' = \{B_1, \ldots, B_t\}$ *mit* $O(\mathfrak{S}'') = p^t$, *ferner enthält* $\mathfrak{S}'$ *dann und nur dann Elemente von der Ordnung* p^2, *wenn* $p = 2$ *ist.*)

Endlich wollen wir für die im Satz 3 betrachtete Gruppe $\mathfrak{S}$ mit (23) auch noch die Produktregel der Elemente explizit angeben, die allerdings etwas kompliziert aussieht.

Zu diesem Zweck führen wir noch eine *durchgängige Bezeichnung* ein. Und zwar ordnen wir jedem $\alpha (\in \mathsf{K})$ auf Grund von (6), (9) die ganzen Zahlen $(\alpha)_i$ $(i = 0, \pm 1, \ldots)$ eindeutig durch

$$\alpha = (\alpha)_{u-1}\omega^{u-1} + \cdots + (\alpha)_1\omega + (\alpha)_0 = \sum_{i=-\infty}^{\infty} (\alpha)_i \omega^i$$
$$(0 \leqq (\alpha)_i \leqq p-1;\ (\alpha)_i = 0 \text{ für } i < 0 \text{ oder } i \geqq u). \tag{32}$$

Man bemerke, daß dann wegen (12), (14) insbesondere

$$e_i = -(\omega^u)_i \qquad (0 \leqq i \leqq u-1) \tag{33}$$

gilt.

Satz 3'. *In der im Satz* 3 *definierten Gruppe* $\mathfrak{G}$ *mit der (maximalen) Ordnung* (23) *lassen sich passende Elemente* P_α $(\alpha \in \mathsf{K}, P_0 = 1)$ *angeben so, daß die*

$$P_\alpha Q^a \qquad (\alpha \in \mathsf{K};\quad a = 0, \ldots, q^v - 1) \tag{34}$$

ein volles Representantensystem von $\mathfrak{G}$ *nach der zentralen Untergruppe* $\mathfrak{G}'' = \{B_1, \ldots, B_t\}$ *bildet und für das Produkt dieser Representanten im Fall* $p \neq 2$ *die Regel*

$$P_\alpha Q^a \cdot P_\beta Q^b = \tag{35}$$
$$= P_{\alpha+\omega^a\beta} Q^{a+b} \prod_{0 \leqq i < k \leqq u-1} \left(B_{k-i}^{(\alpha)_k (\omega^a \beta)_i} \prod_{r=0}^{a-1} B_{k-i}^{-e_i (\omega^r \beta)_{k-1} (\omega^r \beta)_{u-1} + e_i e_k \binom{(\omega^r \beta)_{u-1}}{2}} \right)$$

gilt. Im Fall $p = 2$ *ist rechts (das letzte Glied im Exponenten des letzten Faktors wegen seines Verschwindens zu streichen und) der Faktor*

$$\prod_{i=0}^{u-1} C^{(\alpha)_i (\omega^a \beta)_i} \prod_{i=1}^{u-1} \prod_{r=0}^{a-1} C^{e_i (\omega^r \beta)_{i-1} (\omega^r \beta)_{u-1}} \tag{36}$$

hinzuzufügen.

Zur Bequemlichkeit des Lesers werden wir die Sätze 1, 3, 3' vollständig beweisen, obwohl Satz 1 in anderer Zusammenstellung in der Arbeit von GOLFAND [1] enthalten ist. Ein Teil der hierzu führenden Schlüsse rührt von SCHMIDT [6] her (vgl. auch GOLFAND [1]), jedoch werden wir diesen Teil des Beweises etwas leichter gestalten können. Für die Sätze 2, 2' geben wir keinen vollständigen Beweis, da diese Sätze auch schon in unserer Arbeit [3] zu finden sind.

§ 2. Beweis der Auflösbarkeit der einstufig nichtnilpotenten Gruppen.

Zwei Untergruppen einer Gruppe nennen wir fremd, wenn sie nur das Einselement gemeinsam haben.

Lemma 1. *Ist eine einstufig nichtnilpotente Gruppe* $\mathfrak{G}$ *einfach und sind* $\mathfrak{H}_1, \mathfrak{H}_2$ *zwei echte Untergruppen von ihr, von denen* $\mathfrak{H}_1$ *maximal ist und* $\mathfrak{H}_2$ *nicht enthält, so sind* $\mathfrak{H}_1, \mathfrak{H}_2$ *fremd.*

Denn nehmen wir an, daß für den Durchschnitt $\mathfrak{D} = \mathfrak{H}_1 \cap \mathfrak{H}_2 (\neq \mathfrak{H}_1, \mathfrak{H}_2)$ gegen die Behauptung $\mathfrak{D} \neq 1$ gilt. Da $\mathfrak{H}_1, \mathfrak{H}_2$ nilpotent sind, so hat $\mathfrak{D}$ in beiden je einen Normalisator größer als $\mathfrak{D}$. Bezeichnet also $\mathfrak{H}_3$ den Normalisator

von $\mathfrak{D}$ in $\mathfrak{G}$, so sind $\mathfrak{H}_1 \cap \mathfrak{H}_3$, $\mathfrak{H}_2 \cap \mathfrak{H}_3$ größer als $\mathfrak{D}$. Wegen des letzteren ist $\mathfrak{H}_3$ keine Untergruppe von $\mathfrak{H}_1$. Wegen der Einfachheit von $\mathfrak{G}$ gilt auch $\mathfrak{H}_3 \neq \mathfrak{G}$. Wir haben gewonnen, daß auch $\mathfrak{H}_3$ an Stelle von $\mathfrak{H}_2$ den Voraussetzungen vom Lemma 1 genügt. Da dabei $\mathfrak{H}_1 \cap \mathfrak{H}_3$ größer als $\mathfrak{H}_1 \cap \mathfrak{H}_2$ ist, so kommen wir mit wiederholter Anwendung zu Untergruppen $\mathfrak{H}_2, \mathfrak{H}_3, \ldots$, die mit $\mathfrak{H}_1$ einen ständig zunehmenden Durchschnitt haben. Dieser Widerspruch beweist Lemma 1.

Lemma 2. *Ist die einstufig nichtnilpotente Gruppe $\mathfrak{G}$ einfach und $\mathfrak{H}$ eine maximale Untergruppe von ihr, so sind Ordnung und Index von $\mathfrak{H}$ zueinander prim.*

Im anderen Falle hätte $\mathfrak{H}$ eine Sylowgruppe $\mathfrak{P}_1$, die in einer Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ echt enthalten ist. Die Anwendung vom Lemma 1 ergibt, daß $\mathfrak{H}$, $\mathfrak{P}$ fremd sind. Dieser Widerspruch beweist Lemma 2.

Hilfssatz 1. *Jede einstufig nichtnilpotente Gruppe $\mathfrak{G}$ ist nichteinfach.*

Denn nehmen wir an, daß $\mathfrak{G}$ einfach ist. Wir zeigen vor allem, daß $\mathfrak{G}$ zwei maximale Untergruppen enthält, die nicht konjugiert sind. Zu diesem Zweck nehmen wir eine maximale Untergruppe $\mathfrak{H}_1$ von $\mathfrak{G}$. Wegen Lemma 2 gibt es eine Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$, wofür $O(\mathfrak{H}_1), O(\mathfrak{P})$ relativ prim sind. Folglich bildet eine $\mathfrak{P}$ enthaltende maximale Untergruppe $\mathfrak{H}_2$ mit $\mathfrak{H}_1$ zusammen ein gewünschtes Untergruppenpaar. Bezeichne $r_i (i = 1, 2)$ den Index von $\mathfrak{H}_i$. Wegen der Einfachheit von $\mathfrak{G}$ bilden die Konjugierten von $\mathfrak{H}_1, \mathfrak{H}_2$ insgesamt $r_1 + r_2$ verschiedene maximale Untergruppen von $\mathfrak{G}$. Diese sind nach Lemma 1 paarweise fremd, weshalb sie

$$\sum_{i=1}^{2} (O(\mathfrak{G}) - r_i)$$

verschiedene Elemente ($\neq 1$) enthalten. Folglich ist diese Summe kleiner als $O(\mathfrak{G})$, d. h.

$$O(\mathfrak{G}) < r_1 + r_2.$$

Da aber eine natürliche Zahl nie durch die Summe von zwei echten Teilern übertroffen werden kann, so ist Hilfssatz 1 durch den erhaltenen Widerspruch bewiesen.

Hilfssatz 2. *Jede einstufig nichtnilpotente Gruppe $\mathfrak{G}$ ist auflösbar.*

Denn bezeichne $\mathfrak{N} (\neq \mathfrak{G})$ eine maximale normale Untergruppe von $\mathfrak{G}$. Die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ ist einfach und hat lauter nilpotente echte Untergruppen, ist also wegen Hilfssatz 1 gewiß nilpotent. Auch $\mathfrak{N}$ ist nilpotent, folglich ist $\mathfrak{G}$ auflösbar.

§ 3. Die Sylowgruppen der einstufig nichtnilpotenten Gruppen.

Hilfssatz 3. *Für jede einstufig nichtnilpotente Gruppe $\mathfrak{G}$ ist $O(\mathfrak{G})$ durch genau zwei verschiedene Primzahlen p, q teilbar. Bei passender Bezeichnung ist die p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ normal. Dann sind die q-Sylowgruppen zyklisch und nicht normal. Es werde eine der q-Sylowgruppen und ein erzeugendes Element von ihr mit $\mathfrak{Q}$ bzw. Q bezeichnet (also $\mathfrak{Q}=\{Q\}$). Der Durchschnitt aller q-Sylowgruppen ist $\{Q^q\}$. Diese Untergruppe und die Kommutatorgruppe $\mathfrak{P}'$ von $\mathfrak{P}$ liegen im Zentrum von $\mathfrak{G}$. Die Faktorgruppe $\mathfrak{G}/\mathfrak{P}'$ ist einstufig nichtabelsch.*

Denn nehmen wir auf Grund vom Hilfssatz 2 eine normale Untergruppe $\mathfrak{N}$ von $\mathfrak{G}$ mit einem Primzahlindex q in $\mathfrak{G}$. Da $\mathfrak{N}$ nilpotent ist, so gilt eine direkte Zerlegung

$$\mathfrak{N}=\mathfrak{P}\times\mathfrak{P}_1\times\cdots\times\mathfrak{P}_r\times\mathfrak{Q}_0, \tag{37}$$

wobei $\mathfrak{Q}_0$ die q-Sylowgruppe von $\mathfrak{N}$ ist und die übrigen Faktoren lauter Sylowgruppen von $\mathfrak{G}$ sind. Bezeichne $\mathfrak{Q}$ eine q-Sylowgruppe von $\mathfrak{G}$ über $\mathfrak{Q}_0$. Da $\mathfrak{G}$ nicht nilpotent ist, so darf angenommen werden, daß $\mathfrak{Q}$ mit $\mathfrak{P}$ nicht elementweise vertauschbar ist. Da $\mathfrak{P}$ charakteristisch in $\mathfrak{N}$ also normal in $\mathfrak{G}$ ist, so ist $\mathfrak{P}\mathfrak{Q}$ eine Untergruppe von $\mathfrak{G}$. Da sie nichtnilpotent ist, so muß

$$\mathfrak{G}=\mathfrak{P}\mathfrak{Q} \tag{38}$$

gelten. Dabei kann $\mathfrak{Q}$ nicht normal in $\mathfrak{G}$ sein, denn dann wäre $\mathfrak{G}$ das direkte Produkt von $\mathfrak{P}$ und $\mathfrak{Q}$, was unmöglich ist.

$\mathfrak{Q}$ muß zyklisch sein, denn sonst hätte $\mathfrak{Q}$ zwei echte Untergruppen $\mathfrak{Q}_1, \mathfrak{Q}_2$ mit $\mathfrak{Q}=\{\mathfrak{Q}_1, \mathfrak{Q}_2\}$. Dann wären die echten Untergruppen $\mathfrak{P}\mathfrak{Q}_1, \mathfrak{P}\mathfrak{Q}_2$ von $\mathfrak{G}$ also auch $\mathfrak{G}$ nilpotent, was aber falsch ist.

Für das erzeugende Element Q von $\mathfrak{Q}$ gilt $Q^q\in\mathfrak{Q}_0$, also $\mathfrak{Q}_0=\{Q^q\}$. Ferner reduziert sich (37) nach obigem auf $\mathfrak{N}=\mathfrak{P}\times\mathfrak{Q}_0$, weshalb $\mathfrak{Q}_0$ im Zentrum von $\mathfrak{G}$ liegt. Hieraus folgt auch, daß $\mathfrak{Q}_0$ in allen q-Sylowgruppen von $\mathfrak{G}$ enthalten, also ihr Durchschnitt ist.

Da $\mathfrak{P}'$ charakteristisch in $\mathfrak{P}$ also normal in $\mathfrak{G}$ ist, ferner $\mathfrak{P}'\subset\mathfrak{G}'$ gilt, so ist $\mathfrak{P}'\mathfrak{Q}$ eine echte also nilpotente Untergruppe von $\mathfrak{G}$. Hiernach ist $\mathfrak{P}'$ elementweise mit $\mathfrak{Q}$ vertauschbar. Dabei kann $\mathfrak{Q}$ jede q-Sylowgruppe von $\mathfrak{G}$ sein. Um also zu beweisen, daß $\mathfrak{P}'$ im Zentrum von $\mathfrak{G}$ liegt, genügt es zu zeigen, daß die durch alle q-Sylowgruppen von $\mathfrak{G}$ erzeugte Gruppe $\mathfrak{H}$ gleich $\mathfrak{G}$ ist. Das ist aber klar, denn die q-Sylowgruppen von $\mathfrak{G}$ sind solche in $\mathfrak{H}$, weshalb $\mathfrak{H}$ nicht nilpotent also gleich $\mathfrak{G}$ ist.

Zum Beweis der letzten Behauptung vom Hilfssatz 3 schicken wir die Bemerkung voran, daß eine einstufig nichtnilpotente Gruppe dann und nur dann einstufig nichtabelsch ist, wenn ihre Sylowgruppen Abelsch sind. Da nun $\mathfrak{P}/\mathfrak{P}'$ Abelsch ist, so hat $\mathfrak{G}/\mathfrak{P}'$ lauter Abelsche Sylowgruppen. Es genügt also zu zeigen, daß $\mathfrak{G}/\mathfrak{P}'$ einstufig nichtnilpotent ist. Wenn das falsch ist, so

ist $\mathfrak{G}/\mathfrak{P}'$ sogar Abelsch. Hieraus folgt $\mathfrak{G}' \subseteq \mathfrak{P}'$ also $\mathfrak{G}' = \mathfrak{P}'$. Wir nehmen aus $\mathfrak{P}$ ein mit Q nichtvertauschbares Element P. Dann gilt

$$PQP^{-1} = KQ$$

mit einem Element $K(\neq 1)$ von $\mathfrak{P}'$, das also im Zentrum von $\mathfrak{G}$ liegt. Es folgt

$$PQ^qP^{-1} = K^qQ^q.$$

Da aber auch Q^q im Zentrum von $\mathfrak{G}$ liegt, so folgt $K^q = 1$. Wegen $K \in \mathfrak{P}'$ ergibt dies $K = 1$. Mit diesem Wiederspruch haben wir den Beweis vom Hilfssatz 3 beendet.

§ 4. Beweis der Sätze 1, 3, 3'.

Im Besitz vom Hilfssatz 3 würde der Beweis der Sätze 2, 2' keine großen Schwierigkeiten machen, jedoch wollen wir uns damit nicht beschäftigen sondern berufen wir uns diesbezüglich, wie schon gesagt, auf unsere Arbeit [3]. Unsere Aufgabe bleibt dann die Sätze 1, 3, 3' auf Grund vom Hilfssatz 3 und der Sätze 2, 2' zu beweisen. Dieser Beweis wird mit vielen ziemlich mühsamen Rechnungen verbunden sein.

Wir bezeichnen mit $\mathfrak{G}$ zunächst eine beliebige einstufig nichtnilpotente Gruppe. Für diese übernehmen wir alle Bezeichnungen aus Hilfssatz 3.

Nach dem Schluß vom Hilfssatz 3 ist $\mathfrak{G}/\mathfrak{P}'$ einstufig nichtabelsch. Hieraus und aus Satz 2' (angewendet auf $\mathfrak{G}/\mathfrak{P}'$) folgt die Existenz eines mit Q nichtvertauschbaren Elementes A_0 in $\mathfrak{P}$ aber außerhalb von $\mathfrak{P}'$ derart, daß für die Elemente

$$A_i = Q^i A_0 Q^{-i} \qquad (0 \leqq i \leqq u-1) \tag{39}$$

die Beziehungen

$$A_0^p, \ldots, A_{u-1}^p \in \mathfrak{P}', \tag{40}$$

$$A_iA_k \equiv A_kA_i \pmod{\mathfrak{P}'} \qquad (0 \leqq i < k \leqq u-1), \tag{41}$$

$$QA_{u-1}Q^{-1} \equiv A_0^{-e_0} \cdots A_{u-1}^{-e_{u-1}} \pmod{\mathfrak{P}'} \tag{42}$$

gelten. Selbst für Q gilt nach Hilfssatz 3

$$o(Q) = q^v \tag{43}$$

mit einem $v(\geqq 1)$.

Da $o(A_0)$, $o(Q)$ je eine Potenz von p bzw. q ist und A_0, Q nicht vertauschbar sind, so gilt

$$\mathfrak{G} = \{A_0, Q\}. \tag{44}$$

Wir zeigen, daß nach passender Wahl von A_0 die Kongruenz (42) in die Gleichung

$$QA_{u-1}Q^{-1} = A_0^{-e_0} \cdots A_{u-1}^{-e_{u-1}} \tag{45}$$

übergeht. Zu diesem Zweck setzen wir

$$A_0^* = A_0 X$$

mit einem bald näher zu bestimmenden X ($\in \mathfrak{P}'$). Es gilt $A_0^* \equiv A_0 \pmod{\mathfrak{P}'}$, weshalb A_0^* ein mit A_0 gleichberechtigtes Element ist. Entsprechend (39) setzen wir

$$A_i^* = Q^i A_0^* Q^{-i} \qquad (0 \leqq i \leqq u-1).$$

Da nach Hilfssatz 3 X im Zentrum von $\mathfrak{G}$ liegt. so gilt einfach

$$A_i^* = A_i X \qquad (0 \leqq i \leqq u-1).$$

Nun folgt aus (42)

$$Q A_{u-1} Q^{-1} = A_0^{-e_0} \cdots A_{u-1}^{-e_{u-1}} Y$$

mit einem $Y(\in \mathfrak{P}')$. Wird hier $A_i = A_i^* X^{-1}$ eingesetzt, so entsteht

$$Q A_{u-1}^* Q^{-1} = A_0^{*-e_0} \cdots A_{u-1}^{*-e_{u-1}} X^{e_0+\cdots+e_{u-1}+1} Y.$$

Der Exponent von X ist nach (12) gleich $\psi(1)$ also zu p prim. Folglich kann man für X eine passende Potenz von Y wählen derart, daß die letzte Gleichung die Form (45) hat (mit A_i^* statt A_i). Hiernach läßt sich (45) in der Tat annehmen.

Wir führen die Kommutatoren

$$B_i = A_i A_0 A_i^{-1} A_0^{-1} \qquad (1 \leqq i \leqq u-1) \tag{46}$$

ein. Außerdem setzen wir bequemlichkeitshalber

$$B_0 = 1, \; B_{-i} = B_i^{-1} \qquad (1 \leqq i \leqq u-1). \tag{47}$$

Alle B_i liegen in $\mathfrak{P}'$ also im Zentrum von $\mathfrak{G}$.

Aus (46), (47) folgen

$$A_i A_0 A_i^{-1} = B_i A_0, \quad A_0 A_i A_0^{-1} = B_{-i} A_i \qquad (0 \leqq i \leqq u-1).$$

Also gilt

$$A_k A_i A_k^{-1} = B_{k-i} A_i \qquad (0 \leqq i, k \leqq u-1)$$

zunächst für $i = k = 0$, dann aber wegen (39) allgemein. Noch allgemeiner folgt hieraus

$$A_k^y A_i^x A_k^{-y} = B_{k-i}^{xy} A_i^x \qquad (0 \leqq i, k \leqq u-1) \tag{48}$$

für beliebige ganze Zahlen x, y.

Wegen (40) liegen alle A_k^p im Zentrum von $\mathfrak{G}$. Somit folgt aus (48)

$$B_i^p = 1 \qquad (1 \leqq i \leqq u-1). \tag{49}$$

Aus (39), (44), (45) ergibt sich $\mathfrak{G} = \{A_0, \ldots, A_{u-1}\}\{Q\}$. Da der erste Faktor in $\mathfrak{P}$ enthalten ist, so folgt

$$\mathfrak{P} = \{A_0, \ldots, A_{u-1}\}. \tag{50}$$

Hieraus und aus (47), (48) folgt

$$\mathfrak{P}' = \{B_1, \ldots, B_{u-1}\}. \tag{51}$$

Wir weisen jetzt Abhängigkeiten zwischen den $B_1, \ldots, B_{u-1}$ aus. Wegen (48) gilt

$$A_{u-1} A_{i-1} A_{u-1}^{-1} = B_{u-i} A_{i-1} \qquad (1 \leqq i \leqq u-1).$$

Nach Transformation mit Q ergibt sich wegen (39), (45)

$$A_0^{-e_0} \cdots A_{u-1}^{-e_{u-1}} A_i A_{u-1}^{e_{u-1}} \cdots A_0^{e_0} = B_{u-i} A_i.$$

Die linke Seite entsteht so, daß man A_i der Reihe nach mit $A_k^{-e_k}$ $(k = u-1, u-2, \ldots, 0)$ transformiert. Wegen (48) entsteht also (nach Kürzung mit A_i):

$$\prod_{k=0}^{u-1} B_{k-i}^{-e_k} = B_{u-i},$$

wofür man (vgl. (12)) bequemer

$$\prod_{k=-\infty}^{\infty} B_{k-i}^{-e_k} = 1 \qquad (1 \leqq i \leqq u-1)$$

schreiben kann. Man ersetze k durch $k+i$ und gehe auf das Inverse über:

$$\prod_{k=-\infty}^{\infty} B_k^{e_{k+i}} = 1$$

Dies lautet nach (47) als

$$\prod_{k=1}^{\infty} B_k^{e_{i+k} - e_{i-k}} = 1$$

d. h. (vgl. (12))

$$\prod_{k=1}^{u-1} B_k^{e_{i+k} - e_{i-k}} = 1 \qquad (1 \leqq i \leqq u-1). \tag{52}$$

Hieraus folgern wir jetzt, daß im Fall $2 \nmid u$ notwendig alle B_k gleich 1 sind, d. h. nach (51) $\mathfrak{P}' = 1$, also $\mathfrak{G}$ einstufig nichtabelsch ist, womit die erste Behauptung vom Satz 3 bewiesen sein wird.

Zum Beweis denken wir (52) additiv geschrieben. Dann haben wir ein homogen lineares Gleichungssystem für die $B_1, \ldots, B_u$ mit der Determinante $u-1$-ter Ordnung

$$|e_{i+k} - e_{i-k}| \qquad (i, k = 1, \ldots, u-1). \tag{53}$$

Es genügt zu zeigen, daß diese Determinante im Fall $2 \nmid u$ zu p prim ist, denn das hat wegen (49) zur Folge, daß (52) nur die triviale Lösung $B_1 = \cdots = B_{u-1} = 1$ hat.

Zu unserem Zweck formen wir die Determinante (53) um. Indem wir

$$e_i = (-1)^{u+i} s_{u-i} \qquad (i = 0, \pm 1, \ldots)$$

setzen, so folgt aus (12), (14), daß s_k $(k = 1, \ldots, u)$ das k-te elementar symmetrische Polynom der Konjugierten von ω ist, ferner

$$s_0 = 1 \quad \text{und} \quad s_k = 0 \quad \text{für} \quad k < 0, k > u$$

gelten. Andererseits geht (53) in die Determinante ($u-1$-ter Ordnung)

$$|(-1)^{u+i+k}s_{u-i-k}-(-1)^{u+i-k}s_{u-i+k}|$$

über. Man ersetze i durch $u-i$, wodurch höchstens das Vorzeichen der Determinante geändert wird:

$$|(-1)^{i+k}(s_{i-k}-s_{i+k})|.$$

Hier läßt sich $(-1)^{i+k}$ streichen. So entsteht bis auf das Vorzeichen die Determinante

$$|s_{i+k}-s_{i-k}|.$$

Diese ist nach RÉDEI [5] gleich

$$\prod_{1\leqq i<k\leqq u}(1-\omega_i\omega_k),$$

wobei $\omega_1=\omega, \omega_2, \ldots, \omega_u$ die Konjugierten von ω bezeichnen. Diese stimmen (bis auf die Reihenfolge) mit den Potenzen

$$\omega^p, \omega^{p^2}, \ldots, \omega^{p^u}$$

überein. Wenn wir also zeigen, daß im Fall $2 \nmid u$ stets

$$\omega^{p^i}\omega^{p^k} \neq 1 \qquad (1\leqq i<k\leqq u)$$

gilt, so werden wir unsere Behauptung bewiesen haben.

Die zu beweisende Ungleichung ist wegen (8) gleichbedeutend mit $q \nmid p^i+p^k$ d. h. mit

$$p^{k-i} \not\equiv -1 \pmod q \qquad (1\leqq i<k\leqq u).$$

Da dies im Fall $2 \nmid u$ wegen $1\leqq k-i\leqq u-1$ aus (1) folgt, so ist unsere Behauptung richtig.

Fortan dürfen wir deshalb (22) annehmen. Wegen (8), (12), (14) gilt dann bekanntlich die „Symmetrieeigenschaft"

$$e_{t+i}=e_{t-i} \qquad (i=\pm 1, \pm 2, \ldots). \tag{54}$$

Hieraus folgt, daß (52) für $i=t$ identisch erfüllt ist, auch unterscheiden sich die einem Paar $(i=)\,t+j, t-j$ zugehörigen Fälle unwesentlich. Deshalb genügt es aus (52) nur die Fälle $i=t+1, \ldots, u-1$ beizubehalten. In diesen Fällen hat man das Produkt in (52) nur auf $k=1, \ldots, i$ zu erstrecken, da für die übrigen k wegen (12) der Exponent von B_k in (52) verschwindet. Insbesondere für $k=i$ ist dieser Exponent wegen (12) gleich $-e_0$ d. h. wegen (12), (22), (54) gleich -1. Hiernach reduziert sich (52) auf

$$B_i=\prod_{k=1}^{i-1}B_k^{e_{i+k}-e_{i-k}} \qquad (t+1\leqq i\leqq u-1). \tag{55}$$

Wegen (40) gehört A_0^p ins Zentrum von $\mathfrak{S}$, also folgt aus (39), daß alle A_i^p gleich sind. Wir setzen

$$A_0^p=\cdots=A_{u-1}^p=C(\in\mathfrak{P}') \tag{56}$$

und wollen C berechnen.

Wir schicken folgende Bemerkung voran. In einem aus den $A_0, \ldots, A_{u-1}$ gebildeten Potenzprodukt

$$\ldots A_k^y A_i^x \ldots \qquad (k > i)$$

darf man die angeschriebenen zwei Faktoren vertauschen so, daß man wegen (48) gleichzeitig den Faktor B_{k-i}^{xy} hinzufügt. Diese Regel werden wir ohne Verweis öfters anwenden.

Nach (39), (56) gilt $(QA_{u-1}Q^{-1})^p = C$, also nach (45)

$$C = (A_0^{-e_0} \cdots A_{u-1}^{-e_{u-1}})^p.$$

Hieraus folgt

$$C = A_0^{-pe_0} \cdots A_{u-1}^{-pe_{u-1}} \Big(\prod_{0 \leqq i < k \leqq u-1} B_{k-i}^{e_i e_k} \Big)^{\binom{p}{2}}.$$

Im Fall $p \neq 2$ ist $p \Big| \binom{p}{2}$, also fällt der letzte Faktor wegen (49) heraus. Wird auch (56) berücksichtigt, so entsteht

$$C^{e_0 + \ldots + e_{u-1}+1} = 1.$$

Der Exponent ist nach (12) gleich $\psi(1)$ also (wie schon bemerkt) zu p prim. Wegen $C \in \mathfrak{P}'$, $o(C) | p$ gilt also jetzt $C = 1$. Im Fall $p = 2$ können wir ähnlich verfahren mit dem Unterschied, daß jetzt $\binom{p}{2} = 1$ gilt. Folglich haben wir

$$C = 1 \text{ (für } p \neq 2) \quad \text{bzw.} \quad C = \prod_{0 \leqq i < k \leqq u-1} B_{k-i}^{e_i e_k} \text{ (für } p = 2). \tag{57}$$

Wir beweisen, daß im Fall $p = 2$ (einfacher)

$$C = B_1^{e_{t-1}} B_2^{e_{t-2}} \cdots B_t^{e_0} \qquad (p = 2) \tag{58}$$

gilt. Der Beweis wird umständlich. Wir machen dabei oft aus $B_i^2 = 1$ Gebrauch. Man beachte auch, daß nach (12), (54) und $2 \nmid \psi(1)$ die folgenden gelten: $e_0 = e_u = 1$, $e_{u-i} = e_i$, $e_t = 1$, ferner $e_i = 0$ für $i < 0$ oder $i > u$, endlich ist jedes e_i gleich 0 oder 1.

Nach (57_2) gilt

$$C = \prod_{d=1}^{u-1} \prod_{i=0}^{u-d-1} B_d^{e_i e_{i+d}} = \Big(\prod_{d=1}^{u-1} \prod_{i=0}^{u-d} B_d^{e_i e_{i+d}} \Big) \Big(\prod_{d=1}^{u-1} B_d^{e_d} \Big).$$

Da $e_i e_{i+d}$ bei Ersetzung von i durch $u-d-i$ invariant bleibt, so genügt es, wenn man das zweifache Produkt nur auf die geraden $d = 2k (k = 1, \ldots, t-1)$ und auf $i = \frac{1}{2}(u-d) = t-k$ erstreckt. Wegen $e_{t-k} e_{t+k} = e_{t+k}^2 = e_{t+k}$ gilt also

$$C = \Big(\prod_{k=1}^{t-1} B_{2k}^{e_{t+k}} \Big) \Big(\prod_{d=1}^{u-1} B_d^{e_d} \Big). \tag{59}$$

Wir beweisen jetzt, daß allgemein

$$C=\left(\prod_{d=1}^{s-1}\prod_{i=1}^{d}B_d^{e_{s-i}e_{s-i+d}}\right)\left(\prod_{d=1}^{s-1}\prod_{k=0}^{d}B_d^{e_{t-k}e_{t-k+d}}\right) \qquad (t+1\leqq s\leqq u) \tag{60}$$

gilt.

Dieses zeigen wir zuerst für $s=u$. Rechts fallen dann die Faktoren mit $i<d$ heraus, somit ist die rechte Seite gleich

$$\left(\prod_{d=1}^{u-1}B_d^{e_d}\right)\left(\prod_{d=1}^{u-1}\prod_{k=0}^{d}B_d^{e_{t-k}e_{t-k+d}}\right).$$

Zwei Werte $k, d-k$ von k liefern gleiche Faktoren. Da diese herausfallen, so bleibt nur für die geraden $d=2l(l=1,\ldots,t-1)$ der zu $k=\frac{d}{2}=l$ gehörende Faktor übrig (mit dem Exponenten $e_{t-l}e_{t+l}=e_{t+l}^2=e_{t+l}$):

$$\prod_{d=1}^{u-1}B_d^{e_d}\prod_{l=1}^{t-1}B_{2l}^{e_{t+l}}.$$

Dies stimmt mit (59) überein. Das beweist (60) für $s=u$.

Wir bezeichnen die rechte Seite von (60) einen Augenblick mit C_s. Zum vollständigen Beweis von (60) genügt es $C_{s+1}C_s^{-1}=1$ für $t+1\leqq s\leqq u-1$ zu beweisen. Das heißt wir haben zu zeigen, daß

$$\left(\prod_{d=1}^{s}\prod_{j=1}^{d}B_d^{e_{s+1-j}e_{s+1-j+d}}\right)\left(\prod_{d=1}^{s-1}\prod_{i=1}^{d}B_d^{e_{s-i}e_{s-i+d}}\right)^{-1}\prod_{k=0}^{s}B_s^{e_{t-k}e_{t-k+s}} \quad (t+1\leqq s\leqq u-1)$$

gleich 1 ist. Man führe $j=1+i$ ein $\left(\text{und schreibe }\prod_{i=0}^{d-1}\text{ für }\prod_{j=1}^{d}\right)$. Hierdurch werden die ersten zwei Multiplikanden miteinander gleich. Nach Abtrennung des zu $d=s$ gehörenden Faktors entsteht also

$$\prod_{i=0}^{s-1}B_s^{e_{s-i}e_{s-i+s}}\prod_{d=1}^{s-1}B_d^{e_se_{s+d}e^{-1}_{s-d}e_s}\prod_{k=0}^{s}B_s^{e_{t-k}e_{t-k+s}}$$

Das zweite Produkt ist nach (55) gleich $B_s^{e_s}$. Dies läßt sich in das erste Produkt einschmelzen so, daß man dieses auch auf $i=s$ erstreckt. Nachher darf $s-i$ durch i ersetzt werden. Es genügt das dritte Produkt auf $0\leqq k\leqq t$ zu erstrecken (die übrigen Faktoren sind gleich 1), ferner darf nachher $t-k$ durch k ersetzt werden. So bekommt man:

$$\prod_{i=0}^{s}B_s^{e_ie_{i+s}}\prod_{k=0}^{t}B_s^{e_ke_{k+s}}.$$

Es genügt beide Produkte auf $0\leqq i\leqq u-s$ bzw. $0\leqq k\leqq u-s$ zu erstrecken. Sie sind also miteinander gleich, somit ist ihr Produkt gleich 1. Dies beweist (36).

Wir benötigen (60) nur für $s = t+1$:

$$C = \left(\prod_{d=1}^{t} \prod_{i=1}^{d} B_d^{r^t+1-i\, r^t+1-i+d} \right) \left(\prod_{d=1}^{t} \prod_{k=0}^{d} B_d^{e_t-k\, e_t-k+d} \right).$$

Nach Abtrennung des zu $k = d$ gehörenden Bestandteiles sind die übriggebliebenen zwei Faktoren gleich. Nach Weglassen dieser zwei Faktoren hat man

$$C = \prod_{d=1}^{t} B_d^{e_t-d\, r^t}.$$

Wegen $e_t = 1$ wurde hiermit (58) bewiesen.

Da wegen (44), (39), (45), (50), (43) $\mathfrak{G}' = \mathfrak{P}$ ist, so entnimmt man aus den bisherigen die Richtigkeit vom Satz 1. Auch sieht man, daß die betrachtete Gruppe $\mathfrak{G}$ zu den Invarianten p, q^e gehört und daß in dieser erzeugende Elemente A_i, B_i, C, Q vorhanden sind, für die die Gleichungen (24) bis (31) gelten, außerdem die B_i ins Zentrum von $\mathfrak{G}$ gehören.

Umgekehrt soll jetzt $\mathfrak{G}$ die durch die Gleichungen (24) bis (31) und durch die Zusatzbedingung definierte Gruppe bezeichnen, daß alle B_i ins Zentrum gehören. Aus obigem folgt jedenfalls, daß jede einstufig nichtnilpotente Gruppe, die zu den Invarianten p, q^e gehört, eine Faktorgruppe von $\mathfrak{G}$ sein muß. Die Frage, welche diese Faktorgruppen sind, werden wir später beantworten. Zuerst wollen wir beweisen, daß $\mathfrak{G}$ in der im Satz 3′ beschriebenen Form angebbar ist und für seine Ordnung (23) gilt.

Wir führen die Bezeichnung (vgl. (32))

$$P_\alpha = A_0^{(\alpha)_0} \cdots A_{u-1}^{(\alpha)_{u-1}} \qquad (\alpha \in K) \tag{61}$$

ein. Wir sehen, daß die Gleichungen (24) bis (31) nach Hinzufügung der Gleichungen $B_1 = \cdots = B_t = 1$ eben in die Gleichungen (16) bis (20) übergehen. Hieraus folgt, daß unter den homomorphen Bildern von $\mathfrak{G}$ die (im Satz 2′ d. h.) im Satz 2 beschriebene Gruppe vorkommt. Dies hat zur Folge, daß die P_α lauter verschiedene Elemente von $\mathfrak{G}$ sind. Wir setzen

$$\mathfrak{B} = \{B_1, \ldots, B_t\}. \tag{62}$$

Dieses $\mathfrak{B}$ ist dann eine zentrale Untergruppe von $\mathfrak{G}$. Auch ist nach dem eben gesagten klar, daß sich die Elemente von $\mathfrak{G}$ eindeutig in der Form

$$P_\alpha Q^a B \qquad (\alpha \in K;\ a = 0, \ldots, q^e - 1;\ B \in \mathfrak{B}) \tag{63}$$

schreiben lassen. Es gilt für das nächste die Produktregel für die in der Form (63) angeschriebenen Elemente von $\mathfrak{G}$ aufzustellen.

Da die B in (63) Zentrumelemente sind, so genügt es, wenn wir (35) (für $p = 2$ mit der Ergänzung (36)) beweisen. Zuerst berechnen wir $P_\alpha B_\beta$. Es gilt

$$P_\alpha B_\beta = A_0^{(\alpha)_0} \cdots A_{u-1}^{(\alpha)_{u-1}} A_0^{(\beta)_0} \cdots A_{u-1}^{(\beta)_{u-1}}.$$

Mittels der oben (nach (56)) besprochenen Regel folgt hieraus

$$P_\alpha P_\beta = A_0^{(\alpha)_0+(\beta)_0} \cdots A_{u-1}^{(\alpha)_{u-1}+(\beta)_{u-1}} \prod_{i<k} B_{k-i}^{(\alpha)_k (\beta)_i},$$

wobei (und auch nachher) „$i<k$" statt „$0 \leqq i < k \leqq u-1$" steht. Da

$$(\alpha)_i + (\beta)_i \equiv (\alpha+\beta)_i \pmod p \quad (p \neq 2)$$

bzw.

$$(\alpha)_i + (\beta)_i = (\alpha+\beta)_i + 2(\alpha)_i(\beta)_i \quad (p=2)$$

gelten, so folgt unter Berücksichtigung von (24), (31), (61)

$$P_\alpha B_\beta = P_{\alpha+\beta} C^{(\alpha)_0(\beta)_0+\cdots+(\alpha)_{u-1}(\beta)_{u-1}} \prod_{i<k} B_{k-i}^{(\alpha)_k (\beta)_i}. \tag{64}$$

Dann berechnen wir $QP_\beta Q^{-1}$. Nach (29), (30), (61) gilt

$$QP_\beta Q^{-1} = A_1^{(\beta)_0} \cdots A_{u-1}^{(\beta)_{u-2}} (A_0^{-e_0} \cdots A_{u-1}^{-e_{u-1}})^{(\beta)_{u-1}}. \tag{65}$$

Hier hat der letzte Faktor den Wert:

$$A_0^{-e_0(\beta)_{u-1}} \cdots A_{u-1}^{-e_{u-1}(\beta)_{u-1}} \left(\prod_{i<k} B_{k-i}^{e_i e_k}\right)^{\binom{(\beta)_{u-1}}{2}}. \tag{66}$$

Wir zeigen, daß in (65) und (66) die vor den Klammern stehenden Potenzprodukte den Wert

$$P_{\omega\beta-(\beta)_{u-1}\omega^u} \text{ bzw. } P_{(\beta)_{u-1}\omega^u} \tag{67}$$

haben. Denn nach (32) gilt

$$\omega\beta - (\beta)_{u-1}\omega^u = (\beta)_0\omega + (\beta)_1\omega^2 + \cdots + (\beta)_{u-2}\omega^{u-1}. \tag{68}$$

Ferner gilt nach (33)

$$((\beta)_{u-1}\omega^u)_i \equiv -e_i(\beta)_{u-1} \pmod p \qquad (0 \leqq i \leqq u-1). \tag{69}$$

Dabei gilt diese Kongruenz im Fall $p=2$ sogar als Gleichung. Hieraus folgt mit Rücksicht auf (24), (31), (61) die Richtigkeit der Behauptung über (67). Zur vollständigen Auswertung der rechten Seite von (65) müssen wir noch das Produkt der beiden Elemente in (67) berechnen. Unter nochmaliger Beachtung von (68), (69) erhalten wir für dieses Produkt wegen (64) den Wert

$$P_{\omega\beta} C^{-(e_1(\beta)_0+\cdots+e_{u-1}(\beta)_{u-2})(\beta)_{u-1}} \prod_{i<k} B_{k-i}^{-e_i(\beta)_{k-1}(\beta)_{u-1}}. \tag{70}$$

Da nach (31) stets $C^2=1$ ist, so darf das Vorzeichen im Exponenten von C unterdrückt werden. Die rechte Seite von (65) berechnet sich nunmehr als Produkt des letzten Faktors in (66) und von (70). Also entsteht

$$QP_\beta Q^{-1} = P_{\omega\beta} \prod_{i=1}^{u-1} C^{e_i(\beta)_{i-1}(\beta)_{u-1}} \prod_{i<k} B_{k-i}^{-e_i(\beta)_{k-1}(\beta)_{u-1}+e_i e_k \binom{(\beta)_{u-1}}{2}}. \tag{71}$$

Nunmehr können wir

$$P_\alpha Q^a \cdot P_\beta Q^b \qquad (\alpha, \beta \in K;\ a, b = 0, \ldots, q^v-1)$$

berechnen. Zu diesem Zweck schreiben wir dieses Produkt als

$$P_\alpha (Q^a P_\beta Q^{-a}) Q^{a+b}.$$

Man setze einen Augenblick

$$Q P_{\omega^r \beta} Q^{-1} = P_{\omega^{r+1}\beta} D_r,$$

wobei D_r den Kofaktor von $P_{\omega\beta}$ in (71) für $\omega^r\beta$ statt β bezeichnet. Es gilt dann

$$Q^a P_\beta Q^{-a} = P_{\omega^a \beta} \prod_{r=0}^{a-1} D_r,$$

also

$$P_\alpha Q^a P_\beta Q^b = P_\alpha P_{\omega^a \beta} Q^{a+b} \prod_{r=0}^{a-1} D_r.$$

Wenden wir noch rechts auf das Produkt der ersten zwei Faktoren (64) an und setzen für D_r den gesagten Wert ein, so erhalten wir zunächst für den Fall $p \neq 2$ wegen (31_1) eben die Formel (35). Im Fall $p = 2$ verfärt man ebenso mit dem Unterschied, daß man dann überall auch noch die Potenzen von C zu berücksichtigen hat, die im vorigen Fall unterdrückt werden durften. Man sieht, daß dabei eben der „Korrektionsfaktor" (36) entsteht.

Unsere nächste Absicht ist — wie oben angemeldet — zu beweisen, daß die Ordnung der betrachteten Gruppe $\mathfrak{G}$ durch (23) angegeben ist. Diesen Beweis erbringen wir folgenderweise. Nach (6), (63) gilt

$$O(\mathfrak{G}) = p^u q^v O(\mathfrak{B}).$$

Wegen (62) hängt also die Richtigkeit von (23) nur davon ab, ob die $B_1, \ldots, B_t$ unabhängig sind. Diese Unabhängigkeit können wir so ausweisen, daß wir sie zunächst voraussetzen und beweisen, daß unter dieser Voraussetzung die Elemente (63) auf Grund der Produktregel (35) (die im Fall $p = 2$ mit dem Korrektionsfaktor (36) ergänzt werden soll) eine Gruppe bilden. (Das ist selbstverständlich so gemeint, daß dabei auch vorausgesetzt wird, daß die B_i Zentrumelemente sind und (25), (26), (27), (31) gelten.) Es genügt die Assoziativität auszuweisen, da (63) für $\alpha = 0, a = 0, B = 1$ offenbar das Einselement ist, ferner wegen (35) die Existenz des Linksinversen klar ist. (Im Fall $p = 2$ hat man dabei stets auch den Korrektionsfaktor (36) zu beachten.) Da die B_i Zentrumelemente sind, so genügt es

$$(P_\alpha Q^a P_\beta Q^b) P_\gamma Q^c = P_\alpha Q^a (P_\beta Q^b P_\gamma Q^c) \tag{72}$$
$$(\alpha, \beta, \gamma \in K;\ a, b, c = 0, \ldots, q^v - 1)$$

auszuweisen.

Zunächst betrachten wir den Fall $p \neq 2$. Wir setzen

$$P_\alpha Q^a P_\beta Q^b = P_{\alpha+\omega^a\beta} Q^{a+b} F(\alpha, \beta, a), \tag{73}$$

wobei $F(\alpha, \beta, a)$ den dritten Faktor auf der rechten Seite von (35) bezeichnet. Dieses $F(\alpha, \beta, a)$ ist ein Potenzprodukt aus den B_i, also ein Zentrumelement.

Da ferner (35) nach der Ersetzung $B_i = 1$ $(i = 1, 2, \ldots)$ in (11) übergeht, also (72) wegen Satz 2 nach dieser Ersetzung richtig ist, so haben wir statt (72) nur

(74) $$F(\alpha, \beta, a)\, F(\alpha + \omega^a \beta, \gamma, a+b) = F(\alpha, \beta + \omega^b \gamma, a)\, F(\gamma, \beta, b)$$

auszuweisen. Wir setzen zur Abkürzung

(75) $$f(\alpha, \beta, a) = (\alpha)_k (\omega^a \beta)_i - e_i \sum_{r=0}^{a-1} (\omega^r \beta)_{k-1} (\omega^r \beta)_{u-1} + e_i e_k \sum_{r=0}^{a-1} \binom{(\omega^r \beta)_{u-1}}{2},$$

woraus nach (35)

(76) $$F(\alpha, \beta, a) = \prod_{0 \leqq i < k \leqq u-1} B_{k-i}^{f(\alpha, \beta, a)}$$

folgt. Indem wir

(77) $$f(a) = f(\alpha, \beta, a) + f(\alpha + \omega^a \beta, \gamma, a+b) - f(\alpha, \beta + \omega^b \gamma, a) - f(\beta, \gamma, b)$$

setzen, so läßt sich das zu beweisende (74) wegen (76), (77) in der Form

$$\prod_{0 \leqq i < k \leqq u-1} B_{k-i}^{f(a)} = 1$$

schreiben. Da aber nach (77) $f(0) = 0$ gilt, so genügt es, wenn wir

(78) $$\prod_{0 \leqq i < k \leqq u-1} B_{k-i}^{f(a+1) - f(a)} = 1 \qquad (a = 0, 1, \ldots)$$

zeigen. Zu diesem Zweck berechnen wir (vgl. (75)) den von e_i, e_k freien, dann den mit e_i, endlich den mit $e_i e_k$ multiplizierten Bestandteil von $f(a)$ mod p. (Für das spätere bemerken wir, daß die hier folgende Berechnung für die ersten zwei Bestandteile auch im Fall $p = 2$ richtig ist.)

Der erste dieser drei Bestandteile ist

$$(\alpha)_k (\omega^a \beta)_i + (\alpha + \omega^a \beta)_k (\omega^{a+b} \gamma)_i - (\alpha)_k (\omega^a \beta + \omega^{a+b} \gamma)_i - (\beta)_k (\omega^b \gamma)_i.$$

Da im allgemeinen (vgl. (32)) $(\varrho + \sigma)_j \equiv (\varrho)_j + (\sigma)_j \pmod p$ ist $(\varrho, \sigma \in \mathsf{K})$, was wir im folgenden öfters anwenden, so ist der gefundene Ausdruck mod p kongruent mit

(79) $$(\omega^a \beta)_k (\omega^{a+b} \gamma)_i - (\beta)_k (\omega^b \gamma)_i.$$

Der zweite Bestandteil ist

$$-e_i \Bigg(\sum_{r=0}^{a-1} (\omega^r \beta)_{k-1} (\omega^r \beta)_{u-1} + \sum_{r=0}^{a+b-1} (\omega^r \gamma)_{k-1} (\omega^r \gamma)_{u-1} -$$

$$- \sum_{r=0}^{a-1} (\omega^r \beta + \omega^{r+b} \gamma)_{k-1} (\omega^r \beta + \omega^{r+b} \gamma)_{u-1} - \sum_{r=0}^{b-1} (\omega^r \gamma)_{k-1} (\omega^r \gamma)_{u-1} \Bigg).$$

Dies ist mod p kongruent mit

(80) $$e_i \sum_{r=0}^{a-1} ((\omega^r \beta)_{k-1} (\omega^{r+b} \gamma)_{u-1} + (\omega^{r+b} \gamma)_{k-1} (\omega^r \beta)_{u-1}).$$

Der dritte Bestandteil ist

$$e_i e_k \Bigg(\sum_{r=0}^{a-1} \binom{(\omega^r \beta)_{u-1}}{2} + \sum_{r=0}^{a+b-1} \binom{(\omega^r \gamma)_{u-1}}{2} - \sum_{r=0}^{t-1} \Bigg(((\omega^r \beta + \omega^{r+b} \gamma)_{u-1}) - \sum_{r=0}^{b-1} \binom{(\omega^r \gamma)_{u-1}}{2} \Bigg) \Bigg).$$

Da aber im vorliegenden Fall $p \neq 2$ aus $x \equiv y \pmod p$ die Kongruenz $\binom{x}{2} \equiv \binom{y}{2} \pmod p$ folgt (x, y ganze Zahlen), da ferner $\binom{x+y}{2} = \binom{x}{2} + \binom{y}{2} + xy$ gilt, so findet man leicht, daß der gefundene Ausdruck mod p kongruent mit

$$-e_i e_k \sum_{r=0}^{a-1} (\omega^r \beta)_{u-1} (\omega^{r+b} \gamma)_{u-1} \tag{81}$$

ist.

Indem wir

$$\mu = \omega^{a+b} \gamma, \quad \nu = \omega^a \beta \tag{82}$$

setzen, so gilt nach den Resultaten (79), (80), (81)

$$\begin{aligned} f(a+1) - f(a) \equiv (\omega\mu)_i (\omega\nu)_k - (\mu)_i (\nu)_k + \\ + e_i ((\mu)_{u-1} (\nu)_{k-1} + (\mu)_{k-1} (\nu)_{u-1}) - e_i e_k (\mu)_{u-1} (\nu)_{u-1} \pmod p. \end{aligned} \tag{83}$$

Nach (68), (69) gilt (wegen $(\beta)_{-1} = 0$)

$$(\omega\beta)_i \equiv (\beta)_{i-1} - e_i (\beta)_{u-1} \pmod p \qquad (\beta \in \mathsf{K};\ i = 0, \ldots, u-1).$$

Wird auf beide Faktoren des ersten Gliedes auf der rechten Seite von (83) angewendet, so entsteht (mit der neuen Bezeichnung $f(i, k) = f(a+1) - f(a)$)

$$\begin{aligned} (f(a+1) - f(a) =) f(i, k) \equiv (\mu)_{i-1} (\nu)_{k-1} - (\mu)_i (\nu)_k + \\ (e_i (\mu)_{k-1} - e_k (\mu)_{i-1}) (\nu)_{u-1} \pmod p. \end{aligned} \tag{84}$$

(Für das spätere bemerken wir, daß die hier ausgeführte Umformung der rechten Seiten von (83), (84) auch für $p = 2$ gilt.)

Da die rechte Seite von (84) homogen bilinear in den Variablen $(\mu)_r$, $(\nu)_r$ ist, ferner, $1, \omega, \ldots, \omega^{u-1}$ eine Basis von K bildet, so genügt es, wenn wir (78) (nach Einsetzung von (84)) für den Fall

$$\mu = \omega^m, \nu = \omega^n \qquad (m, n = 0, \ldots, u-1) \tag{85}$$

zeigen.

Für (85) gilt

$$(\mu)_m = 1, (\nu)_n = 1,$$

dagegen verschwinden jetzt alle übrigen $(\mu)_r$, $(\nu)_r$. Wenn also $m \geqq n$ ist, so folgt aus (84) für alle i, k $(0 \leqq i < k \leqq u-1)$ offenbar $f(i, k) \equiv 0 \pmod p$, weshalb (78) für diesen Fall richtig ist. Es ist also nur noch der Fall $m < n$ übrig. Zunächst sei sogar $m < n < u-1$. Jetzt ist nach (85) $(\nu)_{u-1} = 0$, woraus nach (84) folgt, daß

$$f(m, n) \equiv -1 \pmod p, \qquad f(m+1, n+1) \equiv 1 \pmod p$$

gelten und alle übrigen $f(i, k)$ mod p verschwinden. Auch jetzt ist also (78) erfüllt. Endlich sei $m < n = u-1$. Jetzt ist $(\nu)_{u-1} = 1$, $(\nu)_{k-1} = 0$ $(k = 0, \ldots, u-1)$, weshalb die linke Seite von (78) so lautet:

$$\prod_{0 \leqq i < k \leqq u-1} B_{k-i}^{-(\mu)_i (\nu)_k + e_i (\mu)_{k-1} - e_k (\mu)_{i-1}}.$$

Entsprechend den drei Gliedern im Exponenten zerlegt sich dieses Produkt wie leicht zu sehen in das folgende Produkt von drei Faktoren:

$$B_{u-1-m}^{-1} \prod_{i=0}^{m} B_{m+1-i}^{e_i} \prod_{k=m+2}^{u-1} B_{k-m-1}^{-e_k}.$$

Da $e_u = 1$ ist, so läßt sich der erste Faktor streichen, wenn nur gleichzeitig im letzten Faktor auch $k = u$ zugelassen wird. Somit verwandelt sich unser Produkt nach weiterer leichter Umformung in

$$\prod_{i=1}^{m+1} B_i^{e_{m+1-i}} \prod_{k=1}^{u-m-1} B_k^{-e_{m+1+k}}.$$

Wegen (12) dürfen für i und k alle Werte $1, 2, \ldots, u-1$ zugelassen werden. So entsteht

$$\prod_{k=1}^{u-1} B_k^{e_{m+1-k}-e_{m+1+k}}$$

Wegen $1 \leqq m+1 \leqq u-1$ ist dies nach (52) gleich 1, womit (78) auch für diesen Fall bewiesen ist.

Wir haben noch den Fall $p = 2$ zu betrachten. Jetzt hat man in (73) rechts noch den Faktor (36) d. h. $C^{g(\alpha,\beta,a)}$ mit

$$(86) \qquad g(\alpha, \beta, a) = \sum_{i=0}^{u-1} (\alpha)_i (\omega^a \beta)_i + \sum_{i=0}^{u-1} \sum_{\tau=0}^{a-1} e_i (\omega^\tau \beta)_{i-1} (\omega^\tau \beta)_{u-i}$$

hunzuzufügen. (In der zweiten Summe durften wir (wegen $(\beta)_{-1} = 0$) auch $i = 0$ zulassen.) Indem wir zu (77) ähnlich

$$(87) \quad g(a) = g(\alpha, \beta, a) + g(\alpha + \omega^a \beta, \gamma, a+b) - g(\alpha, \beta + \omega^b \gamma, b) - g(\beta, \gamma, b)$$

setzen, so haben wir wegen $g(0) = 0$ nur zu beweisen, daß (entsprechend dem vorigen (78)) jetzt

$$(88) \qquad C^{g(a+1)-g(a)} \prod_{0 \leqq i < k \leqq u-1} B_{k-i}^{f(a+1)-f(a)} = 1 \qquad (a = 0, 1, \ldots)$$

gilt. Hierzu wird nötig, daß wir $g(a+1) - g(a) \bmod 2$ berechnen.

Wir sehen, daß wenn man in den ersten zwei Gliedern auf der rechten Seite von (75) $k = i$ einsetzt und über $i = 0, \ldots, u-1$ summiert, dann der erhaltene Wert wegen (86) mod 2 kongruent mit $g(\alpha, \beta, a)$ wird. Folglich entsteht aus (83) eine richtige Kongruenz, wenn man darin f, k, p bzw. durch g, i, 2 ersetzt, auf der rechten Seite das letzte Glied streicht und rechts über $i = 0, \ldots, u-1$ summiert:

$$(89) \qquad \begin{aligned} g(a+1) - g(a) \equiv & \sum_{i=0}^{u-1} \Big((\omega\mu)_i (\omega\nu)_i - (\mu)_i (\nu)_i \Big) + \\ & + \sum_{i=0}^{u-1} e_i \Big((\mu)_{u-1} (\nu)_{i-1} + (\mu)_{i-1} (\nu)_{u-1} \Big) \pmod 2, \end{aligned}$$

wobei wieder die Bezeichnung (82) gebraucht wurde. Die rechte Seite ent-

steht aus der (von (83) also) von (84), daß man $e_i e_k (\mu)_{u-1} (\nu)_{u-1}$ addiert, dann $k = i$ einsetzt und nachher über $i = 0, \ldots, u-1$ summiert. Folglich gilt (wegen $e_i^2 \equiv e_i \pmod 2$)

$$g(a+1) - g(a) \equiv \sum_{i=0}^{u-1} ((\mu)_{i-1} (\nu)_{i-1} - (\mu)_i (\nu)_i + e_i (\mu)_{u-1} (\nu)_{u-1}) \pmod 2.$$

Die rechte Seite ist gleich

$$(-1 + e_0 + \cdots + e_{u-1}) (\mu)_{u-1} (\nu)_{u-1}.$$

Da ferner $\psi(1) = 1 + e_0 + \cdots + e_{u-1} \equiv 1 \pmod 2$ ist, so folgt hieraus

$$g(a+1) - g(a) \equiv (\mu)_{u-1} (\nu)_{u-1} \pmod 2 \qquad (a = 0, 1, \ldots). \tag{90}$$

Was nun den zweiten Faktor in (88) betrifft, hierüber haben wir im vorigen Fall $p \neq 2$ bewiesen (vgl. (78)), daß er dann gleich 1 ist. Da aber wegen der Bemerkung in den Klammern vor (36) im jetzigen Fall $p = 2$ die Kongruenz (83) erst nach Streichung des letzten Gliedes der rechten Seite richtig ist, so folgt, daß jetzt der zweite Faktor in (88) gleich

$$\prod_{0 \leqq i < k \leqq u-1} B_{k-1}^{e_i e_k (\mu)_{u-1} (\nu)_{u-1}}$$

ist. Hieraus und aus (90) folgt wegen (57_2) und $B_j^2 = 1$ $(j = 1, 2, \ldots)$ die Richtigkeit von (88).

Wir haben somit folgendes bewiesen. Wenn die Gruppe $\mathfrak{G}$ die durch die Gleichungen (24) bis (31) und durch die Zusatzbedingung definiert ist, daß die B_i ins Zentrum gehören, so gilt für $\mathfrak{G}$ Satz 3′ und für die Ordnung von $\mathfrak{G}$ gilt (23). Als weitere unmittelbare Folgerungen bemerken wir, daß

$$\mathfrak{G}' = \mathfrak{P} = \{A_1, \ldots, A_{u-1}\}$$

die Kommutatorgruppe und zugleich die (normale) p-Sylowgruppe von $\mathfrak{G}$ ist und ins Zentrum von $\mathfrak{G}$ gehört, daß ferner

$$O(\mathfrak{G}/\mathfrak{G}') = q^v, \; O(\mathfrak{G}'/\mathfrak{G}'') = p^u, \; O(\mathfrak{G}'') = p^t \tag{91}$$

gelten. Außerdem ist $\mathfrak{G}/\mathfrak{G}''$ wegen Satz 2 isomorph mit der zu den Invarianten p, q^v gehörenden einstufig nichtabelschen Gruppe.

Wir haben noch, wie gesagt, diejenigen Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ anzugeben, für die $\mathfrak{G}/\mathfrak{N}$ einstufig nichtnilpotent ist und zu den Invarianten p, q^v gehört.

Zuerst zeigen wir, daß das vor allem für $\mathfrak{N} = 1$ der Fall ist. Offenbar ist $\mathfrak{G}$ nichtnilpotent. Es genügt noch zu zeigen, daß alle echten Untergruppen von $\mathfrak{G}$ nilpotent sind, d. h. wenn $X, Y (\in \mathfrak{G})$ nicht vertauschbar sind und $o(X), o(Y)$ je eine Potenz von p bzw. q ist, dann notwendig $\mathfrak{G} = \{X, Y\}$ gilt. Nach (8) und Satz 3′ gilt jedenfalls

$$Q^q P_\beta Q^{-q} = P_\beta K \qquad (\beta \in \mathsf{K})$$

mit einem K aus $\{B_1, \ldots, B_t\}$. Dann gilt allgemein $Q^{qk} P_\beta Q^{-qk} = P_\beta K^k$, also $K^{q^v - 1} = 1$. Da aber $o(K) | p$ ist, so folgt $K = 1$, also liegt Q^q im Zentrum von $\mathfrak{G}$. Hieraus folgt, daß Y von der Form $PQ^a (P \in \{A_0, \ldots, A_{u-1}\})$ sein muß mit einem zu q primen a. Man darf $a = 1$ annehmen. Ferner muß $X \in \{A_0, \ldots, A_{u-1}\}$ gelten Hiernach ist

$$X = P_\alpha B, \quad Y = P_\beta B' Q \qquad (\alpha, \beta \in \mathsf{K};\ B, B' \in \{B_1, \ldots, B_t\})$$

mit einem $\alpha \neq 0$. Hieraus folgt nach Satz 3′ sofort, daß jedenfalls $\{X, Y, B_1, \ldots, B_t\} = \mathfrak{G}$ gilt. Da aber die B_i in der Kommutatorgruppe der p-Sylowgruppe von $\mathfrak{G}$ liegen, so folgt aus vorigem (vgl. ZASSENHAUS [7] S. 107) sogar $\{X, Y\} = \mathfrak{G}$.

Um endlich alle die gefragten $\mathfrak{N}$ zu bestimmen nehmen wir zuerst an, daß $\mathfrak{G}/\mathfrak{N}$ eine zu den Invarianten p, q^v gehörende einstufig nichtnilpotente Gruppe ist. Dann gilt $p^u q^v | O(\mathfrak{G}/\mathfrak{N})$, also $\mathfrak{N} \subseteqq \mathfrak{P}$, $O(\mathfrak{N}) | p^t$. Andererseits ist klar, daß $\mathfrak{P}$ genau nur die folgenden Normalteiler von $\mathfrak{G}$ enthält: $\mathfrak{P}$ und die Untergruppen von $\mathfrak{P}'$. Folglich kann $\mathfrak{N}$ nur eine Untergruppe von $\mathfrak{P}'$ sein.

Umgekehrt zeigen wir, daß jede Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ $(\mathfrak{N} \subseteqq \mathfrak{P}')$ einstufig nichtnilpotent ist und zu den Invarianten p, q^v gehört. Insbesondere für $\mathfrak{N} = \mathfrak{P}'$ folgt dies aus Satz 2. Hiernach ist $\mathfrak{G}/\mathfrak{N}$ jedenfalls nichtnilpotent. Hätte $\mathfrak{G}/\mathfrak{N}$ eine nichtnilpotente echte Untergruppe, so hätte $\mathfrak{G}$ umsomehr eine solche, was aber unmöglich ist, da sich oben selbst $\mathfrak{G}$ schon als eine einstufig nichtnilpotente Gruppe erwiesen hat. Folglich ist auch $\mathfrak{G}/\mathfrak{N}$ einstufig nichtnilpotent. Wegen (91) gehört sie zu den Invarianten p, q^v. Somit haben wir gezeigt, daß die gefragten $\mathfrak{N}$ eben die sämtlichen Untergruppen von $\mathfrak{P}'$ sind. Das beendet auch schon den Beweis der Sätze 1, 3, 3′.

Literatur.

[1] JU. A. GOLFAND, Über Gruppen, deren sämtliche Untergruppen speziell sind, *Doklady Akad. Nauk SSSR* N. S. **60** (1948), 1313—1315. (Russisch).

[2] G. A. MILLER and H. C. MORENO, Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.* **4** (1903), 398—404.

[3] L. RÉDEI, Das „schiefe Produkt" in der Gruppentheorie mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören, *Comment. Math. Helv.* **20** (1947), 225—264.

[4] L. RÉDEI, Ein Satz über die endlichen einfachen Gruppen, *Acta Math.* **84** (1951), 129—153.

[5] L. RÉDEI, Eine Determinantenidentität für symmetrische Funktionen, *Acta Math. Acad. Sci. Hungar.* **2** (1951), 105—107.

[6] O. JU. SCHMIDT, Über Gruppen, deren sämtliche Teiler spezielle Gruppen sind, *Mat. Sbornik* **31** (1924), 366—372. (Russisch mit deutscher Zusammenfassung).

[7] H. ZASSENHAUS, Lehrbuch der Gruppentheorie, *Leipzig und Berlin*, 1937.

(Eingegangen am 28 September, 1955.)