Math. Proc. Camb. Phil. Soc. (1976), 79, 25
With 5 text-figures
MPCPS 79-4
Printed in Great Britain

A new combinatorial approach to M_{24}

BY R. T. CURTIS
Department of Pure Mathematics and Statistics, Cambridge

(*Received* 15 *June* 1974)

In this paper, we define M_{24} from scratch as the subgroup of S_{24} preserving a Steiner system $S(5, 8, 24)$. The Steiner system is produced and proved to be unique and the group emerges naturally with many of its properties apparent.

All nine maximal subgroups of M_{24} are introduced and described.

It is hoped that the reader will appreciate the advantages of the techniques developed here, and through them will acquire a greater familiarity with the workings of this amazing group.

In the latter part of the paper some tabular information about the group is collected together. J. H. Conway has kindly given permission for his table of subsets of Ω to be included and J. A. Todd has allowed me to add the character table of M_{24} from his elegant paper (3).

It is intended to follow this paper with a new, short proof, using terminology introduced here, that the list of nine maximal subgroups is complete.

The Steiner System $S(5, 8, 24)$.

Definition. A Steiner System $S(5, 8, 24)$ is a collection of 8-element subsets of a 24-element set, Ω, with the property that any five of the twenty-four lie in just one of them.

We observe that, if such a system exists, then there are $\binom{24}{5}\Big/\binom{8}{5} = 759$ of these 8-element sets or octads.

THEOREM A. *There exists a Steiner System* $S(5, 8, 24)$.

Method of Proof. We shall consider the power set of Ω, $P(\Omega)$, as a 24-dimensional vector space over the field with two elements GF_2 where the sum of two sets is defined to be their symmetric difference. We shall produce a subspace, $\mathscr{C}$, of $P(\Omega)$ whose smallest members are subsets of size eight and shall show, moreover, that $\mathscr{C}$ contains just 759 of these 'octads'. Clearly no two octads can have five points in common as their sum would then have six points or less in it. Thus these octads must form a Steiner System $S(5, 8, 24)$.

Proof. Let Λ be an 8-element set and consider *any* two 3-dimensional subspaces of $P(\Lambda)$ whose members are all tetrads (i.e. 4-element subsets) and whose intersection is the empty subset.

For instance:

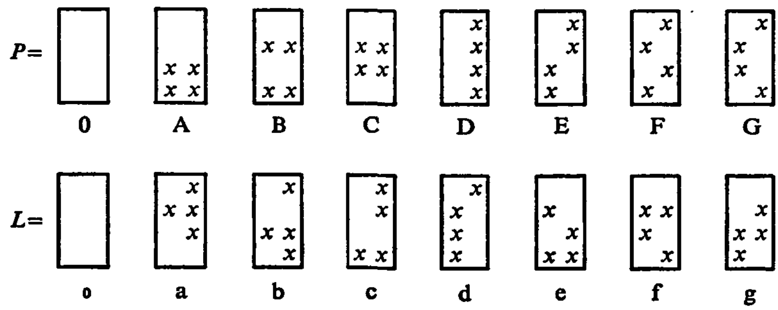
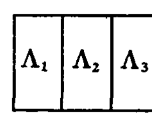


Fig. 1

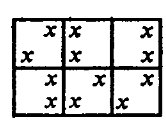
We notice that any member of L, say, defines a unique 2-dimensional subspace or *line* of P; namely the set of members of P that it cuts evenly (i.e. 2·2). Thus the members of L are in one-to-one correspondence with the lines of P. We shall call P the point-space and L the line-space and use the notation $A \in c$, $B \notin e$ to mean that A is on the line associated with c and B is not on the line associated with e. Notice that if $X \in P$ and $t \in L$ then $X \in t \Rightarrow |X+t| = 4$, $X \notin t \Rightarrow |X+t| = 2$ or 6. The correspondence is shown in Fig. 2.

By consideration of dimension, we see that any *even* subset of Λ can be written uniquely as $X+t$ or $X'+t$, where $X \in P$, $t \in L$ and $X'+X = \Lambda$.

We now take three copies of Λ and define the space $\mathscr{C}$ (of $\mathscr{C}$-sets) to consist of all sets of the form:

$$\underset{\text{in } \Lambda_1}{(X \text{ or } X')+t} \quad \underset{\text{in } \Lambda_2}{(Y \text{ or } Y')+t} \quad \underset{\text{in } \Lambda_3}{(Z \text{ or } Z')+t} \qquad \text{for}$$  ,

where $X+Y+Z = 0$. $\mathscr{C}$ is plainly 12-dimensional. A typical $\mathscr{C}$-set can be named for instance

$[AB'C]_d$ denotes $[A+d, B'+d, C+d] \equiv$  .

We now investigate the sizes of the $\mathscr{C}$-sets.

Name (modulo complementation in Λ_i)	Description	Intersection with Λ_1	Λ_2	Λ_3
$[0\ 0\ 0]_0$	—	0/8	0/8	0/8
$[X\ X\ 0]_0$	$X \neq 0$	4/4	4/4	0/8
$[X\ Y\ Z]_0$	X, Y, Z distinct	4/4	4/4	4/4
$[0\ 0\ 0]_t$	$t \neq 0$	4/4	4/4	4/4
$[X\ X\ 0]_t$	$0 \neq X \notin t \neq 0$	2/6	2/6	4/4
$[X\ X\ 0]_t$	$0 \neq X \in t \neq 0$	4/4	4/4	4/4
$[X\ Y\ Z]_t$	$\{X, Y, Z\} = t \neq 0$	4/4	4/4	4/4
$[X\ Y\ Z]_t$	$\{X, Y, Z\} \cap t = \{X\}$	4/4	2/6	2/6

In each case $X+Y+Z = 0$ and m/n means m or n. We see that the smallest $\mathscr{C}$-sets $(\neq 0)$ are of size 8.

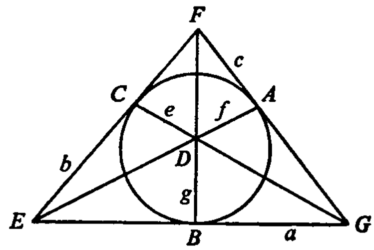


Fig. 2

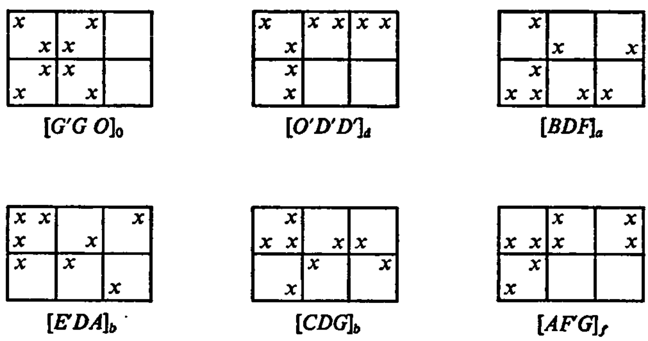


Fig. 3

We count the octads. Let us call the set of octads $\mathscr{C}_8$.

3	of shape	$[0\ \ 0\ \ 0]_0$	
$7.3.2.2 = 84$	of shape	$[X\ \ X\ \ 0]_0$	
$7.4.3.2 = 168$	of shape	$[X\ \ X\ \ 0]_t$	
$7.3.3.2.2.2 = 504$	of shape	$[X\ \ Y\ \ Z]_t$	*Total* 759

This completes the proof of Theorem A.

In fact the construction enables us to describe the octads in a very revealing manner. It shows that each octad, other than $\Lambda_1, \Lambda_2, \Lambda_3$, intersects at least one of these 'bricks' – the 'heavy brick' – in just four points. In Fig. 3 we draw a number of octads for which Λ_1 is a heavy brick, so that each is made of a 'brick tetrad' in the brick Λ_1, and a 'square tetrad' in the square $\Lambda_2 + \Lambda_3$. These prompt the following remarks.

The brick tetrad may be any one of the 70 tetrads in that brick. These fall into 35 groups of two, tetrads being grouped when their union is the brick.

The square tetrad, however, must be one of the 140 *special tetrads* that intersect all the rows of the square with the same parity, and all the columns of the square with the same parity. These fall into 35 groups of 4, tetrads being in the same group when their union is an octad.

There is a correspondence between the two systems of 35 groups, which is illustrated in Fig. 4 (the MOG or Miracle Octad Generator). This has 35 pictures which show against each complementary pair of brick tetrads, the corresponding group of special square tetrads. We obtain an octad by taking either of the brick tetrads together with any one of the square tetrads from the same picture. The reader should verify for himself how each of the tetrads in Fig. 3 arises from one of the MOG pictures.

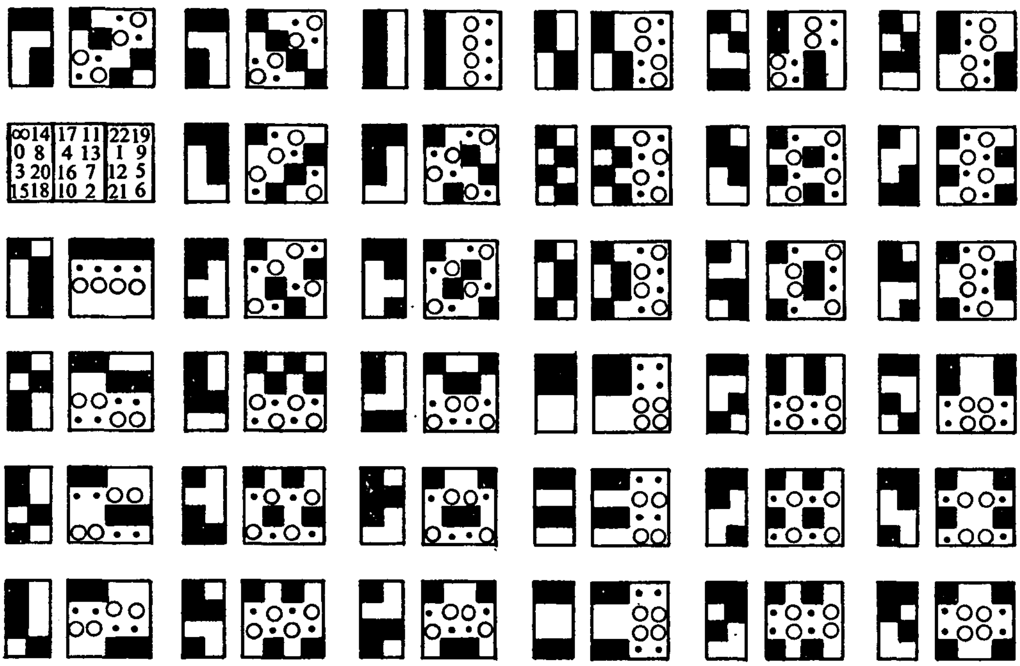


Fig. 4. (The MOG.)

Now the MOG diagram has all the 6 symmetries bodily permuting $\Lambda_1, \Lambda_2, \Lambda_3$ so we can take any one of these as a heavy brick, and the other two (in any order) as the square, when the above description will cover any octad other than one of the Λ_i, since this octad will have at least one heavy brick.

Note that the MOG has a 36th picture which gives names $\infty, 0, 1, \ldots, 22$ for the 24 points of Ω. These names will be explained later.

Example. Find the octad which contains the points $22, 1, 12, 6, 8$. Since this has the four points $(22, 1, 12, 6)$ in the brick Λ_3, and one point (8) in $\Lambda_1 + \Lambda_2$ we look for that MOG pattern which has

x	
x	
x	
	x

as brick tetrad, finding it to be bottom left. Here we see that the corresponding square tetrad (in the square $\Lambda_1 + \Lambda_2$) which contains the point (8) is $(0, 8, 16, 7)$ and so the required octad is

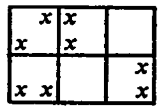
				x	
x	x			x	
		x	x	x	
					x

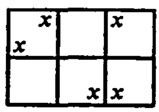
$= (0, 8, 16, 7, 22, 1, 12, 6)$.

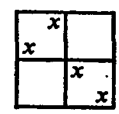
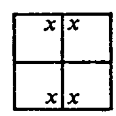
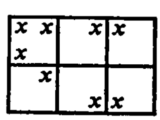
Example. Find the octad containing the points $0, 15, 18, 5, 6$.

x					
					x
x	x				x

Here Λ_1 must be a heavy brick with brick tetrad containing $0, 15, 18$. We examine the five pictures in which $0, 15, 18$ belong to the same brick tetrad and find that in the top right hand corner picture 5 and 6 belong to the same special tetrad 5, 6, 4, 17. The octad is therefore

 $= (0, 15, 14, 18, 17, 4, 5, 6)$.

Example. Find the octad containing the five points 0, 14, 2, 22, 21. In the MOG these appear as  and so the heavy brick must be Λ_1 or Λ_3 since the tetrad 0, 14, 22, 21 is not special.

If Λ_3 is the brick the corresponding square tetrad in $\Lambda_1 + \Lambda_2$ is  shown in the MOG by the top left hand picture where we observe that 5 and 6 do not lie in the same brick tetrad. Thus Λ_1 must be the brick,  must be the square tetrad in $\Lambda_2 + \Lambda_3$ and from the bottom right hand picture of the MOG we see that the required octad is  $= (\infty, 0, 14, 20, 11, 22, 2, 21)$.

With a small amount of practice this process takes a matter of seconds.

Having produced a particular $S(5, 8, 24)$, we return momentarily to the general case. We have remarked that there are $\binom{24}{5} \Big/ \binom{8}{5} = 759$ octads. Similarly it is clear that there are $\binom{23}{4} \Big/ \binom{7}{4} = 253$ octads containing a given point and $\binom{22}{3} \Big/ \binom{6}{3} = 77$ octads containing a given two points. Thus there are $253 - 77 = 176$ octads containing a chosen one point of a given pair but not the other. In this way, letting

$$S_8 \equiv \{a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8\}$$

be an octad and $S_j \equiv \{a_1 a_2 \dots a_j\}$ $(j < 8)$, we get the following table due to Leech:

759								
506	253							
330	176	77						
210	120	56	21					
130	80	40	16	5				
78	52	28	12	4	1			
46	32	20	8	4	0	1		
30	16	16	4	4	0	0	1	
30	0	16	0	4	0	0	0	1

Fig. 5

where the $j+1$th entry in the $i+1$th line is the number of octads intersecting S_i in S_j. In particular the bottom line shows that any two octads intersect in 0, 2, 4 or 8 points.

LEMMA 1 (*Todd*). *If* $S, T \in \mathscr{C}_8$ *and* $|S \cap T| = 4 \Rightarrow S + T \in \mathscr{C}_8$.

Proof. Let $S = \{a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8\}$ and $T = \{a_1 a_2 a_3 a_4 b_5 b_6 b_7 b_8\}$ be two octads and consider the octad containing the five points $a_5 a_6 a_7 a_8 b_5$ which we suppose not to be $S+T$. This can contain no further point of S without being S and, since it only contains one point of T, it must contain a further b, say b_6. Similarly the octad defined by the points $a_5 a_6 a_7 a_8 b_7$ may be assumed to contain b_8. But now the octad defined by $a_5 a_6 a_7 b_5 b_7$ must contain a further point of S which cannot be a_8 and so may be taken to be a_1. It must now contain a further point of T which may not be an a (or we should have five a's) but whether we add b_6 or b_8 we find we have five points of a previous octad. So our original assumption was false and $S+T$ is an octad.

COROLLARY. *Corresponding to each* 4 *points of* Ω *there is a partition of the* 24 *points into* 6 *tetrads with the property that the union of any two tetrads is an octad. Such a configuration will be called a sextet.*

Now let $Y = Y_1 \cup Y_2 \cup \ldots \cup Y_s$ be a decomposition of Y into disjoint sets Y_i. A subset X will be said to cut this decomposition $r_1 . r_2 \ldots r_s$ if X has exactly r_i points in Y_i $(|X| = r_1 + r_2 + \ldots + r_s)$.

LEMMA 2. *An octad cuts the* 6 *tetrads of a sextet* $4^2 . 0^4$, $3 . 1^5$ *or* $2^4 . 0^2$.

Proof. This follows immediately from the definition of a sextet and the fact that any two octads intersect in 0, 2, 4 or 8 points.

LEMMA 3. *The intersection matrix for the tetrads of two sextets is one of the following*:

$$(1)\ \begin{pmatrix} 4&0&0&0&0&0\\ 0&4&0&0&0&0\\ 0&0&4&0&0&0\\ 0&0&0&4&0&0\\ 0&0&0&0&4&0\\ 0&0&0&0&0&4 \end{pmatrix} \qquad (2)\ \begin{pmatrix} 2&2&0&0&0&0\\ 2&2&0&0&0&0\\ 0&0&2&2&0&0\\ 0&0&2&2&0&0\\ 0&0&0&0&2&2\\ 0&0&0&0&2&2 \end{pmatrix}$$

$$(3)\ \begin{pmatrix} 2&0&0&0&1&1\\ 0&2&0&0&1&1\\ 0&0&2&0&1&1\\ 0&0&0&2&1&1\\ 1&1&1&1&0&0\\ 1&1&1&1&0&0 \end{pmatrix} \qquad (4)\ \begin{pmatrix} 3&1&0&0&0&0\\ 1&3&0&0&0&0\\ 0&0&1&1&1&1\\ 0&0&1&1&1&1\\ 0&0&1&1&1&1\\ 0&0&1&1&1&1 \end{pmatrix}$$

Proof. An easy corollary to Lemma 2.

We are now in a position to prove the following theorem.

THEOREM B. *The Steiner System* $S(5, 8, 24)$ *is unique up to relabelling the points and the subgroup of* S_{24} *preserving the octads has order* 244, 823, 040 *and is quintuply transitive on the* 24 *points.*

Proof. Let $x_1, x_2, x_3, x_4, x_5, x_6$ be an ordered set of 6 points in an octad O_1 of the Steiner System $S(5, 8, 24)$ defined on the 24-point set Ω. Suppose that x_7 is a further point of Ω not in O_1. We shall show that the $S(5,8,24)$ may be assumed to be the one we have already seen and that the group of permutations of Ω preserving the system is sharply transitive on such ordered sets of 7 points and so has order

$$24.23.22.21.20.3.16.$$

Let the sextet defined by the tetrad x_1, x_2, x_3, x_4 be called S_∞, and let its tetrads be the columns of the 4×6 array:

$$S_\infty = \begin{array}{|cc|cc|cc|}\hline x_1 & x_5 & x_7 & & & \\ x_2 & x_6 & & & & \\ x_3 & & & & & \\ x_4 & & & & & \\ \hline\end{array} \quad \text{(where } O_1 \text{ consists of the first two columns).}$$

Now, using Lemmas 2 and 3 we shall obtain sufficient sextets to imply the $S(5,8,24)$.

The octad containing the five points x_2, x_3, x_4, x_5, x_7 must cut S_∞ 3.1^5 and so by re-arranging the un-named 17 points, if necessary, we may assume that

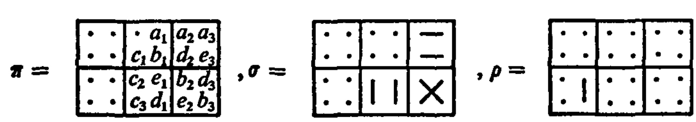
$$S_0 = \begin{array}{|cc|cc|cc|}\hline 0 & x & 1 & 1 & 1 & 1 \\ x & 0 & 2 & 2 & 2 & 2 \\ x & 0 & 3 & 3 & 3 & 3 \\ x & 0 & 4 & 4 & 4 & 4 \\ \hline\end{array} \quad \text{is a sextet.}$$

Remark. S_∞ and S_0 together imply that every symmetric difference of 2 rows with 2 columns in the right hand square, $\Omega + O_1$, is an octad. This gives $\frac{1}{2}.6.6 + 2.6 = 30$ octads disjoint from O_1 which we see from Fig. 5 to be all.

The octad containing x_1, x_3, x_4, x_5, x_7 cuts both S_∞ and S_0 3.1^5 and so by arranging the bottom 3 rows of $\Omega + O_1$, if necessary, and the above remark, we may assume that:

$$S_1 = \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 2 & 3 & 4 \\ 0 & 0 & 2 & 1 & 4 & 3 \\ x & 0 & 3 & 4 & 1 & 2 \\ x & 0 & 4 & 3 & 2 & 1 \\ \hline\end{array} \quad \text{is a sextet.}$$

At this stage, we note that the full group of rearrangements of the un-named 17 points which preserve the sextets S_∞, S_0 and S_1 is given by:



(where dots denote fixed points and π is a 3-element taking $y_1 \to y_2 \to y_3 \to y_1$ for $y = a, b, c, d$ or e).

Now the octad containing the points x_1, x_2, x_5, x_6, x_7 cuts S_∞ $2^4.0^2$ and so, using the element π, may be assumed to cut the first four columns of S_∞ 2^4. But it cuts S_0 $2^4.0^2$ also; so contains the top point of the fourth column. S_1 now implies that it is:

$$\begin{array}{|cc|cc|cc|}\hline x & x & x & x & & \\ x & x & x & x & & \\ \hline & & & & & \\ & & & & & \\ \hline\end{array}$$

Thus: $$S_2 = \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 1 & 2 & 2 \\ x & x & 1 & 1 & 2 & 2 \\ \hline 0 & 0 & 3 & 3 & 4 & 4 \\ 0 & 0 & 3 & 3 & 4 & 4 \\ \hline\end{array} \quad \text{is a sextet.}$$

Similarly the octad containing x_1, x_2, x_3, x_5, x_7 cannot contain points marked 0 in $\begin{array}{|cc|cc|cc|}\hline x & x & x & 0 & 0 & 0 \\ x & & 0 & 0 & & \\ \hline x & & 0 & & 0 & \\ x & & 0 & & & 0 \\ \hline\end{array}$ without having five points in a previous octad, and so it must be one of $\begin{array}{|cc|cc|cc|}\hline x & x & x & & & \\ x & & & & & x \\ \hline x & & & x & & \\ & & & & x & \\ \hline\end{array}$ or $\begin{array}{|cc|cc|cc|}\hline x & x & x & & & \\ x & & & & x & \\ \hline x & & & & & x \\ & & & x & & \\ \hline\end{array}$ (since it cuts each of S_∞, S_0 and S_1 3.1^5).

Under the action of the permutation σ, these are equivalent and so we may assume that:

$$S_3 = \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 2 & 3 & 4 \\ x & 0 & 3 & 4 & 1 & 2 \\ \hline x & 0 & 4 & 3 & 2 & 1 \\ 0 & 0 & 2 & 1 & 4 & 3 \\ \hline\end{array} \text{ is a sextet,}$$

when

$$S_4 = \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 2 & 3 & 4 \\ x & 0 & 4 & 3 & 2 & 1 \\ \hline & 0 & 2 & 1 & 4 & 3 \\ x & 0 & 3 & 4 & 1 & 2 \\ \hline\end{array} \text{ is forced to be.}$$

Finally consider the octad containing the points $\begin{array}{|cc|cc|cc|}\hline x & x & x & & & \\ & & & & & \\ \hline x & & x & & & \\ & & & & & \\ \hline\end{array}$ which must have one further point in the second column and points in the first and third rows of one of the last three columns (since it cuts both S_∞ and S_0 $2^4.0^2$). S_4 implies that these are $\begin{array}{|cc|cc|cc|}\hline x & x & x & x & & \\ & & & & & \\ \hline x & & x & x & & \\ & & & & & \\ \hline\end{array}$ and using ρ we take the octad to be $\begin{array}{|cc|cc|cc|}\hline x & x & x & x & & \\ & & & & & \\ \hline x & x & x & x & & \\ & & & & & \\ \hline\end{array}$

Thus:

$$S_5 = \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 1 & 3 & 3 \\ 0 & 0 & 2 & 2 & 4 & 4 \\ \hline x & x & 1 & 1 & 3 & 3 \\ 0 & 0 & 2 & 2 & 4 & 4 \\ \hline\end{array} \text{ is a sextet.}$$

Note that there is *no* permutation of the 17 un-named points fixing the sextets S_∞, S_0, S_1, S_2, S_3, S_4 and S_5.

Now whenever 2 of our sextets intersect evenly (i.e. a tetrad of one cuts the tetrads of the other $2^2.0^4$), we may take the symmetric difference of suitable octads in them to give a new octad and sextet. Thus:

$$\begin{array}{|cc|cc|cc|}\hline x & x & x & x & & \\ x & x & x & x & & \\ \hline & & & & & \\ & & & & & \\ \hline\end{array} + \begin{array}{|cc|cc|cc|}\hline x & x & x & x & & \\ & & & & & \\ \hline x & x & x & x & & \\ & & & & & \\ \hline\end{array} = \begin{array}{|cc|cc|cc|}\hline & & & & & \\ x & x & x & x & & \\ \hline x & x & x & x & & \\ & & & & & \\ \hline\end{array} \Rightarrow \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 1 & 3 & 3 \\ 0 & 0 & 2 & 2 & 4 & 4 \\ \hline 0 & 0 & 2 & 2 & 4 & 4 \\ x & x & 1 & 1 & 3 & 3 \\ \hline\end{array}$$

In this way we may soon verify that each of the 35 sextets defined by a partition of O_1 into 2 tetrads is as shown in the MOG.

LEMMA 4. *If every octad intersecting a given octad O in four points is known, then all octads follow by symmetric differencing.*

Proof. Let $x, y, z \in O$ (3 distinct points). Any octad containing x, y, z must contain a further point of O and so be a known octad. From Fig. 5 there exist 21 such. Now any two of these intersect in 4 points and so their symmetric difference is an octad disjoint from x, y, z. There are $\binom{21}{2} = 210$ of these which must all be distinct since, if $U + V = W + T$ where U, V, W and T are octads containing x, y, z, then 2 points of $U \backslash \{x, y, z\}$ are in W, say, i.e. U and W have 5 points in common. From Fig. 5, we see that these are *all* the octads disjoint from x, y, z. So we have *every* octad disjoint from *some* 3 points of O, i.e. every octad.

We have thus shown that the only $S(5, 8, 24)$ is that given by the MOG. Moreover if $y_1, y_2, y_3, y_4, y_5, y_6, y_7$ are 7 points of the same type as the x's then there is *just one* permutation of the 24 points which preserves the octads and takes $y_i \to x_i$ for each $i = 1-7$. This completes the proof of Theorem B.

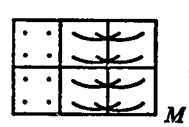
Let us call this quintuply transitive group M_{24} and its subgroup fixing k points M_{24-k} $(k < 5)$.

Now suppose that α is an element of order 23 in M_{24}; we number the points of Ω as the projective line $\infty, 0, 1, 2, \ldots, 22$ so that $\alpha: i \to i+1$ (modulo 23) and fixes ∞. In fact there is a full $L_2(23)$ acting on this line and preserving the octads as may be readily verified by applying the remaining generator $\gamma: i \to -1/i$ to the sextets

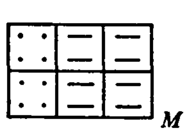
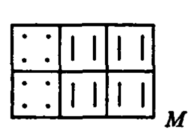
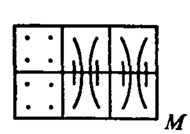
$$S_\infty, S_0, S_1, S_2, S_3, S_4, S_5$$

and checking that their images are indeed sextets. (Or more simply by verifying that γ is an involution of M_{24} – see page 36.) We shall call this group the Projective subgroup of M_{24}.

A class of involution. Since M_{24} is quintuply transitive on the points of Ω it is transitive on the octads. From Theorem B we see that the stabilizer of an octad must act as A_8 on the points of that octad (being exactly 6-tuply transitive on them) and so have shape $K . A_8$, where K is a group of order 16 fixing the octad pointwise.

One element of K which we have, in effect, already seen is the involution bodily interchanging the last 2 bricks of the MOG. viz.  , where dots denote fixed points. (Since there are other important 4×6 arrangements of the 24 points of Ω we shall in future add the subscript M to denote that we are meaning the MOG array.)

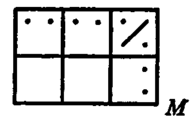
Moreover it is clear that the elements:

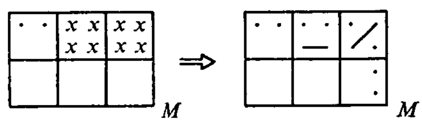
  

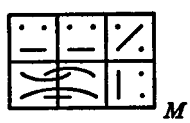
fix every sextet of the MOG and are thus in the group M_{24}.

But together these elements generate an elementary abelian group of order 16 and so constitute a copy of K.

Thus to every octad F and every 2 points i and j not in F there is a unique involution of M_{24} fixing every point of F and interchanging the 2 points i and j; let us call this element F_{ij}. We note that $F_{ij} = F_{kl} \Leftrightarrow \{i, j, k, l\}$ is a special tetrad of the 16-ad $F + \Omega$, i.e. if it is the intersection of an octad with $F + \Omega$. Thus using the MOG, it is an easy matter to construct the element F_{ij}.

Example. Find the F_{ij} involution having the action:  . We seek octads containing the two points $\{1, 19\}$ and four of $C = \{\infty, 14, 17, 11, 22, 9, 5, 6\}$; the remaining two points of this octad must form a transposition. Thus



and we soon arrive at 

[Note that the octad defined by $\{1, 19\}$ and any three of C must contain a fourth of C, and so the problem reduces to simple octad finding.]

The space $\mathscr{C}$.

So far we have seen only $\varnothing$, Ω, 759 octads and 759 16-ads in $\mathscr{C}$. Now

$$2^{12} = 4096 = 1 + 759 + 2576 + 759 + 1$$

and so there are just 2576 more $\mathscr{C}$-sets to be found.

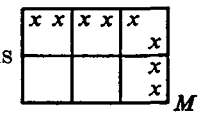
The sum of 2 octads which intersect in 2 points will have size 12 and will be called a *dodecad*. The total number of dodecads which occur in this way (with repetitions) is $759 . \binom{8}{2} . 16/2$ (using figure 5) and the *maximum* number of ways a dodecad may occur as the sum of 2 octads is when every 5 points of the dodecad belong to one octad of such a pair and is thus

$$(1/2) . \binom{12}{5} . (1/6) = 2.3.11.$$

Thus the *minimum* number of dodecads is $23 . \binom{8}{2} . 4 = 2576$. But we have seen this to be the *maximum* also. Thus the only $\mathscr{C}$-sets other than $\varnothing$, Ω, $\mathscr{C}_8$ and $\mathscr{C}_{16}$ are the dodecads $\mathscr{C}_{12}$. Further every 5 points of a dodecad determine a unique 6th point which together with the 5 form the intersection of some octad with the dodecad. Thus there is a Steiner system $S(5, 6, 12)$ defined on the points of a dodecad.

THEOREM C. *The space $\mathscr{C}$ consists of the empty set $\varnothing$, the whole set Ω, 759 octads, 2576 dodecads and 759 16-ads. M_{24} is transitive on each of these classes of subset and the proper subgroups of M_{24} arising as stabilizers of $\mathscr{C}$-sets are: $2^4 . A_8$ fixing an octad and its complementary 16-ad and M_{21} fixing a dodecad.*

Proof. It remains to prove transitivity on dodecads.

It suffices to show that the subgroup $2^4.S_6$ of the stabilizer of an octad F which fixes 2 points of that octad as a pair, is transitive on the 16 octads intersecting F in just those 2 points (see Fig. 5). As octad F we take the first brick of the MOG and, as fixed pair, the top 2 points of it. One of the 16 octads is  and we observe that no element of the 2^4 fixing every point of F fixes this octad. Thus the 2^4 is transitive on the 16 octads and the stabilizer of one of them is a group S_6 acting on the 6 points of F not in the special pair. We note in passing that the S_6 must also act on the points of the other octad that we fixed (by the symmetry of the situation) and that the 2 actions cannot be permutation identical since, if they were, it would be possible to produce a non-trivial element of M_{24} fixing 8 points of a dodecad. Plainly these 8 points cannot constitute an octad and so, by Theorem B, any such permutation must be the identity. Thus the 2 actions of S_6 must appear and it is, therefore, possible to fix a point of one 6 and remain transitive on the other 6. We have thus seen that the stabilizer of a dodecad is quintuply transitive on the 12 points of the dodecad and since its order is $|M_{24}|/2576 = 12.11.10.9.8$ it is sharply quintuply transitive.

We shall call this group M_{12}.

It is clear that the complement of a dodecad must itself be a dodecad – such a pair of complementary dodecads will be called a *duum*. The transitivity of M_{24} on dodecads implies that there is a permutation of M_{24} interchanging the 2 dodecads of a duum and so there is a subgroup $M_{12}.2$ in M_{24}.

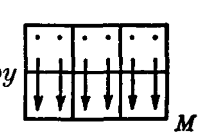
As with M_{24} we shall refer to the subgroup of M_{12} fixing k points as M_{12-k} $(k < 5)$.

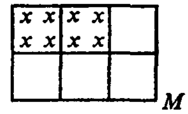
Lemma 5. *The only element of* M_{24} *fixing* 7 *points not in an octad is the identity.*

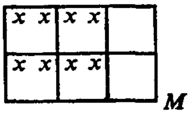
Proof. Any element fixing 6 points of an octad must fix the other 2 (since it lies in A_8) and so lie in the elementary abelian 2-group of fixed point free involutions. The subgroup fixing 6 points not in an octad has order 3 and a generator for this group has shape $1^6.3^6$, where each 3-cycle completes an octad defined by some 5 of the 6 fixed points (since the normalizer of this group must permute the 6 points as S_6).

Corollary 1. *The* 15 *involutions fixing an octad point-wise are all conjugate.*

Proof. Let π be an element of order 15 in the A_8 fixing an octad F and one point i outside it. The disjoint cycles of π must be of lengths 1, 3, 5 or 15 and, since no non-trivial element of M_{24} fixes 9 points of Ω (lemma 5), it has shape $3.5.1.15$; this is plainly transitive on the involutions F_{ij}, $j \notin F+i$.

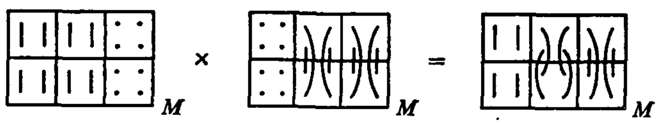
Corollary 2. *The* 3-*element fixing the top row of the MOG is given by* .

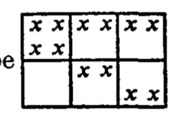
Proof. Since the symmetric difference of the top row of the MOG with any column is an octad the triples which are cycled must be as shown. Giving the first column the downward sense, we observe that the octad  must be taken into

 and so all must cycle downwards.

Note: this process enables us to write down the unique subgroup of order 3 fixing any set of 6 points not in an octad.

A further class of involution. We notice that:



and so there is a further class of involutions which have no fixed point. Moreover we see that there is a unique sextet which is fixed tetrad-wise by this element – for the above involution this is S_∞ (the columns of the MOG). If M is a dodecad fixed by the involution and having 2 points in each tetrad of this sextet then the 'name' S_M completely defines the involution (in this case we could choose M to be ).

We must now show that corresponding to every symbol S_M – where S is a sextet and M is a dodecad cutting across the tetrads of S 2^6 – there is an involution of M_{24} whose name is S_M. It suffices to show that:

Lemma 6. *M_{12} is transitive on sextets cutting the duum* $(2.2)^6$.

Proof. Let the dodecads be X and Y. M_{12} is quintuply transitive on the points of both X and Y. The sextet defined by 4 points of X, say, must cut the duum

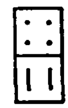
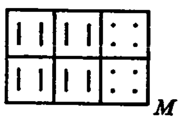
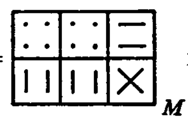
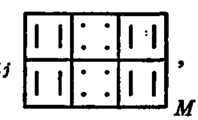
$$(4.0)(2.2)^4(0.4)$$

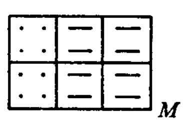
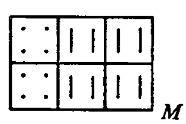
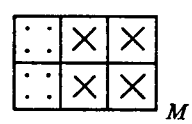
– a consequence of our proof that there are just 2576 dodecads. We now show that M_{12} has just two orbits on *tetrads* cutting 2.2 across the duum. One of these must give the last-mentioned type of sextet and so we shall have shown that there is just one orbit of sextets cutting $(2.2)^6$. Now fixing 2 points of X defines a partition of Y into two halves s.t. each half makes an octad with the fixed points. As we saw before, the stabilizer in M_{12} of the 2 points acts as S_6 on both these two halves with *non*-permutation identical actions. Thus this S_6 contains a subgroup fixing a point of one half and transitive on the 6 points of the other half. So the only distinction between pairs of points of Y is whether they lie in the same or different halves. This proves the lemma and implies that the involutions S_M are all conjugate.

To complete our work on the involutions of M_{24} and to give an example of working with the MOG we prove:

LEMMA 7. *There are just two classes of involution in M_{24} namely the F_{ij} and the S_M.*

Proof. Let $\pi \in M_{24}$, $\pi^2 = 1$.

Since there is an odd number of octads π fixes one, say the first MOG brick. Now the action of $\mathrm{Stab}_{M_{24}}(\Lambda_1)$ on Λ_1 is A_8 and so π must fix no point, 4 points or all points of Λ_1. If all points are fixed then π must belong to the 2^4 group and so is an F_{ij}. In the other two cases we mimic the action of π on Λ_1 with an element F_{ij}. Thus, under conjugation by A_8, suppose the action of π on Λ_1 is  or  and multiply by $\rho =$  or by $\sigma =$  respectively. Thus $\pi\rho$ (or $\pi\sigma$) $\in 2^4$ and, in particular, π and ρ (π and σ) commute. The involutions of 2^4 commuting with ρ are clearly just those 7 fixing each MOG brick; one of these gives the F_{ij} , and the other 6 visibly give involutions S_M (where S is one of the sextets defined by the tetrads A, D, E of the point-space P (page 26)). Those commuting with σ are just the 3 which preserve sextet A tetrad-wise, viz:

and all these lead to F_{ij} elements.

Let us call a set of 3 disjoint octads (such as the bricks of the MOG) a *trio*.

LEMMA 8. *M_{24} is transitive on trios.*

Proof. Consider an element of shape $3.5.1.15$ in the A_8 fixing an octad and a point outside it. This element must have 2 orbits of length 15 on the 30 octads disjoint from the fixed one; plainly one of these consists of those octads containing the fixed point and the other of the rest. Thus the stabilizer of an octad is transitive on the 15 trios containing the fixed octad.

The Trio Stabilizer.

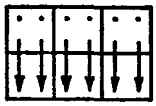
There are $(759.15)/3 = 3795$ trios and so the order of the subgroup fixing one of them is $|M_{24}|/3795 = 2^6.3.2.168$.

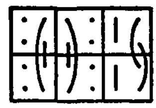
Definition. A sextet whose tetrads may be grouped in pairs to form the trio T is said to be a *refinement* of T.

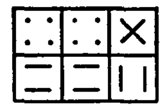
Now every sextet is a refinement of 15 trios (the number of ways 6 objects may be paired) and so the number of refinements of a trio is: $(1771.15)/3795 = 7$.

For the MOG trio these are plainly A, B, C, D, E, F, G.

Now we know that these form a vector subspace of $\mathscr{C}^*$ and so the maximum action the trio group can have on the refinements is $L_3(2)$ (which is isomorphic to $L_2(7)$). The permutations:


M $(ABC)(D)(EFG)$


M $(AE)(BF)(C)(D)(G)$


M $(A)(B)(C)(DE)(FG)$

clearly generate $L_2(7)$. Moreover the bodily interchanges of the MOG bricks form an S_3 which fixes all refinements. Thus the trio group has shape:

$$2^6.(S_3 \times L_2(7))$$

fixing all octads and refinements	fixing the refinements but permuting the octads	fixing octads but permuting refinements.

The factor space $P(\Omega)/\mathscr{C}$.

Consider the map $\phi: P(\Omega) \to L(\mathscr{C}, GF_2)$ (the space of linear maps from $\mathscr{C}$ to the field GF_2) defined by:

$$\begin{aligned}(C)(X\phi) &= 0 \quad \text{if} \quad |C \cap X| \in 2Z \\ &= 1 \quad \text{if} \quad |C \cap X| \in 2Z+1,\end{aligned}$$

where $C \in \mathscr{C}$ and $X \in P(\Omega)$.

This map is plainly a homomorphism and the space $\mathscr{C}$ is contained in its kernel. But the bilinear form $(X, Y) = 0$ if and only if $|X \cap Y| \in 2Z$ (for X and $Y \in P(\Omega)$) gives a zero quadratic form on $\mathscr{C}$ and so $\operatorname{Ker}\phi = \mathscr{C}$. Thus $P(\Omega)/\mathscr{C}$ is isomorphic to the dual space of $\mathscr{C}$ and so, from now on, we shall refer to it as $\mathscr{C}^*$.

Let $X \in P(\Omega)$. If $|X| \geqslant 5$, then adding an octad F containing 5 points of X to X results in a smaller set $X+F$. Since $X \equiv X+F \pmod{\mathscr{C}}$ we see:

LEMMA 9. *Any set $P(\Omega)$ is congruent,* mod $\mathscr{C}$, *to a monad (one point), a dyad (two points), a triad (three points) or a sextet (the 6 tetrads of a sextet being congruent to one another* mod $\mathscr{C}$).

There are:

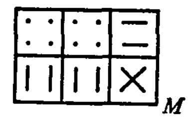
24	monads
$\binom{24}{2} = 276$	dyads
$\binom{24}{3} = 2024$	triads
$(1/6)\binom{24}{4} = 1771$	sextets.

We note that $1+24+276+2024+1771 = 4096 = 2^{12}$. The quintuple transitivity of M_{24} implies transitivity on each of these sets.

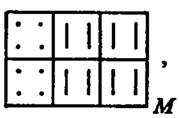
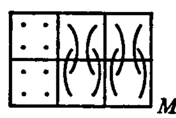
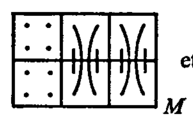
We see that the stabilizers of a monad, a dyad and a triad are respectively:

$$M_{23}, \quad M_{22}.2 \quad \text{and} \quad M_{21}.S_3.$$

The sextet stabilizer.

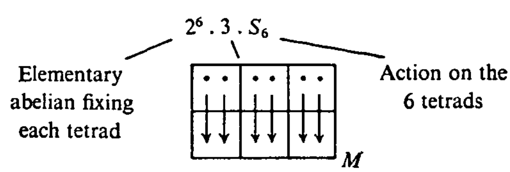
The stabilizer of a sextet has order $|M_{24}|/1771 = 2^6.3.6!$. If we choose as sextet S_∞ (i.e. the columns of the MOG) we find that the element  acts as a transposition on the tetrads. But clearly the sextet stabilizer is doubly transitive on the tetrads since M_{20} is transitive on the 20 points remaining.

Thus every transposition of tetrads occurs and the action on the tetrads is S_6. Now every involution fixing two tetrads pointwise and preserving the others is in the group, i.e.

 ,  and  etc.

There are $\binom{6}{2}.3 = 45$ of these.

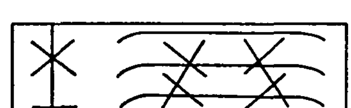
Since any two clearly commute (their action on the individual tetrads being the elements of the V_4 in A_4) they generate a normal elementary abelian subgroup of order at least 2^6. From the order of the sextet group it is at most 2^6 and so the whole group has shape:



The Octern Group.

To complete our description of the subgroups of M_{24}, we introduce a further maximal subgroup known as the Octern group O^n. O^n may be defined as the centralizer in M_{24} of a certain element of order 3 in $S_{24}\backslash M_{24}$, or, alternatively, as the stabilizer of a certain purely dodecad 4-dimensional subspace of $\mathscr{C}$. We display here the set Ω arranged as a 3×8 array whose columns are the cycles of this 3-element (the eight *terns*), the first tern having opposite sense of rotation to the others. The subspace consists of those $\mathscr{C}$-sets which are unions of terns.

∞	14	18	8	0	20	15	3
17	7	10	16	11	2	13	4
22	21	12	19	6	9	1	5



It turns out that $O^n \cong L_2(7)$ and is generated by the element fixing the rows and cycling the last seven columns of the figure, together with the involution displayed above.

We have now seen all the maximal subgroups of M_{24}. In fact every maximal subgroup is conjugate to one of the following:

Monad Stabilizer	M_{23}	Duum Stabilizer	$M_{12}.2$
Dyad Stabilizer	$M_{22}.2$	Trio Stabilizer	$2^6.(S_3 \times L_2(7))$
Triad Stabilizer	$M_{21}.S_3$	Octern Group	$L_2(7)$
Sextet Stabilizer	$2^6.3.S_6$	Projective Group	$L_2(23)$
Octad Stabilizer	$2^4.A_8$		

A short proof of this statement is the content of a sequel to this paper. We conclude with some tabular information which the reader will find useful.

The orbits on the subsets of Ω.

The orbits on the subsets of Ω under the action of M_{24} have been worked out by Todd. Conway has exhibited the information in a convenient tabular form, (2), and has furnished a simple proof that the list is complete. We shall adhere to his notation for the various subsets and reproduce here his table and proof.

THEOREM D. *The subsets of* Ω *fall into* 49 *orbits under the action of* M_{24}, *related as in the following table. Each node corresponds to one orbit, and the nodes are joined by lines indicating the number of ways a set of one type can be converted to one of another by the addition or removal of a single point. Thus in an umbral heptad* (U_7), *there is one point whose removal leaves a special hexad* (S_6), *removal of any of the other* 6 *leaving an umbral hexad* (U_6) *instead.*

Proof. In each case we consider (i) what the set is congruent to modulo and (ii) the nearest $\mathscr{C}$-set(s). If the set is congruent to a monad, dyad or triad modulo $\mathscr{C}$ then there is a unique nearest $\mathscr{C}$-set (namely the sum of the original set with the monad, dyad or triad it is congruent to). If the set is congruent to a sextet then there are just six nearest $\mathscr{C}$-sets. As an example of this we consider 8-element sets. Each 8-element set is congruent to one of: (*a*) the empty set $\varnothing$, (*b*) a unique dyad T, (*c*) the 6 tetrads of a sextet modulo $\mathscr{C}$.

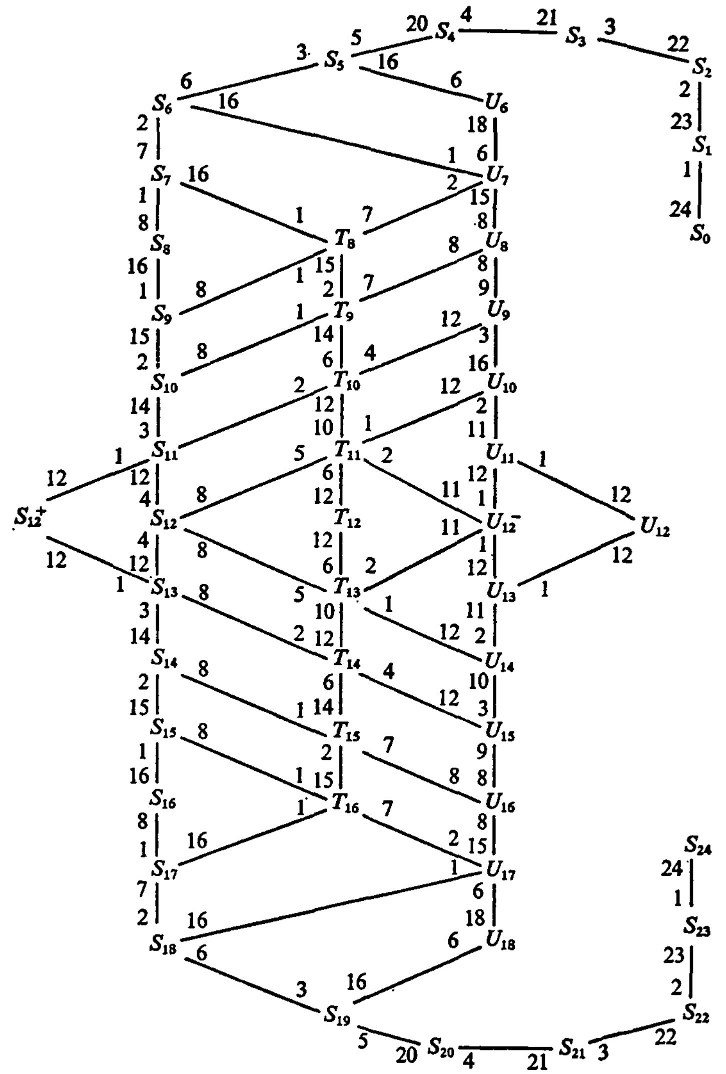
In case (*a*), the set S is an octad. M_{24} is transitive on these.

In case (*b*), S is obtained from the octad $S+T$ by adding one point and subtracting another. The octad group is independently transitive on an octad and its complement and so M_{24} is transitive on sets of this type which will be called *transverse octads* T_8.

In case (*c*) $S+T_i$ (T_i one of the tetrads) is an octad if T_i contains 2 points of S and a dodecad if it is disjoint from S. Counting points of S shows that there are four tetrads of the first kind and two of the second, so that S can be obtained (in 2 ways) by removing 4 points from a dodecad. The quintuple transitivity of M_{12} on the points of the fixed dodecads show M_{24} to be transitive on such sets S which will be called *umbral octads* U_8.

Note. The 2 tetrads of the sextet congruent to S modulo $\mathscr{C}$ which are disjoint from S form an octad which is determined by S. In particular the group fixing a U_8 also fixes an octad. We shall use this fact in the sequel.

In general, a set of cardinal $n \leqslant 12$ is called *special* (S_n) if it contains or is contained in a special octad (octad), otherwise *umbral* (U_n) if it is contained in an umbral dodecad,



The action of M_{24} on $P(\Omega)$

and *transverse* (T_n) if not. A non-umbral dodecad is *extraspecial* (S_{12}^+) if it contains three special octads, *special* if it contains just one (S_{12}), *penumbral* (U_{12}^-) if it contains all but one of the points of an umbral dodecad, and *transverse* (T_{12}) in all other cases. Sets of more than 12 points are described by the same adjectives as their complements.

REFERENCES

(1) Curtis, R. T. On the Mathieu Group M_{24} and Related Topics. Ph.D. Thesis, Cambridge 1972.

(2) Conway, J. H. Three Lectures on Exceptional Groups. Chap. vii in *Finite Simple Groups* (M. B. Powell and G. Higman).

(3) Todd, J. A. *Ann. Mat. Pura Appl. series IV*, **71** (1966), 199–238.

Characters of M_{24}. Order 244823040.

1^{24}	$1^8 2^8$	$1^6 3^6$	$1^4 5^4$	$1^4 4^4 2^2$	$1^3 7^3$	$1^3 7^3$	$1^2 8^2 4\,2$	$1^2 6^2 3^2 2^2$	$1^2 11^2$	$1\,15\,5\,3$	$1\,15\,5\,3$	$1\,14\,7\,2$	$1\,14\,7\,2$	$1\,23$	$1\,23$	12^2	6^4	4^6	3^8	2^{12}	$10^2 2^2$	$21\,3$	$21\,3$	$4^4 2^4$	$12\,6\,4\,2$
g	21504	1080	60	128	42	42	16	24	11	15	15	14	14	23	23	12	24	96	504	7680	20	21	21	384	12
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
23	7	5	3	3	2	2	1	1	1	0	0	0	0	0	0	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1
45	−3	0	0	1	α	$\bar\alpha$	−1	0	1	0	0	$-\alpha$	$-\bar\alpha$	−1	−1	1	−1	1	3	5	0	$\bar\alpha$	α	−3	0
45	−3	0	0	1	$\bar\alpha$	α	−1	0	1	0	0	$-\bar\alpha$	$-\alpha$	−1	−1	1	−1	1	3	5	0	α	$\bar\alpha$	−3	0
231	7	−3	1	−1	0	0	−1	1	0	β	β	0	0	1	1	0	0	3	0	−9	1	0	0	−1	−1
231	7	−3	1	−1	0	0	−1	1	0	$\bar\beta$	β	0	0	1	1	0	0	3	0	−9	1	0	0	−1	−1
252	28	9	2	4	0	0	0	1	−1	−1	−1	0	0	−1	−1	0	0	0	0	12	2	0	0	4	1
253	13	10	3	1	1	1	−1	−2	0	0	0	−1	−1	0	0	1	1	1	1	−11	−1	1	1	−3	0
483	35	6	−2	3	0	0	−1	2	−1	1	1	0	0	0	0	0	0	3	0	3	−2	0	0	3	0
770	−14	5	0	−2	0	0	0	1	0	0	0	0	0	γ	$\bar\gamma$	1	1	−2	−7	10	0	0	0	2	−1
770	−14	5	0	−2	0	0	0	1	0	0	0	0	0	$\bar\gamma$	γ	1	1	−2	−7	10	0	0	0	2	−1
990	−18	0	0	2	α	$\bar\alpha$	0	0	0	0	0	α	$\bar\alpha$	1	1	1	−1	−2	3	−10	0	$\bar\alpha$	α	6	
990	−18	0	0	2	$\bar\alpha$	α	0	0	0	0	0	$\bar\alpha$	α	1	1	1	−1	−2	3	−10	0	α	$\bar\alpha$	6	0
1035	−21	0	0	3	2α	$2\bar\alpha$	−1	0	1	0	0	0	0	0	0	−1	1	−1	−3	−5	0	$-\bar\alpha$	$-\alpha$	3	0
1035	−21	0	0	3	$2\bar\alpha$	2α	−1	0	1	0	0	0	0	0	0	−1	1	−1	−3	−5	0	$-\alpha$	$-\bar\alpha$	3	0
1035	27	0	0	−1	−1	−1	1	0	1	0	0	−1	−1	0	0	0	2	3	6	35	0	−1	−1	3	0
1265	49	5	0	1	−2	−2	1	1	0	0	0	0	0	0	0	0	0	−3	8	−15	0	1	1	−7	−1
1771	−21	16	1	−5	0	0	−1	0	0	1	1	0	0	0	0	−1	−1	−1	7	11	1	0	0	3	0
2024	8	−1	−1	0	1	1	0	−1	0	−1	−1	1	1	0	0	0	0	0	8	24	−1	1	1	8	−1
2277	21	0	−3	1	2	2	−1	0	0	0	0	0	0	0	0	0	2	−3	6	−19	1	−1	−1	−3	0
3312	48	0	−3	0	1	1	0	0	1	0	0	−1	−1	0	0	0	−2	0	−6	16	1	1	1	0	0
3520	64	10	0	0	−1	−1	0	−2	0	0	0	1	1	1	1	0	0	0	−8	0	0	−1	−1	0	0
5313	49	−15	3	−3	0	0	−1	1	0	0	0	0	0	0	0	0	0	−3	0	9	−1	0	0	1	1
5544	−56	9	−1	0	0	0	0	1	0	−1	−1	0	0	1	1	0	0	0	0	24	−1	0	0	−8	1
5796	−28	−9	1	4	0	0	0	−1	−1	1	1	0	0	0	0	0	0	0	0	36	1	0	0	−4	−1
10395	−21	0	0	−1	0	0	1	0	0	0	0	0	0	−1	−1	0	0	3	0	−45	0	0	0	3	0

$\alpha = \frac{1}{2}(-1+i\sqrt{7})$ $\beta = \frac{1}{2}(-1+i\sqrt{15})$ $\gamma = \frac{1}{2}(-1+i\sqrt{23})$