

ON SUBGROUPS OF M_{24} . II: THE MAXIMAL SUBGROUPS OF M_{24}

BY
CHANG CHOI

Abstract. In this paper we effect a systematic study of transitive subgroups of M_{24} , obtaining 5 transitive maximal subgroups of M_{24} of which one is primitive and four imprimitive. These results, along with the results of the paper, *On subgroups of M_{24}* , I, enable us to enumerate all the maximal subgroups of M_{24} . There are, up to conjugacy, nine of them. The complete list includes one more in addition to those listed by J. A. Todd in his recent work on M_{24} . The two works were done independently employing completely different methods.

In this paper we effect a systematic study of transitive subgroups of M_{24} , obtaining five transitive maximal subgroups of M_{24} . This result, along with the previous results on the maximal subgroups among the intransitives [3], enables us to enumerate all the maximal subgroups of M_{24} . There are, up to conjugacy, nine of them.

We dispose of the study of primitive subgroups by observing that a proper transitive subgroup of M_{24} is either $\text{PSL}_2(23)$ or imprimitive (Proposition 1.1).

Six different types of systems of imprimitivity can be obtained from the 24 points of M_{24} , Ω , viz., $24/n$ blocks of length n for $n=12, 8, 6, 4, 3$, and 2 , respectively. The systems of imprimitivity with $24/n$ blocks of length n are denoted by $n^i | n^i | \dots | n^i$. Obviously, when $n \geq 6$, the systems are of the same type as sets of n distinct points, as defined in the preceding paper [3, p. 1]. An imprimitive group G with the above type of systems of imprimitivity will be called an imprimitive group of type n^m where $n \cdot m = 24$.

The kernel of imprimitivity, viz., the normal intransitive subgroup of G which contains all the substitutions which do not interchange the systems of imprimitivity $n^i | n^i | \dots | n^i$, is usually denoted by K . Let B_j denote a system of imprimitivity. Then, in general, K is constructed by multiplying the elements of certain cosets of the constituents K^{B_j} which correspond by an isomorphism. Let K_j denote the kernel of the restriction of the kernel K on B_j . If K_j is the identity, then K is built by establishing a simple isomorphism between the corresponding substitutions of K^{B_j} . In this case we denote $K \approx K^{B_1} | K^{B_2} | \dots | K^{B_t}$.

The image of imprimitive group G will be denoted by G^* . If the transitive group

Received by the editors August 3, 1970.

AMS 1969 subject classifications. Primary 20D, 20E.

Key words and phrases. Mathieu groups, 5-fold transitive permutation groups, maximal subgroups, primitive representations.

Copyright © 1972, American Mathematical Society

G^* according to which the systems of imprimitivity are permuted is itself imprimitive, it is possible [5, p. 399] to combine these systems until we obtain systems which are permuted according to a primitive group. In our studies, G^* will always be taken as a primitive group. Thus it is conceivable that the systems of imprimitivity are sometimes a certain union of orbits of K .

A systematic study of the imprimitive subgroups of M_{24} is done by a classification of the systems of imprimitivities and their kernels.

Except for those introduced above and in the preceding paper [3] of this series, the notation and terminology in general follow Wielandt [8]. The geometry of n^t , developed in [3], is indispensable to the following study of imprimitive subgroups. Some elementary information on n^t , $G_{(n^t)}$, and $\Delta_m(n^t)$ is liberally employed without individual specific reference.

These studies will eventually yield the following theorem.

THEOREM II. M_{24} has up to conjugacy the following nine maximal subgroups:

- (1) $\text{PSL}_2(23)$ (primitive),
- (2) $N_{M_{24}}(M_{12})$ with imprimitive image C_2 ,
- (3) $G_{[8]}^3$ with imprimitive image S_3 ,
- (4) $G_{(4)}^*$ with imprimitive image S_6 ,
- (5) $\text{PSL}_2(7)$ with imprimitive image $\text{PSL}_2(7)$,
- (6) M_{23} (intransitive),
- (7) $N_{M_{24}}(M_{22})$ (intransitive),
- (8) $N_{M_{24}}(M_{21})$ (intransitive),
- (9) $N_{M_{24}}(\text{syl}_2(M_{19}))$ (intransitive).

1. The primitive subgroups. The following shows that any proper transitive subgroup of M_{24} is either $\text{PSL}_2(23)$ or imprimitive.

PROPOSITION 1.1. *If $G \subseteq M_{24}$ and G is primitive, then $G \cong \text{PSL}_2(23)$ or $G = M_{24}$. All $\text{PSL}_2(23)$ are conjugates in M_{24} .*

Proof. The proof will be carried out in two parts.

A. G is doubly transitive.

B. G is primitive but not doubly transitive.

For case A, we establish first that 11 divides $|G|$. Suppose 11 does not divide $|G|$, and consider $G_{[1]}$. $G_{[1]}$ is transitive on 23 points and is primitive. Consider $\text{syl}_{23}(G_{[1]})$. Since $|N_{M_{24}}(\text{syl}_{23}(M_{24}))| = 23 \cdot 11$, when 11 does not divide $|G|$, $|N_{G_{[1]}}(\text{syl}_{23}(G_{[1]}))| = 23$. Then by Burnside, $\text{syl}_{23}(G_{[1]})$ has a normal complement N in $G_{[1]}$.

If N is E , then $|G_{[1]}| = 23$ and $|G| = 24 \cdot 23$. But the degree of G is 24 and 24 is not a power of a prime [1, p. 221], so $N \neq E$. Since $G_{[1]}$ is primitive, nonidentity N is transitive on 23 and then $23 \cdot 23$ divides $|G_{[1]}|$ which is impossible.

Therefore we have $|G| = 24 \cdot 23 \cdot 11 \cdots$. Now we separate case A into two cases:

a. G is not 3-transitive, and b. G is 3-transitive. In case a, A, it is obvious that 7

does not divide $|G|$. We consider two cases for case α, A : α . 5 divides $|G_{[1]}|$, and β . 5 does not divide $|G_{[1]}|$. For α, A , $|G| = 24 \cdot 23 \cdot 11 \cdot 5 \cdot 3^X \cdot 2^Y$, $X=0, 1, 2$, $Y=0, 1, \dots, 7$. Since $|N_G(\text{syl}_{23}(G))| = 23 \cdot 11$,

$$24 \cdot 5 \equiv 5 \pmod{23}, \quad 3^X 2^Y \equiv 14 \pmod{23}.$$

But there is no solution for $3^X 2^Y \equiv 14 \pmod{23}$. Therefore the case α, A does not occur.

Now consider the case β, A . If an element of order 2 normalizes $\text{syl}_{11}(G)$ in G , it must be of type 2^{12} . So in $G_{[1]}$ no element of order 2 can normalize $\text{syl}_{11}(G_{[1]})$. Since $|C_{M_{24}}(\text{syl}_{11}(M_{24}))| = 11$ and $|N_{M_{24}}(\text{syl}_{11}(M_{24}))| = 11 \cdot 5 \cdot 2$, when 5 does not divide $|G_{[1]}|$, we have that $\text{syl}_{11}(G_{[1]})$ has a normal complement N in $G_{[1]}$. Since $G_{[1]}$ is primitive and N is normal in $G_{[1]}$, N is primitive and 23 divides $|N|$. Since 11 does not divide $|N|$, $\text{syl}_{23}(N)$ has a normal complement N' in N . If N' is not E , N' is primitive and 23 divides $|N'|$, which is impossible, so $N' = E$ and $|G_{[1]}| = 23 \cdot 11$ and $|G| = 24 \cdot 23 \cdot 11$.

Therefore we have found, in case β, A , a possibility of an existence of a doubly but not triply transitive subgroup of order $24 \cdot 23 \cdot 11$ of M_{24} . Indeed, E. Witt [9, p. 264] constructs such a subgroup in M_{24} which is a $\text{PSL}_2(23)$ in the following way.

In M_{24} , let A be an element of order 23. A leaves fixed a point which we shall call ∞ . Let 0 be another point and set $i = A^i 0$. We know $|N_{M_{24}}(A)| = 11 \cdot 23$. Let B be an element of $N_{M_{24}}(A)$ of order 11 which fixes 0. By Witt's lemma [3, Lemma 1.2] there is an element C of order 2 in $N_{M_{24}}(B)$ which interchanges ∞ and 0. Let $\rho \neq 1$ be a suitable quadratic residue mod 23. Then A, B, C permute the points according to $X+1, \rho X, -X^{-1}$, and $\text{PSL}_2(23) = \langle A, B, C \rangle$.

By the above construction, any doubly transitive subgroup of order $24 \cdot 23 \cdot 11$ of M_{24} is a $\text{PSL}_2(23)$.

Now we show that all $\text{PSL}_2(23)$ are conjugate. A computation shows $\Lambda_{2^{12}, 3^8, 23^1} = 23 = |C_{M_{24}}(23 \text{ 1})|$. Thus any element of order 23 in M_{24} can be expressed as products of elements 2^{12} and 3^8 exactly 23 times. Furthermore, $a \cdot b = \alpha \cdot \beta = c$ where a and α are of type 2^{12} , b and β are of type 3^8 and c is of type 23 1 if and only if $\alpha = a^\xi, \beta = b^\xi, \xi \in C_{M_{24}}(23 \text{ 1})$.

Let A be a $\text{PSL}_2(23)$. The following is easily seen. Let c be an element of order 23 in A , then there are elements of type 2^{12} and 3^8 denoted by a and b , respectively, such that $a \cdot b = c$ and $A = \langle a, b \rangle$.

Let two $\text{PSL}_2(23)$'s, A and B , be given. Let $c \in A$ and $\gamma \in B$ and $c^{23} = \gamma^{23} = 1$. Then there is an element $g \in M_{24}$ such that $\langle c \rangle^g = \langle \gamma \rangle$. Thus $c^g = \gamma^i, 1 \leq i \leq 22$. Now by the above, there are two elements 2^{12} and 3^8 , call them α and β , respectively, such that $\alpha \cdot \beta = \gamma^i$ and $B = \langle \alpha, \beta \rangle$. Now

$$c^g = a^g \cdot b^g = \alpha \cdot \beta = \gamma^i.$$

Thus $a^g = \alpha^\xi, b^g = \beta^\xi$ where $\xi \in C_{M_{24}}(\gamma^i)$ and $\alpha = a^{g\xi^{-1}}, \beta = b^{g\xi^{-1}}$ and A and B are conjugate.

Now we go back to case b,A: G is 3-transitive. In this case $G_{[1]}$ is 2-transitive and $|G_{[1]}| = 23 \cdot 22 \cdot \dots$. Suppose 5 does not divide $|G_{[1]}|$. Since an element of order 2 cannot normalize $\text{syl}_{11}(G_{[1]})$, syl_{11} in $G_{[1]}$ must have a normal complement N in $G_{[1]}$. Now N is primitive and 23 divides $|N|$. Consider $\text{syl}_{23}(N)$. Then 11 does not divide $|N|$, so that $\text{syl}_{23}(N)$ has a normal complement N' in N . If $N' = E$, $|N| = 23$ and $G_{[1]} = 23 \cdot 11$, which is not the case. So $N' \neq E$ and 23 divides $|N'|$ which is also impossible since if 23 divides $|N'|$ then $(23)^2$ divides $|N|$. Therefore 5 divides $|G_{[1]}|$ and 5 divides $|G|$, and $|G| = 24 \cdot 23 \cdot 22 \cdot 5 \cdot \dots$.

We claim 7 also divides $|G|$. Suppose 7 does not divide $|G|$. Since $|N_6(\text{syl}_{23}(G))| = 23 \cdot 11$, by Sylow,

$$24 \cdot 10 \equiv 10 \pmod{23},$$

$$3^\alpha \cdot 2^\beta \equiv 7 \pmod{23}, \quad \alpha = 0, 1, 2; \beta = 0, 1, \dots, 6.$$

But there is no solution for the above equation. Therefore 7 divides $|G|$ and $|G| = 24 \cdot 23 \cdot 22 \cdot 7 \cdot 5 \cdot \dots$. Then $|G_{[3]}| = 5 \cdot 7 \cdot \dots$, and G is 4-transitive and $G = M_{24}$.

Next we consider the second case.

B. Suppose G is primitive but not 2-transitive. We quote two lemmas for this case.

LEMMA α (WEISS, 1934 [8, p. 48]). *Let the lengths of the orbits of $G_{[1]}$, ordered according to increasing magnitude, be $1 = n_1 \leq n_2 \leq \dots \leq n_k$. If there is an index $j > 1$ such that n_j and the maximal orbit length n_k are relatively prime, then G is imprimitive or a regular group of prime degree.*

LEMMA β [8, p. 50]. *If a prime p is a divisor of the order of $G_{[1]}$, then p also divides the order of $G_{[1]}^\Gamma$. Γ is an orbit of $G_{[1]}$.*

Now, if G is primitive but not 2-transitive, then 23 does not divide $|G|$. Also, we have that 11 does not divide $|G|$. If 11 divides $|G|$, syl_{11} has orbits of lengths 1, 1, 11, 11. Since $G_{[1]}$ cannot fix any other points and 23 does not divide $|G|$, $G_{[1]}$ has orbits of lengths 1, 11, 12. Now, $(11, 12) = 1$ and, by Lemma α , G is imprimitive, which is a contradiction. Lastly, we claim 7 does not divide $|G|$. If 7 divides $|G|$, syl_7 has orbits of lengths 1, 1, 1, 7, 7, 7. If $G_{[1]}$ has 3 orbits, then the possibilities of the orbit lengths are, since $G_{[1]}$ cannot have an orbit of length 2,

$$1, 8, 15; \quad 1, 7, 16; \quad 1, 9, 14.$$

By Lemma α , G is imprimitive.

If $G_{[1]}$ has 4 orbits, then the possibilities of the orbit lengths are 1, 7, 8, 8; 1, 7, 7, 9. By Lemma α , again G is imprimitive. Therefore $|G| \mid (2^3)^2 7^3 3^2 5$. We claim 5 divides $|G|$, otherwise G is solvable, but the degree of G , 24, is not a power of a prime. Therefore 5 divides $|G_{[1]}|$. By Lemma β , the shortest orbit of $G_{[1]}$ has length ≥ 5 . If the shortest orbit has length 5, then since elements of order 5 in M_{24} have the cycle form $1^4 5^4$, we have the following choices of orbits of $G_{[1]}$.

	shortest		longest	
1	5	6	6	6
1	5	5	6	7
1	5	5	5	8
1	5	8		10

Except for the case 1, 5, 8, 10, the other cases can be eliminated by Lemma α . For the case 1, 5, 8, 10, let the orbit of length 8 be Γ . 5 divides $|G_{[1]}^\Gamma|$ and 5 is greater than the largest proper factor of 8, so $G_{[1]}^\Gamma$ is primitive. By Jordan, $G_{[1]}^\Gamma$ is $8-5+1=4$ -fold transitive. Then 7 divides $|G_{[1]}^\Gamma|$ and 7 divides $|G|$ which is a contradiction.

If the shortest orbit has length 6, then we have choices 1, 6, 7, 10 and 1, 6, 6, 11. By Lemma α , these are eliminated.

If the shortest orbit has length 7, then we have choice 1, 7, 16. By Lemma α , this is eliminated.

If the shortest orbit has length 10, then we have choice 1, 10, 13. By Lemma α , this is eliminated.

If the shortest orbit has length 11, then we have choice 1, 11, 12. By Lemma α , this is eliminated.

2. The imprimitive subgroups. The essential feature of the discussions on imprimitive subgroups in this paper is their tracing. Given an imprimitive subgroup G of a given type, we need to know whether G exists in M_{24} and if it does, whether it is maximal, otherwise in what imprimitive subgroup we can locate it.

The results of such tracings on all the imprimitive subgroups are presented here at the outset of the discussion in synopsis form for reference. For example, a group of type 3^8 with nontrivial kernel must be located in $G_{[8]}^3$ according to Propositions 7.1 and 4.4, as listed in the following summary.

Thus we summarize the results on imprimitive subgroups as follows.

Propositions (in summary).

TYPE 12^2 .

PROPOSITION 3.1. G of type 12^2 is one of $N_{M_{24}}(G_{(12^4)}), i=1, 2, 5$. $G_{(12^4)}, i=1, 2, 5$, are contained in $N_{M_{24}}(G_{(12^4)}), i=1, 2, 5$, respectively.

TYPE 8^3 .

PROPOSITION 4.1. G of type 8^3 has block system $8^*|8^*|8^*$.

PROPOSITION 4.2. G of type 8^3 is in $G_{[8]}^3$. $G_{[8]}^3$ has order $2^{10} \cdot 3^2 \cdot 7$ and the image is S_3 .

PROPOSITION 4.3. All $G_{[8]}^3$ are conjugate in M_{24} .

PROPOSITION 4.4. $N_{M_{24}}(3^8) \subset G_{[8]}^3$.

TYPE 6^4 .

PROPOSITION 5.1. G of type 6^4 is in one of the following: a group of type 12^2 , $N_{M_{24}}(2^{12})$ or $G_{[8]}^3$.

TYPE 4⁶. Classification by K . K_i denotes the kernel of restriction of K on a system B_i of imprimitivity.

PROPOSITION 6.1. (a) $K \neq E$, $K_1 \neq E$, $K_1 \cap K_2 \neq E$. G is in $G_{(4)}^*$. $G_{(4)}^*$ has order $2^{10} \cdot 3^3 \cdot 5$ and its image is S_6 .

PROPOSITION 6.2. (b) $K \neq E$, $K_1 \neq E$, $K_1 \cap K_2 = E$. G does not exist. (d) $K = E$. G is in a group of type 12^2 .

PROPOSITION 6.3. (c) $K \neq E$, $K_1 = E$. G is in one of the following: $N_{M_{24}}(2^{12})$, $G_{[8 \cdot]}^3$, or $G_{(4)}^*$.

PROPOSITION 6.4. $G_{(4)}^*$ contains $G_{(4)}$, $G_{(6 \cdot \cdot)}$, $N_{M_{24}}(2^{12})$, $N_{M_{24}}(G_{(12 \cdot \cdot)})$, and $N_{M_{24}}(G_{(12^v)})$.

TYPE 3⁸.

PROPOSITION 7.1. $K \neq E$. G is in $N_{M_{24}}(3^8)$.

PROPOSITION 7.2. $K = E$. G is a $\text{PSL}_2(7)$ in S_{24} . These $\text{PSL}_2(7)$ of degree 24 are all conjugate in M_{24} . $\text{PSL}_2(7) \not\subseteq G_{[8 \cdot]}^3$.

TYPE 2¹².

PROPOSITION 8.1. $K \neq E$, then G is either in $G_{(4)}^*$ or in $G_{[8 \cdot]}^3$. $K = E$, then G is in one of a group of type 12^2 .

Thus we will see, at the end of the discussions of the imprimitive subgroups, that, by Propositions 3.1 through 8.1, there are only 4 imprimitive subgroups which are not contained in any other imprimitive subgroup of M_{24} , namely, $N_{M_{24}}(G_{(12^v)})$, $G_{[8 \cdot]}^3$, $G_{(4)}^*$, and $\text{PSL}_2(7)$.

In §9, it will be shown that the above four imprimitive subgroups, along with the primitive one, $\text{PSL}_2(23)$, constitute the entire list of transitive maximal subgroups of M_{24} , up to conjugacy.

Furthermore, we note here that among the nine maximal subgroups among the intransitives of M_{24} [3, Theorem I], we see that $G_{(12^i)}$, $i = 1, 2, 5$, are in $N_{M_{24}}(G_{(12^i)})$, $i = 1, 2, 5$ (Proposition 3.1), and $G_{(4)}$ and $G_{(6 \cdot \cdot)}$ are in $G_{(4)}^*$ (Proposition 6.4).

Now we proceed to prove the above propositions.

3. Groups of type 12^2 .

PROPOSITION 3.1. Let G be a group of type 12^2 , then $G \subseteq N_{M_{24}}(G_{(12^i)})$, $i = 1, 2, 5$. $(N_{M_{24}}(G_{(12^i)}))^* = C_2$ and the kernels are $G_{(12^i)}|G_{(12^i)}$, $i = 1, 2, 5$.

Proof. $G_{(12^{\cdot \cdot \cdot})}$ and $G_{(12^v)}$ are intransitive on $12^{\cdot \cdot \cdot}$ and 12^v respectively. Therefore the only available systems of imprimitivity of length 12 are $12^i|12^i$, $12^i|12^{\cdot \cdot}$, and $12^v|12^v$. Since there is a substitution interchanging the two sets 12^i and $(12^i)^c$, we have three imprimitive groups with kernels $G_{(12^i)}$, $i = 1, 2, 5$, images C_2 , and systems of imprimitivity $12^i|12^i$, $i = 1, 2, 5$. These are $N_{M_{24}}(G_{(12^i)})$, $i = 1, 2, 5$. Thus given $12^i|12^i$, $N_{M_{24}}(G_{(12^i)})$ is the only imprimitive group with the given systems of imprimitivity. And given $(12^i|12^i)_1$ and $(12^i|12^i)_2$, there is an element $g \in M_{24}$ such that $(12^i|12^i)_1^g = (12^i|12^i)_2$. So there is essentially only one imprimitive group

with systems of imprimitivity $12^4|12^4$. It is apparent that $N_{M_{24}}(G_{(12^4)})$ are the biggest imprimitive groups with systems $12^4|12^4$.

4. Groups of type 8^3 .

PROPOSITION 4.1. *A group G of type 8^3 has block systems of type $8'|8'|8'$.*

Proof. Since $G_{(8^{\dots})}$ is intransitive on $8''$, $8''|8''|8''$ cannot be systems of imprimitivity.

According to [3, Proposition 4.3] each $8'''$ determines a unique $8'$, one of the orbits of $G_{(8^{\dots})}$. Thus G with system $8'''|8'''|8'''$ can be described as one with system $8'|8'|8'$.

In the following proposition we construct a group of type 8^3 with system $8'|8'|8'$, called $G_{[8^3]}$.

PROPOSITION 4.2. *$G_{[8^3]}$ has order $2^{10}3^{27}$ and its imprimitive image is S_3 . It is the biggest imprimitive group with such given systems of imprimitivity, and is unique.*

Proof. Consider the holomorph of the elementary abelian group of order 2^4 , \mathfrak{A}_{2^4} . \mathfrak{A}_{2^4} has 15 normal subgroups of order 2^3 . The group of order 2^3 is semiregular on the 16 points and has two orbits of length 8. The holomorph permutes these 15 subgroups transitively by conjugation. The normalizer in H of one of these 15 subgroups must be of index 15 and of order $2^{10}3 \cdot 7$. Therefore, the order of the stabilizer of one of these two orbits of length 8 must be at least $2^9 \cdot 3 \cdot 7$, so each orbit is a $8'$, and we have a system $8'|8'|8'$. Therefore, the order of the group in M_{24} which fixes these three $8'$'s setwise is $2^9 \cdot 3 \cdot 7$ and this is the order of the kernel of $G_{[8^3]}$.

The kernel of imprimitivity contains an element of order 7, say σ . σ has type $7^3 1^3$. Let

$$\sigma = (E_1)(E_2)(E_3)(p_1)(p_2)(p_3).$$

The E_i is a $7'$ and $E_i \cup p_j$ is either a $8'$ or a $8''$. Given any E_i , there is a unique point which, added to E_i , makes E_i a $8'$. This point must be one of p_i . Let $E_1 \cup p_1 = 8'$, then $E_1 \cup p_2 = 8''$ and $E_1 \cup p_3 = 8''$. We have seen in [3] that there is an element τ of order 3 which centralizes σ . Since $\text{syl}_7(S_7)$ is selfcentralizing, τ must be of type 3^8 and permutes E_i 's and p_i 's cyclically. We fix notations so that

$$E_1^* = E_2, \quad E_2^* = E_3, \quad p_1^* = p_2, \quad p_2^* = p_3,$$

then $E_1 \cup p_1 = 8'$, $E_2 \cup p_2 = 8'$ and $E_3 \cup p_3 = 8'$. Thus we have a system $8'|8'|8'$. This system must coincide with the systems of imprimitivity of $G_{[8^3]}$ which was described above. Now τ permutes these three blocks cyclically. Furthermore, we know there is an element of type $1^{82}8$, i , which centralizes σ . This involution must fix one block and interchange the remaining two blocks. Thus the imprimitivity image is S_3 , and the imprimitive group has order

$$|G_{[8^3]}| = 2^9 \cdot 3 \cdot 7 \cdot 2 \cdot 3 = 2^{10} \cdot 3^2 \cdot 7.$$

Any such group with given $8'|8'|8'$ must be unique.

Next, we shall show that given two systems of $8'|8'|8'$, say $(8'|8'|8')_1$ and $(8'|8'|8')_2$, they are conjugate, i.e. there exists an element g in M_{24} such that $(8'|8'|8')_1^g = (8'|8'|8')_2$. For this we need the following lemma.

LEMMA 4.3.1. *Given a set $8'$, denoted by $\#8'$, then there are 30 $8'$'s such that $|\#8' \cap 8'| = 0$, 280 $8'$'s such that $|\#8' \cap 8'| = 4$, and 448 $8'$'s such that $|\#8' \cap 8'| = 2$.*

These are the only possibilities of intersection of two $8'$'s. Furthermore, let $G_{(8')} = \mathfrak{H}$, and if A and A' are two of fixed type, then there exists an element $\gamma \in \mathfrak{H}$ such that $A' = A'$.

Proof. There are $[M_{24} : \mathfrak{H}] = 3 \cdot 11 \cdot 23 = 759$ $8'$'s. The action of M_{24} on these 759 $8'$'s is in permutation isomorphism with M_{24} on 759 cosets of \mathfrak{H} . Now by computation, we see that $(1_{\mathfrak{H}})^{M_{24}} = \chi_1 + \chi_{23} + \chi_{7 \cdot 36} + \chi_{23 \cdot 21}$. So \mathfrak{H} has four orbits on the 759 $8'$'s.

The 759 $8'$'s each contain $\binom{8}{5} 5$'s and there are $\binom{24}{5} 5$'s all told. Since M_{24} is 5-fold transitive, each 5 is contained in exactly $759 \cdot \binom{8}{5} / \binom{24}{5} = 1$ $8'$, i.e. $8'$'s form a Steiner system. Therefore $\#8'$ meets any other $8'$ in at most 4 points.

Each 4 is in exactly $759 \cdot \binom{8}{4} / \binom{24}{4} = 5$ $8'$'s, so each 4 in $\#8'$ is the intersection of $\#8'$ with 4 other $8'$'s. Hence there are $\binom{8}{4} \cdot 4 = 280$ $8'$'s meeting $\#8'$ in 4 points.

Each 3 is in exactly $759 \cdot \binom{8}{3} / \binom{24}{3} = 21$ $8'$'s. In $\#8'$, each 3 is in 5 4's, each the intersection of $\#8'$ with 4 other $8'$'s. So we get 20 $8'$'s meeting $\#8'$ in 4 points containing the given 3. Hence there is no $8'$ meeting $\#8'$ in exactly 3 points.

Each 2 is in $759 \cdot \binom{8}{2} / \binom{24}{2} = 77$ $8'$'s. In a given $\#8'$, 2 is in $\binom{6}{2} = 15$ 4's, each the intersection of $\#8'$ with 4 other $8'$'s, so there are $77 - 1 - 15 \cdot 4 = 16$ $8'$'s meeting $\#8'$ in a given pair of points. Hence there are $\binom{8}{2} \cdot 16 = 448$ $8'$'s meeting $\#8'$ in 2 points.

We can regard $\Omega - \#8'$ as the points of $V_4(F_2)$, and then the 15 subspaces of dimension 3 and their complement form 30 $8'$'s disjoint from $\#8'$.

Since $1 + 280 + 448 + 30 = 759$, this accounts for all $8'$'s.

Now we can show our proposition:

PROPOSITION 4.3. *Let $(8'|8'|8')_1$ and $(8'|8'|8')_2$ be two systems of type $8'|8'|8'$. Then they are conjugate.*

Proof. Let $(8'|8'|8')_1 = A|B|C$ and $(8'|8'|8')_2 = A'|B'|C'$. Then there exists an element $g \in M_{24}$ such that

$$A|B|C \xrightarrow{g} A'|B''|C''.$$

Now $A' \cap B'' = \emptyset$ and $A' \cap B' = \emptyset$, so by the above proposition there exists an element $h \in H = G_{(A)}$ such that

$$A'|B''|C'' \xrightarrow{h} A'|B'|C'''.$$

But $C''' = C'$ as the complement of $A' \cup B'$. Thus $(8'|8'|8')_1 \approx (8'|8'|8')_2$.

Now we conclude the discussion of $G_{[8']}^3$ with an inclusion relation $N_{M_{24}}(3^8) \subset G_{[8']}^3$.

PROPOSITION 4.4. $N_{M_{24}}(3^8) \subset G_{[8]}^3$.

Proof. We can represent the kernel K of $G_{[8]}^3$ as the subgroup of the holomorph of \mathfrak{A}_{2^4} consisting of the matrices $\begin{bmatrix} A & B \\ 0 & I \end{bmatrix}$, where $A \in \text{SL}(3, 2)$, I is the 2×2 identity, B a 3×2 matrix over GF [2]. Then K is the semidirect product of L and M , where $L = \{\begin{bmatrix} A & 0 \\ 0 & I \end{bmatrix}\}$ and $M = \{\begin{bmatrix} I & B \\ 0 & I \end{bmatrix}\}$. M is elementary abelian of order 2^6 and is characteristic in K ($M = O_2(K)$, the maximal normal 2-group of K). Then $G_{[8]}^3$ is the split extension of K by $S_3 = \langle \tau, i \mid \tau^3 = i^2 = (\tau i)^2 = 1 \rangle$. The complements of M in K are in 1-1 correspondence with the cocycles in $Z^1(L, M)$ which is a 2-group [4, p. 121]. τ acts on the set of complements by conjugation. Hence τ normalizes at least one complement N of M in K . Then $N \cong K/M \cong \text{SL}(3, 2) \cong \text{PSL}_2(7)$. Since the outer automorphism of N has order 2 and $Z(N) = E$, $\langle N, \tau \rangle = N \times T$ where T is of order 3. A generator of T has type 3^8 and we may assume $T = \langle \tau \rangle$. Then $\langle N, \tau, i \rangle$ normalizes $\langle \tau \rangle$. Since $|\langle N, \tau, i \rangle| = 2^4 \cdot 3^2 \cdot 7 = |N_{M_{24}}(3^8)|$, we have $N_{M_{24}}(\tau) = \langle N, \tau, i \rangle \subset G_{[8]}^3$.

It can be shown that N acts as $\text{PSL}_2(7)$ on the eight 3-cycles of τ .

We insert the following lemma for future reference.

LEMMA 4.4.1. $\text{Syl}_3(M_{24})$ has four subgroups of order 9 and they all have an orbit of length 9.

Proof. Let $G_{(3)}$ fix the last 3 points, I, II, III, setwise. Then $G_{(3)}$ is S_3 on $\{I, II, III\}$. The kernel of map is $M_{21} = \text{PSL}_3(4)$. Now the subgroup of $G_{(3)}$ corresponding to A_3 on $\{I, II, III\}$ may be represented as $\text{PGL}_3(4)$ on the remaining 21 points. Now $|\text{syl}_3(\text{PGL}_3(4))| = 3^3 = |\text{syl}_3(M_{24})|$, so $\text{syl}_3(M_{24})$ on the 21 points can be regarded as $\text{syl}_3(\text{PGL}_3(4))$, and we have

$$\text{syl}_3(\text{PGL}_3(4)) = \left\langle \begin{bmatrix} \rho & & \\ & \bar{\rho} & \\ & & 1 \end{bmatrix}, \begin{bmatrix} & 1 & \\ 1 & & \\ & & 1 \end{bmatrix}, \begin{bmatrix} & 1 & \\ & & 1 \\ \bar{\rho} & & \end{bmatrix} \right\rangle$$

and the first two generate $\text{syl}_3(\text{PSL}_3(4))$. Thus $\text{syl}_3(M_{24})$ is nonabelian and of exponent 3. Therefore by [4, p. 93] there are two elements, A and B , such that $\text{syl}_3(M_{24}) = \langle A, B \rangle$ and $A^3 = B^3 = [A, B]^3 = 1$, $A[A, B] = [A, B]A$, $B[A, B] = [A, B]B$. Thus $Z = \langle [A, B] \rangle = G' = \Phi(G)$ where $G = \text{syl}_3(M_{24})$. Using a suitable notation for 21 points of $\text{PG}(2, 2^2)$, A and B and $[A, B]$ can be chosen as follows:

$$A = (1\ 17\ 18)(8\ 11\ 14)(2\ 21\ 9)(3\ 20\ 5)(13\ 4\ 19)(6\ 15\ 12)(7)(10)(16)(\text{I})(\text{II})(\text{III}),$$

$$B = (1\ 17\ 18)(2\ 21\ 13)(3\ 20\ 9)(4\ 19\ 5)(6\ 8\ 16)(7\ 12\ 11)(10\ 15\ 14)(\text{I}\ \text{II}\ \text{III}),$$

$$[A, B] = (6\ 12\ 15)(7\ 10\ 16)(8\ 11\ 14)(2\ 4\ 3)(5\ 9\ 13)(19\ 20\ 21)(1)(17)(18)(\text{I})(\text{II})(\text{III}).$$

Now $\text{syl}_3(M_{24})/\langle [A, B] \rangle = \langle A, B \rangle$ and there are four subgroups of order 9 in $\text{syl}_3(M_{24})$, namely $\langle AB \rangle$, $\langle (AB)^2 \rangle$, $\langle A \rangle$, and $\langle B \rangle$. It is easily seen that $\langle A \rangle$ and $\langle (AB)^2 \rangle$ have orbits 9, 3, 3, 3, 3, 1, 1, 1. All elements are of type $3^6 1^6$ and $\langle AB \rangle$ and $\langle B \rangle$ have orbits 9, 9, 3, 3, and six elements are of type 3^8 and two are of type $3^6 1^6$.

5. Groups of type 6^4 .

PROPOSITION 5.1. *Let G be a group of type 6^4 with primitive G^* . Let K be the kernel of imprimitivity, then one of the following applies:*

- (a) $K=E$ and G is of type 12^2 .
- (b) $K \neq E$ and G is with system $6' | 6' | 6' | 6'$, and $G \subseteq N_{M_{24}}(2^{12})$ or $G \subseteq G_{[8 \cdot]}^3$.
- (c) $K \neq E$, G is with system $6'' | 6'' | 6'' | 6''$, and $5 \nmid |G|$. And $G \subseteq N_{M_{24}}(2^{12})$ or $G \subseteq G_{[8 \cdot]}^3$.

Proof. (a) $K=E$. $G^*=S_4$ and G must be regular. The normal subgroup of order 12 has two orbits of length 12, so G has systems of imprimitivity of length 12. Consequently $G \subseteq N_{M_{24}}(G_{(12^4)})$ for some i , $i=1, 2, 5$.

(b) $K \neq E$ and G is with $6' | 6' | 6' | 6'$. Then $K \subseteq G_{(6 \cdot)}$, which has orbits of length 16 and 2. Since K is $1/2$ -transitive, every orbit of K must have length 2. Then either $|K|=2$ and $G \subseteq N_{M_{24}}(2^{12})$ or K is a four group with 3 involutions of type $1^8 2^8$ whose fixed point sets are disjoint. Thus $G \subseteq G_{[8 \cdot]}^3$.

(c) $K \neq E$ and G is with system $6'' | 6'' | 6'' | 6''$.

(1) Let $5 \mid |G|$. Since 5 divides $|K|$, K is 2-transitive on each block B_i , so K is \bar{A}_5 , \bar{S}_5 , A_6 or S_6 on each B_i . Groups of order 9, by Lemma 4.4.1, have orbits of length 9, so A_6 or S_6 are not possible. Next, if K were not faithful on B_i , the kernel K_i would have order 3 by knowledge of $G_{[6 \cdot]}$. So $|K|$ would be divisible by 9 and this is again impossible. A kernel system $\bar{S}_5 | \bar{S}_5 | \bar{S}_5 | \bar{S}_5$ is impossible because $1^4 \in \bar{S}_5$ produces $(1^2)^4(4)^4$. Next consider $K \cong \bar{A}_5 | \bar{A}_5 | \bar{A}_5 | \bar{A}_5$.

Since $K|B_i$ is faithful and is \bar{A}_5 , $G|B_i$ is at least A_6 . So there is an element $\sigma \in G$ such that $\sigma^{B_1} = 1^3 3$. $\sigma \notin K$ because any element of order 3 in K , restricted on B_1 , has type 3^2 . Therefore $\sigma^{B_2 \cup B_3 \cup B_4}$ must permute these 3 blocks cyclically. In M_{24} , the only possible component of σ^{B_1} on $B_2 \cup B_3 \cup B_4$ is $1^3 3^5$. I.e.

$$\begin{array}{ccc} B_1 & B_2 \cup B_3 \cup B_4 \\ 1^3 3 & 1^3 3^5 \end{array}$$

Now elements of type $1^3 3^5$ on $B_2 \cup B_3 \cup B_4$ cannot permute B_i 's, $i \neq 1$, cyclically.

(2) Let $5 \nmid |G|$. Then G is solvable and $G^*=A_4$ or S_4 . Choose a minimal G -normal subgroup N of K . Then $|N|=2^\alpha$ or 3^β .

(A) If $|N|=2$ or 3 , then G is an imprimitive group with systems of imprimitivity of length 2 or 3 and its kernels have order 2 or 3. Thus $G \subset N_{M_{24}}(2^{12})$ or $N_{M_{24}}(3^8)$ which is in $G_{[8 \cdot]}^3$ by Proposition 4.4.

(B) If $|N|=2^\alpha$, then N is intransitive on each block of length 6 and since the lengths of orbits of N must be powers of 2 and the union of orbits must have length 6, every orbit of N has length 2. $B_i=6''$, so N is faithful on B_i .

For N^{B_i} , we have the following three choices.

If $N^{B_i} = c_2 \times c_2 \times c_2$, then excluding the identity, altogether 18×4 points are fixed by N . Meanwhile, each element can fix only 8 points, so $8 \times 7 = 56$ points is the maximal number of points which can be fixed by N , which is a contradiction.

Next, if N^{B_1} = the positive part of $c_2 \times c_2 \times c_2$, then we combine the fixed points to form 3 $\mathbf{8}'$'s which cannot overlap, since G would then be intransitive. So we get systems of imprimitivity of length 8 and $G \subseteq G_{[8]}^3$ if it exists.

Lastly, if $N^{B_1} = \langle (ab)(cd) \rangle \cdot \langle (ef) \rangle$, then we would have elements of type $1^{4 \cdot 4} 2^4 = 1^{16} 2^4$, which is impossible.

(C) $|N| = 3^2$. We eliminate this case by Lemma 4.4.1 which shows that any group of order 3^2 has at least one orbit of length 9, which is a contradiction, since as a subgroup of the kernel, N cannot have orbits longer than 6.

6. Groups of type 4^6 . Let G be an imprimitive group with systems of imprimitivity $B_1|B_2|B_3|B_4|B_5|B_6$ where $|B_i| = 4$. Let G^* be primitive, i.e. \bar{A}_5 , \bar{S}_5 , A_6 or S_6 , then they are all doubly transitive. Let K be the kernel of imprimitivity and denote the kernel of K on B_i by K_i .

The discussion will be divided into four cases.

- (a) $K \neq E$, $K_1 \neq E$, $K_1 \cap K_2 \neq E$,
- (b) $K \neq E$, $K_1 \neq E$, $K_1 \cap K_2 = E$,
- (c) $K \neq E$, $K_1 = E$,
- (d) $K = E$.

We obtain for case (a) the following:

PROPOSITION 6.1. *In M_{24} , we have a group of type 4^6 with kernel K of type (a) above. Denote this group by $G_{(4)}^*$, $G_{(4)}^*$ has order $2^{10} \cdot 3^3 \cdot 5$ and its image is S_6 . Any group of type 4^6 with type (a) kernel is contained in one of the conjugates of $G_{(4)}^*$ in M_{24} .*

Proof. Take any 4 points of the 24 points. Call them B_1 . For any other point p , $B_1 \cup p$ determines a unique $\mathbf{8}' = B_1 \cup B_i$, where $B_i - p$ is the orbit of length 3 of $G_{(B_1 \cup p)}$. Thus we obtain 5 other B 's, B_2, B_3, B_4, B_5 and B_6 . Obviously $G_{(B_1)}$ maps B_i to B_j , $i, j = 2, 3, 4, 5, 6$, and is transitive on $\{B_2, B_3, B_4, B_5, B_6\}$. $G_{[B_1 \cup B_2]}$ is the elementary abelian group of order 2^4 and is regular on the remaining 16 points, therefore $G_{(B_1)}$ is doubly transitive on $\{B_2, B_3, B_4, B_5, B_6\}$. Obviously, these B_i , $i = 2, \dots, 6$, are the unique blocks of $G_{[B_1]}$ and of $G_{(B_1)}$ as well by [3, Proposition 2.4]. Thus B_i is $\Gamma_j - x$, $j = 1, \dots, 5$, where Γ_j is the 5 lines through $x = (0 \ 0 \ 1)$ in $\text{PSL}_3(4) = M_{21}$. Thus

$$\Gamma_1 = [0, 1, 0] = \{(0 \ 0 \ 1); (1 \ 0 \ 0); (1 \ 0 \ 1); (\bar{d} \ 0 \ 1); (d \ 0 \ 1)\},$$

$$\Gamma_2 = [1, 1, 0] = \{(0 \ 0 \ 1); (1 \ 1 \ 0); (1 \ 1 \ 1); (\bar{d} \ \bar{d} \ 1); (d \ d \ 1)\},$$

$$\Gamma_3 = [d, 1, 0] = \{(0 \ 0 \ 1); (\bar{d} \ 1 \ 0); (1 \ d \ 1); (\bar{d} \ 1 \ 1); (d \ \bar{d} \ 1)\},$$

$$\Gamma_4 = [\bar{d}, 1, 0] = \{(0 \ 0 \ 1); (d \ 1 \ 0); (1 \ \bar{d} \ 1); (d \ 1 \ 1); (\bar{d} \ d \ 1)\}.$$

$$\Gamma_5 = [1, 0, 0] = \{(0 \ 0 \ 1); (0 \ 1 \ 0); (0 \ 1 \ 1); (0 \ \bar{d} \ 1); (0 \ d \ 1)\}.$$

Since $|G_{(B_1)}| = 2^9 \cdot 3^2 \cdot 5$, the kernel of imprimitivity of $G_{(B_1)}$ on $\{B_2, \dots, B_6\}$ has order $\geq 2^6 \cdot 3$. Since $|\text{syl}_2(A_6)| = 2^6$, $B_i \cup B_j = \mathbf{8}'$, $i, j > 1$. Let $B_i \cup B_j$ be denoted by B_{ij} .

Let M be the intersection of M_{24} with the biggest imprimitive group of S_{24} on B_i 's. Obviously $G_{(B_1)} \subset M$. Consider $B_1 \cup B_2 = \mathbf{8}'$. $G_{(B_{12})}$ is A_8 on B_{12} . It contains a substitution interchanging B_1 and B_2 . Then B_{1j} , $j \neq 2$, goes to a $\mathbf{8}'$ which contains B_2 . Let this $\mathbf{8}' = B_2 \cup \{b_1, b_2, b_3, b_4\}$. Extend $B_2 \cup \{b_1\}$ to a $\mathbf{8}' = B_2 \cup B_i$, $b_1 \in B_i$. If $\{b_2, b_3, b_4\} \not\subset B_i$, then $B_2 \cup B_i = \mathbf{8}'$ and $B_2 \cup \{b_1, b_2, b_3, b_4\} = \mathbf{8}'$. Thus two $\mathbf{8}'$ share 5 points $\{B_2 \cup b_1\}$ which is impossible. Thus $\{b_1, b_2, b_3, b_4\} = B_i$. Thus the substitution is in M , and M is triply transitive.

Finally, the field conjugation which is in $G_{(B_1)}$ fixes $\Gamma_1, \Gamma_2, \Gamma_5$ and interchanges Γ_3 and Γ_4 , so M is primitive and contains a transposition. Therefore the image of M is S_6 on $\{B_1, B_2, \dots, B_6\}$. Now $|M| = |G_{(B_1)}| \cdot 6 = 2^9 \cdot 3^2 \cdot 5 \cdot 6 = 2^{10} \cdot 3^3$, and $|\text{Ker}| = 2^6 \cdot 3$. Since $|\text{syl}_2(A_8)| = 2^6$, obviously $K_1 \cap K_2 \neq E$. M will be denoted $G_{(4)}^*$, to indicate it is a kind of transitive extension of $G_{(4)}$.

Let G be an imprimitive group with six blocks of length 4 with $K \neq E$, $K_1 \neq E$, $K_1 \cap K_2 \neq E$, and G^* is primitive in S_6 . Then G^* is at least doubly transitive and consequently any union of two blocks must be a $\mathbf{8}'$. Let

$$\beta_1 | \beta_2 | \beta_3 | \beta_4 | \beta_5 | \beta_6$$

be the block system. Consider $G_{(\beta_1)}$. $G_{(\beta_1)}$ is imprimitive with block system

$$\beta_1 | B_2 | B_3 | B_4 | B_5 | B_6$$

where any union of two blocks is a $\mathbf{8}'$. Let $p \in \beta_2$ and $p \in B_i$ for some i , then $\beta_1 \cup p$ determines a unique $\mathbf{8}'$, thus $\beta_2 = B_i$ for some i . Thus G must be in the $G_{(\beta_1)}^*$, and any two such systems of imprimitivity are similar.

Next we have

PROPOSITION 6.2. *There exists no group of type 4^6 with kernel type (b). A group of type 4^6 with kernel type (d) can be represented as a group of type 12^2 .*

Proof. Let G be a type 4^6 with type (b) kernel. Then $K_1 \neq E$ and $K_1 \cap K_2 = E$. Then the subgroup of K fixing B_1 pointwise is faithfully represented on B_2 . K_1 cannot contain an element of order 3 since it would fix $4 + 5 = 9$ points. Hence K_1 has order 8, 2 or 4.

If $|K_1| = 8$, then its center is of type 2^2 on 5 blocks; then the center has cycle $1^4 2^{10}$, which is impossible.

If $|K_1| = 2$, then nonidentity elements have type 21^2 on 5 blocks or 2^2 on 5 blocks, which is impossible.

If $|K_1| = 4$, then K_1 cannot be V_4 on B_2 or have elements of type $1^4 2^{10}$. K_1 cannot be C_4 on B_2 or have elements of type $1^4 2^{10}$. Hence K_1 must be $c_2 \times c_2$. Then, the total number of points fixed (excluding identity) on B_2, B_3, B_4, B_5, B_6 is $4 \times 5 = 20$, whereas each element can fix only 4 points, totalling 12, so this is a contradiction.

Let G have type (d) kernel, i.e. the trivial kernel. Then G is S_6, A_6, \bar{S}_5 or \bar{A}_5 and they are all 2-transitive. $G_{(B_1)}$ is transitive on B_1 , so 2^2 divides $|G_{(B_1)}|$. So G cannot be \bar{A}_5 (whose order is $2^2 \cdot 3 \cdot 5$).

Suppose $G = S_6$. Then $G_{(B_1)}$ is S_5 on $\{B_2, \dots, B_6\}$. $G_{(B_1)}^{B_1} \cong G_{(B_1)}/G_{\{B_1\}}$ is transitive

on B_1 so 4 divides $|G_{(B_1)}/G_{[B_1]}|$. Now $G_{[B_1]}$ is either A_5 or E . If it is A_5 , $|G_{(B_1)}/G_{[B_1]}| = 2$, which is impossible. So $G_{[B_1]}$ must be E . Then $G_{(B_1)}^{B_1}$ is at most S_4 and sometimes S_5 , which is impossible. Therefore G is not S_6 . With the same argument exclude $G = A_6$.

Suppose $G = \bar{S}_5$. Consider $\bar{A}_5 \triangleleft \bar{S}_5$. \bar{A}_5 cannot be an imprimitive group with $K = E$ as shown above, so \bar{A}_5 is intransitive with two orbits of length 12. Thus G can be represented as an imprimitive group of type 12^2 .

For case (c), we need a lemma.

LEMMA 6.3.1. $C_{M_{24}}(5^4 1^4) \subset G_{(4)}^*$, and $C_{M_{24}}(5^4 1^4) \cong C_5 \times A_4$.

Proof. $G_{(4)}$ has compound character

$$(1_{G_{(4)}})^{M_{24}} = \chi_1 + \chi_{23} + 2 \cdot \chi_{7 \cdot 36} + 2 \cdot \chi_{23 \cdot 21} + \chi_{23 \cdot 45}^{(3)} + \chi_{23 \cdot 55} + \chi_{23 \cdot 144} + \chi_{55 \cdot 64}.$$

The compound character $(1_{G_{(4)}})^{M_{24}}$ must be a linear combination of the above 8 irreducible characters with smaller integer coefficients; besides, it must obey the eight criteria of a compound character of a subgroup [6, p. 157]. A computation shows that

$$(1_{G_{(4)}})^{M_{24}} = \chi_1 + \chi_{7 \cdot 36} + \chi_{23 \cdot 21} + \chi_{23 \cdot 45}^{(3)}.$$

(Incidentally, a laborious computation shows that the above is the only possible compound character of an overgroup of $G_{(4)}$, thus $G_{(4)}^*$ is seen to be maximal. The maximality of $G_{(4)}^*$, however, will be shown in a simpler way in Theorem II.)

By $(1_{G_{(4)}})^{M_{24}}$, we know $G_{(4)}^*$ has $2304 = 2^8 \cdot 3^2$ elements of type $1^4 5^4$ and these form a single class in $G_{(4)}^*$. Thus $|C_{G_{(4)}^*}(1^4 5^4)| = |C_{M_{24}}(1^4 5^4)| = 2^2 \cdot 3 \cdot 5$ and $C_{M_{24}}(1^4 5^4) \subset G_{(4)}^*$.

Restriction of $C_{M_{24}}(5^4 1^4)$ on the four points left fixed by $5^4 1^4$ shows that $C_{M_{24}}(5^4 1^4) = C_5 \times A_4$.

PROPOSITION 6.3. *If G is of type 4^6 with type (c) kernel, then G is in one of the following: $N_{M_{24}}(2^{12})$, $G_{[8 \cdot 1]^3}$, $G_{(4)}^*$.*

Proof. Let $K \neq E$, $K_1 = E$. Then the kernel systems are of the form $K^{B_1} | K^{B_2} | \dots | K^{B_6}$ and K^{B_i} and K^{B_j} are conjugates and two transitive constituents are connected by a simple automorphism.

If $|K| = 2$, then $K = \langle 2^{12} \rangle$ and $G \subseteq N_{M_{24}}(2^{12})$.

If $|K| = 8$, then its center is $\langle 2^{12} \rangle$ and $G \subseteq N_{M_{24}}(2^{12})$.

If $|K| = 4$ and $K = C_4$, then again $G \subseteq N_{M_{24}}(2^{12})$.

If $|K| = 4$ and $K = c_2 \times c_2$, let X_i , $i = 1, 2, 3$, be three nonidentity elements. Let $X_i = 1^{828}$ and the eight points left fixed by X_i be Γ_i . Then $\Gamma_i \cap \Gamma_j = \emptyset$ and Γ_i form blocks of length 8 and $G \subseteq G_{[8 \cdot 1]^3}$.

If $K \cong S_4$, then we have $(1^2)^6 (2)^6$ which is impossible in M_{24} .

If $K \cong V_4$ or A_4 , then $K \approx V_4 | V_4 | V_4 | V_4 | V_4 | V_4$ or $A_4 | A_4 | A_4 | A_4 | A_4 | A_4$. Since G^* is at least doubly transitive, 5 divides the order of G . Let $\sigma^5 = 1$, then σ is of type

$1^4 5^4$. σ normalizes K and thus centralizes it. Therefore $K \subset C_{M_{24}}(1^4 5^4)$. Since $C_{M_{24}}(5^4 1^4) = C_5 \times A_4$, $K \cong A_4$ (or V_4) in the centralizer of $1^4 5^4$. And the systems of imprimitivity of G coincide with the six orbits of A_4 (or V_4). By Lemma 6.3.1, $C_{M_{24}}(1^4 5^4) = A_4 \times C_5 \subset G_{(4)}^*$ and the systems of imprimitivity of G coincide with the systems of imprimitivity of $G_{(4)}^*$. Since $G_{(4)}^*$ is the biggest imprimitive group with this system of imprimitivity, $G \subset G_{(4)}^*$.

We conclude the discussion of groups of type 4^6 with the following inclusion relationships.

PROPOSITION 6.4. $G_{(4)}^*$ contains: (1) $G_{(4)}$, (2) $G_{(6^{**})}$, (3) $N_{M_{24}}(2^{12})$, (4) $N_{M_{24}}(G_{(12^{**})})$, (5) $N_{M_{24}}(G_{(12^v)})$.

Proof. (1) by the construction of $G_{(4)}^*$.

(2) The kernel of the imprimitive group $G_{(4)}^*$ has order $2^6 \cdot 3$. Syl₃ of the kernel must have type $1^6 3^6$ and the six blocks must have form

$$(\cdot)(\cdot\cdot\cdot)(\cdot)(\cdot\cdot\cdot)(\cdot)(\cdot\cdot\cdot)(\cdot)(\cdot\cdot\cdot)(\cdot)(\cdot\cdot\cdot)(\cdot)(\cdot\cdot\cdot).$$

Since the normalizer of $1^6 3^6$ in M_{24} mod $\langle 1^6 3^6 \rangle$ is S_6 , the normalizer of $\langle 1^6 3^6 \rangle$ in the kernel of $G_{(4)}^*$ is $\langle 1^6 3^6 \rangle$. Therefore $2^6 \cdot 2 = 2^7$ elements of type $1^6 3^6$ are in the kernel. Thus $C_{G_{(4)}^*}(1^6 3^6)$ has order $2^3 \cdot 3^3 \cdot 5$ which is the order of $C_{M_{24}}(1^6 3^6)$. Therefore $N_{M_{24}}(1^6 3^6) = G_{(6^{**})}$ is in $G_{(4)}^*$.

(3) By Lemma 6.3.1, we know $C_{M_{24}}(5^4 1^4)$ is in $G_{(4)}^*$. So $G_{(4)}^*$ has elements of order 10 type $10^2 2^2$. These elements have imprimitive image of type 51. The fifth powers of these elements have type 2^{12} and they must be in the kernel. Since $K_1 \cap K_2 \neq E$ where K_i denotes the kernel of the kernel of $G_{(4)}^*$ on B_i , there are elements of type $1^8 2^8$ in the kernel. Since $|C_{M_{24}}(1^8 2^8)| = 2^{10} \cdot 3 \cdot 7$, there must be at least 45 elements of type $1^8 2^8$ in the kernel and since $|C_{M_{24}}(2^{12})| = 2^9 \cdot 3 \cdot 5$, there must be at least 18 elements of type 2^{12} in the kernel. Since syl₂ of the kernel is normal in the kernel of $G_{(4)}^*$, we have 63 elements of 2-power order. Thus,

$$63 = (45 + x) + (18 + y), \quad x = y = 0.$$

Thus $|N_{G_{(4)}^*}(2^{12})| = 2^9 \cdot 3 \cdot 5 = |N_{M_{24}}(2^{12})|$ and $N_{M_{24}}(2^{12}) \subset G_{(4)}^*$.

(4) Consider $B_1 \cup B_2 \cup B_3$. Since 12^I contains an 8^I it is either 12^{**} or 12^{iv} . Since $G_{(12^{iv})}$ is intransitive on 12^{iv} , $B_1 \cup B_2 \cup B_3$ must be a 12^{**} . $G_{(4)}^* 12^{**}$ has order $2^6 3 \cdot |S_3| \cdot |S_3| = 2^8 \cdot 3^3$ which is the order of $G_{(12^{**})}$. Therefore $N_{M_{24}}(G_{(12^{**})})$ is also in $G_{(4)}^*$.

(5) By [3, Proposition 8.2 (E)], $G_{(12^v)}$ on 12^v is an imprimitive group of degree 12, order 240. The kernel has order 2 and the image is \bar{S}_5 (in S_6).

Let $\tau_L = (ab)(cd)(ef)(gh)(ij)(kl)$ and let $\langle \tau_L \rangle$ be the kernel of the imprimitivity. By [3, Proposition 8.3], $G_{(12^v)}$ on $(12^v)^c$ has a similar representation. Let $\tau_R = (\alpha\beta)(\gamma\delta)(\epsilon\zeta)(\eta\theta)(\iota\kappa)(\lambda\mu)$ and let $\langle \tau_R \rangle$ be the kernel of the imprimitivity of $G_{(12^v)}$ on $(12^v)^c$. Let $G_{(12^v)}^{12^v}$ be denoted by $G_{(12^v)_L}$ and $G_{(12^v)}^{(12^v)^c}$ by $G_{(12^v)_R}$. Then

$$\langle \tau_L \rangle = Z(G_{(12^v)_L}) \quad \text{and} \quad \langle \tau_R \rangle = Z(G_{(12^v)_R}).$$

Now consider an element τ in $G_{(12^v)}$.

$$\tau = \tau_L(\cdot\cdot)(\cdot\cdot)(\cdot\cdot)(\cdot\cdot)(\cdot\cdot)(\cdot\cdot).$$

R

The action of τ on $(12^v)^c$ is of type 2^8 since $12^v (\approx (12^v)^c)$ does not contain an $8'$.

Under the conjugation by $G_{(12^v)}$, τ_L remains invariant, and also, since no non-identity element of M_{24} can fix more than 8 points, R remains invariant, so $R \in Z(G_{(12^v)_R})$, and $R = \tau_R$. Therefore $\tau = \tau_L \cdot \tau_R$ and we have

$$G_{(12^v)} \subset C_{M_{24}}(\langle \tau \rangle).$$

Therefore $\langle \tau \rangle = Z(G_{(12^v)})$ is a characteristic subgroup of $G_{(12^v)}$, and $G_{(12^v)} \triangleleft N_{M_{24}}(G_{(12^v)})$. Thus $\langle \tau \rangle \triangleleft N_{M_{24}}(G_{(12^v)})$ and $N_{M_{24}}(G_{(12^v)}) \subset N_{M_{24}}(\langle \tau \rangle)$, where τ is 2^{12} type. The assertion follows from $N_{M_{24}}(2^{12}) \subset G_{(4)}^*$.

7. Groups of type 3^8 . Let G be a group of type 3^8 with a primitive G^* . Since 5, 7, 11, 23 cannot divide the order of K , $|K| = 2^\alpha \cdot 3^\beta$. The discussion will be divided into three cases: (a) 3 divides $|K|$; (b) 3 does not divide $|K|$; (c) $K = E$.

For cases (a) and (b) we have

PROPOSITION 7.1. *Let G be a group of type 3^8 with nontrivial kernel, then $K = \langle 3^8 \rangle$ and $G \subset G_{[8]}^3$.*

Proof. (1) Let σ be an element of type 3^8 and let $\sigma \in K$. Since no element in M_{24} can fix more than 8 points, $\text{syl}_3(K) = \langle \sigma \rangle$. Furthermore, $\langle \sigma \rangle \triangleleft K$ and K has no other elements of type 3^8 other than σ and σ^2 . So $\langle \sigma \rangle \triangleleft G$ and $G \subset N_{M_{24}}(3^8)$. By Proposition 4.4, $G \subset N_{M_{24}}(3^8) \subset G_{[8]}^3$.

(2) Suppose $\text{syl}_3(K)$ does not contain elements of type 3^8 but contains elements of type $1^6 3^6$. Since G^* is primitive in S_8 , G^* is at least doubly transitive on B_i , $i = 1, \dots, 8$. Therefore K contains at least 4 distinct elements of type $1^6 3^6$, and K cannot contain elements of type 3^8 , so $|\text{syl}_3(K)|$ cannot be 3^3 but 3^2 . We have seen, in Lemma 4.4.1, that any subgroup of order 3^2 has an orbit of length 9. Therefore (2) does not occur.

(b) 3 does not divide $|K|$ and $|K| = 2^\alpha$.

In this case, orbits of K on any block of imprimitivity have length 2 and 1, and $|K| = 2$, otherwise $3 \mid |K|$. Since orbits of K form systems of imprimitivity of shorter lengths, the case (b) is impossible.

For the case $K = E$, we need the following:

LEMMA 7.2.1. *Every imprimitive group G that admits only the identity as the kernel of imprimitivity is insolvable.*

Proof. G^* is primitive. If G is solvable then G^* is solvable primitive. G^* must be of degree p^α for some prime p , and it contains as a minimal normal subgroup an elementary abelian group L of order p^α . To L , there corresponds a normal subgroup of G . Since L is regular and of degree p^α , it follows that this subgroup is intransitive. Hence G contains a kernel that differs from E .

By the above lemma, G^* can be any of the following five insolvable primitive groups of degree 8, viz., S_8 , A_8 , the holomorph of \mathfrak{A}_{2^3} , $\text{PGL}_2(7)$ and $\text{PSL}_2(7)$.

A_8 contains elements of type $3^1 5^1$. Elements of order 15 in M_{24} have type $15\ 5\ 3\ 1$. These elements cannot permute the 8 blocks in the fashion of $3^1 5^1$. Thus M_{24} cannot contain $G^* = A_8$. Accordingly M_{24} cannot contain $G^* = S_8$.

The holomorph of \mathfrak{A}_{2^3} contains elements of type $1^4 2^2$. On the 4 blocks left fixed, we have $1^4 2^4$, $1^6 3^2$ or 3^4 . The remaining parts of these elements, namely $1^4 2^4$, 3^4 and 3^4 , cannot permute the remaining 4 blocks in the fashion of 2^2 .

$\text{PGL}_2(7)$ contains elements of type 8. Only elements of type 8^3 or 24 in S_{24} would permute the 8 blocks in this fashion. But 8^3 or 24 are not in M_{24} .

Thus if G of type 3^8 with trivial kernel exists, it must be a $\text{PSL}_2(7)$ of degree 24. For this group we have

PROPOSITION 7.2. *In M_{24} , we have a $\text{PSL}_2(7)$ of degree 24, which acts as a group of type 3^8 with trivial kernel. All such $\text{PSL}_2(7)$ are conjugate in M_{24} . Furthermore, $\text{PSL}_2(7) \not\subseteq G_{[8]}^3$.*

Proof. By Carmichael [2, p. 164] we have $M_{24} = \langle A, B, C \rangle$ where

$$A = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22\ 23)(24),$$

$$B = (3\ 17\ 10\ 7\ 9)(5\ 4\ 13\ 14\ 19)(11\ 12\ 23\ 8\ 18)(21\ 16\ 15\ 20\ 22)(1)(2)(6)(24),$$

$$C = (1\ 24)(2\ 23)(3\ 12)(4\ 16)(5\ 18)(6\ 10)(7\ 20)(8\ 14)(9\ 21)(11\ 17)(13\ 22)(19\ 15).$$

Let $D = C^{(A^2 B)^{11}}$, $E = AC^{(1)}$. Then

$$D = (23\ 24)(1\ 22)(16\ 21)(11\ 7)(13\ 15)(14\ 18)(19\ 5)(12\ 4)(20\ 9)(3\ 2)(17\ 10)(8\ 6),$$

$$E = (1\ 23\ 24)(2\ 12\ 22)(3\ 16\ 11)(4\ 18\ 15)(5\ 10\ 17)(6\ 20\ 9)(7\ 14\ 19)(8\ 21\ 13).$$

Then

$$D \cdot E = (1\ 2\ 16\ 13\ 4\ 22\ 23)(3\ 12\ 18\ 19\ 10\ 5\ 7)(6\ 21\ 11\ 14\ 15\ 8\ 20)(9)(17)(24).$$

Let $G = \langle D, E \rangle$, then G is a $(2\ 3\ 7)$ group, i.e. a group generated by two generators of order 2 and 3 respectively, and whose product has order 7. Let

$$B_1 = \{9, 17, 24\}, \quad B_2 = \{20, 10, 23\}, \quad B_3 = \{8, 19, 22\},$$

$$B_4 = \{4, 15, 18\}, \quad B_5 = \{14, 12, 13\}, \quad B_6 = \{11, 3, 16\},$$

$$B_7 = \{21, 7, 2\}, \quad B_8 = \{6, 5, 1\}.$$

Now G is seen to be an imprimitive group with systems of imprimitivity B_1, \dots, B_8 and

$$D^* = (B_1 B_2)(B_3 B_8)(B_4 B_5)(B_6 B_7),$$

$$E^* = (B_1 B_8 B_2)(B_3 B_7 B_5)(B_4)(B_6),$$

$$D^* E^* = (B_8 B_7 B_6 B_5 B_4 B_3 B_2)(B_1).$$

(¹) The above generators of $\text{PSL}_2(7)$ in M_{24} were obtained by Rudi List, following the suggestion by D. Livingstone of the existence of $\text{PSL}_2(7)$ in M_{24} .

Thus we have $G^* = \langle D^*, E^* \rangle$ is the $\text{PSL}_2(7)$ in S_8 .

If the kernel of the imprimitivity is not identity, then by Proposition 7.1, the kernel must be $\langle 3^8 \rangle$, and $G \subset N_{M_{24}}(3^8)$. Then by Proposition 4.4, $G \subset G_{[8]}^3$. $G_{[8]}^3$ has a normal subgroup N and $G_{[8]}^3/N \cong S_3$. N has orbits of length 8, thus there can be no elements of type 3^8 in N . Thus E in the above cannot be in N . Suppose D is in N . Then $D \cdot E$ of order 7 is not in N . But $G_{[8]}^3/N \cong S_3$ cannot contain an element of order 7. Suppose D is also not in N . Then S_3 must contain a $(2, 3, 7)$ group which is impossible. Thus the kernel of imprimitivity is the identity alone, and also $G \not\subset G_{[8]}^3$.

A computation shows that $\Lambda_{2^{12}, 3^8, 7^3, 1^3} = 2 \cdot 3 \cdot 7 = |C_{M_{24}}(7^3 1^3)|$. Thus any element of type $7^3 1^3$ in M_{24} can be expressed as products of elements of types 2^{12} and 3^8 exactly 42 times. Thus $a \cdot b = \alpha \cdot \beta = 7^3 1^3$ with a and α of type 2^{12} and b and β of type 3^8 if and only if $\alpha = a^\xi$ and $\beta = b^\xi$, $\xi \in C_{M_{24}}(7^3 1^3)$. Exactly the same argument as in Proposition 1.1 gives that all $\text{PSL}_2(7)$ are conjugate in M_{24} .

8. Groups of type 2^{12} . Let G be an imprimitive group with systems of length 2. Since 3, 5, 7, 11, 23 do not divide $|K|$, $|K| = 2^\alpha$. The discussion will be divided into three cases: (a) $K \neq E$ and $2^{12} \in K$; (b) $K \neq E$ and $2^{12} \notin K$; (c) $K = E$. We have the following:

PROPOSITION 8.1. *Let G be a group of type 2^{12} . If the kernel contains an element of type 2^{12} , then $G \subseteq G_{(4)}^*$. If the kernel contains an element of $1^8 2^8$, then $G \subseteq G_{[8]}^3$. If the kernel is trivial, then G is of type 12^2 .*

Proof. (a) Suppose $2^{12} \in K$. Then K cannot contain any other element except 1. Therefore $K = \langle 2^{12} \rangle$ and $G \subset G_{(4)}^*$ by Proposition 6.4.

(b) Suppose $2^{12} \notin K$ and $1^8 2^8 \in K$. Since all the elements in K are of type $1^8 2^8$ and no element can fix more than 8 points, $|K| = 2^2$. The 8 points left fixed by each element form systems of imprimitivity of length 8, and if G exists, then $G \subseteq G_{[8]}^3$.

(c) $K = E$. We assume that G^* is a primitive group of degree 12. There are six primitive groups of degree 12 [7, p. 130]. They are (1) S_{12} and A_{12} ; (2) $\text{PSL}_2(11)$ and $\text{PGL}_2(11)$; (3) M_{11} and M_{12} .

(1) S_{12} and A_{12} . Since neither $|S_{12}|$ nor $|A_{12}|$ divides M_{24} , G^* cannot be S_{12} or A_{12} .

(2) $\text{PSL}_2(11)$ and $\text{PGL}_2(11)$. 24 does not divide $|\text{PSL}_2(11)|$, so $\text{PSL}_2(11)$ cannot be transitive on the 24 points, so G^* cannot be $\text{PSL}_2(11)$. $\text{PSL}_2(11)$ is transitive on 12 points, therefore $\text{PGL}_2(11)$ has systems of imprimitivity of length 12. Thus if G exists, G is of type 12^2 .

(3) M_{11} and M_{12} . M_{11} has elements of type 84 as a group of degree 12. On the 8 blocks we have 8^2 and on the 4 blocks we have 8 or 4^2 . We have no element in M_{24} which accommodates these types. So $G^* \neq M_{11}$. Accordingly $G^* \neq M_{12}$ since $M_{11} \subset M_{12}$.

9. The maximal subgroups of M_{24} .

THEOREM II. M_{24} contains 9 conjugate classes of maximal subgroups, namely

Subgroup	Order	Described in Proposition(s)
$\text{PSL}_2(23)$, primitive	$2^3 \cdot 3 \cdot 11 \cdot 23$	1.1
$N_{M_{24}}(M_{12})$, imprimitive	$2^7 \cdot 3^3 \cdot 5 \cdot 11$	3.1
$G_{[8]^3}$, imprimitive	$2^{10} \cdot 3^2 \cdot 7$	4.2
$G_{(4)}^*$, imprimitive	$2^{10} \cdot 3^3 \cdot 5$	6.1
$\text{PSL}_2(7)$, imprimitive	$2^3 \cdot 3 \cdot 7$	7.2
M_{23} , intransitive	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	[3, 2.0]
$N_{M_{24}}(M_{22})$, intransitive	$2^8 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	[3, 2.0]
$N_{M_{24}}(M_{21})$, intransitive	$2^7 \cdot 3^3 \cdot 5 \cdot 7$	[3, 2.0]
$G_{(8^{\cdot})}$, intransitive	$2^{10} \cdot 3^2 \cdot 5 \cdot 7$	[3, 2.3]

Proof. By Propositions 3.1 through 8.1, the imprimitive subgroups of M_{24} which are not contained in other imprimitive subgroups are $N_{M_{24}}(G_{(12^{\cdot})})$, $G_{[8]^3}$, $G_{(4)}^*$, and $\text{PSL}_2(7)$. Thus the transitive maximal subgroups of M_{24} are to be found among the five subgroups, namely, the above four imprimitive subgroups and the unique proper primitive subgroup, $\text{PSL}_2(23)$, discussed in Proposition 1.1. The simple comparison of orders among themselves reveals that, except for $\text{PSL}_2(7)$, all the others are transitive maximal subgroups. By mere comparison of orders, $\text{PSL}_2(7) \subset G_{[8]^3}$ is possible, but Proposition 7.2 shows that this is not the case, thus $\text{PSL}_2(7)$ is a maximal as well.

We have seen that $G_{(12^i)}$, $i=1, 2, 5$, are in $N_{M_{24}}(G_{(12^{\cdot})})$ respectively by Proposition 3.1, and Proposition 6.4 shows that $G_{(4)}$ and $G_{(6^{\cdot})}$ are in $G_{(4)}^*$. Thus out of 9 maximal subgroups among the intransitives enumerated in [3, Theorem I], we have only four to consider. They are $G_{(1)}$, $G_{(2)}$, $G_{(3)}$ and $G_{(8^{\cdot})}$. The first three are shown to be maximal by [3, Propositions 2.1 and 2.2]. $G_{(8^{\cdot})}$ is a maximal subgroup since there is no transitive maximal subgroup which contains it as seen by comparison of orders of the subgroups.

ACKNOWLEDGEMENT. The author is deeply indebted to Professor Donald Livingstone for his help and encouragement throughout the research and writing of this paper.

REFERENCES

1. W. S. Burnside, *Theory of groups of finite order*, 2nd ed., 1911; reprint, Dover, New York, 1955. MR 16, 1086.
2. R. D. Carmichael, *Introduction to the theory of groups of finite order*, Ginn, Boston, Mass., 1937.
3. Chang Choi, *On subgroups of M_{24} . I: Stabilizers of subsets*, Trans. Amer. Math. Soc. **167** (1972), 1–27.
4. B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der math. Wissenschaften, Band 134, Springer-Verlag, Berlin and New York, 1967. MR 37 #302.

5. C. Jordan, *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris, 1870.
6. D. E. Littlewood, *The theory of group characters and matrix representations of groups*, Oxford Univ. Press, New York, 1940. MR 2, 3.
7. G. A. Miller, *Collected works*. Vol. I, Univ. of Illinois Press, Urbana, Ill., 1935.
8. H. Wielandt, *Finite permutation groups*, Lectures, University of Tübingen, 1954/55; English transl., Academic Press, New York, 1964. MR 32 #1252.
9. E. Witt, *Die 5-fach transitiven Gruppen von Mathieu*, Abh. Math. Sem. Univ. Hamburg 12 (1937), 256–264.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF NOTRE DAME, NOTRE DAME, INDIANA 46556

Current address: Department of Mathematics, Indiana University at South Bend, South Bend, Indiana 46615