Math. Zeitschr. 105, 110–113 (1968)

A Simple Group of Order 44,352,000

DONALD G. HIGMAN and CHARLES C. SIMS

Received November 20, 1967

The group G of the title is obtained as a primitive permutation group of degree 100 in which the stabilizer of a point has orbits of lengths 1, 22 and 77 and is isomorphic to the Mathieu group M_{22}. Thus G has rank 3 in the sense of [1]. G is an automorphism group of a graph constructed from the Steiner system $\mathfrak{S}(3, 6, 22)$.

WITT [3] defined a Steiner system $\mathfrak{S}(d, m, n)$ to be a set S of n points together with a set B of subsets of S (referred to here as *blocks*) such that each block contains exactly m points and each set of d points is contained in exactly one block. WITT [4] showed that Steiner systems $\mathfrak{S}(3, 6, 22)$ exist and that they are unique up to isomorphism. The automorphism group $\overline{M}_{22}$ of an $\mathfrak{S}(3,6,22)$ contains the Mathieu group M_{22} as a subgroup of index 2 and is the normalizer of M_{22} in M_{24}.

Throughout the rest of the paper we shall use the following notation: S and B will denote the sets of points and blocks, respectively, of a fixed $\mathfrak{S}(3, 6, 22)$. Points will be denoted by Greek letters $\alpha, \beta, \ldots$ and blocks by Roman letters $u, v, \ldots$. For each $\alpha \in S$, $[\alpha]$ will denote the set of blocks containing α.

We shall use the following facts about $\mathfrak{S}(3, 6, 22)$ and $\overline{M}_{22}$:

(1) Each point α is contained in exactly 21 blocks. Thus $|[\alpha]| = 21$.

(2) Two distinct points are contained in exactly 5 blocks.

(3) Two distinct blocks have 0 or 2 points in common, 16 blocks being disjoint from a given block and 60 meeting it in 2 points.

(4) If u is a block not in $[\alpha]$, then exactly 6 blocks in $[\alpha]$ are disjoint from u.

(5) Given distinct points α and β and distinct blocks u and v in $[\alpha] \cap [\beta]$ there exist exactly 4 blocks disjoint from u and v.

(6) No 3 blocks are pairwise disjoint.

(7) $\overline{M}_{22}$ contains an involution fixing exactly 8 points and 21 blocks.

(1)–(6) are easily proved by counting arguments. (7) can be seen from an inspection of the character table of $\overline{M}_{22}$ given in [2].

We now construct an undirected graph $\mathscr{G}$ with vertex set

$$\{*\} \cup S \cup B,$$

where $*$ is a new symbol. In $\mathscr{G}$,

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

(b) Each point $\alpha \in S$ is joined to the 21 blocks in $[\alpha]$.

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

Let $\bar{G}$ denote the automorphism group of $\mathcal{G}$. It is clear that the stabilizer of $*$ in $\bar{G}$ is isomorphic to the automorphism group of $\mathfrak{S}(3,6,22)$, that is, $\bar{M}_{22}$. We shall show that $\bar{G}$ is transitive on the vertices of $\mathcal{G}$, from which it follows that $\bar{G}$ has order 88,704,000. Since by (7) $\bar{G}$ contains an odd permutation, $\bar{G}$ is not simple but contains a simple subgroup G of index 2.

Take $\alpha \in S$ and let $S(\alpha)$ and $B(\alpha)$ be the sets of vertices of $\mathcal{G}$ at distance 1 and 2 from α, respectively. $S(\alpha)=\{*\} \cup [\alpha]$. Thus $|S(\alpha)|=22$ and no two vertices of $S(\alpha)$ are joined. If $\beta \in S-\{\alpha\}$, then β is joined to $*$ and so $\beta \in B(\alpha)$. If $v \in B-[\alpha]$, then by (4) v is joined to some block in $[\alpha]$ and so $v \in B(\alpha)$. Hence

$$B(\alpha)=(S-\{\alpha\}) \cup (B-[\alpha])$$

and $|B(\alpha)|=77$.

We shall prove that

(i) *Each vertex in* $B(\alpha)$ *is joined to exactly* 6 *vertices in* $S(\alpha)$.

(ii) *Three distinct vertices in* $S(\alpha)$ *are joined to exactly one vertex in* $B(\alpha)$.

(iii) *Two vertices in* $B(\alpha)$ *are joined if and only if they are not joined to a common vertex in* $S(\alpha)$.

From (i), (ii), (iii) *and the uniqueness of* $\mathfrak{S}(3,6,22)$ *it follows that the stabilizer of* α *in* $\bar{G}$ *is also isomorphic to* $\bar{M}_{22}$ *and this implies that* $\bar{G}$ *is transitive.*

Proof of (i). A vertex in $B(\alpha)$ is either a point $\beta \in S-\{\alpha\}$ or a block u in $B-[\alpha]$. If $\beta \in S-\{\alpha\}$, then by (2) β is joined to $*$ and to the 5 blocks containing α and β and to no other vertices in $S(\alpha)$. If $u \in B-[\alpha]$, then by (4) u is joined to the 6 blocks in $[\alpha]$ disjoint from u and to no other vertices in $S(\alpha)$.

Proof of (ii). We consider in turn each of the three types of sets of 3 distinct vertices in $S(\alpha)$. Since by (i) each vertex in $B(\alpha)$ is joined to 20 triples and there are $77 \cdot 20$ triples altogether, it suffices to show that each triple is joined to at least one vertex in $B(\alpha)$.

Type I. $\{*, v, w\}$, $v, w \in [\alpha]$. In this case $*$, v and w are joined to β, where $v \cap w=\{\alpha, \beta\}$.

Type II. $\{u, v, w\}$, $u, v, w \in [\alpha] \cap [\beta]$, $\beta \in S-\{\alpha\}$. Here u, v and w are joined to β.

Type III. $\{u,v,w\}$, $u, v, w \in [\alpha]$, $u \cap v=\{\alpha, \beta\}$, $u \cap w=\{\alpha, \gamma\}$, $v \cap w=\{\alpha, \delta\}$, with β, γ and δ distinct points of $S-\{\alpha\}$. We must show the existence of a block disjoint from u, v and w. Let $\bar{w}=w-\{\alpha, \gamma, \delta\}$. By (5) there are 4 blocks disjoint from u and v, say z_1, z_2, z_3, z_4. Suppose all of the z_i intersect w non-trivially. Let $\bar{z}_i=z_i-w$. By (3) $|\bar{z}_i|=4$. Let $1 \leqq i<j \leqq 4$. $w \cap z_i$ and $w \cap z_j$ are contained in $\bar{w}$ and each contain 2 points. Hence $w \cap z_i \cap z_j$ is non-empty. Since $|z_i \cap z_j| \leqq 2$, we have $|\bar{z}_i \cap \bar{z}_j| \leqq 1$. Therefore

$$\Big|\bigcup_i \bar{z}_i\Big| \geqq \sum_i |z_i| - \sum_{i<j} |\bar{z}_i \cap \bar{z}_j| \geqq 16-6=10\,.$$

However,

$$\bigcup_i \bar{z}_i \subseteq S - u \cup v \cup w$$

and $|u \cup v \cup w| = 13$. Thus

$$\left|\bigcup_i \bar{z}_i\right| \leqq 9,$$

a contradiction.

Proof of (iii). By (ii) each vertex in $B(\alpha)$ is joined to 16 other vertices in $B(\alpha)$. By (i) and (ii) we may consider $B(\alpha)$ to be the set of blocks of an $\mathfrak{S}(3,6,22)$ with point set $S(\alpha)$. By (3) it suffices to show that if two vertices in $B(\alpha)$ are joined, then they are not joined to a common vertex in $S(\alpha)$. There are three types of two-element subsets of $B(\alpha)$.

Type I. $\{\beta,\gamma\} \subseteq S - \{\alpha\}$. β and γ are not joined.

Type II. $\{\beta,u\}$, $\beta \in S - \{\alpha\}$, $u \in B - [\alpha]$. If β and u are joined, then $\beta \in u$. If β and u are joined to a common vertex in $S(\alpha)$, then that vertex must be a block $v \in [\alpha]$. But then $\beta \in v$ and so $u \cap v \neq \phi$. Therefore u and v are not joined.

Type III. $\{u,v\} \subseteq B - [\alpha]$. A vertex in $S(\alpha)$ joined to u and v must be a block w in $[\alpha]$. If u is also joined to v, then u, v and w are pairwise disjoint, contradicting (6).

We conclude by giving generating permutations for G. Numbering the vertex $*$ as 1, the points of S as 2, 3, ..., 23, and the blocks in B as 24, 25, ..., 100 in an appropriate manner, G is found to be generated by the permutations

a = (1) (2, 8, 13, 17, 20, 22, 7) (3, 9, 14, 18, 21, 6, 12)
(4, 10, 15, 19, 5, 11, 16) (23) (24, 77, 99, 72, 64, 82, 40)
(25, 92, 49, 88, 28, 65, 90) (26, 41, 70, 98, 91, 38, 75)
(27, 55, 43, 78, 86, 87, 45) (29, 69, 59, 79, 76, 35, 67)
(30, 39, 42, 81, 36, 57, 89) (31, 93, 62, 44, 73, 71, 50)
(32, 53, 85, 60, 51, 96, 83) (33, 37, 58, 46, 84, 100, 56)
(34, 94, 80, 61, 97, 48, 68) (47, 95, 66, 74, 52, 54, 63)

and

b = (1, 35) (2) (3, 81) (4, 92) (5) (6, 60) (7, 59) (8, 46)
(9, 70) (10, 91) (11, 18) (12, 66) (13, 55) (14, 85) (15, 90)
(16) (17, 53) (19, 45) (20, 68) (21, 69) (22) (23, 84)
(24, 34) (25, 31) (26, 32) (27) (28) (29) (30) (33) (36)
(37, 39) (38, 42) (40, 41) (43, 44) (47) (48) (49, 64)
(50, 63) (51, 52) (54, 95) (56, 96) (57, 100) (58, 97)
(61, 62) (65, 82) (67, 83) (71, 98) (72, 99) (73) (74, 77)
(75) (76, 78) (79) (80) (86) (87, 89) (88) (93) (94).

References

1. HIGMAN, D. G.: Finite permutation groups of rank 3. Math. Z. **86**, 145—156 (1964).

2. TODD, J. A.: A representation of the Mathieu group M_{24} as a collineation group. Ann. Mat. Pura App. (4) **71**, 199—238 (1966).

3. WITT, E.: Die 5-fach transitiven Gruppen von Mathieu. Abh. Math. Sem. Hamb. **12**, 256—264 (1937).

4. — Über Steinersche Systeme. Abh. Math. Sem. Hamb. **12**, 265—275 (1937).

Prof. D. G. HIGMAN
Department of Mathematics
University of Michigan
Ann Arbor, Michigan
U.S.A.

Prof. C. C. SIMS
Department of Mathematics
Rutgers, The State University
New Brunswick, N. J. 08903
U.S.A.