A GROUP OF ORDER 8,315,553,613,086,720,000

J. H. CONWAY

0. *Introduction*

We shall discuss the group $\cdot 0$ of all Euclidean congruences (fixing the origin) of the remarkable lattice Λ discovered by John Leech [6], [7] in connection with close-packing of spheres in 24 dimensions. We preface this discussion by a description of the Steiner system $S(5, 8, 24)$ which appears in the construction of Λ and underlies the Mathieu group M_{24}. The group $\cdot 0$ appears to involve 12 of the 14 known simple groups which have not yet been fitted into natural infinite series, the exceptions being the Janko group of order 175560 and the Higman–Janko–McKay group of order 50232960, whose orders do not divide that of $\cdot 0$. We shall describe the embeddings of the Higman–Sims and McLaughlin simple groups in $\cdot 0$.

We use standard mathematical notations without comment. If S is a set of vectors and $x, y \in S$, we write $S(x)$ for the set of vectors of S which are orthogonal to x, and if G is a group acting on S we use G_x $(G_{x,y})$ for the group of all operations of G fixing x (fixing x and y).

1. *The Steiner system* $S(5, 8, 24)$

It is possible [1], in an essentially unique way [13], to select 759 8-element subsets called *special octads* from a 24 element set Ω so that each 5 element subset of Ω is contained in just one special octad. Such a system is called a *Steiner system* $S(5, 8, 24)$. If we define the sum $A+B$ of two sets as their symmetric difference $(A \setminus B) \cup (B \setminus A)$, then the power-set 2^{Ω} of Ω becomes a vector space over the field of two elements, and in this space the sets of any system $S(5, 8, 24)$ span a subspace $\mathscr{C}$ of only 12 dimensions, consisting of the set Ω, the empty set $\varnothing$, the 759 special octads and their complements, and 2576 12-element sets called *umbral dodecads*.

This astonishing fact, proofs of which are implicit in [6], [11], simplifies Carmichael's construction [1] for $S(5, 8, 24)$. If Ω is the set of residue classes modulo 23 together with the formal symbol ∞, so that the group $L = LF_2(23)$ has a natural action on Ω, we can define $\mathscr{C}$ as the subspace of 2^{Ω} spanned by the L-images of the set Q consisting of 0 and the quadratic residues modulo 23. If the term $\mathscr{C}$-set means a member of $\mathscr{C}$, and $\mathscr{C}_n$ is the set of n-element $\mathscr{C}$-sets, then $\mathscr{C}_8$ is the required system $S(5, 8, 24)$ which is conveniently listed in full in Todd's beautiful paper [11] on M_{24}.

Indeed, the Mathieu group M_{24} ([8], [13], [11]) is commonly defined as the set of permutations of Ω fixing the system $\mathscr{C}_8$, or equivalently, the space $\mathscr{C}$. We use the following terminology to describe the orbits of 2^{Ω} under M_{24}. Ω_n denotes the collection of n-element subsets of Ω, and the members of Ω_n are called *n-ads* (in particular monads, duads, etc.).

Received 21 November, 1968.

If $n < 12$, an *n-ad* is *special* if it contains or is contained in a special octad, and otherwise *umbral* if it is contained in an umbral dodecad, *transverse* if not. The same adjectives are applied to the complementary $(24-n)$-ads. A dodecad is *extraspecial* if it contains three special octads, *special* if it contains just one, *penumbral* if it contains just 11 points of some umbral dodecad, and *transverse* if it is neither special, extraspecial, umbral, nor penumbral. In what follows the unqualified terms *octad* and *dodecad* will always mean *special octad* and *umbral dodecad.*

Let $\Omega = \{a_1, \ldots, a_{24}\}$, and define S_i as $\{a_1, \ldots, a_i\}$, the notation being so chosen that S_8 is an octad. Then the $(j+1)$th entry in the $(i+1)$th line of Table 1 is the number of octads intersecting S_i in S_j, and the corresponding entry in Table 2 is the number of dodecads. A brief scrutiny of the tables reveals much of their mode of construction.

TABLE 1. How many octads?

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

TABLE 2. How many dodecads?

2576								
1288	1288							
616	672	616						
280	336	336	280					
120	160	176	160	120				
48	72	88	88	72	48			
16	32	40	48	40	32	16		
0	16	16	24	24	16	16	0	
0	0	16	0	24	0	16	0	0

2. *The Leech lattice*

Let $\{v_i | i \in \Omega\}$ be an orthonormal base for Euclidean 24-space $\mathbb{R}^{24}$: if $S \subseteq \Omega$ let $v_S = \sum v_i$ $(i \in S)$: and let $x = \sum x_i v_i$ be the typical vector of $\mathbb{R}^{24}$. Now for any $S \subseteq \Omega$ and any integer m, define the set $[S, m]$ as the set of all vectors x with integral co-ordinates x_i which satisfy $\sum x_i = 4m$ and also $x_i \equiv m$ or $m+2 \pmod 4$ according as $i \notin S$ or $i \in S$. If $\mathscr{S} \subseteq 2^{\Omega}$ and $M \subseteq \mathbb{Z}$, define $[\mathscr{S}, M]$ as the union of all the sets $[S, m]$ $(S \in \mathscr{S},\ m \in M)$, and define the *Leech lattice* as the set $[\mathscr{C}, \mathbb{Z}]$. Since the vectoı sum of $[C, m]$ and $[D, n]$ is $[C+D, m+n]$, Λ *is* a lattice.

We find a spanning set for Λ. Let X, Y, Z be the sublattices spanned by all vectors of the respective forms $2v_K$ $(K \in \mathscr{C}_8)$, $4v_T$ $(T \in \Omega_4)$, $4v_i - 4v_j$ $(i, j \in \Omega)$. We show that $X \supseteq Y$. Let $T = T_0$ be any tetrad, and let $T+T_1, \ldots, T+T_5$ be the five octads containing T (Table 1). Since $T_i + T_j = (T+T_j)+(T+T_j)$ the union of any two members of the set $\Xi(T) = \{T_0, \ldots, T_5\}$ is an octad, and if T, U, V are three distinct members of $\Xi(T)$ we have $4v_T = 2v_{T+U} + 2v_{T+V} - 2v_{U+V} \in X$, and so $Y \subseteq X$.

Now plainly $Z = [\varnothing, 0]$, whence $Y = [\varnothing, 4\mathbb{Z}]$, since Y contains Z and also a member of $[\varnothing, 4]$, and then $X = [\mathscr{C}, 4\mathbb{Z}]$ since $X \supseteq Y$ and $\mathscr{C}_8$ spans $\mathscr{C}$. It follows that Λ is spanned by the 759 vectors $2v_K$ $(K \in \mathscr{C}_8)$ together with any vector of Λ which has odd co-ordinates, say $v_{\Omega} - 4v_{\infty}$.

Now it is easy to check that for any two vectors x, y of this set of 760 we have $x.x \in 16\mathbb{Z}$, $x.y \in 8\mathbb{Z}$, and so the same is true of any two vectors x, y of Λ. If $x.x = 16n$, we say that x has type n, and if also x is the sum of two vectors of types a and b, that x has type n_{ab}. We write Λ_n for the set of all $x \in \Lambda$ of type n.

It follows that Λ_n is the set of all vectors x with integral coordinates x_i satisfying

(i) the coordinate-sum is a multiple of 4, say $4m$.

(ii) the coordinates are all congruent to m modulo 2.

(iii) the set of i for which x_i takes a given value modulo 4 is a $\mathscr{C}$-set.

(iv) the sum of the squares of the coordinates is $16n$.

We use these to list the vectors of Λ_2—the same ideas soon show that Λ_1 is empty. Conditions (ii) and (iv) leave only the shapes $(2^8, 0^{16})$, $(3, 1^{23})$, $(4^2, 0^{22})$, and $(4, 2^4, 0^{19})$, this last symbol, for instance, denoting the typical vector with one coordinate ± 4, four coordinates ± 2, and nineteen zero coordinates. Condition (iii) now excludes this last case, and indeed (i) and (iii) leave only the three classes Λ_2^2, Λ_2^3, Λ_2^4 below.

Λ_2^2 has 759.2^7 vectors of shape $(2^8, 0^{16})$, the non-zero coordinates having positive product and being in the places of a $\mathscr{C}$-set.

Λ_2^3 has 24.2^{12} vectors of shape $(3, 1^{23})$, the coordinates congruent to 1 modulo 4 being in the places of a $\mathscr{C}$-set.

Λ_2^4 has $\binom{24}{2}.2^2$ vectors of shape $(4^2, 0^{22})$.

The reader should now be able to show that $\Lambda_3 = \Lambda_3^2 \cup \Lambda_3^3 \cup \Lambda_3^4 \cup \Lambda_3^5$, where Λ_3^2 has 2576.2^{11} vectors of shape $(2^{12}, 0^{12})$, Λ_3^3 has $\binom{24}{3}.2^{12}$ vectors of shape $(3^3, 1^{21})$, Λ_3^4 has $759.16.2^8$ of shape $(4, 2^8, 0^{15})$, and Λ_3^5 has 24.2^{11} of shape $(5, 1^{23})$.

3. *The group N*

A congruence of $\mathbb{R}^{24}$ which fixes the origin and also the lattice Λ (as a whole) we call a *rotation* (of Λ).

Now any permutation π of Ω extends to an orthogonal opeiation on $\mathbb{R}^{24}$ when we define $(v_i)\,\pi$ as $v_{i\pi}$, and any subset S of Ω yields an orthogonal operation ε_S defined by $(v_i)\,\varepsilon_S = v_i$ or $-v_i$ according as $i \notin S$ or $i \in S$. The operation π is a rotation provided it preserves $\mathscr{C}$, and so these operations form a group $M = M_{24}$ isomorphic to the Mathieu group on 24 letters. The operation ε_S is a rotation provided $S \in \mathscr{C}$, and so these operations form an elementary abelian group $E = E_{12}$ of order 2^{12} isomorphic with the additive group of $\mathscr{C}$. The group $N = N_{24} = EM$ is a splitting extension of E by M about which we prove two theorems:

THEOREM 1. *A rotation λ fixing a coordinate vector v_i is in N.*

THEOREM 2. *A rotation λ which fixes Λ_2^4 (as a whole) is in N.*

We preface the proofs by a theorem of independent interest:

THEOREM 0. *No rotation has prime order $p > 23$.*

Proof. Such a rotation would have a rational matrix with some primitive pth root of unity as an eigenvalue, and so every primitive pth root of unity must be an eigenvalue, so that the dimension 24 is at least $p-1$, whence $p \leqslant 23$.

Remark. A similar argument shows that no rotation has order 13.23.

Proof of Theorem 1. Let $w_j = (v_j)\,\lambda$, so that for $j \neq i$ w_j is a vector orthogonal to v_i, and $4v_i + 4w_j \in \Lambda_2$. Our enumeration of Λ_2 now shows that $w_j = \pm v_k$ for some $k \in \Omega$, distinct values of j yielding distinct values of k, and so $\lambda = \pi\varepsilon_S$ for some permutation π of Ω and some $S \subseteq \Omega$. But since the non-zero coordinates of $(2v_K)\lambda$ are in the places of $K\pi$, we must have $K\pi \in \mathscr{C}_8$ for every $K \in \mathscr{C}_8$, and so $\pi \in M$. Again, the coordinates of $(v_\Omega - 4v_\infty)\lambda$ which are congruent to 1 modulo 4 are in the places of S, so that $S \in \mathscr{C}$, and so $\lambda = \pi\varepsilon_S$ is in N.

Proof of Theorem 2. Let H be the set of all rotations fixing Λ_2^4 as a whole, and let $x = 4v_i + 4v_j$. Then N_x has just two orbits on $\Lambda_2^4(x)$, one orbit consisting of the two points $\pm(4v_i - 4v_j)$ and the other of the 924 points $\pm 4v_h \pm 4v_k$ for which h, i, j, k are distinct. Since $H \supseteq N$ the orbits of H_x on $\Lambda_2^4(x)$ must be unions of these, and since Theorem 0 prevents H_x from having an orbit of size 926, each element λ of H_x must transform $4v_i - 4v_j$ to itself or its negative. In the first case λ fixes v_i, and in the second case takes v_i to v_j, so that in either case we have $\lambda \in N$ by Theorem 1 (and the transitivity of N on Ω).

We remark that just as the stabiliser of k points in M_{24} is a group M_{24-k} on $24-k$ letters ($k \leqslant 5$), so the stabiliser of k vectors v_i in N_{24} is a group

$$N_{24-k} = E_{12-k} M_{24-k},$$

a splitting extension of an elementary group E_{12-k} of order 2^{12-k} by the group M_{24-k} ($k \leqslant 5$).

4. *The group* ·0

We define the group ·0 as the group of all rotations of Λ.

THEOREM 3. *N is a proper subgroup of* ·0.

Proof. Let $T \in \Omega_4$, and $\Xi = \Xi(T)$ the set defined in Section 2. Let $\eta = \eta_\Xi$ be the operation taking v_i to $v_i - \frac{1}{2}v_U$ whenever $i \in U \in \Xi$. We show that $\zeta_T = \eta\varepsilon_T$ is a rotation by examining its effect on our spanning set for Λ.

If we suppose $\Xi = \{U, V, W, X, Y, Z\}$ and $K \in \mathscr{C}_8$, we have essentially three cases:

(i) K is the union of U and V.

(ii) K intersects U, V, W, X in two points each.

(iii) K intersects Z in three points, U, V, W, X, Y in one point each.

If $y = (2v_K)\eta\varepsilon_Z$, we then have, respectively:

$$y = (2v_K - 4v_{U+V})\varepsilon_Z = -2v_K\varepsilon_Z = -2v_K$$

$$y = (2v_K - 2v_{U+V+W+X})\varepsilon_Z = -2v_{K+U+V+W+X}\varepsilon_Z = -2v_{K+U+V+W+X}$$

$$y = (2v_K - 3v_Z - v_{\Omega\setminus Z})\varepsilon_Z = 2v_{K\setminus Z} - 2v_{Z\cap K} + 3v_Z - v_{\Omega\setminus Z} = (4v_{Z\setminus K} - v_\Omega)\varepsilon_K,$$

so that in each case $y \in \Lambda$, and since $Z + T \in \mathscr{C}$ the vector $(2v_K)\zeta_T = y\varepsilon_{Z+T}$ is also in Λ. To complete the proof that $\zeta_T \in {\cdot}0$ we need only check its effect on some vector of Λ with odd co-ordinates, and since ζ_T is an involution this has already been done in case (iii) above.

We now see that $\cdot 0$ contains the following rotations:

$$\alpha\colon\ v_i \to v_{i+1} \qquad \beta\colon\ v_i \to v_{2i} \qquad \gamma\colon\ v_i \to v_{-1/i}$$

$$\delta\colon\ v_i \to \begin{cases} v_{9i^3} & (i \notin Q) \\ v_{i^3/9} & (i \in Q) \end{cases} \qquad \varepsilon = \varepsilon_Q\colon\ v_i \to \begin{cases} v_i & (i \notin Q) \\ -v_i & (i \in Q) \end{cases}, \text{ and } \zeta = \zeta_T,$$

where $T = \{\infty, 0, 3, 15\}$ is the fixed set of δ, the appropriate Ξ being

$\{\{\infty, 0, 3, 15\}, \{14, 18, 8, 20\}, \{17, 4, 16, 10\}, \{11, 2, 13, 7\}, \{19, 6, 9, 5\}, \{22, 1, 12, 21\}\}$.

The operations α, β, γ plainly generate L, and α, β, γ, δ generate M. It then follows easily that α, β, γ, δ, ε generate N, and so α, β, γ, δ, ε, ζ generate $\cdot 0$, for we shall soon see that N is a maximal proper subgroup of $\cdot 0$.

6. *The order of* $\cdot 0$, *and the maximality of* N

Let H be any subgroup of $\cdot 0$ which strictly contains N.

THEOREM 4. *H is transitive on Λ_2.*

Proof. The orbits of N on Λ_2 are just the sets Λ_2^i ($i = 2, 3, 4$) ,and so the orbits of H must be unions of these. But the orbit of H containing Λ_2^4 cannot be Λ_2^4 itself, by Theorem 2, nor can it be $\Lambda_2^4 \cup \Lambda_2^2$ or $\Lambda_2^4 \cup \Lambda_2^3$, by Theorem 0, and so it must be the entire set Λ_2.

THEOREM 5. *H_x is transitive on $\Lambda_2(x)$, for any $x \in \Lambda_2$.*

Proof. If we take x as $v_\Omega - 4v_\infty$, N_x, and so H_x, contains the element α of order 23 which plainly fixes no member of $\Lambda_2(x)$, so that each orbit of $\Lambda_2(x)$ under H_x has order divisible by 23. But since H is transitive on Λ_2 the same must be true of any other $x \in \Lambda_2$, say $x = 4v_i + 4v_j$. In this case the orbits of N_x on $\Lambda_2(x)$ consist of:

2	points $\pm(4v_i - 4v_j)$
231.2^2	points $\pm 4v_h \pm 4v_k$ (h, i, j, k distinct)
330.2^7	points $2v_K\,\varepsilon_C$ ($K \in \mathscr{C}_8$, $\{i, j\} \cap K = \emptyset$, $C \in \mathscr{C}$)
77.2^6	points $2v_K\,\varepsilon_C$ ($\{i, j\} \subseteq K \in \mathscr{C}_8$, $C \in \mathscr{C}$, $\lvert C \cap \{i, j\}\rvert = 1$)
22.2^{11}	points $(4v_k - v_\Omega)\,\varepsilon_C$ ($k \in \Omega \setminus \{i, j\}$, $C \in \mathscr{C}$, $\lvert C \cap \{i, j\}\rvert = 1$).

(The numbers are easily found from Tables 1 and 2.)

The orbits of H_x on $\Lambda_2(x)$ must be unions of these sets and have orders divisible by 23, and since the above numbers are congruent to 2, 4, 12, 6, 22 (modulo 23) the only possibility is that H_x has but a single orbit on $\Lambda_2(x)$.

From now on we omit proofs of transitivity of subgroups of $\cdot 0$ on configurations of Λ since these proofs are usually similar to and simpler than the proofs of Theorems 4 and 5.

THEOREM 6. *The order of $\cdot 0$ is $196560.93150.2^{10}\lvert M_{22}\rvert$.*

THEOREM 7. *N is a maximal proper subgroup of $\cdot 0$.*

Proofs. The cardinal of Λ_2 is 196560 and for any $x \in \Lambda_2$ the cardinal of $\Lambda_2(x)$ is 93150, so that $|H| = 196560.93150.|H_{x,y}|$ for any orthogonal pair $x, y \in \Lambda_2$. If we take $x = 4v_i + 4v_j$, $y = 4v_i - 4v_j$, then any λ which fixes each of x and y fixes v_i, and so is in N, and so $H_{x,y} = N_{x,y} = N_{22}$, a group of order $2^{10}|M_{22}|$. Since the order of H is completely determined given only that $N \subset H$, there can be but one possibility for H, namely $\cdot 0$ itself.

7. *The group* $\cdot 1$

We define the group $\cdot 1$ as the quotient of $\cdot 0$ by its centre, $\{1, -1\}$. We examine the action of $\cdot 1$ on $\bar{\Lambda}_2$, the set of 98280 *diameters* of Λ_2, each diameter being a pair $\{x, -x\}$ $(x \in \Lambda_2)$.

THEOREM 8. $\cdot 0$ *acts transitively on ordered pairs of vectors of* Λ_2 *with any given scalar product.*

We omit the proof, as we promised. The number of $y \in \Lambda_2$ having scalar product -32, -16, -8, 0, 8, 16, 32 with a given $x \in \Lambda_2$ is

1, 4600, 47104, 93150, 47104, 4600, 1

respectively, and these are the only possible scalar products. The cases $x.y = \pm 32$ are trivial, and we have already tackled the case $x.y = 0$ in Theorem 5.

COROLLARY. $\cdot 1$ *acts on the* 98280 *diameters in such a way that the stabiliser of any diameter has orbits of orders* 1, 4600, 47104, 46575.

COROLLARY. $\cdot 1$ *acts primitively on* $\bar{\Lambda}_2$.

(For the order of any imprimitivity set would at the same time be a divisor of of 98280 and a sum of numbers in the previous corollary.)

THEOREM 9. $\cdot 1$ *is a simple group.*

Proof. We show that $\cdot 0$ has no normal subgroup H with $\{1, -1\} \subset H \subset \cdot 0$. Any such H must act transitively on $\bar{\Lambda}_2$, or else its orbits would be imprimitivity sets for $\cdot 1$. Hence $13 \mid |H|$. The Frattini argument now shows that $\cdot 0$ is the product of H and the normaliser in $\cdot 0$ of a Sylow 13-subgroup of H, and so one of these two groups has an element of order 23. But if the normaliser had an element of order 23, $\cdot 0$ would have a subgroup of order 13.23, and since any group of this order is cyclic this contradicts the remark after Theorem 0. Hence H has an element of order 23, and so $H \cap N$ is a normal subgroup of N of order divisible by 23, which normal subgroup must be N itself, whence by the maximality of N we have $H = N$, which is absurd, since N is not normal in $\cdot 0$.

7. *The group* $\cdot\infty$, *and some subgroups of* $\cdot 0$

We now turn our attention to the infinite group $\cdot\infty$ of *all* Euclidean congruences of Λ, including translations. It is easy to see that any finite subgroup of $\cdot\infty$ is isomorphic to a subgroup of $\cdot 0$. A simplex of one of the shapes indicated in Fig. 1 is said to have type *a*, *abc*, *abcαβγ*, *abcdeαβγδε* respectively, the line joining any

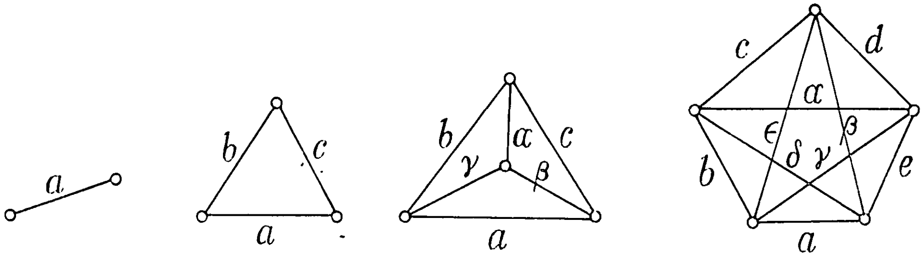

FIG. 1

two points in Fig. 1 being marked with the type of the corresponding vector. Usually this type symbol determines the class under $\cdot\infty$ and so serves as a name, and when it does not we adopt some convenient refinement. If S is the name of a simplex, we use $\cdot S$ for the subgroup of those elements of $\cdot\infty$ which fix every vertex of S, $*S$ for the subgroup of elements fixing S as a whole, and $!S$ for the subgroup fixing the centroid of S. Plainly $\cdot S \subseteq *S \subseteq !S$.

Any simplex S in Λ spans a sublattice L of Λ, and we use the name of S as a name for L. The group $\cdot S$ is more naturally associated with L than with S, and so we write $\cdot S = \cdot L$ and call these groups *lattice stabilisers.* If the lattice L is contained in just n copies of M, then the group $\cdot M$ has index n in $\cdot L$. Many results about subgroups of $\cdot 0$ reduce in this way to easy numerical calculations using Tables 1 and 2. We obtain in particular the orders of the subgroups listed in Table 3, and many inclusions between them. The reader should be warned that each lattice stabiliser has many different names corresponding to distinct spanning simplexes—thus the symbols $\cdot 432$ and $\cdot 632$ represent the same group.

Identifying these subgroups of $\cdot\infty$ with known groups is a haphazard process, and still incomplete. In some cases we use known characterisations of the groups concerned, and in others the identification is immediate when we choose simple coordinates for the vertices of S. Two cases are discussed in the next section.

The enumeration of sublattices which underlies Table 3 uses Theorem 10 below, whose proof uses only the numbers of vectors of types 2, 3, and 4.

THEOREM 10. *The midpoint of any interval of* Λ *is* either

(i) *a lattice point*;

(ii) *the midpoint of a unique interval of type* 2;

(iii) *the midpoint of a unique interval of type* 3; or

(iv) *the midpoint of just* 24 *mutually orthogonal intervals of type* 4.

No two of the possibilities can occur simultaneously.

COROLLARY. *Any interval of type n has some type* n_{ab}, *where* $a+b = \frac{1}{2}(n+k)$ *and k is one of* 0, 2, 3, 4 (*the values corresponding to the cases of Theorem* 10).

We discuss some of the more interesting subgroups. The groups $\cdot 2$ and $\cdot 3$ are new simple groups, and the groups $*2 = !2$ and $*3 = !3$ are extensions of these by automorphisms of period 2. The group $!4$ is N_{24}, while $\cdot 4$ is N_{23}. The groups $\cdot 322$ and $\cdot 332$ are the recently discovered simple groups of McLaughlin and of

Higman and Sims, and ·222 is apparently the simple group $PSU_6(2)$. The group !333 is an extension of an elementary abelian group of order 3^6 by a perfect group having a centre of order 2 and central quotient M_{12}. This group underlies Coxeter's [2] projective representation of M_{12} in the same way that !4 underlies Todd's [11] representation of M_{24}.

Professor J. G. Thompson has determined the centralisers of most of the elements of ·0, and has found several interesting subgroups in this way. In particular the centraliser of a certain element of order 3 is a cyclic group of order 6 extended by a simple group S of the same order as Suzuki's recently discovered simple group. The group S has the Hall–Janko simple group of order 604800 as a subgroup, and has also a simple subgroup of the same order as the group $G_2(4)$, which is known to be a subgroup of Suzuki's simple group. We might remark that the extension which appears in ·0 of a cyclic group of order 2 by the Hall–Janko group acts on a 6-dimensional space, so that the Hall–Janko group has a 6-dimensional projective representation.

8. *The Higman–Sims and McLaughlin groups*

D. G. Higman and C. C. Sims have described [5] a simple group of order $100|M_{22}|$ as the group of even permutations of a certain graph on 100 vertices, and J. McLaughlin has discovered a simple group of order 898128000 which is a group of automorphisms of a graph on 275 vertices. We here identify the Higman–Sims group with our ·332, and sketch the identification of McLaughlin's group with ·322.

Let $X = 4v_i+v_\Omega$, $Y = 4v_j+v_\Omega$, $Z = 0$, where i and j are distinct monads, so that XYZ is a triangle of type 332. Then there are exactly 100 points T for which $XYZT$ has type 332222, namely the point $P = 4v_i+4v_j$, 22 points $Q_k = v_\Omega-4v_k$ $(k\in\Omega\setminus\{i,j\})$, and 77 points $R_K = 2v_K$ $(\{i,j\}\subseteq K\in\mathscr{C}_8)$. If we say that two of these points are *incident* when their difference has type 3, then the incidences are (P, Q_k), (Q_k, R_K) $(k\in K)$, and $(R_K, R_{K'})$ $(K\cap K' = \{i,j\})$, and the incidence graph is visibly identical with the Higman–Sims graph.

Now $X-Y+P-Z = 8v_i$, so that the stabiliser in ·∞ of X, Y, Z, P is a subgroup of N, and in fact this stabiliser is the group M_{22} of permutations of Ω fixing i and j. We identify ·332 with the Higman–Sims group, and at the same time provide an easy proof of the latter's existence, by showing that ·∞ has operations fixing X, Y, Z but disturbing P. For let λ be an operation of ·∞ such that $X\lambda = 2v_C$, $Y\lambda = 2v_D$, $Z\lambda = 0$, where $C\in\mathscr{C}_{12}$, $D\in\mathscr{C}_{12}$, $C+D\in\mathscr{C}_8$. (Such λ exist by the transitivity of ·∞ on triangles of type ·332.) Then the subgroup H of those operations of N fixing each of $X\lambda, Y\lambda, Z\lambda$ fixes no one of the 100 points $T\lambda$ which differ by type 2 vectors from each of $X\lambda$, $Y\lambda$, $Z\lambda$, and so the group $\lambda H\lambda^{-1}$ has operations fixing each of X, Y, Z, but not P. (The argument has proved transitivity of ·∞ on tetrahedra of type 332222 given transitivity on triangles of type 332.)

Sims [10] has shown that the doubly transitive group on 176 letters described by G. Higman is isomorphic to the Higman–Sims group. G. Higman's group is the automorphism group of a 'geometry' of 176 'points' and 176 'quadrics', there being 50 points on each quadric and 50 quadrics through each point. Now there are 352 points W such that WX has type 3 while WY and WZ have type 2, and these naturally form 176 pairs $P_K = \{A_K, B_K\}$ $(K \in \mathscr{C}_8, K \cap \{i, j\} = \{i\})$, $A_K = 2v_K$, and $B_K = X - A_K$. There are similarly 176 pairs $Q_K = \{C_K, D_K\}$ obtained by interchanging the roles of i and j. If we take our ' points ' as the pairs P_K, and ' quadrics ' as pairs Q_K, and say P_K is on $Q_{K'}$ if and only if $|K \cap K'| = 2$, then we obtain G. Higman's geometry and another proof of the identity of his group with the Higman–Sims group.

If we consider instead of a triangle of type 322, we find that there are just 275 points which complete it to a tetrahedron of type 322222, and that the incidence graph (x and y are incident if and only if $x-y$ has type 3) is now McLaughlin's graph. The details of the identification are rather complicated, but the result is a fairly simple definition of McLaughlin's graph. If we take for our triangle XYZ $X = 0$, $Y = 4v_i + v_\Omega$, $Z = -4v_j + v_\Omega$ $(i \neq j)$, then the 275 points fall naturally into three sets—we have 22 points U_k $(k \in \Omega \setminus \{i, j\})$, 77 points V_K $(\{i, j\} \subseteq K \in \mathscr{C}_8)$, and 176 points $W_{K'}$ $(K' \in \mathscr{C}_8, \{i, j\} \cap K' = \{i\})$—and the incidences can be simply described by combinatorial conditions on k, K, K'.

9. *Miscellaneous remarks*

Let u_n be the number of lattice vectors of type n, and let $F(\tau) = \sum_0^\infty u_n q^n$, where $q = e^{2\pi i n \tau}$. Then from Hecke's work it follows that $F(\tau)$ is a modular form of dimension -12, and so is a linear combination of the basic forms $\sum_1^\infty \tau(n) q^n$ and $1 + c\sum_1^\infty \sigma_{11}(n) q^n$, where $\tau(n)$ is Ramanujan's famous function, $\sigma_{11}(n)$ is the sum of the 11th powers of the divisors of n, and $c = 65520/691$. (For the relevant modular form theory see [4] or [3], noting that [3] has the wrong value for c.) Since $u_0 = 1$, $u_1 = 0$, we obtain the exact formula

$$u_n = \frac{65520}{691}(\sigma_{11}(n) - \tau(n)).$$

Ramanujan's remarkable congruence $\tau(n) \equiv \sigma_{11}(n)$ (mod 691) is particularly evident, and indeed we can use the formula to find congruences for $\tau(n)$ modulo any prime power dividing g/c, where g is the order of $\cdot 0$. Thus to modulus 23 we have $u_n \equiv u_n(\alpha)$, where $u_n(\alpha)$ is the number of vectors of Λ_n which are fixed by the element α of order 23. But the fixed vectors of α are those of the shape $av_\infty + bv_{\Omega \setminus \infty}$, and since this has type n if and only if $16n = a^2 + 23b^2$ we obtain $\tau(n) \equiv \sigma_{11}(n) \equiv 0$ (mod 23) should n be a non-residue modulo 23.

A more exciting prospect is to use the modular form theory to determine new lattices and possibly therefore some new simple groups. I have already used the formula above together with the argument of Theorem 10 to show that Λ is characterised by the fact that (on a suitable scale) it is a unimodular lattice in which every squared length is an even integer greater than 2. It then follows from some work of V. Niemeier that there are just 24 even unimodular lattices in 24 dimensions.

TABLE 3

Name	*Order*	*Structure*	*Name*	*Order*	*Structure*
$\cdot 0$	$2^{22}\,3^{9}\,5^{4}\,7^{2}\,11.13.23$	New perfect	$\cdot 222$	$2^{15}\,3^{6}\,5.7.11$	$\mathrm{PSU}_6(2)$ (?)
$\cdot 1$	$2^{21}\,3^{9}\,5^{4}\,7^{2}\,11.13.23$	New simple	$\cdot 322$	$2^{7}\,3^{6}\,5^{3}\,7.11$	M^c
$\cdot 2$	$2^{18}\,3^{6}\,5^{3}\,7.11.23$	New simple	$\cdot 332$	$2^{9}\,3^{2}\,5^{3}\,7.11$	HS
$\cdot 3$	$2^{10}\,3^{7}\,5^{3}\,7.11.23$	New simple	$\cdot 333$	$2^{4}\,3^{7}\,5.11$	$3^5.M_{11}$
$\cdot 4$	$2^{18}\,3^{2}\,5.7.11.23$	$2^{11}\,M_{23}$	$.422$	$2^{17}\,3^{2}\,5.7.11$	$2^{10}.M_{22}$
$\cdot 5$	$2^{8}\,3^{6}\,5^{3}\,7.11$	$M^c.2$	$.432$	$2^{7}\,3^{2}\,5.7.11.23$	M_{23}
$\cdot 6_{22}$	$2^{16}\,3^{6}\,5.7.11$	$\mathrm{PSU}_6(2).2$ (?)	$\cdot 433$	$2^{10}\,3^{2}\,5.7$	$2^4.A_8$
$\cdot 6_{32}$	$2^{10}\,3^{3}\,5.7.11.23$	M_{24}	$\cdot 442$	$2^{12}\,3^{2}\,5.7$	$2^5.2^4.A_7$
$\cdot 7$	$2^{9}\,3^{2}\,5^{3}\,7.11$	HS	$\cdot 443$	$2^{7}\,3^{2}\,5.7$	$M_{21}.2$
$\cdot 8_{22}$	$2^{18}\,3^{6}\,5^{3}\,7.11.23$	$\cdot 2$	$\cdot 522$	$2^{7}\,3^{6}\,5^{3}\,7.11$	M^c
$\cdot 8_{32}$	$2^{7}\,3^{6}\,5^{3}\,7.11$	M^c	$\cdot 532$	$2^{8}\,3^{6}\,5.7$	$\mathrm{PSU}_4(3).2$
$\cdot 8_{42}$	$2^{15}\,3^{2}\,5.7$	$2^5.2^4.A_8$	$\cdot 533$	$2^{4}\,3^{2}\,5^{3}\,7$	$\mathrm{PSU}_3(5)$
$\cdot 9_{33}$	$2^{5}\,3^{7}\,5.11$	$3^5.M_{11}.2$	$\cdot 542$	$2^{7}\,3^{2}\,5.7.11$	M_{22}
$\cdot 9_{42}$	$2^{7}\,3^{2}\,5.7.11.23$	M_{23}	$\cdot 633$	$2^{6}\,3^{3}\,5.11$	M_{12}
$\cdot 10_{33}$	$2^{10}\,3^{2}\,5^{3}\,7.11$	$HS.2$	$*2 = !2$	$2^{19}\,3^{6}\,5^{3}\,7.11.23$	$(\cdot 2).2$
$\cdot 10_{42}$	$2^{17}\,3^{2}\,5.7.11$	$2^{10}.M_{22}$	$*3 = !3$	$2^{11}\,3^{7}\,5^{3}\,7.11.23$	$(\cdot 3).2$
$\cdot 11_{43}$	$2^{10}\,3^{2}\,5.7$	$2^4.A_8$	$*4$	$2^{19}\,3^{2}\,5.7.11.23$	$(\cdot 4).2$
$\cdot 11_{52}$	$2^{8}\,3^{6}\,5.7$	$\mathrm{PSU}_4(3).2$	$!4$	$2^{22}\,3^{3}\,5.7.11.23$	$2^{12}.M_{24}$
			$!333$	$2^{7}\,3^{9}\,5.11$	$3^6.2.M_{12}$
			$!442$	$2^{15}\,3^{4}\,5.7$	$2^5.2^4.A_9$

HS, M^c, p^n denote respectively the Higman–Sims group, the McLaughlin group, and the elementary group of order p^n. $A.B$ denotes an extension of the group A by the group B. The notation is otherwise standard.

This work can be regarded as a theorem on even unimodular quadratic forms by passing to the ‘norm-forms’ of the lattices concerned.

The so-called ‘mass-formula’ of Siegel [9] gives the sum of the reciprocals of the orders of the groups of automorphs of these forms, which is approximately 10^{-14}, so that each of the groups has order at least 10^{14}. (This gives another proof of Theorem 3.) Unfortunately the corresponding constant in 32 dimensions (the next similar case) is approximately 10^8, so that there are at least 10^8 even unimodular lattices in this dimension, and most of them could have very small groups. We must either add further conditions or search for lattices of other shapes. I have not yet had much success with these ideas, but have high hopes of the method.

References

1. R. D. Carmichael, *Introduction to the theory of groups of finite order* (New York, 1937).
2. H. S. M. Coxeter, *Proc. Roy. Soc. Ser. A*, 247 (1958), 279–293.
3. R. C. Gunning, *Lectures on modular forms* (Princeton, 1962).
4. E. Hecke, *Math. Ann.*, 114 (1937), 1-29 and 316–351 (*or Math. Werke*, 644–707).
5. D. G. Higman and C. C. Sims, “ A simple group of order 44,352,000 ” (unpublished).
6. John Leech, *Canad. J. Math.*, 16 (1964), 657-682.
7. ———, *Canad. J. Math.*, 19 (1967), 251–267.
8. E. Mathieu, *J. Math. Pures. Appl.*, 18 (1873), 25–46.
9. C. L. Siegel, *Danske Vid. Selskab Mat-fys. Medd.*, 34 (1964), Nr 6 (*or Gesamm Abh.*, 443–458).
10. C. C. Sims, “ On the isomorphism between two groups of order 44,352,000 ” (unpublished).
11. J. A. Todd, *Ann. di Math. Pura ed Appl.* (IV) LXXI, 199-238.
12. E. Witt, *Abh. Math. Sem. Univ. Hamburg*, 12 (1938), 256–264.
13. ———, *Abh. Math. Sem. Univ. Hamburg*, 12 (1938), 265–274.

University of Cambridge.