TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 150, August 1970

ON 2-GROUPS WITH NO NORMAL ABELIAN SUBGROUPS OF RANK 3, AND THEIR OCCURRENCE AS SYLOW 2-SUBGROUPS OF FINITE SIMPLE GROUPS

BY
ANNE R. MacWILLIAMS[1]

Abstract. We prove that in a finite 2-group with no normal Abelian subgroup of rank $\geqq 3$, every subgroup can be generated by four elements. This result is then used to determine which 2-groups T with no normal Abelian subgroup of rank $\geqq 3$ can occur as S_2's of finite simple groups G, under certain assumptions on the embedding of T in G.

Introduction. In view of the Feit-Thompson theorem (namely, that all finite groups of odd order are solvable), it is natural to classify and search for finite simple groups by considering the structure of a Sylow 2-subgroup and its embedding in the group.

There are comparatively few 2-groups with no normal Abelian subgroup of rank 2—such a 2-group must be cyclic, dihedral, semidihedral, or generalized quaternion. Of these, only dihedral and semidihedral groups can (and do) occur as Sylow 2-subgroups of simple groups (Brauer [4, Theorem 2, p. 321]). However, there is a greater range of 2-groups with no normal Abelian subgroup of rank 3; this paper is part of a project to determine which such 2-groups can occur as Sylow 2-subgroups of simple groups.

The first result is a theorem about 2-groups with no normal Abelian subgroup of rank 3 (apart from questions about simple groups). We show that every subgroup of such a 2-group can be generated by four elements. This is best-possible; in fact, there are 2-groups satisfying the hypothesis and having elementary subgroups of rank 4. Analogs of the four-generator theorem for odd primes are more restrictive; for instance, if p is odd and P is a p-group with no normal Abelian subgroup of rank 3, then every subgroup of P can be generated by three elements (Thompson; Huppert [9, Satz III. 12.3, p. 343]) and every Abelian subgroup of P can be generated by two elements (Feit and Thompson [6, Lemma 8.4(i), p. 797]).

Received by the editors September 12, 1969.

AMS Subject Classifications. Primary 2029, 2040; Secondary 2025, 2027, 2043.

Key Words and Phrases. p-group, Sylow p-subgroup, automorphism, rank, generators, conjugate, transfer homomorphism, fusion.

[1] The author thanks the National Science Foundation for its support, via a National Science Foundation Graduate Fellowship, during this work.

We then suppose that T is a 2-group with a normal Abelian subgroup of rank 2 but none of rank 3; $T\ncong D_8$; and T is a Sylow 2-subgroup of a simple group G. It then follows (Thompson [10]) that T has exactly one normal four-group, say W. We work out all the possibilities for T, using constructive methods together with fusion arguments, under each of the following additional assumptions:

1. $[N_G(T):C_G(T)]$ is divisible by odd primes (so that T admits an automorphism of odd order).

2. $[N_G(T):C_G(T)]$ is a power of 2, and the three involutions of W are all fused together in G. (Then $C_T(W)$ is a maximal subgroup of T and admits an automorphism of order 3.)

If we assume $[N_G(T):C_G(T)]$ is divisible by odd primes (Theorem 1), we find that 3 divides $[N_G(T):C_G(T)]$, and: If $N_G(T)/C_G(T)$ contains a subgroup of order 3 which centralizes W, then T is isomorphic to the Sylow 2-subgroup of the Janko-Hall and Janko-Higman groups; also G has either one or two conjugacy classes of involutions, and if two, it is determined which fusions of T-classes of involutions take place in G. (The Janko-Hall group has two classes of involutions and the Janko-Higman group has one.) If $N_G(T)/C_G(T)$ contains a subgroup of order 3 which does not centralize W, then T is either a four-group or is isomorphic to the Sylow 2-subgroup of $\mathrm{PSU}_3(16)$.

If we assume $[N_G(T):C_G(T)]$ is a power of 2 and the involutions of W are all G-conjugate (Theorem 2), we find that: Either T is isomorphic to the Sylow 2-subgroup of $\mathrm{PSL}_3(q)$ for $q\equiv 1 \bmod 4$ (that is, $T\cong Z_{2^r}\wr Z_2$ for $r\geqq 2$); or $T=\langle Z_{2^r}\wr Z_2, z\rangle$ where z either inverts the base group or raises it to the power $-1+2^{r-1}$; or T is a certain group of order 2^8.

Finally we prove what may be regarded as a sort of converse to Theorem 1; namely, that any simple group G with a Sylow 2-subgroup T isomorphic to the Sylow 2-subgroup of the Janko-Hall and Janko-Higman groups, must have $N_G(T):C_G(T)$ divisible by odd primes.

Notations. Let X be a group. We write $Z(X)$ for the center of X, and $\Phi(X)$ for the Frattini subgroup of X; and $\mathrm{Aut}(X)$, $\mathrm{Inn}(X)$ for the groups of automorphisms, respectively inner automorphisms, of X. $\mathrm{SCN}(X)$ means the set of self-centralizing normal Abelian subgroups of X; $\mathrm{SCN}_n(X)=\{A\in \mathrm{SCN}(X) : \text{rank } A\geqq n\}$.

If Y is any subset of X, and f is any function on X, we write $f|_Y$ for the restriction of f to Y.

If $X_1,\ldots,X_n$ are subgroups of X with $X=X_1\geqq X_2\geqq\cdots\geqq X_n$ and X_{i+1} normal in X_i for $i=1,\ldots,n-1$, the stability group of the chain $X_1\geqq\cdots\geqq X_n$ means $\{\alpha\in\mathrm{Aut}(X) : X_i^\alpha=X_i$ for $i=1,\ldots,n$, and α acts trivially on X_i/X_{i+1} for $i=1,\ldots,n-1\}$.

An involution of X is an element of order 2 in X.

If $x, h\in X$, we write $[h,x]$ for $h^{-1}x^{-1}hx$, and h^x for $x^{-1}hx$. x and $y\in X$ are said to be fused in X if there is $g\in X$ with $x^g=y$.

If X and H are subgroups of some group, we write

$$N_X(H) = \{x \in X : H^x = H\},$$
$$C_X(H) = \{x \in X : h^x = h \quad \text{for every } h \in H\},$$
$$C_X(h) = \{x \in X : h^x = h\} \quad \text{for } h \in H.$$

$A_X(H)$ means the group of automorphisms of H induced by conjugation from X; thus $A_X(H) \simeq N_X(H)/C_X(H)$. $H \lhd X$ means H is a normal subgroup (not necessarily proper) of X.

If X and Y are groups then $X \hookrightarrow Y$ means X is isomorphic to a subgroup of Y; for instance, if $H \leqq G$ are groups, then $N_G(H)/C_G(H \hookrightarrow \text{Aut}\,(H))$.

If G is a p-group, then $\Omega_n(G)$ means the subgroup of G generated by the elements of order $\leqq p^n$; $\mho^n(G)$ means the subgroup generated by the p^nth powers of the elements of G.

Σ_n respectively Σ_n^+ denote the symmetric and alternating groups of degree n.

E_{2^r} denotes an elementary Abelian group of order 2^r.

1. A theorem on 2-groups with no normal Abelian subgroups of rank 3.

1.1. *Useful standard results.*

LEMMA FA. *Let P be a p-group, and let C,D be normal subgroups of P with $C \subseteq D$ and C Abelian. Then there is $K \in \text{SCN}\,(D)$ with $C \leqq K$ and $K \lhd P$.*

Proof. Take a subgroup K of P such that (i) $C \leqq K \leqq D$, $K \lhd P$, and K Abelian. (ii) K is maximal subject to (i). Then $C_D(K) \lhd P$. If $C_D(K) > K$, there is a subgroup R of D with $C_D(K) \geqq R > K$, $[R:K]=p$, and $R \lhd P$. R is Abelian since R contains centrally a subgroup of index p. But then R satisfies (i), contradicting the maximality of K.

LEMMA FB. *If G is a 2-group, then $\Phi(G) = \langle g^2 : g \in G\rangle$.*

Proof. In general, the Frattini subgroup of a p-group is generated by its squares and commutators. If $x, y \in G$, then

$$1 \equiv (xy)^2 = xyxy = x^2x^{-1}y^2y^{-1}xy \equiv [x, y] \mod \langle g^2 : g \in G\rangle.$$

Therefore $[G, G] \subseteq \langle g^2 : g \in G\rangle$, and the result follows.

LEMMA FC. *If G is a 2-group and T, N are subgroups of G such that T normalizes N, then $\Phi(TN) = \langle \Phi(T), \Phi(N), [T, N]\rangle$.*

Proof. For $t \in T$, $n \in N$,

$$(tn)^2 = tntn = t^2t^{-1}n^2n^{-1}tn \equiv [t, n] \mod \langle \Phi(T), \Phi(N)\rangle.$$

The lemma follows from Lemma FB.

For the next lemma we need to observe a few things about the characters of finite Abelian groups. If G is a finite Abelian group, the irreducible complex characters of G are simply homomorphisms from G to the multiplicative group of the complex field. If λ is such a homomorphism, and $g \in G$, we may write the value of λ at g as $\langle g, \lambda\rangle$. The set of such homomorphisms becomes an Abelian group, denoted by G^*, if we define the product of λ and μ by $\langle g, \lambda\mu\rangle = \langle g, \lambda\rangle\langle g, \mu\rangle$.

(i) $G^* \cong G$.

Proof. Write $G = G_1 \times \cdots \times G_k$ as a direct product of cyclic groups. Then for $\lambda \in G^*$, the restriction λ_i of λ to G_i is an element of G_i^*. If $\lambda_i = 1$ for each i, then $\lambda = 1$. So the map $\eta \colon \lambda \to (\lambda_1, \dots, \lambda_k)$ is an injection of G^* into $G_1^* \times \cdots \times G_k^*$.

However, $|G^*|$ = number of conjugacy classes of G, $= |G|$; and for each i, $|G_i^*| = |G_i|$, hence $|G_1^* \times \cdots \times G_k^*| = |G_1^*| \times \cdots \times |G_k^*| = |G_1| \times \cdots \times |G_k| = |G|$. So η is an isomorphism of G^* onto $G_1^* \times \cdots \times G_k^*$. So it will suffice to show that $G_i^* \cong G_i$ for each i, i.e. to show that $G^* \cong G$ if G is cyclic of order n say.

Let ω be a primitive complex nth root of 1, and let $G = \langle g\rangle$. Then $\langle g, \lambda\rangle = \omega$ determines an element of G^*. $\langle g, \lambda^2\rangle = \omega^2$ and so $\lambda, \lambda^2, \dots, \lambda^n = 1$ are distinct elements of G^*. Moreover, any element of G^* must send g to some nth root of 1; so $\lambda, \lambda^2, \dots, \lambda^n$ exhaust G^*. So G^* is cyclic of order n, as desired.

(ii) If $H \leqq G$ for finite Abelian groups H and G, then each linear character of H can be extended to one of G.

Proof. Let $\lambda \in H^*$ and let μ be an irreducible constituent of λ^G = the character of G induced by λ. $(\lambda^G, \mu) = (\lambda, \mu|_H)$ by Frobenius reciprocity. So λ is a constituent of $\mu|_H$. But λ and μ are both linear, hence $\lambda = \mu|_H$; i.e., μ extends λ.

(iii) If G is a finite Abelian group, then the correspondences

$$N \xrightarrow{\varphi} \{\lambda \in G^* : \ker \lambda \supseteq N\}$$
$$(\text{Intersection of the kernels of the } \lambda \in A) \xleftarrow{\theta} A$$

between subgroups of G and G^*, invert one another, so define a one-one correspondence. Moreover, if $N \leftrightarrow A$, then $N \cong G^*/A$.

Proof. The pairing $\langle\ ,\ \rangle$ between the two Abelian groups G and G^* treats G and G^* symmetrically; more precisely, G plays the same role to G^* with respect to $\langle\ ,\ \rangle$ as does G^* to G. The correspondences φ and θ can be rephrased:

$$N \xrightarrow{\varphi} \{\lambda \in G^* : \langle g, \lambda\rangle = 1 \text{ for all } g \in N\}$$
$$\{g \in G : \langle g, \lambda\rangle = 1 \text{ for all } \lambda \in A\} \xleftarrow{\theta} A.$$

Thus it is clear that φ and θ are abstractly the same. So if we show $\theta\varphi = 1$ (i.e., for every subgroup N of G, $\theta(\varphi(N)) = N$), we will also have shown $\varphi\theta = 1$.

We now show $\theta\varphi = 1$. Let $M = \theta(\varphi(N))$; $M \supseteq N$. If $M > N$, then M/N has a nontrivial linear character λ. By (ii), there is a linear character μ of G/N whose restriction to M/N is λ. We may view μ as a character of G, with $N \subseteq \ker \mu$. Then $\mu \in \varphi(N)$; but $M \nsubseteq \ker \mu$, so $M \nsubseteq \theta(\varphi(N))$.

Given a subgroup N of G, let $A = \varphi(N)$. Two elements of G^* are congruent mod A if and only if their restrictions to N agree; so $G^*/A \cong G^*|_N$. By (ii), $G^*|_N = N^*$. Also, by (i), $N^* \cong N$; so $N \cong G^*/A$, as claimed.

Now let G be an arbitrary finite group. The set of linear characters of G acts on the set of all characters of G, by multiplication: for λ linear and χ arbitrary, $\chi \to \chi\lambda$.

For χ an arbitrary character of G, define

$$V(\chi) = \frac{1}{|G|} \sum_{g\in G} \chi(g^2).$$

Then (Feit [5, Vol. 1, p. 24]) $\sum_\chi V(\chi)\chi(1)$ (where χ runs over all the irreducible characters of G) is the number of elements of G whose square is 1.

(iv) If λ is linear and $\lambda^2=1$, then $V(\chi\lambda)=V(\chi)$.

Proof. $V(\chi\lambda)=(1/|G|)\sum_g \chi(g^2)\lambda(g^2)$; but $\lambda(g^2)=\lambda(g)^2=1$ since $\lambda^2=1$.

(v) If χ is any irreducible character of G, N is a normal subgroup of G, and χ vanishes on $G-N$, then $[G:N]\leqq\chi(1)^2$.

Proof. $1=(\chi,\chi)_G=(|N|/|G|)(\chi|_N,\chi|_N)_N$. By Clifford's theorem, $\chi|_N=a\sum_{i=1}^t \theta_i$ where the θ_i are G-conjugate and so all of the same degree. So

$$(\chi|_N,\chi|_N)_N = a^2t \leqq a^2t^2 \leqq (at(\deg\theta_i))^2 = \chi(1)^2.$$

Hence $1\leqq(|N|/|G|)\chi(1)^2$, as desired.

LEMMA FD. *If G is a 2-group with $[G:\Phi(G)]\geqq 2^{2k+1}$, then $\sum_\chi V(\chi)\chi(1) \equiv 0 \bmod 2^{k+1}$ (the sum ranging over all irreducible characters χ of G).*

Proof. For each χ, $V(\chi)$ is an integer (Feit [5]); so we need only consider the χ with degree $\leqq 2^k$.

Suppose $\chi(1)=2^{k-e}$ $(e\geqq 0)$. $A=(G/\Phi(G))^*$ acts on the irreducible characters of G by λ: $\chi\to\chi\lambda$. We will show χ is in an orbit of size $\geqq 2^{e+1}$, and then Lemma FD will follow from (iv).

Let C be the subgroup of A fixing χ; then the size of the orbit containing χ is $[A:C]$. Let N be the intersection of the kernels of the $\lambda\in C$. Then for $g\notin N$, there is $\lambda\in C$ with $\lambda(g)\neq 1$, but $\lambda(g)\chi(g)=\chi(g)$; hence $\chi(g)=0$ for all $g\notin N$. So by (v), $\chi(1)^2\geqq[G:N]$. But $[G:N]=|C|$ by (iii). So

$$|C| \leqq \chi(1)^2 = (2^{k-e})^2 = 2^{2k-2e};$$

hence $[A:C]\geqq 2^{(2k+1)-(2k-2e)}=2^{2e+1}\geqq 2^{e+1}$, as desired.

1.2. *Proof of the theorem.*

FOUR GENERATOR THEOREM. *Let G be a 2-group with no normal Abelian subgroup of rank 3. Then every subgroup of G can be generated by four (or fewer) elements.*

Proof of four generator theorem. Assume false and let G be a counterexample of minimal order.

(i) If G has a subgroup T with $[T:\Phi(T)]\geqq 2^6$ (i.e., T requires *more* than five generators), then G has a subgroup U with $[U:\Phi(U)]=2^5$.

Thus to prove the theorem, we need only show G has no subgroups T with $[T:\Phi(T)]=2^5$.

Proof. Choose T so that $[T:\Phi(T)] \geqq 2^6$ and $|T|$ is minimal subject to this condition. There is a subgroup U of T with $[U:\Phi(T)]=2^5$. If $\Phi(U)$ is proper in $\Phi(T)$, then $[U:\Phi(U)] \geqq 2^6$, which contradicts the minimality of $|T|$.

(ii) If G has a cyclic subgroup K of index $\leqq 2^3$, then G has no subgroups T with $[T:\Phi(T)]=2^5$.

Proof. For such a T, $2^3 \geqq [G:K] \geqq [T:T \cap K] \geqq 2^4$, the last inequality because $T/\Phi(T)$ is elementary of rank 5, and $T \cap K$ is cyclic so can project onto at most a subgroup of order 2 in $T/\Phi(T)$.

(iii) G has a normal four-group, W say.

Proof. If not, G is cyclic or is a 2-group of maximal class (Blackburn [3, Theorem 1.1, p. 3]). So G contains a cyclic subgroup of index 2 (Blackburn [2, Theorem 3.4, p. 68]). This contradicts (ii) since G is a counterexample to the theorem.

(iv) W is the only normal four-group of G.

Proof. Let X be a normal four-group of G, $X \neq W$, $[X, W] \subseteq X \cap W$. If X centralizes W then XW is a normal Abelian subgroup of order $\geqq 8$, and is elementary since generated by involutions; so G has a normal E_8, contrary to hypothesis. So $[X, W]=X \cap W$ is of order 2, and $D=XW \cong D_8$.

G stabilizes the two chains $X > X \cap W > 1$ and $W > X \cap W > 1$, so stabilizes $D > \Phi(D) > 1$. The stability group of $D > \Phi(D) > 1$ is just Inn (D); so $G=DC_G(D)$. Write $C=C_G(D)$; $[G:C]=4$.

If Y is a normal four-group of C, then $Y \lhd G$ and $Y \neq W$ and Y centralizes W, so YW is a normal E_8 or E_{16} of G. So C has no normal four-group. The argument of (iii) (applied to C instead of G) shows that C has a cyclic subgroup K of index 2; thus $[G:K]=8$, contradicting (ii).

(v) $W \leqq \Phi(G)$.

Proof. If not, let M be a maximal subgroup of G with $W \nleqq M$. By Lemma FA (with $C=1$), there is $K \in$ SCN (M), $K \lhd G$. $\Omega_1(K) \lhd G$ and $\Omega_1(K) \neq W$, so K is cyclic by (iv), of order 2^ξ say. $M/K \hookrightarrow$ Aut (K). $|\text{Aut}\,(K)|=2^{\xi-1}$ and so $|M| \leqq 2^\xi 2^{\xi-1}=2^{2\xi-1}$.

If $|G|=32$ and G has a five-generator subgroup, G itself is elementary, so SCN$_3$ (G) is nonempty. So $|G| \geqq 64$, $|M| \geqq 32$. So $2^5 \leqq 2^{2\xi-1}$; $5 \leqq 2\xi-1$; $3 \leqq \xi$.

We will show $[M:K] \leqq 2$; then $[G:K] \leqq 4$, which contradicts (ii).

Suppose $M > K$. Let R be a subgroup with $M \geqq R > K$ and $[R:K]=2$. R is non-Abelian since $K \in$ SCN (M). For $\xi \geqq 3$, there are four non-Abelian 2-groups with cyclic subgroups of order 2^ξ and index 2; they are dihedral, semidihedral, generalized quaternion, and $P(\xi)$, where $P(\xi)=\langle c, k\colon k$ of order 2^ξ, c of order 2, $ckc=k^{1+2^{\xi-1}}\rangle$. $P(\xi)$ has exactly three involutions, which (together with 1) constitute a characteristic four-group.

Let R be a subgroup with $M \geqq R > K$, $[R:K]=2$, and $R \lhd G$. R either centralizes or inverts $\mho^1(K)$ (which is of order $\geqq 4$). If R centralizes $\mho^1(K)$, then $R \cong P(\xi)$, and its characteristic four-group is normal in G and contained in M, so $\neq W$, contrary to (iv). So R inverts $\mho^1(K)$.

Suppose $[M:K] \geqq 4$. Let S, R be subgroups with $M \geqq S > R > K$, $[S:R]=2$, $[R:K]=2$, $S, R \lhd G$. If S/K is cyclic, then R/K induces on $\mho^1(K)$ the square of the automorphism induced by S/K. But R inverts $\mho^1(K)$ and inversion is not a square in $\mathrm{Aut}\,(\mho^1(K))$. So S/K is a four-group. Two of the three subgroups properly between S and K invert $\mho^1(K)$ and the third centralizes $\mho^1(K)$. G permutes these three subgroups, so must normalize the one which centralizes $\mho^1(K)$, contrary to the preceding paragraph. So $[M:K] \leqq 2$, as desired.

(vi) Suppose N is a normal subgroup of G which contains W and centralizes W. Then $[N:\Phi(N)] \leqq 2^4$.

Proof. If $[N:\Phi(N)] \geqq 2^5$, then the number of elements of N whose square is 1 is $\equiv 0 \bmod 8$, by Lemma FD. In particular, $N-W$ contains involutions. Since W is central in N, the involutions of $N-W$ are partitioned into cosets of W; each such coset uniquely determines an E_8 of N which contains W. So the number of such E_8's is $(8k-4)/4$ (where $8k$ is the number of elements of N whose square is 1). $(8k-4)/4=2k-1$, an odd number. $N \lhd G$, so G permutes these E_8's by conjugation. G is a 2-group, so must normalize one of these E_8's.

(vii) If W is central in G, then $|G| \geqq 2^8$.

Proof. Since every maximal subgroup of G contains W, G and all its maximal subgroups are four-generator groups by (vi). So if $|G| < 2^8$, we must have $|G|=2^7$ and some subgroup T of index 4 in G is a five-generator group, therefore elementary. Let M be a maximal subgroup of G with $T \leqq M$. $M=\langle m, T\rangle$ where $m \notin T$, $m^2 \in T$. So m induces on T an automorphism X of order 2. Regard T as a vector space over the field of two elements. Then in the ring of linear transformations of T, $0=X^2-1=(X-1)^2$. So

$$\begin{tikzcd}
\mathrm{Ker}\,(X-1) \arrow[r, phantom, "\geqq"] \arrow[d, equal] & \mathrm{Im}\,(X-1) \arrow[d, equal] \\
C_T(m) & {[T, m].}
\end{tikzcd}$$

But $\mathrm{Dim}\,(\mathrm{Ker}\,(X-1))+\mathrm{Dim}\,(\mathrm{Im}\,(X-1))=\mathrm{Dim}\,(T)=5$. So $|C_T(m)| \geqq 2^3$.

M is non-Abelian; for otherwise $\langle m^2\rangle=\Phi(M)$ is of order $\leqq 2$ and so $[M:\Phi(M)] \geqq 2^5$, contradicting (vi). Therefore $Z(M)=C_T(m) \lhd G$, so G has a normal E_8.

Case I. *Some maximal subgroup M of G has* SCN_3 (M) *nonempty.* $W \subseteq M$ by (v). M has a normal E_8, E say, such that $E \supseteq W$. For if X is any normal E_8 of M, X acts on W and $|C_x(W)| \geqq 4$; also $C_x(W) \lhd M$; so if $W \nsubseteq C_x(W)$, replace X by a suitable E_8 of $WC_x(W)$.

$E \ntriangleleft G$. Let $H=E^g$ for $g \in G-M$. $E \cap H=W$. Write $V=EH$; then $V \cong D_8 \times Z_2$ and $V \lhd G$.

Take $e, h \in G$ with $E=\langle e, W\rangle$, $H=\langle h, W\rangle$. Write $f=eh$. Then $f^2=w$ generates $\Phi(V)$ and so is central in G. $F=\langle f, W\rangle$ is normal in G since it is the only $Z_4 \times Z_2$ of V. Take $w_1 \in W$ such that $W=\langle w, w_1\rangle$.

Let $C=C_G(V)$; $C \lhd G$. By Lemma FA, there is $B \in \mathrm{SCN}(C)$ with $B \supseteq W$ and $B \lhd G$.

(viii) B does not contain w as a square.

Proof. Suppose $x \in B$, $x^2=w$. Then $x \in \Omega_2(B)$. $K=\Omega_2(B)F$ is a normal Abelian subgroup of G. K contains the three involutions of W and also the involution xf. So $|\Omega_1(K)| \geqq 8$ and $\Omega_1(K) \lhd G$.

Therefore $B=\langle b\rangle \times \langle w\rangle$ for b of order 2^m, $m \geqq 1$.

Aut (V). V can be presented as $\langle f, e, w_1 : f^4=1,\ e^2=1,\ efe=f^{-1}=fw;\ w_1^2=1,$ w_1 central$\rangle$ where $\langle w\rangle=\Phi(V)$.

Any set of elements x, y, z of V such that (1) x is of order 4 (there are four such x), (2) y is a noncentral involution of V (there are eight such y), (3) z is a central involution of V other than w (there are two such z) will have: x, y, z generate V and satisfy the same relations as those given above for f, e, w_1. So the automorphisms of V correspond one-to-one with the choices for x, y, z. So $|\mathrm{Aut}\,(V)|=4 \cdot 8 \cdot 2=64$.

Let automorphisms of V be defined as follows:

$$
\begin{aligned}
\alpha&: \ f \to fw;\ e, w_1 \to \text{selves}.\\
\beta&: \ f, w_1 \to \text{selves};\ e \to ew.\\
\xi&: \ f \to fw_1;\ e, w_1 \to \text{selves};\ h \to hw_1.\\
\eta&: \ f, w_1 \to \text{selves};\ e \to ew_1;\ h \to hw_1.\\
\zeta&: \ f, e \to \text{selves};\ w_1 \to ww_1.\\
\theta&: \ f, w_1 \to \text{selves};\ e \to fe.
\end{aligned}
$$

Then α and β are the inner automorphisms induced by e and f respectively. $\langle \alpha, \beta, \xi, \eta\rangle \cong E_{16}$.

ζ centralizes α and β; $\zeta^{-1}\xi\zeta=\alpha\xi$, $\zeta^{-1}\eta\zeta=\beta\eta$; $\zeta^2=1$.

$\theta^{-1}\alpha\theta=\alpha\beta$, $\theta^{-1}\beta\theta=\beta$; $\theta^{-1}\xi\theta=\xi\eta$, $\theta^{-1}\eta\theta=\eta$; $[\theta, \zeta]=1$; $\theta^2=\beta$.

Write $\mathrm{Out}\,(V)$ for $\mathrm{Aut}\,(V)/\mathrm{Inn}\,(V)$. Then $\mathrm{Out}\,(V)=\langle \bar\eta, \bar\xi, \bar\theta\rangle \times \langle \bar\zeta\rangle \cong D_8 \times Z_2$ with $\langle \bar\eta\rangle$ as derived group.

The subgroup of $\mathrm{Aut}\,(V)$ which sends each of E and H to themselves is $\langle \mathrm{Inn}\,(V), \xi, \eta, \zeta\rangle$. The subgroup of $\mathrm{Aut}\,(V)$ which fixes W elementwise is $\langle \mathrm{Inn}\,(V), \xi, \eta, \theta\rangle$. The subgroup of $\mathrm{Aut}\,(V)$ which fixes elementwise the quotient $V/\langle w\rangle$ is $\langle \mathrm{Inn}\,(V), \zeta\rangle$.

Case I.1. $m=1$. I.e. $B=W$. W is central in C, so $W \in \mathrm{SCN}\,(C) \Rightarrow C=W$. So $G/W \hookrightarrow \mathrm{Aut}\,(V)$; hence $|G| \leqq 4 \cdot 64=2^8$.

(ix) In Case I.1, suppose $\eta_0, \zeta_0 \in G$ induce (by conjugation) the automorphisms η, ζ on V; suppose $x, y \in V$. Then $[x\eta_0, y\zeta_0] \equiv f \bmod W$.

Proof.

$$
\begin{aligned}
[x\eta_0, y\zeta_0] &= [x\eta_0, \zeta_0][x\eta_0, y]^{\zeta}\\
&= [x, \zeta_0]^{\eta}[\eta_0, \zeta_0][x, y]^{\eta\zeta}[\eta_0, y]^{\zeta}\\
&= (x^{-1}x^{\zeta})^{\eta}[\eta_0, \zeta_0][x, y]^{\eta\zeta}(y^{-\eta}y)^{\zeta}.
\end{aligned}
$$

Since $[V, \zeta]=\langle w\rangle$ and $[V, \eta]=\langle w_1\rangle$, we have

$$[x\eta_0, y\zeta_0] \equiv [\eta_0, \zeta_0] \quad \text{mod } W.$$

But in Aut V, $[\eta, \zeta]=\beta$; so in G, $[\eta_0, \zeta_0]\equiv f \text{ mod } C_G(V)=W$.

Let T be a five-generator subgroup of G, i.e., $[T{:}\Phi(T)]=2^5$. Then $2^5\leqq |T|\leqq 2^8$. $[T : T\cap V]=[TV{:}\,V]\leqq |\text{Out}\,(V)|=16$.

Case I.1a. T is elementary of rank 5. $[T : T\cap V]\leqq 16 \Rightarrow [T\cap V]\geqq 2$. $T\cap V$ is elementary; the only elementary subgroups of V are the subgroups of E and H, so $T\cap V\subseteq E$ or H.

Suppose $|T\cap V|=8$. Then $T\cap V=E$ or H, and $T/T\cap V\cong E_4$. Now T normalizes $T\cap V$, so $A_{TV}(V)\subseteq\langle \text{Inn}\,(V), \xi, \eta, \zeta\rangle$; also T centralizes W, so $A_{TV}(V)\subseteq\langle\text{Inn}\,(V), \xi, \eta\rangle$. But

$$E_4 \cong T/T\cap V \cong TV/V \to \langle \xi, \bar\eta\rangle.$$

Since $\langle\xi, \bar\eta\rangle$ is a four-group, we must have $A_{TV}(V)=\langle\text{Inn}\,(V), \xi, \bar\eta\rangle$. So T contains an element $x\eta_0$ where $x\in V$ and $\eta_0\in G$ induces the automorphism η on V.

$$[e, x\eta_0] \equiv [e, \eta_0] \quad \text{mod } \langle w\rangle = e^{-1}e^{\eta} = w_1.$$
$$[h, x\eta_0] \equiv [h, \eta_0] \quad \text{mod } \langle w\rangle = h^{-1}h^{\eta} = w_1.$$

So whether $T\cap V$ is E or H, $\Phi(T)$ contains an element congruent to w_1 mod $\langle w\rangle$; but T was elementary.

Suppose $|T\cap V|=4$. Then

$$E_8 \cong T/T\cap V \cong TV/V \hookrightarrow \text{Out}\,(V) \cong D_8\times Z_2.$$

Out (V) has two E_8's, namely $\langle\xi, \bar\eta, \bar\zeta\rangle$ and $\langle\bar\theta, \bar\eta, \bar\zeta\rangle$. So T must contain elements $x\eta_0, y\zeta_0$ where $\eta_0, \zeta_0\in G$ induce η, ζ on V, and $x, y\in V$. But then $\Phi(T)\neq 1$ by (ix).

Suppose $|T\cap V|=2$. Then

$$E_{16} \cong T/T\cap V \cong TV/V \to \text{Out}\,(V) \cong D_8\times Z_2,$$

which is impossible. Therefore Case I.1a is impossible.

Case I.1b. $|T|=2^6$ and $|\Phi(T)|=2$.

$[T : T\cap V]\leqq 16 \Rightarrow |T\cap V|\geqq 4$.

Suppose $T\supseteq V$. Then $\Phi(T)=\langle w\rangle$ and so $T/V\cong E_4$. Also $A_T(V)$ centralizes $V/\langle w\rangle$, so $A_T(V)\subseteq\langle\text{Inn}\,(V), \zeta\rangle$. So

$$E_4 \cong T/V \hookrightarrow \langle\bar\zeta\rangle \cong Z_2,$$

which is impossible.

Suppose $|T\cap V|=8$. Then $T\cap V$ is a maximal subgroup of V, so is $E, H, F=\langle f, W\rangle$, or one of four D_8's of V. If $T\cap V$ is not elementary, then $\Phi(T)=\langle w\rangle$ and so $T/T\cap V$ is elementary; so

$$E_8 \cong T/T\cap V \cong TV/V \hookrightarrow \text{Out}\,(V) \cong D_8\times Z_2.$$

Out (V) has two E_8's, both of which contain $\bar\eta$ and $\bar\zeta$. So T contains elements

$x\eta_0$, $y\zeta_0$ as in (ix). Therefore by (ix), $\Phi(T)$ contains an element of order 4. But this contradicts $|\Phi(T)|=2$. If $T \cap V$ is elementary, then $T \cap V=E$ or H. T normalizes $T \cap V$, so $A_{TV}(V) \subseteq \langle \mathrm{Inn}\,(V), \xi, \eta, \zeta\rangle$. Therefore

$$TV/V \hookrightarrow \langle \bar{\xi}, \bar{\eta}, \bar{\zeta}\rangle.$$

But $[TV\colon V]=[T : T \cap V]=8$. So $A_{TV}(V)=\langle \mathrm{Inn}\,(V), \xi, \eta, \zeta\rangle$ and T contains elements $x\eta_0$, $y\zeta_0$ as in (ix); so by (ix), $\Phi(T)$ contains an element of order 4, contrary to $|\Phi(T)|=2$.

Suppose $|T \cap V|=4$. Then

$$16 = [T : T \cap V] = [TV\colon V] = \mathrm{Out}\,(V).$$

So $A_{TV}(V)=\mathrm{Aut}\,(V)$.

We show $T \cap V=W$. For T normalizes $T \cap V$. If $T \cap V$ is cyclic then $T \cap V=\langle f\rangle$ or $\langle fw_1\rangle$. However, T contains an element $x\xi_0$, where $x \in V$, and $\xi_0 \in G$ induces the automorphism ξ of V; and $x\xi_0$ exchanges the two subgroups $\langle f\rangle$, $\langle fw_1\rangle$ of V. So $T \cap V$ is elementary and so $T \cap V \subseteq E$ or H. T contains an element $x\theta_0$, where $x \in V$, and $\theta_0 \in G$ induces the automorphism θ of V; if $T \cap V \nsubseteq W$, then $x\theta_0$ would not normalize $T \cap V$ since $x\theta_0$ exchanges E and H.

T contains an element $x\zeta_0$, where $x \in V$, and $\zeta_0 \in G$ induces the automorphism ζ of V. So $\Phi(T)$ contains $[w_1, x\zeta_0]=[w_1, \zeta_0]=w$. So $\Phi(T)=\langle w\rangle$, and so $T/T \cap V$ is elementary. But

$$T/T \cap V \cong TV/V \cong \mathrm{Out}\,(V) \cong D_8 \times Z_2.$$

Therefore Case I.1b is impossible.

Case I.1c. $|T|=2^7$ and $|\Phi(T)|=4$.

$[T : T \cap V] \leqq 16 \Rightarrow |T \cap V| \geqq 8$.

Suppose $T \supseteq V$. Then $[T\colon V]=8$ and so $A_T(V)$ is a maximal subgroup of $\mathrm{Aut}\,(V)$; and $A_T(V)$ contains $\mathrm{Inn}\,(V)$. Every maximal subgroup of $\mathrm{Out}\,(V)$ contains $\bar{\eta}$; so T contains an element η_0 which induces η on V. Then $\Phi(T)$ contains $[e, \eta_0] =e^{-1}e^{\eta}=w_1$. Also $\Phi(T) \supseteq \Phi(V)=\langle w\rangle$. So $\Phi(T)=W$, and $T/V \cong E_8$. $\mathrm{Out}\,(V)$ contains two E_8's, both of which contain $\langle \bar{\eta}, \bar{\zeta}\rangle$. So T contains elements η_0, ζ_0 inducing η, ζ on V; by (ix), $\Phi(T) \supseteq \langle f, W\rangle$. This contradicts $|\Phi(T)|=4$.

Suppose $|T \cap V|=8$. Then

$$16 = [T : T \cap V] = [TV\colon V]$$

and so $A_{TV}(V)=\mathrm{Aut}\,(V)$. T contains elements $x\eta_0$, $y\zeta_0$ as in (ix), so by (ix), $\Phi(T)$ contains an element of the coset fW. So $|\Phi(T) \cap V| \geqq 4$; hence $\Phi(T) \subseteq V$, and $T/T \cap V$ is elementary. But

$$T/T \cap V \cong TV/V \cong \mathrm{Out}\,(V) \cong D_8 \times Z_2.$$

Therefore Case I.1c is impossible.

Case I.1d. $|T|=2^8$ and $|\Phi(T)|=8$. Then $T=G$ and G induces all of $\mathrm{Aut}\,(V)$ on V. $\Phi(G) \geqq W$ by (v). Also G contains η_0, ζ_0 inducing η, ζ on V, so $\Phi(G) \supseteq \langle f, W\rangle$ by (ix). By hypothesis, $|\Phi(G)|=8$; so $\Phi(G)=\langle f, W\rangle$ and therefore G/V is elementary. But

$$G/V \cong \operatorname{Out}(V) \cong D_8\times Z_2.$$

Therefore Case I.1d is impossible.

Case I.2. $m=2$. Then $\langle b^2\rangle=\mho^1(B)\lhd G$, so b^2 is central in G. So $W=\langle w, b^2\rangle$ is central in G. We may take $w_1=b^2$ in our computation of $\operatorname{Aut}(V)$.

C/B acts faithfully on B and stabilizes the chain $B>W>1$, so is at most elementary of order 4.

(x) In Case I.2, $\Phi(C)\subseteq W$; and hence

$$\begin{aligned}\Phi(CV) &= \Phi(C)\Phi(V) \quad \text{since } C \text{ centralizes } V\\ &= W.\end{aligned}$$

Proof. By Lemma FB, it suffices to show $x^2\in W$ for all $x\in C$.

$B^2\subseteq W$. Let $x\in C$, $x\notin B$. $x^2\in B$ since C/B is elementary. Now $C_B(x)=W$ since x induces a nontrivial automorphism $\in$ the stability group of $B>W>1$. x centralizes x^2, so $x^2\in W$.

(xi) In Case I.2, $[C:B]\leqq 2$.

Proof. If $[C:B]=4$, then $[CV:\Phi(CV)]=2^5$; and $CV\lhd G$. But this contradicts (vi).

Case I.2.1. $C=B$. Then $|CV|=32$. W is central in G, so $|G|\geqq 2^8$ by (vii), and also $A_G(V)\subseteq\langle\operatorname{Inn}(V), \xi, \eta, \theta\rangle$. $G/CV\hookrightarrow\operatorname{Out}(V)$. So we must have $|G|=2^8$ and $A_G(V)=\langle\operatorname{Inn}(V), \xi, \eta, \theta\rangle$.

If T is a subgroup of G with $[T:\Phi(T)]=2^5$, then by (v) and (vi), $|T|=2^5$ or 2^6 and $|\Phi(T)|=1$ or 2. Since $\Phi(CV)=W$, $T\not\supseteq CV$. $[T:T\cap CV]=[TCV:CV]\leqq 2^3$.

Case I.2.1a. T is elementary of rank 5. $[T:T\cap CV]\leqq 2^3\Rightarrow|T\cap CV|\geqq 2^2$. Since $CV-V$ contains no involutions, the only elementary subgroups of CV are the subgroups of E and H. So $T\cap CV\subseteq E$ or H.

Suppose $T\cap CV=E$ or H. Since T normalizes $T\cap CV$, $A_{TCV}(V)\subseteq\langle\operatorname{Inn}(V), \xi, \eta\rangle$. But $4=[T:T\cap CV]=[TCV:CV]$ and so $A_{TCV}(V)=\langle\operatorname{Inn}(V), \xi, \eta\rangle$. So T contains an element $x\eta_0$, where $x\in V$, and $\eta_0\in G$ induces the automorphism η of V.

$$[e, x\eta_0] \equiv [e, \eta_0] \mod \langle w\rangle = e^{-1}e^{\eta} = w_1.$$

$$[h, x\eta_0] \equiv [h, \eta_0] \mod \langle w\rangle = h^{-1}h^{\eta} = w_1.$$

So whether $T\cap CV$ is E or H, $\Phi(T)$ contains an element congruent to w_1 mod $\langle w\rangle$; but T was elementary.

Suppose $|T\cap CV|=4$. Then

$$E_8\cong T/T\cap CV\cong TCV/CV\hookrightarrow\langle\xi, \bar{\eta}, \bar{\theta}\rangle\cong D_8,$$

which is impossible. So Case I.2.1a is impossible.

Case I.2.1b. $|T|=2^6$ and $|\Phi(T)|=2$.

$$[T:T\cap CV]\leqq 2^3\Rightarrow|T\cap CV|\geqq 8, \qquad T\not\supseteq CV\Rightarrow|T\cap CV|\leqq 16.$$

Suppose $|T \cap CV| = 16$. Then $T \cap CV$ is a maximal subgroup of CV, so is the inverse image in CV of one of the seven hyperplanes of CV/W. If we write $\overline{C}\overline{V}$ for CV/W, then $\overline{C}\overline{V} = \langle \bar{b}, \bar{f}, \bar{e} \rangle$ and the seven hyperplanes are:

1. $\langle \bar{b}, \bar{f} \rangle$
2. $\langle \bar{b}, \bar{f}\bar{e} \rangle$
3. $\langle \bar{b}, \bar{e} \rangle$
4. $\langle \bar{b}\bar{f}, \bar{e} \rangle$
5. $\langle \bar{b}\bar{f}, \bar{e}\bar{f} \rangle$
6. $\langle \bar{b}\bar{e}, \bar{f} \rangle$
7. $\langle \bar{e}, \bar{f} \rangle = \overline{V}$.

The Frattini subgroups of their inverse images are:

1. $\langle b^2, f^2 \rangle = W$
2. $\langle w_1 \rangle$
3. $\langle w_1 \rangle$
4. $\langle (bf)^2, [bf, e] \rangle = \langle w_1 w, w \rangle = W$
5. W
6. $\langle (be)^2, [be, f] \rangle = \langle w_1, w \rangle = W$
7. $\langle w \rangle$.

Since $|\Phi(T)| = 2$, we must have $T \cap CV = \langle b, ef, W \rangle$ or $\langle b, e, W \rangle$ or V.

If $T \cap CV = V$, then $\Phi(T) = \langle w \rangle$, and

$$E_4 \cong T/T \cap CV \cong TCV/CV \hookrightarrow \langle \bar{\xi}, \bar{\eta}, \bar{\theta} \rangle \cong D_8.$$

Every four-group of $\langle \bar{\xi}, \bar{\eta}, \bar{\theta} \rangle$ contains $\bar{\eta}$; so T contains an element $x\eta_0$, where $x \in CV$, and $\eta_0 \in G$ induces the automorphism η on V. Then $\Phi(T)$ contains $[e, x\eta_0] \equiv [e, \eta_0] \bmod \langle w \rangle \equiv w_1 \bmod \langle w \rangle$. So $\Phi(T) \supseteq W$, contrary to $|\Phi(T)| = 2$.

Therefore $T \cap CV$ is $\langle b, E \rangle$ or $\langle b, H \rangle$; $\Phi(T) = \langle w_1 \rangle$.

T normalizes $T \cap V = E$ or H; so $A_{TCV}(V) \subseteq \langle \mathrm{Inn}\,(V), \xi, \eta \rangle$. Also

$$4 = [T : T \cap CV] = [TCV : CV] \hookrightarrow \langle \bar{\xi}, \bar{\eta} \rangle;$$

so $A_{TCV}(V) = \langle \mathrm{Inn}\,(V), \xi, \eta \rangle$ and T contains elements $x\xi_0, y\eta_0$, where $x, y \in CV$, and $\xi_0, \eta_0 \in G$ induce ξ, η on V.

If $T \cap V = E$, then $\Phi(T)$ contains $[e, x\xi_0] = [e, \xi_0][e, x]^\xi = [e, x]^\xi = w$ or 1, according as x does not or does centralize e. Also $\Phi(T)$ contains $[e, y\eta_0] = [e, \eta_0][e, y]^\eta = w_1[e, y]^\eta = w_1 w$ or w_1, according as y does not or does centralize e. But $\Phi(T) = \langle w_1 \rangle$, so x and y must centralize e. $C_{CV}(e) = \langle B, E \rangle = T \cap CV$; so we may take $x = y = 1$.

If $T \cap V = H$, then $\Phi(T)$ contains the elements

$$[h, x\xi_0] = [h, \xi_0][h, x]^\xi = w_1 w \text{ or } w_1$$
$$[h, y\eta_0] = [h, \eta_0][h, y]^\eta = w_1 w \text{ or } w_1$$

according as x, y do not or do centralize h. Since $\Phi(T) = \langle w_1 \rangle$, $x, y \in C_{CV}(h) = \langle B, H \rangle = T \cap CV$; so again we may take $x = y = 1$.

So $T = \langle b, w, e \text{ or } h, \xi_0, \eta_0 \rangle$; $\Phi(T) = \langle w_1 \rangle$.

Consider $R=\langle B, \xi_0, \eta_0\rangle$. $G=\langle R, V, \theta_0\rangle$ where $\theta_0 \in G$ induces θ on V. Now $\langle \operatorname{Inn}(V), \xi, \eta\rangle$ is an Abelian subgroup of Aut (V); therefore in G,

$$[V, \xi_0] \equiv [V, \eta_0] = [V, \xi_0\eta_0] \equiv 1 \mod B = C_G(V).$$

Also $[\xi_0, \eta_0]\equiv 1 \mod B$. So the three subgroups $\langle B, \xi_0\rangle$, $\langle B, \eta_0\rangle$, $\langle B, \xi_0\eta_0\rangle$ of R all normal in RV.

We consider the action of G on these three subgroups. $B \lhd G$. In Aut (V), $[\eta, \theta]=1$ and $[\xi, \theta]=\eta$; so in G,

$$[\eta_0, \theta_0] \equiv 1 \quad \text{and} \quad [\xi_0, \theta_0] \equiv \eta_0 \mod B.$$

Therefore θ_0 normalizes R and $\langle B, \eta_0\rangle$, and exchanges $\langle B, \xi_0\rangle$ and $\langle B, \xi_0\eta_0\rangle$.

Since $\Phi(T)=\langle w_1\rangle=\langle b^2\rangle$, η_0 either centralizes or inverts b. If η_0 centralizes b, then $\langle B, \eta_0\rangle$ is Abelian of order 16 and exponent 4 and has Frattini subgroup of order 2; hence $\Omega_1(\langle B, \eta_0\rangle)\cong E_8$ and is normal in G. Therefore η_0 inverts b.

Also ξ_0 and $\xi_0\eta_0$ either centralize or invert b. So of the three elements ξ_0, η_0, and $\xi_0\eta_0$, two must invert b and one must centralize b. The one centralizing b will (with B) generate an Abelian group, the others will generate non-Abelian groups. Two of these groups are G-conjugate and the third normal in G; so the Abelian one must be $\langle B, \eta_0\rangle$, contrary to the above. Therefore $|T \cap CV|\neq 16$.

Suppose $|T \cap CV|=8$. Then

$$8 = [T : T \cap CV] = [TCV : CV] = [G : CV],$$

so $TCV=G$ and $T/T \cap CV\cong TCV/CV\cong D_8$. Therefore $\Phi(T)\nsubseteq T \cap CV$. Since $|\Phi(T)|=2$, $\Phi(T) \cap (T \cap CV)=1$ and so $T \cap CV$ is elementary, so $\subseteq E$ or H. $|T \cap CV|=8$, so $T \cap CV=E$ or H. But T contains an element $x\theta_0$, where $x \in CV$, and $\theta_0 \in G$ induces θ on V; $x\theta_0$ exchanges E and H. This is impossible since $T \cap CV \lhd T$.

Case I.2.2. $[C:B]=2$. Then $Z(C)=W$; $\Phi(CV)=\Phi(C)\Phi(V)$ (since C centralizes V)$=W$; $Z(CV)=W$. $|CV|=64$. By (vii), $|G|\geqq 2^8$; hence $[G:CV]\geqq 4$.

G normalizes CV and W, so acts on CV/W.

(xi) In Case I.2.2, $C_G(CV/W)=CV$.

Proof. If not, let R be a subgroup of G with $C_G(CV/W)\supseteq R>CV$, $[R:CV]=2$, and $R \lhd G$. R stabilizes the chain $CV>W>1$; the stability group of this chain is elementary, so $\Phi(R)$ centralizes CV. But also $\Phi(R)\subseteq CV$; so $\Phi(R)\subseteq Z(CV)=W$. So $\Phi(R)=W$, and $[R:\Phi(R)]=2^5$; this contradicts (vi).

So G/CV acts faithfully on CV/W. But $C \lhd G$, $V \lhd G$; so as G-module, $CV/W=(C/W)\times(V/W)$ is the direct product of two four-groups; so $[G:CV]\leqq 4$. Hence $[G:CV]=4$ and G contains elements λ, μ inducing the following automorphisms of CV/W: λ centralizes V/W and bW, and sends cW to cbW for $c \in C-B$; μ centralizes C/W and fW, and sends eW to $efW=hW$.

Since $[G:CV]=4$, $|G|=2^8$. By (vi), G and all its maximal subgroups are four-generator groups. So if G has a subgroup T with $[T:\Phi(T)]=2^5$, then either T is elementary of order 2^5, or $|T|=2^6$ and $|\Phi(T)|=2$. Since $\Phi(CV)=W$, $T\not\supseteq CV$. $[T:T\cap CV]=[TCV:CV]\leqq 4$.

(xii) In Case I.2.2, if G has a subgroup T with $[T:\Phi(T)]=2^5$, then G has a subgroup T with $[T:\Phi(T)]=2^5$ and $T\supseteq W$.

Proof. Let T be a subgroup of G with $[T:\Phi(T)]=2^5$ and $|T|$ minimal. W is elementary and central in G, so $\Phi(TW)=\Phi(T)$. If $W\nsubseteq T$, consider TW; there is a subgroup L of TW with $\langle\Phi(T), W\rangle\leqq L$ and $[L:\Phi(T)]=2^5$. Then $|L|=|T|$; so by minimality of $|T|$, $[L:\Phi(L)]=2^5$.

Case I.2.2a. T is elementary of rank 5, $T\supseteq W$.

$[T:T\cap CV]\leqq 4 \Rightarrow |T\cap CV|\geqq 8$.

Suppose $|T\cap CV|=32$; then $T\subseteq CV$ is the inverse image in CV of a hyperplane of $CV/W=\langle\bar{c}, \bar{b}, \bar{f}, \bar{e}\rangle$. Any hyperplane intersects the two-dimensional subspace $\langle\bar{b},\bar{f}\rangle$ of CV/W; so $|T\cap\langle b,f, W\rangle|\geqq 8$. But $\langle b,f, W\rangle=\langle b,f\rangle\cong \boldsymbol{Z}_4\times \boldsymbol{Z}_4$; so T is not elementary.

Suppose $|T\cap CV|=16$. Then $[T : T\cap CV]=2$, so T contains an element $x\lambda$, $x\mu$, or $x\lambda\mu$ for $x\in CV$. If T contains $x\lambda$, then T/W elementary $\Rightarrow (T\cap CV)/W \subseteq \boldsymbol{C}_{CV/W}(\lambda)=\langle\bar{b}, \bar{V}\rangle$. If T contains $x\mu$, then T/W elementary $\Rightarrow (T\cap CV)/W\subseteq \boldsymbol{C}_{CV/W}(\mu)=\langle\bar{f}, \bar{C}\rangle$. If T contains $x\lambda\mu$, then T/W elementary $\Rightarrow (T\cap CV)/W \subseteq \boldsymbol{C}_{CV/W}(\lambda\mu)=\langle\bar{b},\bar{f}\rangle$. Now $\langle b, V\rangle$ and $\langle f, C\rangle$ are of order 32 and $\langle b,f\rangle$ is of order 16; so in any of these three cases, $T\cap CV$ contains a maximal subgroup of $\langle b,f\rangle\cong Z_4\times Z_4$, and so T is not elementary.

Suppose $|T\cap CV|=8$. Then $[T : T\cap CV]=4$, so T contains elements $x\lambda$, $y\mu$ for some $x, y\in CV$. T/W elementary $\Rightarrow (T\cap CV)/W\subseteq C_{CV/W}(\langle\lambda, \mu\rangle)=\langle\bar{b},\bar{f}\rangle$. So $T\cap CV$ is a maximal subgroup of $\langle b,f\rangle\cong Z_4\times Z_4$; so T is not elementary. So Case I.2.2a is impossible.

Case I.2.2b. $|T|=2^6$ and $|\Phi(T)|=2$.

$[T : T\cap CV]\leqq 4 \Rightarrow |T\cap CV|\geqq 16$.

Suppose $|T\cap CV|=32$. Then $[T : T\cap CV]=2$ and T contains an element $x\lambda$, $x\mu$, or $x\lambda\mu$ for some $x\in CV$.

Suppose $x\lambda\in T$. Then $(T\cap CV)/W\subseteq C_{CV/W}(\lambda)=\langle\bar{b}, \bar{V}\rangle$. For if not, $(T\cap CV)/W$ contains $\bar{c}\bar{a}$ for some $\bar{a}\in\langle\bar{b}, \bar{V}\rangle$, and $[\bar{c}\bar{a}, \bar{x}\bar{\lambda}]=\bar{b}$; so $\Phi(T)$ contains an element of the coset bW; but this contradicts $|\Phi(T)|=2$. So $T\cap CV\subseteq\langle b, V, W\rangle$; since $|T\cap CV|=32$, $T\cap CV=\langle b, V, W\rangle=\langle b, V\rangle$. But $\Phi(\langle b, V\rangle)=W$, contradicting $|\Phi(T)|=2$.

Suppose $x\mu\in T$. Then $(T\cap CV)/W\subseteq C_{CV/W}(\mu)=\langle\bar{c},\bar{f}\rangle$. For if not, $(T\cap CV)/W$ contains $\bar{e}\bar{a}$ for some $\bar{a}\in\langle\bar{c},\bar{f}\rangle$, and $[\bar{e}\bar{a}, \bar{x}\bar{\mu}]=f$; so $\Phi(T)$ contains an element of fW, contrary to $|\Phi(T)|=2$. So $T\cap CV=\langle C,f\rangle$; but $\Phi(\langle c,f\rangle)=W$, contradicting $|\Phi(T)|=2$.

Suppose $x\lambda\mu\in T$. Then $(T\cap CV)/W\subseteq C_{CV/W}(\lambda\mu)=\langle\bar{b},\bar{f}\rangle$. For if not, then $(T\cap CV)/W$ contains one of $\bar{c}\bar{a}$, $\bar{e}\bar{a}$, $\bar{c}\bar{e}\bar{a}$ for $\bar{a}\in\langle\bar{b},\bar{f}\rangle$; correspondingly, $[\bar{c}\bar{a}, \bar{x}\bar{\lambda}\bar{\mu}]=\bar{b}$, $[\bar{e}\bar{a}, \bar{x}\bar{\lambda}\bar{\mu}]=\bar{f}$, $[\bar{c}\bar{e}\bar{a}, \bar{x}\bar{\lambda}\bar{\mu}]=\overline{bf}$; and $\Phi(T)$ contains an element of bW, fW, or bfW, contrary to $|\Phi(T)|=2$. So $T\cap CV\subseteq\langle b,f\rangle$, contrary to $|T\cap CV|=32$.

Suppose $|T \cap CV| = 16$. Then $[TCV{:}CV] = 4$, so T contains elements $x\lambda$ and $y\mu$ for $x, y \in CV$. As above, $(T \cap CV)/W \subseteq \langle \bar{b}, \bar{f} \rangle$, so $T \cap CV = \langle b, f \rangle$; but $\Phi(\langle b, f \rangle) = W$, contrary to $|\Phi(T)| = 2$. So Case I.2.2b is impossible.

Case I.3. $m \geqq 3$. Let $d = b^{2^{m-2}}$; $\langle d \rangle = \mho^{m-2}(B)$, so $\langle d \rangle \lhd G$. $d^2 = w_1$ is central in G, so W is central in G.

(xiii) In Case I.3, if G has a subgroup T with Frattini quotient of rank 5, then so does $G/\langle w_1 \rangle$.

Proof. If $w_1 \notin T$, then $G/\langle w_1 \rangle$ contains an isomorphic copy of T. If $w_1 \in \Phi(T)$, then $T/\langle w_1 \rangle$ has Frattini quotient isomorphic to that of T. If $w_1 \in T$ but $w_1 \notin \Phi(T)$, then $d \notin T$; let $D = \langle d \rangle$. $\Phi(TD) = \langle \Phi(T), \Phi(D), [T, D] \rangle$ (by Lemma FC) $=$ $\langle \Phi(T), w_1 \rangle$. So $[TD{:}\Phi(TD)] = [T{:}\Phi(T)]$, and $TD/\langle w_1 \rangle$ has Frattini quotient of rank 5.

So by induction on $|G|$, $G/\langle w_1 \rangle$ has a normal E_8, say $K/\langle w_1 \rangle$. $w\langle w_1 \rangle$ and $d\langle w_1 \rangle$ are central involutions of $G/\langle w_1 \rangle$, so we may take $K \supseteq \langle d, W \rangle$. $\Phi(K) = \langle w_1 \rangle$ and K is of order 16 and exponent 4; so K is non-Abelian because otherwise $\Omega_1(K)$ would be a normal E_8 of G. Therefore $Z(K) = W$. $K \cap V \lhd G$ and $\Phi(K \cap V) \subseteq \Phi(K) \cap \Phi(V) = 1$; so $K \cap V = W$ and $|KV| = 64$.

(xiv) In Case I.3, $Z(KV) = W$.

Proof. Let $a \in K$, $v \in W$ with $av \in Z(KV)$. Then $av = (av)^d = a^d v$ since d centralizes V. So $a \in C_K(D) = \langle d, W \rangle$. Therefore for $x \in V$, $av = (av)^x = a^x v^x = av^x$ since $\langle d, W \rangle$ centralizes V. So $v \in Z(V) = W$; so $av \in Z(K) = W$.

G acts on KV/W, since KV and W are normal in G.

(xv) In Case I.3, $C_G(KV/W) = KV$.

Proof. If not, take a subgroup R of G such that $C_G(KV/W) \supseteq R > KV$, $[R{:}KV] = 2$, and $R \lhd G$. R stabilizes the chain $KV > W > 1$, and the stability group of this chain is elementary; so $\Phi(R)$ centralizes KV. But also $\Phi(R) \subseteq KV$, so $\Phi(R) \subseteq Z(KV) = W$. So $\Phi(R) = W$ and $[R{:}\Phi(R)] = 2^5$; this contradicts (vi).

So G/KV acts faithfully on KV/W. $K \lhd G$ and $V \lhd G$; so as G-module, $KV/W = (K/W) \times (V/W)$ is a direct product of four-groups each invariant under G. Therefore $[G{:}KV] \leqq 4$. By (vii), $|G| \geqq 2^8$; so we have $|KV| = 2^6$, $|G| = 2^8$, and $[G{:}KV] = 4$.

G has no subgroups requiring 5 or more generators which contain KV. For by (vi), G and all its maximal subgroups are four-generator groups; and $\Phi(KV) = W$ so KV is a four-generator group.

Let T be any subgroup of G. We will show TKV requires at least as many generators as T (i.e., $[TKV{:}\Phi(TKV)] \geqq [T{:}\Phi(T)]$). This will prove that every subgroup of G is a four-generator group, and so finish Case I.

W is elementary and central in G, so $\Phi(TW) = \Phi(T)$ and hence TW requires at least as many generators as T. So we will be done if we can show that $(TW)KV$ requires at least as many generators as TW; i.e., we may assume $T \supseteq W$.

We will now show $[TD{:}\Phi(TD)] \geqq [T{:}\Phi(T)]$. For $\Phi(TD) = \langle \Phi(T), \Phi(D), [T, D] \rangle$ (by Lemma FC) $= \langle \Phi(T), w_1 \rangle$. If $TD \neq T$ then $[\Phi(TD){:}\Phi(T)] \leqq 2$ and $[TD{:}T] = 2$, so $[TD:\Phi(TD)]\geqq[T:\Phi(T)]$. So we may assume that $T\supseteq D$, and therefore that $w_1\in\Phi(T)$.

We will now show $[TF:\Phi(TF)]\geqq[T:\Phi(T)]$. For $\Phi(TF)=\langle\Phi(T), \Phi(F), [T, F]\rangle \subseteq\langle\Phi(T), w, W\rangle$ since F, $W\lhd G$ and $[F:W]=2$. Since $w_1\in\Phi(T)$, $[\Phi(TF):\Phi(T)] \leqq 2$, and the conclusion follows. So we may assume that $T\supseteq F$, and therefore that $W\subseteq\Phi(T)$.

We will now show $[TV:\Phi(TV)]\geqq[T:\Phi(T)]$. $\Phi(TV)=\langle\Phi(T), \Phi(V), [T, V]\rangle \subseteq\langle\Phi(T), F\rangle$ since $V, F\lhd G$ and $[V:F]=2$. Since $W\subseteq\Phi(T)$, $[\Phi(TV):\Phi(T)]\leqq 2$, and the conclusion follows. So we may assume $T\supseteq V$.

We now show $[TK:\Phi(TK)]\geqq[T:\Phi(T)]$, which will complete the argument. For $\Phi(TK)=\langle\Phi(T), \Phi(K), [T, K]\rangle\subseteq\langle\Phi(T), d, W\rangle$ since K and $\langle d, W\rangle\lhd G$ and $[K:\langle d, W\rangle]=2$. Since $W\subseteq\Phi(T)$, $[\Phi(TK):\Phi(T)]\leqq 2$, and the conclusion follows.

Case II. *Every maximal subgroup M of G has* SCN_3 *(M) empty*. Every proper subgroup of G is contained in some maximal subgroup, so is a four-generator group by induction on $|G|$. So we need only show G is a four-generator group.

If W is central in G, then G is a four-generator group by (vi). Also $W\subseteq\Phi(G)$ by (v), so if G is a counterexample to the theorem, then $[G:W]\geqq 2^5$, so $|G|\geqq 2^7$.

(xvi) If $|G|=2^7$ and W is noncentral in G, then G is a four-generator group.

Proof. Let $K=C_G(W)$; $|K|=2^6$. By (vi) (applied to K instead of G), K is a four-generator group, so $|\Phi(K)|\geqq 4$. $W\subseteq\Phi(G)$, so if $\Phi(K)\neq W$ then $\langle\Phi(K), W\rangle\subseteq\Phi(G)$ $\Rightarrow |\Phi(G)|\geqq 8\Rightarrow[G:\Phi(G)]\leqq 16$. So if G is not a four-generator group, we must have $\Phi(K)=W$.

$\Phi(K)$ is generated by the squares of the elements of K (by Lemma FB), so there is $x\in K$, $x\notin W$, with x^2 a noncentral involution of G $(x^2\in W)$. For this x, if $g\in G-K$ then $(x^g)^2=(x^2)^g\neq x^2$, so $x^g\not\equiv x \bmod W$. So there are elements $a, b\in K$ with $K=\langle a, b, x, x^g\rangle$; then $G=\langle a, b, x, g\rangle$.

Let $\Omega_1(Z(G))=\langle w\rangle$; $w\in\Phi(G)$ since $W\subseteq\Phi(G)$. Therefore $G/\langle w\rangle$ requires as many generators as G; so by induction on $|G|$, $G/\langle w\rangle$ has a normal E_8, $V/\langle w\rangle$ say. $V\lhd G$, $\Phi(V)=\langle w\rangle$, and V is of exponent 4 and order 16. V is non-Abelian since otherwise $E_8\cong\Omega_1(V)\lhd G$.

$V\cong Q_8\times Z_2$, $D_8\times Z_2$, or $Q_8\circ Z_4$. For if $x, y\in V$ have $[x, y]\neq 1$, then $[x, y]=w$ and $R=\langle x, y\rangle\cong Q_8$ or D_8. $V=RC_V(R)$. $|C_V(R)\cap R|=2$, so $|C_V(R)|=4$ and $C_V(R)\cong E_4$ or Z_4. If E_4, then $V\cong Q_8\times Z_2$ or $D_8\times Z_2$; if Z_4, then $V\cong Q_8\circ Z_4\cong D_8\circ Z_4$.

If $V\cong D_8\times Z_2$, then G must permute the two E_8's E and H of V; then $N_G(E)=N_G(H)$ is a maximal subgroup of G with SCN_3 nonempty, contrary to assumption. So $V\not\cong D_8\times Z_2$.

(xvii) In Case II, if $V\cong Q_8\circ Z_4$ then G is a four-generator group.

Proof. Write $V=Q\circ\langle z\rangle$ where z is central of order 4, $z^2=w$, and $i, j, k\in Q$ represent the nonidentity cosets of $\langle w\rangle$ in $Q\cong Q_8$. Then the cosets of $\langle w\rangle$ in V are represented by i, j, k; z; zi, zj, zk. The cosets represented by i, j, k are the only cosets consisting of noncentral elements of order 4 in V, so these cosets are permuted by G; hence $Q \lhd G$. Q contains three Z_4's—$\langle i\rangle$, $\langle j\rangle$, and $\langle k\rangle$—which are permuted by G, so one—say $\langle i\rangle$—is normal in G. Also $\langle z\rangle = Z(V) \lhd G$.

Write $C = C_G(Q)$. $C \lhd G$ and $[G:CQ] \leqq 2$. If $G > CQ$ then $G = \langle CQ, g\rangle$ where $j^g \equiv k \bmod \langle w\rangle$.

By Lemma FA, there is $B \in \mathrm{SCN}\,(C)$ with $B \supseteq \langle z\rangle$ and $B \lhd G$. Every such B is cyclic; for if not, consider $K = \langle \Omega_2(B), i\rangle$. K is a normal Abelian subgroup of G and contains the three involutions of $\Omega_1(B)$ and also the involution zi; so $\Omega_1(K) \lhd G$ and is of order $\geqq 8$.

Write $B = \langle b\rangle$ of order 2^ξ; $\xi \geqq 2$ since $z \in B$. If $\xi = 2$ then $B \in \mathrm{SCN}\,(C) \Rightarrow |C| \leqq 8$ and $|G| \leqq 64$; then G is a four-generator group since $W \subseteq \Phi(G)$. So $\xi \geqq 3$.

If $C = B$ then $CQ = \langle b, Q\rangle = \langle b, j, k\rangle$, and if $G > CQ$ then $G = \langle b, j, g\rangle$. So we may assume $C > B$. Let $C \geqq R > B$ with $[R:B] = 2$. R is non-Abelian since $B \in \mathrm{SCN}\,(C)$. The only non-Abelian 2-groups with a cyclic subgroup of index 2 and order 2^ξ are dihedral, semidihedral, generalized quaternion, and $P(\xi) = \langle c, b\colon b$ has order 2^ξ, $c^2 = 1$, $cbc = b^{1+2^{\xi-1}}\rangle$. $P(\xi)$ has exactly three involutions, which (together with 1) constitute a characteristic four-group.

Let $C \geqq R > B$ with $[R:B] = 2$ and $R \lhd G$. R either centralizes or inverts $\mho^1(B)$ (whose order is $\geqq 4$). If R centralizes $\mho^1(B)$, then $R \cong P(\xi)$ and its characteristic four-group X is normal in G. $W \subseteq V$, $W \nsubseteq Z(V)$, and $X \leqq C$, so X centralizes W and $X \neq W$; so XW is a normal E_8 of G. Therefore R inverts $\mho^1(B)$.

We now show $[C:B] \leqq 2$. For if not, let R, S be subgroups of G with $C \geqq S > R > B$, $[S:R] = 2$, $[R:B] = 2$, and $R, S \lhd G$. If S/B is cyclic, then $R/B = (S/B)^2$ so R induces on $\mho^1(B)$ the square of the automorphism which S induces on $\mho^1(B)$; but R inverts $\mho^1(B)$ and inversion is not a square in $\mathrm{Aut}\,(\mho^1(B))$. So S/B is a four-group. Two of the three subgroups properly between S and B, invert $\mho^1(B)$, and the third centralizes $\mho^1(B)$. G permutes these three subgroups so must normalize the one which centralizes $\mho^1(B)$, but this is impossible.

Therefore $C = \langle c, b\rangle$ for $c \in C - B$. $CQ = \langle c, b, j, k\rangle$; if $G > CQ$ then $G = \langle c, b, j, j^g, g\rangle = \langle c, b, j, g\rangle$ for $g \in G - CQ$.

So if G is a counterexample to the theorem, $V \cong Q_8 \times Z_2$. Write $V = Q \times \langle w_1\rangle$, where $Q \cong Q_8$ has derived group $\langle w\rangle$, and $w_1 \in W - \langle w\rangle$. Let i, j, k represent the three nonidentity cosets of $\langle w\rangle$ in Q. $W = Z(V)$ and V has three maximal subgroups containing W, namely $\langle W, i\rangle$, $\langle W, j\rangle$, and $\langle W, k\rangle$. These are permuted by G, so one—say $\langle W, i\rangle$—is normal in G.

Write $C = C_G(V)$. $C \lhd G$, and by Lemma FA, there is $B \in \mathrm{SCN}\,(C)$ with $B \geqq W$ and $B \lhd G$. Now w is not a square in B; for if $x \in B$ has $x^2 = w$, then $x \in \Omega_2(B)$, and $K = \langle \Omega_2(B), i, W\rangle$ is a normal Abelian subgroup of G; K contains the three involutions of W and also the involution xi; so $\Omega_1(K) \lhd G$ and is of rank at least 3, so contains a normal E_8 of G.

So $B = \langle b\rangle \times \langle w\rangle$ where b is of order 2^m, $m \geqq 1$. If $m > 1$ then $\langle b^{2^{m-1}}\rangle = \mho^{m-1}(B)$ $\lhd G$ and so $W = \langle b^{2^{m-1}}, w\rangle$ is central in G, so that G is a four-generator group by (vi). So $m=1$ and $B=W$. $W\in \mathrm{SCN}(C)$ and W central in $C \Rightarrow C=W$, so $G/W \hookrightarrow \mathrm{Aut}(V)$.

Aut (V). An abstract $Q_8\times Z_2$, with $\langle w\rangle$ as Frattini subgroup, can be presented as $\langle x, y, z\colon x^2=w, y^2=w, y^{-1}xy=xw=x^{-1}; z^2=1, z \text{ central}\rangle$.

Now any a, b, c such that:

(1) a, b are of order 4 and are independent mod the center (there are $12\cdot 8$ such ordered pairs (a, b)),

(2) c is a central involution $\neq w$ (there are two such c)

will generate $Q_8\times Z_2$ and satisfy the same relations as those given above for x, y, z. So the automorphisms of $Q_8\times Z_2$ are in one-one correspondence with the choices for a, b, c. So $|\mathrm{Aut}(V)|=12\cdot 8\cdot 2=3\cdot 64$.

We exhibit the following automorphisms of $V=\langle i, j, k, w_1\rangle$:

I_i, I_j, I_k = inner automorphisms induced by i, j, k. (Then $I_iI_j = I_k$.)
α: $i, w_1 \to$ selves, $j\to jw_1$, $k\to kw_1$.
β: $j, w_1 \to$ selves, $i\to iw_1$, $k\to kw_1$.
γ: $k, w_1\to$ selves, $i\to iw_1$, $j\to jw_1$. (Then $\alpha\beta = \gamma$.)
ζ: $i, j, k\to$ selves, $w_1\to ww_1$.
θ: $i, w_1\to$ selves, $j\to k$, $k\to j$.

Then $\langle \mathrm{Inn}(V), \alpha, \beta\rangle \cong E_{16}$.

ζ centralizes $\mathrm{Inn}(V)$ and $\zeta^2=1$; $\zeta\alpha\zeta=I_i\alpha$, $\zeta\beta\zeta=I_j\beta$, $\zeta\gamma\zeta=I_k\gamma$.

$\theta^2=1$, θ centralizes ζ; $\theta I_i\theta=I_i$, $\theta I_j\theta=I_k=I_iI_j$, $\theta\alpha\theta=\alpha$, $\theta\beta\theta=\gamma=\alpha\beta$.

These automorphisms generate a full Sylow 2-subgroup of Aut (V), namely the Sylow 2-subgroup stabilizing $\langle W, i\rangle$ and exchanging $\langle W, j\rangle$ and $\langle W, k\rangle$. We have chosen notation in G so that $\langle W, i\rangle \lhd G$, which amounts to saying that $A_G(V)$ lies in this particular Sylow 2-subgroup of Aut (V).

$G/W\to \mathrm{Aut}(V) \Rightarrow [G\colon W]\leqq 64$, $|G|\leqq 2^8$. So by (xvi), $|G|=2^8$ and $A_G(V)$ is the full Sylow 2-subgroup of Aut (V). So G contains elements $\alpha_0, \beta_0, \gamma_0, \zeta_0$ inducing the automorphisms $\alpha, \beta, \gamma, \zeta$ on V. Now in Aut (V),

$$[\alpha, \zeta] = I_i, \qquad [\beta, \zeta] = I_j, \qquad [\gamma, \zeta] = I_k;$$

hence in G,

$$[\alpha_0, \zeta_0] \equiv i, \qquad [\beta_0, \zeta_0] \equiv j, \qquad [\gamma_0, \zeta_0] \equiv k \mod C_G(V) = W.$$

$\Phi(G)\geqq W$ by (v), and so $\Phi(G)\supseteq\langle W, i, j, k\rangle = V$. So $|\Phi(G)|\geqq 16$ and $[G\colon\Phi(G)]\leqq 2^4$.

This finishes Case II, and hence finishes the proof of the theorem.

2. **Some useful results for dealing with simple groups.** In this section we present two useful lemmas, and also establish some notation and properties for Aut $(Z_4\times Z_4)$.

Lemma A (Thompson's transfer theorem). *Let G be a finite group of even order with no subgroup of index 2; let T be a Sylow 2-subgroup of G, and M a maximal subgroup of T. Let $x\in G$ be an involution outside M. Then some G-conjugate of x lies in M.*

Proof. Consider the representation G^* of G as a permutation-group on the set $\{My : y \in G\}$ of right cosets of M in G. x^* is represented by a product of transpositions; the fixed points of x^* are the cosets My with $Myx = My$, i.e., $yxy^{-1} \in M$. If no yxy^{-1} lies in M, then x^* is a product of an *odd* number of transpositions. Therefore the intersection of G^* with the alternating group on $\{My : y \in G\}$ is of index 2 in G^*, contrary to hypothesis.

LEMMA 1 (THOMPSON [10]). *Suppose that T is a Sylow 2-subgroup of a simple group G*; SCN$_3$ (T) *is empty*; *and $T \not\cong D_8$. Then T has at most one normal four-group.*

Proof. Suppose not, and let A, B be distinct normal four-groups of T. $D = \langle A, B\rangle$ is normal in T. If $[A, B] = 1$, then D is a normal E_8 or E_{16} of T; therefore $[A, B] = A \cap B$ is of order 2, and $D \cong D_8$.

T stabilizes the two chains $A > A \cap B > 1$ and $B > A \cap B > 1$, hence stabilizes $D > A \cap B = D' > 1$. So $T = D \circ C_T(D)$; write $C = C_T(D)$. $C_T(D)$ can have no normal four-group R since then RA and RB contain normal E_8's of T. Therefore by Blackburn [3, Theorem 1.1, p. 3], C is cyclic or of maximal class; also, $|C| > 2$ since $T \not\cong D_8$. A 2-group of maximal class contains a cyclic subgroup of index 2 (Blackburn [2, Theorem 3.4, p. 68]), and is therefore dihedral, semidihedral, or generalized quaternion; in any case, $\Phi(C)$ is cyclic. $\Phi(T) = \Phi(CD) = \Phi(C)\Phi(D)$ (since C and D centralize each other) $= \Phi(C)$; therefore, the involution z of $D' = C \cap D$ is the only involution of T which is a square in T.

(i) If t is an involution, other than z, of T, then $C_T(t)$ contains z as a square.

Proof. The involutions of T other than z are:

1. Involutions of D; for $t \in D$, $C_T(t) \supseteq C$ and C contain z as a square.

2. Involutions of C; their centralizers contain D and so contain z as a square.

3. Cross-involutions, namely cd where $c \in C - \langle z\rangle$, $d \in D - \langle z\rangle$, and either $c^2 = d^2 = 1$ or $c^2 = d^2 = z$. If $c^2 = d^2 = z$ then $C_T(cd)$ contains c and d, hence contains z as a square. If $c^2 = d^2 = 1$, then C must be dihedral or semidihedral; write

$$C = \langle y, g : y^2 = 1, g^{2^a} = 1, y^{-1}gy = g^{-1} \text{ respectively } g^{-1+2^{a-1}}\rangle$$

where $a \geqq 3$ since C has no normal four-group. Then $c \in y\langle g\rangle$ if C is dihedral; $c \in y\langle g^2\rangle$ if C is semidihedral. We may alter the choice of notation in C so that $c = y$. Then cd is centralized by $g^{2^{a-2}}f$ where f is an element of order 4 in D (since $d \notin \langle z\rangle$). So $C_T(cd)$ contains z, $g^{2^{a-2}}f$, and d; now $\langle z, g^{2^{a-2}}f\rangle$ is a four-group, and $[g^{2^{a-2}}f, d] = [f, d] = z$; hence $\langle z, g^{2^{a-2}}f, d\rangle \cong D_8$ with $\langle z\rangle$ as derived group and so is square.

(ii) If $t \neq z$ is an involution of T and $C_T(t)$ contains z as a square, then t is not fused to z in G.

Proof. If t is fused to z in G, then there is $h \in G$ such that $t^h = z$ and $C_T(t)^h \subseteq T$ (by Sylow's theorem in $C_G(z)$). $C_T(t)^h$ is a subgroup of T which contains z^h as a square; therefore $z^h = z$; but this contradicts $t^h = z$.

By (i) and (ii), z is not fused in G to any involution of T other than z itself. But then G cannot be simple, by a theorem of Glauberman (Glauberman [7, Theorem 1]; we shall refer to this theorem as "Glauberman's theorem"). This contradiction proves Lemma 1.

Aut $(\boldsymbol{Z}_4\times\boldsymbol{Z}_4)$. Aut $(\boldsymbol{Z}_4\times\boldsymbol{Z}_4)$ is of order $3\cdot 32$ and contains a characteristic subgroup $\mathfrak{B}^+$ which is the set of automorphisms fixing $\Omega_1(\boldsymbol{Z}_4\times\boldsymbol{Z}_4)$ (elementwise) and is also the stability group of the chain $\boldsymbol{Z}_4\times\boldsymbol{Z}_4>\Omega_1(\boldsymbol{Z}_4\times\boldsymbol{Z}_4)>1$. $\mathfrak{B}^+\cong E_{16}$ and Aut $(\boldsymbol{Z}_4\times\boldsymbol{Z}_4)/\mathfrak{B}^+\cong\Sigma_3$. So Aut $(\boldsymbol{Z}_4\times\boldsymbol{Z}_4)$ has a subgroup $\mathfrak{H}$ of order $3\cdot 16$ and index 2 which contains all the Sylow 3-subgroups of Aut $(\boldsymbol{Z}_4\times\boldsymbol{Z}_4)$. These Sylow 3-subgroups are therefore conjugate to each other by elements of $\mathfrak{B}^+$. Therefore all the Sylow 3-subgroups of Aut $(\boldsymbol{Z}_4\times\boldsymbol{Z}_4)$ have the same effect on $\mathfrak{B}^+$ by conjugation. If σ is any 3-automorphism of $\boldsymbol{Z}_4\times\boldsymbol{Z}_4$, then $\mathfrak{B}^+=C_{\mathfrak{B}^+}(\sigma)\times[\mathfrak{B}^+,\sigma]$ where $C_{\mathfrak{B}^+}(\sigma)$ and $[\mathfrak{B}^+,\sigma]$ are both four-groups.

$C_{\mathfrak{B}^+}(\sigma)$ and $[\mathfrak{B}^+,\sigma]$ are characteristic subgroups of Aut $(\boldsymbol{Z}_4\times\boldsymbol{Z}_4)$, so consist of the same matrices (with integers mod 4 as coefficients) no matter what basis is chosen for $\boldsymbol{Z}_4\times\boldsymbol{Z}_4$. These matrices are:

$$C_{\mathfrak{B}^+}(\sigma)\colon \begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}3&0\\0&3\end{pmatrix},\ \begin{pmatrix}1&2\\2&3\end{pmatrix},\ \begin{pmatrix}3&2\\2&1\end{pmatrix}.$$

$$[\mathfrak{B}^+,\sigma]\colon \begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}3&0\\2&3\end{pmatrix},\ \begin{pmatrix}3&2\\0&3\end{pmatrix},\ \begin{pmatrix}1&2\\2&1\end{pmatrix}.$$

We write Z for the automorphism of $\boldsymbol{Z}_4\times\boldsymbol{Z}_4$ which inverts every element.

Aut $(\boldsymbol{Z}_4\times\boldsymbol{Z}_4)$ has three Sylow 2-subgroups, which in matrix form are

$$\left\langle\begin{pmatrix}1&1\\0&1\end{pmatrix},\mathfrak{B}^+\right\rangle,\qquad \left\langle\begin{pmatrix}1&0\\1&1\end{pmatrix},\mathfrak{B}^+\right\rangle,\quad\text{and}\quad \left\langle\begin{pmatrix}0&1\\1&0\end{pmatrix},\mathfrak{B}^+\right\rangle.$$

All three of these Sylow 2-subgroups have the *same* action on $C_{\mathfrak{B}^+}(\sigma)$ (they centralize $Z=\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right)$ and exchange $\left(\begin{smallmatrix}1&2\\2&3\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}3&2\\2&1\end{smallmatrix}\right)$); but they all have *different* actions on $[\mathfrak{B}^+,\sigma]$ (they each centralize a different nonidentity element).

For reference, we compute the action of $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ on $\mathfrak{B}^+$:

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\colon Z\to Z$$

$$\begin{pmatrix}1&2\\0&1\end{pmatrix}\to\begin{pmatrix}1&0\\2&1\end{pmatrix}$$

$$\begin{pmatrix}1&0\\2&1\end{pmatrix}\to\begin{pmatrix}1&2\\0&1\end{pmatrix}$$

$$\begin{pmatrix}1&0\\0&3\end{pmatrix}\to Z\begin{pmatrix}1&0\\0&3\end{pmatrix}=\begin{pmatrix}3&0\\0&1\end{pmatrix}.$$

Thus

$$C_{\mathfrak{B}^+}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \left[\mathfrak{B}^+, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right] = \left\langle Z, \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\right\rangle.$$

3. The case where $[(N_G(T):C_G(T)]$ has odd prime divisors.

THEOREM 1. *Suppose that T is a Sylow 2-subgroup of a simple group G; $\mathrm{SCN}_3\,(T)$ is empty but $\mathrm{SCN}_2\,(T)$ is not empty; and $T \not\cong D_8$. Then (Lemma 1) T has exactly one normal four-group, say W.*

Suppose also that some odd prime divides $[N_G(T):C_G(T)]$.

Then 3 divides $[N_G(T):C_G(T)]$, and one of the following holds:

Case 1.1. $A_G(T)$ contains a subgroup of order 3 which centralizes W. Then $[(N_GT):TC_G(T)]=3$; T is isomorphic to the following group of order 2^7; and G has at most two classes of involutions, represented by z_1 and iv:

$$W = \langle z_1, z_2\rangle$$

$$C_T(W) = \langle W, i, j, k, t, u, v\colon \langle i, j, k\rangle \cong Q_8 \text{ with } z_1 \text{ as square,}$$

$$\text{and } \langle t, u, v\rangle \cong Q_8 \text{ with } z_1z_2 \text{ as square;}$$

$$[i, t] = 1, [j, t] = z_2, [k, t] = z_2;$$

$$[i, u] = z_2, [j, u] = 1, [k, u] = z_2;$$

$$[i, v] = z_2, [j, v] = z_2, [k, v] = 1\rangle.$$

$$T = \langle C_T(W), \tau\colon \tau^2 = 1; z_1^\tau = z_1, z_2^\tau = z_2z_1; \tau \text{ centralizes}$$

$$i, j, \text{and } k; [\hat{t}, \tau] = iz_2, [u, \tau] = jz_2, [v, \tau] = kz_2\rangle.$$

Case 1.2. $A_G(T)$ contains a subgroup of order 3 which acts fixed-point-freely on W. Then either T is a four-group; or else $[N_G(T):TC_G(T)]=3$ or 15, and T is isomorphic to the following special group of order 2^6 with exactly three involutions:

$$A = \langle a\rangle \times \langle b\rangle \cong Z_4 \times Z_4.$$

$$T = \Big\langle A, e, f, h\colon e \text{ has matrix } \begin{pmatrix}3 & 0\\ 2 & 3\end{pmatrix} \text{ on } A$$

$$f \text{ has matrix } \begin{pmatrix}3 & 2\\ 0 & 3\end{pmatrix} \text{ on } A$$

$$h \text{ has matrix } \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix} \text{ on } A$$

$$\text{with respect to the basis } \{a, b\} \text{ of } A;\ e^2 = b^2, f^2 = a^2b^2,$$

$$h^2 = a^2;\ e, f, h \text{ centralizes each other};\ h = e^{-1}f^{-1} = efa^2\Big\rangle.$$

Proof of Theorem 1. By the Schur-Zassenhaus theorem, $N_G(T)=TS$ for some subgroup S of odd order. Then $S/C_S(T)$ acts faithfully on $T/\Phi(T)$. $T/\Phi(T)$ is of rank at most 4 by the four generator theorem. So $S/C_S(T) \hookrightarrow GL_4(2)$ and the only odd prime divisors of $[N_G(T):C_G(T)]$ are $\in \{3, 5, 7\}$.

(i) If θ is an automorphism of T of odd order, θ centralizes every normal Abelian subgroup of T which it normalizes, if and only if θ centralizes W.

Proof. Suppose θ centralizes W; let A be a normal Abelian subgroup of T normalized by θ. A is cyclic or of rank 2. If cyclic, then Aut (A) is a 2-group, so θ centralizes A. If of rank 2, then $\Omega_1(A) \lhd T$, so $\Omega_1(A) = W$ by Lemma 1. If A is not homocyclic, Aut (A) is a 2-group; for, write $A = \langle a\rangle \times \langle b\rangle$ where a is of order 2^r and b of order $2^s < 2^r$. Then $A/\Phi(A)$ is a four-group whose nonidentity elements are $a\Phi(A)$, $ab\Phi(A)$, and $b\Phi(A)$; of these cosets, the first two consist of elements of order 2^r while $b\Phi(A)$ consists of elements of order $\leqq 2^{r-1}$, so the only action Aut (A) can have on $A/\Phi(A)$ is to exchange $a\Phi(A)$ and $ab\Phi(A)$. So [Aut (A): Aut_0 $(A)] \leqq 2$, where Aut_0 (A) is the set of automorphisms of A which act trivially on $A/\Phi(A)$. Aut_0 (A) is a 2-group, so Aut (A) is a 2-group.

So we may assume A is homocyclic of rank 2. Then Aut $(A)/\text{Aut}_0$ $(A) \cong \Sigma_3$, and Aut $(A)/\text{Aut}_0$ (A) induces Σ_3 on each subquotient $\Omega_i(A)/\Omega_{i-1}(A)$, in particular on W. So the only nonidentity odd-order automorphisms of A are of order 3 and they are fixed-point-free on W. Since θ centralizes W, then, θ centralizes A.

Let q be any odd prime divisor of $[N_G(T):C_G(T)]$ and let $Q/C_S(T)$ be a subgroup of $S/C_S(T)$ of order q.

(ii) If Q centralizes W, then $T_1 = [T, Q]$ is a special 2-group.

Proof. Let A be a characteristic Abelian subgroup of T_1. Since T_1 is normal in T, A is normal in T, and Q centralizes A by (i). Also $[T_1, Q] = T_1$. Therefore T_1 is special by a theorem of Thompson (Huppert [9, Satz III. 13.6, p. 352]).

$T_1 \lhd T$, so $\Phi(T_1) \lhd T$; hence if T_1 is special, $|\Phi(T_1)| \leqq 4$. Also $[T_1:\Phi(T_1)] \leqq 16$ by the four generator theorem. If $m =$ rank of $T_1/\Phi(T_1)$, then $m \leqq 4$ but also e divides m, where e is the smallest positive integer such that $2^e - 1$ is divisible by q. $T_1/\Phi(T_1)$ is fixed-point-free under Q.

Suppose $q = 7$. Then Q centralizes W and so T_1 is special by (ii); and m has to be 3. $T_1 \lhd T$ so cannot be elementary of order 8; hence $\Phi(T_1) > 1$. $|\Phi(T_1)| = 2$ or 4 and so Q centralizes $\Phi(T_1)$. Therefore if T_0 is a hyperplane of $\Phi(T_1)$, Q acts on T_1/T_0. But T_1/T_0 is a nonelementary group of order 16, and no such group admits an automorphism of order 7. This contradiction establishes that 7 does not divide $[N_G(T):C_G(T)]$.

Suppose $q = 5$. Then Q centralizes W and so T_1 is special by (ii); and m has to be 4. We observe that $T = T_1$. For in any case, $T = C_T(Q)T_1$; so if $T > T_1$, there is $T_2 > T_1$ such that T_2 admits TQ and $[T_2:T_1] = 2$.

$$\begin{aligned} T_2/\Phi(T_1) &= C_{T_2/\Phi(T_1)}(Q)[T_2/\Phi(T_1), Q] \\ &= C_{T_2/\Phi(T_1)}(Q)T_1/\Phi(T_1). \end{aligned}$$

So $T_2/\Phi(T_1) = \langle t\Phi(T_1), T_1/\Phi(T_1)\rangle$ where $t\Phi(T_1)$ is fixed by Q and $T_1/\Phi(T_1)$ is irreducible under Q, and $t^2 \in \Phi(T_1)$. $[T_1/\Phi(T_1), t]$ is a proper Q-subgroup of

$T_1/\Phi(T_1)$, so is 1. But then $T_2/\Phi(T_1)$ is elementary of rank 5, contradicting the four generator theorem.

Therefore $T=T_1$ is special; $|\Phi(T)|=2$ or 4. If 2, then $T\cong Q_8 \circ Q_8$ or $Q_8 \circ D_8$. $Q_8 \circ Q_8$ admits no automorphism of order 5, so $T\cong Q_8 \circ D_8$; but $Q_8 \circ D_8$ has more than one normal four-group, contrary to Lemma 1.

So $|\Phi(T)|=4$, and $W=\Phi(T)=Z(T)=T'$. W contains all the involutions of T since if $x \in T$ were an involution outside W, then $\langle x, W\rangle$ would be a normal E_8 of T. Therefore by Glauberman's theorem, all the involutions of W must be fused together in G; and so fused in $N_G(T)$ by Burnside's theorem (Huppert [9, Hilfssatz IV.2.5, p. 418]).

So 3 divides $[N_G(T):C_G(T)]$, 7 does not. Now $|GL_4(2)|=2^6\cdot 3^2\cdot 5\cdot 7$; so $S/C_S(T) \hookrightarrow GL_4(2)$ and is of order $3\cdot 5$ or $3^2\cdot 5$. But $GL_4(2)$ contains no subgroups of order $3^2\cdot 5$. For a group of this order must be Abelian by Sylow's theorem. Now a Sylow 3-subgroup of $GL_4(2)$ is of form $\langle\theta\rangle\times\langle\psi\rangle$ where θ has a two-dimensional fixed point set and ψ has no nonzero fixed points; θ cannot be centralized by a 5-element of $GL_4(2)$ since 5-elements have no invariant two-dimensional subspaces.

So $[S:C_S(T)]=15$; and $S/C_S(T)$ contains a subgroup of order 3 which acts fixed-point-freely on W. (This situation will be investigated in greater detail under Case 1.2.)

We now have that 3 must divide $[N_G(T):C_G(T)]$ and that $S/C_S(T)$ is Abelian of order 3, 9, or 15.

Case 1.1. *$S/C_S(T)$ contains a subgroup $Q/C_S(T)$ of order* 3 *which centralizes W.* $T_1=[T, Q]$ is normal in TQ. For $x\in S$, $T_1^x=[T, Q]^x=[T^x, Q^x]=[T, Q]$ (since $S/C_S(T)$ is Abelian$)=T_1$. So $N_G(T)=TS$ normalizes T_1.

(iii) No element of $Z(T)\cap T_1$ can be fused in G to a central element of T which lies outside T_1.

Proof. Fusion within $Z(T)$ is all accomplished in $N_G(T)$ by Burnside's theorem; and $N_G(T)$ cannot conjugate an element of T_1 to an element outside T_1.

T_1 is special, and $m=\text{rank } T_1/\Phi(T_1)$ is 2 or 4.

(iv) If $m=2$ then T cannot be a Sylow 2-subgroup of a simple group G.

Proof. Suppose $m=2$. If T_1 is Abelian then T_1 is a normal four-group of T. $T_1\neq W$ since T_1 is fixed-point-free under Q and W is centralized by Q. But T has only one normal four-group by Lemma 1.

So T_1 is non-Abelian with $[T_1:T_1']=4$. But T_1 is also special, so $T_1'=Z(T_1)$ $=\Phi(T_1)$ is elementary. So if $T_1=\langle x, y\rangle$ (for x and y independent mod $\Phi(T_1)$), then $T_1'=\langle[x, y]\rangle$ so is of order 2. So $|T_1|=8$ and $T_1\cong D_8$ or Q_8. T_1 admits a nontrivial 3-automorphism, so $T_1\cong Q_8$.

The central involution z of T_1 is central in T. By Glauberman's theorem, z is fused in G to some other involution of T. So by (iii), z is fused to a noncentral involution of T.

$[T_1/\langle z\rangle, T]$ is a proper Q-subgroup of $T_1/\langle z\rangle$, so is 1, i.e., T centralizes $T_1/\langle z\rangle$. Therefore $T=C\circ T_1$, where $C=C_T(T_1)$, and $\text{SCN}_3(T)$ empty $\Rightarrow$ $\text{SCN}_3(C)$ empty.

The noncentral involutions of T are of two forms: (1) the noncentral involutions of C (these are centralized by T_1); (2) xy where $x \in C$, $x^2=z$, $y \in T_1 - \langle z \rangle$ (these are centralized by y). So for every noncentral involution t of T, $C_T(t)$ contains z as a square.

Case 1. Every element of SCN (C) is cyclic (i.e., C has no normal four-group). Then C is cyclic or of maximal class (Blackburn [3, Theorem 1.1, p. 3]). If of maximal class, C is dihedral, semidihedral, or generalized quaternion (as in proof of Lemma 1). z is the only involution of T which is a square in T, since $\Phi(T) = \Phi(C)\Phi(T_1) = \Phi(C)$ is cyclic.

Some involution $t \neq z$ of T is fused to z in G; there is $g \in G$ with $t^g = z$ and $C_T(t)^g \subseteq T$. $C_T(t)^g$ must be a subgroup of T which contains $t^g = z$ as a nonsquare and z^g as a square; but then z^g must be z, which contradicts $t^g = z$.

Case 2. Some $B \in$ SCN (C) is not cyclic.

1.2.1. If H is any normal Abelian rank 2 subgroup of C, then z is not a square in H.

Proof. There is $y \in T_1$ with $y^2 = z$. Suppose $h \in H$ has $h^2 = z$. $\langle y, H \rangle$ is a normal Abelian subgroup of $T = C \circ T_1$. But $\langle y, H \rangle$ contains the three involutions of H and also the involution yh; so $\Omega_1(\langle y, H \rangle)$ is of order $\geqq 8$, contradicting SCN$_3$ (T) empty.

$z \in B$, but z is not a square in B (1.2.1). $B = \langle b \rangle \times \langle z \rangle$ where b is of order 2^a $(a \geqq 1)$. $\Omega_1(B) = W$.

If $a = 1$ then $B \in$ SCN $(C) \Rightarrow C = B$ or $C \cong D_8$. If $C = B$ then T has no noncentral involutions, which is impossible because z must be fused in G to a noncentral involution of T. $C \cong D_8$ is impossible by Lemma 1.

If $a \geqq 2$, let $H = \Omega_2(B) = \langle b^{2^{a-2}} \rangle \times \langle z \rangle$.

1.2.2. $B = C_C(H)$.

Proof. Immediate if $a = 2$, since then $H = B \in$ SCN (C).

If $a \geqq 3$ and $C_C(H) > B$, let $C_C(H) \geqq R > B$ where $R \lhd T$ and $[R:B] = 2$; write $R = \langle r, B \rangle$. Then $r^2 \in B$, so r induces (by conjugation) an automorphism of order 2 of B. Therefore $r^{-1}br = bw$ or $b^{-1}w$ for some $w \in W$. But if the latter, then r does not centralize H. So $r^{-1}br = bw$ for some $w \in W$.

$C_B(r) = \langle b^2, W \rangle$; $r^2 \in C_B(r)$. For any integer i,

$$(rb^i)^2 = r^2(bw)^i b^i = r^2 b^{2i} w^i.$$

So we can choose $r \in R - B$ so that $r^2 \in W$.

If there is some $r \in R - B$ with $r^2 = 1$, then $\langle r, W \rangle$ is precisely the set of involutions of R and so is a normal E_8 of T, contradicting SCN$_3$ (T) empty.

So $R - B$ contains no involutions, but there is $r \in R - B$ with $r^2 \in W$ but $r^2 \neq 1$, and $\langle r, H \rangle$ is precisely the set of elements of order $\leqq 4$ in R. So $\langle r, H \rangle \lhd T$. $\langle r, H \rangle$ is Abelian of order 16 and exponent 4 and contains only three involutions, so every involution—including z—of $\langle r, H \rangle$ is a square in $\langle r, H \rangle$, contradictory to 1.2.1.

Since $a \geqq 2$, $\mho^{a-1}(B)$ consists of a single involution $\neq z$. $\mho^{a-1}(B) \lhd T$ and z is central in T; so W is central in T. So T stabilizes the two chains $H > W > 1$ and $T_1 > \langle z \rangle > 1$.

Since the stability groups of these chains are elementary, $\Phi(T) \subseteq C_T(T_1) \cap C_T(H) = C_C(H) = B$ by 1.2.2. Therefore, no involution of $T - B$ is a square in T.

The involutions of B (being just those of W) are central in T. So some involution t of $T - B$ must be fused to z in G; there is $g \in G$ with $t^g = z$ and $C_T(t)^g \subseteq T$. $C_T(t)^g$ must be a subgroup of T which contains $t^g = z$ as a nonsquare and z^g as a square. The only involutions of T which could be squares in T are central, and we have seen that z is fused to no central involution of T other than itself; so $z^g = z$, which contradicts $t^g = z$.

By (iv), $T_1/\Phi(T_1)$ is of rank 4. Since $T_1 \lhd T$, $\Phi(T_1) \neq 1$. The Q-module $V = T_1/\Phi(T_1)$ is fixed-point-free under Q, and its fifteen nonidentity elements fall into five Q-orbits of length 3, each of which (together with 1) constitutes an irreducible Q-submodule of V. Moreover, if V_1, V_2 are any two irreducible Q-submodules of V, with nonidentity elements x_1, y_1, z_1 respectively x_2, y_2, z_2 such that the two sets x_i, y_i, z_i $(i = 1, 2)$ are cycled in the same order by a given generator of $Q/C_S(T)$, then all five irreducible Q-submodules of V are exhibited as columns in the following chart:

$$\text{(v)} \qquad \begin{array}{ccccc} x_1 & x_2 & x_1x_2 & x_1z_2 & x_1y_2 \\ y_1 & y_2 & y_1y_2 & y_1x_2 & y_1z_2 \\ z_1 & z_2 & z_1z_2 & z_1y_2 & z_1x_2. \end{array}$$

Moreover, if we choose a generator $aC_S(T)$ for $Q/C_S(T)$, and choose x_i, y_i, z_i so that $x_i^a = y_i$, $y_i^a = z_i$, $z_i^a = x_i$ $(i = 1, 2)$, then a transforms each element in the chart (v) to the one below it.

$$T = C_T(Q)T_1 \quad \text{and} \quad C_T(Q) \cap T_1 \subseteq \Phi(T_1).$$

(vi) $C_T(V) = T_1$.

Proof. If not, there is R with $T \geqq R > T_1$, $[R:T_1] = 2$, $R = \langle r, T_1 \rangle$ for $r \in C_T(Q)$, and $R \subseteq C_T(V)$. $R/\Phi(T_1)$ contains a central subgroup of index 2 and so is Abelian. $r^2 \in C_T(Q) \cap T_1 \subseteq \Phi(T_1)$, so $R/\Phi(T_1)$ is elementary of rank 5, contradicting the four-generator theorem.

In fact, $C_T(Q) \cap T_1 = \Phi(T_1)$. For if $|\Phi(T_1)| = 2$, then Q centralizes $\Phi(T_1)$ since it normalizes $\Phi(T_1)$; and if $|\Phi(T_1)| = 4$ then $\Phi(T_1) = W$ by Lemma 1, so Q centralizes $\Phi(T_1)$ by hypothesis on Q. Thus $T/\Phi(T_1)$ is a split extension of V by $C_T(Q)/\Phi(T_1)$; and the action of T/T_1 on V is the same as that of $C_T(Q)/\Phi(T_1)$.

So the action of T/T_1 on V centralizes that of $Q/C_S(T)$. Therefore each $t \in T$ permutes the five irreducible Q-submodules of V, and centralizes any which it normalizes.

(vii) If $T > T_1$, then T normalizes exactly one of the irreducible Q-submodules of

V, say $E/\Phi(T_1)$. Moreover, for every $t \in T-T_1$, $E/\Phi(T_1)$ is the only irreducible Q-submodule normalized by t.

Proof. There are five irreducible Q-submodules, so at least one—say V_1—is sent to itself by T. If $t \in T-T_1$ normalized V_1 and also another irreducible Q-submodule V_2, then t would centralize V_1 and V_2, hence would centralize $V_1 \times V_2 = V$, contradicting (vi).

(viii) If U is an irreducible Q-submodule of V, and $U=K/\Phi(T_1)$, then: if $|\Phi(T_1)|=2$, K is $\cong$ either E_8 or Q_8; if $|\Phi(T_1)|=4$, K is $\cong$ either E_{16} or $Q_8 \times Z_2$.

Proof. If $|\Phi(T_1)|=2$, then $|K|=8$. The only Abelian group of order 8 having an elementary quotient admitting a fixed-point-free automorphism of order 3, is E_8; the only non-Abelian one is Q_8.

If $|\Phi(T_1)|=4$, then $\Phi(T_1)=W$. $|K|=16$ and W is central in K, and K/W is a four-group.

If K is Abelian, $K \cong E_{16}$. For K is of exponent at most 4. Now the order of $x \in K$ depends only on xW since W is central and elementary in K. So if there is $x \in K$ of order 4, then (via Q) every coset of W in K (other than W itself) consists of elements of order 4. So $K \cong \mathbf{Z}_4 \times \mathbf{Z}_4$. But the 3-automorphisms of this would not centralize W.

If K is non-Abelian then $K \cong Q_8 \times Z_2$. For $W=\mathbf{Z}(K)$, and K has three maximal subgroups (all Abelian) containing W, which are permuted cyclically by Q and are therefore isomorphic. If they are isomorphic to $\mathbf{Z}_4 \times \mathbf{Z}_2$, we can choose $i, j, k \in K$ which together with W generate these three maximal subgroups, and such that $i^a=j, j^a=k, k^a=i$. $i^2=w \neq 1$, $w \in W$. $j^2=(i^a)^2=(i^2)^a=w^a=w$ since Q centralizes W; similarly $k^2=w$. And also $[i,j]=[j,k]=[k,i]=w$, since (for instance)

$$\begin{aligned} w = (ij)^2 \quad (\text{since } ij \equiv k \mod W) &= i^2[i,j^{-1}]j^2 \\ &= i^2j^2[i,j] \quad \text{since } j^{-1} \equiv j \mod \mathbf{Z}(K) \\ &= ww[i,j] \\ &= [i,j]. \end{aligned}$$

Therefore $\langle i, j, k, w\rangle \cong Q_8$, and $K \cong Q_8 \times Z_2$.

If these three maximal subgroups of K are $\cong E_8$, then we can choose involutions i, j, k of K which together with W generate these three maximal subgroups, and such that $i^a=j$, $j^a=k$, $k^a=i$. Now $ij \equiv k \mod W$, so $(ij)^2=k^2=1$. But since i and j are involutions, $(ij)^2=[i,j]$; so $K=\langle i, j, W\rangle$ is Abelian, contrary to assumption.

(ix) $|\Phi(T_1)|=4$ (and therefore $\Phi(T_1)=W$).

Proof. If $|\Phi(T_1)|=2$, then $E \lhd T \Rightarrow E \cong Q_8$ by (viii). $T_1=E \circ \mathbf{C}_{T_1}(E)$. $\mathbf{C}_{T_1}(E)$ is Q-invariant, so by (viii) is $\cong E_8$ or Q_8; but also $\mathbf{C}_{T_1}(E) \lhd T$, so $\mathbf{C}_{T_1}(E) \cong Q_8$; and $T=T_1$ by (vii). But then $T \cong Q_8 \circ Q_8$, which has normal E_8's.

(x) $E \cong Q_8 \times \mathbf{Z}_2$, and $\mathbf{C}_{T_1}(E)=W=\Phi(T_1)$.

Proof. Since $E \lhd T$, $E \cong Q_8 \times Z_2$ by (viii).

$\mathbf{C}_{T_1}(E) \cap E=\mathbf{Z}(E)=W$. $\mathbf{C}_{T_1}(E)$ is Q-invariant and normal in T, so if $\mathbf{C}_{T_1}(E) > W$ then $T=T_1$ by (vii) and $\mathbf{C}_{T_1}(E) \cong Q_8 \times Z_2$ by (viii).

Suppose the square of $C_{T_1}(E)$ is the same (nonidentity) element of W as the square of E. Then take $x_1, y_1, z_1 \in E$, $x_2, y_2, z_2 \in C_{T_1}(E)$, or order 4 and cyclically permuted by Q; and make the chart (v) using the images in T_1/W of these x_i, y_i, z_i $(i=1, 2)$. Then the first two columns in the chart contain cosets of W which consist of elements of order 4; and the last three columns (the "diagonals") contain cosets of W which consist of involutions. These latter three then come from E_{16}'s of T_1, the first two from $Q_8 \times Z_2$'s (by (viii)). T permutes these three E_{16}'s so must normalize one, contradicting $\mathrm{SCN}_3(T)$ empty.

Therefore the square of $C_{T_1}(E)$ is different from the square of E; so $T=T_1 \cong Q_8 \times Q_8$. But this is impossible by (xi).

(xi) If $T \cong Q_8 \times Q_8$ then T cannot be a Sylow 2-subgroup of a simple group G (Glauberman [7, Corollary 8, p. 419]).

Proof. Write the two Q_8's with generators i, j, k and square z, respectively a, b, c and square x, so that $T=\langle i, j, k\rangle \times \langle a, b, c\rangle$. Then z, x are each the square of twelve elements of T while zx is the square of thirty-six elements of T. So zx is a characteristic involution of T. z, x, and zx are the only involutions of T, so by Glauberman's theorem, zx is conjugate in G to z or x. Hence by Burnside's theorem zx is conjugate in $N_G(T)$ to z or x, but this is impossible since zx is a characteristic involution of T.

(xii) Elements $i, j, k, t, u, v, z_1, z_2 \in T_1$ can be chosen so that:

$W=\langle z_1, z_2\rangle$.

$E=\langle i, j, k, z_2\rangle$ and $\langle i, j, k\rangle$ is a Q_8 with z_1 as square. $i^a=j, j^a=k, k^a=i$.

$\langle t, u, v\rangle$ is a Q_8 with z_1z_2 as square. $t^a=u$, $u^a=v$, $v^a=t$.

$$\begin{array}{lll} [i, t] = 1, & [j, t] = z_2, & [k, t] = z_2. \\ [i, u] = z_2, & [j, u] = 1, & [k, u] = z_2. \\ [i, v] = z_2, & [j, v] = z_2, & [k, v] = 1. \end{array}$$

Proof. By (x), $T_1/W \hookrightarrow$ the stability group of $E > W > 1$. But $T_1/W \cong E_{16} \cong$ the stability group of $E > W > 1$; so T_1/W induces the full stability group. So if z_1 is the square of E and we choose $i, j, k \in E$ so that $\langle i, j, k\rangle$ is a Q_8 and $E=\langle i, j, k\rangle \times \langle z_2\rangle$, then there are elements t, u, v of T_1 such that

$$\begin{array}{lll} i^t = i, & j^t = jz_2, & k^t = kz_2, \\ i^u = iz_2, & j^u = j, & k^u = kz_2, \\ i^v = iz_2, & j^v = jz_2, & k^v = k. \end{array}$$

(These three automorphisms are the nonidentity elements of a four-group in Aut E, namely the subgroup "shearing $\langle i, j, k\rangle$ onto z_2.")

If $i, j, k \in E$ have been chosen so that $i^a=j$, $j^a=k$, and $k^a=i$ (the proof of (viii) shows that they can be so chosen), then the relations

$$[i, t] = 1, \qquad [j, t] = z_2, \qquad [k, t] = z_2$$

become, under conjugation by a,

$$\begin{array}{lll} [j, t^a] = 1, & [k, t^a] = z_2, & [i, t^a] = z_2; \\ [k, t^{a^2}] = 1, & [i, t^{a^2}] = z_2, & [j, t^{a^2}] = z_2. \end{array}$$

Therefore $u \equiv t^a \bmod W$ and $v \equiv t^{a^2} \bmod W$; and since W is central in T_1, we can choose t, u, v acting as above on E so that $t^a = u$, $u^a = v$, $v^a = t$.

$\langle t, u, v, W\rangle / W$ is one of the five irreducible Q-submodules of V. The chart (v) for the submodules $\langle i, j, k, W\rangle / W$ and $\langle t, u, v, W\rangle / W$ is

$$\begin{array}{ccccc} i & t & it & iv & iu \\ j & u & ju & jt & jv \\ k & v & kv & ku & kt. \end{array}$$

(Note that $\{i, j, k\}$ and $\{t, u, v\}$ are "sharper" sets of generators than were assumed in (v), in the sense that Q permutes $\{i, j, k\}$ and $\{t, u, v\}$ themselves, not just their cosets modulo W. This same sharpness with respect to Q holds then for all five columns in the chart.) The inverse image in T_1 of each submodule is isomorphic to E_{16} or $Q_8 \times Z_2$, by (viii).

$\langle t, u, v, W\rangle \cong Q_8 \times Z_2$. For if E_{16}, then by squaring elements in the columns of the chart we see that $\langle t, u, v, W\rangle$ is the *only* E_{16} of the five; thus $\langle t, u, v, W\rangle \lhd T$, contradicting $\mathrm{SCN}_3(T)$ empty.

The square in $\langle t, u, v, W\rangle$ is not $z_1 =$ the square in $\langle i, j, k\rangle$. For if it were, the squares in the five would be: $z_1, z_1, 1, z_2, z_2$ respectively; so again one and only one $\cong E_{16}$ and would be normal in T.

We now show that the square in $\langle t, u, v, W\rangle$ is not z_2 (whereupon it must be z_1z_2, and (xii) is proved).

Suppose the square in $\langle t, u, v, W\rangle$ is z_2. Then $\langle t, u, v\rangle$ centralizes $\langle it, ju, kv\rangle$ (which shears $\langle i, j, k\rangle$ onto z_1z_2 and has square z_1z_2), so $T_1 \cong Q_8 \times Q_8$. $T > T_1$ by (xi). Take new notation in T_1 as follows: let $\langle a, b, c\rangle$, $\langle d, e, f\rangle$ be Q_8's of T_1 with squares x, y respectively, such that

$$T_1 = \langle a, b, c\rangle \times \langle d, e, f\rangle,$$

and the sets a, b, c and d, e, f are cycled in the same order by Q. The chart (v) for these generators is

$$\begin{array}{lccccc} & a & d & ad & af & ae \\ & b & e & be & bd & bf \\ & c & f & cf & ce & cd \\ \text{Squares:} & x & y & xy & xy & xy. \end{array}$$

Now the subgroups $\langle a, b, c, W\rangle$ and $\langle d, e, f, W\rangle$ of T_1 centralize each other, while the subgroups of T_1 corresponding to the last three columns of the chart have centralizer in T_1 equal to W. Therefore T must act separately on the first two and two of the last three; and so $[T:T_1]=2$ (by (vii)), T exchanges $\langle a, b, c, W\rangle$ and $\langle d, e, f, W\rangle$, and therefore W is not central in T. $T=C_T(Q)T_1$ and $C_T(Q)\cap T_1=W$. $|C_T(Q)|=8$ and $C_T(Q)$ is non-Abelian (since W is not central in T), so $C_T(Q)\cong D_8$ and we can take an involution $\tau\in C_T(Q)$ such that $C_T(Q)=\langle W, \tau\rangle$. d, e, f can be chosen so that $a^\tau=d$, $b^\tau=e$, $c^\tau=f$. Then $C_V(\tau)\supseteq\langle ad, be, cf, W\rangle/W$; $C_V(\tau)=E/W$ is of order 4 by (vii), so $E=\langle ad, be, cf, W\rangle$.

We now show that $T-T_1=\tau T_1$ contains eight involutions, all conjugate in T to τ. The involutions of τT_1 are the elements τk where $k\in T_1$ and τ inverts k. V is elementary, so each such k must have $kW\in C_V(\tau)$, and the involutions of τT_1 all lie in $\tau\langle ad, be, cf, W\rangle$.

The involutions of τW are τ and $\tau xy=\tau^x$.

τadW, τbeW, and τcfW are sent to one another by Q, since $\tau\in C_T(Q)$. Also Q normalizes T. If all the involutions of τadW are T-conjugate to τ, then all the involutions of the Q-conjugates of τadW will be T-conjugate to τ (since $\tau\in C_T(Q)$). Hence all the involutions of $\tau\langle ad, be, cf, W\rangle$ will be T-conjugate to τ.

$\tau adW=\{\tau ad, \tau adxy, \tau adx, \tau ady\}$. We compute that:

$$\begin{aligned}(ad)^\tau &= da = ad \quad \text{since } a \text{ centralizes } d.\\ (adxy)^\tau &= adxy.\\ (adx)^\tau &= day;\ (adx)(day) = (ad)(da)xy = 1.\\ (ady)^\tau &= dax;\ (ady)(dax) = 1.\end{aligned}$$

So the involutions of τadW are τadx and τady. Now

$$\begin{aligned}\tau^a &= \tau(\tau a^{-1}\tau)a = \tau d^{-1}a = \tau dya = \tau ady.\\ \tau^{ax} &= (\tau^a)^x = (\tau ady)^x = \tau^x ady = \tau xyady = \tau adx.\end{aligned}$$

So the involutions of τadW are T-conjugate to τ. Hence the involutions of τT_1 are all conjugate to τ in T.

We now show that this T cannot be a Sylow 2-subgroup of a simple group G. The T-conjugacy classes of involutions of T are $\{xy\}$, $\{x, y\}$, and the eight involutions of τT_1. By Glauberman's theorem, xy is fused in G to τ or to x.

Suppose xy is fused to τ; then there is $g\in G$ with $\tau^g=xy$ and $C_T(\tau)^g\subseteq T$. $C_T(\tau)$ is of order $|T|/8=16$, so $|C_{T_1}(\tau)|=8$; $C_{T_1}(\tau)=\langle ad, be, cf, xy\rangle\cong Q_8$. Thus $C_T(\tau)$ contains xy as a square. So $C_T(\tau)^g\subseteq T$ contains $(xy)^g$ as a square. Now $\Phi(T)\subseteq T_1$ and the only involutions of T_1 are x, y and xy; so the only involutions of T which are squares in T, are x, y, and xy. $(xy)^g\neq xy$, so $(xy)^g=x$ or y.

So if τ is fused to xy, then x is fused to xy. So in any case x is fused to xy in G, and there is $g\in G$ with $x^g=xy$ and $C_T(x)^g=T_1^g\subseteq T$. T_1 is the only maximal subgroup of T to contain a central four-group in which every element is a square; so $T_1^g=T_1$. But then $x^g=xy$ is impossible because xy is a characteristic involution of T_1.

(xiii) T_1 is generated by two E_{16}'s; and $[T:T_1]=2$.

Proof. The chart (v) for the generators $\{i, j, k\}$ and $\{t, u, v\}$ is

$$\begin{array}{llllll} & i & t & it & iv & iu \\ & j & u & ju & jt & jv \\ & k & v & kv & ku & kt \\ \text{Squares:} & z_1 & z_1z_2 & z_2 & 1 & 1. \end{array}$$

So by (viii), the last two submodules come from E_{16}'s of T_1. T must act separately on the two sets of submodules other than E/W which come from $Q_8\times Z_2$'s respectively E_{16}'s; so $[T:T_1]=2$ by (vii).

(xiv) $T=T_1C_T(Q)$ where $C_T(Q)\cong D_8$. We can take an involution $\tau\in C_T(Q)-W$ such that

$$\begin{aligned} T = \langle i, j, k, t, u, v, z_1, z_2, \tau \colon & \ i, j, k, t, u, v, z_1, z_2 \\ & \text{satisfy the relations given in (xii);} \\ & z_1^\tau = z_1,\ z_2^\tau = z_1z_2;\ \tau^2 = 1;\ \tau \text{ centralizes } i, j, \text{ and } k; \\ & [t, \tau] = iz_2,\ [u, \tau] = jz_2,\ [v, \tau] = kz_2\rangle. \end{aligned}$$

Proof. $T=T_1C_T(Q)$ and $T_1\cap C_T(Q)=W$; so $|C_T(Q)|=8$. T must conjugate $\langle t, u, v, W\rangle$ to $\langle it, ju, kv, W\rangle$, and hence z_1z_2 to z_2. So $C_T(Q)\cong D_8$ and there is an involution $\tau\in C_T(Q)$ such that $C_T(Q)=\langle W, \tau\rangle$.

By (vii), $C_V(\tau)\supseteq E/W$. The automorphism X induced on V by τ is of order 2, so in the ring of endomorphisms of V, $0=X^2-1=(X-1)^2$, and so

$$\begin{tikzcd} \operatorname{Ker}(X-1) \arrow[r, phantom, "\supseteq"] \arrow[d, equal] & \operatorname{Im}(X-1) \arrow[d, equal] \\ C_V(\tau) & {[V, \tau].} \end{tikzcd}$$

Also Dim Ker $(X-1)+$Dim Im $(X-1)=$Dim $(V)=4$; so $C_V(\tau)=[V, \tau]=E/W$.

Since $\tau\in C_T(Q)$ and τ normalizes E/W, τ centralizes E/W, and so $[i, \tau]$, $[j, \tau]$, and $[k, \tau]$ are all $\in W$. We will now show that $[i, \tau]=[j, \tau]=[k, \tau]=1$. For, writing $[i, \tau]=w\in W$ and conjugating by a, we get

$$w = w^a = [i^a, \tau^a] = [j, \tau],$$

and similarly $w=[k, \tau]$. Now either $ij=k$ or $ij=kz_1$; since $z_1\in Z(T)$, in either case we have $(ij)^\tau=(ij)w$. So

$$(ij)w = (ij)^\tau = i^\tau j^\tau = (iw)(jw) = ijw^2 = ij.$$

Hence $w=1$.

We will now normalize i, j, and k so that $[t, \tau]=iz_2$, $[u, \tau]=jz_2$, $[v, \tau]=kz_2$. Since $E/W=C_V(\tau)=[V, \tau]$, $[t, \tau]=e$ for some $e\in E$. Now $t^2=z_1z_2$; conjugating by τ, we get

$$z_2 = (t^2)^\tau = (t^\tau)^2 = (te)^2 = t^2e^te = z_1z_2e^te.$$

So e must satisfy $e^t e = z_1$. The elements of E satisfying this are $\{iw : w \in W\}$. So $t^\tau = tiw$ for some $w \in W$.

Now i^{-1}, j^{-1}, k^{-1} are carried to one another by a as are i, j, and k, and indeed they satisfy the relations of (xii) with respect to t, u, v, z_1, z_2 just as do i, j, and k. So if necessary we may replace i, j, k by i^{-1}, j^{-1}, k^{-1} to get: $w = 1$ or z_2.

Since $\tau^2 = 1$,

$$\begin{aligned} t = t^{\tau^2} &= (tiw)^\tau = t^\tau i^\tau w^\tau \\ &= (tiw)iw^\tau = tz_1 ww^\tau. \end{aligned}$$

Therefore w must satisfy $ww^\tau = z_1$. So $w = z_2$, and $[t, \tau] = iz_2$. Conjugating by a, we get $[t, \tau]^a = [t^a, \tau^a] = [u, \tau] = jz_2$; and $[v, \tau] = kz_2$.

So the isomorphism type of T is determined.

$\Phi(T) = E$ is of index 8 in T; so $5 \nmid [N_G(T) : C_G(T)]$ since an automorphism of order 5 of T must act faithfully on $T/\Phi(T)$ and 5 does not divide $|GL_3(2)|$. Therefore $[N_G(T) : TC_G(T)] = 3$, as claimed in the statement of Theorem 1.

We will now show that G has at most two classes of involutions, represented by z_1 and iv.

The involutions of T_1 are the nonidentity elements of the two E_{16}'s $X = \langle iv, jt, ku, W\rangle$ and $Y = X^\tau = \langle iu, jv, kt, W\rangle$. The involutions of τT_1 are the elements τr where $r \in T_1$ and τ inverts r. Such r must have $rW \in C_V(\tau) = E/W$, hence $r \in E$; so the involutions of τT_1 lie in τE. The involutions of τW are τ and τz_1. The involutions of $\tau iW = \{\tau i, \tau iz_1, \tau iz_2, \tau iz_1z_2\}$ are τiz_2 and τiz_1z_2; conjugating by a, we find that τjW and τkW likewise contain two involutions each. Hence τT_1 contains eight involutions.

Now $\langle C_{T_1}(\tau), W\rangle/W \subseteq C_V(\tau) = E/W$, hence $C_{T_1}(\tau) \subseteq E$. Computing inside E, we get $C_E(\tau) = \langle i, j, k\rangle$. So $[T_1 : C_{T_1}(\tau)] = 8$, so there are eight T_1-conjugates of τ, all lying in τT_1. Hence all the involutions of τT_1 are T_1-conjugate.

Also, each coset of W in X is a single T_1-conjugacy class of involutions; for $[iv, T_1]$ contains:

$$\begin{aligned} [iv, i] &= [v, i] = z_2, \\ [iv, j] &= [i, j][v, j] = z_1z_2, \\ [iv, k] &= [i, k][v, k] = z_1. \end{aligned}$$

Hence $[iv, T_1] = W$. Conjugating by a, we get $[jt, T_1] = W$ and $[ku, T_1] = W$. So $X - W$ is a single class under T_1Q. Since $X^\tau = Y$, $(X - W) \cup (Y - W)$ is a single class under TQ.

So there are four classes of involutions of T under conjugation by TQ, namely $\{z_1\}$; $\{z_2, z_1z_2\}$; the involutions of τT_1; and $(X - W) \cup (Y - W)$. In particular, X and Y are the *only* E_{16}'s of T. Also, $\Phi(T) = E$, so the only involutions which are squares in T are the involutions of W.

(xv) If τ and z_1 are fused in G, then z_2 and z_1 are fused in G.

Proof. Suppose τ is G-conjugate to z_1. $C_T(\tau)=\langle\tau, i, j, k\rangle$, so z_1 is a square in $C_T(\tau)$. So if T^* is a Sylow 2-subgroup of $C_G(\tau)$ (and hence of G) with $T^*\supseteq C_T(\tau)$, then z_1 is a square in T^*, so $z_1\in W^*$. Also $\tau\in W^*$. So W^* contains two different G-conjugates of the central involution τ of T^*.

(xvi) τ and z_1 are fused in G (whereupon by (xv), G has at most two classes of involutions, represented by z_1 and iv).

Proof. τ is fused to some element of T_1, by Lemma A. If τ is not fused to z_1, then one of the following holds:

(xvi.i) τ is fused to z_2, and z_1 is not fused to z_2 or τ.

(xvi.ii) τ is not fused to z_2 but is fused to $iv\in X$, and z_1 is not fused to iv, and z_2 is not fused to iv.

If (xvi.ii) holds, then $C_T(iv)=X$ and $C_T(\tau)=(\langle i, j, k\rangle\times\langle\tau\rangle)^g$ are both Sylow 2-subgroups of $C_G(iv)$ (where $\tau^g=iv$). But this contradicts Sylow's theorem in $C_G(iv)$ since $X\not\cong Q_8\times Z_2$.

Therefore (xvi.i) holds. z_1 is fused to some involution of T other than itself, by Glauberman's theorem; therefore z_1 is fused to iv.

Now T_1, $Q\subseteq N_G(X)$ and T_1 is a Sylow 2-subgroup of $N_G(X)$. $C_{T_1}(X)=X$ and $A_{T_1Q}(X)\cong\Sigma_4^+$. We will show that $A_G(X)$ is transitive on the nonidentity elements of X, which contradicts (xvi.i) and so proves (xvi). We already have that $X-W$ is a single class under T_1Q.

Since z_1 is fused to iv, there is a Sylow 2-subgroup T^* of G in which iv is the central involution, such that $T^*\supseteq X=C_T(iv)$. T_1^* is then a Sylow 2-subgroup of $N_G(X)$ (since T_1^* is the normalizer in T^* of both of the E_{16}'s of T^*), and there is $y\in N_G(X)$ with $(T_1^*)^y=T_1$. Then $(W^*)^y=W$, so $(iv)^y\in W$. So the set $(X-W)\cup\{(iv)^y\}$ is part of an orbit of $A_G(X)$ on the nonidentity elements of X. No orbit of $A_G(X)$ can have size 13 since 13 does not divide $|GL_4(2)|$. So if $A_G(X)$ is not transitive, it must have two orbits of sizes 14 and 1, the orbit of size 1 being $\subseteq W$; call this orbit $\{z\}$.

If this occurs, we observe that $A_G(X)$ is faithfully represented on $X/\langle z\rangle$, i.e., $A_G(X)$ intersects the stability group L of the chain $X>\langle z\rangle>1$ trivially. For $A_G(X)\cap L\lhd A_G(X)$; and since $A_{T_1}(X)$ is a Sylow 2-subgroup of $A_G(X)$ and $[X, T_1]$ is all of W, $A_G(X)\cap L$ has order 2 (if nontrivial). Then $A_G(X)/A_G(X)\cap L$ has order twice an odd number, so has a normal 2-complement $N_1/A_G(X)\cap L$; N_1 has order twice an odd number so has a normal 2-complement N. N is then a normal 2-complement in $A_G(X)$. But $A_G(X)$ contains $A_{T_1Q}(X)$ which does *not* have a normal 2-complement; so $A_G(X)$ cannot have a normal 2-complement.

So $A_G(X)$ has a faithful representation in $GL_3(2)$, whose order is $2^3\cdot 3\cdot 7$. Moreover, $|A_G(X)|$ is 12 times an odd number and is divisible by 14, so is $12\cdot 7$; but this is impossible since $GL_3(2)$ has no subgroups of index 2.

Case 1.2. *$S/C_S(T)$ contains a subgroup $Q/C_S(T)$ of order* 3 *which acts fixed-point-freely on W.* Then $W=\Omega_1(Z(T))$.

Let A be a subgroup of T with $A\supseteq W$, A Abelian, $A\lhd TQ$, and A maximal subject to these conditions. A is of rank 2 and is homocyclic (for we have seen in the proof of (i) in Case 1.1 that a nonhomocyclic group would not admit an automorphism of order 3).

If $A=W$, then $T=W$ (so that T is a four-group). For suppose $T>A=W$. TQ acts on T/W and preserves $\Omega_1(Z(T/W))=Z/W$ say; moreover, T acts trivially on Z/W, so the TQ-invariant subgroups of Z/W are just the Q-invariant subgroups. Suppose $C_{Z/W}(Q)>1$. Then there is a TQ-invariant subgroup L of T with $Z\geqq L>W$, and $[L\colon W]=2$. But W is central in T, so L is Abelian, which contradicts the maximality of $A=W$. Therefore Z/W is fixed-point-free under Q and is a direct product of irreducible Q-modules, each of which is a four-group. Let K/W be one of these irreducible Q-modules; then W is central in K, and Q acts fixed-point-freely on W and on K/W. We now show (Lemma 2) that K is Abelian, which again contradicts the maximality of $A=W$.

Lemma 2. *Let K be a group of order 16, with a central four-subgroup W, such that K admits an automorphism σ of order 3 which preserves W and acts fixed-point-freely on W and on K/W. Then $K\cong E_{16}$ or $Z_4\times Z_4$.*

Proof. Let $k\in K$, $k\notin W$. kW, $(kW)^\sigma$, and $(kW)^{\sigma^2}$ are the three nonidentity cosets of W in K. $k^2\in W$, and since W is elementary and central, $(kW)^2=k^2$.

If $k^2=1$, then $(kW)^2=((kW)^\sigma)^2=((kW)^{\sigma^2})^2=1$, and so K is of exponent 2 and hence elementary Abelian.

If $k^2=w\neq 1$, then $(kW)^2=w$; $((kW)^\sigma)^2=w^\sigma$; and $((kW)^{\sigma^2})^2=w^{\sigma^2}$. So each element of W is a square in K.

Now $K=\langle k, k^\sigma, W\rangle$; and

$$[k, k^\sigma] = k^{-1}(k^\sigma)^{-1}kk^\sigma = kwk^\sigma w^\sigma kk^\sigma = ww^\sigma(kk^\sigma)^2.$$

But $kk^\sigma\equiv k^{\sigma^2} \bmod W$, so $(kk^\sigma)^2=w^{\sigma^2}$; so

$$[k, k^\sigma] = ww^\sigma w^{\sigma^2} = 1.$$

So K is Abelian of exponent 4 and every involution is a square; hence $K\cong Z_4\times Z_4$.

If $T=A$ then G cannot be simple unless T is a four-group, by a result of R. Brauer [4, Theorem 1, p. 317].

Thus if T is not a four-group, $T>A>W$. Let $B=\Omega_2(A)$; $B\cong Z_4\times Z_4$.

(xvii) $A=C_T(B)$.

Proof. $C_T(B)$ is Q-invariant. Also $C_T(B)$ is metacyclic (Alperin [1, Corollary, p. 110]) and the only metacyclic 2-group admitting an automorphism of order 3 which acts on W as Q does, is Abelian (since otherwise its derived group is cyclic and Q-invariant) and homocyclic; so $C_T(B)=A$ by maximality of A.

Therefore $T/A \hookrightarrow \operatorname{Aut} B$; since T centralizes W, $T/A \to \mathfrak{B}^+$ (see Chapter II). T/A is Q-invariant, so the image of T/A in $\mathfrak{B}^+$ either contains $[\mathfrak{B}^+, \sigma]$ or else is contained in $C_{\mathfrak{B}^+}(\sigma)$ (where σ is any 3-automorphism of B).

We now show that A must be of exponent 4.

(xviii) If A is of exponent 2^r for $r \geqq 3$, then the subgroup of $\mathfrak{B}^+$ induced on B by T/A does not contain $[\mathfrak{B}^+, \sigma]$ (and hence lies in $C_{\mathfrak{B}^+}(\sigma)$).

Proof. Suppose the contrary, and let T_1 be the inverse image in T of $[\mathfrak{B}^+, \sigma]$; T_1 is fixed-point-free under Q since A and T_1/A are.

If $T_1 - A$ has no involutions then T_1 is of exponent 4 by a result of G. Higman [8], which contradicts our assumption regarding A.

So T_1 contains an involution t, $t \notin A$. Let ρ be a generator for $A_Q(T)$; since ρ is fixed-point-free on T_1,

$$tt^{\rho}t^{\rho^2} = 1, \qquad tt^{\rho^2}t^{\rho} = 1$$

and therefore t^{ρ} commutes with t^{ρ^2}; hence also $[t^{\rho^2}, t] = 1$ and $[t, t^{\rho}] = 1$, so t, t^{ρ}, and t^{ρ^2} all centralize each other. $tt^{\rho}t^{\rho^2}$ is fixed by ρ, so must equal 1. Also $1, t, t^{\rho}, t^{\rho^2}$ form a complete set of coset representatives for A in T_1. So they constitute a four-group V which is a Q-complement to A in T_1.

Choose a basis for A, and take the 2^{r-2}th powers of the members of this basis as a basis for B. We can then write matrices for automorphisms of A and B.

$[\mathfrak{B}^+, \sigma]$ contains the matrix $\left(\begin{smallmatrix}1 & 2\\ 2 & 1\end{smallmatrix}\right)$, so there is $v \in V$ such that v induces $\left(\begin{smallmatrix}1 & 2\\ 2 & 1\end{smallmatrix}\right)$ on B. If $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ is the matrix of v on A, we have

$$(*) \qquad \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \equiv \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix} \mod 4.$$

Since $v^2 = 1$, we also have

$$(**) \qquad \begin{pmatrix}\alpha^2+\beta\gamma & \beta(\alpha+\delta)\\ \gamma(\alpha+\delta) & \beta\gamma+\delta^2\end{pmatrix} = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}^2 \equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \mod 2^r.$$

β and γ are each twice an odd number by (*), so $(\alpha+\delta)$ is a multiple of 2^{r-1} by (**). Also $\alpha^2 = \delta^2$ by (**), i.e. $(\alpha\delta^{-1})^2 = 1$. ($\alpha$ and δ are odd and therefore invertible mod 2^r.) Therefore $\alpha\delta^{-1} = \pm 1 + i2^{r-1}$ for $i = 0$ or 1; i.e.,

$$\alpha = \delta(\pm 1 + i2^{r-1}).$$

Therefore $\alpha+\delta = \delta(\pm 1 + 1 + i2^{r-1})$ is $\equiv 0 \mod 2^{r-1}$, so -1 must occur, i.e. $\alpha = -\delta + i2^{r-1}$. But then $\alpha \equiv -\delta \mod 4$, whereas (*) implies that $\alpha \equiv \delta \mod 4$. This contradiction establishes (xviii).

(xix) If A is of exponent 2^r for $r \geqq 3$, then $[T:A] = 2$, and for suitable choice of basis in A,

$$T = \left\langle A, t \colon t^2 = 1 \text{ and the matrix of } t \text{ on } A \text{ is } \begin{pmatrix}-1+i2^{r-1} & j2^{r-1}\\ j2^{r-1} & -1+(i+j)2^{r-1}\end{pmatrix}\right\rangle$$

for some $i, j = 0$ or 1.

Proof. By (xviii), the subgroup of $\mathfrak{B}^+$ induced on B by T/A lies in $C_{\mathfrak{B}^+}(\sigma)$, and so $[T, Q] = A$. $T = [T, Q]C_T(Q)$ splits T over A, with $C_T(Q)$ elementary of order 2 or 4.

All the elements of order 3 in Aut (A) are conjugate in Aut (A). So if ρ is a chosen generator for $A_Q(T)$, we can take any 3-matrix we like to represent the action of ρ on A, by choosing basis suitably in A. Choose the matrix $\left(\begin{smallmatrix}0&1\\-1&-1\end{smallmatrix}\right)$ for ρ. Then the automorphisms of A induced by elements of $C_T(Q)$ have matrices $\left(\begin{smallmatrix}\alpha&\beta\\\gamma&\delta\end{smallmatrix}\right)$ which must centralize $\left(\begin{smallmatrix}0&1\\-1&-1\end{smallmatrix}\right)$—this is equivalent to $\delta=\alpha-\beta$ and $\gamma=-\beta$.

Since $C_T(Q)$ is elementary, we must have (mod 2^r)

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\equiv\begin{pmatrix}\alpha&\beta\\-\beta&\alpha-\beta\end{pmatrix}^2=\begin{pmatrix}\alpha^2-\beta^2&2\alpha\beta-\beta^2\\-2\alpha\beta+\beta^2&\alpha^2-2\alpha\beta\end{pmatrix}$$

or equivalently

$$\alpha^2-\beta^2\equiv 1 \mod 2^r, \qquad 2\alpha\beta\equiv\beta^2 \mod 2^r.$$

β cannot be odd. For if it were, we could cancel it in $2\alpha\beta\equiv\beta^2$, getting $2\alpha\equiv\beta$, so β is even.

So β is even; then α must be odd since $\left(\begin{smallmatrix}\alpha&\beta\\-\beta&\alpha-\beta\end{smallmatrix}\right)$ is nonsingular. Since $2\alpha\beta\equiv\beta^2$, either β is twice an odd number or $2\alpha\beta\equiv\beta^2\equiv 0 \mod 2^r$.

If β is twice an odd number—say $\beta=2\beta_0$ for odd β_0—the equation $2\alpha\beta\equiv\beta^2 \mod 2^r$ becomes

$$\begin{aligned}2\alpha 2\beta_0 &\equiv 4\beta_0^2 \mod 2^r\\ \Leftrightarrow 4\alpha &\equiv 4\beta_0 \mod 2^r\\ \Leftrightarrow \beta_0 &\equiv \alpha+k2^{r-2} \quad \text{for some integer } k.\end{aligned}$$

Then the equation $\alpha^2-\beta^2\equiv 1 \mod 2^r$ becomes

$$\alpha^2-(2\alpha+k2^{r-1})^2\equiv 1 \mod 2^r \Leftrightarrow -3\alpha^2\equiv 1 \mod 2^r.$$

In particular, $-3\alpha^2\equiv 1 \mod 8$. But this is impossible since the square of any odd number is $\equiv 1 \mod 8$.

So $2\alpha\beta\equiv\beta^2\equiv 0 \mod 2^r$. Therefore $\beta=j2^{r-1}$ ($j=0$ or 1). $\alpha^2-\beta^2\equiv 1 \mod 2^r$ becomes $\alpha^2\equiv 1 \mod 2^r$, so $\alpha=\pm 1+i2^{r-1}$ ($i=0$ or 1). If $\alpha=1+i2^{r-1}$ then $\left(\begin{smallmatrix}\alpha&\beta\\-\beta&\alpha-\beta\end{smallmatrix}\right)$ centralizes B, which contradicts $A=C_T(B)$. So $\alpha=-1+i2^{r-1}$ and the matrix $\left(\begin{smallmatrix}\alpha&\beta\\-\beta&\alpha-\beta\end{smallmatrix}\right)$ is as claimed in (xix).

Thus there is only one nonidentity automorphism of B—namely inversion—which can be induced by $C_T(Q)$. Since $T>A$ and $C_T(Q)$ is faithful on B, the proof of (xix) is complete.

(xx) If A is of exponent 2^r for $r\geqq 3$, then every $F\cong E_8$, $F\subseteq T$ has $N_T(F)=\langle F, B\rangle$.

Proof. Since $[T:A]=2$, $[F:F\cap A]=2$ and $F\cap A=W$. $F=\langle f, W\rangle$ for some involution f outside A; f induces the matrix given in (xix) on A.

$N_T(F)=\langle f\rangle N_A(F)$ since $T=\langle f\rangle A$. We compute $N_A(F)$. If $\{a, b\}$ is our chosen basis for A, then $a^{2^{r-2}}$ and $b^{2^{r-2}}$ normalize F since f inverts them. But

$$\begin{aligned}[a^{2^{r-3}}, f] &= a^{-2^{r-3}}(a^{2^{r-3}})^f\\ &= a^{-2^{r-3}}(a^{-1}w)^{2^{r-3}} \quad \text{for some } w\in W\\ &= a^{-2^{r-2}}w^{2^{r-3}}\notin F.\end{aligned}$$

Also $[b^{2^{r-3}}, f] \notin F$ and $[(ab)^{2^{r-3}}, f] \notin F$. So $N_A(F) = B$.

Now consider the particular four-group $F = \langle t, W\rangle$ where $C_T(Q) = \langle t\rangle$. By (xx), the Sylow 2-subgroups of $A_G(F)$ are four-groups. F admits BQ and so $|A_G(F)|$ is at least 12. Since $|GL_3(2)| = 2^3 \cdot 3 \cdot 7$, $|A_G(F)|$ is either $2^2 \cdot 3$ or $2^2 \cdot 3 \cdot 7$; the latter is impossible since $GL_3(2)$ has no subgroups of index 2. So $A_G(F) = A_{TQ}(F)$ is of order 12 with a normal four-group, namely, the stability group of the chain $F > W > 1$.

t is fused in G to an element of A—hence of $W = \Omega_1(Z(T))$—by Lemma A. Let T^* be a Sylow 2-subgroup of $C_G(t)$ (and so of G) which contains F. $N_{T^*}(F) = \langle F, B^*\rangle$ by (xx). So $N_{T^*}(F)$ induces a four-group on F, and a different four-group from that induced by $N_T(F)$ (since $t \in W^*$, $t \notin W$). But then $A_G(F) > A_{TQ}(F)$.

This contradiction establishes that A is of exponent 4. $A = \Omega_2(A) = C_T(A)$ by (xvii), and $T/A \hookrightarrow \operatorname{Aut}(A)$.

(xxi) The subgroup of $\mathfrak{B}^+$ induced on A by T/A is not contained in $C_{\mathfrak{B}^+}(\sigma)$ (and hence contains $[\mathfrak{B}^+, \sigma]$).

Proof. Suppose the contrary; then $[T, Q] = A$. $T = [T, Q]C_T(Q) = AC_T(Q)$ splits T over A, with $C_T(Q)$ elementary of order 2 or 4.

We will show that $\Phi(T) = W$ by showing that all squares of elements of T lie in W (Lemma FB of §1). For a typical element of T is cx for $c \in C_T(Q)$, $x \in A$; and

$$(cx)^2 = cxcx = ccx[x, c]x = c^2x^2[x, c]^x \in W$$

since c stabilizes the chain $A > W > 1$ and so $[x, c] \in W$, and also $c^2 = 1$ and $x^2 \in W$.

Therefore if c is an involution of $C_T(Q)$, $\langle c, W\rangle$ is a normal E_8 of T, contradicting $\mathrm{SCN}_3(T)$ empty.

By (xxi), $A_T(A) \supseteq [\mathfrak{B}^+, \sigma]$. $Q/C_S(T)$ acts fixed-point-freely on the four-group of T/A corresponding to $[\mathfrak{B}^+, \sigma]$, and induces an automorphism of order 3 on the inverse image in T of this four-group.

LEMMA 3. *Let σ be a fixed but arbitrary 3-automorphism of $A \cong \mathbf{Z}_4 \times \mathbf{Z}_4$. Let R be an extension of A by $[\mathfrak{B}^+, \sigma]$ such that σ extends to an automorphism of order 3 of R which is fixed-point-free on R/A. Then $\Phi(R) = W$, and R is of one of two isomorphism types.*

In detail, if a basis $\{a, b\}$ is chosen for A, these two isomorphism types can be described most simply as extensions of A:

Split case. $R = \langle A, e, f, h$: e induces $\left(\begin{smallmatrix}3&0\\2&3\end{smallmatrix}\right)$ on A (i.e., $a^e = a^3$ and $b^e = a^2b^3$), f induces $\left(\begin{smallmatrix}3&2\\0&3\end{smallmatrix}\right)$ on A, h induces $\left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$ on A; e, f, h are all involutions and $ef = h$ (so that R is the semidirect product of A and $\langle e, f, h\rangle\rangle$.

If σ is taken to have the matrix $\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)$ on A, then e, f, h can be chosen so that $e^\sigma = f$, $f^\sigma = h$, and $h^\sigma = e$.

G. Higman case. $R = \langle A, e, f, h$: e, f, h induce $\left(\begin{smallmatrix}3&0\\2&3\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}3&2\\0&3\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$ respectively on A; $e^2 = b^2$, $f^2 = a^2b^2$, $h^2 = a^2$; e, f, h commute with one another and represent the three nonidentity cosets of W in the group $\langle e, f, h\rangle$, which is isomorphic to $\mathbf{Z}_4 \times \mathbf{Z}_4$;

if σ is taken to have the matrix $\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)$ on A, then e, f, h can be chosen so that $e^\sigma=f$, $f^\sigma=h$, $h^\sigma=e$, and $h=e^{-1}f^{-1}=efa^2\rangle$.

Note. It is clear that R must be of the same isomorphism types no matter which 3-matrix we take for σ, since all 3-automorphisms of A are conjugate in Aut (A) and so this is a matter of choice of basis in A.

Proof. We have seen in §2 that the matrices of $[\mathfrak{B}^+, \sigma]$ are the same for any choice of basis in A, and are $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}3&0\\2&3\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}3&2\\0&3\end{smallmatrix}\right)$, and $\left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$.

Take $e \in R$ such that eA induces $\left(\begin{smallmatrix}3&0\\2&3\end{smallmatrix}\right)$ on A (with respect to a basis $\{a, b\}$ of A such that σ has the matrix $\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)$). Then $(eA)^\sigma$ induces $\left(\begin{smallmatrix}3&0\\2&3\end{smallmatrix}\right)^\sigma=\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix}3&0\\2&3\end{smallmatrix}\right)\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)=\left(\begin{smallmatrix}3&2\\0&3\end{smallmatrix}\right)$ on A, and $(eA)^{\sigma^2}$ induces $\left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$ on A. So for any $f \in (eA)^\sigma$ and $h \in (eA)^{\sigma^2}$, f induces $\left(\begin{smallmatrix}3&2\\0&3\end{smallmatrix}\right)$ on A, h induces $\left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$ on A, and e, f, h represent the nonidentity cosets of A in R.

The following information will be useful (now and later):

	$\begin{pmatrix}3&0\\2&3\end{pmatrix}$	$\begin{pmatrix}3&2\\0&3\end{pmatrix}$	$\begin{pmatrix}1&2\\2&1\end{pmatrix}$
Fixed points $\in A$	W	W	W
Coboundaries $\in A$	$\langle a^2\rangle$	$\langle b^2\rangle$	$\langle a^2b^2\rangle$
Elements of order 4 in A which are inverted	aW	bW	abW

We now observe that $R^2=W$ (whence $\Phi(R)=W$ by Lemma FB of §1). For $A^2=W$. $R^2 \subseteq A$; and each element of R which lies in a nonidentity coset of A induces (by conjugation) an automorphism of A whose fixed point set is just W; the square of such an element must lie in W.

$R/W \cong E_{16}$, and is fixed-point-free under σ since R/A and A/W are.

Consider the coset eA. By the coboundary data, $(eA)^2 \subseteq W$ is either $\{1, a^2\}$ or $\{b^2, a^2b^2\}$. We can choose the coset representative e so that $e^2=1$ or b^2 respectively. The element eW of R/W belongs to some irreducible σ-submodule L/W of R/W, with $|L|=16$ and $R/W=(L/W)\times(A/W)$. We can choose f and h so that $f \equiv e^\sigma$ mod W and $h \equiv f^\sigma$ mod W. Then e, f, and h represent the nonidentity cosets of W in L (as well as of A in R). Moreover, $(eW)^2=e^2$ (since W is elementary and central); therefore $f^2=(fW)^2=((eW)^\sigma)^2=(e^2)^\sigma$, and $h^2=(e^2)^{\sigma^2}$. So e^2, f^2, and h^2 are either all 1 or are b^2, a^2b^2, and a^2 respectively.

Each element of R can be written in exactly one way as $e^\alpha f^\beta a^\gamma b^\delta w$, for α, β, γ, δ each equal to 0 or 1, and $w \in W$. The isomorphism type of R is determined once we know how to multiply two elements of this form and get a third element of this form. We will know this once we know the commutator relations between e, f, a, and b, and the squares ($\in W$) of e, f, a, and b. The hypotheses of Lemma 3, and our choices of e, f, and h, give us all of this information except $[e, f]$. But $L=\langle e, f, W\rangle$ satisfies the hypotheses of Lemma 2; so $L \cong E_{16}$ or $Z_4 \times Z_4$, and $[e, f]=1$ in either case.

So R has two possible isomorphism types, corresponding in our notation to $e^2=1$ and $e^2=b^2$. (They differ since one contains involutions outside W and the other does not.)

If $L \cong E_{16}$ and we take $f=e^\sigma$ and $h=f^\sigma$, then $\{1, e, f, h\}$ is an irreducible σ-submodule of L, hence a four-group, and the split case of Lemma 3 holds. ($h^\sigma=e$ since $\sigma^3=1$.)

If $L \cong Z_4 \times Z_4$ (i.e., $e^2=b^2$), then $\{e,f\}$ is a basis for L. We can in fact choose notation in L so that $e^\sigma=f, f^\sigma=h$, and $h=e^{-1}f^{-1}=efa^2$. For, all we know so far about the action of σ on L is its action on W and on $L/W=\{W, eW, fW, hW\}$; now Aut (L) has exactly four 3-elements which act as σ does on W and L/W, and they can all be obtained from each other by changes of basis in L corresponding to similarity transformations $\Delta \in$ the stability group of the chain $L>W>1$. So if we take $\{e,f\}$ as a basis for L, then for each 3-matrix M acting as prescribed on W and L/W, there will be a basis $\{ew_1, fw_2\}$ of L (for some $w_1, w_2 \in W$) with respect to which σ has the matrix M; $\{ew_1, fw_2\}$ is the image of $\{e,f\}$ under some Δ. Since $\{ew_1, fw_2\} \equiv \{e,f\}$ mod W, the elements ew_1, fw_2, a, b satisfy the same commutator-relations and have the same squares as e, f, a, b.

So far, we have specified e, f, and h only up to congruence mod W; we now choose them specifically so that σ has the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 3 & 3 \end{smallmatrix}\right)$ with respect to $\{e,f\}$. (This matrix acts as prescribed on W and L/W.) Then $e^\sigma=f, f^\sigma=h$, and $h=f^\sigma=e^{-1}f^{-1}=efa^2$; and the G. Higman case of Lemma 3 holds.

Write R/A for the subgroup of T/A corresponding to $[\mathfrak{B}^+, \sigma]$; R is then of one of the two isomorphism types named in Lemma 3.

(xxii) If $T=R$ then T is of G. Higman type.

Proof. The split R has normal E_8's.

We will now show that T must be R.

Assume $T>R$. Then $T=C_T(Q)[T, Q]=C_T(Q)R$ splits T over R. For any nonidentity $c \in C_T(Q)$, $\langle R, c\rangle$ is a subgroup of T containing R with index 2. Now $R/\Phi(R)$ is of rank 4; so by the four-generator theorem, $\Phi(\langle R, c\rangle)$ must be properly larger than $\Phi(R)=W$. $\Phi(T) \subseteq A$; so the only way this can happen is for $[c, r]$ (for some $r \in R$) to be an element of order 4 in A. Then $[R, c] \cap A>W$, and $[R, c]$ is Q-invariant; so $[R, c]=A$.

Since $c^2=1$, $1=[c^2, r]=[c, r]^c[c, r]$, so c must invert $[c, r]$. Now the automorphisms $\left(\begin{smallmatrix} 3 & 2 \\ 2 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 2 \\ 2 & 3 \end{smallmatrix}\right) \in C_{\mathfrak{B}^+}(\sigma)$ do not invert any of the elements of order 4 in A. So no c can occur which induces either of these automorphisms on A.

So if $T>R$, then $T=\langle R, z\rangle$ where z inverts A, $z^2=1$, and $[R, z]=A$. For either of the two R named in Lemma 3, the only way to have $[R, z]=A$ is for the commutators $[e, z]$, $[f, z]$, $[h, z]$ to be elements of order 4 in A.

We may assume a basis in A has been chosen so that some generator σ of $Q/C_S(T)$ has matrix $\left(\begin{smallmatrix} 0 & 1 \\ 3 & 3 \end{smallmatrix}\right)$ on A, and $e^\sigma=f, f^\sigma=h, h^\sigma=e$ as in Lemma 3. Then the commutators $[e, z]$, $[f, z]$, and $[h, z]$ are carried into one another by Q, and represent the three nonidentity cosets of W in A.

The only involutions $\in zR$ are those of zA. For if $k=e, f$, or h, and $x \in A$, then

$$(zkx)^2 = zkx\,zkx = k[k, z]x^{-1}kx \equiv k[k, z]k \mod W.$$

$[k, z] \in A-W$, so $k[k, z]k \in A-W$; so $(zkx)^2 \neq 1$. Therefore, every involution of zR lies in one of the four T-conjugate E_8's $\langle z, W\rangle$, $\langle z^e, W\rangle$, $\langle z^f, W\rangle$, and $\langle z^h, W\rangle$.

Also, $C_T(Z)=\langle z, C_R(z)\rangle$; but z^k is A-conjugate to each element of z^kW for each $k=e, f, h$, or 1, and z is conjugate to each z^k; so $[R:C_R(z)]=4\cdot 4=16$, hence $|C_R(z)|=4$, and $C_T(z)=\langle z, W\rangle$. Hence the involutions of zR form a single T-conjugacy class and the centralizer in T of any one of them is $\cong E_8$.

Also, $N_T(\langle z, W\rangle)=\langle z, N_R(\langle z, W\rangle)\rangle$. A normalizes $\langle z, W\rangle$, and induces the stability group of $\langle z, W\rangle > W > 1$. If $N_R(\langle z, W\rangle) > A$, then $k \in N_R(\langle z, W\rangle)$ for $k=e, f$, or h; but $[z, k] \notin W$; so $N_R(\langle z, W\rangle)=A$. Hence each of the four T-conjugates F of $\langle z, W\rangle$ has $N_T(F)=\langle F, A\rangle$, and A induces the stability group of $F > W > 1$.

Suppose R is of G. Higman type. Then these four E_8's are the only E_8's of T, since R contains no involutions outside W. So each E_8 F of T has $|A_G(F)|$ divisible by 2 to the second power only, and $A_T(F)$ is the stability group of the chain $F > W > 1$.

Take $F=\langle z, W\rangle$; then TQ normalizes F, so $|A_G(F)|=12$ or $12\cdot 7$ (since $|GL_3(2)| = 2^3\cdot 3\cdot 7$). But $12\cdot 7$ is impossible since $\mathrm{GL}_3(2)$ has no subgroups of index 2. Therefore $A_G(F)=A_{TQ}(F)$ is of order 12 with a normal four-group.

By Lemma A, z is fused into R, hence into W. So there is $x \in G$ with $z^x \in W$ and $C_T(z)^x=F^x \subseteq T$. By conjugating inside T, we may assume $F^x=F$. Write T^* for $T^{x^{-1}}$, W^* for $W^{x^{-1}}$; then $F \subseteq T$ and $F \subseteq T^*$. So $A_G(F)$ contains the stability group of $F > W > 1$ and the stability group of $F > W^* > 1$. These stability groups differ since $z \in W^*$, $z \notin W$. So $A_G(F) > A_{TQ}(F)$, which is impossible.

Therefore R splits over A. T has several sorts of E_8's; we will sort the E_8's of T (or equivalently, of G) according to the structure of their normalizers and centralizers in T.

We first investigate the involutions of R. The involutions of A are the non-identity elements of W. The involutions of eA are the elements of eW and eaW; these are carried by σ into the involutions of fA and hA, which are therefore the elements of fW, fbW, hW, and $ha^{-1}b^{-1}W$. $\{e, f, h, 1\}$ and $\{ea, fb, ha^{-1}b^{-1}, 1\}$ are both four-groups. So the involutions of R all lie in the two E_{16}'s,

$$X = \langle e, f, h, W\rangle; \qquad Y = \langle ea, fb, ha^{-1}b^{-1}, W\rangle$$

of R. $X^z = Y$ since $e^z \in eA-eW$; and $X \cap Y = W$.

Let s be any involution of $X-W$; $C_T(s) \supseteq X$. We show that $C_T(s)=X$. For any $r \in R$, $X^{zr}=Y$; so $C_T(s) \subseteq R$. If $C_T(s) > X$, then $C_T(s)$ contains some element y of $A-W$ (since A/W is incident to R/X). But $s=kw$ for $k=e, f$, or h, and $w \in W$; and $[kw, y]=[k, y] \neq 1$ for $y \in A-W$.

Our information about the involutions of T now allows us to sort the E_8's of T according to the structure of their normalizers and centralizers in T. We distinguish three possibilities:

Style 1. $F \nsubseteq R$. These F are $\langle z, W\rangle$ and its T-conjugates. $N_T(F)=\langle F, A\rangle$; $C_T(F)=F$.

Style 2. $W \subseteq F \subseteq R$. Then $F \subseteq X$ or Y; $X^z=Y$, so we will assume $F \subseteq X$. $N_T(F) \subseteq R$ (since each $zr \in zR$ sends X to Y, and $X \cap Y=W$); $F \supseteq \Phi(R)$, so $N_T(F)=R$. $C_T(F)=X$.

Style 3. $F \subseteq R$, $W \nsubseteq F$. Then $F \subseteq X$ or Y, say X. $F=K \times \langle w\rangle$ for some $w \in W$ and some four-group K of X with $K \cap W=1$. As in Style 2, $N_T(F) \subseteq R$. $N_T(F) \supseteq C_T(F)=X$. If $N_T(F)>X$, then $N_T(F)$ contains some element y of $A-W$ (since A/W is incident to R/X). Now $K=\{1, ew_1, fw_2, hw_3\}$ for w_1, w_2, $w_3 \in W$, and

$$[ew_1, y] = [e, y], \quad [fw_2, y] = [f, y], \quad [hw_3, y] = [h, y].$$

For fixed $y \in A-W$, these three commutators generate all of W. So $[F, y] \subseteq F$ is impossible for $y \in A-W$. Hence $N_T(F)=C_T(F)=X$.

(xxiii) If F is of Style 1 in T, then F cannot be of Style 2 in any Sylow 2-subgroup T^* of G with $T^* \supseteq F$.

Proof. If F is of Style 2 in T^*, then $N_{T^*}(F)=R^*$ is a Sylow 2-subgroup of $N_G(F)$. Also $N_T(F)=\langle F, A\rangle$ is a 2-subgroup of $N_G(F)$, so by Sylow's theorem in $N_G(F)$, some conjugate of $\langle F, A\rangle$ lies in R^*. But $\langle F, A\rangle$ is a split extension of A by an involution inverting A, and $R^* \cong R$ contains no subgroups of this isomorphism type.

(xxiv) If F is of Style 1 in T, then F cannot be of Style 3 in any T^*.

Proof. By (xxiii), $N_T(F)=\langle F, A\rangle$ is a 2-subgroup of $N_G(F)$ of largest possible order, so is a Sylow 2-subgroup of $N_G(F)$. If F is of Style 3 in T^*, then $N_{T^*}(F) \cong E_{16}$, and by Sylow's theorem in $N_G(F)$, some conjugate of $N_{T^*}(F)$ lies in $\langle F, A\rangle$. But $\langle F, A\rangle$ contains no E_{16}.

(xxv) z is not fused to W in G.

Proof. Suppose the contrary. Write $F=C_T(z)=\langle z, W\rangle$. Since W is central in T, there is $x \in G$ with $z^x \in W$ and $F^x \subseteq T$. By (xxiii) and (xxiv), F^x must be of Style 1 in T; all the E_8's of Style 1 in T are T-conjugate, so we may assume x has been chosen so that $F^x=F$.

Now the largest power of 2 which divides $|A_G(F)|$ is 4. It follows as above (by consideration of $GL_3(2)$) that $A_G(F)=A_{TQ}(F)$. But T^x induces on F the stability group of $F>W^x>1$, while T induces the stability group of $F>W>1$. These stability groups differ since $z^x \in W$, $z^x \notin W^x$. Hence $A_G(F)>A_{TQ}(F)$, and this contradiction proves (xxv).

z is fused into R, by Lemma A; take $x \in G$ with $z^x \in R$. z^x is not G-conjugate to W, by (xxv). So $C_T(z^x)=E$ say is an E_{16} and is a Sylow 2-subgroup of $C_G(z^x)$. $F^x=C_T(z)^x$ is a 2-subgroup of $C_G(z^x)$, so by Sylow's theorem in $C_G(z^x)$, there is $y \in C_G(z^x)$ such that $F^{xy} \subseteq E$. But then F^{xy} is of Style 2 or 3 in T, which contradicts (xxiii) or (xxiv).

This contradiction completes the proof that $T=R$; so by (xxii), T is of the isomorphism type claimed in Case 1.2 of Theorem 1. We showed at the beginning (before starting Case 1.1) that $N_G(T):C_G(T)=3$, 9, or 15. If 9, then $S/C_S(T)$ contains a subgroup of order 3 which centralizes W, so that Case 1.1 holds, which is impossible. So the proof in Case 1.2 is complete.

4. The case where $N_G(T)=TC_G(T)$ and the involutions of W are all conjugate in G.

THEOREM 2. *Suppose that T is a Sylow 2-subgroup of a simple group G;* $\mathrm{SCN}_3(T)$ *is empty but* $\mathrm{SCN}_2(T)$ *is not empty; and $T\not\cong D_8$. Then (Lemma 1) T has exactly one normal four-group, say W.*

Suppose $N_G(T)=TC_G(T)$ and the involutions of W are all conjugate in G.

Then one of the following holds:

Case 2.1. $T\cong \boldsymbol{Z}_{2^r} \wr \boldsymbol{Z}_2$ $(r\geqq 2)$.

Case 2.2. *T is the semidirect product of $A\cong \boldsymbol{Z}_{2^r}\times \boldsymbol{Z}_{2^r}$ $(r\geqq 3)$ by a four-group $\langle t, z\rangle$ such that t interchanges the two members of some basis for A, and z either inverts each element of A or raises each element of A to the power $-1+2^{r-1}$.*

Case 2.3. *T is of order 2^8, and can be described as follows:*

$$A = \langle a\rangle\times\langle b\rangle \cong \boldsymbol{Z}_4\times \boldsymbol{Z}_4.$$

R is the semidirect product of A by a four-group $\{1, e, f, h\}$, such that e, f, h have the matrices $\binom{3\ \ 0}{2\ \ 3}$, $\binom{3\ \ 2}{0\ \ 3}$, $\binom{1\ \ 2}{2\ \ 1}$ respectively on A (with respect to the basis $\{a, b\}$ of A).

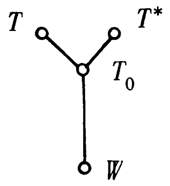
T is the semidirect product of R by a four-group $\langle t, z\rangle$ such that: z inverts each element of A, and $[z, e]=a$, $[z, f]=b$, $[z, h]=a^{-1}b^{-1}$; t interchanges a and b, and $[h, t]=1$, $[e, t]=h$, $[f, t]=h$.

THEOREM 3 (*the proof of which is part of the proof of Theorem* 2). *Suppose that T is the 2-group described in Case* 1.1 *of Theorem* 1, *and G is a simple group whose Sylow 2-subgroups are isomorphic to T. Then $[N_G(T):C_G(T)]$ must be divisible by some odd prime (so that Case* 1.1 *of Theorem* 1 *holds in full).*

Proof of Theorem 2. If W is central in T, the three involutions of W are G-conjugate, hence are $N_G(T)$-conjugate by Burnside's theorem. But this is impossible since $N_G(T)=TC_G(T)$.

So $T_0=C_T(W)$ is of index 2 in T.

Write $W=\langle z_1, z_2\rangle$ with z_1 central in T. By hypothesis there is a Sylow 2-subgroup of G in which z_2 is the central involution. $C_G(z_2)\supseteq T_0$; take T^* to be a Sylow 2-subgroup of $C_G(z_2)$ (and so of G) such that $T^*\supseteq T_0$.



T and T^* both contain T_0 with index 2, so both normalize T_0. So in $N_G(T_0)/T_0$, T/T_0 and T^*/T_0 generate a dihedral group D/T_0 whose order is twice an odd number.

$W=\Omega_1(Z(T_0))$ is characteristic in T_0 so is normal in D. T induces the transposition $(z_1)(z_2, z_1z_2)$ of $W-\{1\}$, while T^* induces $(z_2)(z_1, z_1z_2)$; so D induces the full symmetric group on $W-\{1\}$. So from the Sylow 3-subgroup of D/T_0, we can construct a group S/T_0 which is dihedral of order $2\cdot 3^n$ for some n; S_0/T_0 (say) is cyclic of order 3^n, and $S_0=T_0\langle g\rangle$ where we may take g to be any element of order 3^n in S; $S=T\langle g\rangle$. g permutes z_1, z_2, z_1z_2 cyclically. g^3 centralizes T_0; for if not, g^3 (being of odd order) must induce a nontrivial automorphism of $T_0/\Phi(T_0)$, but $T_0/\Phi(T_0)$ is of rank $\leqq 4$ by the four-generator theorem, and $GL_4(2)$ has no cyclic subgroups of order 9.

Let $T_0 \geqq A \geqq W$ such that A is Abelian; $A \lhd S$; and A is maximal subject to these conditions. A is of rank 2, and $\Omega_1(A)=W$ is cyclically permuted by g. Therefore A is homocyclic (since otherwise A could admit no nontrivial 3-automorphism, as in the proof of (i) in Case 1.1 of Theorem 1).

(i) If $A=W$, then $T_0=A=W$ (and hence $T\cong D_8$).

Proof. If $T_0>A=W$, let $Z/W=\Omega_1(Z(T_0/W))$. Z/W is S-invariant; and T_0 acts trivially on Z/W, so the S-submodules of Z/W are submodules for $S/\langle T_0, g^3\rangle \cong \Sigma_3$.

If $C_{Z/W}(g)>1$, then $C_{Z/W}(g)$ is T-invariant, so there is a T-invariant subgroup L of $C_{Z/W}(g)$ with $[L: W]=2$. Then L is S-invariant, and Abelian since W is central in L; this contradicts the maximality of $A=W$.

So Z/W is fixed-point-free under g. Each nonidentity element generates (under g) an irreducible module for the automorphism of order 3 induced by g. Every such irreducible module is a four-group, so the total number of irreducible g-submodules of Z/W is $\frac{1}{3}(|Z/W|-1)$, which is odd. T/T_0 permutes these g-submodules, hence fixes one, say K/W. Then $K \lhd S$; $|K|=16$, and W and K/W are both fixed-point-free under g. By Lemma 2 (in proof of Case 1.2 of Theorem 1), K is Abelian, again contrary to the maximality of $A=W$.

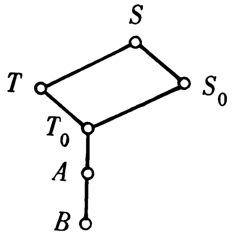
By (i) and the hypothesis that $T\not\cong D_8$, we must have $A>W$. So $B=\Omega_2(A)\cong Z_4\times Z_4$. $C_T(B)=C_{T_0}(B)$ so admits g. Also $C_T(B)$ is metacyclic (Alperin [1, Corollary, p. 110]); and the only metacyclic 2-group admitting an automorphism of order 3 which acts on W as g does, is Abelian and homocyclic. So $C_T(B)=A$ by the maximality of A.

Therefore $T/A \hookrightarrow \operatorname{Aut}(B)$; since $T_0=C_T(W)$, $A_T(B)\cap \mathfrak{B}^+=A_{T_0}(B)$ (see §2).

Now g normalizes T_0, so $A_{T_0}(B)$ $(\subseteq \mathfrak{B}^+)$ is invariant under the 3-automorphism of B induced by g. So $A_{T_0}(B)$ either contains $[\mathfrak{B}^+, \sigma]$ or is contained in $C_{\mathfrak{B}^+}(\sigma)$ (where σ is any 3-automorphism of B; see §2). Thus either $A_{T_0}(B)=[\mathfrak{B}^+, \sigma]\times X$, or $A_{T_0}(B)=X$, for some subgroup X of $C_{\mathfrak{B}^+}(\sigma)$.

$A_{T_0}(B)$ is also T-invariant; or equivalently, X is $A_T(B)$-invariant. Now the *same* subgroups X of $C_{\mathfrak{B}^+}(\sigma)$ are T-invariant no matter which Sylow 2-subgroup of

Aut B we choose to contain T, and in fact no matter what basis we choose for B. These X are 1, $\langle Z\rangle$, and $C_{\mathfrak{B}^+}(\sigma)$.



By the Frattini argument, since $\langle g\rangle$ is a Sylow 3-subgroup of S,

$$S = S_0N_S(\langle g\rangle) = T_0\langle g\rangle N_S(\langle g\rangle) = T_0N_S(\langle g\rangle).$$

But $S=T\langle g\rangle$, so $N_S(\langle g\rangle)=N_T(\langle g\rangle)\langle g\rangle$; so,

$$S = T_0N_T(\langle g\rangle)\langle g\rangle.$$

But $S=T\langle g\rangle$ with $T\cap\langle g\rangle=1$, and $T_0N_T(\langle g\rangle)\subseteq T$; so

$$T = T_0N_T(\langle g\rangle).$$

(ii) If $A_{T_0}(B)\supseteq[\mathfrak{B}^+,\sigma]$, let R_0/A be the subgroup of T_0/A corresponding to $[\mathfrak{B}^+,\sigma]$. Then $R_0\lhd\langle T,g\rangle=S$, and

$$T_0 = R_0C_{T_0}(\langle g\rangle), \qquad T = R_0N_T(\langle g\rangle)$$

where both products are semidirect.

Proof. $R_0\lhd\langle T,g\rangle$ since $[\mathfrak{B}^+,\sigma]\lhd\text{Aut}\,(Z_4\times Z_4)$.

Since R_0/A and A are fixed-point-free under g, so is R_0; so $R_0=[R_0,g]\subseteq[T_0,g]$. But T_0/R_0 is centralized by g; therefore $[T_0,g]=R_0$. So

$$T_0 = [T_0,g]C_{T_0}(\langle g\rangle) = R_0C_{T_0}(\langle g\rangle)$$
$$T = T_0N_T(\langle g\rangle) = R_0C_{T_0}(\langle g\rangle)N_T(\langle g\rangle) = R_0N_T(\langle g\rangle).$$

And $R_0\cap C_T(\langle g\rangle)=R_0\cap N_T(\langle g\rangle)=1$ since R_0 is fixed-point-free under g.

(iii) If $A_{T_0}(B)\subseteq C_{\mathfrak{B}^+}(\sigma)$, then

$$T_0 = AC_{T_0}(\langle g\rangle), \qquad T = AN_T(\langle g\rangle)$$

where both products are semidirect.

Proof. Since A is fixed-point-free under g, $A=[A,g]\subseteq[T_0,g]$. But T_0/A $\hookrightarrow C_{\mathfrak{B}^+}(\sigma)$, so $[T_0,g]=A$. So

$$T_0 = [T_0,g]C_{T_0}(\langle g\rangle) = AC_{T_0}(\langle g\rangle)$$
$$T = T_0N_T(\langle g\rangle) = AC_{T_0}(\langle g\rangle)N_T(\langle g\rangle) = AN_T(\langle g\rangle).$$

And $A\cap C_{T_0}(\langle g\rangle)=A\cap N_T(\langle g\rangle)=1$ since A is fixed-point-free under g.

Case 2.1. $T_0=A$. We show that $T\cong Z_{2^r}\wr Z_2$ (where A is of exponent 2^r). For $[T:T_0]=2 \Rightarrow T=AN_T(\langle g\rangle)$ (by (iii)) where $N_T(\langle g\rangle)$ is of order 2. Now in S/T_0, T/T_0 inverts $\langle g\rangle T_0/T_0$; so in Aut (A), T/A must induce a transposition of the nonidentity elements of the four-group $A/\mho^1(A)$. This means there is $a\in A$ with $A=\langle a\rangle\times\langle a^t\rangle$. Since $t^2=1$, $(a^t)^t=a$, i.e., t simply exchanges a and a^t.

Case 2.2. *$T_0>A$ and A of exponent 2^r for $r\geqq 3$.* Each element x of T_0-A induces (by conjugation) an automorphism of A which restricts to a *nonidentity* automorphism of $B=\Omega_2(A)$. $x^2\in A$, so this automorphism of A must be of order 2. We now show that under these conditions, certain automorphisms $\in\mathfrak{B}^+$ cannot be induced on B by T_0/A.

Choose a basis $\{a, b\}$ for A such that $a^g=b$, $b^g=a^{-1}b^{-1}$ (such a basis exists because all 3-elements of Aut (A) are conjugate in Aut (A)); take $\{a^{2^{r-2}}, b^{2^{r-2}}\}$ as a basis for B. We can then write matrices with coefficients integers mod 2^r for the automorphisms of A, and restriction to B just means reading the matrix mod 4.

(iv) Suppose A is of exponent 2^r for $r\geqq 3$, and bases for A and $B=\Omega_2(A)$ have been chosen as above. Then no matrix of the form $\left(\begin{smallmatrix}\text{odd} & 2\\ 2 & \text{odd}\end{smallmatrix}\right)$ can be the restriction to B of an automorphism θ of A with $\theta^2=1$.

Proof. Let θ have matrix $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$. Then

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\equiv\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}^2\equiv\begin{pmatrix}\alpha^2+\beta\gamma & (\alpha+\delta)\beta\\ (\alpha+\delta)\gamma & \beta\gamma+\delta^2\end{pmatrix} \mod 2^r.$$

If $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)\equiv\left(\begin{smallmatrix}\text{odd} & 2\\ 2 & \text{odd}\end{smallmatrix}\right)$ mod 4, then α, δ are odd and β, $\gamma\equiv 2$ mod 4, so that $\beta\gamma\equiv 4$ mod 8. But the square of any odd number is $\equiv 1$ mod 8; so α^2, $\delta^2\equiv 1$ mod 8 and $\alpha^2+\beta\gamma\equiv 1$ mod 8 is impossible.

Assume in (v)–(x) that $T_0>A$ and A is of exponent 2^r for $r\geqq 3$.

(v) $[T_0:A]=2$ and $T_0=\langle z, A\rangle$ where z is an involution inverting B. T is the semidirect product of A by $N_T(\langle g\rangle)$, with $N_T(\langle g\rangle)=\langle z, t\rangle$ where z centralizes g and t inverts g.

Proof. $[\mathfrak{B}^+, \sigma]$ contains the matrix $\left(\begin{smallmatrix}1 & 2\\ 2 & 1\end{smallmatrix}\right)$ (with respect to *any* basis of B). So by (iv), $A_{T_0}(B)\nsupseteq[\mathfrak{B}^+, \sigma]$. Therefore $A_{T_0}(B)\subseteq C_{\mathfrak{B}^+}(\sigma)$. Now $C_{\mathfrak{B}^+}(\sigma)$ contains the matrices $\left(\begin{smallmatrix}1 & 2\\ 2 & 3\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}3 & 2\\ 2 & 1\end{smallmatrix}\right)$, which T_0/A cannot induce on B by (iv). So $A_{T_0}(B)=\langle Z\rangle$ (i.e., T_0/A inverts B). The rest of (v) follows from (iii).

(vi) The matrix of z on A is of the form

$$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}+\begin{pmatrix}i & j\\ j & i+j\end{pmatrix}2^{r-1}$$

for some $i, j\in\{0, 1\}$.

Proof. Let z have matrix $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$. z centralizes g and we have arranged that g has matrix $\left(\begin{smallmatrix}0 & 1\\ -1 & -1\end{smallmatrix}\right)$. So

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}\equiv\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \mod 2^r.$$

This is equivalent to $\gamma\equiv-\beta$ and $\delta\equiv\alpha-\beta$. So the matrix of z is of the form

$$\begin{pmatrix}\alpha & \beta\\ -\beta & \alpha-\beta\end{pmatrix}.$$

Also

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\equiv\begin{pmatrix}\alpha & \beta\\ -\alpha & \alpha-\beta\end{pmatrix}^2\equiv\begin{pmatrix}\alpha^2-\beta^2 & 2\alpha\beta-\beta^2\\ \beta^2-2\alpha\beta & \alpha^2-2\alpha\beta\end{pmatrix}\quad\text{mod } 2^r,$$

or equivalently,

$$\alpha^2-\beta^2\equiv 1\quad\text{mod } 2^r,\qquad \beta^2\equiv 2\alpha\beta\quad\text{mod } 2^r.$$

However, $\beta\equiv 0$ mod 4 since z inverts B, and α is odd; so $\beta^2\equiv 2\alpha\beta$ mod $2^r\Rightarrow\beta\equiv 0$ mod 2^{r-1}. Then

$$1\equiv\alpha^2-\beta^2\equiv\alpha^2\quad\text{mod } 2^r,$$

so α is one of the four square roots of 1 mod 2^r, namely ± 1, and $\pm 1+2^{r-1}$. $\alpha\equiv -1$ mod 4 since z inverts B; so α is -1 or $-1+2^{r-1}$, and (vi) is proved.

(vii) The matrix of z on A is

$$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\quad\text{or}\quad\begin{pmatrix}-1+2^{r-1} & 0\\ 0 & -1+2^{r-1}\end{pmatrix}.$$

Proof. $N_T(\langle g\rangle)=\langle t, z\rangle$ where t inverts g and centralizes z (by (v)). Let t have matrix $(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix})$. g has matrix $(\begin{smallmatrix}0 & 1\\ -1 & -1\end{smallmatrix})$; so in order for t to invert g, we must have

$$\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\equiv\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix}\quad\text{mod } 2^r.$$

This is equivalent to $\gamma\equiv-\alpha+\beta$, $\delta\equiv-\alpha$ mod 2^r. So the matrix of t is of the form

$$\begin{pmatrix}\alpha & \beta\\ -\alpha+\beta & -\alpha\end{pmatrix}.$$

Also t centralizes z, which by (vi) is equivalent to

$$\begin{pmatrix}\alpha & \beta\\ -\alpha+\beta & -\alpha\end{pmatrix}\begin{pmatrix}i & j\\ j & i+j\end{pmatrix}\equiv\begin{pmatrix}i & j\\ j & i+j\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ -\alpha+\beta & -\alpha\end{pmatrix}\quad\text{mod } 2.$$

This gives

$$\begin{pmatrix}\alpha i+\beta j & \alpha j+\beta i+\beta j\\ \alpha i+\beta i+\alpha j & \beta j+\alpha i\end{pmatrix}\equiv\begin{pmatrix}\alpha i+\alpha j+\beta j & \beta i+\alpha j\\ \alpha i+\beta i+\beta j & \beta j+\alpha i+\alpha j\end{pmatrix}\quad\text{mod } 2,$$

i.e.,

$$\begin{pmatrix}0 & \beta j\\ \alpha j & 0\end{pmatrix}\equiv\begin{pmatrix}\alpha j & 0\\ \beta j & \alpha j\end{pmatrix}\quad\text{mod } 2.$$

If $j=1$ this requires β and α both even, in which case the matrix of t is singular. So $j=0$, and (vii) follows from (vi).

(viii) If $N_T(\langle g\rangle)$ is cyclic, $=\langle t\rangle$ with $t^2=z$, then t is fused into A.

Proof. We consider the transfer homomorphism $\tau\colon G \to T/A$.

Suppose z inverts A. Then we consider the value of τ at t.

$$\tau(t) = \left(\prod\left\{yty^{-1}: \begin{smallmatrix}\text{cosets } Ty\\ \text{with } Tyt=Ty\end{smallmatrix}\right\}\right)\left(\prod\left\{xt^2x^{-1}: \begin{smallmatrix}\text{cosets } Tx\\ \text{with } Txt\neq Tx\\ \text{but } Txt^2=Tx\end{smallmatrix}\right\}\right)A.$$

The xt^2x^{-1} are involutions so lie in T_0 (since $(T/A)-(T_0/A)$ contain no involutions $\Rightarrow T-T_0$ contains none). The yty^{-1} are of order 4 and so do not lie in zA since zA consists entirely of involutions. If no yty^{-1} lies in A, then $\tau(t)\equiv tA \bmod T_0/A$ (because the number of cosets Ty with $Tyt=Ty$ is odd), contradicting the simplicity of G.

Suppose z raises A to the power $-1+2^{r-1}$. Only one involution of W is central in T; assume a basis $\{a, b\}$ of A has been chosen so that $a^{2^{r-1}}b^{2^{r-1}} \in W$ is the central involution of T. (The matrix of z is invariant under changes of basis in A. This change of basis may change the matrix $\left(\begin{smallmatrix}0 & 1\\ -1 & -1\end{smallmatrix}\right)$ of g, but we are not going to use g.) Write $\hat{a}$, $\hat{b}$ for $a^{2^{r-1}}$, $b^{2^{r-1}}$.

Consider the value of τ at z.

$$\tau(z) = \prod\{yzy^{-1}:\quad \text{cosets } Ty \text{ with } Tyz = Ty\}A.$$

The yzy^{-1} are involutions so lie in T_0. If none lies in A, then $\tau(z)=zA$, contradicting the simplicity of G. So z is fused into A, hence into W. The three involutions of W are fused together in G, so z is fused to $\hat{a}\hat{b}$ and there is $h \in G$ with $z^h=\hat{a}\hat{b}$ and $C_T(z)^h \subseteq T$.

$C_T(z)=\langle t, W\rangle=(\langle t\rangle \times \langle \hat{a}\hat{b}\rangle)\langle \hat{a}\rangle$ where $\hat{a}$ centralizes $\hat{a}\hat{b}$ and conjugates t to $t\hat{a}\hat{b}$.

$t^2=z$, so $(t^h)^2=z^h=\hat{a}\hat{b}$. Suppose $t^h \notin A$. There is one T-conjugacy-class of elements of order 4 in $T-A$ whose square is $\hat{a}\hat{b}$, and this class is represented by zab; so by conjugation in T we may assume $t^h=zab$. $(\hat{a}\hat{b})^h$ and $(\hat{a})^h$ are involutions so lie in T_0; so $C_T(z)^h \subseteq T_0$.

$(\hat{a}\hat{b})^h$ must be an involution of T_0 which centralizes zab and is not $\hat{a}\hat{b}=(zab)^2$. We observe that zA contains no such involutions (and therefore $(\hat{a}\hat{b})^h=\hat{a}$ or $\hat{b}$). For if $x \in A$ and zx centralizes zab, then

$$\begin{aligned} 1 &= [zab, zx] = [zab, x][zab, z]^x \\ &= [z, x][ab, z] \equiv x^2a^{-2}b^{-2} \quad \bmod W. \end{aligned}$$

But if $x^2\equiv a^2b^2 \bmod W$ then zx is not an involution.

So $\langle t, \hat{a}\hat{b}\rangle^h=\langle zab, W\rangle$. $\hat{a}^h$ must be an involution of T_0 lying outside $\langle zab, W\rangle$ (and hence $\in zA$), and conjugating zab to $(zab)(\hat{a}\hat{b})^h$. Write $\hat{a}^h=zc$ for $c \in A$; then

$$\begin{aligned} (zab)^{zc} &= z^c(ab)^z = c^{-1}zc(ab)^z = zc^{-z}c(ab)^z \\ &= zc^{2+2^{r-1}}(ab)^{-1+2^{r-1}}. \end{aligned}$$

If this equals $zab(\hat{a}\hat{b})^h$, which is congruent to zab mod W, then $c^2\equiv(ab)^2 \bmod W$. But then $c \notin \mho^1(A)$ and so zc is not an involution.

So no such $\hat{a}^h$ exists. Therefore $t^h \in A$, and (viii) is proved.

(ix) $N_T(\langle g\rangle)$ is a four-group.

Proof. Suppose $N_T(\langle g\rangle)$ is cyclic. We survey the T-centralizers of the elements of order 4 in T.

Elements of tA or tzA: the centralizer in T is of order 4 times the order of the centralizer in A. The square of any such element inverts B and so the centralizer in A is contained in W. Since W is not central in T, this centralizer in A is just $\langle \hat{a}\hat{b}\rangle$ (notation as in proof of (viii)). So the T-centralizer of such an element is of order 8; and in particular, $C_T(t)=\langle t, \hat{a}\hat{b}\rangle$.

Elements of zA: the centralizer in T is of order at most 4 times $|W|$.

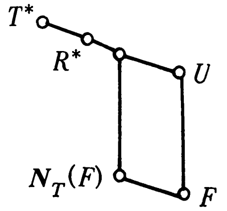
Elements of A: the centralizer in T is A, of order 2^{2r}.

Of these three sorts of centralizers, the one of largest order is A.

Let U be a Sylow 2-subgroup of $C_G(t)$. By (viii) and Sylow's theorem, U is a conjugate of A (for A, being the only Abelian maximal subgroup of $C_T(W)$, is characteristic in T). By Sylow's theorem in $C_G(t)$, we may choose U to contain $C_T(t)=\langle t, \hat{a}\hat{b}\rangle = F$ say. Then U normalizes F.

$N_T(F)=\langle F, \hat{a}\rangle$, where a acts on F by conjugating t to $t\hat{a}\hat{b}$. For $N_T(F)=\langle t, N_A(F)\rangle$, and $N_A(F)$ consists of the elements $x\in A$ with $[x, t]\in\langle \hat{a}\hat{b}\rangle$. Now the map $x\to x^{-1}x^t$ is a homomorphism from A into itself; the kernel is $C_A(T)=\langle \hat{a}\hat{b}\rangle$, of order 2. $N_A(F)$ is the inverse image under this homomorphism of $\langle \hat{a}\hat{b}\rangle$, which is of order twice $|C_A(t)|$, or 4. Since W normalizes F by inspection, $W=N_A(F)$.

Let $T^*\supseteq R^*\supseteq U$ where R^* is a Sylow 2-subgroup of $N_G(F)$ and T^* is a Sylow 2-subgroup of G. By Sylow's theorem in $N_G(F)$, we may choose R^* to contain $N_T(F)$. This may replace U by an $N_G(F)$-conjugate of U, but the new U will still contain F.



$U=A^*$, and $\hat{a}\in T_0^*$ since $T^*-T_0^*$ contains no involutions. (The characteristic subgroups A^*, T_0^* are to T^* as A, T_0 are to T.) $\hat{a}$ does not centralize F, so $\hat{a}\in T_0^*-U=T_0^*-A^*$. So $\hat{a}$ inverts $t\in\Omega_2(A^*)$. But we have just observed that $\hat{a}$ does not invert t. This contradiction proves (ix).

(x) T is the semidirect product of A by the four-group $N_T(\langle g\rangle)=\langle t, z\rangle$. A basis of A can be chosen so that t has the matrix $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$ and z has either the matrix $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$ or

$$\begin{pmatrix}-1+2^{r-1} & 0\\ 0 & -1+2^{r-1}\end{pmatrix}$$

Proof. t inverts g, so must induce a transposition of the nonidentity elements of the four-group $A/\mho^1(A)$. This means there is $a \in A$ with $A = \langle a\rangle \times \langle a^t\rangle$; $(a^t)^t = a$ since $t^2 = 1$. Take $\{a, a^t\}$ as basis for A.

Case 2.3. *$T_0 > A$ and $A \cong Z_4 \times Z_4$.* The remarks following (i) then hold, with $B = A$. In particular, (ii) or (iii) holds with $B = A$.

(xi) $A_{T_0}(A) \supseteq [\mathfrak{B}^+, \sigma]$ (and (ii) holds).

Proof. Suppose $A_{T_0}(A) \subseteq C_{\mathfrak{B}^+}(\sigma)$ (and hence (iii) holds). Now all of the automorphisms $\in C_{\mathfrak{B}^+}(\sigma)$ have fixed-point-set just W; so all squares of elements of $T_0 - A$ lie in W; and also $A^2 = W$. So $\Phi(T_0) = W$, by Lemma FB of §1.

Now $T_0 > A \Rightarrow A_{T_0}(A)$ is either $\langle Z\rangle$ or $C_{\mathfrak{B}^+}(\sigma)$. In either case there is an involution $z \in C_{T_0}(\langle g\rangle)$ which inverts A. z is central in $N_T(\langle g\rangle)$ since Z is central in $\mathrm{Aut}\,(Z_4 \times Z_4)$. $\langle z, W\rangle \cong E_8$. $[z, N_T(\langle g\rangle)] = 1$, and $[z, T_0] \subseteq [T_0, T_0] \subseteq W$. But $T = T_0 N_T(\langle g\rangle)$; so $\langle z, W\rangle$ is a normal E_8 of T, contradicting $\mathrm{SCN}_3\,(T)$ empty.

Now all Sylow 3-subgroups of $\mathrm{Aut}\,(A)$ are conjugate via $[\mathfrak{B}^+, \sigma]$; so by (xi), $\langle T, g\rangle = S$ induces *every* 3-automorphism of A. In particular, no matter which basis is taken in A, the matrix $\left(\begin{smallmatrix}0 & 1\\ 3 & 3\end{smallmatrix}\right)$ will be induced by some 3-element of S. And (ii) holds no matter which Sylow 3-subgroup of S is taken as $\langle g\rangle$.

(*) So, no matter which basis is taken for A, we may assume g has been chosen to induce $\left(\begin{smallmatrix}0 & 1\\ 3 & 3\end{smallmatrix}\right)$ on A, and (ii) will hold for this choice of g.

Moreover, the automorphism σ induced on T_0 by this g will be of order exactly 3, will preserve R_0, and will act fixed-point-freely on R_0/A (where R_0/A is the subgroup of T_0/A corresponding to $[\mathfrak{B}^+, \sigma]$, as in (ii)). So Lemma 3 (in proof of Case 1.2 of Theorem 1) applies to R_0 and σ. In particular, there are elements $e, f, h \in R_0$ as described in Lemma 3, with $e^\sigma = f$, $f^\sigma = h$, and $h^\sigma = e$. (Recall that Lemma 3 was a method of choosing $e, f, h \in R_0$ so as to satisfy the above, where σ is *any* automorphism of order 3 of R_0 whose restriction to A is $\left(\begin{smallmatrix}0 & 1\\ 3 & 3\end{smallmatrix}\right)$ with respect to a chosen basis for A.)

For convenience, we will write R instead of R_0.

(xii) Suppose $g \in S$ has been chosen in accordance with (*) (so that we have R as in Lemma 3). Write σ for the automorphism of T_0 induced by g. Suppose Y is any subgroup of T_0 with $Y > R$ and $[Y : R] = 2$. Then $Y = \langle y, R\rangle$ for some involution $y \in C_{T_0}(\langle g\rangle)$. The isomorphism type of Y is completely determined by R, the automorphism of A induced by y, and $[y, e]$ (for then $[y, f] = [y, e]^\sigma$, $[y, h] = [y, e]^{\sigma^2}$). Furthermore, we must have $[y, e] \in A$, $[y, e] \notin W$.

Proof. By (ii), $T_0 = RC_{T_0}(\langle g\rangle)$ where this product is semidirect and $C_{T_0}(\langle g\rangle) \cong T_0/R$ is elementary. So $Y = \langle R, y\rangle$ for some involution $y \in C_{T_0}(\langle g\rangle)$.

T_0/A is elementary, so $A \supseteq \Phi(Y) \supseteq \Phi(R) = W$. If $\Phi(Y) = W$ then $[Y : \Phi(Y)] = 2^5$, which contradicts the four-generator theorem. So $\Phi(Y) > W$; since Y is σ-invariant, $\Phi(Y)$ is σ-invariant and so $\Phi(Y) = A$.

Y is a split extension of R, so its isomorphism type is completely determined by R and the action of y on R, which latter consists of the automorphism of A induced by y and the commutators $[y, e]$, $[y, f]$, and (redundantly) $[y, h]$. Via σ, these three commutators are determined by $[y, e]$. Computation of $\Phi(Y)$ reveals that $\Phi(Y)=A$ if and only if $[y, e] \notin W$. In detail, $\Phi(Y)$ is generated by the squares of the elements of Y. If $x \in A$, then $[x, y] \in W$, and

$$(xy)^2 = xyxy = x^2y[y, x]y = x^2[y, x]^y \in W.$$

If $r \in R$, $r \notin A$,

$$\begin{aligned}(ry)^2 &= ryry = r^2[y, r]^y \\ &\equiv [y, r] \mod W, \quad \text{since } [y, r] \in A\end{aligned}$$

and y stabilizes the chain $A > W > 1$. So $\Phi(Y) > W$ if and only if $[y, r] \in A - W$ for some $r \in R$, $r \notin A$. This is equivalent to $[y, k] \in A - W$ for $k=e, f$, or h; but if one of these commutators lies in $A - W$, they all do since they are σ-conjugate.

(xiii) $A_{T_0}(A) = \mathfrak{B}^+$ is impossible.

Proof. If $A_{T_0}(A) = \mathfrak{B}^+$, then no matter what basis is chosen for A, there is $y \in C_{T_0}(\langle g \rangle)$ inducing $\left(\begin{smallmatrix}1 & 2\\ 2 & 3\end{smallmatrix}\right)$ on A. $y^2 = 1$, so

$$1 = [y^2, e] = [y, e]^y[y, e],$$

and y inverts $[y, e]$. But by (xii), $[y, e] \in A - W$; and $\left(\begin{smallmatrix}1 & 2\\ 2 & 3\end{smallmatrix}\right)$ does not invert any element of $A - W$.

By (xiii), $A_{T_0}(A)$ is either $[\mathfrak{B}^+, \sigma]$ or $[\mathfrak{B}^+, \sigma] \times \langle Z \rangle$. Both of these candidates for $A_{T_0}(A)$ will yield T with $\mathrm{SCN}_3\,(T)$ empty. In order to construct these T, we will choose a basis in A, and then take g as in (*) so that we can use Lemma 3 to describe R.

$A_T(A)$ is contained in some Sylow 2-subgroup of Aut (A). Since all the Sylow 2-subgroups of Aut (A) are conjugate in Aut (A), we can choose which Sylow 2-subgroup of matrices will contain the matrix-group corresponding to Aut (A), by a choice of basis in A.

(xiv) We now assume our basis $\{a, b\}$ in A is one such that the matrix-group for $A_T(A)$ lies in $\langle \left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right), \mathfrak{B}^+ \rangle$. (There are many such bases, and we will later refine this choice.)

$\langle \left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right), \mathfrak{B}^+ \rangle$ centralizes $\left(\begin{smallmatrix}1 & 2\\ 2 & 1\end{smallmatrix}\right)$ and interchanges $\left(\begin{smallmatrix}3 & 0\\ 2 & 3\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}3 & 2\\ 0 & 3\end{smallmatrix}\right)$. So the normalization (xiv) implies that in R/A, hA is centralized and eA, fA interchanged by T/A.

(xv) Suppose $N_T(\langle g \rangle) = \langle t, N_{T_0}(\langle g \rangle) \rangle$ for t an involution, and t has matrix $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$ on A. Then R must split over A, and $[h, t] \in A$ is of the form $a^{\zeta}b^{-\zeta}$.

Proof. $[h, t] \in A$ since hA is central in T/A. Since $t^2 = 1$,

$$1 = [h, t^2] = [h, t][h, t]^t,$$

and so t must invert $[h, t]$, which is therefore of the form $a^{\zeta}b^{-\zeta}$ (for some number ζ). Also

$$\begin{aligned}[h^2, t] &= [h, t]^h[h, t] = (a^{\zeta}b^{-\zeta})^h(a^{\zeta}b^{-\zeta}) \\ &= (ab^2)^{\zeta}(a^2b)^{-\zeta}a^{\zeta}b^{-\zeta} = 1.\end{aligned}$$

But $h^2 = 1$ if R splits and a^2 if not; and $[a^2, t] = a^2b^2 \neq 1$.

Case 2.3.1. We now work out what T has to be if $A_{T_0}(A)=[\mathfrak{B}^+, \sigma]$, i.e., $T_0=R$. Assume that a basis $\{a, b\}$ of A has been chosen satisfying (xiv), and that $g \in S$ has then been chosen satisfying (*), so that R is as described by Lemma 3. In constructing T as an extension of R, we will make further changes of basis in A; these changes of basis will *not* preserve the 3-matrix $\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)$ of g, but *will* (essentially) preserve relations which hold strictly within the 2-group R itself, and will also preserve (xiv).

By (ii), $T=RN_T(\langle g\rangle)=R\langle t\rangle$ say, for t of order 2.

(xvi) In Case 2.3.1, we may assume t has the matrix $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ on A.

Proof. t inverts g, where g satisfies (*), i.e., the matrix of g on A is $\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)$. So the matrix of t is an involution $\in \langle\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \mathfrak{B}^+\rangle-\mathfrak{B}^+$, inverting $\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)$. Now $\langle\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \mathfrak{B}^+\rangle-\mathfrak{B}^+$ has four involutions, namely the elements of the coset $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\langle\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)\rangle$; and of these, two—namely $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&3\\3&0\end{smallmatrix}\right)$—invert $\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)$. So the matrix of t on A is either $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}0&3\\3&0\end{smallmatrix}\right)$.

If it is $\left(\begin{smallmatrix}0&3\\3&0\end{smallmatrix}\right)$, change basis in A by the similarity-matrix $\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right)$ (this is where we lose track of the 3-matrix). This change of basis does not alter (xiv), since $\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right)\in\mathfrak{B}^+\subseteq$ every Sylow 2-subgroup of Aut (A). Moreover, $\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right)$ centralizes $\left(\begin{smallmatrix}3&0\\2&3\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}3&2\\0&3\end{smallmatrix}\right)$, and $\left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$, and also centralizes every square in R (namely, it centralizes W); so the relations between e, f, h, and A, and their squares, will read exactly the same after this change of basis as before. Finally, t will have the matrix $\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix}0&3\\3&0\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right)=\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ with respect to the new basis.

By (xvi), (xv) applies; therefore R splits over A, and $[h, t]=a^{\zeta}b^{-\zeta}$ for some number ζ.

$\langle h, A\rangle \lhd T$ and has two E_8's, namely $\langle h, W\rangle$ and $\langle hab, W\rangle$. In order for $\mathrm{SCN}_3(T)$ to be empty, t must exchange these two E_8's; this means $h^t \in habW$, i.e., $[h, t]=ab^3$ or a^3b.

(xvii) In Case 2.3.1, we may assume $[h, t]=a^3b$.

Proof. If $[h, t]=ab^3$, make the change of basis $a \rightarrow b$, $b \rightarrow a$ in A (i.e., transform A by the similarity-matrix $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$). This does not affect (xiv), and does not change the matrix of t on A. $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ centralizes $\left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$ and exchanges $\left(\begin{smallmatrix}3&0\\2&3\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}3&2\\0&3\end{smallmatrix}\right)$; so in R, h will have the same matrix as before, and e will have the matrix f had and f will have the matrix e had, with respect to the new basis. e^2, f^2, and $[e, f]$ will read the same after the change of basis as before, since they are equal to 1. So if after making this change of basis, we reverse the roles of the letters e and f, we will get R again exactly as in the statement of Lemma 3. Finally, $[h, t]$ will appear as a^3b with respect to the new basis.

To construct T as a split extension of R, it remains only to determine $[e, t]$ and (redundantly) $[f, t]$. We now work out what $[e, t]$ and $[f, t]$ are, without making any more changes of basis.

Since T/A interchanges eA and fA, $[e, t]$ and $[f, t]$ lie in hA. Write $[e, t]=hx$, $[f, t]=hy$ for $x, y \in A$. Now $ef=h$, so $[e, t]$ determines $[f, t]$ as follows:

$$a^3b = [h, t] = [ef, t] = [e, t]^f[f, t] = (hx)^f(hy).$$

Since 1, e, f, h form a four-group, we have

$$a^3b = fhxfhy = exey = x^e y.$$

We now compute $[e, t]$. Since $e^2=1$,

$$1 = [e^2, t] = [e, t]^e[e, t],$$

so e inverts $[e, t]$. Similarly $t^2=1 \Rightarrow t$ inverts $[e, t]$. The inverse of a typical element $ha^\xi b^\eta$ of hA is $ha^{-\xi+2\eta}b^{-\eta+2\xi}$. If we write $[e, t]=hx=ha^\alpha b^\beta$, then inversion by e gives

$$\begin{tikzcd}[column sep=small] (ha^\alpha b^\beta)^e \arrow[d, equal] & = & ha^{-\alpha+2\beta}b^{-\beta+2\alpha} \\ h(a^3)^\alpha(a^2b^3)^\beta & = & ha^{-\alpha+2\beta}b^{-\beta}, \end{tikzcd}$$

or equivalently, $-\beta+2\alpha=-\beta$, so that α is even. Inversion by t gives

$$\begin{tikzcd}[column sep=small] (ha^\alpha b^\beta)^t \arrow[d, equal] & = & ha^{-\alpha+2\beta}b^{-\beta+2\alpha} \\ ha^3ba^\beta b^\alpha & = & ha^{\beta+3}b^{\alpha+1}, \end{tikzcd}$$

or equivalently, $\beta+3=-\alpha+2\beta$, $\alpha+1=-\beta+2\alpha$, or equivalently, $\beta=3+\alpha$, so that β is determined by α.

So we seem to have two groups T: one with $\alpha=0$ (i.e., $[e, t]=hb^3$) and one with $\alpha=2$ (i.e., $[e, t]=ha^2b$).

But these two T are isomorphic. For if we take $\hat{a}=a$, $\hat{b}=b$; $\hat{e}=ea^2$, $\hat{f}=fb^2$, $\hat{h}=ha^2b^2$; $\hat{t}=ta^2b^2$, then the matrices of $\hat{e}, \hat{f}, \hat{h}, \hat{t}$ on A (with respect to $\{\hat{a}, \hat{b}\}=\{a, b\}$) are the same as those of e, f, h, t; $\hat{e}\hat{f}=\hat{h}$ and $\hat{e}, \hat{f}, \hat{h}$ are involutions; $[\hat{h}, \hat{t}]=[h, t]$ since a^2b^2 is central; and

$$[\hat{e}, \hat{t}] = [ea^2, ta^2b^2] = [ea^2, t] = [e, t]a^2b^2.$$

So in Case 2.3.1,

$$T = \langle \text{split } R, t\colon t^2 = 1, t \text{ has matrix } \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \text{ on A};$$
$$[h, t] = a^3b, \quad [e, t] = hb^3, \quad [f, t] = ha\rangle.$$

(Note that these relations *do* define a group, since the relations given between t and R define an automorphism of order 2 of the group R.)

This T has $\mathrm{SCN}_3(T)$ empty. For if not, T has a normal E_8, F say, containing W (by the Lemma below). $F \subseteq C_T(W)=T_0$, and projects onto exactly one nonidentity coset of A in T_0. This coset must be hA since $(eA)^t=fA$. But we have explicitly arranged that no $E_8 \subseteq \langle h, A\rangle$ is normal in T.

LEMMA. *If W is a normal four-group of any 2-group T, and T has a normal E_8 (F say), then T has a normal E_8 containing W.*

Proof. $C_F(W) \lhd T$, contains $F \cap W$, and is of order $\geqq 4$ because $|\mathrm{Aut}\ (W)|=6$. If $F \not\supseteq W$, then $|F \cap W| \leqq 2$, so $|C_F(W)W| \geqq (4\cdot 4)/2=8$; so $C_F(W)W$ is a normal elementary subgroup of T of order $\geqq 8$, containing W. So there is K with $C_F(W)W \geqq K > W$ such that $K \lhd T$ and $K \simeq E_8$.

Now suppose $A_{T_0}(A) = [\mathfrak{B}^+, \sigma] \times \langle Z \rangle$. Assume that a basis $\{a, b\}$ of A has been chosen satisfying (xiv), and that $g \in S$ has then been chosen satisfying (*), so that R is as described by Lemma 3.

(xviii) If $A_{T_0}(A) = [\mathfrak{B}^+, \sigma] \times \langle Z \rangle$, then $T_0 = \langle z \rangle R$ is a split extension of R by an involution which inverts A and centralizes g. Moreover, we may assume (by choice of basis in A) that $[z, e] = a$; and $[z, f] = a^\sigma = b$; $[z, h] = b^\sigma = a^{-1}b^{-1}$.

Proof. The first statement follows from (ii).

Taking $Y = T_0$ in (xii), we see that $[z, e] \in A - W$ and $[z, e]$ (together with R) completely determines T_0. Since $e^2 \in W$,

$$1 = [z, e^2] = [z, e][z, e]^e,$$

so e must invert $[z, e]$. Therefore $[z, e] \in aW$.

Let Δ be one of the matrices $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 2 \\ 2 & 3 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 3 & 2 \\ 2 & 1 \end{smallmatrix}\right)$. Then Δ centralizes $\mathfrak{B}^+$ *and* $\left(\begin{smallmatrix} 0 & 1 \\ 3 & 3 \end{smallmatrix}\right)$; so if we change basis in A by Δ, the matrices of e, f, h, and σ will read exactly the same after the change of basis as before. In particular, (*) still holds with respect to the new basis, so (xii) still applies.

$[z, e]$ will be replaced by $[z, e]^\Delta$. Now these matrices form a group which acts transitively on the elements of aW; so there is a unique Δ such that $[z, e]^\Delta = a$. Having made the change of basis $\{a, b\} \to \{a^\Delta, b^\Delta\}$ for this Δ, we will have

$$[z, e] = a,$$
$$[z, f] = [z^\sigma, e^\sigma] = a^\sigma = b$$

(since the matrix of σ is unchanged)

$$[z, h] = b^\sigma = a^{-1}b^{-1}.$$

Now $T = RN_T(\langle g \rangle)$, where $N_T(\langle g \rangle)$ is either a four-group or cyclic of order 4.

Case 2.3.2. We now work out what T has to be if $N_T(\langle g \rangle)$ is a four-group, say $\langle t, z \rangle$ where t is an involution inverting g.

(xix) In Case 2.3.2, we may assume t has the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ on A.

Proof. As in (xvi), the matrix of t is either $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & 3 \\ 3 & 0 \end{smallmatrix}\right)$; if it is $\left(\begin{smallmatrix} 0 & 3 \\ 3 & 0 \end{smallmatrix}\right)$, replace t by tz.

By (xix), (xv) applies; therefore R splits over A, and $[h, t] = a^\zeta b^{-\zeta}$ for some number ζ. $[e, t]$ and $[f, t]$ lie in hA since T/A interchanges eA and fA; write $[e, t] = hx$, $[f, t] = hy$; for $x, y \in A$. (Once we determine $[e, t]$, $[f, t]$, and $[h, t]$, T is completely determined.)

As in Case 2.3.1, $[e, t]$ determines $[f, t]$ once $[h, t]$ has been chosen; for

$$[h, t] = [ef, t] = [e, t]^f[f, t] = x^e y \qquad \text{(as in Case 2.3.1).}$$

Writing $x = a^\alpha b^\beta$, $y = a^\gamma b^\delta$, this gives

$$a^\zeta b^{-\zeta} = (a^\alpha b^\beta)^e(a^\gamma b^\delta) = a^{3\alpha}(a^2b^3)^\beta a^\gamma b^\delta = a^{-\alpha+2\beta+\gamma}b^{-\beta+\delta},$$

or equivalently, $\zeta = -\alpha + 2\beta + \gamma = \beta - \delta$.

Also, $e^2=1$ and $t^2=1 \Rightarrow [e, t]$ is inverted by e and t. Inversion by e gives α even, as in Case 2.3.1. Inversion by t gives

$$\begin{array}{c} (ha^{\alpha}b^{\beta})^t = ha^{-\alpha+2\beta}b^{-\beta+2\alpha} \\ \| \\ ha^{\zeta}b^{-\zeta}a^{\beta}b^{\alpha} = ha^{\zeta+\beta}b^{-\zeta+\alpha}, \end{array}$$

or equivalently, $-\alpha+2\beta=\zeta+\beta$, $-\beta+2\alpha=-\zeta+\alpha$, or equivalently, $-\alpha+\beta=\zeta$. So we have

(%) $$\zeta = \underset{(1)}{-\alpha+2\beta+\gamma} = \underset{(2)}{\beta-\delta} = \underset{(3)}{-\alpha+\beta}.$$

(1)=(3) gives

(%%) $$0 = \beta+\gamma;$$

(2)=(3) gives

(%%) $$0 = -\alpha+\delta.$$

Also, conjugation of T_0 by t must preserve the relations $a=[z, e]$, $b=[z, f]$. This gives

$$b = a^t = [z^t, e^t] = [z, fx] = [z, x][z, f]^x = [z, x]\,b;$$

so $[z, x]=1$, so $x \in W$. Therefore α and β are even; so by (%%), γ and δ are also even; by (%), ζ is even and

(%%%) $$\zeta = -\alpha+\beta.$$

So once $\zeta=0$ or 2 has been chosen, $\alpha=0$ or 2 determines β, γ, and δ via (%%) and (%%%).

So we get four T, all of which are split extensions of T_0 as in (xviii) (for split R) by an involution t centralizing z and having matrix $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ on A, and defined by the following four sets of relations:

(1) $\zeta=2$ and $\alpha=2$:

$$[h, t] = a^2b^2, \qquad [e, t] = ha^2, \qquad [f, t] = hb^2.$$

(2) $\zeta=2$ and $\alpha=0$:

$$[h, t] = a^2b^2, \qquad [e, t] = hb^2, \qquad [f, t] = ha^2.$$

(3) $\zeta=0$ and $\alpha=2$:

$$[h, t] = 1, \qquad [e, t] = ha^2b^2, \qquad [f, t] = ha^2b^2.$$

(4) $\zeta=0$ and $\alpha=0$:

$$[h, t] = 1, \qquad [e, t] = h, \qquad [f, t] = h.$$

These four sets of relations *do* define groups. Indeed, we will show that the four sets are equivalent (by choosing new generators), so that they all define groups if and only if one does, and the groups are isomorphic. And (4) is easily seen to define a group since the relations given between t and T_0 define an automorphism of order 2 of T_0.

The T of (4) has $\mathrm{SCN}_3(T)$ empty. For if not, T has a normal E_8, F say, containing W. $F \subseteq C_T(W) = T_0$ and projects onto precisely one nonidentity coset of A in T_0. This coset is not eA, fA, or hA because the action of z prevents any such E_8 from being normal in T. The only remaining coset of A in T_0 which contains involutions is zA. For $x \in A$,

$$(zx)^h = za^{-1}b^{-1}x^h \equiv za^{-1}b^{-1}x \mod W,$$

so that $\langle zx, W\rangle^h \neq \langle zx, W\rangle$.

We now show that (1), (2), (3), (4) are equivalent. Consider first

$$\hat{t} = tab^{-1}; \quad \hat{e} = ea^2, \hat{f} = fb^2, \hat{h} = ha^2b^2;$$
$$\hat{z} = za^2. \qquad (\hat{a} = a, \hat{b} = b.)$$

Then the restriction of $\hat{}$ to T_0 preserves the relations defining T_0. (The relations defining T_0 are of the form

$$\begin{aligned} x^\alpha &= 1 && (x \in T_0); \\ [x, y] &= z && (x, y \in T_0, z \in A); \\ ef &= h. \end{aligned}$$

The first two sorts of relations are automatically preserved by $\hat{}$, since the commutators by $\hat{}$ are central involutions of T_0 and $\hat{}$ is the identity on A; and $ef = h$ is also preserved by $\hat{}$.)

$$\begin{aligned} [\hat{z}, \hat{t}] &= [za^2, tab^{-1}] = [z, tab^{-1}]^{a^2}[a^2, tab^{-1}] \\ &= [z, ab^{-1}][z, t]^{ab^{-1}}[a^2, t] = a^2b^2[z, t]a^2b^2 \\ &= [z, t]. \\ [\hat{h}, \hat{t}] &= [ha^2b^2, tab^{-1}] = [h, tab^{-1}] = [h, ab^{-1}][h, t]^{ab^{-1}} \\ &= a^2b^2[h, t]. \\ [\hat{e}, \hat{t}] &= [ea^2, tab^{-1}] = [e, tab^{-1}]^{a^2}[a^2, tab^{-1}] \\ &= [e, ab^{-1}][e, t]^{ab^{-1}}[a^2, t] \\ &= e^{-1}(a^{-1}b)\, eab^{-1}(ab^{-1})^{-1}[e, t](ab^{-1})[a^2, t] \\ &= (a^{-1}b)^e[e, t]ab^{-1}a^2b^2 \\ &= [e, t](a^{-1}b)^f ab^{-1}a^2b^2 \quad \text{since} \quad [e, t] \in hA \quad \text{and} \quad eh = f \\ &= [e, t](ab^2b^{-1})ab^{-1}a^2b^2 \\ &= [e, t]b^2. \\ [\hat{f}, \hat{t}] &= [f, t]a^2. \end{aligned}$$

So the switch to hats gives (1) ↔ (3), (2) ↔ (4).

Consider next

$$\hat{t} = ta^2b^2; \qquad \hat{e} = ea^2, \hat{f} = fb^2, \hat{h} = ha^2b^2;$$
$$\hat{z} = z. \qquad (\hat{a} = a, \hat{b} = b.)$$

The restriction of $\hat{}$ to T_0 preserves the relations defining T_0 (as before).

$$[\hat{z}, \hat{t}] = [z, t].$$
$$[\hat{h}, \hat{t}] = [h, t].$$
$$[\hat{e}, \hat{t}] = [ea^2, ta^2b^2] = [e, t]a^2b^2.$$
$$[\hat{f}, \hat{t}] = [f, t]a^2b^2.$$

So the switch to hats gives (1) ↔ (2), (3) ↔ (4).

Therefore all four sets of relations are equivalent.

Case 2.3.3. We now work out what T has to be if $N_T(\langle g\rangle)$ is cyclic of order 4, say $\langle t\rangle$ where $t^2=z$.

(xx) In Case 2.3.3, we may assume t has the matrix $\left(\begin{smallmatrix}2&3\\1&2\end{smallmatrix}\right)$ on A.

Proof. t inverts g, where g satisfies (*), i.e., the matrix of g on A is $\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)$; and $t^2=z$; so the matrix of t is an element of $\langle\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \mathfrak{B}^+\rangle-\mathfrak{B}^+$ whose square is $\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right)$ and which inverts $\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)$. Now $\langle\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \mathfrak{B}^+\rangle-\mathfrak{B}^+$ has four elements whose square is $\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right)$, namely the elements of the coset $\left(\begin{smallmatrix}2&3\\1&2\end{smallmatrix}\right)\langle\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)\rangle$; and two of these—namely $\left(\begin{smallmatrix}2&3\\1&2\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right)\left(\begin{smallmatrix}2&3\\1&2\end{smallmatrix}\right)$—invert $\left(\begin{smallmatrix}0&1\\3&3\end{smallmatrix}\right)$. If the matrix of t is $\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right)\left(\begin{smallmatrix}2&3\\1&2\end{smallmatrix}\right)$, replace t by tz.

(xxi) In Case 2.3.3 (assuming t has the matrix $\left(\begin{smallmatrix}2&3\\1&2\end{smallmatrix}\right)$ on A), $[h, t]$ is either ab^2 or a^3.

Proof. $t^2=z$, and $[h, z]=ab$ by (xviii); so

$$ab = [h, z] = [h, t^2] = [h, t][h, t]^t.$$

Also, $[h, t] \in A$ since hA is central in T/A. Writing $[h, t]=a^\xi b^\eta$, we have

$$ab = (a^\xi b^\eta)(a^\xi b^\eta)^t = a^\xi b^\eta(a^2b^3)^\xi(ab^2)^\eta = a^{3\xi+\eta}b^{3\eta+3\xi},$$

so that ξ, η must satisfy $1=3\xi+\eta$, $1=3\xi+3\eta$. There are two solutions, namely $\eta=2$ and $\xi=1$; $\eta=0$ and $\xi=3$.

(xxii) In Case 2.3.3, R is of G. Higman type.

Proof. If R splits, then $h^2=1$ and so h inverts $[h, t]$. But this is impossible by (xxi), as h does not invert ab^2 or a^3.

So T is completely determined once we determine $[e, t]$, $[f, t]$, and $[h, t]$. $[e, t]$ and $[f, t]$ lie in hA since T/A interchanges eA and fA. Write $[e, t]=hx=ha^\alpha b^\beta$, $[f, t]=hy=ha^\gamma b^\delta$ (for $x, y \in A$).

As in the first two cases, $[e, t]$ determines $[f, t]$ once $[h, t]$ has been chosen; for $h=efa^2$, and

$$\begin{aligned}[h, t] &= [efa^2, t] = [ef, t]^{a^2}[a^2, t] = [e, t]^f[f, t]a^2b^2 \\ &= (hx)^f(hy)a^2b^2 = f^{-1}(hx)f(hy)a^2b^2 = h^2(h^{-1}f^{-1})x(fh)ya^2b^2 \\ &= h^2(x^ey)a^2b^2, \quad \text{since } fh \equiv e \text{ mod center of } R \\ &= b^2x^ey \\ &= b^2(a^\alpha b^\beta)^e(a^\gamma b^\delta) = b^2a^{-\alpha+2\beta+\gamma}b^{-\beta+\delta}.\end{aligned}$$

In summary, the relation between $[e, t]$, $[f, t]$, and $[h, t]$ is

$$(\%) \qquad [h, t] = b^2a^{-\alpha+2\beta+\gamma}b^{-\beta+\delta}.$$

Also, $t^2=z$ and $[e, z]=a^{-1}$; so

$$\begin{aligned}a^{-1} &= [e, z] = [e, t^2] = [e, t][e, t]^t = (hx)(hx)^t \\ &= (hx)h[h, t]x^t \\ &= h^2x^hx^t[h, t] \\ &= a^2(ab^2)^\alpha(a^2b)^\beta(a^2b^3)^\alpha(ab^2)^\beta[h, t];\end{aligned}$$

so that

$$(\%\%) \qquad a^{-1} = a^2a^{-\alpha-\beta}b^{\alpha-\beta}[h, t].$$

Also, $f^2=a^2b^2$; so

$$\begin{aligned}1 &= [a^2b^2, t] = [f^2, t] = [f, t]^f[f, t] = (hy)^f(hy) \\ &= f^{-1}(hy)f(hy) \\ &= h^2y^ey, \quad \text{since } fh \equiv e \text{ mod center of } R \\ &= a^2(a^\gamma b^\delta)^e(a^\gamma b^\delta) = a^2a^{3\gamma}(a^2b^3)^\delta a^\gamma b^\delta \\ &= a^2a^{2\delta}.\end{aligned}$$

Therefore δ must be odd.

We now apply (%) and (%%) with our two values for $[h, t]$. First suppose $[h, t]=ab^2$; then (%) yields

$$1 = -\alpha+2\beta+\gamma, \qquad 0 = -\beta+\delta, \quad \text{i.e.,} \; \beta = \delta.$$

Thus β is odd, so $2\beta=2$ and the first equation becomes $\gamma=\alpha-1$. (%%) yields $0=-\alpha-\beta$, $2=\alpha-\beta$, or equivalently (since β is odd), $\beta=-\alpha$. So α is odd; and α determines β, γ, and δ, hence completely determines T.

Next, suppose $[h, t]=a^3$; then (%) yields

$$-1 = -\alpha+2\beta+\gamma, \qquad 2 = -\beta+\delta, \quad \text{i.e.,} \; \beta = 2+\delta.$$

Thus β is odd, so $2\beta=2$ and the first equation becomes $\gamma=\alpha+1$. (%%) yields $2=-\alpha-\beta$, $0=\alpha-\beta$, or equivalently (since β is odd), $\beta=\alpha$. So α is odd; and α determines β, γ, and δ, hence completely determines T.

So we get four T, all of which are extensions of T_0 as in (xviii) (for nonsplitting R) by an element t with $t^2=z$, where t has matrix $\left(\begin{smallmatrix}2&3\\1&2\end{smallmatrix}\right)$ on A. The T are defined by the following four sets of relations:

(1) $[h, t]=ab^2$ and $\alpha=1$:

$$[h, t] = ab^2, \qquad [e, t] = hab^3, \qquad [f, t] = hb^3.$$

(2) $[h, t]=ab^2$ and $\alpha=3$:

$$[h, t] = ab^2, \qquad [e, t] = ha^3b, \qquad [f, t] = ha^2b.$$

(3) $[h, t]=a^3$ and $\alpha=1$:

$$[h, t] = a^3, \qquad [e, t] = hab, \qquad [f, t] = ha^2b^3.$$

(4) $[h, t]=a^3$ and $\alpha=3$:

$$[h, t] = a^3, \qquad [e, t] = ha^3b^3, \qquad [f, t] = hb.$$

These four sets of relations *do* define groups. Indeed, we will show that the four sets are equivalent (by choosing new generators), so that they all define groups if and only if one does, and the groups are isomorphic. And (4) defines a group because the relations given between t and T_0 define an automorphism of T_0 whose square is the inner automorphism induced by z.

The T of (4) has $\mathrm{SCN}_3(T)$ empty. For if not, T has a normal E_8, F say, containing W. $F\subseteq C_T(W)=T_0$ and projects onto precisely one nonidentity coset of A in T_0. The only such coset containing involutions is zA; and for $x \in A$, $\langle zx, W\rangle^h \neq \langle zx, W\rangle$ as in Case 2.3.2.

We now show that (1), (2), (3), (4) are equivalent. Consider first $\hat{t}=tab^{-1}$; $\hat{e}=ea^2$, $\hat{f}=fb^2$, $\hat{h}=ha^2b^2$. ($\hat{a}=a$, $\hat{b}=b$.) Then $\hat{z}=(t)^2=(tab^{-1})^2=za^2$. Then (as in Case 2.3.2) the restriction of $\hat{}$ to T_0 preserves the relations defining T_0.

Computing as in Case 2.3.2, we get

$$[\hat{h}, \hat{t}] = [h, t]a^2b^2.$$
$$[\hat{e}, \hat{t}] = [e, t]b^2.$$
$$[\hat{f}, \hat{t}] = [f, t]a^2.$$

So the switch to hats gives (1) ↔ (3), (2) ↔ (4).

Consider next $\hat{t}=ta^2b^2$; $\hat{e}=ea^2$, $\hat{f}=fb^2$, $\hat{h}=ha^2b^2$. ($\hat{a}=a$, $\hat{b}=b$.) Then $\hat{z}=(\hat{t})^2=(ta^2b^2)^2=z$. The restriction of $\hat{}$ to T_0 preserves the relations defining T_0. As in Case 2.3.2,

$$[\hat{h}, \hat{t}] = [h, t].$$
$$[\hat{e}, \hat{t}] = [e, t]a^2b^2.$$
$$[\hat{f}, \hat{t}] = [f, t]a^2b^2.$$

So the switch to hats gives (1) ↔ (2), (3) ↔ (4).

We will now show (by fusion arguments) that under our hypotheses, the groups T obtained in Cases 2.3.1 and 2.3.3 cannot be Sylow 2-subgroups of a simple group G. This will complete the proof of Theorem 2. We will also show that the T of Case 2.3.1 is isomorphic to the T of Case 1.1 of Theorem 1, and indeed will prove a stronger statement (Theorem 3) about this T.

THEOREM 3 (PROPOSITION 2.3.1). *Suppose T is the 2-group obtained in Case 2.3.1 of Theorem 2, namely*:

$$A = \langle a\rangle \times \langle b\rangle \cong \mathbf{Z}_4 \times \mathbf{Z}_4.$$

R is the split extension of A by a four-group $\{1, e, f, h\}$ where e, f, h have matrices $\left(\begin{smallmatrix} 3 & 0 \\ 2 & 3 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 3 & 2 \\ 0 & 3 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$ *respectively on A (with respect to the basis $\{a, b\}$ of A).*

$$T = \langle R, t\colon t^2 = 1;\ a^t = b,\ b^t = a;\ [h, t] = a^3b,\ [e, t] = hb^3,\ [f, t] = ha\rangle.$$

If G is a group with T as a Sylow 2-subgroup and $N_G(T) = TC_G(T)$, then G is not simple. (In particular, this T cannot occur under the hypotheses of Theorem 2.)

Moreover, T is isomorphic to the 2-group obtained in Case 1.1 of Theorem 1. (In particular, if G is a simple group with a Sylow 2-subgroup isomorphic to that of Case 1.1 of Theorem 1, then necessarily $[N_G(T) : C_G(T)]$ is divisible by some odd prime.)

Proof of Theorem 3. We first list the T-classes and the T-centralizers of the involutions of T, and the same for the elements of order 4.

Involutions.

$\{a^2b^2\}$; central in T.

$\{a^2, b^2\}$; $C_T(a^2) = C_T(b^2) = R$.

$eW \cup fbW$.

$fW \cup eaW$.

$hW \cup habW$. $C_T(e) = C_T(f) = C_T(h) = \langle e, f, W\rangle \cong E_{16}$.

$t\langle ab^{-1}\rangle \cup tha^2b\langle ab\rangle$; $C_T(t) = \langle t\rangle \times \langle hb, ab\rangle \cong \mathbf{Z}_2 \times Q_8$.

(teA and tfA contain no involutions since $T/A \cong D_8$ with teA and tfA of order 4.)

Elements of order 4.

abW; $C_T(ab) = \langle t, A\rangle$ of order 2^5.

$aW \cup bW$; $C_T(a) = A$ of order 2^4.

$ebW \cup fabW$; $C_T(eb) = A_1$ (see table for R/W below) of order 2^4.

$faW \cup eabW$; $C_T(fa) = A_2$ of order 2^4.

haW; $C_T(ha) = \langle A_1, tab\rangle$ of order 2^5.

hbW; $C_T(hb) = \langle A_2, t\rangle$ of order 2^5.

$tb^2\langle ab^{-1}\rangle \cup tha^2b^{-1}\langle ab\rangle$; $C_T(tb^2) = \langle tb^2\rangle \circ \langle ab, hb\rangle \cong \mathbf{Z}_4 \circ Q_8$ of order 2^4.

(teA and $tfA = (teA)^t$ contain no elements of order 4. For if $x \in A$,

$$\begin{aligned}(tex)^2 &= [t, e]x^{te}x = (hb^3)^{-1}x^{te}x \\ &= bhx^{te}x = ha^2bx^{te}x.\end{aligned}$$

Now for all $x \in A$,

$$x^{te}x \in \langle a^{te}a,\ b^{te}b\rangle \subseteq \langle ab,\ W\rangle.$$

So $ha^2bx^{te}x$ is always of order 4 since it never lies in $hW \cup habW$.

The group R/W is as follows:

$eabW$	ebW	aW	eW	eaW
faW	$fabW$	bW	fW	fbW
hbW	haW	abW	hW	$habW$
A_2	A_1	A	E	E^t.

The vertical columns are four-groups in R/W, whose inverse images in R we give the names A_1, A_2, A, E, E^t as shown. A_1, A_2, $A \cong Z_4 \times Z_4$ and are normal in T; E, $E^t \cong E_{16}$.

R contains three $Q_8 \times Z_2$'s, namely the inverse images of the horizontal boxes. R normalizes them, and in each one it acts transitively on the four Q_8's; i.e., each element x of order 4 is sheared onto each central involution w (i.e., there is y with $x^y = xw$, or equivalently, $[x, y] = w$).

Suppose G is a simple group with T as a Sylow 2-subgroup and $N_G(T) = TC_G(T)$. By Lemma A, t is fused into R in G. If t is not fused to W, then $C_T(t)$ is a Sylow 2-subgroup of $C_G(t)$, and also some conjugate of the T-centralizer of an involution of $R - A$ is a Sylow 2-subgroup of $C_G(t)$. But $C_T(t) \cong Z_2 \times Q_8$ and the T-centralizers of the involutions of $R - A$ are $\cong E_{16}$, contradicting Sylow's theorem in $C_G(t)$.

So t is fused to W in G.

There is $d \in G$ with $t^d \in W$ and $C_T(t)^d \subseteq C_T(t^d)$. For if t is fused to a^2b^2, take $d \in G$ with $t^d = a^2b^2$; T is then a Sylow 2-subgroup of $C_G(t^d)$. If t is not fused to a^2b^2, take $d \in G$ with $t^d = a^2$ (or b^2); R is then a Sylow 2-subgroup of $C_G(t^d)$. In either case, Sylow's theorem (in $C_G(t^d)$) implies that d can be adjusted by multiplication from $C_G(t^d)$ to have the property claimed.

Now $C_T(t) = \langle t\rangle \times \langle ab, hb\rangle$ has $\langle t, a^2b^2\rangle$ as its central four-group, and a^2b^2 as its square. The only involutions of T which are squares of Q_8's of T are a^2, b^2, and a^2b^2. So $(a^2b^2)^d$ and t^d are both $\in W$; therefore $Z(C_T(t)^d) = W$. This forces $C_T(t)^d$ to be one of the three $Q_8 \times Z_2$'s of R.

Therefore in $N_G(C_T(t)^d)$, each element of order 4 is sheared onto t. In particular, hb is conjugate to thb and hab^2 to $thab^2$. Now thb and $thab^2$ are T-conjugate, as are hab^2 and ha; so hb is G-conjugate to ha.

We now observe that there can be no fusion in G between hb, ha, and ab (thus we have reached a contradiction and so proved Theorem 3). For the centralizers in T of hb, ha, and ab are Sylow 2-subgroups of their centralizers in G. If (for example) hb is fused to ha, there is $d\in G$ with $(hb)^d=ha$ and $C_T(hb)^d=C_T(ha)$. $C_T(hb)$, $C_T(ha)$ contain A_2, A_1 as characteristic subgroups (e.g., because these are the only Abelian subgroups of index 2), so $A_2^d=A_1$. Therefore $N_G(A_2)^d=N_G(A_2^d)$ $=N_G(A_1)$. T^d and T are both Sylow 2-subgroups of $N_G(A_1)$ so there is $k\in N_G(A_1)$ with $A_2^{dk}=A_1$ and $T^{dk}=T$, i.e. $dk\in N_G(T)$. But $N_G(T)=TC_G(T)$, and A_2 and A_1 are not conjugate in $TC_G(T)$.

We now show that T is isomorphic to the 2-group U say obtained in Case 1.1 of Theorem 1. U was given by:

$$\begin{aligned}
W &= \langle z_1, z_2\rangle.\\
C_U(W) &= \langle W, i, j, k, x, u, v\colon \langle i, j, k\rangle \cong Q_8 \text{ with } z_1 \text{ as square, and}\\
&\qquad \langle x, u, v\rangle \cong Q_8 \text{ with } z_1z_2 \text{ as square;}\\
&\qquad [i, x] = 1, [j, x] = z_2, [k, x] = z_2\\
&\qquad [i, u] = z_2, [j, u] = 1, [k, u] = z_2\\
&\qquad [i, v] = z_2, [j, v] = z_2, [k, v] = 1.\rangle
\end{aligned}$$

(We write x instead of the t used in Theorem 1, to avoid confusion with the t of Case 2.3.1 of Theorem 2.)

$$\begin{aligned}
U = \langle C_U(W), \tau\colon \tau^t = 1;\ & z_1^\tau = z_1, z_2^\tau = z_1z_2;\\
& \tau \text{ centralizes } i, j, \text{ and } k;\\
& [x, \tau] = iz_2, [u, \tau] = jz_2, [v, \tau] = kz_2\rangle.
\end{aligned}$$

We first show $R\cong C_U(W)$. For take i, j, $k=ab$, hb, hab^2 respectively; $z_1=a^2b^2$. x, u, $v=a$, eab, eb respectively; $z_1z_2=a^2$ (so that $z_2=b^2$). Then the relations above for z_1, z_2, i, j, k, x, u, v are satisfied.

Now once we find a set $\{z_1, z_2, i, j, k, x, u, v\}$ satisfying these relations, the set $\{z_1, z_2, i, j, k, x^{-1}, u^{-1}, v^{-1}\}$ also satisfies these relations (since W is elementary and central in $C_U(W)$). Noting this, we take $\tau=t$. t centralizes i, j, and k, and acts as prescribed on W. And

$$\begin{aligned}
[a^{-1}, t] &= (ab)b^2,\\
[(eab)^{-1}, t] &= (hb)b^2,\\
[(eb)^{-1}, t] &= (hab^2)b^2,
\end{aligned}$$

i.e.,

$$\begin{aligned}
[x^{-1}, \tau] &= iz_2,\\
[u^{-1}, \tau] &= jz_2,\\
[v^{-1}, \tau] &= kz_2.
\end{aligned}$$

Thus, the generators $z_1=a^2b^2$, $z_2=b^2$; $i, j, k=ab$, hb, hab^2; x, u, $v=a^{-1}$, $(eab)^{-1}$, $(eb)^{-1}$; $\tau=t$ satisfy precisely the relations given for U.

At this point it is easy to see that T is a split extension of a $Q_8 \circ D_8$ by a four-group (which is the way in which the Sylow 2-subgroup of the Janko-Hall and Janko-Higman groups is usually described). For, using the notation for T obtained in Theorem 2, $Q=\langle ab, hb, hab^2\rangle \cong Q_8$ with a^2b^2 as square; $D=\langle t, W\rangle \cong D_8$; and $[D, Q]=1$, $D \cap Q=\langle a^2b^2\rangle$, so $DQ=D \circ Q=H$ say. It is convenient to depict H by making a table consisting of a representative for each coset of $\langle a^2b^2\rangle$ in H, as follows:

1	$\boxed{a^2}$	$\boxed{t}$	ta^2
ab	$a^{-1}b$	tab	$\boxed{tab^{-1}}$
hb	ha^2b	thb	$\boxed{tha^2b}$
hab^2	$ha^{-1}b^2$	$thab^2$	$\boxed{tha^{-1}b^2}$

where the cosets consisting of involutions are the ones in boxes. These cosets generate H.

$\langle e,f\rangle \cap H=1$; and $\langle e,f\rangle$ acts on the set $\{t, tab^{-1}, tha^2b, tha^{-1}b^2\}$ as follows:

$$h\colon t \leftrightarrow tab^{-1},\ tha^2b \leftrightarrow tha^{-1}b^2$$
$$e\colon t \leftrightarrow tha^2b,\ tab^{-1} \leftrightarrow tha^{-1}b^2$$
$$f\colon t \leftrightarrow tha^{-1}b^2,\ tab^{-1} \leftrightarrow tha^2b.$$

Thus $\langle e,f\rangle$ normalizes H, and T is as claimed.

PROPOSITION 2.3.3. *Suppose T is the 2-group obtained in Case 2.3.3 of Theorem 2, namely:*

$A=\langle a\rangle \times \langle b\rangle \cong Z_4 \times Z_4$.

$R=\langle A, e, f, h$: e, f, h have matrices $\left(\begin{smallmatrix}3 & 0\\ 2 & 3\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}3 & 2\\ 0 & 3\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1 & 2\\ 2 & 1\end{smallmatrix}\right)$ respectively on A (with respect to the basis $\{a, b\}$ of A); $e^2=b^2, f^2=a^2b^2$, $h^2=a^2$; $efa^2=h$; e, f, h centralize one another$\rangle$.

T is the split extension of R by a cyclic group $\langle t\rangle$ of order 4, where $t^2=z$ inverts A, and t has the matrix $\left(\begin{smallmatrix}2 & 3\\ 1 & 2\end{smallmatrix}\right)$ on A;

$$[e, t] = ha^3b^3, \qquad [f, t] = hb, \qquad [h, t] = a^3;$$
$$[e, z] = a^{-1}, \qquad [f, z] = b^{-1}, \qquad [h, z] = ab.$$

Suppose T is a Sylow 2-subgroup of a group G, and suppose the involutions of $W=\Omega_1(A)$ are all fused together in G. Then G is not simple.

In particular, this T cannot occur under the hypotheses of Theorem 2.

Proof of Proposition 2.3.3.

(xvii) The only cosets of A in T which contain involutions are A and zA.

Proof. T/R is cyclic, so the involutions of T lie in $T_0=\langle z, R\rangle$. The only involutions of R are those of A; and the only involutions of zR are those of zA, since for $x \in A$ and $k=e, f$, or h,

$$\begin{aligned}(zkx)^2 = (zk)^2x^{zk}x &\equiv [z, k]x^{zk}x \mod W \\ &\equiv [z, k] \mod W,\end{aligned}$$

but $[z, k] \notin W$.

(xviii) The T-classes of the elements of order 4 in T, and the orders of the T-centralizers of representatives, are:

Class	Order of T-centralizer of a representative
1. abW.	2^6
2. $aW \cup bW$.	2^5
3. $eW \cup fabW \cup eaW \cup faW$.	2^4
4. Complement of 3. in $eA \cup fA$.	2^4
5. hA.	2^4
6. $tA \cup thA$.	2^3
7. $tzA \cup tzhA$.	2^3

Proof. It helps to note that if $x \in A$ and $k=1$, e, f, or h,

$$\begin{aligned}(tkx)^2 &= (tk)^2x^{tk}x = t^2k^tkx^{tk}x \\ &= zk^tkx^{tk}x,\end{aligned}$$

which is an involution if and only if $k^tk \in A$ (by (xvii)). This occurs for $k=1$ and $k=h$. The same holds if t is replaced by $tz=t^{-1}$.

h and A conjugate together the elements of tA; $(tA)^e=thA$.

(xix) The only $Z_4 \times Z_4$'s of T lie in R.

Proof. The only elements of order 4 with centralizers of order $\geqq 16$, lie in R by (xviii).

(xx) For $y \in A$, y of order 4, the only involutions of $C_T(y)$ are those of W.

Proof. $C_T(y)$ is a union of cosets of A, but no element of zA centralizes y; statement follows from (xvii).

(xxi) If G is simple then t is fused into A.

Proof. Consider the transfer homomorphism τ: $G \to T/R$. Its value at z is

$$\tau(z) = \prod \{yzy^{-1}\text{: cosets } Ty \text{ with } Tyz = Ty\}R.$$

If no such yzy^{-1} lay in R, they would all lie in zR. Since the number of cosets Ty with $Tyz=Ty$ is odd, we would have $\tau(z)\neq 1$, contradicting simplicity of G.

Therefore z is fused into R in G. Hence there is $d \in G$ with $z^d=a^2b^2$ and $C_T(z)^d \subseteq T$.

The elements of $T-A$ whose squares are a^2b^2 are $ea^\xi b^\eta$ for η odd, and $fa^\xi b^\eta$ for

ξ even. These are all T-conjugate by (xviii). So if $t^d \in C_T(z)^d$ is not in A, we may assume $t^d = eb$.

$C_T(z) = (\langle t\rangle \times \langle a^2b^2\rangle)\langle a^2\rangle$ where a^2 shears t onto a^2b^2 (i.e., $t^{a^2} = ta^2b^2$, i.e., $[t, a^2] = a^2b^2$). So in $C_T(z)^d \subseteq T$ with $t^d = eb$, there must be involutions x, y such that x centralizes eb and $x \neq (eb)^2 = a^2b^2$, and y shears eb onto x and $y \notin \langle eb, x\rangle$. $x, y \in A \cup zA$ by (xvii).

But for $c \in A$,

$$\begin{aligned}[eb, zc] &= [eb, c][eb, z]^c \\ &= [e, c][e, z][b, z] \equiv [e, z] \mod W;\end{aligned}$$

and $[e, z] \notin W$.

So no element of zA centralizes eb. So $x \in A$, and $\langle eb, x\rangle \supseteq W$. But the same calculation shows that no element of zA can shear eb onto $x \in W$. So $y \in A$, hence $\in W \subseteq \langle eb, x\rangle$; thus there is no suitable $y \in T$.

This contradiction establishes that $t^d \in A$, as desired.

Now suppose that G is simple. By (xxi) ,there is $d \in G$ with $t^d \in A$. Write

$$V = C_T(t^d)^{d^{-1}}, \qquad V_0 = A^{d^{-1}}.$$

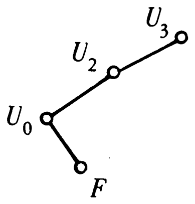
Then $V \supseteq V_0$ and $V_0 \cong \mathbf{Z}_4 \times \mathbf{Z}_4$.

Take $t^d = ab$ if possible; otherwise, take $t^d = a$ or b. Then by (xviii), V is a Sylow 2-subgroup of $C_T(t)$.

Let U be a conjugate of V by an element of $C_G(t)$ such that $U \supseteq C_T(t) = \langle t\rangle \times \langle a^2b^2\rangle = F$ say; let U_0 be the corresponding conjugate of V_0. $t \in U_0$, and also $a^2b^2 \in \Omega_1(U_0)$ by (xx). Therefore $F \subseteq U_0$; and U_0 normalizes F.

$N_T(F) = \langle F, a^2\rangle$, where a^2 shears t onto a^2b^2 (i.e., $[t, a^2] = a^2b^2$).

Let $U_2 \supseteq U_0$ be a Sylow 2-subgroup of $N_G(F)$, and let $U_3 \supseteq U_2$ be a Sylow 2-subgroup of G.



Let T^* be a suitable conjugate of U_3 by an element of $N_G(F)$ so that the corresponding conjugate U_2^* contains $N_T(F)$. Thus in T^*, t lies in a $\mathbf{Z}_4 \times \mathbf{Z}_4$ (namely, the corresponding conjugate U_0^* of U_0) which also contains $F = \langle t, a^2b^2\rangle$ with index 2; and there is an involution (namely a^2) in $T^* - \Omega_1(F) = T^* - W^*$ which shears t onto a^2b^2. ($\Omega_1(F) = \Omega_1(U_0^*) = W^*$; for U_0^* is a $\mathbf{Z}_4 \times \mathbf{Z}_4$ of T^*, so $U_0^* \subseteq R^*$ by (xix), hence $\Omega_1(U_0^*) = W^*$.)

We now observe that no element of order 4 in T^* which lies in a $\mathbf{Z}_4 \times \mathbf{Z}_4$ (Y^* say) of T^*, can be sheared by an involution of $T^* - W^*$ onto an independent involution

$\in Y^*$. (By Sylow's theorem, this is equivalent to the same statement with the stars removed.)

For by (xix), $Y \subseteq R$ and so its elements of order 4 are of the form kx for $x \in A$ and $k = 1$, e, f, or h. The only involutions of $T - W$ are zc for $c \in A$, by (xvii).

$$\begin{aligned}[kx, zc] &= [kx, c][kx, z]^c \quad \text{but } [kx, z] \in A \text{, so commutes with } c \\ &= [k, c][k, z][x, z] = [k, c][k, z]x^2.\end{aligned}$$

If k is e, f, or h, then $[k, c]$ and $x^2 \in W$ but $[k, z] \notin W$, so the commutator $[kx, zc]$ is not an involution. If $k = 1$, we have $[x, zc] = x^2$ and so our element x of order 4 is *inverted* by the involution zc—*not* sheared onto an independent involution.

This contradiction completes the proof of Proposition 2.3.3.

REFERENCES

1. J. Alperin, *Centralizers of Abelian normal subgroups of p-groups*, J. Algebra **1** (1964), 110–113. MR **29** #4800.

2. N. Blackburn, *On a special class of p-groups*, Acta Math. **100** (1958), 45–92. MR **21** #1349.

3. ———, *Generalizations of certain elementary theorems on p-groups*, Proc. London Math. Soc. (3) **11** (1961), 1–22. MR **23** #A208.

4. R. Brauer, *Some applications of the theory of blocks of characters of finite groups*. II, J. Algebra **1** (1964), 307–334. MR **30** #4836.

5. W. Feit, *Characters of finite groups*, Notes printed by Yale University, New Haven, Conn., 1965.

6. W. Feit and J. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029. MR **29** #3538.

7. G. Glauberman, *Central elements in core-free groups*, J. Algebra **4** (1966), 403–420. MR **34** #2681.

8. G. Higman, *Suzuki 2-groups*, Illinois J. Math. **7** (1963), 79–96. MR **26** #1365.

9. B. Huppert, *Endliche Gruppen*. I, Die Grundlehren der math. Wissenschaften, Band 134, Springer-Verlag, Berlin and New York, 1967. MR **37** #302.

10. J. Thompson, *Non-solvable finite groups whose nonidentity solvable subgroups have solvable normalizers* (to appear).

UNIVERSITY OF CHICAGO,
CHICAGO, ILLINOIS 60637