1

Introduction

1.1 Motivation

The Mathieu group M_{24} together with its subgroups M_{23}, M_{22}, M_{12} and M_{11} are arguably the most famous, most studied and most beautiful groups that exist. Indeed M_{24} and M_{12} acting with degrees 24 and 12 respectively are the only quintuply transitive permutation groups other than the alternating and symmetric groups, and similarly their point stabilizing subgroups M_{23} and M_{11} are the only quadruply transitive groups. A permutation group G acting on a set X is said to be n-transitive if, and only if, given n distinct points of X, $\{x_1, x_2, \ldots, x_n\}$ say, and any other n distinct points $\{y_1, y_2, \ldots, y_n\}$, there is a permutation $\pi \in G$ such that $\pi(x_i) = y_i$ for $i = 1, \ldots, n$. In the case of M_{12} with $n = 5$ this element π is unique and we say that M_{12} is *sharply* 5-transitive; similarly M_{11} is sharply 4-transitive. This implies that their orders are given by

$$|M_{12}| = 12\,.\,11\,.\,10\,.\,9\,.\,8 = 95\,040 \text{ and } |M_{11}| = 11\,.\,10\,.\,9\,.\,8 = 7920.$$

The order of M_{24} has the form

$$|M_{24}| = 24\,.\,23\,.\,22\,.\,21\,.\,20\,.\,|H|,$$

where H denotes the stabilizer in M_{24} of five points; it emerges naturally in our proof of the uniqueness of the Steiner system S(5, 8, 24) in Chapter 3. The fact that the Mathieu groups are the only quintuply and quadruply transitive groups, other than the alternating and symmetric groups, is now known to hold as a consequence of the Classification of Finite Simple Groups, see Section 11.8. However, up to now no direct proof of this remarkable fact has been found. They were discovered by Emil Mathieu and their existence was announced in two papers (Mathieu, 1861, 1873). Not only are these groups of huge interest in their own right, but they are involved in many of the other sporadic simple groups and play important roles in coding theory, sphere packing and other combinatorial structures. They arise most naturally as groups of permutations preserving certain Steiner systems, see Chapter 2 of this book, in particular S(5, 8, 24) and S(5, 6, 12) and their subsystems, and it is through these block designs that they are best studied.

1.2 Other Constructions

As befits mathematical structures of such beauty and importance, the Mathieu groups have been constructed in many different ways. Before proceeding to the approach that is the subject of this book, I shall give a brief description of some, but far from all, of these alternatives, which are fascinating in their diversity.

Mathieu himself in the aforementioned papers constructed the groups by 'gluing together' copies of the projective special linear groups $L_2(11)$ and $L_2(23)$ acting on 12 and 24 points, respectively. Indeed, he believed his construction could be carried out for primes larger than 11 and 23. In fact, numerologically speaking $n = 48$ has much in common with 24 and 12: $n - 1$ is prime, $n - 2$ is twice a prime and $n - 5$ is also prime. But sadly M_{48} does not exist! Of course Mathieu knew that the order of M_{12} divides the order of M_{24} but he was not aware that it is in fact a subgroup.

Witt's approach, see Witt (1938a,b), was to start with a well-known Steiner system $S(l, m, n)$ and build successive transitive extensions $S(l+1, m+1, n+1)$, $S(l + 2, m + 2, n + 2), \ldots$. Thus he started with the projective plane of order 4, which is a Steiner system S(2, 5, 21), and showed that it can be extended to an S(3, 6, 22). He then proved that this new system had a triply transitive group of automorphisms, which is in fact a group of shape $M_{22} : 2$, the simple Mathieu group M_{22} extended by an outer automorphism of order 2. This process could then be repeated to form an S(4, 7, 23) preserved by the quadruply transitive simple Mathieu group M_{23}. Finally he extended this system to an S(5, 8, 24) that has the magnificent, quintuply transitive simple group M_{24} as its group of symmetries. This Steiner system cannot be extended to an S(6, 9, 25) as the number of *nonads* in such a system would be

$$\binom{25}{6}\bigg/\binom{9}{6},$$

which is not an integer.

Todd's approach also focused on the Steiner system S(5, 8, 24) and his paper (Todd, 1966) actually lists the 759 octads, but it is an alternative method that he lectured on in Cambridge in the late 1960s that I wish to mention here.[1] The symmetric group S_6 is exceptional in that it has an outer automorphism of order 2. If we think of $G \cong S_6$ as permuting the six points of the projective line $\{\infty, 0, \ldots, 4\}$ then the copy of S_5 fixing ∞ clearly has index 6 in G, but so does the transitive subgroup $H \cong \mathrm{PGL}_2(5)$, which also has index 6. Thus G acts in a non-permutation identical way on two different sets of size 6. These two sets are interchanged by the outer automorphism. In Sylvester's terminology a partition of six letters into three pairs is known as a *syntheme* and a set of five synthemes that includes all 15 unordered pairs is a synthematic total or simply a *total*. It is easy to see that there are just six possible totals, one of which is

$$\infty/01\,234 \sim \begin{array}{c} \infty 0\,.\,14\,.\,23 \\ \infty 1\,.\,20\,.\,34 \\ \infty 2\,.\,31\,.\,40 \\ \infty 3\,.\,42\,.\,01 \\ \infty 4\,.\,03\,.\,12 \end{array}.$$

It is readily checked that this total is preserved by

$$\langle x \mapsto x+1 \cong (\infty)(0\;1\;2\;3\;4), x \mapsto 2/x \cong (\infty\;0)(1\;2)(3\;4)\rangle \cong \mathrm{PGL}_2(5)$$

and so has just six images under the action of S_6. Todd demonstrated longhand that a transposition on the six points induces a permutation of cycle shape 2^3 on the totals, and vice versa, and similarly a 3-cycle on one side has cycle shape 3^2 on the other. These conjugacy classes of shapes $1^4.2/2^3$ and $1^3.3/3^2$ are then used to define the 132 hexads of a Steiner system S(5, 6, 12) on the $6+6$ points and totals, namely: $90 = (\binom{6}{2} \times 3) \times 2$ hexads consisting of four fixed points on one side and a corresponding transposition on the other; $40 = \binom{6}{3} \times 2$ corresponding to three fixed points on one side and a corresponding 3-cycle on the other side; together with the set of six points and the set of six totals. Thus giving $90+40+2 = 132$. The automorphism group of this Steiner system is M_{12} which in turn is shown to act non-permutation identically on two sets of size 12 and, in an analogous manner, the actions on the two 12s are used to define a Steiner system S(5, 8, 24) on the 12+12 points. The automorphism group of this system is, of course, M_{24}.

In his Three Lectures on Exceptional Groups (see Conway, 1971 or Conway and Sloane, 1988, Chapter 10) Conway directly constructs M_{24} by extending $\mathrm{PSL}_2(23)$ acting on the 24-point projective line. He adjoins a permutation

$$\delta : x \mapsto x^3/9 \;(x \in Q) \quad \text{and} \quad x \mapsto 9x^3 \;(x \in N),$$

[1] Graham Higman was himself describing this method in lectures in Oxford at around the same time.

where Q denotes the quadratic residues modulo 23 and N denotes the non-residues, and proceeds to deduce that the resulting group has the familiar properties.

In Curtis (1989, 1990) the current author produces five elements of order 3 permuting the 12 pentagonal faces of a dodecahedron that together generate M_{12}, and seven involutions permuting the 24 heptagonal faces of the genus 3 Klein map that generate M_{24}. Algebraic and combinatorial explanations for these generators are also given. The details of these constructions are given in Chapter 13 of this book.

1.3 The Construction of This Book

The main properties of M_{24} may be deduced from each of the above constructions, and from many others not mentioned here. However, none of them helps us to actually work within the group itself, to recognize when a permutation on 24 letters is in our chosen copy of M_{24}, or to write down a permutation of the group having certain desirable properties. Of course modern algebra packages such as GAP and MAGMA are wonderfully efficient for working with permutation groups of such low degree, and it may seem indulgent to develop techniques that are only relevant to a particular small family of groups. However, I would claim that the Mathieu groups are so exceptional, as has been demonstrated earlier, and so intimately involved in other mathematical structures that a dedicated theory is justified. Moreover, it is our contention that a deeper understanding of the intricacies and sheer beauty of these remarkable structures is afforded by the approach described later.

1.4 The Centrality of M_{24}

Besides being an extraordinary structure in its own right, the group M_{24} plays a central role within the sporadic simple groups and hence within wider mathematics. Firstly, of course, the Conway group $\cdot O$ that Conway himself often called 'M_{24} writ large', grows out of M_{24} and the binary Golay code $\mathscr{C}$ by way of the Leech lattice Λ. In his book entitled *Twelve Sporadic Groups* Robert Griess (1998) describes the sporadic groups that are visible within $\cdot O$ as the 'first generation'. Due to their connection to Λ, see Conway et al. (1982), in working with these groups many people have found MOG techniques useful.

The involvement of M_{24} does not stop with the first generation though, as the largest Fischer group Fi_{24} contains maximal subgroups of shape 2^{11}. M_{24}

in an analogous way to Co_1. However, in Co_1 the elementary abelian group of order 2^{11} is isomorphic to $\mathscr{C}$ factored by the all 1s vector and the extension is a semidirect product, that is to say it is a *split* extension as is indicated by the colon in $2^{11} : M_{24}$. In the Fischer group the elementary abelian group is isomorphic to the even part of the dual code $\mathscr{C}^*$, see Chapter 4, and the extension is *non-split*, which is indicated by the 'upper dot' in $2^{11} {}^{\cdot} M_{24}$. So in the latter case this affine subgroup contains no copy of M_{24}; however, the techniques of this book have still proved useful, see Conway (1973) and Rowley and Walker (2012, 2021). Moreover, the Conway group Co_1 is involved in the Monster group M, since the centralizer of an involution of ATLAS class $2B$ has shape $2_+^{1+24}.Co_1$. Accordingly, they have made extensive use of the MOG in their investigations of both M and the Baby Monster B, see Rowley (2005); Rowley and Walker (2004a,b).

The last sporadic simple group to be discovered was the Janko group J_4 and it too contains a subgroup of shape $2^{11} : M_{24}$, see Section14.3. Indeed, it was intensive use of the MOG by Benson and others, see Benson (1980), in their work on J_4 that led to the hexacode, see Chapter 6.

Besides its pivotal role in finite groups, M_{24} and the underlying combinatorial structures crop up in unexpected places. For instance, in Berlekamp et al. (1982, page 436) the Miracle Octad Generator is reproduced in connection with the game *Mogul*.

A deep connection between the algebraic structures dealt with here and number theory was discovered when John McKay noticed some intriguing numerological coincidences that are explained briefly in Section 11.9; the resulting investigations were christened *Monstrous Moonshine* by Conway; see Conway and Norton (1979).

These structures and the techniques for working with them have recently become of great interest to Theoretical Particle Physicists working in String Theory. In Monstrous Moonshine the degrees of the irreducible complex representations of the Monster group M are related to the modular function as explained in Section 11.9; here it is those of M_{24} that are related to an object they call a 'mock modular form', see Taormina and Wendland (2013, 2015a,b).