Endliche Gruppen, in denen alle das Zentrum enthaltenden Untergruppen Zentralisatoren sind

Von

MANFRED REUTHER

Wir wollen in dieser Arbeit diejenigen endlichen Gruppen bestimmen, in denen alle das Zentrum enthaltenden Untergruppen Zentralisatoren sind. 1955 charakterisierte Gaschütz [2] die zentrumsfreien endlichen Gruppen mit dieser Eigenschaft. Unser Ergebnis lautet:

Hauptsatz. *In einer endlichen Gruppe G sind genau dann alle das Zentrum enthaltenden Untergruppen Zentralisatoren, wenn G die folgende Gestalt hat:*

$$G = G_1 \times \cdots \times G_n \times H \quad \textit{mit}$$

(a) $\mathrm{ggT}(|G_i|, |G_j|) = 1$ *für alle* $1 \leqq i, j \leqq n$ *mit* $i \neq j$,

(b) G_i *ist eine Gruppe der Ordnung* $p_i^{a_i} q_i^{b_i}$, p_i *und* q_i *Primzahlen mit* $p_i > q_i$, *und* $G_i/Z(G_i)$ *ist eine Gruppe der Ordnung* $p_i q_i$, *oder*
G_i *ist eine* p_i*-Gruppe,* p_i *eine Primzahl, mit*
(1) $G_i/Z(G_i)$ *ist modular,*
(2) G_i' *ist zyklisch.*

(c) H *ist abelsch.*

Aus [2, Satz 1] folgt, daß es genügt, das Problem für Gruppen von Primzahlpotenzordnung zu behandeln, d.h. den folgenden Satz zu beweisen:

Satz. *Sei G eine p-Gruppe, p eine Primzahl. Genau dann sind alle das Zentrum enthaltenden Untergruppen Zentralisatoren, wenn gilt*

(1) $G/Z(G)$ *ist modular,*

(2) G' *ist zyklisch.*

Aus dem Beweis ergibt sich außerdem, daß unter den Voraussetzungen des Satzes gilt:

$$G = G_1 \cdots G_n \quad \text{mit } Z(G) \leqq G_i \leqq G \quad \text{und}$$

(a) $[G_i, G_j] = 1$ für $i \neq j$,

(b) $G_i/Z(G_i)$ ist verbandsisomorph zur abelschen Gruppe vom Typ (p^{n_i}, p^{n_i}).

Neben den allgemein üblichen Bezeichnungen (siehe etwa [3, 6]) benutzen wir $U \cup V$ für das Erzeugnis zweier Untergruppen U, V von G, $\exp(G)$ für den Exponenten von G, $\mathbb{Z}$ für den Ring der ganzen Zahlen sowie $\mathfrak{C}(G) := \{C_G(U) \mid U \leqq G\}$, $\mathfrak{V}(G) := \{U \mid U \leqq G\}$ und, für $U \leqq G$, $[G/U] := \{V \mid U \leqq V \leqq G\}$.

Die Arbeit stammt teilweise aus einer unter der Anleitung von Prof. R. Schmidt (Kiel) angefertigten Dissertation.

1. Modulare p-Gruppen. In diesem Abschnitt stellen wir der Übersicht halber einige Hilfssätze zusammen, die beim Beweis gebraucht werden. Wir beginnen mit einer zahlentheoretischen Aussage.

Lemma 1. *Seien i, n, s natürliche Zahlen, p eine Primzahl und $r := 1 + p^s$.*

a) *Aus $p^i \mid n$ folgt $p^i \mid \dfrac{r^n - 1}{r - 1}$.*

b) *Sei $s \geqq 2$, falls $p = 2$. Dann gilt: Aus $p^i \mid \dfrac{r^n - 1}{r - 1}$ folgt $p^i \mid n$.*

c) *Sei $s \geqq 2$, falls $p = 2$. Dann ist die Abbildung $\varphi : \mathbb{Z}/(p^i) \to \mathbb{Z}/(p^i)$ definiert durch $n^\varphi := \dfrac{r^n - 1}{r - 1} \pmod{p^i}$ eine Bijektion.*

Beweis. Wir zeigen zunächst die Aussage

(*) *Sei $n = p^i a$ mit $p \nmid a$ sowie k eine natürliche Zahl mit $2 \leqq k \leqq n$. p^{i+1} teilt dann $\dbinom{n}{k} p^{k-1}$, ausgenommen der Fall $p = 2$, $k = 2$, $i = 1$, $n \equiv 2 \pmod 4$.*

Sei o.B.d.A. $k \leqq i + 1$. Es ist

$$\binom{n}{k} p^{k-1} = \frac{p^{k-1} p^i a (p^i a - 1) \cdots (p^i a - p) \cdots (p^i a - tp) \cdots (p^i a - k + 1)}{1 \cdots p \cdots tp \cdots (k-1) \cdot k}.$$

Wir betrachten die Ausdrücke der Form $\dfrac{p^i a - tp}{tp}$ mit $p \leqq tp < k$. Sei $tp = p^j b$ mit $p \nmid b$. Dann ist $p^j b = tp \leqq k \leqq i + 1$, also sicherlich $j \leqq i$. Somit ist $p^i a - tp = p^j (p^{i-j} a - b)$, und folglich kürzt sich der gesamte p-Bestandteil von tp gegen den von $p^i a - tp$. Dies gilt für alle t mit $p \leqq tp < k$. Ist also $k \not\equiv 0 \pmod p$, so kürzen sich alle p-Bestandteile des Nenners auf diese Weise, und im Zähler bleibt p^{i+1} wegen $k \geqq 2$ übrig. Ist aber $k \equiv 0 \pmod p$, etwa $k = p^j b$ mit $p \nmid b$, so kürzen sich alle p-Bestandteile bis auf p^j auf die oben beschriebene Art. Somit bleibt p^{l+i} mit $l := p^j b - 1 - j$. Da $l \geqq 1$, außer für $p = 2$, $j = 1$, $b = 1$, bleibt p^{i+1} im Zähler übrig. Damit haben wir (*) bewiesen.

Nach dem binomischen Lehrsatz gilt

$$\frac{r^n - 1}{r - 1} = n + \sum_{k=2}^{n} \binom{n}{k} p^{(k-1)s}.$$

a) Nach (*) teilt p^i alle Summanden $\binom{n}{k} p^{(k-1)s}$ mit $k \geqq 2$, also auch $\dfrac{r^n - 1}{r-1}$, außer eventuell, wenn $p = 2$, $k = 2$, $i = 1$, $n \equiv 2 \pmod 4$, $s = 1$. Wegen $(k-1)\, s \geqq 1$ ist aber auch dann $p^{(k-1)s}$ durch p teilbar.

b) Sei $n = p^j a$ mit $p \nmid a$. Zu zeigen ist $j \geqq i$. Angenommen, es sei $j < i$: Aus der Voraussetzung folgt offenbar, daß n von p geteilt wird. Nach (*) haben wir damit $p^{j+1} \mid \binom{n}{k} p^{(k-1)s}$ für alle $2 \leqq k \leqq n$ ($p^{j+1} \mid \binom{n}{k} p^{k-1}$ nach (*) außer bei $p = 2$, $k = 2$, $j = 1$. Wegen $s \geqq 2$ teilt 4 dann aber $\binom{n}{2} p^s$). Da p^{j+1} nach Annahme und nach der Voraussetzung auch $\dfrac{r^n - 1}{r - 1}$ teilt, folgt der Widerspruch $p^{j+1} \mid n$.

c) Es ist nur die Injektivität von φ zu zeigen. Seien m, n natürliche Zahlen mit $m \geqq n$. Aus $m^\varphi \equiv n^\varphi \pmod{p^i}$ und der Definition von r folgt sofort $r^m - 1 \equiv r^n - 1 \pmod{p^{i+s}}$ und somit $(m-n)^\varphi \equiv 0 \pmod{p^i}$. Aus b) folgt nun $m \equiv n \pmod{p^i}$. q.e.d.

Die modularen nichthamiltonschen p-Gruppen sind genau die zu abelschen p-Gruppen verbandsisomorphen p-Gruppen. Aus [4, 5] folgt sofort der erste Teil des folgenden Lemmas.

Lemma 2. *Die p-Gruppe G sei verbandsisomorph zur abelschen Gruppe vom Typ (p^a, p^a). Dann gilt*

$$G = \langle x, y \mid x^{p^a} = y^{p^a} = 1;\ y^{-1} x y = x^r;\ r = 1 + p^s;\ s \geqq 2,\ \textit{falls}\ p = 2 \rangle\,.$$

Für natürliche Zahlen i, j, m, n gilt außerdem

a) $[y^i x^j, y^m x^n] = [y, x]^k$ *mit* $k := \dfrac{r^i - 1}{r - 1}\, n - j\, \dfrac{r^m - 1}{r - 1}$.

b) $(y^i x^j)^n = y^{ni} x^{jl}$ *mit* $l := \dfrac{r^{ni} - 1}{r^i - 1}$.

c) $o(y^i x^j) = \mathrm{kgV}(o(y^i), o(x^j))$.

Beweis. a) Aus $y^{-1} x y = x^r$ folgt per Induktion $[y^i, x] = [y, x]^{\frac{r^i - 1}{r - 1}}$. Aufgrund bekannter Kommutatorformeln gilt $[y^i x^j, y^m x^n] = [y^i, x]^n\, [x, y^m]^j$.

b) Sei $b := \dfrac{r^{(n-1)i} - 1}{r^i - 1}$. Durch Induktion nach n folgt

$$(y^i x^j)^n = y^{(n-1)i} x^{jb} y^i x^j = y^{ni} x^{jb} [x^{jb}, y^i]\, x^j = y^{ni} x^{jb + (r^i - 1) jb + j} = y^{ni} x^{jl}.$$

c) Sei $n = p^m$. Nach b) ist genau dann $(y^i x^j)^n = 1$, wenn $y^{ni} x^{jl} = 1$ mit $l = \dfrac{r^{ni} - 1}{r^i - 1}$, d.h. wegen $\langle x \rangle \cap \langle y \rangle = 1$, wenn $y^{ni} = x^{jl} = 1$. Mit Lemma 1 folgt die Behauptung. q.e.d.

Lemma 3. *Sei G eine beliebige Gruppe. Dann ist $G/Z(G)$ nicht hamiltonsch.*

Beweis. Sei $G/Z(G)$ hamiltonsch. Dann ist $G/Z(G) = Q/Z(G) \times A/Z(G) \times B/Z(G)$, wobei $Q/Z(G)$ eine Quaternionengruppe der Ordnung 8, $A/Z(G)$ eine Gruppe vom Exponenten 1 oder 2 und $B/Z(G)$ eine abelsche Gruppe von ungerader Ordnung ist. Es ist o.B.d.A. $B = Z(G)$. Sei $U/Z(G)$ die minimale Untergruppe von $Q/Z(G)$. G besitzt modulo $Z(G)$ ein Erzeugendensystem von Elementen der Ordnung 4 mit $\langle Z(G), x_1\rangle \cap \cdots \cap \langle Z(G), x_n\rangle = U$. Dann ist aber

$$Z(G) = C_G(\langle x_1, \ldots, x_n\rangle) = C_G(x_1) \cap \cdots \cap C_G(x_n) \geqq U\,. \text{ q.e.d.}$$

Sei nun $G/Z(G)$ eine modulare p-Gruppe. Nach [4, 5] existiert ein Normalteiler A von G mit $Z(G) \leqq A$ und ein Element $t \in G$ mit folgenden Eigenschaften:

(a) $A/Z(G)$ ist abelsch,

(b) $G = A\langle t\rangle$,

(c) Es gibt eine natürliche Zahl s ($s \geqq 2$, falls $p = 2$) mit $Z(G)\,t^{-1}at = Z(G)\,a^{1+p^s}$ für alle $a \in A$.

Lemma 4. *Sei $G/Z(G)$ eine modulare p-Gruppe. Dann ist* $\exp(G/Z(G)) = \exp(A/Z(G))$.

Beweis. Wir setzen $m := \max\{\exp(A/Z(G)), o(Z(G)\,t)\}$. Sei $g = t^i a$ mit $a \in A$. Analog wie in Lemma 2b) zeigt man $(Z(G)t^i a)^m = Z(G)\,t^{mi}a^l$ mit $l := \dfrac{r^{mi}-1}{r^i-1}$. Da nach Lemma 1 der p-Anteil von l gleich dem p-Anteil von m ist, folgt $(Z(G)\,t^i a)^m = Z(G)$. Daher ist $m = \exp(G/Z(G))$.

Sei nun $p^n := o(Z(G)\,t)$. Dann gibt es ein $a \in A$, das mit $t^{p^{n-1}}$ nicht kommutiert. Wegen $1 \neq [a, t^{p^{n-1}}] = [a, t]^k$ mit $k := \dfrac{r^{(p^{n-1})}-1}{r-1}$ ergibt Lemma 1 $1 \neq [a, t]^{p^{n-1}} = [a^{p^{n-1}}, t]$. Folglich ist $a^{p^{n-1}} \notin Z(G)$ und somit

$$o(Z(G)\,t) = p^n \leqq \exp(A/Z(G)). \quad \text{q.e.d.}$$

2. Beweis des Satzes. Wir zeigen zunächst, daß die angegebenen Bedingungen notwendig sind.

Lemma 5. *Sei G eine p-Gruppe mit $\mathfrak{C}(G) = [G/Z(G)]$. Dann gilt*

a) *Die Abbildung $\tau\colon [G/Z(G)] \to [G/Z(G)]$ definiert durch $U^\tau := C_G(U)$ ist eine Dualität.*

b) *$G/Z(G)$ ist modular.*

c) *$G/Z(G)$ ist verbandsisomorph zu einer abelschen p-Gruppe.*

Beweis. Die Aussage a) ist trivial. $G/Z(G)$ ist semimodular nach unten und als Gruppe, die eine Dualität besitzt, damit auch semimodular nach oben. Folglich ist $G/Z(G)$ modular. Aus b) und Lemma 3 folgt bekanntlich (siehe etwa [6]) die Behauptung c). q.e.d.

Lemma 6. *Sei $G = HK$ mit $Z(G) \leqq H, K$ und $K \leqq C_G(H)$. Aus $\mathfrak{C}(G) = [G/Z(G)]$ folgt $\mathfrak{C}(H) = [H/Z(H)]$.*

Beweis. Sei $U \leqq H$ mit $Z(H) \leqq U$. Aufgrund des modularen Gesetzes gilt

$$C_H(C_H(U)) = C_G(C_G(U) \cap H) \cap H = (C_G(C_G(U)) \cup C_G(H)) \cap H = \\ = (U \cup C_G(H)) \cap H = U. \quad \text{q.e.d.}$$

Lemma 7. *Sei G eine p-Gruppe mit $\mathfrak{C}(G) = [G/Z(G)]$. Dann gilt:*

$$G = G_1 \cdots G_n \quad \textit{mit} \quad Z(G) \leqq G_i \leqq G \quad \textit{und}$$

(a) $[G_i, G_j] = 1$ *für* $i \neq j$,

(b) *$G_i/Z(G)$ ist verbandsisomorph zur abelschen Gruppe vom Typ (p^{n_i}, p^{n_i}).*

Beweis. Nach Lemma 5 existiert eine abelsche p-Gruppe A und ein Verbandsisomorphismus σ von $[G/Z(G)]$ auf $\mathfrak{V}(A)$. Sei $x_1 \in G$ mit $o(Z(G)\,x_1)$ maximal in $G/Z(G)$ und $X_1 := \langle Z(G), x_1\rangle$.

Dann ist $[X_1/Z(G)]$ eine maximale Teilkette nach $Z(G)$ in $[G/Z(G)]$, und daher ist auch $\mathfrak{V}(X_1^\sigma)$ eine maximale Teilkette nach 1 in $\mathfrak{V}(A)$. Also gibt es ein Element $a \in A$ von maximaler Ordnung in A mit $X_1^\sigma = \langle a\rangle$. Da $\mathfrak{V}(X_1^\sigma)$ eine Kette ist, sind nach Lemma 5 $[A/C_G(X_1)^\sigma]$ und $\mathfrak{V}(\langle a\rangle)$ isomorphe Verbände. Wegen $\langle a\rangle \leqq C_G(X_1)^\sigma$, und da $o(a)$ maximal ist, existiert ein Element $b \in A$ mit $A = \langle b\rangle \times C_G(X_1)^\sigma$ und $o(a) = o(b)$.

Sei $Y_1 := \langle b\rangle^{\sigma^{-1}}$. Dann ist $Y_1/Z(G)$ zyklisch. Sei also $y_1 \in G$ mit $Y_1 = \langle Z(G), y_1\rangle$. Es ist $o(Z(G)\,y_1) = o(Z(G)\,x_1)$. Außerdem haben wir $G = Y_1\, C_G(X_1)$ und $Z(G) = = Y_1 \cap C_G(X_1)$. Somit gilt auch $G = X_1\, C_G(Y_1)$.

Wir setzen $G_1 := X_1\, Y_1 \leqq G$. Es ist $X_1 \cap Y_1 = Z(G)$. Aus dem oben Gezeigten folgt, daß $G_1/Z(G)$ verbandsisomorph zu $\langle a\rangle\,\langle b\rangle$, einer abelschen Gruppe vom Typ (p^{n_1}, p^{n_1}) mit $p^{n_1} := \exp(G/Z(G))$, ist. Es gilt $G_1\, C_G(G_1) = X_1 \cup (Y_1 \cup (C_G(X_1) \cap \cap C_G(Y_1))) = X_1 \cup ((Y_1 \cup C_G(X_1)) \cap C_G(Y_1)) = X_1\, C_G(Y_1) = G$. Nach Lemma 6 ist $\mathfrak{C}(C_G(G_1)) = [C_G(G_1)/Z(C_G(G_1))]$. Sukzessiv mit $C_G(G_1)$ anstelle von G fortfahrend erhält man die Behauptung. q.e.d.

Lemma 8. *Sei G eine p-Gruppe mit $\mathfrak{C}(G) = [G/Z(G)]$. Dann ist G' zyklisch.*

Beweis. Nach den Lemmata 2, 7 ist $G = G_1 \cdots G_n$ mit

$$Z(G) \leqq G_i \leqq G, \quad [G_i, G_j] = 1 \quad \text{für } i \neq j \quad \text{und}$$

$$G_i = \langle Z(G), x_i, y_i \mid o(Z(G)\,x_i) = o(Z(G)\,y_i) = p^{n_i}; \quad y_i^{-1} x_i y_i = x_i^{r_i} z_i \quad \text{mit} \\ z_i \in Z(G); \quad r_i = 1 + p^{s_i} \quad \text{mit} \quad 1 \leqq s_i \leqq n_i; \; s_i \geqq 2, \\ \text{falls } p = 2\rangle.$$

Sei $n_1 \geqq \cdots \geqq n_n$. Nach [7, Lemma 3] ist für $i \geqq 2$ $\mathrm{cl}(G_i) = 2$, d.h. wir können $r := r_1$ und, für $i \geqq 2$, $r_i = 1$ setzen. Ferner ist $G_i' = \langle [x_i, y_i]\rangle$ und $G' = \langle [x_i, y_i] \mid 1 \leqq i \leqq n\rangle$. Offenbar genügt es, $G_i' \geqq G_{i+1}'$ für $1 \leqq i \leqq n - 1$ nachzuweisen. Nach Lemma 6 ist damit o.B.d.A. $n = 2$.

Wir setzen $U := \langle Z(G), x_1 x_2, y_1 y_2\rangle$. Da $n_1 \geqq n_2$ und $[x_1, x_2] = [y_1, y_2] = 1$, gilt $o(Z(G)\,x_1 x_2) = o(Z(G)\,y_1 y_2) = p^{n_1}$. Wegen $Z(G) = \langle Z(G), x_1 x_2\rangle \cap \langle Z(G), y_1 y_2\rangle$ ist damit $U/Z(G)$ verbandsisomorph zur abelschen Gruppe vom Typ (p^{n_1}, p^{n_1}). Nach den Lemmata 5, 7 ist $G/Z(G)$ verbandsisomorph zur abelschen Gruppe A vom Typ $(p^{n_1}, p^{n_1}, p^{n_2}, p^{n_2})$. Außerdem sind aufgrund von Lemma 5 die Verbände $[C_G(U)/Z(G)]$ und $[G/U]$ isomorph. Eine Betrachtung in A liefert sofort einen Verbandsisomorphismus von $C_G(U)/Z(G)$ zu der abelschen Gruppe vom Typ (p^{n_2}, p^{n_2}). Daher gibt es in $C_G(U)/Z(G)$ ein Element $Z(G)\, x_1^{b_1} y_1^{c_1} x_2^{b_2} y_2^{c_2}$ der Ordnung p^{n_2}. Wir setzen $g_1 := x_1^{b_1} y_1^{c_1}$ und $g_2 := x_2^{b_2} y_2^{c_2}$.

Angenommen, es sei $g_2^{p^{n_2-1}} \in Z(G)$. Wegen $g_1 g_2 \in C_G(U)$ und $(Z(G)\, g_1 g_2)^{p^{n_2-1}} = Z(G) g_1^{p^{n_2-1}}$ ist dann $[x_1, g_1^{p^{n_2-1}}] = [x_1 x_2, g_1^{p^{n_2-1}}] = 1$ sowie $[y_1, g_1^{p^{n_2-1}}] = [y_1 y_2, g_1^{p^{n_2-1}}] = 1$. Also folgt $g_1^{p^{n_2-1}} \in C_{G_1}(x_1) \cap C_{G_1}(y_1) = Z(G)$ und damit der Widerspruch $(g_1 g_2)^{p^{n_2-1}} \in Z(G)$. Somit ist $g_2^{p^{n_2-1}} \notin Z(G)$.

Da die Klasse von G_2 zwei ist, gibt es ein Element $t \in Z(G)$ mit $g_2^{p^{n_2-1}} = t \cdot x_2^{b_2 p^{n_2-1}} \cdot y_2^{c_2 p^{n_2-1}}$. Also teilt p nicht b_2 oder nicht c_2.

Aus $[g_1 g_2, y_1 y_2] = 1$ folgt mittels bekannter Kommutatorformeln

$$1 = ([x_2, y_2]^{y_2^{c_2}})^{b_2} ([x_1, y_1]^{y_1^{c_1}})^{b_1}.$$

Teilt p also nicht b_2, so ergibt sich die Behauptung $G_1' \geqq G_2'$. Aus $[g_1 g_2, x_1 x_2] = 1$ erhält man analog $1 = [x_1, y_1]^{1+r+\cdots+r^{c_1-1}} [x_2, y_2]^{c_2}$ und daher, wenn p nicht c_2 teilt, die Behauptung. q.e.d.

Damit haben wir die Notwendigkeit der Bedingungen nachgewiesen. Es bleibt zu zeigen, daß in einer Gruppe mit der angegebenen Struktur jede Untergruppe oberhalb des Zentrums ein Zentralisator ist. Wir beweisen zunächst

Lemma 9. *Sei G eine nilpotente Gruppe der Klasse zwei mit zyklischer Kommutatorgruppe. Dann ist $\mathfrak{C}(G) = [G/Z(G)]$.*

Zum Beweis benötigen wir ein Lemma von Baer [1]: Sei A eine abelsche Gruppe und X eine zyklische Gruppe mit $\exp(A) \mid |X|$. $\mathrm{Hom}(A, X) := \{f \mid f: A \to X,\ f$ Gruppenhomomorphismus$\}$ ist bezüglich $a^{fg} := a^f a^g$ $(a \in A;\ f, g \in \mathrm{Hom}(A, X))$ eine abelsche Gruppe. Es gilt

(a) $A \cong \mathrm{Hom}(A, X)$,

(b) Die Abbildung $\perp : \mathfrak{V}(A) \to \mathfrak{V}(\mathrm{Hom}(A, X))$ definiert durch

$$B^{\perp} := \{f \mid f \in \mathrm{Hom}(A, X);\ B \leqq \mathrm{Kern}\, f\}$$

ist eine Dualität. Für $B \leqq A$ ist ferner $B^{\perp} \cong A/B$.

Beweis. Wir setzen $Z := Z(G)$. Aus den Voraussetzungen folgt trivialerweise $\exp(G/Z) \mid |G'|$. Die für jedes $Zg \in G/Z$ durch $(Zh)^{f_{Zg}} := [g, h]$ definierte Zuordnung $f_{Zg} : G/Z \to G'$ ist ein Homomorphismus, da die Klasse von G zwei ist. Also wird durch $(Zg)^f := f_{Zg}$ eine Abbildung $f: G/Z \to \mathrm{Hom}(G/Z, G')$ definiert. Wegen $\mathrm{cl}(G) = 2$ ist f ein injektiver Homomorphismus. Aus dem Lemma von Baer folgt nun, daß f sogar ein Isomorphismus ist. Insbesondere gilt $\mathrm{Hom}(G/Z, G') = \{f_{Zg} \mid Zg \in G/Z\}$.

Sei nun $U \leqq G$ mit $Z \leqq U$. Für $(U/Z)^{\perp} = \{f_{Zg} \mid Zg \in C_G(U)/Z\}$ gilt, da f ein Isomorphismus ist, $(U/Z)^{\perp} \cong C_G(U)/Z$. Nach dem Lemma von Baer ist $(U/Z)^{\perp} \cong G/U$.

Damit haben wir insgesamt $G/U \cong C_G(U)/Z$. Für $C_G(U)$ anstelle von U folgt analog $G/C_G(U) \cong C_G(C_G(U))/Z$. Also ist $|C_G(C_G(U))| = |U|$. Wegen $U \leqq C_G(C_G(U))$ ist daher $U = C_G(C_G(U))$. q.e.d.

Bevor wir den Beweis beenden können, müssen wir die vorliegenden p-Gruppen noch näher untersuchen.

Lemma 10. *Sei G eine p-Gruppe mit modularer Zentrumsfaktorgruppe und zyklischer Kommutatorgruppe. Dann ist $G = G_1 \cdots G_n$ mit $Z(G) \leqq G_i \leqq G$ und*

(1) $[G_i, G_j] = 1$ *für* $i \neq j$,

(2) $G_i/Z(G_i)$ *ist verbandsisomorph zur abelschen Gruppe vom Typ* (p^{n_i}, p^{n_i}).

Beweis. Wir setzen $Z := Z(G)$. Nach den Lemmata 7, 9 ist o.B.d.A. $\mathrm{cl}(G) \geqq 3$. Wie wir bereits in Abschnitt 1 erwähnt haben, existiert ein Normalteiler A von G mit $Z \leqq A$ und ein Element $t \in G$ mit

(a) A/Z ist abelsch,

(b) $G = A\langle t\rangle$,

(c) Es gibt eine natürliche Zahl s ($s \geqq 2$, falls $p = 2$) mit $Zt^{-1}at = Za^r$ für alle $a \in A$, wobei $r = 1 + p^s$.

Sei $A/Z = \langle Za_1\rangle \times \cdots \times \langle Za_l\rangle$ mit $p^m := o(Za_1) \geqq \cdots \geqq o(Za_l)$. Es ist $o(Za_1) > o(Za_2)$; denn sonst wäre wegen $\langle a_1\rangle \cap \langle a_2\rangle \leqq Z$, und da $(G/Z)' = \mho_s(A/Z)$ zyklisch ist, $\mho_s(A/Z) = 1$, d.h. $\mathrm{cl}(G) \leqq 2$. Wegen $[a_1, t] \in G'$, G' zyklisch und $G'Z/Z = \langle [a_1, t]\rangle Z/Z$ ist $G' = \langle [a_1, t]\rangle$. Sei $G_1 := Z\langle a_1, t\rangle$.

Wir zeigen

$$(*) \qquad [t, a_1^{p^{m-1}}] \neq 1\,.$$

Wegen $o(Za_1) > o(Za_2)$ ist $a_i^{p^{m-1}} \in Z$ für $i \geqq 2$, d.h. $[a_1, a_i^{p^{m-1}}] = 1$. Damit ist auch $[a_1^{p^{m-1}}, a_i] = 1$, d.h. $A \leqq C_G(a_1^{p^{m-1}})$. Da $G = A\langle t\rangle$, folgt die Behauptung (*).

Dann gilt aber auch $[t^{p^{m-1}}, a_1] \neq 1$; denn wegen

$$[a_1, t^{p^{m-1}}] = [a_1, t]^{\frac{r^{(p^{m-1})}-1}{r-1}}$$

folgt dieses aus (*) und Lemma 1.

Aus Lemma 4 folgt nun $o(Zt) = o(Za_1) = p^m$. Wegen (*) ist ferner $\langle Za_1\rangle \cap \langle Zt\rangle = Z$. Also ist G_1/Z eine modulare nichthamiltonsche Gruppe vom Exponenten p^m, die einen zyklischen Normalteiler $Z\langle a_1\rangle/Z$ der Ordnung p^m mit zyklischer Faktorgruppe der Ordnung p^m besitzt. Folglich ist G_1/Z verbandsisomorph zur abelschen Gruppe vom Typ (p^{n_1}, p^{n_1}) mit $n_1 := m$. Wir müssen noch $G = G_1 C_G(G_1)$ nachweisen. Die Behauptung folgt dann durch Induktion.

Nach (*) ist $|G'| = p^m$. Für beliebiges $h \in G$ ist außerdem

$$|G : C_G(h)| = |\{h^g \mid g \in G\}| = |\{[h, g] \mid g \in G\}| \leqq |G'| = p^m\,.$$

Da $t^{p^{m-1}} \notin C_G(a_1)$ und da $C_G(a_1)$ normal in G ist, gilt $G = C_G(a_1)\langle t\rangle$. Genauso folgt, weil $Z\langle a_1\rangle$ ein Normalteiler von G ist, $G = C_G(t)\langle a_1\rangle$. Damit ist $G_1 C_G(G_1) = \langle a_1\rangle \cup \{\langle t\rangle \cup (C_G(a_1) \cap C_G(t))\} = \langle a_1\rangle \cup \{(\langle t\rangle \cup C_G(a_1)) \cap C_G(t)\} = G$. q.e.d.

Wir können nun den Beweis unseres Satzes beenden.

Lemma 11. *Sei G eine p-Gruppe mit modularer Zentrumsfaktorgruppe und zyklischer Kommutatorgruppe. Dann ist $\mathfrak{C}(G) = [G/Z(G)]$.*

Beweis. Aufgrund der Lemmata 2, 10 sowie wegen [7, Lemma 3] gilt

$$\begin{aligned} G = \langle Z(G), x_1, y_1, \ldots, x_n, y_n \,|\, & o(Z(G)x_i) = o(Z(G)y_i) = p^{n_i};\\ & y_1^{-1}x_1y_1 = x_1^r z_1 \text{ mit } z_1 \in Z(G);\ r = 1 + p^s \text{ mit } 1 \leqq s \leqq n_1;\\ & s \geqq 2, \text{ falls } p = 2;\ 1 \neq [x_i, y_i] \in Z(G) \text{ für } i \geqq 2;\ [x_i, x_j] =\\ & [x_i, y_j] = [y_i, y_j] = 1 \text{ für alle } i \neq j;\ [x_i, y_i] = [x_1, y_1]^{p^{n_1 - n_i}}\rangle \end{aligned}$$

mit $n_1 \geqq \cdots \geqq n_n$. Ferner ist $G' = \langle [x_1, y_1]\rangle$. Der Gruppe G ordnen wir nun die folgende Gruppe H der Klasse zwei zu:

$$\begin{aligned} H = \langle Z(H), v_1, w_1, \ldots, v_n, w_n \,|\, & o(Z(H)v_i) = o(Z(H)w_i) = p^{n_i};\\ & 1 \neq [v_i, w_i] \in Z(H) \text{ für alle } i;\\ [v_i, v_j] = [v_i, w_j] = [w_i, w_j] = 1 & \text{ für alle } i \neq j;\ [v_i, w_i] = [v_1, w_1]^{p^{n_1 - n_i}}\rangle. \end{aligned}$$

H erfüllt die Voraussetzungen von Lemma 9, und daher ist $\mathfrak{C}(H) = [H/Z(H)]$. Wir stellen zunächst einige einfache Bemerkungen zusammen:

Die Darstellung eines Elementes aus $G/Z(G)$ in der Form $Z(G)\, y_1^{c_1} x_1^{d_1} \cdots y_n^{c_n} x_n^{d_n}$ mit $1 \leqq c_i,\ d_i \leqq p^{n_i}$ ist eindeutig. Ebenso ist die Darstellung eines Elementes aus $H/Z(H)$ in der Form $Z(H)\, w_1^{c_1} v_1^{d_1} \cdots w_n^{c_n} v_n^{d_n}$ mit $1 \leqq c_i,\ d_i \leqq p^{n_i}$ eindeutig.

Unter Benutzung von Lemma 2 erhält man

$$\begin{aligned} &[y_1^{c_1} x_1^{d_1} \cdots y_n^{c_n} x_n^{d_n},\, y_1^{e_1} x_1^{f_1} \cdots y_n^{e_n} x_n^{f_n}] = [y_1, x_1]^k \quad \text{mit}\\ &k := \frac{r^{c_1} - 1}{r - 1} f_1 - d_1 \frac{r^{e_1} - 1}{r - 1} + \sum_{i=2}^{n} p^{n_1 - n_i}(c_i f_i - d_i e_i). \end{aligned}$$

Wegen $\mathrm{cl}(H) = 2$ gilt mit demselben k

$$\left[w_1^{\frac{r^{c_1}-1}{r-1}} v_1^{d_1} \cdots w_n^{c_n} v_n^{d_n},\, w_1^{\frac{r^{e_1}-1}{r-1}} v_1^{f_1} \cdots w_n^{e_n} v_n^{f_n}\right] = [w_1, v_1]^k.$$

Aus Lemma 2 folgt

$$o(Z(G)\, y_1^{c_1} x_1^{d_1} \cdots y_n^{c_n} x_n^{d_n}) = \mathrm{kgV}(o(Z(G)\, y_1^{c_1}), \ldots, o(Z(G)\, x_n^{d_n})).$$

Da die Klasse von H zwei ist, ist analog

$$o(Z(H)\, w_1^{c_1} v_1^{d_1} \cdots w_n^{c_n} v_n^{d_n}) = \mathrm{kgV}(o(Z(H)\, w_1^{c_1}), \ldots, o(Z(H)\, v_n^{d_n})).$$

Mit Lemma 1 ergibt sich

$$o(Z(G)\, y_1^{c_1} x_1^{d_1} \cdots y_n^{c_n} x_n^{d_n}) = o(Z(H)\, w_1^{\frac{r^{c_1}-1}{r-1}} v_1^{d_1} \cdots w_n^{c_n} v_n^{d_n}).$$

Aus diesen Bemerkungen und Lemma 1 folgt

$$|\,C_G(y_1^{c_1} x_1^{d_1} \cdots y_n^{c_n} x_n^{d_n})/Z(G)\,| = |\,C_H\,(w_1^{\frac{r^{c_1}-1}{r-1}}\, v_1^{d_1} \cdots w_n^{c_n} v_n^{d_n})\,/Z(H)\,|\,.$$

Wegen $\mathfrak{C}(H) = [H/Z(H)]$ haben wir damit die folgende Aussage bewiesen:

(*) *Seien* $g, h \in G$. *Dann ist*

($*_1$) $|G : C_G(g)| = o(Z(G)\,g)$,

($*_2$) $C_G(g) \neq C_G(h)$, *falls* $\langle Z(G), g\rangle \neq \langle Z(G), h\rangle$.

Sei $g \in G$. Wir zeigen, daß dann $[G/C_G(g)]$ eine Kette ist. Sei also $Z(G)\,g$ ein Element minimaler Ordnung in $G/Z(G)$ mit der Eigenschaft, daß $[G/C_G(g)]$ keine Kette ist. Ferner sei $p^m := o(Z(G)\,g)$. Nach (*) ist $|\,C_G(g^p) : C_G(g)\,| = p$. Wegen der Minimalität von $Z(G)\,g$ ist $[G/C_G(g^p)]$ eine Kette. Aufgrund der Modularität von $G/Z(G)$ ist $[G/C_G(g)]$ damit isomorph zum Untergruppenverband der abelschen Gruppe vom Typ (p^{m-1}, p). $[G/C_G(g)]$ hat also genau $p+1$ minimale Elemente, und davon haben genau p — etwa $U_1, \ldots, U_p$ — die Eigenschaft, daß $[G/U_i]$ eine Kette ist. Da $G/Z(G)$ eine Dualität besitzt, folgt aus (*) und der Minimalität von $Z(G)\,g$, daß es Elemente $g_i \in G$, $1 \leqq i \leqq p$, mit $U_i = C_G(g_i)$ gibt. Sei o.B.d.A. $g_p = g^p$. Dann ist $C_G(g_1) \neq C_G(g^p)$. Wegen $g \in C_G(g) \leqq C_G(g_1)$ ist $\langle Z(G)\,g, Z(G)\,g_1\rangle$ abelsch. Nach (*) ist $o(Z(G)\,g_1) = p^{m-1}$. Also ist $\langle Z(G)\,g, Z(G)\,g_1\rangle$ isomorph zur abelschen Gruppe vom Typ (p^m, p^b) für ein b mit $b \leqq m$. Da wegen $C_G(g_1) \neq C_G(g^p)$ auch $\langle Z(G)\,g_1\rangle \neq \langle Z(G)\,g^p\rangle$ ist, gilt $b \geqq 1$. Daher gibt es ein Element $Z(G)\,h \in \langle Z(G)\,g, Z(G)\,g_1\rangle$ mit $o(Z(G)\,h) = p^m$ und $\langle Z(G)\,g\rangle \neq \langle Z(G)\,h\rangle$. Es ist $C_G(g) \leqq C_G(h)$, und aus ($*_1$) folgt $C_G(g) = C_G(h)$ im Widerspruch zu ($*_2$).

Also ist für jedes $g \in G$ $[G/C_G(g)]$ eine Kette. Sei nun X eine Untergruppe maximaler Ordnung mit $Z(G) \leqq X$, die kein Zentralisator ist. Aus (*) und dem eben Gezeigten folgt, da $G/Z(G)$ eine Dualität besitzt, daß $[G/X]$ keine Kette ist. Weil $G/Z(G)$ eine modulare nichthamiltonsche Gruppe ist, existieren also von X verschiedene Untergruppen A und B von G mit $X = A \cap B$. Aufgrund der Maximalität von X sind A und B Zentralisatoren von G. Daher ist auch X als Durchschnitt zweier Zentralisatoren ein Zentralisator. q.e.d.

Literaturverzeichnis

[1] R. Baer, Dualism in abelian groups. Bull. Amer. Math. Soc. **43**, 121–124 (1937).

[2] W. Gaschütz, Gruppen, deren sämtliche Untergruppen Zentralisatoren sind. Arch. Math. **6**, 5–8 (1955).

[3] B. Huppert, Endliche Gruppen I. Berlin-Heidelberg-New York 1967.

[4] K. Iwasawa, Über die endlichen Gruppen und die Verbände ihrer Untergruppen. J. Fac. Sci. Imp. Univ. Tokyo, Sect. I **4**, 171–199 (1941).

[5] F. Napolitani, Sui p-gruppi modulari finiti. Rend. Sem. Mat. Univ. Padova **39**, 296–303 (1967).

[6] M. Suzuki, Structure of a group and the structure of its lattice of subgroups. Berlin-Göttingen-Heidelberg 1956.

[7] B. YAKOVLEV, Lattice isomorphisms of solvable groups. Algebra and Logic 9, 210—222 (1970).

Eingegangen am 30. 4. 1976

Anschrift des Autors:

M. Reuther
Mathematisches Seminar
Universität Kiel
Olshausenstr. 40—60
D-2300 Kiel