An Elementary Proof of the Simplicity of the Mathieu Groups M_{11} and M_{23}

Robin J. Chapman

In this note I prove the simplicity of the Mathieu groups of prime degree, M_{11} and M_{23}, using no group theory beyond Sylow's theorems and basic facts about permutation groups. The only facts about the groups M_{11} and M_{23} which are needed are their orders, and the fact that they are transitive permutation groups on 11 and 23 letters respectively. Most textbooks dealing with the Mathieu groups prove the simplicity of M_{11} by more complicated arguments. For instance Rotman [1], uses a lemma of Burnside whose proof lies beyond the scope of introductory courses on group theory.

Let p be a prime number, and G be a subgroup of S_p, the symmetric group of degree p. It is easy to see that $p \mid |G|$ if and only if G is transitive, i.e., if $1 \leq j, k \leq p$ then there is $\sigma \in G$ with $\sigma(j) = k$, for the only elements of order p in S_p are the p-cycles. We shall assume that G is transitive, and by replacing G by a conjugate if necessary we may also assume that G has $P = \langle (1\,2 \cdots p) \rangle$ as a Sylow p-subgroup. Let $n = |G|$, m_G be the number of Sylow p-subgroups of G, and r_G be the index $|N_G(P) : P|$, where $N_G(P)$ is the normalizer of P in G. As all Sylow p-subgroups of G are conjugate in G then

$$n = |G| = |P|\,|N_G(P) : P|\,|G : N_G(P)| = pr_G m_G.$$

By Sylow's third theorem $m_G \equiv 1 (\mathrm{mod}\ p)$. Also $P \leq N_G(P) \leq N_{S_p}(P)$ and $N_{S_p}(P)$ is the group of all affine transformations modulo p, i.e., the set of maps of the form

$$x \mapsto ax + b \pmod{p}$$

where $p \nmid a$. Hence $|N_{S_p}(P)| = p(p-1)$ and so $r_G = |N_G(P) : P|$ is a factor of $p - 1$. It follows that r_G is the least positive residue of n/p modulo p. The following lemma forms the basis of our proof of simplicity.

Lemma 1. *Let G be a transitive subgroup of S_p, and suppose $m_G > 1$. Then $r_G > 1$.*

Proof: Suppose $m_G > 1$ and $r_G = 1$. Then G has exactly $m_G(p-1) = n - m_G$ elements of order p. Each of these elements has no fixed points on $\{1, 2, \ldots, p\}$. Hence G has at most m_G elements with fixed points. Each stabilizer G_j of $j \in \{1, 2, \ldots, p\}$ in G consists of m_G elements having at least one fixed point. It follows that $G_1 = G_2 = \cdots = G_p$, the set of all elements of G with fixed points. This means that G_1 is trivial and so $m_G = 1$ contrary to hypothesis. □

We can now prove the simplicity of an interesting class of groups.

Theorem 1. *Let G be a transitive subgroup of S_p, and suppose $|G| = pmr$ where $m > 1$, $m \equiv 1 \pmod{p}$, $r < p$ and r is prime. Then G is simple.*

Proof: We must have $r_G = r$ and $m_G = m$. Let H be a non-trivial normal subgroup of G. It is easy to see that the orbits of H on $\{1, 2, \ldots, p\}$ are permuted by G. As G is transitive and H is non-trivial all the orbits of H must have the same size $s > 1$, so $s = p$ and H is transitive. It follows that $P' \leq H$ for some Sylow p-subgroup P' of G. By Sylow's second theorem all Sylow p-subgroups of G are conjugate in G, and so H contains all Sylow p-subgroups of G. Hence $m_H = m$ and $|H| = pmt$ where $t|r$. But $t > 1$ by the Lemma and as r is prime, $t = r$, $H = G$ and G is simple. □

We recall briefly some facts about the Mathieu groups, M_{11}, M_{12}, M_{22}, M_{23} and M_{24}. These were the first sporadic simple groups to be discovered—by Mathieu in 1861 and 1873—and are most easily defined as automorphism groups of certain combinatorial structures known as Steiner systems. For instance M_{11} is the automorphism group of the (unique) Steiner system of type $S(4, 5, 11)$—this is a collection of 5-element subsets of an 11-element set X with the property that each 4-element subset of X is contained in exactly one of the sets in the system. Similarly M_{23} is the automorphism group of the (unique) Steiner system of type $S(4, 7, 23)$. For more details see chapter nine of Rotman's book [**1**]. Rotman finds the orders of these groups; in particular $|M_{11}| = 7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$ and $|M_{23}| = 10200960 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$.

Theorem 2. *The Mathieu groups M_{11} and M_{23} are simple.*

Proof: The group M_{11} is a transitive subgroup of S_{11} of order $n = 7920$. Now $n/p = 720 \equiv 5 \pmod{11}$ so $r_G = 5$ and $m_G = 144 > 1$. By Theorem 1 M_{11} is simple.

Similarly the group M_{23} is a transitive subgroup of S_{23} of order $n = 10200960$. Now $n/p = 443520 \equiv 11 \pmod{23}$ so $r_G = 11$ and $m_G = 40320 > 1$. By Theorem 1 M_{23} is simple. □

From the simplicity of M_{11} and M_{23} it is easy to deduce the simplicity of M_{12} and M_{24} (see Corollary 9.22 in [**1**]).

REFERENCE

1. J. Rotman, *An Introduction to the Theory of Groups*, (3rd ed.), Allyn and Bacon, 1984.

Department of Mathematics
University of Exeter
EX4 4QE
United Kingdom
rjc@maths.exeter.ac.uk