# Symplectic Automorphisms of K3-Surfaces

# (after S. Mukai and V.V. Nikulin)

Geoffrey Mason
*University of California at Santa Cruz*

A short, but fairly complete, account is given of the work of MUKAI and NIKULIN on so-called symplectic automorphisms of $K3$-surfaces. (Nikulin calls such automorphisms *algebraic*.)

## 1. INTRODUCTION

If $X$ is a $K3$-surface then, essentially by definition, $X$ has a nowhere-vanishing holomorphic 2-form $\omega$. The group $G$ of automorphisms of $X$ which preserves $\omega$ is called the group of *symplectic automorphisms* of $X$, and the combined work of MUKAI [7] and NIKULIN [8] gives a complete list of the possibilities for the isomorphism type of $G$ (it is known that $G$ is a finite group). In fact, one can be much more precise, in particular Mukai shows that there is an imbedding $i:G \rightarrow M_{23}$ where $M_{23}$ is one of the sporadic Mathieu groups (see below) and that this induces a $\mathbb{Q}G$-isomorphism from the total rational cohomology $V = H^*(X, \mathbb{Q})$ of $X$ to the usual permutation module $P$ (of degree 24) of $M_{23}$. Furthermore by Hodge theory one knows that $dim V^G \geqslant 5$ ($V^G$ = the space of $G$-invariants in $V$), so that because of the isomorphism $V \cong P$ we find that $i(G)$ has at least five orbits on the 24 letters being permuted. Mukai shows that, conversely, if $H \leqslant M_{23}$ has at least five orbits on the 24 letters then there is a $K3$-surface on which $H$ acts (effectively) as symplectic automorphisms. Because of the surprising connection with $M_{23}$, these results are of interest to finite group-theorists as well as others.

I have taken the opportunity of simplifying Mukai's group-theoretic analysis of the possibilities for $G$. Thus only some standard facts, available in [6] and the elementary parts of [4], are needed, and the only *classification* results we use are the results of BRAUER [2] giving the simple groups of order $2^a \cdot 3^b \cdot 5$ (needed only if $a \leqslant 7$, $b \leqslant 2$!). There is almost nothing new here, although we should comment that for the possibility $G \cong \mathbb{Z}_2 \times \mathbb{Z}_8$ Mukai has to refer to Nikulin, whose proof that this cannot occur is quite intricate. In fact we will eliminate this possibility quite easily at the outset, making the overall proof reasonably short.

## 2. $K3$-SURFACES

We recall some pertinent facts about $K3$-surfaces. $K3$-surfaces were named (by A. Weil) after Kummer, Kähler, Kodaira and the beautiful mountain $K2$ in Kashmir. They form one of 10 classes of minimal models of compact connected 2-dimensional complex manifolds in the Enriques-Kodaira classification (and one of 5 classes of such manifolds with Kodaira dimension 0). Double coverings of the complex projective plane with a branch curve of degree 6 having only simple singularities are examples, but there are $K3$-surfaces that cannot be constructed in this way. (In fact, the set of algebraic $K3$-surfaces is a union of countably many 19-dimensional families in the 20-dimensional family of all $K3$-surfaces.) For background material on $K3$-surfaces we refer the reader to [1]. Those readers not familiar with $K3$-surfaces may take the relevant results below as axioms without impairing their understanding of the later group-theoretic analysis.

We may define a $K3$-surface $X$ to be a compact, 2-dimensional complex manifold such that $X$ has first Betti number 0 and trivial canonical bundle. Then the cohomology space $V = H^*(X,\mathbb{Q})$ is even, that is the groups $H^1(X,\mathbb{Q})$ and $H^3(X,\mathbb{Q})$ are trivial. The Hodge decomposition yields a representation of $V$ as a direct sum

$$V = H^0(X) \oplus H^{2,0}(X) \times \oplus H^{1,1}(X) \oplus H^{0,2}(X) \oplus H^4(X)\,, \qquad (2.1)$$

each of the five summands being non-trivial. In fact we have

$$dim H^0 = dim H^{2,0} = dim H^{0,2} = dim H^4 = 1 \text{ and } dim H^{1,1} = 20\,. \qquad (2.2)$$

In particular $dim V = 24$. Now the group $G$ of symplectic automorphisms of $X$ is the group of automorphisms of $X$ which acts trivially on $H^{2,0}(X)$. Then by duality $G$ is trivial on $H^{0,2}(X)$, as well as being trivial on $H^0(X)$ and $H^4(X)$. Mukai establishes that $H^{1,1}(X)$ also has a non-zero $G$-invariant, whence

$$dim V^G \geqslant 5. \qquad (2.3)$$

## 3. THE REPRESENTATION OF $G$ ON $H^*(X,\mathbb{Q})$

We have already remarked that $G$ is a finite group, and Mukai's method is to first compute the character of $G$ on the rational $G$-space $V$. This proceeds as follows: first fix a point $p \in X$, and let $G_p = \{g \in G \mid g \cdot p = p\}$ be the corresponding isotropy group. Then $G_p$ acts on the tangent space $T_p$ at $p$ (essentially via the map $g \mapsto dg$ sending an element $g \in G_p$ to its differential). This action is faithful, so realizing $G_p$ as a subgroup of $GL(T_p) \cong GL_2(\mathbb{C})$. But in fact, because $G_p$ preserves the 2-form $\omega$, $G_p$ preserves a non-degenerate symplectic form on $T_p$, yielding

*There is an imbedding $G_p \to SL_2(\mathbb{C})$. In particular, the abelian subgroups of $G_p$ are cyclic.* (3.1)

Of course, all finite subgroups of $SL_2(\mathbb{C})$ are well known. Next, one knows that for each $g \in G$, the set $F(g) = \{p \in X \mid g{\cdot}p = p\}$ of fixed-points of $g$ is finite. Using a version of the Atiyah-Singer index theorem Mukai proves the following crucial result.

*The cardinality* $|F(g)|$ *of the g-fixed-points depends only on the order* $|g|$ *of* $g$, *and is given by the formula* $|Fg| = \frac{24}{n}\prod_{p|n}(1+\frac{1}{p})$. (3.2)

Here, $n = |g| \geq 2$, and $p$ ranges over the prime divisors of $n$. This determines the character of $G$ on $V$; because of the fact that $H^*(X,\mathbb{Q})$ is even and $F(g)$ is finite, the Lefschetz fixed-point-formula tells us the following:

*If* $V = H^*(X,\mathbb{Q})$ *affords the character* $\chi$ *of* $g$ *then for all* $1 \neq g \in G$ *we have* $\chi(g) = |F(g)|$. (3.3)

We complete this section with the possibilities for $\chi(g)$ which follow from (2.2), (3.2) and (3.3). We may write $\chi(n)$ instead of $\chi(g)$ if $g$ has order $n$, and we obtain the following

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 11 | 12 | 15 | 16 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\chi(n)$ | 24 | 8 | 6 | 4 | 4 | 2 | 3 | 2 | 2 | 2 | 1 | 1 | 1 | 1 |

(3.4)

All we need, to determine the nature of $G$, are the results (2.3) and (3.1)-(3.4), and as we said these may be taken as axioms in the following since nothing more concerning the nature of $\chi$ will be needed.

## 4. The Mathieu groups $M_{23}$ and $M_{24}$

We record some results concerning the Mathieu groups. Let $\Omega$ be a set of cardinality 24 on which the symmetric group $\Sigma_{24}$ acts in the usual fashion. $\Sigma_{24}$ contains a (maximal) subgroup $M_{24}$ (which acts quintuply transitively!) on $\Omega$. It can be defined as the stabilizer in $\Sigma_{24}$ of a collection of 759 subsets of $\Omega$ of size 8 with the property that no two have more than 4 elements of $\Omega$ in common, and is closely related to the so-called extended binary Golay code. See [3] for more details. $M_{24}$ is a simple group, as is the subgroup $M_{23}$ which is by definition the isotropy group (in $M_{24}$) of a point of $\Omega$. Both $M_{23}$ and $M_{24}$ are among the so-called sporadic simple groups, which accounts for the interest of the results to group-theorists. However, both the simplicity and sporadic nature of these groups is irrelevant as regards the present discussion. Exactly why $M_{23}$ plays a rôle is presently unclear.

Next we list those isomorphism types of subgroups of $M_{23}$ which, up to conjugacy, are maximal subject to having at least five orbits on $\Omega$. The results can be readily checked, for example, from table 3 of [3].

(i) $PSL_2(7)(\cong SL_3(2))$
(ii) $A_6(\cong PSL_2(9))$
(iii) $\Sigma_5$
(iv) $E_{16} : A_5$ (no elements of order 6)
(v) $E_9 : Q_8$

(vi) $E_9 : D_8$
(vii) $(A_4 \times A_4) : \mathbf{Z}_2$ (a 3-Sylow being inverted by an involution)
(viii) $E_{16} : D_{12}$ (trivial center)
(ix) $(Q_8 * Q_8) : \mathbf{Z}_3$ (no elements of order 12)
(x) $E_{16} : \Sigma_4$ (no elements of order 6)
(xi) $GL_2(3)(\cong Q_8 : \Sigma_3)$

Here, we have used fairly standard notation: $A_n$ is the alternating group on $n$ letters, $\Sigma_n$ the corresponding symmetric group, $E_{p^r}$ the elementary abelian group of order $p^r$ for a prime $p$, $Q_8$ the quaternion group of order 8 and $D_{2k}$ the dihedral group of order $2k$. Furthermore, if $A$ and $B$ are groups, then $A : B$ denotes a semidirect product with normal subgroup $A$, and $A * B$ a central product of $A$ and $B$ (i.e., a quotient of $A \times B$ by a subgroup of its centre). The information provided specifies a unique group in each of (i)-(xi).

We remark that the requirement of having at least five orbits on $\Omega$ does not prevent some of the groups listed exhibiting several different orbit structures (though it is evident that the *number* of orbits depends only on the group). Thus $M_{23}$ contains a conjugacy class of $PSL_2(7)$ with orbit lengths 1,1,1,7,14 and another with orbits 1,1,7,7,8.

Denote by $P$ the permutation module for $M_{24}$ obtained from its action on $\Omega$. We regard $P$ as a $\mathbf{Q}H$-module for each subgroup $H$ of $M_{24}$ by restriction. If $P$ affords the character $\pi$ then of course for $g \in M_{24}$ one has

$$\pi(g) = \# \text{ of letters in } \Omega \text{ fixed by } g.$$

It is readily verified that the following holds:

*If $g \in M_{23}$ then the value of $\pi(g)$ depends only on the order of $g$, and is given by the same formula as in (3.2), viz.* $\pi(g) = \frac{24}{n}\prod_{p|n}(1+\frac{1}{p})$ *where* $n = |g|$. (4.1)

5. Mukai's results

It was Mukai who first noticed the strange coincidence of (4.1) and (3.2) and used it to prove the following results:

Theorem (Mukai). *If $G$ is a group of symplectic automorphisms of the $K3$-surface $X$ then there is an imbedding $i : G \to M_{23}$ such that $i(G)$ is a subgroup of one of the groups listed in* (i)-(xi) *above.*

Theorem. *If $V = H^*(X, \mathbf{Q})$ and $P$ are as above then the imbedding $i$ induces a $\mathbf{Q}G$-isomorphism of modules $\alpha : V \to P$.*

Remarks

(i) Granted the existence of $i$, the second theorem is a consequence of (4.1).
(ii) Granted the existence of *any* imbedding $G \to M_{23}$, $\alpha$ still exists, whence by (2.3) we can conclude that $i(G)$ has at least five orbits on $\Omega$ and hence is in one of the groups (i)-(xi). Thus to prove the theorems, we

only need *some* imbedding $G \to M_{23}$.

(iii) Mukai exhibits $K3$-surfaces admitting each of the groups (i)-(xi) as symplectic automorphisms, but we will not deal with that result here.

The remainder of this paper is concerned with a proof of Mukai's theorem. As we already mentioned, we use only the results (2.3), (3.1)-(3.4), together with the following facts concerning $M_{23}$.

## 6. Some properties of $M_{23}$

We list here some more technical results concerning the 2-structure of $M_{23}$. First we introduce the group $\hat{A}_8$, the (universal) central extension of $A_8$ by $\mathbb{Z}_2$, i.e., the non-split extension $1 \to \mathbb{Z}_2 \to \hat{A}_8 \to A_8 \to 1$. This group will play a rôle in what follows. For now we need only the following:

*$\hat{A}_8$ and $M_{23}$ have isomorphic Sylow 2−subgroups, of order $2^7$.* (6.1)

(See [5].) Let $T$ be a 2-Sylow subgroup of $M_{23}$. As $M_{23}$ has a subgroup of the shape $E_{16} : A_7$, the following properties of $T$ are easily verified.

*Let $J = J(T)$ be the subgroup of $T$ generated by all abelian subgroups of maximal order (which order is 16). Then $J$ has order $2^6$ and it contains exactly two subgroups of type $E_{16}$, three of type $\mathbb{Z}_4 \times \mathbb{Z}_4$, and no others of order 16 which are abelian.* (6.2)

An immediate consequence is

*$T$ has no subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_8$ .* (6.3)

## 7. Nikulin's result

Given our group $G$ of symplectic automorphisms, let $a(n) = \#\{g \in G \mid |g| = n\}$. Then of course we have

$$\sum_{n \geqslant 1} a(n) = |G|$$

and it is also well known that, in the notation of (3.3),

$$|G|^{-1} \Sigma a(n) \chi(n) = dim V^G$$

this latter quantity being $\geqslant 5$ by (2.3). For example if $|G|$ is a prime $p$ we get $a(1) = 1$, $a(p) = p-1$, $\chi(1) = 24$, $\chi(p) = 24/p+1$ and find that

$$|G|^{-1} \Sigma a(n) \chi(n) = 48/p+1 \geqslant 5.$$

This forces $p \leqslant 7$, and a similar analysis shows that if $G$ is cyclic of order $n = |G|$ then the inequality $n \geqslant 9$ leads to $|G|^{-1} \Sigma a(n) \chi(n) < 5$. So we get

*If $g \in G$ then $|g| \leqslant 8$ .* (7.1)

Next we prove

*If $t \in G$ is an involution then $C_G(t)$ is isomorphic to a subgroup of $\hat{A}_8$.* (7.2)

As a corollary, we obtain

*A 2-Sylow subgroup of G is isomorphic to a subgroup of $M_{23}$.* (7.3)

The corollary follows from (7.2) and (6.1). To prove (7.2), let $F = F(t)$ be the points of the $K3$-surface $X$ fixed by $t$, so that $|F| = 8$ by (3.4). Of course the group $C = C_G(t)$ preserves $F$. Now if an element $g \in C$ fixes each point of $F$ then $|g| = 1$ or 2 by (3.4), whereas by (3.1) no two distinct involutions of $G$ can fix a common point of $X$. This shows that only $<t>$ fixes each point of $F$, yielding an imbedding $C/<t> \hookrightarrow \Sigma_8$. Let us write $\bar{C} = C/<t>$, thinking of $\bar{C}$ as a group permuting $F$.

Suppose that $\bar{C}$ contains an odd permutation. Then it contains a permutation $\bar{x}$ of the shape (12), (1234), (12)(34)(56), (123456), or (12345678). In the first four cases $\bar{x}$ fixes points of $F$, as does the group $<x,t>$. By (3.1) we get $<x,t>$ cyclic, so $|x|=2|\bar{x}|=4$, 8, 4 or 12, respectively. So the fourth case is out by (7.1). In the first three cases, $\chi(x) = 4$, 2, or 4 by (3.4), whereas since $F(x) \subseteq F$ we see that $|F(x)| = 6$, 4, or 2 respectively. This contradiction shows that $\bar{x}$ can only be an 8-cycle.

Now as $G$ has no elements of order 16 by (7.1) then $<x,t> \cong \mathbb{Z}_2 \times \mathbb{Z}_8$. Let $u$ be the unique involution of $<x,t>$ which has a square root in $<x,t>$, and apply a similar procedure to $C_G(u) = B$, say, setting $E = F(u)$. Of course $<x,t> \leqslant B$. Moreover as $t \neq u$ then $t$ fixes no element of $E$ by (3.1), whereas any element $y \in <x,t>$ of order 8 must satisfy $y^4 = u$, so $y$ fixes just 2 points of $E$ by (3.4), so $y$ has shape (1234)(56) in its action on $E$ as $y$ induces an element of order 4. Thus $<x,t>$ induces a group of even permutations of $E$, putting $<x,t>/<u> \hookrightarrow A_8$.

Finally, this means either $<x,t> \hookrightarrow \mathbb{Z}_2 \times A_8$ or $<x,t> \hookrightarrow \hat{A}_8$, and since neither $\mathbb{Z}_2 \times A_8$ nor $\hat{A}_8$ contains $\mathbb{Z}_2 \times \mathbb{Z}_8$ (cf. (6.1)-(6.3)), this shows that $\bar{x}$ does not exist.

Thus we get $\bar{C} \hookrightarrow A_8$, so that $C \hookrightarrow \mathbb{Z}_2 \times A_8$ or $C \hookrightarrow \hat{A}_8$. Assume the first case. Then no involution of $\bar{C}$ fixes a point of $F$ by (3.1), so a Sylow 2-subgroup of $\bar{C}$ has order at most 8. Also, $\bar{C}$ cannot contain an element of the shape (123) by (3.4), and it has no elements of order 5 or 7 since there are no elements of order $2p$ for $p \geqslant 5$ by (7.1). Thus $|\bar{C}|$ divides 24 and we easily verify that, whatever the possibility for $C$, the group $\hat{A}_8$ has a subgroup isomorphic to $C$. So in any case $C \hookrightarrow \hat{A}_8$ as required.

*Let $A \leqslant G$ be an abelian subgroup of even order. Then $A$ is isomorphic to a subgroup of one of the following groups: $E_{16}$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_6$.* (7.4)

PROOF. $A$ contains an involution $t$, so by (7.2) we get $A \hookrightarrow \hat{A}_8$. If $A$ is a 2-group then we may take $A \leqslant T$, a 2-Sylow of $\hat{A}_8$, in which case one of the first three possibilities applies by (6.2). If $A$ is not a 2-group, it must have order $2^a \cdot 3$ for some $a$ since there are no elements of order $2p$ for primes

$p \geqslant 5$. Similarly there are no elements of order 12, so the 2-Sylow subgroup of $A$ is $E_{2^a}$ and $A \cong E_{2^{a-1}} \times \mathbb{Z}_6$. Finally, setting $\bar{A} = A/\langle t\rangle \leqslant A_8$ as in the proof of (7.2), it was shown there that an element of $\bar{A}$ of order 3 necessarily has the shape (123)(456). Then if $4 \mid |\bar{A}|$ then $\bar{A}$ contains an involution $\bar{b}$ fixing both 7 and 8. Then $\bar{b}$ pulls back to an element of order 4 in $A \leqslant \hat{A}_8$, and as $A$ contains no such element this is impossible. So $4 \nmid |\bar{A}|$, that is $a \leqslant 2$ and (7.4) follows.

We can use similar arguments to that of the proof of (7.2), applied to elements of odd prime order $p$. If $x$ is such an element then $C_G(x)$ acts on the set $F(x) = F$ of fixed points of $x$ in its action on the surface $X$. Again the group $C_G(x)/\langle x\rangle$ induces a group of permutations on $X$. If $p \geqslant 5$ then $|X| < p$ by (3.4), so $p \nmid |C_G(x){:}\langle x\rangle|$, which forces $\langle x\rangle$ to be already a $p$-Sylow subgroup of $G$. If $p = 3$ then $|X| = 6$ and $C_G(x)/\langle x\rangle \leqslant \Sigma_6$. In this case no element of $C_G(x)/\langle x\rangle$ of order 3 can be a permutation of the shape (123) (by (3.1) and (7.1)), so $|C_G(x)/\langle x\rangle|$ cannot be divisible by 9, that is $|C_G(x)|$ is not divisible by $3^3$. By taking $x$ to be an element in the center of a 3-Sylow subgroup, say $R$, of $G$, we deduce that $|R| \leqslant 9$. Hence, we have proved

*$|G|$ divides* $2^7 \cdot 3^2 \cdot 5 \cdot 7$ . (7.5)

(NIKULIN). *Any abelian subgroup of G is contained in one of the following groups:* $E_{16}$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_6$, $E_9$, $\mathbb{Z}_5$ or $\mathbb{Z}_7$. (7.6)

PROOF. We are done by (7.4) if the abelian group has even order. If not, it has order dividing $3^2 \cdot 5 \cdot 7$ by (7.5) and each element has order 3, 5, or 7 by (7.1). The result follows.

## 8. THE CASE WHERE $|G|$ IS DIVISIBLE BY 7

We show in this section

*If $7 \mid |G|$ then G is isomorphic to a subgroup of $L_2(7)$.* (8.1)

We fix a 7-Sylow subgroup $S$ of $G$, so that $|S| = 7$ by (7.5). By (7.1) we see that $S$ is its own centralizer in $G$, that is $S = C_G(S)$. Set $N = N_G(S)$.

*The order of N is odd.* (8.2)

PROOF. Otherwise there is an involution $t \in N$, and since $t$ does not centralize $S$ then $\langle S,t\rangle \cong D_{14}$. Setting $H = \langle S,t\rangle$, $H$ contains the identity, 6 elements of order 7 and 7 of order 2. This yields

$$dim V^H = \frac{1}{14}(24+6\cdot 3+7\cdot 8) = 7.$$

On the other hand we also have

$$dimV^S = \frac{1}{7}(24+6\cdot 3) = 6,$$

putting us in the situation that $S \leqslant H$ and yet $dimV^H > dimV^S$. This is impossible, and the result follows.

*S normalizes no non-trivial subgroup of G of order coprime to 7.* (8.3)

PROOF. For let $1 \neq H \leqslant G$ satisfy $H \lhd HS$ and $7 \nmid |H|$. By a well known result [4, Theorem 6.2.] we can take $H$ to be a $p$-group for some prime $p$. As $S = C_G(S)$ we must have $7 \mid |H|-1$, so by (7.5) we see that $p = 2$. Moreover $S$ acts on $Z(H)$, and by (7.6) together with $7 \mid |Z(H)|-1$ we find that $Z(H) \cong E_8$. Set $K = Z(H)\cdot S$. Then $K$ contains 48 elements of order 7 and 7 involutions, yielding

$$dimV^K = \frac{1}{56}(24+7\cdot 8+48\cdot 3) = 4.$$

This contradicts (2.3), and completes the proof.

*If G is solvable then* $G \cong \mathbb{Z}_7$ *or* $\mathbb{Z}_7{:}\mathbb{Z}_3$ . (8.4)

PROOF. Since $S$ normalizes the Fitting subgroup $F(G)$ of $G$ it normalizes each of the $p$-Sylow subgroups of $F(G)$ also. By (8.3), such a $p$-Sylow subgroup of $F(G)$ is trivial if $p \neq 7$, so we must have $F(G) = S \lhd G$ since $C_G(F(G)) \leqslant F(G)$ ensures that $F(G)$ is non-trivial. Since $C_G(S) = S$ then $G/S \leqslant Aut(S) \cong \mathbb{Z}_6$. Now the result follows from (8.2).

*If G is non-solvable then G is non-abelian simple and* $|N| = 21$. (8.5)

PROOF. Let $E$ be a minimal (non-trivial) normal subgroup of $G$. By (8.3) we get $7 \mid |E|$, so that $S \leqslant E$. If $E = S$ then $G$ is solvable, the converse being true by (8.4).

Suppose $E \neq S$. Since $E$ is the direct product of isomorphic simple groups $E$ must itself be simple and non-abelian. Now by a theorem of BURNSIDE [4, Theorem 7.43], if $N_E(S) = S$ then $E = K{:}S$ for some group $K$ of order coprime to 7. This is impossible by (8.3), so $N_E(S) > S$. After (8.2) we get $N_E(S) = N$ has order 21.

Finally, the Frattini argument [4, Theorem 1.37] yields $G = E\cdot N_G(S) = E\cdot N = E$, so that $G = E$ is non-abelian simple, and we are done.

*The order of G is not divisible by* 5 . (8.6)

PROOF. If false, $G$ has a Sylow 5-subgroup $F$ of order 5, and $C_G(F) = F$ by (7.1). If $N_G(F) = F$ then $G = K{:}F$ for some group $K$ of order prime to 5 by Burnside's theorem [loc cit], against the simplicity of $G$ (cf. (8.4) and (8.5)). So we have $|N_G(F){:}F| = 2$ or 4 since $N_G(F)/F \leqslant Aut(F) \cong \mathbb{Z}_4$.

Now after (8.5) we have $|G| = 2^a \cdot 3^b \cdot 5 \cdot 7$ with $b \geq 1$. Moreover by Sylow's theorem applied to both $N_G(S)$ and $N_G(F)$ we have $|G:N_G(F)| \equiv 1 \pmod 5$ and $|G:N_G(S)| = 1 \pmod 7$, and in the latter case we even know that $|N_G(S)| = 21$. The only possibilities are the following:

(i) $|N_G(F)| = 10, |G| = 2^6 \cdot 3^2 \cdot 5 \cdot 7$.

(ii) $|N_G(F)| = 20, |G| = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

We use the equations $|G| = \Sigma a(n)$ and $dim V^G = |G|^{-1} \Sigma a(n) \chi(n) \geq 5$, eliminate $a(2)$ from them, and arrive at the inequalities

$$0 \leq |G|^{-1}[2a(3)+4a(4)+4a(5)+6a(6)+5a(7)+6a(8)] \leq 3 + \frac{16}{|G|}. \qquad (*)$$

In case (i) we have $a(5) = 2|G|/5$ and $a(7) = 2|G|/7$, which gives

$$0 \leq |G|^{-1}[2a(3)+4a(4)+6a(6)+6a(8)] \leq 3 + \frac{16}{|G|} - \frac{8}{5} = \frac{10}{7},$$

in particular $0 \leq \frac{16}{|G|} - \frac{1}{35}$. Thus $|G| \leq 16 \cdot 35$, a contradiction.

In case (ii) we have $a(5) = |G|/5$, $a(7) = 2|G|/7$. Moreover in this case $N_G(F)$ contains an element $x$ of order 4. By (7.1) $C_G(x)$ is a 2-group, of order at most 8 since $|C_G(x)|$ divides $|G|$. So either $|C_G(x)| = 8$ and $x$ is not conjugate to its inverse, or else $C_G(x) = \langle x \rangle$ and $x$ is conjugate to its inverse. In either case we get $a(4) \geq \frac{|G|}{4}$. Now (*) yields

$$0 \leq |G|^{-1}[2a(3)+6a(b)+6a(8)] \leq 3 + \frac{16}{|G|} - \frac{4}{5} - \frac{10}{7} - 1,$$

yielding $|G| \leq 70$, contradiction.

Proof of (8.1). We may assume $G$ non-solvable by (8.4), whence it is simple of order $2^a \cdot 3 \cdot 7$ by (8.6) and (8.5). In fact (8.5) and Sylow's theorem force $|G| = 2^a \cdot 3 \cdot 7$ with $a = 3$ or 6. If $a = 3$ then $G \cong L_2(7)$, being a simple group of order 168.

It remains to show that $a = 6$ is impossible. In fact we will show that $G$ has a subgroup of index 7, which clearly suffices. Now by a theorem of Frobenius [4, Theorem 7.4.5(a)] there is a 2-group $U$ in $G$ such that $N_G(U)/C_G(U)$ is *not* a 2-group. Choose $U$ with $|U|$ maximal. By (8.3), $N_G(U)$ has order $2^b \cdot 3$ for some $b$. Let $T$ be a 2-Sylow of $G$ containing $U$ with $T_1 = N_T(U)$ a 2-Sylow of $N_G(U)$. If $T_1 = T$ then $N_G(U)$ has index 7 in $G$ as required, so we can assume that $T_1 \underset{\neq}{<} T$. Hence $|U| \leq 16$ since $|T| = 2^6$. Note that $C_G(U) \leq U = O_2(N_G(U))$ by choice of $U$. Let $R \cong \mathbf{Z}_3$ be a 3-Sylow of $N_G(U)$.

Suppose first that $|U| \leq 4$. Then $R$ acts faithfully on $U$, so $U \cong E_4$ and $U = C_G(U)$. Now from (6.2), we see that $T$ (having index 2 in a 2-Sylow of $M_{23}$) certainly has a normal subgroup $E$ isomorphic to $E_8$. Then one checks that $|C_{EU}(U)| \geq 8$, against $U = C_G(U)$. So $|U| \geq 8$.

Next, since $C_G(U) \leq U$ then certainly $Z(T) \leq Z(U)$. So if $R$ centralizes $Z(U)$

then $N(Z(T))$ contains both $T$ and $R$ and hence has index 7 in $G$ since $Z(T)$ cannot be normal in $G$ by simplicity. So $R$ does not centralize $Z(U)$, and this is enough to ensure that $U$ is abelian.

If $U \cong E_{16}$ then $U \trianglelefteq T$ since all $E_{16}$'s in a 2-Sylow of $M_{23}$ are normal. This is false, so if $|U| = 16$ then $U \cong \mathbf{Z}_4 \times \mathbf{Z}_4$ by (6.2). Then $U$ is the unique subgroup of $T_1$ of type $\mathbf{Z}_4 \times \mathbf{Z}_4$, so $U$ is characteristic in $T_1$, whence normal in $T$. So in fact $|U| = 8$ and since $R$ does not centralize $U$ then $U \cong E_8$. Let $U_0 = C_U(R) \cong \mathbf{Z}_2$, so that $U_0 = Z(N_G(U))$. By choice of $U$, $N_G(U_0) = N_G(U)$.

Now $|T_1 : U| = 2$ and $U$ is not the only $E_8$-subgroup of $T_1$. Thus $T_1$ has exactly two $E_8$-subgroups, call them $U$ and $U_1$, and $T_1 = UU_1$. This forces $T_2 = N_T(T_1)$ to satisfy $|T_2 : T_1| = 2$. Then $U, U_1$ are *not* the only two $E_8$-subgroups of $T_2$ (otherwise $N_T(U) \not\leqslant T_1$), so there is $x \in T_2 \setminus T_1$ lying in an $E_8$-subgroup of $T_2$. Since $U^x = U_1$, the only possibility is that $x$ centralizes $U \cap U_1 (\cong E_4)$, in particular $x \in C_G(U_0) = N_G(U)$, so $x \in T_1$. This is not the case and (8.1) is proved.

## 9. The case where $|G|$ is divisible by 5

Here we prove

*If 5 divides $|G|$ then $G$ is isomorphic to a subgroup of one of the groups:* (9.1)
$\Sigma_5$, $A_6$, $E_{16}{:}A_5$.

We fix a Sylow 5-subgroup $F$ of $G$. By (7.1) we have $C_G(F) = F$. Let $N = N_G(F)$. Then $N/F \leqslant Aut(F) \cong \mathbf{Z}_4$.

*If $A$ is a non-trivial $F$-invariant subgroup of $G$ of order prime to 5 then* (9.2)
$A \cong E_{16}$.

**Proof.** By [4, Theorem 6.2.2] $F$ normalizes a $p$-Sylow subgroup of $A$ for each prime $p$; call such an $A$-invariant $p$-Sylow $S_p$. By (7.1) we get $5 \mid |S_p| - 1$, which forces $A = S_2$. Similarly as $C_A(F) = 1$ by (7.1) we must have $|A| = 16$ since $|A| \leqslant 2^7$, and the result follows easily.

*The conclusions of* (9.1) *hold if $G$ is solvable.* (9.3)

**Proof.** If $F \leqslant F(G)$ then $F = F(G)$ by (7.1) and the nilpotence of $F(G)$. Then $G/F \leqslant Aut(F) \cong \mathbf{Z}_4$, so $G \leqslant \mathbf{Z}_5{\cdot}\mathbf{Z}_4 \leqslant \Sigma_5$.

If $F \not\leqslant F(G)$ then $F(G) \cong E_{16}$ by (9.2). Moreover $F{\cdot}F(G) \trianglelefteq G$, in fact $F{\cdot}F(G)/F(G) = F(G/F(G))$, so $G \leqslant E_{16} \cdot (\mathbf{Z}_5{\cdot}\mathbf{Z}_4)$. But this latter group contains, besides the identity, 35 involutions, 5·28 elements of order 4, 5·16 elements of order 8 and $2^6$ elements of order 5. This yields

$$dim V^G = \frac{1}{320}(24 + 8{\cdot}35 + 4{\cdot}5{\cdot}28 + 2{\cdot}5{\cdot}16 + 4{\cdot}2^6) = 4,$$

contradiction. So in fact $G \leqslant E_{16} \cdot D_{10} \leqslant E_{16}{\cdot}A_5$, as required.

PROOF OF (9.1). We may assume that $G$ is non-solvable by (9.3). Let $E$ be a minimal normal subgroup of $G$, and assume first that $5 \| E|$. If $E$ is solvable then $E$ is an elementary abelian $p$-group for some $p$, whence $E = F$ and $G$ is solvable. So $E$ is non-solvable, hence non-abelian simple since it must be a direct product of isomorphic simple groups.

By Brauer's result [2] we get $E \cong A_5$ or $A_6$. In the first case $G \leqslant Aut(E) \cong \Sigma_5$ and we are done. In the second case, $G/E \leqslant Out(A_6) \cong E_4$, and it is well known that the three subgroups of index 2 in $Aut(A_6)$ are of type $PGL_2(9)$, $\Sigma_6$ and $M_{10}$, respectively ($M_{10}$ is the stabilizer of two points in the action of $M_{12}$ on 12 points). Now $PGL_2(9)$ contains an element of order 10, which shows that $G$ is neither $PGL_2(9)$ nor the full automorphism group $Aut(A_6)$.

The enumeration of elements of $\Sigma_6$ is well known, and leads to $dim V^G = 4$. Similarly, a subgroup $M_{10}$ in $M_{23}$ has only four orbits on $\Omega$ as is readily checked, and hence, since we know that the character of any $M_{10}$ on $V = H^*(X, \mathbf{Q})$ is the same as that of an $M_{10}$ on $P = \mathbf{Q}\Omega$, we must get $dim V^G = 4$ in this case, too.

So the result is proved if $5 \| E|$. Assume therefore that 5 does not divide $|E|$. By (9.1), $E \cong E_{16}$ and $E = C_G(E)$ by (7.6). As $G$ is non-solvable then so is $G/E$ and hence a minimal normal subgroup of $G/E$ must be isomorphic to $A_5$ or $A_6$. As we have already seen that the group $E_{16} \cdot (\mathbf{Z}_5 \cdot \mathbf{Z}_4)$ cannot occur, it follows that $G/E \cong A_5$ or $A_6$. Now the group $M_{23}$ contains a subgroup $E_{16} \cdot A_6$ with 4 orbits on $\Omega$, and as we have seen before this forces $dim V^G = 4$ if $G \cong E_{16} \cdot A_6$. So in fact $G \cong E_{16} \cdot A_5$.

There are two possibilities for the isomorphism type of $E$ considered as an $\mathbf{F}_2 A_5$-module. In the first, $A_5$ is transitive on the non-identity elements of $E$; in this case $G$ has a subgroup $H$ of index 5, order $2^6 \cdot 3$, with a normal 2-Sylow $U$ and Sylow 3-subgroup $R$ ($\cong Z_3$) satisfying $C_U(R) = 1$. Then one finds (see (10.3)) that $U \cong J(T)$ in the notation of (6.2), in particular $E$ has a complement in $U$, hence in $G$ by a well known result of GASCHÜTZ ([6, I.17.4]). So $G \cong E_{16} \cdot A_5$ is a split extension isomorphic to the group $M_{20}$ of [3], and certainly lies in $M_{23}$.

The other possibility is that there are two orbits in the action on $E^\#$, of lengths 5 and 10. In this case the subgroup $H$ of $G$ or order $2^6 \cdot 3$ has a normal 2-Sylow $U$, 3-Sylow $R$, and $C_E(R) = C_U(R) \cong E_4$. Then $H$ contains 27 involutions, 32 elements of order 3, 36 of order 4, and 96 of order 6, yielding

$$dim V^H = \frac{1}{192}(24+8\cdot 27+6\cdot 32+4\cdot 36+2\cdot 96) = 4.$$

This contradiction completes the proof of (9.1).

## 10. THE CASE WHERE $|G|$ IS DIVISIBLE BY 9

We turn to the cases in which neither 5 nor 7 divide $|G|$. So $G$ is solvable of order $2^a \cdot 3^b$ with $a \leqslant 7$ and $b \leqslant 2$. Here we prove

*If $9 \mid |G|$ then $G$ is isomorphic to a subgroup of one of the following:* (10.1)
$E_9 : Q_8$, $E_9 \cdot D_8$, $(A_4 \times A_4) \cdot \mathbf{Z}_2$.

PROOF. Let $R$ be a Sylow 3-subgroup of $G$, so that $R \cong \mathbf{Z}_3 \times \mathbf{Z}_3$ by (7.1). Suppose first that $R \leqslant F(G)$. By (7.6) we get $R = F(G)$, so as $R = C_G(R)$ then $G/R \leqslant Aut(R) \cong GL_2(3)$. As $G/R$ is a 2-group it must be isomorphic to a 2-subgroup of $GL_2(3)$. This latter group has three maximal subgroups, of type $\mathbf{Z}_8$, $Q_8$ and $D_8$ respectively. Now the group $E_9 : \mathbf{Z}_8$ has 9 involutions, 18 elements of order 4, 36 of order 8, and 8 of order 3, yielding

$$dim V^G = \frac{1}{72}(24+8 \cdot 9+4 \cdot 18+2 \cdot 36+6 \cdot 8) = 4.$$

This shows that a 2-Sylow of $G$ cannot contain $\mathbf{Z}_8$, hence lies in $Q_8$ or $D_8$, giving the first two possibilities.

Before continuing the proof of (10.1) we interpolate two useful results.

*Suppose $B$ is a 2-group with $|B:Z(B)| = 4$. Then its derived group $B'$* (10.2)
*has order $|B'| = 2$.*

PROOF. Let $|B| = 2^n$. If $x \in B \setminus Z(B)$ then $C_B(x) = Z(B)\langle x \rangle$ has index 2 in $B$. Thus $B$ has exactly $2^{n-2} + \frac{1}{2}(2^n - 2^{n-2})$ conjugacy classes, that is $5 \cdot 2^{n-3}$ classes. On the other hand let $|B'| = 2^c$. Note that $c \geqslant 1$ as $B$ is non-abelian. Then $B$ has $|B:B'| = 2^{n-c}$ characters of degree 1, and since the number of irreducible characters equals the number of conjugacy classes, $B$ has $5 \cdot 2^{n-3} - 2^{n-c}$ irreducible characters of degree $\geqslant 2$. Since $|G|$ equals the sum of the squares of the degrees of the irreducible characters we must have

$$2^n \geqslant 2^{n-c} + 4(5 \cdot 2^{n-3} - 2^{n-c}).$$

This reduces to $2^{n-c} \geqslant 2^{n-1}$, whence $c = 1$ as required.

*Suppose $B$ is a 2-group in $M_{23}$ such that $|B| \leqslant 2^6$ and $B$ has an auto-* (10.3)
*morphism $\alpha$ of order 3 satisfying $C_B(\alpha) = 1$. Then either $B$ is abelian or else $B \cong J(T)$ in the notation of (6.2).*

PROOF. Suppose that $B$ is non-abelian. Set $Z = Z(B) \underset{\neq}{<} B$. Since $\alpha$ fixes no elements of $B^\#$ the same is also true of $Z$ and $B/Z$. If $|B:Z| = 4$ then $|B'| = 2$ by (10.2), so $\alpha$ centralizes $B'$. This is false, so we have $|B/Z| = 16$ and $|Z| = 4$. In fact, $C_Z(\alpha) = 1$ forces $Z \cong E_4$. Again (10.2) together with $C_{B/Z}(\alpha) = 1$ force $B/Z$ abelian, so $B/Z \cong E_{16}$ or $\mathbf{Z}_4 \times \mathbf{Z}_4$. In the latter case, if we choose $x \in B$ so that $xZ$ has order 4 in $B/Z$, then $\langle x, Z \rangle \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_8$, and both are impossible by (6.2). So in fact $B/Z \cong E_{16}$ and $B/Z$ is generated by subgroups $B_1/Z$ of order 4 which are $\alpha$-invariant. Now (10.2) yields that each $B_1$ is abelian, and the result follows from (6.2).

We return to the proof of (10.1) and consider next the case that

$R \cap F(G) = 1$. Then $F = F(G)$ is a 2-group. Now we have $F = <C_F(R_1) | \mathbf{Z}_3 \cong R_1 \leqslant R>$ by [4, Theorem 6.2.4], and since $C_F(R) = 1$ by (7.6) then for each $R_1 \leqslant R$ of order 3 the group $C_F(R_1)$ satisfies the conclusions of (10.3). It follows from (7.6) that $C_F(R_1) = 1$ or $E_4$ for each such $R_1$. As $|F| \leqslant 2^6$ there is some $\mathbf{Z}_3 \cong R_0 \leqslant R$ with $C_F(R_0) = 1$, so again (10.3) yields $F \cong E_{16}$ or $F \cong J(T)$ with the notation of (6.2). In the latter case we see that $FR$ contains 27 involutions, $2^7 + 6 \cdot 2^4$ elements of order 3, 36 of order 4, $18 \cdot 2^4$ of order 6, and hence that $dim V^{FR} = 4$. This is impossible, so that $F \cong E_{16}$ and $FR \cong A_4 \times A_4$.

Finally, $G/FR$ must be a subgroup of $D_8$. If $G/FR$ has an element of order 4 then $G$ has a subgroup $H$ of the form $E_{16} \cdot (E_9 \cdot \mathbf{Z}_4)$. This group contains 51 involutions, 80 elements of order 3, 9·28 of order 4, 9·16 of order 8, and 48 of order 6; we compute that $dim V^H = 4$, contradiction. So $G/FR$ has exponent 2. Let $x$ be an involution of $G \setminus FR$. Now $FR$ has just two normal subgroups isomorphic to $A_4$, so $x$ either fixes or interchanges them.

If $x$ interchanges these two $A_4$'s then the group $H = FR<x>$ contains 27 involutions, 80 elements of order 3, 36 of order 4 and 144 of order 6; this leads to the contradiction $dim V^{FR<x>} = 4$. So $x$ normalizes each of the $A_4$'s normal in $FR$. If $A_1$ is one of these normal $A_4$'s then $A_1 <x> \cong \Sigma_4$ or $\mathbf{Z}_2 \times A_4$. If the second case holds, and if $A_2$ is the other normal $A_4$, we must have $A_2 <x> \cong \Sigma_4$ or $\mathbf{Z}_2 \times A_4$, and then $FR<x>$ contains either $\mathbf{Z}_4 \times \mathbf{Z}_3$ or $E_{32}$, respectively. This contradicts (7.6), so in fact $A_i <x> \cong \Sigma_4$ for $i = 1, 2$, which gives the third possibility of (10.1).

It remains to consider the possibility that $R \cap F(G) \neq 1$, $R \leqslant F(G)$. Then $R \cap F(G) = R_0 \cong \mathbf{Z}_3$, and since $C_G(R) = R$ by (7.6) we get $F(G) \cong \mathbf{Z}_3 \times E_4$ by (7.6) once more. As there are no elements of order 12, another application of (7.6) shows that $C_G(R_0) = F(G)R \cong \mathbf{Z}_3 \times A_4$ and of course $|G:C_G(R_0)| \leqslant 2$. If $G = C_G(R_0)$ then $G \leqslant A_4 \times A_4$. If $|G:C_G(R_0)| = 2$ then $|N_G(R):R| = 2$ and there is an involution $x \in N_G(R)$. We easily see that $G = F(G)R<x>$ is isomorphic either to a subgroup of the group $(A_4 \times A_4) \cdot \mathbf{Z}_2$ already considered, or to the group $\Sigma_3 \times E_4$. But if $G \cong \Sigma_3 \times E_4$ we easily find that $dim V^G = 7$, whereas for the group $K \cong \mathbf{Z}_3 \times E_4$ of index 2 we get $dim V^K = 6$. This contradiction completes the proof of (10.1).

## 11. End of proof

In this last section we assume that $|G| = 2^a \cdot 3^b$ with $b \leqslant 1$. After (7.3) we may assume that $b = 1$. Note that the last paragraph established

$$G \ncong \Sigma_3 \times E_4 . \tag{11.1}$$

We must show, of course, that $G$ is isomorphic to a subgroup of one of the groups (i)-(xi) in Section 4.

Let $R \cong \mathbf{Z}_3$ be a Sylow 3-subgroup of $G$, and assume first that $R \leqslant F(G)$, that is $R \lhd G$. After (7.6) we get $C_G(R) = R \times E$ where $E$ is one of 1, $\mathbf{Z}_2$, or $E_4$, and of course $|G:C_G(R)| \leqslant 2$. If $E = 1$ then $G \cong \mathbf{Z}_3$ or $\Sigma_3$ and we are done. If $E \cong \mathbf{Z}_2$ then either $G = C_G(R) \cong \mathbf{Z}_6$ or else a 2-Sylow of $G$ has order 4 and hence is $E_4$ or $\mathbf{Z}_4$. If $E_4$ then $G \cong \mathbf{Z}_2 \times \Sigma_3$ is contained (for example) in $\Sigma_5$. If $\mathbf{Z}_4$ then $G \cong \mathbf{Z}_3 \cdot \mathbf{Z}_4$ is contained in the group $(A_4 \times A_4) \cdot \mathbf{Z}_2$ of (vii).

Finally, assume that $E \cong E_4$. If $G = C_G(R)$ then $G \cong \mathbf{Z}_3 \times E_4$ is contained in $A_4 \times A_4$. Otherwise, a Sylow 2-subgroup $T$ of $G$ has order 8. If $T$ is non-abelian then $T \cong D_8$ and $G$ is again contained in $(A_4 \times A_4) \cdot \mathbf{Z}_2$. If $T$ is isomorphic to $E_8$ then $G \cong \Sigma_3 \times E_4$, against (11.1). The only other possibility is $T \cong \mathbf{Z}_2 \times \mathbf{Z}_4$, and we show this to be impossible as follows: let $x$ be the unique non-identity square in $T$. Then $G = C_G(x)$, so $G \leqslant \hat{A}_8$ by (7.2), so $G/\langle x \rangle (\cong \mathbf{Z}_2 \times \Sigma_3) \leqslant A_8$. Referring to the proof of (7.2), we see that, up to conjugacy, $G/\langle x \rangle$ must be the subgroup of $A_8$ given by $\langle (12)(34)(56)(78) \rangle \times \langle (135)(246), (35)(46) \rangle$. In particular, a 2-Sylow of $G/\langle x \rangle$ has the non-identity elements (12)(34)(56)(78), (12)(36)(45)(78) and (35)(46). Pulling these back to $G$, the first two pull back to $E_4$'s, the third to $\mathbf{Z}_4$. So a 2-Sylow of $G$, of order 8, contains $\mathbf{Z}_4$ and two distinct $E_4$'s, hence must be $D_8$. Thus it is not $\mathbf{Z}_2 \times \mathbf{Z}_4$, which is the desired contradiction.

We may now assume that $R \nleqslant F(G)$, in which case $F(G) = Q$ is a 2-group satisfying $C_G(Q) \leqslant Q$. We set $Y = \Omega_1(Z(Q))$, the subgroup of $Z(Q)$ $(\neq 1)$ generated by its involutions. Suppose that $|Y| \geqslant 4$. Then if $Q/Y$ has an element $xY$ of order $\geqslant 4$ then the abelian group $\langle x, Y \rangle$ contains either $\mathbf{Z}_4 \times E_4$ or $\mathbf{Z}_8 \times \mathbf{Z}_2$. This contradicts (7.6), so $Q/Y$ has exponent 2, that is, it is elementary abelian. Thus the Frattini subgroup $\Phi(Q)$ of $Q$ lies in $Y$. Now in fact this argument shows that $\Phi(Q) \leqslant Y_0$ whenever $E_4 \cong Y_0 \leqslant Y$. Then we get $\Phi(Q) \leqslant \cap Y_0$ where the intersection runs over the $E_4$-subgroups of $Y$. If $|Y| \geqslant 8$ this intersection is trivial, so that $\Phi(Q) = 1$ and $Q$ is itself elementary abelian.

If $|Y| = 4$ then $Z(Q)$ has rank 2. As it admits $R$, (7.6) yields either $Y = Z(Q) \cong E_4$ or else $Z(Q) \cong \mathbf{Z}_4 \times \mathbf{Z}_4$. In the latter case $\langle x, Z(Q) \rangle$ is abelian of order $\geqslant 2^5$ whenever $x \in Q \setminus Z(Q)$, against (7.6). So if $Z(Q) \cong \mathbf{Z}_4 \times \mathbf{Z}_4$ then $Q = Z(Q)$. Finally, if $|Y| = 2$ then $Z(Q)$ is cyclic, hence centralized by $R$, so $Y = Z(Q) \cong \mathbf{Z}_2$ by (7.6) once more. So there are the following possibilities for $Q$:

(a) $Q \cong E_{2^a}$, $2 \leqslant a \leqslant 4$.

(b) $Q \cong \mathbf{Z}_4 \times \mathbf{Z}_4$.

(c) $Z(Q) \cong E_4$, $Q \neq Z(Q)$.

(d) $Z(Q) \cong \mathbf{Z}_2$.

*If* (b) *holds then* $G \leqslant E_{16}{:}\ \Sigma_4$ *(group* (x)). (11.2)

**Proof.** The group $L = E_{16}{:}\Sigma_4$ is the (unique) extension indicated which has no elements of order 6. By (10.3) we see that $O_2(L) \cong J(T)$ in the notation of (6.2). Moreover $L \cong J(T){:}\Sigma_3$. Now a 3-Sylow $P$ of $L$ fixes each of the three $\mathbf{Z}_4 \times \mathbf{Z}_4$-subgroups of $J(T)$ (cf. 6.2)), so at least one of these is fixed by $N_L(P) \cong \Sigma_3$, yielding a subgroup $(\mathbf{Z}_4 \times \mathbf{Z}_4){:}\Sigma_3$ within $L$.

Finally, since $G \cong (\mathbb{Z}_4 \times \mathbb{Z}_4){:}\mathbb{Z}_3$ or $(\mathbb{Z}_4 \times \mathbb{Z}_4){:}\Sigma_3$ the result follows.

*If (c) holds then* $C_Q(R) \cap Z(Q) = 1$. (11.3)

PROOF. If not then $R$ centralizes $Z(Q) \cong E_4$, so that $Y = Z(Q) = C_Q(R)$ by (7.6). Now we have already seen that $Q/Y$ is elementary abelian, and since $C_{Q/Y}(R) = 1$ then $Q/Y \cong E_4$ or $E_{16}$. In the latter case there are 5 distinct $R$-invariant subgroups $D/Y$ of $Q/Y$ of order 16 which partition $Q/Y$. Since $Q$ is not elementary abelian, some $D$ is not $E_{16}$, so as $C_D(R) = Y$ then $D$ cannot even be abelian.

So whatever the possibility for $Q/Y$, there is a non-abelian subgroup of $D$ of order 16 which admits $R$ and $C_D(R) = Z(D) \cong E_4$. Using (10.2) we see that $D \cong \mathbb{Z}_2 \times Q_8$, $DR \cong \mathbb{Z}_2 \times SL_2(3)$. But then $DR$ has 3 involutions, 8 elements of order 3, 12 of order 4, and 24 of order 6. This yields the contradiction

$$dim V^{DR} = \frac{1}{48}(24+8\cdot 3+6\cdot 8+4\cdot 12+2\cdot 24) = 4.$$

*If* (c) *holds then either* $|Q| = 2^6$, $C_Q(R) = 1$ *and* $G \leqslant E_{16} : \Sigma_4$ *(type* (x)); *or* $|Q| = 2^5$, $C_Q(R) \cong \mathbb{Z}_2$ *and* $G \leqslant E_{16} : D_{12}$ *(type* (viii)). (11.4)

PROOF. We have $Y = Z(Q) \cong E_4$, $Q/Y$ elementary abelian, and $C_Y(R) = 1$. If $|Q| = 16$ then $|Q'| = 2$ by (10.2), so $1 \neq Q' \leqslant Y \cap C(R)$, contradiction. So $|Q| \geqslant 2^5$. We have $Q/Y = B/Y \times D/Y$ where $B/Y = C_{Q/Y}(R)$, and $|B{:}Y| \leqslant 4$ by (7.6). If $B/Y = 1$ we may apply (10.3) to see that $Q = D \cong J(T)$ in the notation of (6.2). If now $G = QR$ then clearly $G \leqslant E_{16} : \Sigma_4$, in fact $G \cong E_{16}{:}A_4$, the subgroup of index 2. If $G \neq QR$ then a 2-Sylow $U$ of $G$ has order $2^7$ and $G \cong Q{:}\Sigma_3$. In this case each of the two $E_{16}$'s in $Q$ are normal in $U$ by (6.2) (since $U$ is a 2-Sylow of $M_{23}$), hence again $G \cong E_{16}{:}\Sigma_4$.

Now assume that $B/Y \neq 1$. Since $C_D(R) = 1$ we can apply (10.3) to $D$ and conclude that either $D$ is abelian of order 16 or $D \cong J(T)$ in the notation of (6.2). Assume first that $D \cong E_{16}$. If $|B{:}Y| = 4$ then $B = Y \times C_B(R) \cong E_{16}$ (by (7.6)), and the group $QR$ is isomorphic to the group denoted by $H$ in the last paragraph of the proof of (9.1). That calculation therefore gives $dim V^{QR} = 4$, a contradiction. So if $D \cong E_{16}$ then $|B{:}Y| = 2$, that is $C_Q(R) \cong \mathbb{Z}_2$. Thus $QR = D{\cdot}R{\cdot}C_Q(R) \cong E_{16}{:}\mathbb{Z}_6$. If $QR = G$ we are done. If there is an involution of $G$ inverting $R$ then $G \cong E_{16}{:}D_{12}$ as required. Otherwise $G \cong E_{16}{:}(\mathbb{Z}_3{\cdot}\mathbb{Z}_4)$, $G$ contains 19 involutions, 32 elements of order 3, 60 of order 4, 32 of order 6, and 48 of order 8, yielding the contradiction

$$dim V^G = \frac{1}{192}(24+8\cdot 19+6\cdot 32+4\cdot 60+2\cdot 32+2\cdot 48) = 4.$$

So we may now assume $B/Y \neq 1$ and $D \cong E_{16}$. So either $D \ncong \mathbb{Z}_4 \times \mathbb{Z}_4$ or else $D \cong J(T)$ and $D$ contains an $R$-invariant subgroup $D_0 \cong \mathbb{Z}_4 \times \mathbb{Z}_4$. Choose an involution $x \in C_B(R)$ and let $H = DR<x>$ or $D_0R<x>$ in the two cases. Consider $O_2(H)$: if all involutions of $O_2(H)$ lie in $Y<x> \cong E_8$ then $O_2(H)$ contains 7 involutions and 24 elements of order 4, whence $dim V^{O_2(H)} = \frac{1}{3}(24+8\cdot7+4\cdot24)$ is not an integer. So there are involutions in $O_2(H) - Y<x>$. These being permuted by $R$ in cycles of length 3, we see that $O_2(H)$ contains 19 involutions and 12 elements of order 4. So in this case $dim V^{O_2(H)} = 1/32(24+8\cdot19+4\cdot12) = 7$. On the other hand $D_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_4$ satisfies $dim V^{D_1} = \frac{1}{16}(24+8\cdot3+4\cdot12) = 6$, yielding the contradiction $D_1 \leqslant O_2(H)$, $dim V^{D_1} < dim V^{O_2(H)}$. This completes the proof of (11.4).

*If* (d) *holds then either* $G \leqslant GL_2(3)$ *(type* (xi)) *or* $G \cong (Q_8{*}Q_8){:}\mathbb{Z}_3$ *(type* (11.5) (ix)).

PROOF. Let $Y = Z(Q) \cong \mathbb{Z}_2$. If $|Q| = 8$ we must have $Q \cong Q_8$ and $QR \cong SL_2(3)$. If $G = QR$ we are done and if there is an involution in $G \setminus QR$ then $G \cong GL_2(3)$. Otherwise, a 2-Sylow of $G$ is isomorphic to $Q_{16}$, $G$ has 1 involution, 8 elements of order 3, 18 of order 4, 8 of order 6, and 12 of order 8, yielding

$$dim V^G = \frac{1}{48}(24+8+6\cdot8+4\cdot18+2\cdot8+2\cdot12) = 4.$$

So we may now assume that $|Q| \geqslant 16$.

Note that by (7.2), we get $G/Y \leqslant A_8$, in particular $|Q/Y| \leqslant 2^5$. If $Q/Y$ is elementary abelian then $\Phi(Q) = Z(Q) = Y$, so $Q \cong Q_8{*}Q_8$ (cf. [4, Theorem 5.4.9]) and $QR \cong (Q_8{*}Q_8){:}\mathbb{Z}_3$. Thus if $G = QR$ we are done. If not, we see that, up to conjugacy, $G/Y$ is the group $<(12)(34),(13)(24),(56)(78),(57)(68),(123)(456),(23)(56)>$. Then using (3.4), we see that $G$ itself contains 19 involutions, 32 elements of order 3, 60 of order 4, 32 of order 6, and 48 of order 8. This gives

$$dim V^G = \frac{1}{192}(24+8\cdot19+6\cdot32+4\cdot60+2\cdot32+2\cdot48) = 4.$$

Now assume that $Q/Y$ is not elementary abelian. If $C_{Q/Y}(R) = 1$ then $|Q{:}Y| = 16$ and we get $Q/Y \cong \mathbb{Z}_4 \times \mathbb{Z}_4$ by (10.2). As $A_8$ has no subgroup of the shape $(\mathbb{Z}_4 \times \mathbb{Z}_4){:}\mathbb{Z}_3$ this is impossible, so $C_{Q/Y}(R) \cong \mathbb{Z}_2$ and $C_Q(R) \cong E_4$. Setting $B = C_Q(R)$, since $N_Q(B) > B$ and $R$ acts on $N_Q(B)/B$ without non-trivial fixed-points, it must be the case that $C_Q(B) = N_Q(B)$ has order $2^4$ or $2^6$. Since $|Q| \leqslant 2^6$ and $Z(Q) \cong \mathbb{Z}_2$ we must have $|C_Q(B)| = 2^4$ and $|Q| = 2^6$. Looking at the subgroups of $A_8$ ($\geqslant QR/Y$), we see that $Q/Y$ has a subgroup $D/Y \cong E_{16}$ which admits $R$ with $C_D(R) = Y$. Then $D \cong Q_8{*}Q_8$, $QR \cong (Q_8{*}Q_8){:}Z_6$ and $QR$ contains 27 involutions, 32 elements of order 3, 36 of order 4, and 96 of order 6. This yields

$$dim V^{QR} = \frac{1}{192}(24+8{\cdot}27+6{\cdot}32+4{\cdot}36+2{\cdot}96) = 4,$$

a contradiction. This completes the proof of (11.5).

It remains to consider case (a), i.e., $Q$ elementary abelian. This is easy. If $Q \cong E_4$ then $G \cong A_4$ or $\Sigma_4$. If $Q \cong E_8$ then $QR \cong \mathbf{Z}_2 \times A_4$. If $G = QR$ or if there is an involution inverting $R$ then $G \leqslant \mathbf{Z}_2 \times \Sigma_4$, which is contained in the group $(A_4 \times A_4):\mathbf{Z}_2$ (type (vii)). If there is no involution inverting $R$ and $G \neq QR$ then $G \cong E_4{\cdot}(\mathbf{Z}_3{\cdot}\mathbf{Z}_4)$ is still isomorphic to a subgroup of $(A_4 \times A_4):\mathbf{Z}_2$ (type (vii)).

Finally assume that $Q \cong E_{16}$. If $C_Q(R) = 1$ then $G \leqslant E_{16}:\Sigma_3 \leqslant E_{16}:\Sigma_4$ (type (x)). If $C_Q(R) \neq 1$ then $C_Q(R) \cong E_4$. If $G = QR$ then $G \cong E_4 \times A_4 \leqslant (A_4 \times A_4):\mathbf{Z}_2$ (type (vii)), and if there is an involution $x$ inverting $R$ then $x$ cannot centralize $C_Q(R)$ by (7.6) (for in this case $Q\langle x\rangle$ contains $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_4$). Thus $C_Q(R)\langle x\rangle \cong D_8$ and again $G \leqslant (A_4 \times A_4):\mathbf{Z}_2$ (type (vii)). The last possibility is that no involution of $G$ inverts $R$. In this case the group $N_G(R)$ has 2-Sylow $\mathbf{Z}_2 \times \mathbf{Z}_4$, and we showed earlier (when considering the case $R \leqslant F(G)$) that $G$ cannot contain such a group. This completes the proof of the Main Theorem.

REFERENCES

1. W. Barth, C. Peters, A. van de Ven (1984). *Compact Complex Surfaces, Ergebnisse, 3 Folge, Band 4,* Springer.
2. R. Brauer (1980). *Simple Groups of Order* $5{\cdot}2^a{\cdot}3^b$, *Collected works, vol. II,* 421-470, MIT Press.
3. J. Conway (1971). Three lectures on exceptional groups. *Finite Simple Groups,* Academic Press.
4. D. Gorenstein (1968). *Finite Groups,* Harper and Row.
5. D. Gorenstein, K. Harada (1974). *Finite Groups whose 2-Subgroups are Generated by at most 4 Elements,* Mem. AMS. No. 147.
6. B. Huppert (1967). *Endliche Gruppen I, Grundlehren, Band 134,* Springer.
7. S. Mukai, *Finite Groups of Automorphisms of K3-Surfaces and the Mathieu group,* preprint.
8. V.V. Nikulin (1980). Finite groups of automorphisms of Kählerian surfaces of type $K3$. English translation in *Moscow Math. Soc. 30,* 71-137.