COMPOSITIO MATHEMATICA

REINHOLD BAER

Gruppen mit vom Zentrum wesentlich verschiedenem Kern und abelscher Faktorgruppe nach dem Kern

Compositio Mathematica, tome 4 (1937), p. 1-77

<http://www.numdam.org/item?id=CM_1937__4__1_0>

© Foundation Compositio Mathematica, 1937, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (http://http://www.compositio.nl/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Gruppen mit vom Zentrum wesentlich verschiedenem Kern und abelscher Faktorgruppe nach dem Kern

von

Reinhold Baer

Princeton N.J.

Bekanntlich wird die Struktur von Gruppen mit zyklischer Faktorgruppe nach dem Kern durch die Struktur des Kerns und die Lage des Zentrums im Kern völlig bestimmt [1]). Es liegt also nahe, den Kernbegriff auch für die Lösung des Strukturproblems bei allgemeineren Gruppenklassen fruchtbar zu machen. Natürlich kommen dafür in erster Linie solche Gruppenklassen in Frage, bei denen Zentrum und Kern wesentlich verschieden sind. Das Naheliegendste wäre dann, Gruppen mit nicht-Abelschem Kern zu untersuchen; aber deren Struktur wird durch die Struktur gewisser gruppeninvariant definierter Untergruppen mit Abelschem Kern bestimmt [2]).

Gruppen mit vom Zentrum verschiedenen Kern und Abelscher Faktorgruppe nach dem Kern sind direktes Produkt ihrer Primärkomponenten. Da wir im folgenden nur solche Gruppen untersuchen wollen, genügt es, Primärgruppen zu betrachten. Um zu erreichen, daß Zentrum und Kern sich wesentlich unterscheiden, beschränken wir uns auf Gruppen mit wesentlichem Kern, d. s. Gruppen, deren Kern eine maximale Untergruppe ohne nicht-invariante Untergruppen ist, und die vom Kern verschieden sind. [Durch die letzte Bedingung werden nur Abelsche und hamiltonsche Gruppen, deren Struktur ja bekannt ist [3]), von der Betrachtung ausgeschlossen.] Dies sind genau die vom Kern verschiedenen Gruppen, deren Kern jedes mit ihm elementweise vertauschbare Element enthält.

[1]) Der Kern einer Gruppe besteht aus der Gesamtheit der jede Untergruppe in sich transformierenden Gruppenelemente; vergl. hierzu R. Baer [Comp. Math. 1 (1934), 254—283], im folgenden mit K. zitiert.

[2]) Vergl. R. Baer, Gruppen mit hamiltonschem Kern [Comp. Math. 2 (1935), 241—246], im folgenden mit HK. zitiert.

[3]) Vergl. K., Fußnote [1]), S. 254.

Für Primärgruppen mit wesentlichem Kern und Abelscher Faktorgruppe nach dem Kern geben wir eine vollständige Lösung des Strukturproblems, die wir in einem Spezialfall zu einer expliziten Aufzählung mit Hilfe von Zahlinvarianten [analog etwa der Charakterisierung der endlichen Abelschen Gruppen] ausbauen.

Wesentlich für unsere Lösung des Strukturproblems ist folgendes „Reziprozitätsgesetz": Die Ordnungen der Kernelemente sind beschränkt; ist p^m die Maximalordnung der Kernelemente, so liefert die Abbildung der Gruppenelemente auf ihre p^m-ten Potenzen eine isomorphe Abbildung der Faktorgruppe nach dem Kern, also auch der von der Gruppe im Kern induzierten Automorphismengruppe, auf das System und also die Gruppe aller Kommutatoren von Gruppenelementen mit Kernelementen.

Dieses Reziprozitätsgesetz ist stets erfüllt, wenn $p \neq 2$, $p \neq 3$; ist $p = 2$ oder $p = 3$, so gibt es einige Ausnahmen.

Sehen wir von diesen Ausnahmegruppen ab, so werden genau die ein solches Reziprozitätsgesetz erfüllenden Automorphismengruppen durch Primärgruppen mit wesentlichem Kern und Abelscher Faktorgruppe nach dem Kern in ihrem Kern induziert; schärfer: ein Normalteiler einer Primärgruppe ist dann und nur dann wesentlicher Kern, die Faktorgruppe nach dem Kern Abelsch und die Gruppe keine Ausnahmegruppe, wenn die in dem betrachteten Normalteiler induzierte Automorphismengruppe das Reziprozitätsgesetz erfüllt.

Das Reziprozitätsgesetz erfüllende Automorphismengruppen werden völlig bestimmt durch ihre Struktur als abstrakte Gruppe, die Struktur ihres Definitionsbereiches und eine Reihe invarianter Zahlen. Diese Automorphismengruppen können also ebenfalls explicite aufgezählt werden, doch charakterisieren der Kern und die in ihm induzierte Automorphismengruppe nicht mehr vollständig die Gruppenstruktur; dazu sind i. A. noch zwei weitere Invarianten nötig. Die Fälle, in denen sie entbehrlich sind, werden explicite aufgezählt und die Abhängigkeit der Invarianten von einander näher untersucht.

Bezeichnungen.

$\mathfrak{K}(\mathfrak{G})$ = Kern von $\mathfrak{G}$ = Gesamtheit der Elemente aus $\mathfrak{G}$, die mit jeder Untergruppe von $\mathfrak{G}$ vertauschbar sind.

$\mathfrak{Z}(\mathfrak{G})$ = Zentrum von $\mathfrak{G}$ = Gesamtheit der Elemente aus $\mathfrak{G}$, die mit jedem Element aus $\mathfrak{G}$ vertauschbar sind.

$\mathfrak{C}(\mathfrak{G})$ = Kommutatorgruppe von $\mathfrak{G}$ = kleinster Normalteiler mit Abelscher Faktorgruppe.

$\mathfrak{D}(\mathfrak{G})$ = Gesamtheit der Kommutatoren von Elementen aus $\mathfrak{G}$ mit Elementen aus $\mathfrak{K}(\mathfrak{G})$.

$\mathsf{A}(\mathfrak{G})$ = Gruppe aller von Elementen aus $\mathfrak{G}$ in $\mathfrak{R}(\mathfrak{G})$ induzierten Automorphismen.
$\mathfrak{A} \times \mathfrak{B} \times \ldots =$ direktes Produkt der Gruppen $\mathfrak{A}, \mathfrak{B}, \ldots$
$\mathfrak{A} \cap \mathfrak{B} \cap \ldots =$ Durchschnitt der Gruppen $\mathfrak{A}, \mathfrak{B}, \ldots$
$\{\ldots\} =$ von den eingeschlossenen Elementen oder Elementmengen erzeugte Untergruppe.
$\mathfrak{G}_p$ = zur Primzahl p gehörige Primärkomponente der Gruppe $\mathfrak{G}$ = Gesamtheit der Elemente von $\mathfrak{G}$, deren Ordnung eine Potenz von p ist [$\mathfrak{G}_p$ ist nicht immer Untergruppe von $\mathfrak{G}$].
Unabhängig heißen die Elemente $\mathfrak{a}, \mathfrak{b}, \ldots \neq 1$ einer abelschen Gruppe, wenn $\{\mathfrak{a}, \mathfrak{b}, \ldots\} = \{\mathfrak{a}\} \times \{\mathfrak{b}\} \times \ldots$.
Basis = unabhängiges System von Erzeugenden einer abelschen Gruppe.
$[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a}\mathfrak{b}\mathfrak{a}^{-1}\mathfrak{b}^{-1}$.

§ 1.

Rückführung auf primäre Gruppen.

SATZ 1.: *Ist* $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ *abelsch und* $\mathfrak{R}(\mathfrak{G}) \neq \mathfrak{Z}(\mathfrak{G})$, *so ist* $\mathfrak{G}$ *direktes Produkt seiner Primärkomponenten* [4]).

BEWEIS: Aus den in H. K. bewiesenen Sätzen folgt, daß es genügt, unseren Satz unter der Voraussetzung zu beweisen, daß $\mathfrak{R}(\mathfrak{G})$ abelsch ist. Sei also im folgenden $\mathfrak{R}(\mathfrak{G})$ abelsch. Wir führen den Beweis in mehreren Schritten.

1.) $\mathfrak{G}$ enthält nur Elemente endlicher Ordnung. Denn in Gruppen mit Elementen unendlicher Ordnung und abelschem $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ ist [5]) $\mathfrak{R}(\mathfrak{G}) = \mathfrak{Z}(\mathfrak{G})$.

2.) Für jedes p ist $\mathfrak{G}_p$ eine Untergruppe von $\mathfrak{G}$.

Wir zeigen zunächst:

2a.) Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei Elemente aus $\mathfrak{G}_p$, so ist $[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a}\mathfrak{b}\mathfrak{a}^{-1}\mathfrak{b}^{-1}$ ein Element aus $\mathfrak{R}(\mathfrak{G})_p$.

Ist nämlich etwa p^a bzw. p^b die Ordnung von $\mathfrak{a}$ bzw. $\mathfrak{b}$ mod $\mathfrak{R}(\mathfrak{G})$, so ist [6]):

$$\mathfrak{b}^{p^b}\mathfrak{a}\mathfrak{b}^{-p^b}\mathfrak{a}^{-1} = \prod_{i=1}^{p^b} \mathfrak{b}^{i-1}[\mathfrak{b}, \mathfrak{a}]\mathfrak{b}^{1-i}.$$

Da $\mathfrak{b}^{p^b}$ in $\mathfrak{R}(\mathfrak{G})$ liegt, so wird nach K., § 1 (7) die linke Seite eine

---

[4]) Läßt man die Voraussetzung: $\mathfrak{R}(\mathfrak{G}) \neq \mathfrak{Z}(\mathfrak{G})$ fort, so wird der Satz falsch, da dann Elemente unendlicher Ordnung in $\mathfrak{G}$ auftreten können. Ist aber $\mathfrak{R}(\mathfrak{G}) = \mathfrak{Z}(\mathfrak{G})$ und enthält $\mathfrak{G}$ nur Elemente endlicher Ordnung, so folgt unser Satz aus K, § 3, Lemma.

[5]) Nach R. BAER: Zentrum und Kern von Gruppen mit Elementen unendlicher Ordnung [Comp. Math. **2** (1935), 247—249], Satz.

[6]) Nach R. BAER [Math. Zeitschr. **38** (1934), 375—416], im folgenden mit E. zitiert, und zwar nach § 5, Zusatz, Bedingung 3., S. 407, welche Bedingung auch erfüllt ist, wenn die dort $\mathfrak{z}_k$, $\mathfrak{z}_l$ genannten Elemente nicht unabhängig sind, wie die Herleitung der Bedingung 4. von E, § 5, Satz, S. 402—403 zeigt.

Potenz von $\mathfrak{a}$, die in $\mathfrak{R}(\mathfrak{G})$ liegt, und die linke Seite hat also die Form: $\mathfrak{a}^{rp^a}$.

Die rechte Seite wird nach K., § 2 (10):

$$\prod_{i=1}^{p^b} [\mathfrak{b}, \mathfrak{a}]\mathfrak{b}^{p^b(i-1)h} = [\mathfrak{b}, \mathfrak{a}]^{p^b}\mathfrak{b}^{p^b h[p^b(p^b-1)2^{-1}]}.$$

Da $\mathfrak{a}$, $\mathfrak{b}$ zu $\mathfrak{G}_p$ gehören, und da $\mathfrak{R}(\mathfrak{G})$ abelsch ist, $\mathfrak{a}^{p^a}$, $\mathfrak{b}^{p^b}$ zu $\mathfrak{R}(\mathfrak{G})$ gehören, so gehört also $[\mathfrak{b}, \mathfrak{a}]$ zu $\mathfrak{R}(\mathfrak{G})_p$.

Um 2.) zu beweisen, betrachten wir zwei Elemente $\mathfrak{a}$, $\mathfrak{b}$ der resp. Ordnungen p^a, p^b mod $\mathfrak{R}(\mathfrak{G})$ und es sei $n = \max(a, b)$. Da $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ abelsch ist, so wird also $(\mathfrak{a}\mathfrak{b})^{p^n}$ ein Element aus $\mathfrak{R}(\mathfrak{G})$ und wir erhalten:

$$(\mathfrak{a}\mathfrak{b})^{p^n} = \left(\prod_{i=0}^{p^n-1} \mathfrak{b}^i\mathfrak{a}\mathfrak{b}^{-i}\right)\mathfrak{b}^{p^n} = \left(\prod_{i=0}^{p^n-1} [\mathfrak{b}^i, \mathfrak{a}]\mathfrak{a}\right)\mathfrak{b}^{p^n} =$$

$$= \left(\prod_{i=0}^{p^n-1} [\mathfrak{b}^i, \mathfrak{a}]\mathfrak{a}^{ih_i p^a}\right)\mathfrak{a}^{p^n}\mathfrak{b}^{p^n} \qquad \text{nach K., § 2 (10),}$$

da $[\mathfrak{b}^i, \mathfrak{a}]$ in $\mathfrak{R}(\mathfrak{G})$ liegt. Da $\mathfrak{a}^{p^a}$, $\mathfrak{a}^{p^n}$, $\mathfrak{b}^{p^n}$ und wegen 2a.) auch $[\mathfrak{b}^i, \mathfrak{a}]$ in $\mathfrak{R}(\mathfrak{G})_p$ liegen, und da $\mathfrak{R}(\mathfrak{G})$ abelsch ist, so ist $(\mathfrak{a}\mathfrak{b})^{p^n}$ ein Element aus $\mathfrak{R}(\mathfrak{G})_p$ und also $\mathfrak{a}\mathfrak{b}$ eines aus $\mathfrak{G}_p$, womit 2.) gezeigt ist.

3.) Hat jedes Element aus $\mathfrak{G}$ endliche Ordnung, und ist jedes $\mathfrak{G}_p$ eine Untergruppe von $\mathfrak{G}$, so ist $\mathfrak{G}$ direktes Produkt seiner Primärkomponenten.

Da $\mathfrak{G}$ nach 1.) von den in den $\mathfrak{G}_p$ enthaltenen Elementen erzeugt wird, so genügt es zu zeigen:

Zu verschiedenen Primärkomponenten gehörige Elemente sind miteinander vertauschbar.

Um dies zu zeigen, betrachten wir ein Element $\mathfrak{p}$ aus $\mathfrak{G}_p$, $\mathfrak{q}$ aus $\mathfrak{G}_q$, mit $p \neq q$; dann gehören $\mathfrak{q}\mathfrak{p}\mathfrak{q}^{-1}$ und $\mathfrak{q}^{-1}$ und also auch $\mathfrak{q}\mathfrak{p}\mathfrak{q}^{-1}\mathfrak{p}^{-1}$ zu $\mathfrak{G}_p$, und analog sieht man, daß $\mathfrak{q}\mathfrak{p}\mathfrak{q}^{-1}\mathfrak{p}^{-1}$ zu $\mathfrak{G}_q$ gehört. Da aber $\mathfrak{G}_p$ und $\mathfrak{G}_q$ nur die Gruppeneins gemein haben, so ist also $\mathfrak{q}\mathfrak{p}\mathfrak{q}^{-1}\mathfrak{p}^{-1} = 1$, d.h. $\mathfrak{q}$ mit $\mathfrak{p}$ vertauschbar, wie behauptet.

Damit ist 3.) und wegen 1.) und 2.) auch unser Satz bewiesen.

DEFINITION: $\mathfrak{G}$ *ist eine Gruppe mit wesentlichem Kern, wenn*

1.) $\mathfrak{R}(\mathfrak{G}) < \mathfrak{G}$ *und*

2.) *es keine Untergruppe* $\mathfrak{A}$ *von* $\mathfrak{G}$ *gibt, die sowohl* $\mathfrak{R}(\mathfrak{G}) < \mathfrak{A} \leqq \mathfrak{G}$ *als auch* $\mathfrak{R}(\mathfrak{A}) = \mathfrak{A}$ *erfüllt.*

$\mathfrak{G}$ ist also eine Gruppe mit wesentlichem Kern, wenn der Kern eine echte Untergruppe [hierdurch werden nur die abelschen und

hamiltonschen Gruppen von der Betrachtung ausgeschlossen] und eine maximale Untergruppe ohne nicht-invariante Untergruppen ist.

SATZ 2.: *Es sei* $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ *abelsch.*

Dann und nur dann ist $\mathfrak{G}$ *eine Gruppe mit wesentlichem Kern, wenn*

1.) $\mathfrak{G}$ *direktes Produkt seiner Primärkomponenten ist,*

2.) *diese Primärkomponenten entweder abelsche oder hamiltonsche Gruppen oder Gruppen mit wesentlichem Kern sind,*

3.) *wenigstens eine der Primärkomponenten eine Gruppe mit wesentlichem Kern ist.*

BEWEIS: A. Es seien die Bedingungen 1.)—3.) erfüllt, und es sei speziell w eine Primzahl derart, daß $\mathfrak{G}_w$ eine Gruppe mit wesentlichem Kern ist. Nach K., § 3., Satz 4 ist $\mathfrak{R}(\mathfrak{G}) = \prod_p \mathfrak{R}(\mathfrak{G}_p)$, und da $\mathfrak{R}(\mathfrak{G}_w) < \mathfrak{G}_w$ ist, so ist auch $\mathfrak{R}(\mathfrak{G}) < \mathfrak{G}$.

Ist nun $\mathfrak{U}$ eine $\mathfrak{R}(\mathfrak{G})$ umfassende Untergruppe von $\mathfrak{G}$, die $\mathfrak{R}(\mathfrak{U}) = \mathfrak{U}$ erfüllt, so sei $\mathfrak{u}$ irgend ein Element aus $\mathfrak{U}$. Dann ist $\mathfrak{u} = \prod_{i=1}^{n} \mathfrak{u}_i$ mit $\mathfrak{u}_i$ in $\mathfrak{G}_{p_i}$, wo $p_1, \ldots, p_n$ verschiedene Primzahlen sind. Weiter ist, da wegen $\mathfrak{R}(\mathfrak{U}) = \mathfrak{U}$ und 1.) auch $\mathfrak{U}$ direktes Produkt seiner Primärkomponenten ist,

$$\mathfrak{R}(\mathfrak{G}_{p_i}) \leqq \{\mathfrak{R}(\mathfrak{G}_{p_i}), \mathfrak{u}_i\} \leqq \mathfrak{G}_{p_i} \cap \mathfrak{U} = \mathfrak{U}_{p_i} = \mathfrak{R}(\mathfrak{U}_{p_i})$$

und also ist wegen Bedingung 2.):

$$\mathfrak{R}(\mathfrak{G}_{p_i}) = \{\mathfrak{R}(\mathfrak{G}_{p_i}), \mathfrak{u}_i\},$$

d.h. $\mathfrak{u}_i$ gehört zu $\mathfrak{R}(\mathfrak{G}_{p_i})$, und also $\mathfrak{u}$ zu $\mathfrak{R}(\mathfrak{G})$, d.h. $\mathfrak{U} = \mathfrak{R}(\mathfrak{G})$, d.h. $\mathfrak{G}$ ist eine Gruppe mit wesentlichem Kern.

B. Wir zeigen zunächst:

(1) *Ist* $\mathfrak{G}$ *eine Gruppe mit wesentlichem Kern, so ist jedes mit* $\mathfrak{R}(\mathfrak{G})$ *elementweise vertauschbare Element in* $\mathfrak{R}(\mathfrak{G})$ *enthalten.*

Ist nämlich $\mathfrak{g}$ ein mit $\mathfrak{R}(\mathfrak{G})$ elementweise vertauschbares Element, so ist $\{\mathfrak{R}(\mathfrak{G}), \mathfrak{g}\}$ mit $\mathfrak{R}(\mathfrak{G})$ abelsch oder hamiltonsch [nach K., § 4., Satz 5.] und also $\{\mathfrak{R}(\mathfrak{G}), \mathfrak{g}\} = \mathfrak{R}(\mathfrak{G})$, d.h. $\mathfrak{g}$ in $\mathfrak{R}(\mathfrak{G})$, womit (1) bewiesen.

Ist nun $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ abelsch und $\mathfrak{G}$ eine Gruppe mit wesentlichem Kern, so ist wegen (1) sicher $\mathfrak{R}(\mathfrak{G}) \neq \mathfrak{Z}(\mathfrak{G})$, und $\mathfrak{G}$ also nach Satz 1 direktes Produkt seiner Primärkomponenten: $\mathfrak{G} = \prod_p \mathfrak{G}_p$. Nach K., § 3, Satz 4 ist $\mathfrak{R}(\mathfrak{G}) = \prod_p \mathfrak{R}(\mathfrak{G}_p)$ und nach K., § 3 (11) ist $\mathfrak{R}(\mathfrak{G}_p) = \mathfrak{R}(\mathfrak{G})_p$.

Ist jetzt $\mathfrak{U} = \mathfrak{R}(\mathfrak{U})$ und $\mathfrak{R}(\mathfrak{G}_n) \leqq \mathfrak{U} \leqq \mathfrak{G}_n$, so ist

$$\{\mathfrak{U}, \mathfrak{R}(\mathfrak{G})\} = \mathfrak{U} \times \prod_{q \neq p} \mathfrak{R}(\mathfrak{G}_q) = \mathfrak{R}(\{\mathfrak{U}, \mathfrak{R}(\mathfrak{G})\}) \text{ und}$$

$$\mathfrak{R}(\mathfrak{G}) \leqq \{\mathfrak{U}, \mathfrak{R}(\mathfrak{G})\} \leqq \mathfrak{G},$$

also, da $\mathfrak{G}$ eine Gruppe mit wesentlichem Kern ist,

$$\mathfrak{R}(\mathfrak{G}) = \{\mathfrak{U}, \mathfrak{R}(\mathfrak{G})\}, \text{ also } \mathfrak{U} \leqq \mathfrak{R}(\mathfrak{G}), \text{ also } \mathfrak{U} = \mathfrak{R}(\mathfrak{G}_p).$$

Außerdem muß $\mathfrak{R}(\mathfrak{G}_p) < \mathfrak{G}_p$ für wenigstens ein p gelten, da $\mathfrak{G} > \mathfrak{R}(\mathfrak{G})$ ist, womit 1.)—3.) als notwendig erwiesen sind.

Satz 3.: *Es sei $\mathfrak{G}$ eine Primärgruppe.*

Dann und nur dann ist $\mathfrak{G}$ eine Gruppe mit wesentlichem Kern, wenn

1. $\mathfrak{R}(\mathfrak{G}) < \mathfrak{G}$,
2. *jedes mit $\mathfrak{R}(\mathfrak{G})$ elementweise vertauschbare Element aus $\mathfrak{G}$ zu $\mathfrak{R}(\mathfrak{G})$ gehört.*

Beweis: Die Notwendigkeit der Bedingung 1. ist trivial, die der Bedingung 2. eine Folge von (1). — Seien also die Bedingungen 1., 2. erfüllt und $\mathfrak{G} = \mathfrak{G}_p$ für ein gewisses p.

Ist zunächst $p \neq 2$, so ist nach K., Fußnote [1]) jede $\mathfrak{U} = \mathfrak{R}(\mathfrak{U})$ erfüllende Untergruppe $\mathfrak{U}$ von $\mathfrak{G}$ abelsch und aus 1., 2. folgt, daß $\mathfrak{G}$ eine Gruppe mit wesentlichem Kern ist.

Sei $p = 2$; wäre $\mathfrak{R}(\mathfrak{G})$ hamiltonsch, so wäre $\mathfrak{G} = \mathfrak{R}(\mathfrak{G})$ nach H. K., Zusatz 3, was 1. widerspricht; also:

$\mathfrak{R}(\mathfrak{G})$ ist abelsch.

Wir teilen jetzt die nicht in $\mathfrak{R}(\mathfrak{G})$ enthaltenen Elemente aus $\mathfrak{G}$ in zwei Klassen ein, und zwar gehöre ein nicht in $\mathfrak{R}(\mathfrak{G})$ enthaltenes Element $\mathfrak{g}$ zu $\mathfrak{R}$, wenn

$$\mathfrak{R}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{g}\}) = \mathfrak{R}(\mathfrak{G})$$

ist, sonst zu $\mathfrak{S}$.

Ist $\mathfrak{S}$ leer, so folgt aus 1., daß $\mathfrak{G}$ einen wesentlichen Kern hat; wir wollen also zeigen, daß die Annahme,

$$\mathfrak{S} \textit{ enthält Elemente,}$$

zu einem Widerspruch führt.

Ist $\mathfrak{s}$ ein Element aus $\mathfrak{S}$, so ist

$$\mathfrak{R}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{s}\}) > \mathfrak{R}(\mathfrak{G});$$

wegen Bedingung 2. ist also $\mathfrak{R}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{s}\})$ hamiltonsch, wegen H. K., Zusatz 3, also

$$\mathfrak{R}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{s}\}) = \{\mathfrak{R}(\mathfrak{G}), \mathfrak{s}\}.$$

Da $\mathfrak{N}(\mathfrak{G})$ abelsch ist, so folgt aus der Existenz von Elementen $\mathfrak{s}$ in $\mathfrak{S}$ und aus K., Fußnote [1]):

a. $\mathfrak{N}(\mathfrak{G}) = \{\mathfrak{a}\} \times \mathfrak{Z}$,

wo $\mathfrak{a}$ die Ordnung 4 hat und $\mathfrak{Z}$ direktes Produkt von Zyklen der Ordnung 2 ist.

b. $\mathfrak{s}^2 = \mathfrak{a}^2$, $\mathfrak{s}^{-1}\mathfrak{a}\mathfrak{s} = \mathfrak{a}^{-1}$, $\mathfrak{s}\mathfrak{z} = \mathfrak{z}\mathfrak{s}$ für $\mathfrak{z}$ aus $\mathfrak{Z}$ und $\mathfrak{s}$ aus $\mathfrak{S}$.

Ist $\mathfrak{s}'$ ein zweites Element aus $\mathfrak{S}$, so induzieren $\mathfrak{s}$ und $\mathfrak{s}'$ wegen b. in $\mathfrak{N}(\mathfrak{G})$ denselben Automorphismus, d.h. aber wegen Bedingung 2:

c. sind $\mathfrak{s}$ und $\mathfrak{s}'$ Elemente aus $\mathfrak{S}$, so ist $\mathfrak{s}'\mathfrak{s}^{-1}$ in $\mathfrak{N}(\mathfrak{G})$ enthalten, und hieraus folgt weiter:

d. für irgendein $\mathfrak{s}$ aus $\mathfrak{S}$ ist

$$\{\mathfrak{N}(\mathfrak{G}), \mathfrak{S}\} = \{\mathfrak{N}(\mathfrak{G}), \mathfrak{s}\} = \mathfrak{H}$$

eine hamiltonsche Primärgruppe und es ist $\mathfrak{H} > \mathfrak{N}(\mathfrak{G})$.

Aus $\mathfrak{H} = \mathfrak{N}(\mathfrak{H})$ und Bedingung 1. folgt $\mathfrak{G} > \mathfrak{H}$ und $\mathfrak{R}$ enthält also wenigstens ein Element. Ist $\mathfrak{r}$ aus $\mathfrak{R}$, so ist

$$\mathfrak{N}(\{\mathfrak{N}(\mathfrak{G}), \mathfrak{r}\}) = \mathfrak{N}(\mathfrak{G})$$

und aus K., § 5, Satz 7 und K., § 5, Folgerung 1 aus Satz 8 folgt:

1) $\mathfrak{r}^2$ liegt in $\mathfrak{N}(\mathfrak{G})$;

2) $\mathfrak{r}^4 = \mathfrak{a}^2 = \mathfrak{s}^2$, wo $\mathfrak{a}$ ein gemäß a. bestimmtes Element und $\mathfrak{s}$ aus $\mathfrak{S}$ ist; speziell hat also $\mathfrak{r}$ die Ordnung 8.

3) $\mathfrak{r}^{-1}\mathfrak{f}\mathfrak{r} = \mathfrak{f}\mathfrak{a}^{2h(\mathfrak{f})}$ für $\mathfrak{f}$ aus $\mathfrak{N}(\mathfrak{G})$, wo $h(\mathfrak{f}) = 0$ oder 1 und der Wert 1 für gewisse $\mathfrak{f}$ angenommen wird.

Da $\mathfrak{r}^2$ wegen 2) ein Element der Ordnung 4 in $\mathfrak{N}(\mathfrak{G})$ ist, so können wir wegen a. o. B. d. A. annehmen [7]):

1*) $\mathfrak{r}^2 = \mathfrak{a}$.

Nach unserer Annahme gibt es ein Element $\mathfrak{s}$ in $\mathfrak{S}$ und, wie wir gezeigt haben, ein Element $\mathfrak{r}$ aus $\mathfrak{R}$ und wir betrachten: $\mathfrak{w} = \mathfrak{s}\mathfrak{r}$.

Da $\mathfrak{r}$ wegen 1*) mit $\mathfrak{a}$ vertauschbar ist, $\mathfrak{s}$ wegen b. aber nicht, da weiter $\mathfrak{N}(\mathfrak{G})$ abelsch ist, so ist $\mathfrak{w}$ nicht in $\mathfrak{N}(\mathfrak{G})$ enthalten. $\mathfrak{w}$ gehört auch nicht zu $\mathfrak{S}$, da sonst $\mathfrak{r}$ wegen b., c. in $\mathfrak{N}(\mathfrak{G})$ enthalten wäre, was ausgeschlossen ist. Also:

$\mathfrak{w}$ gehört zu $\mathfrak{R}$.

Bedenken wir, daß $\mathfrak{r}$ und $\mathfrak{s}$ mod $\mathfrak{N}(\mathfrak{G})$ verschieden sind und mod $\mathfrak{N}(\mathfrak{G})$ die Ordnung 2 haben, also mod $\mathfrak{N}(\mathfrak{G})$ unabhängig sind, so folgt aus E., § 5, Zusatz S. 407

$$[\mathfrak{r}, \mathfrak{s}]\mathfrak{r}[\mathfrak{r}, \mathfrak{s}]\mathfrak{r}^{-1} = \mathfrak{r}^2\mathfrak{s}\mathfrak{r}^{-2}\mathfrak{s}^{-1} = \mathfrak{a}\mathfrak{s}\mathfrak{a}^{-1}\mathfrak{s}^{-1} = \mathfrak{a}^2$$

wegen 1*) und b.

---

[7]) Natürlich nur für ein $\mathfrak{r}$ aus $\mathfrak{R}$.

Weiter ist

$$\begin{aligned}[\mathfrak{s}, \mathfrak{r}] &= \mathfrak{s}\mathfrak{r}\mathfrak{s}\mathfrak{r}\mathfrak{r}^{-1}\mathfrak{s}^{-2}\mathfrak{r}^{-1} = \mathfrak{w}^2\mathfrak{r}^{-1}\mathfrak{a}^2\mathfrak{r}^{-1} \text{ wegen b.} \\ &= \mathfrak{w}^2\mathfrak{r}^{-1}\mathfrak{r}^4\mathfrak{r}^{-1} \text{ wegen 2.)} \\ &= \mathfrak{w}^2\mathfrak{a}^2,\end{aligned}$$

wo $\mathfrak{w}^2$ wegen 1.) ein Element der Ordnung 4 aus $\mathfrak{R}(\mathfrak{G})$ ist.

Dies zusammen mit obiger Formel ergibt:

$$\begin{aligned}\mathfrak{a}^2 &= [\mathfrak{r}, \mathfrak{s}]\mathfrak{r}[\mathfrak{r}, \mathfrak{s}]\mathfrak{r}^{-1} = \mathfrak{w}^{-2}\mathfrak{a}^2\mathfrak{r}\mathfrak{w}^{-2}\mathfrak{a}^2\mathfrak{r}^{-1} \\ &= \mathfrak{w}^2\mathfrak{r}\mathfrak{w}^2\mathfrak{r}^{-1}, \text{ da } \mathfrak{a}^2 = \mathfrak{w}^4 \text{ nach 2.)} \\ &= \mathfrak{w}^4\mathfrak{a}^{2x} \quad \text{nach 3.)} \\ &= \mathfrak{a}^2\mathfrak{a}^{2x} \quad \text{nach 2.),}\end{aligned}$$

also $\mathfrak{a}^{2x} = 1$, d.h. $\mathfrak{r}\mathfrak{w}^2 = \mathfrak{w}^2\mathfrak{r}$.

Also wird:

$$\begin{aligned}\mathfrak{w}^2 &= \mathfrak{r}^{-1}\mathfrak{w}^2\mathfrak{r} = \\ &= \mathfrak{w}^{-1}\mathfrak{w}^2\mathfrak{w} = \mathfrak{s}^{-1}\mathfrak{r}^{-1}\mathfrak{w}^2\mathfrak{r}\mathfrak{s} = \mathfrak{s}^{-1}\mathfrak{w}^2\mathfrak{s}.\end{aligned}$$

Da aber andererseits $\mathfrak{w}^2$ ein Element der Ordnung 4 aus $\mathfrak{R}(\mathfrak{G})$ ist, so folgt aus a., b., daß

$$\mathfrak{w}^{-2} = \mathfrak{s}^{-1}\mathfrak{w}^2\mathfrak{s},$$

d.h. $\mathfrak{w}^{-2} = \mathfrak{w}^2$, d.h. $\mathfrak{w}^2$ hätte höchstens die Ordnung 2, was unmöglich ist.

Damit ist der gesuchte Widerspruch aufgewiesen, unser Satz bewiesen und auch der

Zusatz 1: *Primärgruppen mit wesentlichem Kern haben abelschen Kern.*

Aus Satz 2. folgt noch der

Zusatz 2: *Es sei* $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ *abelsch.*

Dann und nur dann hat $\mathfrak{G}$ *einen wesentlichen Kern, wenn*

1. $\mathfrak{R}(\mathfrak{G}) < \mathfrak{G}$,
2. *jedes mit* $\mathfrak{R}(\mathfrak{G})$ *elementweise vertauschbare Element zu* $\mathfrak{R}(\mathfrak{G})$ *gehört.*

§ 2.

Hilfssätze und Grundformeln.

Auf Grund der Ergebnisse des § 1 sind wir in der Lage, uns auf die Untersuchung primärer Gruppen $[\mathfrak{G} = \mathfrak{G}_p]$ zu beschränken. Alle im folgenden auftretenden Gruppen seien deshalb als primär vorausgesetzt.

(1) *Dann und nur dann ist die Untergruppe* $\mathfrak{A}$ *von* $\mathfrak{G}$ *wesentlicher Kern von* $\mathfrak{G}$, *wenn*

1. $\mathfrak{A} < \mathfrak{G}$,
2. $\mathfrak{K}(\{\mathfrak{A}, \mathfrak{g}\}) = \mathfrak{A}$ *für jedes* $\mathfrak{g}$ *aus* $\mathfrak{G}$ *ist.*

Die Notwendigkeit folgt aus $\mathfrak{K}(\{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\}) \geqq \mathfrak{K}(\mathfrak{G})$ und $\mathfrak{K}[\mathfrak{K}(\mathfrak{U})] = \mathfrak{K}(\mathfrak{U})$, das Hinreichen daraus, daß mit $\mathfrak{K}(\mathfrak{U}) = \mathfrak{U}$ und $\mathfrak{U} \geqq \mathfrak{V}$ auch $\mathfrak{K}(\mathfrak{V}) = \mathfrak{V}$ ist.

(2) *Ist* $\mathfrak{A}$ *eine Untergruppe von* $\mathfrak{G}$ *und* $\mathfrak{r}$ *nicht in* $\mathfrak{A}$ *enthalten, so ist dann und nur dann*

$$\mathfrak{A} = \mathfrak{K}(\{\mathfrak{A}, \mathfrak{r}\}),$$

wenn

1. $\mathfrak{A}$ *abelsch ist,*
2. $\mathfrak{r}^{p^{n(\mathfrak{r})}} = \mathfrak{a}(\mathfrak{r})$ *ein Element von der in* $\mathfrak{A}$ *maximalen Ordnung* p^m [*die existiert*] *ist, wobei* $p^{n(\mathfrak{r})}$ *die Ordnung von* $\mathfrak{r}$ *mod* $\mathfrak{K}(\mathfrak{G})$ *ist,*
3. $\mathfrak{r}^{p^m} = \mathfrak{c}(\mathfrak{r})$ *ein Element der Ordnung* $p^{n(\mathfrak{r})}$ *aus* $\mathfrak{A}$ [*und also* $n(\mathfrak{r}) \leqq m$] *ist,*
4. $\mathfrak{r}^{-1}\mathfrak{k}\,\mathfrak{r} = \mathfrak{k}\mathfrak{c}(\mathfrak{r})^{h(\mathfrak{k}, \mathfrak{r})}$ *für jedes* $\mathfrak{k}$ *aus* $\mathfrak{A}$ *gilt und es ein* $\mathfrak{e}$ *in* $\mathfrak{A}$ *mit* $\mathfrak{r}^{-1}\mathfrak{e}\,\mathfrak{r} = \mathfrak{e}\mathfrak{c}(\mathfrak{r})$ *gibt* [*so daß also* $\mathfrak{r}$ *in* $\mathfrak{A}$ *einen Automorphismus der Ordnung* $p^{n(\mathfrak{r})}$ *induziert*],
5. $m > 1$ *ist, falls* $p = 2$.

Man beachte, daß $\mathfrak{a}(\mathfrak{r})$ und $\mathfrak{c}(\mathfrak{r})\,[= \mathfrak{a}(\mathfrak{r})^{p^{m-n(\mathfrak{r})}}]$ mit $\mathfrak{r}$ vertauschbare Elemente aus $\mathfrak{A}$ sind. — Die „Funktionen" $n(\mathfrak{r})$, m, $h(\mathfrak{k}, \mathfrak{r})$, $\mathfrak{a}(\mathfrak{r})$, $\mathfrak{c}(\mathfrak{r})$ hängen außer von den angegebenen Variablen auch noch von $\mathfrak{A}$ ab; da die „Bezugsgruppe" $\mathfrak{A}$ im folgenden stets aus dem Zusammenhang eindeutig erkennbar sein wird, deuten wir diese Abhängigkeit in den benutzten Symbolen nicht an.

(2) ist eine triviale Folge aus K., § 5, Satz 7.

(3) *Ist* $\mathfrak{G}$ *eine Gruppe mit wesentlichem Kern, so ist* $\mathfrak{K}(\mathfrak{G})$ *direktes Produkt von zyklischen Gruppen beschränkter Ordnung und die Maximalordnung der Elemente aus* $\mathfrak{K}(\mathfrak{G})$ *ist gleichzeitig eine obere Schranke für die Ordnungen der Elemente von* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$; *ist* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *überdies abelsch, so ist* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *ebenfalls direktes Produkt zyklischer Gruppen* [*von durch die Maximalordnung in* $\mathfrak{K}(\mathfrak{G})$ *beschränkter Ordnung*].

Dies folgt aus (1), (2) und K., § 5, Lemma.

(4) *Es sei* $\mathfrak{A} = \mathfrak{K}(\{\mathfrak{A}, \mathfrak{u}\}) \neq \{\mathfrak{A}, \mathfrak{u}\}$. *Dann gilt für jedes* $\mathfrak{k}$ *aus* $\mathfrak{A}$:

$$\mathfrak{c}(\mathfrak{k}\,\mathfrak{u}) = \begin{cases} \mathfrak{c}(\mathfrak{u}), & \text{falls } p \neq 2 \text{ ist,} \\ \mathfrak{c}(\mathfrak{u})^{1+2^{m-1}h(\mathfrak{k}, \mathfrak{u})}, & \text{falls } p = 2 \text{ ist.} \end{cases}$$

Es ist nämlich

$$\mathfrak{c}(\mathfrak{k}\mathfrak{u}) = (\mathfrak{k}\mathfrak{u})^{p^m} = \left(\prod_{i=0}^{p^m-1} \mathfrak{u}^i \mathfrak{k} \mathfrak{u}^{-i}\right) \mathfrak{u}^{p^m} =$$

$$= \left(\prod_{i=0}^{p^m-1} \mathfrak{k}\mathfrak{c}(\mathfrak{u})^{-ih(\mathfrak{k},\mathfrak{u})}\right) \mathfrak{c}(\mathfrak{u}) =$$

$$= \mathfrak{k}^{p^m} \mathfrak{c}(\mathfrak{u})^{1-\frac{p^m(p^m-1)}{2} h(\mathfrak{k},\mathfrak{u})},$$

woraus (4) folgt, da p^m die Maximalordnung in $\mathfrak{A}$ ist.

(5) *Es sei* $\mathfrak{A} = \mathfrak{R}(\{\mathfrak{A}, \mathfrak{u}\}) = \mathfrak{R}(\{\mathfrak{A}, \mathfrak{v}\})$, $\{\mathfrak{A}, \mathfrak{u}, \mathfrak{v}\}/\mathfrak{A}$ *abelsch und* $\mathfrak{u}, \mathfrak{v}$ *nicht in* $\mathfrak{A}$ *enthalten.*

a. $$\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{a}(\mathfrak{v}),\mathfrak{u})} = \begin{cases} [\mathfrak{v}, \mathfrak{u}]^{p^{n(\mathfrak{v})}}, & \text{falls } p \neq 2 \text{ ist,} \\ [\mathfrak{v}, \mathfrak{u}]^{2^{n(\mathfrak{v})}} \mathfrak{c}(\mathfrak{v})^{h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})2^{n(\mathfrak{v})-1}}, & \text{falls } p = 2 \text{ ist.} \end{cases}$$

b. $$\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{c}(\mathfrak{v}),\mathfrak{u})} = \begin{cases} 1, & \text{falls } p \neq 2 \text{ ist,} \\ \mathfrak{c}(\mathfrak{v})^{h([\mathfrak{u},\mathfrak{v}],\mathfrak{v}) \cdot 2^{m-1}}, & \text{falls } p = 2 \text{ ist.} \end{cases}$$

Nach E., § 5, Zusatz, Bedingung 3.), S. 407 [welche Bedingung, wie früher bemerkt, auch angewandt werden kann, wenn $\mathfrak{u}$ und $\mathfrak{v}$ nicht mod $\mathfrak{A}$ unabhängig sind] wird nämlich

$$\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{a}(\mathfrak{v}),\mathfrak{u})} = \mathfrak{a}(\mathfrak{v})\,\mathfrak{u}\,\mathfrak{a}(\mathfrak{v})^{-1}\mathfrak{u}^{-1} = \prod_{i=1}^{p^{n(\mathfrak{v})}} \mathfrak{v}^{i-1}[\mathfrak{v}, \mathfrak{u}]\mathfrak{v}^{1-i} =$$

$$= \prod_{i=1}^{p^{n(\mathfrak{v})}} [\mathfrak{v}, \mathfrak{u}]\mathfrak{c}(\mathfrak{v})^{(i-1)h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})}, \text{ nach (2), 4.}$$

$$= [\mathfrak{v}, \mathfrak{u}]^{p^{n(\mathfrak{v})}} \mathfrak{c}(\mathfrak{v})^{\sum_{i=1}^{p^{n(\mathfrak{v})}} (i-1) \cdot h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})}, \text{ nach (2), 1.),}$$

woraus a. folgt, da $\mathfrak{c}(\mathfrak{v})$ nach (2), 3. die Ordnung $p^{n(\mathfrak{v})}$ hat. — Aus a. folgt b., da $\mathfrak{c}(\mathfrak{v}) = \mathfrak{a}(\mathfrak{v})^{p^{m-n(\mathfrak{v})}}$ nach (2), 2., 3. und p^m die Maximalordnung in $\mathfrak{A}$ ist.

(6) *Es sei* $\mathfrak{A} = \mathfrak{R}(\{\mathfrak{A}, \mathfrak{u}\}) = \mathfrak{R}(\{\mathfrak{A}, \mathfrak{v}\})$, $\{\mathfrak{A}, \mathfrak{u}, \mathfrak{v}\}/\mathfrak{A}$ *abelsch und* $\mathfrak{u}, \mathfrak{v}$ *nicht in* $\mathfrak{A}$ *enthalten*[8]).

a. $$[\mathfrak{v}^i, \mathfrak{u}] = [\mathfrak{v}, \mathfrak{u}]^i \mathfrak{c}(\mathfrak{v})^{\frac{i(i-1)}{2} h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})}$$

b. $$(\mathfrak{u}\mathfrak{v})^i = [\mathfrak{v}, \mathfrak{u}]^{\frac{i\cdot(i-1)}{2}} \mathfrak{c}(\mathfrak{v})^{\frac{i(i-1)(i-2)}{6} h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})} \cdot$$
$$\cdot \mathfrak{c}(\mathfrak{u})^{\frac{(2i-1)i(i-1)}{6} h([\mathfrak{u},\mathfrak{v}],\mathfrak{u}) + \frac{i(i-1)(i-2)(3i-1)}{24} h([\mathfrak{v},\mathfrak{u}],\mathfrak{v}) h(\mathfrak{c}(\mathfrak{v}),\mathfrak{u})} \cdot \mathfrak{u}^i \cdot \mathfrak{v}^i.$$

[8]) Die folgenden Formeln sind im wesentlichen Spezialfälle von E., § 5, (1), S. 402.

BEWEIS: ad a. Die Formel a. ist offenbar für $i = 1$ wahr; ist sie bereits für $i - 1$ bewiesen, so wird

$$\begin{aligned}[\mathfrak{v}^i, \mathfrak{u}] &= \mathfrak{v}^i \mathfrak{u} \mathfrak{v}^{-i} \mathfrak{u}^{-1} = \mathfrak{v}\mathfrak{v}^{i-1} \mathfrak{u} \mathfrak{v}^{1-i} \mathfrak{u}^{-1} \mathfrak{u}\mathfrak{v}^{-1}\mathfrak{u}^{-1} \\ &= \mathfrak{v}[\mathfrak{v}^{i-1}, \mathfrak{u}]\mathfrak{u}\mathfrak{v}^{-1}\mathfrak{u}^{-1} \\ &= \mathfrak{v}[\mathfrak{v}, \mathfrak{u}]^{i-1} \mathfrak{c}(\mathfrak{v})^{\frac{(i-1)(i-2)}{2} h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})} \mathfrak{u}\mathfrak{v}^{-1}\mathfrak{u}^{-1} \\ &= [\mathfrak{v}, \mathfrak{u}]^{i-1} \mathfrak{c}(\mathfrak{v})^{\left[i-1+\frac{(i-1)(i-2)}{2}\right] h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})} \mathfrak{v}\mathfrak{u}\mathfrak{v}^{-1}\mathfrak{u}^{-1},\end{aligned}$$

da ja $\mathfrak{v}$ mit $\mathfrak{c}(\mathfrak{v})$ vertauschbar ist, woraus a. durch vollständige Induktion folgt.

ad b. Die Formel b. ist offenbar für $i = 1$ wahr; ist sie bereits für $i - 1$ bewiesen, so wird

$$(\mathfrak{u}\mathfrak{v})^i = (\mathfrak{u}\mathfrak{v})^{i-1}\mathfrak{u}\mathfrak{v} = \mathfrak{f}_{i-1}\mathfrak{u}^{i-1}\mathfrak{v}^{i-1}\mathfrak{u}\mathfrak{v},$$

wenn wir zur Abkürzung

$$\mathfrak{f}_{i-1} = [\mathfrak{v}, \mathfrak{u}]^{\frac{(i-1)(i-2)}{2}} \mathfrak{c}(\mathfrak{v})^{\frac{(i-1)(i-2)(i-3)}{6} h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})} \cdot \mathfrak{c}(\mathfrak{u})^{\frac{(2i-3)(i-1)(i-2)}{6} h([\mathfrak{u},\mathfrak{v}],\mathfrak{u}) + \frac{(i-1)(i-2)(i-3)(3i-4)}{24} h([\mathfrak{v},\mathfrak{u}],\mathfrak{v}) h(\mathfrak{c}(\mathfrak{v}),\mathfrak{u})}$$

setzen, und es wird also wegen a.

$$\begin{aligned}(\mathfrak{u}\mathfrak{v})^i &= \mathfrak{f}_{i-1}\mathfrak{u}^{i-1}[\mathfrak{v}^{i-1}, \mathfrak{u}]\mathfrak{u}\mathfrak{v}^i \\ &= \mathfrak{f}_{i-1}\mathfrak{u}^{i-1}[\mathfrak{v}, \mathfrak{u}]^{i-1} \mathfrak{c}(\mathfrak{v})^{\frac{(i-1)(i-2)}{2} h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})} \mathfrak{u}\mathfrak{v}^i \\ &= \mathfrak{f}_{i-1}[\mathfrak{v}, \mathfrak{u}]^{i-1} \mathfrak{c}(\mathfrak{u})^{(i-1)^2 h([\mathfrak{u},\mathfrak{v}],\mathfrak{u}) + \frac{(i-1)^2(i-2)}{2} h([\mathfrak{v},\mathfrak{u}],\mathfrak{v}) h(\mathfrak{c}(\mathfrak{v}),\mathfrak{u})} \cdot \\ &\qquad \cdot \mathfrak{c}(\mathfrak{v})^{\frac{(i-1)(i-2)}{2} h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})} \mathfrak{u}^i\mathfrak{v}^i,\end{aligned}$$

und hieraus folgt b. durch vollständige Induktion.

(7) *Es sei* $\mathfrak{A} = \mathfrak{R}(\{\mathfrak{A}, \mathfrak{u}\}) = \mathfrak{R}(\{\mathfrak{A}, \mathfrak{v}\})$, $\{\mathfrak{A}, \mathfrak{u}, \mathfrak{v}\}/\mathfrak{A}$ *abelsch und* $\mathfrak{u}, \mathfrak{v}$ *nicht in* $\mathfrak{A}$ *enthalten. Dann ist:*

$$\mathfrak{c}(\mathfrak{u}\mathfrak{v}) = \begin{cases} \mathfrak{c}(\mathfrak{u})\mathfrak{c}(\mathfrak{v}), \textit{ falls } p \neq 2,\ p \neq 3, \\ \mathfrak{c}(\mathfrak{u})^{1+3^{m-1}h([\mathfrak{v},\mathfrak{u}],\mathfrak{u})}\mathfrak{c}(\mathfrak{v})^{1+3^{m-1}h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})}, \textit{ falls } p = 3 \textit{ ist}, \\ [\mathfrak{u}, \mathfrak{v}]^{2^{m-1}} \mathfrak{c}(\mathfrak{u})^{1+h(\mathfrak{c}(\mathfrak{v}),\mathfrak{u})}\mathfrak{c}(\mathfrak{v})^{1+h(\mathfrak{c}(\mathfrak{u}),\mathfrak{v})}, \textit{ falls } p = 2 < m \textit{ ist}, \\ [\mathfrak{u}, \mathfrak{v}]^2 \mathfrak{c}(\mathfrak{u})^{1+h(\mathfrak{c}(\mathfrak{v}),\mathfrak{u})\,[1+h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})]} \\ \qquad \mathfrak{c}(\mathfrak{v})^{1+h(\mathfrak{c}(\mathfrak{u}),\mathfrak{v})}, \textit{ falls } p = 2 = m \textit{ ist}^{9}). \end{cases}$$

Dies folgt aus (6) b., wenn man dort $i = p^m$ setzt und bedenkt,

---

[9]) $p = 2$, $m = 1$ kann wegen (2), 5. nicht eintreten.

daß p^m die Maximalordnung in $\mathfrak{A}$ ist, daß $\frac{1-3^m}{2} \equiv 2 \bmod 3$ ist, daß $-2^{m-1} \equiv 2^{m-1} \bmod 2^m$ ist, und man schließlich noch (5)b. berücksichtigt.

§ 3.

Das Reziprozitätsgesetz.

DEFINITION: *Es sei $\mathfrak{G}$ eine Primärgruppe mit wesentlichem Kern und abelscher Faktorgruppe nach dem Kern. p^m sei die Maximalordnung in $\mathfrak{N}(\mathfrak{G})$.*

$\mathfrak{G}$ heiße vollkommen, wenn für irgendzwei mod $\mathfrak{N}(\mathfrak{G})$ unabhängige Elemente $\mathfrak{u}, \mathfrak{v}$ gilt:

$$(\mathfrak{u}\mathfrak{v})^{p^m} = \mathfrak{u}^{p^m} \cdot \mathfrak{v}^{p^m},$$

sonst unvollkommen.

Wenn wir im folgenden von vollkommenen oder unvollkommenen Gruppen sprechen, so werden wir, sofern nichts anderes erwähnt, alle in der Definition erwähnten Eigenschaften voraussetzen.

Wegen K., § 5, Satz 7 sind die Primärgruppen mit zyklischer Faktorgruppe nach dem Kern vollkommen, die wir, soweit es bequem ist, wegen K., § 5-6 von der Betrachtung ausschließen können.

LEMMA 1: *Es sei $\mathfrak{G}$ vollkommen. Ist $\mathfrak{S}$ ein System mod $\mathfrak{N}(\mathfrak{G})$ unabhängiger Elemente, so bilden die Elemente $\mathfrak{c}(\mathfrak{s}) = \mathfrak{s}^{p^m}$ mit $\mathfrak{s}$ aus $\mathfrak{S}$ ein System unabhängiger Elemente aus $\mathfrak{N}(\mathfrak{G})$.*

BEWEIS: Es seien $\mathfrak{u}_1, \ldots, \mathfrak{u}_l$ irgend $l \geqq 1$ verschiedene Elemente aus $\mathfrak{S}$ und $1 = \prod_{i=1}^{l} \mathfrak{c}(\mathfrak{u}_i)^{w_i}$ mit $0 \leqq w_i < p^{n(\mathfrak{u}_i)}$, wo $p^{n(\mathfrak{u}_i)}$ die Ordnung von $\mathfrak{u}_i$ mod $\mathfrak{N}(\mathfrak{G})$ und also nach § 2, (2), 3 die Ordnung von $\mathfrak{c}(\mathfrak{u}_i)$ ist. Da die $\mathfrak{u}_i$ aus $\mathfrak{S}$ sind, so ist $\mathfrak{u} = \prod_{i=1}^{l} \mathfrak{u}_i^{w_i}$ dann und nur dann ein Element aus $\mathfrak{N}(\mathfrak{G})$, wenn $w_1 = \ldots = w_l = 0$ ist. Nun ist

$$\mathfrak{c}(\mathfrak{u}) = \mathfrak{u}^{p^m} = \left[\prod_{i=1}^{l} \mathfrak{u}_i^{w_i}\right]^{p^m} = \prod_{\substack{i=1 \\ w_i \neq 0}}^{l} (\mathfrak{u}_i^{w_i})^{p^m}, \text{ da } \mathfrak{G} \text{ vollkommen ist,}$$

$$= \prod_{\substack{i=1 \\ w_i \neq 0}}^{l} \left(\mathfrak{u}_i^{p^m}\right)^{w_i} = \prod_{i=1}^{l} \mathfrak{c}(\mathfrak{u}_i)^{w_i} = 1,$$

und nach § 2, (2), 3 ist also $\mathfrak{u}$ in $\mathfrak{R}(\mathfrak{G})$ enthalten, womit Lemma 1. bewiesen ist.

LEMMA 2: *$\mathfrak{G}$ sei vollkommen.*

a. *Für jedes $\mathfrak{u}$ liegt $\mathfrak{c}(\mathfrak{u})$ in $\mathfrak{Z}(\mathfrak{G})$.*

b. *Sind $\mathfrak{u}, \mathfrak{v}, \mathfrak{w}$ mod $\mathfrak{R}(\mathfrak{G})$ unabhängig*[10]*, so ist $[\mathfrak{u}, \mathfrak{v}]$ mit $\mathfrak{w}$ vertauschbar*[11]*.*

c. *Für jedes $\mathfrak{k}$ aus $\mathfrak{R}(\mathfrak{G})$ und beliebige $\mathfrak{u}, \mathfrak{v}$ gilt*[12]*:*

$$h(\mathfrak{k}, \mathfrak{u}) \equiv h(\mathfrak{k}, \mathfrak{v}) \text{ mod } p^{\min[n(\mathfrak{u}), n(\mathfrak{v})]}.$$

d. *Ist 2^n die Maximalordnung der Elemente aus $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ und ist $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ nicht zyklisch, so ist*[13]*:*

$$n < m.$$

BEWEIS: Es seien zunächst $\mathfrak{u}$ und $\mathfrak{v}$ zwei mod $\mathfrak{R}(\mathfrak{G})$ unabhängige Elemente. Nach Lemma 1. sind dann auch $\mathfrak{c}(\mathfrak{u})$ und $\mathfrak{c}(\mathfrak{v})$ unabhängige Elemente aus $\mathfrak{R}(\mathfrak{G})$. Weiter wird:

$$\begin{aligned}(\mathfrak{u}\mathfrak{v})^{-1}\mathfrak{k}(\mathfrak{u}\mathfrak{v}) &= \mathfrak{k}\mathfrak{c}(\mathfrak{u}\mathfrak{v})^{h(\mathfrak{k},\mathfrak{u}\mathfrak{v})} = \\ &= \mathfrak{k}\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{k},\mathfrak{u}\mathfrak{v})}\mathfrak{c}(\mathfrak{v})^{h(\mathfrak{k},\mathfrak{u}\mathfrak{v})} \\ &= \mathfrak{v}^{-1}(\mathfrak{u}^{-1}\mathfrak{k}\mathfrak{u})\mathfrak{v} = \mathfrak{v}^{-1}\mathfrak{k}\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{k},\mathfrak{u})}\mathfrak{v} = \\ &= \mathfrak{k}\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{k},\mathfrak{u})}\mathfrak{c}(\mathfrak{v})^{h(\mathfrak{k},\mathfrak{v})+h(\mathfrak{k},\mathfrak{u})h(\mathfrak{c}(\mathfrak{u}),\mathfrak{v})}.\end{aligned}$$

Also ist wegen § 2, (2), 3

$$h(\mathfrak{k}, \mathfrak{u}) \equiv h(\mathfrak{k}, \mathfrak{u}\mathfrak{v}) \text{ mod } p^{n(\mathfrak{u})}$$

und, da $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ abelsch ist, also $\mathfrak{u}\mathfrak{v}$ und $\mathfrak{v}\mathfrak{u}$ in $\mathfrak{R}(\mathfrak{G})$ denselben Automorphismus induzieren, auch

$$h(\mathfrak{k}, \mathfrak{v}) \equiv h(\mathfrak{k}, \mathfrak{u}\mathfrak{v}) \text{ mod } p^{n(\mathfrak{v})},$$

und hieraus folgt

$$h(\mathfrak{k}, \mathfrak{u})\, h(\mathfrak{c}(\mathfrak{u}), \mathfrak{v}) \equiv 0 \text{ mod } p^{n(\mathfrak{v})}.$$

Hieraus folgt a., da es Elemente $\mathfrak{k}$ mit $h(\mathfrak{k}, \mathfrak{u}) = 1$ gibt, und da $\mathfrak{c}(\mathfrak{u})$ mit $\mathfrak{u}$ vertauschbar ist.

Aus den beiden ersten Kongruenzen folgt c., falls $\mathfrak{u}, \mathfrak{v}$ mod $\mathfrak{R}(\mathfrak{G})$ unabhängig sind, und allgemein, wenn man bedenkt, daß $h(\mathfrak{k}, \mathfrak{u}^i) \equiv h(\mathfrak{k}, \mathfrak{u})$ und daß, falls $\mathfrak{u}, \mathfrak{v}$ mod $\mathfrak{R}(\mathfrak{G})$ abhängig sind,

---

[10]) Hier genügt es anzunehmen, daß $\mathfrak{c}(\mathfrak{u})$, $\mathfrak{c}(\mathfrak{v})$, $\mathfrak{c}(\mathfrak{w})$ unabhängig sind.

[11]) Hieraus und aus c. folgt, daß $[\mathfrak{u}, \mathfrak{v}]$ in $\mathfrak{Z}(\mathfrak{G})$ liegt, wenn $\mathfrak{w}$ von maximaler Ordnung mod $\mathfrak{R}(\mathfrak{G})$ ist.

[12]) $h(\mathfrak{k}, \mathfrak{u})$ bestimmt sich aus: $\mathfrak{u}^{-1}\mathfrak{k}\mathfrak{u} = \mathfrak{k}\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{k},\mathfrak{u})}$.

[13]) In § 10 wird sich zeigen, daß dies auch gilt, wenn $\mathfrak{G}$ unvollkommen ist.

etwa $\mathfrak{v} = \mathfrak{u}^i\mathfrak{w}$ mit mod $\mathfrak{R}(\mathfrak{G})$ unabhängigen $\mathfrak{u}, \mathfrak{w}$ oder $\mathfrak{u} = \mathfrak{v}^i\mathfrak{w}$ mit mod $\mathfrak{R}(\mathfrak{G})$ unabhängigem $\mathfrak{v}, \mathfrak{w}$ ist.

Sind $\mathfrak{u}, \mathfrak{v}, \mathfrak{w}$ mod $\mathfrak{R}(\mathfrak{G})$ unabhängig, so sind $\mathfrak{c}(\mathfrak{u})$, $\mathfrak{c}(\mathfrak{v})$, $\mathfrak{c}(\mathfrak{w})$ unabhängig und aus E., § 5, S. 407, Zusatz, Bedingung 2. folgt

$$1 = [\mathfrak{u}, \mathfrak{v}]\mathfrak{w}[\mathfrak{v}, \mathfrak{u}]\mathfrak{w}^{-1}[\mathfrak{v}, \mathfrak{w}]\mathfrak{u}[\mathfrak{w}, \mathfrak{v})\mathfrak{u}^{-1}[\mathfrak{w}, \mathfrak{u}]\mathfrak{v}[\mathfrak{u}, \mathfrak{w}]\mathfrak{u}^{-1} =$$
$$= \mathfrak{c}(\mathfrak{w})^{h([\mathfrak{u},\mathfrak{v}],\mathfrak{w})}\mathfrak{c}(\mathfrak{u})^{h([\mathfrak{v},\mathfrak{w}],\mathfrak{u})}\mathfrak{c}(\mathfrak{v})^{h([\mathfrak{w},\mathfrak{u}],\mathfrak{v})},$$

woraus b. folgt.

Um schließlich d. zu beweisen, betrachten wir ein $\mathfrak{m}$ mit $n(\mathfrak{m}) = n$. Da $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ nicht zyklisch ist, so gibt es ein $\mathfrak{u}$, so daß $\mathfrak{m}, \mathfrak{u}$ mod $\mathfrak{R}(\mathfrak{G})$ unabhängig sind, und da $p = 2$ ist, also $m > 1$ nach § 2, (2), 5, so kann $\mathfrak{u}$ so bestimmt werden, daß $n(\mathfrak{u}) < m$ wird. Schließlich gibt es ein $\mathfrak{n}$ in $\mathfrak{R}(\mathfrak{G})$ mit $h(\mathfrak{n}, \mathfrak{m}) = 1$ und aus c. folgt dann $h(\mathfrak{n}, \mathfrak{v}) = 1$ für jedes $\mathfrak{v}$.

Aus § 2, (4) folgt:

$$\mathfrak{c}(\mathfrak{n}\mathfrak{v}) = \mathfrak{c}(\mathfrak{v})^{1+2^{m-1}} \text{ für jedes } \mathfrak{v}$$

und, falls $n(\mathfrak{v}) < m$ ist, wegen § 2, (2), 3 sogar:

$$\mathfrak{c}(\mathfrak{n}\mathfrak{v}) = \mathfrak{c}(\mathfrak{v}).$$

So erhalten wir:

$$\mathfrak{c}(\mathfrak{n}\mathfrak{u}\mathfrak{m}) = \mathfrak{c}(\mathfrak{u}\mathfrak{m})^{1+2^{m-1}} = \mathfrak{c}(\mathfrak{u})\mathfrak{c}(\mathfrak{m})^{1+2^{m-1}}, \text{ da } n(\mathfrak{u}) < m,$$
$$= \mathfrak{c}(\mathfrak{n}\mathfrak{u})\mathfrak{c}(\mathfrak{m}) = \mathfrak{c}(\mathfrak{u})\mathfrak{c}(\mathfrak{m}),$$

also $1 = \mathfrak{c}(\mathfrak{m})^{2^{m-1}}$, also $n = n(\mathfrak{m}) \leqq m - 1$, womit d. bewiesen ist.

Im folgenden sei stets $\chi_{\mathfrak{g}}(\mathfrak{k}) = \mathfrak{g}^{-1}\mathfrak{k}\mathfrak{g}$ der von $\mathfrak{g}$ in $\mathfrak{R}(\mathfrak{G})$ induzierte Automorphismus, $\mathbf{A}(\mathfrak{G})$ die Gruppe aller in $\mathfrak{R}(\mathfrak{G})$ induzierten Automorphismen, $\mathfrak{D}(\mathfrak{G})$ die Gesamtheit aller Elemente $\mathfrak{k}^{-1}\chi_{\mathfrak{g}}(\mathfrak{k})$ mit $\mathfrak{k}$ aus $\mathfrak{R}(\mathfrak{G})$.

Satz 1: *Es sei $\mathfrak{G}$ vollkommen.*

a. *$\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$, $\mathbf{A}(\mathfrak{G})$ und $\mathfrak{D}(\mathfrak{G})$ sind isomorphe Gruppen.*

b. *$\{\chi_{\mathfrak{g}}\} \to \{\mathfrak{c}(\mathfrak{g})\}$ definiert eine situationstreue Abbildung*[14]) *von $\mathbf{A}(\mathfrak{G})$ auf $\mathfrak{D}(\mathfrak{G})$.*

c. *$\chi_{\mathfrak{g}} \to \mathfrak{c}(\mathfrak{g})$ ist eine isomorphe Abbildung von $\mathbf{A}(\mathfrak{G})$ auf $\mathfrak{D}(\mathfrak{G})$ und entsprechend $\mathfrak{R}(\mathfrak{G})\mathfrak{g} \to \mathfrak{c}(\mathfrak{g})$ eine isomorphe Abbildung von $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ auf $\mathfrak{D}(\mathfrak{G})$. [Reziprozitätsgesetz.]*

Bemerkung: Die Einschiebung der Aussage b. hat ihren Sinn darin, daß zur Herstellung der Zuordnung b. nur die Kenntnis

[14]) Für den Begriff der situationstreuen Abbildung vergl. etwa K., § 7.

der Automorphismengruppe $\mathbf{A}(\mathfrak{G})$ nötig ist, zur Herstellung der Zuordnung c. aber die Kenntnis der ganzen Gruppe $\mathfrak{G}$. Im § 9 wird sich zeigen, daß es Primärgruppen mit wesentlichem Kern und abelscher Faktorgruppe nach dem Kern gibt, in denen a., b., aber nicht c. richtig ist.

Beweis: Wenn $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ zyklisch ist, ist unser Satz eine Folge von K., § 5, Satz 7; wir können also annehmen, daß $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ nicht zyklisch ist.

Nach § 2, (3) existiert eine Basis $\mathfrak{B}$ von $\mathfrak{G}$ mod $\mathfrak{R}(\mathfrak{G})$. Dann stellen die Elemente

$$\prod_{i=1}^{b} \mathfrak{b}_i^{b_i} \text{ mit } 0 \leqq b,\ 0 \leqq b_i < p^{n(\mathfrak{b}_i)},\ \mathfrak{b}_i \text{ aus } \mathfrak{B},\ \mathfrak{b}_i \neq \mathfrak{b}_k \text{ für } i \neq k,$$

ein volles Repräsentantensystem von $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ dar [bei Benutzung einer Wohlordnung von $\mathfrak{B}$].

Da $\mathfrak{G}$ vollkommen ist, so ist

$$\mathfrak{c}\left(\prod_{i=1}^{b} \mathfrak{b}_i^{b_i}\right) = \prod_{i=1}^{b} \mathfrak{c}(\mathfrak{b}_i)^{b_i}$$

und wir definieren:

$$\alpha\left(\mathfrak{R}(\mathfrak{G}) \prod_{i=1}^{b} \mathfrak{b}_i^{b_i}\right) = \mathfrak{c}\left(\prod_{i=1}^{b} \mathfrak{b}_i^{b_i}\right).$$

Offenbar ist α eine in ganz $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ definierte, eindeutige[15]) Abbildung auf einen Teil von $\mathfrak{D}(\mathfrak{G})$.

Da wegen § 2, (4) und wegen Lemma 2., d. gilt

$$\mathfrak{c}(\mathfrak{f}\mathfrak{g}) = \mathfrak{c}(\mathfrak{g}) \text{ für jedes } \mathfrak{f} \text{ aus } \mathfrak{R}(\mathfrak{G}),\ \text{jedes } \mathfrak{g} \text{ aus } \mathfrak{G},$$

so wird $\alpha(\mathfrak{G}/\mathfrak{R}(\mathfrak{G})) = \mathfrak{D}(\mathfrak{G})$, und hieraus folgt auch, daß α multiplikativ ist.

Schließlich ist α umkehrbar eindeutig nach Lemma 1., da $\mathfrak{B}$ eine Basis von $\mathfrak{G}$ mod $\mathfrak{R}(\mathfrak{G})$ ist. α ist also ein Isomorphismus, und daraus folgen a., b., c.

Satz 2: *Es sei $\mathfrak{G}$ eine Primärgruppe mit wesentlichem Kern und $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ abelsch, aber nicht zyklisch.*

a. *$\mathfrak{G}$ ist vollkommen, wenn $p \neq 2$, $p \neq 3$.*

b. *Ist $p = 3$, so ist $\mathfrak{G}$ dann und nur dann vollkommen, wenn für irgendzwei mod $\mathfrak{R}(\mathfrak{G})$ unabhängige Elemente $\mathfrak{u}, \mathfrak{v}$ gilt:*

$$[\mathfrak{u}, \mathfrak{v}]^{3^{m-1}} \textit{ liegt in } \mathfrak{Z}(\mathfrak{G}).$$

---

[15]) Wenn man noch $\mathfrak{B}$ irgendwie wohlordnet und die Reihenfolge der Faktoren gemäß dieser Wohlordnung festlegt; übrigens ist der Wert von α von der gewählten Wohlordnung unabhängig, wie aus der Formel $\mathfrak{c}(\mathfrak{f}\mathfrak{g}) = \mathfrak{c}(\mathfrak{g})$ für $\mathfrak{f}$ aus $\mathfrak{R}(\mathfrak{G})$ folgt.

c. *Ist* $p = 2$, *so ist* $\mathfrak{G}$ *dann und nur dann vollkommen, wenn* [16])

$$n < m \text{ und } [\mathfrak{u}, \mathfrak{v}]^{2^{m-1}} = 1$$

für irgendzwei mod $\mathfrak{R}(\mathfrak{G})$ *unabhängige Elemente* $\mathfrak{u}, \mathfrak{v}$ *gilt* [17]).

Beweis: a. folgt aus § 2, (7), b. folgt aus § 2, (7) in Verbindung mit Lemma 1. und Lemma 2., b. — Die Notwendigheit der in c. angegebenen Bedingungen folgt aus Lemma 2., d., Lemma 2., a. und § 2, (7); sind aber unsere Bedingungen erfüllt, so folgt aus § 2, (5), b., daß jedes $\mathfrak{c}(\mathfrak{g})$ in $\mathfrak{Z}(\mathfrak{G})$ liegt, und aus § 2, (7) dann die Vollkommenheit von $\mathfrak{G}$.

Zusatz: *Ist* $\mathfrak{G}$ *eine Primärgruppe mit wesentlichem Kern, so ist dann und nur dann* $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ *abelsch, wenn* $\mathfrak{D}(\mathfrak{G}) \leqq \mathfrak{Z}(\mathfrak{G})$ *gilt.*

Die Notwendigkeit der Bedingung folgt für vollkommene Gruppen aus Lemma 2. a.; für unvollkommene Gruppen wird sie im § 9, § 10 hergeleitet werden. — Ist umgekehrt die Bedingung erfüllt, so wird:

$$(\mathfrak{u}\mathfrak{v})^{-1}\mathfrak{f}(\mathfrak{u}\mathfrak{v}) = \mathfrak{f}\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{f},\mathfrak{u})}\mathfrak{c}(\mathfrak{v})^{h(\mathfrak{f},\mathfrak{u})} = (\mathfrak{v}\mathfrak{u})^{-1}\mathfrak{f}(\mathfrak{v}\mathfrak{u}),$$

d.h. $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ ist abelsch.

§ 4.

Automorphismengruppen mit Reziprozitätsgesetz.

Es sei $\mathfrak{A}$ eine abelsche Primärgruppe, und p^m die [endliche] Maximalordnung der Elemente von $\mathfrak{A}$. Ist $\mathbf{A}$ eine Gruppe von [eigentlichen] Automorphismen von $\mathfrak{A}$, so sei

$\mathfrak{Z}(\mathbf{A})$ = Gesamtheit der $\alpha(\mathfrak{z}) = \mathfrak{z}$ für jedes α aus $\mathbf{A}$ erfüllenden Elemente $\mathfrak{z}$ aus $\mathfrak{A}$,

$\mathfrak{D}(\mathbf{A})$ = Gesamtheit der Elemente $\mathfrak{f}\alpha(\mathfrak{f}^{-1})$ mit α aus $\mathbf{A}$, $\mathfrak{f}$ aus $\mathfrak{A}$.

Definition 1.: $\mathbf{A}$ *heißt vollkommen* [18]), *wenn*

1. $\mathfrak{D}(\mathbf{A}) \leqq \mathfrak{Z}(\mathbf{A})$,

2. *es eine isomorphe Abbildung* $\mathfrak{c} = \mathfrak{c}(\alpha)$ *von* $\mathbf{A}$ *auf die Gesamtheit* [*und also Gruppe*] $\mathfrak{D}(\mathbf{A})$ *gibt, so daß gilt:*

21. $\alpha(\mathfrak{f}) = \mathfrak{f}\mathfrak{c}(\alpha)^{h(\mathfrak{f},\alpha)}$ *für jedes* $\mathfrak{f}$ *aus* $\mathfrak{A}$;

---

[16]) Im § 10 wird sich zeigen, daß auch die unvollkommenen Gruppen $n < m$, nämlich $n = 1$, $m = 2$ erfüllen.

[17]) Die Existenz unvollkommener Gruppen wird in § 9 für $p = 3$ und in § 10 für $p = 2$ gezeigt.

[18]) In § 5 wird gezeigt werden, daß vollkommene Gruppen in ihrem Kern vollkommene Automorphismengruppen induzieren.

2 2. *es gibt ein Element* $\mathfrak{a}(\alpha)$ *in* $\mathfrak{A}$, *so daß* $\mathfrak{a}(\alpha)^{p^{m-n(\alpha)}} = \mathfrak{c}(\alpha)$, *wo* $p^{n(\alpha)}$ *die Ordnung von* α *ist, und* $\alpha[\mathfrak{a}(\alpha)] = \mathfrak{a}(\alpha)$.

Es ist also **A** eine Primärgruppe und, wenn p^n die Maximalordnung in **A** ist, so ist $n \leqq m$. In den Anwendungen werden wir noch annehmen, daß $n < m$, falls $p = 2$ ist. — Weiter ist $p^{n(\alpha)}$ auch die Ordnung von $\mathfrak{c}(\alpha)$ und also $\mathfrak{a}(\alpha)$ ein Element von der in $\mathfrak{A}$ maximalen Ordnung p^m.

Man bemerke weiter:

ist $\bar{\mathfrak{c}}(\alpha)$ *eine zweite* 2. *genügende isomorphe Abbildung von* **A** *auf* $\mathfrak{D}(\mathbf{A})$, *so gibt es eine zu* p *teilerfremde Zahl* c, *so daß* $\bar{\mathfrak{c}}(\alpha) = \mathfrak{c}(\alpha)^c\,[= \mathfrak{c}(\alpha^c)]$ *für alle* α *aus* **A** *gilt.*

Durch die Zuordnung: $\gamma[\mathfrak{c}(\alpha)] = \bar{\mathfrak{c}}(\alpha)$ wird nämlich ein Automorphismus γ von $\mathfrak{D}(\mathbf{A})$ erklärt, bei dem wegen 2 1. jeder Zyklus von $\mathfrak{D}(\mathbf{A})$ in sich übergeht. Also ist sicher

$$\bar{\mathfrak{c}}(\alpha) = \mathfrak{c}(\alpha)^{c(\alpha)}, \text{ wo } (\mathfrak{c}(\alpha), p) = 1 \text{ ist.}$$

Sind dann α und β unabhängig, so sind auch $\mathfrak{c}(\alpha)$ und $\mathfrak{c}(\beta)$ unabhängig, und es wird:

$$\begin{aligned}\mathfrak{c}(\alpha\beta)^{c(\alpha\beta)} &= \mathfrak{c}(\alpha)^{c(\alpha\beta)}\,\mathfrak{c}(\beta)^{c(\alpha\beta)} \\ &= \mathfrak{c}(\alpha)^{c(\alpha)}\,\mathfrak{c}(\beta)^{c(\beta)},\end{aligned}$$

also $\mathfrak{c}(\alpha) \equiv \mathfrak{c}(\beta) \equiv \mathfrak{c}(\alpha\beta) \bmod p^{\min[n(\alpha),\, n(\beta)]}$, woraus unsere Behauptung folgt.

Satz 1. *Es sei* $\mathfrak{A}$ *eine abelsche Primärgruppe,* p^m *die (endliche) Maximalordnung der Elemente von* $\mathfrak{A}$ *und* $\mathfrak{Z}$, $\mathfrak{D}$ *zwei Untergruppen von* $\mathfrak{A}$.

Dann und nur dann gibt es eine vollkommene Gruppe **A** *von Automorphismen von* $\mathfrak{A}$, *die*

$$\mathfrak{Z}(\mathbf{A}) = \mathfrak{Z} \text{ und } \mathfrak{D}(\mathbf{A}) = \mathfrak{D}$$

erfüllt, wenn

1.) $\mathfrak{A}/\mathfrak{Z}$ *zyklisch ist und es*

2.) *einen direkten Faktor von* $\mathfrak{A}$ *gibt, der* $\mathfrak{D}$ *enthält, in* $\mathfrak{Z}$ *enthalten ist und direktes Product von Zyklen der Ordnung* p^m *ist.*

Beweis: A. Es sei **A** eine vollkommene Automorphismengruppe von $\mathfrak{A}$ und $\mathfrak{a}(\alpha)$, $\mathfrak{c}(\mathfrak{a})$ die in die Definition der Vollkommenheit eingehenden Funktionen.

(1) *Ist* μ *ein Element aus* **A** *von der in* **A** *maximalen Ordnung* p^n, *so ist*

$$\mathfrak{Z}(\mathbf{A}) = \mathfrak{Z}(\{\mu\}).$$

Wegen $\{\mu\} \leqq \mathbf{A}$ ist $\mathfrak{Z}(\mathbf{A}) \leqq \mathfrak{Z}(\{\mu\})$. Ist umgekehrt $\mathfrak{w}$ aus $\mathfrak{Z}(\{\mu\})$ und α aus $\mathbf{A}$, so ist $\alpha = \mu^i\beta$, wo μ und β unabhängig sind, wenn $\beta \neq 1$ ist, wie aus K., § 5, Lemma folgt, da μ von in $\mathbf{A}$ maximaler Ordnung ist. Es gilt

$$\begin{aligned}\beta[\mu(\mathfrak{w})] &= \beta(\mathfrak{w}) = \mathfrak{w}\mathfrak{c}(\beta)^{h(\mathfrak{w},\beta)}\\ &= \mathfrak{w}\mathfrak{c}(\mu\beta)^{h(\mathfrak{w},\mu\beta)} =\\ &= \mathfrak{w}\mathfrak{c}(\mu)^{h(\mathfrak{w},\mu\beta)}\mathfrak{c}(\beta)^{h(\mathfrak{w},\mu\beta)},\end{aligned}$$

und, da mit μ und β auch $\mathfrak{c}(\mu)$ und $\mathfrak{c}(\beta)$ unabhängig sind, so wird:

$$\begin{aligned}0 &\equiv h(\mathfrak{w}, \mu\beta) \bmod p^n,\\ h(\mathfrak{w}, \beta) &\equiv h(\mathfrak{w}, \mu\beta) \bmod p^{n(\beta)},\end{aligned}$$

also $\beta(\mathfrak{w}) = \alpha(\mathfrak{w}) = \mathfrak{w}$, womit (1) bewiesen ist.

(2) $\mathfrak{A}/\mathfrak{Z}(\mathbf{A})$ ist ein Zyklus der Ordnung p^n.

Dies folgt aus (1), da $\mathfrak{A}/\mathfrak{Z}(\{\mu\})$ ein Zyklus der Ordnung p^n ist [vergl. Definition 1., bes. 2, 1.].

(3) *Es gibt Elemente* $\mathfrak{e}$ *in* $\mathfrak{A}$, *die* $\alpha(\mathfrak{e}) = \mathfrak{e}\mathfrak{c}(\alpha)$ *für jedes* α *aus* $\mathbf{A}$ *erfüllen.*

Es sei μ ein Element von der in $\mathbf{A}$ maximalen Ordnung p^n. Da μ und $\mathfrak{c}(\mu)$ dieselbe Ordnung haben, so gibt es sicher Elemente $\mathfrak{e}$ in $\mathfrak{A}$, die $\mu(\mathfrak{e}) = \mathfrak{e}\mathfrak{c}(\mu)$ erfüllen.

Ist jetzt β aus $\mathbf{A}$ so, daß μ und β unabhängig sind, so wird:

$$\begin{aligned}\beta[\mu(\mathfrak{e})] &= \beta[\mathfrak{e}\mathfrak{c}(\mu)] = \beta(\mathfrak{e})\mathfrak{c}(\mu) \text{ nach Definition 1., 1.}\\ &= \mathfrak{e}\mathfrak{c}(\beta)^{h(\mathfrak{e},\beta)}\mathfrak{c}(\mu)\\ &= \mathfrak{e}\mathfrak{c}(\beta\mu)^{h(\mathfrak{e},\beta\mu)} = \mathfrak{e}\mathfrak{c}(\beta)^{h(\mathfrak{e},\beta\mu)}\mathfrak{c}(\mu)^{h(\mathfrak{e},\beta\mu)};\end{aligned}$$

da mit β und μ auch $\mathfrak{c}(\beta)$ und $\mathfrak{c}(\mu)$ unabhängig sind, so wird:

$$h(\mathfrak{e}, \beta\mu) \equiv 1 \bmod p^n,\ h(\mathfrak{e}, \beta\mu) \equiv h(\mathfrak{e}, \beta) \bmod p^{n(\beta)},$$

also $\beta(\mathfrak{e}) = \mathfrak{e}\mathfrak{c}(\beta)$.

Ist nun α irgendein Automorphismus aus $\mathbf{A}$, so ist wieder $\alpha = \mu^i\beta$, wo μ, β unabhängig sind, wenn nur $\beta \neq 1$ ist, und es wird:

$$\begin{aligned}\alpha(\mathfrak{e}) &= \beta[\mu^i(\mathfrak{e})] = \beta[\mathfrak{e}\mathfrak{c}(\mu^i)] = \mathfrak{e}\mathfrak{c}(\beta)\mathfrak{c}(\mu^i)\\ &= \mathfrak{e}\mathfrak{c}(\beta\mu^i) = \mathfrak{e}\mathfrak{c}(\alpha).\end{aligned}$$

Damit ist (3) gezeigt und wegen (2) auch:

(4) *Ist* $\mathfrak{e}$ *ein Element aus* $\mathfrak{A}$, *das* $\alpha(\mathfrak{e}) = \mathfrak{e}\mathfrak{c}(\alpha)$ *für jedes* α *aus* $\mathbf{A}$ *erfüllt, und ist* $\mathfrak{u}$ *aus* $\mathfrak{A}$, *so daß* $\mathfrak{u}\mathfrak{e}^{-i}$ *in* $\mathfrak{Z}(\mathbf{A})$ *liegt, so ist:*

$$\alpha(\mathfrak{u}) = \mathfrak{u}\mathfrak{c}(\alpha)^i.$$

(5) *Jedes Element aus* $\mathfrak{D}(\mathbf{A})$ *ist Potenz eines Elementes der Ordnung* p^m *aus* $\mathfrak{Z}(\mathbf{A})$.

Sei $\mathfrak{e}$ ein Element niederster Ordnung unter den $\alpha(\mathfrak{e}) = \mathfrak{e}\mathfrak{c}(\alpha)$ für jedes α aus $\mathbf{A}$ erfüllenden Elementen; ein solches existiert nach (3). $\mathfrak{e}$ ist dann Repräsentant einer erzeugenden Restklasse von $\mathfrak{A}/\mathfrak{Z}(\mathbf{A})$ [wegen (1), (2)].

Ist β aus $\mathbf{A}$ beliebig, so ist also $\mathfrak{a}(\beta) = \mathfrak{e}^u\mathfrak{u}$ mit $0 \leqq u < p^n$, $\mathfrak{u}$ in $\mathfrak{Z}(\mathbf{A})$.

Ist $u = 0$, so ist nichts mehr zu zeigen; ist $u \neq 0$, so ist $u = u'p^{u''}$ mit $(u', p) = 1$, $0 \leqq u'' < n$.

Wegen Definition 2, 2 ist:

$$\mathfrak{a}(\beta) = \beta[\mathfrak{a}(\beta)] = \beta[\mathfrak{e}^u\mathfrak{u}] = \mathfrak{e}^u\mathfrak{u}\mathfrak{c}(\beta)^u = \mathfrak{a}(\beta)\mathfrak{c}(\beta)^u \text{ nach (4)};$$

also wird $\mathfrak{c}(\beta)^u = 1$, d.h. $u'' \geqq n(\beta) > 0$.

Weiter ist

$$\mathfrak{u}^{p^{m-1}} = \mathfrak{a}(\beta)^{p^{m-1}}\mathfrak{e}^{-u'p^{m-1+u''}} = \mathfrak{a}(\beta)^{p^{m-1}}, \text{ da } u'' > 0,$$

und dies ist $\neq 1$, also $\mathfrak{u}$ wie $\mathfrak{a}(\beta)$ von der Ordnung p^m.

Schließlich ist

$$\mathfrak{u}^{p^{m-n(\beta)}} = \mathfrak{a}(\beta)^{p^{m-n(\beta)}}\mathfrak{e}^{-u'p^{m-n(\beta)+u''}} = \mathfrak{c}(\beta), \text{ da } u'' \geqq n(\beta),$$

und damit (5) erwiesen, da $\mathfrak{u}$ in $\mathfrak{Z}(\mathbf{A})$ liegt.

Aus (5) folgt jetzt die Notwendigkeit der Bedingung 2.): sei nämlich $\mathfrak{B}$ eine Basis von $\mathfrak{D}(\mathbf{A})$; eine solche existiert nach K., § 5, Lemma. Dann existiert nach (5) ein System $\mathfrak{B}^*$ in $\mathfrak{Z}(\mathbf{A})$, dessen sämtliche Elemente die Ordnung p^m haben, und so daß jedes Element aus $\mathfrak{B}$ Potenz genau eines Elementes aus $\mathfrak{B}^*$, eine gewisse Potenz jedes Elementes aus $\mathfrak{B}^*$ ein Element aus $\mathfrak{B}$ ist. $\mathfrak{B}^*$ läßt sich dann (genau wie beim Beweise von K., § 5. Lemma) zu einer Basis von $\mathfrak{A}$ ergänzen, so daß die von $\mathfrak{B}^*$ erzeugte Untergruppe von $\mathfrak{A}$ genau die in Bedingung 2.) geforderten Eigenschaften hat.

B. Sind umgekehrt die Bedingungen 1.) und 2.) erfüllt, so ist $\mathfrak{A}/\mathfrak{Z}$ ein Zyklus der Ordnung p^n, und es sei $\mathfrak{e}$ ein beliebiges in einer erzeugenden Restklasse von $\mathfrak{A}/\mathfrak{Z}$ enthaltenes Element. Dann läßt sich jedes Element aus $\mathfrak{A}$ eindeutig auf die Form

$$\mathfrak{e}^z\mathfrak{z} \text{ mit } 0 \leqq z < p^n, \ \mathfrak{z} \text{ in } \mathfrak{Z}$$

bringen.

Ist $\mathfrak{c}$ ein Element aus $\mathfrak{D}$, so definieren wir:

$$\varphi_{\mathfrak{c}}(\mathfrak{e}^z\mathfrak{z}) = \mathfrak{e}^z\mathfrak{z}\mathfrak{c}^z.$$

$\varphi_\mathfrak{c}$ ist für jedes $\mathfrak{c}$ eindeutig in ganz $\mathfrak{A}$ definiert, und da $\mathfrak{c}$ in $\mathfrak{Z}$ liegt, so ist $\varphi_\mathfrak{c}(\mathfrak{A}) = \mathfrak{A}$.

Ist weiter

$$\varphi_\mathfrak{c}(\mathfrak{e}^x\mathfrak{x}) = \varphi_\mathfrak{c}(\mathfrak{e}^y\mathfrak{y}), \text{ so ist auch } \mathfrak{e}^x\mathfrak{x}\mathfrak{c}^x = \mathfrak{e}^y\mathfrak{y}\mathfrak{c}^y,$$

also, da $\mathfrak{c}$ in $\mathfrak{Z}$ liegt, $0 \leqq x,\ y < p^n$ ist, $x = y$ und infolgedessen $\mathfrak{x} = \mathfrak{y}$, d.h. $\varphi_\mathfrak{c}$ ist umkehrbar eindeutig.

Schließlich ist, falls $x + y = z + ep^n$ mit $0 \leqq x, y, z < p^n$, $e = 0, 1$ ist

$$\varphi_\mathfrak{c}(\mathfrak{e}^x\mathfrak{x})\varphi_\mathfrak{c}(\mathfrak{e}^y\mathfrak{y}) = \mathfrak{e}^{x+y}\mathfrak{x}\mathfrak{y}\,\mathfrak{c}^{x+y} = \mathfrak{e}^z[\mathfrak{e}^{ep^n}\mathfrak{x}\mathfrak{y}]\,\mathfrak{c}^z,$$

da ja p^n die Maximalordnung in $\mathfrak{D}$ ist,

$$= \varphi_\mathfrak{c}(\mathfrak{e}^z[\mathfrak{e}^{ep^n}\mathfrak{x}\mathfrak{y}]) = \varphi_\mathfrak{c}(\mathfrak{e}^{x+y}\mathfrak{x}\mathfrak{y}) = \varphi_\mathfrak{c}(\mathfrak{e}^x\mathfrak{x}\cdot\mathfrak{e}^y\mathfrak{y}), \qquad \text{d.h.}$$

$\varphi_\mathfrak{c}$ ist ein Automorphismus.

Setzen wir $\mathfrak{c}(\varphi_\mathfrak{c}) = \mathfrak{c}$, so ist dann und nur dann $\varphi_{\mathfrak{c}'} = \varphi_\mathfrak{c}$, wenn $\mathfrak{c}(\varphi_{\mathfrak{c}'}) = \mathfrak{c}(\varphi_\mathfrak{c})$ ist. Weiter ist:

$$\begin{aligned}\varphi_{\mathfrak{c}\mathfrak{c}'}(\mathfrak{e}^z\mathfrak{z}) &= \mathfrak{e}^z\mathfrak{z}(\mathfrak{c}\mathfrak{c}')^z = \mathfrak{e}^z\mathfrak{z}\mathfrak{c}^z\mathfrak{c}'^z = \\ &= \varphi_{\mathfrak{c}'}(\mathfrak{e}^z\mathfrak{z}\mathfrak{c}^z), \text{ da } \mathfrak{c} \text{ in } \mathfrak{Z}, \\ &= \varphi_{\mathfrak{c}'}[\varphi_\mathfrak{c}(\mathfrak{e}^z\mathfrak{z})],\end{aligned}$$

d.h. $\varphi_{\mathfrak{c}\mathfrak{c}'} = \varphi_\mathfrak{c}\varphi_{\mathfrak{c}'}$ und also

$$\mathfrak{c}(\varphi_\mathfrak{c}\varphi_{\mathfrak{c}'}) = \mathfrak{c}(\varphi_{\mathfrak{c}\mathfrak{c}'}) = \mathfrak{c}\mathfrak{c}' = \mathfrak{c}(\varphi_\mathfrak{c})\mathfrak{c}(\varphi_{\mathfrak{c}'})$$

und damit ist die Gruppe $\mathbf{A}$ aller $\varphi_\mathfrak{c}$ mit $\mathfrak{c}$ in $\mathfrak{D}$ als vollkommen erwiesen.

$\mathfrak{Z}(\mathbf{A}) = \mathfrak{Z}$ und $\mathfrak{D}(\mathbf{A}) = \mathfrak{D}$ folgen unmittelbar aus der Definition von $\mathbf{A}$.

Damit ist unser Satz bewiesen und wegen (3), (4) auch der

Zusatz 1: *Ist* $\mathbf{A}$ *vollkommen,* $\mathfrak{c}(\alpha)$ *eine der Definition* 1. *genügende isomorphe Abbildung von* $\mathbf{A}$ *auf* $\mathfrak{D}(\mathbf{A})$, *so ist*

$$\alpha(\mathfrak{k}) = \mathfrak{k}\mathfrak{c}(\alpha)^{h(\mathfrak{k})} \text{ für } \mathfrak{k} \text{ aus } \mathfrak{A},$$

wo $h(\mathfrak{k})$ *nur von* $\mathfrak{k}$, *nicht von* α *abhängt.*

Die Invarianten vollkommener Automorphismengruppen.

Ist $\mathbf{A}$ eine vollkommene Gruppe von Automorphismen der abelschen Primärgruppe $\mathfrak{A}$, so ist $\mathfrak{A}/\mathfrak{Z}(\mathbf{A})$ zyklisch von der Ordnung p^n, wo p^n gleichzeitig die Maximalordnung der Elemente von $\mathbf{A}$ ist: $n = n(\mathbf{A})$.

Haben zwei Restklassen von $\mathfrak{A}/\mathfrak{Z}(\mathbf{A})$ die gleiche Ordnung p^i mit $0 \leqq i \leqq n$, so ist die Minimalordnung ihrer Elemente dieselbe, etwa p^{n_i} und es ist

$$0 = n_0 - 0 \leqq n_1 - 1 \leqq \ldots \leqq n_i - i \leqq \ldots \leqq n_n - n.$$

Unter diesen $n+1$ Zahlen $n_i - i$ sind $u+1 = u(\mathbf{A})+1$ verschiedene und es seien die Zahlen $u(i, \mathbf{A})$ für $0 \leqq i \leqq u(\mathbf{A})$ so bestimmt, daß $n_j - j < n_{j+1} - j - 1$ dann und nur dann, wenn $j = u(i, \mathbf{A})$ für geeignetes i. Schließlich sei $v(i, \mathbf{A}) = n_{u(i,\mathbf{A})}$ und

$$0 = u(0, \mathbf{A}) = v(0, \mathbf{A}),\ n = u(u(\mathbf{A}), \mathbf{A}),\ u(i, \mathbf{A}) < u(i+1, \mathbf{A}).$$

Ist $\mathfrak{P}$ eine abelsche Gruppe, deren sämtliche Elemente $\neq 1$ die Ordnung p haben, so ist $\mathfrak{P}$ direktes Produkt von Zyklen der Ordnung p und die Anzahl dieser Faktoren ist dieselbe in allen derartigen Produktzerlegungen. Sie heißt der *Grad* $d = d(\mathfrak{P})$ von $\mathfrak{P}$. Die Anzahl der Elemente von $\mathfrak{P}$ ist dann p^d oder d, je nachdem $\mathfrak{P}$ endlich oder unendlich ist.

Es sei $\mathfrak{A}^i$ die Untergruppe aller Elemente einer Ordnung $\leqq p$, die Potenzen von Elementen der Ordnung p^i sind. Dann sei:

$$w(\mathbf{A}) = d\big(\mathfrak{A}^m/\mathfrak{A}^m \cap \mathfrak{D}(\mathbf{A})\big),$$

wo p^m die Maximalordnung in $\mathfrak{A}$ ist.

ZUSATZ 2: *Es sei $\mathfrak{A}$ eine abelsche Primärgruppe der (endlichen) Maximalordnung p^m und $\mathbf{A}$ eine vollkommene Gruppe von Automorphismen von $\mathfrak{A}$.*

Dann ist

$$\mathfrak{A} = \prod_{i=1}^{u(\mathbf{A})} \{\mathfrak{e}_i\} \times \mathfrak{B} \times \prod_{\nu} \{\mathfrak{m}_\nu\},$$

wo $p^{v(i,\mathbf{A})}$ die Ordnung von $\mathfrak{e}_i$, p^m die von $\mathfrak{m}_\nu$ ist;

$$\mathfrak{Z}(\mathbf{A}) = \prod_{i=1}^{u(\mathbf{A})} \{\mathfrak{e}_{i-1}\mathfrak{e}_i^{-p^{u(i,\mathbf{A})-u(i-1,\mathbf{A})}}\} \times \mathfrak{B} \times \prod_{\nu} \{\mathfrak{m}_\nu\},\quad \mathfrak{e}_0 = 1;$$

$$\mathfrak{D}(\mathbf{A}) = \prod_{\nu} \{\mathfrak{m}_\nu^{p^{k_\nu}}\},\quad 0 \leqq k_\nu < m.$$

Dabei ist $w(\mathbf{A}) = d(\mathfrak{B}^m)$, *wenn* $v(u(\mathbf{A}), \mathbf{A}) < m$ *ist,*
$= d(\mathfrak{B}^m) + 1$, *wenn* $v(u(\mathbf{A}), \mathbf{A}) = m$ *ist.*

BEWEIS: Nach Satz 1. ist $\mathfrak{A}/\mathfrak{Z}(\mathbf{A})$ zyklisch von der Ordnung p^n. Weiter ist nach Satz 1. $\mathfrak{A} = \mathfrak{A}^* \times \prod_{\nu} \{\mathfrak{m}_\nu\}$, wo $\mathfrak{m}_\nu$ ein Element der Ordnung p^m aus $\mathfrak{Z}(\mathbf{A})$ ist, $\mathfrak{D}(\mathbf{A})$ in $\prod_{\nu} \{\mathfrak{m}_\nu\}$, aber in keinem

echten Faktor enthalten ist. Ist dann $\mathfrak{Z}^* = \mathfrak{A}^* \cap \mathfrak{Z}(\mathbf{A})$, so ist auch $\mathfrak{A}^*/\mathfrak{Z}^*$ zyklisch von der Ordnung p^n, und die Minimalordnungen in den Restklassen von $\mathfrak{A}^*/\mathfrak{Z}^*$ sind dieselben wie in den entsprechenden sie enthaltenden Restklassen von $\mathfrak{A}/\mathfrak{Z}(\mathbf{A})$. Sei dann $\mathfrak{e}_{u(\mathbf{A})}$ ein Element niederster Ordnung aus einer $\mathfrak{A}^*/\mathfrak{Z}^*$ erzeugenden Restklasse und $\mathfrak{e}_i$ für $0 \leqq i < u(\mathbf{A})$ ein Element niederster Ordnung aus $\mathfrak{Z}^* \mathfrak{e}_{u(\mathbf{A})}^{p^{n-u(i,\mathbf{A})}}$, so daß $\mathfrak{e}_0 = 1$ und $p^{v(i,\mathbf{A})}$ die Ordnung von $\mathfrak{e}_i$ ist. Die Gleichung $\mathfrak{x}^{p^{r+1}} = \mathfrak{e}_i^{p^r}$ hat für $0 \leqq r < v(i, \mathbf{A})$ keine Lösung $\mathfrak{x}$ in $\mathfrak{A}^*$, da sonst $\mathfrak{e}_i \mathfrak{x}^{-p}$ niedere Ordnung als $\mathfrak{e}_i$ hätte, aber mod $\mathfrak{Z}^*$ dieselbe Untergruppe von $\mathfrak{A}^*/\mathfrak{Z}^*$ erzeugte wie $\mathfrak{e}_i$. Da die $\mathfrak{e}_i$ mit $0 < i$ alle verschiedene Ordnung $\neq 1$ haben, so ergibt der Beweis von K., § 5, Lemma, daß die $\mathfrak{e}_i$ mit $0 < i$ in einer Basis von $\mathfrak{A}^*$ enthalten sind,[19]) d.h. $\mathfrak{A}^* = \prod_{i=1}^{u(\mathbf{A})} \{\mathfrak{e}_i\} \times \mathfrak{B}$.

Da in jeder Restklasse von $\mathfrak{A}^*/\mathfrak{Z}^*$ eine Potenz eines $\mathfrak{e}_i$ Element niederster Ordnung ist, so ist es möglich, die $\mathfrak{e}_i$ durch Elemente aus $\mathfrak{Z}^*$ zu einer Basis von $\mathfrak{A}^*$ zu ergänzen, so daß also $\mathfrak{B}$ als Untergruppe von $\mathfrak{Z}^*$ angenommen werden kann.

Ist $\mathfrak{Z}^{**}$ die aus $\mathfrak{B}$ durch Hinzufügen der Elemente $\mathfrak{e}_{i-1}\mathfrak{e}_i^{-p^{u(i,\mathbf{A})-u(i-1,\mathbf{A})}}$ mit $0 < i$ entstehende Gruppe, so ist sicher $\mathfrak{Z}^{**} \leqq \mathfrak{Z}^*$; da aber $\mathfrak{A}^*/\mathfrak{Z}^{**}$ ein Zyklus der Ordnung p^n ist, so ist $\mathfrak{Z}^* = \mathfrak{Z}^{**}$.

Ist nun

$$1 = \prod_{i=1}^{u(\mathbf{A})} \left(\mathfrak{e}_{i-1}\mathfrak{e}_i^{-p^{u(i,\mathbf{A})-u(i-1,\mathbf{A})}}\right)^{a_i p^{b_i}} \text{ mit zu } p \text{ primen } a_i, \text{ so wird}$$

$$1 = \prod_{i=1}^{u(\mathbf{A})} \mathfrak{e}_i^{f(i)}, \text{ wobei}$$

$$f(i) = a_{i+1}p^{b_{i+1}} - a_i p^{b_i + u(i,\mathbf{A}) - u(i-1,\mathbf{A})} \text{ für } 0 < i < u(\mathbf{A}),$$
$$= -a_{u(\mathbf{A})} p^{b_{u(\mathbf{A})} - u(u(\mathbf{A})-1,\mathbf{A}) + n} \text{ für } i = u(\mathbf{A}).$$

Da, wie oben gezeigt, die $\mathfrak{e}_i$ mit $0 < i$ Teil einer Basis sind, so müssen die einzelnen Faktoren $= 1$ sein, d.h. $f(i) \equiv 0 \bmod p^{v(i,\mathbf{A})}$. Hieraus folgt zunächst:

$$v(u(\mathbf{A}),\mathbf{A}) \leqq n + b_{u(\mathbf{A})} - u(u(\mathbf{A}) - 1, \mathbf{A}) =$$
$$= u(u(\mathbf{A}), \mathbf{A}) + b_{u(\mathbf{A})} - u(u(\mathbf{A}) - 1, \mathbf{A}).$$

Haben wir bereits gezeigt, daß

---

[19]) Dies kann man auch folgern aus § 1 von R. Baer, Types of elements and the characteristic subgroups of Abelian groups [Proc. London Math. Soc. (2) **39** (1935), 481—514], im folgenden mit T. citiert.

$$v(j, \mathbf{A}) \leqq u(j, \mathbf{A}) + b_j - u(j-1, \mathbf{A}) \text{ für } i < j \leqq u(\mathbf{A})$$

ist, so ist also, da die Ordnung von e_i kleiner als die von $e_{i+1}^{p^{u(i+1,\mathbf{A})-u(i,\mathbf{A})}}$ ist,

$$v(i, \mathbf{A}) < v(i+1, \mathbf{A}) - u(i+1, \mathbf{A}) + u(i, \mathbf{A}) \leqq b_{i+1},$$

und also $0 \equiv f(i) \equiv -a_i p^{b_i + u(i,\mathbf{A}) - u(i-1,\mathbf{A})} \bmod p^{v(i,\mathbf{A})}$,

$$\text{d.h. } v(i, \mathbf{A}) \leqq u(i, \mathbf{A}) + b_i - u(i-1, \mathbf{A}),$$

womit diese Ungleichung für $0 < i \leqq u(\mathbf{A})$ bewiesen ist.

Da nach einer oben gemachten Bemerkung $p^{v(i,\mathbf{A})-u(i,\mathbf{A})+u(i-1,\mathbf{A})}$ die Ordnung von $e_{i-1} e_i^{-p^{u(i,\mathbf{A})-u(i-1,\mathbf{A})}}$ ist, so folgt aus der Ungleichung, daß diese Elemente voneinander (und natürlich von den Elementen aus $\mathfrak{B}$) unabhängig sind.

Aus dem Bewiesenen folgt jetzt der Zusatz 2., wenn man noch bedenkt, daß $\mathfrak{A}^m / \mathfrak{A}^m \cap \mathfrak{D}(\mathbf{A}) = \prod_\nu \{\mathfrak{m}_\nu^{p^{m-1}}\}$ ist.

ZUSATZ 3.: *Es sei $\mathfrak{A}$ eine abelsche Primärgruppe der Maximalordnung p^m, D eine abelsche Primärgruppe der Maximalordnung p^n, u und $u(i)$, $v(i)$ für $0 < i \leqq u$ positive ganze Zahlen und w eine nicht-negative endliche oder unendliche Anzahl.*

Dann und nur dann gibt es eine vollkommene Automorphismengruppe $\mathbf{A}$ in $\mathfrak{A}$, so daß

a.) *$\mathbf{A}$ und D isomorph sind,*

b.) *$u(\mathbf{A}) = u$, $u(i, \mathbf{A}) = u(i)$, $v(i, \mathbf{A}) = v(i)$ für $0 < i \leqq u(\mathbf{A})$ und $w(\mathbf{A}) = w$ ist, wenn*

1.) $0 = v(0) < v(1) < \ldots < v(i) < \ldots < v(u)$,

2.) $0 = u(0) < u(1) < \ldots < u(i) < \ldots < u(u) = n$,

3.) $0 < v(1) - u(1) < \ldots < v(i) - u(i) < \ldots < v(u) - u(u)$,

4.) *$\mathfrak{A}$ für jedes i mit $0 < i \leqq u$ einen zyklischen direkten Faktor der Ordnung $p^{v(i)}$ besitzt,*

5.) *$d(\mathfrak{A}^m) = w + d(D^1)$ ist.*

Die Notwendigkeit der Bedingungen 1.)—3.) und 5.) folgt aus der Definition der Invarianten $u(\mathbf{A})$, $u(i, \mathbf{A})$, $v(i, \mathbf{A})$, $w(\mathbf{A})$, die Notwendigkeit von 4.) aus Zusatz 2. Sind umgekehrt die Bedingungen erfüllt, so ist

$$\mathfrak{A} = \prod_{i=1}^{u} \{e_i\} \times \mathfrak{B}' \times \prod_\nu \{\mathfrak{b}_\nu\} \times \prod_\nu \{\mathfrak{m}_\nu\},$$

wo e_i die Ordnung $p^{v(i)}$ hat, die Maximalordnung in $\mathfrak{B}'$ kleiner als p^m ist, $\mathfrak{b}_\nu$ und $\mathfrak{m}_\nu$ die Ordnung p^m haben, es $d(D^1)$ Faktoren $\{\mathfrak{m}_\nu\}$ und $w - 1$ oder w Faktoren $\{\mathfrak{b}_\nu\}$ gibt, je nachdem ob w endlich und gleichzeitig $m = v(u)$ ist oder nicht.

Wie beim Beweis des Zusatz 2. zeigt man dann, daß man

$$\mathfrak{Z} = \prod_{i=1}^{u} \{\mathfrak{e}_{i-1}\mathfrak{e}_i^{-p^{u(i)-u(i-1)}}\} \times \mathfrak{B}' \times \prod_{\nu} \{\mathfrak{b}_\nu\} \times \prod_{\nu} \{\mathfrak{m}_\nu\} \text{ mit } \mathfrak{e}_0 = 1$$

setzen darf, daß dann $\mathfrak{A}/\mathfrak{Z}$ ein Zyklus der Ordnung p^n wird; weiter kann man Zahlen k_ν so bestimmen, daß $0 \leqq k_\nu < m$ und D isomorph $\mathfrak{D} = \prod\{\mathfrak{m}_\nu^{p^{k_\nu}}\}$ wird. Dann folgt aus Satz 1. das Hinreichen unserer Bedingungen.

Satz 2.: *Es sei* $\mathbf{A}^{(i)}$ *eine vollkommene Automorphismengruppe in der abelschen Primärgruppe* $\mathfrak{A}^{(i)}$ $(i = 1, 2)$.

Dann und nur dann gibt es eine $\mathbf{A}^{(1)}$ *in* $\mathbf{A}^{(2)}$ *transformierende, isomorphe Abbildung von* $\mathfrak{A}^{(1)}$ *auf* $\mathfrak{A}^{(2)}$, *wenn*

1.) $\mathfrak{A}^{(1)}$ *isomorph* $\mathfrak{A}^{(2)}$,
2.) $\mathbf{A}^{(1)}$ *isomorph* $\mathbf{A}^{(2)}$,
3.) $u(\mathbf{A}^{(1)}) = u(\mathbf{A}^{(2)})$, $u(i, \mathbf{A}^{(1)}) = u(i, \mathbf{A}^{(2)})$, $v(i, \mathbf{A}^{(1)}) = v(i, \mathbf{A}^{(2)})$,
4.) $w(\mathbf{A}^{(1)}) = w(\mathbf{A}^{(2)})$ *ist.*

Beweis: Die Notwendigkeit der Bedingungen folgt wegen Satz 1. und seiner Zusätze daraus, daß eine $\mathbf{A}^{(1)}$ in $\mathbf{A}^{(2)}$ transformierende, isomorphe Abbildung von $\mathfrak{A}^{(1)}$ auf $\mathfrak{A}^{(2)}$ auch $\mathfrak{Z}(\mathbf{A}^{(1)})$ auf $\mathfrak{Z}(\mathbf{A}^{(2)})$ und $\mathfrak{D}(\mathbf{A}^{(1)})$ auf $\mathfrak{D}(\mathbf{A}^{(2)})$ abbildet.

Es seien also die Bedingungen 1.)—4.) erfüllt und

$$\mathfrak{A}^{(i)} = \prod_{j=1}^{u(\mathbf{A}^{(i)})} \{\mathfrak{e}_{ij}\} \times \mathfrak{B}^{(i)} \times \prod_{\nu} \{\mathfrak{m}_{\nu i}\}$$

eine Darstellung von $\mathfrak{A}^{(i)}$ gemäß Zusatz 2. Dabei kann wegen (3), (4) $\mathfrak{e}_{iu(\mathbf{A}^{(i)})} = \mathfrak{e}_i$ als ein $\alpha(\mathfrak{e}_i) = \mathfrak{e}_i \mathfrak{c}_i(\alpha)$ für α aus $\mathfrak{A}^{(i)}$ erfüllendes Element gewählt werden, wenn $\mathfrak{c}_i(\alpha)$ die in die Vollkommenheitsdefinition eingehende isomorphe Abbildung von $\mathbf{A}^{(i)}$ auf $\mathfrak{D}(\mathbf{A}^{(i)})$ ist.

Wegen 1. ist die Maximalordnung in $\mathfrak{A}^{(1)}$ und $\mathfrak{A}^{(2)}$ dieselbe, etwa p^m, und wegen 2. haben $\mathbf{A}^{(1)}$ und $\mathbf{A}^{(2)}$ dieselbe Maximalordnung p^n.

Es ist $\mathfrak{B}^{(i)} = \mathfrak{R}^{(i)} \times \mathfrak{S}^{(i)}$, wo die Maximalordnung in $\mathfrak{R}^{(i)}$ kleiner als p^m ist, während $\mathfrak{S}^{(i)}$ direktes Produkt zyklischer Gruppen der Ordnung p^m ist.

Wegen 3. haben $\mathfrak{e}_{1j}$ und $\mathfrak{e}_{2j}$ dieselbe Ordnung.

$d(\mathfrak{S}^{(1)^1}) = d(\mathfrak{S}^{(2)^1})$ folgt also aus 4., und mithin sind $\mathfrak{S}^{(1)}$ und $\mathfrak{S}^{(2)}$ isomorph.

Da nach 2. $\mathbf{A}^{(1)}$ und $\mathbf{A}^{(2)}$ isomorph sind, so wird

$$d\left(\prod_{\nu}\{\mathfrak{m}_{\nu 1}^{p^{m-1}}\}\right) = d(\mathbf{A}^{(1)1}) = d(\mathbf{A}^{(2)1}) = d\left(\prod_{\nu}\{\mathfrak{m}_{\nu 2}^{p^{m-1}}\}\right),$$

und mithin sind $\prod_{\nu}\{\mathfrak{m}_{\nu 1}\}$ und $\prod_{\nu}\{\mathfrak{m}_{\nu 2}\}$ isomorph.

Also folgt aus 1., daß $\mathfrak{R}^{(1)}$ und $\mathfrak{R}^{(2)}$ isomorph sind.

Sei jetzt $\mathfrak{c}_i(\alpha)$ die in die Vollkommenheitsdefinition eingehende isomorphe Beziehung von $\mathbf{A}^{(2)}$ auf $\mathfrak{D}(\mathbf{A}^{(2)})$, τ eine gemäß 2. existierende isomorphe Abbildung von $\mathbf{A}^{(1)}$ auf $\mathbf{A}^{(2)}$, ϱ eine isomorphe Abbildung von $\mathfrak{R}^{(1)}$ auf $\mathfrak{R}^{(2)}$, σ eine von $\mathfrak{S}^{(1)}$ auf $\mathfrak{S}^{(2)}$.

Dann gibt es, wie man leicht sieht, eine isomorphe Abbildung φ von $\mathfrak{A}^{(1)}$ auf $\mathfrak{A}^{(2)}$, die

in $\mathfrak{R}^{(1)}$ mit ϱ und
in $\mathfrak{S}^{(1)}$ mit σ übereinstimmt,

und die weiter

$$\varphi(\mathfrak{e}_{1j}) = \mathfrak{e}_{2j},$$
$$\varphi[\mathfrak{c}_1(\alpha)] = \mathfrak{c}_2[\tau(\alpha)] \text{ erfüllt.}$$

Ist jetzt α aus $\mathbf{A}^{(1)}$ beliebig, so ist nach Zusatz 1. zu Satz 1.:

$$\alpha(\mathfrak{k}) = \mathfrak{k}\,\mathfrak{c}_1(\alpha)^{h_1(\mathfrak{k})} \text{ für } \mathfrak{k} \text{ aus } \mathfrak{A}^{(1)}.$$

Es wird dann

$$\varphi[\alpha(\mathfrak{k})] = \varphi(\mathfrak{k})\,\mathfrak{c}_2[\tau(\alpha)]^{h_1(\mathfrak{k})}$$

und, da für α_2 aus $\mathbf{A}^{(2)}$, $\mathfrak{k}_2$ aus $\mathfrak{A}^{(2)}$ gilt

$$\alpha_2(\mathfrak{k}_2)\mathfrak{k}_2^{-1} = \alpha_2(\mathfrak{e}_2^{h_2(\mathfrak{k}_2)})\,\mathfrak{e}_2^{-h_2(\mathfrak{k}_2)},$$

so folgt $h_1(\mathfrak{k}) \equiv h_2[\varphi(\mathfrak{k})] \bmod p^n$ und wir erhalten

$$\varphi[\alpha(\mathfrak{k})] = \varphi(\mathfrak{k})\,\mathfrak{c}_2[\tau(\alpha)]^{h_2[\varphi(\mathfrak{k})]} = \tau(\alpha)(\varphi(\mathfrak{k}))$$

oder
$$\tau(\alpha) = \varphi[\alpha(\varphi^{-1}(\ldots))], \text{ d.h.}$$

φ ist eine $\mathbf{A}^{(1)}$ in $\mathbf{A}^{(2)}$ transformierende, isomorphe Abbildung von $\mathfrak{A}^{(1)}$ auf $\mathfrak{A}^{(2)}$, die sogar die Beziehungen $\mathfrak{c}_i(\alpha)$ erhält und eine gegebene isomorphe Abbildung von $\mathbf{A}^{(1)}$ auf $\mathbf{A}^{(2)}$ umfaßt.

ZUSATZ: *Die Bedingung* 4. *ist eine Folge der Bedingungen* 1.—3., *wenn wenigstens eine der folgenden Bedingungen erfüllt ist:* [20])

a.) $\mathbf{A}^{(i)}$ *ist endlich;*

b.) $\mathbf{A}^{(i)}$ *ist unendlich, aber* $d(\mathbf{A}^{(i)1}) < d(\mathfrak{A}^{(i)m})$.

---

[20]) Der Beweis zeigt, daß dies nicht mehr gilt, wenn keine der Bedingungen a) oder b) erfüllt ist.

Es ist nämlich

$$d(\mathfrak{A}^{(i)m}) = d(\mathbf{A}^{(i)1}) + w(\mathbf{A}^{(i)}),$$

und demnach ist $w(\mathbf{A}^{(i)})$ durch $d(\mathfrak{A}^{(i)m})$ und $d(\mathbf{A}^{(i)1})$ und also durch $\mathfrak{A}^{(i)}$ und $\mathbf{A}^{(i)}$ bestimmt, wenn a.) oder b.) erfüllt ist.

SATZ 3: *Es sei* $\mathbf{A}^{(i)}$ *eine vollkommene Automorphismengruppe in der abelschen Primärgruppe* $\mathfrak{A}^{(i)}$ $(i = 1, 2)$.

Dann und nur dann gibt es eine $\mathbf{A}^{(1)}$ *in* $\mathbf{A}^{(2)}$ *transformierende, isomorphe Abbildung von* $\mathfrak{A}^{(1)}$ *auf* $\mathfrak{A}^{(2)}$, *wenn es eine isomorphe Abbildung von* $\mathfrak{A}^{(1)}$ *auf* $\mathfrak{A}^{(2)}$ *gibt, die* $\mathfrak{Z}(\mathbf{A}^{(1)})$ *in* $\mathfrak{Z}(\mathbf{A}^{(2)})$ *und* $\mathfrak{D}(\mathbf{A}^{(1)})$ *in* $\mathfrak{D}(\mathbf{A}^{(2)})$ *überführt.*

Es ist nur das Hinreichen der Bedingung zu zeigen: sei

$$\mathfrak{A}^{(1)} = \mathfrak{B} \times \prod_{j=1}^{u(\mathbf{A}^{(1)})} \{\mathfrak{e}_j\} \times \prod_{\nu} \{\mathfrak{m}_\nu\},$$

$$\mathfrak{Z}(\mathbf{A}^{(1)}) = \mathfrak{B} \times \prod_{\nu} \{\mathfrak{m}_\nu\} \times \prod_{j=1}^{u(\mathbf{A}^{(1)})} \{\mathfrak{e}_{j-1}\mathfrak{e}_j^{-p^{u(j,\mathbf{A}^{(1)})-u(j-1,\mathbf{A}^{(1)})}}\},$$

$$\mathfrak{D}(\mathbf{A}^{(1)}) = \prod_{\nu} \{\mathfrak{m}_\nu^{p^{k_\nu}}\}$$

eine Zerlegung von $\mathfrak{A}^{(1)}$ gemäß Zusatz 2 zu Satz 1.; ist dann $\varkappa$ eine $\mathfrak{Z}(\mathbf{A}^{(1)})$ in $\mathfrak{Z}(\mathbf{A}^{(2)})$ und $\mathfrak{D}(\mathbf{A}^{(1)})$ in $\mathfrak{D}(\mathbf{A}^{(2)})$ überführende isomorphe Abbildung von $\mathfrak{A}^{(1)}$ auf $\mathfrak{A}^{(2)}$, so wird:

$$\mathfrak{A}^{(2)} = \varkappa(\mathfrak{A}^{(1)}) = \varkappa(\mathfrak{B}) \times \prod_{j=1}^{u(\mathbf{A}^{(1)})} \{\varkappa(\mathfrak{e}_j)\} \times \prod_{\nu} \{\varkappa(\mathfrak{m}_\nu)\}$$

$$\mathfrak{Z}(\mathbf{A}^{(2)}) = \varkappa[\mathfrak{Z}(\mathbf{A}^{(1)})] =$$

$$= \varkappa(\mathfrak{B}) \times \prod_{j=1}^{u(\mathbf{A}^{(1)})} \{\varkappa(\mathfrak{e}_{j-1})\varkappa(\mathfrak{e}_j)^{-p^{u(j,\mathbf{A}^{(1)})-u(j-1,\mathbf{A}^{(1)})}}\} \times \prod_{\nu} \{\varkappa(\mathfrak{m}_\nu)\},$$

$$\mathfrak{D}(\mathbf{A}^{(2)}) = \varkappa[\mathfrak{D}(\mathbf{A}^{(1)})] = \prod_{\nu} \{\varkappa(\mathfrak{m}_\nu)^{p^{k_\nu}}\},$$

und dies ist offenbar eine Zerlegung von $\mathfrak{A}^{(2)}$ bezgl. $\mathbf{A}^{(2)}$ gemäß Zusatz 2. zu Satz 1. Bedenkt man noch, daß $\mathfrak{D}(\mathbf{A}^{(i)})$ und $\mathbf{A}^{(i)}$ stets isomorph sind, so folgt aus Zusatz 3. zu Satz 1., daß die Bedingungen 1.—4. des Satzes 2. erfüllt sind, und also ist Satz 3. eine Folge von Satz 2.

ZUSATZ: *Es sei* $\mathbf{A}^{(i)}$ *für* $i = 1, 2$ *eine vollkommene Automorphismengruppe in der abelschen Primärgruppe* $\mathfrak{A}$.

Dann und nur dann ist $\mathbf{A}^{(1)} = \mathbf{A}^{(2)}$, *wenn* $\mathfrak{Z}(\mathbf{A}^{(1)}) = \mathfrak{Z}(\mathbf{A}^{(2)})$ *und* $\mathfrak{D}(\mathbf{A}^{(1)}) = \mathfrak{D}(\mathbf{A}^{(2)})$ *ist.*

Es ist nur das Hinreichen der Bedingung zu zeigen: es sei $\mathfrak{c}_i(\alpha)$ eine in die Vollkommenheitsdefinition eingehende, isomorphe Ab-

bildung von $\mathbf{A}^{(2)}$ auf $\mathfrak{D}(\mathbf{A}^{(2)})$; da $\mathfrak{D}(\mathbf{A}^{(1)}) = \mathfrak{D}(\mathbf{A}^{(2)})$ ist, so wird durch die Gleichung $\mathfrak{c}_1(\alpha) = \mathfrak{c}_2[\lambda(\alpha)]$ eine isomorphe Abbildung λ von $\mathbf{A}^{(1)}$ auf $\mathbf{A}^{(2)}$ definiert. Wegen (3), (4) gibt es einen Repräsentanten $\mathfrak{e}$ einer erzeugenden Restklasse von $\mathfrak{A}/\mathfrak{Z}(\mathbf{A}^{(1)}) = \mathfrak{A}/\mathfrak{Z}(\mathbf{A}^{(2)})$, so daß

$$\alpha(\mathfrak{e}) = \mathfrak{e}\,\mathfrak{c}_2(\alpha) \text{ für alle } \alpha \text{ aus } \mathbf{A}^{(2)}$$

gilt, und also eine zu p teilerfremde Zahl c, so daß

$$\alpha(\mathfrak{e}^c) = \mathfrak{e}^c\mathfrak{c}_1(\alpha) \text{ für alle } \alpha \text{ aus } \mathbf{A}^{(1)}$$

gilt, und hierdurch sind die Automorphismen α aus $\mathbf{A}^{(i)}$ völlig bestimmt.

Für α aus $\mathbf{A}^{(1)}$ wird also

$$\lambda(\alpha)(\mathfrak{e}^c) = \mathfrak{e}^c\mathfrak{c}_2[\lambda(\alpha)]^c = \mathfrak{e}^c\mathfrak{c}_1(\alpha)^c = \mathfrak{e}^c\mathfrak{c}_1(\alpha^c) = \alpha^c(\mathfrak{e}^c),$$

und wegen $\mathfrak{Z}(\mathbf{A}^{(1)}) = \mathfrak{Z}(\mathbf{A}^{(2)})$ und (3), (4) wird also: $\lambda(\alpha) = \alpha^c$, d.h. $\mathbf{A}^{(1)} = \mathbf{A}^{(2)}$, wie behauptet.

§ 5.

Charakterisierung des Kerns vollkommener Gruppen.

Satz: *Es sei* $\mathfrak{G}$ *eine Primärgruppe,* $\mathfrak{A}$ *eine Untergruppe von* $\mathfrak{G}$ *und* $\chi_{\mathfrak{g}}(\mathfrak{k}) = \mathfrak{g}^{-1}\mathfrak{k}\mathfrak{g}$ *die von* $\mathfrak{g}$ *aus* $\mathfrak{G}$ *in* $\mathfrak{A}$ *induzierte isomorphe Abbildung.*

Dann und nur dann ist $\mathfrak{G}$ *vollkommen und* $\mathfrak{A} = \mathfrak{R}(\mathfrak{G})$, *wenn*

1. $\mathfrak{A}$ *ein echter, abelscher Normalteiler von* $\mathfrak{G}$ *mit Elementen beschränkter Ordnung ist,*

2. *die von* $\mathfrak{G}$ *in* $\mathfrak{A}$ *induzierte Automorphismengruppe vollkommen ist und die in die Vollkommenheitsdefinition* (§ 4.) *eingehende isomorphe Abbildung durch*

$$\mathfrak{c}(\chi_{\mathfrak{g}}) = \mathfrak{g}^{p^m} = \mathfrak{c}(\mathfrak{g}) \quad [p^m = \textit{Maximalordnung in } \mathfrak{A}]$$

hergestellt wird,

3. $\chi_{\mathfrak{g}} = 1$ *dann und nur dann ist, wenn* $\mathfrak{g}$ *in* $\mathfrak{A}$ *liegt,*

4. $m > 1$ *ist, falls* $p = 2$ *ist.*

Beweis: Die Notwendigkeit der Bedingung 1. ist eine Folge von § 2, (1), 1, und § 2, (3), die der Bedingung 2. von § 3, Satz 1, die der Bedingung 3. von § 1, Satz 3, die der Bedingung 4. von § 2, (1) und § 2, (2), 5.

Es seien umgekehrt die Bedingungen 1.—4. erfüllt; dann folgt aus § 2, (2), daß

$$\mathfrak{A} = \mathfrak{R}(\{\mathfrak{A}, \mathfrak{g}\}) \text{ für jedes } \mathfrak{g} \text{ aus } \mathfrak{G}$$

ist, aus § 2, (1) also, daß $\mathfrak{A} = \mathfrak{K}(\mathfrak{G})$ wesentlicher Kern von $\mathfrak{G}$ ist; wegen 2. und 3. ist $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ isomorph einer Untergruppe von $\mathfrak{A}$; also ist $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ abelsch. Wegen 3. ist die Zuordnung: $\mathfrak{g} \to \chi_{\mathfrak{g}}$ eine isomorphe Abbildung von $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ auf die von $\mathfrak{G}$ in $\mathfrak{K}(\mathfrak{G})$ induzierte Automorphismengruppe und wegen 2. definiert also die Zuordnung: $\mathfrak{g} \to \mathfrak{g}^{p^m}$ eine isomorphe Abbildung von $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ auf $\mathfrak{D}(\mathfrak{G})$, d.h. $\mathfrak{G}$ ist vollkommen.

FOLGERUNG: *Ist $\mathfrak{G}$ vollkommen, $\mathfrak{g}$ aus $\mathfrak{G}$ beliebig, so gibt es ein zu $\mathfrak{g}$ mod $\mathfrak{K}(\mathfrak{G})$ kongruentes Element $\hat{\mathfrak{g}}$, so daß — unter $p^{n(\mathfrak{g})}$ die Ordnung von $\mathfrak{g}$ mod $\mathfrak{K}(\mathfrak{G})$ verstanden — $\mathfrak{a}(\hat{\mathfrak{g}}) = \hat{\mathfrak{g}}^{p^{n(\hat{\mathfrak{g}})}}$ in $\mathfrak{Z}(\mathfrak{G})$ liegt.*

BEWEIS: Es sei **A** die Gruppe der von $\mathfrak{G}$ in $\mathfrak{K}(\mathfrak{G})$ induzierten Automorphismen $\chi_{\mathfrak{g}}(\mathfrak{k}) = \mathfrak{g}^{-1}\mathfrak{k}\mathfrak{g}$. Da $\mathfrak{Z}(\mathfrak{G}) \leqq \mathfrak{K}(\mathfrak{G})$ ist, so ist [in der Bezeichnung des § 4] $\mathfrak{Z}(\mathfrak{G}) = \mathfrak{Z}(\mathbf{A})$. Aus Satz 2. folgt dann wegen § 4, (3) die Existenz eines Elementes $\mathfrak{e}$, so daß

$$\chi_{\mathfrak{g}}(\mathfrak{e}) = \mathfrak{e}\mathfrak{c}(\mathfrak{g}) \quad \text{für jedes } \mathfrak{g} \text{ aus } \mathfrak{G}$$

gilt, und $\mathfrak{e}$ ist Repräsentant einer erzeugenden Restklasse der wegen § 4, Satz 1. zyklischen Gruppe $\mathfrak{K}(\mathfrak{G})/\mathfrak{Z}(\mathfrak{G})$.

Insbesondere ist also

$$\mathfrak{a}(\mathfrak{g}) = \mathfrak{e}^g\mathfrak{u} \text{ mit } 0 \leqq g < p^n = \text{Ordnung von } \mathfrak{K}(\mathfrak{G})/\mathfrak{Z}(\mathfrak{G}) \text{ und } \mathfrak{u} \text{ in } \mathfrak{Z}(\mathfrak{G}).$$

Dann wird

$$\mathfrak{a}(\mathfrak{g}) = \mathfrak{g}^{-1}\mathfrak{a}(\mathfrak{g})\mathfrak{g} = \mathfrak{a}(\mathfrak{g})\mathfrak{c}(\mathfrak{g})^g$$

und also $g \equiv 0 \bmod p^{n(\mathfrak{g})}$, da ja $\chi_{\mathfrak{g}}$ und $\mathfrak{c}(\mathfrak{g})$ dieselbe Ordnung $p^{n(\mathfrak{g})}$ haben [vergl. § 2, (2)]. Wir setzen $g = \hat{g}p^{n(\mathfrak{g})}$, wo $\hat{g}$ eine ganze Zahl ist, und $\hat{\mathfrak{g}} = \mathfrak{e}^{-\hat{g}}\mathfrak{g}$.

$\hat{\mathfrak{g}}$ und $\mathfrak{g}$ sind kongruent mod $\mathfrak{K}(\mathfrak{G})$, da $\mathfrak{e}$ in $\mathfrak{K}(\mathfrak{G})$ liegt, und es wird also $n(\mathfrak{g}) = n(\hat{\mathfrak{g}})$. Weiter wird:

$$\mathfrak{a}(\hat{\mathfrak{g}}) = (\mathfrak{e}^{-\hat{g}}\mathfrak{g})^{p^{n(\mathfrak{g})}} = \left(\prod_{i=0}^{p^{n(\mathfrak{g})}-1} \chi_{\mathfrak{g}}^{-i}(\mathfrak{e}^{-\hat{g}})\right) \cdot \mathfrak{g}^{p^{n(\mathfrak{g})}} =$$

$$= \left(\prod_{i=0}^{p^{n(\mathfrak{g})}-1} \mathfrak{e}^{-\hat{g}}\mathfrak{c}(\mathfrak{g})^{-i\hat{g}}\right)\mathfrak{a}(\mathfrak{g}) =$$

$$= \mathfrak{e}^{-g}\mathfrak{c}(\mathfrak{g})^{\hat{g}\frac{p^{n(\mathfrak{g})}(p^{n(\mathfrak{g})}-1)}{2}}\mathfrak{a}(\mathfrak{g}) =$$

$$= \mathfrak{u}\mathfrak{c}(\mathfrak{g})^z$$

und, da $\mathfrak{u}$ und $\mathfrak{c}(\mathfrak{g})$ in $\mathfrak{Z}(\mathfrak{G})$ liegen [nach § 3, Lemma 2., a.], so liegt $\mathfrak{a}(\widehat{\mathfrak{g}})$ in $\mathfrak{Z}(\mathfrak{G})$, womit unsere Behauptung bewiesen ist.

LEMMA: *Es sei $\mathfrak{G}$ eine Primärgruppe, $\mathfrak{A}$ eine die Bedingungen* 1., 3., 4. *des Satzes erfüllende Untergruppe von $\mathfrak{G}$.*

Dann und nur dann ist auch die Bedingung 2. *des Satzes erfüllt, wenn $\mathfrak{G}/\mathfrak{A}$ abelsch ist und es eine Basis $\mathfrak{B}$ von $\mathfrak{G}$ mod $\mathfrak{A}$ gibt, so daß gilt* [21]:

a. *es gibt eine für alle $\mathfrak{k}$ aus $\mathfrak{A}$ definierte Funktion $h(\mathfrak{k})$, so daß $\mathfrak{b}^{-1}\mathfrak{k}\mathfrak{b} = \mathfrak{k}\mathfrak{c}(\mathfrak{b})^{h(\mathfrak{k})}$ für alle $\mathfrak{b}$ aus $\mathfrak{B}$ ist;*

b. $\gamma\left[\mathfrak{A}\prod_{i=1}^{n}\mathfrak{b}_i^{b_i}\right] = \mathfrak{c}\left(\prod_{i=1}^{n}\mathfrak{b}_i^{b_i}\right)$ *für $\mathfrak{b}_i$ aus $\mathfrak{B}$, $\mathfrak{b}_i \neq \mathfrak{b}_k$ für $i \neq k$, $0 \leqq b_i < p^{n(\mathfrak{b}_i)}$ ist eine isomorphe Abbildung von $\mathfrak{G}/\mathfrak{A}$ auf das System [und also die Gruppe] $\mathfrak{C}(\mathfrak{G}, \mathfrak{A})$ aller Kommutatoren von Elementen aus $\mathfrak{G}$ mit Elementen aus $\mathfrak{A}$.*

c. *ist $p = 2$, enthält $\mathfrak{B}$ wenigstens zwei Elemente, so ist $n(\mathfrak{b}) \neq m$ für jedes $\mathfrak{b}$ aus $\mathfrak{B}$.*

a., b. *und* c. *sind dann für jede Basis von $\mathfrak{G}$ mod $\mathfrak{A}$ erfüllt.*

BEWEIS: A. Es sei auch die Bedingung 2. erfüllt. Nach dem Satze ist dann $\mathfrak{G}$ vollkommen und $\mathfrak{A} = \mathfrak{K}(\mathfrak{G})$. a. folgt dann aus § 4, Zusatz 1. zu Satz 1., während b. in der Bedingung 2. enthalten ist, c. aus § 3, Satz 2., c. folgt.

B. Es seien a., b. und c. erfüllt. Wegen Bedingung 3. ist $\chi_{\mathfrak{u}} = \chi_{\mathfrak{v}}$ dann und nur dann, wenn $\mathfrak{u}$ kongruent $\mathfrak{v}$ mod $\mathfrak{A}$ ist.

Ist $\mathfrak{g}$ aus $\mathfrak{G}$, so ist $\mathfrak{g}$ kongruent mod $\mathfrak{A}$ einem eindeutig bestimmten [22] Element $\overline{\mathfrak{g}} = \prod_{i=1}^{n}\mathfrak{b}_i^{b_i}$, d.h. $\mathfrak{g} = \mathfrak{k}\overline{\mathfrak{g}}$ mit $\mathfrak{k}$ aus $\mathfrak{A}$ und es wird:

$$\begin{aligned}
\mathfrak{c}(\mathfrak{g}) &= (\mathfrak{k}\overline{\mathfrak{g}})^{p^m} = \left(\prod_{i=0}^{p^m-1}\overline{\mathfrak{g}}^{i}\mathfrak{k}\overline{\mathfrak{g}}^{-i}\right)\overline{\mathfrak{g}}^{p^m} \\
&= \left(\prod_{i=0}^{p^m-1}\mathfrak{k}\mathfrak{c}(\overline{\mathfrak{g}})^{-ih(\mathfrak{k})}\right)\mathfrak{c}(\overline{\mathfrak{g}}) \text{ nach a., b.} \\
&= \mathfrak{k}^{p^m}\mathfrak{c}(\overline{\mathfrak{g}})^{-h(\mathfrak{k})\frac{p^m(p^m-1)}{2}}\mathfrak{c}(\overline{\mathfrak{g}}) \\
&= \mathfrak{c}(\overline{\mathfrak{g}}),
\end{aligned}$$

da p^m die Maximalordnung in $\mathfrak{A}$ ist und c. gilt. [22a] Hieraus folgt:

dann und nur dann ist $\mathfrak{u}$ kongruent $\mathfrak{v}$ mod $\mathfrak{A}$, wenn $\mathfrak{c}(\mathfrak{u}) = \mathfrak{c}(\mathfrak{v})$ ist.

---

[21] p^m = Maximalordnung in $\mathfrak{A}$, $\mathfrak{c}(\mathfrak{b}) = \mathfrak{b}^{p^m}$.

[22] Wenn man $\mathfrak{B}$ irgendwie wohlordnet.

[22a] Wenn $\mathfrak{G}/\mathfrak{A}$ zyklisch ist, so ist wegen § 2, (2) nichts zu beweisen.

Setzen wir jetzt

$$\mathfrak{c}(\chi_{\mathfrak{g}}) = \mathfrak{c}(\overline{\mathfrak{g}}),\ \mathfrak{a}(\chi_{\mathfrak{g}}) = \overline{\mathfrak{g}}^{p^{n(\mathfrak{g})}},$$

so verifiziert man rasch das Erfülltsein der Bedingung 2., wenn man nur gezeigt hat:

$$\mathfrak{c}(\mathfrak{g}) \text{ liegt stets in } \mathfrak{Z}(\mathfrak{G}).$$

Dies folgt sofort nach dem oben bewiesenen, wenn man zeigt: sind $\mathfrak{b}_1$, $\mathfrak{b}_2$ verschiedene Elemente aus $\mathfrak{B}$, so ist $\mathfrak{c}(\mathfrak{b}_1)$ mit $\mathfrak{b}_2$ vertauschbar.

Wegen a. und b. gibt es ein e, so daß

$$\mathfrak{b}_i^{-1} e \mathfrak{b}_i = e\mathfrak{c}(\mathfrak{b}_i)$$

ist, und es wird, da $\mathfrak{G}/\mathfrak{A}$ abelsch ist:

$$(\mathfrak{b}_1\mathfrak{b}_2)^{-1} e(\mathfrak{b}_1\mathfrak{b}_2) = \mathfrak{b}_2^{-1} e\mathfrak{c}(\mathfrak{b}_1)\mathfrak{b}_2 = e\mathfrak{c}(\mathfrak{b}_1)\mathfrak{c}(\mathfrak{b}_2)^{1+h(\mathfrak{c}(\mathfrak{b}_1))} =$$
$$= (\mathfrak{b}_2\mathfrak{b}_1)^{-1} e(\mathfrak{b}_2\mathfrak{b}_1) = e\mathfrak{c}(\mathfrak{b}_1)^{1+h(\mathfrak{c}(\mathfrak{b}_2))}\mathfrak{c}(\mathfrak{b}_2).$$

Da $\mathfrak{b}_1$, $\mathfrak{b}_2$ mod $\mathfrak{A}$ unabhängig sind, so folgt aus b., daß $\mathfrak{c}(\mathfrak{b}_1)$, $\mathfrak{c}(\mathfrak{b}_2)$ unabhängig sind, und also ist

$$\mathfrak{c}(\mathfrak{b}_2)^{h(\mathfrak{c}(\mathfrak{b}_1))} = 1, \text{ d.h. } \mathfrak{c}(\mathfrak{b}_1) \text{ mit } \mathfrak{b}_2 \text{ vertauschbar.}$$

§ 6.

Erweiterung zu vollkommenen Gruppen.

LEMMA: *Es sei* $\mathfrak{A}$ *eine abelsche Primärgruppe der [endlichen] Maximalordnung* p^m, **A** *eine vollkommene Automorphismengruppe in* $\mathfrak{A}$. *Ist* p^n *die Maximalordnung in* **A**, *so ist* $n \leqq m$; *ist* $p = 2$, *so sei* $n \neq m$.

Sei **B** *eine Basis von* **A**, $[\beta_1, \beta_2]$ *für irgendwelche Paare* $\beta_1 \neq \beta_2$ *aus* **B** *als Element in* $\mathfrak{A}$ *definiert,* $\mathfrak{a}(\beta)$ *für jedes* β *aus* **B** *ein Element der Ordnung* p^m *aus* $\mathfrak{Z}(\mathbf{A})$.

Dann und nur dann gibt es eine vollkommene Primärgruppe $\mathfrak{G}$, *deren Kern* $\mathfrak{A}$ *ist, die im Kern genau* **A** *induziert, und die eine Basis* $\mathfrak{B}$ *von* $\mathfrak{G}$ *mod* $\mathfrak{R}(\mathfrak{G})$ *besitzt, so daß*

$$\mathfrak{a}(\beta) = \mathfrak{b}(\beta)^{p^{n(\beta)}} \text{ und}$$
$$[\beta_1, \beta_2] = \mathfrak{b}(\beta_1)\mathfrak{b}(\beta_2)\mathfrak{b}(\beta_1)^{-1}\mathfrak{b}(\beta_2)^{-1} \text{ für } \beta_1 \neq \beta_2$$

ist, wobei β, β_i *aus* **B**, $p^{n(\beta)}$ *die Ordnung von* β, $\mathfrak{b}(\beta)$ *das [eindeutig bestimmte] Element aus* $\mathfrak{B}$ *ist, das in* $\mathfrak{A}$ *den Automorphismus* β *induziert, und wo* $\mathfrak{b}(\beta)$ *in ganz* **B** *definiert ist, wenn*

1.) *es eine in die Vollkommenheitsdefinition eingehende isomorphe Abbildung* $\mathfrak{c}(\alpha)$ *von* $\mathbf{A}$ *auf* $\mathfrak{D}(\mathbf{A})$ *gibt, so daß*

$$\mathfrak{c}(\beta) = \mathfrak{a}(\beta)^{p^{m-n(\beta)}} \text{ ist,}$$

2.) $[\beta_1, \beta_2] = [\beta_2, \beta_1]^{-1}$,

3.) $\beta_3([\beta_2, \beta_1]) = [\beta_2, \beta_1]$, *falls* $\beta_i \neq \beta_k$ *für* $i \neq k$ *ist,*

4.) $[\beta_1, \beta_2]^{p^{n(\beta)}} = 1$ *ist und*

5.) $[\beta_1, \beta_2]^{3^{m-1}}$ *für* $p = 3$ *in* $\mathfrak{Z}(\mathbf{A})$ *liegt,*

6.) $[\beta_1, \beta_2]^{2^{n-1}}$ *für* $p = 2$ *in* $\mathfrak{Z}(\mathbf{A})$ *liegt.*

Beweis: A. Die Notwendigkeit von 1.) folgt aus § 5., Lemma, a., die von 2.) ist klar, die von 3.) eine Folge aus § 3., Lemma 2., b. — Bedenkt man, daß $\mathfrak{a}(\beta)$ in $\mathfrak{Z}(\mathbf{A})$ liegt, so folgt aus § 2., (5), a.:

$$1 = \begin{cases} [\beta_1, \beta_2]^{p^{n(\beta_1)}}, & \text{falls } p \neq 2 \text{ ist} \\ [\beta_1, \beta_2]^{2^{n(\beta_1)}} \mathfrak{c}(\beta_1)^{h([\beta_2, \beta_1], \beta_1) 2^{n(\beta_1)-1}}, & \text{falls } p = 2 \text{ ist.} \end{cases}$$

Damit ist 4.) hergeleitet, falls $p \neq 2$ ist.

Ist $p = 2$, so ist wegen 1.) und Zusatz 1. des § 4:

$$1 = [\beta_1, \beta_2]^{2^{n(\beta_1)}} \mathfrak{c}(\beta_1)^{2^{n(\beta_1)-1} h([\beta_2, \beta_1])}$$

oder

$$[\beta_1, \beta_2]^{2^{n(\beta_1)}} = \mathfrak{c}(\beta_1)^{2^{n(\beta_1)-1} h([\beta_1, \beta_2])}.$$

Da $\mathfrak{c}(\beta_1)$ in $\mathfrak{Z}(\mathbf{A})$ liegt, so ist nach 1. und Zusatz 1. des § 4

$$2^{n(\beta_1)} h([\beta_1, \beta_2]) \equiv 0 \bmod 2^n,$$

d.h.

$$h([\beta_1, \beta_2]) \equiv 0 \bmod 2, \text{ falls } n(\beta_1) < n.$$

Damit ist aus Symmetriegründen 4.) für $p = 2$ gezeigt, wenn nur $\min[n(\beta_1), n(\beta_2)] < n$ ist. — Sei also schließlich $n(\beta_1) = n(\beta_2) = n$. Dann folgt aus Symmetriegründen:

$$\begin{aligned} [\beta_1, \beta_2]^{2^n} &= \mathfrak{c}(\beta_1)^{2^{n-1} h([\beta_1, \beta_2])} \\ &= \mathfrak{c}(\beta_2)^{2^{n-1} h([\beta_1, \beta_2])}. \end{aligned}$$

Da $\mathbf{A}$ volkommen ist, β_1 und β_2 unabhängig sind, so sind auch $\mathfrak{c}(\beta_1)$ und $\mathfrak{c}(\beta_2)$ unabhängig, d.h.

$$\mathfrak{c}(\beta_1)^{2^{n-1} h([\beta_1, \beta_2])} = \mathfrak{c}(\beta_2)^{2^{n-1} h([\beta_1, \beta_2])} = 1$$

und damit ist 4.) und wegen 3.) also auch 6.) hergeleitet. 5.) schließlich folgt aus § 3, Satz 2., b.

B. Es seien also die Bedingungen 1.)—6.) erfüllt. Dann adjungieren wir zu $\mathfrak{A}$ für jedes β aus $\mathbf{B}$ ein Element $\mathfrak{b}(\beta)$ mit den folgenden Relationen:

$$(\mathrm{R})\begin{cases}\mathfrak{b}(\beta)^{p^{n(\beta)}} = \mathfrak{a}(\beta),\\ \mathfrak{b}(\beta)^{-1}\mathfrak{k}\mathfrak{b}(\beta) = \beta(\mathfrak{k}) \text{ für } \mathfrak{k} \text{ aus } \mathfrak{A},\\ \mathfrak{b}(\beta_1)\mathfrak{b}(\beta_2)\mathfrak{b}(\beta_1)^{-1}\mathfrak{b}(\beta_2)^{-1} = [\beta_1, \beta_2] \text{ für } \beta_1 \neq \beta_2.\end{cases}$$

Um zu zeigen, daß hierdurch eine Erweiterungsgruppe $\mathfrak{G}$ von $\mathfrak{A}$ durch **A** definiert wird, die in $\mathfrak{A}$ genau **A** induziert, haben wir nachzuweisen, daß die Bedingungen von E., § 5, Zusatz, S. 407 erfüllt sind.: E., 1. folgt aus 2.), E., 2. aus 3.); E., 3. ergibt sich so: da $\mathfrak{a}(\beta)$ in $\mathfrak{Z}(\mathbf{A})$ liegt, so ist einerseits

$$\mathfrak{a}(\beta_1)\beta_2[\mathfrak{a}(\beta_1)^{-1}] = \mathbf{1}.$$

Ist $\beta_1 \neq \beta_2$, so wird andererseits:

$$\prod_{i=1}^{p^{n(\beta_2)}} \beta_2^{1-i}([\beta_2, \beta_1]) = \prod_{i=1}^{p^{n(\beta_2)}} [\beta_2, \beta_1]\mathfrak{c}(\beta_2)^{(1-i)h([\beta_2,\beta_1])} =$$

$$= [\beta_2, \beta_1]^{p^{n(\beta_2)}}\mathfrak{c}(\beta_2)^{h([\beta_2,\beta_1])\frac{p^{n(\beta_2)}(p^{n(\beta_2)}-1)}{2}} =$$

$$= \mathbf{1}$$

wegen 4.) und 6.), da $p^{n(\beta)}$ die Ordnung von $\mathfrak{c}(\beta)$ ist, womit auch E., 3. hergeleitet ist.

Daß $\mathfrak{G}$ eine vollkommene Gruppe mit $\mathfrak{A}$ als Kern ist, folgt aus § 5, Satz und § 5, Lemma, wenn wir nur § 5, Lemma, b. verifiziert haben [daß die übrigen Bedingungen erfüllt sind, ist offenbar]. Hierfür genügt es wegen § 2., (4) und $n < m$ für $p = 2$ zu zeigen:

$$\left(\prod_{i=1}^{r} \mathfrak{b}(\beta_i)^{b_i}\right)^{p^m} = \prod_{i=1}^{r} \left(\mathfrak{b}(\beta_i)^{p^m}\right)^{b_i} \text{ für } 0 \leqq b_i < p^{n(\beta_i)},$$

$$\beta_i \neq \beta_k \text{ für } i \neq k.$$

Wir beweisen es durch vollständige Induktion nach r. Für $r = 1$ ist es wahr; ist es schon für $r - 1$ bewiesen, so wird

$$\prod_{i=1}^{r} \left(\mathfrak{b}(\beta_i)^{p^m}\right)^{b_i} = \prod_{i=1}^{r-1} \left(\mathfrak{b}(\beta_i)^{p^m}\right)^{b_i} \mathfrak{b}(\beta_r)^{p^m b_r} =$$

$$= \left(\prod_{i=1}^{r-1} \mathfrak{b}(\beta_i)^{b_i}\right)^{p^m} \mathfrak{b}(\beta_r)^{b_r p^m} = \mathfrak{c}\left(\prod_{i=1}^{r-1} \mathfrak{b}(\beta_i)^{b_i}\right)\mathfrak{c}(\beta_r)^{b_r}$$

andererseits

$$\left(\prod_{i=1}^{r} \mathfrak{b}(\beta_i)^{b_i}\right)^{p^m} = \left(\prod_{i=1}^{r-1} \mathfrak{b}(\beta_i)^{b_i}\,\mathfrak{b}(\beta_r)^{b_r}\right)^{p^m} = \mathfrak{c}\left(\prod_{i=1}^{r-1} \mathfrak{b}(\beta_i)^{b_i}\right)\mathfrak{c}(\beta_r)^{b_r}$$

nach § 2, (6), b., da ja $\mathfrak{c}(\beta)$ in $\mathfrak{Z}(\mathbf{A})$ liegt und 4.)—6.) anwendbar sind.

Daß die übrigen $\mathfrak{G}$ auferlegten Bedingungen von $\mathfrak{G}$ erfüllt werden, folgt aus (R).

SATZ: *Es sei* $\mathfrak{A}$ *eine abelsche Primärgruppe und* $\mathbf{A}$ *eine Automorphismengruppe in* $\mathfrak{A}$.

Dann und nur dann gibt es eine vollkommene Gruppe mit $\mathfrak{A}$ *als Kern, die in* $\mathfrak{A}$ *genau* $\mathbf{A}$ *induziert, wenn* $\mathbf{A}$ *vollkommen ist und für* $p = 2$ *entweder* $\mathbf{A}$ *zyklisch ist und die Maximalordnung in* $\mathfrak{A}$ *ungleich 2 oder größer als die in* $\mathbf{A}$ *ist.*

BEWEIS: Die Notwendigkeit der Bedingungen folgt aus § 3, Satz 1. und § 3, Lemma 2., a., d., ihr Hinreichen aus § 6, Lemma, da $[\beta_1, \beta_2] = 1$ für alle $\beta_1 \neq \beta_2$ aus $\mathbf{B}$ die Bedingungen 2.)—6.) dieses Lemma erfüllt.

§ 7.
Isomorphie vollkommener Gruppen.

Es sei $\mathfrak{A}$ eine abelsche Primärgruppe der endlichen Maximalordnung p^m, $\mathbf{A}$ eine vollkommene Automorphismengruppe in $\mathfrak{A}$; ist p^n die Maximalordnung in $\mathbf{A}$, so ist $n \leqq m$ und, falls $p = 2$ ist, sei $n \neq m$.

Es sei nun $\mathfrak{G}$ eine vollkommene Primärgruppe mit $\mathfrak{A}$ als Kern und $\mathbf{A}$ als im Kern induzierter Automorphismengruppe; nach dem Satz des § 6 existieren solche Gruppen.

Ist $\mathfrak{B}$ eine Basis von $\mathfrak{G}$ mod $\mathfrak{A}$, so bildet die Gesamtheit $\mathbf{B}$ der [23]) $\chi_\mathfrak{b}$ mit $\mathfrak{b}$ aus $\mathfrak{B}$ eine Basis von $\mathbf{A}$ und wegen der Folgerung des § 5 kann $\mathfrak{B}$ ohne Änderung von $\mathbf{B}$ so ausgewählt werden, daß [24]) $\mathfrak{a}(\mathfrak{b}) = \mathfrak{b}^{p^{n(\mathfrak{b})}}$ für $\mathfrak{b}$ aus $\mathfrak{B}$ in $\mathfrak{Z}(\mathbf{A}) = \mathfrak{Z}(\mathfrak{G})$ liegt. Wir werden im folgenden nur solche Basen von $\mathfrak{G}$ mod $\mathfrak{A}$ betrachten.

Ist $\mathfrak{B}$ eine solche Basis, so heißt

$$\mathfrak{a}(\chi_\mathfrak{b}) = \mathfrak{b}^{p^{n(\mathfrak{b})}} \text{ für } \mathfrak{b} \text{ aus } \mathfrak{B}$$

eine von $\mathfrak{G}$ [vermittels $\mathfrak{B}$] realisierte $\mathfrak{a}$-Funktion von $\mathbf{A}$ in $\mathfrak{A}$ und

$$[\chi_{\mathfrak{b}_1}, \chi_{\mathfrak{b}_2}] = \mathfrak{b}_1\mathfrak{b}_2\mathfrak{b}_1^{-1}\mathfrak{b}_2^{-1} \text{ für } \mathfrak{b}_1 \neq \mathfrak{b}_2 \text{ aus } \mathfrak{G}$$

ein von $\mathfrak{G}$ [vermittels $\mathfrak{B}$] realisiertes Kommutatorensystem von $\mathbf{A}$ in $\mathfrak{A}$.

Eine $\mathfrak{a}$-Funktion und ein Kommutatorensystem von $\mathbf{A}$ in $\mathfrak{A}$,

---

[23]) $\chi_\mathfrak{g}(\mathfrak{f}) = \mathfrak{g}^{-1}\mathfrak{f}\mathfrak{g}$ für $\mathfrak{f}$ aus $\mathfrak{A} = \mathfrak{K}(\mathfrak{G})$, $\mathfrak{g}$ aus $\mathfrak{G}$.

[24]) $p^{n(\mathfrak{b})}$ = Ordnung von $\mathfrak{b}$ mod $\mathfrak{A}$, also = Ordnung von $\chi_\mathfrak{b}$, also = Ordnung von $\mathfrak{c}(\mathfrak{b}) = \mathfrak{b}^{p^m}$.

die von derselben Gruppe vermittels derselben Basis realisiert sind, heißen *zusammengehörig*.

Zwei $\mathfrak{a}$-Funktionen und ebenso zwei Kommutatorensysteme von $\mathbf{A}$ in $\mathfrak{A}$ heißen *assoziiert*, wenn sie von derselben Gruppe $\mathfrak{G}$ realisiert werden.

LEMMA: *Es sei* $\mathbf{B}$ *eine Basis der vollkommenen Automorphismengruppe* $\mathbf{A}$ *in der abelschen Primärgruppe* $\mathfrak{A}$.

a. *Ist* $\mathfrak{a}(\beta)$ *für alle* β *aus* $\mathbf{B}$ *ein Element aus* $\mathfrak{Z}(\mathbf{A})$, *so ist dann und nur dann* $\mathfrak{a}(\beta)$ *eine realisierbare* $\mathfrak{a}$*-Funktion von* $\mathbf{A}$ *in* $\mathfrak{A}$, *wenn es eine in die Vollkommenheitsdefinition eingehende isomorphe Abbildung* $\mathfrak{c}(\alpha)$ *von* $\mathbf{A}$ *auf* $\mathfrak{D}(\mathbf{A})$ *gibt, so daß* [25])

$$\mathfrak{c}(\beta) = \mathfrak{a}(\beta)^{p^{m-n(\beta)}} \text{ für alle } \beta \text{ aus } \mathbf{B}$$

ist.

b. *Ist* $[\beta_1, \beta_2]$ *für alle Paare verschiedener Elemente* β_1, β_2 *aus* $\mathbf{B}$ *ein Element aus* $\mathfrak{A}$, *so ist* $[\beta_1, \beta_2]$ *dann und nur dann ein realisierbares Kommutatorensystem von* $\mathbf{A}$ *in* $\mathfrak{A}$, *wenn*

1. $[\beta_1, \beta_2] = [\beta_2, \beta_1]^{-1}$,
2. $\beta_3([\beta_2, \beta_1]) = [\beta_2, \beta_1]$, *falls* $\beta_i \neq \beta_k$ *für* $i \neq k$ *ist*,
3. $[\beta_1, \beta_2]^{p^{n(\beta_1)}} = 1$ *ist und*
4. $[\beta_1, \beta_2]^{3^{m-1}}$ *für* $p = 3$ *in* $\mathfrak{Z}(\mathbf{A})$ *liegt und*
5. $[\beta_1, \beta_2]^{2^{n-1}}$ *für* $p = 2$ *in* $\mathfrak{Z}(\mathbf{A})$ *liegt.*

c. *Jede realisierbare* $\mathfrak{a}$*-Funktion von* $\mathbf{A}$ *in* $\mathfrak{A}$ *und jedes realisierbare Kommutatorensystem von* $\mathbf{A}$ *in* $\mathfrak{A}$ *sind* [*für eine geeignete Gruppe* $\mathfrak{G}$] *zusammengehörig.*

d. *Zwei realisierbare* $\mathfrak{a}$*-Funktionen* $\mathfrak{a}_1(\beta)$ *und* $\mathfrak{a}_2(\beta)$ *von* $\mathbf{A}$ *in* $\mathfrak{A}$ *sind dann und nur dann assoziiert, wenn es für jedes* β *aus* $\mathbf{B}$ *ein Element* $\mathfrak{f}(\beta)$ *aus* $\mathfrak{A}$ *gibt, so daß*

$$\mathfrak{a}_1(\beta) = \begin{cases} \mathfrak{f}(\beta)^{p^{n(\beta)}}\mathfrak{a}_2(\beta), & \text{falls } p \neq 2 \text{ oder } p = 2,\ n(\beta) < n, \\ \mathfrak{f}(\beta)^{2^{n(\beta)}}\mathfrak{a}_2(\beta)^{1+h(\mathfrak{f}(\beta))2^{m-1}}, & \text{falls } p = 2,\ n(\beta) = n \end{cases}$$

gilt. [*Natürlich liegt dann* $\mathfrak{f}(\beta)^{p^{n(\beta)}}$ *in* $\mathfrak{Z}(\mathbf{A})$.]

e. *Zwei realisierbare Kommutatorensysteme* $[\beta_1, \beta_2]_1$ *und* $[\beta_1, \beta_2]_2$ *sind dann und nur dann assoziiert, wenn es eine in die Vollkommenheitsdefinition eingehende isomorphe Abbildung* $\mathfrak{c}(\alpha)$ *von* $\mathbf{A}$ *auf* $\mathfrak{D}(\mathbf{A})$ *und für jedes* β *aus* $\mathbf{B}$ *eine Zahl* $k(\beta)$ *mit* $0 \leqq k(\beta) < p^{n(\beta)}$ *gibt, so daß*

---

[25]) $p^{n(\alpha)}$ = Ordnung von α.

$$[\beta_1, \beta_2]_1 = \mathfrak{c}(\beta_1)^{-k(\beta_2)p^{n-n(\beta_2)}} \mathfrak{c}(\beta_2)^{k(\beta_1)p^{n-n(\beta_1)}} [\beta_1, \beta_2]_2$$

ist.

BEWEIS: a., b., c. folgen sofort aus § 6., Lemma. — Um d., e. zu beweisen, betrachten wir eine $\mathfrak{a}_1(\beta)$ und $\mathfrak{a}_2(\beta)$ bzw. $[\beta_1, \beta_2]_1$ und $[\beta_1, \beta_2]_2$ realisierende Gruppe $\mathfrak{G}$ und eine Basis $\mathfrak{B}_i$ von $\mathfrak{G}$ mod $\mathfrak{R}(\mathfrak{G})$, vermittels derer gerade $\mathfrak{a}_i(\beta)$ bzw. $[\beta_1, \beta_2]_i$ realisiert wird; sei $\mathfrak{b}_i(\beta)$ das eindeutig bestimmte Element aus $\mathfrak{B}_i$, das in $\mathfrak{R}(\mathfrak{G}) = \mathfrak{A}$ gerade den Automorphismus β aus **B** induziert.

Da $\mathfrak{b}_1(\beta)$ und $\mathfrak{b}_2(\beta)$ denselben Automorphismus in $\mathfrak{A}$ induzierende Elemente der vollkommenen Gruppe $\mathfrak{G}$ sind, so folgt aus § 1., Satz 3., 2., daß $\mathfrak{b}_1(\beta)$ und $\mathfrak{b}_2(\beta)$ derselben Restklasse von $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ angehören, d.h.

$$\mathfrak{b}_1(\beta) = \mathfrak{f}(\beta)\mathfrak{b}_2(\beta) \text{ mit } \mathfrak{f}(\beta) \text{ in } \mathfrak{A}.$$

Wegen § 2, (4) und $n < m$ für $p = 2$ wird also

$$\mathfrak{b}_1(\beta)^{p^m} = \mathfrak{b}_2(\beta)^{p^m} = \mathfrak{c}(\beta),$$

und $\mathfrak{c}(\alpha) = \mathfrak{r}^{p^m}$, wo $\mathfrak{r}$ ein α in $\mathfrak{A}$ induzierendes Element aus $\mathfrak{G}$ ist, ist nach § 3, Satz 1 eine in die Vollkommenheitsdefinition eingehende isomorphe Abbildung von **A** auf $\mathfrak{D}(\mathbf{A}) = \mathfrak{D}(\mathfrak{G})$.

Es wird

$$\mathfrak{a}_1(\beta) = [\mathfrak{b}_1(\beta)]^{p^{n(\beta)}} = [\mathfrak{f}(\beta)\mathfrak{b}_2(\beta)]^{p^{n(\beta)}} =$$

$$= \left(\prod_{i=0}^{p^{n(\beta)}-1} \mathfrak{b}_2(\beta)^i \mathfrak{f}(\beta) \mathfrak{b}_2(\beta)^{-i}\right) \mathfrak{b}_2(\beta)^{p^{n(\beta)}} =$$

$$= \left(\prod_{i=0}^{p^{n(\beta)}-1} \beta^{-i}(\mathfrak{f}(\beta))\right) \mathfrak{a}_2(\beta) = \left(\prod_{i=0}^{p^{n(\beta)}-1} \mathfrak{f}(\beta)\mathfrak{c}(\beta)^{-ih[\mathfrak{f}(\beta)]}\right) \mathfrak{a}_2(\beta) =$$

$$= \mathfrak{f}(\beta)^{p^{n(\beta)}} \mathfrak{c}(\beta)^{-h[\mathfrak{f}(\beta)]\frac{p^{n(\beta)}(p^{n(\beta)}-1)}{2}} \mathfrak{a}_2(\beta).$$

Da $\mathfrak{c}(\beta)$, $\mathfrak{a}_2(\beta)$, $\mathfrak{a}_1(\beta)$ in $\mathfrak{Z}(\mathbf{A})$ liegen, so liegt auch $\mathfrak{f}(\beta)^{p^{n(\beta)}}$ in $\mathfrak{Z}(\mathbf{A})$, d.h. es ist

$$p^{n(\beta)}h[\mathfrak{f}(\beta)] \equiv 0 \bmod p^n,$$

und hieraus sowie der Tatsache, daß $p^{n(\beta)}$ die Ordnung von $\mathfrak{c}(\beta)$ ist, folgt die Notwendigkeit der in d. angegebenen Bedingung, deren Hinreichen man leicht mit Hilfe der angestellten Überlegungen folgert.

Weiter ist

$$[\beta_1, \beta_2]_1 = \mathfrak{b}_1(\beta_1)\mathfrak{b}_1(\beta_2)\mathfrak{b}_1(\beta_1)^{-1}\mathfrak{b}_1(\beta_2)^{-1} =$$
$$= \mathfrak{f}(\beta_1)\mathfrak{b}_2(\beta_1)\mathfrak{f}(\beta_2)\mathfrak{b}_2(\beta_2)\mathfrak{b}_2(\beta_1)^{-1}\mathfrak{f}(\beta)_1^{-1}\mathfrak{b}_2(\beta_2)^{-1}\mathfrak{f}(\beta_2)^{-1} =$$
$$= \mathfrak{c}(\beta_2)^{h(\mathfrak{f}(\beta_1))}\mathfrak{c}(\beta_1)^{-h(\mathfrak{f}(\beta_2))}[\beta_1, \beta_2]_2,$$

und e. folgt sofort. Hieraus folgt auch der

ZUSATZ: *Sind zwei* $\mathfrak{a}$*-Funktionen [bzw. Kommutatorensysteme] von* $\mathbf{A}$ *in* $\mathfrak{A}$ *assoziiert, so ist jede Realisierung der einen* $\mathfrak{a}$*-Funktion [bzw. des einen Kommutatorensystems] auch eine Realisierung der anderen* $\mathfrak{a}$*-Funktion [bzw. des anderen Kommutatorensystems].*

SATZ 1.: *Es sei* $\mathfrak{G}^{(i)}$ *für* $i = 1, 2$ *eine vollkommene Gruppe,* $\mathbf{A}^{(i)}$ *die in* $\mathfrak{N}(\mathfrak{G}^{(i)})$ *von* $\mathfrak{G}^{(i)}$ *induzierte Automorphismengruppe,* $\mathfrak{c}_i(\alpha)$ *die durch* $\mathfrak{G}^{(i)}$ *gemäß § 3, Satz 1., c. induzierte isomorphe Abbildung von* $\mathbf{A}^{(i)}$ *auf* $\mathfrak{D}(\mathfrak{G}^{(i)})$.

Dann und nur dann sind $\mathfrak{G}^{(1)}$ *und* $\mathfrak{G}^{(2)}$ *isomorph, wenn es eine isomorphe Abbildung* $\varkappa$ *von* $\mathfrak{N}(\mathfrak{G}^{(1)})$ *auf* $\mathfrak{N}(\mathfrak{G}^{(2)})$ *gibt, so daß gilt*

1. $\varkappa[\mathfrak{Z}(\mathfrak{G}^{(1)})] = \mathfrak{Z}(\mathfrak{G}^{(2)})$,
2. $\varkappa[\mathfrak{D}(\mathfrak{G}^{(1)})] = \mathfrak{D}(\mathfrak{G}^{(2)})$

und also wird durch

$$\varkappa[\mathfrak{c}_1(\alpha)] = \mathfrak{c}_2[\lambda(\alpha)]$$

eine isomorphe Abbildung λ *von* $\mathbf{A}^{(1)}$ *auf* $\mathbf{A}^{(2)}$ *definiert;*

3. *sei* $\mathbf{B}$ *eine Basis von* $\mathbf{A}^{(1)}$;

a. *ist* $\mathfrak{a}_1(\beta)$ *eine über* $\mathbf{B}$ *definierte, von* $\mathfrak{G}^{(1)}$ *realisierte* $\mathfrak{a}$*-Funktion von* $\mathbf{A}^{(1)}$ *in* $\mathfrak{N}(\mathfrak{G}^{(1)})$ *und* $\mathfrak{a}_2[\lambda(\beta)]$ *eine in* $\lambda(\mathbf{B})$ *definierte, von* $\mathfrak{G}^{(2)}$ *realisierte* $\mathfrak{a}$*-Funktion von* $\mathbf{A}^{(2)}$ *in* $\mathfrak{N}(\mathfrak{G}^{(2)})$, *so sind*

$$\varkappa[\mathfrak{a}_1(\beta)] = \mathfrak{a}_2^*[\lambda(\beta)] \text{ und } \mathfrak{a}_2[\lambda(\beta)] \text{ assoziiert;}$$

b. *ist* $[\beta_1, \beta_2]_1$ *ein in* $\mathbf{B}$ *definiertes, von* $\mathfrak{G}^{(1)}$ *realisiertes Kommutatorensystem von* $\mathbf{A}^{(1)}$ *in* $\mathfrak{N}(\mathfrak{G}^{(1)})$ *und* $[\lambda(\beta_1), \lambda(\beta_2)]_2$ *ein in* $\lambda(\mathbf{B})$ *definiertes, von* $\mathfrak{G}^{(2)}$ *realisiertes Kommutatorensystem von* $\mathbf{A}^{(2)}$ *in* $\mathfrak{N}(\mathfrak{G}^{(2)})$, *so sind*

$$\varkappa([\beta_1, \beta_2]_1) = \lambda[(\beta_1), \lambda(\beta_2)]_2^* \text{ und } [\lambda(\beta_1), \lambda(\beta_2)]_2 \text{ assoziiert.}$$

BEMERKUNG: Bedingung 3. besagt, daß die Klasse assoziierter, von $\mathfrak{G}^{(1)}$ realisierter, in $\mathbf{B}$ definierter $\mathfrak{a}$-Funktionen [bzw. Kommutatorensysteme] von $\mathbf{A}^{(1)}$ in $\mathfrak{N}(\mathfrak{G}^{(1)})$ durch $\varkappa$ in die Klasse assoziierter, von $\mathfrak{G}^{(2)}$ realisierter, in $\lambda(\mathbf{B})$ definierter $\mathfrak{a}$-Funktionen [bzw. Kommutatorensysteme] von $\mathbf{A}^{(2)}$ in $\mathfrak{N}(\mathfrak{G}^{(2)})$ übergeführt wird. Wesentlich ist, daß $\varkappa$ zusammengehörige $\mathfrak{a}_1$, $[\ldots, \ldots]_1$ nicht wieder in zusammengehörige $\mathfrak{a}_2$, $[\ldots, \ldots]_2$ überzuführen braucht; es können vielmehr beide oder eines dieser Paare nicht-zusammengehörig sein. — Man beachte weiter, daß es leicht, wenn auch umständlich, möglich ist, sich von der Beziehung auf die Basis $\mathbf{B}$ zu befreien.

BEWEIS: Die Notwendigkeit von 1. und 2. folgt daraus, daß $\mathfrak{Z}(\mathfrak{G}), \mathfrak{R}(\mathfrak{G}), \mathfrak{D}(\mathfrak{G})$ gruppeninvariant definierte Untergruppen sind, und die Notwendigkeit von 3. folgt wegen 1., 2. aus E., § 5, (A), S. 407.

Seien also die Bedingungen 1.—3. erfüllt. Dann gibt es zunächst ein zu $[\beta_1, \beta_2]_1$ assoziierter Kommutatorensystem $[\beta_1, \beta_2]_{11}$, das mit $\mathfrak{a}_1(\beta)$ zusammengehört, und ein mit $[\lambda(\beta_1), \lambda(\beta_2)]_2$ assoziiertes Kommutatorensystem $[\lambda(\beta_1), \lambda(\beta_2)]_{22}$, das mit $\mathfrak{a}_2[\lambda(\beta)]$ zusammengehört. Wegen Lemma e. gibt es dann für jedes β aus $\mathbf{B}$ eine Zahl $k_i(\beta)$ mit $0 \leqq k_i(\beta) < p^{n(\beta)}$, so daß

$$[\beta_1, \beta_2]_{11} = \mathfrak{c}_1(\beta_1)^{-k_1(\beta_2)p^{n-n(\beta_2)}} \mathfrak{c}_1(\beta_2)^{k_1(\beta_1)p^{n-n(\beta_1)}} [\beta_1, \beta_2]_1$$

und

$$[\lambda(\beta_1), \lambda(\beta_2)]_{22} = \\ = \mathfrak{c}_2[\lambda(\beta_1)]^{-k_2(\beta_2)p^{n-n(\beta_2)}} \mathfrak{c}_2[\lambda(\beta_2)]^{k_2(\beta_1)p^{n-n(\beta_1)}} [\lambda(\beta_1), \lambda(\beta_2)]_2$$

ist.

Wegen 3. b. ist schließlich:

$$[\lambda(\beta_1), \lambda(\beta_2)]_2 = \\ = \mathfrak{c}_2[\lambda(\beta_1)]^{-k_3(\beta_2)p^{n-n(\beta_2)}} \mathfrak{c}_2[\lambda(\beta_2)]^{k_3(\beta)p^{n-n(\beta_1)}} [\lambda(\beta_1), \lambda(\beta_2)]_2^*.$$

Wir zeigen zunächst:

(1) *Es gibt einen* [*eigentlichen*] *Automorphismus* φ *von* $\mathfrak{R}(\mathfrak{G}^{(2)})$, *so daß*

$\mathfrak{D}(\mathfrak{G}^{(2)})$ *und* $\mathfrak{R}(\mathfrak{G}^{(2)})/\mathfrak{Z}(\mathfrak{G}^{(2)})$ *elementweise invariant bleiben* [*insbesondere also* $\mathfrak{Z}(\mathfrak{G}^{(2)})$ *in sich übergeht*],

$$\varphi([\lambda(\beta_1), \lambda(\beta_2)]_2^*) = [\lambda(\beta_1), \lambda(\beta_2)]_2^* \quad \textit{ist},$$

und

$$\varphi(\mathfrak{a}_2^*[\lambda(\beta)]) \text{ und } [\lambda(\beta_1), \lambda(\beta_2)]_{21} = \\ = \mathfrak{c}_2[\lambda(\beta_1)]^{-k_1(\beta_2)p^{n-n(\beta_2)}} \cdot \mathfrak{c}_2[\lambda(\beta_2)]^{k_1(\beta_1)p^{n-n(\beta_1)}} [\lambda(\beta_1), \lambda(\beta_2)]_2^*$$

zusammengehören.

Da $\mathbf{A}^{(2)}$ eine vollkommene Automorphismengruppe in $\mathfrak{R}(\mathfrak{G}^{(2)})$ ist, da weiter $\mathfrak{c}_2[\lambda(\alpha)]$ eine in die Vollkommenheitsdefinition eingehende isomorphe Abbildung von $\mathbf{A}^{(2)}$ auf $\mathfrak{D}(\mathbf{A}^{(2)}) = \mathfrak{D}(\mathfrak{G}^{(2)})$ ist, da schließlich

$$\mathfrak{a}_2^*[\lambda(\beta)]^{p^{m-n(\beta)}} = \varkappa\left[\mathfrak{a}_1(\beta)^{p^{m-n(\beta)}}\right] = \varkappa[\mathfrak{c}_1(\beta)] = \mathfrak{c}_2[\lambda(\beta)] \text{ ist,}$$

so folgt aus § 4, Zusatz 2. zu Satz 1.:

$$\mathfrak{R}(\mathfrak{G}^{(2)}) = \mathfrak{F} \times \prod_{j=1}^{u} \{\mathfrak{e}_j\} \times \prod_{\beta \text{ in } \mathbf{B}} \{\mathfrak{a}_2^*[\lambda(\beta)]\},$$

$$\mathfrak{Z}(\mathfrak{G}^{(2)}) = \mathfrak{F} \times \prod_{\beta \text{ in } \mathbf{B}} \{\mathfrak{a}_2^*[\lambda(\beta)]\} \times \prod_{j=1}^{u} \left\{\mathfrak{e}_{j-1}\mathfrak{e}_j^{-p^{u(j)-u(j-1)}}\right\},\ \mathfrak{e}_0 = 1$$

$$\mathfrak{D}(\mathfrak{G}^{(2)}) = \prod_{\beta \text{ in } \mathbf{B}} \{\mathfrak{c}_2[\lambda(\beta)]\}.$$

Ist $0 \leqq k(\beta) < p^{n(\beta)}$, so wird durch

$$\varphi(\mathfrak{x}) = \mathfrak{x} \text{ für } \mathfrak{x} \text{ in } \mathfrak{F} \times \prod_{j=1}^{u} \{\mathfrak{e}_j\}$$

$$\varphi(\mathfrak{a}_2^*[\lambda(\beta)]) = \begin{cases} \mathfrak{a}_2^*[\lambda(\beta)]\mathfrak{e}_u^{k(\beta)p^n} & \text{, falls } p \neq 2 \text{ ist,} \\ \mathfrak{a}_2^*[\lambda(\beta)]\mathfrak{e}_u^{k(\beta)2^n}\mathfrak{c}_2[\lambda(\beta)]^{k(\beta)2^{n-1}} & \text{, falls } p = 2 \text{ ist,} \end{cases}$$

ein Automorphismus von $\mathfrak{K}(\mathfrak{G}^{(2)})$ definiert, da die $\mathfrak{a}_2^*$ sämtlich von der Maximalordnung p^m sind, während die hinzutretenden Faktoren sämtlich wegen $p^m \neq 2$ niedere Ordnung haben.

Da $\mathfrak{a}_2^*, \mathfrak{e}_u^{p^n}$ und $\mathfrak{c}_2$ sämtlich zu $\mathfrak{Z}(\mathfrak{G}^{(2)})$ gehören, so ist $\varphi[\mathfrak{Z}(\mathfrak{G}^{(2)})] = \mathfrak{Z}(\mathfrak{G}^{(2)})$ und, da $\varphi(\mathfrak{e}_u) = \mathfrak{e}_u$, so bleibt jedes Element von $\mathfrak{K}(\mathfrak{G}^{(2)})/\mathfrak{Z}(\mathfrak{G}^{(2)})$ bei φ invariant.

Weiter ist

$$\begin{aligned} \varphi(\mathfrak{c}_2[\lambda(\beta)]) &= \varphi(\mathfrak{a}_2^*[\lambda(\beta)])^{p^{m-n(\beta)}}, \text{ wie oben gezeigt,} \\ &= \mathfrak{c}_2[\lambda(\beta)]\,\mathfrak{e}_u^{k(\beta)p^{m+n-n(\beta)}}, \text{ da } m > n, \text{ falls } p = 2, \\ &= \mathfrak{c}_2[\lambda(\beta)], \text{ da } p^m \text{ die Maximalordnung in } \mathfrak{K}(\mathfrak{G}^{(2)}) \text{ ist,} \end{aligned}$$

und φ läßt mithin jedes Element aus $\mathfrak{D}(\mathfrak{G}^{(2)})$ invariant, da $\mathfrak{D}(\mathfrak{G}^{(2)})$ von den $\mathfrak{c}_2[\lambda(\beta)]$ mit β aus $\mathbf{B}$ erzeugt wird.

Schließlich ist

$$[\lambda(\beta_1), \lambda(\beta_2)]_2^* = \mathfrak{f}(\beta_1, \beta_2) \prod_{j=1}^{u} \mathfrak{e}_j^{l_j(\beta_1,\beta_2)} \prod_{\beta \text{ in } \mathbf{B}} \mathfrak{a}_2^*[\lambda(\beta)]^{r(\beta;\beta_1,\beta_2)},$$

wo nur endlich viele Exponenten $\neq 0$ sind. Da $[\lambda(\beta_1), \lambda(\beta_2)]_2^* = \varkappa([\beta_1, \beta_2]_1)$ ist, so folgt aus Lemma, b., 3., daß

$$[\lambda(\beta_1), \lambda(\beta_2)]_2^{*p^{n(\beta_i)}} = 1,$$

und also daß $r(\beta; \beta_1, \beta_2) \equiv 0 \bmod p^{m-n(\beta_i)}$ ist; da $m > n$, falls $p = 2$ ist, so zieht also $p = 2$ nach sich: $r(\beta; \beta_1, \beta_2) \equiv 0 \bmod 2$.

Da $m - n(\beta_i) + n \geqq m$, $n - 1 + m - n(\beta_i) \geqq n$ für $p = 2$, da p^m die Maximalordnung in $\mathfrak{K}(\mathfrak{G}^{(i)})$ und p^n die Maximalordnung in $\mathfrak{D}(\mathfrak{G}^{(i)})$ ist, so folgt hieraus:

$$\varphi([\lambda(\beta_1), \lambda(\beta_2)]_2^*) = [\lambda(\beta_1), \lambda(\beta_2)]_2^*.$$

Wegen 3. a. und Lemma, d. gibt es für jedes β aus $\mathbf{B}$ ein Element $\mathfrak{f}(\beta)$ in $\mathfrak{K}(\mathfrak{G}^{(2)})$, so daß

$$\mathfrak{a}_2^*[\lambda(\beta)] = \begin{cases} \mathfrak{f}(\beta)^{p^{n(\beta)}}\mathfrak{a}_2[\lambda(\beta)] & \text{, falls } p \neq 2 \text{ ist,} \\ \mathfrak{f}(\beta)^{2^{n(\beta)}}\mathfrak{a}_2[\lambda(\beta)]\mathfrak{c}_2[\lambda(\beta)]^{h[\mathfrak{f}(\beta)]2^{n(\beta)-1}} & \text{, falls } p = 2 \text{ ist,} \end{cases}$$

und es ist $h[\mathfrak{f}(\beta)] \equiv 0 \bmod p^{n-n(\beta)}$, da $\mathfrak{f}(\beta)^{p^{n(\beta)}}$ in $\mathfrak{Z}(\mathfrak{G}^{(2)})$ liegt, so daß $\mathfrak{c}_2[\lambda(\beta)]^{h[\mathfrak{f}(\beta)]2^{n(\beta)-1}} = \mathfrak{c}_2[\lambda(\beta)]^{h[\mathfrak{f}(\beta)]2^{n-1}}$ für $p = 2$ wird. Es wird:

$$\varphi(\mathfrak{a}_2^*[\lambda(\beta)]) = \begin{cases} \mathfrak{f}(\beta)^{p^{n(\beta)}}\mathfrak{a}_2[\lambda(\beta)]e_u^{k(\beta)p^n} & \text{, falls } p \neq 2, \\ \mathfrak{f}(\beta)^{2^{n(\beta)}}\mathfrak{a}_2[\lambda(\beta)]\mathfrak{c}_2[\lambda(\beta)]^{2^{n-1}[h(\mathfrak{f}(\beta))+k(\beta)]}e_u^{k(\beta)2^n}, & \\ & \text{falls } p = 2, \end{cases}$$

und also ist $\varphi(\mathfrak{a}_2^*[\lambda(\beta)])$ wegen Lemma, d. ebenfalls zu $\mathfrak{a}_2[\lambda(\beta)]$ assoziiert.

Da nun $\mathfrak{a}_2[\lambda(\beta)]$ und $[\lambda(\beta_1), \lambda(\beta_2)]_{22}$ zusammengehören, so gehören $\varphi(\mathfrak{a}_2^*[\lambda(\beta)])$ und

$$\mathfrak{c}_2[\lambda(\beta_1)]^{-h[\mathfrak{f}(\beta_2)]-k(\beta_2)p^{n-n(\beta_2)}}\mathfrak{c}_2[\lambda(\beta_2)]^{h[\mathfrak{f}(\beta_1)]+k(\beta_1)p^{n-n(\beta_1)}}[\lambda(\beta_1), \lambda(\beta_2)]_{22}$$

zusammen [vergl. den Beweis von Lemma, d., e.].

Nun wird:

$$\mathfrak{c}_2[\lambda(\beta_1)]^{-h[\mathfrak{f}(\beta_2)]-k(\beta_2)p^{n-n(\beta_2)}}\mathfrak{c}_2[\lambda(\beta_2)]^{h[\mathfrak{f}(\beta_1)]+k(\beta_1)p^{n-n(\beta_1)}}[\lambda(\beta_1), \lambda(\beta_2)]_{22} =$$
$$= \mathfrak{c}_2[\lambda(\beta_1)]^{-h[\mathfrak{f}(\beta_2)]-[k(\beta_2)+k_2(\beta_2)]p^{n-n(\beta_2)}} \cdot$$
$$\cdot \mathfrak{c}_2[\lambda(\beta_2)]^{h[\mathfrak{f}(\beta_1)]+[k(\beta_1)+k_2(\beta_1)]p^{n-n(\beta_1)}}[\lambda(\beta_1), \lambda(\beta_2)]_2 =$$
$$= \mathfrak{c}_2[\lambda(\beta_1)]^{-h[\mathfrak{f}(\beta_2)]-[k(\beta_2)+k_2(\beta_2)+k_3(\beta_2)]p^{n-n(\beta_2)}} \cdot$$
$$\cdot \mathfrak{c}_2[\lambda(\beta_2)]^{h[\mathfrak{f}(\beta_1)]+[k(\beta_1)+k_2(\beta_1)+k_3(\beta_1)]p^{n-n(\beta_1)}} \cdot [\lambda(\beta_1), \lambda(\beta_2)]_2^*.$$

Da $h[\mathfrak{f}(\beta)] \equiv 0 \bmod p^{n-n(\beta)}$ ist, so kann man $k(\beta)$ in zulässiger Weise aus

$$h[\mathfrak{f}(\beta)] + [k(\beta) + k_2(\beta) + k_3(\beta)]p^{n-n(\beta)} \equiv k_1(\beta)p^{n-n(\beta)} \bmod p^n$$

bestimmen. Tut man dies, so gehören

$\varphi(\mathfrak{a}_2^*[\lambda(\beta)])$ und

$$\mathfrak{c}_2[\lambda(\beta_1)]^{-k_1(\beta_2)p^{n-n(\beta_2)}}\mathfrak{c}_2[\lambda(\beta_1)]^{k_1(\beta_1)p^{n-n(\beta_1)}}[\lambda(\beta_1), \lambda(\beta_2)]_2^*$$

zusammen und (1) ist bewiesen.

Nun ist $\varphi[\varkappa(\mathfrak{k})]$ für $\mathfrak{k}$ aus $\mathfrak{K}(\mathfrak{G}^{(1)})$ eine isomorphe Abbildung von $\mathfrak{K}(\mathfrak{G}^{(1)})$ auf $\mathfrak{K}(\mathfrak{G}^{(2)})$, die $\mathfrak{Z}(\mathfrak{G}^{(1)})$ in $\mathfrak{Z}(\mathfrak{G}^{(2)})$, $\mathfrak{D}(\mathfrak{G}^{(1)})$ in $\mathfrak{D}(\mathfrak{G}^{(2)})$ und also auch $\mathbf{A}^{(1)}$ in $\mathbf{A}^{(2)}$ überführt [da φ jedes Element von $\prod_{j=1}^{u}\{e_j\} \times \mathfrak{D}(\mathfrak{G}^{(2)})$ invariant läßt und $\mathfrak{Z}(\mathfrak{G})^{(2)}$ in sich überführt,

tut dies die in 2. erwähnte Abbildung λ], und die überdies ein zusammengehöriges Paar $\mathfrak{a}$-Funktion, Kommutatorensystem, die von $\mathfrak{G}^{(1)}$ in $\mathfrak{K}(\mathfrak{G}^{(1)})$ realisiert werden, in ein zusammengehöriges, von $\mathfrak{G}^{(2)}$ in $\mathfrak{K}(\mathfrak{G}^{(2)})$ realisiertes Paar überführt, und die sich also nach E., § 5, (A), S. 407 bzw. E., § 2, Satz 2., S. 391 zu einer isomorphen Abbildung von $\mathfrak{G}^{(1)}$ auf $\mathfrak{G}^{(2)}$ erweitern läßt.

Folgerung 1.: *Die vollkommenen Gruppen* $\mathfrak{G}^{(1)}$ *und* $\mathfrak{G}^{(2)}$ *sind isomorph, wenn es*

I. *eine Bedingung* 1., 2., 3. b. *von Satz* 1. *erfüllende, isomorphe Abbildung* $\varkappa$ *von* $\mathfrak{K}(\mathfrak{G}^{(1)})$ *auf* $\mathfrak{K}(\mathfrak{G}^{(2)})$ *gibt, und wenn es*

II. *eine Zerlegung* $\mathfrak{K}(\mathfrak{G}^{(2)}) = \mathfrak{B}^{(2)} \times \prod_{j=1}^{u} \{\mathfrak{e}_j\} \times \prod_{\beta \text{ in } \mathbf{B}} \{\mathfrak{a}[\lambda(\beta)]\}$ *von* $\mathfrak{K}(\mathfrak{G}^{(2)})$ *bzgl.* $\mathbf{A}^{(2)}$ *gemäß* § 4., *Zusatz* 2. *zu Satz* 1. *gibt, so daß* $[\lambda(\beta_1), \lambda(\beta_2)]_2$ *in* $\mathfrak{B}^{(2)} \times \prod_{j=1}^{u} \{\mathfrak{e}_j\}$ *liegt.*

Dies folgt aus Satz 1., wenn wir gezeigt haben:

(2) *sind* I., II. *erfüllt und* $\mathfrak{a}_i$, $\mathfrak{a}_i^*$ *wie in Satz* 1., 3., a. *definiert, so gibt es einen* $\mathfrak{B}^{(2)} \times \prod_{j=1}^{u} \{\mathfrak{e}_j\} \times \mathfrak{D}(\mathbf{A}^{(2)})$ *elementweise invariant lassenden Automorphismus* φ *von* $\mathfrak{K}(\mathfrak{G}^{(2)})$, *der*

$$\varphi(\mathfrak{a}_2^*[\lambda(\beta)]) = \mathfrak{a}_2[\lambda(\beta)]$$

erfüllt.

Nun ist

$$\mathfrak{a}_2^*[\lambda(\beta)]^{p^{m-n(\beta)}} = [\varkappa(\mathfrak{a}_1[\beta])]^{p^{m-n(\beta)}} = \varkappa[\mathfrak{a}_1(\beta)^{p^{m-n(\beta)}}] =$$
$$= \varkappa[\mathfrak{c}_1(\beta)] = \mathfrak{c}_2[\lambda(\beta)] = (\mathfrak{a}_2[\lambda(\beta)])^{p^{m-n(\beta)}},$$

und, da $n(\beta) > 0$, also $m - n(\beta) < m$ ist, so ist $\mathfrak{a}_2^*[\lambda(\beta)](\mathfrak{a}_2[\lambda(\beta)])^{-1}$ ein Element von niederer als p^m-ter Ordnung aus $\mathfrak{Z}(\mathfrak{G}^{(2)}) = \mathfrak{Z}(\mathbf{A}^{(2)})$, und mithin existiert ein $\mathfrak{B}^{(2)} \times \prod_{j-1}^{u} \{\mathfrak{e}_j\}$ elementweise invariant lassender Automorphismus φ von $\mathfrak{K}(\mathfrak{G}^{(2)})$, der $\varphi(\mathfrak{a}_2^*[\lambda(\beta)]) = \mathfrak{a}_2[\lambda(\beta)]$ erfüllt; da $\mathfrak{D}(\mathbf{A}^{(2)})$ durch die $\mathfrak{c}_2[\lambda(\beta)]$ mit β aus $\mathbf{B}$ erzeugt wird, und da $\mathfrak{a}_2^*[\lambda(\beta)]^{p^{m-n(\beta)}} = \mathfrak{a}_2[\lambda(\beta)]^{p^{m-n(\beta)}} = \mathfrak{c}_2[\lambda(\beta)]$ ist, so leistet φ das Verlangte und (2) ist bewiesen.

Folgerung 2.: *Zwei vollkommene Gruppen* $\mathfrak{G}^{(1)}$ *und* $\mathfrak{G}^{(2)}$, *die denselben Kern* $\mathfrak{A}$ *haben, und die in* $\mathfrak{A}$ *dieselbe* [*vollkommene*] *Automorphismengruppe* $\mathbf{A}$ *induzieren, sind isomorph, wenn beide dasselbe Kommutatorensystem* $[\beta_1, \beta_2]$ *— definiert über derselben Basis* $\mathbf{B}$ *von* $\mathbf{A}$ *— realisieren, und es eine Zerlegung* $\mathfrak{A} = \mathfrak{B} \times \prod_{j=1}^{u} \{\mathfrak{e}_j\} \times \prod_{\beta \text{ in } \mathbf{B}} \{\mathfrak{a}(\beta)\}$

von $\mathfrak{A}$ *bzgl.* $\mathbf{A}$ *gemäß* § 4., *Satz* 1. *gibt, so daß* $[\beta_1, \beta_2]$ *in* $\mathfrak{B} \times \prod_{j=1}^{u} \{e_j\}$ *liegt.*

Zum Beweise betrachten wir die durch $\mathfrak{G}^{(i)}$ gemäß § 3., Satz 1., c. induzierte isomorphe Abbildung $\mathfrak{c}_i(\alpha)$ von $\mathbf{A}$ auf $\mathfrak{D}(\mathbf{A}) = \mathfrak{D}(\mathfrak{G}^{(i)})$. Nach der an § 4., Definition 1. angeschlossenen Bemerkung gibt es eine zu p teilerfremde Zahl c, so daß $\mathfrak{c}_1(\alpha)^c = \mathfrak{c}_2(\alpha)$ ist.

Sei nun $\varkappa$ der $\mathfrak{B} \times \prod_{j=1}^{u} \{e_j\}$ elementweise invariant lassende Automorphismus von $\mathfrak{A}$, der $\varkappa[\mathfrak{a}(\beta)] = \mathfrak{a}(\beta)^c$ für β aus $\mathbf{B}$ erfüllt. Dann wird

$$\varkappa[\mathfrak{c}_1(\alpha)] = \mathfrak{c}_1(\alpha)^c = \mathfrak{c}_2(\alpha),$$

d.h. die in Satz 1., 2. auftretende isomorphe Abbildung λ von $\mathbf{A}$ auf sich ist die identische Abbildung. Weiter ist

$$\varkappa[\mathfrak{Z}(\mathfrak{G}^{(1)})] = \varkappa[\mathfrak{Z}(\mathbf{A})] = \mathfrak{Z}(\mathbf{A}) = \mathfrak{Z}(\mathfrak{G}^{(2)}),$$
$$\varkappa[\mathfrak{D}(\mathfrak{G}^{(1)})] = \mathfrak{D}(\mathbf{A}) = \mathfrak{D}(\mathfrak{G}^{(2)})$$

und

$$[\lambda(\beta_1), \lambda(\beta_2)]_2^* = [\beta_1, \beta_2]_2^* = \varkappa([\beta_1, \beta_2]) = [\beta_1, \beta_2];$$

mithin ist $\varkappa$ eine die Bedingungen I., II. der Folgerung 1. erfüllende isomorphe Abbildung $\mathfrak{R}(\mathfrak{G}^{(1)}) = \mathfrak{A}$ auf $\mathfrak{R}(\mathfrak{G}^{(2)}) = \mathfrak{A}$ und Folgerung 2. folgt aus Folgerung 1.

Daß die in den Folgerungen 1. und 2. gemachten Annahmen über die Lage des Kommutatorensystems i. A. nicht entbehrlich sind, zeigt das folgende

Beispiel *von zwei nicht-isomorphen vollkommenen Gruppen, die denselben Kern* $\mathfrak{A}$ *haben, in diesem dieselbe Automorphismengruppe* $\mathbf{A}$ *induzieren, die dieselbe isomorphe Beziehung* $\mathfrak{c}(\alpha)$ *von* $\mathbf{A}$ *auf* $\mathfrak{D}(\mathbf{A})$ *gemäß* § 3, *Satz* 1., c. *induzieren und dasselbe Kommutatorensystem realisieren.*

Es sei

$$\mathfrak{A} = \{\mathfrak{e}\} \times \prod_{i=1}^{3} \{\mathfrak{a}_i\} \times \{\mathfrak{z}\},$$

wo $\mathfrak{e}$ und $\mathfrak{a}_i$ die Ordnung p^m, $\mathfrak{z}$ die Ordnung p haben, $p \neq 2$ und $m > 1$ ist. Nach § 4, Zusatz 1. zu Satz 3. gibt es genau eine vollkommene Automorphismengruppe $\mathbf{A}$ in $\mathfrak{A}$ mit

$$\mathfrak{Z}(\mathbf{A}) = \prod_{i=1}^{3} \{\mathfrak{a}_i\} \times \{\mathfrak{z}\}$$

$$\mathfrak{D}(\mathbf{A}) = \{\mathfrak{a}_1^p\} \times \{\mathfrak{a}_2\} \times \{\mathfrak{a}_3\},$$

und zwar ist

$$\mathbf{A} = \prod_{i=1}^{3} \{\alpha_i\}$$

mit

$$\alpha_1(\mathfrak{e}^e \mathfrak{z}^z \prod_{i=1}^{3} \mathfrak{a}_i^{a_i}) = \mathfrak{e}^e \mathfrak{z}^z \prod_{i=1}^{3} \mathfrak{a}_i^{a_i} \mathfrak{a}_1^{pe}$$

$$\alpha_j(\mathfrak{e}^e \mathfrak{z}^z \prod_{i=1}^{3} \mathfrak{a}_i^{a_i}) = \mathfrak{e}^e \mathfrak{z}^z \prod_{i=1}^{3} \mathfrak{a}_i^{a_i} \mathfrak{a}_j^{e} \text{ für } j = 2, 3.$$

Schließlich wird durch

$$\mathfrak{c}(\alpha_1) = \mathfrak{a}_1^p, \ \mathfrak{c}(\alpha_j) = \mathfrak{a}_j \text{ für } j = 2, 3$$

eine in die Vollkommenheitsdefinition eingehende isomorphe Abbildung von $\mathbf{A}$ auf $\mathfrak{D}(\mathbf{A})$ definiert.

$$[\alpha_1, \alpha_j] = [\alpha_j, \alpha_1] = 1 \text{ für } j = 2, 3$$

$$[\alpha_2, \alpha_3] = [\alpha_3, \alpha_2]^{-1} = \mathfrak{a}_1$$

liegt in $\mathfrak{Z}(\mathbf{A})$ und ist wegen Lemma, b. ein realisierbares Kommutatorensystem. Für jede dieses Kommutatorensystem und $\mathbf{A}$ realisierende, vollkommene Erweiterung ist

$$\mathfrak{E} = \{[\alpha_i, \alpha_k], \ \mathfrak{D}(\mathbf{A})\} = \prod_{i=1}^{3} \{\mathfrak{a}_i\}$$

die Kommutatorgruppe.

Ist $\mathfrak{b}_1(\alpha_i) = \mathfrak{a}_i$ und $\mathfrak{b}_2(\alpha_1) = \mathfrak{a}_1\mathfrak{z}$, $\mathfrak{b}_2(\alpha_j) = \mathfrak{a}_j$ für $j = 2, 3$, so sind wegen Lemma, a. sowohl $\mathfrak{b}_1$ als auch $\mathfrak{b}_2$ realisierbare $\mathfrak{a}$-Funktionen und beide gehören zu $\mathfrak{c}$, d.h.

$$\mathfrak{b}_i(\alpha_j)^{p^{m-n(\alpha_j)}} = \mathfrak{c}(\alpha_j).$$

Nach Lemma, d. liegen alle zu $\mathfrak{b}_1$ assoziierten $\mathfrak{a}$-Funktionen in $\mathfrak{E}$, aber keine zu $\mathfrak{b}_2$ assoziierte, und hieraus folgt nach Satz 1., daß die durch $[\alpha_i, \alpha_k]$, $\mathfrak{b}_1$ bestimmte und die durch $[\alpha_i, \alpha_k]$, $\mathfrak{b}_2$ bestimmte vollkommene, u.s.w. Erweiterung von $\mathfrak{A}$ nicht isomorph sein können, womit unsere Behauptung bewiesen ist.

Satz 2.: *Es sei $\mathfrak{A}$ eine abelsche Primärgruppe der [endlichen] Maximalordnung p^m und $\mathbf{A}$ eine vollkommene, nichtzyklische Automorphismengruppe in $\mathfrak{A}$ der Maximalordnung p^n und $n < m$, falls $p = 2$ ist.*

Dann und nur dann sind alle realisierbaren Kommutatorensysteme von $\mathbf{A}$ in $\mathfrak{A}$ assoziiert, wenn entweder

a. *$p = 3$ und $\mathfrak{A}$ direktes Produkt von drei, $\mathbf{A}$ von zwei Zyklen der Ordnung 3 ist, oder*

b. $p = 2$ *und sowohl* $\mathfrak{A}$ *direktes Produkt zweier Zyklen der Ordnung* 2^m *mit einem der Ordnung* 2 *als auch* $\mathbf{A}$ *direktes Produkt zweier Zyklen der Ordnung* 2 *ist.*

BEWEIS: A. Es sei $\mathbf{B}$ eine Basis von $\mathbf{A}$; nach Lemma, b. ist $[\beta_1, \beta_2]_0 = 1$ für $\beta_1 \neq \beta_2$ aus $\mathbf{B}$ ein realisierbares Kommutatorensystem von $\mathbf{A}$ in $\mathfrak{A}$. Weiter sei $\mathfrak{c}(\alpha)$ eine in die Vollkommenheitsdefinition eingehende, isomorphe Abbildung von $\mathbf{A}$ auf $\mathfrak{D}(\mathbf{A})$.

(3) *Enthält* $\mathbf{B}$ *wenigstens drei Elemente, so gibt es ein nicht zu* $[\beta_1, \beta_2]_0$ *assoziiertes realisierbares Kommutatorensystem von* $\mathbf{A}$ *in* $\mathfrak{A}$.

Seien nämlich α_1, α_2, α_3 drei verschiedene, beliebige, aber feste Elemente aus $\mathbf{B}$ und sei etwa [26]) $n(\alpha_1) \leqq n(\alpha_2) \leqq n(\alpha_3)$. Wir definieren:

$$[\alpha_k, \alpha_i]^{-1} = [\alpha_i, \alpha_k] = \mathfrak{c}(\alpha_1) \text{ für } i < k,$$

$$[\beta, \alpha_i] = [\alpha_i, \beta] = 1 \text{ für } \beta \neq \alpha_k \text{ aus } \mathbf{B},$$

$$[\beta_1, \beta_2] = [\beta_2, \beta_1] = 1 \text{ für } \beta_i \neq \alpha_k \text{ aus } \mathbf{B}.$$

Da $[\gamma_1, \gamma_2]$ für $\gamma_1 \neq \gamma_2$ aus $\mathbf{B}$ stets in $\mathfrak{Z}(\mathbf{A})$, sogar in $\mathfrak{D}(\mathbf{A}) = \mathfrak{Z}(\mathbf{A})$ liegt, und da $\mathfrak{c}(\alpha_1)^{p^{n(\alpha_1)}} = 1$ ist, so ist $[\gamma_1, \gamma_2]$ nach Lemma, b. ein realisierbares Kommutatorensystem. Ist $[\gamma_1, \gamma_2]_1$ zu $[\gamma_1, \gamma_2]$ assoziiert, so ist

$$[\alpha_2, \alpha_3]_1 = \mathfrak{c}(\alpha_1)\mathfrak{c}(\alpha_2)^{a_1}\mathfrak{c}(\alpha_3)^{a_2} \neq 1$$

nach Lemma, e. und also $[\gamma_1, \gamma_2]$ nicht zu $[\gamma_1, \gamma_2]_0$ assoziiert, womit (3) bewiesen ist.

(4) *Gibt es ein Element der Ordnung* p *in* $\mathfrak{Z}(\mathbf{A})$, *das nicht in* $\mathfrak{D}(\mathbf{A})$ *liegt, so gibt es ein nicht zu* $[\beta_1, \beta_2]_0$ *assoziiertes, realisierbares Kommutatorensystem von* $\mathbf{A}$ *in* $\mathfrak{A}$.

Wegen (3) können wir beim Beweise von (4) annehmen, daß $\mathbf{B}$ genau zwei Elemente β_1 und β_2 enthält; weiter sei $\mathfrak{p} \neq 1$ ein Element der Ordnung p aus $\mathfrak{Z}(\mathbf{A})$, das nicht in $\mathfrak{D}(\mathbf{A})$ liegt. Dann ist

$$[\beta_1, \beta_2] = [\beta_2, \beta_1]^{-1} = \mathfrak{p}$$

nach Lemma, b. ein realisierbares Kommutatorensystem, und dies ist nicht zu $[\beta_1, \beta_2]_0$ assoziiert, da es nicht in $\mathfrak{D}(\mathbf{A})$ liegt, während jedes zu $[\beta_1, \beta_2]_0$ assoziierte Kommutatorensystem nach Lemma, e. in $\mathfrak{D}(\mathbf{A})$ liegt.

B [27]). Es enthalte $\mathbf{B}$ genau zwei verschiedene Elemente β_1

---

[26]) $p^{n(\alpha)}$ = Ordnung von α.

[27]) Das folgende läßt sich durch Benutzung der Sätze des § 8, die aber meist tiefer liegen als das hier gebrauchte, abkürzen.

und β_2 und jedes Element der Ordnung p aus $\mathfrak{Z}(\mathbf{A})$ gehöre zu $\mathfrak{D}(\mathbf{A})$.

Dann hat eine Darstellung von $\mathfrak{A}$ gemäß § 4, Zusatz 2. zu Satz 1. die Form:

$$\begin{aligned}\mathfrak{A} &= \{e\} \times \{\mathfrak{a}(\beta_1)\} \times \{\mathfrak{a}(\beta_2)\},\\ \mathfrak{Z}(\mathbf{A}) &= \{\mathfrak{a}(\beta_1)\} \times \{\mathfrak{a}(\beta_2)\},\\ \mathfrak{D}(\mathbf{A}) &= \{\mathfrak{c}(\beta_1)\} \times \{\mathfrak{c}(\beta_2)\},\end{aligned}$$

wo e die Ordnung p^n und $\mathfrak{a}(\beta_i)$ die Ordnung p^m hat. O. B. d. A. sei $n(\beta_1) \leqq n(\beta_2)$.

(5) *Jedes realisierbare Kommutatorensystem ist zu einem der Form*

$$[\beta_1, \beta_2] = [\beta_2, \beta_1]^{-1} = e^{sp^{n(\beta_2)-n(\beta_1)}}$$

assoziiert.

Es ist nämlich

$$[\beta_1, \beta_2] = e^r\, \mathfrak{a}(\beta_1)^{a_1}\, \mathfrak{a}(\beta_2)^{a_2}.$$

Nach Lemma, b., 3. ist $[\beta_1, \beta_2]^{p^{n(\beta_1)}} = 1$ und also

$$r \equiv 0 \bmod p^{n(\beta_2)-n(\beta_1)}, \text{ da } n = n(\beta_2) \text{ ist,}$$

$$a_i \equiv 0 \bmod p^{m-n(\beta_1)}, \text{ also}$$

$$\mathfrak{a}(\beta_i)^{a_i} = \mathfrak{c}(\beta_i)^{b_i p^{n-n(\beta_{i\pm1})}},$$

und (5) folgt aus Lemma, e.

(6) $$[\beta_1, \beta_2] = [\beta_2, \beta_1]^{-1} = e^{sp^{n(\beta_2)-n(\beta_1)}}$$

ist ein realisierbares Kommutatorensystem von $\mathbf{A}$ *in* $\mathfrak{A}$,

a. *wenn* $p \neq 2$, $p \neq 3$ *ist,*

b. *falls* $p = 3$ *ist, dann und nur dann, wenn*

$$s \cdot 3^{m-1+n(\beta_2)-n(\beta_1)} \equiv 0 \text{ mod } 3^n \text{ ist,}$$

c. *falls* $p = 2$ *ist, dann und nur dann, wenn*

$$s \cdot 2^{2n(\beta_2)-1-n(\beta)} \equiv 0 \text{ mod } 2^n \text{ ist.}$$

Dies folgt aus Lemma, b., wenn man $n(\beta_2) = n$ beachtet.

Ein realisierbares Kommutatorensystem von $\mathbf{A}$ in $\mathfrak{A}$ der Form

$$[\beta_1, \beta_2] = [\beta_2, \beta_1]^{-1} = e^{sp^{n(\beta_2)-n(\beta_1)}}$$

ist wegen Lemma, e. dann und nur dann zu $[\beta_1, \beta_2]_0$ assoziiert, wenn $e^{sp^{n(\beta_2)-n(\beta_1)}} = 1$ ist, d.h. wenn

$$s \equiv 0 \bmod p^{n(\beta_1)}$$

ist. Damit also alle realisierbaren Kommutatorensysteme von **A** in $\mathfrak{A}$ zu $[\beta_1, \beta_2]_0$ assoziiert sind, muß also jedenfalls $p = 2$ oder $p = 3$ sein. Ist weiter $p = 3$, so ist dies wegen (6), b. dann und nur dann der Fall, wenn jede $s \cdot 3^{m-1+n-n(\beta_1)} \equiv 0 \bmod 3^n$ erfüllende Zahl s auch $s \equiv 0 \bmod 3^{n(\beta_1)}$ erfüllt, und dies ist dann und nur dann der Fall, wenn $m = 1$ ist. Ist schließlich $p = 2$, so ist dies wegen (6), c. dann und nur dann der Fall, wenn jede $s \cdot 2^{2n-1-n(\beta_1)} \equiv 0 \bmod 2^n$ erfüllende Zahl s auch $s \equiv 0 \bmod 2^{n(\beta_1)}$ erfüllt, und dies tritt dann und nur dann ein, wenn $n = n(\beta_i) = 1$ ist, da $n(\beta_1) \leqq n(\beta_2) = n$ ist, womit alles bewiesen ist.

FOLGERUNG: *Es sei* $\mathfrak{A}$ *eine abelsche Primärgruppe,* **A** *eine vollkommene Automorphismengruppe in* $\mathfrak{A}$.

Dann und nur dann sind irgendzwei vollkommene Gruppen, deren Kern $\mathfrak{A}$ *ist, und die in* $\mathfrak{A}$ *genau* **A** *induzieren, isomorph, wenn entweder die Bedingung* a. *oder die Bedingung* b. *von Satz* 2. *erfüllt ist* [28]).

Die Notwendigkeit der Bedingungen folgt aus Satz 1. und Satz 2., wenn man bedenkt, daß das Kommutatorensystem $[\beta_1, \beta_2]_0 = 1$ bei allen Automorphismen in sich übergeht, ihr Hinreichen folgt aus Satz 2., da Folgerung 1. aus Satz 1. auf das einzige realisierbare Kommutatorensystem $[\beta_1, \beta_2]_0 = 1$ anwendbar ist.

§ 8.

Vollkommene Gruppen, die mod Kern direktes Produkt zweier Zyklen sind.

In diesem § 8. werden wir einige Sätze über abelsche Gruppen benötigen, die hier kurz ohne Beweis [29]) zusammengestellt seien:

Es sei $\mathfrak{P}$ eine abelsche Primärgruppe der endlichen Maximalordnung p^m und, falls $\mathfrak{p}$ ein Element aus $\mathfrak{P}$ ist, sei $p^{n(\mathfrak{p})}$ die Ordnung von $\mathfrak{p}$. Das Element $\mathfrak{e}$ von $\mathfrak{P}$ heißt einfach in $\mathfrak{P}$, wenn die Gleichung

$$\mathfrak{e}^{p^i} = \mathfrak{p}^{p^{i+1}} \text{ für } 0 \leqq i < n(\mathfrak{e})$$

---

[28]) Man beachte, daß durch a. die Struktur von **A** als Automorphismengruppe wegen § 4, Satz 2 [$u = 1, v(1) = 1, w = 0$] bestimmt ist, und daß **A** durch $\mathfrak{A}$ und b. wegen § 4, Zusatz zu Satz 3 eindeutig festgelegt ist, so daß also gilt:

an vollkommenen Gruppen, die durch den Kern und die nicht zyklische, im Kern induzierte Automorphismengruppe bestimmt sind, gibt es für $p \neq 2, p \neq 3$ *keine, für* $p = 3$ *genau eine und für* $p = 2$ *genau eine für jedes* $m > 1$.

[29]) Für die Beweise u.s.f. vergl. T., § 1.

in $\mathfrak{P}$ unlösbar ist. Ein in $\mathfrak{P}$ einfaches Element ist auch in jeder Untergruppe von $\mathfrak{P}$ einfach; dagegen kann ein Element in einer Untergruppe von $\mathfrak{P}$ einfach sein, ohne in $\mathfrak{P}$ einfach zu sein. Sind $\mathfrak{e}_1, \ldots, \mathfrak{e}_r$ einfache Elemente und $n(\mathfrak{e}_1) < \ldots < n(\mathfrak{e}_r)$, so gibt es eine direkte Produktzerlegung:

$$\mathfrak{P} = \{\mathfrak{e}_1\} \times \cdots \times \{\mathfrak{e}_r\} \times \mathfrak{P}'.$$

Zwei Elemente $\mathfrak{p}$ und $\mathfrak{q}$ aus $\mathfrak{P}$ heißen *isotyp in* $\mathfrak{P}$, wenn es einen $\mathfrak{p}$ in $\mathfrak{q}$ überführenden [eigentlichen] Automorphismus von $\mathfrak{P}$ gibt. I. A. kann aus der Isotypie bzw. Nicht-Isotypie in Untergruppen nicht auf die in Obergruppen geschlossen werden; doch sind zwei Elemente eines direkten Faktors von $\mathfrak{P}$ dann und nur dann in diesem isotyp, wenn sie in $\mathfrak{P}$ isotyp sind.

Isotypieinvarianten sind der Ordnungsexponent $n(\mathfrak{p})$, der *Höhenexponent* [30]) $e(\mathfrak{p})$ und also auch

$$s(\mathfrak{p}) = n(\mathfrak{p}) + e(\mathfrak{p})$$

und die Reihe der Zahlen

$$\mathbf{I}(\mathfrak{p}) : s(\mathfrak{p}),\ s(\mathfrak{p}^p),\ \ldots,\ s(\mathfrak{p}^{p^{n(\mathfrak{p})-1}}).$$

[Es ist stets $s(\mathfrak{p}^{p^i}) \leqq s(\mathfrak{p}^{p^{i+1}})$.] Aus $\mathbf{I}(\mathfrak{p})$ liest man die folgenden Invarianten ab:

Die Anzahl $d(\mathfrak{p})$ der verschiedenen unter den Zahlen aus $\mathbf{I}(\mathfrak{p})$, die aus den sämtlichen verschiedenen unter den Zahlen aus $\mathbf{I}(\mathfrak{p})$ bestehende Reihe $n_1(\mathfrak{p}) < \ldots < n_{d(\mathfrak{p})}(\mathfrak{p})$ und die Zahl

$$z_i(\mathfrak{p}) = e(\mathfrak{p}^{p^{k_i}}),$$

wo k_i eine kleinste Zahl mit

$$n_i(\mathfrak{p}) = s(\mathfrak{p}^{p^{k_i}})$$

ist. Dann ist auch

$$0 < n_1(\mathfrak{p}) - z_1(\mathfrak{p}) < \ldots < n_{d(\mathfrak{p})}(\mathfrak{p}) - z(\mathfrak{p}_{d(\mathfrak{p})}) = n(\mathfrak{p}).$$

Für einfache Elemente $\mathfrak{e}$ ist $d(\mathfrak{e}) = 1$, $e(\mathfrak{e}) = 0$; ist $\mathfrak{p}$ ein beliebiges Element, so gibt es $d(\mathfrak{p})$ einfache Elemente $\mathfrak{e}_i(\mathfrak{p})$, so daß

$$\mathfrak{p} = \prod_{i=1}^{d(\mathfrak{p})} \mathfrak{e}_i(\mathfrak{p})^{p^{z_i(\mathfrak{p})}} \quad \text{und} \quad n[\mathfrak{e}_i(\mathfrak{p})] = n_i$$

ist, und hieraus folgert man:

---

[30]) Dies ist nach H. Prüfer die größte Zahl derart, daß die Gleichung $\mathfrak{p}^{p^e} = \mathfrak{q}$ eine Lösung $\mathfrak{q}$ in $\mathfrak{P}$ hat.

die Elemente $\mathfrak{p}$ *und* $\mathfrak{q}$ *aus* $\mathfrak{P}$ *sind dann und nur dann isotyp in* $\mathfrak{P}$, *wenn*

$$d(\mathfrak{p}) = d(\mathfrak{q}),\quad n_i(\mathfrak{p}) = n_i(\mathfrak{q}),\quad z_i(\mathfrak{p}) = z_i(\mathfrak{q})$$

ist, oder gleichwertig, wenn $\mathbf{I}(\mathfrak{p}) = \mathbf{I}(\mathfrak{q})$ *ist.*

Es sei $\mathfrak{A}$ eine abelsche Primärgruppe der Maximalordnung p^m, $\mathbf{A}$ eine vollkommene Automorphismengruppe in $\mathfrak{A}$ und

$$\mathbf{A} = \{v\} \times \{\varkappa\},$$

wo p^n die Ordnung von v, p^k die von $\varkappa$, $m \geqq n \geqq k > 0$ und, falls $p = 2$ ist, $m > n$ ist. Schließlich sei $\mathfrak{c}(\alpha)$ eine in die Vollkommenheitsdefinition eingehende isomorphe Abbildung von $\mathbf{A}$ auf $\mathfrak{D}(\mathbf{A})$.

Wir machen jetzt die spezielle Annahme, die für den ganzen Verlauf dieses § gelten soll, daß die im § 4 definierte Invariante $u(\mathbf{A}) = 1$ ist, so daß also die Darstellung von $\mathfrak{A}$ gemäß § 4., Zusatz zu Satz 1. die Form

$$(*)\quad \begin{cases} \mathfrak{A} & = \mathfrak{B} \times \{e\} \times \{\mathfrak{a}(v)\} \times \{\mathfrak{a}(\varkappa)\}, \\ \mathfrak{Z}(\mathbf{A}) & = \mathfrak{B} \times \{e^{p^n}\} \times \{\mathfrak{a}(v)\} \times \{\mathfrak{a}(\varkappa)\}, \\ \mathfrak{D}(\mathbf{A}) & = \{\mathfrak{c}(v)\} \times \{\mathfrak{c}(\varkappa)\}, \end{cases}$$

hat, wo $\mathfrak{a}(v)$, $\mathfrak{a}(\varkappa)$ die Ordnung p^m, e die Ordnung p^v mit $n \leqq v = v(1, \mathbf{A}) \leqq m$ haben und $\mathfrak{a}(v)^{p^{m-n}} = \mathfrak{c}(v)$, $\mathfrak{a}(\varkappa)^{p^{m-k}} = \mathfrak{c}(\varkappa)$ ist.

Da jedes realisierbare Kommutatorensystem von $\mathbf{A}$ in $\mathfrak{A}$ nur aus $[v, \varkappa]$ und $[\varkappa, v] = [v, \varkappa]^{-1}$ besteht, können wir uns auf die Betrachtung realisierbarer Kommutatoren $[v, \varkappa]$ beschränken. Zwei Kommutatoren heißen *äquivalent*, wenn sie [u. a.] durch isomorphe [vollkommene, $\mathfrak{A}$ zum Kern habende, in $\mathfrak{A}$ genau $\mathbf{A}$ induzierende] Gruppen realisiert werden.

Definition: *Ein Element aus* $\mathfrak{A}$ *heiße normiert* [*bzgl. der Darstellung* $(*)$[31]) *von* $\mathfrak{A}$], *wenn es*

a. *die Form*

$$\mathfrak{b}\, e^{p^w} \text{ mit } 0 \leqq w \leqq v,\ \mathfrak{b} \text{ in } \mathfrak{B}$$

hat, und wenn

b. *die Invarianten* $d(\mathfrak{b})$, $n_i(\mathfrak{b})$, $z_i(\mathfrak{b})$ *von* $\mathfrak{b}$ *in* $\mathfrak{B}$ *noch die folgenden Bedingungen erfüllen*:

---

[31]) die im folgenden festgehalten wird, solange nichts Anderes gesagt.

1. $w - z_i > \min [0, v - n_i]$ *für jedes* i *mit* $1 \leqq i \leqq d(\mathfrak{b})$;
2. *ist* $w \neq v$ *und* $n \leqq w - z_i$ *für ein* i, *so ist auch* $w - z_i < v - n_i$.

SATZ 1: a. *Zwei vollkommene Gruppen, die* $\mathfrak{A}$ *zum Kern haben und in* $\mathfrak{A}$ *genau* **A** *induzieren, sind isomorph, wenn sie denselben Kommutator von* **A** *in* $\mathfrak{A}$ *realisieren.*

b. *Jeder realisierbare Kommutator von* **A** *in* $\mathfrak{A}$ *ist zu einem normierten äquivalent.*

c. *Das normierte Element* $\mathfrak{b}\mathfrak{e}^{p^w}$ *ist dann und nur dann ein realisierbarer Kommutator, wenn*

$$\mathfrak{b}^{p^k} = 1, \quad k \geqq v - w$$

und

$$w \geqq 1 \text{ ist, falls } p = 3 \text{ und } v = k = n = m \text{ oder}$$
$$p = 2 \text{ und } v = k = n \text{ ist.}$$

BEWEIS: Es sei $[\nu, \varkappa]$ ein realisierbarer Kommutator von **A** in $\mathfrak{A}$. Wegen $(*)$ ist dann:

$$[\nu, \varkappa] = \mathfrak{b}\mathfrak{e}^r \mathfrak{a}(\tau)^s \mathfrak{a}(\varkappa)^t$$

mit $\mathfrak{b}$ in $\mathfrak{B}$, $0 < r \leqq p^v$, $0 \leqq s$, $t < p^m$.

Nach § 7., Lemma, b., 3. wird dann

$$1 = [\nu, \varkappa]^{p^k} \text{ und also, da } m \geqq v \geqq n \geqq k > 0 \text{ ist,}$$
$$1 = \mathfrak{b}^{p^k}, \quad r \equiv 0 \bmod p^{v-k}, \quad s \equiv t \equiv 0 \bmod p^{m-k},$$

d.h. für geeignete r', s', t' wird

$$[\nu, \varkappa] = \mathfrak{b}\mathfrak{e}^{r' p^{v-k}} \mathfrak{c}(\nu)^{s' p^{n-k}} \mathfrak{c}(\varkappa)^{t'},$$

da $\mathfrak{c}(\nu) = \mathfrak{a}(\nu)^{p^{m-n}}$, $\mathfrak{c}(\varkappa) = \mathfrak{a}(\varkappa)^{p^{m-k}}$ ist. Nach § 7, Lemma, e. ist also

$$[\nu, \varkappa]_1 = \mathfrak{b}\mathfrak{e}^{r' p^{v-k}}, \quad \mathfrak{b} \text{ in } \mathfrak{B}, \quad 0 < r' \leqq p^k$$

ein zu $[\nu, \varkappa]$ assoziierter Kommutator und mithin ist a. eine Folge von § 7., Folgerung 2. aus Satz 1.

Sei jetzt $r' p^{v-k} = u p^w$ mit $(u, p) = 1$, $0 < u \leqq p^{v-w}$, $v - k \leqq w \leqq v$. Dann gibt es eine Zahl u' mit $(u', p) = 1$, $uu' \equiv 1 \bmod p^{v-w}$ [wenn $v = w$ ist, ist die erste dieser Bedingungen keine Folge der zweiten] und durch

$$\varphi_1(\mathfrak{x}) = \mathfrak{x} \text{ für } \mathfrak{x} \text{ aus } \mathfrak{B} \times \{\mathfrak{a}(\nu)\} \times \{\mathfrak{a}(\varkappa)\},$$
$$\varphi_1(\mathfrak{e}) = \mathfrak{e}^{u'}$$

wird ein Automorphismus φ_1 von $\mathfrak{A}$ definiert, der jedes Element

aus $\mathfrak{D}(\mathbf{A})$ invariant läßt und $\mathfrak{Z}(\mathbf{A})$ in sich überführt. Wegen a. und § 7., Satz 1. sind also die Kommutatoren $[\nu, \varkappa]_1$ und $[\nu, \varkappa]_2 = \varphi_1([\nu, \varkappa]_1)$ äquivalent.

Dabei ist

$$[\nu, \varkappa]_2 = \mathfrak{b}\mathfrak{e}^{p^w} \text{ mit } \mathfrak{b} \text{ in } \mathfrak{B},\ v - k \leqq w \leqq v,$$

d.h. $[\nu, \varkappa]_2$ erfüllt die Normierungsbedingung a.

Sei nun

$$\mathfrak{b} = \prod_{i=1}^{d} \mathfrak{b}_i^{p^{z_i}}$$

eine die Invarianten von $\mathfrak{b}$ in $\mathfrak{B}$ in Evidenz setzende Darstellung von $\mathfrak{b}$ als Produkt von in $\mathfrak{B}$ einfachen Elementen, d.h.

$$d = d(\mathfrak{b}),\ n(\mathfrak{b}_i) = n_i(\mathfrak{b}),\ z_i = z_i(\mathfrak{b})$$

mit, falls $\mathfrak{b} \neq 1$ ist [32]),

$$0 < n_1(\mathfrak{b}) < \ldots < n_d(\mathfrak{b})$$
$$0 < n_1(\mathfrak{b}) - z_1 < \ldots < n_d(\mathfrak{b}) - z_d = n(\mathfrak{b}) \leqq k.$$

Wir setzen nun:

$\mathfrak{b}' = \prod_{i=1}^{d}{}' \mathfrak{b}_i^{p^{z_i}}$, wo $\prod'$ alle i mit $w - z_i > \min[0, v - n_i]$ durchläuft,

$\mathfrak{b}'' = \prod_{i=1}^{d}{}'' \mathfrak{b}_i^{p^{z_i}}$, wo $\prod''$ alle i mit $w - z_i \leqq \min[0, v - n_i]$ durchläuft,

so daß $\mathfrak{b} = \mathfrak{b}'\mathfrak{b}''$ ist; sowohl $\mathfrak{b}'$ als auch $\mathfrak{b}''$ kann die Gruppeneins sein.

Für die in $\prod''$ auftretenden i ist $w \leqq z_i$ und also:

$$\mathfrak{b}'' = \left[\prod_{i=1}^{d}{}'' \mathfrak{b}_i^{p^{z_i - w}}\right]^{p^w} = \mathfrak{g}^{p^w};$$

dabei ist

$$n(\mathfrak{g}) = \max_{i \text{ aus } \prod''} [n_i - z_i + w] \leqq v.$$

Da die $\mathfrak{b}_i$ und also auch $\mathfrak{g}$ aus $\mathfrak{B}$ stammen, wird also durch

$$\varphi_2(\mathfrak{x}) = \mathfrak{x} \text{ für } \mathfrak{x} \text{ aus } \mathfrak{B} \times \{\mathfrak{a}(\nu)\} \times \{\mathfrak{a}(\varkappa)\},$$
$$\varphi_2(\mathfrak{e}) = \mathfrak{e}\mathfrak{g}^{-1}$$

ein Automorphismus φ_2 von $\mathfrak{A}$ definiert, der $\mathfrak{D}(\mathbf{A})$ und $\mathfrak{A}/\mathfrak{Z}(\mathbf{A})$ elementweise invariant läßt. Wegen a. und § 7., Satz 1., sind also

---

[32]) Ist $\mathfrak{b} = 1$, so ist $[\nu, \varkappa]_2$ bereits normiert.

die Kommutatoren $[v, x]_2$ und $[v, x]_3 = \varphi_2([v, x]_2)$ äquivalent. Dabei ist

$$[v, x]_3 = e^{p^w} g^{-p^w} b = e^{p^w} b' = e^{p^w} \prod_{i=1}^{d}{}' b_i^{p^{z_i}}$$

und

$$b' = \prod_{i=1}^{d}{}' b_i^{p^{z_i}} = \prod_{i=1}^{d'} b_i'^{p^{z_i}}$$

ist eine die Invarianten

$$d' = d(b'),\ n_i(b') = n(b_i'),\ z_i(b') = z_i'$$

von b' in $\mathfrak{B}$ in Evidenz setzende Darstellung von b' als Produkt von in $\mathfrak{B}$ einfachen Elementen, so daß also $[v, x]_3$ bereits die Normierungsbedingungen a. und b. 1. erfüllt. Ist auch b. 2. erfüllt, so ist $[v, x]_3$ bereits ein normierter Kommutator und Satz 1., b. bewiesen. Ist aber b. 2. nicht erfüllt, so ist $w < v$ und es gibt einen Index j mit $1 \leqq j \leqq d(b')$, so daß

$$n \leqq w - z_j',\ v - n_j(b') \leqq w - z_j'$$

ist, d.h. $w - z_j' \geqq \max [n, v - n_j(b')]$.

Insbesondere ist also $w > z_j'$, $w - z_j' \geqq n$ und

$$b_j^* = b_j' e^{-p^{w-z_j'}}$$

liegt in $\{e^{p^n}\} \times \mathfrak{B} \leqq \mathfrak{Z}(\mathbf{A})$. Weiter ist:

$$n(b_j') = n_j(b') \geqq v - w + z_j' = n\left(e^{-p^{w-z_j'}}\right), \text{ d.h.}$$
$$n(b_j^*) = n(b_j'),$$

und b_j^*, b_j' sind beide in $\mathfrak{B} \times \{e^{p^n}\}$ und auch in $\mathfrak{B} \times \{e\}$ einfache Elemente. Aus dem im Anfang dieses § 8. Bemerkten folgt also: es gibt einen Automorphismus φ_3 von $\mathfrak{A}$, der jedes Element von $\mathfrak{D}(\mathbf{A})$, von $\{e\} \times \{a(v)\} \times \{a(x)\}$ und von $\mathfrak{A}/\mathfrak{Z}(\mathbf{A})$ invariant läßt, so daß

$$\varphi_3(b_i') = \begin{cases} b_i' & \text{für } i \neq j \\ b_j^* & \text{für } i = j \end{cases}$$

wird. Nach a. und § 7., Satz 1. sind also $[v, x]_3$ und $[v, x]_4 = \varphi_3([v, x]_3)$ äquivalente Kommutatoren, und, da

$$[v, x]_4 = e^{p^w} \prod_{i=1}^{d'} b_i'^{p^{z_i'}} \cdot e^{-p^{w-z_j'}} \cdot p^{z_j'} = b'$$

offenbar normiert ist, so ist damit Satz 1., b. vollständig bewiesen.

c. folgt sofort aus § 7., Lemma, b., 3.—5.

Aus der im Beweis durchgeführten Konstruktion eines zu dem gegebenen Kommutator äquivalenten, normierten Kommutator folgt der

ZUSATZ: *Es sei* $[v, x] = \mathfrak{b}\mathfrak{e}^r\,\mathfrak{a}(v)^s\,\mathfrak{a}(x)^t$ *mit* $0 < r \leqq p^v$ *und* $\mathfrak{b}$ *in* $\mathfrak{B}$ *ein realisierbarer Kommutator von* $\mathbf{A}$ *in* $\mathfrak{A}$.

Weiter sei p^w *die größte* r *teilende Potenz von* p, *also* $0 \leqq w \leqq v$, *und*

$$\mathfrak{b} = \prod_{i=1}^{d} \mathfrak{b}_i^{p^{z_i}}$$

eine die Invarianten $d(\mathfrak{b}) = d$, $n_i(\mathfrak{b}) = n(\mathfrak{b}_i)$ *und* $z_i(\mathfrak{b}) = z_i$ *von* $\mathfrak{b}$ *in* $\mathfrak{B}$ *in Evidenz setzende Darstellung von* $\mathfrak{b}$ *als Produkt von in* $\mathfrak{B}$ *einfachen Elementen.*

Sei schließlich $\mathfrak{b}' = \prod_{i=1}^{d}{}' \mathfrak{b}_i^{p^{z_i}}$, *wo* Π' *alle und nur die* i *mit* $w - z_i > min\,[0, v - n_i(\mathfrak{b})]$ *durchläuft, und* $w' = v$, *wenn entweder* $w = v$, *oder es, falls* $w \neq v$ *ist, wenigstens ein* i *gibt, so daß* $w - z_i \geqq max\,[1 + min\,[0, v - n_i(\mathfrak{b})], v - n_i(\mathfrak{b}), n]$, *und* $w' = w$ *in allen andern Fällen.*

Dann ist $[v, x]' = \mathfrak{b}'\mathfrak{e}^{p^{w'}}$ *ein normierter, zu* $[v, x]$ *äquivalenter Kommutator von* $\mathbf{A}$ *in* $\mathfrak{A}$.

SATZ 2.: *Die beiden normierten, realisierbaren Kommutatoren* $[v, x]^{(1)} = \mathfrak{b}^{(1)}\mathfrak{e}^{p^{w_1}}$ *und* $[v, x]^{(2)} = \mathfrak{b}^{(2)}\mathfrak{e}^{p^{w_2}}$ *von* $\mathbf{A}$ *in* $\mathfrak{A}$ *sind dann und nur dann äquivalent, wenn* $w_1 = w_2$ *ist und* $\mathfrak{b}^{(1)}$ *und* $\mathfrak{b}^{(2)}$ *in* $\mathfrak{B}$ *isotyp sind.*

BEWEIS: Das Hinreichen der Bedingungen folgt aus Satz 1., a. und § 7., Satz 1., da sich jeder Automorphismus von $\mathfrak{B}$ zu einem $\{\mathfrak{e}\} \times \{\mathfrak{a}(v)\} \times \{\mathfrak{a}(x)\}$ elementweise invariant lassenden Automorphismus von $\mathfrak{A}$ erweitern läßt.

Die Notwendigkeit der Bedingungen wird in mehreren Schritten gezeigt:

(1) *Zwei normierte, realisierbare Kommutatoren von* $\mathbf{A}$ *in* $\mathfrak{A}$ *sind dann und nur dann assoziiert, wenn sie identisch sind.*

Folgt aus Normierungsbedingung a. und § 7., Lemma, e.

(2) *Ist* $\mathfrak{b}\mathfrak{e}^{p^w}$ *ein normiertes Element,* $w \neq v$, φ *ein* $\mathfrak{D}(\mathbf{A})$ *und* $\mathfrak{Z}(\mathbf{A})$ *je in sich überführender Automorphismus von* $\mathfrak{A}$,

$$\varphi(\mathfrak{b}\mathfrak{e}^{p^w}) = \mathfrak{e}^f\mathfrak{g} \text{ mit } 0 < f \leqq p^v,\ \mathfrak{g} \text{ in } \mathfrak{B} \times \{\mathfrak{a}(v)\} \times \{\mathfrak{a}(x)\},$$

so ist f *genau durch* p^w *teilbar.*

Man beachte, daß $\mathfrak{e}^f\mathfrak{g}$ *nicht* normiert zu sein braucht.

Sei $\mathfrak{b} = \prod_{i=1}^{d} \mathfrak{b}_i^{p^{z_i}}$ eine die Invarianten $d = d(\mathfrak{b})$, $n_i = n_i(\mathfrak{b}) = n(\mathfrak{b}_i)$,

$z_i = z_i(\mathfrak{b})$ von $\mathfrak{b}$ in $\mathfrak{B}$ in Evidenz setzende Darstellung von $\mathfrak{b}$ als Produkt der in $\mathfrak{B}$ einfachen Elemente $\mathfrak{b}_i$.

Es wird:

$$\varphi(\mathfrak{e}) = \mathfrak{e}^r \mathfrak{u}, \quad \varphi(\mathfrak{b}_i) = \mathfrak{e}^{r_i}\mathfrak{u}_i \text{ mit } 0 < r, r_i \leqq p^v$$

und $\mathfrak{u}$, $\mathfrak{u}_i$ in $\mathfrak{B} \times \{\mathfrak{a}(\nu)\} \times \{\mathfrak{a}(\varkappa)\}$.

Da $\mathfrak{Z}(\mathbf{A}) = \varphi[\mathfrak{Z}(\mathbf{A})]$, und da $\mathfrak{e}$ Repräsentant einer erzeugenden Restklasse des Zyklus $\mathfrak{A}/\mathfrak{Z}(\mathbf{A})$ ist, so ist auch $\varphi(\mathfrak{e})$ Repräsentant einer erzeugenden Restklasse von $\mathfrak{A}/\mathfrak{Z}(\mathbf{A})$ und also $(r, p) = 1$.

Wegen $n(\mathfrak{b}_i) = n_i$ ist

$$r_i p^{n_i} \equiv 0 \bmod p^v$$

und, da $\mathfrak{b}_i$ und also auch $\varphi(\mathfrak{b}_i)$ in $\mathfrak{Z}(\mathbf{A})$ liegt, so ist

$$r_i \equiv 0 \bmod p^n.$$

Also wird

$$\mathfrak{e}^f \mathfrak{g} = \varphi(\mathfrak{e}^{p^w}\mathfrak{b}) = \mathfrak{e}^{rp^w + \sum_{i=1}^{d} r_i p^{z_i}} \prod_{i=1}^{d} \mathfrak{u}_i^{p^{z_i}} \mathfrak{u}^{p^w}$$

und mithin

$$f \equiv r p^w + \sum_{i=1}^{d} r_i p^{z_i} \bmod p^v.$$

Um (2) zu zeigen, genügt es also zu zeigen:

$$(+) \qquad r_i p^{z_i} \equiv 0 \bmod p^{w+1} \textit{ für alle } i.$$

Nun ist stets:

$$r_i p^{z_i} \equiv 0 \bmod p^{n+z_i}.$$

$(+)$ ist also für alle i bewiesen, für die $n + z_i > w$ ist.

Sei also $n + z_i \leqq w$; wegen $w \neq v$ und Normierungsbedingung b., 2. ist also:

$$w - z_i < v - n_i.$$

Wegen Normierungsbedingung b., 1. ist also:

$$v > n_i$$

und mithin

$$r_i p^{z_i} \equiv 0 \bmod p^{v-n_i+z_i};$$

hieraus folgt $(+)$ und also (2) wegen $w < v - n_i + z_i$.

(3) *Ist* $\mathfrak{b}\mathfrak{e}^{p^w}$ *normiert, sind* $d(\mathfrak{b})$, $n_i(\mathfrak{b})$, $z_i(\mathfrak{b})$ *die Invarianten von* $\mathfrak{b}$ *in* $\mathfrak{B}$, *so tritt das Paar* v, w *nicht in der Reihe der Paare* $n_i(\mathfrak{b})$, $z_i(\mathfrak{b})$ *auf.*

Wäre nämlich etwa $n_j(\mathfrak{b}) = v$, $z_j(\mathfrak{b}) = w$, so wäre

$$0 < n_j(\mathfrak{b}) - z_j(\mathfrak{b}) = v - w \text{ oder } v - n_j = w - z_j,$$

also $v > n_j$ wegen der Normierungsbedingung b., 1.; Widerspruch.

(4) *Es sei* $\mathfrak{b}\mathfrak{e}^{p^w}$ *normiert,* $d(\mathfrak{b})$, $n_i(\mathfrak{b})$, $z_i(\mathfrak{b})$ *die Invarianten*[33]) *von* $\mathfrak{b}$ *in* $\mathfrak{B}$ *und* $d(\mathfrak{e}^{p^w}\mathfrak{b})$, $n_i(\mathfrak{b}\mathfrak{e}^{p^w})$, $z_i(\mathfrak{b}\mathfrak{e}^{p^w})$ *die Invarianten*[33]) *von* $\mathfrak{b}\mathfrak{e}^{p^w}$ *in* $\mathfrak{B}\times\{\mathfrak{e}\}$.

a. *Jedes der Paare:* $n_i(\mathfrak{b})$, $z_i(\mathfrak{b})$ *ist gleich einem eindeutig bestimmten der Paare:*

$$n_j(\mathfrak{b}\mathfrak{e}^{p^w}),\ z_j(\mathfrak{b}\mathfrak{e}^{p^w}).$$

b. $d(\mathfrak{b}) \leqq d(\mathfrak{b}\mathfrak{e}^{p^w}) \leqq d(\mathfrak{b}) + 1$.

c. *Dann und nur dann ist*

$$d(\mathfrak{b}\mathfrak{e}^{p^w}) = d(\mathfrak{b}) + 1,$$

wenn $w < v$ *und* $0 < [n_i(\mathfrak{b}) - v][n_i(\mathfrak{b}) - z_i(\mathfrak{b}) + w - v]$ *ist.*

d. *Ist* $d(\mathfrak{b}\mathfrak{e}^{p^w}) = d(\mathfrak{b}) + 1$, *so besteht die Reihe der Paare* $n_i(\mathfrak{b}\mathfrak{e}^{p^w})$, $z_i(\mathfrak{b}\mathfrak{e}^{p^w})$ *aus der Reihe der Paare* $n_i(\mathfrak{b})$, $z_i(\mathfrak{b})$ *und dem Paar* v, w.

Da $\mathfrak{e}$ ein in $\{\mathfrak{e}\}\times\mathfrak{B}$ und in $\mathfrak{A}$ einfaches Element ist, und da die in $\mathfrak{B}$ einfachen Elemente auch in $\{\mathfrak{e}\}\times\mathfrak{B}$ und $\mathfrak{A}$ einfach sind, so setzt $\mathfrak{e}^{p^w}\prod_{i=1}^{d(\mathfrak{b})}\mathfrak{b}_i^{p^{z_i}}$ die Invarianten von $\mathfrak{b}\mathfrak{e}^{p^w}$ in $\mathfrak{B}\times\{\mathfrak{e}\}$ in Evidenz, wenn nur $\mathfrak{b} = \prod_{i=1}^{d(\mathfrak{b})}\mathfrak{b}^{p^{z_i}}$ die Invarianten von $\mathfrak{b}$ in Evidenz setzt, und wenn die in c. angegebenen Bedingungen erfüllt sind, womit das Hinreichen dieser Bedingungen und auch d. erwiesen ist.

Seien jetzt die ad c. angegebenen Bedingungen nicht erfüllt; ist zunächst $v = w$, so ist $\mathfrak{b} = \mathfrak{b}\mathfrak{e}^{p^w}$ und in diesem Falle ist a. evident, $d(\mathfrak{b}) = d(\mathfrak{b}\mathfrak{e}^{p^w})$, also auch b. evident, und die Notwendigkeit von $v \neq w$ ad c. gezeigt.

Sei also $v > w$. Dann gibt es ein j mit

$$(**) \qquad 0 \geqq [n_j(\mathfrak{b}) - v][n_j(\mathfrak{b}) - z_j(\mathfrak{b}) + w - v].$$

Wäre nun $w < z_j(\mathfrak{b})$, so wäre nach Normierungsbedingungen b., 1. auch

$$0 > w - z_j(\mathfrak{b}) > v - n_j(\mathfrak{b}),$$

was unmöglich ist. Also ist $w \geqq z_j(\mathfrak{b})$ und wir setzen:

$$\mathfrak{b}_j^* = \mathfrak{b}_j\mathfrak{e}^{p^{w-z_j(\mathfrak{b})}}.$$

---

[33]) Man beachte, daß $\mathfrak{b}$ in $\mathfrak{B}$, $\mathfrak{B}\times\{\mathfrak{e}\}$ und $\mathfrak{A}$, $\mathfrak{b}\mathfrak{e}^{p^w}$ in $\mathfrak{B}\times\{\mathfrak{e}\}$ und $\mathfrak{A}$ dieselben Invarianten hat.

Wäre $n_j(\mathfrak{b}) < v - w + z_j(\mathfrak{b})$, so wäre nach Normierungsbedingung b. 1. auch $v - n_j(\mathfrak{b}) > 0$ und also $n_j(\mathfrak{b}) - z_j(\mathfrak{b}) + w - v \geqq 0$, was wegen $(**)$ unmöglich ist. Also ist $n_j(\mathfrak{b}) \geqq v - w + z_j(\mathfrak{b})$ und mithin:

$$n(\mathfrak{b}_j^*) = n(\mathfrak{b}_j)^* = n_j(\mathfrak{b}).$$

Schließlich ist $\mathfrak{b}_j^*$ mit $\mathfrak{b}_j$ und $\mathfrak{e}$ ein in $\mathfrak{B} \times \{\mathfrak{e}\}$ einfaches Element, und also setzt

$$\mathfrak{b}\mathfrak{e}^{p^w} = \prod_{\substack{i=1 \\ i \neq j}}^{d(\mathfrak{b})} \mathfrak{b}_i^{p^{z_i(\mathfrak{b})}} \cdot \mathfrak{b}_j^{*\,p^{z_j(\mathfrak{b})}}$$

in Evidenz, daß $\mathfrak{b}$ und $\mathfrak{b}\mathfrak{e}^{p^w}$ in $\mathfrak{B} \times \{\mathfrak{e}\}$ dieselben Invarianten haben, womit der Beweis von (4) vollendet ist.

(5) *Sind* $\mathfrak{b}^{(1)}\mathfrak{e}^{p^{w_1}}$ *und* $\mathfrak{b}^{(2)}\mathfrak{e}^{p^{w_2}}$ *zwei normierte Elemente, so gibt es dann und nur dann einen Automorphismus* φ *von* $\mathfrak{A}$, *der*

$$\varphi[\mathfrak{D}(\mathbf{A})] = \mathfrak{D}(\mathbf{A}),\ \varphi[\mathfrak{Z}(\mathbf{A})] = \mathfrak{Z}(\mathbf{A}),\ \varphi[\mathfrak{b}^{(1)}\mathfrak{e}^{p^{w_1}}] = \mathfrak{b}^{(2)}\mathfrak{e}^{p^{w_2}}$$

erfüllt, wenn

$$w_1 = w_2 \text{ ist und } \mathfrak{b}^{(1)} \text{ und } \mathfrak{b}^{(2)} \text{ in } \mathfrak{B} \text{ isotyp sind.}$$

Daß die Bedingungen hinreichen, ist klar. Existiere also ein derartiger Automorphismus φ.

Ist zunächst eine der Zahlen w_i, etwa $w_1 < v$, so folgt aus (2), daß $w_1 = w_2$ und also auch $w_2 < v$ ist. Also ist dann und nur dann $w_1 \neq v$, wenn $w_2 \neq v$ ist, und mithin ist stets:

$$w_1 = w_2 = w.$$

Weiter sind $\mathfrak{e}^{p^w}\mathfrak{b}^{(1)}$ und $\mathfrak{e}^{p^w}\mathfrak{b}^{(2)}$ in $\mathfrak{A}$ isotyp, haben also dieselben Invarianten in $\mathfrak{A}$; nach (3) und (4) haben also auch $\mathfrak{b}^{(1)}$ und $\mathfrak{b}^{(2)}$ dieselben Invarianten in $\mathfrak{B}$, sind also isotyp in $\mathfrak{B}$, womit (5) bewiesen ist.

Aus (1) und (5) folgt sofort die Notwendigkeit der im Satz 2. angegebenen Bedingungen.

FOLGERUNG: *Es sei* $\mathfrak{A} = \mathfrak{B}^{(i)} \times \{\mathfrak{e}_i\} \times \{\mathfrak{a}_i(\nu)\} \times \{\mathfrak{a}_i(\varkappa)\}$ *für* $i = 1, 2$ *eine Zerlegung* i *von* $\mathfrak{A}$ *vom Typus* $(*)$, $[\nu, \varkappa]$ *ein realisierbarer Kommutator von* $\mathbf{A}$ *in* $\mathfrak{A}$, $[\nu, \varkappa]_i = \mathfrak{b}^{(i)}\mathfrak{e}^{p^{w_i}}$ *ein dazu äquivalenter, bzgl. der Zerlegung* i *normierter Kommutator,* $d(\mathfrak{b}^{(i)})$, $n_j(\mathfrak{b}^{(i)})$, $z_j(\mathfrak{b}^{(i)})$ *für* $1 \leqq j \leqq d(\mathfrak{b}^{(i)})$ *die Invarianten von* $\mathfrak{b}^{(i)}$ *in* $\mathfrak{B}^{(i)}$.
Dann ist

$$w_1 = w_2,\ d(\mathfrak{b}^{(1)}) = d(\mathfrak{b}^{(2)}),\ n_j(\mathfrak{b}^{(1)}) = n_j(\mathfrak{b}^{(2)}),\ z_j(\mathfrak{b}^{(1)}) = z_j(\mathfrak{b}^{(2)}).$$

BEWEIS: Wegen § 4., Satz 2. gibt es einen Automorphismus

φ von $\mathfrak{A}$, der

$$\varphi[\mathfrak{D}(\mathbf{A})] = \mathfrak{D}(\mathbf{A}),\ \varphi[\mathfrak{Z}(\mathbf{A})] = \mathfrak{Z}(\mathbf{A}),$$

$\varphi(e_1) = e_2$, $\varphi[\mathfrak{a}_1(\nu)]] = \mathfrak{a}_2(\nu)$, $\varphi[\mathfrak{a}_1(\varkappa)] = \mathfrak{a}_2(\varkappa)$, $\varphi(\mathfrak{B}^{(1)}) = \mathfrak{B}^{(2)}$ erfüllt. Also ist [wegen § 7., Satz 2.]

$$[\nu, \varkappa]_3 = e_2^{p^{w_1}} \varphi(\mathfrak{b}^{(1)})$$

ein zu $[\nu, \varkappa]$ äquivalenter Kommutator, und da $e_1^{p^{w_1}} \mathfrak{b}^{(1)}$ bzgl. der Zerlegung 1 normiert ist, so ist $e_2^{p^{w_1}} \varphi(\mathfrak{b}^{(1)})$ bzgl. der Zerlegung 2 normiert. Da $e_2^{p^{w_1}} \varphi(\mathfrak{b}^{(1)})$ und $e_2^{p^{w_2}} \mathfrak{b}^{(2)}$ also bzgl. der Zerlegung 2 normierte, äquivalente Kommutatoren von $\mathbf{A}$ in $\mathfrak{A}$ sind, so folgt aus Satz 2., daß $w_1 = w_2$ ist, und daß $\varphi(\mathfrak{b}^{(1)})$ und $\mathfrak{b}^{(2)}$ in $\mathfrak{B}^{(2)}$ isotyp sind, also in $\mathfrak{B}^{(2)}$ dieselben Invarianten haben, woraus unsere Behauptung folgt, da $\mathfrak{b}^{(1)}$ dieselben Invarianten in $\mathfrak{B}^{(1)}$ hat wie $\varphi(\mathfrak{b}^{(1)})$ in $\mathfrak{B}^{(2)}$.

Diese Folgerung besagt also, daß die aus dem normierten Kommutator $[\nu, \varkappa]$ abgelesenen Zahlen: w, d, n_i, z_i unabhängig von der speziellen Darstellung (*) sind; da sich weiter jeder Automorphismus von $\mathfrak{D}(\mathbf{A})$ zu einem $\mathfrak{B} \times \{\mathfrak{e}\}$ elementweise invariant lassenden Automorphismus von $\mathfrak{A}$ erweitern läßt, so folgt aus Satz 2., Satz 1., a. und § 7., Satz 1 bzw. § 7., Folgerung 1. aus Satz 1., daß sie unabhängig von der Auswahl der Basis ν, $\varkappa$ von $\mathbf{A}$ sind, und wir haben:

die Zahlen w, d, n_i, z_i sind *Invarianten* der [den Kommutator $[\nu, \varkappa]$ realisierenden] $\mathfrak{A}$ zum Kern habenden, im Kern genau die Automorphismengruppe $\mathbf{A}$ induzierenden, vollkommenen Gruppe.

Aus Satz 1., a. und Satz 2. folgt dann:

Die vollkommenen Primärgruppen, deren Faktorgruppe nach dem Kern direktes Produkt zweier Zyklen ist, und bei denen die im § 4. *definierte Invariante* $u(\mathbf{A})$ *der im Kern induzierten Automorphismengruppe* $\mathbf{A}$ *insbesondere* $= 1$ *ist, sind durch die folgenden Invarianten* [*bis auf Isomorphismen*] *eindeutig bestimmt*:

1. *die Struktur des Kerns*;
2. *die Struktur der im Kern induzierten Automorphismengruppe* [*als Automorphismengruppe*];
3. *die Zahlen* w, d, n_i, z_i *für* $1 \leqq i \leqq d$.

Dabei sind diese Invarianten dann und nur dann in der angegebenen Weise realisierbar, wenn sie den folgenden Bedingungen genügen:

I. der Kern ist eine abelsche Primärgruppe der endlichen

Maximalordnung p^m und die im Kern induzierte Automorphismengruppe ist vollkommen [nach § 6, Satz.].

Wegen § 4., Satz 2. und Zusatz dazu können wir also die Invariante 2. durch die folgende ersetzen

2*. $n, k, v,$

und es muß gelten

I*. $0 < k \leqq n \leqq v \leqq m$ und $n < m$, falls $p = 2$ ist [nach § 4., Zusatz 2. zu Satz 1. und § 6., Satz.].

II. der Kern ist direktes Produkt einer abelschen Gruppe vom Typus [34]) $(p^{n_1}, \ldots, p^{n_d}, p^v, p^m, p^m)$ mit einer abelschen Gruppe, die direkter Faktor der ganzen Gruppe ist [nach § 4., Zusatz 2. und 3. zu Satz 1., und dem im Anfang des § 8. über einfache Elemente Bemerkten].

III. $v - k \leqq w \leqq v$

und $1 \leqq w$, falls $p = 3, v = k = n = m$

oder $p = 2, v = k = n$ ist [nach Satz 1., c.].

IV. $0 < n_1 - z_1 < \ldots < n_d - z_d \leqq k, \quad 0 < n_1 < \ldots < n_d \leqq m$ [nach Satz 1., c. und dem über Isotypie-Invarianten Gesagten].

V. $w - z_i > \min [0, v - n_i]$ für jedes i [nach Normierungsbedingung b., 1.].

VI. Ist $w \neq v$, so ist $w - z_i < v - n_i$ für jedes i für das $n \leqq w - z_i$ ist [nach Normierungsbedingung b., 2.].

Über den allgemeinen Fall vollkommener Primärgruppen, deren Faktorgruppe nach dem Kern direktes Produkt zweier Zyklen ist, sei nur bemerkt, daß das Problem ihrer Klassifikation, wie auch aus den obigen Überlegungen zu entnehmen ist, wesentlich auf die Lösung des folgenden Problems herauskommt: in einer abelschen Primärgruppe $\mathfrak{A}$, deren Elemente beschränkte Ordnungen haben, sei eine Untergruppe $\mathfrak{Z}$ derart ausgezeichnet, daß $\mathfrak{A}/\mathfrak{Z}$ zyklisch ist; welches sind die notwendigen und hinreichenden Bedingungen dafür, daß es einen $\mathfrak{Z}$ in sich überführenden Automorphismus von $\mathfrak{A}$ gibt, der ein gegebenes Element in ein anderes gegebenes Element von $\mathfrak{A}$ überführt?

§ 9.

Die unvollkommenen Gruppen mit $p = 3$.

In diesem §, in dem wir nur zur Primzahl 3 gehörige Primärgruppen $\mathfrak{G}$ mit wesentlichem Kern und abelscher Faktorgruppe nach dem Kern betrachten wollen, wollen wir zeigen:

[34]) d.h. ist direktes Produkt von Zyklen von in der Klammer angegebener Ordnung.

Zu jedem $m \geqq 1$ gibt es eine unvollkommene Gruppe $\mathfrak{D}_{3,m}$ derart, daß eine Gruppe $\mathfrak{G}$, für die 3^m die Maximalordnung der Elemente von $\mathfrak{R}(\mathfrak{G})$ ist, und für die, falls $m = 1$ ist, $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ direktes Produkt zweier Zyklen ist, dann und nur dann unvollkommen ist, wenn sie dem direkten Produkt von $\mathfrak{D}_{3,m}$ mit beliebig vielen Zyklen von 3^m nicht überschreitender Ordnung isomorph ist. — $\mathfrak{D}_{3,m}$ ist also durch die Eigenschaft charakterisiert, die kleinste unvollkommene Gruppe zu sein, für die 3^m die Maximalordnung der Kernelemente ist.

Da Gruppen mit zyklischer Faktorgruppe nach dem Kern vollkommen sind, wollen wir im folgenden stets annehmen, daß die Faktorgruppe nach dem Kern nicht zyklisch ist.

Es sind zwei wesentlich verschiedene Fälle zu unterscheiden, je nachdem $m > 1$ oder $m = 1$ ist.

$$m > 1.$$

(1) *Ist $\mathfrak{G}$ unvollkommen, so ist $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ direktes Produkt zweier Zyklen der Ordnung 3^m.*

Zum Beweise betrachten wir die Gesamtheit $\mathfrak{V}(\mathfrak{G})$ der Elemente aus $\mathfrak{G}$, deren Ordnung mod $\mathfrak{R}(\mathfrak{G})$ nicht größer als 3^{m-1} ist. Da $m - 1 > 0$ ist, so ist $\mathfrak{V}(\mathfrak{G}) > \mathfrak{R}(\mathfrak{G})$; da $\mathfrak{V}(\mathfrak{G})/\mathfrak{R}(\mathfrak{G})$ eine charakteristische Untergruppe von $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ ist, so ist $\mathfrak{V}(\mathfrak{G})$ eine charakteristische Untergruppe und also ein Normalteiler von $\mathfrak{G}$. Da $\mathfrak{R}(\mathfrak{G})$ wesentlicher Kern von $\mathfrak{G}$ und $\mathfrak{V}(\mathfrak{G}) > \mathfrak{R}(\mathfrak{G})$ ist, so ist $\mathfrak{R}[\mathfrak{V}(\mathfrak{G})] = \mathfrak{R}(\mathfrak{G})$ nach § 2, (1) und $\mathfrak{R}(\mathfrak{G})$ wesentlicher Kern von $\mathfrak{V}(\mathfrak{G})$. Aus § 2, (2) und § 3, Satz 2., b. folgt, da die Ordnungen in $\mathfrak{V}(\mathfrak{G})/\mathfrak{R}(\mathfrak{G})$ sämtlich $\leqq 3^{m-1}$ sind, daß

(1; 1) *$\mathfrak{V}(\mathfrak{G})$ vollkommen ist.*

Wir zeigen weiter:

(1; 2) *Ist $\mathfrak{S}$ ein mod $\mathfrak{R}(\mathfrak{G})$ unabhängiges System aus $\mathfrak{G}$, so ist das System aller $\mathfrak{c}(\mathfrak{s}) = \mathfrak{s}^{3^m}$ mit $\mathfrak{s}$ aus $\mathfrak{S}$ ein unabhängiges System in $\mathfrak{R}(\mathfrak{G})$.*

Wir setzen:

$$\varepsilon(\mathfrak{s}) = \begin{Bmatrix} 1 \\ 3 \end{Bmatrix} \text{ wenn } n(\mathfrak{s}) \begin{Bmatrix} < \\ = \end{Bmatrix} m,$$

wo $3^{n(\mathfrak{s})}$ die Ordnung von $\mathfrak{s}$ mod $\mathfrak{R}(\mathfrak{G})$ ist, und bilden die Gesamtheit $\mathfrak{V}(\mathfrak{S})$ aller Elemente $\mathfrak{s}^{\varepsilon(\mathfrak{s})}$ mit $\mathfrak{s}$ aus $\mathfrak{S}$. Da $m > 1$ ist, so ist $\mathfrak{V}(\mathfrak{S})$ mod $\mathfrak{R}(\mathfrak{G})$ unabhängig, und, da $\mathfrak{V}(\mathfrak{S}) \leqq \mathfrak{V}(\mathfrak{G})$ ist, so folgt aus (1; 1) und § 3., Lemma 1., daß die Gesamtheit der $\mathfrak{c}(\mathfrak{s}^{\varepsilon(\mathfrak{s})}) = \mathfrak{c}(\mathfrak{s})^{\varepsilon(\mathfrak{s})}$ mit $\mathfrak{s}$ aus $\mathfrak{S}$ ein unabhängiges System aus $\mathfrak{R}(\mathfrak{G})$ ist, woraus (1; 2) folgt.

Wäre nun zunächst $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ direktes Produkt von wenigstens drei Zyklen, so gibt es zu jedem Paar mod $\mathfrak{R}(\mathfrak{G})$ unabhängiger Elemente $\mathfrak{u}$, $\mathfrak{v}$ ein Element $\mathfrak{w}$, so daß $\mathfrak{u}$, $\mathfrak{v}$, $\mathfrak{w}$ mod $\mathfrak{R}(\mathfrak{G})$ unabhängig sind. Wegen (1; 2) und § 3., Lemma 2., b. und Fußnote [10]) dazu wird dann: [35])

$$h([\mathfrak{u}, \mathfrak{v}], \mathfrak{w}) \equiv 0 \bmod 3.$$

Da weiter $\mathfrak{c}(\mathfrak{g})$ in $\mathfrak{Z}(\mathfrak{G})$ nach § 2., (5), b. ist, so wird:

$$\begin{aligned}(\mathfrak{u}\mathfrak{w})^{-1}[\mathfrak{u}, \mathfrak{v}](\mathfrak{u}\mathfrak{w}) &= [\mathfrak{u}, \mathfrak{v}]\mathfrak{c}(\mathfrak{u})^{h([\mathfrak{u}, \mathfrak{v}], \mathfrak{u})}\, \mathfrak{c}(\mathfrak{w})^{h([\mathfrak{u}, \mathfrak{v}], \mathfrak{w})} \\ &= [\mathfrak{u}, \mathfrak{v}]\, \mathfrak{c}(\mathfrak{u}\mathfrak{w})^{h([\mathfrak{u}, \mathfrak{v}], \mathfrak{u}\mathfrak{w})} = \\ &= [\mathfrak{u}, \mathfrak{v}]\mathfrak{c}(\mathfrak{u})^{h([\mathfrak{u}, \mathfrak{v}], \mathfrak{u}\mathfrak{w})[1+3^{m-1}h([\mathfrak{w}, \mathfrak{u}], \mathfrak{u})]} \cdot \\ &\qquad \cdot \mathfrak{c}(\mathfrak{w})^{h([\mathfrak{u}, \mathfrak{v}], \mathfrak{u}\mathfrak{w})[1+3^{m-1}h([\mathfrak{u}, \mathfrak{w}], \mathfrak{w})]}\end{aligned}$$

nach § 2., (7).

Da $1 + 3^{m-1}x$ wegen $m > 1$ zu 3 teilerfremd ist, so folgt aus (1; 2), daß $h([\mathfrak{u}, \mathfrak{v}], \mathfrak{u}\mathfrak{w}) \equiv 0 \bmod 3$ ist, und hieraus folgt analog, daß $h([\mathfrak{u}, \mathfrak{v}], \mathfrak{u}) \equiv 0 \bmod 3$ ist. Aus Symmetriegründen ist also auch $h([\mathfrak{u}, \mathfrak{v}], \mathfrak{v}) \equiv 0 \bmod 3$. Mithin ist $[\mathfrak{u}, \mathfrak{v}]^{3^{m-1}}$ in $\mathfrak{Z}(\mathfrak{G})$ enthalten und wegen § 3., Satz 2., b. wäre also $\mathfrak{G}$ vollkommen.

Da $\mathfrak{G}$ unvollkommen ist, ist mithin $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ direktes Produkt zweier Zyklen. Hätten diese beiden Zyklen je eine von 3^m verschiedene [also kleinere] Ordnung, so wäre $\mathfrak{G} = \mathfrak{B}(\mathfrak{G})$ und wegen (1; 1) wäre $\mathfrak{G}$ vollkommen.

Wäre schließlich $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ direktes Produkt eines Zyklus der Ordnung 3^m mit einem niederer Ordnung, so sei etwa $\mathfrak{u}$, $\mathfrak{v}$ eine Basis mod $\mathfrak{R}(\mathfrak{G})$ mit $m = n(\mathfrak{u}) > n(\mathfrak{v})$. Nach § 2., (5), a. wird dann $[\mathfrak{v}, \mathfrak{u}]^{3^{n(\mathfrak{v})}} = \mathfrak{c}(\mathfrak{u})^{h(\mathfrak{a}(\mathfrak{v}), \mathfrak{u})}$. Da $m - 1 \geqq n(\mathfrak{v})$ ist, und da $\mathfrak{c}(\mathfrak{u})$ nach § 2., (5), b. in $\mathfrak{Z}(\mathfrak{G})$ enthalten ist, so liegt $[\mathfrak{v}, \mathfrak{u}]^{3^{m-1}}$ in $\mathfrak{Z}(\mathfrak{G})$ und wegen § 2., (6), a. und § 3., Satz 2., b. wäre also $\mathfrak{G}$ vollkommen, womit (1) bewiesen ist.

(2) *Ist $\mathfrak{G}$ unvollkommen, so gibt es eine Basis $\mathfrak{u}$, $\mathfrak{v}$ mod $\mathfrak{R}(\mathfrak{G})$ und eine Untergruppe $\mathfrak{B}$ von $\mathfrak{R}(\mathfrak{G})$, so daß*

1. $\mathfrak{u}^{-1}[\mathfrak{u}, \mathfrak{v}]\mathfrak{u} = [\mathfrak{u}, \mathfrak{v}]\mathfrak{c}(\mathfrak{u})$
   $\mathfrak{v}^{-1}[\mathfrak{u}, \mathfrak{v}]\mathfrak{v} = [\mathfrak{u}, \mathfrak{v}]\mathfrak{c}(\mathfrak{v})$,

---

[35]) Für $\mathfrak{k}$ aus $\mathfrak{R}(\mathfrak{G})$ bestimmt sich $h(\mathfrak{k}, \mathfrak{g})$ aus $0 \leqq h(\mathfrak{k}, \mathfrak{g}) < 3^{n(\mathfrak{g})}$ und $\mathfrak{g}^{-1}\mathfrak{k}\mathfrak{g} = \mathfrak{k}\mathfrak{c}(\mathfrak{g})^{h(\mathfrak{k}, \mathfrak{g})}$.

2. $\mathfrak{G} = \{\mathfrak{u}, \mathfrak{v}\} \times \mathfrak{B}$
$\mathfrak{R}(\mathfrak{G}) = \{\mathfrak{a}(\mathfrak{u})\} \times \{\mathfrak{a}(\mathfrak{v})\} \times \{[\mathfrak{u}, \mathfrak{v}]\} \times \mathfrak{B}$
$\mathfrak{Z}(\mathfrak{G}) = \{\mathfrak{a}(\mathfrak{u})\} \times \{\mathfrak{a}(\mathfrak{v})\} \times \mathfrak{B}$
$\mathfrak{D}(\mathfrak{G}) = \{\mathfrak{a}(\mathfrak{u})\} \times \{\mathfrak{a}(\mathfrak{v})\},$

wobei $\mathfrak{a}(\mathfrak{u}) = \mathfrak{c}(\mathfrak{u})$, $\mathfrak{a}(\mathfrak{v}) = \mathfrak{c}(\mathfrak{v})$, $m = n(\mathfrak{u}) = n(\mathfrak{v})$ *ist.*

Wegen (1) gibt es eine zweigliedrige Basis $\mathfrak{r}, \mathfrak{s}$ von $\mathfrak{G}$ mod $\mathfrak{R}(\mathfrak{G})$ und es ist $m = n(\mathfrak{r}) = n(\mathfrak{s})$. Wäre nun etwa $h([\mathfrak{r}, \mathfrak{s}], \mathfrak{r}) \equiv 0 \bmod 3$, so folgerte man wegen $m > 1$ und (1; 2), daß auch $h([\mathfrak{r}, \mathfrak{s}], \mathfrak{s}) \equiv 0 \bmod 3$ ist, und hieraus folgt wieder, daß $\mathfrak{G}$ vollkommen ist.

Mithin sind die Zahlen $h([\mathfrak{r}, \mathfrak{s}], \mathfrak{r}) = r$ und $h([\mathfrak{r}, \mathfrak{s}], \mathfrak{s}) = s$ zu 3 teilerfremde Zahlen. Dann können wir eine Zahl z so bestimmen, dass $r \cdot z \equiv 1 \bmod 3^m$ ist. Da dann z ebenfalls zu 3 teilerfremd ist, so ist auch $\mathfrak{r}^z, \mathfrak{s}$ eine Basis mod $\mathfrak{R}(\mathfrak{G})$ und es wird wegen § 2., (6), a. und § 2., (5), b.:

$$h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{r}^z) \equiv rz \equiv 1 \bmod 3^m$$
$$h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{s}) \equiv sz \bmod 3^m.$$

Nach § 2., (7) wird wie üblich (z.B. S. [58] 58)

$$h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{r}^z) \equiv h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{r}^z\mathfrak{s})\,(1 + 3^{m-1}h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{r}^z)) \bmod 3^m,$$

also $$1 \equiv h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{r}^z\mathfrak{s})\,(1 + 3^{m-1}) \bmod 3^m$$

und wegen $m > 1$ also

$$h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{r}^z\mathfrak{s}) \equiv 1 - 3^{m-1} \bmod 3^m.$$

Mithin wird

$$\begin{aligned} h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{s}) &\equiv h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{r}^z\mathfrak{s})\,(1 + 3^{m-1}h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{s})) \bmod 3^m \\ &\equiv (1 - 3^{m-1})(1 + 3^{m-1}h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{s})) \bmod 3^m \\ &\equiv 1 + (h([\mathfrak{r}^z, \mathfrak{s}], \mathfrak{s}) - 1)3^{m-1} \bmod 3^m \quad \text{und also} \\ &\equiv 1 \bmod 3^m. \end{aligned}$$

Setzen wir jetzt $\mathfrak{u} = \mathfrak{r}^z$, $\mathfrak{v} = \mathfrak{s}$, so wird

$$h([\mathfrak{u}, \mathfrak{v}], \mathfrak{u}) \equiv h([\mathfrak{u}, \mathfrak{v}], \mathfrak{v}) \equiv 1 \bmod 3^m$$

und für $\mathfrak{k}$ aus $\mathfrak{R}(\mathfrak{G})$ also wie oben

$$h(\mathfrak{k}, \mathfrak{u}) \equiv h(\mathfrak{k}, \mathfrak{u}\mathfrak{v})(1 + 3^{m-1}) \bmod 3^m,$$
$$h(\mathfrak{k}, \mathfrak{v}) \equiv h(\mathfrak{k}, \mathfrak{u}\mathfrak{v})(1 + 3^{m-1}) \bmod 3^m,$$

d.h. dann und nur dann ist $h(\mathfrak{k}, \mathfrak{u}) \equiv 0 \bmod 3^m$, wenn $h(\mathfrak{k}, \mathfrak{v}) \equiv 0 \bmod 3^m$ ist, d.h. $\mathfrak{Z}(\mathfrak{G})$ besteht genau aus den mit $\mathfrak{u}$[oder $\mathfrak{v}$] vertauschbaren Elementen, woraus (2) folgt.

(3) *Es gibt eine Erweiterung* $\mathfrak{D}_{3,m}$ *des direkten Produkts* $\mathfrak{A}_{3,m} = \{\mathfrak{m}\} \times \{\mathfrak{n}\} \times \{\mathfrak{e}\}$ *dreier Zyklen der Ordnung* 3^m *mit zwei Elementen* $\mathfrak{u}$, $\mathfrak{v}$, *so daß*

$$\mathfrak{u}^{3^m} = \mathfrak{m},\ \mathfrak{v}^{3^m} = \mathfrak{n},$$
$$[\mathfrak{u}, \mathfrak{v}] = \mathfrak{e},$$
$$\mathfrak{u}^{-1}\mathfrak{m}\,\mathfrak{u} = \mathfrak{m},\ \mathfrak{u}^{-1}\mathfrak{n}\,\mathfrak{u} = \mathfrak{n},\ \mathfrak{u}^{-1}\mathfrak{e}\,\mathfrak{u} = \mathfrak{e}\,\mathfrak{m},$$
$$\mathfrak{v}^{-1}\mathfrak{m}\mathfrak{v} = \mathfrak{m},\ \mathfrak{v}^{-1}\mathfrak{n}\mathfrak{v} = \mathfrak{n},\ \mathfrak{v}^{-1}\mathfrak{e}\,\mathfrak{v} = \mathfrak{e}\,\mathfrak{n}$$

ist.

Zunächst nämlich induzieren $\mathfrak{u}$, $\mathfrak{v}$ in $\mathfrak{A}_{3,m}$ je Automorphismen der Ordnung 3^m. — Weiter ist

$$\prod_{i=1}^{3^m} \mathfrak{u}^{i-1}[\mathfrak{u}, \mathfrak{v}]\mathfrak{u}^{1-i} = \prod_{i=1}^{3^m} \mathfrak{e}\,\mathfrak{m}^{1-i} = \mathfrak{e}^{3^m}\mathfrak{m}^{3^m - \frac{3^m(3^m-1)}{2}} = \mathfrak{1} =$$
$$= \mathfrak{u}^{3^m}\mathfrak{v}\,\mathfrak{u}^{-3^m}\mathfrak{v}^{-1}$$

und entsprechend:

$$\prod_{i=1}^{3^m} \mathfrak{v}^{i-1}[\mathfrak{v}, \mathfrak{u}]\mathfrak{v}^{1-i} = \mathfrak{v}^{3^m}\mathfrak{u}\,\mathfrak{v}^{-3^m}\mathfrak{u}^{-1}.$$

Wegen E., § 5., Zusatz, S. 407 folgt hieraus sofort (3).

(4) $\mathfrak{D}_{3,m}$ *ist unvollkommen, und es ist:*

$$\mathfrak{A}_{3,m} = \mathfrak{R}(\mathfrak{D}_{3,m}) = \mathfrak{C}(\mathfrak{D}_{3,m}),$$
$$\{\mathfrak{m}\} \times \{\mathfrak{n}\} = \mathfrak{Z}(\mathfrak{D}_{3,m}) = \mathfrak{D}(\mathfrak{D}_{3,m}).$$

Zunächst ist wegen § 2., (6) a. und § 2., (7), die wegen § 2., (2) anwendbar sind

$$(\mathfrak{u}^i\mathfrak{v}^k)^{3^m} = \mathfrak{m}^{i[1+ik3^{m-1}]}\mathfrak{n}^{k[1+ik3^{m-1}]}$$

und also

$$(\mathfrak{u}^i\mathfrak{v}^k)^{-1}\mathfrak{e}(\mathfrak{u}^i\mathfrak{v}^k) = \mathfrak{e}\,\mathfrak{m}^i\mathfrak{n}^k =$$
$$= \mathfrak{e}[(\mathfrak{u}^i\mathfrak{v}^k)^{3^m}]^{1-ik\cdot 3^{m-1}},$$

woraus wegen § 2., (1) und § 2., (2) folgt, daß $\mathfrak{A}_{3,m}$ wesentlicher Kern von $\mathfrak{D}_{3,m}$ ist. $\mathfrak{D}_{3,m}/\mathfrak{A}_{3,m}$ ist direktes Produkt zweier Zyklen der Ordnung 3^m. Also ist

$$\mathfrak{A}_{3,m} = \mathfrak{R}(\mathfrak{D}_{3,m}) = \mathfrak{C}(\mathfrak{D}_{3,m}),\quad \{\mathfrak{m}\} \times \{\mathfrak{n}\} = \mathfrak{Z}(\mathfrak{D}_{3,m}) = \mathfrak{D}(\mathfrak{D}_{3,m}),$$

und aus § 3., Satz 2., b. folgt, daß $\mathfrak{D}_{3,m}$ unvollkommen ist, da ja $\mathfrak{e}^{3^{m-1}} \neq \mathfrak{1}$ nicht in $\mathfrak{Z}(\mathfrak{D}_{3,m})$ liegt. Damit ist auch gezeigt:

(5) *In* $\mathfrak{D}_{3,m}$ *gelten die in* § 3., *Satz* 1., a., b., *aber nicht die in* § 3., *Satz* 1., c. *angegebenen Beziehungen.*

Aus (1)—(4) folgt dann:

dann und nur dann ist $\mathfrak{G}$ *unvollkommen, wenn* $\mathfrak{G}$ *isomorph* $\mathfrak{D}_{3,m} \times \mathfrak{B}$, *wo* $\mathfrak{B}$ *eine abelsche Gruppe ist, deren Elemente eine Ordnung* $\leqq 3^m$ *haben.*

Unvollkommene Gruppen $\mathfrak{G}^{(i)}$ *sind dann und nur dann isomorph, wenn*

1. *ihre Kerne isomorph sind, oder wenn*
2. *ihre Zentren isomorph sind, oder wenn sie*
3. *dieselbe Maximalordnung im Kern haben und* $\mathfrak{Z}(\mathfrak{G}^{(1)})/\mathfrak{D}(\mathfrak{G}^{(1)})$ *isomorph* $\mathfrak{Z}(\mathfrak{G}^{(2)})/\mathfrak{D}(\mathfrak{G}^{(2)})$ *ist.*

Man bemerke, daß diese Gruppen „fast vollkommen" sind, wie schon (5) zeigt, und daß sie genau den durch § 8., Satz 1., c. ausgeschlossenen Fall $w = 0$ realisieren. Es wird sich zeigen, daß die Dinge in dem noch zu behandelnden Falle $m = 1$ völlig anders liegen.

$$m = 1.$$

In diesem Falle sind $\mathfrak{K}(\mathfrak{G})$ und $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ direkte Produkte von Zyklen der Ordnung 3.

(6) *Sind* $\mathfrak{u}, \mathfrak{v}$ *mod* $\mathfrak{K}(\mathfrak{G})$ *unabhängig, so sind die folgenden Aussagen gleichwertig*:

a. $\mathfrak{c}(\mathfrak{u}) = \mathfrak{u}^3$ *und* $\mathfrak{c}(\mathfrak{v}) = \mathfrak{v}^3$ *sind unabhängige Elemente aus* $\mathfrak{K}(\mathfrak{G})$;

b. $[\mathfrak{u}, \mathfrak{v}]$ *ist mit* $\mathfrak{u}$ *und* $\mathfrak{v}$ *vertauschbar*;

c. $\mathfrak{u}$ *und* $\mathfrak{v}$ *sind mit genau denselben Elementen aus* $\mathfrak{K}(\mathfrak{G})$ *vertauschbar*;

d. $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\}$ *ist vollkommen.*

A. Da $\mathfrak{K}(\mathfrak{G})$ wesentlicher Kern, $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ abelsch und $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\} > \mathfrak{K}(\mathfrak{G})$ ist, so ist $\mathfrak{K}(\mathfrak{G})$ auch wesentlicher Kern von $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\}$ und $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\}/\mathfrak{K}(\mathfrak{G})$ abelsch. Also sind b. und d. wegen § 3., Satz 2., b. äquivalent; a. folgt aus d. wegen § 3., Lemma 1., und c. folgt aus d. wegen § 5., Satz und § 4., (1).

B. Wir zeigen, daß b. *eine Folge von* a. ist. — Sind nämlich $\mathfrak{c}(\mathfrak{u})$ und $\mathfrak{c}(\mathfrak{v})$ unabhängig, so gilt, da $\mathfrak{c}(\mathfrak{u})$, $\mathfrak{c}(\mathfrak{v})$ in $\mathfrak{Z}(\mathfrak{G})$ nach § 2., (5), b.

für jedes $\mathfrak{k}$ aus $\mathfrak{K}(\mathfrak{G})$ und i, k mit $i^2 \equiv k^2 \equiv 1 \bmod 3$ ist

$$\begin{aligned}\mathfrak{c}(\mathfrak{u}^i\mathfrak{v}^k)^{h(\mathfrak{k},\,\mathfrak{u}^i\mathfrak{v}^k)} &= \mathfrak{c}(\mathfrak{u})^{ih(\mathfrak{k},\,\mathfrak{u})}\mathfrak{c}(\mathfrak{v})^{kh(\mathfrak{k},\,\mathfrak{v})} \\ &= \mathfrak{c}(\mathfrak{u})^{i[1+ikh([\mathfrak{v},\mathfrak{u}],\,\mathfrak{u})]\,h(\mathfrak{k},\,\mathfrak{u}^i\mathfrak{v}^k)} \cdot \mathfrak{c}(\mathfrak{v})^{k[1+ikh([\mathfrak{u},\,\mathfrak{v}])]\,h(\mathfrak{k},\,\mathfrak{u}^i\mathfrak{v}^k)}\end{aligned}$$

wegen § 2., (6), a. und § 2., (7),

und da $\mathfrak{c}(\mathfrak{u})$, $\mathfrak{c}(\mathfrak{v})$ unabhängig sind, so wird:

$$h(\mathfrak{k}, \mathfrak{u}) \equiv [1+ikh([\mathfrak{v}, \mathfrak{u}], \mathfrak{u})]\, h(\mathfrak{k}, \mathfrak{u}^i\mathfrak{v}^k) \bmod 3,$$
$$h(\mathfrak{k}, \mathfrak{v}) \equiv [1+ikh([\mathfrak{u}, \mathfrak{v}], \mathfrak{v})]\, h(\mathfrak{k}, \mathfrak{u}^i\mathfrak{v}^k) \bmod 3.$$

Da nach § 2., (2) die von $\mathfrak{u}$ [bzw. von $\mathfrak{v}$] invariant gelassenen Elemente von $\mathfrak{R}(\mathfrak{G})$ eine Untergruppe vom Index 3 bilden, so folgt

$$1 + ikh([\mathfrak{v}, \mathfrak{u}], \mathfrak{u}) \equiv \pm 1 \bmod 3$$
$$1 + ikh([\mathfrak{u}, \mathfrak{v}], \mathfrak{v}) \equiv \pm 1 \bmod 3$$

für alle $ik \equiv \pm 1 \bmod 3$, d.h. aber

$$h([\mathfrak{v}, \mathfrak{u}], \mathfrak{u}) \equiv h([\mathfrak{u}, \mathfrak{v}], \mathfrak{v}) \equiv 0 \bmod 3,$$

d.h. $[\mathfrak{u}, \mathfrak{v}]$ ist mit $\mathfrak{u}$ und mit $\mathfrak{v}$ vertauschbar.

C. Wir zeigen, daß b. *eine Folge von* c. ist. — Ist nämlich die Gesamtheit $\mathfrak{F}$ der mit $\mathfrak{u}$ vertauschbaren Elemente aus $\mathfrak{R}(\mathfrak{G})$ gleich der Gesamtheit der mit $\mathfrak{v}$ vertauschbaren Elemente aus $\mathfrak{R}(\mathfrak{G})$, so ist $\mathfrak{R}(\mathfrak{G})/\mathfrak{F}$ wegen § 2., (2) ein Zyklus der Ordnung 3. Angenommen, $[\mathfrak{u}, \mathfrak{v}]$ liegt nicht in $\mathfrak{F}$; dann ist $[\mathfrak{u}, \mathfrak{v}]$ Element einer erzeugenden Restklasse von $\mathfrak{R}(\mathfrak{G})/\mathfrak{F}$ und also:

$$h([\mathfrak{u}, \mathfrak{v}], \mathfrak{v})^2 \equiv h([\mathfrak{v}, \mathfrak{u}], \mathfrak{u})^2 \equiv 1 \bmod 3.$$

Weiter sind $\mathfrak{c}(\mathfrak{u})$ und $\mathfrak{c}(\mathfrak{v})$ wegen des ad B. bewiesenen voneinander abhängig, und da man ev. $\mathfrak{v}^{-1}$ an Stelle von $\mathfrak{v}$ betrachten kann, so können wir o. B. d. A. $\mathfrak{c}(\mathfrak{u}) = \mathfrak{c}(\mathfrak{v})$ annehmen.

Wegen § 2., (5), b. liegen $\mathfrak{c}(\mathfrak{u})$, $\mathfrak{c}(\mathfrak{v})$ in $\mathfrak{Z}(\mathfrak{G})$ und wegen § 2., (6), a. und § 2., (7) wird für $i^2 \equiv k^2 \equiv 1 \bmod 3$:

$$\mathfrak{c}(\mathfrak{u}^i\mathfrak{v}^k) = \mathfrak{c}(\mathfrak{u})^{i[1+h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})]+k[1+h([\mathfrak{v},\mathfrak{u}],\mathfrak{u})]}.$$

Da wegen § 2., (2) der Exponent von $\mathfrak{c}(\mathfrak{u})$ für kein $ik \not\equiv 0 \bmod 3$ verschwinden darf, so muß von den Zahlen: $1 + h([\mathfrak{u}, \mathfrak{v}], \mathfrak{v})$, $1 + h([\mathfrak{v}, \mathfrak{u}], \mathfrak{u})$ genau eine $\equiv 0$, die andere $\not\equiv 0 \bmod 3$ sein. O. B. d. A. sei etwa:

$$1 \equiv h([\mathfrak{v}, \mathfrak{u}], \mathfrak{u}) \equiv h([\mathfrak{v}, \mathfrak{u}], \mathfrak{v}) \bmod 3.$$

Dann wird $\mathfrak{c}(\mathfrak{u}^i\mathfrak{v}^k) = \mathfrak{c}(\mathfrak{u})^{-k}$ und für jedes $\mathfrak{k}$ aus $\mathfrak{R}(\mathfrak{G})$ gilt also:

$$ih(\mathfrak{k}, \mathfrak{u}) + kh(\mathfrak{k}, \mathfrak{v}) \equiv -kh(\mathfrak{k}, \mathfrak{u}^i\mathfrak{v}^k) \bmod 3.$$

Es ergibt sich also für $i = 1$, $k = -1$, $\mathfrak{k} = [\mathfrak{u}, \mathfrak{v}]$:

$$0 \equiv h([\mathfrak{u}, \mathfrak{v}], \mathfrak{u}\mathfrak{v}^{-1}) \bmod 3.$$

Da aber alle Elemente aus $\mathfrak{F}$ mit $\mathfrak{u}\mathfrak{v}^{-1}$ vertauschbar sind, so besagt dies, daß alle Elemente aus $\mathfrak{R}(\mathfrak{G})$ mit $\mathfrak{u}\mathfrak{v}^{-1}$ vertauschbar

sind, da ja $[\mathfrak{u}, \mathfrak{v}]$ ein erzeugendes Element von $\mathfrak{K}(\mathfrak{G})/\mathfrak{Z}$ repräsentiert; da aber $\mathfrak{K}(\mathfrak{G})$ wesentlicher Kern von $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\}$ ist, so müßte also $\mathfrak{u}\mathfrak{v}^{-1}$ nach § 1., Satz 3. zu $\mathfrak{K}(\mathfrak{G})$ gehören, was unmöglich ist, da $\mathfrak{u}, \mathfrak{v}$ mod $\mathfrak{K}(\mathfrak{G})$ unabhängig sind. — Also ist b. eine Folge von c.

Aus A., B., C. folgt (6).

(7) *Dann und nur dann ist* $\mathfrak{G}$ *unvollkommen, wenn* $\mathfrak{c}(\mathfrak{u})$ *und* $\mathfrak{c}(\mathfrak{v})$ *für irgendwelche* $\mathfrak{u}, \mathfrak{v}$ *abhängig sind.* [36] [36a])

Das Hinreichen der Bedingung folgt aus § 3., Lemma 1. — Sei also $\mathfrak{G}$ unvollkommen und $\mathfrak{M}$ ein maximales mod $\mathfrak{K}(\mathfrak{G})$ unabhängiges System derart, daß $\mathfrak{c}(\mathfrak{u}), \mathfrak{c}(\mathfrak{v})$ unabhängig sind, wenn $\mathfrak{u} \neq \mathfrak{v}$ aus $\mathfrak{M}$ ist [37]). Aus (6), a., b. und § 3., Satz 2., b. folgt, daß $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{M}\}$ vollkommen ist; also ist $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{M}\} < \mathfrak{G}$ und es gibt ein Element $\mathfrak{w}$ in $\mathfrak{G}$, das nicht in $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{M}\}$ liegt. Da $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ nur Elemente der Ordnung 3 enthält, so ist auch das aus $\mathfrak{w}$ und den Elementen von $\mathfrak{M}$ bestehende System mod $\mathfrak{K}(\mathfrak{G})$ unabhängig; also gibt es wenigstens ein $\mathfrak{u}$ in $\mathfrak{M}$, so daß $\mathfrak{c}(\mathfrak{u})$ und $\mathfrak{c}(\mathfrak{w})$ abhängig sind. Enthielte nun $\mathfrak{M}$ noch ein von $\mathfrak{u}$ verschiedenes Element $\mathfrak{v}$, so sind sowohl $\mathfrak{c}(\mathfrak{u}), \mathfrak{c}(\mathfrak{v})$ als auch $\mathfrak{c}(\mathfrak{v}), \mathfrak{c}(\mathfrak{w})$ unabhängig; also folgt aus (6), a., c., daß mit $\mathfrak{u}$ dieselben Elemente aus $\mathfrak{K}(\mathfrak{G})$ wie mit $\mathfrak{v}$, mit $\mathfrak{v}$ dieselben wie mit $\mathfrak{w}$ vertauschbar sind, daß also $\mathfrak{c}(\mathfrak{u})$ und $\mathfrak{c}(\mathfrak{w})$ unabhängig wären, was unmöglich ist. Also enthält $\mathfrak{M}$ genau ein Element und hieraus folgt (7).

(8) *Ist* $\mathfrak{G}$ *unvollkommen und* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *direktes Produkt zweier Zyklen* [*der Ordnung* 3], *so ist* $\mathfrak{K}(\mathfrak{G})/\mathfrak{Z}(\mathfrak{G})$ *direktes Produkt zweier Zyklen der Ordnung* 3 *und es gibt eine Basis* $\mathfrak{r}, \mathfrak{s}$ *von* $\mathfrak{G}$ mod $\mathfrak{K}(\mathfrak{G})$, *so daß die Relationen*

$$\mathfrak{r}^3 = \mathfrak{s}^3 = \mathfrak{c},$$
$$\mathfrak{r}^{-1}[\mathfrak{r}, \mathfrak{s}]\mathfrak{r} = \mathfrak{s}^{-1}[\mathfrak{r}, \mathfrak{s}]\mathfrak{s} = [\mathfrak{r}, \mathfrak{s}]\mathfrak{c}$$

gelten.

Es sei $\mathfrak{u}, \mathfrak{v}$ eine Basis von $\mathfrak{G}$ mod $\mathfrak{K}(\mathfrak{G})$. Wegen § 2., (2) und wegen (6), c., d. bilden die Untergruppen der von $\mathfrak{u}$ bzw. $\mathfrak{v}$ invariant gelassenen Elemente aus $\mathfrak{K}(\mathfrak{G})$ verschiedene Untergruppen vom Index 3 von $\mathfrak{K}(\mathfrak{G})$ und, da alle Elemente aus $\mathfrak{K}(\mathfrak{G})$ die Ordnung 3 haben, so ist also $\mathfrak{K}(\mathfrak{G})/\mathfrak{Z}(\mathfrak{G})$ direktes Produkt zweier Zyklen der Ordnung 3.

---

[36]) Dies ist nicht mehr richtig, wenn $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ zyklisch ist.

[36a]) Also liegt jedes $\mathfrak{c}(\mathfrak{g})$ in $\mathfrak{Z}(\mathfrak{G})$.

[37]) Ist $\mathfrak{G}$ unendlich, so folgt die Existenz von Systemen $\mathfrak{M}$ in üblicher Weise durch Wohlordnung und transfinite Induktion.

Wegen (6), a., d. [oder wegen (7)] sind $\mathfrak{c}(\mathfrak{u}) = \mathfrak{u}^3$ und $\mathfrak{c}(\mathfrak{v}) = \mathfrak{v}^3$ abhängige Elemente, d.h. $\mathfrak{c}(\mathfrak{u}) = \mathfrak{c}(\mathfrak{v})^{\pm 1}$, da $\mathfrak{c}(\mathfrak{u}) \neq 1$, $\mathfrak{c}(\mathfrak{v}) \neq 1$ wegen § 2., (2), und wir können also o. B. d. A. annehmen: $\mathfrak{c}(\mathfrak{u}) = \mathfrak{c}(\mathfrak{v}) = \mathfrak{c}$.

Ist $i^2 \equiv k^2 \equiv 1 \bmod 3$, so folgt aus § 2., (2), § 2., (6), a., und § 2., (7), daß

$$1 \neq \mathfrak{c}(\mathfrak{u}^i \mathfrak{v}^k) = \mathfrak{c}^{i[1+h([\mathfrak{u},\,\mathfrak{v}]\,\mathfrak{v})]\,+k[1+h([\mathfrak{v},\,\mathfrak{u}],\,\mathfrak{u})]}$$

ist, und mithin ist von den Zahlen $1+h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})$ und $1+h([\mathfrak{v},\mathfrak{u}],\mathfrak{u})$ genau eine $\equiv 0$, die andere $\not\equiv 0 \bmod 3$; wegen (6) b., d. ist von den Zahlen $h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})$ und $h([\mathfrak{v},\mathfrak{u}],\mathfrak{u})$ höchstens eine $\equiv 0 \bmod 3$. Also können nur die folgenden vier Fälle eintreten:

Fall	I	II	III	IV
$h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})$	1	-1	-1	0
$h([\mathfrak{v},\mathfrak{u}],\mathfrak{u})$	-1	0	1	-1

Liegt Fall I vor, so setzen wir $\mathfrak{u} = \mathfrak{r}$, $\mathfrak{v} = \mathfrak{s}$, während wir $\mathfrak{v} = \mathfrak{r}$, $\mathfrak{u} = \mathfrak{s}$ im Falle III setzen. Im Falle II setzen wir $\mathfrak{r} = \mathfrak{u}\mathfrak{v}$, $\mathfrak{s} = \mathfrak{u}^{-1}\mathfrak{v}$ und erhalten

$$\mathfrak{c}(\mathfrak{r}) = \mathfrak{c} = \mathfrak{c}(\mathfrak{s}),$$

$$\begin{aligned} h([\mathfrak{r},\mathfrak{s}],\mathfrak{s}) &\equiv -h([\mathfrak{r},\mathfrak{s}],\mathfrak{u}) + h([\mathfrak{r},\mathfrak{s}],\mathfrak{v}) \equiv \\ &\equiv -[h([\mathfrak{u},\mathfrak{v}],\mathfrak{u}) - h([\mathfrak{v},\mathfrak{u}]),\mathfrak{u}] + \\ &\qquad + h([\mathfrak{u},\mathfrak{v}],\mathfrak{v}) - h([\mathfrak{v},\mathfrak{u}],\mathfrak{v}) \equiv \\ &\equiv 1 \bmod 3, \end{aligned}$$

und, da $\mathfrak{r}$, $\mathfrak{s}$ mod $\mathfrak{N}(\mathfrak{G})$ unabhängig sind, so zeigt unsere Falltafel, daß

$$h([\mathfrak{s},\mathfrak{r}],\mathfrak{r}) \equiv -1 \bmod 3 \text{ ist.}$$

Im Falle IV schließlich wählen wir:

$$\mathfrak{r} = \mathfrak{v}\mathfrak{u}, \quad \mathfrak{s} = \mathfrak{v}^{-1}\mathfrak{u},$$

und damit ist (8) völlig bewiesen.

(9) *Es gibt eine Erweiterung* $\mathfrak{D}_{3,1}$ *des direkten Produkts* $\mathfrak{A}_{3,1} = \{\mathfrak{m}\} \times \{\mathfrak{n}\} \times \{\mathfrak{c}\}$ *dreier Zyklen der Ordnung* 3 *mit zwei Elementen* $\mathfrak{u}$, $\mathfrak{v}$, *so daß gilt*:

$\mathfrak{u}^3 = \mathfrak{v}^3 = \mathfrak{c}$;
$\mathfrak{u}^{-1}\mathfrak{m}\mathfrak{u} = \mathfrak{m}\mathfrak{c}$, $\mathfrak{u}^{-1}\mathfrak{n}\mathfrak{u} = \mathfrak{n}$, $\mathfrak{u}^{-1}\mathfrak{c}\mathfrak{u} = \mathfrak{c}$;
$\mathfrak{v}^{-1}\mathfrak{m}\mathfrak{v} = \mathfrak{m}$, $\mathfrak{v}^{-1}\mathfrak{n}\mathfrak{v} = \mathfrak{n}\mathfrak{c}$, $\mathfrak{v}^{-1}\mathfrak{c}\mathfrak{v} = \mathfrak{c}$;
$[\mathfrak{u},\mathfrak{v}] = \mathfrak{m}\mathfrak{n}$.

Da $\mathfrak{u}, \mathfrak{v}$ in $\mathfrak{A}_{3,1}$ Automorphismen induzieren, da weiter

$$\prod_{i=1}^{3} \mathfrak{u}^{i-1}[\mathfrak{u}, \mathfrak{v}]\mathfrak{u}^{1-i} = \prod_{i=1}^{3} \mathfrak{u}^{i-1}\mathfrak{m}\mathfrak{n}\mathfrak{u}^{1-i} = \prod_{i=1}^{3} \mathfrak{m}\mathfrak{n}\mathfrak{c}^{1-i} = \mathfrak{1} =$$
$$= \mathfrak{c}\mathfrak{v}\mathfrak{c}^{-1}\mathfrak{v}^{-1} = \mathfrak{u}^{3}\mathfrak{v}\mathfrak{u}^{-3}\mathfrak{v}^{-1}$$

und entsprechend

$$\prod_{i=1}^{3} \mathfrak{v}^{i-1}[\mathfrak{v}, \mathfrak{u}]\mathfrak{v}^{1-i} = \mathfrak{1} = \mathfrak{v}^{3}\mathfrak{u}\mathfrak{v}^{-3}\mathfrak{u}^{-1}$$

ist, so folgt (9) aus E. § 5., Zusatz, S. 407.

(10) $\mathfrak{D}_{3,1}$ *ist unvollkommen und es ist:*

$\mathfrak{K}(\mathfrak{D}_{3,1}) = \mathfrak{A}_{3,1}$, $\mathfrak{Z}(\mathfrak{D}_{3,1}) = \mathfrak{D}(\mathfrak{D}_{3,1}) = \{\mathfrak{c}\}$,
$\mathfrak{C}(\mathfrak{D}_{3,1}) = \{\mathfrak{m}\mathfrak{n}\} \times \{\mathfrak{c}\}$.

Insbesondere ist also $\mathfrak{D}_{3,1}/\mathfrak{K}(\mathfrak{D}_{3,1})$ *direktes Produkt zweier Zyklen der Ordnung* 3.

Aus § 2., (2) folgt zunächst

$$\mathfrak{A}_{3,1} = \mathfrak{K}(\{\mathfrak{A}_{3,1}, \mathfrak{u}\}) = \mathfrak{K}(\{\mathfrak{A}_{3,1}, \mathfrak{v}\}),$$

und hieraus und § 2., (6), a. und § 2., (7) folgt:

für $i^2 \equiv k^2 \equiv 1 \bmod 3$ ist

$\mathfrak{c}(\mathfrak{u}^{i}\mathfrak{v}^{k}) = \mathfrak{c}^{-i}$
$(\mathfrak{u}^{i}\mathfrak{v}^{k})^{-1}\mathfrak{m}^{r}\mathfrak{n}^{s}\mathfrak{c}^{t}(\mathfrak{u}^{i}\mathfrak{v}^{k}) = \mathfrak{m}^{r}\mathfrak{n}^{s}\mathfrak{c}^{t+ir+ks} = \mathfrak{m}^{r}\mathfrak{n}^{s}\mathfrak{c}^{t}\mathfrak{c}(\mathfrak{u}^{i}\mathfrak{v}^{k})^{-r-iks}$,

und wegen § 2., (2) ist also auch

$$\mathfrak{A}_{3,1} = \mathfrak{K}(\{\mathfrak{A}_{3,1}, \mathfrak{u}^{i}\mathfrak{v}^{k}\}),$$

woraus wegen § 2., (1) sofort folgt, daß $\mathfrak{A}_{3,1}$ wesentlicher Kern von $\mathfrak{D}_{3,1}$ ist. $\mathfrak{D}_{3,1}/\mathfrak{A}_{3,1}$ ist direktes Produkt zweier Zyklen der Ordnung 3. Hieraus und aus § 3., Satz 2., b. folgen jetzt sofort die übrigen Behauptungen von (10).

Aus (8)—(10) folgt dann:

Dann und nur dann ist $\mathfrak{G}$ *unvollkommen und gleichzeitig* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *direktes Produkt zweier Zyklen der Ordnung* 3, *wenn* $\mathfrak{G}$ *isomorph* $\mathfrak{D}_{3,1} \times \mathfrak{B}$ *ist, wo* $\mathfrak{B}$ *eine abelsche Gruppe ist, deren Elemente eine Ordnung* $\leqq 3$ *haben.*

Unvollkommene Gruppen, deren Faktorgruppe nach dem Kern direktes Produkt zweier Zyklen der Ordnung 3 *ist, sind dann und nur dann isomorph, wenn*

1. *ihre Kerne isomorph sind, oder wenn*
2. *ihre Zentren isomorph sind, oder wenn*
3. *die Gruppen* $\mathfrak{Z}/\mathfrak{D}$ *isomorph sind.*

Man bemerke, daß im Gegensatz zu dem Falle $m > 1$ diese Gruppen „vollkommen unvollkommen" sind, da nicht einmal § 3., Satz 1., a. gilt. — $\mathfrak{D}(\mathfrak{G})$ ist ein Zyklus der Ordnung 3, $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ aber direktes Produkt zweier Zyklen der Ordnung 3.

Man bemerke weiter, daß für $m = 1$ [im Gegensatz zu $m > 1$] *aus der Unvollkommenheit von* $\mathfrak{G}$ *nicht folgt, daß* $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ *direktes Produkt zweier Zyklen ist,* wie folgendes *Beispiel* zeigt:

Es sei $\mathfrak{A} = \{\mathfrak{l}\} \times \{\mathfrak{m}\} \times \{\mathfrak{n}\} \times \{\mathfrak{c}\}$ direktes Produkt von vier Zyklen der Ordnung 3.

a) Es existiert eine Erweiterung $\mathfrak{Q}$ von $\mathfrak{A}$ durch $\mathfrak{u}, \mathfrak{v}, \mathfrak{w}$ mit den Relationen:

$$\mathfrak{u}^3 = \mathfrak{v}^3 = \mathfrak{w}^3 = \mathfrak{c};$$
$$\mathfrak{u}^{-1}\mathfrak{l}\mathfrak{u} = \mathfrak{l}\mathfrak{c},\ \mathfrak{u}^{-1}\mathfrak{x}\mathfrak{u} = \mathfrak{x} \text{ für } \mathfrak{x} \text{ aus } \{\mathfrak{m}\} \times \{\mathfrak{n}\} \times \{\mathfrak{c}\},$$
$$\mathfrak{v}^{-1}\mathfrak{m}\mathfrak{v} = \mathfrak{m}\mathfrak{c},\ \mathfrak{v}^{-1}\mathfrak{x}\mathfrak{v} = \mathfrak{x} \text{ für } \mathfrak{x} \text{ aus } \{\mathfrak{l}\} \times \{\mathfrak{n}\} \times \{\mathfrak{c}\},$$
$$\mathfrak{w}^{-1}\mathfrak{n}\mathfrak{w} = \mathfrak{n}\mathfrak{c},\ \mathfrak{w}^{-1}\mathfrak{x}\mathfrak{w} = \mathfrak{x} \text{ für } \mathfrak{x} \text{ aus } \{\mathfrak{m}\} \times \{\mathfrak{l}\} \times \{\mathfrak{c}\};$$
$$[\mathfrak{u}, \mathfrak{v}] = [\mathfrak{v}, \mathfrak{u}]^{-1} = \mathfrak{l}^{-1}\mathfrak{m}^{-1},$$
$$[\mathfrak{v}, \mathfrak{w}] = [\mathfrak{w}, \mathfrak{v}]^{-1} = \mathfrak{l}\mathfrak{n}^{-1},$$
$$[\mathfrak{w}, \mathfrak{u}] = [\mathfrak{u}, \mathfrak{w}]^{-1} = \mathfrak{n}\mathfrak{m}^{-1}.$$

Dies folgt aus E., § 5., Zusatz, S. 407, da einmal $\mathfrak{u}, \mathfrak{v}, \mathfrak{w}$ in $\mathfrak{A}$ Automorphismen induzieren, da weiter

$$\prod_{i=1}^{3} \mathfrak{u}^{i-1}[\mathfrak{u}, \mathfrak{v}]\mathfrak{u}^{1-i} = \prod_{i=1}^{3} \mathfrak{u}^{i-1}\mathfrak{l}^{-1}\mathfrak{m}^{-1}\mathfrak{u}^{1-i} = \prod_{i=1}^{3} \mathfrak{l}^{-1}\mathfrak{m}^{-1}\mathfrak{c}^{i-1} = 1 = \mathfrak{u}^3\mathfrak{v}\,\mathfrak{u}^{-3}\mathfrak{v}^{-1}$$

und entsprechend

$$\prod_{i=1}^{3} \mathfrak{u}^{i-1}[\mathfrak{u}, \mathfrak{w}]\mathfrak{u}^{1-i} = 1 = \mathfrak{u}^3\mathfrak{w}\,\mathfrak{u}^{-3}\mathfrak{w}^{-1},$$
$$\prod_{i=1}^{3} \mathfrak{v}^{i-1}[\mathfrak{v}, \mathfrak{u}]\mathfrak{v}^{1-i} = 1 = \mathfrak{v}^3\mathfrak{u}\,\mathfrak{v}^{-3}\mathfrak{u}^{-1},$$
$$\prod_{i=1}^{3} \mathfrak{v}^{i-1}[\mathfrak{v}, \mathfrak{w}]\mathfrak{v}^{1-i} = 1 = \mathfrak{v}^3\mathfrak{w}\,\mathfrak{v}^{-3}\mathfrak{w}^{-1},$$
$$\prod_{i=1}^{3} \mathfrak{w}^{i-1}[\mathfrak{w}, \mathfrak{u}]\mathfrak{w}^{1-i} = 1 = \mathfrak{w}^3\mathfrak{u}\,\mathfrak{w}^{-3}\mathfrak{u}^{-1},$$
$$\prod_{i=1}^{3} \mathfrak{w}^{i-1}[\mathfrak{w}, \mathfrak{v}]\mathfrak{w}^{1-i} = 1 = \mathfrak{w}^3\mathfrak{v}\,\mathfrak{w}^{-3}\mathfrak{v}^{-1},$$

und da schließlich

$$[\mathfrak{u}, \mathfrak{v}]\mathfrak{w}[\mathfrak{v}, \mathfrak{u}]\mathfrak{w}^{-1}[\mathfrak{v}, \mathfrak{w}]\mathfrak{u}[\mathfrak{w}, \mathfrak{v}]\mathfrak{u}^{-1}[\mathfrak{w}, \mathfrak{u}]\mathfrak{v}[\mathfrak{u}, \mathfrak{w}]\mathfrak{v}^{-1} = \mathfrak{c}^{-1}\mathfrak{c} = 1 \text{ ist.}$$

b) $\mathfrak{Q}$ ist unvollkommen,

$$\mathfrak{A} = \mathfrak{K}(\mathfrak{Q}) = \mathfrak{C}(\mathfrak{Q}),\ \{\mathfrak{c}\} = \mathfrak{D}(\mathfrak{Q}) = \mathfrak{Z}(\mathfrak{Q}),$$

und $\mathfrak{Q}/\mathfrak{K}(\mathfrak{Q})$ ist direktes Produkt dreier Zyklen der Ordnung 3.

Zunächst ist wegen § 2., (2)

$$\mathfrak{A} = \mathfrak{K}(\{\mathfrak{A}, \mathfrak{u}\}) = \mathfrak{K}(\{\mathfrak{A}, \mathfrak{v}\}) = \mathfrak{K}(\{\mathfrak{A}, \mathfrak{w}\}),$$

und für $i^2 \equiv k^2 \equiv l^2 \equiv 1 \bmod 3$ folgt also aus § 2., (6), a. und § 2., (7)

$$\mathfrak{c}(\mathfrak{u}^i\mathfrak{v}^k) = \mathfrak{c}^{-k},\ \mathfrak{c}(\mathfrak{v}^k\mathfrak{w}^l) = \mathfrak{c}^l,\ \mathfrak{c}(\mathfrak{w}^l\mathfrak{u}^i) = \mathfrak{c}^l,$$

und wegen

$$\begin{aligned}
(\mathfrak{u}^i\mathfrak{v}^k)^{-1}\mathfrak{l}^q\mathfrak{m}^r\mathfrak{n}^s\mathfrak{c}^t(\mathfrak{u}^i\mathfrak{v}^k) &= \mathfrak{l}^q\mathfrak{m}^r\mathfrak{n}^s\mathfrak{c}^t\mathfrak{c}(\mathfrak{u}^i\mathfrak{v}^k)^{-ikq-r}\\
(\mathfrak{v}^k\mathfrak{w}^l)^{-1}\mathfrak{l}^q\mathfrak{m}^r\mathfrak{n}^s\mathfrak{c}^t(\mathfrak{v}^k\mathfrak{w}^l) &= \mathfrak{l}^q\mathfrak{m}^r\mathfrak{n}^s\mathfrak{c}^t\mathfrak{c}(\mathfrak{v}^k\mathfrak{w}^l)^{lkr+s}\\
(\mathfrak{w}^l\mathfrak{u}^i)^{-1}\mathfrak{l}^q\mathfrak{m}^r\mathfrak{n}^s\mathfrak{c}^t(\mathfrak{w}^l\mathfrak{u}^i) &= \mathfrak{l}^q\mathfrak{m}^r\mathfrak{n}^s\mathfrak{c}^t\mathfrak{c}(\mathfrak{w}^l\mathfrak{u}^i)^{s+ilq},
\end{aligned}$$

und § 2., (2) ist also auch

$$\mathfrak{A} = \mathfrak{K}(\{\mathfrak{A}, \mathfrak{u}^i\mathfrak{v}^k\}) = \mathfrak{K}(\{\mathfrak{A}, \mathfrak{v}^k\mathfrak{w}^l\}) = \mathfrak{K}(\{\mathfrak{A}, \mathfrak{w}^l\mathfrak{u}^i\}),$$

und entsprechend wird dann

$$\mathfrak{c}(\mathfrak{u}^i\mathfrak{v}^k\mathfrak{w}^l) = \mathfrak{c}^{-i+k+l+ikl} \neq 1,$$

$$(\mathfrak{u}^i\mathfrak{v}^k\mathfrak{w}^l)^{-1}\mathfrak{l}^q\mathfrak{m}^r\mathfrak{n}^s\mathfrak{c}^t(\mathfrak{u}^i\mathfrak{v}^k\mathfrak{w}^l) = \mathfrak{l}^q\mathfrak{m}^r\mathfrak{n}^s\mathfrak{c}^t\mathfrak{c}(\mathfrak{u}^i\mathfrak{v}^k\mathfrak{w}^l)^{[iq+kr+ls][-i+k+l+ikl]},$$

da $-i+k+l+ikl \not\equiv 0 \bmod 3$ ist, d.h.

$$\mathfrak{A} = \mathfrak{K}(\{\mathfrak{A}, \mathfrak{u}^i\mathfrak{v}^k\mathfrak{w}^l\}).$$

Nun folgt aus § 2., (1), daß $\mathfrak{A}$ wesentlicher Kern von $\mathfrak{G}$ ist und hieraus folgt b) —

Es sei schließlich bemerkt, daß, falls $\mathfrak{G}$ unvollkommen, $m = 1$ ist, $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ und $\mathfrak{K}(\mathfrak{G})/\mathfrak{Z}(\mathfrak{G})$ isomorph sind, wenn nur eine dieser Gruppen endlich ist; sind aber beide unendlich, so kann $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ von höherer Mächtigkeit als $\mathfrak{K}(\mathfrak{G})/\mathfrak{Z}(\mathfrak{G})$ sein.

§ 10.

Die unvollkommenen Gruppen mit $p = 2$.

In diesem §, in dem wir nur zur Primzahl 2 gehörige Primärgruppen $\mathfrak{G}$ mit wesentlichem Kern und abelscher Faktorgruppe nach dem Kern betrachten wollen, werden wir zeigen:

Es gibt ein Paar unvollkommener Gruppen $\mathfrak{G}_{2,1}$ *und* $\mathfrak{G}_{2,-1}$ *derart,*

daß $\mathfrak{G}$ *dann und nur dann unvollkommen ist, wenn*

entweder $\mathfrak{G}$ *isomorph* $\mathfrak{G}_{2,1} \times \mathfrak{B}$
oder $\mathfrak{G}$ *isomorph* $\mathfrak{G}_{2,-1} \times \mathfrak{B}$

ist, wo $\mathfrak{B}$ *irgendeine abelsche Gruppe mit Elementen einer* 4 *nicht überschreitenden Ordnung ist, und zwar tritt der erste Fall ein, wenn* $\mathfrak{C}(\mathfrak{G}) \leqq \mathfrak{Z}(\mathfrak{G})$ *ist, sonst der zweite. —* $\mathfrak{G}_{2,1}$ *bzw.* $\mathfrak{G}_{2,-1}$ *ist also durch die Eigenschaft charakterisiert, die kleinste unvollkommene Gruppe mit abelscher bzw. nichtabelscher Faktorgruppe nach dem Zentrum zu sein.*

Da Gruppen mit zyklischer Faktorgruppe nach dem Kern stets vollkommen sind, wollen wir im folgenden stets annehmen, daß die Faktorgruppe nach dem Kern nicht zyklisch ist.

(1) *Sind* $\mathfrak{u}$ *und* $\mathfrak{v}$ *mod* $\mathfrak{R}(\mathfrak{G})$ *unabhängig, so sind die folgenden Aussagen gleichwertig*:

a. $\{\mathfrak{R}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\}$ *ist vollkommen*;

b. $n(\mathfrak{u}) < m$, $n(\mathfrak{v}) < m$, $[\mathfrak{u}, \mathfrak{v}]^{2^{m-1}} = 1$;

c. $\mathfrak{c}(\mathfrak{u})$ *und* $\mathfrak{c}(\mathfrak{v})$ *sind unabhängig*;

d. *ist* $n(\mathfrak{u}) \geqq n(\mathfrak{v})$, *so ist jedes mit* $\mathfrak{u}$ *vertauschbare Element aus* $\mathfrak{R}(\mathfrak{G})$ *auch mit* $\mathfrak{v}$ *vertauschbar.*

Beweis: Daß a. und b. gleichwertig sind, folgt aus §3., Satz 2., c. in Verbindung mit § 2, (6), a. — Weiter folgt c. wegen § 3., Lemma 1. aus a. und d. wegen § 5., Satz, § 4., (1) aus a.

Ist d. wahr, aber c. nicht, so sind $\mathfrak{u}^* = \mathfrak{u}^{2^{n(\mathfrak{u})-1}}$, $\mathfrak{v}^* = \mathfrak{v}^{2^{n(\mathfrak{v})-1}}$ ebenfalls mod $\mathfrak{R}(\mathfrak{G})$ unabhängig, aber [wegen § 2., (2)] ist $\mathfrak{c}(\mathfrak{u}^*) = \mathfrak{c}(\mathfrak{v}^*)$. Wegen d. sind dann genau dieselben Elemente aus $\mathfrak{R}(\mathfrak{G})$ mit $\mathfrak{u}^*$ wie mit $\mathfrak{v}^*$ vertauschbar; da diese Elemente aber wegen § 2., (2) eine Untergruppe vom Index 2 in $\mathfrak{R}(\mathfrak{G})$ bilden, so folgt: $\mathfrak{u}^{*-1}\mathfrak{f}\mathfrak{u}^* = \mathfrak{v}^{*-1}\mathfrak{f}\mathfrak{v}^*$ für $\mathfrak{f}$ aus $\mathfrak{R}(\mathfrak{G})$. Nach § 1., Satz 3., 2. wäre also $\mathfrak{u}^* \equiv \mathfrak{v}^*$ mod $\mathfrak{R}(\mathfrak{G})$, was unmöglich ist, d.h. aus d. folgt c.

Sei jetzt c. *wahr*; wir zeigen:

(1; 1) $\mathfrak{c}(\mathfrak{u})$ *und* $\mathfrak{c}(\mathfrak{v})$ *liegen in* $\mathfrak{Z}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\})$.

Wegen § 2., (2) gibt es ein Element $\mathfrak{k}$ in $\mathfrak{R}(\mathfrak{G})$, so daß $\mathfrak{v}^{-1}\mathfrak{k}\mathfrak{v} = \mathfrak{k}\mathfrak{c}(\mathfrak{v})$ ist. Dann wird:

$$(\mathfrak{u}\mathfrak{v})^{-1}\mathfrak{k}(\mathfrak{u}\mathfrak{v}) = \mathfrak{v}^{-1}\mathfrak{k}\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{k},\mathfrak{u})}\mathfrak{v} = \mathfrak{k}\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{k},\mathfrak{u})}\mathfrak{c}(\mathfrak{v})^{1+h(\mathfrak{k},\mathfrak{u})h(\mathfrak{c}(\mathfrak{u}),\mathfrak{v})} =$$
$$= (\mathfrak{v}\mathfrak{u})^{-1}\mathfrak{k}(\mathfrak{v}\mathfrak{u}) = \mathfrak{u}^{-1}\mathfrak{k}\mathfrak{c}(\mathfrak{v})\mathfrak{u} = \mathfrak{k}\mathfrak{c}(\mathfrak{v})\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{k},\mathfrak{u})+h(\mathfrak{c}(\mathfrak{v}),\mathfrak{u})}.$$

Wegen c. wird also $\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{c}(\mathfrak{v}),\mathfrak{u})} = 1$, d.h. $\mathfrak{c}(\mathfrak{v})$ ist mit $\mathfrak{u}$ vertauschbar; da $\mathfrak{c}(\mathfrak{v})$ auf jeden Fall mit $\mathfrak{v}$ vertauschbar ist, so liegt also

$\mathfrak{c}(\mathfrak{v})$ in $\mathfrak{Z}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\})$ und entsprechend zeigt man dies für $\mathfrak{c}(\mathfrak{u})$.

(1; 2) *Es gibt ungerade Zahlen u, v, so daß* $\mathfrak{c}(\mathfrak{u}\mathfrak{v}) = \mathfrak{c}(\mathfrak{u})^u \mathfrak{c}(\mathfrak{v})^v$ *ist.*

Fall 1: $n(\mathfrak{u}) > 1$, $n(\mathfrak{v}) > 1$.

Wegen § 2., (2) gibt es ein Element $\mathfrak{k}$ in $\mathfrak{R}(\mathfrak{G})$, so daß $(\mathfrak{u}\mathfrak{v})^{-1}\mathfrak{k}(\mathfrak{u}\mathfrak{v}) = \mathfrak{k}\mathfrak{c}(\mathfrak{u}\mathfrak{v})$ ist; dann wird wegen (1; 1):

$$\begin{aligned}\mathfrak{c}(\mathfrak{u}\mathfrak{v}) &= \mathfrak{c}(\mathfrak{u})^{h(\mathfrak{k},\mathfrak{u})}\,\mathfrak{c}(\mathfrak{v})^{h(\mathfrak{k},\mathfrak{v})} \\ &= [\mathfrak{u}, \mathfrak{v}]^{2^{m-1}}\,\mathfrak{c}(\mathfrak{u})\mathfrak{c}(\mathfrak{v}) \text{ wegen § 2., (7).}\end{aligned}$$

Da 2^m die Maximalordnung in $\mathfrak{R}(\mathfrak{G})$ ist, so folgt durch Quadrieren dieser Gleichung wegen c:

$$h(\mathfrak{k}, \mathfrak{u}) \equiv 1 \bmod 2^{n(\mathfrak{u})-1},\quad h(\mathfrak{k}, \mathfrak{v}) \equiv 1 \bmod 2^{n(\mathfrak{v})-1},$$

d.h. $u = h(\mathfrak{k}, \mathfrak{u})$, $v = h(\mathfrak{k}, \mathfrak{v})$ sind geeignete ungerade Zahlen.

Fall 2: $n(\mathfrak{u}) = 1$ oder $n(\mathfrak{v}) = 1$.

O. B. d. A. sei $n(\mathfrak{u}) = 1$. Da $m > 1$ wegen § 2., (2) ist, so ist $n(\mathfrak{u}) < m$ und wegen (1; 1) folgt aus § 2., (7) und § 2., (5), a:

$$\begin{aligned}\mathfrak{c}(\mathfrak{u}\mathfrak{v}) &= [\mathfrak{u}, \mathfrak{v}]^{2^{m-1}}\,\mathfrak{c}(\mathfrak{u})\mathfrak{c}(\mathfrak{v}) = \\ &= \left([\mathfrak{u}, \mathfrak{v}]^{2^{n(\mathfrak{u})}}\right)^{2^{m-1-n(\mathfrak{u})}}\mathfrak{c}(\mathfrak{u})\mathfrak{c}(\mathfrak{v}) = \\ &= \left(\mathfrak{c}(\mathfrak{v})^{h(\mathfrak{a}(\mathfrak{u}),\mathfrak{v})}\,\mathfrak{c}(\mathfrak{u})^{h([\mathfrak{u},\mathfrak{v}],\mathfrak{u})\,2^{n(\mathfrak{u})-1}}\right)^{2^{m-1-n(\mathfrak{u})}}\mathfrak{c}(\mathfrak{u})\mathfrak{c}(\mathfrak{v}) = \\ &= \mathfrak{c}(\mathfrak{u})^{1+2^{m-2}h([\mathfrak{u},\mathfrak{v}],\mathfrak{u})}\,\mathfrak{c}(\mathfrak{v})^{1+h(\mathfrak{a}(\mathfrak{u}),\mathfrak{v})\,2^{m-1-n(\mathfrak{u})}}.\end{aligned} \tag{*}$$

Man beachte, daß zum Beweis von (*) allein die Voraussetzung $m > n(\mathfrak{u})$ benötigt wurde. — Da $n(\mathfrak{u}) = 1$ ist, so erhalten wir

$$\mathfrak{c}(\mathfrak{u}\mathfrak{v}) = \mathfrak{c}(\mathfrak{u})^{1+2^{m-2}h([\mathfrak{u},\mathfrak{v}],\mathfrak{u})}\,\mathfrak{c}(\mathfrak{v})^{1+2^{m-2}h(\mathfrak{a}(\mathfrak{u}),\mathfrak{v})},$$

woraus (1; 2) für $m > 2$ folgt. — Ist aber $m = 2$, so folgt aus c. und (1; 1) für jedes $\mathfrak{k}$ aus $\mathfrak{R}(\mathfrak{G})$:

$$\begin{aligned}h(\mathfrak{k}, \mathfrak{u}\mathfrak{v})[1 + h([\mathfrak{u}, \mathfrak{v}], \mathfrak{u})] &\equiv h(\mathfrak{k}, \mathfrak{u}) \bmod 2, \\ h(\mathfrak{k}, \mathfrak{u}\mathfrak{v})[1 + h(\mathfrak{a}(\mathfrak{u}), \mathfrak{v})] &\equiv h(\mathfrak{k}, \mathfrak{v}) \bmod 2^{n(\mathfrak{v})}.\end{aligned}$$

Da man $\mathfrak{k}$ so wählen kann, daß $h(\mathfrak{k}, \mathfrak{u})$ oder $h(\mathfrak{k}, \mathfrak{v})$ ungerade wird, so müßen $1 + h([\mathfrak{u}, \mathfrak{v}], \mathfrak{u})$ und $1 + h(\mathfrak{a}(\mathfrak{u}), \mathfrak{v})$ beide ungerade sein, womit (1; 2) vollständig bewiesen ist.

(1; 3) $\mathfrak{D}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\}) \leqq \mathfrak{Z}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\})$.

Dies folgt sofort aus § 2., (4) und (1; 1), (1; 2).

(1; 4) *Ist* $n(\mathfrak{u}) \geqq n(\mathfrak{v})$ *so ist*

$$\mathfrak{Z}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{u}\}) \leqq \mathfrak{Z}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{v}\}).$$

Aus c., (1; 1), (1; 2) folgt nämlich für jedes $\mathfrak{k}$ aus $\mathfrak{K}(\mathfrak{G})$:

$$h(\mathfrak{k}, \mathfrak{u}) \equiv uh(\mathfrak{k}, \mathfrak{u}\mathfrak{v}) \bmod 2^{n(\mathfrak{u})},$$
$$h(\mathfrak{k}, \mathfrak{v}) \equiv vh(\mathfrak{k}, \mathfrak{u}\mathfrak{v}) \bmod 2^{n(\mathfrak{v})}.$$

Ist nun $n(\mathfrak{u}) \geqq n(\mathfrak{v})$ und $\mathfrak{k}$ mit $\mathfrak{u}$ vertauschbar, so wird $h(\mathfrak{k}, \mathfrak{u}) \equiv 0 \bmod 2^{n(\mathfrak{u})}$, also auch $h(\mathfrak{k}, \mathfrak{u}\mathfrak{v}) \equiv 0 \bmod 2^{n(\mathfrak{u})}$, also auch $h(\mathfrak{k}, \mathfrak{v}) \equiv 0 \bmod 2^{n(\mathfrak{v})}$, d.h. $\mathfrak{k}$ ist auch mit $\mathfrak{v}$ vertauschbar.

Damit ist bereits gezeigt, daß c. *und* d. *gleichwertig sind.*

(1; 5) *Es gibt Elemente* $\mathfrak{u}_1, \mathfrak{v}_1$ *in* $\mathfrak{K}(\mathfrak{G})$, *so daß* $\mathfrak{a}(\mathfrak{u}_1\mathfrak{u})$, $\mathfrak{a}(\mathfrak{v}_1\mathfrak{v})$ *in* $\mathfrak{Z}(\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\})$ *liegen.*

Es sei etwa $n(\mathfrak{u}) \geqq n(\mathfrak{v})$; wegen (1; 4) ist dann $\mathfrak{Z}(\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}\}) \leqq \mathfrak{Z}(\{\mathfrak{K}(\mathfrak{G}), \mathfrak{v}\})$, d.h. $\mathfrak{Z}(\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\}) = \mathfrak{Z}(\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}\})$ und wegen § 2., (2) ist $\mathfrak{K}(\mathfrak{G})/\mathfrak{Z}(\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\})$ ein Zyklus der Ordnung $2^{n(\mathfrak{u})}$. Sei $\mathfrak{e}$ Repräsentant einer erzeugenden Restklasse dieses Zyklus; dann wird:

$\mathfrak{a}(\mathfrak{u}) = \mathfrak{e}^r\mathfrak{u}_2$, $\mathfrak{a}(\mathfrak{v}) = \mathfrak{e}^s\mathfrak{v}_2$ mit $0 \leqq r$, $s < 2^{n(\mathfrak{u})}$ und $\mathfrak{u}_2, \mathfrak{v}_2$ in $\mathfrak{Z}(\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\})$. Da $\mathfrak{a}(\mathfrak{u})$ stets mit $\mathfrak{u}$ vertauschbar ist, so wird also $r = 0$ und wir können $\mathfrak{u}_1 = 1$ wählen; ist auch $s = 0$, so können wir auch $\mathfrak{v}_1 = 1$ wählen; ist aber $s \neq 0$, so ist, da ja $\mathfrak{a}(\mathfrak{v})$ mit $\mathfrak{v}$ vertauschbar ist, sicher $s \equiv 0 \bmod 2^{n(\mathfrak{v})}$, etwa $s = t\,2^{n(\mathfrak{v})}$ und wir setzen: $\mathfrak{v}_1 = \mathfrak{e}^{-t}$. Dann wird

$$\mathfrak{a}(\mathfrak{v}_1\mathfrak{v}) = (\mathfrak{v}_1\mathfrak{v})^{2^{n(\mathfrak{v})}} = \left(\prod_{i=0}^{2^{n(\mathfrak{v})}-1} \mathfrak{v}^i\mathfrak{v}_1\mathfrak{v}^{-i}\right)\mathfrak{v}^{2^{n(\mathfrak{v})}} =$$
$$= \left(\prod_{i=0}^{2^{n(\mathfrak{v})}-1} \mathfrak{v}_1\mathfrak{c}(\mathfrak{v})^{-ih(\mathfrak{v}_1, \mathfrak{v})}\right)\mathfrak{a}(\mathfrak{v}) =$$
$$= \mathfrak{v}_1^{2^{n(\mathfrak{v})}}\mathfrak{c}(\mathfrak{v})^{-h(\mathfrak{v}_1, \mathfrak{v})2^{n(\mathfrak{v})-1}(2^{n(\mathfrak{v})}-1)}\mathfrak{a}(\mathfrak{v}) =$$
$$= \mathfrak{v}_2\mathfrak{c}(\mathfrak{v})^{-h(\mathfrak{v}_1, \mathfrak{v})2^{n(\mathfrak{v})-1}(2^{n(\mathfrak{v})}-1)}$$

wegen (1; 1) ein Element aus $\mathfrak{Z}(\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\})$, womit (1; 5) bewiesen ist.

(1; 6) *Ist* $\mathfrak{r}$ *aus* $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\}$, *so ist* $n(\mathfrak{r}) < m$.

Da $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\}/\mathfrak{K}(\mathfrak{G})$ nicht zyklisch ist, da $m > 1$ ist, so gibt es ein Element $\mathfrak{s}$ in $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\}$, so daß $\mathfrak{r}, \mathfrak{s} \bmod \mathfrak{K}(\mathfrak{G})$ unabhängig sind, $n(\mathfrak{s}) \leqq n(\mathfrak{r})$, $n(\mathfrak{s}) < m$. Wegen (1; 5) können wir o. B. d. A. annehmen, daß $\mathfrak{a}(\mathfrak{r})$ und $\mathfrak{a}(\mathfrak{s})$ in $\mathfrak{Z}(\{\mathfrak{K}(\mathfrak{G}), \mathfrak{u}, \mathfrak{v}\})$ liegen.

Ist dann $\mathfrak{e}$ ein wegen § 2., (2) existierendes Element aus $\mathfrak{K}(\mathfrak{G})$ mit $\mathfrak{r}^{-1}\mathfrak{e}\,\mathfrak{r} = \mathfrak{e}\mathfrak{c}(\mathfrak{r})$, so wird

$$\begin{aligned}\mathfrak{c}((\mathfrak{e}\mathfrak{z})\mathfrak{x}) &= \mathfrak{c}(\mathfrak{e}\mathfrak{z})^{1+2^{m-2}h([\mathfrak{e}\mathfrak{z},\,\mathfrak{x}],\,\mathfrak{e}\mathfrak{z})}\mathfrak{c}(\mathfrak{x}) \quad \text{wegen } (*),\\ &= \mathfrak{c}(\mathfrak{z})^{x}\mathfrak{c}(\mathfrak{x}) \text{ wegen § 2., (4)},\\ &= \mathfrak{c}(\mathfrak{z}(\mathfrak{e}\mathfrak{x})) \text{ wegen (1; 3)},\\ &= \mathfrak{c}(\mathfrak{z})^{y}\mathfrak{c}(\mathfrak{e}\mathfrak{x}) \text{ wegen } (*),\\ &= \mathfrak{c}(\mathfrak{z})^{y}\mathfrak{c}(\mathfrak{x})^{1+2^{m-1}} \text{ wegen § 2., (4)}\end{aligned}$$

und also $1 = \mathfrak{c}(\mathfrak{x})^{2^{m-1}}$ wegen c., woraus $n(\mathfrak{x}) \leqq m-1$ wegen § 2., (2) folgt.

(1; 7) $[\mathfrak{u}, \mathfrak{v}]^{2^{m-1}} = 1$.

Wir bestimmen $\mathfrak{u}_1$, $\mathfrak{v}_1$ gemäß (1; 5); dann wird wegen § 2., (5), a.

$$1 = [\mathfrak{v}_1\mathfrak{v},\ \mathfrak{u}_1\mathfrak{u}]^{2^{n(\mathfrak{v})}}\mathfrak{c}(\mathfrak{v}_1\mathfrak{v})^{h([\mathfrak{u}_1\mathfrak{u},\ \mathfrak{v}_1\mathfrak{v}],\ \mathfrak{v}_1\mathfrak{v})2^{n(\mathfrak{v})-1}};$$

da $n(\mathfrak{v}) < m$ wegen (1; 6) ist, so folgt hieraus

$$[\mathfrak{v}_1\mathfrak{v},\ \mathfrak{u}_1\mathfrak{u}]^{2^{m-1}} = \mathfrak{c}(\mathfrak{v}_1\mathfrak{v})^{h([\mathfrak{v}_1\mathfrak{v},\ \mathfrak{u}_1\mathfrak{u}],\ \mathfrak{v}_1\mathfrak{v})2^{m-2}},$$

und entsprechend erhält man

$$[\mathfrak{u}_1\mathfrak{u},\ \mathfrak{v}_1\mathfrak{v}]^{2^{m-1}} = \mathfrak{c}(\mathfrak{u}_1\mathfrak{u})^{h([\mathfrak{u}_1\mathfrak{u},\ \mathfrak{v}_1\mathfrak{v}],\ \mathfrak{u}_1\mathfrak{u})2^{m-2}},$$

woraus wegen c. und § 2., (4) folgt:

$$\begin{aligned}1 &= [\mathfrak{u}_1\mathfrak{u},\ \mathfrak{v}_1\mathfrak{v}]^{2^{m-1}}\\ &= [\mathfrak{u},\ \mathfrak{v}]^{2^{m-1}}\mathfrak{c}(\mathfrak{u})^{h(\mathfrak{v}_1\mathfrak{u})2^{m-1}}\mathfrak{c}(\mathfrak{v})^{-h(\mathfrak{u}_1\mathfrak{v})2^{m-1}}\\ &= [\mathfrak{u},\ \mathfrak{v}]^{2^{m-1}} \text{ wegen (1; 6) und § 2., (2)}.\end{aligned}$$

Wegen (1; 6) und (1; 7) folgt b. aus c., womit (1) vollständig bewiesen ist.

(2) *Dann und nur dann ist* $\mathfrak{G}$ *unvollkommen, wenn* $\mathfrak{c}(\mathfrak{u})$ *und* $\mathfrak{c}(\mathfrak{v})$ *für jedes Elementepaar* $\mathfrak{u}$, $\mathfrak{v}$ *abhängig sind.*

Das Hinreichen der Bedingung folgt aus § 3., Lemma 1. Um die Notwendigkeit einzusehen, betrachten wir ein maximales mod $\mathfrak{R}(\mathfrak{G})$ unabhängiges System $\mathfrak{M}$ derart, daß $\mathfrak{c}(\mathfrak{u})$ und $\mathfrak{c}(\mathfrak{v})$ unabhängig sind, wenn nur $\mathfrak{u} \neq \mathfrak{v}$ aus $\mathfrak{M}$ ist. Aus (1) a., b., c. folgt dann, daß $\{\mathfrak{R}(\mathfrak{G}), \mathfrak{M}\}$ vollkommen ist. Ist nun $\mathfrak{G}$ unvollkommen, so gibt es also ein Element $\mathfrak{w}$, so daß $n(\mathfrak{w}) = 1$, und so daß das aus $\mathfrak{w}$ und den Elementen aus $\mathfrak{M}$ bestehende System unabhängig ist. Dann gibt es ein $\mathfrak{u}$ in $\mathfrak{M}$, so daß $\mathfrak{c}(\mathfrak{u})$ und $\mathfrak{c}(\mathfrak{w})$ abhängig sind. Enthielte nun $\mathfrak{M}$ wenigstens zwei Elemente, so gäbe es in $\mathfrak{M}$ ein von $\bar{\mathfrak{u}}$ verschiedenes Element $\mathfrak{v}$. Sei $\bar{\mathfrak{u}} = \mathfrak{u}^{2^{n(\mathfrak{u})-1}}$, $\bar{\mathfrak{v}} = \mathfrak{v}^{2^{n(\mathfrak{v})-1}}$; dann sind $\bar{\mathfrak{u}}, \bar{\mathfrak{v}}, \mathfrak{w}$ drei mod $\mathfrak{R}(\mathfrak{G})$ unabhängige

Elemente der Ordnung 2 mod $\mathfrak{R}(\mathfrak{G})$; wegen § 2., (2) wird $\mathfrak{c}(\bar{\mathfrak{u}}) = \mathfrak{c}(\mathfrak{w})$, $\mathfrak{c}(\bar{\mathfrak{u}})$ und $\mathfrak{c}(\bar{\mathfrak{v}})$ unabhängig und also auch $\mathfrak{c}(\bar{\mathfrak{v}})$ und $\mathfrak{c}(\mathfrak{w})$ unabhängig. Aus (1), c., d. folgt dann

$$\mathfrak{Z}(\{\mathfrak{R}(\mathfrak{G}), \bar{\mathfrak{u}}\}) = \mathfrak{Z}(\{\mathfrak{R}(\mathfrak{G}), \bar{\mathfrak{v}}\}) = \mathfrak{Z}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{w}\})$$

und aus (1) d., c. folgt dann, daß $\mathfrak{c}(\bar{\mathfrak{u}})$ und $\mathfrak{c}(\mathfrak{w})$ unabhängig sind; Widerspruch! Also enthält $\mathfrak{M}$ nur ein Element, wenn $\mathfrak{G}$ unvollkommen ist und hieraus folgt (2).

(3) *Ist* $n \geqq 2$, $m > 2$, *so ist* $\mathfrak{G}$ *vollkommen.*

Es sei $\mathfrak{m}$ ein Element von mod $\mathfrak{R}(\mathfrak{G})$ maximaler Ordnung: $n(\mathfrak{m}) = n$; da $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ nicht zyklisch ist, so gibt es ein Element $\mathfrak{u}$ mit $n(\mathfrak{u}) = 1$, so daß $\mathfrak{m}$ und $\mathfrak{u}$ mod $\mathfrak{R}(\mathfrak{G})$ unabhängig sind.

Ist zunächst $n < m$, so ist wegen § 2., (6), a.

$$[\mathfrak{m}^2, \mathfrak{u}]^{2^{m-1}} = [\mathfrak{m}, \mathfrak{u}]^{2^m} \mathfrak{c}(\mathfrak{m})^{2^{m-1} h([\mathfrak{u}, \mathfrak{m}], \mathfrak{m})} = 1$$

und aus (1) b., c. folgt, daß $\mathfrak{c}(\mathfrak{m}^2)$ und $\mathfrak{c}(\mathfrak{u})$ unabhängig sind, da ja $\mathfrak{m}^2$ und $\mathfrak{u}$ mod $\mathfrak{R}(\mathfrak{G})$ unabhängig sind, und (3) folgt aus (2).

Ist weiter $n = m$, so ist $n(\mathfrak{m}) > 2$ und also $\mathfrak{m}^4$ und $\mathfrak{u}$ mod $\mathfrak{R}(\mathfrak{G})$ unabhängig. Dann wird wegen § 2., (6), a.

$$[\mathfrak{m}^4, \mathfrak{u}]^{2^{m-1}} = [\mathfrak{m}, \mathfrak{u}]^{2^{m+1}} \mathfrak{c}(\mathfrak{m})^{6h([\mathfrak{u}, \mathfrak{m}], \mathfrak{m}) 2^{m-1}} = 1,$$

und wieder folgt aus (1) b., c., daß $\mathfrak{c}(\mathfrak{m}^4)$, $\mathfrak{c}(\mathfrak{u})$ unabhängig sind, und also (3) aus (2).

(4) *Es sei* $\mathfrak{G}$ *unvollkommen und* $n = 1$.

a. *Es gibt ein Element* $\mathfrak{c}$ *der Ordnung* 2 *in* $\mathfrak{Z}(\mathfrak{G})$, *so daß* $\mathfrak{c}(\mathfrak{g}) = \mathfrak{c}$ *für jedes nicht in* $\mathfrak{R}(\mathfrak{G})$ *enthaltene Element* $\mathfrak{g}$ *aus* $\mathfrak{G}$.

b. $m = 2$.

c. $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ *und* $\mathfrak{R}(\mathfrak{G})/\mathfrak{Z}(\mathfrak{G})$ *sind je direktes Produkt zweier Zyklen der Ordnung* 2.

d. *Ist* $\mathfrak{C}(\mathfrak{G}) \leqq \mathfrak{Z}(\mathfrak{G})$, *so liegt* $\mathfrak{a}(\mathfrak{g})$ *nicht in* $\mathfrak{Z}(\mathfrak{G})$, *wenn* $\mathfrak{g}$ *nicht in* $\mathfrak{R}(\mathfrak{G})$ *liegt.*

e. *Ist* $\mathfrak{C}(\mathfrak{G}) \not\leqq \mathfrak{Z}(\mathfrak{G})$, *so gibt es eine Basis* $\mathfrak{r}$, $\mathfrak{s}$ *von* $\mathfrak{G}$ *mod* $\mathfrak{R}(\mathfrak{G})$, *so daß* $\mathfrak{a}(\mathfrak{r})$, $\mathfrak{a}(\mathfrak{s})$ *in* $\mathfrak{Z}(\mathfrak{G})$ *liegen, während* $[\mathfrak{r}, \mathfrak{s}]$ *weder mit* $\mathfrak{r}$ *noch mit* $\mathfrak{s}$ *vertauschbar ist.*

a. folgt aus (2), $n = 1$ und § 2., (2).

(4; 1) *Sind* $\mathfrak{u}$, $\mathfrak{v}$ *mod* $\mathfrak{R}(\mathfrak{G})$ *unabhängig, so ist:*

$$[\mathfrak{u}, \mathfrak{v}]^2 = \mathfrak{c}^{h(\mathfrak{a}(\mathfrak{v}), \mathfrak{u}) + h([\mathfrak{u}, \mathfrak{v}], \mathfrak{v})} = \mathfrak{c},$$

$$[\mathfrak{u}, \mathfrak{v}] = \mathfrak{a}(\mathfrak{u}\mathfrak{v})\, \mathfrak{a}(\mathfrak{u})\, \mathfrak{a}(\mathfrak{v})\, \mathfrak{c}^{h(\mathfrak{a}(\mathfrak{u}), \mathfrak{v})},$$

$$\mathfrak{a}(\mathfrak{u}\mathfrak{v}) = [\mathfrak{u}, \mathfrak{v}]\, \mathfrak{a}(\mathfrak{u})\, \mathfrak{a}(\mathfrak{v})\, \mathfrak{c}^{h(\mathfrak{a}(\mathfrak{u}), \mathfrak{v})}.$$

Aus (4), a. und § 2., (7) folgt nämlich

$$\mathfrak{c} = \mathfrak{c}(\mathfrak{u}\mathfrak{v}) = [\mathfrak{u}, \mathfrak{v}]^{2^{m-1}}\mathfrak{c}(\mathfrak{u})\mathfrak{c}(\mathfrak{v}) = [\mathfrak{u}, \mathfrak{v}]^{2^{m-1}},$$

und wegen § 2., (2) ist also 2^m die genaue Ordnung von $[\mathfrak{u}, \mathfrak{v}]$. Wegen $n(\mathfrak{v}) = n = 1$ und § 2., (5), a. und wegen (4), a. ist weiter:

$$[\mathfrak{u}, \mathfrak{v}]^2 = \mathfrak{c}^{h(\mathfrak{a}(\mathfrak{v}),\mathfrak{u})+h([\mathfrak{u},\mathfrak{v}],\mathfrak{v})}$$

und also $[\mathfrak{u}, \mathfrak{v}]^4 = 1$. Mithin ist $m \leqq 2$, und da $m > 1$ wegen § 2., (2) ist, so folgt $m = 2$, d.h. b. und auch die erste Formel (4; 1). Weiter ist:

$$\begin{aligned}\mathfrak{a}(\mathfrak{u}\mathfrak{v}) = (\mathfrak{u}\mathfrak{v})^2 = \mathfrak{u}\mathfrak{v}\,\mathfrak{u}\mathfrak{v} = [\mathfrak{u}, \mathfrak{v}]\mathfrak{v}\mathfrak{u}^2\mathfrak{v} = [\mathfrak{u}, \mathfrak{v}]\mathfrak{v}\,\mathfrak{a}(\mathfrak{u})\mathfrak{v} = \\ = [\mathfrak{u}, \mathfrak{v}]\mathfrak{a}(\mathfrak{u})\mathfrak{c}^{h(\mathfrak{a}(\mathfrak{u}),\mathfrak{v})}\mathfrak{a}(\mathfrak{v}),\end{aligned}$$

woraus wegen $\mathfrak{a}(\mathfrak{u})^2 = \mathfrak{a}(\mathfrak{v})^2 = \mathfrak{c} = \mathfrak{c}^{-1}$ die beiden andern Formeln (4; 1) folgen.

Sind weiter $\mathfrak{u}$, $\mathfrak{v}$, $\mathfrak{w}$ mod $\mathfrak{R}(\mathfrak{G})$ unabhängig, so wird wegen $n(\mathfrak{u}\mathfrak{v}\mathfrak{w}) = 1$

$$\begin{aligned}\mathfrak{a}(\mathfrak{u}\mathfrak{v}\mathfrak{w}) &= \mathfrak{u}\mathfrak{v}\mathfrak{w}\,\mathfrak{u}\mathfrak{v}\mathfrak{w} = \\ &= \mathfrak{u}\mathfrak{v}[\mathfrak{w}, \mathfrak{u}]\mathfrak{u}\mathfrak{w}\mathfrak{v}\mathfrak{w} = \\ &= \mathfrak{u}\mathfrak{v}[\mathfrak{w}, \mathfrak{u}]\mathfrak{u}[\mathfrak{w}, \mathfrak{v}]\mathfrak{v}\,\mathfrak{a}(\mathfrak{w}) = \\ &= \mathfrak{c}^{h([\mathfrak{w},\mathfrak{u}],\mathfrak{u})+h([\mathfrak{w},\mathfrak{u}],\mathfrak{v})+h([\mathfrak{w},\mathfrak{v}],\mathfrak{v})} \cdot [\mathfrak{w}, \mathfrak{u}][\mathfrak{w}, \mathfrak{v}]\mathfrak{a}(\mathfrak{u}\mathfrak{v})\mathfrak{a}(\mathfrak{w}), \\ &\qquad \text{da } \mathfrak{c} \text{ nach a. in } \mathfrak{Z}(\mathfrak{G}),\ \mathfrak{u}^2 \text{ in } \mathfrak{R}(\mathfrak{G}) \text{ liegt,} \\ &= \mathfrak{c}^{h([\mathfrak{w},\mathfrak{u}],\mathfrak{u})+h([\mathfrak{w},\mathfrak{u}],\mathfrak{v})+h([\mathfrak{w},\mathfrak{v}],\mathfrak{v})+h(\mathfrak{a}(\mathfrak{u}),\mathfrak{v})} \cdot \\ &\qquad \cdot [\mathfrak{w}, \mathfrak{u}][\mathfrak{w}, \mathfrak{v}][\mathfrak{u}, \mathfrak{v}]\mathfrak{a}(\mathfrak{u})\mathfrak{a}(\mathfrak{v})\mathfrak{a}(\mathfrak{w}) \\ &\qquad \text{nach (4; 1) dritte Formel;}\end{aligned}$$

wegen a., b. und der ersten Formel (4; 1) wird also:

$$\mathfrak{c} = \mathfrak{a}(\mathfrak{u}\mathfrak{v}\mathfrak{w})^2 = \mathfrak{c}^6 = 1,$$

was a. widerspricht.

Also ist $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ als nicht-zyklische Gruppe direktes Produkt zweier Zyklen der Ordnung 2, und da nach § 2., (2) für nicht in $\mathfrak{R}(\mathfrak{G})$ gelegenes $\mathfrak{g}$ stets $\mathfrak{R}(\mathfrak{G})/\mathfrak{Z}(\{\mathfrak{R}(\mathfrak{G}), \mathfrak{g}\})$ die Ordnung 2 hat, so folgt aus (1), d., c. und (4), a., daß $\mathfrak{R}(\mathfrak{G})/\mathfrak{Z}(\mathfrak{G})$ direktes Produkt zweier Zyklen der Ordnung 2 ist, womit auch (4), c. bewiesen ist.

Sei jetzt $\mathfrak{u}, \mathfrak{v}$ eine Basis von $\mathfrak{G}$ mod $\mathfrak{R}(\mathfrak{G})$. Wegen (4; 1) ist dann:

$$\begin{aligned}1 &\equiv h(\mathfrak{a}(\mathfrak{v}), \mathfrak{u}) + h([\mathfrak{u}, \mathfrak{v}], \mathfrak{v}) \bmod 2, \\ 1 &\equiv h(\mathfrak{a}(\mathfrak{u}), \mathfrak{v}) + h([\mathfrak{v}, \mathfrak{u}], \mathfrak{u}) \bmod 2.\end{aligned}$$

Ist $\mathfrak{C}(\mathfrak{G}) \leqq \mathfrak{Z}(\mathfrak{G})$, so ist also

$$1 \equiv h(\mathfrak{a}(\mathfrak{v}), \mathfrak{u}) \equiv h(\mathfrak{a}(\mathfrak{u}), \mathfrak{v})) \bmod 2, \text{ was d. beweist.}$$

Ist $\mathfrak{C}(\mathfrak{G}) \not\leqq \mathfrak{Z}(\mathfrak{G})$ und

$$1 \equiv h([\mathfrak{u}, \mathfrak{v}], \mathfrak{v}) \equiv h([\mathfrak{v}, \mathfrak{u}], \mathfrak{u}) \bmod 2, \text{ so ist}$$
$$0 \equiv h(\mathfrak{a}(\mathfrak{v}), \mathfrak{u}) \equiv h(\mathfrak{a}(\mathfrak{u}), \mathfrak{v}) \bmod 2$$

und $\mathfrak{u}$, $\mathfrak{v}$ ist eine gesuchte Basis mod $\mathfrak{R}(\mathfrak{G})$. Da $\mathfrak{C}(\mathfrak{G}) \not\leqq \mathfrak{Z}(\mathfrak{G})$ ist, $\mathfrak{c}$ wegen a. in $\mathfrak{Z}(\mathfrak{G})$ liegt, so kann wegen § 2, (6), a. sicher $[\mathfrak{u}, \mathfrak{v}]$ nicht in $\mathfrak{Z}(\mathfrak{G})$ liegen, und von den Größen $h([\mathfrak{v}, \mathfrak{u}], \mathfrak{u})$, $h([\mathfrak{u}, \mathfrak{v}], \mathfrak{v})$ ist wenigstens eine ungerade. O. B. d. A. sei also

$$h([\mathfrak{u}, \mathfrak{v}], \mathfrak{v}) \equiv 1 \bmod 2,$$
$$h([\mathfrak{v}, \mathfrak{u}], \mathfrak{u}) \equiv 0 \bmod 2.$$

Dann wird wegen (4; 1), dritte Formel

$$h(\mathfrak{a}(\mathfrak{u}\mathfrak{v}), \mathfrak{v}) \equiv h(\mathfrak{a}(\mathfrak{v}), \mathfrak{u}\mathfrak{v}) \equiv 0 \bmod 2, \text{ also}$$
$$h([\mathfrak{u}\mathfrak{v}, \mathfrak{v}], \mathfrak{v}) \equiv h([\mathfrak{v}, \mathfrak{u}\mathfrak{v}], \mathfrak{u}\mathfrak{v}) \equiv 1 \bmod 2,$$

und $\mathfrak{u}\mathfrak{v}$, $\mathfrak{v}$ bilden eine gesuchte Basis mod $\mathfrak{R}(\mathfrak{G})$, womit (4), e. bewiesen ist.

(5) *Ist $\mathfrak{G}$ unvollkommen, so ist $n = 1$.*

Wegen (3) und $n \leqq m$ haben wir nur zu zeigen, daß es keine unvollkommenen Gruppen mit $n = m = 2$ geben kann.

Ist $\mathfrak{W}(\mathfrak{G})$ die Gesamtheit der Elemente $\mathfrak{g}$ mit $n(\mathfrak{g}) \leqq 1$, so ist $\mathfrak{W}(\mathfrak{G})$ eine charakteristische Untergruppe von $\mathfrak{G}$ mit $\mathfrak{R}(\mathfrak{G})$ als wesentlichem Kern und abelscher, nicht-zyklischer Faktorgruppe nach dem Kern. $\mathfrak{W}(\mathfrak{G})$ ist unvollkommen, da es sonst ein Paar unabhängiger Elemente $\mathfrak{c}(\mathfrak{u})$, $\mathfrak{c}(\mathfrak{v})$ mit $\mathfrak{u}$, $\mathfrak{v}$ in $\mathfrak{W}(\mathfrak{G}) \leqq \mathfrak{G}$ gäbe, was wegen (2) die Vollkommenheit von $\mathfrak{G}$ nach sich zöge. Wegen (4), b. ist dann mit $\mathfrak{W}(\mathfrak{G})/\mathfrak{R}(\mathfrak{G})$ auch $\mathfrak{G}/\mathfrak{R}(\mathfrak{G})$ direktes Produkt zweier Zyklen.

Sei nun $\mathfrak{m}$ ein Element mit $n(\mathfrak{m}) = n = 2$ und

$$\mathfrak{U} = \{\mathfrak{W}(\mathfrak{G}), \mathfrak{m}\}.$$

Dann wird $\mathfrak{R}(\mathfrak{U}) = \mathfrak{R}(\mathfrak{G})$ wesentlicher Kern von $\mathfrak{U}$ und $\mathfrak{U}/\mathfrak{R}(\mathfrak{U})$ direktes Produkt eines Zyklus der Ordnung 4 mit einem der Ordnung 2. Sei $\mathfrak{m}$, $\mathfrak{u}$ eine Basis von $\mathfrak{U}$ mod $\mathfrak{R}(\mathfrak{U})$.

Dann ist $\mathfrak{m}^2$, $\mathfrak{u}$ eine Basis von $\mathfrak{W}(\mathfrak{G})$ mod $\mathfrak{R}(\mathfrak{G})$ und nach § 2., (6), a. ist:

$$[\mathfrak{m}^2, \mathfrak{u}] = [\mathfrak{m}, \mathfrak{u}]^2 \mathfrak{c}(\mathfrak{m})^{h([\mathfrak{u}, \mathfrak{m}], \mathfrak{m})}.$$

Da $[\mathfrak{m}^2, \mathfrak{u}]$ nach (4; 1) genau die Ordnung 4 hat und also

$$[\mathfrak{m}^2, \mathfrak{u}]^2 = \mathfrak{c}(\mathfrak{m})^{2h([\mathfrak{u}, \mathfrak{m}], \mathfrak{m})} \neq 1$$

ist, so folgt:

$$h([\mathfrak{u}, \mathfrak{m}], \mathfrak{m}) = \pm 1.$$

Fall 1: $\mathfrak{C}[\mathfrak{W}(\mathfrak{G})] \leqq \mathfrak{Z}[\mathfrak{W}(\mathfrak{G})]$.

Dann wird nach obigem

$$[\mathfrak{m}^2, \mathfrak{u}] = \mathfrak{u}^{-1}[\mathfrak{m}^2, \mathfrak{u}]\mathfrak{u} = [\mathfrak{m}^2, \mathfrak{u}]\mathfrak{c}(\mathfrak{u})^{\pm h(\mathfrak{c}(\mathfrak{m}), \mathfrak{u})},$$

da ja $\mathfrak{c}(\mathfrak{u})$ die Ordnung 2 hat. Also ist

$$1 = \mathfrak{c}(\mathfrak{u})^{h(\mathfrak{c}(\mathfrak{m}), \mathfrak{u})},$$

d.h. $\mathfrak{c}(\mathfrak{m}) = \mathfrak{a}(\mathfrak{m}) = \mathfrak{a}(\mathfrak{m}^2)$ mit $\mathfrak{u}$ vertauschbar, was (4), d. widerspricht, da ja $\mathfrak{a}(\mathfrak{m}^2)$ mit $\mathfrak{m}^2$ vertauschbar ist.

Fall 1. kann also nicht eintreten.

Fall 2: $\mathfrak{C}[\mathfrak{W}(\mathfrak{G})] \nleqq \mathfrak{Z}[\mathfrak{W}(\mathfrak{G})]$.

Da $\mathfrak{c}(\mathfrak{u}) = \mathfrak{c}(\mathfrak{m}^2)$ wegen (4), a. in $\mathfrak{Z}[\mathfrak{W}(\mathfrak{G})]$ liegt, da $\mathfrak{C}[\mathfrak{W}(\mathfrak{G})] = \{\mathfrak{c}(\mathfrak{u}), [\mathfrak{m}^2, \mathfrak{u}]\}$ nach § 2., (6), a. ist, da $\mathfrak{a}(\mathfrak{m}) = \mathfrak{a}(\mathfrak{m}^2)$ ist, so können wegen (4; 1) nur die folgenden drei Fälle eintreten:

Fall	I	II	III
$h(\mathfrak{a}(\mathfrak{m}), \mathfrak{u})$	1	0	0
$h(\mathfrak{a}(\mathfrak{u}), \mathfrak{m}^2)$	0	1	0

Da nun

$$\begin{aligned} h([\mathfrak{m}^2, \mathfrak{u}], \mathfrak{m}^2) &\equiv h([\mathfrak{m}^2, \mathfrak{u}], \mathfrak{m}) \bmod 4 \\ &\equiv 2h([\mathfrak{m}, \mathfrak{u}], \mathfrak{m}) + h([\mathfrak{u}, \mathfrak{m}], \mathfrak{m})h(\mathfrak{c}(\mathfrak{m}), \mathfrak{m}) \bmod 4 \\ &\equiv 0 \bmod 2 \end{aligned}$$

ist [$\mathfrak{c}(\mathfrak{m})$ ist mit $\mathfrak{m}$ vertauschbar], so kann wegen (4; 1), erste Formel nur I eintreten.

Da also $\mathfrak{a}(\mathfrak{u})$ mit $\mathfrak{m}^2$ vertauschbar ist, so ist $\mathfrak{m}^{-1}\mathfrak{a}(\mathfrak{u})\mathfrak{m} = \mathfrak{a}(\mathfrak{u})\mathfrak{c}^z$.

Da $\mathfrak{u}^2 = \mathfrak{a}(\mathfrak{u})$ ist, so wird weiter

$$\begin{aligned} \mathfrak{u}^{-1}[\mathfrak{m}, \mathfrak{u}]\mathfrak{u} &= \mathfrak{u}^{-1}\mathfrak{m}\mathfrak{u}\mathfrak{m}^{-1}\mathfrak{u}^{-1}\mathfrak{u} = \mathfrak{u}^{-1}\mathfrak{m}\mathfrak{u}^2\mathfrak{u}^{-1}\mathfrak{m}^{-1} = \mathfrak{c}^z\mathfrak{u}\mathfrak{m}\mathfrak{u}^{-1}\mathfrak{m}^{-1} = \\ &= \mathfrak{c}^z[\mathfrak{u}, \mathfrak{m}] \\ &= \mathfrak{c}^y[\mathfrak{m}, \mathfrak{u}], \end{aligned}$$

und daraus folgt: $[\mathfrak{m}, \mathfrak{u}]^2 = \mathfrak{c}^{z+y}$.

Da $\mathfrak{c} = \mathfrak{c}(\mathfrak{m}^2) = \mathfrak{c}(\mathfrak{m})^2$ ist, so ist also $[\mathfrak{m}, \mathfrak{u}]^2$ mit $\mathfrak{m}$ vertauschbar und

$$\begin{aligned} \mathfrak{m}^{-1}[\mathfrak{m}, \mathfrak{u}]^2\mathfrak{m} &= [\mathfrak{m}, \mathfrak{u}]^2 \\ &= (\mathfrak{m}^{-1}[\mathfrak{m}, \mathfrak{u}]\mathfrak{m})^2 = ([\mathfrak{m}, \mathfrak{u}]\mathfrak{c}(\mathfrak{m})^{h([\mathfrak{m}, \mathfrak{u}], \mathfrak{m})})^2 = \\ &= [\mathfrak{m}, \mathfrak{u}]^2\mathfrak{c}(\mathfrak{m})^2, \text{ da } h([\mathfrak{m}, \mathfrak{u}], \mathfrak{m}) = \pm 1, \text{ wie oben gezeigt,} \\ &= [\mathfrak{m}, \mathfrak{u}]^2\mathfrak{c}, \end{aligned}$$

und das ist unmöglich, da $\mathfrak{c} \neq 1$ ist.

Fall 2. kann also auch nicht eintreten, womit (5) bewiesen ist.

(6) *Für* $\varepsilon = \pm 1$ *gibt es eine Erweiterung* $\mathfrak{Q}_{2,\varepsilon}$ *des direkten Produkts*

$$\mathfrak{A} = \{\mathfrak{r}\} \times \{\mathfrak{s}\} \times \{\mathfrak{c}\}$$

der beiden Zyklen $\{\mathfrak{r}\}$, $\{\mathfrak{s}\}$ *der Ordnung* 2 *mit dem Zyklus* $\{\mathfrak{c}\}$ *der Ordnung* 4 *durch zwei Elemente* $\mathfrak{u}$, $\mathfrak{v}$ *mit den Relationen*:

$$\mathfrak{u}^2 = \mathfrak{r}\mathfrak{c},\ \mathfrak{r}^2 = \mathfrak{s}\mathfrak{c};$$

$$[\mathfrak{u}, \mathfrak{v}] = \mathfrak{c};$$

$$\mathfrak{u}^{-1}\mathfrak{r}\mathfrak{u} = \mathfrak{r}\mathfrak{c}^{1-\varepsilon},\ \mathfrak{u}^{-1}\mathfrak{s}\mathfrak{u} = \mathfrak{s}\mathfrak{c}^2,\ \mathfrak{u}^{-1}\mathfrak{c}\mathfrak{u} = \mathfrak{c}^{\varepsilon},$$

$$\mathfrak{v}^{-1}\mathfrak{r}\mathfrak{v} = \mathfrak{r}\mathfrak{c}^2,\ \mathfrak{v}^{-1}\mathfrak{s}\mathfrak{v} = \mathfrak{s}\mathfrak{c}^{1-\varepsilon},\ \mathfrak{v}^{-1}\mathfrak{c}\mathfrak{v} = \mathfrak{c}^{\varepsilon}.$$

Zunächst induzieren nämlich $\mathfrak{u}$ und $\mathfrak{v}$ in $\mathfrak{A}$ Automorphismen der Ordnung 2. — Weiter ist:

$$\mathfrak{u}^{-1}\mathfrak{u}^2\mathfrak{u} = \mathfrak{u}^{-1}\mathfrak{r}\mathfrak{c}\mathfrak{u} = \mathfrak{u}^2\mathfrak{c}^{1-\varepsilon}\mathfrak{c}^{\varepsilon-1} = \mathfrak{u}^2,$$

$$\mathfrak{v}^{-1}\mathfrak{v}^2\mathfrak{v} = \mathfrak{v}^{-1}\mathfrak{s}\mathfrak{c}\mathfrak{v} = \mathfrak{v}^2\mathfrak{c}^{1-\varepsilon}\mathfrak{c}^{\varepsilon-1} = \mathfrak{v}^2,$$

$$\mathfrak{u}^2\mathfrak{v}\,\mathfrak{u}^{-2}\mathfrak{v}^{-1} = \mathfrak{c}^{2+\varepsilon-1} = \mathfrak{c}^{1+\varepsilon} = [\mathfrak{u}, \mathfrak{v}]\mathfrak{u}[\mathfrak{u}, \mathfrak{v}]\mathfrak{u}^{-1},$$

$$\mathfrak{v}^2\mathfrak{u}\mathfrak{v}^{-2}\mathfrak{u}^{-1} = \mathfrak{c}^{2+\varepsilon-1} = \mathfrak{c}^{1+\varepsilon} = \mathfrak{c}^{-1-\varepsilon} = [\mathfrak{v}, \mathfrak{u}]\mathfrak{v}[\mathfrak{v}, \mathfrak{u}]\mathfrak{v}^{-1}.$$

Hieraus folgt (6) wegen E., § 5., Zusatz, S. 407.

(7) $\mathfrak{Q}_{2,\varepsilon}$ *ist unvollkommen, und es ist*:

$$\mathfrak{A} = \mathfrak{R}(\mathfrak{Q}_{2,\varepsilon}),\ \{\mathfrak{c}\} = \mathfrak{C}(\mathfrak{Q}_{2\ \varepsilon}),\ \{\mathfrak{c}^2\} = \mathfrak{D}(\mathfrak{Q}_{2,\varepsilon}) \leqq \mathfrak{Z}(\mathfrak{Q}_{2,\varepsilon});$$

$\mathfrak{C}(\mathfrak{Q}_{2,\varepsilon}) \leqq \mathfrak{Z}(\mathfrak{Q}_{2,\varepsilon})$ *dann und nur dann, wenn* $\varepsilon = +1$.

Wegen § 2., (2) ist sicher $\mathfrak{A} = \mathfrak{R}(\{\mathfrak{A}, \mathfrak{u}\}) = \mathfrak{R}(\{\mathfrak{A}, \mathfrak{v}\})$, wegen § 2., (7) also

$$\mathfrak{c}(\mathfrak{u}\mathfrak{v}) = [\mathfrak{u}, \mathfrak{v}]^2\mathfrak{c}(\mathfrak{u})\mathfrak{c}(\mathfrak{v}) = \mathfrak{c}^2, \text{ da } \mathfrak{c}(\mathfrak{u}) = \mathfrak{c}(\mathfrak{v}) = \mathfrak{c}^2 \text{ in } \mathfrak{Z}(\mathfrak{Q}_{2,\varepsilon}),$$

und

$$\mathfrak{u}\mathfrak{v}\mathfrak{r}^r\mathfrak{s}^s\mathfrak{c}^c\mathfrak{v}\mathfrak{u} = \mathfrak{r}^r\mathfrak{s}^s\mathfrak{c}^c\mathfrak{r}^{r(2+1-\varepsilon)+s(1-\varepsilon+2)+c2(\varepsilon-1)} =$$

$$= \mathfrak{r}^r\mathfrak{s}^s\mathfrak{c}^c\,\mathfrak{c}(\mathfrak{u}\mathfrak{v})^{(r+s)\frac{3-\varepsilon}{2}+c(\varepsilon-1)};$$

wegen § 2., (2) ist also auch $\mathfrak{A} = \mathfrak{R}(\{\mathfrak{A}, \mathfrak{u}\mathfrak{v}\})$, und da $\mathfrak{Q}_{2,\varepsilon}/\mathfrak{A}$ direktes Produkt zweier Zyklen der Ordnung 2 ist, so folgt aus § 2., (1), daß $\mathfrak{A}$ wesentlicher Kern von $\mathfrak{Q}_{2,\varepsilon}$ ist, woraus die übrigen Behauptungen von (7) wegen (1), a., b. folgen.

Aus (4)—(7) folgen nun die im Beginn des § ausgesprochenen Behauptungen und überdies:

Zwei unvollkommene Gruppen sind dann und nur dann isomorph, wenn

1. *in beiden Gruppen das Zentrum die Kommutatorgruppe enthält bzw. nicht enthält,*

2. *die Kerne isomorph sind.*

Man bemerke, daß die unvollkommenen Gruppen wieder nicht einmal § 3., Satz 1., a. erfüllen, da $\mathfrak{D}$ zyklisch ist, die Faktorgruppe nach dem Kern aber nicht.

Es sei schließlich bemerkt, daß es möglich ist, $\mathfrak{Q}_{2,\varepsilon}$ durch zwei Erzeugende $\mathfrak{u}$, $\mathfrak{v}$ mit den Relationen

$$\mathfrak{u}^8 = \mathfrak{v}^8 = \mathfrak{1},$$

$$\mathfrak{u}^4 = \mathfrak{v}^4 = [\mathfrak{u}, \mathfrak{v}]^2,$$

$$\mathfrak{u}^{-1}[\mathfrak{u}, \mathfrak{v}]\mathfrak{u} = \mathfrak{v}^{-1}[\mathfrak{u}, \mathfrak{v}]\mathfrak{v} = [\mathfrak{u}, \mathfrak{v}]^{\varepsilon}$$

zu charakterisieren. Dies verifiziert man, indem man

$$\mathfrak{r} = \mathfrak{u}^2[\mathfrak{v}, \mathfrak{u}], \quad \mathfrak{s} = \mathfrak{v}^2[\mathfrak{v}, \mathfrak{u}], \quad \mathfrak{c} = [\mathfrak{u}, \mathfrak{v}]$$

setzt und nachrechnet, daß die in (6) angegebenen Relationen erfüllt sind, sowie daß $\mathfrak{Q}_{2,\varepsilon}$ die hier angegebenen Relationen erfüllt.

(Eingegangen den 1. November 1934. Abgeändert eingegangen den 23. April 1935.)