Illinois Journal of Mathematics
Volume 47, Number 1/2, Spring/Summer 2003, Pages 31–47
S 0019-2082

A 2-LOCAL CHARACTERIZATION OF M_{12}

MICHAEL ASCHBACHER

Dedicated to Reinhold Baer on the 100th anniversary of his birth

ABSTRACT. A characterization of the Mathieu group M_{12} is established; the characterization is used by Aschbacher and Smith in their classification of the quasithin finite simple groups.

This is one in a series of papers providing simplified, modern, computer free treatments of the existence and uniqueness of the sporadic groups, and of the normalizers of subgroups of prime order and Sylow subgroups in these groups. Such information is the minimum necessary for purposes of the Classification of Finite Simple Groups. The series also seeks to avoid appeals to references other than basic texts like [A1] and [A2], or other papers in the series which operate under the same constraints.

Here we treat the Mathieu group M_{12}. To identify M_{12} in the context of the Classification, one needs a 2-local characterization of M_{12}. The characterization given here is one chosen for the purposes of [AS], where the quasithin groups of even characteristic are classified. This is the place in the Classification where M_{12} arises. Here is our characterization:

THEOREM 1. *Let G be a finite group, z an involution in G, $H = C_G(z)$, $Q = O_2(H)$, and $X \in \mathrm{Syl}_3(H)$. Assume*

(a) *Q is extraspecial of order 32,*
(b) *$H/Q \cong S_3$ and $C_Q(X) = \langle z \rangle$, and*
(c) *z is not weakly closed in Q with respect to G.*

Then one of the following holds:

(1) *There is a normal E_8-subgroup V of G with $G/V \cong L_3(2)$.*
(2) *$G \cong A_8$ or A_9, and the two Q_8-subgroups of Q are not normal in H.*
(3) *$G \cong M_{12}$, and the two Q_8-subgroups of Q are normal in H.*

Received August 16, 2002.
2000 *Mathematics Subject Classification.* 20D05.
This work was partially supported by NSF DMS-0203417.

In [W], W. Wong characterizes M_{12} via the centralizer of a 2-central involution and the condition that G has at most two classes of involutions; of course there is also a nonsimple example arising in (1). Wong's result can also be retrieved from a theorem of Brauer and Fong in [BF] with less natural hypotheses. Both proofs are highly character-theoretic and proceed by determining the group order and appealing to a result of Stanton [S] which says M_{12} is the unique simple group of order $|M_{12}|$. Unfortunately the discussion in [S] is the barest of sketches. It appeals to a result of Brauer in [B] which shows that the character table of such a group is unique; then Stanton states without proof that using the character table, one can show that a subgroup of degree 12 exists, and that one can then use the resulting doubly transitive representation to prove the group is unique. He also appeals to the calculation of the character table by Frobenius in [F]. Finally Brauer also omits details of his calculations showing the character table is unique; see the footnote on page 67 of [B].

Our proof is character free. After some local analysis, we use the Thompson order formula to determine the group order. Then we use local analysis to construct an M_{11}-subgroup and the uniqueness of the corresponding Steiner system (cf. [A2]) to identify the group as M_{12}. Theorem 1 also gives a characterization of A_8 and A_9 which is needed in [AS].

The existence and subgroup structure of M_{12} is an easy consequence of the representation of M_{12} on its Steiner system—see, for example, Lemma 19.4 in [A2] for a construction of this Steiner system and M_{12}. For completeness, in Section 5 we show that M_{12} satisfies the hypotheses of Theorem 1, list the normalizers of subgroups of prime order and Sylow subgroups of M_{11} and M_{12}, and provide proofs that these lists are correct. This information is "well known" but it is not clear that proofs appear in the literature.

See [A1] for the definition of basic notation and terminology on finite groups.

1. Preliminary lemmas

LEMMA 1.1. *Let G be a finite group and $E \cong E_{2^n}$ be a TI-subgroup of G strongly closed in $N_G(E)$ with respect to G. Then if $G \neq N_G(E)$, $N_G(E)$ is transitive on $E^\#$.*

Proof. Assume $G \neq M = N_G(E)$ and let $e, f \in E^\#$. Then as E is a TI-subgroup of G there exists $g \in G$ with $a = e^g \notin E$. As E is strongly closed in M, $a \notin M$. If $|af|$ is even then the involution z in $X = \langle af \rangle$ centralizes a and f and $fz \in f^X \cup a^X$. Thus as $C_G(f) \leq M$ and E is strongly closed in M, $fz \in E$, so $a \in C_G(z) \leq M$, a contradiction. Thus $|af|$ is odd, so $f \in a^G = e^G$. As this holds for all $e, f \in E^\#$ and E is a TI-subgroup of G, M is transitive on $E^\#$. □

In the next lemma let G be a finite group with two classes of involutions with representatives z and t. For x an involution in G define

$$\mathcal{A}(x) = \{(u, v) \in z^G \times t^G : x \in \langle uv \rangle\}$$

and set $a(x) = |\mathcal{A}(x)|$. The Thompson Order Formula for groups with two classes of involutions says:

LEMMA 1.2 (Thompson Order Formula). $|G| = |C_G(z)|a(t) + |C_G(t)|a(z)$.

Proof. See, for example, 45.6 in [A1]. □

2. Groups of type M_{12} and A_8

In this section we consider groups satisfying the following hypothesis:

HYPOTHESIS 2.1. G is a finite group, z an involution in G, $H = C_G(z)$, $Q = O_2(H)$, $X \in \mathrm{Syl}_3(H)$, and

(a) Q is extraspecial of order 32,
(b) $H/Q \cong S_3$ and $C_Q(X) = \langle z \rangle$, and
(c) z is not weakly closed in Q with respect to G.

Thus throughout this section we assume G satisfies Hypothesis 2.1. Also set $\tilde{H} = H/\langle z \rangle$ and $H^* = H/Q$. By Hypothesis 2.1 we may choose $g \in G - H$ with $s = z^g \in Q$; set $E = Q \cap Q^g$. By a standard construction (cf. 23.10 in [A1]) we can identify $Z(Q)$ with $\mathbf{F}_2$ and regard $\tilde{Q}$ as an orthogonal space over $\mathbf{F}_2$ with bilinear form $(\tilde{x}, \tilde{y}) = [x, y]$ and $q(\tilde{x}) = x^2$; moreover $H^* \leq O(\tilde{Q})$.

LEMMA 2.2.
(1) $Q \cong Q_8^2$.
(2) $N_H(X) = X\langle z, u \rangle$ *with* $\langle u, z \rangle$ *of order 4 and* u *inverts* X.

Proof. As $C_{\tilde{Q}}(X) = 0$, the orthogonal space $\tilde{Q}$ is of maximal Witt index, so (1) holds. Further by a Frattini argument, $H = N_H(X)Q$, so $S_3 \cong H^* \cong N_H(X)/C_Q(X) = N_H(X)/\langle z \rangle$, and therefore (2) holds. □

LEMMA 2.3. *Let* P_u *be the preimage in* Q *of* $C_{\tilde{Q}}(u)$. *Then:*

(1) u *inverts* P_u *and* Q *is transitive on the set* $\tilde{u}\tilde{P}_u$ *of involutions in* $\tilde{u}\tilde{Q}$.
(2) *Either*
   (a) u *interchanges the two* Q_8*-subgroups of* Q, $P_u = C_Q(u) \cong E_8$, *and* H *has three orbits on involutions in* $Q - \{z\}$, *each of length 6, or*
   (b) u *acts on both* Q_8*-subgroups of* Q, $P_u \cong \mathbf{Z}_2 \times \mathbf{Z}_4$, *and* H *has two orbits on involutions in* $Q - \{z\}$ *of length 6 and 12.*

Proof. By 2.2(1), $Q = Q_1 * Q_2$ with $Q_i \cong Q_8$, and as $\tilde{Q}$ is an orthogonal space of maximal Witt index, $\tilde{Q}_1^\# \cup \tilde{Q}_2^\#$ is the set of nonsingular points of $\tilde{Q}$, so Q_1 and Q_2 are the unique Q_8-subgroups of Q and $Q - \{z\}$ has 18 involutions.

As $C_{\tilde{Q}}(X) = 0$ and u inverts X, $\tilde{P}_u = [\tilde{Q}, u]$ is of rank 2 and totally isotropic. So either $\tilde{P}_u$ is totally singular and $P_u \cong E_8$ or $P_u \cong \mathbf{Z}_2 \times \mathbf{Z}_4$. In either case Q is transitive on the set $\tilde{u}\tilde{P}_u$ of involutions in $\tilde{u}\tilde{Q}$ (cf. Exercise 2.8(1) in [A2]), so $|uq| = |u|$ for each $q \in P_u$, and hence u inverts q. So (1) is established.

Suppose next that $Q_1^u = Q_2$. Then $\tilde{P}_u \cap \tilde{Q}_i = 0$ for $i = 1, 2$, so $\tilde{P}_u$ is totally singular and hence $P_u \cong E_8$. As u inverts P_u, $P_u = C_Q(u)$. The members of $\tilde{P}_u^\#$ are representatives for the orbits of H on singular points of $\tilde{Q}$, and each such orbit is of length 3, so (a) holds.

So assume $Q_i^u = Q_i$ for $i = 1, 2$. Then $0 \neq C_{\tilde{Q}_i}(u)$ is nonsingular, so $\tilde{P}_u$ is not totally singular and hence $P_u \cong \mathbf{Z}_2 \times \mathbf{Z}_4$. In particular $\tilde{P}_u$ contains a unique singular point $\tilde{v}$, so v^H is the unique orbit of length 6 of H on involutions, and the other nontrivial orbit is of length 12. □

Lemma 2.3 divides our analysis into two cases: Define G to be of *type* A_8 if case (a) of 2.3(2) holds and define G to be of *type* M_{12} if case (b) of 2.3(2) holds.

Lemma 2.4.

(1) *$s^H \cap C_Q(u) \neq \varnothing$, so s^H is of order 6 and without loss we may take $s \in C_Q(u)$.*

(2) *$E \cong E_8$ and $Q^g \cap H = E\langle u \rangle \cong \mathbf{Z}_2 \times D_8$.*

(3) *u is an involution.*

(4) *$T = Q(Q^g \cap H) = Q\langle u \rangle \in \mathrm{Syl}_2(H)$.*

Proof. By 8.15 in [A2], $\Phi(E) = 1$ and $m(E) \leq 3$. On the other hand, by 8.7 in [A2], $z \in Q^g$, so $Q^g \cap H = C_{Q^g}(z) \cong \mathbf{Z}_2 \times D_8$ is of order 16, so as $|H^*|_2 = 2$, $|E| \geq 8$. We conclude $E \cong E_8$ and $T = Q(Q^g \cap H) \in \mathrm{Syl}_2(H)$. In particular we may take $u \in T$. Indeed, $Q^g \cap H - E$ contains an involution v, so by 2.3(1), we may take $\tilde{v} = \tilde{u}$. Then $\langle u, z \rangle = \langle v, z \rangle \cong E_4$, so u is an involution in $Q^g \cap H$. In particular $s \in C_Q(u)$. □

Lemma 2.5.

(1) *$E = C_G(E)$.*

(2) *If $E \trianglelefteq H$ then $M = \langle H, Q^g \rangle = N_G(E)$ and $M/E \cong L_3(2)$ acts naturally on E.*

Proof. First $C_G(E) = C_H(E) = C_Q(E) = E$, by 2.4(2) and because $C_{\tilde{Q}}(X) = 0$. Further if E is normal in H then as E is also normal in Q^g, $M \leq N_G(E)$. As $C_G(E) = E$, $N_G(E)/E \leq GL(E) \cong L_3(2)$. Then as H/E is the stablizer of the point z of E in $GL(E)$, H/E is maximal in $N_G(E)/E$, so $M = N_G(E)$ and $M/E \cong L_3(2)$. $\square$

LEMMA 2.6. *Assume G is of type A_8 and let $M = N_G(E)$. Then:*

(1) $E \trianglelefteq H$.
(2) *Every involution in H is fused into Q under M.*
(3) *Every involution in $M - E$ is conjugate to u or uz.*

Proof. First $C_Q(s) \cong \mathbf{Z}_2 \times D_8$, so there are two E_8 subgroups E and E_1 in $C_Q(s)$. Then as G is of type A_8, 2.3(2) says $P_u = E$ or E_1. But as $E\langle u\rangle \cong \mathbf{Z}_2 \times D_8$, $[u, E] \neq 1$, so $E_1 = P_u$.

Next $\langle \tilde{s}^X\rangle$ is a totally singular subspace of $\tilde{Q}$, so $\langle \tilde{s}^X\rangle = \tilde{E}$ or $\tilde{E}_1$, and as $E_1 = P_u$ is centralized by u, but $\langle \tilde{s}^X\rangle$ is not, the former holds. Therefore $H = X\langle u\rangle Q$ acts on E, so that (1) holds.

By 2.5, $M/E \cong L_3(2)$, so as $L_3(2)$ has one class of involutions, (2) holds. Similarly each involution in $M - E$ is fused into $uE \subseteq uQ$, so by 2.3(1), each such involution is conjugate to u or uz. $\square$

LEMMA 2.7. *Let G be of type M_{12}. Then:*

(1) $z^G \cap Q = \{z\} \cup s^H$ *is of order 7.*
(2) *H has three orbits on involutions of Q with representatives z, s, and t.*
(3) *H is transitive on involutions in $H - Q$.*
(4) *Every involution in H is fused into Q under $\langle H, Q^g\rangle$.*
(5) *G has two classes of involutions with representatives z and t.*

Proof. By 2.4(1), if $z \neq s \in z^G \cap Q$ then $s^H \cap C_Q(u) \neq \varnothing$, while by 2.3(2), $C_Q(u)$ contains just 3 involutions, so (1) holds. Part (2) follows from 2.3(2). By 2.3(1), each involution in $H - Q$ is conjugate to u or uz and as u inverts $P_u \cong \mathbf{Z}_2 \times \mathbf{Z}_4$, $uz \in u^{P_u}$, so (3) holds. Indeed, we may take $u \in Q^g$, so as Q^g is fused to Q in $\langle Q, Q^g\rangle$ (cf. 8.7 in [A2]), (3) implies (4). Finally (1), (2), and (4) imply (5). $\square$

LEMMA 2.8. *Assume $E^\# = z^G \cap Q$. Then:*

(1) *$G = N_G(E)$ with E the natural module for $G/E \cong L_3(2)$.*
(2) *G splits over E if and only if G is of type A_8.*

Proof. Let $M = N_G(E)$. As $E^\# = z^G \cap Q$, $E \trianglelefteq H$, so by 2.5, E is the natural module for $M/E \cong L_3(2)$. We must show $G = M$, so assume not. By hypothesis, $E^\# = z^G \cap Q$, so by 2.6(2) and 2.7(4), E is strongly closed in H with respect to G and then also strongly closed in M as H is of odd index in G. As M has more than one class of involutions, 7.6 in [A2] says M is not strongly embedded in G, so $C_G(j) \not\leq M$ for some involution $j \in T$. As $H = C_G(z) \leq M$ and M is transitive on $E^\#$, $j \notin E$.

Let $J = C_G(j)$ and $M_J = M \cap J$. Then $U = C_E(j) \cong E_4$ and U is strongly closed in $M_J = N_J(U)$ with respect to J, so by 1.1, M_J is transitive on $U^{\#}$. This is impossible as M_J is a 2-group, so (1) is established.

Suppose G is of type A_8. Then there are four X-complements to $\tilde{E}$ in $\tilde{Q}$, two of which are $\tilde{Q}_1$ and $\tilde{Q}_2$, interchanged by u, and the other three are u-invariant and totally singular. Pick one of the latter and let U denote its preimage in Q. Then $U \cong E_8$, so $U = \langle z \rangle \times [U, X]$ and $X\langle u \rangle[U, X]$ is a complement to E in H. Therefore as $|G : H|$ is odd, G splits over E by Gaschütz' Theorem (cf. 10.4 in [A1]).

On the other hand, if G is of type M_{12} then $\tilde{Q}_1$ and $\tilde{Q}_2$ are the only X-complements to $\tilde{E}$ in $\tilde{Q}$, so as $z \in \Phi(Q_i)$, G does not split over E in this case. $\square$

3. Groups of type A_8

In this section we continue to assume Hypothesis 2.1 and the notation established in Section 2. In addition we assume G is of type A_8. If $E^{\#} = z^G \cap Q$ then G is the split extension of $E \cong E_8$ by $L_3(2)$. Thus in this section we also assume $E^{\#} \neq z^G \cap Q$. Under these hypotheses, we will show G is A_8 or A_9.

Let $T = Q\langle u \rangle$. Then $T \in \mathrm{Syl}_2(H)$ and as $\langle z \rangle = Z(T)$ and $H = C_G(z)$, $T \in \mathrm{Syl}_2(G)$.

Lemma 3.1.

(1) *$A = P_u\langle u \rangle \cong E_{16}$ and $A = J(T)$.*
(2) *$|z^G \cap A| = 9$.*
(3) *$N_G(A)/A \cong \Omega_4^+(2)$ acts naturally on A.*
(4) *$Q = EF$ where $E \cap F = \langle z \rangle$, $E^{\#} \cup F^{\#} = z^G \cap Q$, $F = Q \cap Q^y$ for some $y \in G - H$, and $N_G(F)$ is the split extension of F by $L_3(2)$.*

Proof. By 2.5(2) and 2.6(1), $M = N_G(E)$ is of type A_8, so applying 2.8 to M we conclude that M is isomorphic to a parabolic of $L_4(2)$. Therefore (1) holds as it holds in $L_4(2)$. Notice also that $C_G(A) = C_H(A) = A$. Let $K = N_G(A)$; as $A = C_G(A)$, $K/A \leq GL(A) \cong L_4(2)$. As $Z(T) = \langle z \rangle$ and $T = N_H(A) = H \cap K$, $N_K(T) = T$. Then as $T/A \cong E_4$, $K = TJ$, where $J/A = O(K/A)$, by the Burnside Normal p-complement Theorem (cf. 39.1 in [A1]).

As $A = J(T)$, 7.7 in [A2] says $z^G \cap A = z^K$, so

$$|z^G \cap A| = |z^K| = |K : C_K(z)| = |K : T| = |J/A|.$$

Suppose $z^G \cap A = A^{\#}$. Then $15 = |z^G \cap A| = |J/A|$. This is impossible as the normalizer in $L_4(2) \cong A_8$ of a subgroup of order 15 contains no subgroup isomorphic to $T/A \cong E_4$.

So $z^G \cap A \neq A^\#$. On the other hand, $E^\# \neq z^G \cap Q$ by hypothesis, so there is $y \in G - H$ with $z^y \in Q - E$. Let $F = Q \cap Q^y$. By symmetry between E and F, $F \cong E_8$ and $N_G(F)$ is the split extension of F by $GL(F)$, so $F^\# \subseteq z^G$. As $E = Q \cap Q^r$ for each $z^r \in E - \langle z \rangle$, $F \cap E = \langle z \rangle$, and then by an order argument, $Q = EF$. Now either $E^\# \cup F^\# = z^G \cap Q$ and (4) holds, or by 2.3(2), all involutions in Q are in z^G. But in that case, by 2.6(2), all involutions in H are in z^G, whereas A contains involutions not conjugate to z. Hence (4) is established.

Next T has orbits u^T and $(uz)^T$ of length 4 on $A - Q$, orbits $\{1\}$ and $\{z\}$ of length 1, and 3 orbits of length 2 on $A \cap Q - \langle z \rangle$. By (4), $Q - E$ contains involutions conjugate to z and not conjugate to z, so by 2.6(3), we may take $u \in z^G$ and $uz \notin z^G$. Similarly exactly two of the orbits of length 2 are in z^G, so (2) is established. Hence J/A is of order 9, so J/A is a Sylow 3-subgroup of $GL(A) \cong L_4(2)$. Then the normalizer in $GL(A)$ of J/A is of order $36 = |K/A|$, so K/A is that normalizer, and hence (3) holds. $\square$

In the remainder of the section let A and F be the subgroups of G defined in 3.1, and set $L = \langle N_G(E), N_G(F) \rangle$.

LEMMA 3.2. $L \cong A_8$.

Proof. Let $G_0 = N_G(E)$, $G_1 = N_G(A)$, $G_2 = N_G(F)$, and $\mathcal{F} = (G_0, G_1, G_2)$. We show that $\mathcal{F}$ is an A_3-system of L, as defined in Section 4 of Appendix I of [AS]. Then the lemma follows from Theorem I.4.1 in [AS].

Let $Q_i = O_2(G_i)$ and for $J \subseteq I = \{0, 1, 2\}$, let

$$G_J = \bigcap_{j \in J} G_j.$$

By 2.5, 2.6, and 3.1(4), $G_0/Q_0 \cong G_2/Q_2 \cong L_3(2)$, while by 3.1(3), $G_1/Q_1 \cong \Omega_4^+(2)$. As $T \leq G_i$ for each i, $T \leq G_I$. Further $H = G_0 \cap G_2$ is the maximal parabolic of G_i stabilizing the point z in Q_i for $i = 0, 2$. On the other hand, by 3.1(3), $T = C_{G_1}(z)$, so $G_I = T$. Further for $i = 0, 2$, $G_{1,i} = N_{G_i}(A)$ is the maximal parabolic of G_i stabilizing the line $A \cap Q_i$ of Q_i, and hence as $G_1/Q_1 \cong \Omega_4^+(2)$, $G_{1,0}$ and $G_{1,2}$ are the two maximal parabolics of G_1. Thus we have verified conditions (D1)–(D3) of the definition of "A_3-system" in [AS]. By definition, $L = \langle \mathcal{F} \rangle$, and as G_i is irreducible on Q_i for each i, no nontrivial subgroup of T is normal in each G_i, verifying condition (D4). This completes the proof of the lemma. $\square$

PROPOSTION 3.3. *Let G be of type A_8. Then either:*

(1) *$z^G \cap Q = E^\#$ is of order 7 and G is the split extension of $E \cong E_8$ by $L_3(2)$ acting naturally on E, or*
(2) *$z^G \cap Q$ is of order 13 and $G \cong A_8$ or A_9.*

Proof. By 3.2, $L \cong A_8$, so we may assume $G \neq L$. Further we can represent L as the alternating group on $\Omega = \{1, \ldots, 8\}$ and G by right multiplication on the coset space G/L. Then L has two classes of involutions with representatives z acting without fixed points on Ω and $t = (1,2)(3,4)$, and by construction $H = C_G(z) \leq L$. Therefore the coset L is the unique point of G/L fixed by each member of z^L by 7.3 in [A2]. But by 7.6 in [A2], L is not strongly embedded in G, so $K = C_G(t) \not\leq L$.

Let $J = O^2(K))$ and $X = L_{1,2,3,4}$ be the stabilizer in L of the set of points of Ω moved by t. Then $X = O^2(C_L(t))$. As L is the unique fixed point of z on G/L, $C_L(t)$ is the unique fixed point of z on $K/(K \cap L)$, so by 7.4 in [A2], $|K : K \cap L|$ is odd and $K \cap L$ controls K-fusion of its 2-elements. Thus as $K \not\leq L$, $J \not\leq L$, and we conclude from a standard transfer result (37.5 in [A1]) that $X = J \cap L$. In particular as $|K : K \cap L|$ is odd, $O_2(X) \in \mathrm{Syl}_2(J)$, and J has one class of involutions. Now $i = (5,6)(7,8)$ is an involution in $O_2(X)$ and $it \in z^L$, so $C_G(it) \leq L$. Thus $C_J(i) = C_J(it) \leq J \cap L = X$, so $C_J(i) = O_2(X) \cong E_4$. Therefore as $J \not\leq X$, it follows from Exercise 16.6 in [A1] that $J \cong L_2(4)$. But now the centralizers and fusion pattern of involutions in G are the same as in A_9, so by the Thompson Order Formula 1.2, $|G| = |A_9| = 9|L|$. But by 8.12 in [A2] (with $U = A$) G is simple. Thus $L \cong A_8$ and the permutation representation of G on G/L is faithful, so as that representation is of degree 9 and $|G| = |A_9|$, the representation defines an isomorphism of G with A_9. □

4. Groups of type M_{12}

In this section we continue to assume Hypothesis 2.1 and the notation established in Section 2. In addition we assume G is of type M_{12} and $E^\# \neq z^G \cap Q$. Under these hypotheses, we will show G is M_{12}.

Let $T = Q\langle u \rangle$; arguing as in the previous section, $T \in \mathrm{Syl}_2(G)$. Set $V = \langle z, s \rangle$ and $M = N_G(V)$. By 2.7, G has two classes of involutions with representatives z and $t \in Q$.

Lemma 4.1.

(1) *$V^\# = z^G \cap E$, so we may take $t \in E$.*

(2) *$u \in z^G$, $tV \subseteq t^G$, and $C_M(t) = YC_Q(t)$, where Y is of order 3.*

(3) *$M = \langle Q, Q^g \rangle$ is the split extension of $R = O_2(M)$ of order 32 by $Y\langle r \rangle \cong S_3$, $r, rt \in t^G$, and $N_M(Y) = Y\langle r \rangle \times \langle t \rangle$.*

Proof. By 2.7, $z^G \cap Q = \{z\} \cup s^H$ is of order 7, so (cf. the last paragraph of the proof of 2.8) $z^G \cap Q = F^\#$, where F is the unique normal E_8-subgroup of H. By hypothesis, $E \neq F$, so $E \cap F = V$, establishing (1). Next $C_Q(s) = EF$ with all involutions in $C_Q(s)$ contained in $E \cup F$, so the involutions in $C_Q(s) - E$ are in z^G. By symmetry the set uV of involutions in $Q^g \cap H - E$ is contained in z^G, establishing the first part of (2).

Let $M_0 = \langle Q, Q^g\rangle$ and $R = C_Q(s)(Q^g \cap H)$. By 8.15 in [A2], $M = M_0C_H(V)$, so as $C_H(V) \leq Q$, $M = M_0$. Then again by 8.15 in [A2], $R = O_2(M)$, $M/R \cong S_3$, and $1 < V < E < R$ is a chief series for M with R/E and V the natural module for M/R and $[M, E] \leq V$. In particular $[t, R] = V$, so $tV = t^R$ and $|C_M(t)| = |M|/4 = 3|C_Q(t)|$, completing the proof of (2), and there exists $Y \in \mathrm{Syl}_3(M)$ with $N_M(Y) = \langle t, r\rangle Y \cong \mathbf{Z}_2 \times S_3$, where $r \in Q - R$ inverts Y. As $z^G \cap Q \subseteq R$, $r, rt \in t^G$. Hence (3) is established. $\square$

LEMMA 4.2.

(1) $C_G(t) = \langle t\rangle \times K\langle r\rangle$ *with* $V \in \mathrm{Syl}_2(K)$ *and* $z^G \cap C_G(t) \subseteq K$.

(2) *Either*

   (a) $K \cong A_4$, $\langle r\rangle K \cong S_4$, *and* $V = O_2(K)$, *or*

   (b) $K \cong A_5$ *and* $K\langle r\rangle \cong S_5$.

Proof. First $C_H(t) = C_Q(t) \cong \mathbf{Z}_2 \times D_8$ and by 4.3 in [A3], $C_Q(t) \in \mathrm{Syl}_2(C_G(t))$. Next by 4.1, $C_M(t) = C_Q(t)Y = \langle t\rangle \times VY\langle r\rangle$ with $VY\langle r\rangle \cong S_4$. Moreover by 4.1, tV and all involutions in r^{YV} and $(rt)^{YV}$ are in t^G, so $z^G \cap C_M(t) = V^{\#}$.

Let $I = C_G(t)$. Then $t^I \cap V\langle r\rangle = \varnothing$, so by Thompson transfer there is a subgroup I_0 of index 2 of I with $I = \langle t\rangle \times I_0$. We may take $r \in I_0$ and $r^I \cap V = \varnothing$, so by another application of Thompson transfer, there is a subgroup K of index 2 in I_0 with $VY = M \cap K$. Then $V = C_K(z)$, so by Exercise 16.6 in [A1], $K = YV$ or $K \cong A_5$, completing the proof. $\square$

LEMMA 4.3.

(1) *If* $K \cong A_4$ *then* $|G| = 2^6 \cdot 3^3 \cdot 7$.

(2) *If* $K \cong A_5$ *then* $|G| = |M_{12}| = 2^6 \cdot 3^3 \cdot 5 \cdot 11$.

Proof. This follows from the Thompson Order Formula 1.2, as we see soon. Adopt the notation of that lemma. Let $\bar{G} = M_{12}$. By 5.3, $\bar{G}$ is of type M_{12}, so we have corresponding elements and subgroups $\bar{z}$, $\bar{H}$ etc. in $\bar{G}$.

From 2.3 and 2.4(3), H is the split extension of Q_8^2 by S_3 with S_3 faithful on each of the Q_8-subgroups of Q, so H is determined up to isomorphism, and hence there is an isomorphism $\alpha : \bar{H} \to H$. By 2.7 and 4.1, $(\bar{x}^{\bar{G}} \cap \bar{H})\alpha = x^G \cap H$ for $x = t, z$.

Suppose $K \cong A_5$. We see in a moment that when $K \cong A_4$, $|G| \neq |M_{12}|$, so $\bar{K} \cong A_5$ by 4.2. Hence by 4.2, there is an isomorphism $\zeta : C_{\bar{G}}(\bar{t}) \to C_G(t)$ with $(\bar{x}^{\bar{G}} \cap C_{\bar{G}}(\bar{t}))\zeta = x^G \cap C_G(t)$ for $x = t, z$. Then by the Thompson Order Formula, $|\bar{G}| = |G|$, establishing (2).

Thus we may assume $K \cong A_4$. Let $(x, y) \in \mathcal{A}(z)$. By 2.3, 2.7, and 4.1, $y \in t^H$ of order 12, so $a(z) = 12a_t(z)$, where $a_t(z)$ is the number of pairs $(x, t) \in \mathcal{A}(z)$. Similarly $x \in s^H$ or u^H. If $b \in s^H$ then $z \in \langle bt\rangle$ if and only if $|bt| = 4$ and there are 4 such elements b as $|s^H \cap C_Q(t)| = 2$. Similarly if $b \in u^H$ then by 2.3, $\tilde{t} \notin C_{\tilde{Q}}(b)$, so $z \in \langle bt\rangle$ if and only if $[b, t]$ is of order 4. Equivalently

$z \notin \langle bt \rangle$ if and only if $[b, \tilde{t}]$ is singular if and only if $\langle [b,t], z\rangle = C_Q(b) = \langle s, z\rangle$ if and only if $b \in Q^g \cup Q^{gh} - E$, where $s^h = sz$. So there are 8 choices for b with $z \notin \langle bt \rangle$, and therefore, as $|u^H| = 24$, there are 16 choices for x in this case. Therefore $a_t(z) = 20$ and $a(z) = 240$.

Next let $(x, y) \in \mathcal{A}(t)$. By 4.2, $x \in z^Y$, so $a(t) = 3a_z(t)$. Finally if $y \in t^G \cap C_G(t)$ then $(z, y) \in \mathcal{A}(t)$ if and only if $y = tz$, so $a_z(t) = 1$ and $a(t) = 3$. Then by the Thompson Order Formula 1.2,

$$|G| = |H| \cdot a(t) + |C_G(t)| \cdot a(z) = 2^6 \cdot 3 \cdot 3 + 2^4 \cdot 3 \cdot 240 = 12{,}096 = 2^6 \cdot 3^3 \cdot 7.$$

□

REMARK 4.4. We wish to show $G \cong M_{12}$. To do so we first construct a subgroup S of G isomorphic to S_6. This shows that 5 divides the order of G, so by 4.3, $|G| = |M_{12}|$. Then we extend S to $N_G(S) \cong \mathrm{Aut}(A_6)$, which of course contains an M_{10}-subgroup. This M_{10}-subgroup is our candidate for the stabilizer of 2 points in a set of 12 points permuted 5-transitively by G. We extend our M_{10}-subgroup to an M_{11}-subgroup and conclude G is 5-transitive on the cosets of this subgroup, so that $G \cong M_{12}$. We begin to implement this sketch.

LEMMA 4.5. *There exists X_1 of order 3 in $C_G(X)$ inverted by z, and, replacing u by uz if necessary, centralizing u.*

Proof. By 2.2(2), $C_H(X) = X\langle z\rangle$, so by Thompson transfer, $C_G(X) = P\langle z\rangle$, where $P = O(C_G(X))$ and z inverts P/X. Also u inverts X, so u acts on P and then $P = C_P(u)C_P(uz)X$. By 4.3, 27 divides $|G|$, so 3 divides $|P/X|$, and then without loss 3 divides $|C_P(u)|$. Hence we may pick $X_1 \leq C_P(u)$ as claimed.

We observe also for later use that as $u, uz \in z^G$, $C_P(u)$ and $C_P(uz)$ are of order 1 or 3, so P is of order 9 or 27, and hence $|C_G(X)| = 18$ or 54. □

Let $A(z) = (z^G \cap Q) \cup \{1\}$. We saw during the proof of 4.1 that $A(z)$ is a subgroup of G isomorphic to E_8. Set $S = \langle A(z), A(u), X, X_1\rangle$.

LEMMA 4.6. *$S \cong S_6$.*

Proof. Let $X = \langle x\rangle$, $X_1 = \langle x_1\rangle$, $A = A(z)$, $\langle a\rangle = C_{[A,X]}(u)$, $z_1 = z$, $z_2 = x_1 z$, $z_3 = au$, $z_4 = ux$, and $z_5 = u$. Then (z_1, z_3, z_4, z_5) has Coxeter diagram $A_1 \oplus A_3$ and

$$AX\langle u\rangle = \langle z_1, z_3, z_4, z_5\rangle \cong \mathbf{Z}_2 \times S_4.$$

Next $V = C_Q(u)$ by 2.3(2), so $a = s$ or sz. By 2.3(1), $z \neq v^2$ for $v \in H - Q$. Thus taking $w \in A\langle u\rangle$ with $w^2 = a$, $w \in O_2(C_G(a)) = Q_a$. Suppose $a = s$. Then as $u \in Q^g$, $A\langle u\rangle = \langle z, w, u\rangle \leq Q^g$, which is impossible as $A \cap Q^g = A \cap E = V$. Thus $a = sz$ and as $u \in Q^g$, $az = s \in Q \cap Q_u$. Then by symmetry between z and u, $\langle su\rangle = C_{[A(u),X_1]}(z)$. Also $z_3 = au = (su)z$, so again by symmetry between z and u, (z_5, z_3, z_2, z_1) has Coxeter diagram $A_1 \oplus A_3$ and $A(u)X_1\langle z\rangle = \langle z_5, z_3, z_2, z_1\rangle$. It follows that $(S, \{z_1, \ldots, z_5\})$ is a Coxeter system of type A_5, so $S \cong S_6$. (cf. 30.19 in [A1]) □

LEMMA 4.7. *$C_G(t) \cong \mathbf{Z}_2 \times S_5$ and $|G| = |M_{12}| = 2^6 \cdot 3^3 \cdot 5 \cdot 11$.*

Proof. By 4.6, 5 divides $|G|$, so the claim follows from 4.3. □

LEMMA 4.8. *$N_G(S) \cong \mathrm{Aut}(A_6)$.*

Proof. First $C_G(S) \leq C_H(X) \leq S$, so $C_G(S) = 1$. Thus it suffices to show $S < N_G(S)$. Adopt the notation of the proof of 4.6, and as in that proof let $w \in A\langle u\rangle$ with $w^2 = a$. Now by construction of S, u and z are transpositions in S, so $C_S(z) \cong \mathbf{Z}_2 \times S_4$ is maximal in S, while from the proof of 4.6, $AX\langle u\rangle \cong \mathbf{Z}_2 \times S_4$, so $C_S(z) = AX\langle u\rangle$. Also $a \in [X, A] \leq E(S)$ and hence $s = za$ is the product of three 2-cycles and $C_S(s) = A\langle u\rangle X_s$ with X_s of order 3. Notice $A(s) = V\langle u\rangle$ and A are the two E_8-subgroups of $A\langle u\rangle$, $C_S(z) = N_H(A \cap E(S))$, and $C_S(s) = N_{H^g}(A(s) \cap E(S))$. Further $A \cap E(S) = \langle a, wu\rangle$ or $\langle a, wuz\rangle$, and replacing w by wz if necessary, we may assume it is the latter. As u and z are transpositions centralizing s and $a \in C_{E(S)}(s)$, $A(s) \cap E(S) = \langle a, uz\rangle$.

We saw $w \in Q_a$; let $P = \langle w, y\rangle$ be the Q_8-subgroup of Q_a containing w. As $z \in Q_a$ and $\langle w\rangle = C_P(z)$, $z^y = za = s$. As $u \notin Q$, $z \notin Q_u$; then as $az \in Q_u$, $a \notin Q_u$, so $u \notin Q_a$. By the choice of w, $\langle w, u\rangle \cong D_8$, so u inverts w and hence acts on P. Thus y interchanges the two 4-subgroups $\langle u, a\rangle$ and $\langle uw, a\rangle$ in $\langle u, w\rangle$, so as y interchanges s and z, it interchanges $\langle uwz, a\rangle = A(s) \cap E(S)$ and $\langle uz, a\rangle = A \cap E(S)$, and hence also $C_S(s)$ and $C_S(z)$. Therefore as $S = \langle C_S(z), C_S(s)\rangle$, y induces an outer automorphism on S, completing the proof. □

Let L be the subgroup of $N_G(S)$ isomorphic to M_{10} and $D = XX_1$.

LEMMA 4.9. *$N_G(D)$ is the split extension of $D \cong E_9$ by $GL_2(3)$, with $N_G(S) \cap N_G(D) = DP$, where P is semidihedral of order 16 and $N_L(D) = O_{3,2}(N_G(D))$.*

Proof. As $N_G(S) \cong \mathrm{Aut}(A_6)$ and $D \cong E_9$, $D \in \mathrm{Syl}_3(N_G(S))$ and $N_G(S) \cap N_G(D) = DP$ with P semidihedral of order 16. As $|G|_3 = 27$ by 4.7, a Sylow 3-subgroup B of $N_G(D)$ is of order 27. As observed at the end of the proof of 4.5, $|C_G(X)| = 18$ or 54, so $C_G(D) = D$ or B. In the former case as $\mathrm{Aut}(D) \cong GL_2(3)$, the lemma holds, so we may assume the latter. But then $B = D \times C_B(uz)$ and $\mathbf{Z}_4 \cong \Phi(P)$ centralizes $C_B(uz)$, impossible as $\langle uz\rangle C_B(uz)$ is conjugate to $X\langle z\rangle$, which centralizes no element of order 4. □

By 4.9, z inverts an element of order 3 in $N_G(D) - D$, so there is an involution $v \in N_G(D) \cap C_G(Z(P))$ with vz of order 3. Let $M = L \cup LvL$.

LEMMA 4.10. *M is a subgroup of G isomorphic to M_{11} and 4-transitive on M/L.*

Proof. We show M is a subgroup of G which is 4-transitive on M/L; then by Exercise 6.6.7 in [A2], $M \cong M_{11}$. Indeed, if M is a subgroup of G, then as $M = L \cup LvL$, M is 2-transitive on M/L and M acts on $M/L - \{L\}$ as on $L/(L \cap L^v)$. But $N_L(D) \trianglelefteq N_G(D)$ by 4.9, so $N_L(D) \leq L \cap L^v$ and then as $N_L(D)$ is maximal in L, $N_L(D) = L \cap L^v$. Therefore as L is 3-transitive on $L/N_L(D)$, M is 4-transitive on M/L, as desired.

So it remains to show M is a subgroup of G. We just saw that $L \cap L^v = N_L(D)$ and L is 3-transitive on $L/N_L(D)$, so $L = N_L(D) \cup N_L(D)rN_L(D)$, where $r \in N_L(P) - P$ is an involution. Once again adopt the notation of the proof of 4.6 and let $b = uz$, so that b inverts D and hence $\langle b \rangle = Z(P)$. Now $P \cap L \cong Q_8$, so $P \cap L \leq Q_b$ by an observation during the proof of 4.6. As $[r, P \cap L] \not\leq \langle b \rangle$, $r \notin Q_b$, but as $r \in N_G(P)$, $\langle r, P \rangle$ is a 2-group, so $rz \in Q_b$. Therefore $rQ_b = zQ_b$ so $3 = |vz|$ divides $|vr|$, and hence $|vr| = 3$ or 6. In the latter case replace r by br to get rv of order 3. Therefore $r^v = v^r$.

This is the extra ingredient necessary to show M is a subgroup of G. Namely to show M is a subgroup of G it suffices to show $l^v \in M$ for each $l \in L$. But $L = N_L(D) \cup N_L(D)rN_L(D)$ and v acts on $N_L(D)$, so it suffices to show $(xry)^v \in M$ for each $x, y \in N_L(D)$. Finally

$$(xry)^v = x^v r^v y^v = x^v v^r y^v = (x^v r)v(ry^v) \in LvL \subseteq M$$

as $x^v, y^v \in N_L(D)$ since v acts on $N_L(D)$. □

LEMMA 4.11. *$G \cong M_{12}$.*

Proof. We show $G = M \cup MzM$ with $M \cap M^z = L$. Therefore G is 2-transitive on G/M and M acts on $G/M - \{M\}$ as on M/L, so as M is 4-transitive on M/L by 4.10, G is 5-transitive on G/M. Further by 4.7, $|G : M| = |M_{12} : M_{11}| = 12$, so by Exercise 6.6.7 in [A2], $G \cong M_{12}$.

Let $G_0 = M \cup MzM$. We show G_0 is a subgroup of G and $M \cap M^z = L$. Then

$$|G_0 : M| = 1 + |M : L| = 12 = |G : M|$$

so $G = G_0$, as desired. Thus it suffices to show that G_0 is a subgroup of G and $M \cap M^z = L$.

As $z \in S \leq N_G(L)$, $L \leq M \cap M^z$, while as M is 2-transitive on M/L, L is maximal in M, so indeed $L = M \cap M^z$. As $M = L \cup LvL$, it suffices, as in the proof of the previous lemma, to show vz is of order 3. But that holds by choice of v. □

We summarize the results in this section:

PROPOSITION 4.12. *Let G be of type M_{12}. Then either:*

(1) $z^G \cap Q = E^\#$ *is of order 7 and G is the nonsplit extension of $E \cong E_8$ by $L_3(2)$ acting naturally on E.*
(2) $z^G \cap Q = F^\#$ *for some subgroup F of order 8 with $H = N_G(F)$ and $G \cong M_{12}$.*

Observe that Propositions 3.3 and 4.12 supply a proof of Theorem 1.

5. M_{12}

In this section $(X, \mathcal{C})$ is a Steiner system for $M = M_{24}$ and D is a dodecad for that system. See Chapter 6 in [A2] for the definition and a discussion of these notions. Let $G = N_M(D)$; then by 19.4 in [A2]:

LEMMA 5.1.

(1) $G = M_{12}$ *is of order* $2^6 \cdot 3^3 \cdot 5 \cdot 11$.
(2) G *is faithful and 5-transitive on* D.

LEMMA 5.2.

(1) *For $x \in D$, $G_x = M_{11}$.*
(2) *For W a 2-subset of D, $G_W \cong M_{10}$ is the nonsplit extension of A_6 by $\mathbf{Z}_2$ and $N_G(W) \cong \mathrm{Aut}(A_6)$.*
(3) *For V a 3-subset of D, G_V is the split extension of E_9 by Q_8 and $N_G(V)$ is the extension of E_9 by $GL_2(3)$ acting faithfully on $O_3(G_V)$.*

Proof. This follows from Exercise 6.6 in [A2]. □

LEMMA 5.3. *Let U be a 4-subset of D. Then:*

(1) $G_U \cong Q_8$, $N_G(U)/G_U \cong S_4$, *and* $U = \mathrm{Fix}_D(z)$ *for z the involution in G_U.*
(2) $N_G(U) = C_G(z)$ *is the split extension of $Q = O_2(C_G(z)) \cong Q_8^2$ by S_3, $C_Q(Y) = \langle z \rangle$ for $Y \in \mathrm{Syl}_3(C_G(z))$, and both Q_8-subgroups of Q are normal in $C_G(z)$.*

Proof. Let $W \subseteq V \subseteq U$ with W, V of order 2,3, respectively. By 5.1 and 5.2(2), G_W acts faithfully and 3-transitively on $D - W$ as M_{10}, so $G_U \cong Q_8$ and $\mathrm{Fix}_D(z) = U$ for z the involution in G_U. In particular z is in the center of $N_G(U)$ and $C_G(z) \leq N_G(\mathrm{Fix}(z)) = N_G(U)$, so $C_G(z) = N_G(U)$.

As G is 5-transitive on D, $N_G(U)$ is 4-transitive on U, so $N_G(U)/G_U \cong S_4$. Therefore $Q = O_2(C_G(z))$ is of order 32, $C_G(z)/Q \cong S_3$, and for $Y \in \mathrm{Syl}_2(C_G(z))$, $C_Q(Y) \leq G_U$ as the image of Y in S_4 is selfcentralizing. We may take Y to act on V, so by 5.2(3), $C_{G_U}(Y) = \langle z \rangle$, and therefore $C_Q(Y) = \langle z \rangle$.

Let $Q_1 = G_U$ and $\tilde{Q} = Q/\langle z \rangle$. As Y is irreducible on $\tilde{Q}_1$, $\tilde{Q}_1 \leq Z(\tilde{Q})$, and then as $\mathrm{Inn}(Q_1) = C_{\mathrm{Aut}(Q_1)}(\tilde{Q}_1)$, $Q = Q_1 * Q_2$, where $Q_2 = C_Q(Q_1)$. As

$C_{Q_2}(Y) = \langle z \rangle$, $Q_2 \cong Q_8$ or E_8. Finally by 5.2(2), $N_G(W) \cap C_G(Q_1) \cong \mathbf{Z}_4$, so $Q_2 \cong Q_8$, completing the proof. □

REMARK 5.4. Lemma 5.3 tells us that M_{12} is a group of type M_{12} in the sense of Section 2. This together with the order of M_{12} appearing in 5.1(1) was used in 4.3 and 4.7 to show that if $\bar{G}$ is a group of type M_{12} then either $\bar{G}$ is a nonsplit extension of E_8 by $L_3(2)$ or $|\bar{G}| = |M_{12}|$ and $\bar{G}$ has two classes of involutions with representatives $\bar{z}$ and $\bar{t}$, where $C_{\bar{G}}(\bar{z}) \cong C_G(z)$ and $C_{\bar{G}}(\bar{t}) \cong \mathbf{Z}_2 \times S_5$. We conclude:

LEMMA 5.5.
(1) *G has two classes of involutions z^G and t^G with z fixing 4 points of D and t fixed point free on D.*
(2) *$C_G(t) \cong \mathbf{Z}_2 \times S_5$.*

For by Remark 5.4, each group of type M_{12} with the same order as M_{12} has two classes of involutions with $C_G(t) \cong \mathbf{Z}_2 \times S_5$ for t a non-2-central involution. Further M_{10} has one class of involutions, so by 5.2, t has no fixed points on D.

LEMMA 5.6. *Let $P \in \mathrm{Syl}_3(G)$. Then:*
(1) *$P \cong 3^{1+2}$, $Z = Z(P)$ fixes 3 points of D, and $N_G(\mathrm{Fix}(Z))$ is the split extension of E_9 by $GL_2(3)$.*
(2) *$N_G(P)/P \cong E_4$.*
(3) *G has two classes 3A and 3B of subgroups of order 3.*
(4) *$3A = Z^G$ and for $Y \in 3B$, Y is fixed point free on D and $N_G(Y) \cong S_3 \times A_4$.*
(5) *$3A \cap P$ is of order 7.*

Proof. By 5.1, P is of order 27. Then 5.2 implies (1) and (2). Let $3\mathrm{A} = Z^G$. By 5.2, $V = \mathrm{Fix}_D(Z) \subset \mathrm{Fix}(z)$, for a suitable involution z fixing 4 points of D, z inverts $E = O_3(G_V)$, and $P = C_P(z)E$. Further $N_G(P) = P\langle z, s \rangle$, where $s \in C_G(z)$ is an an involution inducing a transposition on V, so by 5.5, $s, sz \in z^G$. Therefore $E = C_E(s) \times C_E(sz)$ with $C_P(j) \in \mathrm{Syl}_3(C_G(j))$ for $j = z, s, sz$. Then as $N_G(V)$ is transitive on subgroups of order 3 in E, all are in 3A and each is conjugate to $C_P(z)$. Therefore $N_G(P)$ has four orbits on subgroups of order 3 in P with representatives $C_E(s) = Z$, $C_E(sz)$, $C_P(z)$, and Y, and the first three subgroups are in 3A with $\langle s \rangle \in \mathrm{Syl}_2(C_G(Z))$ and $s \in z^G$. But by 5.5, a fixed point free involution $t \in G$ centralizes a subgroup of order 3, which must then be in Y^G. This establishes (3) and (5).

By 5.2, Y is fixed point free on D, so Y has four cycles of length 3. We have seen that $YZ\langle s \rangle$ is the stablizer of the cycle on V and Z is weakly closed in YZ, so Z is transitive on the remaining 3 cycles. Thus $Y\langle s \rangle$ is the kernel of the action of $N_G(Y)$ on the cycles of Y and $N_G(Y)/Y\langle s \rangle \leq S_4$. Finally we may take $t \in C_G(Y)$, so by 5.5, $N_G(Y) \cap C_G(t) \cong S_3 \times E_4$, and hence we conclude $N_G(Y) \cong S_3 \times A_4$. $\square$

LEMMA 5.7. *Let $R \in \mathrm{Syl}_5(G)$. Then $N_G(R) \cong \mathbf{Z}_2 \times F$, where F is Frobenius of order 20.*

Proof. By 5.1, R is of order 5, so by 5.5, we may take t to be a fixed point free involution centralizing R and $N_G(R) \cap C_G(t) = \langle t \rangle \times F$, where F is Frobenius of order 20. Then $|C_G(R)| = 2m$ with m odd. By 5.6, m is prime to 3, so by 5.1, $m = 5$ or 55. Therefore either $N_G(R) \leq C_G(t)$ and the lemma holds, or $|N_G(R) : R| = 88$, and the latter contradicts Sylow's Theorem. $\square$

LEMMA 5.8. *Let $S \in \mathrm{Syl}_{11}(G)$. Then $N_G(S)$ is Frobenius of order 55.*

Proof. By the previous lemmas in this section, S is selfcentralizing of order 11. Now Sylow's Theorem completes the proof. $\square$

LEMMA 5.9. *Let $A = N_M(\{D, D+X\})$. Then:*

(1) *$|A : G| = 2$ and $A = \mathrm{Aut}(G)$.*
(2) *$N_A(P)/P \cong D_8$ for $P \in \mathrm{Syl}_3(G)$.*
(3) *$C_A(O_2(C_G(z))) = \langle z \rangle$ for $z \in G$ an involution fixing 4 points of D.*
(4) *There is one class of involutions in $A - G$ and $C_G(a) \cong \mathbf{Z}_2 \times A_5$ for each involution $a \in A - G$.*

Proof. By 19.5 in [A2], $|A : G| = 2$. Let $B = \mathrm{Aut}(G)$, $P \in \mathrm{Syl}_3(G)$, $Z = Z(P)$, $V = \mathrm{Fix}_D(Z)$, and $L = N_G(V)$. By 5.6, L is the split extension of $E \cong E_9$ by $GL_2(3)$, so $L = \mathrm{Aut}(L)$ and therefore $N_B(L) = L \times K$, where $K = C_B(L)$. From the proof of 5.6, there is an involution z fixing 4 points of D inverting E; then $C_L(z)$ is a complement to E in L and $C_{\mathrm{Aut}(C_G(z))}(C_L(z)) = 1$, so K centralizes $C_G(z)$.

We next show $I = C_B(Q) = \langle z \rangle$, where $Q = O_2(C_G(z))$; this will prove $K = 1$ and hence $L = N_B(L)$. Namely from Section 2 there is a fixed point free involution $t \in Q$, and $C_Q(t) \in \mathrm{Syl}_2(C_G(t))$ with $C_G(t) \cong \mathbf{Z}_2 \times S_5$. Thus $|I : J| = 2$, where $J = C_I(C_G(t))$. But $O^2(C_G(z)) \leq C_G(J)$ and $G = \langle C_G(t), O^2(C_G(z)) \rangle$ as the latter subgroup is 5-transitive on D. Thus $J = 1$, proving (3).

We have shown $L = N_B(L)$. But by a Frattini argument, $B = GN_B(P)$ and by 5.6(5), P has just two maximal subgroups E and E_1 all of whose subgroups of order 3 are in 3A. Thus as $L = N_G(E)$, $E^b = E_1$ for $b \in N_B(P) - G$, completing the proof of (1) and (2). Further if $Y \in \mathrm{Syl}_3(C_G(z))$ then each $h \in C_A(z)$ with $h^2 \in \langle z \rangle$ is fused into $N_A(Y) \cap C_A(z)$ under $C_G(z)$, while by (2), $N_A(Y)$ has Sylow 2-groups isomorphic to D_8, so there is one class of involutions in $A - G$, and if a is such an involution in $C_A(z)$ then a Sylow 2-subgroup of $C_G(\langle a, z \rangle)$ is contained in Q, and hence $|C_G(a)|_2 \leq 8$.

Let $S \in \mathrm{Syl}_{11}(G)$. By 5.8 and a Frattini argument, we may take $a \in N_A(S)$ and then a centralizes R of order 5 acting on S. Now by 5.7, a centralizes the involution $t \in C_G(R)$, and then as R is selfcentralizing in $\mathrm{Aut}(E(C_G(t))$, a centralizes $E(C_G(t)) \cong A_5$. By 21.1 in [A2], the order of the centralizer of involutions in M_{24} is not divisible by 9 or 11, so $|\langle t\rangle E(C_G(t))| = |C_G(a)|$. Thus $C_G(a) = \langle t\rangle \times E(C_G(t)$, completing the proof of (4). □

LEMMA 5.10. *Let $x \in D$ and $G_x = M_{11}$ the stablizer in G of x. Then G_x is of order $2^4 \cdot 3^2 \cdot 5 \cdot 11$ and:*

(1) *G_x has semidihedral Sylow 2-subgroups of order 16, one class z^{G_x} of involutions, and $C_{G_x}(z) \cong GL_2(3)$.*
(2) *$P_x \in \mathrm{Syl}_3(G_x)$ is a selfcentralizing TI-set isomorphic to E_9 with $N_{G_x}(P_x)/P_x$ of order 16, so G_x has one class Z^{G_x} of subgroups of order 3 and $N_{G_x}(Z)$ is the extension of P_x by E_4.*
(3) *For $R \in \mathrm{Syl}_5(G_x)$, $N_{G_x}(R)$ is Frobenius of order 20.*
(4) *For $S \in \mathrm{Syl}_{11}(G_x)$, $N_{G_x}(S)$ is Frobenius of order 55.*
(5) *$M_{11} = \mathrm{Aut}(M_{11})$.*

Proof. Of course $|G : G_x| = |D| = 12$, giving the order of G_x. We can pick $x \in W \subseteq V \subseteq U$ as in 5.2. Then $|G_x : G_W| = |D - \{x\}| = 11$, so G_W contains a Sylow 2-subgroup of G_x and by 5.2, that Sylow group is semidihedral and G_W has one class of involutions, so G_x has one class of involutions. Pick z to be the involution in G_V; then $C_{G_x}(z) = C_G(z)_x \cong GL_2(3)$ by 5.3, so (1) holds.

Similarly picking $P \in \mathrm{Syl}_3(G)$ with $\mathrm{Fix}_D(Z(P)) = V$, $P_x = P_V \cong E_9$ with $N_{G_x}(P_x) = N_G(P_x)_x$ of order 16 and $N_G(Z(P)) \leq N_G(P_x)$ by 5.6. Then $P_x \in \mathrm{Syl}_3(G_x)$ and $N_{G_x}(P_x)$ is transitive on $P_x^{\#}$, so as $N_G(Z(P)) \leq N_G(P_x)$, P_x is a TI-set in G_x, establishing (2). Parts (3) and (4) follow from 5.7 and 5.8.

Let $A = \mathrm{Aut}(G_x)$. By a Frattini argument, $A = G_x N_A(P_x)$ and as $N_{G_x}(P_x)$ is its own automorphism group, $N_A(P_x) = N_{G_x}(P_x)B$, where $B = C_A(N_{G_x}(P_x)$. As $N_{G_x}(P_x) \cap C_{G_x}(z) \in \mathrm{Syl}_2(C_{G_x}(P_x)$, B centralizes $C_{G_x}(z)$. Finally

$$\langle C_{G_x}(z), N_{G_x}(P_x)\rangle = I$$

is 4-transitive on $D - \{x\}$, so $I = G_x$. Hence as B centralizes I, $B = 1$, so $A = G_x$. □

REFERENCES

[A1] M. Aschbacher, *Finite group theory*, Cambridge Univ. Press, Cambridge, 1986.
[A2] ———, *Sporadic groups*, Cambridge Univ. Press, Cambridge, 1994.
[A3] ———, *A characterization of ${}^2E_6(2)$*, Groups and combinatorics—in memory of Michio Suzuki, Advanced Studies in Pure Math., vol. 32, Math. Soc. Japan, Tokyo, 2001, pp. 209–244.

[AS] M. Aschbacher and S. Smith, *The classification of quasithin groups*, Mathematical Surveys and Monographs, Amer. Math. Soc., Providence, RI, to appear.

[B] R. Brauer, *On permutation groups of prime degree and related classes of groups*, Ann. Math. **44** (1943), 57–79.

[BF] R. Brauer and P. Fong, *A characterization of the Mathieu group M_{12}*, Trans. Amer. Math. Soc. **122** (1966), 18–47.

[F] G. Frobenius, *Über die Charaktere der mehrfachen transitiven Gruppen*, Sitz. Preuss. Akad. Wiss. (1904), 558–571.

[S] R. Stanton, *The Mathieu groups*, Canadian J. Math. **3** (1951), 164–174.

[W] W. Wong, *A characterization of the Mathieu group M_{12}*, Math. Z. **84** (1964), 378–388.

Department of Mathematics, Caltech, Pasadena, CA 91125, USA
E-mail address: asch@its.caltech.edu