$\mathbf{Ru} < \mathbf{E_7(5)}$ and $\mathbf{HS} < \mathbf{E_7(5)}$

P. B. Kleidman
30 West 10th Street
New York, NY 10011

U. Meierfrankenfeld
Michigan State University
East Lansing, MI 48824

A. J. E. Ryba
Marquette University
Milwaukee, WI 53233

In this paper we describe our discovery that the sporadic simple groups Ru, HS and M_{22} are contained in the simple Chevalley group $E_7(5)$.

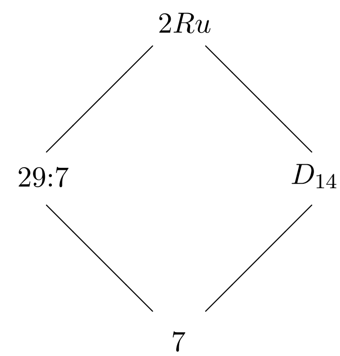
The work of [9] produces a short list of the possibilities for a sporadic simple subgroup of an exceptional group of Lie type. Apart from possible embeddings of M_{22}, HS and Ru in groups of type E_7 in characteristic 5, all of the embeddings of [9] are already known to occur. Thus our paper completes the classification of sporadic simple subgroups of exceptional groups of Lie type.

We offer two proofs of the embedding $Ru < E_7(5)$. The first is a computer proof, and the second is totally by hand. In particular, the second proof provides the only known computer-free construction of Ru. Moreover, our computer proof includes the first published presentation of Ru and thus gives the first easily verifyable computer construction of Ru. Similarly we give a hand proof and a computer proof of the embedding $HS < E_7(5)$. As a step in our hand proof of $HS < E_7(5)$ we establish the embedding $M_{22} < E_7(5)$: of course, since M_{22} is a subgroup of HS, this result also follows as a consequence of our computer proof of $HS < E_7(5)$.

We were led to conjecture the inclusions $Ru < E_7(5)$ and $HS < E_7(5)$ for the following reasons. The double cover $2.Ru$ has a faithful 28-dimensional character χ, and the character values of $\chi + \chi^*$ are all compatible with the character values of groups of type E_7 acting on their natural 56-dimensional module. Similarly the double cover $2.HS$ has a faithful 56-dimensional character, whose values are compatible with the character values of groups of type E_7 acting on their natural 56-dimensional module. Now $Ru, 2.Ru, HS$ and $2.HS$ all contain a subgroup $5^2{:}20$, an elementary abelian group of order 25 extended by a cyclic group of order 20 acting faithfully on the 5^2. Since 20 is not the order of an element in the Weyl group $W(E_7) = 2 \times S_6(2)$, it can be shown that $5^2{:}20$ does not embed in groups of type $E_7(\mathbf{K})$, where $\mathbf{K}$ is a field of characteristic prime to 5. Thus Ru and HS embed in $E_7(q)$ only if $5 \mid q$. On the other hand, all local subgroups of $2.Ru$ and $2.HS$ embed in $2.E_7(5)$, whence our conjectures $Ru < E_7(5)$ and $HS < E_7(5)$.

Throughout, G denotes the double cover $2.E_7(5)$, $\overline{G}$ denotes the simple group $E_7(5)$ and V is the natural 56-dimensional module for G over $GF(5)$. Most of our notation follows that of the ATLAS[At]. The four sections of our paper are independent and are arranged in chronological order. A later, independent, proof of $Ru < E_7(5)$ appears in [7].

Figure 1: Generating $2Ru$



1 A Computer Construction of Ru as a Subgroup of $E_7(5)$.

We used R. A. Parker's meataxe system (see [10]) to work with 56×56 matrices over $GF(5)$, representing G. Since Ru contains $2^6.G_2(2)$, where the $G_2(2)$ acts transitively on the 63 hyperplanes in the normal 2^6, it follows that any faithful representation of Ru over a field in odd characteristic has dimension at least 63. In particular Ru can not act on V and so $Ru \not\leq G$. Thus we seek to classify subgroups $2.Ru$ in G.

Any subgroup $2.Ru$ can be generated as in Figure 1. There is a unique class of groups of order 29 in G, with normalizer

$$(6 \times (29 \times 449).7).2 < (6 \times U_7(5)).2 < (2 \times U_8(5)).2.$$

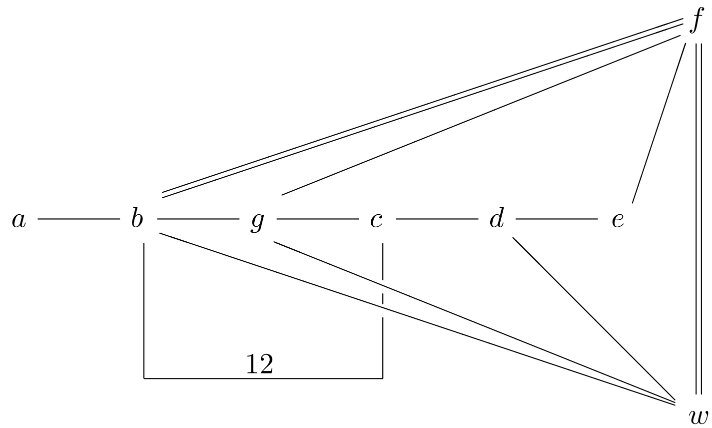
Moreover, an element of order 7 in $N_G(29)$ satisfies

$$C_G^*(7) = (SU_3(5).3 \times 7).2 \times SL_2(125).$$

(Here C^* denotes the invertilizer: that is the set of elements which either invert or centralize a given element.) An involution inverting the 7 extends $SU_3(5).3$ to $SU_3(5).Sym(3)$. There are precisely 9450 involutions in $SU_3(5).Sym(3) \setminus SU_3(5)$, and so the 7 is contained in precisely 2×9450 groups D_{14} in G. The factor of 2 comes from the involution in $SL_2(125)$, which lies in the center of G. Now G has just 3 classes of involutions, with representatives Z, X, ZX. Here $\langle Z \rangle = Z(G)$, and X and ZX have respective traces $+8$ and -8 on V. Thus we call the involutions conjugate to X and ZX plus involutions and minus involutions, respectively. Obviously the 2×9450 groups D_{14} come in pairs – one containing plus involutions, the other containing minus involutions.

Thus to classify subgroups isomorphic to $2.Ru$ in G, it suffices to check each of these 9450 plus D_{14}'s, and determine which ones together with the 29 generate $2.Ru$. On the computer, we found all 9450 such D_{14} groups, called $X_1, \ldots, X_{9450}$ say, and investigated the groups $Y_i = \langle 29, X_i \rangle$. We discarded any Y_i that contains an element with an order which is not the order of an element of $2.Ru$. Precisely 6 remained, $Y_1, \ldots, Y_6$ say. In order to identify these six groups, we use the presentation of Ru given by the following Theorem.

Figure 2: The Coxeter group X



Let X denote the Coxeter group with the Coxeter diagram given in Figure 2. (Thus X is generated by involutions a, b, c, d, e, f, g and w whose pairwise products have orders 2, 3, 4, or 12 according as the corresponding nodes of the diagram are unjoined, joined by an unmarked single edge, joined by a double edge, or joined by an edge marked 12.) Let R be the quotient of X obtained by adjoining the following additional relations: $c = g^{fed}$, $w = c^{gbag}c^{gabg}c$, $d = (bfg)^8$, $e = (bc)^6 = (abc)^4$, $(be)^d(be)^{dfbef} = db^a g^{bfabgbfg} = (ec)^{de}(ec)^{dw} = (cw)^{bcba}(cw)^{bwc} = c^{bcdewb}(db)^{wedcbcbcdewd} = 1$.

Theorem 1.1 *The group R is isomorphic to the Rudvalis group.*

Proof: Let T (respectively L) denote the group presented by those generators and relations of R that do not mention f or g, (respectively f, g, or w). Computer coset enumeration shows that the image of T in R has index 8120. Moreover, standard permutation group computations show that in the resulting permutation representation of R the images of T and L have sizes $11232 = |L_3(3){:}2|$ and $1600 \times |L_3(3){:}2| = |{}^2F_4(2)'|$. Moreover, the image of T has orbits of lengths 1, 1755 and 2304 in the permutation representation of R.

A second enumeration (of the cosets of the trivial subgroup in L) shows that $|L| = |L_3(3){:}2|$. It is routine to show that $L_3(3){:}2$ is a quotient of L, and thus the group L and its images in T and R are copies of $L_3(3){:}2$. A final coset enumeration shows that there are 1600 cosets of the image of L in T, and hence $|T| = |{}^2F_4(2)'|$. Our earlier computation of the size of the image of T in a permutation representation of R proves that the image of T in R has size $|{}^2F_4(2)'|$ and thus $|R| = 8120|T| = |Ru|$.

We now use a standard argument (see for example [17]) to show that the groups T and R must be simple. We illustrate this argument for the group T. The image of L in the permutation representation of T on the 1600 cosets of the image of L in T has orbits of sizes 1, 312, 351 and 936. In particular this faithful permutation representation of T must be primitive. Thus any minimal non-identity normal subgroup, N say, in T must be transitive on the cosets of the image of L. Moreover $N \cap L$ is isomorphic to a normal subgroup of $L_3(3){:}2$ and therefore $|N \cap L| \in \{1, |L_3(3)|, |L_3(3){:}2|\}$. We deduce that the characteristically simple group N has order 1600, $|{}^2F_4(2)'/2|$, or $|{}^2F_4(2)'|$. The classification of finite simple group shows that only the last of these orders is possible, and in particular T must be simple. Another appeal to the classification of finite simple groups gives $T \cong {}^2F_4(2)'$. A similar (slightly easier) argument now shows that R is simple and thus since the simple group Ru is characterized by its order, $R \cong Ru$. **QED**

We now apply Theorem 1.1 to identify the six subgroups $Y_1, \ldots, Y_6$ of G. For each of these groups we know generating matrices x, y, z of orders 29, 7, 2 (from the subgroups 29:7, 7 and D_{14} of Figure 1). We may assume that the element y is replaced by one of its powers so that $x^y = x^{16}$. Moreover, in each of the groups $Y_1, \ldots, Y_6$, experiment shows that we may replace x by one of its powers so that, modulo scalar matrices, xz has order 15 and xzx has order 20. (In fact there are two mutually inverse choices for x with these properties. We can make either choice of x.) We compute the following matrices in the group generated by x, y and z. Let $j = (x^3zxz)^{10}z$, $a = [z,j]^6$, $b = [z,j^2]^4$, $c = (b[z,j^3]^3)^6[z,j^3]^3$, $d = ([z,j^3]^3(ab^{j^2})^2)^2([z,j^3]^3(ab^{j^2})^2)^{z^j}$, $e = z$, $k = [a,x^4]^{(b[a,x^4]^5)^6ab}$, $l = c^{k^4}$, $f = l^{cd}l^{dc}l$, $g = c^{def}$, and $w = c^{gbag}c^{gabg}c$. Modulo scalar matrices, each of the groups $Y_1, \ldots, Y_6$ is generated by its elements a, b, c, d, e, f, g, w — since in each case the following words recover the generators x, y, z (modulo scalars): $z = e$, $m = aba(abgc)^5abg$, $y = [(mf)^{13}e(md)^{12}e(md)^{12}, e]$, $n = e[b,aw]^{(abgc)^5gc}$, $p = (ewg(abgc)^5a(abgc)^5bg(abgc)^5bawg(abgc)^5cbg)^{fw(ne^{fw})^3}$, $q = (pa)^7$, $r = (pb)^6$, $s = (pc)^{10}$, $x = (y^{-1}ps^rq^{rsqsqr})^{-2}$. Moreover, modulo scalar matrices, for each of the groups $Y_1, \ldots, Y_6$ the generators a, b, c, d, e, f, g, w satisfy the relations of R of Theorem 1.1. Therefore, $Z(G)Y_i/Z(G) \cong Ru$, for $i = 1, \ldots, 6$. Since we have already observed that Ru can not be a subgroup of G, we must have $Y_i \cong 2.Ru$ for $i = 1, \ldots, 6$.

Now $N_G(29) \cap N_G(7) \cong 12$ acts on $Y_1, \ldots, Y_6$. Furthermore, $N_{2.Ru}(29) \cap N_{2.Ru}(7) \cong 4$, and so each of $Y_1, \ldots, Y_6$ contains the subgroup of order 4 in $N_G(29) \cap N_G(7)$. Moreover, the group of order 3 in $N_G(29) \cap N_G(7)$ cannot normalize one of $Y_1, \ldots, Y_6$, for this group of order 3 centralizes the 29 (in G) and yet there is no group of order 3 in the 29−centralizer of $2.Ru$. Thus $N_G(29) \cap N_G(7)$ has two orbits of size 3 on $Y_1, \ldots, Y_6$. Now $2.Ru$ contains a unique class of 29:7, and we have

$$C^*_{2.Ru}(7) = Q_8 \times D_{14} \leq Q_8 \times Sz(8).$$

Thus the 7 is contained in precisely two groups D_{14}. Consequently each $2.Ru$ in G can be generated in just two ways as in (*), one way with a plus D_{14} and the other with the minus D_{14}. We have therefore proved that there are just two classes of $2.Ru$ in G.

Therefore, there are just two classes of subgroup isomorphic to Ru in $\overline{G}$. The non-abelian composition factors of centralizers of involutions in $\mathrm{Aut}(\overline{G})$ are $L_2(5)$, $O^+_{12}(5)$, $L_8(5)$, $U_8(5)$, $E_6(5)$, and ${}^2E_6(5)$, none of which contain Ru. Consequently the outer automorphism of $\overline{G}$ must interchange the two classes of Ru in $\overline{G}$.

We have now proved assertions (A) and (B), as well as part of (D), in the Theorem below. Our construction gives an explicit matrix action of $2.Ru$ on the natural 56-dimensional $GF(5)$-module for $2.E_7(5)$ and a standard application of the meataxe (see [10]) provides the decomposition of this module given in (D). The 133−dimensional adjoint module for the Lie algebra associated with $E_7(5)$ is a constituent of the symmetric square of the 56-dimensional module. We used the meataxe to determine that 133 is the smallest degree of a non-trivial constituent of the action of Ru on the symmetric square of the $56-$dimensional module. (The $56-$dimensional module has two irreducible $28-$dimensional constituents, thus we analyzed the two $406-$dimensional modules obtained as symmetric squares of $28-$dimensional representations, and the $784-$dimensional tensor product of the two $28-$dimensional representations. The last of these computations is close to the size limit for our implementation of the Meataxe.) The statements in (C) follow.

Theorem 1.2 *(A) The simple Chevalley group $E_7(5)$ contains precisely two classes of subgroups isomorphic to Ru.*

(B) The outer automorphism of $E_7(5)$ fuses the two classes.

(C) Each subgroup Ru acts irreducibly on the 133-dimensional Lie algebra associated with $E_7(5)$.

(D) In the double cover $2.E_7(5)$, each Ru lifts to $2.Ru$, and acts indecomposably with two irreducible constituents of dimension 28 on the natural 56-dimensional $GF(5)$-module for $2.E_7(5)$.

2 A Computer-free Construction of the Rudvalis Group as a Subgroup of $E_7(5)$.

In this chapter we will give a computer-free proof of the following Theorem.

Theorem 2.1 *Suppose that $E_6(5)$ has a subgroup ${}^2F_4(2)$ which acts irreducibly on the 27-dimensional $GF(5)E_6(5)$-modules, then $E_7(5)$ has a subgroup isomorphic to the Rudvalis group.*

We remark that an unpublished paper of M. Aschbacher on the maximal subgroups of E_6 contains a computer free proof that $E_6(5)$ indeed has a subgroup isomorphic to ${}^2F_4(2)$ which acts irreducibly on the $27-$spaces for $E_6(5)$.

Lemma 2.2 *Let X be a 2-dimensional vector space over $GF(5)$, S a Sylow 2-subgroup of $GL(X)$, A the unique subgroup of S isomorphic to $C_4 \times C_4$, ϕ an automorphism of S such that $X^\phi \cong X^*$, the dual module of X. Then ϕs inverts A for some s in S.*

Proof: Note first that there exist 1-dimensional subspaces X_1, X_2 of X with $X = X_1 \oplus X_2$, $S = N_{GL(X)}(\{X_1, X_2\})$ and $A = N_{GL(X)}(X_1) \cap N_{GL(X)}(X_2)$. Let ψ be the automorphism of A given by inversion. Then X^* and X^ψ are isomorphic as $A-$modules. Hence also X^ϕ and X^ψ are isomorphic as $A-$modules and there exists $s \in N_{GL(X)}(A))$ such that ϕs and ψ agree on A. Since $N_{GL(X)}(A) = S$, $s \in S$ and the lemma is proved. **QED**

Let E be the parabolic subgroup of G such that $E = QL$ with $Q = O_5(E)$, $|Q| = 5^{27}$ and $L \cong C_4 \times E_6(5)$. By assumption, L has ${}^2F_4(2)$ as a subgroup. But it can be proved that such a ${}^2F_4(2)$ cannot be extended to a $2.Ru$ in G. Instead we will look for a different class of complements with respect to Q. For this we first have to study the action of ${}^2F_4(2)$ on its 27-dimensional irreducible module over $GF(5)$.

Let F be a group with ${}^2F_4(2)' \leq F \leq C_4 \times {}^2F_4(2)$. Let S be a Sylow 2-subgroup of F and let P_1 and P_2 be the two maximal subgroups of F containing S, ordered so that $Z(P_1/Z(F)) \neq 1$. Let Γ_0 be the coset-graph of F with respect to P_1 and P_2. Then Γ_0 is the generalized octagon associated with ${}^2F_4(2)$. For $\gamma \in \Gamma_0$, let $\triangle^k(\gamma)$ be the set of vertices in Γ_0 at distance exactly k from γ. Further put $\alpha = P_1$ and $\beta = P_2$ and note that α and β are vertices of Γ_0. Put $T = F', L_i = P_i \cap T,\ Q_i = O_2(L_i),\ Z_i = Z(Q_i)$ and $V_1 = \langle {Z_2}^{P_1} \rangle$. Let $1 \neq z_1 \in Z_1$. If P_i normalizes a subgroup R_i in F or in some $F-$module, and if $\delta = P_i g \in \Gamma_0$, put $R_\delta = R_i^g$.

We assume that the reader is familiar with the structures of P_1, P_2 and S (see for example [11] or [5]). We remark here that $|S \cap T| = 2^{11}$, L_1/Q_1 is a Frobenius group of order 20, Z_1 has order 2, V_1/Z_1 is the unique irreducible L_1/Q_1 module of order 16, V_1 is elementary abelian, $L_2/Q_2 \cong Sym(3)$ and Z_2 is the unique irreducible L_2/Q_2-module of order 4.

We pay special attention to groups F such that

$$F/Z(F) \cong {}^2F_4(2),\ |Z(F)| = 2,\ F' \cong ({}^2F_4(2))' \quad \text{and} \quad F/F' \cong C_4. \tag{+}$$

Lemma 2.3 *Let W be a faithful irreducible 27−dimensional $GF(5)F$-module.*

(a) Let $U_1 = C_W(V_1)$.

(aa) $W = C_W(V_1) \oplus [C_W(Z_1), V_1] \oplus [W, Z_1]$,

(ab) $[C_W(Z_1), V_1] = \bigoplus_{\gamma \in \triangle^2(\alpha)} U_\gamma$,

(ac) $[W, Z_1] = \sum_{\gamma \in \triangle^4(\alpha)} U_\gamma = \bigoplus_{\gamma \in \triangle^3(\beta) \setminus \triangle^2(\alpha)} U_\gamma$,

(ad) $U_1 = C_W(V_1)$ is 1-dimensional, $C_W(V_1) = C_W(Q_1)$, $P_1/C_{P_1}(U_1) \cong C_4$ and U_1 is not isomorphic to its dual $GF(5)P_1$ module,

(ae) $[C_W(Z_1), V_1]$ is irreducible of dimension 10 and if ϕ is any automorphism of P_1, then $[C_W(Z_1), V_1]^\phi$ and the dual of $[C_W(Z_1), V_1]$ are not isomorphic as $GF(5)P_1-$modules,

(af) $[W, Z_1]$ is irreducible of dimension 16. If (+) holds $[W, Z_1]$ is isomorphic to its dual $GF(5)P_1-$module.

(b)

(ba) $W = C_W(Z_2) \bigoplus [W, Z_2]$.

(bb) $[W, Z_2] = \bigoplus_{\gamma \in \triangle^3(\beta)} U_\gamma$,

(bc) $C_W(Z_2) = \bigoplus_{\gamma \in \triangle^1(\beta)} U_\gamma$,

(bd) $[W, Z_2]$ is irreducible of dimension 24. If (+) holds $[W, Z_2]$ is isomorphic to its dual $GF(5)P_2-$module,

(be) $C_W(Z_2)$ is irreducible of dimension 3 and not isomorphic to its dual $GF(5)P_2$ module.

(c) Let $X \leq Y$ be $GF(5)P_1-$modules such that Y and Y/X are isomorphic to $[W, Z_1]$ as P_1-modules. Then Y splits over X.

(d) F' has two classes of involutions. If z_1 and i are representatives of these classes then $C_W(z_1)$ is 11-dimensional while $C_W(i)$ is 15-dimensional. Moreover, $|C_F(i)| = 2^{11} \cdot 3$.

(e) F has a unique class of elements d of order three such that $C_{F'}(d)$ has even order. Moreover, for any such d and any $t \in C_{F'}(d)$ with $|t| = 2$, we have $N_{F'}(D) \cap C_{F'}(t) \cong D_{24}$. If (+) holds then $|C_F(d)| = 2^5 \cdot 3^3$

(f) Let d be an element of order five in F. Then $C_F(d)$ is a $\{2, 5\}-$group.

Proof: (aa) and (ba) follow from the fact that V_1, Z_2 and Z_1 are $2-$groups and so coprime action applies.

Let $R_1 = [W, Z_1]$ and $\Sigma = \{H \leq V_1 \mid V_1 = Z_1 \oplus H\}$. Note that Q_1 and P_1 act transitively on Σ. By co-prime action

$$R_1 = \oplus_{H \in \Sigma} C_{R_1}(H).$$

It follows that $\dim R_1$ is a multiple of 16. Since $\dim W = 27$ we conclude that $\dim R_1 = 16$, hence $\dim C_{R_1}(H) = 1$ and thus Q_1 acts irreducibly on R_1. In particular the first half of (af) holds. Let $\gamma \in \triangle(\beta)$ with $\gamma \neq \alpha$. Since there exist exactly 8 elements of Σ containing Z_γ, we have $\dim C_{R_1}(Z_\gamma) = 8$. Further, $\dim C_W(Z_\gamma) = \dim C_W(Z_1) = 27 - 16 = 11$ and so

$$\dim C_W(Z_2) = \dim(C_W(Z_1) \cap C_W(Z_\gamma)) = 11 - 8 = 3.$$

Let $\Sigma_1 = \{H \leq V_1 \mid Z_1 \leq H, |V_1/H| = 2\}$ and $Y_1 = [C_W(Z_1), V_1]$. Then

$$Y_1 = \bigoplus_{H \in \Sigma_1} C_{Y_1}(H).$$

Note that P_1 has two orbits Σ_2 and Σ_3 on Σ_1 of lengths 5 and 10, respectively. So the dimension of Y_1 is a multiple of 5. Since $\dim [Y_1, Z_\gamma] = \dim [C_W(Z_1), Z_\gamma] = \dim [C_W(Z_\gamma), Z_1] = \dim C_{R_1}(Z_\gamma) = 8$ and $\dim C_W(Z_1) = 11$, we get $\dim Y_1 = 10$. Suppose that $C_{Y_1}(H) \neq 0$ for $H \in \Sigma_3$. Since Z_γ lies in exactly one member of Σ_2, the group Z_γ lies in exactly 6 members of Σ_3 and thus $C_{Y_1}(Z_\gamma)$ is 6-dimensional, a contradiction to $\dim C_{Y_1}(Z_\gamma) = 10 - 8 = 2$. So

$$Y_1 = \bigoplus_{H \in \Sigma_2} C_{Y_1}(H) \text{ and } \dim C_{Y_1}(H) = 2 \text{ for } H \in Z_2.$$

Recall that $U_1 = C_W(V_1)$. Then $C_W(Z_1) = U_1 \oplus Y_1$ and hence $\dim U_1 = 11 - 10 = 1$.

As W is irreducible, $U_1 \neq U_\gamma$, and so we have $[U_\gamma, V_1] \neq 1$. Observe that $C_{L_\gamma}(U_\gamma) \geq O^2(L_\gamma)$ (since L_γ acts as a subgroup of $GL_1(5) \cong C_4$ on U_γ). However, $V_1 \leq C_T(Z_\gamma) = L_\gamma$, and V_1 does not centralize U_γ. As $V_1 O^2(L_\gamma)/O^2(L_\gamma) \cong C_2$ is the unique proper subgroup of $L_\gamma/O^2(L_\gamma) \cong C_4$ we deduce that $C_T(U_\gamma) = C_{L_\gamma}(U_\gamma) = O^2(L_\gamma)$, thus $L_\gamma/C_{L_\gamma}(U_\gamma) \cong C_4 \cong P_\gamma/C_{P_\gamma}(U_\gamma)$ and hence U_1 is not self-dual as a $GF(5)P_1-$module.

Since V_1 inverts U_γ and Z_1 centralizes U_γ, U_γ lies in Y_1. Moreover, since $V_1 \leq L_\gamma$, the group V_1 acts on U_γ, thus $C_{V_1}(U_\gamma)$ is the hyperplane in Σ_2 that contains Z_γ. Now $C_{V_1}(U_\gamma) = V_1 \cap O^2(L_\gamma) = V_1 \cap Q_\gamma$. Moreover the single hyperplane of Σ_2 that contains Z_γ also contains

$Z_\gamma Z_1 = Z_\beta$ and so also contains $Z_{\gamma'}$, where $\triangle^1(\beta) = \{\alpha, \gamma, \gamma'\}$. Hence $V_1 \cap Q_\gamma = V_1 \cap Q_{\gamma'}$, and $\Sigma_2 = \{V_1 \cap Q_\delta \mid \delta \in \triangle^2(\alpha)\}$. So $C_{Y_1}(V_1 \cap Q_\gamma) = U_\gamma + U_{\gamma'}$, and

$$Y_1 = \bigoplus_{\delta \in \triangle^2(\alpha)} U_\delta.$$

In particular (ab) holds. Now $C_T(U_\gamma + U_{\gamma'}) = O^2(L_\gamma) \cap O^2(L_{\gamma'}) = Q_\gamma \cap Q_{\gamma'}$ and $|S \cap T/Q_\gamma \cap Q_{\gamma'}| = 32$. Since a Sylow $2-$subgroup of $GL_2(5)$ has order 32 and is isomorphic to C_4 wreath C_2 we conclude that $S \cap T/Q_\gamma \cap Q_{\gamma'} \cong C_4$ wreath C_2, that $S = (S \cap T)\, C_S\, (U_\gamma + U_{\gamma'})$ and that the action of S on $U_\gamma + U_{\gamma'}$ is irreducible, but not self-dual. Thus Y_1 is irreducible of dimension 10. Suppose there exists an automorphism ϕ of P_1 so that $[C_W(Z_1), V_1]^\phi$ is isomorphic to the dual module of $[C_W(Z_1), V_1]$. As $Frob_{20}$ has no outer automorphisms, we may assume without loss that ϕ centralizes $P_1/O_2(P_1)$. Then $(U_\gamma + U_{\gamma'})^\phi$ is isomorphic, as an $S-$module, to the dual module of $U_\gamma + U_{\gamma'}$. In particular, ϕ normalizes $C_S(U_\gamma + U_{\gamma'})$. Now $O_2(P_2)/C_S(U_\gamma + U_{\gamma'})$ is the unique subgroup of $S/C_S(U_\gamma + U_{\gamma'})$ isomorphic to $C_4 \times C_4$ and so by Lemma 2.2, up to an inner automorphism of S, the automorphism ϕ inverts $O_2(P_2)/C_S(U_\gamma + U_{\gamma'}))$. As $O_2(P_2)O_2(P_1) = S$ and $C_S(U_\gamma + U_{\gamma'}) \le O_2(P_1)$ we conclude that ϕ inverts $S/O_2(P_1) \cong C_4$, a contradiction to $[P_1, \phi] \le O_2(P_1)$. Thus no such ϕ exists and (ad) is proved.

Let $U_2 = C_W(Z_2)$. Then

$$U_2 = U_\alpha + U_\gamma + U_{\gamma'}.$$

and so (bc) holds. For $X \le P_2$, let $\tilde{X} = XC_{P_2}(U_2)/C_{P_2}(U_2)$. As $C_{L_2}(U_\alpha) = O^2(L_1) \cap L_2 = Q_1 = \bigcap_{\rho \in \triangle^1(\alpha)} L_\rho$, we have $C_{L_2}(U_2) = \bigcap_{\rho \in \triangle^2(\beta)} L_\rho$ and so by [5, 9.4.3]

$$\tilde{L_2} \cong (C_4 \times C_4).Sym(3)$$

In particular, (be) holds.

We will now determine $\tilde{P_2}$, which does depend on the precise structure of F. Since, by assumption, F is irreducible on W and since $C_W(Q_1)$ is $1-$dimensional, F acts absolutely irreducibly on W. Hence all elements of $Z(F)$ act as scalars on W and so also on U_2. Now no element of $\tilde{L_2}$ acts as a scalar and so $\tilde{Z(F)}\tilde{L_2} \cong Z(F) \times \tilde{L_2}$. As the full monomial subgroup of $GL(U_2)$ is isomorphic to $C_4 \times \tilde{L_2}$ we see that at least one of the following holds

- $Z(F) = 1$ and $\tilde{P_2} \cong (C_4 \times C_4).Sym(3)$
- $|Z(F)| \le 2$, $F \cong Z(F) \times {}^2F_4(2)$ and $\tilde{P_2} \cong C_2 \times (C_4 \times C_4).Sym(3)$
- $F/F' \cong C_4$ or $C_2 \times C_4$ and $\tilde{P_2} \cong C_4 \wr Sym(3)$

We remark that $\tilde{P_2}$ is uniquely determined by the structure of F except when $F \cong {}^2F_4(2)$. In this case its easy to see that F has two different irreducible $27-$dimensional representations giving rise to the two different possibilities for $\tilde{P_2}$.

Note that Q_1 is a normal subgroup of S generated by involutions. Furthermore we have $C_{S \cap T}(U_\gamma + U_{\gamma'}) \le Q_1$ and so $Q_1/C_{Q_1}(U_\gamma + U_{\gamma'})$ has order eight. Hence by the structure of $C_4 \wr C_2$, Q_1 acts as a D_8 on $U_\gamma + U_{\gamma'}$. In particular $O_2(P_1)$ acts irreducibly on $U_\gamma + U_{\gamma'}$.

Suppose in this paragraph that (+) holds. We wish to show that $U_\gamma + U_{\gamma'}$ is self–dual as an $O_2(P_1)-$module. Let B be the set of elements in P_2 that act as scalars on U_2, let $C = C_{P_2}(U_\gamma + U_{\gamma'})$, let $D = O_2(P_1) \cap O_2(P_2)$ and let $E = [O_2(P_2), S]$. As B is normal in P_2 with $O_2(P_2)/B \cong C_4 \times C_4$, [5, 9.4.3] implies $B \not\leq O_2(P_1)$ and so $B \not\leq D$. On the other hand, by the structure of $\tilde{S}$, there are exactly two subgroups $\tilde{X}$ of $\widetilde{O_2(P_2)}$ such that $\widetilde{Z(F)}\tilde{E} \leq \tilde{X}$ and $\widetilde{O_2(P_2)}/\tilde{X} \cong C_4$, namely $\tilde{C}\tilde{E}$ and $\tilde{B}\tilde{E}$. Since $S/O_2(P_1) \cong C_4$, the group $\tilde{D}$ meets the conditions on $\tilde{X}$ and so $\tilde{D} = \tilde{C}\tilde{E}$ and $D = CE$. But $E \leq Q_1 \cap Q_2$ and thus $D = C(Q_1 \cap Q_2)$. Since $O_2(P_1) = Q_1 D$ we conclude that $O_2(P_1) = CQ_1$. In particular, $O_2(P_1)$ acts as a D_8 and so self–dually on $U_\gamma + U_{\gamma'}$.

Back to the general case. Recall (ab) and put $Y_2 = \bigoplus_{\delta \in \triangle^2(\alpha) \setminus \triangle^1(\beta)} U_\delta$. Let $g \in L_1 \setminus L_2$. Then $P_2^g \cap S = O_2(P_1)$. Further $(U_\gamma + U_{\gamma'})^g$ is a Wedderburn component for $O_2(P_1)$ on Y_2 (and is self–dual if (+) holds). It follows that the $S-$module Y_2 is isomorphic to the $S-$module induced from the $O_2(P_1)-$module $(U_\gamma + U_{\gamma'})^g$ and is irreducible (and is self dual if (+) holds).

Pick $\delta \in \triangle^4(\alpha)$. By [5, 7.4,7.5], $Z_1 \leq L_\delta$ and $Z_1 \not\leq Q_\delta$. So Z_1 inverts U_δ and $U_\delta \leq [W, Z_1]$. As seen above Q_1 acts irreducibly on $R_1 = [W, Z_1]$. Further, Q_1 acts transitively on the subset $\triangle^3(\beta) \setminus \triangle^2(\alpha)$ of $\triangle^4(\alpha)$, $\dim[W, Z_1] = 16$ and $| \triangle^3(\beta) \setminus \triangle^2(\alpha)| = 16$. So

$$R_1 = [W, Z_1] = \bigoplus_{\delta \in \triangle^3(\beta) \setminus \triangle^2(\alpha)} U_\delta = \sum_{\delta \in \triangle^4(\alpha)} U_\delta.$$

Let $R_2 = [W, Z_2]$. From its definition, Y_2 is 8−dimensional and from our earlier calculation of $\dim[W, Z_2]$, the space $C_{[W,Z_2]}(Z_1)$ is 8−dimensional. Hence $Y_2 = [C_W(Z_1), Z_2] = C_{[W,Z_2]}(Z_1)$. So by coprime action, $R_2 = \bigoplus_{\delta \in \triangle^1(\beta)} C_{R_2}(Z_d) = Y_2 \oplus {Y_2}^d \oplus {Y_2}^{d^2}$, where d is an element of order 3 in L_2. It follows that

$$R_2 = \bigoplus_{\delta \in \triangle^3(\beta)} U_\delta.$$

Moreover, as Y_2 is irreducible (and self-dual if (+) holds) as an $S-$module, R_2 is irreducible (and self-dual if (+) holds) as a P_2-module. In particular, (bb) and (bd) hold.

So to complete the proof of (a) and (b), it remains to show that R_1 is self-dual as a P_1-module if (+) holds. Pick $H \in \Sigma$. Then $O^2(N_{P_1}(H))$ centralizes $C_{R_1}(H)$. As R_2 is self-dual as a P_2-module, S acts self-dually on R_2 and on R_1. This implies that $N_{P_1}(H) = SO^2(N_{P_1}(H))$ acts self-dually on $C_{R_1}(H)$. Since $R_1 = \bigoplus_{H \in \Sigma} C_{R_1}(H)$, the group P_1 is self-dual on R_1 and (a) and (b) are proved.

To prove (c) let $H \in \Sigma$. Then Y (respectively X) is induced from the 2 (1)-dimensional $N_{P_1}(H)$ module $C_Y(H)$, $(C_X(H))$. As Q_1 acts transitively on Σ, we have $N_{P_1}(H)Q_1 = P_1$. Thus $N_{P_1}(H)/O_2(N_{P_1}(H)) \cong Frob_{20}$ and $N_{P_1}(H)$ is generated by its 2-elements. Since $C_X(H)$ and $C_Y(H)/C_X(H)$ are isomorphic as $N_{P_1}(H)-$modules, all the 2−elements and so all the elements of $N_{P_1}(H)$ act as scalars on $C_Y(H)$. Hence $C_Y(H)$ splits over $C_X(H)$ and so also Y splits over X.

That F' has two classes of involutions is well known (see for example [3]). Clearly $C_W(z_1)$ is 11-dimensional. We can choose $i \in V_1$. Namely, choose $i \in V_1$ but $i \notin Z_\delta$ for $\delta \in \triangle^1(\alpha)$. Then i centralizes U_1, moreover i lies in exactly three elements of Σ_2 and in eight elements of Σ. Hence $\dim C_W(i) = 1 + 2 \cdot 3 + 8 = 15$ and so (d) holds.

(e) and (f) are well known and are easily deduced from [3]. **QED**

Lemma 2.4 *Let $K = D_8 \wr Sym(5)$ and let t be an automorphism of order 2 which centralizes $K/O_2(K)$ but not $O_2(K)/Z(O_2(K))$. Let A be a non-abelian subgroup of $O_2(O^2(K))$ such that $|N_K(A)|$ is divisible by five and $Z(K) \not\leq A$. Then $|A| = 2^8$, $N_{K\langle t\rangle}(A)/A \sim D_8.Frob_{20}$ and $N_{K\langle t\rangle}(A)$ induces an outer automorphism on $O_2(N_{K\langle t\rangle}(A))/A$.*

Proof: Let x be an element of order five in K normalizing A. Put $X = \langle x\rangle$, $I = O_2(O^2(K))$ and $J = [Z(I), K]$. Then $I/Z(K)$ has order 2^{12}, the group X acts fixed point freely on $I/Z(K)$, also $|J| = 2^4$ and $Z(I) = I' = Z(K)J$. As A is not abelian and $Z(K) \not\leq A$, $A' = J = Z(A)$. Also $AZ(I) \neq I$ since otherwise $Z(K) \leq I' \leq A' \leq A$. Hence $|A/J| = 2^4$ and $|A| = 2^8$. Let $A^* = AZ(I)$ and note that $\Phi(A^*) = \Phi(A) = J$. Let $D_1, \ldots, D_5$ be the five $D_8's$ that are naturally permuted by K, ordered so that $D_{i+1} = D_i^x$. Let $D_1 = \langle a_1^*, b_1^*\rangle$, with a_1^* and b_1^* of order two. Inductively define $a_{i+1}^* = a_i^x$ and $b_{i+1}^* = b_i^x$. Let $z_i^* = [a_i^*, b_i^*] \in Z(D_i)$. For $c \in \{a, b, z\}$ let c_i be the product of the c_j^* with $1 \leq j \leq 5$ and $j \neq i$. If $a_1 \in A^*$ then $A^* \leq \langle a_1^X\rangle Z(I) = \langle a_1, \ldots a_5\rangle Z(I)$ and A^* is abelian, a contradiction. Similarly $b_1 \notin A^*$ and $a_1b_1 \notin A^*$. Thus A^* has an element s of the form a_1b_i with $2 \leq i \leq 5$ or of the form $a_1b_ib_j$ with $1 \leq i < j \leq 5$. Note that $(a_1b_2)^2 = [a_1, b_2] = z_3^*z_4^*z_5^* \notin J$ and so the case $s = a_1b_2$, and more generally the case $s = a_1b_i$, is impossible. Note also that $(a_1b_1)^2 = z_1 \in J$. So we get $i \neq 1$ in the second case. Suppose that $i = 2$ and $j = 3$. Then $s^x = a_2b_3b_4$ and $[s, s^x] = [a_1, b_2b_3][b_2, a_2][b_3, a_2]$. Since the first two of these factors are in J but the last one is not, this case is impossible. Similarly, the cases $(i, j) = (2, 4), (3, 5)$ and $(4, 5)$ are ruled out. Thus $(i, j) = (2, 5)$ or $(3, 4)$. Since $[A^*, X] = A$, there exist exactly two choices for A for a given X. Note that an element in the normalizer of X which acts as (2354) on $D_1, \ldots, D_5$ interchanges these two choices. Let $L = K\langle t\rangle$. Then $|N_L(X)/N_L(X) \cap N_L(A)| = 2$. Let $D_0 = C_{O_2(K)}(X)$. Then $[D_0, I] \leq J$ and so $D_0 \leq N_K(A)$ and $N_{O_2(K)}(A) = D_0A$. Since $O^2(K)$ does not normalize A^* we conclude that $N_L(A) \leq N_L(X)O_2(K)$ and we have to decide whether $N_L(A)/D_0A$ is isomorphic to $C_2 \times D_{10}$ or to $Frob_{20}$. In the first case we may assume that t normalizes A. As X acts irreducibly on A/J we conclude that $[A, t] \leq J$ and so $A^*/Z(I) = C_{I/Z(I)}(t)$. But then K normalizes $A^*/Z(I)$, a contradiction. The very last statement follows as $N_{K\langle t\rangle}(A) \not\leq K$. **QED**

Lemma 2.5 *(a) $E_6(5)$ has two conjugacy classes of involutions. There exist representatives r and s of these classes such that*

$$C_{E_6(5)}(r) \sim 4.D_5(5).4 \quad \textit{and} \quad C_{E_6(5)}(s) \sim 2.(L_2(5) \times L_6(5)).2.$$

Moreover, if U is a 27-dimensional $GF(5)-$module for $E_6(5)$, then $C_U(r)$ is 11-dimensional and $C_U(s)$ is 15-dimensional. As a $C_{E_6(5)}(r)-$module U is the direct sum of three irreducible submodules of dimensions 1, 10 and 16. The kernel of the action of $C_{E_6(5)}(r)$ on the invariant 1-space is $C_{E_6(5)}(r)'$.

(b) $2.E_7(5)$ has three conjugacy classes of involutions. There exist representatives z, z_0 and i of these classes such that $z_0 \in Z(2.E_7(5))$, $i = z \cdot z_0$ and

$$C_{2.E_7(5)}(z) \sim 2^2.(L_2(5) \times D_6(5)).2$$

Moreover, $C_V(z)$ is a tensor product of natural modules for $SL_2(5)$ and $\Omega_{12}^+(5)$, and $[V, z]$ is a half-spin module for $2.D_6(5)$.

Proof: The conjugacy classes of involutions and their centralizers are well known and easily deduced, for example by the methods found in [2]. The information about U and V is easily computed using the subgroup $5^{27}E_6(5)$ of $E_7(5)$, the subgroup $5^{1+56}2E_7(5)$ of $E_8(5)$, the Steinberg relations and the weight theory of modules for groups of Lie type. **QED**

Recall that E is a parabolic subgroup $QL \sim 5^{27}.(4 \times E_6(5))$ in G. Let $X_1 = C_V(Q)$, $X_3 = [V, Q]$ and $X_2 = [X_3, Q]$. Then

$$0 < X_1 < X_2 < X_3 < V$$

is the unique chief series for E on V, moreover $E = N_G(X_1)$, the modules X_1 and V/X_3 are 1-dimensional and X_2 and X_3/X_2 are 27−dimensional mutually dual E−modules.

By assumption L' contains a subgroup ${}^2F_4(2)$ acting irreducibly on Q. Hence L contains a subgroup $\tilde{F}$ fulfilling (+), and acting irreducibly on Q.

Define $\widetilde{S}, \widetilde{P}_1$ and $\widetilde{P}_2$ (as subgroups of $\tilde{F}$) in a way analogous to the above. The reader should notice that $Z(\tilde{F}) = Z(G)$ centralizes Q, thus Q is irreducible, but not faithful as an $\tilde{F}$−module. But we still can apply Lemma 2.3 to $\tilde{F}/Z(G)$ and conclude that $\widetilde{P}_1$ normalizes a non-trivial subgroup $\langle f_- \rangle$ of Q. Let $f_+ \in \widetilde{P}_1$ be of order 5 and $r \in \widetilde{P}_1 \cap \widetilde{F}'$ of order 4 with ${f_+}^r = {f_+}^2$. As seen in the proof of Lemma 2.3, $\langle r \rangle$ acts faithfully on $\langle f_- \rangle$. So either ${f_-}^r = {f_-}^2$ or ${f_-}^r = {f_-}^3$. Note that there exists σ in $N_G(L)$ inducing a graph automorphism on L (indeed such a σ can be chosen to invert the Cartan subgroup of G). Then the action of L on Q^σ is dual to the action of L on Q and replacing $\tilde{F}$ and f by $\tilde{F}^\sigma$ and f^σ if necessary, we may assume that ${f_-}^r = {f_-}^2$. Put $f = f_+ f_-$. Then $f^r = f^2$. Let u be an element of order 4 in $\widetilde{P}_1$ centralized by f_+. Let $Z_1 = Z(\widetilde{P}_1 \cap \widetilde{F}')$.

Lemma 2.6 *(a) The element u centralizes f_-.*

(b) f_- is a root element of G and $C_G(f_-) \sim 5^{1+32}.2^2.D_6(5)$. The $C_G(f_-)$−module $[V, f_-]$ is a natural orthogonal 12−space for $\Omega^+_{12}(5)$ and the subspace X_1 is a singular 1-space. The quotient, $([V, f_-] + X_2)/X_2$ is 1−dimensional and $[V, f_-] \cap X_2 = X_1 \oplus [C_{X_2}(Z_1), Q_1]$.

(c) $C_G(f_-) \cap C_G(Z_1) \sim \langle f_- \rangle \times 2^2.D_6(5)$

(d) $C_V(f_-) \leq [X_3, Z_1] + [V, f_-] + X_2$

Proof: (a): Pick $s \in Z(L)$ and $e \in L'$ with $u = se$. Note that $e \in \tilde{F}$ and so $e^2 \in \tilde{F}' = F'$ and $e^2 \in Q_1$. In particular, $u^2F' = s^2F'$. Since $F/F' \cong C_4$ and $F = \langle u \rangle Z(F)F'$ we get $s^2 \neq 1$ and $|s| = 4$. Since s inverts Q, it is enough to show that e inverts f_-. Let $D = C_{L'}(Z_1)$. By Lemma 2.3, $C_Q(Z_1)$ has order 5^{11} and $\langle f_- \rangle$ is the unique cyclic subgroup of Q normalized by $\widetilde{P}_1$ and so by Lemma 2.5a, D has shape $4.D_5(5).4$, moreover D normalizes $\langle f_- \rangle$ and $C_D(f_-) = D'$. As a D−module, Q is the direct sum of irreducible modules of dimensions 1, 10 and 16. Using Lemma 2.3ab we conclude, by the action of $\widetilde{P}_1$ on the 10-dimensional space, that $\widetilde{P}_1$ is contained in a subgroup Y of D, such that Y/Z_1 is isomorphic to the subgroup of index 4 in $D_8 \wr Sym(5)$. In addition, $C_Y(f_+) \cap D' = Z_1$, and so $su \notin D'$. Thus e does not centralize f_-. As $e^2 \in Q_1$, the element e^2 does centralize f_- and so e inverts f_-. Thus (a) holds.

(b): As D lies in a parabolic P (of shape $5^{16}D$ in $E_6(5)$) that fixes a 1−space in Q, the group $\langle f_- \rangle$ is normalized by the parabolic $QZ(L)P$ of G and thus is a root group. Hence also the second, third and fourth statements in (b) hold. As Q centralizes V/X_3 and X_3/X_2 but not V/X_2 and as V/X_3 is one dimensional, $([V, f_-] + X_2)/X_2$ is 1-dimensional. Now $[X_2, f_-] = X_1$

and $([X_2, Q_1] + X_1)/X_1$ is the unique 10-dimensional subspace of X_2/X_1 invariant under P_1 and thus also the last statement in (b) holds.

(c): By (b), Z_1 centralizes $[V, f_-]$ and so (c) holds.

(d): As Z_1 centralizes $[V, f_-]$, the element f_- centralizes $[V, Z_-]$. Now both $C_V(f_-)+X_2/X_2$ and $[X_3, Z_1] + [V, f_-] + X_2/X_2$ are 17-dimensional and (d) holds. **QED**

Since $\tilde{S} = O_2(O^2(\tilde{P}_1))\langle u\rangle\langle r\rangle$, the group $\widetilde{S}$ normalizes $O^2(\widetilde{P}_1)\langle f\rangle$. Put $S = \widetilde{S}$, $P_1 = \langle S, f\rangle, P_2 = \widetilde{P}_2$ and $F = \langle P_1, P_2\rangle$.

Lemma 2.7 *(a) F normalizes a complement M_0 in X_3 to X_2. Put $M = M_0 + X_1$. Then $N_E(M) \cap Q = 1$. In particular, $F \cap Q = 1$ and F fulfills (+).*

(b) P_1 normalizes exactly two 1-spaces in V namely X_1 and U_1, where $U_1 \le M_0$. Moreover, $C_V(O^2(P_1)) = X_1 + U_1$.

(c) $[V, f_-] = X_1 + U_1 + [C_{X_2}(Z_1), Q_1]$

Proof: Put $U_1 = [C_V(Q_1), f, r]$. Note that Q_1 centralizes a 1-space in each of the modules X_i/X_{i-1}, and $C_V(Q_1)$ is 4-dimensional. As $[V, Q] \not\le X_2$, $[V, f_-] \not\le X_2$. Since $[X_3, f_-] \le X_2$ and $V = C_V(Q_1)X_3$, we conclude $[C_V(Q_1), f_-] \not\le X_2$. On the other hand as L acts completely reducibly on V, we have $[C_V(Q_1), f_+] = 1$. Thus $[C_V(Q_1), f] \not\le X_2$. By Lemma 2.3ad applied to F' and the modules X_3/X_2 and X_2/X_1, the element r^2 inverts $C_{X_3/X_1}(Q_1)$. In particular, $[r, f]$ centralizes X_3 and, as r inverts f and f has odd order, we conclude that f centralizes $C_{X_3/X_1}(Q_1)$. It follows that $([C_V(Q_1), f] + X_1)/X_1$ is $1-$dimensional and not contained in X_2/X_1. Hence U_1 is $1-$dimensional, $U_1 \le X_3$, $U_1 \not\le X_2$ and P_1 normalizes U_1.

Let $U_2 = \langle U_1^{P_2}\rangle$. As $|P_2/S| = 3$, the space U_2 is at most 3-dimensional. By Lemma 2.3 applied to $W = X_3/X_2$, we know that $(U_2 + X_2)/X_2$ is 3-dimensional. Thus U_2 is a 3-space and $U_2 \cap X_2 = 1$. Let $U_3 = \langle [U_2, Q_1]^{P_1}\rangle$. Since $[U_2, Q_1]$ is a 2-space and $|P_1/S| = 5$, we similarly have that U_3 is 10-dimensional and $U_3 \cap X_2 = 1$. Let $U_4 = \langle [U_3, Z_2]^{P_2}\rangle$. Since $[U_3, Z_2]$ is eight dimensional, U_4 is 24-dimensional and $U_4 \cap X_2 = 1$. Let $U_5 = [U_4, Z_1]$. Since X_3/X_2 and X_2/X_1 are dual as $E-$modules, Lemma 2.3af implies that $[V, Z_1]X_2/X_2$ and $[X_2, Z_1]$ are isomorphic and absolutely irreducible as P_1-modules and as $S-$modules. (Note here that Z_1 is trivial on X_1 and V/X_3.) By Lemma 2.3c, $[V, Z_1]$ splits over $[X_2, Z_1]$ as a P_1-module. It is now easy to see that every $S-$submodule of $[V, Z_1]$ is invariant under P_1. In particular P_1 normalizes U_5. Put $M_0 = U_2 + U_4$. Note that by Lemma 2.3, $(M_0 + X_2)/X_2 = X_3/X_2$ and that M_0 has dimension at most $3 + 24 = 27$. Thus $M_0 \cap X_2 = 0$ and M_0 is a complement to X_2 in X_3. Then

$$M_0 = U_1 + (U_2 \cap U_3) + (U_3 \cap U_4) + U_5 = U_1 + U_3 + U_5.$$

and so $F = \langle P_1, P_2\rangle$ normalizes M_0.

It follows that $[X_3, N_E(M) \cap Q] \le M \cap X_2 = X_1$. Since Q does not centralize X_3/X_1 and E is irreducible on Q, we have $N_E(M) \cap Q = 1$. Since $FQ = \widetilde{F}Q$, the last statement of (a) also holds.

As f_+ centralizes $C_V(Q_1)$ the last statement in (b) holds once we prove that $C_{C_V(Q_1)}(f_-) = X_1 + U_1$. As seen above $[C_V(Q_1), f_-] \not\le X_2$ and by a dual argument $[C_V(Q_1), f_-] \neq 0$. Hence $C_{C_V(Q_1)}(f_-)$ is at most 2-dimensional and so $C_{C_V(Q_1)}(f_-) = X_1 + U_1$. As r centralizes X_1 but not U_1, the P_1-modules X_1 and U_1 are not isomorphic. Thus (b) holds.

As seen above $U_1 \leq [V, f_-]$. Thus (c) follows from Lemma 2.6b. **QED**

Let $\chi_0 = X_1^G$ and $\zeta_0 = Z_1^G$.

Lemma 2.8 *$U_1 \in \chi_0$ and $C_M(Z_1) = \bigoplus \{X \mid X \in \chi_0,\ X \leq C_M(Z_1)\}$.*

Proof: We claim that E acts transitively on $\{Z \in \zeta_0 \mid [X_1, Z] = 1\}$. Indeed, for any such Z, we have $\dim[V, Z] = 32 = \dim[X_3/X_1, Z] = 2 \cdot \dim[X_2/X_1, Z]$. Thus the claim follows from Lemma 2.5a. By this claim, G acts transitively on $\{(Z, X) \in \zeta_0 \times \chi_0 \mid [X, Z] = 1\}$ and thus $C_G(Z_1)$ acts transitively on $\{X \in \chi_0 \mid [X, Z_1] = 1\}$. By Lemma 2.5b, $C_G(Z_1) \sim 2^2.(L_2(5) \times D_6(5)).2$ and $C_V(Z_1)$ is the tensor product of natural modules for $SL_2(5)$ and $\Omega_{12}^+(5)$. By Lemma 2.6c, f_- lies in the factor $SL_2(5)$ and so $[V, f_-]$ is one of six 12-spaces invariant under $2^2.D_6(5)$. By Lemma 2.6b, X_1 is a singular point in $[V, f_-]$ and it follows that $\{X \in \chi_0 \mid [X, Z_1] = 1\}$ is precisely the union of the sets of singular points in the six 12-spaces. By Lemma 2.7c, $X_1 + U_1 = C_{[V,f_-]}(Q_1)$ and so $X_1 + U_1$ is a non-degenerate subspace of $[V, f_-]$. As X_1 is singular in $[V, f_-]$, the space $X_1 + U_1$ is of "+"-type and so contains exactly one member of χ_0 distinct from X_1. By Lemma 2.5c, U_1 is the only $1-$space in $X_1 + U_1$, which is invariant under P_1 and distinct from X_1. So $U_1 \in \chi_0$. By the proof of Lemma 2.3ab, $[C_{M_0}(Z_1), V_1]$ is the direct sum of 5 pairwise non-isomorphic irreducible Q_1-modules, each of which is the direct sum of two conjugates of U_1 under F. Moreover, Q_1 normalizes each of the six 12-spaces and it is now easy to see that $C_M(Z_1)$ intersects each of the six 12-spaces in a 2-space of "+"- type. This clearly implies the lemma. **QED**

Lemma 2.9 *$N_E(M) \cap C_G(Z_1) = P_1$ and F contains a Sylow 2-subgroup of $N_E(M)$.*

Proof: Put $N = N_E(M)$ and $Y = C_N(Z_1)$. By Lemma 2.7, $N \cap Q = 1$. By Lemma 2.5a,

$$C_E(Z_1) \sim 5^{11}.(C_4 \times 4.D_5(5).4)$$

and $C_E(Z_1)$ normalizes a 10-space in X_3/X_2. By the proof of Lemma 2.8, Y normalizes $X_1 + U_1$ and a decomposition of this 10-space into an orthogonal sum of five 2-spaces of "+"-type. Let K be the full normalizer in $C_E(Z_1)$ of this decomposition. Then

$$K \sim 5^{11}(C_4 \times 2.\frac{1}{2}\,(D_8 \wr Sym(5)).2).$$

Let M_1 be the complement in X_3 to X_2 normalized by L. We claim that $U_3 \not\leq M_1$ and $U_5 \not\leq M_1$. As U_1 is $S-$invariant and $S \leq L$, we have $U_1 \leq M_1$. Since $P_2 \leq L$ we get $U_2 \leq M_1$. Suppose that $U_3 \leq M_1$. Then $\tilde{P}_1$ normalizes U_3 and since $f_- \in P_1\widetilde{P_1}$ we conclude that f_- normalizes U_3. Note that f_- centralizes X_3/X_2 and $U_3 \leq X_3$. Hence $[U_3, f_-] \leq X_2 \cap U_2 = 0$ and so f_- centralizes U_3, a contradiction to Lemma 2.6d. Thus U_3 is not contained in M_1. It follows that neither $U_3 \cap U_4$ nor U_4 are contained in M_1. As $P_2 \leq L$ acts irreducibly on U_4 we conclude that $U_4 \cap M_1 = 0$ and so finally $U_5 \not\leq M_1$.

As $Y \cap Q = 1$, Y is isomorphic to a subgroup of $K/O_3(K)$ and so $Y/O_2(Y)$ is isomorphic to a section of $Sym(5)$. As 5 divides the order of P_1 we conclude that $O_2(P_1O_2(Y)/O_2(Y)) = 1$ and so $O_2(P_1) \leq O_2(Y)$. As $C_Q(O_2(P_1)) = \langle f_- \rangle$, any conjugate of L in E containing $O_2(P_1)$ is of the form L^x for some $x \in \langle f_- \rangle$. By Sylow's theorem $O_2(Y)$ lies in some conjugate of L in

E and so $O_2(Y) \leq L^x$ for some $x \in \langle f_- \rangle$. Thus $O_2(Y)$ normalizes $[M_1, Z_1]^x$. By Lemma 2.6b, x centralizes $[M_1, Z_1]$ and so $O_2(Y)$ normalizes $[M_1, Z_1]$, $[X_2, Z_1]$ and $U_5 = [M, Z_1]$. Since all of these $Y-$modules are irreducible and $U_5 \leq [V, Z_1] = [X_2, Z_1] \oplus [M_1, Z_1]$ we conclude that these $O_2(Y)-$modules are pairwise isomorphic and so $O_2(Y)$ acts self-dually on $[X_2, Z_1]$.

For each $X \leq E$, we write X^* for $C_X(X_1)$. Since $Z(L)$ acts transitively on $X_1^{\#}$, the groups $\tilde{F}, F$ and P_1 also act transitively on $X_1^{\#}$. Thus $Y = Y^* P_1$. Let C (respectively $\hat{C}$) be the largest subgroup of K^* centralizing (centralizing or inverting) $(U_3 + X_2)/X_2$. Then $\hat{C}Q/Q \cong C_4$. Since $O_2(Y)$ acts self-dually on $[X_2, Z_1]$ and the elements of $\hat{C}$ act as scalars we conclude that $\hat{C} \cap Y$ centralizes or inverts $[X_2, Z_1]$. Hence $\hat{C} \cap Y^* \leq C$ and $Y^*C \cap \hat{C} = (Y^* \cap \hat{C})C = C$. Thus no element of Y^*C/C inverts $(U_3 + X_2)/X_2$. We are now in a position to apply Lemma 2.4 (with $K\langle t \rangle = K^*/C$ and $A = O_2(Y^*)C/C \cap O_2(O^2(K^*/C))$. Note that A is not abelian as $Q_1C/C \leq A$ and $Q_1 \cap C = Z_1$. As $r \in P_1^*$, the group P_1^* has $Frob_{20}$ as a quotient. Since Y^*C normalizes A we conclude that $Y^*C \leq O_2(Y^*)P_1^*$ and $A = Q_1C/C$. From the structure of D_8, from the last two statements in Lemma 2.4 and from $O_2(Y^*) \cap \hat{C} \leq C$ we conclude that $O_2(Y^*)C = Q_1C$. Thus $Y^*C = P_1^*C$. Since $C \cap Y^* \cap Q = 1$, we have $C \cap Y^* = Z_1 \leq P_1^*$. So $Y^* = P_1^*$ and $Y = P_1$, proving the first statement of the lemma.

Since $Z_1 = Z(S) \cap S'$, $N_G(S) \leq C_G(Z_1)$ and so S a Sylow 2-subgroup of N. **QED**.

Lemma 2.10 *There exists $t \in N_G(P_1) \cap N_G(M)$ with $X_1 \neq X_1^t$.*

Proof: Let $t \in N_G(P_1)$. By Lemma 2.7b, $C_V(O^2(P_1)) = U_1 + X_1$ and so t normalizes $U_1 + X_1$. Also by Lemma 2.3ae, the isomorphism types of the two $10-$dimensional modules in V invariant under P_1 are not conjugate under an automorphism of P_1. So t normalizes U_3. Hence $t \in N_G(M)$ if and only if $t \in N_G(U_5)$.

Note that P_1 is contained in $\langle f_- \rangle\, C_L(Z_1)$. Let $\langle t_1 \rangle = Z(C_{L'}(Z_1))$. Then by Lemma 2.5a, t_1 is of order 4 and $[t_1, P_1] \leq Z_1$. So $t_1 \in N_G(P_1)$. Further $C_G(Z_1)$ is of shape $2^2.(L_2(q) \times D_6(5)).2$. Note that $[V, f_-]$ is 12-dimensional and there exists a quadratic form on $[V, f_-]$ invariant (up to scalar multiplication) under the action of $N_G(\langle f_- \rangle)$. Moreover, $[V, f_-]$ is equal to the sum of X_1, U_1 and the 10-dimensional subspace of X_2, which is normalized by P_1. In particular P_1 normalizes a decomposition of $[V, f_-]$ into an orthogonal sum of six 2-dimensional subspaces of "+"-type. Let T_0 be the largest subgroup of $2^2.D_6(5)$, which normalizes this decomposition and normalizes $X_1 + U_1$. Then P_1 normalizes T_0 and T_0/Z_1 is isomorphic to a subgroup of index 4 in $(D_8 \times D_8 \wr \Sigma_5)$.

Let $T = C_{T_0}(f)$. Then $T/Z_1 \cong D_8 \times C_2$ and T normalizes $O^2(P_1)$ and so also Q_1 and $V_1 = Q_1'$. Moreover, $t_1 \in T$, $[t_1, T] \leq Z_1$, $T' = Z(G)Z_1$ and $T \cap P_1/Z_1 \cong C_4$. Pick $t_2 \in T$ with $t_2^2 \in Z_1$ and $[t_2, T] \not\leq Z_1$. We will show that either t_2 or t_1t_2 fulfills the conclusion of the lemma. It is easy to check in T_0 that t_2 centralizes a 1-space in each of the six 2-spaces and that these six 1-spaces form a 6-space of "+"-type. As the central involution of $\Omega_6^+(5)$ lifts to an element of order four in $2.\Omega_6^+(5) \cong SL_4(5)$ we conclude that t_2 and by symmetry t_1t_2 are elements of order 4. It follows that

$$\langle t_1, t_2 \rangle \cong Q_8 \quad \text{and} \quad \langle t_1, t_2 \rangle \cap P_1 = Z_1.$$

We will now examine the action of $\langle t_1, t_2 \rangle$ on the set Π of 16-spaces in V invariant under $O^2(P_1)$. Note that $|\Pi| = 5 + 1 = 6$. Put $H = [V_1, f]$. Then $\langle t_1, t_2 \rangle$ normalizes H and acts faithfully on the 2-dimensional space $C_{[V,Z_1]}(H)$. So the orbits of $\langle t_1, t_2 \rangle$ on the 1-dimensional subspaces of $C_{[V,Z_1]}(H)$, and hence also on Π, are all of length 2. Now by Lemma 2.9, t_1 does not normalize M and so $[M, Z_1] \neq [M, Z_1]^{t_1}$. Hence $[M, Z_1] = [M, Z_1]^t$ for $t = t_2$ or for $t = t_1t_2$. Recall that $U_5 = [M, Z_1]$ and thus the selected t is in $N_G(M)$.

It remains to show that t normalizes P_1. Since t normalizes $O^2(P_1)$, it is enough to prove that $[t_1, N_S(\langle f\rangle)] \leq P_1$. Since $T = \langle t_1, t_2\rangle (T \cap P_1)$, $T \cap P_1$ is the largest subgroup of T acting trivially on Π. As $N_S(\langle f\rangle)$ acts trivially on Π, the same is true for $[t_1, N_S(\langle f\rangle)]$ and so $[t_1, N_S(\langle f\rangle)] \leq T \cap P_1 \leq P_1$, completing the proof of the Lemma. **QED**

Lemma 2.11 *Let $R = \langle F, F^t\rangle$. Then F has three orbits on the right cosets of F in R. The orbit stabilizers are F, P_1 and a group of order $2^5{\cdot}3{\cdot}5^2{\cdot}13$. In particular $|R| = 2^{15}{\cdot}3^3{\cdot}5^3{\cdot}7{\cdot}13{\cdot}29$.*

Proof: Note first that R normalizes M. We will divide the proof into several steps.

1 *Let $\chi = X_1^R$ and $\zeta = z_1^R$. Then R acts transitively on*
(a) $\{(X, z) \mid X \in \chi,\ z \in \zeta$ *and* z *centralizes* $X\}$,
(b) $\{(X, z) \mid X \in \chi, z \in \zeta$ *and* z *inverts* $X\}$.

Clearly a Sylow 2-subgroup of $N_R(X_1)$ contains representatives of each class of involutions in $N_R(X_1)$. By Lemma 2.9, S is Sylow 2−subgroup of $N_R(X_1)$ and so F contains representatives of each class of involutions in $N_R(X_1)$. As $F/F' \cong C_4$, all the involutions in F are contained in $Z(G) \times F'$. By Lemma 2.3, F' has two classes of involutions with representatives z_1 and i. Moreover $C_W(i)$ is 15-dimensional and so $\dim C_V(i) = 2 + 2 \cdot 15 = 32$. Hence F has two orbits on $F \cap \zeta$ with representatives z_1 and z_0i, where z_0 is the central involution in G. Now z_1 centralizes X_1 and z_0i inverts X_1. Thus (1) holds.

2 *(a)* $C_R(z_1)$ *acts transitively on* $C_M(z_1) \cap \chi$ *and* $|C_M(z_1) \cap \chi| = 12$,
(b) $C_R(z_1)$ *and* P_1 *act transitively on* $[M, z_1] \cap \chi$ *and* $|[M, z_1] \cap \chi| = 80$,
(c) $|C_R(z_1)| = 2^{15} \cdot 3 \cdot 5$,
(d) $C_{N_R(X_1)}(i) \leq F$.

The two transitivity statements for $C_R(z_1)$ follow from (1). By Lemma 2.8, $|C_M(z_1) \cap \chi_0| = 12$. Moreover, by Lemma 2.3, U_3 contains 10 elements of U_1^F and so $C_M(z_1) \cap \chi$ contains at least the 11 elements of $C_M(z_1) \cap \chi_0 \setminus \{X_1\}$. Conjugation by t shows that $C_M(z_1) \cap \chi$ also contains the 11 elements of $C_M(z_1) \cap \chi_0 \setminus \{U_1\}$. Thus $C_M(z_1) \cap \chi = C_M(z_1) \cap \chi_0$ and (a) holds. By Lemma 2.9, $C_R(z_1) \cap N_R(X_1) = P_1$ and so

$$|C_R(z_1)| = 12 \cdot |C_R(z_1) \cap N_R(X_1)| = 12 \cdot |P_1| = 2^{15} \cdot 3 \cdot 5.$$

Now $|[M, z_1] \cap \chi| = |C_R(z_1)| \,/\, |C_R(z_1) \cap N_R(X)|$, where $X \in \chi$ is inverted by z_1. By Lemma 2.3d, $|C_F(i)| = 2^{11} \cdot 3$. Further, $|C_R(z_1) \cap N_R(X)| \geq |C_F(i)|$ and so $|[M, z_1] \cap \chi| \leq 80$. Finally, P_1 has an orbit of length 80 on $[M, z_1] \cap \chi$. Indeed, there are 80 points at distance 4 from a in Γ_0 (the generalized octagon associated to F), these 80 points correspond to 80 elements in U_0^F and U_0^F is a subset of χ. So $|[M, z_1] \cap \chi| = 80$, moreover $|C_R(z_1) \cap N_R(X)| = |C_F(i)|$ and P_1 acts transitively on $[M, z_1] \cap \chi$. This completes the proof of (2).

3 $N_R(X_1) = F = N_R(F)$. *In particular, the actions of R on X_1^R and on R/F are isomorphic.*

Let $N = C_R(X_1)$. Then, as in (1), N has two classes of involutions, with representatives z_1 and i. By (2)(d) and Lemma 2.8, F' contains the centralizers of z_1 and i in N. Hence by a standard argument, see for example [6, 9.2.1], $F' = N$. Thus $N_R(X_1) = F$. Now X_1 is the unique 1-space in M normalized by F and so $N_R(F) \leq N_R(X_1)$.

Let Γ be the graph with vertices χ and edges $\{X_1, U_1\}^R$. Since $R = \langle F, F^t \rangle$ we have

4 Γ *is connected.*

5 *Let $a, b \in \chi$. Suppose there exists $z \in \zeta$, such that z normalizes a and b. Then a and b have distance at most 2 in Γ. If z centralizes a or b, then a and b have distance at most 1.*

Suppose first that z centralizes a. Then we may assume without loss that $a = X_1$ and $z = z_1$. Then (2) implies that $b = X_1$ or $b \in U_1^F$ and so a and b are at distance at most 1.

In the general case pick $c \in \chi$ so that z centralizes c. Then a and b are at distance at most 1 from c, and (5) is proved.

For a vertex a, put $R_a = N_R(a)$, and for an edge $\{a, b\}$, let $1 \neq z(a,b) \in Z(R'_a \cap R'_b)$. Note that, if $(a,b) = (X_1, U_1)^g$, then $z(a,b) = z_1^g = z(b,a)$. For $g \in F$, we identify $\alpha^g \in \Gamma_0$ with $U_1^g \in \Gamma$.

6 *(a) R acts transitively on geodesics of length 2 in Γ. Moreover, the stabilizer of a geodesic of length 2 is isomorphic to $C_2 \times Frob_{20}$*

(b) Let d and e be at distance 2 in Γ. Then $R_d \cap R_e$ acts transitively on the set of pairs (a,b) such that $\{a,b\}$ is an edge with $z(a,b) \in R_d \cap R_e$. Moreover, $R_a \cap R_b \cap R_d \cap R_e$ is isomorphic to $C_2 \times C_4$.

Let a and b be in α^F. Suppose that a and b are at distance less than or equal to 6 in Γ_0. Then there exists $c \in \alpha^F$, such that c is (in Γ_0) at distance 2 from a and at distance at most 4 from b. Put $z = z(X_1, c)$. Then by Lemma 2.3ab&ac, z centralizes a and normalizes b. Thus (5) implies that either $a = b$ or a is adjacent to b in Γ. Suppose that every pair of elements in α^F are adjacent in Γ. Then every pair of elements in $\alpha^F \cup \{X_1\}$ are adjacent. Since Γ is connected, we conclude that $\alpha^F \cup \{X_1\}$ is the set of vertices of Γ. Hence $|R| = |F| \cdot (|F|+1)$ and so $|R|_2 = 2^{14}$, a contradiction to (2)(c). So there are two elements of α^F, that have distance 8 in Γ_0, and have distance 2 in Γ. Since P_1 is transitive on $\triangle^8(\alpha)$ and since every geodesic of length two in Γ is conjugate to one with X_1 as its midpoint, we conclude that R is transitive on geodesics of length 2 in Γ. Moreover, the stabilizer in F of two elements of distance 8 in α^F is a $C_2 \times F_{20}$. Hence (a) is proved.

To prove (b) we assume without loss that $a = X_1$ and $b = U_1$. Since $z(a,b)$ normalizes d and e, we get by (5) that $d, e \in \alpha^F$ and that d and e are at distance less than or equal to 4 from b in Γ_0. Since d and e are at distance 8 from each other, b lies on a geodesic from d to e in Γ_0 and is at distance 4 from both d and e. Now F acts transitively on paths of length 8 in Γ_0 starting with a vertex in α^F and the stabilizer of such a path is a $C_2 \times C_4$. This proves (b).

7 *Let d and e be at distance 2 in Γ. Then $R_d \cap R_e$ acts transitively on $R_d \cap R_e \cap \zeta$. Moreover, if $z \in R_d \cap R_e \cap \zeta$, then $R_d \cap R_e \cap C_R(z)$ has order $2^5.3$ and has a normal Sylow $3-$subgroup.*

Let $z \in R_d \cap R_e \cap \zeta$. By (6), $R_d \cap R_e$ acts transitively on $R_d \cap R_e \cap \zeta$ and $R_d \cap R_e \cap C_R(z)$ acts transitively on all pairs (a,b) such that $\{a,b\}$ is an edge with $z = z(a,b)$. Put $A = R_a \cap R_b \cap R_d \cap R_e$ and $B = R_d \cap R_e \cap C_R(z)$. Then $|A| = 8$. Next we show that there are exactly 12 choices for (a,b). Indeed a is in $C_V(z) \cap \chi$ and so by (2)(a), there are exactly twelve choices for a. Moreover, as $R_a \cap R_b = C_{R_a}(z)$, b is uniquely determine by z and a. It follows that $|B| = 8 \cdot 12 = 2^5 \cdot 3$. We claim that A is normal in B. For this let $\{\bar{a}, \bar{b}\}$ be an edge different from $\{a,b\}$ with $z = z(\bar{a},\bar{b})$. Again choose notation so that $a = X_1$. Since $z = z(\bar{a},\bar{b})$, z centralizes $\bar{a}$ and $\bar{b}$ and so $\bar{a}$ and $\bar{b}$ are at distance 2 from b in Γ_0. It follows from [5] that A normalizes $\bar{a}$ and $\bar{b}$, and so $A = R_{\bar{a}} \cap R_{\bar{b}} \cap R_d \cap R_e$. Thus A is independent of the choice of (a,b) and therefore normal in B. Let $\widetilde{B} = C_B(d)$ and $\widetilde{A} = C_A(d)$. Let $g \in A$ with $|g| = 4$. As $\langle g \rangle$ acts faithfully on the group of order five in $R_a \cap R_d \cap R_e$, $g^2 \neq z_0$. As $g \notin Z(G)F'$, $g^2 \notin F'$ and so $g^2 \neq z$. Thus $g^2 = z_0 z$. Since z and z_0 invert d, g^2 centralizes d. Thus $A/\widetilde{A}$ is elementary abelian, $|A/\widetilde{A}| = 2$ and $\widetilde{A} \cong C_4$. Let i be the involution in $\widetilde{A}$. Suppose that the Sylow 3$-$subgroups of B are not normal in B. Since 3 divides $\widetilde{B}$ and $|\widetilde{B}/\widetilde{A}|_2 \leq 4$, $\widetilde{B}/\widetilde{A} \cong A_4$. Let $Y = O_2(\widetilde{B})$ and $Y^* = [Y, O^2(\widetilde{B})]$. Then $Y = Y^*\widetilde{A}$ and $[Y^*, \widetilde{A}] = 1$. Hence $\widetilde{A} \leq Z(Y)$ and $Y/Z(Y)$ is elementary abelian. It follows that $|Y'| \leq 2$. Hence either Y is abelian, $Y^* \cap \widetilde{A} = 1$ and $Y \cong C_4 \times C_2 \times C_2$ or Y is not abelian, $Y^* \cong Q_8$ and $Y \cong C_4 \circ Q_8 \cong C_4 \circ D_8$. In particular, $\langle i \rangle = \Phi(Y)$. Note that $\widetilde{A} = C_R(d) \cap R_e \cap C_R(i)$. We claim that all involutions in $C_R(d) \cap R_e$ are conjugate under $R_d \cap R_e$. Indeed let j be any such involution. Since d and e have distance 2, (5) implies that $j \notin \zeta$. Thus $z_0 j \in \zeta$ and by the first part of (7), the conjugacy class of $z_0 j$ in $R_d \cap R_e$ is uniquely determined. Thus the claim holds. Moreover, by the structure of Y there exists an involution j in $\widetilde{B}$ different from i. Then by the claim $j = i^h$ for some $h \in R_d \cap R_e$. Now $[\widetilde{A}, j] = 1$ and $\widetilde{A} \leq C_R(d) \cap R_e \cap C_R(j) = \widetilde{B}^h$. As $\widetilde{B}^h/Y^h$ has order three, $\widetilde{A} \leq Y^h$. Hence

$$i \in \Phi(\widetilde{A}) \leq \Phi(Y^h) = \langle i^h \rangle = \langle j \rangle$$

a contradiction, which proves (7).

8 *Let a be at distance 2 from X_1 in Γ. Then $|F \cap R_a| = 2^5 \cdot 3 \cdot 5^2 \cdot 13$ and $F \cap R_a$ has exactly two orbits on the neighbors of X_1 in Γ.*

Let $z \in F \cap R_a \cap \zeta$ and D be the Sylow 3$-$subgroup of $C_{F \cap R_a}(z)$. By Lemma 2.3e $|N_F(D)| = 3^3 \cdot 2^5$ and so by (7), $C_{F \cap R_a}(z)$ contains a Sylow 2-subgroup of $N_F(D)$. Put $K = F' \cap R_a$. Then by Lemma 2.3, $C_K(z) \cong D_{24}$. Since $F \cap R_a$ acts transitively on the involutions in K, we conclude that the Sylow 2-subgroups of K are dihedral groups of order 8 and that K has exactly one class of involutions. By (6), $|K|$ is divisible by 5, and since $|F'| = 2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$, we have $|K| = 2^3 \cdot 3^{1+u} \cdot 5^{1+v} \cdot 13^w$, where u is 0, 1 or 2, and v and w are 0 or 1. Since $C_K(z)$ is a maximal subgroup of $N_{F'}(D)$, u is 0 or 2. We claim that K has an orbit on α^F with orbit stabilizer $C_2 \times Frob_{20}$ and an orbit with an orbit stabilizer of order 2^5. Indeed let b be at distance 1 from X_1 and a in Γ. Then by (6), $F \cap R_b \cap R_a \cong C_2 \times Frob_{20}$. Moreover, any 2-subgroup of F fixes a point in α^F and so there exists c in α^F so that 2^5 divides $|F \cap R_a \cap R_c|$. Suppose 5 divides $|F \cap R_a \cap R_c|$. Then $2 \leq |O_2(F' \cap R_a \cap R_c)| \leq 8$ and so $O^2(F' \cap R_a \cap R_c)$ centralizes $O_2(F' \cap R_a \cap R_c)$, a contradiction since the involutions in K are not centralized by elements of order 5 in K. So $|F \cap R_a \cap R_c| = 2^5$. In particular

$$1755 = |\alpha^F| \geq |b^K| + |c^K| = 2^2 \cdot 3^{1+u} \cdot 5^v \cdot 13^w + 3^{1+u} \cdot 5^{1+v} \cdot 13^w,$$

and so

$$(*) \qquad 65 \geq 3^u \cdot 5^v \cdot 13^w.$$

Now $|K/N_K(D)| = 5^{1+v} \cdot 13^w$ and $|K/N_K(D)|$ is congruent to 1 modulo 3, so we must have $v = 1$. By Lemma 2.3, the centralizers of elements of order 5 in F are $\{2,5\}-$groups and no involution in K is centralized by an element of order five . Thus the centralizers of elements of order five in K are 5-groups. In particular the Sylow 5-subgroups of K are $TI-$sets, and so the number of Sylow 5-subgroups in K is congruent to 1 modulo 25. Since no divisor of $2^3 \cdot 3^3$ is 1 mod 25, $w \neq 0$. Thus $w = 1$ and by $(*)$, $u = 0$ and the equal sign holds in $(*)$. This means that $F \cap R_b$ has no further orbit on α^F and (8) is proved.

We remark that using the list of maximal subgroups of the Tits group or the classification of groups with dihedral Sylow 2-subgroups it is not difficult to see that $K \cong L_2(25)$, but we will not need this fact.

9 *F has three orbits on R/F with lengths 1, 1755 and 2304.*

In view of (8) it is enough to prove that there exist no points at distance 3 from X_1 in Γ. One easily checks in Γ_0 that there exist points b, c, d in α^F such that b has distance 8 from both c and d in Γ_0 and c and d are at distance 2 in Γ_0. Then c and d are adjacent in Γ and b is at distance 2 from c and d in Γ. Let a be at distance 2 from X_1. By (8), $F \cap R_a$ has two orbits on the neighbors of a in Γ. One orbit is the set of common neighbors of X_1 and a. By (6) there exists $g \in R$ with $b^g = X_1$ and $c^g = a$. Then d^g lies in the second orbit and has distance 2 from X_1 In particular every point adjacent to a is at distance at most 2 to X_1 in Γ. This completes the proof of (9) and of Lemma 2.11. **QED**

It now follows from Lemma 2.11 that R has the following properties:

(a) R has a subgroup F with $F/Z(G) \cong {}^2F_4(2)$.

(b) F has 3 orbits on R/F with lengths 1, 1755 and 2304.

By [12] we conclude that $\overline{R}$ is isomorphic to the Rudvalis group. This completes the proof of Theorem 2.1.

3 A Computer-free Construction of the Higman-Sims Group as a Subgroup of E$_7$(5).

In this chapter we will prove the following Theorem:

Theorem 3.1 *$E_7(5)$ contains subgroups isomorphic to M_{22} and the Higman-Sims group.*

We start with some of the properties of M_{22} we will need in the proof of the theorem.

Lemma 3.2 *Let $M = M_{22}$ act faithfully on $\Omega = \{1, 2, \ldots, 22\}$, let $\omega \in \Omega$ and let D be the stabilizer of a hexad $\mathcal{H}$ in Ω.*

(a) M_ω *acts transitively on* $\Omega \setminus \{\omega\}$ *and* $M_\omega \cong L_3(4)$.

(b) $D \sim 2^4.Alt(6)$, D *acts transitively on* $\Omega \setminus \mathcal{H}$ *and any subgroup of shape* $2^4Alt(6)$ *in* M *is conjugate to* D.

(c) *Let* $E \leq M_\omega$ *with* $E \cong 2^4Alt(5)$. *Then* E *has orbits of lengths 1, 5 and 16 or of lengths 1, 1 and 20 on* Ω. *In the first case* E *stabilizes a hexad, and in the second case* $N_M(E) \sim 2^4Sym(5)$.

(d) *Let* $A \leq B \leq M$ *with* $A \cong Alt(6)$ *and* $B \cong Alt(7)$. *Then* A *is not contained in a conjugate of* D.

(e) *Let* $A \leq D$ *such that* $A \cong Alt(5)$ *and such that* $O_2(D)$ *is a natural* $SL_2(4)-$*module for* A. *Then* A *has orbits of lengths 1 and 5 on* $\mathcal{H}$ *and orbits of lengths 1 and 15 or of lengths 6 and 10 on* $\Omega \setminus \mathcal{H}$.

(f) *Let* $A \leq D$ *such that* $A \cong Alt(5)$ *and such that* $O_2(D)$ *is a natural* $\Omega_4{}^-(2)-$*module for* A. *Then* A *acts transitively on* $\mathcal{H}$ *and has orbits of lengths* $1, 5$ *and* 10 *on* $\Omega \setminus \mathcal{H}$.

(g) *If* $A \leq D$ *with* $A \cong Alt(6)$, *then* A *has orbits of lengths 1 and 15 or of lengths 6 and 10 on* $\Omega \setminus \mathcal{H}$.

(h) *If* $A \leq M_\omega$ *with* $A \cong Alt(6)$, *then* A *has orbits of lengths 1, 6 and 15 on* Ω.

(i) M *has no subgroup of index 56.*

Proof: The maximal subgroups of M_{22} and their orbits on Ω are listed in Table 10.3 on page 285 of [4]. We use this table without further reference. In particular, (a) and (b) hold. ¿From the definition of a Steiner system, the set $\Omega \setminus \{\omega\}$ together with the set of hexads containing ω form a projective plane of order 4. In particular both the two point stabilizer and the stabilizer of an incident point hexad pair have shape $2^4SL_2(4) = 2^4Alt(5)$ where the 2^4 is a natural $SL_2(4)-$module. Let E^* be the normalizer of a pair of points. Then $E^* \cong 2^4Sym(5)$ and (c) holds.

To prove (h), let f be an element of order five in A. Then f has exactly one fixed point η on $\Omega \setminus \{\omega\}$. Clearly A does not fix η and $|\eta^A|$ divides $|A|$ and is congruent to 1 modulo 5. Thus $|\eta^A| = 6$. As f acts fixed-point freely on the remaining 15 points and A has no orbit of length 5, (h) holds.

(g): By (h) we may assume that A has no fixed points on Ω. Then by the same argument as in the proof of (h), A has orbits of length 6 and 10 on $\Omega \setminus \mathcal{H}$.

For (e) and (f) we note that if A fixes a point η outside $\mathcal{H}$, then the action of A on $\Omega \setminus (\mathcal{H} \cup \{\omega\})$ is isomorphic to the action of A on $O_2(D)^\#$. Since in case (f) there exists a unique class of subgroups $Alt(5)$ in $O_2(D)A$, (f) holds. In case (e), we need to rule out the possibility that the orbits of A on $\Omega \setminus \mathcal{H}$ have lengths 5, 5 and 6. In this case, the elements of order three in A would have 4 fixed-points on $\Omega \setminus \mathcal{H}$, but only one fixed-point on $O_2(D)$, a contradiction.

(d) Note that B is unique up to conjugation and has an orbit Ξ of length 7. Hence A has orbits of length 1 and 6 on Ξ and so is transitive on $\Omega \setminus \Xi$ by (h). As no two hexads can intersect in a set of size 5, the orbit of length 6 is not a hexad. Thus (d) holds.

Since M has no maximal subgroup of index dividing 56, (i) holds. **QED**

For the convenience of the reader we recall the definition of the HS group as found [8]. Let (S, B) be the Steiner System of type $(3, 6, 22)$. Let $\mathcal{G}$ be the (undirected) graph with vertex set $\{*\} \cup S \cup \mathcal{B}$, where $*$ is a new symbol. In $\mathcal{G}$

(a) The vertex $*$ is joined to each point in S.

(b) Each point $\alpha \in S$ is joined to the 21 hexads containing α.

(c) Two hexads are joined if and only if they are disjoint.

Then by [8], $Aut(\mathcal{G})$ is transitive on $\mathcal{G}$ and $Aut(\mathcal{G})$ has a simple subgroup of index 2 and order 44,352,000, now called the Higman Sims group HS. We refer to $\mathcal{G}$ as the Higman-Sims graph.

The next two lemmas characterize M_{22} and HS in terms of certain subgroups.

Lemma 3.3 *Let M be a group and L, M_1 and M_2 subgroups of M such that $L \cong L_3(4)$, $M_1 \sim 2^4 Sym(5)$, $M_2 \sim 2^4 Alt(6)$, $L \cap M_1 \cong L \cap M_2 \sim 2^4 Alt(5)$, $M_1 \cap M_2 \sim 2^4 Sym(4)$, $L \cap M_1 \cap M_2 \sim 2^4 Alt(4)$ and $M = \langle L, M_1, M_2 \rangle$. Then $M \cong M_{22}$.*

Proof: Put $\Gamma = M/L$ and $\alpha = L \in \Gamma$. Let $t \in M_1 \cap M_2 \setminus L$. Since $M_1 \cap L$ is normal in M_1, we have $M_1 \cap L \le L^t$. As $M_1 \cap M_2$ does not normalize $L \cap M_2$, the element t does not normalize L and so $L \cap L^t = L \cap M_1$. Put $\Gamma_0 = \{\alpha\} \cup \alpha^{tL}$. Then $|\Gamma_0| = 1 + 21 = 22$.

Now $|\alpha^{M_2}| = |M_2/M_2 \cap L| = 6$ and $\alpha^{M_2} = \{\alpha\} \cup \alpha^{t(M_2 \cap L)} \subset \Gamma_0$. Further, as $M_1 = \langle t \rangle (M_1 \cap L)$, we have

$$\alpha^{M_2 M_1} = \alpha^{M_2 \langle t \rangle (M_1 \cap L)} = \alpha^{M_2 (M_1 \cap L)} = \alpha \cup \alpha^{t(M_2 \cap L)(M_1 \cap L)}.$$

Since $M_1 \cap L$ acts transitively on $\alpha^{tL} \setminus \{\alpha\}$ we get that $\alpha^{M_2 M_1} = \Gamma_0$. Hence M_1 and L normalize Γ_0. Note that $M_2 = \langle M_2 \cap L,\ M_2 \cap M_1 \rangle$ and so $M = \langle M_1,\ M_2,\ L \rangle = \langle M_1,\ L \rangle$. Thus M normalizes Γ_0, also $\Gamma = \Gamma_0$ and $|M/L| = 22$. Put $B = \alpha^{M_2}$ and $\mathcal{B} = \{B^m | m \in M\}$. We claim that $(\Gamma, \mathcal{B})$ is a Steiner System of type $(3, 6, 22)$. Since L is doubly transitive on $\Gamma \setminus \{\alpha\}$, M is triply transitive on Γ. Hence each set of three elements in Γ lies in e elements of $\mathcal{B}$ where e is a positive integer independent of the set of three. Counting tuples (H, a, b, c) such that $H \in \mathcal{B}$ and a, b, c are pairwise different elements of H we get

$$|\mathcal{B}| \cdot 6 \cdot 5 \cdot 4 = 22 \cdot 21 \cdot 20 \cdot e.$$

As $|\mathcal{B}| = |M/M_2| = 22 \cdot |L|/|M_2| = 77$ we get $e = 1$ and the claim is established.

Since $M \le Aut(\Gamma, \mathcal{B}) \cong Aut(M_{22})$ and $|M| = 22 \cdot |L| = |M_{22}|$, we deduce that $M \cong M_{22}$. **QED**

Lemma 3.4 *Let H be a group, M and D subgroups of H, and L a subgroup of M. Suppose that each of the following holds:*

(i) $M \cong M_{22}$, $L \cong L_3(4)$ and $D \sim 2^4 Sym(6)$,

(ii) There exists $t \in N_H(L)$ with $t^2 \in L$ such that $D \cap M \sim 2^4 Sym(5)$, $D \cap M^t \sim 2^4 Alt(6)$, and $D \cap D^t \sim 2^4 Sym(4)$.

(iii) $H = \langle M, L, D, t\rangle$.

Then H is isomorphic to HS, $C_2 \times HS$ or $Aut(HS)$.

Proof: Let Γ be the graph whose vertices are the right cosets of M in H, and whose edges are the sets $\{Mh, Mth\}$ for $h \in H$. Put $\alpha = M$ and $\beta = Mt$.

Note that $\langle H_\alpha, H_{\{\alpha,\beta\}}\rangle = \langle M, L\langle t\rangle\rangle$ and $D = \langle D \cap M,\ D \cap M^t\rangle$. So $\langle H_\alpha, H_{\{\alpha,\beta\}}\rangle = H$ and Γ is connected.

Let $\triangle^i(\alpha)$ be the set of vertices at distance exactly i from α and put $\triangle(\alpha) = \triangle^1(\alpha)$. Then $|\triangle(\alpha)| = 22$, $L = H_{\alpha\beta}$ and L acts transitively on $\triangle(\beta) \setminus \{\alpha\}$. Let $r \in D \cap M \setminus L$ and put $\gamma = \alpha^{trt}$. Then $\{\beta,\gamma\} = \{\alpha,\beta\}^{rt}$ and $\{\beta,\gamma\}$ is an edge. Since $r \in D$ and $D \cap M^t$ is normal in D, r normalizes $D \cap M^t$. Moreover, $t^2 \in L \leq M$ and so r^t normalizes $D^t \cap M$. Thus $D^t \cap M \leq H_\alpha \cap {H_\alpha}^{r^t} = H_{\alpha\gamma}$. In particular γ is not adjacent to α and thus $\gamma \in \triangle^2(\alpha)$.

Suppose that $H_{\alpha\gamma} \neq D^t \cap M$. As $D^t \cap M$ is maximal in M we get $H_{\alpha\gamma} = H_\alpha = H_\gamma$, and $\triangle(\alpha) \cap \triangle(\gamma) = \beta^{H\alpha} = \triangle(\alpha) = \triangle(\gamma)$, and since Γ is connected, $\Gamma = \{\alpha,\gamma\} \cup \triangle(\alpha)$. Thus L fixes exactly the vertices α, β and γ. Hence $\gamma = \gamma^t$ and $t \in H_\gamma = H_\alpha$, a contradiction. We have proved

1 *H acts transitively on geodesics of length 2, $H_{\alpha\gamma} \sim 2^4 Alt(6)$, $|\triangle^2(\alpha)| = 77$, $|\triangle(\alpha) \cap \triangle(\gamma)| = 6$ and $H_{\alpha\beta\gamma} \sim 2^4 Alt(5)$.*

By part (c) of Lemma 3.2, $H_{\alpha\beta\gamma}$ acts transitively on $\triangle(\gamma)\setminus\triangle(\alpha)$. Let $\delta \in \triangle(\gamma)\setminus\triangle(\alpha)$. Then $H_{\alpha\gamma\delta} \cong Alt(6)$ and $H_{\alpha\beta\gamma\delta} \cong Alt(5)$. Suppose that δ is at distance 2 from a. Then $\triangle^3(\alpha) = \emptyset$, thus $\Gamma = \{\alpha\} \cup \triangle(a) \cup \triangle^2(\alpha)$ and $|\Gamma| = 100$. It is now easy to see that Γ is isomorphic to the Higman-Sims graph (see for example [19] for a formal proof). As $|H| = 100 \cdot |M_{22}| = |HS|$, $H \cong HS$.

So we may assume from now on that δ is not in distance 2 from α. It follows that

2 *$\delta \in \triangle^3(\alpha)$ and H acts transitively on geodesics of length 3.*

By Lemma 3.2 part (h), $H_{\alpha\gamma\delta}$ has orbits of lengths 1, 6 and 15 on $\triangle(\delta)$. Further by (2), $H_{\alpha\delta}$ acts transitively on $\triangle^2(\alpha) \cap \triangle(\delta)$. Since $\triangle(\beta) \cap \triangle(\delta) \subset \triangle^2(\alpha) \cap \triangle(\delta)$, we get $|\triangle^2(\alpha) \cap \triangle(\delta)|$ is 7, 16 or 22.

Suppose $|\triangle^2(\alpha) \cap \triangle(\delta)| = 7$. Then $|H_{\alpha\delta}| = 7 \cdot |H_{\alpha\gamma\delta}|$ and $H_{\alpha\delta} \cong Alt(7)$. Now $H_{\alpha\gamma} \sim 2^4.Alt(6)$ and $H_{\alpha\gamma} \cap H_{\alpha\delta} = H_{\alpha\gamma\delta} \cong Alt(6)$. This contradicts Lemma 3.2, part (d).

Suppose that $|\triangle^2(\alpha) \cap \triangle(\delta)| = 22$. Then $|H_{\alpha\delta}| = 22 \cdot |H_{\alpha\gamma\delta}| = 2^4 \cdot 3^2 \cdot 5 \cdot 11$ and $|H_\alpha/H_{\alpha\delta}| = 56$, a contradiction to Lemma 3.2, part (i).

Thus $|\triangle^2(\alpha) \cap \triangle(\delta)| = 16$ and $|H_{\alpha\delta}| = 16 \cdot |Alt(6)|$. Since $H_{\alpha\delta}$ acts non-trivially on the six points in $\triangle(d) \setminus \triangle^2(\alpha)$, we conclude that $H_{\alpha\delta}$ has a factor group $Alt(6)$ or $Sym(6)$. This implies $H_{\alpha\delta} \sim 2^4 Alt(6)$ and $\triangle(\delta) \setminus \triangle^2(\alpha)$ is a hexad in the $H_\delta-$invariant Steiner system $\triangle(\delta)$. Since $H_{\alpha\gamma\delta}$ has orbits of lengths 1 and 15 on $\triangle^2(\alpha) \cap \triangle(\delta)$, the group $H_{\alpha\beta\gamma\delta}$ ($\cong Alt(5)$) fixes a unique point in $\triangle^2(\alpha) \cap \triangle(\delta)$, namely γ. Note that $H_{\alpha\beta\delta} \cong H_{\alpha\gamma\delta} \cong Alt(6)$ and that $H_{\alpha\beta\delta}$ does not fix γ. So $H_{\alpha\beta\delta}$ fixes no point in $\triangle^2(\alpha) \cap \triangle(\delta)$ and by Lemma 3.2, part (g), $H_{\alpha\beta\delta}$ has orbits of lengths 6 and 10 on $\triangle^2(\alpha) \cap \triangle(\delta)$. Now parts (e) and (f) of Lemma 3.2 imply that $H_{\alpha\beta\gamma\delta}$ has orbits of lengths 1, 5 and 10 on $\triangle^2(\alpha) \cap \triangle(\delta)$ and acts transitively on $\triangle(\delta) \setminus \triangle^2(a)$. Let $\varepsilon \in \triangle(d) \setminus \triangle^2(\alpha)$. Then $H_{\alpha\delta\varepsilon} \sim 2^4 Alt(5)$. Since $H_{\alpha\delta\varepsilon}$ lies in a unique subgroup $2^4.Alt(6)$ of H_α and since the stabilizer in H_α of points at distance 3 from α are $2^4 Alt(6)$'s, we get that δ is the unique point in $\triangle^3(\alpha)$ fixed by $H_{\alpha\delta\varepsilon}$. In particular $\varepsilon \notin \triangle^3(\alpha)$. We have proved

3 $H_{\alpha\delta} \sim 2^4Alt(6),\ |\triangle^3(\alpha)| = 77,\ \varepsilon \in \triangle^4(\alpha),\ H_{\alpha\delta\varepsilon} \sim 2^4Alt(5),\ H_{\alpha\beta\gamma\delta\varepsilon} \cong D_{10}$ *and* H *acts transitively on geodesics of length 4.*

By (1) and part (b) of Lemma 3.2, a subgroup $2^4Alt(5)$ of $H_{\beta\gamma}$ which has orbits of lengths 1, 1 and 20 on $\triangle(\beta)$ has orbits of lengths 1, 5 and 16 on $\triangle(\gamma)$. Note that $\triangle(\delta) \setminus \triangle^2(a)$ is an orbit of length 16 for $H_{\alpha\delta\varepsilon}$ on $\triangle(\delta)$, and so $H_{\alpha\delta\varepsilon}$ has orbits of lengths 1, 1 and 20 on $\triangle(\varepsilon)$. Since $H_{\alpha\varepsilon}$ acts transitively on $\triangle^3(\alpha) \cap \triangle(\varepsilon)$ and since $\triangle(\gamma) \cap \triangle(\varepsilon) \subset \triangle^3(\alpha) \cap \triangle(\varepsilon)$, we get that $|\triangle^3(\alpha) \cap \triangle(\varepsilon)|$ is 21 or 22. Suppose that $|\triangle^3(\alpha) \cap \triangle(\varepsilon)| = 22$, then $|H_{\alpha\varepsilon}| = 22 \cdot |H_{\alpha\delta\varepsilon}| = 22 \cdot |2^4Alt(5)|$ and thus $|H_\alpha / H_{\alpha\varepsilon}| = 21$, a contradiction. Thus $|\triangle^3(\alpha) \cap \triangle(\varepsilon)| = 21$ and $\triangle(\varepsilon) \setminus \triangle^3(\alpha) = \{\eta\}$ for some η. Thus $H_{\alpha\varepsilon} = H_{\alpha\varepsilon\eta} \cong L_3(4)$. Thus $|\triangle^4(\alpha)| = 22$ and ε is the unique point in $\triangle^4(\alpha)$ fixed by $H_{\alpha\varepsilon\eta}$ and so $\eta \notin \triangle^4(\alpha)$. Hence

4 $H_{\alpha\varepsilon} \cong L_3(4),\ |\triangle^4(\alpha)| = 22,\ \eta \in \triangle^5(\alpha),\ H_{\alpha\varepsilon\eta} = H_{\alpha\varepsilon}$ *and* H *is transitive on geodesics of length 5.*

Since $H_{\alpha\eta}$ is transitive on $\triangle^4(\alpha) \cap \triangle(\eta)$ and $\triangle(\delta) \cap \triangle(\eta) \subset \triangle^4(\alpha) \cap \triangle(\eta)$ we conclude that $\triangle^4(\alpha) \cap \triangle(\eta) = \triangle(\eta)$ and $H_{\alpha\eta} = H_\alpha \cong M_{22}$. Thus

5 $H_{\alpha\eta} = H_\alpha,\ \triangle^5(\alpha) = \{\eta\},\ \Gamma = \sum_{0\le i\le 5} \triangle^i(\alpha)$ *and* $|\Gamma| = 200$*.*

Let ϕ be the map that sends a vertex μ in Γ to the unique point at distance 5 from μ. Then ϕ is obviously a bijection and $(\mu^\phi)^g = (\mu^g)^\phi$ for all μ in Γ and g in $\mathrm{Aut}(\Gamma)$. In particular $\{\alpha^\phi, \beta^\phi\}$ is the set of fixed-points of $H_{\alpha\beta}$ on Γ. So β^ϕ is adjacent to α^ϕ and therefore ϕ is a graph automorphism of Γ. Put $\Gamma_0 = \Big\{\{\mu, \mu^\phi\} \mid \mu \in \Gamma\Big\}$ and let $\{\mu, \mu^\phi\}$ be adjacent to $\{\lambda, \lambda^\phi\}$ if μ is adjacent to λ or λ^ϕ. Then $|\Gamma_0| = 100$, M has orbits of lengths 1, 22 and 77 on Γ_0 and H acts transitively on Γ_0. So as above Γ_0 is the Higman-Sims graph and $\mathrm{Aut}(\Gamma_0) \cong \mathrm{Aut}(HS)$. Let N be the kernel of the action of $\mathrm{Aut}(\Gamma)$ on Γ_0. We claim that $N = \{1, \phi\}$. Indeed, let $n \in N$. Then $\alpha^n \in \{\alpha, \alpha^\phi\}$ and replacing n by $n\phi$ if necessary we may assume that $\alpha^n = \alpha$. Since β^ϕ is not adjacent to α, we have $\beta^n = \beta$. So n fixes the neighbors of all its fixed-points and since Γ is connected, we conclude that $n = 1$. Thus $N = \{1, \phi\}$ and $\mathrm{Aut}(\Gamma) \cong C_2 \times \mathrm{Aut}(HS)$. Further, $|H| = 200 \cdot |M| = 2 \cdot |HS|$ and so $H \cong \mathrm{Aut}(HS)$ or $C_2 \times HS$ and the lemma is proved.
QED

Lemma 3.5 *(a)* G *has a subgroup* T *of order 3 with* $N_G(T) \sim SU_6(5) \circ SU_3(5)).Sym(3)$*.*

(b) Put $U = N_G(T)$, $U_1 = [V, T]$ *and* $U_2 = C_V(T)$*. Then* $V = U_1 \oplus U_2$*, moreover,* U_1 *and* U_2 *are irreducible as* U *modules,* $U_1 \cong W_6 \otimes_{GF(25)} W_3$ *and* $GF(25) \otimes_{GF(5)} U_2 \cong \bigwedge^3 W_6$*, where* W_i *is the natural* $i-$*dimensional* $GF(25)-$*module for* $SU_i(5)$*, for i=3,6.*

(c) $N_G(U_1) = U$*.*

Proof: It is clear from the extended Dynkin diagram of type E_7 that $2.E_7(\mathbf{K})$ has a subgroup $H \cong SL_3(\mathbf{K}) \circ SL_6(\mathbf{K})$. Moreover, the central involution of the Weyl group induces a graph automorphism on both of the factors and so an application of Lang's theorem yields a subgroup $(SU_6(5) \circ SU_3(5)).Sym(3)$ in $E_7(5)$. Using the embedding of $\mathbf{K}^{1+56}2.E_7(\mathbf{K})$ in $E_8(\mathbf{K})$, the Steinberg relations and weight theory it is easy to check that the 56−dimensional $\mathbf{K}E_7(\mathbf{K})-$module is as an $H-$module the direct sum of $X_3 \otimes X_6$, $X_3^* \otimes X_6^*$ and $\bigwedge^3 X_6$ where X_i is a natural module for $SL_i(\mathbf{K})$, $i = 3, 6$. As H is a maximal connected closed subgroup of $2.E_7(\mathbf{K})$ and is of index two in its normalizer, all the statements of the lemma are now readily verified.

Lemma 3.6 *There exists an involution* $\bar{f}$ *in* $\overline{U}\backslash\overline{U}'$ *such that* $C_{\overline{U}}(\bar{f}) \sim L_4(5).2^2 \times Sym(5) \times \langle\bar{f}\rangle$. *Moreover, for any such* $\bar{f}$,

$$C_{\overline{G}}(\bar{f}) \sim (2 \times L_8(5)).2$$

and $C_{\overline{U}}(\bar{f})$ *acts transitively on the elementary abelian subgroups of order 16 contained in the normal subgroup* $L_4(5)$ *in* $C_{\overline{U}}(f)$.

Proof: It is easy to verify that $\mathrm{Aut}(U_6(5))$ has three classes of involutions that do not induce a diagonal automorphism on $U_6(5)$. The derived groups of the respective centralizers in $U_6(5)$ are $PSp_6(5)$, $D_3(5)$ and ${}^2D_3(5)$, and the first two of these three classes of involutions lie in the same coset of $\mathrm{Inn}(U_6(5))$.

Since $\Omega_6^-(5)$ ($\cong 2.{}^2D_3(5)$) acts absolutely irreducibly on the exterior cube of its natural module, we conclude that the centralizer of $\Omega_6^-(5)$ on the 20−dimensional module lies in the center of the full linear group acting on the 20−space. It follows that $\overline{U} \setminus \overline{U}'$ contains no involution centralizing a ${}^2D_3(5)$ in $U_6(5)$ and so contains an involution centralizing a $D_3(5)$ in $U_6(5)$.

Let $\bar{f}$ be any such involution. Note that the normalizer of $D_3(5)$ in $U_6(5)$ is $PSO_6{}^-(5)$ extended by an involution which multiplies the quadratic form associated to $PSO_6{}^-(5)$ by a fourth root of unity. So $C_{U_6(5)}(\bar{f}) \sim L_4(5).2^2$ and the two classes of elementary abelian subgroups of order 16 in $C_{U_6(5)}(\bar{f})'$ are fused in $C_{U_6(5)}(\bar{f})$. Moreover, $\mathrm{Aut}(U_3(5))$ has exactly one class of involutions outside $\mathrm{Inn}(U_3(5))$ and the corresponding centralizers are $Sym(5)$'s. Therefore $C_{\overline{U}'}(\bar{f}) \sim L_4(5).2^2 \times Sym(5)$.

It remains to determine $C_{\overline{G}}(\bar{f})$. Note that $\overline{G}$ has three classes of involutions whose centralizers have shapes $2.(L_2(5) \times D_6(5)).2$, $(C_2 \times E_6(5)).2$, and $(C_2 \times L_8(5)).2$. Under the actions of the derived groups of these centralizers V decomposes into direct sums of irreducible modules of dimensions 24 and 32; 1, 1, 27, and 27; and 28 and 28, respectively. On the other hand, from the action on the 20− and 36−spaces, we know that V is the direct sum of irreducible modules of dimensions $18, 18, 10$ and 10 for $C_U(f)'$. It follows that $C_{\overline{G}}(\bar{f}) \sim (C_2 \times L_8(5)).2$, and the lemma is proved. **QED**

From now on let T, U and f be as in Lemma 3.6. Note that f^2 is the central involution of G. Put $N = C_U(f)$, $F = \langle f \rangle$ and $R = N_G(F)$. Then $\overline{R} = C_{\overline{G}}(\bar{f})$ and so by Lemma 3.6 $R \sim C_4 \circ 2 \cdot L_8(5).2$. Let $\widehat{R}'$ be a group with $\widehat{R}' \cong SL_8(5)$ so that $\widehat{R}'$ has R' as a quotient group. For X in R', let $\widehat{X}$ be the inverse image of X in $\widehat{R}'$. As $Z(\bar{N}') = 1$, it is easy to see that the natural 8−dimensional module for $\widehat{R}'$ is, as a module for $\hat{N}'$, the tensor product of a 4−dimensional module for $SL_4(5)$ and a 2−dimensional module for $SL_2(5)$. Since elements in $GL_4(5) \otimes GL_2(5) \leq GL_8(5)$ have determinant plus or minus one, $\overline{R}'$ has two classes of subgroups isomorphic to $L_4(5) \times L_2(5)$. Since $R = NR'$, R fixes these classes. Moreover, as the element inverting f can be chosen to invert a Cartan subgroup of R', R does not induce an outer diagonal automorphism on R'.

The character tables of $L_3(4)$ and its covers (see [3]) show that there is a group of shape $4.L_3(4)$ which has a faithful irreducible character χ of degree 8. Note that R contains a subgroup L of shape $2.L_3(4)$. We plan to extend L to a subgroup M_{22} and then to a subgroup HS of G. Let S be a Sylow 2−subgroup of L, let $B = N_L(S)$ and let A_1 and A_2 be the two elementary abelian groups of order 2^5 in S. Note that $\widehat{L}$ is perfect and that $\widehat{A}_i$ is the central product of a cyclic group of order 4 with an extra-special group of order 2^5. Moreover a natural 8−dimensional module for $\hat{R}'$ is as an $\widehat{A}_i$−module the direct sum of two isomorphic irreducible modules of dimension 4. Thus $C_{\widehat{R}'}(\widehat{A}_i) \cong GL_2(5)$ and we can choose L, S and A_1, so that $\overline{A}_1$ is contained in the normal $L_4(5)$ in $\overline{N}$. It follows that $N_{\overline{R}'}(\overline{A}_1) \le N$ and has shape $2^4 Sym(6) \times Sym(5)$. Let $\overline{B}_2$ be the projection of A_2 onto the $L_4(5)$ in N. Let $\overline{B}_2$ be the projection of A_2 onto the $L_4(5)$ in N. Put $L_i = N_L(A_i)$. Our goal is to show that both L_i's can be extended to a subgroup $2^5 Sym(6)$ in U. Inside $2^5 Sym(6)$ we will choose appropriate subgroups $2^5 Sym(5)$ and $2^5 Alt(6)$ which will allow us to apply Lemma 3.3 and Lemma 3.4 to find M_{22} and HS in $\overline{G}$.

Lemma 3.7 *In R', the subgroup A_2 is conjugate to B_2 but not to A_1.*

Proof: Put $C_i = O^2(C_{\widehat{R}'}(\widehat{A}_i))$. Then $C_i \cong SL_2(5)$. Suppose that $[S, C_1] = 1$. Then $C_1 \le C_{\widehat{R}'}(\widehat{A}_2)$ and $C_1 = C_2$. Since $L = \langle L_1, L_2 \rangle$, the group L normalizes C_1, a contradiction. Hence $[S, C_1] \neq 1$ and similarly $[S, C_2] \neq 1$. As $B/A_i \cong Alt(4)$, we have $B = O^2(B)A_i$. Since $Out(C_i)$ is a 2−group and A_i centralizes C_i we conclude that S induces inner automorphisms on C_i. Hence S normalizes a unique subgroup Q_8 in C_i. Denote this Q_8 by Q_i and note that S induces inner automorphisms on Q_1. In particular $[\widehat{A}_2, Q_1] \le Z(Q_1) \cdot Z(\widehat{R}')$. Thus Q_1 induces inner automorphisms on $\widehat{A}_2$. Put $R_i = Q_1 \widehat{A}_i$ (where we really mean Q_1 and not Q_i). Then R_1 and R_2 are both the central product of an extra-special group of order 2^7 with a cyclic group of order 4. Put $X = C_{R_2}(\widehat{A}_2)$. It follows that $R_2 = X\widehat{A}_2$, that S normalizes X and that X contains a Q_8 invariant under S. Thus $Q_2 \le X$, $R_2 = Q_2\widehat{A}_2 = Q_2 B_2$ and $\hat{B}_2 = C_{R_2}(Q_1)$.

Note that $N_{\widehat{R}'}(R_1)/R_1 \cong Sp_6(2)$. Note $\bar{A}_1$ and $\bar{B}_2$ are both nondegenerate 4−spaces in the 6−dimensional symplectic space $R_1/Z(R_1)$ (where the symplectic form is given by the commutator map). Hence by Witt's theorem, A_1 and B_2 are conjugate under $N_{\widehat{R}'}(R_1)$ proving the first statement of the lemma.

Since $C_{\widehat{R}'}(\widehat{A}_i)$ acts transitively on the Q_8's in $C_{\widehat{R}'}(\widehat{A}_i)$ and since $N_{\widehat{R}'}(A_1) \cap N_{\widehat{R}'}(Q_1)$ induces the full automorphism group of Q_1 on Q_1, we conclude that A_1 and B_2 are conjugate in R' if and only if they are conjugate under $Y = C_{\widehat{R}'}(Q_1)$. Note that Y is isomorphic to the subgroup of index two in $GL_4(5)$. Since B normalizes Y and $[A_1, B] = A_1$, A_1 and hence also B_2 are contained in Y'. Put $S_0 = A_1 B_2$. Since A_1 and B_2 normalize each other we conclude that S_0 is a Sylow 2−subgroup of $Y/Z(Y)$ and that A_1 and B_2 are the two maximal elementary abelian subgroups of S_0. It follows that A_1 and B_2 are not conjugate in Y'. Moreover, $\mathrm{Out}(Y') \cong D_8$, $\mathrm{Out}(Y')$ acts on $\{A_1^{Y'}, B_2^{Y'}\}$ and $\mathrm{Out}(Y')'$ fixes $A_1^{Y'}$ and $B_2^{Y'}$. As the group of outer automorphisms of Y' induced by Y is $\mathrm{Out}(Y')'$, A_1 and B_2 are not conjugate in Y. So A_1 and B_2 are not conjugate in R' and lemma is established. **QED**

Lemma 3.8 *$N_{\overline{R}'}(\overline{A}_1)$ acts transitively on $L_3(4)$'s in $\overline{R}'$ containing $\overline{A}_1$ and on subgroups $2^4 Alt(5)$ in $N_{\overline{R}'}(\overline{A}_1)$ which can be extended to an $L_3(4)$ in $\overline{R}'$.*

Proof: Recall that $N_{\overline{R}'}(\overline{A}_1) \sim 2^4 Sym(6) \times Sym(5)$ and, as $[S, C_i] \neq 1$ in the notation of the previous lemma, any $2^4 Alt(5)$ in $N_{\overline{R}'}(\overline{A}_1)$, which can be extended to a $L_3(4)$ in $\overline{R}'$, projects non-trivially on the $Sym(5)$. Hence $N_{\overline{R}'}(\overline{A}_1)$ acts transitively on such subgroups. Note that $\overline{L}_1$ is such a subgroup and that $L_1^* \stackrel{def}{=} N_{\overline{R}'}(\overline{L}_1) \sim 2^4 Sym(5)$. Put $\overline{W} = N_{\overline{R}'}(\overline{L}_1) \cap N_{\overline{R}'}(\overline{A}_2)$. As $\bar{A}_1$ and $\bar{A}_2$ are the only maximal elementary abelian subgroups of $\bar{S} = \bar{A}_1 \bar{A}_2$, we have

$N_{L_1^*}(A_2) = N_{L_1^*}(S)$. Since S/A_1 is the Sylow $2-$subgroup of L_1/A_1, we have $\overline{W} \sim 2^4 Sym(4)$. We claim that W is contained in a $2^4 Alt(6) \times Sym(5)$ subgroup of $N_{\overline{R}'}(\overline{A}_1)$. For this let i be an involution in $\overline{W} \setminus \overline{L}_1$. Then it is enough to show that the inverse image of $[\widehat{A}_2, i]$ is not elementary abelian. Let C_2 be the projection of A_2 onto the normal $Sym(5)$ in $\overline{N}$. Then $[\widehat{B}_2, i]$ is elementary abelian, while $[\widehat{C}_2, i]$ is not. So also $[\widehat{A}_2, i]$ is not elementary abelian, and the claim is proved.

It is now easy to see that $\overline{W} \cap \overline{L}_1$ is contained in exactly two subgroups $2^4 Alt(5)$ of $N_{\overline{R}'}(\overline{A}_2)$ and these two subgroups are interchanged by W. Since any $L_3(4)$ in $\overline{R}'$ containing $\overline{L}_1$ is generated by $\overline{L}_1$ and a $2^4 Alt(5)$ in $N_{\overline{R}'}(\overline{A}_2)$ containing $\overline{W} \cap \overline{L}_1$ the lemma is proved. **QED**

Lemma 3.9 *Put $L_0 = N_R(L)$. Then $|L_0/LF| = 2$ and A_1 and A_2 are conjugate in L_0.*

Proof: Since $\mathrm{Out}(R'/Z(R')) \cong D_8$, since R' has four orbits on $A_1^{\mathrm{Aut}(R')}$ and since $PGL_8(5)$ acts transitively on those four orbits, the normalizer of any such orbit in $\mathrm{Out}(R')$ is a group of order 2 that is not contained in the center of $\mathrm{Out}(R')$. It follows that R fixes two of these orbits and interchanges the remaining two. Moreover, by Lemma 3.8, $L_8(5)$ has four orbits on $(A_1, L)^{\mathrm{Aut}(R')}$ and, by Lemma 3.7, each orbit of subgroups $L_3(4)$ in $\overline{R}'$ leads to two orbits of R' on $(A_1, L)^{\mathrm{Aut}(R')}$. It follows that $\overline{R}'$ has exactly two classes of subgroups $L_3(4)$. Suppose R interchanges those two classes. Then R could not normalize any of the orbits of R' on $A_1^{\mathrm{Aut}(R')}$, a contradiction. So $|L_0/LF| = 2$. Suppose that A_1 and A_2 are not conjugate in L_0. Then they are also not conjugate in R. By Lemma 3.7, we conclude that A_1 and B_2 are not conjugate in R, and this contradicts Lemma 3.6. So A_1 and A_2 must be conjugate in L_0. **QED**

Lemma 3.10 *Put $X = N_G(A_1)$. Then $X \leq U$ and $X \sim 6.(2^4.3^4.Sym(6) \times U_3(5)).Sym(3)$.*

Proof: Let $X_0 = N_U(A_1)$. By the action of A_1 on the natural $6-$dimensional $GF(25)-$module W for $SU_6(5)$ we see that, modulo the normal $SU_3(5)$ in U, X_0 is a full monomial subgroup of $U_6(5).Sym(3)$. It follows that $X_0 \sim 6.(2^4.3^4.Sym(6) \times U_3(5)).Sym(3)$. Moreover, X_0 has two orbits Σ_1 and Σ_2 on the hyperplanes in A_1 which do not contain $Z(G)$. Choose notation so that $|\Sigma_1| = 6$ and $|\Sigma_2| = 10$. Recall that $V \cong U_1 \oplus U_2$ where U_1 and U_2 are defined and described in Lemma 3.5.

Let H_1, H_2, H_3 be three different elements of Σ_1. Then its is easy to check that $H_1 \cap H_2 \not\leq H_3$. As $W = \bigoplus_{H \in \Sigma_1}(C_W(H))$, this implies that H_1 acts fixed–point freely on U_2. Since U_1 is a direct sum of copies of W as an A_1-module, we get $\bigoplus_{H \in \Sigma_1} C_V(H) = U_1$.

Also $C_V(H)$ is either $6-$dimensional, if $H \in \Sigma_1$, or $20/10 = 2-$dimensional, if $H \in \Sigma_2$. Thus $N_G(A_1)$ normalizes Σ_1 and so also U_1. Since U is maximal in G, we conclude that $X \leq U$. Hence $X = X_0$. **QED**

Lemma 3.11 *There exists $t \in N_R(L)$ and $D \leq U$ such that $t^2 \in L$, $A_1^t = A_2$, $L_1 \leq D$, $D \sim 2^5 Sym(6)$, t normalizes $N_D(B)$ and t does not normalize $N_{D'}(B)$.*

Proof: Let $Y = X/A_1$. Then $Y \sim 3.(3^4 Sym(6) \times U_3(5))Sym(3)$. Let K be the image of L_1 in Y. Then $K \cong Alt(5)$ and we are looking for subgroups $Sym(6)$ of Y containing K. Let

Y_1 be the normal subgroup $3.3^4 Sym(6)$ of Y, let Y_2 be the normal subgroup $SU_3(5)$ of Y and let K_i be the projection of K onto Y_i. Then Y acts transitively on subgroups $3 \cdot Alt(6)$ (the triple cover of $Alt(6)$) and transitively on subgroups $Alt(5)$ in Y_2. Moreover, the normalizer of an $Alt(5)$ in $U_3(5).Sym(3)$ is a $C_2 \times Sym(5)$ and the normalizer of an $Alt(6)$ is $Aut(Alt(6))$. It follows that K_2 can be embedded into exactly two subgroups $3 \cdot Alt(6)$ of Y_2 and f interchanges these two $3 \cdot Alt(6)$'s. Furthermore Y has one orbit on subgroups $3 \cdot Alt(6)$ in Y_1 and one orbit on subgroups $Alt(5)$ in Y_1 for which $\overline{A}_1$ is a natural $SL_2(4)-$module. (Note here that $3 \cdot Alt(6)$ exists in Y_1, since $3^4 Alt(6)$ has 9 classes of $Alt(6)$'s while $3^{1+4} Alt(6)$ has only 3 classes.) Now $Y/Y_2 \sim 3^{4+1}(C_2 \times Sym(6))$. The normalizer of the image of K in Y/Y_2 is a $C_2 \times Sym(5)$ and the normalizer of the image of a $3 \cdot Alt(6)$ of Y_1 in Y/Y_2 is a $Sym(6)$. It follows that K_1 can be embedded into exactly two subgroups $3 \cdot Alt(6)$ of Y_1 and f interchanges these two $3 \cdot Alt(6)$'s. Let D_i be any of the two subgroups $3 \cdot Alt(6)$ in Y_i with $K_i \leq D_i$. Then there exists precisely one subgroup A in $D_1 D_2$ such that $K \leq A$, $A = A'$ and $A/Z(A) \cong Alt(6)$. Similarly there exists precisely one subgroup $\widehat{A}$ in $D_1^f D_2$ such that $K \leq \widehat{A}$, $\widehat{A} = \widehat{A}'$ and $\widehat{A}/Z(\widehat{A}) \cong Alt(6)$. We claim that exactly one of A and $\widehat{A}$ is an $Alt(6)$, while the other is the triple cover. Indeed, let x_i, y_i be elements of order 3 in D_i such that $\langle x_1 x_2, y_1 y_2 \rangle Z(Y)$ is a Sylow $3-$subgroup of $AZ(Y)$. Then $\langle {x_1}^f {x_2}^f, y_1 y_2 \rangle Z(Y)$ is a Sylow $3-$subgroup of $\widehat{A}Z(Y)$. Note that

$$[x_1 x_2, y_1 y_2] = [x_1, y_1]\,[x_2, y_2] \quad \text{and} \quad [{x_1}^f {x_2}^f, y_1 y_2] = [x_1, y_1]^f\,[x_2, y_2]. \qquad (*)$$

Since $[x_1, y_1]$ and $[x_2, y_2]$ are both contained in $Z(Y)$ and unequal to 1 and since f inverts $Z(Y)$, we see that exactly one of the two expressions in $(*)$ is equal to 1. This proves our claim.

Choose notation so that $A \cong Alt(6)$. From what we proved so far it follows that A and A^f are the only two $Alt(6)$ subgroups in Y which contain K. It is easy to see that $N_Y(K)/Z(Y) \cong C_2 \times Sym(5)$. Furthermore, there exists a subgroup of index 2 in $N_Y(K)$ which normalizes A. Since f does not normalize A, this subgroup is, modulo the center of Y, isomorphic to $Sym(5)$. Put $E = A(N_Y(K) \cup N_Y(A))$ and let $\widehat{D}$ be the inverse image of E in X. Then $E/Z(Y) \cong Sym(6)$ and $\widehat{D}/T \cong 2^5 Sym(6)$. (Recall that T is the cyclic group of order three with $U = N_G(T)$.)

By Lemma 3.9, there exists $t \in N_R(L)$ with ${A_1}^t = A_2$. Choose t so that t normalizes B. Then $t^2 \in BF$ and since t inverts F, we have $t^2 \in B$. In particular $t^2 \in L$. Note that A_1 and A_2 are the only elementary abelian groups of order 2^5 in B. Put $J = N_G(B) \cap N_G(A_1)$. As $t \in N_G(B) \setminus J$, we conclude that J is of index two in $N_G(B)$. For $Q \subset N_G(B)$ let Q^* be the image of Q in $N_G(B)/B$. Since $J \leq X$, it is easily verified that J^* is an elementary abelian group of order 9 extended by an elementary abelian group of order 8. Pick a in $N_{\widehat{D}'}(B) \setminus BT$ and b in $N_{\widehat{D}}(B)$ with $[a, B] \leq A_1$ and such that a^* and b^* are involutions. Since $U_3(5)$ contains no $Sym(6)$, b induces an outer automorphism on Y_2. The same is true for f and so b and f both invert $O_3(J^*)$. Note that a centralizes T and inverts $O_3(J^*)/T$. As A_1 is in the $SU_6(5)$ subgroup of U but A_2 is not, the element t is not in U. Since $T \leq O_3(J)$, we conclude $O_3(J)^* = T^* T^{*t} = O_3(J^*)$. It follows that $\langle a^*, t^* \rangle$ acts as a D_8 on $O_3(J^*)$. Since $\langle a^*, t^* \rangle$ is a dihedral group, we conclude that $\langle a^*, t^* \rangle \cong D_8$. Let $x^* = [a^*, t^*]$.

We claim that $x^* T^* = b^* T^*$. Indeed, x^* inverts $O_3(J^*)$ and $|C_{N_G(B)^*}(O_3(J)^*)/O_3(J^*)| = 2$. Hence x^* lies in the same coset of $O_3(J^*)$ as f^* or as b^*. Since $N_{\bar{R}'}(A_1) \sim 2^4.Sym(6) \times Sym(5)$, $N_{R'}(B)^* \cong C_2 \times C_2$. Furthermore f and t are in $N_R(B)$ and so $N_R(B)^*$ is a Sylow $2-$subgroup of $N_G(B)^*$. Since $f \notin R'$ we conclude that $f^* \notin N_G(B)^{*\prime} O_3(J^*) = \langle x^* \rangle O_3(J^*)$. So $x^* O_3(J^*) = b^* O_3(J^*)$. Moreover, a^* centralizes b^* and x^* and hence $b^* T^* = C_{x^* O_3(J^*)}(a^*) = x^* T^*$.

In particular, we can choose b so that $b^* = x^* = [a^*, b^*]$. Put $D = \widehat{D}' \langle b \rangle$. Then $\overline{D} \sim 2^4 Sym(6)$. In addition, $N_D(B) = B \langle a, b \rangle$ and so t normalizes $N_D(B)$. On the other hand, $N_{D'}(B) = B\langle a \rangle$ and so $N_{D'}(B)^t = B\langle ab \rangle \neq N_{D'}(B)$. **QED**

Proof of Theorem 3.1:

We are now able to construct HS and M_{22} in $\bar{G}$. For this choose L, t and D as in Lemma 3.11 and put $M_1 = N_D(L_1)$. By Lemma 3.10, $N_{D'^t}(B)$ is contained in D, but not in D'. Since $N_{D'^t}(B)/O_2(D) \cong Sym(4)$, we conclude that $N_{D'^t}(B)$ is contained in M_1. Note that $L_1^t = L_2$ and so $L_2 \leq D'^t$. Put $M_2 = D'^t$. Then $\overline{M}_1 \sim 2^4 Sym(5)$ and $\overline{M}_2 \sim 2^4 Alt(6)$. Moreover,

$$M_1 \cap L = L_1, \; M_2 \cap L = L_2, \quad \text{and} \quad M_1 \cap M_2 = N_{D'^t}(B).$$

Put $M = \langle L, M_1, M_2 \rangle$. Then by Lemma 3.3, $\overline{M} \cong M_{22}$. Now $D \cap M = M_1$, $D^t \cap M = M_2$ and $D \cap D^t = N_D(B)$. Let $H = \langle D, L, t \rangle$. Then by Lemma 3.4, $\bar{H} \cong HS, C_2 \times HS$ or $Aut(HS)$. Thus in any case $\bar{H}' \cong HS$ and Theorem 3.1 is proved. The dedicated reader might check that actually $\bar{H}$ itself is already the Higman-Sims group.

4 A Computational proof that HS is a Subgroup of $E_7(5)$.

In this section we give a computer dependent proof that $HS < E_7(5)$. Our strategy is to use a machine calculation to prove that HS acts (absolutely) irreducibly on a $133-$dimensional, $5-$modular, Lie algebra. We then apply the extensive theory of modular Lie algebras to deduce that the Lie algebra is simple, that it is a classical modular Lie algebra of type E_7 over $GF(5)$, and thence $HS < E_7(5)$.

Computation 4.1 *We construct an explicit* $133-$*dimensional (absolutely) irreducible matrix representation of* HS *over* $GF(5)$.

Method: We remark that although it seems natural to construct the $133-$dimensional representation as a constituent of a tensor product of smaller representations of HS, all useful tensor products are too large for our implementation of the meataxe. For example, the $133-$dimensional, $5-$modular representations of HS are constituents in the symmetric cube of the $21-$dimensional representation and in the tensor product of a $21-$dimensional representation with a $55-$dimensional representation, however these representations have degrees 1771 and 1155. In order to avoid such large computations, we shall locate a $133-$dimensional representation as a constituent of the symmetric square of a $28-$dimensional representation of the double cover of HS: this latter representation can be found in a previously known representation of the Harada–Norton group.

We start with the $133-$dimensional matrix representation of HN over $GF(5)$ that is constructed in [15]. We locate matrices, x_1 and y_1, that represent HN elements of classes $40A$ and $12C$ (since these classes have small centralizers, we locate such elements by a random search). Let $x = {x_1}^{20}$. Every dihedral group generated by the $2A-$element x and a conjugate of the

$2B-$element ${y_1}^6$ has a central involution. By collecting such involutio ns together with the matrix x_1, it is an easy matter to generate enough matrices to represent the centralizer of x in HN (we just keep adding involutions until we observe a group that contains an element of order 11). The group $C_{HN}(x)$ has structure $2.HS.2$.

We use the meataxe [10] to decompose the restriction of our $HN-$module into its irreducible constituents of degrees 1, 21, 28, 28, and 55, under the group $2.HS = (C_{HN}(x))'$. Another application of the meataxe to the symmetric square of either of the irreducible $28-$dimensional $2.HS-$modules yields an (absolutely) irreducible matrix representation of HS of degree 133. **QED**

Let E denote the $133-$dimensional $HS-$module afforded by the matrix representation of Computation 4.1. In our calculations with E we shall use a fixed basis $e_1, e_2, \ldots, e_{133}$ of E: moreover for technical reasons, we use a basis on which a particular subgroup

$$P \sim 2^4.2^3 < 2^4.(2 \times Sym(4)) < 2^4.Sym(6) < HS$$

acts monomially. We let ${e_1}^*, {e_2}^*, \ldots, {e_{133}}^*$ denote the dual basis of the dual module E^* (this module is isomorphic to E, but for computational purposes it is convenient to distinguish E and E^*).

Computation 4.2 *We compute an $HS-$invariant product, $*$: $\Lambda^2 E \to E$.*

Method: The output from this computation is a list of components, $a_{i,j,k}$ of an invariant rank three tensor such that the map $e_i \wedge e_j \mapsto \sum_k a_{i,j,k}\, e_k$ extends to an $HS-$invariant multilinear map. It is convenient to use duality to observe that the map ${e_k}^* \mapsto \sum_{i,j} a_{i,j,k}\, {e_i}^* \wedge {e_j}^*$ extends to an $HS-$invariant multilinear map. Moreover, since the group HS acts irreducibly on E^*, it is easy to use the group action to compute these tensor components once we know the image of any single vector of E^* under an $HS-$invariant map: $E^* \to \Lambda^2 E^*$.

The module $\Lambda^2 E^*$ has degree 8778 and is too large to decompose directly with our implementation of the meataxe: in order to locate all copies of E^* in $\Lambda^2 E^*$ we use the condensation techniques described in [14]. Let π denote the idempotent $(\sum_{p \in P} p)/|P|$ of the group algebra $GF(5)HS$. The condensation programs of [14] compute matrix representations of the Hecke algebra $\pi GF(5)HS\pi$ on the condensed modules $E^*\pi$ and $\Lambda^2 E^*\pi$ (which have degrees 1 and 50). (It is in the computation of these matrix representations of the Hecke algebra that our programs require the group P to act monomially on E and E^*.) A standard meataxe calculation locates the single copy of $E^*\pi$ in the $\pi GF(5)HS\pi-$module $\Lambda^2 E^*\pi$. Thus there is a single embedding of E^* in the $HS-$module $\Lambda^2 E^*$. Moreover, the embedding of Hecke algebra modules gives the image of the $1-$dimensional space of fixed points of P on E^* under the $HS-$invariant map: $E^* \to \Lambda^2 E^*$. As we remarked above, the action of HS now determines the components of the $HS-$invariant tensor $a_{i,j,k}$. **QED**

For each $e \in E$ we write $*e$ for the matrix that represents the action of right multiplication by e on our $HS-$invariant algebra. After completing Computation 4.2, we ran a simple precautionary program to verify $HS-$invariance of our tensor. For each basis vector e_i and for each of generator, h, of HS, we checked that the matrices $(*e_i)^h$ and $*({e_i}^h)$ are identical.

Computation 4.3 *The $HS-$invariant product $*$: $\Lambda^2 E \to E$ of Computation 2 is a Lie product on E. Moreover the Killing form on $(E, *)$ is non-singular.*

Method: A straightforward computation shows that for each basis vector e_i we have

$$(*e_i)(*e_1) - (*e_1)(*e_i) - (*((e_i)(*e_1))) = 0.$$

Hence the Jacobi identity holds for any triple of basis vectors of the form e_1, e_i, e_j. Therefore right multiplication by e_1 is a derivation of $(E, *)$; and, by applying the action of HS, we deduce that $*(e_1^h)$ is a derivation of $(E, *)$ for any choice of $h \in HS$. Since HS is irreducible on E, we deduce that $*$ is a Lie product on E.

A random search quickly produces $e \in E$ with $\mathrm{Tr}((*e)(*e)) \neq 0$. It follows that the Killing form on E is not identically zero: irreducibility of E as a $HS-$module now shows that the Killing form is non-singular. **QED**

We complete the proof that $HS < E_7(5)$ by applying standard results to show that the automorphism group of $(E, *)$ can only be $\mathrm{Aut}(E_7(5))$. The following lemma from [13] shows that $(E, *)$ is a simple Lie algebra.

Lemma 4.4 *Suppose that $(X, *)$ is a finite dimensional (non-associative) algebra and that $A \leq Aut(X, *)$ acts irreducibly on X. Then one of the following holds:*
(a) The algebra $(X, *)$ is simple.
(b) The $A-$module X is induced from a module of a proper subgroup of A.
(c) The product $*$ is identically zero.

Proof: Let I be a minimal non-zero ideal of $(X, *)$, and let $\mathcal{I} = \{I^a | a \in A\}$. We say that a subset of $\mathcal{I}$ is independent if it consists of independent (vector) subspaces of X. Let $\mathcal{J} = \{I_1, I_2, \dots I_l\}$ be a maximal independent subset of $\mathcal{I}$. Let $Y = \oplus_{k=1}^{l} I_k$, then Y is an ideal of $(X, *)$.

Let I^a be any $A-$image of I. Maximality of $\mathcal{J}$ shows that $I^a \cap Y$ is a non-zero ideal; hence, since I^a is a minimal ideal, we have $I^a \subset Y$. Thus, Y contains a non-zero $A-$submodule of X, and, since X is irreducible, we have $X = Y$.

We now suppose that neither (a) nor (b) holds: thus $I \neq X$ and hence $\mathrm{Stab}_A I$ is a proper subgroup of A. Moreover, since X is not induced, there is an $a \in A$ with $I^a \notin \mathcal{J}$. Then, $I^a * I_k \subset I^a \cap I_k = \{0\}$, for each $I_k \in \mathcal{J}$. Thus $I^a * X = I^a * Y = \sum I^a * I_k = \{0\}$. The $A-$invariance of $*$ now gives $I_k * X = \{0\}$ for each $I_k \in \mathcal{J}$, and thus $X * X = \sum I_k * X = \{0\}$.
QED

Let $(\overline{E}, *)$ be the Lie algebra obtained from $(E, *)$ by extending the scalars to the algebraic closure of $GF(5)$. Since E is absolutely irreducible as a $HS-$module and it is not induced (since HS has no subgroup of index 133), Lemma 4.4 shows that the Lie algebra $(\overline{E}, *)$ is simple. Moreover, by Computation 4.3, the simple Lie algebra $(\overline{E}, *)$ has a non-singular Killing form.

Over an algebraically closed field, F say, of characteristic $p > 3$, the modular Lie algebras with a non-singular trace form are completely classified by a theorem of Block and Zassenhaus [1] (this result is also given in [16], page 49). Block and Zassenhaus show that such a modular

Lie algebra is a direct sum of abelian Lie algebras, total matrix algebras $M_n(F)$ where $p|n$, and classical simple Lie algebras of types $A_1, \ldots, E_8$. In particular, our algebra $(\overline{E}, *)$ must be the classical simple Lie algebra of type E_7 (since no other simple algebra in the list provided by [1] has dimension 133). Therefore, the $HS-$invariant algebra $(E, *)$ is a $GF(5)-$form of E_7. By Theorem IV.6.1 of [16] there is just one $GF(5)-$form of E_7 : thus $(E, *)$ is the classical simple Lie algebra of type E_7 over $GF(5)$. It now follows from [18] that $Aut(E, *)$ has structure $E_7(5).2$ and we obtain $HS < E_7(5)$.

References

[1] R. Block and H. Zassenhaus, The Lie algebras with a nondegenerate trace form, *Ill. J. Math.* **8** (1964), 543–549.

[2] R. W. Carter, *Finite groups of Lie type : Conjugacy classes and complex characters* Wiley, New York, 1985.

[3] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *The Atlas of Finite Group*, Oxford University Press, London, 1985.

[4] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices, and groups* 2nd ed., Springer-Verlag, New York, 1992.

[5] P. S. Fan: Amalgams of Prime Index, *J. Algebra* **98** (1986), 375–421.

[6] D. Gorenstein *Finite Groups*, Chelsea Publishing Company, New York, 1982.

[7] R. L. Griess and A. J. E. Ryba, Embeddings of $U_3(8)$, $Sz(8)$ and the Rudvalis group in algebraic groups of type E_7., *Invent. Math.* **116** (1994), 215–241.

[8] D. G. Higman and C. C. Sims, A Simple Group of Order 44,352,000, *Math. Z.* **105** (1968), 110–113.

[9] Peter B. Kleidman and R. A. Wilson, Sporadic Subgroups of Finite Exceptional Groups of Lie Type, *J. Alg.* **157** (1993), 316–330.

[10] R. A. Parker, The Computer Calculation of Modular Characters (the Meat-Axe), in M. D. Atkinson, ed., *Computational Group Theory*, Academic Press, London, 1984.

[11] R. Ree, A family of simple groups associated with the simple Lie algebra of type (F_4), *Amer. J. Math* **83** (1961), 401–420.

[12] A. Rudvalis, A Rank 3 Simple Group of Order $2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$ I, *J. Algebra* **86** (1984), 219–258.

[13] A. J. E. Ryba, *Algebras related to some sporadic simple groups*, Ph.D. Thesis, Cambridge University, 1985.

[14] A. J. E. Ryba, Condensation programs and their application to the decomposition of modular representations, *J. Symbolic Comput.* **9** (1990) 591–600.

[15] A. J. E. Ryba and R. A. Wilson, Matrix Generators for the Harada-Norton group, *Experimental Math.* **3** (1994), 137–145.

[16] G. B. Seligman, *Modular Lie Algebras*, Springer-Verlag, Berlin, 1967.

[17] L. H. Soicher, *Presentations of some finite groups*, Ph.D. Thesis, Cambridge University, 1985.

[18] R. Steinberg, Automorphisms of Classical Lie Algebras, *Pac. J. Math.* **11** (1961), 1119–1129.

[19] D. Wales, Uniqueness of the Graph of a Rank Three Group, *Pacific J. Math.***30** (1969), 271-276.