Composito Mathematica

Reinhold Baer

Der Kern, eine charakteristische Untergruppe

Compositio Mathematica, tome 1 (1935), p. 254-283

<http://www.numdam.org/item?id=CM_1935__1__254_0>

Der Kern, eine charakteristische Untergruppe

von

Reinhold Baer

Manchester

An invariant definierten Untergruppen einer beliebigen Gruppe $\mathfrak{G}$ sind im wesentlichen zwei bekannt: die Kommutatorgruppe $\mathfrak{C}(\mathfrak{G})$ und das Zentrum $\mathfrak{Z}(\mathfrak{G})$. Da $\mathfrak{G}/\mathfrak{C}(\mathfrak{G})$ kommutativ ist, so ist die Struktur dieser Gruppe relativ leicht zu überblicken; doch ist der Aufbau von $\mathfrak{G}$ aus $\mathfrak{G}/\mathfrak{C}(\mathfrak{G})$ und $\mathfrak{C}(\mathfrak{G})$ schwer zu übersehen, da $\mathfrak{C}(\mathfrak{G})$ i. A. nicht kommutativ ist und also die Restklassen von $\mathfrak{G}/\mathfrak{C}(\mathfrak{G})$ in $\mathfrak{C}(\mathfrak{G})$ ganze Automorphismenklassen einer Gruppe von meist komplizierter Struktur induzieren. Fassen wir andererseits das Zentrum ins Auge, so ist dieses zwar kommutativ, aber die Restklassen von $\mathfrak{G}/\mathfrak{Z}(\mathfrak{G})$ induzieren in $\mathfrak{Z}(\mathfrak{G})$ nur den identischen Automorphismus, so daß das dritte invariante Bestimmungsstück, das bei kommutativem Normalteiler zur Verfügung steht, in diesem Fall ausfällt.

Wir wollen hier eine invariant definierte Untergruppe einführen, die mit dem Zentrum die Übersichtlichkeit der Struktur gemein hat, ohne daß in ihr nur der identische Automorphismus induziert wird: den Kern $\mathfrak{K}(\mathfrak{G})$ von $\mathfrak{G}$. Wie ein Element aus $\mathfrak{G}$ dann und nur dann zum Zentrum gehört, wenn es jedes Element aus $\mathfrak{G}$ in sich transformiert, so *gehört ein Element dann und nur dann zum Kern, wenn es jede Untergruppe von $\mathfrak{G}$ in sich transformiert.*

Der Kern ist abelsch oder hamiltonsch [1]); ist er hamiltonsch, so haben alle Elemente aus $\mathfrak{G}$ endliche Ordnung. Enthält der Kern ein Element unendlicher Ordnung, so stimmt er mit dem

---

[1]) *Hamiltonsche Gruppen sind nicht-kommutative Gruppen, deren sämtliche Untergruppen Normalteiler sind. Sie lassen sich stets als direktes Produkt einer Quaternionengruppe, einer kommutativen Gruppe, deren sämtliche Elemente die Ordnung 2 haben, und einer kommutativen Gruppe, deren sämtliche Elemente ungerade Ordnung haben, darstellen.* Vergl. R. Dedekind, Gesammelte Werke Bd. II, [Braunschweig (1931)], 87—102; Wendt [Math. Ann. 59 (1904), 187—192]; R. Baer [Sitzungsberichte Heidelberg, 1933, Nr. 2, 14].

Zentrum überein. Dies gilt auch, wenn die Gruppe primär ist, und der Kern Elemente beliebig hoher Ordnung enthält.

Während die Faktorgruppe nach dem Zentrum nie zyklisch sein kann, kann die nach dem Kern zwar kein unendlicher, wohl aber ein endlicher Zyklus sein. Ist dies der Fall, so ist die Gruppe direktes Produkt primärer Gruppen, und der Kern der Gruppe ist [stets] das direkte Produkt der Kerne der Primärgruppen; entsprechendes gilt für die Faktorgruppen nach dem Kern. Hat eine derartige Primärgruppe einen hamiltonschen Kern [gehört also zur Primzahl 2], so ist sie mit ihrem Kern identisch.

Es gilt nun die überraschende Tatsache, daß die Struktur einer Gruppe mit zyklischer Faktorgruppe nach dem Kern bereits durch die Struktur des Kernes und die Lage des Zentrums der Gruppe im Kern völlig bestimmt ist, und hieraus folgt auch, daß derartige Gruppen, wenn sie den Kern gemein haben, dann und nur dann isomorph sind, wenn sie im Kern konjugierte Automorphismengruppen induzieren.

Ein Überblick über alle möglichen Gruppen mit zyklischer Faktorgruppe nach dem Kern wird dann durch den folgenden Satz geliefert: Ist $\mathfrak{A}$ eine kommutative Primärgruppe, $\mathfrak{B}$ eine echte Untergruppe von $\mathfrak{A}$, so gibt es dann und nur dann eine [und wenn überhaupt eine, dann im wesentlichen nur eine] Gruppe, deren Kern $\mathfrak{A}$, deren Zentrum $\mathfrak{B}$ ist, wenn $\mathfrak{B}$ ein Element von in $\mathfrak{A}$ maximaler Ordnung enthält, $\mathfrak{A}/\mathfrak{B}$ zyklisch [von einer die Maximalordnung in $\mathfrak{A}$ nicht überschreitenden Ordnung] ist [gehört $\mathfrak{A}$ zur Primzahl 2, so ist noch notwendig, daß die Maximalordnung der Elemente aus $\mathfrak{A}$ größer oder gleich 4 ist]. Überdies ist dann die Faktorgruppe nach dem Kern isomorph $\mathfrak{A}/\mathfrak{B}$.

Zum Schluss untersuchen wir noch die Beziehungen zwischen dem Kern und den situationstreuen Abbildungen der Gruppe.

Bezeichnungen:

$\mathfrak{C}(\mathfrak{G})$ = Kommutatorgruppe von $\mathfrak{G}$ = kleinste Untergruppe von $\mathfrak{G}$, deren Faktorgruppe kommutativ ist.

$\mathfrak{K}(\mathfrak{G})$ = 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.

$\mathfrak{G}_p$ = zur Primzahl p gehörige Primärkomponente von $\mathfrak{G}$ = Gesamtheit der Elemente von $\mathfrak{G}$, deren Ordnung eine Potenz von p ist [$\mathfrak{G}_p$ ist nicht immer Untergruppe von $\mathfrak{G}$].

$\mathfrak{A} \times \ldots \times \mathfrak{B} \times \ldots =$ direktes Produkt der Gruppen $\mathfrak{A}, \ldots, \mathfrak{B}, \ldots$
$\mathfrak{A} \cap \mathfrak{B} =$ Durchschnitt von $\mathfrak{A}$ und $\mathfrak{B}$.
$\{\ldots\} =$ von den eingeschlossenen Elementen oder Elementmengen erzeugte Untergruppe.

§ 1.

Aus der zu Beginn gegebenen Definition des Kerns folgert man sofort folgende einfache Charakterisierung:

(1) Dann und nur dann gehört das Element $\mathfrak{g}$ aus $\mathfrak{G}$ zum Kern $\mathfrak{K}(\mathfrak{G})$, wenn $\mathfrak{g}^{-1}\mathfrak{B}\mathfrak{g} = \mathfrak{B}$ für alle zyklischen Untergruppen $\mathfrak{B}$ von $\mathfrak{G}$ erfüllt ist.

Bemerkung: Ist $\mathfrak{U}$ eine Untergruppe von $\mathfrak{G}$, so sei $\mathfrak{N}(\mathfrak{U})$ der Normalisator von $\mathfrak{U}$, d.h. die größte Untergruppe von $\mathfrak{G}$, deren Normalteiler $\mathfrak{U}$ ist.

Dann gilt:

$\mathfrak{K}(\mathfrak{G}) =$ Durchschnitt aller Normalisatoren von Untergruppen von $\mathfrak{G}$
$=$ Durchschnitt aller Normalisatoren von *zyklischen* Untergruppen von $\mathfrak{G}$.

Dies legt Verallgemeinerungen des Kernbegriffs in der Weise nahe, daß man den Durchschnitt aller Normalisatoren von Untergruppen $\mathfrak{U}$ von $\mathfrak{G}$ betrachtet, so daß $\mathfrak{N}(\mathfrak{U})/\mathfrak{U}$ zyklisch oder kommutativ ist oder sonst einer ausgezeichneten Gruppenklasse angehört.

Weiter gilt:

(2) $\mathfrak{K}(\mathfrak{G})$ ist eine charakteristische Untergruppe [2]) von $\mathfrak{G}$, insbesondere also ein Normalteiler.

Denn $\mathfrak{K}(\mathfrak{G})$ ist gruppeninvariant definiert.

(3) $\mathfrak{K}(\mathfrak{G}) \geqq \mathfrak{Z}(\mathfrak{G})$.

(4) Für jede Untergruppe $\mathfrak{U}$ von $\mathfrak{G}$ ist $\mathfrak{K}(\mathfrak{U}) \geqq \mathfrak{U} \cap \mathfrak{K}(\mathfrak{G})$.

(5) $\mathfrak{K}(\mathfrak{G})$ ist abelsch oder hamiltonsch.

Denn wegen (4) ist $\mathfrak{K}[\mathfrak{K}(\mathfrak{G})] = \mathfrak{K}(\mathfrak{G})$ und also jede Untergruppe von $\mathfrak{K}(\mathfrak{G})$ Normalteiler von $\mathfrak{K}(\mathfrak{G})$.

(6) Enthält $\mathfrak{K}(\mathfrak{G})$ nur Elemente endlicher Ordnung, so ist $\mathfrak{K}(\mathfrak{G})$ direktes Produkt primärer Gruppen.

Dies folgt aus dem entsprechenden [bekannten] Satz über kommutative Gruppen und aus Fußnote [1]), falls $\mathfrak{K}(\mathfrak{G})$ hamiltonsch ist.

(7) Ist $\mathfrak{k}$ ein Element aus $\mathfrak{K}(\mathfrak{G})$, $\mathfrak{g}$ aus $\mathfrak{G}$, so gibt es eine ganze

---

[2]) Das ist eine Untergruppe, die bei allen Automorphismen von $\mathfrak{G}$ in sich übergeht.

Zahl l, so daß $\mathfrak{k}^{-1}\mathfrak{g}\mathfrak{k}\mathfrak{g}^{-1} = \mathfrak{g}^l$ ist, und es ist $\mathfrak{g}^l$ Element aus $\mathfrak{C}(\mathfrak{G}) \cap \mathfrak{K}(\mathfrak{G})$ und $\{\mathfrak{g}^{l+1}\} = \{\mathfrak{g}\}$.

Folgt aus (1) und (2).

(8) Enthält $\mathfrak{G}$ nur Elemente endlicher Ordnung, so ist $\mathfrak{k}$ aus $\mathfrak{G}$ dann und nur dann Element aus $\mathfrak{K}(\mathfrak{G})$, wenn es eine ganze Zahl $l = l(\mathfrak{x}, \mathfrak{k})$ gibt, so daß $\mathfrak{k}^{-1}\mathfrak{x}\mathfrak{k} = \mathfrak{x}^l$ ist.

Dies folgt aus (1) und (7), wenn man noch bedenkt, daß bei endlichen Gruppen aus $\mathfrak{k}^{-1}\mathfrak{U}\mathfrak{k} \leqq \mathfrak{U}$ stets $\mathfrak{k}^{-1}\mathfrak{U}\mathfrak{k} = \mathfrak{U}$ folgt.

Es sei schließlich noch angegeben, wie man Kerne höherer Ordnung bilden kann [analog wie beim Zentrum]: $\mathfrak{K}^{(1)}(\mathfrak{G}) = \mathfrak{K}(\mathfrak{G})$; ist bereits $\mathfrak{K}^{(\nu)}(\mathfrak{G})$ für eine Ordinalzahl ν gebildet, so ist $\mathfrak{K}^{(\nu+1)}(\mathfrak{G})$ die Gesamtheit der Elemente aus Restklassen von $\mathfrak{K}\,[\mathfrak{G}/\mathfrak{K}^{(\nu)}(\mathfrak{G})]$; ist λ eine Limeszahl und $\mathfrak{K}^{(\nu)}(\mathfrak{G})$ für alle $\nu < \lambda$ gebildet, so ist $\mathfrak{K}^{(\lambda)}(\mathfrak{G})$ die Vereinigungsmenge [und also Gruppe] aller $\mathfrak{K}^{(\nu)}(\mathfrak{G})$ mit $\nu < \lambda$, welches Verfahren abbricht, wenn $\mathfrak{K}^{(\nu+1)}(\mathfrak{G}) = \mathfrak{K}^{(\nu)}(\mathfrak{G})$ ist.

§ 2.

(9) *Es sei $\mathfrak{A}$ ein kommutativer Normalteiler von $\{\mathfrak{A}, \mathfrak{g}\}$, wo $\mathfrak{g}$ ein beliebiges Element aus $\mathfrak{G}$ ist, und $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$. Ist $\{\mathfrak{A}, \mathfrak{g}\}/\mathfrak{A}$ unendlich, so ist $\{\mathfrak{A}, \mathfrak{g}\}$ kommutativ und direktes Produkt von $\mathfrak{A}$ mit einem unendlichen Zyklus.*

Da $\mathfrak{g}$ ein Element von unendlicher Ordnung sein muß, und $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$ ist, so ist $\mathfrak{a}^{-1}\mathfrak{g}\mathfrak{a} = \mathfrak{g}^{\pm 1}$ für jedes $\mathfrak{a}$ aus $\mathfrak{A}$.

Mit $\mathfrak{g}$ muß auch $\mathfrak{g}\cdot\mathfrak{a}^{-1}$ von unendlicher Ordnung sein und es wird also entsprechend

$$\mathfrak{a}^{-1}\cdot\mathfrak{g} = \mathfrak{a}^{-1}\mathfrak{g}\mathfrak{a}^{-1}\mathfrak{a} = (\mathfrak{g}\mathfrak{a}^{-1})^{\pm 1}.$$

Wäre nun $\mathfrak{a}^{-1}\mathfrak{g}\mathfrak{a} = \mathfrak{g}^{-1}$, so wäre

$$\begin{aligned}\mathfrak{a}^{-1}\mathfrak{g} &= (\mathfrak{g}\mathfrak{a}^{-1})^{\pm 1}\\ &= \mathfrak{a}^{-1}\mathfrak{g}\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{g}^{-1}\mathfrak{a}^{-1}.\end{aligned}$$

Wäre weiter $\mathfrak{g}^{-1}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{g} = \mathfrak{g}\mathfrak{a}^{-1}$, so wäre $\mathfrak{g} = \mathfrak{g}^{-1}$ d.h. $\mathfrak{g}^2 = 1$, was unmöglich ist. Also müßte $\mathfrak{a}^{-1}\mathfrak{g} = \mathfrak{g}^{-1}\mathfrak{a}^{-1} = (\mathfrak{g}\mathfrak{a}^{-1})^{-1} = \mathfrak{a}\mathfrak{g}^{-1}$ sein. Dann wird aber $\mathfrak{g}^2 = \mathfrak{a}^2$, d.h. $\{\mathfrak{A}, \mathfrak{g}\}/\mathfrak{A}$ höchstens von der Ordnung 2, was auch unmöglich ist. Also wird $\mathfrak{a}^{-1}\mathfrak{g}\mathfrak{a} = \mathfrak{g}$ für jedes $\mathfrak{a}$ aus $\mathfrak{A}$, woraus (9) folgt.

Satz 1: *Ist $\mathfrak{K}(\mathfrak{G})$ hamiltonsch, so enthält $\mathfrak{G}$ nur Elemente endlicher Ordnung.*

Beweis: Da $\mathfrak{K}(\mathfrak{G})$ hamiltonsch ist, so enthält $\mathfrak{K}(\mathfrak{G})$ nur Elemente endlicher Ordnung und einen direkten Faktor von der Struktur der Quaternionengruppe [nach Anm. [1])]. Es gibt also insbesondere in $\mathfrak{K}(\mathfrak{G})$ zwei Elemente $\mathfrak{a}$, $\mathfrak{b}$, die $\mathfrak{a}^4 = \mathfrak{b}^4 = 1$, $\mathfrak{a}^2 = \mathfrak{b}^2$, $\mathfrak{a}^{-1}\mathfrak{b}\mathfrak{a} = \mathfrak{b}^{-1}$, $\mathfrak{b}^{-1}\mathfrak{a}\mathfrak{b} = \mathfrak{a}^{-1}$ erfüllen.

Sei nun $\mathfrak{g}$ ein Element von unendlicher Ordnung aus $\mathfrak{G}$. Dann wird wieder $\mathfrak{a}^{-1}\mathfrak{g}\mathfrak{a} = \mathfrak{g}^{\pm 1}$.

Wäre zunächst $\mathfrak{a}^{-1}\mathfrak{g}\mathfrak{a} = \mathfrak{g}^{-1}$, so wird $\mathfrak{a}^{-1}\mathfrak{g}\mathfrak{a}\mathfrak{g}^{-1} = \mathfrak{g}^{-2}$ nach (7) des § 1. ein Element aus $\mathfrak{K}(\mathfrak{G})$ und also hätte $\mathfrak{g}^{-2}$ und also auch $\mathfrak{g}$ endliche Ordnung, was unmöglich ist. Also müßte $\mathfrak{a}^{-1}\mathfrak{g}\mathfrak{a} = \mathfrak{g}$ sein. Dann wird aber

$$\begin{aligned} \mathfrak{a}^{-1}\mathfrak{g}\mathfrak{b}\mathfrak{a} &= \mathfrak{g}\mathfrak{a}^{-1}\mathfrak{b}\mathfrak{a} = \mathfrak{g}\mathfrak{b}^{-1} \\ &= (\mathfrak{g}\mathfrak{b})^{\pm 1}, \end{aligned}$$

da auch $\mathfrak{g} \cdot \mathfrak{b}$ unendliche Ordnung haben muß. Hätte nämlich $\mathfrak{g}\mathfrak{b}$ endliche Ordnung, so hätte auch die Restklasse von $\mathfrak{g}$ mod $\mathfrak{K}(\mathfrak{G})$ endliche Ordnung und damit auch $\mathfrak{g}$ selbst, da ja alle Elemente aus $\mathfrak{K}(\mathfrak{G})$ endliche Ordnung haben.

Wäre nun zunächst $\mathfrak{g}\mathfrak{b}^{-1} = \mathfrak{g}\mathfrak{b}$, so wäre $\mathfrak{b}^2 = 1$, was den Eigenschaften der Quaternionengruppe widerspricht.

Also wird

$$\begin{gathered} \mathfrak{g}\mathfrak{b}^{-1} = (\mathfrak{g}\mathfrak{b})^{-1} = \mathfrak{b}^{-1}\mathfrak{g}^{-1}, \text{ d.h.} \\ \mathfrak{g} = \mathfrak{b}^{-1}\mathfrak{g}^{-1}\mathfrak{b} \text{ und } \mathfrak{g}^2 = \mathfrak{b}^{-1}\mathfrak{g}^{-1}\mathfrak{b}\mathfrak{g}. \end{gathered}$$

Wegen (7) des § 1. wäre also $\mathfrak{g}^2$ Element aus $\mathfrak{K}(\mathfrak{G})$, d.h. $\mathfrak{g}$ hätte endliche Ordnung.

Damit ist also unsere Annahme der Existenz von Elementen unendlicher Ordnung widerlegt und Satz 1 bewiesen.

Satz 2: $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *ist kein unendlicher Zyklus.*

Dies folgt für kommutatives $\mathfrak{K}(\mathfrak{G})$ aus (9), für nicht-kommutatives $\mathfrak{K}(\mathfrak{G})$ aus dem Satz 1, da Restklassen unendlicher Ordnung nur Elemente unendlicher Ordnung enthalten können.

(10) *Es sei $\mathfrak{A}$ ein kommutativer Normalteiler von $\{\mathfrak{A}, \mathfrak{g}\}$ und $\mathfrak{g}$ aus $\mathfrak{G}$. Weiter sei $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$ und $\{\mathfrak{A}, \mathfrak{g}\}/\mathfrak{A}$ endlich von der Ordnung $n > 0$ [also ein Zyklus von der Ordnung n]. Dann ist*

$$\begin{aligned} \mathfrak{C}[\{\mathfrak{A}, \mathfrak{g}\}] \leqq \{\mathfrak{g}^n\} \leqq \mathfrak{Z}[\{\mathfrak{A}, \mathfrak{g}\}] & \\ = \textit{Gesamtheit der Elemente } & \alpha(\mathfrak{a})\mathfrak{a}^{-1} \textit{ mit } \mathfrak{a} \textit{ aus } \mathfrak{A} \\ & \textit{und } \alpha(\mathfrak{a}) = \mathfrak{g}^{-1}\mathfrak{a}\mathfrak{g}. \end{aligned}$$

Die Ordnung von $\mathfrak{C}[\{\mathfrak{A}, \mathfrak{g}\}]$ ist gleich der Ordnung von α, also ein Teiler von n.

$\mathfrak{g}^i$ ist Element von $\mathfrak{Z}[\{\mathfrak{A}, \mathfrak{g}\}] \leqq \mathfrak{K}[\{\mathfrak{A}, \mathfrak{g}\}]$, wenn nur $\alpha^i = 1$ ist.

Nach Voraussetzung ist $\mathfrak{g}^n = \mathfrak{c}$ Element aus $\mathfrak{A}$, also mit $\mathfrak{g}$ und mit jedem Element aus $\mathfrak{A}$ vertauschbar, also Element aus $\mathfrak{Z}[\{\mathfrak{A}, \mathfrak{g}\}]$.

Ist $\mathfrak{H}$ die Gesamtheit der Elemente $\alpha(\mathfrak{a})\mathfrak{a}^{-1}$ mit $\mathfrak{a}$ aus $\mathfrak{A}$, so ist $\mathfrak{H} \leqq \{\mathfrak{c}\}$, da $\alpha(\mathfrak{a})\mathfrak{a}^{-1} = \mathfrak{g}^{-1}\mathfrak{a}\mathfrak{g}\mathfrak{a}^{-1} = \mathfrak{g}^{l}$, also $\mathfrak{g}^{l}$ in $\mathfrak{A}$ wegen (7), § 1., also $\mathfrak{g}^{l} = \mathfrak{c}^{s}$ ist. $\mathfrak{H}$ ist also zyklisch; da $\alpha(\mathfrak{c}) = \mathfrak{c}$ ist, da weiter $\alpha(\mathfrak{a}) = \mathfrak{h}\mathfrak{a}$ für jedes $\mathfrak{a}$ aus $\mathfrak{A}$ und geeignetes $\mathfrak{h}$ aus $\mathfrak{H}$ ist, da also $\alpha^{i}(\mathfrak{a}) = \mathfrak{h}^{i}\mathfrak{a}$ wird und da schließlich jedes $\mathfrak{h}$ aus $\mathfrak{H}$ auftritt, so wird die Ordnung von α gleich der Ordnung von $\mathfrak{H}$. Da $\mathfrak{g}^{-i}\mathfrak{a}\mathfrak{g}^{i}\mathfrak{a}^{-1} = \alpha^{i}(\mathfrak{a})\mathfrak{a}^{-1} = \mathfrak{h}^{i}$ ist, so ist also $\mathfrak{H} = \mathfrak{C}[\{\mathfrak{A}, \mathfrak{g}\}]$, und damit sind alle Behauptungen bewiesen.

Satz 3: *Enthält* $\mathfrak{K}(\mathfrak{G})$ *Elemente unendlicher Ordnung, so ist* $\mathfrak{Z}(\mathfrak{G}) = \mathfrak{K}(\mathfrak{G})$.

Beweis: Enthält $\mathfrak{K}(\mathfrak{G})$ Elemente unendlicher Ordnung, so ist $\mathfrak{K}(\mathfrak{G})$ nach Satz 1. kommutativ. Sei $\mathfrak{u}$ ein Element unendlicher Ordnung aus $\mathfrak{K}(\mathfrak{G})$ und $\mathfrak{g}$ aus $\mathfrak{G}$ beliebig. Ist $\mathfrak{g}$ ein Element unendlicher Ordnung, so ist es nach (9) mit $\mathfrak{K}(\mathfrak{G})$ vertauschbar. Ist aber $\mathfrak{g}$ ein Element endlicher Ordnung, so ist $\mathfrak{K}(\mathfrak{G})$ ein kommutativer Normalteiler von $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\mathfrak{u}\}$ und $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\mathfrak{u}\}/\mathfrak{K}(\mathfrak{G})$ endlich, etwa von der Ordnung $n > 0$. Nach (10) wird also wegen $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\} = \{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\mathfrak{u}\}$ und $\alpha(\mathfrak{a}) = \mathfrak{g}^{-1}\mathfrak{a}\mathfrak{g} = (\mathfrak{g}\mathfrak{u})^{-1}\mathfrak{a}(\mathfrak{g}\mathfrak{u})$ und $(\mathfrak{g}\mathfrak{u})^{n} = \mathfrak{g}^{n}\prod_{j=0}^{n-1}\alpha^{j}(\mathfrak{u})$ sowohl

$$\mathfrak{C}[\{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\}] \leqq \{\mathfrak{g}^{n}\}$$

als auch

$$= \mathfrak{C}[\{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\mathfrak{u}\}] \leqq \{\mathfrak{g}^{n}\prod_{j=0}^{n-1}\alpha^{j}(\mathfrak{u})\}.$$

Also gibt es ganze Zahlen v und s mit

$$\mathfrak{g}^{nv} = \mathfrak{g}^{ns} \cdot \prod_{j=0}^{n-1}\alpha^{j}(\mathfrak{u}^{s}) = \mathfrak{c} = \text{erzeugendes Element von } \mathfrak{C}[\{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\}],$$

und es wird

$$\mathfrak{g}^{n(v-s)} = \prod_{j=0}^{n-1}\alpha^{j}(\mathfrak{u}^{s}) = \mathfrak{u}^{sn}\mathfrak{c}^{xs\frac{n(n-1)}{2}},$$

wo x aus $\alpha(\mathfrak{u})\mathfrak{u}^{-1} = \mathfrak{c}^{x}$ bestimmt ist. Also wird

$$\mathfrak{u}^{sn} = \mathfrak{g}^{n\left(v-s-vxs\frac{n(n-1)}{2}\right)}.$$

Da die Ordnung von $\mathfrak{c}$ gleich der Ordnung von α, also endlich ist, und da $\mathfrak{g}^{nv} = \mathfrak{c}$ ist, so ist auch die Ordnung von $\mathfrak{g}$ endlich. Da die Ordnung von $\mathfrak{u}$ unendlich ist, so ist also $\{\mathfrak{u}\} \cap \{\mathfrak{g}\} = \{1\}$ und also $\mathfrak{u}^{sn} = 1$, also $sn = 0$. Ist $n = 0$, so ist $\mathfrak{g}$ Element von $\mathfrak{K}(\mathfrak{G})$, also, da $\mathfrak{K}(\mathfrak{G})$ kommutativ ist, gewiß mit allen Elementen von $\mathfrak{K}(\mathfrak{G})$ vertauschbar. Ist $n > 0$, so wird $s = 0$, und also

$\mathfrak{c} = \mathfrak{g}^{nv} = 1$, also $\mathfrak{C}[\{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\}] = \{1\}$, d.h. $\mathfrak{g}$ ist mit allen Elementen von $\mathfrak{K}(\mathfrak{G})$ vertauschbar.

Also ist $\mathfrak{K}(\mathfrak{G}) = \mathfrak{Z}(\mathfrak{G})$.

Bemerkung: Aus dem Satz folgt insbesondere, daß $\mathfrak{Z}(\mathfrak{G}) = \mathfrak{K}(\mathfrak{G})$ ist, wenn $\mathfrak{G}$ nur Elemente unendlicher Ordnung enthält. Z.B. besteht also der Kern einer freien Gruppe nur aus der Gruppeneins.

Folgerung: *Ist* $\mathfrak{K}(\mathfrak{G}) > \mathfrak{Z}(\mathfrak{G})$, *so ist* $\mathfrak{K}(\mathfrak{G})$ *direktes Produkt primärer Gruppen.*

Dies folgt aus (6) des § 1., da $\mathfrak{K}(\mathfrak{G})$ nach Satz 3. keine Elemente unendlicher Ordnung enthalten kann.

§ 3.

Die Darstellung einer Gruppe als direktes Produkt von zu verschiedenen Primzahlen gehörigen Primärgruppen [die dann die Primärkomponenten sind] ist, wenn sie überhaupt möglich ist, abgesehen von der Reihenfolge und von Faktoren, die nur aus der Gruppeneins bestehen, eindeutig.

Satz 4: *Ist* $\mathfrak{G}$ *als direktes Produkt seiner Primärkomponenten darstellbar, d.h.*

$$\mathfrak{G} = \mathfrak{G}_2 \times \mathfrak{G}_3 \times \ldots \times \mathfrak{G}_p \times \ldots,$$

so ist

$$\mathfrak{K}(\mathfrak{G}) = \mathfrak{K}(\mathfrak{G}_2) \times \mathfrak{K}(\mathfrak{G}_3) \times \ldots \times \mathfrak{K}(\mathfrak{G}_p) \times \ldots .$$

Beweis: Wir beweisen zunächst:

$$\mathfrak{K}(\mathfrak{G}_p) = \mathfrak{K}(\mathfrak{G}) \cap \mathfrak{G}_p. \tag{11}$$

Wegen (4) des § 1. gilt nämlich sicher einerseits:

$$\mathfrak{K}(\mathfrak{G}_p) \geqq \mathfrak{K}(\mathfrak{G}) \cap \mathfrak{G}_p. \tag{11a}$$

Sei umgekehrt $\mathfrak{k}$ ein Element aus $\mathfrak{K}(\mathfrak{G}_p)$ und $\mathfrak{g}$ ein beliebiges Element aus $\mathfrak{G}$. Dann läßt sich $\mathfrak{g}$ auf genau eine Weise auf die Form $\mathfrak{g} = \mathfrak{p} \cdot \mathfrak{q}$ bringen, wo $\mathfrak{p}$ aus $\mathfrak{G}_p$, $\mathfrak{q}$ aus $\prod\limits_{q \neq p} \mathfrak{G}_q$ ist. Dann wird, da $\mathfrak{k}$ aus $\mathfrak{K}(\mathfrak{G}_p) \leqq \mathfrak{G}_p$ ist,

$$\mathfrak{k}^{-1}\mathfrak{g}\,\mathfrak{k} = \mathfrak{k}^{-1}\mathfrak{p}\,\mathfrak{k}\mathfrak{q} = \mathfrak{p}^{l}\mathfrak{q}.$$

Sei etwa p^m die Ordnung von $\mathfrak{p}$, h die von $\mathfrak{q}$; dann sind p^m und h teilerfremd und es gibt also ganze Zahlen r und s, so daß $l - 1 = r \cdot p^m + s \cdot h$ wird.

Es wird also

$$\mathfrak{k}^{-1}\mathfrak{g}\,\mathfrak{k} = \mathfrak{p}^{l}\mathfrak{q} = \mathfrak{p}^{1+rp^m+sh}\mathfrak{q} =$$
$$= \mathfrak{p}^{1+sh}\mathfrak{q}^{1+sh} = (\mathfrak{p}\mathfrak{q})^{1+sh} = \mathfrak{g}^{1+sh},$$

woraus wegen (8) des § 1. folgt, daß $\mathfrak{k}$ auch in $\mathfrak{K}(\mathfrak{G})$ enthalten ist, woraus $\mathfrak{K}(\mathfrak{G}_p) \leqq \mathfrak{K}(\mathfrak{G}) \cap \mathfrak{G}_p$ und damit wegen (11a) auch (11) folgt.

Aus (11) folgt, daß $\mathfrak{K}(\mathfrak{G}) \geqq \mathfrak{K}(\mathfrak{G}_p)$ und also auch

$$\mathfrak{K}(\mathfrak{G}) \geqq \mathfrak{K}(\mathfrak{G}_2) \times \mathfrak{K}(\mathfrak{G}_3) \times \ldots \times \mathfrak{K}(\mathfrak{G}_p) \times \ldots \text{ ist.}$$

Ist weiter $\mathfrak{k}$ aus $\mathfrak{K}(\mathfrak{G})$ beliebig, so kann man auch $\mathfrak{k}$ auf die Form $\mathfrak{k} = \mathfrak{p}\mathfrak{q}$ mit $\mathfrak{p}$ aus $\mathfrak{G}_p$, $\mathfrak{q}$ aus $\prod\limits_{p \neq q} \mathfrak{G}_q$ bringen. Da $\mathfrak{p}$ und $\mathfrak{q}$ teilerfremde Ordnung haben, so gibt es eine ganze Zahl s mit $\mathfrak{k}^s = \mathfrak{p}$; also ist $\mathfrak{p}$ in $\mathfrak{K}(\mathfrak{G})$ und wegen (11) in $\mathfrak{K}(\mathfrak{G}_p)$ enthalten, womit der Satz vollständig bewiesen ist.

Bemerkung: *Der Satz 4. gilt nicht mehr für beliebige direkte Produktzerlegung einer Gruppe,* wie folgendes *Beispiel* zeigt: $\mathfrak{Q}$ sei die Quaternionengruppe, $\mathfrak{U}$ ein unendlicher Zyklus und $\mathfrak{G} = \mathfrak{U} \times \mathfrak{Q}$. Dann ist $\mathfrak{K}(\mathfrak{U}) \times \mathfrak{K}(\mathfrak{Q}) = \mathfrak{U} \times \mathfrak{Q} = \mathfrak{G}$; dagegen ist der Kern von $\mathfrak{G}$ wegen Satz 1. des § 2. sicher nicht hamiltonsch, also eine echte Untergruppe von $\mathfrak{G}$.

Dagegen gilt bekanntlich sowohl

$$\mathfrak{Z}(\mathfrak{A} \times \mathfrak{B}) = \mathfrak{Z}(\mathfrak{A}) \times \mathfrak{Z}(\mathfrak{B}) \text{ als auch } \mathfrak{C}(\mathfrak{A} \times \mathfrak{B}) = \mathfrak{C}(\mathfrak{A}) \times \mathfrak{C}(\mathfrak{B}).$$

Später werden wir häufig von folgendem Lemma Gebrauch zu machen haben:

Lemma: *Enthält $\mathfrak{G}$ nur Elemente endlicher Ordnung und ist $\mathfrak{C}(\mathfrak{G}) \leqq \mathfrak{Z}(\mathfrak{G})$, d.h. $\mathfrak{G}/\mathfrak{Z}(\mathfrak{G})$ kommutativ, so ist $\mathfrak{G}$ als direktes Produkt primärer Gruppen darstellbar* [3]).

Dem **Beweis** schicken wir einige Hilfssätze voraus:

(12) *Sind die Voraussetzungen des Lemma erfüllt, ist* $\mathfrak{a}^g = 1$, $\mathfrak{c} = \mathfrak{a}\mathfrak{b}\mathfrak{a}^{-1}\mathfrak{b}^{-1}$, *so ist auch* $\mathfrak{c}^g = 1$.

Setzen wir nämlich $\alpha(\mathfrak{x}) = \mathfrak{a}\mathfrak{x}\mathfrak{a}^{-1}$, so wird $\alpha(\mathfrak{b}) = \mathfrak{c}\mathfrak{b}$, $\alpha(\mathfrak{c}) = \mathfrak{c}$, da $\mathfrak{c}$ in $\mathfrak{C}(\mathfrak{G}) \leqq \mathfrak{Z}(\mathfrak{G})$ enthalten ist. Also wird $\alpha^i(\mathfrak{b}) = \mathfrak{c}^i\mathfrak{b}$ und schließlich:

$$\mathfrak{b} = \mathfrak{a}^g\mathfrak{b}\mathfrak{a}^{-g} = \alpha^g(\mathfrak{b}) = \mathfrak{c}^g\mathfrak{b}, \text{ d.h. } \mathfrak{c}^g = 1.$$

(12a). *Sind die Voraussetzungen des Lemma erfüllt, ist* $\mathfrak{a}^a = \mathfrak{b}^b = 1$, *$(a, b)$ der g. g. T. von a und b und schließlich* $\mathfrak{c} = \mathfrak{a}\mathfrak{b}\mathfrak{a}^{-1}\mathfrak{b}^{-1}$, *so ist* $\mathfrak{c}^{(a,b)} = 1$.

Dies folgt aus (12), wenn man noch bedenkt, daß

$$\mathfrak{c}^{-1} = \mathfrak{b}\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{a}^{-1} \text{ ist.}$$

---

[3]) Ist $\mathfrak{G}$ endlich, so ist unser Lemma ein Spezialfall eines Satzes von Burnside; vergl. BURNSIDE, Theory of groups of finite order, 2nd ed. [Cambridge (1911), 166].

(12b) *Sind die Voraussetzungen des Lemma erfüllt, so ist* $\mathfrak{a}$ *mit* $\mathfrak{b}$ *vertauschbar, wenn* $\mathfrak{a}$ *und* $\mathfrak{b}$ *teilerfremde Ordnungen haben.*
Denn nach (12a) wird dann $\mathfrak{a}\mathfrak{b}\mathfrak{a}^{-1}\mathfrak{b}^{-1} = 1$.

(13) $(\mathfrak{a}\mathfrak{b})^i = \mathfrak{c}_i(\mathfrak{a}\mathfrak{b})\,\mathfrak{a}^i\mathfrak{b}^i$,

wo $\mathfrak{c}_i(\mathfrak{a}\mathfrak{b}) = \prod_{j=1}^{i-1} [(\mathfrak{a}^j\mathfrak{b}^j\mathfrak{a}^{-j}\mathfrak{b}^{-j})(\mathfrak{b}^j\mathfrak{a}^{j+1}\mathfrak{b}^{-j}\mathfrak{a}^{-(j+1)})]$ *ist.*

Dies ist für $i = 1$ trivial. Ist es für i wahr, so haben wir es für $i + 1$ nachzuweisen. Es wird

$$\begin{aligned}(\mathfrak{a}\mathfrak{b})^{i+1} &= (\mathfrak{a}\mathfrak{b})^i\mathfrak{a}\mathfrak{b} = \mathfrak{c}_i(\mathfrak{a}\mathfrak{b}) \cdot \mathfrak{a}^i\mathfrak{b}^i \cdot \mathfrak{a}\mathfrak{b} = \\ &= \mathfrak{c}_i(\mathfrak{a}\mathfrak{b}) \cdot [(\mathfrak{a}^i\mathfrak{b}^i\mathfrak{a}^{-i}\mathfrak{b}^{-i})(\mathfrak{b}^i\mathfrak{a}^{i+1}\mathfrak{b}^{-i}\mathfrak{a}^{-(i+1)})]\,\mathfrak{a}^{i+1}\mathfrak{b}^{i+1} \\ &= \mathfrak{c}_{i+1}(\mathfrak{a}\mathfrak{b})\,\mathfrak{a}^{i+1}\mathfrak{b}^{i+1}.\end{aligned}$$

Beweis des Lemma: Sind $\mathfrak{a}$ und $\mathfrak{b}$ zwei Elemente aus $\mathfrak{G}_p$, so gibt es ein $n > 0$, so daß $\mathfrak{a}^{p^n} = \mathfrak{b}^{p^n} = 1$ ist. Dann wird $(\mathfrak{a}\mathfrak{b})^{p^n} = \mathfrak{c}_{p^n}(\mathfrak{a}\mathfrak{b})$ wegen (13), und da $\mathfrak{Z}(\mathfrak{G}) \geqq \mathfrak{C}(\mathfrak{G})$, also $\mathfrak{C}(\mathfrak{G})$ kommutativ ist, so folgt aus (12), daß $(\mathfrak{a}\mathfrak{b})^{p^{2n}} = \mathfrak{c}_{p^n}^{p^n}(\mathfrak{a}\mathfrak{b}) = 1$ ist.

Also ist jedes $\mathfrak{G}_p$ eine Untergruppe von $\mathfrak{G}$, also eine charakteristische Untergruppe, also ein Normalteiler von $\mathfrak{G}$.

Wegen (12b) hat $\mathfrak{G}_p$ mit der von den $\mathfrak{G}_q$ mit $q \neq p$ erzeugten Untergruppe von $\mathfrak{G}$ nur die Gruppeneins gemein. Da sich schließlich jedes Element als Produkt von Elementen aus $\mathfrak{G}_2$, $\mathfrak{G}_3, \ldots, \mathfrak{G}_p, \ldots$ darstellen läßt, so folgt:

$$\mathfrak{G} = \mathfrak{G}_2 \times \mathfrak{G}_3 \times \ldots \times \mathfrak{G}_p \times \ldots, \text{ wie behauptet.}$$

§ 4.

Satz 5: *Ist* $\mathfrak{K}(\mathfrak{G})$ *hamiltonsch und* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *zyklisch, so ist* $\mathfrak{G} = \mathfrak{G}_2 \times \mathfrak{U}$, *wo* $\mathfrak{U}$ *nur Elemente ungerader Ordnung enthält,* $\mathfrak{K}(\mathfrak{G}) = \mathfrak{G}_2 \times \mathfrak{K}(\mathfrak{U})$ *und* $\mathfrak{G}_2 = \mathfrak{K}(\mathfrak{G}_2)$.

Den **Beweis** führen wir in mehreren Schritten:

(14) *Ist* $\mathfrak{H}$ *eine hamiltonsche Gruppe, so ist* $\mathfrak{C}(\mathfrak{H}) = \mathfrak{Z}(\mathfrak{Q})$, *wo* $\mathfrak{Q}$ *eine beliebige, als direkter Faktor von* $\mathfrak{H}$ *auftretende Quaternionengruppe ist.*

Gemäß Fußnote [1]) ist $\mathfrak{H} = \mathfrak{Q} \times \mathfrak{A}_2 \times \mathfrak{A}_u$, wo $\mathfrak{A}_2$ nur Elemente der Ordnung 2, $\mathfrak{A}_u$ nur solche ungerader Ordnung enthält und $\mathfrak{A}_2 \times \mathfrak{A}_u$ kommutativ ist. Dann ist $\mathfrak{Z}(\mathfrak{H}) = \mathfrak{Z}(\mathfrak{Q}) \times \mathfrak{A}_2 \times \mathfrak{A}_u$ und $\mathfrak{H}/\mathfrak{C}(\mathfrak{Q})$ isomorph $\mathfrak{Q}/\mathfrak{C}(\mathfrak{Q}) \times \mathfrak{A}_2 \times \mathfrak{A}_u$, also $\mathfrak{C}(\mathfrak{Q}) = \mathfrak{C}(\mathfrak{H})$, woraus wegen $\mathfrak{C}(\mathfrak{Q}) = \mathfrak{Z}(\mathfrak{Q})$ unsere Behauptung folgt.

Wegen Satz 1, § 2. ist jedes Element aus $\mathfrak{G}$ von endlicher Ordnung und $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ ein endlicher Zyklus. Er habe die Ordnung $n > 0$. Ist $\mathfrak{r}$ irgend ein Repräsentant irgendeiner erzeugenden Restklasse von $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$, so ist $\mathfrak{r}^n = \mathfrak{e}$ Element von $\mathfrak{K}(\mathfrak{G})$.

Wir unterscheiden drei Fälle, je nachdem

I. $\mathfrak{e}$ *in* $\mathfrak{C}[\mathfrak{K}(\mathfrak{G})]$,

II. $\mathfrak{e}$ *in* $\mathfrak{Z}[\mathfrak{K}(\mathfrak{G})]$, *aber nicht in* $\mathfrak{C}[\mathfrak{K}(\mathfrak{G})]$,

III. $\mathfrak{e}$ *in* $\mathfrak{K}(\mathfrak{G})$, *aber nicht in* $\mathfrak{Z}[\mathfrak{K}(\mathfrak{G})]$

enthalten ist.

ad I. Wir bemerken zunächst, daß $\mathfrak{C}[\mathfrak{K}(\mathfrak{G})]$ wegen (14) ein Zyklus der Ordnung 2 ist und unterscheiden demgemäß zwei Fälle, je nachdem $\mathfrak{e} = 1$ oder $\neq 1$ ist.

I 1. $\mathfrak{e} = 1$.

Ist dann $\mathfrak{k}$ aus $\mathfrak{K}(\mathfrak{G})$ beliebig, so ist

$\mathfrak{k}^{-1}\mathfrak{r}\mathfrak{k}\mathfrak{r}^{-1} = \mathfrak{r}^{x}$ Element aus $\mathfrak{K}(\mathfrak{G})$ wegen (7), § 1. und also $= 1$, d.h. $\mathfrak{r}$ ist in $\mathfrak{Z}(\mathfrak{G})$, also in $\mathfrak{K}(\mathfrak{G})$ enthalten, und mithin $\mathfrak{G} = \mathfrak{K}(\mathfrak{G})$.

I 2. $\mathfrak{e} \neq 1$.

Sei dann $\mathfrak{Q}$ eine Quaternionengruppe, die direkter Faktor von $\mathfrak{K}(\mathfrak{G})$ ist. Dann kann man zwei Erzeugende $\mathfrak{a}$ und $\mathfrak{b}$ von $\mathfrak{Q}$ in üblicher Weise auswählen, und wegen (14) wird $\mathfrak{a}^2 = \mathfrak{b}^2 = \mathfrak{e}$.

Wegen (7) des § 1. gibt es für jedes $\mathfrak{k}$ aus $\mathfrak{K}(\mathfrak{G})$ ein $l = l(\mathfrak{k})$, so daß $\mathfrak{r}^{-1}\mathfrak{k}\mathfrak{r}\mathfrak{k}^{-1} = \mathfrak{r}^{l}$ ein Element aus $\mathfrak{K}(\mathfrak{G})$ wird. Also muß $l \equiv 0 \bmod n$ sein, und wir erhalten:

$$\mathfrak{r}^{-1}\mathfrak{k}\mathfrak{r} = \mathfrak{k}\mathfrak{e}^{\frac{l}{n}}.$$

Da weiter $\mathfrak{r}^{-1}\mathfrak{e}\,\mathfrak{r} = \mathfrak{r}^{-1}\mathfrak{r}^{n}\mathfrak{r} = \mathfrak{r}^{n} = \mathfrak{e}$ ist, so folgt

$$\mathfrak{r}^{-i}\mathfrak{k}\mathfrak{r}^{i} = \mathfrak{k}\mathfrak{e}^{i\frac{l}{n}}.$$

Wegen $\mathfrak{e}^2 = 1$ wird also insbesondere $\mathfrak{r}^{-2}\mathfrak{k}\mathfrak{r}^2 = \mathfrak{k}$, d.h. $\mathfrak{r}^2$ ist Element aus $\mathfrak{Z}(\mathfrak{G}) \leq \mathfrak{K}(\mathfrak{G})$, und also $n = 1$ oder $= 2$.

Wäre $n = 2$, so wäre insbesondere

$$\mathfrak{r}^{-1}\mathfrak{a}\mathfrak{r} = \mathfrak{a}\mathfrak{e}^{l(\mathfrak{a})\cdot 2^{-1}}, \qquad \mathfrak{r}^{-1}\mathfrak{b}\mathfrak{r} = \mathfrak{b}\mathfrak{e}^{l(\mathfrak{b})\cdot 2^{-1}},$$

also $$\mathfrak{r}^{-1}\mathfrak{a}\mathfrak{b}\mathfrak{r} = \mathfrak{a}\mathfrak{e}^{l(\mathfrak{a})\cdot 2^{-1}}\mathfrak{b}\mathfrak{e}^{l(\mathfrak{b})\cdot 2^{-1}} = \mathfrak{a}\mathfrak{b}\mathfrak{e}^{[l(\mathfrak{a})+l(\mathfrak{b})]\cdot 2^{-1}},$$

da $\mathfrak{e} = \mathfrak{a}^2 = \mathfrak{b}^2$ ist. Da $\mathfrak{e}^2 = 1$ ist, ist von den drei Elementen

$$\mathfrak{e}^{l(\mathfrak{a})\cdot 2^{-1}}, \quad \mathfrak{e}^{l(\mathfrak{b})\cdot 2^{-1}}, \quad \mathfrak{e}^{l(\mathfrak{a}\mathfrak{b})\cdot 2^{-1}} = \mathfrak{e}^{[l(\mathfrak{a})+l(\mathfrak{b})]\cdot 2^{-1}}$$

wenigstens eines die Gruppeneins, und wir können o. B. d. A. annehmen, daß $\mathfrak{e}^{l(\mathfrak{a})\cdot 2^{-1}} = 1$ ist. Dann setzen wir $\mathfrak{r}^* = \mathfrak{r}\mathfrak{a}$ und es wird $\mathfrak{r}^{*2} = \mathfrak{r}\mathfrak{a}\mathfrak{r}\mathfrak{a} = \mathfrak{r}^2\mathfrak{a}^2 = 1$, d. h. wir haben diesen Fall auf den Fall I 1. zurückgeführt und es ist $\mathfrak{G} = \mathfrak{K}(\mathfrak{G})$, $n = 1$, was ausgeschlossen war.

Damit haben wir also gefunden:

(15) *Ist* $\mathfrak{K}(\mathfrak{G})$ *hamiltonsch,* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *zyklisch und* $\mathfrak{e}$ *in* $\mathfrak{C}[\mathfrak{K}(\mathfrak{G})]$ *enthalten, so ist* $\mathfrak{G} = \mathfrak{K}(\mathfrak{G})$.

ad II. $\mathfrak{e}$ *ist in* $\mathfrak{Z}[\mathfrak{K}(\mathfrak{G})]$, *aber nicht in* $\mathfrak{C}[\mathfrak{K}(\mathfrak{G})]$ *enthalten.*

Wieder ist $\mathfrak{x}^{-1}\mathfrak{e}\,\mathfrak{x} = \mathfrak{e}$ und also $\mathfrak{x}^{-i}\mathfrak{k}\,\mathfrak{x}^{i} = \mathfrak{k}\mathfrak{e}^{il(\mathfrak{k})n^{-1}}$, insbesondere also $\mathfrak{k} = \mathfrak{e}^{-1}\mathfrak{k}\mathfrak{e} = \mathfrak{x}^{-n}\mathfrak{k}\,\mathfrak{x}^{n} = \mathfrak{k}\mathfrak{e}^{l(\mathfrak{k})}$, d. h. $\mathfrak{e}^{l(\mathfrak{k})} = 1$ für jedes $\mathfrak{k}$ aus $\mathfrak{K}(\mathfrak{G})$.

Ist weiter r die Ordnung von $\mathfrak{e}$, so erhalten wir

$$\mathfrak{x}^{-r}\mathfrak{k}\,\mathfrak{x}^{r} = \mathfrak{k}\mathfrak{e}^{rl(\mathfrak{k})n^{-1}} = \mathfrak{k}$$

für jedes $\mathfrak{k}$ aus $\mathfrak{K}(\mathfrak{G})$, d. h. $\mathfrak{x}^{r}$ ist in $\mathfrak{Z}(\mathfrak{G})$, also in $\mathfrak{K}(\mathfrak{G})$ enthalten. *Also ist n ein Teiler von r.*

Da schließlich Elemente aus dem Zentrum einer hamiltonschen Gruppe nie eine durch 4 teilbare Ordnung haben können, so ist

r und also auch n nicht durch 4 teilbar.

Seien wieder $\mathfrak{a}$ und $\mathfrak{b}$ Erzeugende einer in $\mathfrak{K}(\mathfrak{G})$ enthaltenen Quaternionengruppe. Dann wird

$$\mathfrak{x}^{-1}\mathfrak{a}\,\mathfrak{x} = \mathfrak{a}\mathfrak{e}^{l(\mathfrak{a})n^{-1}}, \quad \mathfrak{x}^{-1}\mathfrak{b}\,\mathfrak{x} = \mathfrak{b}\mathfrak{e}^{l(\mathfrak{b})n^{-1}}$$

und also $\quad \mathfrak{x}^{-1}\mathfrak{a}\mathfrak{b}\,\mathfrak{x} = \mathfrak{a}\mathfrak{b}\mathfrak{e}^{[l(\mathfrak{a})+l(\mathfrak{b})]n^{-1}}$, da ja $\mathfrak{e}$ aus $\mathfrak{Z}[\mathfrak{K}(\mathfrak{G})]$ ist.

Von den drei hier auftretenden Potenzen von $\mathfrak{e}$ ist also mindestens eine gerade; o. B. d. A. sei $\dfrac{l(\mathfrak{a})}{n} \equiv 0 \bmod 2$. Dann hat also $\mathfrak{e}^{l(\mathfrak{a})\cdot n^{-1}}$ ungerade Ordnung. Weiter ist $1 = \mathfrak{x}^{-1}\mathfrak{a}^{4}\,\mathfrak{x} = \mathfrak{a}^{4}\mathfrak{e}^{4l(\mathfrak{a})n^{-1}}$, also $\mathfrak{e}^{4l(\mathfrak{a})n^{-1}} = 1$, also $\mathfrak{e}^{l(\mathfrak{a})n^{-1}} = 1$. Insbesondere ist also $\mathfrak{x}$ mit $\mathfrak{a}^{2}$ vertauschbar. Da $\mathfrak{x}$ auch mit $\mathfrak{e}$ vertauschbar ist, $\mathfrak{a}^{2}$ und $\mathfrak{e}$ beide in $\mathfrak{Z}[\mathfrak{K}(\mathfrak{G})]$ liegen, so liegen $\mathfrak{a}^{2}$ und $\mathfrak{e}$ sogar in $\mathfrak{Z}(\mathfrak{G})$, und es gilt: $\mathfrak{C}(\mathfrak{G}) \leqq \mathfrak{Z}(\mathfrak{G})$.

Nach dem Lemma des § 3. können wir also $\mathfrak{G}$ in Primärfaktoren zerlegen:

$\mathfrak{G} = \mathfrak{G}_2 \times \mathfrak{U}$, wo $\mathfrak{U}$ das Produkt aller zu ungeraden Primzahlen gehörenden Primärfaktoren ist.

Wegen Satz 4. des § 3. wird

$$\mathfrak{K}(\mathfrak{G}) = \mathfrak{K}(\mathfrak{G}_2) \times \mathfrak{K}(\mathfrak{U}),$$

und wegen (11) des § 3. wird schließlich:

$$\mathfrak{G}/\mathfrak{K}(\mathfrak{G}) \text{ isomorph } \mathfrak{G}_2/\mathfrak{K}(\mathfrak{G}_2) \times \mathfrak{U}/\mathfrak{K}(\mathfrak{U}).$$

Mithin ist $\mathfrak{G}_2/\mathfrak{K}(\mathfrak{G}_2)$ ein Zyklus und, da n, wie oben gezeigt, nicht durch 4 teilbar ist, so hat $\mathfrak{G}_2/\mathfrak{K}(\mathfrak{G}_2)$ entweder die Ordnung 1 oder die Ordnung 2.

Angenommen, $\mathfrak{G}_2/\mathfrak{K}(\mathfrak{G}_2)$ habe die Ordnung 2. Dies tritt nach dem eben gezeigten dann und nur dann ein, wenn n gerade ist: $n = 2m$. Da n oben als Teiler von r erwiesen ist, so ist auch r gerade: $r = 2s$, und s ungerade.

Dann ist $\mathfrak{r}_2 = \mathfrak{r}^{ms}$ Repräsentant einer erzeugenden Restklasse von $\mathfrak{G}_2/\mathfrak{K}(\mathfrak{G}_2)$, da $\mathfrak{r}$ die Ordnung $nr = 4ms$, also $\mathfrak{r}_2$ die Ordnung 4 hat und $m \cdot s$ ungerade ist, und da schließlich r^m und $\mathfrak{r}_2$ in derselben Restklasse der Ordnung 2 von $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ liegen.

Es ist $\mathfrak{r}_2^2 = \mathfrak{r}^{2ms} = \mathfrak{e}^s = \mathfrak{e}_2$ ein Element der Ordnung 2, und $\mathfrak{e}_2$ wegen (15) nicht aus $\mathfrak{C}[\mathfrak{K}(\mathfrak{G})] = \mathfrak{C}[\mathfrak{K}(\mathfrak{G}_2)]$.

Es ist $\mathfrak{K}(\mathfrak{G}_2) = \mathfrak{Q} \times \mathfrak{A}$, wo $\mathfrak{Q}$ eine von den Elementen $\mathfrak{a}$ und $\mathfrak{b}$ erzeugte Quaternionengruppe ist, und wo $\mathfrak{A}$ sich so auswählen läßt, daß $\mathfrak{e}_2$ Element von $\mathfrak{A}$ ist, da ja $\mathfrak{Z}[\mathfrak{K}(\mathfrak{G}_2)]$ nur Elemente der Ordnung 2 enthält und $\mathfrak{e}_2$ nicht in $\mathfrak{Z}(\mathfrak{Q})$ enthalten ist. Wir zeigen:

$\mathfrak{r}_2$ *ist mit* $\mathfrak{a}$ *und* $\mathfrak{b}$ *vertauschbar.*

Es wäre nämlich sonst etwa

$$\mathfrak{r}_2^{-1}\,\mathfrak{a}\,\mathfrak{r}_2 = \mathfrak{a}\,\mathfrak{e}_2.$$

Dann wird

$$\begin{aligned} \mathfrak{a}^{-1}\,\mathfrak{r}_2\,\mathfrak{a}^2 &= \mathfrak{r}_2\,\mathfrak{a}^{-1}\mathfrak{e}_2\,\mathfrak{a}^2 = \mathfrak{r}_2\,\mathfrak{a}\,\mathfrak{e}_2 \\ &= \mathfrak{a}^{-1}(\mathfrak{r}_2\,\mathfrak{a})\,\mathfrak{a} = (\mathfrak{r}_2\,\mathfrak{a})^t \end{aligned}$$

für geeignetes t, da ja $\mathfrak{a}$ aus $\mathfrak{K}(\mathfrak{G}_2)$ ist. Also wird:

$$\begin{aligned} \mathfrak{r}_2\,\mathfrak{a}\,\mathfrak{e}_2 &= \mathfrak{r}_2^t\,\mathfrak{a}^t\mathfrak{e}_2^{\frac{t(t-1)}{2}}, \quad \text{also } t = 1 + 2t' \\ &= \mathfrak{r}_2\,\mathfrak{e}_2^{t'}\,\mathfrak{a}^{1+2t'}\mathfrak{e}_2^{(1+2t')t'}, \quad \text{d.h.} \\ \mathfrak{a}\,\mathfrak{e}_2 &= \mathfrak{a}^{1+2t'}\mathfrak{e}_2^{2t'+2t'^2} = \mathfrak{a}^{1+2t'} \quad \text{wegen } \mathfrak{e}_2^2 = 1, \text{ d. h.} \\ \mathfrak{e}_2 &= \mathfrak{a}^{2t'}, \end{aligned}$$

was unmöglich ist, da $\mathfrak{e}_2$ nicht in $\mathfrak{C}[\mathfrak{K}(\mathfrak{G})] = \mathfrak{C}(\mathfrak{Q}) = \mathfrak{Z}(\mathfrak{Q})$ enthalten ist, woraus unsere Behauptung folgt.

Wir zeigen weiter:

$\mathfrak{r}_2$ *ist mit jedem Element aus* $\mathfrak{A}$ *vertauschbar.*

Anderenfalls gäbe es ein Element $\mathfrak{u}$ in $\mathfrak{A}$, mit dem $\mathfrak{r}_2$ nicht vertauschbar ist, und es wäre

$$\mathfrak{r}_2^{-1}\mathfrak{u}\,\mathfrak{r}_2 = \mathfrak{u}\,\mathfrak{e}_2.$$

Also wird $\mathfrak{u}\,\mathfrak{r}_2 = \mathfrak{r}_2\mathfrak{u}\,\mathfrak{e}_2$

$$\begin{aligned} &= \mathfrak{u}^{-1}(\mathfrak{r}_2\mathfrak{u})\,\mathfrak{u}, \text{ da } \mathfrak{u}^2 = 1 \text{ ist} \\ &= (\mathfrak{r}_2\mathfrak{u})^t \quad \text{für geeignetes } t, \text{ da } \mathfrak{u} \text{ aus } \mathfrak{K}(\mathfrak{G}_2), \\ &= \mathfrak{r}_2^t\mathfrak{u}^t\mathfrak{e}_2^{\frac{t(t-1)}{2}}. \end{aligned}$$

Also wird $t = 1 + 2t'$ und

$$\mathfrak{r}_2 \mathfrak{u} \mathfrak{e}_2 = \mathfrak{r}_2 \mathfrak{e}_2^{t'} \mathfrak{u}^{1+2t'} \mathfrak{e}_2^{t'(1+2t')} = \mathfrak{r}_2 \mathfrak{u} \text{ wegen } \mathfrak{u}^2 = \mathfrak{e}_2^2 = 1,$$

also $\mathfrak{e}_2 = 1$, was ausgeschlossen war.

Damit ist also gezeigt, daß $\mathfrak{r}_2$ mit allen Elementen von $\mathfrak{K}(\mathfrak{G}_2)$ vertauschbar ist, also $\mathfrak{r}_2$ in $\mathfrak{Z}(\mathfrak{G}_2)$, also in $\mathfrak{K}(\mathfrak{G}_2)$, also $\mathfrak{G}_2 = \mathfrak{K}(\mathfrak{G}_2)$; also ist $\mathfrak{G}_2/\mathfrak{K}(\mathfrak{G}_2)$ entgegen unserer Annahme nicht von der Ordnung 2.

Damit haben wir also gefunden:

(16) *Ist $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ zyklisch, $\mathfrak{K}(\mathfrak{G})$ hamiltonsch und $\mathfrak{e}$ in $\mathfrak{Z}[\mathfrak{K}(\mathfrak{G})]$, aber nicht in $\mathfrak{C}[\mathfrak{K}(\mathfrak{G})]$ enthalten, so ist die Ordnung von $\mathfrak{G}/\mathfrak{K}(\mathfrak{Q})$ ungerade, $\mathfrak{G} = \mathfrak{G}_2 \times \mathfrak{U}$, wo $\mathfrak{U}$ alle Elemente ungerader Ordnung enthält, und $\mathfrak{G}_2 = \mathfrak{K}(\mathfrak{G}_2)$.*

ad III. $\mathfrak{e}$ *ist nicht in $\mathfrak{Z}[\mathfrak{K}(\mathfrak{G})]$ enthalten.*

Dann hat die Ordnung von $\mathfrak{e}$ die Gestalt $4u$, wo u eine ungerade Zahl ist. Weiter sei $n = 2^w m$, wo m eine ungerade Zahl ist.

Wir setzen $\mathfrak{r}_2 = \mathfrak{r}^{um}$ und $\mathfrak{r}_\mathfrak{u} = \mathfrak{r}^{2^{w+2}}$, so daß 2^{w+2} die Ordnung von $\mathfrak{r}_2$, um die von $\mathfrak{r}_\mathfrak{u}$ und 2^w die Ordnung von $\mathfrak{r}_2$ mod $\mathfrak{K}(\mathfrak{G})$, m die von $\mathfrak{r}_\mathfrak{u}$ mod $\mathfrak{K}(\mathfrak{G})$ wird.

Es wird also $\mathfrak{r}_2^{2^w}$ ein Element der Ordnung 4 aus $\mathfrak{K}(\mathfrak{G})$ und wir können o. B. d. A. annehmen, daß $\mathfrak{r}_2^{2^w} = \mathfrak{a}$ ist, wo $\mathfrak{a}$ ein erzeugendes Element einer Quaternionengruppe aus $\mathfrak{K}(\mathfrak{G})$ ist. Wir zeigen:

(17) $\mathfrak{r}_2$ *ist Element von $\mathfrak{K}(\mathfrak{G})$ und also $n = m$ ungerade.*

Es ist nämlich $\mathfrak{r}_2^{-1} \mathfrak{a} \mathfrak{r}_2 = \mathfrak{a}$ und $\mathfrak{r}_2^{-1} \mathfrak{x} \mathfrak{r}_2 = \mathfrak{x} \mathfrak{a}^{l(\mathfrak{x})}$, also $\mathfrak{r}_2^{-4} \mathfrak{x} \mathfrak{r}_2^4 = \mathfrak{x} \mathfrak{a}^{4l(\mathfrak{x})} = \mathfrak{x}$, d. h. $\mathfrak{r}_2^4$ ist in $\mathfrak{Z}(\mathfrak{G})$, also in $\mathfrak{K}(\mathfrak{G})$ enthalten. Mithin ist $w = 0$, 1 oder 2.

Weiter wird, wenn $\mathfrak{b}$ eine zweite Erzeugende einer Quaternionengruppe aus $\mathfrak{K}(\mathfrak{G})$ ist:

$$\mathfrak{b}^{-1} = \mathfrak{a}^{-1} \mathfrak{b} \mathfrak{a} = \mathfrak{r}_2^{-2^w} \mathfrak{b} \mathfrak{r}_2^{2^w} = \mathfrak{b} \mathfrak{a}^{2^w l(\mathfrak{b})}, \text{ d. h. } \mathfrak{b}^{-2} = \mathfrak{b}^2 = \mathfrak{a}^{2^w l(\mathfrak{b})},$$

also kann w nur gleich 0 oder 1 sein.

Wäre nun $w = 1$, so müßte $l(\mathfrak{b})$ ungerade, d. h. $\mathfrak{r}_2^{-1} \mathfrak{b} \mathfrak{r}_2 = \mathfrak{b} \mathfrak{a}^{\pm 1}$ sein. Dann wird:

$$\begin{aligned} \mathfrak{b}^{-1} \mathfrak{r}_2 \mathfrak{b}^2 &= \mathfrak{r}_2 \mathfrak{a}^{\mp 1} \mathfrak{b} \\ &= \mathfrak{b}^{-1}(\mathfrak{r}_2 \mathfrak{b})\mathfrak{b} = (\mathfrak{r}_2 \mathfrak{b})^t \quad \text{für geeignetes } t, \text{ da } \mathfrak{b} \text{ aus } \mathfrak{K}(\mathfrak{G}) \text{ ist,} \\ &= \mathfrak{r}_2^t \mathfrak{b}^t \mathfrak{a}^{\pm \frac{t(t-1)}{2}}. \end{aligned}$$

Also muß $t = 1 + 2t'$ sein, und es wird

$$\begin{aligned} \mathfrak{a}^{\mp 1} \mathfrak{b} &= \mathfrak{a}^{t'} \mathfrak{b}^{1+2t'} \mathfrak{a}^{\pm (1+2t')t'} \quad \text{oder} \\ \mathfrak{b} &= \mathfrak{a}^{\pm 1 + t'} \mathfrak{b}^{1+2t'} \mathfrak{a}^{\pm (1+2t')t'} = \mathfrak{b} \mathfrak{a}^{\mp 1 - t'} \mathfrak{a}^{2t'} \mathfrak{a}^{\pm (1+2t')t'}, \text{ d. h.} \\ 1 &= \mathfrak{a}^{\mp 1 + t' \pm t' \pm 2t'^2} = \mathfrak{a}^{\mp 1 + 2t''}, \text{ was unmöglich ist.} \end{aligned}$$

Damit ist $w = 0$ und also (17) erwiesen.

Wegen (17) ist $\mathfrak{r}_{\mathfrak{u}} = \mathfrak{r}^4$ ebenfalls Repräsentant einer erzeugenden Restklasse von $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ und es ist $\mathfrak{r}_{\mathfrak{u}}^n = \mathfrak{e}^4$ ein Element ungerader Ordnung. Damit haben wir diesen Fall auf Fall II. zurückgeführt, und also wegen (16) gezeigt:

(18) *Ist $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ zyklisch, $\mathfrak{K}(\mathfrak{G})$ hamiltonsch und $\mathfrak{e}$ nicht in $\mathfrak{Z}[\mathfrak{K}(\mathfrak{G})]$ enthalten, so ist die Ordnung von $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ ungerade, $\mathfrak{G} = \mathfrak{G}_2 \times \mathfrak{U}$, wo $\mathfrak{U}$ alle Elemente ungerader Ordnung enthält, und $\mathfrak{G}_2 = \mathfrak{K}(\mathfrak{G}_2)$.*

Aus (15), (16) und (18) folgt unser Satz und sogar der

Zusatz: *Ist $\mathfrak{K}(\mathfrak{G})$ hamiltonsch, $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ zyklisch, so ist die Ordnung von $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ ungerade.*

Satz 6: *Ist $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ eine zyklische, nicht nur aus der Gruppeneins bestehende Gruppe, so ist $\mathfrak{G}$ direktes Produkt seiner Primärkomponenten.*

Beweis: Sicher ist $\mathfrak{K}(\mathfrak{G}) > \mathfrak{Z}(\mathfrak{G})$, da die Faktorgruppe nach dem Zentrum nicht zyklisch sein kann [außer wenn $\mathfrak{G} = \mathfrak{Z}(\mathfrak{G})$ ist, was ja ausgeschlossen ist]. Nach Satz 3., § 2. enthält also $\mathfrak{K}(\mathfrak{G})$ nur Elemente endlicher Ordnung, nach Satz 2., § 3. ist $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ ein endlicher Zyklus; also haben alle Elemente von $\mathfrak{G}$ endliche Ordnung.

Jetzt folgt unsere Behauptung aus Satz 5., wenn wir noch bewiesen haben:

Ist $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ zyklisch, $\mathfrak{K}(\mathfrak{G})$ kommutativ und haben alle Elemente von $\mathfrak{G}$ endliche Ordnung, so ist $\mathfrak{G}$ direktes Produkt seiner Primärkomponenten.

Dies folgt aus dem Lemma des § 3., da $\mathfrak{C}(\mathfrak{G}) \leqq \mathfrak{Z}(\mathfrak{G})$ wegen (10) des § 2. gilt.

§ 5.

Satz 7: *Es sei $\mathfrak{G}$ eine zur Primzahl p gehörige Primärgruppe, $\mathfrak{A}$ ein echter Normalteiler von $\mathfrak{G}$ und $\mathfrak{G}/\mathfrak{A}$ zyklisch.*

Die Ordnung von $\mathfrak{G}/\mathfrak{A}$ sei etwa p^n, $\mathfrak{r}$ ein beliebiger Repräsentant einer beliebigen $\mathfrak{G}/\mathfrak{A}$ erzeugenden Restklasse und $\alpha(\mathfrak{g}) = \mathfrak{r}^{-1}\mathfrak{g}\,\mathfrak{r}$ für $\mathfrak{g}$ aus $\mathfrak{A}$.

Dann und nur dann ist $\mathfrak{A}$ der Kern von $\mathfrak{G}$, wenn die folgenden Bedingungen erfüllt sind:

1. *$\mathfrak{A}$ ist kommutativ.*
2. *$\mathfrak{C}(\mathfrak{G})$ = Gesamtheit der Elemente $\alpha(\mathfrak{g})\mathfrak{g}^{-1}$ mit $\mathfrak{g}$ aus $\mathfrak{A}$, $\leqq \{\mathfrak{r}^{p^n}\} \leqq \mathfrak{Z}(\mathfrak{G})$ [4].*

[4]) $\{\mathfrak{r}^{p^n}\} \leqq \mathfrak{Z}(\mathfrak{G})$ folgt aus 1.

3. *α hat die Ordnung p^n, also auch $\mathfrak{C}(\mathfrak{G})$* [5].
4. *$\mathfrak{r}^{p^n}$ ist ein Element maximaler Ordnung in $\mathfrak{A}$.*
5. *Falls $p = 2$ ist, ist $2^{n+1} <$ Ordnung von $\mathfrak{r}$.*

Beweis: A. Es sei $\mathfrak{A} = \mathfrak{K}(\mathfrak{G})$. Dann ist $\mathfrak{A}$ wegen (5), § 1. abelsch oder hamiltonsch. Da $\mathfrak{G}$ primär ist, so ist auch $\mathfrak{A}$ primär; ist p ungerade, so muß $\mathfrak{A}$ kommutativ sein; vergl. Fußnote [1]). Ist aber p gerade und $\mathfrak{A}$ hamiltonsch, so folgt aus Satz 5, § 4., daß $\mathfrak{A} = \mathfrak{G} = \mathfrak{K}(\mathfrak{G})$ ist, was durch die Voraussetzung über $\mathfrak{A}$ ausgeschlossen ist. Damit ist die Notwendigkeit der Bedingung 1. gezeigt. Die Notwendigkeit der Bedingungen 2. und 3. folgt aus (10), § 2.

B. Es sei 1., 2., 3. erfüllt. Zunächst einige

Bezeichnungen:

$p^c =$ Index von $\mathfrak{C}(\mathfrak{G})$ in $\{\mathfrak{r}^{p^n}\}$.

$\mathfrak{c} = \mathfrak{r}^{p^{n+c}}$ ist dann erzeugendes Element von $\mathfrak{C}(\mathfrak{G})$.

$\alpha(\mathfrak{g}) = \mathfrak{g}\mathfrak{c}^{h(\mathfrak{g})}$ für $\mathfrak{g}$ aus $\mathfrak{A}$ und $0 \leqq h(\mathfrak{g}) < p^n$.

$\mathfrak{a} = \mathfrak{r}^{p^n}$ ist in $\mathfrak{A}$ enthalten und hat die Ordnung p^{n+c}, da $\mathfrak{a}^{p^c} = \mathfrak{c}$ ist.

$p^{u(\mathfrak{g},r)} =$ Index von $\{\mathfrak{a}\} \cap \{\mathfrak{g}^{p^{n-r}}\}$ in $\{\mathfrak{g}^{p^{n-r}}\}$ für $0 \leqq r < n$.

$p^{v(\mathfrak{g},r)} =$ Ordnung von $\mathfrak{g}^{p^{n-r}}$.

Dann ist $v(\mathfrak{g}, r) \geqq u(\mathfrak{g}, r)$ und es wird

$\mathfrak{g}^{p^{n-r+u}} = \mathfrak{a}^{zp^w}$ mit $z = z(\mathfrak{g}, r)$, $(z, p) = 1$, $0 \leqq w < n + c$.

Da $u \leqq v$ ist, so ist die Ordnung des Elementes linker Hand p^{v-u} und die des Elementes rechter Hand p^{n+c-w}, und es wird also $v - u = n + c - w$, d. h. $w = n + c - v + u \geqq 0$ und $\mathfrak{g}^{p^{n-r+u}} = \mathfrak{a}^{zp^{n+c-v+u}}$.

Wir zeigen zunächst:

(19) *Es seien die Bedingungen* 1., 2., 3. *erfüllt; dann und nur dann ist $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$, wenn für jedes Elementepaar $\mathfrak{x}$, $\mathfrak{y}$ aus $\mathfrak{A}$, jedes $0 \leqq r < n$ und jedes zu p teilerfremde s die folgende Kongruenz nach t auflösbar ist:*

$$\text{(K)} \quad s\{tp^{u(\mathfrak{y},r)} + p^{c+r}[h(\mathfrak{x}) + h(\mathfrak{y}) \cdot 2^{-1}tp^{n-r+u(\mathfrak{y},r)}(1 + tp^{n-r+u(\mathfrak{y},r)})]\} \\ + tz(\mathfrak{y}, r)p^{n+c+u(\mathfrak{y},r)-v(\mathfrak{y},r)} \equiv 0 \mod p^{n+c}.$$

Ist nämlich $\mathfrak{x}$ aus $\mathfrak{A}$ beliebig, so ist dann und nur dann $\mathfrak{x}$ ein Element des Kernes $\mathfrak{K}(\mathfrak{G})$, wenn es für jedes $0 \leqq i < p^n$ und jedes $\mathfrak{y}$ aus $\mathfrak{A}$ ein geeignetes $e = e(i, \mathfrak{x}, \mathfrak{y})$ gibt, so daß

$$\mathfrak{x}^{-1}\,\mathfrak{r}^i\,\mathfrak{y}\,\mathfrak{x} = (\mathfrak{r}^i\,\mathfrak{y})^e \tag{20}$$

---

[5]) **Daß die Ordnung von α gleich der Ordnung von $\mathfrak{C}(\mathfrak{G})$ ist, folgt aus 1. und 2., wie beim Beweis von (10), § 2. gezeigt.**

gilt. Da (20) für $i = 0$ wegen Bedingung 1. stets durch $e = 1$ gelöst wird, so haben wir Bedingungen für die Lösbarkeit von (20) nur für $i \neq 0$ aufzustellen.

Sei mithin etwa $i = sp^r$ mit $(s, p) = 1$ und also $0 \leqq r < n$. Dann wird einerseits

$$\mathfrak{x}^{-1}\mathfrak{r}^i\mathfrak{y}\mathfrak{x} = \mathfrak{r}^i\alpha^i(\mathfrak{x}^{-1})\mathfrak{y}\mathfrak{x} = \mathfrak{r}^i\mathfrak{y}\mathfrak{c}^{-ih(\mathfrak{x})},$$

andererseits

$$(\mathfrak{r}^i\mathfrak{y})^e = \mathfrak{r}^{ie}\prod_{j=0}^{e-1}\alpha^{ij}(\mathfrak{y}) = \mathfrak{r}^{ie}\mathfrak{y}^e\mathfrak{c}^{\sum\limits_{j=0}^{e-1} ijh(\mathfrak{y})} =$$
$$= \mathfrak{r}^{ie}\mathfrak{y}^e\mathfrak{c}^{ih(\mathfrak{y})\frac{e(e-1)}{2}},$$

so daß also (20) gleichwertig ist mit

$$\mathfrak{r}^{i(e-1)} = \mathfrak{y}^{1-e}\mathfrak{c}^{-i\left[h(\mathfrak{x})+h(\mathfrak{y})\frac{e(e-1)}{2}\right]}.$$

Demnach ist $\mathfrak{r}^{i(e-1)}$ Element aus $\mathfrak{A}$, d. h. $i(e-1) = sp^r(e-1)$ ist durch p^n teilbar, oder $s(e-1) \equiv 0 \bmod p^{n-r}$. Wegen $(s, p) = 1$ folgt hieraus sogar, daß $e - 1 \equiv 0 \bmod p^{n-r}$ ist, und wir setzen $e - 1 = fp^{n-r}$. Dann wird (20) gleichwertig mit

$$\mathfrak{a}^{sf} = \mathfrak{y}^{-fp^{n-r}}\mathfrak{c}^{-i[h(\mathfrak{x})+h(\mathfrak{y})(1+fp^{n-r})fp^{n-r}2^{-1}]},$$

oder

$$\mathfrak{y}^{fp^{n-r}} = \mathfrak{a}^{-s\{f+p^{r+c}[h(\mathfrak{x})+h(\mathfrak{y})(1+fp^{n-r})fp^{n-r}2^{-1}]\}},$$

da $\mathfrak{c} = \mathfrak{a}^{p^c}$ ist.

Infolgedessen muß $f \equiv 0 \bmod p^{u(\mathfrak{y},r)}$ sein, d. h. $f = tp^{u(\mathfrak{y},r)}$ und (20) wird gleichwertig mit:

$$\mathfrak{y}^{tp^{n-r+u}} = \mathfrak{a}^{tzp^{n+c-v+u}}$$
$$= \mathfrak{a}^{-s\{tp^u+p^{r+c}[h(\mathfrak{x})+h(\mathfrak{y})(1+tp^{n-r+u})tp^{n-r+u}2^{-1}]\}},$$

wobei $u = u(\mathfrak{y}, r)$, $v = v(\mathfrak{y}, r)$, woraus folgt, daß (20) mit (K) gleichwertig ist, da $\mathfrak{a}$ die Ordnung p^{n+c} hat, womit (19) bewiesen ist.

C. Es sei p ungerade und 1., 2., 3. erfüllt. Wir zeigen zunächst:

(21) *Dann und nur dann ist $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$, wenn Bedingung 4. erfüllt ist.*

Da $n - r + u(\mathfrak{y}, r) \geqq n - r > 0$ ist, so geht (K) für ungerades p über in

$$s\{tp^u + p^{c+r}h(\mathfrak{x})\} + tzp^{n+c+u-v} \equiv 0 \bmod p^{n+c}$$

oder

(K 1) $t\{sp^{u(\mathfrak{y},r)} + z(\mathfrak{y}, r)p^{n+c+u(\mathfrak{y},r)-v(\mathfrak{y},r)}\} + sh(\mathfrak{x})p^{c+r} \equiv 0 \bmod p^{n+c}$.

Die Lösbarkeit von (K 1) ist trivial, falls $h(\mathfrak{x}) = 0$ ist. Sei also $h(\mathfrak{x}) \neq 0$; dann ist $h(\mathfrak{x}) = h'(\mathfrak{x})p^{h''(\mathfrak{x})}$ mit $(h'(\mathfrak{x}), p) = 1$ und $0 \leqq h''(\mathfrak{x}) < n$. Wir zeigen:

(21a) *Gibt es* $\mathfrak{y}$, r *mit* $0 \leqq r < n$ *und* $v(\mathfrak{y}, r) \geqq n + c$, *so ist* (K 1) *nicht immer lösbar.*

Gibt es nämlich für ein $0 \leqq r < n$ in $\mathfrak{A}$ ein $\mathfrak{y}$ mit $v(\mathfrak{y}, r) \geqq n + c$, so ist $v(\mathfrak{y}^{p^{v-n-c}}, r) = n + c$ für $v = v(\mathfrak{y}, r)$. Wir setzen $\mathfrak{y}^* = \mathfrak{y}^{p^{v-n-c}}$ für $v = v(\mathfrak{y}, r)$ und es wird aus (K 1):

$$t p^{u(\mathfrak{y}^*, r)}\{s + z(\mathfrak{y}^*, r)\} + s h'(\mathfrak{x}) p^{c+r+h''(\mathfrak{x})} \equiv 0 \mod p^{n+c}.$$

Ist weiter $\bar{\mathfrak{y}} = \mathfrak{y}^{*d}$ mit $(d, p) = 1$, so wird

$$u(\bar{\mathfrak{y}}, r) = u(\mathfrak{y}^*, r), \quad v(\bar{\mathfrak{y}}, r) = v(\mathfrak{y}^*, r) = n + c, \quad z(\bar{\mathfrak{y}}, r) = d z(\mathfrak{y}^*, r),$$

und es wird aus (K 1):

$$t p^{u(\mathfrak{y}^*, r)}\{s + d z(\mathfrak{y}^*, r)\} + s h'(\mathfrak{x}) p^{c+r+h''(\mathfrak{x})} \equiv 0 \mod p^{n+c}.$$

Wählen wir weiter, was stets möglich ist, $\mathfrak{x}$ aus $\mathfrak{A}$ so aus, daß $h(\mathfrak{x}) = 1$ ist, so wird aus (K 1):

$$t p^{u(\mathfrak{y}^*, r)}\{s + d z(\mathfrak{y}^*, r)\} + s p^{c+r} \equiv 0 \mod p^{n+c}.$$

Da s und z zu p teilerfremd sind, so können wir d so bestimmen, daß $s + d z(\mathfrak{y}^*, r) \equiv 0 \mod p^{n+c}$ wird. Dann wird aus (K 1):

$$s p^{c+r} \equiv 0 \mod p^{n+c},$$

und dies ist unmöglich, da $0 \leqq r < n$ und $(s, p) = 1$ ist, womit (21a) bewiesen ist.

(21b) *Ist* $v(\mathfrak{y}, r) < n + c$, *so ist* (K 1) *stets lösbar.*

Wir zeigen zunächst:

(22) *Ist* $v(\mathfrak{y}, r) < n + c$, *so ist* $u(\mathfrak{y}, r) \leqq c + r$.

Es ist nämlich

$$u(\mathfrak{y}, r) = \begin{cases} u(\mathfrak{y}, n-1) - n + 1 + r & \text{für } u(\mathfrak{y}, n-1) - n + 1 + r \geqq 0, \\ 0 & \text{für } u(\mathfrak{y}, n-1) - n + 1 + r \leqq 0. \end{cases}$$

Da stets $0 \leqq c + r$ ist, ist nur der Fall zu betrachten, daß $u(\mathfrak{y}, n-1) - n + 1 + r > 0$ ist. Dann wird nach unserer Voraussetzung:

$$u(\mathfrak{y}, r) \leqq v(\mathfrak{y}, n-1) - n + 1 + r < n + c - n + 1 + r = c + r + 1,$$

woraus (22) folgt.

Wegen (22) und $u(\mathfrak{y}, r) \leqq v(\mathfrak{y}, r) < n + c$ wird aus (K 1):

$$t\{s + z p^{n+c-v}\} + s h'(\mathfrak{x}) p^{c+r+h''(\mathfrak{x})-u} \equiv 0 \mod p^{n+c-u}.$$

Setzen wir $t = t^* p^{c+r+h''(\mathfrak{x})-u}$, was wegen (22) möglich ist, so wollen wir t^* aus

$$t^*\{s + zp^{n+c-v}\} + sh'(\mathfrak{x}) \equiv 0 \bmod p^{n-r}$$

bestimmen, um eine Lösung von (K 1) zu finden. Die Kongruenz für t^* ist aber stets lösbar, da $n - r > 0$, $n + c - v > 0$ und also $(s + zp^{n+c-v}, p) = 1$, $(sh'(\mathfrak{x}), p) = 1$ ist. Sind t^*, t wie angegeben gewählt, so wird

$$t\{s + zp^{n+c-v}\} + sh'(\mathfrak{x})p^{c+r+h''(\mathfrak{x})-u} \equiv 0 \bmod p^{n+c-u+h''(\mathfrak{x})},$$

also auch $\qquad \equiv 0 \bmod p^{n+c-u},$

womit (21*b*) bewiesen ist.

Beweis von (21): Die Ordnung von $\mathfrak{y}^p$ muß $< p^{n+c}$ wegen (21*a*) sein; dann ist aber die Ordnung von $\mathfrak{y}$ wenigstens $\leqq p^{n+c}$ d. h. Bedingung 4. ist notwendig. — Ist umgekehrt Bedingung 4. erfüllt, so kann die Ordnung von $\mathfrak{y}$ nicht größer als p^{n+c} sein, so daß die von $\mathfrak{y}^{p^{n-r}}$ für jedes $0 \leqq r < n$ also $< p^{n+c}$ wird. Mithin folgt aus (21*b*), daß Bedingung 4. hinreichend ist, womit (21) voll bewiesen ist.

Aus A. und (21) folgt jetzt sofort, daß für ungerades p die Bedingungen 1.—4. notwendig sind. — Sind umgekehrt die Bedingungen 1.—4. erfüllt und p ungerade, so ist $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$ wegen (21). Da p ungerade ist, muß $\mathfrak{K}(\mathfrak{G})$ kommutativ sein, so daß die Restklassen von $\mathfrak{K}(\mathfrak{G})/\mathfrak{A}$ in $\mathfrak{A}$ nur den identischen Automorphismus induzieren können. Dies tut aber wegen Bedingung 3. nur $\mathfrak{A}$ selbst, d. h. $\mathfrak{A} = \mathfrak{K}(\mathfrak{G})$, womit unser Satz für ungerades p voll bewiesen ist.

D. Es sei $p = 2$, $n + c = 1$ und Bedingung 1.—3. erfüllt. Dann zeigen wir:

(23) *Ist* $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$ *und* $n = 1$, $c = 0$, *so ist* $\mathfrak{G} = \mathfrak{K}(\mathfrak{G})$ *hamiltonsch und also* $\mathfrak{A} \neq \mathfrak{K}(\mathfrak{G})$.

Unter den gemachten Voraussetzungen wird

$\mathfrak{r}^2 = \mathfrak{a}$ mit $\mathfrak{a}$ aus $\mathfrak{A}$ und $\mathfrak{a}^2 = 1$,

$$\mathfrak{r}^{-1}\mathfrak{x}\,\mathfrak{r} = \left\{\begin{matrix}\mathfrak{x}\\ \mathfrak{x}\,\mathfrak{a}\end{matrix}\right\} \text{für } \mathfrak{x} \text{ aus } \mathfrak{A}, \text{ und beide Fälle können eintreten.}$$

Ist $\mathfrak{x}$ und $\mathfrak{y}$ aus $\mathfrak{A}$ beliebig, so ist

$$\mathfrak{x}^{-1}\,\mathfrak{r}\,\mathfrak{y}\,\mathfrak{x} = \begin{cases}\mathfrak{r}\,\mathfrak{y}, & \text{wenn } \mathfrak{r}^{-1}\mathfrak{x}\,\mathfrak{r} = \mathfrak{x} \text{ ist}\\ \mathfrak{r}\,\mathfrak{y}\,\mathfrak{a}, & \text{wenn } \mathfrak{r}^{-1}\mathfrak{x}\,\mathfrak{r} = \mathfrak{x}\,\mathfrak{a} \text{ ist.}\end{cases}$$

Wegen $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$ muß es im zweiten Falle eine ganze Zahl t derart geben, daß $(\mathfrak{r}\,\mathfrak{y})^t = \mathfrak{r}\,\mathfrak{y}\,\mathfrak{a}$ wird. Da der zweite Fall unabhängig von der Auswahl von $\mathfrak{y}$ stets eintreten kann, so muß es also zu jedem $\mathfrak{y}$ eine ganze Zahl $t = t(\mathfrak{y})$ geben, so daß $\mathfrak{r}\,\mathfrak{y}\,\mathfrak{a} = (\mathfrak{r}\,\mathfrak{y})^{t(\mathfrak{y})}$ wird. Nun ist aber

$$(\mathfrak{x}\mathfrak{y})^t = \begin{cases} \mathfrak{x}^t\mathfrak{y}^t, \text{ wenn } \mathfrak{x}^{-1}\mathfrak{y}\,\mathfrak{x} = \mathfrak{y} \text{ ist} \\ \mathfrak{x}^t\mathfrak{y}^t\mathfrak{a}^{\frac{t(t-1)}{2}}, \text{ wenn } \mathfrak{x}^{-1}\mathfrak{y}\,\mathfrak{x} = \mathfrak{y}\,\mathfrak{a} \text{ ist.} \end{cases}$$

Es ist also notwendig $t = 1 + 2t'$, und wir haben

$$\mathfrak{x}\,\mathfrak{y}\,\mathfrak{a} = \begin{cases} \mathfrak{x}\,\mathfrak{a}^{t'}\,\mathfrak{y}^{1+2t'} \\ \mathfrak{x}\,\mathfrak{a}^{t'+(1+2t')t'}\mathfrak{y}^{1+2t'} = \mathfrak{x}\,\mathfrak{y}^{1+2t'} \text{ wegen } \mathfrak{a}^2 = 1, \end{cases}$$

und wir haben damit gefunden:

Zu jedem $\mathfrak{y}$ aus $\mathfrak{A}$ gibt es eine ganze Zahl $t'(\mathfrak{y})$, so daß $\mathfrak{a}^{1-t'} = \mathfrak{y}^{2t'}$, wenn $\mathfrak{x}^{-1}\mathfrak{y}\,\mathfrak{x} = \mathfrak{y}$ ist und $\mathfrak{a} = \mathfrak{y}^{2t'}$, wenn $\mathfrak{x}^{-1}\mathfrak{y}\,\mathfrak{x} = \mathfrak{y}\,\mathfrak{a}$ ist.

Um zu zeigen, daß $\mathfrak{G} = \mathfrak{K}(\mathfrak{G})$ ist, genügt es wegen $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$ und (8), § 1. zu zeigen, daß jedes Element der Form $\mathfrak{x}\mathfrak{z}$ jedes Element von $\mathfrak{G}$ in eine Potenz transformiert.

I. $(\mathfrak{x}\mathfrak{z})^{-1}\mathfrak{y}(\mathfrak{x}\mathfrak{z}) = \mathfrak{z}^{-1}(\mathfrak{x}^{-1}\mathfrak{y}\,\mathfrak{x})\mathfrak{z} = \begin{Bmatrix} \mathfrak{y} \\ \mathfrak{y}\,\mathfrak{a} \end{Bmatrix}$, wenn $\mathfrak{x}^{-1}\mathfrak{y}\,\mathfrak{x} = \begin{Bmatrix} \mathfrak{y} \\ \mathfrak{y}\,\mathfrak{a} \end{Bmatrix}$ ist.

Nach dem oben gezeigten ist aber im zweiten Falle $\mathfrak{y}\,\mathfrak{a} = \mathfrak{y}^{1+2t'}$.

II. $(\mathfrak{x}\mathfrak{z})^{-1}\,\mathfrak{x}\mathfrak{y}(\mathfrak{x}\mathfrak{z}) = \mathfrak{z}^{-1}\mathfrak{y}\,\mathfrak{x}\mathfrak{z} = \begin{Bmatrix} \mathfrak{x}\,\mathfrak{y} \\ \mathfrak{x}\,\mathfrak{y}\,\mathfrak{a} \end{Bmatrix}$, wenn $\mathfrak{x}^{-1}\mathfrak{z}^{-1}\mathfrak{y}\,\mathfrak{x} = \begin{Bmatrix} \mathfrak{z}^{-1}\mathfrak{y} \\ \mathfrak{z}^{-1}\mathfrak{y}\,\mathfrak{a} \end{Bmatrix}$ ist. Im zweiten Falle wird

$$\mathfrak{x}\,\mathfrak{y}\,\mathfrak{a} = \begin{cases} \mathfrak{x}\,\mathfrak{y}^{1+2t'}\mathfrak{a}^{t'} = \mathfrak{x}^{1+2t'}\mathfrak{y}^{1+2t'} = (\mathfrak{x}\,\mathfrak{y})^{1+2t'} \\ \mathfrak{x}\,\mathfrak{y}^{1+2t'} = \mathfrak{x}^{1+2t'}\mathfrak{y}^{1+2t'}\mathfrak{a}^{t'} = \mathfrak{x}^{1+2t'}\mathfrak{y}^{1+2t'}\mathfrak{a}^{(1+2t')t'} = (\mathfrak{x}\,\mathfrak{y})^{1+2t'} \end{cases}$$

nach dem oben gezeigten, wenn $\mathfrak{x}^{-1}\mathfrak{y}\,\mathfrak{x} = \begin{Bmatrix} \mathfrak{y} \\ \mathfrak{y}\,\mathfrak{a} \end{Bmatrix}$ ist, womit unsere Behauptung bewiesen, da $\mathfrak{G}$ nicht kommutativ ist.

Aus (23) folgt insbesondere, daß die Bedingung 5. notwendig ist.

E. Es sei $p = 2$, Bedingung 1.—3. und 5. erfüllt. Dann zeigen wir

(24) *Dann und nur dann ist* $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$, *wenn* 4. *erfüllt ist.*

Für $p = 2$ wird nämlich aus der Kongruenz (K):

$$s\{t2^{u(\mathfrak{y},r)} + 2^{c+r}[h(\mathfrak{z}) + h(\mathfrak{y})t2^{n-r-1+u(\mathfrak{y},r)}(1 + t2^{n-r+u(\mathfrak{y},r)})]\} + \\ + tz(\mathfrak{y},r)2^{n+c+u(\mathfrak{y},r)-v(\mathfrak{y},r)} \equiv 0 \bmod 2^{n+c}.$$

Dies wird wegen

$$c + r + n - r + u - 1 + n - r + u = c - r + 2n + 2u - 1 \geqq c + n$$

zu

$$s\{t2^u + 2^{c+r}h(\mathfrak{z}) + h(\mathfrak{y})t2^{n+c+u-1}\} + tz2^{n+c+u-v} \equiv 0 \bmod 2^{n+c}$$

oder

$$\text{(K 2)}\quad t\{s2^{u(\mathfrak{y},r)} + 2^{c+n-1+u(\mathfrak{y},r)}h(\mathfrak{y})s + z(\mathfrak{y},r)2^{n+c+u(\mathfrak{y},r)-v(\mathfrak{y},r)}\} + \\ + 2^{c+r}sh(\mathfrak{z}) \equiv 0 \bmod 2^{n+c}.$$

Fall I: $u(\mathfrak{y}, r) = 0$.

Dann wird $\{\mathfrak{a}\} \cap \{\mathfrak{y}^{2^{n-r}}\} = \{\mathfrak{y}^{2^{n-r}}\}$, also wegen $\alpha(\mathfrak{a}) = \mathfrak{a}$ auch $\alpha(\mathfrak{y}^{2^{n-r}}) = \mathfrak{y}^{2^{n-r}}$, also $\mathfrak{c}^{h(\mathfrak{y})2^{n-r}} = 1$, also $h(\mathfrak{y})2^{n-r} \equiv 0 \bmod 2^n$ oder $h(\mathfrak{y}) \equiv 0 \bmod 2^r$.

I, 1: $r = 0$.

Dann wird aus (K2):

$$t\{s + 2^{c+n-1}sh(\mathfrak{y}) + z2^{n+c-v}\} + 2^c sh(\mathfrak{y}) \equiv 0 \bmod 2^{n+c}.$$

Da $n + c > 1$ wegen Bedingung 5. ist, so ist $s + 2^{n+c-1}sh(\mathfrak{y})$ ungerade, und man kann wie bei (21a) zeigen, daß $n + c \leqq v$ nach sich zöge, daß unsere Kongruenz für eine gewisse $\mathfrak{y}$-Potenz unlösbar wäre. Ist aber umgekehrt $n + c > v$, so zeigt man, wieder unter Berücksichtigung, daß $s(1 + 2^{c+n-1}h(\mathfrak{y}))$ ungerade ist, wie ad (21b), daß unsere Kongruenz lösbar ist.

I, 2: $r > 0$.

Dann wird wegen $h(\mathfrak{y}) \equiv 0 \bmod 2^r$ aus (K 2):

$$t\{s + z2^{c+n-v}\} + 2^{c+r}sh(\mathfrak{x}) \equiv 0 \bmod 2^{n+c},$$

und man zeigt genau wie ad (21a) und (21b), daß diese Kongruenz dann und nur dann stets lösbar ist, wenn $n + c > v(\mathfrak{y}, r)$ ist.

Fall II: $u(\mathfrak{y}, r) \neq 0$.

Dann nimmt (K 2) die Gestalt an:

$$t\{s2^u + z2^{n+c+u-v}\} + 2^{c+r}sh(\mathfrak{x}) \equiv 0 \bmod 2^{n+c},$$

und wieder zeigt man genau wie ad (21a) und (21b), daß diese Kongruenz dann und nur dann stets lösbar ist, wenn $n + c > v(\mathfrak{y}, r)$ ist.

Aus dem ad I. und II. gezeigten folgert man jetzt (24) ebenso wie (21) aus (21a) und (21b).

Aus (24) folgt jetzt sofort, daß unter Voraussetzung von $n + c > 1$ die Bedingungen 1.—4. notwendig für $\mathfrak{A} = \mathfrak{K}(\mathfrak{G})$ sind. Sind umgekehrt 1.—5. erfüllt, so folgt aus (24), daß $\mathfrak{A} \leqq \mathfrak{K}(\mathfrak{G})$ ist. Wäre $\mathfrak{A} < \mathfrak{K}(\mathfrak{G})$, so könnte $\mathfrak{K}(\mathfrak{G})$ wegen 3. nicht kommutativ sein, wäre also hamiltonsch. Da $\mathfrak{a}$ ein Zentrumselement von $\mathfrak{G}$ ist, so auch eines von $\mathfrak{K}(\mathfrak{G})$; andererseits hat $\mathfrak{a}$ die Ordnung 2^{n+c}, und diese ist wegen 5. mindestens 4, was der Tatsache widerspricht, daß Zentrumselemente einer hamiltonschen Primärgruppe stets höchstens die Ordnung 2 haben, womit der Beweis des Satzes vollständig zu Ende geführt ist.

Folgerung 1: *Es sei $\mathfrak{G}$ eine beliebige Gruppe derart, daß $\mathfrak{K}(\mathfrak{G})$ nur Elemente endlicher Ordnung enthält. Gibt es in einer der*

Primärkomponenten von $\mathfrak{K}(\mathfrak{G})$ Elemente beliebig hoher Ordnung, so ist sie in $\mathfrak{Z}(\mathfrak{G})$ enthalten.

Es ist also insbesondere $\mathfrak{K}(\mathfrak{G}) = \mathfrak{Z}(\mathfrak{G})$, wenn $\mathfrak{K}(\mathfrak{G})$ primär ist und Elemente beliebig hoher Ordnung enthält.

Beweis: Da $\mathfrak{K}(\mathfrak{G})$ nur Elemente endlicher Ordnung enthält, so ist $\mathfrak{K}(\mathfrak{G})$ nach (6) des § 1. direktes Produkt seiner Primärkomponenten. Ist $\mathfrak{K}(\mathfrak{G})_p$ eine solche, die Elemente beliebig hoher Ordnung enthält, so ist $\mathfrak{K}(\mathfrak{G})_p$ kommutativ, da im anderen Falle $p = 2$ und die Ordnungen aller Elemente $\leqq 4$ wären [nach Fußnote [1])].

Sei $\mathfrak{g}$ ein beliebiges Element aus $\mathfrak{G}$; ist $\mathfrak{g}$ von unendlicher Ordnung, so ist $\mathfrak{g}$ wegen (9), § 2. mit jedem Element von $\mathfrak{K}(\mathfrak{G})_p$ vertauschbar; ist aber $\mathfrak{g}$ von endlicher Ordnung, so ist $\{\mathfrak{K}(\mathfrak{G})_p, \mathfrak{g}\}/\mathfrak{K}[\{\mathfrak{K}(\mathfrak{G})_p, \mathfrak{g}\}]$ ein endlicher Zyklus, da $\mathfrak{K}[\{\mathfrak{K}(\mathfrak{G})_p, \mathfrak{g}\}] \geqq \mathfrak{K}(\mathfrak{G})_p$ ist.

Jetzt folgt aber aus Satz 6, § 4. und Satz 7, 4., § 5., daß auch dieses $\mathfrak{g}$ mit jedem Element von $\mathfrak{K}(\mathfrak{G})_p$ vertauschbar ist, d. h. $\mathfrak{K}(\mathfrak{G})_p \leqq \mathfrak{Z}(\mathfrak{G})$.

Folgerung 2: *Ist die Primärkomponente $\mathfrak{K}(\mathfrak{G})_p$ nicht in $\mathfrak{Z}(\mathfrak{G})$ enthalten, so ist entweder $p = 2$ und $\mathfrak{K}(\mathfrak{G})_p$ direktes Produkt einer Quaternionengruppe mit Zyklen der Ordnung 2, oder $\mathfrak{K}(\mathfrak{G})_p$ ist direktes Produkt zyklischer Gruppen, deren Ordnungen beschränkt sind.*

Ist also insbesondere $\mathfrak{K}(\mathfrak{G})_p$ für kein p in $\mathfrak{Z}(\mathfrak{G})$ enthalten, so ist $\mathfrak{K}(\mathfrak{G})$ direktes Produkt zyklischer Gruppen und evtl. noch einer Quaternionengruppe.

Beweis: Nach Satz 3 des § 2. kann $\mathfrak{K}(\mathfrak{G})$ keine Elemente unendlicher Ordnung enthalten, da nach Voraussetzung $\mathfrak{K}(\mathfrak{G}) > \mathfrak{Z}(\mathfrak{G})$ ist. Also ist $\mathfrak{K}(\mathfrak{G})$ nach (6), § 1. direktes Produkt seiner Primärkomponenten.

Ist $\mathfrak{K}(\mathfrak{G})_p$ nicht kommutativ, so ist $\mathfrak{K}(\mathfrak{G})_p$ hamiltonsch und wegen Fußnote [1]) wird $p = 2$ und $\mathfrak{K}(\mathfrak{G})_p$ direktes Produkt einer Quaternionengruppe mit einer kommutativen Gruppe, deren sämtliche Elemente die Ordnung 2 haben, die also bekanntlich direktes Produkt von Zyklen der Ordnung 2 ist. — Ist aber $\mathfrak{K}(\mathfrak{G})_p$ kommutativ, so folgt unsere Behauptung aus Folgerung 1 und dem folgenden

Lemma: *Es sei $\mathfrak{A}$ eine kommutative Gruppe; gibt es eine Primzahlpotenz p^n derart, daß $\mathfrak{a}^{p^n} = 1$ für jedes $\mathfrak{a}$ aus $\mathfrak{A}$ gilt, so ist $\mathfrak{A}$ direktes Produkt zyklischer Gruppen.*

Jeder Zyklus von in $\mathfrak{A}$ maximaler Ordnung und jedes direkte

Produkt zweier nur die Gruppeneins gemein habender Zyklen von in $\mathfrak{A}$ maximaler Ordnung ist direkter Faktor von $\mathfrak{A}$ [6]).

Beweis: Es sei $\overline{\mathfrak{A}}$ die Untergruppe aller Elemente der Ordnung p aus $\mathfrak{A}$. Dann ist bekanntlich $\overline{\mathfrak{A}}$ direktes Produkt von Zyklen der Ordnung p und jede Untergruppe von $\overline{\mathfrak{A}}$ ist direkter Faktor von $\overline{\mathfrak{A}}$. Infolgedessen gibt es eine Zerlegung $\overline{\mathfrak{A}} = \overline{\mathfrak{A}}^n \times \ldots \times \overline{\mathfrak{A}}^1$, wo die Elemente von $\overline{\mathfrak{A}}^i$ den Höhenexponenten [7]) $i-1$ haben. Ist dann etwa $\overline{\mathfrak{A}}^i = \prod\limits_{v} \{\mathfrak{a}_{iv}\}$, so sei $\mathfrak{b}_{iv}$ eine Lösung der Gleichung $\mathfrak{x}^{p^{i-1}} = \mathfrak{a}_{iv}$ und man verifiziert, daß $\mathfrak{A} = \prod\limits_{i=1}^{n} \prod\limits_{v} \{\mathfrak{b}_{iv}\}$ ist [8]), womit unsere Behauptungen bewiesen sind, wenn man noch bedenkt, daß bei der Zerlegung von $\overline{\mathfrak{A}}^n$ noch über 2 Elemente $\mathfrak{a}_{nv}$, die verschiedene Zyklen erzeugen, und entsprechend über 2 Elemente $\mathfrak{b}_{nv}$, von in $\mathfrak{A}$ maximaler Ordnung, die zwei nur die Gruppeneins gemein habende Zyklen erzeugen, beliebig verfügt werden kann.

Satz 8: *Es sei $\mathfrak{A}$ eine kommutative zur Primzahl p gehörige Primärgruppe, p^m die [endliche] Maximalordnung von Elementen aus $\mathfrak{A}$, und $\mathfrak{B}$ eine Untergruppe von $\mathfrak{A}$.*

Dann und nur dann gibt es eine Gruppe $\mathfrak{G}$, so daß $\mathfrak{K}(\mathfrak{G}) = \mathfrak{A}$, $\mathfrak{Z}(\mathfrak{G}) = \mathfrak{B}$ und $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ ein Zyklus der Ordnung p^n ist, wenn

a.) *$n \leq m$ ist,*

b.) *$\mathfrak{B}$ ein Element von in $\mathfrak{A}$ maximaler Ordnung enthält,*

---

[6]) Dieses Lemma und sein Beweis sind im wesentlichen, wenn auch nicht explizite, in den Prüferschen Untersuchungen enthalten. Vergl. etwa Heinz Prüfer [Math. Zeitschr. 17 (1923), 48 u. 57].

[7]) Im Sinne von H. Prüfer hat $\mathfrak{a}$ den Höhenexponenten i, wenn zwar die Gleichung $\mathfrak{y}^{p^i} = \mathfrak{a}$, aber nicht mehr die Gleichung $\mathfrak{y}^{p^{i+1}} = \mathfrak{a}$ in $\mathfrak{A}$ lösbar ist.

[8]) Daß $\mathfrak{A} = \prod\limits_{i=1}^{n} \prod\limits_{v} \{\mathfrak{b}_{iv}\}$ ist, sieht man folgendermaßen:

1. Sei $\prod\limits_{i=1}^{n} \prod\limits_{j=1}^{k} \mathfrak{b}_{iv_j}^{x_{ij}} = 1$ und p^v die maximale Ordnung der Elemente $\mathfrak{b}_{1v_1}^{x_{11}}, \ldots, \mathfrak{b}_{nv_k}^{x_{nk}}$; wäre $v > 0$, so wäre $1 = \prod\limits_{i=1}^{n} \prod\limits_{j=1}^{k} \mathfrak{b}_{iv_j}^{x_{ij}p^{v-1}}$ und $\mathfrak{b}_{iv_j}^{x_{ij}p^{v-1}} = \mathfrak{a}_{iv_j}^{y_{ij}}$. Dann folgt aber, daß $\mathfrak{a}_{iv_j}^{y_{ij}} = 1$ ist; d.h. aber p^{v-1} wäre mindestens so groß wie die maximale Ordnung der Elemente $\mathfrak{b}_{iv_j}^{x_{ij}}$; Widerspruch! Also ist $v=0$, d.h. $\mathfrak{b}_{iv_j}^{x_{ij}} = 1$.

2. Sei $\mathfrak{a}$ ein Element aus $\mathfrak{A}$, p^a die Ordnung von $\mathfrak{a}$. Ist $a = 1$, so läßt sich $\mathfrak{a}$ als Element von $\overline{\mathfrak{A}}$ sicher durch die $\mathfrak{b}_{iv}$ ausdrücken; sei dies bereits für $a - 1$ bewiesen; wir zeigen es für a. Da $\mathfrak{a}^{p^{a-1}}$ in $\overline{\mathfrak{A}}$ enthalten ist, so ist $\mathfrak{a}^{p^{a-1}} = \prod\limits_{i=a}^{n} \prod\limits_{j=1}^{k} \mathfrak{a}_{iv_j}^{x_{ij}}$ mit $0 < x_{ij} < p$, und $\mathfrak{a}\left[\prod\limits_{i=a}^{n} \prod\limits_{j=1}^{k} \mathfrak{b}_{iv_j}^{x_{ij}p^{i-a}}\right]^{-1}$ ist ein Element der Ordnung p^{a-1}, also durch die $\mathfrak{b}_{iv}$ ausdrückbar, womit alles bewiesen ist.

c.) $\mathfrak{A}/\mathfrak{B}$ *ein Zyklus der Ordnung* p^n, *d. h. isomorph* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *ist*[8a]),
d.) $m > 1$ *für* $p = 2$ *ist.*

Beweis: A. Nach Satz 7, Bedingung 2. ist $\mathfrak{K}(\mathfrak{G})/\mathfrak{Z}(\mathfrak{G})$ isomorph $\mathfrak{C}(\mathfrak{G})$ und nach Bedingung 3. ist $\mathfrak{C}(\mathfrak{G})$ isomorph $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$. Nach Bedingung 4. muß $n \leqq m$ sein und d.) folgt aus Bedingung 5.

B. Seien umgekehrt die Bedingungen a.)—d.) erfüllt. Dann sei $\mathfrak{a}$ ein Element von in $\mathfrak{A}$ maximaler Ordnung, das in $\mathfrak{B}$ enthalten ist. Wir setzen $\mathfrak{c} = \mathfrak{a}^{p^{m-n}}$. Ist weiter $\mathfrak{e}$ Repräsentant einer erzeugenden Restklasse von $\mathfrak{A}/\mathfrak{B}$, so definieren wir:

$$\alpha(\mathfrak{x}) = \mathfrak{x}\mathfrak{c}^i, \text{ wenn } \mathfrak{x} \equiv \mathfrak{e}^i \bmod \mathfrak{B} \text{ ist.}$$

α ist eindeutig, da die Ordnung von $\mathfrak{c}$ gleich der Ordnung von $\mathfrak{e}$ mod $\mathfrak{B}$ ist. Außerdem ist $\alpha(\mathfrak{a}) = \mathfrak{a}$, $\alpha(\mathfrak{c}) = \mathfrak{c}$, da $\mathfrak{a}$ und $\mathfrak{c}$ Elemente von $\mathfrak{B}$ sind. Also ist auch $\alpha(\mathfrak{A}) = \mathfrak{A}$. — Ist $\mathfrak{x}\mathfrak{c}^x = \mathfrak{y}\mathfrak{c}^y$, so ist $\mathfrak{x} \equiv \mathfrak{y} \bmod \mathfrak{B}$, da $\mathfrak{c}$ in $\mathfrak{B}$ enthalten ist; mithin ist $\mathfrak{c}^x = \mathfrak{c}^y$, also $\mathfrak{x} = \mathfrak{y}$, d. h. α ist umkehrbar eindeutig. — Schließlich ist $\alpha(\mathfrak{x})\alpha(\mathfrak{y}) = \mathfrak{x}\mathfrak{y}\mathfrak{c}^{x+y} = \alpha(\mathfrak{x}\mathfrak{y})$, d. h. α ist ein Automorphismus von $\mathfrak{A}$.

Erweitern wir jetzt $\mathfrak{A}$ zu $\mathfrak{G}$ durch Adjunktion eines Elementes $\mathfrak{r}$, das

$$\mathfrak{r}^{p^n} = \mathfrak{a}, \qquad \mathfrak{r}^{-1}\mathfrak{x}\,\mathfrak{r} = \alpha(\mathfrak{x}) \text{ für } \mathfrak{x} \text{ aus } \mathfrak{a}$$

erfüllt, so folgt aus Satz 7 und den Bedingungen a.)—d.), daß $\mathfrak{K}(\mathfrak{G}) = \mathfrak{A}$, $\mathfrak{Z}(\mathfrak{G}) = \mathfrak{B}$ und $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ ein Zyklus der Ordnung p^n ist, da $\mathfrak{c}$ und also α die Ordnung p^n haben, wenn nur n positiv ist.

Ist $n = 0$, so folgt alles aus der Bemerkung $\mathfrak{A} = \mathfrak{B} = \mathfrak{G}$.

Folgerung 1: *Es sei* $\mathfrak{A}$ *eine kommutative, zur Primzahl* p *gehörige Primärgruppe,* p^m *die* [*endliche*] *Maximalordnung von Elementen aus* $\mathfrak{A}$ *und* $m > 1$, *falls* $p = 2$ *ist; weiter sei* p^{m_1} *die Maximalordnung in* $\mathfrak{A}/\{\mathfrak{m}\}$, *wo* $\mathfrak{m}$ *ein Element von in* $\mathfrak{A}$ *maximaler Ordnung ist.*

Dann und nur dann gibt es eine Gruppe $\mathfrak{G}$ [9]), *so daß* $\mathfrak{K}(\mathfrak{G}) = \mathfrak{A}$ *und* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *ein Zyklus der Ordnung* p^n *ist, wenn* $n \leqq m_1$ *ist.*

Beweis: A. Es gebe ein $\mathfrak{G}$, so daß $\mathfrak{K}(\mathfrak{G}) = \mathfrak{A}$ und $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ ein Zyklus der Ordnung p^n ist. Dann existiert gemäß Satz 7 in $\mathfrak{A}$ ein Element $\mathfrak{c}$ der Ordnung p^n und ein Automorphismus α von $\mathfrak{A}$, so daß $\alpha(\mathfrak{c}) = \mathfrak{c}$, $\alpha(\mathfrak{x}) = \mathfrak{x}\mathfrak{c}^x$ für jedes $\mathfrak{x}$ aus $\mathfrak{A}$ ist, und so daß es ein Element $\mathfrak{e}$ in $\mathfrak{A}$ mit $\alpha(\mathfrak{e}) = \mathfrak{e}\mathfrak{c}$ gibt. Hat dann $\mathfrak{e}$ die Ordnung p^e, so wird $1 = \alpha(\mathfrak{e}^{p^e}) = \alpha(\mathfrak{e})^{p^e} = (\mathfrak{e}\mathfrak{c})^{p^e} = \mathfrak{c}^{p^e}$, d. h. $e \geqq n$ und also auch $m_1 \geqq n$.

[8a]) a.) ist eine Folge von c.).

[9]) Und im Allgemeinen sogar mehrere, wesentlich verschiedene; vergl. § 6.

B. Es sei $m_1 \geqq n$; dann gibt es nach dem Lemma dieses § eine direkte Produktzerlegung $\mathfrak{A} = \{\mathfrak{a}\} \times \{\mathfrak{e}\} \times \prod_\nu \{\mathfrak{b}_\nu\}$, wo $\mathfrak{a}$ ein Element der Ordnung p^m, $\mathfrak{e}$ ein Element der Ordnung p^{m_1} ist. — Wir setzen $\mathfrak{c} = \mathfrak{a}^{p^{m-n}}$ und $b_\nu = \begin{Bmatrix} n - x_\nu \\ 0 \end{Bmatrix}$, falls x_ν die Ordnung von $\mathfrak{b}_\nu$ und $n \begin{Bmatrix} \geqq \\ \leqq \end{Bmatrix} x_\nu$ ist. Dann wird durch $\alpha(\mathfrak{a}) = \mathfrak{a}$, $\alpha(\mathfrak{e}) = \mathfrak{e}\mathfrak{c}$, $\alpha(\mathfrak{b}_\nu) = \mathfrak{b}_\nu \mathfrak{c}^{p^{b_\nu}}$ ein Automorphismus von $\mathfrak{A}$ definiert. Ist $\mathfrak{B}$ die Gesamtheit der Elemente $\mathfrak{x}$ mit $\alpha(\mathfrak{x}) = \mathfrak{x}$, so bilden die Elemente $\mathfrak{e}^i$ mit $0 \leqq i < p^n$ ein volles Repräsentantensystem von $\mathfrak{A}/\mathfrak{B}$, und also ist $\mathfrak{A}/\mathfrak{B}$ ein Zyklus der Ordnung p^n. Insbesondere ist $\mathfrak{a}$ Element von $\mathfrak{B}$. Also erfüllen $\mathfrak{A}$, $\mathfrak{B}$ und die Zahlen p^n und p^m die Bedingungen a.)—d.) des Satzes 8, und mithin existiert eine gesuchte Gruppe $\mathfrak{G}$.

Aus Folgerung 1. ergibt sich insbesondere unter Benutzung von Satz 5, § 3. und Satz 6, § 4., daß *jede Gruppe mit zyklischem Kern und zyklischer Faktorgruppe nach dem Kern mit ihrem Kern identisch ist.*

Folgerung 2: *Ist $\mathfrak{A}$ eine kommutative Primärgruppe, so existiert dann und nur dann eine Primärgruppe $\mathfrak{G}$, so daß $\mathfrak{A} = \mathfrak{K}(\mathfrak{G}) < \mathfrak{G}$ und $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ zyklisch ist, wenn die Ordnungen der Elemente von $\mathfrak{A}$ beschränkt und nicht sämtlich 2 sind und $\mathfrak{A}$ nicht zyklisch ist.*

Folgt sofort aus Folgerung 1., da über das n der Folgerung 1. noch verfügt werden kann, wenn man noch Satz 8. d.) berücksichtigt.

§ 6.

Satz 9: *Es sei $\mathfrak{G}^{(i)}$ für $i = 1,2$ eine Gruppe mit zyklischer Faktorgruppe nach dem Kern. Dann und nur dann gibt es eine isomorphe Abbildung von $\mathfrak{G}^{(1)}$ auf $\mathfrak{G}^{(2)}$, wenn es eine isomorphe Abbildung von $\mathfrak{K}(\mathfrak{G}^{(1)})$ auf $\mathfrak{K}(\mathfrak{G}^{(2)})$ gibt, bei der $\mathfrak{Z}(\mathfrak{G}^{(1)})$ in $\mathfrak{Z}(\mathfrak{G}^{(2)})$ übergeht.*

Beweis: Die Notwendigkeit der Bedingung ist trivial, da Kern und Zentrum gruppeninvariant definierte Untergruppen sind. — Sei also die Bedingung erfüllt[9a]). Da $\mathfrak{G}^{(i)}/\mathfrak{K}(\mathfrak{G}^{(i)})$ zyklisch ist, so wird $\mathfrak{G}^{(i)}$ nach Satz 6, § 4. direktes Produkt der Primärkomponenten:

$$\mathfrak{G}^{(i)} = \mathfrak{G}_2^{(i)} \times \mathfrak{G}_3^{(i)} \times \dots \times \mathfrak{G}_p^{(i)} \times \dots$$

und nach Satz 4, § 3. wird

$$\mathfrak{K}(\mathfrak{G}^{(i)}) = \mathfrak{K}(\mathfrak{G}_2^{(i)}) \times \mathfrak{K}(\mathfrak{G}_3^{(i)}) \times \dots \times \mathfrak{K}(\mathfrak{G}_p^{(i)}) \times \dots$$

[9a]) und $\mathfrak{K}(\mathfrak{G}^{(i)}) \neq \mathfrak{Z}(\mathfrak{G}^{(i)})$, da sonst $\mathfrak{G}^{(i)} = \mathfrak{K}(\mathfrak{G}^{(i)})$ und also nichts zu beweisen ist.

und
$$\mathfrak{Z}(\mathfrak{G}^{(i)}) = \mathfrak{Z}(\mathfrak{G}_2^{(i)}) \times \mathfrak{Z}(\mathfrak{G}_3^{(i)}) \times \ldots \times \mathfrak{Z}(\mathfrak{G}_p^{(i)}) \times \ldots$$

Notwendig wird auch $\mathfrak{G}_p^{(i)}/\mathfrak{K}(\mathfrak{G}_p^{(i)})$ zyklisch und die isomorphe Abbildung von $\mathfrak{K}(\mathfrak{G}^{(1)})$ auf $\mathfrak{K}(\mathfrak{G}^{(2)})$, die $\mathfrak{Z}(\mathfrak{G}^{(1)})$ in $\mathfrak{Z}(\mathfrak{G}^{(2)})$ überführt, induziert eine isomorphe Abbildung von $\mathfrak{K}(\mathfrak{G}_p^{(1)})$ auf $\mathfrak{K}(\mathfrak{G}_p^{(2)})$, bei der $\mathfrak{Z}(\mathfrak{G}_p^{(1)})$ in $\mathfrak{Z}(\mathfrak{G}_p^{(2)})$ übergeht. Da schließlich $\mathfrak{G}^{(1)}$ und $\mathfrak{G}^{(2)}$ dann und nur dann isomorph sind, wenn $\mathfrak{G}_p^{(1)}$ und $\mathfrak{G}_p^{(2)}$ für jede Primzahl isomorph sind, so genügt es, unseren Satz für primäre Gruppen $\mathfrak{G}^{(i)}$ zu beweisen. Da nach Satz 5, § 4. der Kern einer derartigen Primärgruppe nur dann hamiltonsch ist, wenn er mit der Gruppe übereinstimmt, so genügt es sogar, sich auf Primärgruppen mit kommutativem Kern zu beschränken.

Sei also jetzt $\mathfrak{G}^{(i)}$ eine zur Primzahl p gehörige Primärgruppe mit kommutativem Kern, so daß $\mathfrak{G}^{(i)}/\mathfrak{K}(\mathfrak{G}^{(i)})$ ein Zyklus der Ordnung p^{n_i} ist. [Notwendig ist $n_i > 0$]. Weiter sei $\varkappa$ eine isomorphe Abbildung von $\mathfrak{K}(\mathfrak{G}^{(1)})$ auf $\mathfrak{K}(\mathfrak{G}^{(2)})$, so daß $\varkappa[\mathfrak{Z}(\mathfrak{G}^{(1)})] = \mathfrak{Z}(\mathfrak{G}^{(2)})$ ist.

Da $\mathfrak{G}^{(i)}/\mathfrak{K}(\mathfrak{G}^{(i)})$ isomorph $\mathfrak{K}(\mathfrak{G}^{(i)})/\mathfrak{Z}(\mathfrak{G}^{(i)})$ wegen Satz 8a., § 5. ist, so folgt $n_1 = n_2 = n$. Weiter müssen die Ordnungen der Elemente $\mathfrak{K}(\mathfrak{G}^{(i)})$ beschränkt sein, und beide Gruppen haben die gleiche Maximalordnung p^m.

Wir führen wieder die analogen Bezeichnungen wie beim Satz 7, § 5. ein. Sei $\mathfrak{r}_i$ Repräsentant einer erzeugenden Restklasse von $\mathfrak{G}^{(i)}/\mathfrak{K}(\mathfrak{G}^{(i)})$, $\mathfrak{r}_i^{p^n} = \mathfrak{a}_i$, ein Element maximaler Ordnung aus $\mathfrak{K}(\mathfrak{G}^{(i)})$, $\mathfrak{r}_i^{p^m} = \mathfrak{c}_i$, d. h. $\mathfrak{c}_i = \mathfrak{a}_i^{p^{m-n}}$, $\mathfrak{r}_i^{-1}\mathfrak{x}\,\mathfrak{r}_i = \alpha_i(\mathfrak{x})$ für $\mathfrak{x}$ aus $\mathfrak{K}(\mathfrak{G}^{(i)})$. Dann wird $\alpha_i(\mathfrak{x}) = \mathfrak{x}\mathfrak{c}_i^{h(\mathfrak{x})}$ mit $0 \leqq h(\mathfrak{x}) < p^n$, $\alpha_i(\mathfrak{a}_i) = \mathfrak{a}_i$, und es gibt Elemente $\mathfrak{e}_i$, so daß $\alpha_i(\mathfrak{e}_i) = \mathfrak{c}_i\mathfrak{e}_i$ ist.

Wir zeigen zunächst:

(25) *Ist v eine zu p teilerfremde Zahl, so gibt es einen Automorphismus γ von $\mathfrak{K}(\mathfrak{G}^{(2)})$, so daß*
$$\gamma(\mathfrak{a}_2) = \mathfrak{a}_2$$
und
$$\alpha_2[\gamma(\mathfrak{x})]\,\gamma(\mathfrak{x}^{-1}) = \mathfrak{c}_2^{v h(\mathfrak{x})}$$
ist.

Beweis: Nach dem Lemma des § 5. gibt es eine direkte Produktzerlegung: $\mathfrak{K}(\mathfrak{G}^{(2)}) = \{\mathfrak{a}_2\} \times \prod\limits_{\nu}\{\mathfrak{b}_\nu\}$. Dann definieren wir durch $\gamma(\mathfrak{a}_2) = \mathfrak{a}_2$, $\gamma(\mathfrak{b}_\nu) = \mathfrak{b}_\nu^v$ einen Automorphismus von $\mathfrak{K}(\mathfrak{G}^{(2)})$, und es wird $\gamma(\mathfrak{c}_2) = \mathfrak{c}_2$.

Ist $\mathfrak{x}$ aus $\mathfrak{K}(\mathfrak{G}^{(2)})$ beliebig, so läßt sich $\mathfrak{x}$ auf genau eine Weise auf die Form $\mathfrak{a}_2^x\mathfrak{y}$ bringen, wo $\mathfrak{y}$ ein Ausdruck in den $\mathfrak{b}_\nu$ ist, und es wird

$$\alpha_2(\mathfrak{x})\mathfrak{x}^{-1} = \alpha_2(\mathfrak{y})\mathfrak{y}^{-1} = \mathfrak{c}_2^{h(\mathfrak{x})}$$

und
$$\begin{aligned}\alpha_2[\gamma(\mathfrak{x})]\gamma(\mathfrak{x})^{-1} &= \alpha_2[\gamma(\mathfrak{y})]\gamma(\mathfrak{y})^{-1}, \text{ da } \gamma(\mathfrak{a}_2) = \mathfrak{a}_2 \text{ ist} \\ &= \alpha_2[\mathfrak{y}^v]\mathfrak{y}^{-v} = [\alpha_2(\mathfrak{y})\mathfrak{y}^{-1}]^v = \mathfrak{c}_2^{vh(\mathfrak{y})} \\ &= \mathfrak{c}_2^{vh(\mathfrak{x})}.\end{aligned}$$

(26) *Es gibt einen Automorphismus δ von $\mathfrak{K}(\mathfrak{G}^{(2)})$, so daß $\delta(\mathfrak{x}) \equiv \mathfrak{x} \bmod \mathfrak{Z}(\mathfrak{G}^{(2)})$ und $\delta[\varkappa(\mathfrak{a}_1)] = \mathfrak{a}_2$ ist.*

Beweis: Wir bemerken zunächst, daß $\mathfrak{Z}(\mathfrak{G}^{(i)})$ die Gesamtheit der bei α_i invarianten Elemente aus $\mathfrak{K}(\mathfrak{G}^{(i)})$ ist. $\mathfrak{a}_i$ ist also Element von $\mathfrak{Z}(\mathfrak{G}^{(i)})$ und wegen unserer Bedingung ist auch $\varkappa(\mathfrak{a}_1)$ in $\mathfrak{Z}(\mathfrak{G}^{(2)})$ enthalten. Weiter sind $\mathfrak{a}_1$, $\mathfrak{a}_2$ und $\varkappa(\mathfrak{a}_1)$ Elemente der in $\mathfrak{K}(\mathfrak{G}^{(i)})$ maximalen Ordnung p^m.

Fall 1: $\{\varkappa(\mathfrak{a}_1)\} \cap \{\mathfrak{a}_2\} = \{1\}$.

Dann gibt es nach dem Lemma des § 5. eine direkte Produktzerlegung

$$\mathfrak{K}(\mathfrak{G}^{(2)}) = \{\mathfrak{a}_2\} \times \{\varkappa(\mathfrak{a}_1)\} \times \prod_\nu \{\mathfrak{b}_\nu\}$$

und durch $\delta(\mathfrak{a}_2) = \varkappa(\mathfrak{a}_1)$, $\delta[\varkappa(\mathfrak{a}_1)] = \mathfrak{a}_2$, $\delta(\mathfrak{b}_\nu) = \mathfrak{b}_\nu$ wird ein Automorphismus von $\mathfrak{K}(\mathfrak{G}^{(2)})$ definiert, der die verlangten Eigenschaften hat, da $\mathfrak{a}_2$ und $\varkappa(\mathfrak{a}_1)$ in $\mathfrak{Z}(\mathfrak{G}^{(2)})$ enthalten sind.

Fall 2: $\{\varkappa(\mathfrak{a}_1)\} \cap \{\mathfrak{a}_2\} > \{1\}$.

Dann erzeugen entweder $\mathfrak{a}_2$ und $\varkappa(\mathfrak{a}_1)$ denselben Zyklus, oder $\varkappa(\mathfrak{a}_1)\mathfrak{a}_2^{-1}$ ist ein Element niederer als p^m-ter Ordnung. Jedenfalls gibt es nach dem Lemma des § 5. eine direkte Produktzerlegung

$$\mathfrak{K}(\mathfrak{G}^{(2)}) = \{\mathfrak{a}_2\} \times \prod_\nu \{\mathfrak{b}_\nu\},$$

und es ist ebenfalls

$$\mathfrak{K}(\mathfrak{G}^{(2)}) = \{\varkappa(\mathfrak{a}_1)\} \times \prod_\nu \{\mathfrak{b}_\nu\}.$$

Also wird durch $\delta[\varkappa(\mathfrak{a}_1)] = \mathfrak{a}_2$, $\delta(\mathfrak{b}_\nu) = \mathfrak{b}_\nu$ wieder ein gesuchter Automorphismus von $\mathfrak{K}(\mathfrak{G}^{(2)})$ definiert, womit (26) voll bewiesen ist.

Es sei jetzt $\mathfrak{e}$ ein Element aus $\mathfrak{K}(\mathfrak{G}^{(1)})$ mit $\alpha_1(\mathfrak{e}) = \mathfrak{e}\mathfrak{c}_1$. Dann wird

$$\alpha_1(\mathfrak{x})\mathfrak{x}^{-1} = \mathfrak{c}_1^{h(\mathfrak{x})} = \alpha_1(\mathfrak{e}^{h(\mathfrak{x})})\mathfrak{e}^{-h(\mathfrak{x})}.$$

Weiter ist nach unserer Bedingung dann und nur dann $\alpha_1(\mathfrak{x}) = \mathfrak{x}$, wenn $\alpha_2[\varkappa(\mathfrak{x})] = \varkappa(\mathfrak{x})$ ist, oder gleichwertig:

Dann und nur dann ist $\alpha_1(\mathfrak{x})\mathfrak{x}^{-1} = \alpha_1(\mathfrak{y})\mathfrak{y}^{-1}$, wenn

$$\alpha_2[\varkappa(\mathfrak{x})]\varkappa(\mathfrak{x})^{-1} = \alpha_2[\varkappa(\mathfrak{y})]\varkappa(\mathfrak{y})^{-1} \text{ ist.}$$

Also ist insbesondere dann und nur dann

$\alpha_1(\mathfrak{x})\mathfrak{x}^{-1} = \alpha_1(\mathfrak{e}^{h(\mathfrak{x})})\mathfrak{e}^{-h(\mathfrak{x})}$, wenn $\alpha_2[\varkappa(\mathfrak{x})]\varkappa(\mathfrak{x})^{-1} = \alpha_2[\varkappa(\mathfrak{e})^{h(\mathfrak{x})}]\varkappa(\mathfrak{e})^{-h(\mathfrak{x})}$ ist, und mithin gilt:

$$\mathfrak{c}_2^{h[\varkappa(\mathfrak{x})]} = \mathfrak{c}_2^{h[\varkappa(\mathfrak{e})]h(\mathfrak{x})}.$$

Insbesondere muß $h[\varkappa(\mathfrak{e})]$ zu p teilerfremd sein, da ja $\varkappa$ eine isomorphe Abbildung von $\mathfrak{K}(\mathfrak{G}^{(1)})/\mathfrak{Z}(\mathfrak{G}^{(1)})$ auf $\mathfrak{K}(\mathfrak{G}^{(2)})/\mathfrak{Z}(\mathfrak{G}^{(2)})$ induziert.

Sei jetzt v so bestimmt, daß $vh[\varkappa(\mathfrak{e})] \equiv 1 \mod p^n$ ist. Dann bilden wir einen Automorphismus γ für dieses v gemäß (25) und weiter sei δ ein Automorphismus gemäß (26). Wir setzen

$$\eta(\mathfrak{x}) = \gamma(\delta[\varkappa(\mathfrak{x})]) \text{ für } \mathfrak{x} \text{ aus } \mathfrak{K}(\mathfrak{G}^{(1)}),$$

und es wird

$$\eta(\mathfrak{a}_1) = \gamma(\delta[\varkappa(\mathfrak{a}_1)]) = \gamma(\mathfrak{a}_2) = \mathfrak{a}_2, \text{ also auch } \eta(\mathfrak{c}_1) = \mathfrak{c}_2$$

und weiter

$$\eta[\alpha_1(\mathfrak{x})\mathfrak{x}^{-1}] = \eta[\mathfrak{c}_1^{h(\mathfrak{x})}] = \mathfrak{c}_2^{h(\mathfrak{x})}$$

und

$$\begin{aligned}\alpha_2[\eta(\mathfrak{x})]\,\eta(\mathfrak{x})^{-1} &= \alpha_2\big(\gamma[\delta(\varkappa[\mathfrak{x}])]\big) \cdot \gamma\big(\delta[\varkappa(\mathfrak{x})]\big)^{-1} \\ &= \mathfrak{c}_2^{h(\gamma[\delta(\varkappa[\mathfrak{x}])])} = \mathfrak{c}_2^{vh[\varkappa(\mathfrak{x})]}.\end{aligned}$$

Da nun $vh[\varkappa(\mathfrak{e})] \equiv 1 \mod p^n$ ist, so ist $h[\varkappa(\mathfrak{x})] \equiv h[\varkappa(\mathfrak{e})]h(\mathfrak{x}) \mod p^n$ gleichwertig mit $vh[\varkappa(\mathfrak{x})] \equiv h(\mathfrak{x}) \mod p^n$, d. h. es ist

$$\eta[\alpha_1(\mathfrak{x})\mathfrak{x}^{-1}] = \mathfrak{c}_2^{h(\mathfrak{x})} = \mathfrak{c}_2^{vh[\varkappa(\mathfrak{x})]} = \mathfrak{c}_2^{h[\eta(\mathfrak{x})]} = \alpha_2[\eta(\mathfrak{x})]\,\eta(\mathfrak{x})^{-1}.$$

Wir definieren jetzt:

$$\varphi(\mathfrak{r}_1^x\mathfrak{x}) = \mathfrak{r}_2^x\eta(\mathfrak{x}) \text{ für } 0 \leqq x < p^n, \quad \mathfrak{x} \text{ aus } \mathfrak{K}(\mathfrak{G}^{(1)}).$$

Offenbar ist φ eine eindeutige Abbildung von $\mathfrak{G}^{(1)}$ auf $\mathfrak{G}^{(2)}$ und es ist $\varphi(\mathfrak{G}^{(1)}) = \mathfrak{G}^{(2)}$, da η ein Isomorphismus ist.

Ist $\mathfrak{r}_2^x\eta(\mathfrak{x}) = \mathfrak{r}_2^y\eta(\mathfrak{y})$, so ist $x \equiv y \mod p^n$, also wegen der Normierung $x = y$, also $\eta(\mathfrak{x}) = \eta(\mathfrak{y})$, also $\mathfrak{x} = \mathfrak{y}$, d. h. φ ist umkehrbar eindeutig.

Schließlich ist

$$\begin{aligned}\varphi(\mathfrak{r}_1^x\mathfrak{x})\varphi(\mathfrak{r}_1^y\mathfrak{y}) &= \mathfrak{r}_2^x\eta(\mathfrak{x})\,\mathfrak{r}_2^y\eta(\mathfrak{y}) \\ &= \mathfrak{r}_2^{x+y}\mathfrak{c}_2^{h[\eta(\mathfrak{x})]}\,\eta(\mathfrak{x}\,\mathfrak{y}),\end{aligned}$$

und wenn $x + y = z + tp^n$ mit $0 \leqq z < p^n$ ist,

$$\begin{aligned}&= \mathfrak{r}_2^z\mathfrak{a}_2^t\mathfrak{c}_2^{h[\eta(\mathfrak{x})]}\,\eta(\mathfrak{x}\,\mathfrak{y}) \\ &= \mathfrak{r}_2^z\eta(\mathfrak{a}_1^t\mathfrak{c}_1^{h(\mathfrak{x})}\,\mathfrak{x}\,\mathfrak{y}) \\ &= \varphi(\mathfrak{r}_1^z\mathfrak{a}_1^t\mathfrak{c}_1^{h(\mathfrak{x})}\,\mathfrak{x}\,\mathfrak{y}) \\ &= \varphi(\mathfrak{r}_1^{x+y}\mathfrak{c}_1^{h(\mathfrak{x})}\,\mathfrak{x}\,\mathfrak{y}) \\ &= \varphi(\mathfrak{r}_1^x\mathfrak{x}\,\mathfrak{r}_1^y\mathfrak{y}),\end{aligned}$$

womit der Satz voll bewiesen ist.

Folgerung 1: *Ist* $\mathfrak{K}(\mathfrak{G}^{(1)}) = \mathfrak{K}(\mathfrak{G}^{(2)}) = \mathfrak{A}$ *kommutativ* [10]) *und* $\mathfrak{G}^{(i)}/\mathfrak{K}(\mathfrak{G}^{(i)})$ *zyklisch, so sind* $\mathfrak{G}^{(1)}$ *und* $\mathfrak{G}^{(2)}$ *dann und nur dann isomorph, wenn* $\mathfrak{G}^{(1)}$ *und* $\mathfrak{G}^{(2)}$ *in* $\mathfrak{A}$ [*bezgl. der Gruppe aller Automorphismen von* $\mathfrak{A}$] *konjugierte Automorphismengruppen induzieren.*

Beweis: Ist nämlich einerseits φ eine isomorphe Abbildung von $\mathfrak{G}^{(1)}$ auf $\mathfrak{G}^{(2)}$, so induziert φ in $\mathfrak{A}$ einen Automorphismus β. Ist $\{\alpha_i\}$ die von $\mathfrak{G}^{(i)}$ in $\mathfrak{A}$ induzierte [zyklische] Automorphismengruppe, so wird etwa $\alpha_i(\mathfrak{x}) = \mathfrak{r}_i^{-1}\mathfrak{x}\,\mathfrak{r}_i$ und $\beta[\alpha_1(\mathfrak{x})] = \mathfrak{r}_2^{-v}\beta(\mathfrak{x})\mathfrak{r}_2^v = \alpha_2^v[\beta(\mathfrak{x})]$ mit zu p teilerfremden v und also $\beta^{-1}\{\alpha_1\}\beta = \{\alpha_2\}$.

Ist umgekehrt β ein Automorphismus von $\mathfrak{A}$, so daß $\beta^{-1}\{\alpha_1\}\beta = \{\alpha_2\}$ ist, so wird $\beta[\alpha_1(\beta^{-1}[\mathfrak{x}])] = \alpha_2^v(\mathfrak{x})$ mit zu p teilerfremden v oder $\beta[\alpha_1(\mathfrak{x})] = \alpha_2^v[\beta(\mathfrak{x})]$. Also ist dann und nur dann $\mathfrak{x}$ in $\mathfrak{Z}(\mathfrak{G}^{(1)})$, wenn $\beta(\mathfrak{x})$ in $\mathfrak{Z}(\mathfrak{G}^{(2)})$ liegt, d. h. $\beta[\mathfrak{Z}(\mathfrak{G}^{(1)})] = \mathfrak{Z}(\mathfrak{G}^{(2)})$, und mithin sind $\mathfrak{G}^{(1)}$ und $\mathfrak{G}^{(2)}$ nach Satz 9 isomorph.

Folgerung 2: *Es sei* $\mathfrak{A}$ *eine kommutative Primärgruppe,* p^m *die* [*endliche*] *Maximalordnung der Elemente von* $\mathfrak{A}$ *und* $m > 1$, *wenn* $p = 2$ *ist. Weiter sei* $\mathfrak{B}$ *eine Untergruppe von* $\mathfrak{A}$, *die Elemente von in* $\mathfrak{A}$ *maximaler Ordnung enthält, und es sei* $\mathfrak{A}/\mathfrak{B}$ *zyklisch* [*von einer* p^m *nicht überschreitenden Ordnung*].

Dann gibt es eine und im wesentlichen nur eine Primärgruppe $\mathfrak{G}$, *so daß* $\mathfrak{K}(\mathfrak{G}) = \mathfrak{A}$, $\mathfrak{Z}(\mathfrak{G}) = \mathfrak{B}$ *und* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *zyklisch ist.*

Daß es wenigstens eine derartige Gruppe $\mathfrak{G}$ gibt, folgt aus Satz 8, und daß es im wesentlichen nur eine gibt, aus Satz 9.

§ 7.

Es soll noch der Zusammenhang zwischen dem Begriff des *Kerns* und der Theorie der *situationstreuen Abbildungen* untersucht werden. Dabei ist unter einer situationstreuen Abbildung α einer Gruppe $\mathfrak{G}$ auf eine Gruppe $\mathfrak{G}^*$ eine eineindeutige Abbildung der Gesamtheit der Untergruppen von $\mathfrak{G}$ auf die Gesamtheit der Untergruppen von $\mathfrak{G}^*$ zu verstehen, so daß gilt:

a.) Ist $\mathfrak{U}$ eine Untergruppe von $\mathfrak{G}$, so haben $\mathfrak{U}$ und $\alpha(\mathfrak{U})$ die gleiche Mächtigkeit;

b.) Die Gesamtheit der Restklassen von $\mathfrak{G}$ nach $\mathfrak{U}$ hat dieselbe Mächtigkeit wie die Gesamtheit der Restklassen von $\mathfrak{G}^*$ nach $\alpha(\mathfrak{U})$;

c.) Dann und nur dann ist $\mathfrak{U}_1 \leqq \mathfrak{U}_2$, wenn $\alpha(\mathfrak{U}_1) \leqq \alpha(\mathfrak{U}_2)$ ist;

d.) Sind $\mathfrak{U}$ und $\mathfrak{B}$ Untergruppen der Untergruppe $\mathfrak{W}$, so sind $\mathfrak{U}$ und $\mathfrak{B}$ dann und nur dann in $\mathfrak{W}$ konjugiert, wenn $\alpha(\mathfrak{U})$ und $\alpha(\mathfrak{B})$ in $\alpha(\mathfrak{W})$ konjugiert sind. [11])

[10]) Wenn $\mathfrak{A}$ nicht kommutativ ist, gilt eine analoge Aussage.

[11]) Vergl. R. Baer [Sitzungsber. Heidelberg 1933, Nr. 2, 12—17].

Der Kern einer Gruppe besteht aus genau den Gruppenelementen, die in ihr die identische situationstreue Abbildung induzieren [entsprechend wie das Zentrum aus genau den Elementen besteht, die den identischen Automorphismus induzieren].

(27) *Ist* α *eine situationstreue Abbildung von* $\mathfrak{G}$ *auf* $\mathfrak{G}^*$, *so ist* $\alpha[\mathfrak{K}(\mathfrak{G})] = \mathfrak{K}(\mathfrak{G}^*) = \mathfrak{K}[\alpha(\mathfrak{G})]$.

Ist nämlich $\mathfrak{g}$ aus $\mathfrak{G}$ beliebig, so ist

$$\alpha[\{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\}] = \{\alpha[\mathfrak{K}(\mathfrak{G})], \alpha[\{\mathfrak{g}\}]\}.$$

Da $\{\mathfrak{g}\}$ Normalteiler von $\{\mathfrak{K}(\mathfrak{G}), \mathfrak{g}\}$ ist, so ist $\alpha[\{\mathfrak{g}\}]$ Normalteiler von $\{\alpha[\mathfrak{K}(\mathfrak{G})], \alpha[\{\mathfrak{g}\}]\}$. Da weiter $\mathfrak{K}(\mathfrak{G}^*)$ die größte Untergruppe von $\mathfrak{G}^*$ ist, so daß $\{\mathfrak{g}^*\}$ für jedes $\mathfrak{g}^*$ aus $\mathfrak{G}^*$ Normalteiler von $\{\mathfrak{K}(\mathfrak{G}^*), \mathfrak{g}^*\}$ ist, so muß nach dem eben bewiesenen $\mathfrak{K}(\mathfrak{G}^*) \geqq \alpha[\mathfrak{K}(\mathfrak{G})]$ gelten. Also gilt auch $\mathfrak{K}(\mathfrak{G}) \geqq \alpha^{-1}[\mathfrak{K}(\mathfrak{G}^*)]$ und mithin $\mathfrak{K}(\mathfrak{G}^*) = \alpha[\mathfrak{K}(\mathfrak{G})]$, wie behauptet.

Sei jetzt Σ ein System von Untergruppen von $\mathfrak{G}$. Ist $\mathfrak{g}$ ein Element aus $\mathfrak{G}$, so ist

$$\alpha_{\mathfrak{g}}(\mathfrak{U}) = \mathfrak{g}^{-1}\mathfrak{U}\mathfrak{g} \text{ für jedes } \mathfrak{U} \text{ aus } \Sigma$$

eine situationstreue Abbildung von Σ. Ist weiter $\mathfrak{A}$ eine Untergruppe von $\mathfrak{G}$, so sei $A(\mathfrak{A}; \Sigma)$ die Gesamtheit der $\alpha_{\mathfrak{g}}(\mathfrak{U})$ für $\mathfrak{g}$ aus $\mathfrak{A}$, $\mathfrak{U}$ aus Σ.

(28) *Ist* σ *eine situationstreue Abbildung von* $\mathfrak{G}$, *die sich zu einer isomorphen Abbildung erweitern läßt, so ist*

$$A[\sigma(\mathfrak{A}); \sigma(\Sigma)] = \sigma[A(\mathfrak{A}; \Sigma)]$$

für jede Untergruppe $\mathfrak{A}$ *von* $\mathfrak{G}$ *und jedes System* Σ.

Ist nämlich φ eine σ umfassende, isomorphe Abbildung von $\mathfrak{G}$, so wird:

$$\begin{aligned}\sigma[\alpha_{\mathfrak{g}}(\mathfrak{U})] = \sigma[\mathfrak{g}^{-1}\mathfrak{U}\mathfrak{g}] &= \varphi[\mathfrak{g}^{-1}\mathfrak{U}\mathfrak{g}] = \varphi(\mathfrak{g}^{-1})\varphi(\mathfrak{U})\varphi(\mathfrak{g}) \\ &= \varphi(\mathfrak{g})^{-1}\sigma(\mathfrak{U})\varphi(\mathfrak{g}) \\ &= \alpha_{\varphi(\mathfrak{g})}[\sigma(\mathfrak{U})].\end{aligned}$$

Da $\{\varphi(\mathfrak{g})\} = \sigma[\{\mathfrak{g}\}]$ ist, so induzieren die Elemente aus $\sigma(\mathfrak{A})$ in (Σ) genau die Abbildungen aus $\sigma[A(\mathfrak{A}; \Sigma)]$, wie behauptet.

(29) *Ist* σ *eine situationstreue Abbildung von* $\mathfrak{G}$, *so daß für jede zyklische Untergruppe* $\mathfrak{A}$ *von* $\mathfrak{G}$ *gilt*

$$A[\sigma(\mathfrak{A}); \sigma(\Sigma)] = \sigma[A(\mathfrak{A}; \Sigma)],$$

wo Σ *das System aller zyklischen Untergruppen von* $\mathfrak{G}$ *ist, so gibt es eine* σ *umfassende, isomorphe Abbildung von* $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ *auf* $\sigma(\mathfrak{G})/\mathfrak{K}[\sigma(\mathfrak{G})]$.

Wegen (27) ist sicher $\sigma[\mathfrak{K}(\mathfrak{G})] = \mathfrak{K}[\sigma(\mathfrak{G})]$.

Ist weiter $\mathfrak{g}$ aus $\mathfrak{G}$, $\mathfrak{g}^*$ aus $\sigma(\mathfrak{G})$, so sagen wir: $\mathfrak{g} \longleftrightarrow \mathfrak{g}^*$, wenn $\sigma[\alpha_{\mathfrak{g}}(\mathfrak{U})] = \alpha_{\mathfrak{g}^*}[\sigma(\mathfrak{U})]$ für alle zyklischen Untergruppen $\mathfrak{U}$ von $\mathfrak{G}$ gilt.

Ist etwa $\mathfrak{a} \longleftrightarrow \mathfrak{a}^*$ und $\mathfrak{b}^{-1} \longleftrightarrow \mathfrak{b}^{-1*}$, so wird

$$\begin{aligned}\sigma[\alpha_{\mathfrak{a}\mathfrak{b}^{-1}}(\mathfrak{U})] &= \sigma[\mathfrak{b}(\mathfrak{a}^{-1}\mathfrak{U}\,\mathfrak{a})\mathfrak{b}^{-1}] = \sigma[\alpha_{\mathfrak{b}^{-1}}(\mathfrak{a}^{-1}\mathfrak{U}\,\mathfrak{a})] = \\ &= \alpha_{\mathfrak{b}^{-1*}}[\sigma(\alpha_{\mathfrak{a}}[\mathfrak{U}])] \\ &= \alpha_{\mathfrak{b}^{-1*}}[\alpha_{\mathfrak{a}^*}(\mathfrak{U})] \\ &= \alpha_{\mathfrak{a}^*\mathfrak{b}^{-1*}}(\mathfrak{U}), \quad \text{d. h.}\end{aligned}$$

$\mathfrak{a}\mathfrak{b}^{-1} \longleftrightarrow \mathfrak{a}^*\mathfrak{b}^{-1*}$.

Ist weiter $1 \longleftrightarrow \mathfrak{a}^*$, so ist $\alpha_{\mathfrak{a}^*}[\sigma(\mathfrak{U})] = \sigma[\alpha_1(\mathfrak{U})] = \sigma(\mathfrak{U})$ für alle zyklischen Untergruppen $\mathfrak{U}$ von $\mathfrak{G}$ und also $\mathfrak{a}^*$ in $\mathfrak{K}[\sigma(\mathfrak{G})]$ und umgekehrt. Entsprechend ist dann und nur dann $\mathfrak{a} \longleftrightarrow 1$, wenn $\mathfrak{a}$ in $\mathfrak{K}(\mathfrak{G})$ enthalten ist.

Ist schließlich $\mathfrak{a} \longleftrightarrow \mathfrak{a}^*$, $\mathfrak{a}^{-1} \longleftrightarrow \mathfrak{a}^{-1*}$, so wird

$1 = \mathfrak{a}\mathfrak{a}^{-1} \longleftrightarrow \mathfrak{a}^*\mathfrak{a}^{-1*}$, d. h. $\mathfrak{a}^*\mathfrak{a}^{-1*}$ ist in $\mathfrak{K}[\sigma(\mathfrak{G})]$ enthalten.

Mithin vermittelt $\mathfrak{g} \longleftrightarrow \mathfrak{g}^*$ eine einstufig isomorphe Abbildung einer Untergruppe von $\mathfrak{G}/\mathfrak{K}(\mathfrak{G})$ auf eine Untergruppe von $\sigma(\mathfrak{G})/\mathfrak{K}[\sigma(\mathfrak{G})]$ und wegen der Bedingung von (29) ist das eine isomorphe Abbildung der beiden Gruppen aufeinander.

Aus (28) und (29) folgt insbesondere:

(30) *Ist* $\mathfrak{K}(\mathfrak{G}) = \{1\}$, *so läßt sich die situationstreue Abbildung* σ *von* $\mathfrak{G}$ *dann und nur dann zu einem Isomorphismus erweitern, wenn*

$$A[\sigma(\mathfrak{A}); \sigma(\Sigma)] = \sigma[A(\mathfrak{A}; \Sigma)]$$

für alle zyklischen Untergruppen $\mathfrak{A}$ *von* $\mathfrak{G}$ *und das System* Σ *aller zyklischen Untergruppen von* $\mathfrak{G}$ *gilt.*

(Eingegangen den 9. November 1933.)