ÜBER DEN QUASINORMALTEILER DER REGULÄREN p-GRUPPE VON DER KLASSE 2

KIRIO NAKAMURA

In der vorliegenden Arbeit wird untersucht, was für eine Struktur eine Untergruppe $\mathfrak{N}$ von endlicher p-Gruppe $\mathfrak{G}$ habe, wenn $\mathfrak{N}$ mit jeder Untergruppe von $\mathfrak{G}$ als ganzes vertauschbar ist. In diesen $\mathfrak{N}$ tritt natürlich ein nicht nur aus E bestehender Normalteiler von $\mathfrak{G}$ auf und er enthält ein Zentrumselement von der Ordnung p. Wir fragen: Gilt das Ähnliche auch, falls $\mathfrak{N}$ kein Normalteiler ist? Die gestellte Frage läßt sich für regülare $\mathfrak{G}$ beantworten, deren Klasse 2 ist, aber für andere bleibt sie noch offen. Bevor wir diese Frage untersuchen, stellen wir einige Definitionen und nötige Sätze und Hilfssätze zusammen.

1. Bezeichnungen

Im folgenden bedeuten $\mathfrak{A}$, $\mathfrak{B}$, . . . eine Gruppe von endlicher Ordnung $|\mathfrak{A}|$, $|\mathfrak{B}|$, . . . und A, B, . . . ihre Elemente mit der Ordnung $|A|$, $|B|$, . . . Das Erzeugnis von A, B, . . . bezeichnen wir mit $\{A, B, \ldots\}$. Das Zentrum oder die Kommutatorgruppe von $\mathfrak{G}$ bezeichnen wir mit $\mathfrak{Z}$ oder $\mathfrak{G}'$. Ist $\mathfrak{A}$ und $\mathfrak{B}$ als ganzes vertauschbar, so bezeichnen wir mit $\mathfrak{A} \vee \mathfrak{B}$ und das Produkt $\mathfrak{A}\mathfrak{B}$ ist bekanntlich eine Gruppe. Ist $\mathfrak{N}\mathfrak{H} = \mathfrak{H}\mathfrak{N}$ für ein festes $\mathfrak{N}$ und für ein beliebiges $\mathfrak{H} \subseteq \mathfrak{G}$, so heißt $\mathfrak{N}$ quasi-normal in $\mathfrak{G}$ oder ein Quasinormalteiler von $\mathfrak{G}$ und schreiben wir $\mathfrak{G} \underline{\mathfrak{D}} \mathfrak{N}$. Wir betrachten allerdings $\mathfrak{N}$ für $\mathfrak{G} \neq \mathfrak{N} \neq \mathfrak{E}$ lauter. Gelte ebenso für ein festes $N \in \mathfrak{G}$ mit $|N| = p$ und ein beliebiges $G \in \mathfrak{G}$ $[N, G] = G^{p^{g-1}}$ oder E, dann nennen wir N ein Kernelement von $\mathfrak{G}$ und bezeichnen mit $N \in \mathfrak{K}_p$. Dabei sei $N \overline{\in} \mathfrak{Z}$ und für $g = 1$ $[N, G] = E$. Dagegen bezeichnen wir mit $N \in \mathfrak{Z}_p$, falls $|N| = p$ und $N \in \mathfrak{Z}$ ist. Ist $\mathfrak{G}$ regülär (im Sinne von P. Hall s. Satz (A) in 1) und $|G| \leqq p^{\alpha}$, bilden G und E eine charakteristische Untergruppe von $\mathfrak{G}$, die wir mit $\Omega_{\alpha}(\mathfrak{G})$ schreiben. In 3 sind alle betrachteten Gruppen p-Gruppe von der Klasse 2 für $p > 2$ und wir schreiben $|A| = p^a$, $|B| = p^b$, . . . für jedes A, B, . . . $\in \mathfrak{G}$, außer wenn wir besonders angeben werden.

Received June 4, 1965.

2. Reguläre p-Gruppe

Wir benutzen oft die Sätze von P. Hall, die die Struktur der regulären p-Gruppe ans Licht kommen lassen. Daher wollen wir diese Sätze hervorheben. Als eine Charakterisierung der regulären p-Gruppe gilt der

SATZ (A). *$\mathfrak{G}$ ist genau dann regulär, wenn für jedes A und B $(AB)^p = A^pB^pC^p$ mit $C \in \{A, B\}'$ gilt.*

Hiernach nehmen wir $\mathfrak{G}$ reguläre p-Gruppe an. Das Ähnliche wie der Basissatz der abelschen Gruppe ist der

SATZ (B). *In $\mathfrak{G}$ gibt es das eingeordnete Elementsystem $A_1, A_2, \ldots, A_t$ derart, daß jedes $G \in \mathfrak{G}$ in Form $G = A_1^{x_1}A_2^{x_2}\cdots A_t^{x_t}$ eineindeutig ausgedrückt wird.*

Wir nennen dieses Elementsystem eine Basis von $\mathfrak{G}$. Weiter folgt der

SATZ (C). *Die Basis von $\mathfrak{G}$ kann in folgender Art aufgenommen werden.*

1) $|A_1| \geqq |A_2| \geqq \cdots \geqq |A_t|$

2) *Ist $|A_1| \geqq |A_2| \geqq \cdots \geqq |A_s|$ und $|A_s| > |A_{s+1}|$, so gehört A_i $(1 \leqq i \leqq s)$ als Vertreter genau einem Element der Basis von $\mathfrak{G}/\Omega_{\mu-1}(\mathfrak{G})$, wobei $|G| = p^\mu$ für jedes $G \in \mathfrak{G}$ gilt.*

Aus diesen Sätzen erhalten wir den als Permutationssatz geltenden

SATZ (D). *Das Elementsystem $A_{\tau(1)}, A_{\tau(2)}, \ldots, A_{\tau(t)}$ ist auch eine Basis von $\mathfrak{G}$, wobei τ eine Permutation von $1, 2, \ldots, t$ bezeichnet.*

3. Hilfssätze

Es gilt der folgende

HILFSSATZ 1. *Sei $\mathfrak{G} \mathfrak{T} \mathfrak{N}$ und $\mathfrak{N}$ zyklisch. Dann gilt $\mathfrak{G} \mathfrak{D} \mathfrak{N}_1$ derart, daß $\mathfrak{N} \supseteq \mathfrak{N}_1$ und $|\mathfrak{N}_1| = p$ ist.*

Beweis. Wir haben nur $\{G\} \mathrm{v} \mathfrak{N}_1$ für jedes $G \in \mathfrak{G}$ zu zeigen. Sei $\mathfrak{N} = \{N\}$ und $\mathfrak{N}_1 = \{N^{p^{n-1}}\}$ mit $|N| = p^n$. Für beliebiges G von $\mathfrak{G}$ gilt $\{G\} \mathrm{v} \mathfrak{N}$. Falls $\{G\} \cap \mathfrak{N} \neq \mathfrak{E}$ ist, so folgt $\{G\} \cap \mathfrak{N} \supseteq \mathfrak{N}_1$, daher $\{G\} \mathrm{v} \mathfrak{N}_1$. Falls $\{G\} \cap \mathfrak{N} = \mathfrak{E}$ ist, so betrachten wir ein $\mathfrak{H} \subseteq \{G\}\mathfrak{N}$ derart, daß $[\mathfrak{H} : \{G\}] = p$ ist. Da $|\mathfrak{H} \cap \mathfrak{N}| = p$ ist, gilt $\mathfrak{H} \cap \mathfrak{N} = \{N^{p^{n-1}}\}$ und $\mathfrak{H} = \{N^{p^{n-1}}\}\{G\} = \mathfrak{N}_1\{G\}$, daher $\{G\} \mathrm{v} \mathfrak{N}_1$.

Wie wir aus dem Beweis ersehen können, gilt Hilfssatz 1 für allgemeine endliche p-Gruppe.

Nun kommen wir zum Beweis des grundlegenden Hilfssatzes, der recht komplizierte Rechnung erfordert.

HILFSSATZ 2. *Sei* $\mathfrak{G} = \{A, B\}$ *derart, daß* $|A| = |B| = |C| = p^n$ *mit* $[A, B] = C$ *ist, und* $\mathfrak{G} \not\trianglerighteq \mathfrak{N}$. *Dann gilt*

1) *Ist* $A^x B^y \in \mathfrak{Z}$, *so ist* $A^x = B^y = E$.

2) $\mathfrak{G}' = \mathfrak{Z}$.

3) $\mathfrak{N} \cap \mathfrak{Z} \neq \mathfrak{E}$.

Beweis. 1) Es ist $\mathfrak{G}' \subseteq \mathfrak{Z}$, daher $\mathfrak{G}' = \{C\}$. Für jedes $G \in \mathfrak{G}$ haben wir einen Ausdruck $G = A^x B^y C^z$. Sei $G \in \mathfrak{Z}$, dann ist $[A, A^x B^y C^z] = [B, A^x B^y C^z] = E$. Also haben wir $[A, B]^y = C^y = [B, A^x] = C^{-x} = E$, daher $x \equiv y \equiv 0$ (p^n). Folglich gilt $A^x = B^y = E$.

2) Es ist $\mathfrak{G}' \subseteq \mathfrak{Z}$. Sei $G = A^x B^y C^z \in \mathfrak{Z}$, dann ergibt sich aus 1) $A^x = B^y = E$ also $G = C^z \in \mathfrak{G}'$. Dies liefert uns $\mathfrak{G}' \supseteq \mathfrak{Z}$, daher $\mathfrak{G}' = \mathfrak{Z}$.

3) Wir zeigen die Eindeutigkeit des Ausdrucks $G = A^x B^y C^z$. Sei $A^{x_1} B^{y_1} C^{z_1} = A^{x_2} B^{y_2} C^{z_2}$, dann erhalten wir $A^{x_1 - x_2} B^{y_1 - y_2} C^{z_1 - z_2} = E$, daher $A^{x_1 - x_2} = B^{y_1 - y_2} = E$ nach 1). Daraus folgt $A^{x_1} = A^{x_2}$ und $B^{y_1} = B^{y_2}$, also $C^{z_1} = C^{z_2}$. Hiernach führen wir unter der Annahme $\mathfrak{N} \cap \mathfrak{Z} = \mathfrak{E}$ einen Widerspruch. Da $\mathfrak{G}/\mathfrak{G}' \supseteq \mathfrak{N}\mathfrak{G}'/\mathfrak{G}' \simeq \mathfrak{N}/\mathfrak{N} \cap \mathfrak{Z}$ ist, ist $\mathfrak{N}$ abelsch mit den höchstens zwei bestehenden Erzeugenden. Sei $\mathfrak{N} = \{N\}$ mit $|N| = p^m$. Aus Hilfssatz 1 folgt $\mathfrak{G} \not\trianglerighteq \{N^{p^{m-1}}\}$, daher $\{N^{p^{m-1}}\} \mathrm{v} \{A\}$ und $\{N^{p^{m-1}}\} \mathrm{v} \{B\}$. Das ergibt $[N^{p^{m-1}}, A] \in \{N^{p^{m-1}}, A\}' \subseteq \{A\}$. Aus 1) haben wir $\{A\} \cap \mathfrak{Z} = \{A\} \cap \mathfrak{G}' = \mathfrak{E}$ und $[N^{p^{m-1}}, A] = E$. Daraus folgt auch $[N^{p^{m-1}}, B] = E$, also $N^{p^{m-1}} \in \mathfrak{Z}$, was $\mathfrak{N} \cap \mathfrak{Z} \neq \mathfrak{E}$ führt. Wir nehmen also $\mathfrak{N} = \{N_1\} \times \{N_2\}$ mit $N_1 \neq E$ und $N_2 \neq E$ an. Im folgenden sei $i = 1, 2$ oder $i = 1$, $j = 2$ und $i = 2$, $j = 1$, falls nichts besonders ausgesagt wird. Es gebe die Ausdrücke $N_i = A^{x_i p^{\alpha_i}} B^{y_i p^{\beta_i}} C^{z_i p^{\gamma_i}}$, wo x_i, y_i, z_i nicht negative ganzrationale Zahlen modulus p^n aufnehmen und $n > \alpha_i \geqq 0$, $n > \beta_i \geqq 0$, $n > \gamma_i \geqq 0$ gelten. Dann ist nun $N_i^{p^{\delta_i}} = A^{x_i p^{\alpha_i + \delta_i}} B^{y_i p^{\beta_i + \delta_i}} C^{z_i p^{\gamma_i + \delta_i}} C^{p^{\delta_i}(p^{\delta_i} - 1)/2 \times x_i y_i p^{\alpha_i + \beta_i}}$. Ist $\delta_i + \min(\alpha_i, \beta_i) = n$, so ergibt sich $N_i^{p^{\delta_i}} = C^{z_i p^{\gamma_i + \delta_i}}$. Sei $\gamma_i < \min(\alpha_i, \beta_i)$ $(i = 1$ oder $2)$, dann ist $C^{z_i p^{\gamma_i + \delta_i}} \neq E$ $(i = 1$ oder $2)$, daher $\mathfrak{N} \cap \mathfrak{Z} \neq \mathfrak{E}$ und wir schließen $\gamma_i \geqq \min(\alpha_i, \beta_i)$.

(a) Sei $\alpha_i \geqq \beta_i$. Setzen wir $N_i' = A^{x_i p^{\alpha_i - \beta_i}} B^{y_i} C^{z_i p^{\gamma_i - \beta_i} - (x_i y_i / 2) p^{\alpha_i - \beta_i}(p^{\beta_i} - 1)}$, so ist $N_i'^{p^{\beta_i}} = N_i$ und $[N_i', N_j] = C^{x_i y_j p^{\alpha_i - \beta_i + \beta_j} - x_j y_i p^{\alpha_j}}$. Wenn $[N_i', N_j] = E$ gilt, so bekommen wir gleich $x_i y_j p^{\alpha_i - \beta_i + \beta_j} = x_j y_i p^{\alpha_j}$ (p^n). Ist $\beta_j \geqq \beta_i$, so ergibt sich $N_i^{y_j p^{\beta_j - \beta_i}} N_j^{-y_i} \equiv A^{x_i y_j p^{\alpha_i - \beta_i + \beta_j}} B^{y_i y_j p^{\beta_j - \beta_i + \beta_i}} B^{-y_j y_i p^{\beta_j}} A^{-x_j y_i p^{\alpha_j}} = A^{x_i y_j p^{\alpha_i - \beta_i + \beta_j} - x_j y_i p^{\alpha_j}} = E$ modulus $\mathfrak{Z}$, entgegen $\mathfrak{N} \cap \mathfrak{Z} = \mathfrak{E}$ oder $\{N_1\} \cap \{N_2\} = \mathfrak{E}$. In diesem Fall sei $i = 1$,

$j=2$ oder $i=2$, $j=1$.

(b) Sei $\alpha_i \leqq \beta_i$. Wir erwähnen diesen Teil am Schluß.

(c) Sei $\alpha_1 \geqq \beta_1$ und $\alpha_2 \leqq \beta_2$. Setzen wir $N_1' = A^{x_1 p^{\alpha_1-\beta_1}} B^{y_1} C^{z_1 p^{\gamma_1-\beta_1} - (x_1 y_1/2) p^{\alpha_1-\beta_1}(p^{\beta_1}-1)}$ und $N_2' = A^{x_2} B^{y_2 p^{\beta_2-\alpha_2}} C^{z_2 p^{\gamma_2-\alpha_2} - (x_2 y_2/2) p^{\beta_2-\alpha_2}(p^{\alpha_2}-1)}$, dann ist $N_1'^{p^{\beta_1}} = N_1$ und $N_2'^{p^{\alpha_2}} = N_2$. Weiter ist

$$[N_1', N_2] = C^{x_1 y_2 p^{\alpha_1-\beta_1+\beta_2} - x_2 y_1 p^{\alpha_2}} \text{ und } [N_2', N_1] = C^{x_2 y_1 p^{\beta_1} - x_1 y_2 p^{\beta_2-\alpha_2+\alpha_1}}.$$

Für $[N_i', N_j] = E$ ist $x_1 y_2 p^{\alpha_1-\beta_1+\beta_2} \equiv x_2 y_1 p^{\alpha_2}$, $x_2 y_1 p^{\beta_1} \equiv x_1 y_2 p^{\beta_2-\alpha_2+\alpha_1} (p^n)$. Für $\beta_2 \geqq \beta_1$ gilt $N_1'^{y_2 p^{\beta_2-\beta_1}} N_2^{-y_1} = A^{x_1 y_2 p^{\alpha_1-\beta_1+\beta_2}} B^{y_1 y_2 p^{\beta_2-\beta_1+\beta_1}} B^{-y_1 y_2 p^{\beta_2}} A^{-x_2 y_1 p^{\alpha_2}} \equiv E$ modulus $\mathfrak{Z}$ und $\beta_1 \geqq \beta_2$, $\alpha_1 \geqq \beta_1 \geqq \beta_2 \geqq \alpha_2$ ergibt $\alpha_1 \geqq \alpha_2$. Diesmal betrachten wir $N_1^{-x_2} N_2'^{x_1 p^{\alpha_1-\alpha_2}}$ und haben den gleichen Widerspruch.

(d) Sei $\alpha_1 \leqq \beta_1$ und $\alpha_2 \geqq \beta_2$. Wenn wir A mit B und α_i mit β_i vertauschen, so können wir (b), (d) auf je (a), (c) zurückführen.

Es bleibt noch in allen Teilen den Fall $[N_i', N_j] \neq E$ $(i=1, j=2$ oder $i=2, j=1)$. Es gilt ersichtlich $[N_i', N_j] \in \mathfrak{G}' \cap \{N_i'\}\mathfrak{N}$, daher $[N_i', N_j] = C^{\alpha_{ij}} = N_i'^{y_i} N_1^{x_{ij}(1)} N_2^{x_{ij}(2)}$, da $\{N_i'\}\mathfrak{N}$ eine p-Gruppe ist. Weiter ist $N_i'^{y_i} \overline{\in} \mathfrak{N}$. Sonst wäre $\mathfrak{N} \cap \mathfrak{G}' = \mathfrak{N} \cap \mathfrak{Z} \neq \mathfrak{E}$. Wir betrachten $N_i'^{y_i}$. Dann ist $(N_i'^{y_i})^{p^{s_i-1}} = C^{\alpha_{ij} p^{s_i-1}} (N_1^{x_{ij}(1)} N_2^{x_{ij}(2)})^{-p^{s_i-1}} \in \mathfrak{N}$ für $|N_i'^{y_i}| = p^{s_i}$ und $|N_i'^{y_i}| > |N_i^{-x_{ij}(i)}|$, da $\{N_i'\} \supseteq \{N_i'^{y_i}\} \supseteq \{N_i\}$ und $N_i'^{y_i} \overline{\in} \mathfrak{N}$ ist. Das ergibt $N_1'^{y_1 p^{s_1-1}} = C^{\alpha_{12} p^{s_1-1}} N_2^{-x_{12}(2) p^{s_1-1}}$ oder $N_2'^{y_2 p^{s_2-1}} = C^{\alpha_{21} p^{s_2-1}} N_1^{-x_{21}(1) p^{s_2-1}}$. Berücksichtigen wir $E \neq N_i'^{y_i p^{s_i-1}} \in \mathfrak{N}$, so gilt $\mathfrak{N} \cap \mathfrak{Z} \neq \mathfrak{E}$ oder $\{N_1\} \cap \{N_2\} \neq \mathfrak{E}$, entgegen der Annahme.

Weiter gelten die folgende

Hilfssatz 3. *Sei $\mathfrak{G} \mathrel{\dot{\supseteq}} \mathfrak{N}$ und $\mathfrak{G} = \mathfrak{H}\mathfrak{N}$ mit $\mathfrak{H} \cap \mathfrak{N} = \mathfrak{G}' \cap \mathfrak{N} = \mathfrak{E}$. Weiter sei $\mathfrak{H} = \{A, B\}$ derart, daß $|A| = |B| = |C| = p^n$ mit $C = [A, B]$ ist. Dann gilt $\mathfrak{G} = \mathfrak{H} \times \mathfrak{N}$.*

Beweis. Durch Induktion von $|\mathfrak{G}|$. Wenn $|\mathfrak{N}| = p$ und daher $\mathfrak{N} = \{N\}$ ist, so gilt $\{N\} \mathrm{v} \{A\}$ und $\{N\} \mathrm{v} \{B\}$. Daraus folgt $[N, A] = E$ oder $[N, A] = A^{x p^{a-1}}$ und $[N, B] = E$ oder $[N, B] = B^{y p^{a-1}}$. Aus 1) und 2) in Hilfssatz 2 haben wir $\{A\} \cap \mathfrak{G}' = \{B\} \cap \mathfrak{G}' = \mathfrak{E}$, daher $[N, A] = [N, B] = E$: denn $\mathfrak{G}' \cap \mathfrak{H}$ ist im Zentrum von $\mathfrak{H}$ enthalten. Das ergibt sofort $\mathfrak{G} = \mathfrak{H} \times \mathfrak{N}$. Also nehmen wir $|\mathfrak{N}| > p$ an. Wir betrachten $\mathfrak{M} = \mathfrak{H}\mathfrak{N}_1$ mit $\mathfrak{N} \supseteq \mathfrak{N}_1$ und $|\mathfrak{N}_1| = p$. Da $|\mathfrak{N}_1| = p$ ist, ergibt sich $\mathfrak{M} = \mathfrak{H} \times \mathfrak{N}_1$. Daher ist $\mathfrak{N}_1 \subseteq \mathfrak{Z}$, weil $\mathfrak{N}$ abelsch ist. Es gilt eben durch Induktionsvoraussetzung $\mathfrak{G}/\mathfrak{N}_1 \simeq \mathfrak{H}\mathfrak{N}_1/\mathfrak{N}_1 \times \mathfrak{N}/\mathfrak{N}_1$. Daraus folgt für jedes $N \in \mathfrak{N}$ $[N, A] = V^{\alpha}$ und $[N, B] = V^{\beta}$ mit $\mathfrak{N}_1 = \{V\}$, daher $\mathfrak{G} = \mathfrak{H} \times \mathfrak{N}$, da $\mathfrak{G}' \cap \mathfrak{N} = \mathfrak{E}$ ist.

HILFSSATZ 4. *Sei* $\{A\} \cap \{B\} = \mathfrak{E}$ *und* $|N| = p$ *für* $A, B, N \in \mathfrak{G}$ *derart, daß* $\{A\} \mathrm{v} \{N\}$, $\{B\} \mathrm{v} \{N\}$, $\{AB\} \mathrm{v} \{N\}$ *gelten. Dann ist die Behauptung:*

(1) *Ist* $|A| = |B|$, *so ist* $[N, A] = [N, B] = E$ *oder* $[N^x, A] = A^{p^{a-1}}$ *und* $[N^x, B] = B^{p^{a-1}}$.

(2) *Ist* $|A| > |B|$, *so ist* $[N, A] = [N, B] = E$ *oder* $[N^x, A] = A^{p^{a-1}}$ *und* $[N^x, B] = E$.

wobei $x \not\equiv 0 \ (p)$ ist und $[N, G] = G^{p^{g-1}}$ für $g = 1$ $[N, G] = E$ bedeuten soll.

Beweis. Wir betrachten $\mathfrak{A} = \{A\}\{N\}$ und $\mathfrak{B} = \{B\}\{N\}$. Ersichtlich gilt $[N, A] = E$ für $\{N\} \cap \{A\} \neq \mathfrak{E}$. Dagegen ist $[N, A] = A^{\alpha p^{a-1}}$ für $\{N\} \cap \{A\} = \mathfrak{E}$: denn es ist $|\{A, N\}| : |A| = p$, also $\{A, N\} \triangleright \{A\}$. Gleiches gilt für $[N, B]$.

Von nun ab wird $\alpha\beta\gamma \not\equiv 0 \ (p)$ angenommen.

(1) Nun sei $[N, A] = A^{\alpha p^{a-1}}$ für $a > 1$ und $[N, B] = E$. Dann gilt $[N, AB] = [N, A][N, B] = A^{\alpha p^{a-1}} = (AB)^{\gamma p^{a-1}} = A^{\gamma p^{a-1}} B^{\gamma p^{a-1}} [A^\delta, B]^{p^{a-1}} = A^{\gamma p^{a-1}} B^{\gamma p^{a-1}}$, da $A^{\delta p^{a-1}} \in \mathfrak{G}' \subseteq \mathfrak{Z}$ ist, entgegen $\{A\} \cap \{B\} = \mathfrak{E}$ oder $a > 1$. Ebenso $[N, A] = E$ und $[N, B] = B^{\beta p^{a-1}}$ auch nicht gelten. Nächstens gelte $[N, A] = A^{\alpha p^{a-1}}$ und $[N, B] = B^{\beta p^{a-1}}$. Dann muß $[N, AB] = A^{\alpha p^{a-1}} B^{\beta p^{a-1}} = (AB)^{\gamma p^{a-1}} = A^{\gamma p^{a-1}} B^{\gamma p^{a-1}}$ sein, was besagt $\alpha \equiv \beta \equiv \gamma \ (p)$, also $[N^x, A] = A^{p^{a-1}}$ und $[N^x, B] = B^{p^{a-1}}$ für $\alpha x \equiv 1 \ (p)$.

(2) Diesmal sei $[N, A] = E$ und $[N, B] = B^{\beta p^{b-1}}$ für $b > 1$. Dann haben wir $[N, AB] = [N, A][N, B] = B^{\beta p^{b-1}} = (AB)^{\gamma p^{a-1}} = A^{\gamma p^{a-1}} B^{\gamma p^{a-1}} = A^{\gamma p^{a-1}}$, da $b < a$, daher $B^{\beta p^{a-1}} = E$ ist. Hieraus folgt $A^{\gamma p^{a-1}} = B^{\beta p^{b-1}}$, entgegen $\{A\} \cap \{B\} = \mathfrak{E}$.

HILFSSATZ 5. *Seien* $A_1, A_2, \ldots, A_t$ *eine Basis von* $\mathfrak{G}$ *mit der Ordnung* $|A_i| = p^{\mu_i} = p^{\mu}$ *für* $1 \leqq i \leqq s$, *bzw.* $|A_j| = |A_{s+1}| = p^{\mu_2} < p^{\mu}$ *für* $j > s$ (s. Satz (C) in 2). *Für ein* $N \in \mathfrak{G}$ *mit* $|N| = p$ *sind die zwei folgenden Aussagen gleichwertig.*

(1) $N \in \mathfrak{K}_p$

(2) $[N, A_i] = A_i^{p^{a-1}}$ $(1 \leqq i \leqq s)$ $[N, A_j] = E$ $(j \geqq s+1)$.

Beweis. Aus (1) folgt (2). Da $N \overline{\in} \mathfrak{Z}$ ist, gibt es wenigstens ein A_i $(1 \leqq i \leqq t)$ mit $[N, A_i] \neq E$. Aus Hilfssatz 4 folgt sofort (2).

Aus (2) folgt (1). Da $A_1, A_2, \ldots, A_t$ die Basis von $\dot{\mathfrak{G}}$ ist, haben wir für jedes $G \in \dot{\mathfrak{G}}$ einen Ausdruck $G = A_1^{x_1} A_2^{x_2} \cdots A_t^{x_t}$ von G. Aus $\{A_i\} \cap \mathfrak{Z} \supseteq \{A_i\} \cap \dot{\mathfrak{G}}' \neq \mathfrak{E}$ und $|A_j| \leqq p^{a-1}$ folgt $[A_{i_1}, A_{i_2}]^{p^{a-1}} = E$ $(1 \leqq i_1, i_2 \leqq t)$, daher $G^{p^{a-1}} = A_1^{x_1 p^{a-1}} A_2^{x_2 p^{a-1}} \cdots A_t^{x_t p^{a-1}} = A_1^{x_1 p^{a-1}} A_2^{x_2 p^{a-1}} \cdots A_s^{x_s p^{a-1}}$: denn es ist $A_j \in \Omega_{a-1}(\dot{\mathfrak{G}})$. Andererseits haben wir $[N, G] = A_1^{x_1 p^{a-1}} A_2^{x_2 p^{a-1}} \cdots A_s^{x_s p^{a-1}}$ also $[N, G] = G^{p^{a-1}} = G^{p^{\mu-1}}$

Das besagt $[N, G]=G^{p^{\mu-1}}$ für $|G|=p^{\mu}$ und $[N, G]=E$ für $|G|<p^{\mu}$, was $N\in\mathfrak{K}_p$ ergibt.

HILFSSATZ 6. *Sei* $\mathfrak{G}\mathfrak{D}\mathfrak{N}$ *und* $|\mathfrak{N}|=p$. *Dann gibt es ein* $N\in\mathfrak{N}$ *derart, daß* $N\in\mathfrak{Z}_p$ *oder* $N\in\mathfrak{K}_p$ *ist.*

Beweis. Sei $A_1, A_2, \dots, A_t$ eine Basis von $\mathfrak{G}$. Wegen $\mathfrak{G}\mathfrak{D}\mathfrak{N}$ ist $\mathfrak{N}\mathrm{v}\{A_i\}$ $(1\leqq i\leqq t)$, daher nach Hilfssatz 4 $[N, A_i]=E$ $(1\leqq i\leqq t)$ oder $[N, A_i]=A_i^{p^{\alpha-1}}$ $(1\leqq i\leqq s)$ und $[N, A_j]=E$ $(s+1\leqq j\leqq t)$, was $N\in\mathfrak{Z}_p$ oder nach Hilfssatz 5 $N\in\mathfrak{K}_p$ ergibt.

HILFSSATZ 7. *Sei* $\mathfrak{G}\mathfrak{D}\mathfrak{N}$ *und* $\mathfrak{N}\cap\mathfrak{Z}=\mathfrak{E}$. *Dann gilt* $\{G\}\mathrm{v}\{N\}$ *für jedes* $G\in\mathfrak{G}$ *mit* $\{G\}\cap\mathfrak{Z}\neq\mathfrak{E}$ *und* $N\in\mathfrak{N}$ *mit* $|N|=p$.

Beweis. Ist $[N, G]=C\neq E$, so ist wegen $C\in\{G\}\mathfrak{N}$ $C=G^{\alpha}N_1$ mit $N_1\in\mathfrak{N}$. Aus $\{G\}\cap\mathfrak{N}\cap\mathfrak{Z}=\mathfrak{E}$ folgt $(G^{\alpha})^p=(CN_1^{-1})^p=N_1^{-p}=E$. Sonst wäre $\{G\}\cap\mathfrak{N}\cap\mathfrak{Z}\neq\mathfrak{E}$. Hiernach haben wir $G^{\alpha}\in\mathfrak{Z}$, daher $N_1=CG^{-\alpha}\in\mathfrak{Z}$, was wegen $\mathfrak{N}\cap\mathfrak{Z}=\mathfrak{E}$ $N_1=E$ führt. Dies besagt aber $C=G^{\alpha}$ und $\{G\}\mathrm{v}\{N\}$.

Da wir diese Hilfssätze bewiesen haben, so untersuchen wir den

HAUPTSATZ. *Sei* $\mathfrak{G}\mathfrak{D}\mathfrak{N}$. *Dann gibt es in* $\mathfrak{N}$ *ein* N *mit* $N\in\mathfrak{Z}_p$ *oder* $N\in\mathfrak{K}_p$.

Beweis. Sei $A, B\in\mathfrak{G}$. Dann ist $(AB)^p=A^pB^p[A, B]^{p(p-1)/2}=A^pB^p([A, B]^{p-1/2})^p$, da $p>2$ ist. Nach Satz (A) ist $\mathfrak{G}$ regulär. Daher hat $\mathfrak{G}$ eine Basis $A_1, A_2, \dots, A_t$ wie in Hilfssatz 5. Wir führen den Beweis durch Induktion von $|\mathfrak{G}|$. Wegen der Auswahl von der Basis $A_1, A_2, \dots, A_t$ können wir $A_1, A_2, \dots, A_s$ als Basisvertreter der $\mathfrak{G}/\mathfrak{G}'\Omega_{\mu-1}(\mathfrak{G})$ und $\mathfrak{G}'\Omega_{\mu-1}(\mathfrak{G})/\Omega_{\mu-1}(\mathfrak{G})$ aufnehmen und nach Satz (D) $A_1\overline{\in}\mathfrak{G}'\Omega_{\mu-1}(\mathfrak{G})$ annehmen. Daher gibt es in $\mathfrak{G}$ ein maximales $\mathfrak{M}$, das $A_1^p, A_2, \dots, A_t$ enthält. Wir betrachten den Ausdruck $M=A_1^{x_1}A_2^{x_2}\cdots A_t^{x_t}$ für jedes $M\in\mathfrak{M}$. Ersichtlich gilt $A_1^{x_1}\in\mathfrak{M}$, da $A_2, A_3, \dots, A_t\in\mathfrak{M}$ ist, daher $x_1\equiv 0\ (p)$. Dies spricht aus, daß $A_1^p, A_2, \dots, A_t$ eine Basis von $\mathfrak{M}$ ist. Nach Satz (D) haben wir, daß $A_2, A_3, \dots, A_s, A_1^p, \dots, A_t$ auch eine Basis von $\mathfrak{M}$ ist: demnach genügt $\mathfrak{M}$ Induktionsvoraussetzung und wir können aus dem Hilfssatz 6 $\mathfrak{M}\cap\mathfrak{N}\neq\mathfrak{E}$ annehmen. Daher enthält $\mathfrak{M}\cap\mathfrak{N}$ erst recht $\mathfrak{N}$ ein Zentrumselement oder Kernelement N von $\mathfrak{M}$. Wir nennen ein $N\in\mathfrak{Z}_p$ kurz ein Zentrumselement von $\mathfrak{G}$.

(1) Sei $\{A_1\}\cap\mathfrak{Z}=\mathfrak{E}$, daher $|A_1|=|A_2|=|[A_1, A_2]|$. Wir betrachten $\mathfrak{A}=\{A_1, A_2\}$, $\mathfrak{B}=\mathfrak{A}\mathfrak{N}$, $\mathfrak{N}_1=\mathfrak{A}\cap\mathfrak{N}$. Ist $\mathfrak{N}_1\neq\mathfrak{E}$, so haben wir $\{A\}\mathrm{v}\mathfrak{N}_1$ für jedes A

$\in \mathfrak{A}$, da $\{A\}\mathfrak{N} \cap \mathfrak{A} = \{A\}\mathfrak{N}_1$ ist. Es gilt nun $\mathfrak{Z} \cap \mathfrak{N} \supseteq \mathfrak{G}' \cap \mathfrak{N} \supseteq \mathfrak{A}' \cap \mathfrak{N}_1$ und nach Hilfssatz 2 $\mathfrak{A}' \cap \mathfrak{N}_1 \neq \mathfrak{E}$: demnach $\mathfrak{Z} \cap \mathfrak{N} \neq \mathfrak{E}$. Von nun ab haben wir nur den Fall $\mathfrak{A} \cap \mathfrak{N} = \mathfrak{E}$ zu behandeln. Das ergibt aber nach Hilfssatz 3 $\mathfrak{B} = \mathfrak{A} \times \mathfrak{N}$, da $\mathfrak{B}' \cap \mathfrak{N} \subseteq \mathfrak{G}' \cap \mathfrak{N} \subseteq \mathfrak{Z} \cap \mathfrak{N}$ gilt und wir $\mathfrak{Z} \cap \mathfrak{N} = \mathfrak{E}$ annehmen können. Es werde angenommen, daß N ein Zentrumselement von $\mathfrak{M}$ ist. Da $[N, A_1] = E$ ist, ist $N \in \mathfrak{Z}_p$. Falls N dagegen ein Kernelement von $\mathfrak{M}$ ist, so ergibt sich nach Hilfssatz 5 $[N, A_2] = A_2^{p^{a-1}}$, entgegen $[N, A_2] = E$.

(2) Sei $\{A_1\} \cap \mathfrak{Z} \neq \mathfrak{E}$ und $\{A_{i_1}\} \cap \mathfrak{Z} = \mathfrak{E}$ für ein i_1 mit $(1 < i_1 \leq s)$. Nach der Auswahl von der Basis können wir $A_1 A_{i_1}, A_2, \ldots, A_t$ auch als Basis von $\mathfrak{G}$ aufnehmen. Da $(A_1 A_{i_1})^{p^{a-1}} = A_1^{p^{a-1}} A_{i_1}^{p^{a-1}} [A_1, A_{i_1}]^{\binom{p^{a-1}}{2}}$ ist, haben wir $\{A_1 A_{i_1}\} \cap \mathfrak{Z} = \mathfrak{E}$. Daher können wir (2) auf (1) zurückführen.

(3) Sei $\{A_i\} \cap \mathfrak{Z} \neq \mathfrak{E}$ $(1 \leqq i \leqq s$ und $s = 1)$. Es ist $\{N\} \mathrm{v} \{A_i\}$ $(2 \leqq i \leqq t)$ und nach Hilfssatz 7 $\{N\} \mathrm{v} \{A_1\}$. Für $1 \leqq i \leqq t$ gilt $[N, A_i] = E$ oder nach Hilfssatz 5 $[N^x, A_1] = A_1^{p^{a-1}}$ und $[N, A_i] = E$ $(2 \leqq i \leqq t)$. Hilfssatz 6 liefert $N \in \mathfrak{Z}_p$ oder $N^x \in \mathfrak{K}_p$.

(4) Sei $\{A_i\} \cap \mathfrak{Z} \neq \mathfrak{E}$ $(1 \leqq i \leqq s$ und $s > 1)$. Es ist $\{N\} \mathrm{v} \{A_j\}$ $(s+1 \leqq j \leqq t)$ und nach Hilfssatz 7 $\{N\} \mathrm{v} \{A_i\}$ und $\{N\} \mathrm{v} \{A_1 A_i\}$ $(1 \leqq i \leqq s)$. Da $|A_i| > |A_j|$ $(1 \leqq i \leqq s$ und $s+1 \leqq j \leqq t)$ ist, erhalten wir $[N, A_i] = E (1 \leqq i \leqq t)$ oder nach Hilfssatz 5 $[N^x, A_i] = A_i^{p^{a-1}}$ und $[N^x, A_j] = E$. Daher ist $N \in \mathfrak{Z}_p$ oder nach Hilfssatz 7 $N^x \in \mathfrak{K}_p$.

Literatur

[1] Hall, M.: The theory of groups. New York, 1959.
[2] Hall, P.: A contribution to the theory of groups of prime power order. Proc. Lond. Math. Soc., (2) **36**, 29-95 (1933).
[3] Zassenhaus, H.: Lehrbuch der Gruppentheorie I., 1937.

Mathematisches Institut der Nihon-Universität Koriyama (Japan)