Chapter 5

Sporadic groups

5.1 Introduction

In this chapter we introduce the 26 sporadic simple groups. These are in many ways the most interesting of the finite simple groups, but are also the most difficult to construct. These groups may be roughly divided into five types, as follows:

- the five Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24}; these are permutation groups on 11, 12, 22, 23, or 24 points;
- the seven Leech lattice groups Co_1, Co_2, Co_3, McL, HS, Suz, J_2; these are matrix groups in dimension at most 24;
- the three Fischer groups Fi_{22}, Fi_{23}, Fi_{24}'; these are automorphism groups of rank 3 graphs;
- the five Monstrous groups $\mathbb{M}$, $\mathbb{B}$, Th, HN, He; these are defined in terms of centralizers of elements in the Monster; the Monster involves all the 20 sporadic groups mentioned so far;
- the six pariahs J_1, J_3, J_4, O'N, Ly, Ru; these are oddments which do not fit nicely into the above families, and have little to do even with each other.

5.2 The large Mathieu groups

5.2.1 The hexacode

To construct the Mathieu groups we start by defining the *hexacode*. This is the 3-dimensional subspace of $\mathbb{F}_4^6$ spanned by the vectors $(\omega,\overline{\omega},\overline{\omega},\omega,\overline{\omega},\omega)$, $(\overline{\omega},\omega,\omega,\overline{\omega},\overline{\omega},\omega)$ and $(\overline{\omega},\omega,\overline{\omega},\omega,\omega,\overline{\omega})$, where $\mathbb{F}_4=\{0,1,\omega,\overline{\omega}\}$ is the field of order 4. Since the sum of these three vectors is $(\omega,\overline{\omega},\omega,\overline{\omega},\omega,\overline{\omega})$, there is an obvious symmetry group $3 \times S_4$ generated by scalar multiplications and the coordinate permutations $(1,2)(3,4)$, $(1,3,5)(2,4,6)$ and $(1,3)(2,4)$. The non-zero vectors fall into four orbits under this group, as follows:

Orbit representative	Length of orbit
$(1,1,1,1,0,0)$	9
$(\omega,\overline{\omega},\omega,\overline{\omega},\omega,\overline{\omega})$	12
$(1,1,\omega,\omega,\overline{\omega},\overline{\omega})$	6
$(0,1,0,1,\omega,\overline{\omega})$	36

(5.1)

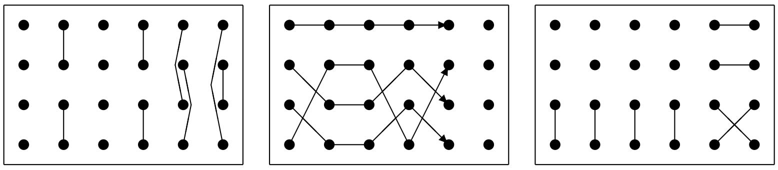
The group of automorphisms of this code is defined to be the set of monomial permutations of the coordinates which fix the code as a set. It is immediate that any diagonal symmetry is a scalar, as it maps each of $(1,1,1,1,0,0)$ and $(0,0,1,1,1,1)$ to a scalar multiple of itself. Modulo scalars, we can extend the group S_4 of permutations to A_6 by adjoining the map

$$(x_1,\dots,x_6) \quad\mapsto\quad (\omega x_1, \overline{\omega} x_2, x_3, x_6, x_4, x_5). \tag{5.2}$$

On the other hand, no automorphism induces an odd permutation, for if so, then looking at the images of $(1,1,1,1,0,0)$ and $(0,0,1,1,1,1)$ we deduce that the coordinate permutation (5,6) is an automorphism, but $(0,1,0,1,\overline{\omega},\omega)$ is not in the hexacode. However, odd permutations are allowed provided they are always followed by the field automorphism $\omega \mapsto \overline{\omega}$. This gives rise to a group $3{}^{\cdot}S_6$ of *semi-automorphisms* of the hexacode.

5.2.2 The binary Golay code

We next construct a set of 24 points, labelled (i,x) where i is an integer from 1 to 6 (corresponding to one of the six coordinates of the hexacode) and $x \in \mathbb{F}_4$. Let the hexacode act on this set in the 'obvious' way, by addition: a hexacode word $(x_1,\dots,x_6)$ maps (i,x) to $(i, x+x_i)$. Similarly the group $3{}^{\cdot}S_6$ of semi-automorphisms acts on the set in the 'obvious' way: if the group element maps 1 in the ith coordinate to λ in the jth coordinate, then it maps (i,x) to $(j,\lambda x)$. These 24 points are generally arranged in a 6×4 array with columns labelled 1 to 6 and rows labelled 0, 1, ω, $\overline{\omega}$ (called the MOG, or Miracle Octad Generator, by Curtis, who first used such an array as a practical tool for calculating in the Golay code) where these symmetries can be conveniently visualised. For example, the group $2^6{:}3{}^{\cdot}S_6$ may be generated by the following permutations of 24 points (where cycles of length 5 are represented by arrows, and it is understood that the head of the arrow maps back to the start).



(5.3)

The largest Mathieu group M_{24} may be viewed as a permutation group on these 24 points, containing the group $2^6{:}3{}^{\cdot}S_6$ just constructed as a maximal subgroup. To effect this construction we shall define the *(extended binary) Golay code* as a set of binary vectors of length 24, with coordinates indexed by the 24 points (i, x). For convenience, we identify each vector with its support (that is, the set of points where it has coordinate 1). The group M_{24} will then be defined as the group of permutations which preserve this set of vectors.

From each hexacode word $(x_1, \ldots, x_6)$ we derive 64 words in the Golay code, as follows. Each coordinate x_i corresponds either to an odd-order set, $\{(i, x_i)\}$ or its complement $\{(i, x) \mid x \neq x_i\}$, or to an even-order set, $\{(i, x_i)\} \triangle \{(i, 0)\}$ (where $\triangle$ denotes symmetric difference of sets) or its complement $\{(i, x) \mid 0 \neq x \neq x_i \text{ or } 0 = x = x_i\}$. Now impose the further conditions that all 6 coordinates have the same parity, and that this parity is equal to the parity of the number of $(i, 0)$ in the set, i.e. the parity of the top row. Thus we may choose the set corresponding to the first coordinate in 4 ways, and the next four coordinates in 2 ways each, and the last set is determined. As an example, here are three Golay code words corresponding to the hexacode word $(0, 1, 0, 1, \omega, \overline{\omega})$.

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	1			1
1		1	1	1	1
1		1	1		

(5.4)

It is straightforward to check from this definition that the Golay code is closed under vector addition (symmetric difference of sets), and so forms a subspace of dimension 12 of $\mathbb{F}_2^{24}$. Moreover, the whole set (corresponding to the vector with 24 coordinates 1) satisfies the conditions to be in the Golay code, so the code is closed under complementation. In total there are 759 sets of size 8 (called *octads*), falling into three orbits under the action of the group $2^6{:}3{}^{\cdot}S_6$. These three orbits are represented by $\{(i, 0)\} \triangle \{(0, x)\}$ (384 octads), $\{(i, x) \mid i \leq 4, x = 0 \text{ or } 1\}$ (360 octads), and $\{(i, x) \mid i \leq 2\}$ (15 octads), or in pictures:

	1	1	1	1	1
1					
1					
1					

1	1	1	1		
1	1	1	1		

1	1				
1	1				
1	1				
1	1				

(5.5)

Hence, by complementation, there are 759 sets of size 16 in the code. All the remaining sets have size 12: there are 2576 of them, lying in three orbits, of lengths $576 + 720 + 1280$, under $2^6{:}3^{\cdot}S_6$. In pictures:

$$\begin{array}{|cccccc|}\hline 1&1&1&1&1&1\\ &&&&&\\ 1&&1&&1&\\ &1&&1&&1\\ \hline\end{array}\quad \begin{array}{|cccccc|}\hline 1&1&1&&&\\ &&&1&1&1\\ &&&1&1&1\\ &&&1&1&1\\ \hline\end{array}\quad \begin{array}{|cccccc|}\hline 1&1&1&&&1\\ 1&1&1&&&1\\ &&&1&&1\\ &&&1&&1\\ \hline\end{array} \tag{5.6}$$

Thus the code has *weight distribution* $0^1 8^{759} 12^{2576} 16^{759} 24^1$.

Now consider the 2^{12} cosets of the Golay code in $\mathbb{F}_2^{24}$, and look for coset representatives of minimal weight (i.e. with as few non-zero coordinates as possible). Certainly the difference (i.e. sum) of two representatives for the same coset is an element of the code, so has weight at least 8. Therefore the vectors of weight 0, 1, 2, and 3 are unique in their cosets, so there are $1 + 24 + \frac{24.23}{2} + \frac{24.23.22}{2.3} = 2325$ such cosets. Two distinct vectors of weight at most 4 in the same coset must be disjoint vectors of weight 4, so there can be at most 6 such vectors in each coset. Therefore there are at least $\frac{24.23.22.21}{4.3.2.6} = 1771$ such cosets. But now we have accounted for at least $2325 + 1771 = 4096 = 2^{12}$ cosets. In particular, every vector of weight 4 determines a partition of the 24 points into 6 sets of size 4. These partitions are called *sextets*, consisting of six *tetrads*.

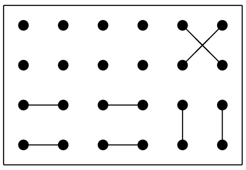
Now we can explicitly calculate these sextets, and we find that there are just four orbits under the group $2^6{:}3^{\cdot}S_6$. The first orbit, of size 1, is the sextet consisting of the 6 columns of the MOG. The second orbit, of size 90, consists of sextets defined by two points in one column and two points in another. Every tetrad in such a sextet splits across two columns in this way, so we write its column distribution as $(22, 22, 22, 22, 22, 22)$. The third orbit, of size 240, consists of sextets defined by three points in one column and one in another column. The column distribution of these sextets is $(31, 31, 1111, 1111, 1111, 1111)$. The fourth orbit, of size 1440, consists of sextets defined by two points in one column and two other points in two other columns. These sextets have column distribution $(211, 211, 211, 211, 1111, 1111)$. This accounts for all 1771 sextets. In pictures, representatives of the three non-trivial orbits are

$$\begin{array}{|cc|cc|cc|}\hline 1&1&3&3&5&5\\ 1&1&3&3&5&5\\ \hline 2&2&4&4&6&6\\ 2&2&4&4&6&6\\ \hline\end{array}\quad \begin{array}{|cccccc|}\hline 1&2&3&3&3&3\\ 2&1&4&4&4&4\\ 2&1&5&5&5&5\\ 2&1&6&6&6&6\\ \hline\end{array}\quad \begin{array}{|cccccc|}\hline 1&1&1&2&5&6\\ 1&2&2&2&4&3\\ 3&5&6&4&3&6\\ 4&6&5&3&5&4\\ \hline\end{array} \tag{5.7}$$

where the six tetrads of each sextet are labelled by the numbers 1 up to 6.

5.2.3 The group M_{24}

By checking the action on a basis of the Golay code, it is easy to verify that the element

$\alpha =$  (5.8)

fixes the code. Moreover, α fuses the four orbits of $2^6{:}3{}^{\cdot}S_6$ on sextets. Since this group is the full sextet stabilizer, it follows that the order of M_{24} is

$$|\mathrm{M}_{24}| = 1771.2^6.3.6! = 244823040 = 2^{10}.3^3.5.7.11.23. \tag{5.9}$$

It follows almost immediately from the transitivity of M_{24} on sextets that it is 5-transitive on points. For we can take the sextet defined by the first four points to any sextet, and then the sextet stabilizer is transitive on its six tetrads. Moreover, fixing the tetrad we have a full S_4 of permutations of the tetrad. Finally, the pointwise stabilizer of this tetrad is a group $2^4{:}A_5$ which is visibly transitive on the remaining 20 points.

Consequently, every set of five points is contained in an octad, but since $\binom{24}{5} = 759\binom{8}{5}$, this octad is unique. (Alternatively, this follows from the fact that the sum of two octads is in the code, so the octads cannot intersect in more than four points.) This combinatorial property is the defining property of a *Steiner system* $S(5,8,24)$. More generally, a Steiner system $S(t,k,v)$ is a system of special k-subsets of a set of size v, with the property that every set of size t is contained in a unique special k-subset (called a *block*). It is easy to see that the (extended binary) Golay code gives rise to a Steiner system $S(5,8,24)$, but the converse is not obvious. It follows however from the fact that, up to relabelling the points, there is a unique $S(5,8,24)$. The proof of uniqueness also gives an alternative proof that M_{24} is 5-transitive. We now sketch this proof.

5.2.4 Uniqueness of the Steiner system $S(5,8,24)$

If $\{1,2,3,4,5,6,7,8\}$ is an octad, the Steiner system property implies that the number of octads containing $\{1,\ldots,i\}$ is $\binom{24-i}{5-i}\Big/\binom{8-i}{5-i}$ for $0 \le i \le 4$ and is 1 for $5 \le i \le 8$. These numbers are 759, 253, 77, 21, 5, 1, 1, 1, 1 for $i = 0,\ldots,8$, respectively. Hence the number of octads not containing the point 1 is $759-253 = 506$, and so on. We complete the *Leech triangle* (see Figure 5.1), in which the ith entry in the jth row is the number of octads intersecting $\{1,\ldots,j-1\}$ in exactly $\{1,\ldots,i-1\}$, using this property that each entry is the sum of the two nearest entries in the row below (cf. Pascal's triangle). In particular we see from the

$$
\begin{array}{ccccccccccccccccc}
 & & & & & & & & 759 & & & & & & & & \\
 & & & & & & & 506 & & 253 & & & & & & & \\
 & & & & & & 330 & & 176 & & 77 & & & & & & \\
 & & & & & 210 & & 120 & & 56 & & 21 & & & & & \\
 & & & & 130 & & 80 & & 40 & & 16 & & 5 & & & & \\
 & & & 78 & & 52 & & 28 & & 12 & & 4 & & 1 & & & \\
 & & 46 & & 32 & & 20 & & 8 & & 4 & & 0 & & 1 & & \\
 & 30 & & 16 & & 16 & & 4 & & 4 & & 0 & & 0 & & 1 & \\
30 & & 0 & & 16 & & 0 & & 4 & & 0 & & 0 & & 0 & & 1
\end{array}
$$

Figure 5.1: The Leech triangle

bottom row of the triangle that two distinct octads intersect in 0, 2 or 4 points. It follows easily that every set of 4 points determines a *sextet*, with the properties described above, and that every octad is either the sum of two tetrads of the sextet, or cuts across these tetrads with intersections of sizes $(3, 1^5)$ or $(2^4, 0^2)$.

Now we might as well arrange our first sextet to consist of the six columns of a MOG array, and choose an octad of shape $(3, 1^5)$ to be the first column plus the top row. Indeed, we can arrange the points so that the sextet containing the tetrad consisting of the last four points in the top row also contains the tetrads consisting of the last four points in the other three rows. These now correspond to hexacode words $(0, 0, 1, 1, 1, 1)$ and its scalar multiples, and the sextet is the second one displayed in Equation 5.7. Next consider the sextet containing the tetrad which consists of the bottom three points of the first column and the second point of the second column. Since the octads containing this tetrad cut across both of our other sextets with the distribution $(3, 1^5)$, we can choose one of them to correspond to the hexacode word $(0, 1, 0, 1, \omega, \overline{\omega})$. Then using the fact that octads intersect evenly, the others correspond to $(0, 1, 1, 0, \overline{\omega}, \omega)$ and (without loss of generality) $(0, 1, \omega, \overline{\omega}, 0, 1)$ and $(0, 1, \overline{\omega}, \omega, 1, 0)$. We now have most of the structure of the hexacode and it is routine to complete the argument.

5.2.5 Simplicity of M_{24}

To prove that M_{24} is simple we can use Iwasawa's Lemma as with the classical groups. It is easy to see that the action of M_{24} on the 1771 sextets is primitive, since the sextet stabilizer has orbits of lengths $1 + 90 + 240 + 1440$ on the 1771 sextets. Moreover, the sextet stabilizer $2^6{:}3{}^{\cdot}S_6$ has a normal abelian subgroup of order 2^6, and the elements of this 2^6 are easily seen to be commutators of elements of $2^6{:}3{}^{\cdot}S_6$. The latter group is generated by conjugates of the third element of Equation 5.3, and to generate M_{24} we need only adjoin the element α defined in Equation 5.8. Since both of these elements are in the normal 2^6 of the stabilizer of the first sextet of Equation 5.7, we have verified all the hypotheses of Iwasawa's Lemma, and therefore conclude that M_{24} is simple.

5.2.6 Subgroups of M_{24}

The stabilizer of a point is by definition the group M_{23}, which therefore has order $|\mathrm{M}_{24}|/24 = 10200960$, while the stabilizer of two points is the group M_{22} of order $|\mathrm{M}_{23}|/23 = 443520$. These three groups M_{22}, M_{23} and M_{24} are collectively known as the large Mathieu groups, and were first described by Mathieu in 1873. The stabilizer of three points similarly has order $|\mathrm{M}_{22}|/22 = 20160$, and is sometimes called M_{21}, but turns out to be isomorphic to $\mathrm{PSL}_3(4)$. This isomorphism can be seen by showing that the Golay code structure gives rise to a projective plane of order 4 on the 21 remaining points. Of course, the multiple transitivity of M_{24} shows that these groups extend to subgroups $\mathrm{M}_{22}{:}2$ and $\mathrm{PSL}_3(4){:}S_3$, both of which are in fact maximal subgroups of M_{24}.

The stabilizer of an octad has order $|\mathrm{M}_{24}|/759 = 32560$. Now if all 8 points of the octad are fixed, then we may assume these are the first two columns of the MOG, so by looking inside the sextet stabilizer we see that there is only an elementary abelian group of order 16 left. Modulo this, the permutation action on the octad has order 20160, and is therefore A_8. Thus the octad stabilizer is 2^4A_8. Indeed, by fixing one of the 16 points outside the octad, we see a subgroup A_8, so the extension splits (i.e. the octad stabilizer is a semidirect product $2^4{:}A_8$). Moreover, the 16 points outside the octad now have a vector space structure on them, and we see the isomorphism $A_8 \cong \mathrm{L}_4(2)$.

The stabilizer of one of the Golay code words of weight 12 (a *dodecad*) is a group of order $|\mathrm{M}_{24}|/2576 = 95040$, and is the group M_{12}. The fact that M_{12} is a subgroup of M_{24} was not known to Mathieu, and was first discovered by Frobenius. In fact, it is not maximal, as the complement of a dodecad is another dodecad, and since M_{24} is transitive on dodecads, we have a subgroup $\mathrm{M}_{12}{:}2$ (which is, in fact, maximal) fixing the pair of complementary dodecads.

Fixing a point in one of these dodecads we obtain the smallest Mathieu group, M_{11} of order $|\mathrm{M}_{12}|/12 = 7920$.

In fact, there are just three more classes of maximal subgroups of M_{24} (for a complete list of the maximal subgroups of all the Mathieu groups, see Table 5.1). One is the stabilizer of a set of three mutually disjoint octads (such as the three bricks of the MOG: these *bricks* are the leftmost 8 points, the rightmost 8 points, and the middle 8 points), and has the shape $2^6{:}(\mathrm{L}_3(2) \times S_3)$, with the quotient S_3 acting as permutations of the three octads. Another is the group $\mathrm{PSL}_2(23)$, which was known to Mathieu, and was in a sense the basis of his original construction. (He first constructed M_{23} and then extended the maximal subgroup 23:11 to $\mathrm{PSL}_2(23)$ to generate M_{24}. It is not easy to prove that M_{24} exists from this definition, and it appears that Mathieu's construction did not entirely convince his contemporaries. Even 30 years later it was possible for Miller to publish a paper purporting to prove that M_{24} did not exist—although, to be fair, he quickly realised his mistake and retracted the claim. The first really convincing construction was that of Witt in 1938—his paper is well worth reading, even today, for those who read German.)

Another way to see the subgroup $PSL_2(23)$ is to construct the Golay code by taking the 24 points to be the points of the projective line $\mathbb{F}_{23} \cup \{\infty\}$, and defining the code to be spanned by the set $\{x^2 \mid x \in \mathbb{F}_{23}\}$ and its images under $t \mapsto t+1$, and complementation. It takes a little bit of work to show that this defines a code with the same weight distribution as the Golay code, and then the uniqueness of the Steiner system $S(5, 8, 24)$ implies it is isomorphic to the Golay code. The group $PSL_2(23)$ of symmetries generated by $t \mapsto t+1$, $t \mapsto 2t$, and $t \mapsto -1/t$ can be extended to M_{24} by adjoining the map $t \mapsto t^3/9$ for t a quadratic residue or 0, and $t \mapsto 9t^3$ for t a non-residue or ∞, i.e. the permutation

$$(1, 18, 4, 2, 6)(8, 16, 13, 9, 12)(5, 21, 20, 10, 7)(11, 19, 22, 14, 17).$$

A correspondence with the MOG may be given by labelling the points of the MOG with the points of the projective line as follows:

$$\begin{array}{|cccccc|} 0 & \infty & 1 & 11 & 2 & 22 \\ 19 & 3 & 20 & 4 & 10 & 18 \\ 15 & 6 & 14 & 16 & 17 & 8 \\ 5 & 9 & 21 & 13 & 7 & 12 \end{array} \qquad (5.10)$$

The last, and smallest, maximal subgroup of M_{24} is a subgroup $PSL_2(7)$ of order 168. As this contains a subgroup S_4 which commutes with an element of order 2 in M_{24}, this leads to a way of generating M_{24} in a nice symmetric way with seven elements of order 2.

5.3 The Leech lattice and the Conway group

5.3.1 The Leech lattice

We construct the biggest Conway group $2{\cdot}Co_1$ (a double cover of the simple group Co_1) as a group of 24×24 real matrices. At the same time we construct a *lattice* (i.e. a discrete set of vectors closed under addition and subtraction) which is invariant under the group, in order to determine the order of the group and other properties. The process is analagous to the construction of M_{24} and the Golay code, using the subgroup $2^6{:}3{\cdot}S_6$ derived from the hexacode. Here we use instead a group $2^{12}{:}M_{24}$ derived from the Golay code to help with the construction.

There is an obvious action of M_{24} on 24-space, in which it permutes the coordinate vectors naturally. There is also an action of the Golay code itself, whereby a codeword acts by negating all the coordinates corresponding to a 1 in

Table 5.1: Maximal subgroups of the Mathieu groups

Group	M_{24}	M_{23}	M_{22}	M_{12}	M_{11}
cocode subgroups	M_{23}	M_{22}	$L_3(4)$	M_{11}	$A_6{\cdot}2$
	$M_{22}{:}2$	$L_3(4){:}2$	$2^4{:}S_5$	$A_6{\cdot}2^2$	$3^2{:}SD_{16}$
	$L_3(4){:}S_3$	$2^4{:}(3\times A_5){:}2$		$3^2{:}2S_4$	$2S_4$
	$2^6{:}3S_6$			$2^{1+4}S_3$	
				4^2D_{12}	
code subgroups	$2^4{:}A_8$	$2^4{:}A_7$	$2^4{:}A_6$	M_{11}	$L_2(11)$
	$M_{12}{:}2$	A_8	A_7	$A_6{\cdot}2^2$	S_5
	$2^6{:}(L_3(2)\times S_3)$	M_{11}	A_7	$3^2{:}2S_4$	
			$2^3{:}L_3(2)$		
			$A_6{\cdot}2$		
			$L_2(11)$		
others	$L_2(23)$	$23{:}11$		$L_2(11)$	
	$L_2(7)$			$2\times S_5$	
				$A_4\times S_3$	

the word. Thus an octad acts by negating an 8-space, for example. Taking both groups together we obtain a group $2^{12}{:}M_{24}$ acting monomially on 24-space.

The Leech lattice is named after John Leech although it was apparently first discovered by Witt in 1940. It may be defined as the $\mathbb{Z}$-linear combinations of the $1104 + 97152 + 98304 = 196560$ images under the group $2^{12}{:}M_{24}$ of the following vectors

$$\begin{array}{|cc|cc|cc|} \hline 4 & 4 & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ \hline \end{array} \quad \begin{array}{|cc|cc|cc|} \hline 2 & 2 & & & & \\ 2 & 2 & & & & \\ 2 & 2 & & & & \\ 2 & 2 & & & & \\ \hline \end{array} \quad \begin{array}{|cc|cc|cc|} \hline -3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ \hline \end{array} \tag{5.11}$$

More helpfully, it may be defined as the set of all integral vectors $(x_1, \ldots, x_{24})$ (i.e. $x_i \in \mathbb{Z}$) such that either all the x_i are even or they are all odd, and congruent modulo 2 to $\frac{1}{4}$ of the sum of the coordinates, and additionally the residue classes modulo 4 are in the Golay code. Thus

$$\begin{aligned} x_i &\equiv m \bmod 2 \\ \sum_{i=1}^{24} x_i &\equiv 4m \bmod 8 \\ \text{for each } k\text{, the set } \{i \mid x_i &\equiv k \bmod 4\} \text{ is in the Golay code} \end{aligned} \tag{5.12}$$

To show that these two definitions are equivalent we first show that all the spanning vectors in the first definition satisfy the congruence conditions in the second definition. This is a straightforward exercise. Conversely, suppose that x is a vector satisfying the conditions of the second definition. If the coordinates of x are odd, subtract the vector $(-3, 1^{23})$ to get a new vector x with even coordinates, still satisfying the conditions. If now x has some coordinates not divisible by 4, we can subtract some octad vectors (i.e. vectors of shape $(2^8, 0^{16})$) until all the coordinates are divisible by 4, and the new vector x still satisfies the conditions. Now the sum of the coordinates is congruent to 0 modulo 8, so the vector x is a sum of vectors of the shape $(\pm 4, \pm 4, 0^{22})$. Hence x is in the lattice spanned by the vectors given in the first definition.

Now it is easy to see that the 196560 vectors listed above are the only vectors of smallest norm in the lattice. (We scale the usual norm by dividing by 8, so that these vectors have norm (i.e. squared length) 4. This is the smallest scale on which all inner products of vectors in the lattice are integers.) Similarly, the vectors of norm 6 fall into four orbits under the group $2^{12}{:}\mathrm{M}_{24}$, with lengths $2576.2^{11} = 5275648$, $\binom{24}{3}.2^{12} = 8290304$, $759.16.2^8 = 3108864$, and $24.2^{12} = 98304$ (making 16773120 in all), and representatives as follows:

$$
\begin{array}{|cc|cc|cc|}
\hline
2 & 2 & 2 & & & \\
 & & & 2 & 2 & 2 \\
 & & & 2 & 2 & 2 \\
 & & & 2 & 2 & 2 \\
\hline
\end{array}
\qquad
\begin{array}{|cc|cc|cc|}
\hline
-3 & -3 & -3 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
\hline
\end{array}
$$
$$
\begin{array}{|cc|cc|cc|}
\hline
2 & -2 & 4 & & & \\
2 & 2 & & & & \\
2 & 2 & & & & \\
2 & 2 & & & & \\
\hline
\end{array}
\qquad
\begin{array}{|cc|cc|cc|}
\hline
5 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
\hline
\end{array}
\tag{5.13}
$$

The 398034000 vectors of norm 8 similarly fall into eight orbits under the group $2^{12}{:}\mathrm{M}_{24}$.

Let Λ denote the Leech lattice. As an abelian group under addition, Λ is isomorphic to $\mathbb{Z}^{24}$, so that $\Lambda/2\Lambda \cong 2^{24}$, a vector space of dimension 24 over $\mathbb{F}_2$. In particular there are just 2^{24} congruence classes mod 2Λ of vectors in Λ. These are just the cosets of 2Λ in Λ. If x and y are in the same congruence class, then $x \pm y$ both lie in 2Λ, so have norm 0 or at least 16. Therefore the sum of the norms of x and y must be at least 16, unless $x = \pm y$. In particular, the vectors of norms 0, 4, and 6 are congruent only to their negatives, while two vectors of norm 8 can be congruent only if they are either negatives of each other, or orthogonal to each other. Since orthogonal vectors are linearly independent, we have accounted for at least

$$
\begin{aligned}
1 + 196560/2 + 16773120/2 + 398034000/48 &= 16777216 \\
&= 2^{24}
\end{aligned}
\tag{5.14}
$$

congruence classes.

5.3.2 The Conway group Co_1

Thus all the vectors of norm 8 in the Leech lattice fall into congruence classes of 48 pairs of mutually orthogonal vectors (which we call *coordinate frames* or *crosses*, or sometimes *double bases*), and therefore there are exactly $398034000/48 = 8292375$ such crosses. Since the stabilizer of a cross is just $2^{12}{:}\mathrm{M}_{24}$ (as is clear from the second definition of the Leech lattice), we only need to prove transitivity on the crosses in order to compute the order of the automorphism group as $8292375.2^{12}.|\mathrm{M}_{24}|$. Clearly this automorphism group has a centre of order 2 generated by the scalar -1. The quotient by the centre is therefore a group Co_1 of order $4\,157\,776\,806\,543\,360\,000 = 2^{21}.3^9.5^4.7^2.11.13.23$.

To prove transitivity on the crosses it is sufficient to exhibit an element which fuses the orbits of the monomial group $2^{12}{:}\mathrm{M}_{24}$. Alternatively, a non-constructive proof can be obtained by showing that any *even integral lattice* (i.e. a lattice such that all inner products are integers, and all norms are even integers) containing the given numbers of vectors of all norms up to and including 8, is isomorphic to the Leech lattice. In effect this gives us a third definition of the Leech lattice, which we record formally in the following Theorem.

THEOREM 1. *If* Λ *is a* 24*-dimensional even integral lattice containing no vectors of norm* 2*,* 196560 *vectors of norm* 4*,* 16773120 *vectors of norm* 6 *and* 398034000 *vectors of norm* 8*, then* Λ *is isomorphic to the Leech lattice.*

Proof. The same counting argument as above (see Equation 5.14) shows that in any such lattice the vectors of norm 8 form coordinate frames. Writing the lattice with respect to a basis such that such a coordinate frame consists of the vectors of shape $(\pm 8, 0^{23})$, we see that $(\pm 8, \pm 8, 0^{22})$ is in twice that lattice, so that $(\pm 4, \pm 4, 0^{22})$ belongs to the lattice. Since all inner products are integral (after dividing by 8), it follows that for any vector in the lattice, all its coordinates are integers, and are congruent, to m say, modulo 2. Hence all vectors of shape $(\pm 4, \pm 4, \pm 4, \pm 4, 0, \ldots, 0)$ belong to the lattice and also form coordinate frames. These vectors therefore determine splittings of the 24 coordinates into sextets, or equivalently, every set of five coordinates determines an octad. Thus we obtain the structure of a Steiner system $S(5, 8, 24)$ on the 24 coordinates. Using the fact that this Steiner system is essentially unique (see Section 5.2.3) we may label the vectors of our coordinate frame so that it is the same Steiner system as before. Moreover, vectors of shape $(\pm 2^8, 0^{16})$ with 2s on an octad are also in the lattice (with signs yet to be determined). Since there are no vectors of norm less than 4, and there are 196560 vectors of norm 4, there must be some vectors of norm 4 with odd coordinates. Changing signs on some coordinates if necessary, we may assume this vector is $(-3, 1^{23})$. Therefore the octad vectors have an even number of $-$ signs, and we have the same Leech lattice as we had before. $\square$

5.3.3 Simplicity of Co_1

We can prove that Co_1 is simple using Iwasawa's Lemma again. To do this we first show that the group acts primitively on the crosses. This is an easy exercise. Then we show that the stabilizer of a cross in $2^{\cdot}\mathrm{Co}_1$ is $2^{12}{:}\mathrm{M}_{24}$. This is more or less obvious given what we already know. Next we show that $2^{\cdot}\mathrm{Co}_1$ is generated by conjugates of the normal abelian subgroup 2^{12} of the cross stabilizer, by first finding an element of this form in $2^{12}{:}\mathrm{M}_{24} \setminus 2^{12}$, so that by the simplicity of M_{24} the whole group $2^{12}{:}\mathrm{M}_{24}$ is generated by such elements. But $2^{12}{:}\mathrm{M}_{24}$ is maximal in $2^{\cdot}\mathrm{Co}_1$, and there are conjugates of the 2^{12} not contained in this copy of $2^{12}{:}\mathrm{M}_{24}$, so $2^{\cdot}\mathrm{Co}_1$ is generated by these conjugates, as required. Finally, we easily see that the 2^{12} is generated by commutators already in $2^{12}{:}\mathrm{M}_{24}$. Hence we have all the ingredients of Iwasawa's Lemma, and conclude that Co_1 is simple.

5.3.4 The small Conway groups

Now that we have shown that $2^{\cdot}\mathrm{Co}_1$ is transitive on crosses, it follows easily that it is transitive on vectors of norm 4, and on vectors of norm 6. For the cross stabilizer is transitive on norm 4 vectors having inner products ± 4 or 0 with each vector of the cross: thus for example $(4, 4, 0^{22})$ with respect to the standard cross, and $(2^8, 0^{16})$ with respect to the cross containing $(4^4, 0^{20})$, and $(3, -1^7, 1^{16})$ with respect to the cross containing $(5, -3, -3, 1^{21})$. Therefore the three orbits of $2^{12}{:}\mathrm{M}_{24}$ on vectors of norm 4 are fused into a single orbit under $2^{\cdot}\mathrm{Co}_1$. Similarly for norm 6, the cross stabilizer is transitive on norm 6 vectors having inner products ± 2 or 0 with each vector of the cross. Examples of such vectors are $(2^{12}, 0^{12})$ with respect to the standard cross, $(-3, 1^3, -3, 1^3, -3, 1^{15})$ and $(2^2, 0^2, 2^2, 0^2, 2^2, 0^2, 2, -2, 0^2, 4, 0^7)$, with respect to the cross containing $(4^4, 0^{20})$, and $(5, 1^{23})$ with respect to the cross containing $(-2, 2^{11}, 4, 0^{11})$. For clarity we display these vectors in the MOG array below. The top row contains a representative vector of the cross, and the bottom row the vector of norm 4.

$$
\begin{array}{ccc}
\begin{array}{|c|c|c|c|c|c|}\hline 4&&&&& \\ 4&&&&& \\ 4&&&&& \\ 4&&&&& \\ \hline\end{array}
&
\begin{array}{|c|c|c|c|c|c|}\hline 4&&&&& \\ 4&&&&& \\ 4&&&&& \\ 4&&&&& \\ \hline\end{array}
&
\begin{array}{|cc|cc|cc|}\hline 2&2&-2&4&& \\ &&&2&2&2 \\ &&&2&2&2 \\ &&&2&2&2 \\ \hline\end{array}
\\[2ex]
\begin{array}{|cc|cc|cc|}\hline -3&-3&-3&1&1&1 \\ 1&1&1&1&1&1 \\ 1&1&1&1&1&1 \\ 1&1&1&1&1&1 \\ \hline\end{array}
&
\begin{array}{|cc|cc|cc|}\hline 2&2&2&-2&4& \\ 2&2&2&2&& \\ \hline &&&&& \\ &&&&& \\ \hline\end{array}
&
\begin{array}{|cc|cc|cc|}\hline 5&1&1&1&1&1 \\ 1&1&1&1&1&1 \\ 1&1&1&1&1&1 \\ 1&1&1&1&1&1 \\ \hline\end{array}
\end{array}
\tag{5.15}
$$

The stabilizer of a vector of norm 4 is denoted Co_2, and has order

$$|\mathrm{Co}_2| \;=\; |\mathrm{Co}_1|/98280$$

$$= 42\,305\,421\,312\,000. \tag{5.16}$$

The stabilizer of a vector of norm 6 is denoted Co_3, and has order

$$\begin{aligned} |\mathrm{Co}_3| &= |\mathrm{Co}_1|/8386560 \\ &= 495\,766\,656\,000. \end{aligned} \tag{5.17}$$

We can proceed further, to define the McLaughlin group and the Higman–Sims group, and determine their orders, by proving transitivity of Co_2 or Co_3 on suitable sets of vectors. In the McLaughlin group case we need to prove that Co_3, the stabilizer of a vector v of norm 6, is transitive on the 552 vectors of norm 4 which have inner product -3 with v. If $v = (-2^{12}, 0^{12})$ then the monomial group $2 \times \mathrm{M}_{12}$ fixes v and has orbits of lengths $24 + 264 + 264$ on these vectors, with representatives $(1^{12}, -3, 1^{11})$, $(2^6, 0^6, 2^2, 0^{10})$ and $(3, -1, 1^{10}, 1^6, -1^6)$ respectively. On the other hand, if $v = (-5, -1^{23})$, then the monomial group M_{23} has orbits of lengths $23+23+253+253$, with representatives $(4, 4, 0^{22})$, $(1, -3, 1^{22})$, $(2, 2^7, 0^{16})$ and $(3, -1^7, 1^{16})$ respectively. The only way for both these sets of orbits to fuse into orbits for Co_3 is as a single orbit of length 552.

Thus the stabilizer in Co_3 of such a vector is a subgroup of index 552 in Co_3, so has order $|\mathrm{Co}_3|/552 = 898128000$. This is the McLaughlin group.

Similarly, in the Higman–Sims case we need to prove that Co_3 is transitive on the 11178 vectors of norm 4 which have inner product -2 with v. When $v = (-2^{12}, 0^{12})$, the monomial group $2 \times \mathrm{M}_{12}$ has six orbits on these vectors, as follows:

Orbit representative	Orbit length
$(-3, 1^{11}, 1^{12})$	24
$(4^2, 0^{10}, 0^{12})$	66
$(2^5, -2, 0^6, 2^2, 0^{10})$	1584
$(1^{10}, -1^2, -1^6, -3, 1^5)$	1584
$(2^4, 0^8, 2^4, 0^8)$	3960
$(3, -1^3, 1^8, -1^4, 1^8)$	3960

(5.18)

But when $v = (-5, -1^{23})$, the group M_{23} has five orbits, as follows:

Orbit representative	Orbit length
$(4, -4, 0^{22})$	23
$(0, 2^8, 0^{15})$	506
$(3, -1^{11}, 1^{12})$	1288
$(1, 3, -1^{15}, 1^7)$	4048
$(2, 2^5, -2^2, 0^{16})$	5313

(5.19)

Again it is easy to see that Co_3 must act transitively on these vectors, since these two sets of orbit lengths are incompatible with anything else.

Thus the stabilizer in Co_3 of such a vector is a subgroup of index 11178 in Co_3, so has order $|\mathrm{Co}_3|/11178 = 44352000$. This is the Higman–Sims group.