ÜBER ENDLICHE GRUPPEN MIT EINER ZU $L_2(2^n)$ ISOMORPHEN FAKTORGRUPPE

BERND BAUMANN

ABSTRACT. In dieser Arbeit wird die Struktur einer 2-Sylogruppe S einer endlichen Gruppe G beschrieben, für die $G/O_2(G)$ isomorph zu $L_2(2^n)$ ist und in der keine nichttriviale charakteristische Untergruppe von S normal ist.

In dieser Arbeit wird die folgende, meines Wissens auf Aschbacher zurückgehende Vermutung bewiesen:

SATZ. Sei G eine endliche Gruppe, für die $G/O_2(G)$ isomorph zu $L_2(2^n)$ ist, und S eine 2-Sylogruppe von G mit $Z(S) \leq O_2(G)$.

(*) Der einzige Normalteiler von G , der charakteristisch in S ist, sei die Einheitsgruppe.

Dann gilt:

(a) Es gibt einen Automorphismus α von S mit $S = Z(O_2(G))^\alpha O_2(G)$.

(b) Es gibt genau einen nichtzentralen Hauptfaktor von G von Zweierpotenzordnung (in einer vorgegebenen Hauptreihe).

(c) Die Nilpotenzklasse von S ist 2.

Die Bezeichnungen sind aus [2] übernommen. Insbesondere ist $L_2(2^n)$ isomorph zur 2-dimensionalen, speziellen linearen Gruppe über einem Körper mit 2^n Elementen, $O_2(G)$ der grösste Normalteiler von Zweierpotenzordnung und $Z(G)$ das Zentrum einer Gruppe G .

Ein entsprechender Satz wurde in [1] unter Verwendung von Methoden aus [3] für Gruppen mit einer zu $SL_2(q)$ isomorphen Faktorgruppe bewiesen, wobei q eine beliebige Primzahl ist. Wie mir Professor Glauberman mitteilte, haben inzwischen er und R. Niles diesen Beweis für beliebige Primzahlpotenzen q verallgemeinert. Dieser Beweis unterscheidet sich jedoch von dem hier wiedergegebenen.

Mein besonderer Dank gilt Professor M. Aschbacher und Professor G. Glauberman, die mich auf zahlreiche Fehler und Unverständlichkeiten im ursprünglichen Manuskript hingewiesen haben.

Folgender wohlbekannte Hilfssatz wird benötigt.

HILFSSATZ. Sei V eine elementar-abelsche 2-Gruppe und G eine zu $L_2(2^n)$ isomorphe Gruppe von Automorphismen von V . Dann ist $|V| \geq 2^{2^n}$.

Received by the editors January 24, 1977 and, in revised form, January 27, 1978.

AMS (MOS) subject classifications (1970). Primary 20D05, 20D30.

© 1979 American Mathematical Society
0002-9939/79/0000-0202/\$03.00

BEWEIS. Wegen $O_2(G) = 1$ ist G eine Gruppe von Automorphismen von $V/C_V(G)$. Daher ist o.B.d.A. $C_V(G) = 1$. Angenommen, $|V| \leq 2^{2n}$. Nach Dickson's Liste der Untergruppen von G enthält G zu $L_2(2^r)$ (für Teiler r von n) isomorphe Untergruppen H . Ist $H = C_G(v)$ für $v \in V^\#$, so ist

$$|v^G| = |G : H| = 2^n(2^{2n} - 1)/2^r(2^{2r} - 1) = 2^{n-r} \sum_{i=1}^{n/r} 2^{2n-2ri} \geq 2^{3n-3r}.$$

Für $r < n/2$ folgt $|v^G| \geq 2^{3n-3r} \geq 2^{2n} \geq |V|$, was nicht sein kann. Deshalb ist dann $r = n/2$ und $|H| = 2^{n/2}(2^n - 1)$. Gilt nun $(|C_G(w)|, 2^n + 1) \neq 1$ für $w \in V^\#$, so erhält man mit Dickson's Liste also $C_G(w) \leq D$, wobei D eine Diedergruppe der Ordnung $2(2^n + 1)$ ist. Insbesondere ist $|w^G| \geq |G : D| = 2^{n-1}(2^n - 1)$. Nun gibt es aber ein $z \in V^\#$, das von einer 2-Sylowgruppe von G zentralisiert wird. Da eine 2-Sylowgruppe von G lediglich in einer maximalen Untergruppe (der Ordnung $2^n(2^n - 1)$) enthalten ist, ist $|z^G| \geq 2^n + 1$. Aus $|w^G| + |z^G| \geq 2^{2n-1} - 2^{n-1} + 2^n + 1 > 2^{2n-1}$ folgt dann $|V| \geq 2^{2n}$. Ist $(|G : C_G(w)|, 2^n + 1) = 1$ für alle $w \in V^\#$, so ist $|V| - 1$ durch $2^n + 1$ teilbar und damit erneut $|V| \geq 2^{2n}$.

Ist V eine elementar-abelsche Gruppe der Ordnung 2^{2n} und G eine zu $L_2(2^n)$ isomorphe Gruppe von Automorphismen von V , so dass eine 2-Sylowgruppe S von G in V eine Gruppe der Ordnung 2^n zentralisiert, so wird im folgenden von einer *natürlichen Darstellung* von G auf V gesprochen. Man verifiziert dann leicht die folgenden Eigenschaften:

- (i) $C_G(C_V(S)) = C_G(v) = S$ für $v \in C_V(S)^\#$,
- (ii) $V = \bigcup_{g \in G} C_V(S^g)$.

BEWEIS VON (a). Sei G ein Gegenbeispiel zu (a), $q = 2^n$, $M = O_2(G)$, $Z = Z(M)$ und $Q = [G, Z]$. Ferner seien α und β Automorphismen von S , so dass $Z^\alpha \neq Z$ gilt und ZZ^β kein Normalteiler von G ist. Die Existenz von α und β folgt aus (*).

(1) $Z/Z(G)$ ist eine elementar-abelsche Gruppe der Ordnung q^2 , auf der G/M eine natürliche Darstellung induziert, und es gilt $|Z : Z(S)| = |Z(S) : Z(G)| = q$. Ferner ist $A(M) \subset A(S)$, und es gilt $|A : A \cap M| = q$ für $A \in A(S) \div A(M)$.

BEWEIS. Aus $Z(S) \leq M$ und (*) folgt $Z(G) < Z(S) < Z$ und $M = C_G(Z)$. Ferner folgt aus (*) $\Omega_1(Z) \not\leq Z(G)$, weshalb G/M treu auf $\Omega_1(Z)$ operiert, und $J(S) \not\leq M$, also die Existenz von $A \in A(S) \div A(M)$. Ist $|A : A \cap M| = 2$, so erhält man $|\Omega_1(Z) : A \cap \Omega_1(Z)| = 2$ aus $|(A \cap M)Z| \leq |A|$, was wegen $((A \cap M)Z)' = 1$ und $A \in A(S)$ gilt. Für $g \in G$ ist dann $|\langle A, A^g \rangle M/M| \leq 6$ und G/M isomorph zu $L_2(2)$. Ist $|A : A \cap M| \geq 2$, so ist daher $\langle A, A^g \rangle M = G$ für $g \in G$ und $a \in A$ mit $o(aa^g M/M) = q + 1$, und es gilt $A \cap A^g \cap Z = Z(G)$. Wegen $|(A \cap M)Z| \leq |A|$ und $|AM : M| \leq q$ bekommt man nun $|A^g \cap Z : Z(G)| \leq |Z : A \cap Z| \leq |A : A \cap M| \leq q$ und damit $|Z : Z(G)| \leq q^2$. Da G/M treu auf $\Omega_1(Z/Z(G))$ operiert, impliziert der Hilfssatz $|Z : Z(G)| = q^2$. Nun erhält man $|A \cap Z : Z(G)| = |Z : A \cap Z| = |A : A \cap M| = q$ und $(A \cap M)Z \in A(M) \cap A(S)$ sowie $A \cap Z = Z(S)$ und damit (1).

(2) Z ist elementar-abelsch.

BEWEIS. Da G/M wegen (1) auf $Z/Z(G)$ eine natürliche Darstellung induziert, gilt

$$Z/Z(G) = \bigcup_{g \in G} Z(S^g/Z(G)) \cap Z/Z(G).$$

Wegen (1) ist ausserdem $Z(S)/Z(G) = Z(S/Z(G)) \cap Z/Z(G)$, also $Z = \bigcup_{g \in G} Z(S^g)$. Nun ist $Z/Z(G)$ elementar-abelsch, also $\mathfrak{U}_1(Z(S)) \leq Z(G)$ womit dann $\mathfrak{U}_1(Z(S)) = \mathfrak{U}_1(Z) = 1$ aus (*) folgt.

(3) Für $z \in Z + Z(S)$ gilt $C_S(z) = C_S(Z) = M$. Ferner gilt $Z^\alpha \leq M$.

BEWEIS. Offensichtlich ist $M = C_S(Z) \leq C_S(z)$. Aus (1) folgt die Existenz von $g \in G$ mit $z \in Z(S^g)$. Gibt es ein $x \in C_S(z)$ mit $x \notin M$, so wird z von $\langle x, S^g \rangle = G$ zentralisiert, was nicht sein kann. Daher ist $C_S(z) = M$. Gilt $Z^\alpha \not\leq M$, so ist $Z \not\leq C_S(Z^\alpha) = M^\alpha = C_S(y)$ für $y \in Z^\alpha + Z(S)$. Dann folgt $|Z^\alpha: Z(S)| = |Z^\alpha: Z^\alpha \cap M| = q$ sowie $S = Z^\alpha M$, und G ist kein Gegenbeispiel.

(4) Für $x \in S + M$ gilt $Z(S) = [x, Z] \times Z(G)$.

BEWEIS. Da x einen involutorischen Automorphismus auf der wegen (2) elementar-abelschen Gruppe Z induziert, ist $|Z: C_Z(x)| = |[x, Z]|$. Wegen (3) und (1) ist aber $|Z: C_Z(x)| = q$. Mit (1) erhält man $q = |[x, Z]| \geq |[xZ(G)/Z(G), Z/Z(G)]| = q$, also $[x, Z] \cap Z(G) = 1$, woraus mit $[x, Z] \leq Z(S)$ dann (4) folgt.

(5) $[S, Z] = Q \cap Z(S)$.

BEWEIS. Sei x ein 2-Element aus $G + N_G(S)$, $R = [S, Z]$ und $L = RR^x$. Aus (4) folgt $R \leq Z(S) \cap Q$. Ausserdem folgt $q = |R: R \cap Z(G)| \leq |R: R \cap R^x|$, also $|L: C_L(x)| = |[L, x]| = q$ und $[x, Z] \leq L$. Wegen $G = \langle x, S \rangle$ ist daher $L = Q$, und es gilt (5).

(6) $Z(S) = Z(J(S))$.

BEWEIS. Sei $g \in G + N_G(S)$, $R = Z(J(S))$ und $A \in A(S^g) + A(M)$. Wegen $(A \cap M)Z \in A(M)$ und $Z(S) \leq R \leq Z(J(M))$ ist $q = |Z(S): A \cap Z(S)| \leq |R: A \cap R| \leq q$, also $|R: A \cap R| = q$ und $R = (R \cap A)Z(S)$. Daher ist $[R, S] \leq R \cap A$. Aus $G = M\langle C_S(R), A \rangle$ und $\langle C_S(R), A \rangle \leq C_G(A \cap R)$ folgt damit, dass $[R, S]$ eine charakteristische Untergruppe von S ist, die normal in G ist. Wegen (*) gilt also $[R, S] = 1$ und $R = Z(S)$.

(7) $J(M)^\alpha \neq J(M)$.

BEWEIS. Sei $R = Z(J(M))$ und $g \in G + N_G(S)$. Angenommen, $J(M)^\alpha = J(M)$. Wegen $Z \leq R$ ist dann $Z < R$ und $Z^\alpha < R$ sowie $C_M(R) < M$. Aus $(A \cap M)Z \in A(M)$ folgt nun $|R: A \cap B \cap R| = q^2$ und $R = (A \cap B \cap R)Z$ für $A \in A(S) + A(M)$, $B \in A(S^g) + A(M)$. Wegen $\langle A, B \rangle M = G$ ist daher $O_2(\langle A, B \rangle C_M(R)) = \langle A, B \rangle C_M(R) \cap M = C_M(R)$. Für $s \in Z^\alpha + Z$ gilt nun $s = rz$ mit $r \in A \cap B \cap R$ und $z \in Z$ sowie $W = C_M(s) = C_M(r) = M \cap M^\alpha$. Da $M \cap M^\alpha$ ein Normalteiler von M und $C_M(r)$ ein Normalteiler von $C_G(r)$ ist, folgt mit $\langle A, B \rangle \leq C_G(R)$ dann, dass W ein Normalteiler von $\langle A, B, M \rangle = G$ ist. Aus $|M: W| \leq |S: M| = q$ und dem Hilfssatz folgt dann $G/W = (M/W) \times L$ mit $L = \langle A, B, W \rangle/W$, wobei L

isomorph zu G/M ist. Gibt es ein $C \in A(S)$ mit $C \nless A W$, so ist CW nicht zu BW konjugiert, also $O_2(\langle C, B, W \rangle / W) \neq 1$, was $C_M(R) \leq W$ und $O_2(\langle C, B, C_M(R) \rangle) = C_M(R)$ widerspricht. Daher ist $J(S) \leq A W$ Widerspruch zu (6).

(8) $|Z^\alpha: Z \cap Z^\alpha| = q$, d.h. $Z \cap Z^\alpha = Z(S)$.

BEWEIS. Wegen $Z(S) = Z(S)^\alpha \leq Z$ und (1) ist $|Z^\alpha: Z \cap Z^\alpha| \leq q$. Ist $|Z^\alpha: Z \cap Z^\alpha| < q$, so gibt es ein $z \in Z \cap Z^\alpha \neq Z(S)$. Nun ist wegen (3) $M = C_S(z) = C_S(Z)$, und aus $Z^\alpha \neq Z$ und $Z = Z(M)$ folgt auch $M^\alpha \neq M$, und man bekommt den Widerspruch $M = C_S(z) \geq M M^\alpha > M$.

(9) $|M: C_M(Z^\alpha)| = q$.

BEWEIS. Aus (7) folgt die Existenz von $A \in A(M^\alpha)$ mit $Z^\alpha \leq A \nless M$. Mit (1) erhält man $A \in A(S)$ und $|A: A \cap M| = q$. Daher ist $|AC_M(Z^\alpha)| = |A| |A \cap M|^{-1} |C_M(Z^\alpha)| = q |C_M(Z^\alpha)|$. Wegen $|S: M^\alpha| = q$ ist nun $|M: C_M(Z^\alpha)| \leq q$, woraus mit $AC_M(Z^\alpha) \leq C_S(Z^\alpha) = M^\alpha$ die Behauptung folgt.

(10) $Z \cap Q^\alpha \leq Z(G)$.

BEWEIS. Angenommen, $Q^\alpha \cap Z \nless Z(G)$. Sei $A \in A(S) + A(M)$ und $g \in G + N_G(S)$. Wegen (9) ist $|M: C_M(Z^\alpha)| = |S: C_S(Z^\alpha)|$ und wegen (5) und (8) also $[M, ZZ^\alpha] = [M, Z^\alpha] = Q^\alpha \cap Z(S) = Q^\alpha \cap Z \nless Z(G)$. Wäre ZZ^α ein Normalteiler von G , so wäre auch $[M, ZZ^\alpha]$ ein Normalteiler von G , was nicht sein kann.

Daher ist ZZ^α kein Normalteiler von G . Aus $[A, B] \leq Z$ für $B = (A \cap M)Z$ folgt dann mit (8) und (3) $|Q^{\alpha g}: Q^{\alpha g} \cap B| = q$, wegen $B \in A(S)$, (1) und (5) also auch $[B, Q^{\alpha g}] = [S^g, Q^{\alpha g}] = Q^{\alpha g} \cap Z(S^g)$. Angenommen, $[Q^\alpha, Q^{\alpha g}] \neq 1$. Aus (3) folgt dann $|Q^\alpha: C_{Q^\alpha}(Q^{\alpha g})| = q$ und mit (5) daher

$$\begin{aligned} Q^{\alpha g} \cap Z(S^g) &= [S^g, Q^{\alpha g}] = [Q^\alpha, Q^{\alpha g}] = [S, Q^\alpha] \\ &= Q^\alpha \cap Z(S) \leq Z(S) \cap Z(S^g) = Z(G). \end{aligned}$$

Wegen $Z = QZ(S)$ und (8) ist aber $Q^\alpha \cap Z(S) = Q^\alpha \cap Z$, und man bekommt einen Widerspruch zur Annahme. Deshalb ist $[Q^\alpha, Q^{\alpha g}] = 1$ und entsprechend $[Q^{\alpha g}, Q^{\alpha g x}] = [Q^\alpha, Q^{\alpha g x}] = 1$ für $x \in A$. Nun ist $C_B(Q^{\alpha g}) = C_A(Q^{\alpha g})Z$, woraus $A \leq N_G(C_B(Q^{\alpha g}))$ folgt. Wegen $C_B(Q^{\alpha g})Q^{\alpha g} \in A(S)$ ist daher $C = C_B(Q^{\alpha g})Q^{\alpha g} = C_B(Q^{\alpha g})Q^{\alpha g x}$ und damit $[B, C] = [B, C^x] = [B, Q^{\alpha g}] = [B, Q^{\alpha g x}] \leq Z(S^g) \cap Z(S^{g x})$. Aus $[B, Q^{\alpha g}] \nless Z(G)$ und $Z(S^g) \cap Z(S^{g x}) = Z(G)$ für $x \in A + M$ erhält man nun einen Widerspruch.

(11) Ist $Q \cap Z(G) \neq 1$ und $x, y \in S + M$ mit $y \notin \langle x \rangle M$, so ist $[x, Z] \cap [y, Z] = 1$.

BEWEIS. Angenommen, (11) ist falsch. Dann ist $q > 2$, und es gibt eine Untergruppe K der Ordnung $q - 1 > 1$ von $N_G(S)$, die transitiv auf $[K, Z(S)]^\#$ operiert. Sei $Q_0 = Q \cap Z(G)$. Wegen (5) und $S = \langle x^K, M \rangle$ ist dann $Q \cap Z(S) = [K, Z(S)][x, Z]$. Ist $u \in [x, Z] + [K, Z(S)]$, so ist wegen (4) $u \notin Q_0$, also $u^K = u[K, Z] + Q_0$. Daher ist

$$Q \cap Z(S) = [K, Z(S)] \cup Q_0 \cup \bigcup_{x \in S} [x, Z].$$

Aus $Q_0 \neq 1$ folgt nun mit (*) die Existenz von $\gamma \in \text{Aut}(S)$ mit $Q_0^\gamma \nless Z(G)$.

Wegen (10) ist dann $Z^\gamma = Z$, weshalb wegen (4) $Q_0^\gamma \cap [x, Z] = 1$ also $Q_0^\gamma \leq [K, Z(S)] \cup Q_0$ und $Q_0^\gamma \cap [K, Z(S)] \neq 1$ gilt. Da K transitiv auf $[K, Z(S)]^\#$ operiert, erhält man $[K, Z(S)] \cap [x, Z] = 1$ sowie $Q \cap Z(S) = [K, Z(S)] \times [x, Z]$ und (11).

(12) $N_G(S) \leq N_G(Z^\alpha)$.

BEWEIS. Angenommen, (12) ist falsch. Dann gibt es einen Automorphismus ξ von S mit $Z^{\alpha\xi} \neq Z^\alpha$, der von einem Element aus $N_G(S)$ induziert wird, und wegen (10) ist $Q^\alpha \cap Z = Q^\alpha \cap Z(S) \leq Z(G)$ invariant bei ξ , also $Q \cap Z(S)$ invariant bei $\alpha\xi\alpha^{-1}$. Nun folgt $Z^{\alpha\xi\alpha^{-1}} \neq Z$ aus $Z^{\alpha\xi} \neq Z^\alpha$. Dies ist aber wegen $Q \cap Z(S) = Q^{\alpha\xi\alpha^{-1}} \cap Z(S) \not\leq Z(G)$ ein Widerspruch zu (10).

(13) $\langle Z^{\alpha G} \rangle$ ist elementar-abelsch.

BEWEIS. Angenommen, (13) ist falsch. Wegen (12) gilt $N_G(S) \leq N_G(Z^\alpha)$. Daher gibt es ein $t \in G$ mit $t^2 \in M$ und $[Q^\alpha, Q^{\alpha t}] \neq 1$. Wegen (10) ist $Q^\alpha \cap Z = Q^\alpha \cap Z(G) = Q^{\alpha t} \cap Z$ und wegen (3) $Q^\alpha \cap Z(G) = C_{Q^\alpha}(Q^{\alpha t})$. Angenommen, $Z(G) \cap Q \neq 1$. Dann ist $q > 2$, und es gibt $x \in Q^\alpha + Z(G)$ und $y \in Q^{\alpha t} + Z(G)$ mit $\langle x \rangle Q^{\alpha t} \neq \langle y' \rangle Q^{\alpha t}$. Dann ist $1 \neq [x, y] \in [x, Q^{\alpha t}] \cap [y, Q^\alpha]$. Aus $[y, Q^\alpha] \leq Z(G)$ folgt nun $[x, y] = [x', y'] \in [x, Q^{\alpha t}] \cap [y', Q^{\alpha t}]$. Wegen (11) ist jedoch $[x, Q^{\alpha t}] \cap [y', Q^{\alpha t}] = 1$, was einen Widerspruch liefert. Daher ist $Q \cap Z(G) = 1$ und $|Q| = q^2$. Sei nun $s \in S$ mit $[Q^\alpha, Q^{\alpha s}] = [Q^{\alpha t}, Q^{\alpha s}] = [Q^\alpha, Q^{\alpha t}]$ und $Q_0 = Q^\alpha Q^{\alpha t} Q^{\alpha s}$ sowie $R = Z(Q_0)$. Für $Q_1, Q_2 \in \{Q^\alpha, Q^{\alpha t}, Q^{\alpha s}\}$ mit $Q_1 \neq Q_2$ sind dann alle Involutionen von $Q_1 Q_2$ in $Q_1 \cup Q_2$ enthalten. Ferner ist $|Q_0| = q^4$ und $|Q_0: C_{Q_0}(Q_1)| = q$, weshalb es $x_1 \in Q^\alpha + R$, $x_2 \in Q^{\alpha t} + R$ und $x_3 \in Q^{\alpha s} + R$ mit $x_1 x_2 \in C_{Q_0}(x_3)$ und $x_1 x_3 \in C_{Q_0}(x_2)$ gibt. Dann ist $(x_1 x_2)^{x_1 x_3} = x_1^{x_1 x_3} x_2 = x_1^{x_3} x_2 = x_3 x_1 x_3 x_2 = x_3 x_2 x_1 x_3 = x_2 x_1$ und wegen $\langle x_1, x_2 \rangle = \langle x_1 x_2, x_2 \rangle$ daher $x_1 x_3 \in N_{Q_0}(\langle x_1, x_2 \rangle)$ sowie $x_3 \in N_{Q_0}(\langle x_1, x_2 \rangle)$. Dann ist aber $\langle x_1, x_2, x_3 \rangle$ eine Gruppe der Ordnung 16 mit einem zyklischen Zentrum $\langle x_1 x_2 x_3 \rangle$ der Ordnung 4. Wegen (3) ist nun $C_{Q_0}(x_1) = C_{Q_0}(Q^\alpha)$, und es folgt $\langle x_1 x_2 x_3 \rangle \leq R$, also $R \not\leq Z(G)$. Angenommen, es gibt eine Involution $z \in R + Z(G)$. Dann ist $z = abc$ mit $a \in Q^\alpha + R$, $b \in Q^{\alpha t} + R$ und $c \in Q^{\alpha s} + R$. Dann ist aber auch $zc = ab$ eine Involution, was nicht sein kann. Daher gilt $\Omega_1(R) = R \cap Z(G)$. Wegen $s^2 \in M$ ist nun $s \in N_S(Q_0)$ also $|S: N_S(R)| < q$ und $|M: N_M(R^{\alpha^{-1}})| < q$ sowie $|M: N_M(R^{\alpha^{-t}})| < q$ und $|Q^{\alpha^{-1}}: N_{Q^{\alpha^{-1}}}(R^{\alpha^{-t}})| < q$. Aus $\Omega_1(R) \leq Z(G)$ folgt $\Omega_1(R^{\alpha^{-t}}) \leq Q$, woraus man $\Omega_1([N_{Q^{\alpha^{-1}}}(R^{\alpha^{-t}}), R^{\alpha^{-t}}]) \leq Q \cap Q^{\alpha^{-1}} = 1$ bekommt. Mit (3) erhält man damit $[Q^{\alpha^{-1}}, R^{\alpha^{-t}}] = 1$ sowie $[Q, R^{\alpha^{-t}\alpha}] = 1$ und $[Q, R^{\alpha^{-t}\alpha t}] = 1$, weswegen $R^{\alpha^{-t}\alpha t} \leq M$ gilt. Nun ist aber $\Omega_1(R^{\alpha^{-t}\alpha t})^\# \leq Q^{\alpha t} + Z(G)$, und $[Q^\alpha, Q^{\alpha t}] \neq 1$ impliziert $R^{\alpha^{-t}\alpha t\alpha^{-1}} \cap M = 1$. Dann ist jedoch S/M nicht elementar-abelsch, was ein Widerspruch ist, der (13) beweist.

(14) Ist $T = \langle Z^{\beta G} \rangle$, so sind $M/C_G(T)$ und T/Z elementar-abelsche Gruppen der Ordnung q^2 , auf denen G/M eine natürliche Darstellung induziert. Ausserdem gilt $[M, T] = [S, Z^\beta]$ und $T = Z(C_M(T))$.

BEWEIS. Wegen (7) gibt es ein $A \in A(S)$ mit $Z^\beta \leq A \not\leq M$. Sei $B = (A \cap M)Z$ und $g \in G + N_G(S)$. Da $Z^{\beta g}$ kein Normalteiler von G ist, gilt

$Z^{\beta g} \ntriangleleft B \in A(M)$, also $|Z^{\beta g}: B \cap Z^{\beta g}| = q$ sowie wegen $Z^{\beta g}C_A(Z^{\beta g}) = \langle Z^{\beta g}A \rangle C_A(Z^{\beta g}) = TC_A(Z^{\beta g}) \in A(M)$ auch $|T: T \cap B| = q$ und $|T/Z: (A \cap T)Z/Z| = q$. Sei $X = A \cap A^g \cap T$. Dann ist $T = Z^{\beta}Z^{\beta g}X$. Wegen $[M, X] \leq Z(G) \leq X$ und $A, A^g \leq C_G(X)$ ist dann X ein Normalteiler von G , und T/XZ sowie $C_M(X)/C_M(T)$ sind elementar-abelsche Gruppen, auf denen G/M natürliche Darstellungen induziert. Angenommen, $X \ntriangleleft Z(G)$. Dann ist $H = C_G(X)$ ein echter Normalteiler von G mit $G = HM$.

Für $q = 2$ wird T/Z von 3 Involutionen erzeugt, und es gilt $|T/Z| = 8$. Für $q > 2$ gibt es $K \leq N_g(S \cap H)$ mit $|K| = q - 1 > 1$. Sei $a \in A + M$ und $Y = [K, Z^{\beta}][a, T]Z/Z$. Dann ist $[A, T/Z] \leq Y$ und $|Y| \leq q^2$. Ausserdem ist YY^g ein Normalteiler von G/Z , der $Z^{\beta}Z/Z$ enthält, also $T/Z = YY^g$, und es gilt $|X: X \cap Z| \leq q$. Wegen $G = \langle A, A^g, M^{\beta} \cap M^{\beta g} \rangle$ folgt aus $X \ntriangleleft Z(G)$ die Existenz von $x \in M^{\beta} \cap M^{\beta g}$ mit $x \notin H$, und es gibt ein $R \in Z^{\beta g}$ mit $x \notin C_M(R)$, wegen (3) also $|R: C_R(x)| = q > |T: C_T(x)|$. Aus $T = Z^{\beta}Z^{\beta g}X$ erhält man $|X: C_X(x)| \geq q$ sowie $|X: X \cap Z(G)| > q$. Daher ist $|X: X \cap Z(G)| = q$. Sei nun $L \leq H$ mit $|L| = q + 1$ und $N = C_M(LC_M(T)/C_M(T))$. Dann ist $G = NH$ sowie $S = NC_S(X)$. Da H/M sowohl auf $Z/Z \cap Z(G)$ als auch auf T/XZ eine natürliche Darstellung induziert, ist $[[T, L]] = q^4$, und es gibt L -invariante Untergruppen V und W von $[T, L] = E$ mit $VW = E$ und $V \leq Q$. Ist W nicht N -invariant, so folgt $1 \neq [N, E] \leq V$, da E von N normalisiert wird und L irreduzibel auf W operiert sowie $V \leq Z(N)$ gilt. Es ist aber $[N, T] \leq [M, T] \leq Q^{\beta} \cap Z \leq Z(G)$ und $V \cap Z(G) = 1$, was einen Widerspruch liefert, aus dem $E \leq Z(N)$ folgt. Hieraus erhält man für $x \in N + C_N(X)$ oder $x \in S + C_S(X)$ dann $|X: C_X(x)| = q$, da $T = EX$ und $|T: C_T(x)| \geq q$ sowie $S = C_S(X)$ gilt. Insgesamt folgt $|X: D \cap X| = |D: C_D(X)| = q$ für $D \in A(S) + A(C_S(X))$.

Sei $P = C_M(KC_M(X)/C_M(X))$ (für $K \leq H$ mit $(S \cap H)K = N_H(S \cap H)$) und $F = [K, T]$. Dann folgt ähnlich wie oben $[P, F] = 1$. Da man K mit $Z^{\beta}Z^{\beta g} = FZ$ wählen kann, gibt es ein $J \in Z^{\beta g}$ mit $|P: C_p(J)| = q$ und wegen $T = Z^{\beta}Z^{\beta g}J = Z^{\beta}Z^{\beta g}X$ folgt $[S, X] = [M, X] = Q^{\beta} \cap Z$.

Sei nun $U = X^{\beta-1}$ und $C = ((A^g \cap M)Z)^{\beta-1}$. Dann ist $C \in A(S) + A(M)$ und $U \leq C$. Ist U ein Normalteiler von G , so auch $[U, M] = Q \cap Z(S)$, was nicht sein kann. Ist $U \ntriangleleft C_M(U^g)$, so folgt $|U: C_U(U^g)| = q$ im Widerspruch zu $[U, U^g] \leq Z(G)$. Daher ist $\langle U^G \rangle$ abelsch. Aus $\langle U^G \rangle C_C(U^g) = U^g C_C(U^g) \in A(M)$ folgt $C \leq N_G((C \cap M)U^g)$ und mit $[C \cap M, U^g] = Z(S^g) \cap Q$ der Widerspruch $C \leq N_G(Z(S^g) \cap Q)$, aus dem $X \leq Z(G)$ und $T = Z^{\beta}Z^{\beta g}$ folgt.

Wegen $C_B(T)T = C_B(T)Z(C_M(T)) \in A(M)$ ist $Z(C_M(T)) = (B \cap B^g \cap Z(C_M(T)))T$. Wegen $M = \langle B, B^g \rangle C_M(T)$ erhält man aber $B \cap B^g \cap Z(C_M(T)) \leq Z$ und $T = Z(C_M(T))$ sowie (14).

(15) $Q \cap Z(G) = 1$.

BEWEIS. Angenommen, (15) ist falsch. Aus (1) folgt dann $q > 2$, und es gibt eine Untergruppe K von $N_G(S)$ mit $|K| = q - 1 > 1$, die wegen (13) Z^{β} und damit $M^{\beta} = C_S(Z^{\beta})$ normalisiert. Ist $[N_G(S), S] \ntriangleleft M^{\beta}$, so lassen sich

$k \in K$ und $s \in S \div M^\beta$ mit $s^k M^\beta \neq s M^\beta$ finden. Aus (11) folgt dann $[s, Z^\beta]^k \neq [s, Z^\beta]$, was jedoch $[s, Z^\beta] \leq Z(G)$ (s. (10)) widerspricht. Daher ist $[N_G(S), S] \leq M^\beta$ und $[K, Z^\beta]$ ein Normalteiler von S . Nun induziert G/M auf $\langle Z^{\beta G} \rangle / Z$ wegen (13) eine natürliche Darstellung, was $||[K, Z^\beta]|| = ||[K, Z(S)]|| ||[K, Z^\beta / Z(S)]|| = q^2$ und damit $[S, Z^\beta] \leq [K, Z^\beta]$ impliziert. Dies ist jedoch ein Widerspruch zu $[S, Z^\beta] \leq Z(G)$.

(16) $\langle Z^{\beta G} \rangle^{\beta^{-1}}$ ist kein Normalteiler von G .

BEWEIS. Sei $T = \langle Z^{\beta G} \rangle^{\beta^{-1}}$ und $R = [M^{\beta^{-1}}, T]$. Angenommen, T ist ein Normalteiler von G . Ist $Z^{\beta^{-1}}$ kein Normalteiler von G , so erhält man $\langle Z^{\beta^{-1}G} \rangle = T$ sowie $[M, T] = [S, Z^{\beta^{-1}}] \leq Z(G)$ aus (14) und (10). Nun ist aber $|M \cap M^{\beta^{-1}}: C_M(T)| = q$, also $1 \neq [M \cap M^{\beta^{-1}}, T] \leq R \leq Q$, was wegen $Q \cap Z(G) = 1$ (s. (15)) nicht sein kann. Daher sind $Z^{\beta^{-1}}$ und $M \cap M^{\beta^{-1}}$ Normalteiler von G , womit aus $|M: M \cap M^{\beta^{-1}}| = |M \cap M^{\beta^{-1}}: C_M(T)| = q$ und dem Hilfssatz $[O^2(G), M] \leq C_M(T)$ folgt. Insbesondere ist dann $1 \neq [M \cap M^{\beta^{-1}}, T] \leq R \leq Q \cap Z(S)$ ein Normalteiler von G , was nicht sein kann.

(17) Für $g \in G \div N_G(S)$ ist $\langle Z^{\beta G} \rangle^{\beta^{-1}} \langle Z^{\beta G} \rangle^{\beta^{-1}g}$ elementar-abelsch.

BEWEIS. Sei $T = \langle Z^{\beta G} \rangle^{\beta^{-1}}$ und $R = [M^{\beta^{-1}}, T]$. Wegen (13) gilt $[Z^{\beta^{-1}}, Z^{\beta^{-1}g}] = 1$, also $Z^{\beta^{-1}} \leq M^{\beta^{-1}g}$ und $Z^{\beta^{-1}g} \leq M^{\beta^{-1}}$, woraus mit (14) $[Z^{\beta^{-1}}, T^g] \leq R^g \leq Q \cap Z(S^g)$ sowie $[Z^{\beta^{-1}g}, T] \leq R \leq Q \cap Z(S)$ folgt. Aus (10) erhält man aber $[M, Z^{\beta^{-1}}] \leq Z(G) \geq [M, Z^{\beta^{-1}g}]$, und wegen $Q \cap Z(G) = 1$ (s. (15)) und $T, T^g \leq C_G(Z) = M$ ist $[Z^{\beta^{-1}}, T^g] = [Z^{\beta^{-1}g}, T] = 1$, also $T^g \leq M^{\beta^{-1}}$ und $T \leq M^{\beta^{-1}g}$. Dann impliziert (14) $[T^g, T] \leq R \cap R^g \leq Z(S) \cap Z(S^g) \cap Q = 1$ und die Behauptung.

(18) Sei $T = \langle Z^{\beta G} \rangle^{\beta^{-1}}$ und g ein wegen (16) existierendes Element aus $G \div N_G(S)$ mit $T^g \neq T$. Ausserdem sei $R = [M^{\beta^{-1}}, T]$, $X = \langle Z^{\beta^{-1}G} \rangle$, $L \in A(S^g) \div A(M)$ mit $Z^{\beta g} \leq L$, $A = ((L \cap M)Z)^{\beta^{-1}}$ und $B = C_A(X)X$. Wegen $L \cap M \not\leq C_G(Z^\beta)$ und $(L \cap M)Z \in A(M) \subseteq A(S)$ ist $A \in A(S) \div A(M)$. Aus (14) folgt $X = Z^{\beta^{-1}}Z^{\beta^{-1}g}$ und $T = ZZ^{\beta g\beta^{-1}}$, weshalb wegen (15) $[T, X] = 1$ sowie $T \leq B \in A(M)$ gilt. Wäre $T^g \leq B$, so wäre $[A, T^g] \leq X \geq [A^g, T^g]$, also $TX = T^gX$. Dann folgte mit (14) $[C_M(X), T] = [C_M(X), T^g] \leq R \cap R^g = 1$, also $TT^g \leq Z(C_m(X)) = X$ im Widerspruch zu $T \neq T^g$. Daher ist $T^g \not\leq B$, d.h. $|B: C_B(T^g)| = |T^g: T^g \cap B| = q$. woraus mit $B \leq C_G(Z^{\beta^{-1}g})$ und (14) $[B, T^g] = R^g$ folgt. Wegen (17) ist nun $[T, T^g] = [T, T^{gx}] = [T^g, T^{gx}] = 1$ für $x \in A$ sowie $C_B(T^g)T^g = C_B(T^g)V \in A(S)$ für $V = \langle T^{gA} \rangle$. Dann ist aber $[B, V] = [B, T^g] = R^g$, was wegen $A \leq N_g(V) \cap N_G(B)$ und $A \not\leq N_G(R^g)$ einen Widerspruch liefert.

BEWEIS VON (b) UND (c). Sei $M = O_2(G)$, $Z = Z(O_2(G))$ und α ein wegen (a) existierender Automorphismus von S mit $Z^\alpha M = S$ sowie $g \in G \div N_G(S)$ und $N = M^\alpha \cap M^{\alpha g}$. Dann wird N von $\langle Z^\alpha, Z^{\alpha g} \rangle$ und wegen $G = M \langle Z^\alpha, Z^{\alpha g} \rangle$ damit von $O^2(G)$ zentralisiert, weshalb aus $|M/N| \leq q^2$ und dem Hilfssatz folgt, dass M/N der einzige nichtzentrale Hauptfaktor von Zweierpotenzordnung von G ist, und es gilt (b). Ausserdem gilt $[S, S, S] \leq N$, also $[S, S, G] = [S, S, S]$, woraus mit (*) auch (c) folgt.

LITERATUR

1. G. Glauberman, *Isomorphic subgroups of finite p -groups*. II, *Canad. J. Math.* **23** (1971), 1023–1039.
2. D. Gorenstein, *Finite groups*, Harper & Row, New York, 1968.
3. C. C. Sims, *Groups and finite permutation groups*, *Math. Z.* **95** (1967), 76–86.

FAKULTÄT FÜR MATHEMATIK, UNIVERSITÄT BIELEFELD, 4800 BIELEFELD 1, FEDERAL REPUBLIC OF GERMANY