SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Mathieu Groups: Construction and Simplicity

av

Ahmed Bechlaoui

2023 - K19

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Mathieu Groups: Construction and Simplicity

Ahmed Bechlaoui

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Rikard Bögvad

2023

Abstract

In this paper, we focus on the construction and simplicity of the Mathieu groups M_{11} and M_{12}, as presented in Donald.S Passman's book "Permutation Groups." The main aim is to provide clearer explanations to the ambiguities involved in understanding the construction and related concepts.

1 Introduction

This thesis aims to explore two of the five Mathieu groups, M_{11} and M_{12}. The Mathieu groups are an intriguing family of finite groups that hold significant applications in combinatorics and group theory. To comprehend Mathieu groups and their significance, it is crucial to introduce the concept of sporadic groups and the classification of finite simple groups. We start by formally state the classification theorem to present a comprehensive overview.

Theorem 1.1. *(Classification of Finite Simple Groups) Every finite simple group is isomorphic to one of the following groups:*

(i) a member of one three infinite classes of groups, namely:

- *the cyclic group of prime order,*
- *the alternating group of degree at least 5,*
- *the groups of Lie type.*

(ii) one of 26 groups called "the sporadic groups"

(iii) the Tits group.

The classification theorem of finite simple groups is a remarkable result in mathematics, sorting all finite simple groups into distinct categories. This theorem is known for its exceptionally long and complex proof, which spans tens of thousands of pages in various research papers and books. Due to its complex nature, providing the complete proof is beyond the scope of this thesis.

The Mathieu groups are some of the most well-known examples of sporadic groups. They are also the first sporadic groups to be discovered. The sporadic groups are interesting because they don't fit into any particular family or natural sequence of groups, and they appear seemingly randomly. In other words, they do not arise from any obvious pattern or structure. The construction of Mathieu groups involves manipulating permutation groups that are "highly transitive" and we will see that this types of transitive groups are extremely rare.

In this thesis, we will focus on the two smaller groups, M_{11} and M_{12}, their constructions and properties, and show that they are indeed simple. specifically, we will establish that these groups belong to the category of finite simple groups.

There are several ways to construct the Mathieu groups M_{11} and M_{12}. We will use a procude due to Ernst Witt, who was a German mathematician that confirmed the existence of these groups by constructing them as successive transitive extensions of permutation groups.

2 Preliminaries

2.1 An Overview of the Theory of Groups

We begin this work by introducing some important definitions and results in group theory that is needed to understand the technical details in later sections.

2.1.1 Group Actions

The following concept we are introducing may be the most important tool for characterizing groups and understanding their structure and behavior, especially in the context of permutation groups (which are groups represented as permutationen).

Definition 2.1. (Group Action) Let G be a group with the identity e and let A be a set. Then a (left) group action of G on A is a function

$$G \times A \longrightarrow A$$

denoted by

$$(g, a) \mapsto g \cdot a$$

which satisfies the following properties

$$(i)\ e \cdot a = a$$
$$(ii)\ g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$$

for all $g_1, g_2 \in G$ and $a \in A$.

There are many different characterizations of group actions, and we will address those that are relevant to our work.

Definition 2.2. The action of a group G on a set A is called transitive if for any two points $a, b \in A$ there exists a $g \in G$ so that $ga = b$.

Definition 2.3. (Orbit) Let G be a group acting on a set A and let $a \in A$. The set

$$Ga = \{ga \mid g \in G\}$$

is called the orbit of a (under the action of G on A).

Remark 2.4. Note that Ga is a subset of A and that the group action is transitive if and only if there is only one orbit.

Definition 2.5. (Stabilizer) Let G be a group acting on a set A and a some fixed element of A. The *stabilizer* of a in G is the set $G_a = \{g \in G \mid ga = a\}$.

Theorem 2.6. *(Orbit-Stabilizer Theorem) Let G be a group acting on a set A. Then it holds that $|Ga| = |G : G_a|$.*

Proof. We show that the mapping

$$\phi : Ga \to G/G_a$$
$$ga \mapsto gG_a$$

is a bijection. We first must show that ϕ is a well defined mapping. Let $g_1a, g_2a \in Ga$ and $g_1a = g_2a$ for some $g_1, g_2 \in G$. Then we have

$$(g_2^{-1}g_1)a = g_2^{-1}(g_1a) = g_2^{-1}(g_2a) = (g_2^{-1}g_2)a = ea = a.$$

This shows that $g_2^{-1}g_1 \in G_a$ which implies $g_1G_a = g_2G_a$ so ϕ is well defined. It is clear that ϕ is surjective by the way it is defined. If $g_1G_a = g_2G_a$ then $g_1 = g_2h$ for some $h \in G_a$ so

$$g_1a = (g_2h)a = g_2(ha) = g_2a$$

thus ϕ is injective. Since bijections preserves the cardinality of the sets the theorem follows. □

Definition 2.7. A group G acting on a set A is said to be *semiregular* if $G_a = \{e\}$ for all $a \in A$. If G is also transitive we say that the group is *regular*.

Definition 2.8. Let G be a transitive permutation group acting on a set A. The action on the set A is said to be *primitive* if for any $a \in A$, G_a is a maximal subgroup of G.

This definition of a primitive action is not standard. However, we will see how it will be used when M_{11} naturally arises as a stabilizer subgroup of M_{12}. The following results will be used in the last section where we are going to prove the simplicity of the Mathieu groups, which we are going to state without proof.

Proposition 2.9. *Let G be a transitive permutation group and let $N \trianglelefteq G$. If $N \neq \{e\}$ and G is primitive, then N is transitive.*

Proposition 2.10. *Let G be a transitive permutation group of prime degree. Then G is primitive*

2.1.2 The Symmetric Group S_n: Introduction and Fundamental Properties

We are no going to see how group actions and permutation groups are related.

Definition 2.11. (Symmetric Group) The symmetric group together with composition operator $(S_n, \circ)$, is the group of permutation of n objects. In other words, it is all the bijections from a set A (whose cardinality is n) to itself. Furthermore, a subgroup of the symmetric group is said to be a permutation group.

Proposition 2.12. *For any non empty set A, the group of permutations of A, S_A acts on A by $\sigma \cdot a = \sigma(a)$ for all $\sigma \in S_A$, $a \in A$.*

Proof. We show that the properties of a group action given in definition 2.1 are satisfied. Let $\sigma_1, \sigma_2 \in S_A$ and $a \in A$. Then

$$(i)\ e \cdot a = e(a) = a$$
$$(ii)\ \sigma_1 \cdot (\sigma_2 \cdot a) = \sigma_1(\sigma_2 \cdot a) = \sigma_1(\sigma_2(a)) = (\sigma_1\sigma_2)(a) = (\sigma_1\sigma_2) \cdot a.$$

□

Proposition 2.13. *Let the group G act on a set A. For each fixed $g \in G$ we get a map σ_g defined by*

$$\sigma_g : A \to A$$
$$\sigma_g(a) = g \cdot a$$

with the following properties:

(1) for each fixed $g \in G, \sigma_g$ is a permutation of A, and
(2) the map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

Proof. The map σ_g is a permutation of A if it has a 2-sided inverse $\sigma_{g^{-1}}$. For all $a \in A$

$$(\sigma_{g^{-1}} \circ \sigma_g)(a) = \sigma_{g^{-1}}(\sigma_g(a)) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = a$$

so $\sigma_{g^{-1}} \circ \sigma_g$ is the identity map from A to A. Thus σ_g has a two sided inverse, hence is a permutation of A. Now let $\phi : G \to S_A$ be defined by $\phi(g) = \sigma_g$. Note that $\sigma_g \in S_A$ by the first part of the proof. Let $g_1, g_2 \in G$. The permutations $\phi(g_1g_2)$ and $\phi(g_1) \circ \phi(g_2)$ are equal if and only if their values agree on every element $a \in A$. For all $a \in A$

$$\phi(g_1g_2)(a) = \sigma_{g_1g_2}(a) = (g_1g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1}(\sigma_{g_2}(a)) = (\phi(g_1) \circ \phi(g_2))(a)$$

which proves that ϕ is a homomorphism. □

Definition 2.14. (Degree) The degree of a permutation group of a finite set is the number of elements in the set.

Example 2.15. The symmetric group S_n acts on a set of n element, so it has degree n.

In fact, every group is isomorphic to a permutation group, which brings us further to an important result called *Cayley's theorem.* This theorem has a central role in this thesis since we are going to construct the Mathieu groups that are represented as permutation groups.

Theorem 2.16. *(Cayley's Theorem) Every finite group is isomorphic to a permutation group. If G is a group of order n, then G is isomorphic to a subgroup of S_n.*

Proof. For a group G with $g, x \in G$ define

$$\lambda_g : G \longrightarrow G$$
$$\lambda_g(x) = gx.$$

Since

$$\lambda_g(x) = \lambda_g(y) \Rightarrow gx = gy \Rightarrow x = y$$

the function is injective. Suppose $y \in G$ and note that $\lambda_g(g^{-1}y) = g^{-1}gy = y$ so it is also surjective hence λ_g is a bijection $\lambda_g \in S_G$, where S_G is the group of permutations of the n elements in G. Now let $H = \{\lambda_g \mid g \in G\}$. We claim that H is a group under composition. If an element $\lambda_g \in H$ is composed with λ_e we get

$$(\lambda_g \circ \lambda_e)(x) = gex = gx = \lambda_g(x)$$

so λ_e is the identity in H. For inverses we get

$$(\lambda_g \circ \lambda_{g^{-1}})(x) = gg^{-1}x = x = \lambda_e(x)$$

which shows that every element has an inverse and $(\lambda_g)^{-1} = \lambda_{g^{-1}}$. Since composition of function is associative the operation on the set is also associative. Let $\lambda_{g_1}, \lambda_{g_2} \in H$ and we get

$$(\lambda_{g_1} \circ \lambda_{g_2})(x) = g_1 g_2 x = \lambda_{g_1 g_2}(x) \in H$$

so the set is closed. We have shown that $(H, \circ)$ is a group. We finish this proof by showing that $G \cong H$. Consider the map

$$\phi : G \longrightarrow H$$
$$\phi(g) = \lambda_g.$$

We show that this is a bijective homomorphism. Note that for elements $g, h \in G$

$$\lambda_{gh}(x) = ghx = (\lambda_g \circ \lambda_h)(x) = \phi(g)\phi(h)(x)$$

so ϕ is indeed a homomorphism. The map is obviously surjective by the way it is defined. For injectivity, the permutations $\phi(g) = \lambda_g$ and $\phi(h) = \lambda_h$ are equal if and only if their values agree on every element $x \in G$. We get that $\lambda_g(x) = \lambda_h(x)$ for all $x \in G$ which implies $gx = hx \Rightarrow g = h$ and the result follows. $\square$

Cayley's theorem highlights the idea that every group can be represented by permutations of its elements. It is good to keep it in mind to build a good intuition for the technical proofs later on.

Proposition 2.17. *Let σ, τ be elements of S_n and suppose σ has cycle decomposition*

$$(a_1\ a_2\ \dots\ a_{k_1})(b_1\ b_2\ \dots\ b_{k_2})\dots .$$

Then $\tau\sigma\tau^{-1}$ has the cycle decomposition

$$(\tau(a_1)\ \tau(a_2)\ ...\ \tau(a_{k_1}))(\tau(b_1)\ \tau(b_2)\ ...\ \tau(b_{k_2}))...\ ,$$

that is, $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.

Proof. Let $\sigma(i) = j$. By using the definition of composition of functions, we get

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau(\sigma(\tau^{-1}(\tau(i)))) = \tau(\sigma(i)) = \tau(j).$$

Thus if σ sends i to j, then $\tau\sigma\tau^{-1}$ sends $\tau(i)$ to $\tau(j)$. This completes the proof. □

Definition 2.18. (Fixed Points) Let G be a group acting on a set $A = \{a_1, ..., a_n\}$ and let H be a subgroup of G. We say that H fixes the set A if it fixes all the elements of A, i.e., $ha_i = a_i$ for all $h \in H$ and $i = 1, ..., n$.

Example 2.19. Let $G = S_3$ be acting on the set $\{1, 2, 3\}$ with $H = \{e, (1\ 2)\}$. Then $(e)(3) = 3$ and $(1\ 2)(3) = 3$ so H fixes 3.

Definition 2.20. (The Alternating Group) An even permutation is a permutation that is a product of an even number of transpositions. The set of even permutations of S_n, denoted by A_n, is called The alternating group of degree n with the usual group multiplication inherited from S_n.

2.1.3 Important Subgroups and Related Concepts

To study groups effectively, it is essential to look at their subgroups, as subgroups play a crucial role in understanding the structure and properties of a given group.

Definition 2.21. (Center) Let G be a group. The set $Z(G) = \{g \in G \mid gx = xg\ for\ all\ x \in G\}$, i.e., the set of elements commuting with all the elements of G is called the *center* of G .

Example 2.22. If G is abelian, then all the elements commute, so $Z(G)$ is the entire group, i.e., $Z(G) = G$.

Definition 2.23. (Centralizer) Let G be a group and let A be a nonempty subset of G. The set $C_G(A) = \{g \in G \mid gag^{-1} = a\ for\ all\ a \in A\}$ is called the *centralizer* of A in G . In other words, $C_G(A)$ is the set of elements of G which commute with every element of A.

Definition 2.24. (Normalizer) Let G be a group and let A be a nonempty subset of G. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. The set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$ is called the *normalizer* of A in G.

The center, centralizer and normalizer are all subgroups of G.

Definition 2.25. (Self-Centralizing Subgroup) Let G be a group and H a subgroup of G. If $C_G(H) \leq H$ or (equivalently) $Z(H) = C_G(H)$, then H is called *self-centralizing*.

Remark 2.26. If G (or H) is abelian then the definition of self-centralizing is equivalent to $H = C_G(H)$.

Definition 2.27. (Double Coset) Let G be a group, and let H and K be subgroups of G. For each $g \in G$, the (H, K)-double coset of g is the set $HgK = \{hgk \mid h \in H, k \in K\}$. If $H = K$, this is called the H-double coset of g. The set of all double cosets is denoted by $H\backslash G/K$.

Note that if we let H or K above be the identity subgroup, then this is just the usual definition of the left- and right cosets, respectively.

Proposition 2.28. *Let G be a group and H an abelian subgroup of G. Then H is self-centralizing if and only if it is not contained in any bigger abelian subgroup of G.*

Proof. Let $H \leq K$ where K is abelian. Then K centralizes H so $K \leq C_G(H)$. But $C_G(H) \leq H$ so $K \leq H$ which yield $H = K$. Conversely, if H is not contained in any larger abelian subgroup, and $x \in C_G(H)$ then $< H, x >$ is abelian, and so has to be H, that is $x \in H$. Hence H is self-centralizing. $\square$

Definition 2.29. (Normal Subgroup) A subgroup H of a group G is said to be normal if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. We will denote this by $H \trianglelefteq G$.

It is sometimes useful to use the following definition of a normal subgroup: A Subgroup H of G is normal in G if and only if $N_G(H) = G$.

Definition 2.30. (Conjugate) Let G be a group and g and h be two elements in G. The element ghg^{-1} is called the conjugate of h by g.

Proposition 2.31. *Let G be a group and H a subgroup of G. Then gHg^{-1} is a subgroup of G.*

Proof. We use the subgroup criterion. Since $e \in H$ we have

$$geg^{-1} = gg^{-1} = e \in gHg^{-1}$$

so gHg^{-1} is nonempty. Suppose that $h_1, h_2 \in H$, then

$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = gh_1h_2^{-1}g^{-1} \in gHg^{-1}.$$

$\square$

Proposition 2.32. *Two elements of S_n are conjugate if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.*

Proof. The fact that conjugate permutations have the same cycle type follows immediately by proposition 2.17. Conversely, suppose that $\sigma, \tau \in S_n$ has the same cycle type. Order the cycles in each permutation in nondecreasing length, including the 1-cycles (note that if several cycles of σ and τ has the same length then there are several ways of doing this). Let ρ be the function that maps the i^{th} integer in the list for σ to the i^{th} integer in the list for τ. Then again by proposition 2.17, ρ is a permutation that fulfills $\rho\sigma\rho^{-1} = \tau$. Since the cycle type of a permutation is a certain partition of n, and that the conjugacy class of a permutation is determined by its cycle type, the number of conjugacy classes of S_n is the number of partition of n, completing the proof. □

Example 2.33. The elements (1 2 4)(3 6)(7 8) and (2 3 8)(7 6)(1 4) in S_8 has both cycle type $3, 2, 2$ so they are conjugate

Definition 2.34. (Simple Group) A simple group is a nontrivial group whose only normal subgroups are the trivial group and the group itself.

Definition 2.35. (Index) If G is a group (possibly infinite) and $H \leq G$, the number of left coset of H in G is called the index of H in G and is denoted by $|G : H|$.

Theorem 2.36. *(Lagrange's Theorem) If G is a finite group and H is a subgroup of G , then the order of H divides the order of G and $|G : H| = \frac{|G|}{|H|}$.*

Proof. Let $|H| = n$ and $|G : H| = k$. We know that the set of left cosets of H in G partition G. The map

$$\begin{aligned} H &\to gH \\ h &\mapsto gh \end{aligned}$$

is clearly a surjection. Since $gh_1 = gh_2$ implies $h_1 = h_2$ the map is also injective. This proves that $|gH| = |H| = n$ and so $|G| = kn$ which implies $k = \frac{|G|}{n} = \frac{|G|}{|H|}$, completing the proof. □

2.1.4 The First Isomorphism Theorem

Theorem 2.37. *(The First Isomorphism Theorem) If $\phi : G \to H$ is a group homomorphism, then $ker\ \phi \trianglelefteq G$ and $G/ker\ \phi \cong \phi(G)$.*

Proof. We show that $gng^{-1} \in ker\ \phi$ for all $g \in G$ and $n \in ker\ \phi$. Let $g \in G$ and $n \in ker\ \phi$ be arbitrary. Since ϕ is an homomorphism we get

$$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e_H$$

thus $gng^{-1} \in ker\ \phi$ which proves the first part. For the second part, define the group map

$$\begin{aligned} \psi : G/ker\ \phi &\to \phi(G) \\ gker\ \phi &\mapsto \phi(g) \end{aligned}.$$

We show that this is an isomorphism. Take some arbitrary $g_1, g_2 \in G$. The map is well defined since

$$\begin{gathered} g_1 ker\ \phi = g_2 ker\ \phi \implies {g_2}^{-1} g_1 \in ker\ \phi \implies \phi({g_2}^{-1} g_1) = e_H \implies \\ \phi(g_2)^{-1} \phi(g_1) = e_H \implies \phi(g_1) = \phi(g_2) \end{gathered} .$$

Note also that

$$\psi((g_1 ker\ \phi)(g_2 ker\ \phi)) = \psi(g_1 g_2 ker\ \phi) = \phi(g_1 g_2) = \phi(g_1)\phi(g_2) = \psi(g_1 ker\ \phi)\psi(g_2 ker\ \phi)$$

so it is an homomorphism. Now suppose that $xker\ \phi \in ker\ \psi$ where $x \in G$. This implies that $\psi(gker\ \phi) = \phi(x) = e_H$ which tells us that $x \in ker\ \phi$. Thus $xker\ \phi = ker\ \phi$ so ker $\psi = \{ker\ \phi\}$. Since a group homomorphism is injective if and only if the kernel is the identity it follows that ψ is injective. For surjectivity, suppose that $y \in \phi(G)$. Then there exist $x \in G$ such that $\phi(x) = y$. Note that $\psi(xker\ \phi) = \phi(x) = y$ so we have found an element in the domain that maps onto the arbitrary element y thus the ψ is indeed surjective and the theorem follows. □

Proposition 2.38. *Let G and H be groups, $K \leq G$ and $\phi : G \twoheadrightarrow H$ a surjective homomorphism. Let c be a nonzero number. If $c \mid |\phi(K)|$ then $c \mid |K|$.*

Proof. Consider the homomorphism $\psi : K \to \phi(K)$. Since ψ is surjective, the previous theorem (theorem 2.37) implies that $|K|/|ker\ \psi| = |\phi(K)|$. The proposition follows. □

2.1.5 Automorphisms and Sylow's Theorem

Definition 2.39. (Automorphism) Let G be a group. An isomorphism from G onto itself is called an *automorphism* of G . The set of all automorphisms of G is denoted by $Aut(G)$.

Proposition 2.40. *$Aut(G)$ is a group under composition.*

Proposition 2.41. *Let G be a group and let H be any non-empty subset of G such that*

$$h \in H,\ g \in G \implies ghg^{-1} \in H.$$

Then G acts by conjugation on H defined by

$$g \cdot h = ghg^{-1}\ for\ all\ g \in G,\ h \in H.$$

Proof. We show that the two axioms for a group action are satisfied

$$(i)\ e \cdot h = ehe^{-1} = h$$

$$(ii)\ g_1 \cdot (g_2 \cdot h) = g_1 \cdot (g_2 h g_2^{-1}) = g_1 g_2 h g_2^{-1} g_1^{-1} = (g_1 g_2) h (g_1 g_2)^{-1} = (g_1 g_2) \cdot h$$

for all $g_1, g_2 \in G,\ h \in H$. □

Proposition 2.42. *Let H be a normal subgroup of the group G . Then G acts by conjugation on H as automorphisms of H. More specifically, the action of G on H by conjugation is defined for each $g \in G$ by*

$$h \mapsto ghg^{-1},\ for\ each\ h \in H.$$

For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism of G into $Aut(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.

Proof. Let ϕ_g be conjugation by g, i.e., let

$$\phi_g : H \to H$$
$$\phi_g(h) = ghg^{-1}.$$

Note that ϕ_g maps H to itself since $ghg^{-1} \in H$ for all $g \in G$. Since conjugation defines an action, $\phi_e = e$ and $\phi_a \circ \phi_b = \phi_{ab}$. Thus, for each fixed $g \in G$, ϕ_g is a bijection from H to itself since it has a two-sided inverse. Also, each ϕ_g is a homomorphism from H to itself because

$$\phi_g(hk) = g(hk)g^{-1} = gh(gg^{-1})kg^{-1} = (ghg^{-1})(gkg^{-1}) = \phi_g(h)\phi_g(k)$$

for all $h, k \in H$. This proves that for each fixed g, ϕ_g is an isomorphism from H onto itself, i.e., an automorphism of H. Now the group action induce a homomorphism

$$\psi : G \longrightarrow S_H$$
$$\psi(g) = \phi_g.$$

Since automorphisms of a group H are permutations of the set H, $Aut(H)$ is a subgroup of S_H and each ϕ_g is an automorphism, so the image of of Ψ is contained in Aut(H). Finally,

$$ker\ \psi = \{g \in G \mid \phi_g = e\} = \{g \in G \mid ghg^{-1} = h\ for\ all\ h \in H\} = C_G(H).$$

Thus by the first isomorphism theorem, $G/C_G(H) \cong \psi(G) \leq Aut(H)$. □

Corollary 2.43. *If K is any subgroup of the group G and $g \in G$, then $K \cong gKg^{-1}$.*

Proof. Let $G = H$ in preceding proposition (Note that G is a normal subgroup of itself). □

Corollary 2.44. *For any subgroup H of G , the qoutient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.*

Proof. This is clear since $H \trianglelefteq N_G(H)$, so if we let $N_G(H)$ play the role of G in the preceding proposition, the corollary follows. □

Proposition 2.45. *The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of integers modulo n.*

Theorem 2.46. *(Cauchy's Theorem) If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.*

Definition 2.47. Let G be a group and let p be a prime.
(1) A group of order p^α for some $\alpha \geq 0$ is called a *p-group*. Subgroups of G which are p-groups are called *p-subgroups*.
(2) If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a *sylow p-subgroup* of G .

Theorem 2.48. *(Sylow Theorems) Let G be a group of order $p^\alpha m$, where p is a prime not dividing m.*
(1) Sylow p-subgroups of G exist.
(2) Any two Sylow p-subgroups of G are conjugate in G.
(3) The number of Sylow p-subgroup of G (which we will denote by n_p) is

$$n_p \equiv 1 \,(mod\, p).$$

Further, n_p divides m.

Proof. For a complete detailed proof of the theorem, see Dummit and Foote's book 'Abstract Algebra' (pp. 140-141). □

Proposition 2.49. *Let $\phi : G \to H$ be a surjective group homomorphism and $N \trianglelefteq G$, then $\phi(N) \trianglelefteq H$.*

Proof. To show that $\phi(N)$ is a normal subgroup of H, we show that $h\phi(n)h^{-1} \in \phi(N)$ for all $h \in H$ and $n \in N$. Since ϕ is surjective, for every $h \in H$ there exists $g \in G$ such that $\phi(g) = h$. We have

$$h\phi(n)h^{-1} = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)\phi(n)\phi(g)^{-1} = \phi(gng^{-1}).$$

Since N is normal in G , $gng^{-1} \in N$ so $\phi(gng^{-1}) = h\phi(n)h^{-1} \in \phi(N)$. □

Proposition 2.50. *Let G and H be groups and $\phi : G \to H$ a surjective homomorphism. If G is abelian then H is abelian.*

Proof. Let $h_1, h_2 \in H$ be two arbitrary elements. Since ϕ is surjective, there exists $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$ so

$$h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) = \phi(g_2g_1) = \phi(g_2)\phi(g_1) = h_2h_1$$

which shows that H is abelian since h_1 and h_2 was arbitrary.

□

Proposition 2.51. *Let G be a group and H a subgroup of G . Then the action of G on the coset G/H by left multiplication is transitive.*

Proof. Let $g_1H, g_2H \in G/H$. Then if $g = g_2g_1^{-1}$ we have

$$g(g_1H) = g_2g_1^{-1}g_1H = g_2H.$$

and this applies to all elements of G/H since g_1H and g_2H was arbitrary. □

Proposition 2.52. *Let H be a transitive abelian group. Then H is regular.*

Proof. Let H act on a set A and fix an arbitrary element $a \in A$. Since H is transitive there exist $h \in H$ such that $ha = b$. Now

$$h^{-1}gha = a \iff g(ha) = ha,$$

so

$$g \in H_{ha} \iff h^{-1}gh \in H_a \iff g \in hH_ah^{-1},$$

and hence (always)

$$H_{ha} = hH_ah^{-1},$$

But H is abelian, so $H_b = H_{ha} = hH_ah^{-1} = Ha$. Hence an element in H_a also fixes all other elements $b \in H$, and hence acts as the trivial permutation, i.e. $H_a =< 1 >$. $\square$

Proposition 2.53. *Let G be a group acting transitively on a set A and let H be a transitive subgroup. Then $G = G_aH = HG_a$ for all $a \in A$*

Definition 2.54. (Elementary abelian group) An elementary abelian group is an abelian group in which all elements other than the identity has the same order p where p is a prime number.

Definition 2.55. Let G be a finite group and H a normal subgroup of G. Then H is called a *normal p-complement* of G for a prime p if H has an order coprime to p and index a power of p.

Theorem 2.56. *Let P be a Sylow p-subgroup of a group G. If P is in the center of its normalizer then G has a normal p-complement.*

Proof. For a complete proof, See D.S. Passmans book 'Permutation Groups' (pp. 103-104). $\square$

2.2 Multiple Transitivity

Before we begin the construction of the Mathieu groups, it is essential to define the special property that these groups carry, namely multiple transitivity. It is nothing more than an extension of the transitivity defined earlier.

Definition 2.57. For an integer $n \geq 1$, the action is *n-transitive* if the set A being acted on has at least n elements and for any pair of n-tuples $(a_1, ..., a_n), (b_1, ..., b_n) \in A^n$ with pairwise distinct entries (that is $a_i \neq a_j, b_i \neq b_j$ when $i \neq j$) there exists a $g \in G$ such that $ga_i = b_i$ for $i = 1, ..., n$. In other words, the action on the subset of A^n of tuples without repeated entries is transitive. If g is unique in the definition of n-transitivity, we say that the action is *sharply* n-transitive.

Remark 2.58. Althought transitivity is a characteristic of group action, we will prescribe it for a group G meaning that the action of G on a given set is transitive.

Proposition 2.59. *If $m \geq 2$, then m-transitivity implies k-transitivity for all $k \leq m$.*

Proof. It is clear by the definition of multiple transitivity. $\square$

Proposition 2.60. *A permutation group G of degree n is sharply k-transitive if and only if G is k-transitive and only the identity in G fixes k points.*

Proof. Suppose G is sharply k-transitive. Then G is k-transitive by definition. Let $A = \{a_1, ..., a_n\}$ be the underlying set G is acting on. Since G is sharply k-transitive, for any $(b_1, ..., b_k) \in A^k$ ($b_i \neq b_j$ *when* $i \neq j$) there exists a unique $g \in G$ such that $gb_i = b_i$ for $i = 1, ..., k$. The identity fixes all the points by the second property of a group action so we can take $g = e$. To see that the identity is the only element that fixes k points, suppose there is some other element g' such that $g'b_i = b_i$ for $i = 1, ..., k$. But that is a contradiction since G is sharply k-transitive (the identity is the unique element that fixes all the b_i). Conversely, suppose that G is k-transitive and only the identity in G fixes k points. Let $(c_1, ..., c_k) \in A^k$. Then given $(b_1, ..., b_k) \in A^k$, by the k-transitivity there is a $g \in G$ such that $gb_i = c_i$ for $i = 1, ..., k$. Suppose that there is another element $h \in G$ such that $hb_i = c_i$ for $i = 1, ..., k$. But then

$$h^{-1}gb_i = h^{-1}c_i = h^{-1}hb_i = b_i$$

and since only the identity fixes k points we have $h^{-1}g = 1$ which implies $h = g$, contradiction. Thus G is sharply k-transitive. $\square$

Proposition 2.61. *The symmetric group S_n is n-transitive and the alternating group A_n is $(n-2)$-transitive for all $n \geq 3$.*

Proof. Given $(a_1, ..., a_n), (b_1, ..., b_n) \in A^n$ with $a_i \neq a_j, b_i \neq b_j$ when $i \neq j$, the permutation (written in Cauchy's two-line notation)

$$\begin{pmatrix} a_1 & \dots & a_n \\ b_1 & \dots & b_n \end{pmatrix}$$

is in S_n and maps a_i to b_i for $i = 1, ..., n$ which proves the first part. Now consider $(a_1, ..., a_{n-2}), (b_1, ..., b_{n-2}) \in A^{n-2}$ with $a_i \neq a_j, b_i \neq b_j$ when $i \neq j$. Then one of the permutations

$$\sigma_1 = \begin{pmatrix} a_1 & \dots & a_{n-2} & a_{n-1} & a_n \\ b_1 & \dots & b_{n-2} & b_{n-1} & b_n \end{pmatrix} \quad , \quad \sigma_2 = \begin{pmatrix} a_1 & \dots & a_{n-2} & a_{n-1} & a_n \\ b_1 & \dots & b_{n-2} & b_n & b_{n-1} \end{pmatrix}$$

is even since they differ by a transposition by $\sigma_1 = (b_{n-1}\ b_n)\sigma_2$ which proves the second part. $\square$

Proposition 2.62. *S_n is sharply n-transitive and sharply $(n-1)$-transitive of degree n. If $n \geq 3$, then A_n is sharply $(n-2)$-transitive of degree n.*

Proof. By the preceding proposition, S_n is n-transitive (it is also $(n-1)$-transitive by proposition 2.59). The fact that the identity is the only element fixing n points follows directly from the definition of the identity. Now if $\sigma \in S_n$ fixes $(n-1)$-points, then clearly $\sigma = 1$. If it fixes $(n-2)$ points, then either $\sigma = 1$ or σ is a transposition. Since A_n contains no transposition, the last statement follows. $\square$

Remark 2.63. Note that sharply 1-transitivity is precisely regularity.

The following two propositions we are going to state are used quite widely in the construction. They are the key in constructing the larger group M_{12} from the smaller M_{11}.

Proposition 2.64. *Let G be a transitive permutation group on a set A. If $k \geq 2$, then G is k-transitive if and only if G_a is $(k-1)$-transitive on $A \setminus \{a\}$*

Proof. If G is k-transitive, then for any $(a_1, ..., a_k), (b_1, ..., b_k) \in A^k$ (with $a_i \neq a_j, b_i \neq b_j$ *when* $i \neq j$), there exists a $g \in G$ such that $g(a_1, ..., a_k) = (b_1, ..., b_k)$. If we let $a = a_1 = b_1$, the element g fixes a so $g \in G_a$. Since the remaining $k-1$ elements are arbitrary, it follows that for all $(a_2, ..., a_k), (b_2, ..., b_k) \in A^{k-1}$ (with $a_i \neq a_j, b_i \neq b_j$ *when* $i \neq j$), there exists a $g \in G_a$ such that $g(a_2, ..., a_k) = (b_2, ..., b_k)$ which is the definition of $(k-1)$-transitivity on $A \setminus \{a\}$. Conversely, let $(a_1, ..., a_k), (b_1, ..., b_k) \in X^k$. Since G is transitive there are two elements g and h such that $ga_1 = a$ and $hb_1 = a$. They permute the k-tuples to $(a = ga_1, ga_2, ..., ga_k)$ respectively $(a = hb_1, hb_2, ..., hb_k)$. Since G_a is $k-1$-transitive there is an element $k \in G_a$ such that

$$k(ga_2, ..., ga_k) = (hb_2, ..., hb_k).$$

Since it belongs to G_a

$$k(a, ga_2, ..., ga_k) = (a, hb_2, ..., hb_k).$$

Then clearly $h^{-1}kg(a_1, , , , a_k) = (b_1, , , , b_k)$, so we have an element that takes a k-tuple to any other k-tuple (with distinct elements). $\square$

Proposition 2.65. *Let G be a permutation group on a set A with n elements. Suppose that G is sharply k-transitive. If $a \in A$ and $k > 1$, then G_a is sharply $(k-1)$-transitive on $A \setminus \{a\}$. It also holds that $|G| = n(n-1)\cdots(n-k+1)$.*

Proof. If G is sharply k-transitive, then for any $(a_1, ..., a_k), (b_1, ..., b_k) \in A^k$ (with $a_i \neq a_j, b_i \neq b_j$ *when* $i \neq j$), there exists a unique $g \in G$ such that $g(a_1, ..., a_k) = (b_1, ..., b_k)$. If we let $a = a_1 = b_1$, the element g fixes a so $g \in G_a$. Since the remaining $k-1$ elements are arbitrary, it follows that for all $(a_2, ..., a_k), (b_2, ..., b_k) \in A^{k-1}$ (with $a_i \neq a_j, b_i \neq b_j$ *when* $i \neq j$) there exists a unique $g \in G_a$ such that $g(a_2, ..., a_k) = (b_2, ..., b_k)$ which is the definition of sharply $(k-1)$-transitivity on $A - \{a\}$. For the second part, note that G is transitive so the associated group action consist of one orbit. By the orbit-stabilizer theorem (theorem 2.6), $|Ga| = |G|/|G_a| = n$ and by induction we get that $G_a = (n-1)\cdots(n-k+1)$ hence $|G| = n(n-1)\cdots(n-k+1)$ (G_a plays the role of G in the formula since G_a is (k-1)-transitive by the first part of the proof).

□

Proposition 2.66. *Let G be transitive on a set A and let $a \in A$. Then G is 2-transitive if and only if for all $g \in G \setminus G_a$ we have $G = G_a \cup G_a g G_a$.*

Proof. Suppose that G is 2-transitive and let $g \in G \setminus G_a$ be given. If $h \in G \setminus G_a$ then $ha = b$ and $ga = c$ for some $a, b, c \in A$ with $b, c \neq a$. By the preceding result, G_a is transitive on $A \setminus \{a\}$ so we can find $k \in G_a$ such that $kb = c$. Hence $kha = kb = c = ga$ and thus $g = kh$ otherwise the operation would not be well defined. This shows that $g^{-1}kha = a$ or in particular $g^{-1}kh \in G_a$ so $h \in G_a g G_a$. We conclude that $G = G_a \cup G_a g G_a$. Now suppose that $G = G_a \cup G_a g G_a$. Given $b, c \in A \setminus \{a\}$, then since G is transitive there exists $g_1, g_2 \in G$ such that $g_1 a = b$ and $g_2 a = c$. Since g_1 and g_2 does not fix a, $g_1, g_2 \notin G_a$ and we must have $g_2 = k_1 g_1 k_2$ for some $k_1, k_2 \in G_a$. Finally,

$$c = g_2 a = k_1 g_1 a = k_1 b$$

which shows that G_a is transitive on $A \setminus \{a\}$ since b and c was arbitrary. The result follows by the preceding proposition. □

Proposition 2.67. *Let G be a t-transitive group of degree n. Let H be the subgroup fixing t points and let P be a sylow p-subgroup of H. Suppose P fixes $w \geq t$ points. Then $N_G(P)$ is t-transitive on the w points fixed by P.*

Proof. We assume that H fixes the points $a_1, ..., a_t$ and show that if P fixes the points $b_1, ..., b_w$ then there exists $n \in N_G(P)$ such that $na_i = b_i$ for $i = 1, ..., w$. Since G is t-transitive there exists a $g \in G$ such that $ga_i = b_i$ for $i = 1, ..., t$. Let $b_1, ..., b_t$ be the points fixed by P i.e. $p'b_i = b_i$ for all $p' \in P$. This gives

$$\begin{aligned} p'b_i = b_i \Rightarrow p'(ga_i) = (p'g)a_i = ga_i \Rightarrow g^{-1}((p'g)a_i) = g^{-1}(ga_i) \Rightarrow \\ \Rightarrow (g^{-1}p'g)a_i = (g^{-1}g)a_i \Rightarrow (g^{-1}p'g)a_i = a_i \end{aligned}$$

so $g^{-1}Pg$ fixes $a_1, ..., a_t$. By proposition 2.43, $g^{-1}Pg \cong P$ hence $g^{-1}Pg$ is also a sylow p-subgroup of H. By Sylow's theorem all sylow p-subgroups are conjugate so there exists $h \in H$ with $h^{-1}(g^{-1}Pg)h = P$. If we let $n = gh$ then $n \in N_G(P)$ and we have $na_i = (gh)a_i = g(ha_i) = ga_i = b_i$. This completes the proof □

The following lemma is meant to exclude some of the impossible cases for a group to have the multiply sharply transitive characterization. It will be applied in the next theorem.

Lemma 2.68. *If G is sharply k-transitive of degree n, then we cannot have $k = 4, n = 10$ or $k = 6, n = 13$.*

Proof. Suppose that $k = 4, n = 10$. Then proposition 2.65 states that $|G| = 10 \cdot 9 \cdot 8 \cdot 7$. By Sylow's theorem G has a Sylow 7-subgroup so there exists an element $x \in G$ of order 7 which generates the Sylow 7-subgroup $< x >$. The element x must be a 7 cycle, say $x = (1\ 2\ 3\ 4\ 5\ 6\ 7)$. Now G is 3-transitive and $< x >$ is a sylow 7-subgroup of the subgroup of G fixing $\{8, 9, 10\}$ hence by previous proposition $N_G(< x >)$ acts 3-transitively on $\{8, 9, 10\}$. This action induce a surjective homomorphism $\phi : N_G(< x >) \twoheadrightarrow S_{\{8,9,10\}} \cong S_3$. Since $C_G(x) \trianglelefteq N_G(< x >)$, $\phi(C_G(x))$ is a normal subgroup of S_3 (proposition 2.49). The only normal subgroups of S_3 are $\{1\}, A_3$ and S_3. Suppose that $\phi(C_G(x)) = \{1\}$ i.e. $C_G(x) \subset ker\ \phi$. Then we have a well defined mapping

$$\tilde{\phi} : N_G(< x >)/C_G(x) \twoheadrightarrow S_3$$
$$nC_G(x) \mapsto \phi(n)$$

This is clearly a surjective homomorphism. But this is a contradiction since surjective homomorphisms preserves the abelian property between the groups and $N_G(< x >)/C_G(x)$ is isomorphic to a subgroup of $Aut(< x >) \cong (\mathbb{Z}/7\mathbb{Z})^\times$ which is abelian but S_3 is not hence $\phi(C_G(x)) \neq \{1\}$. The image $\phi(C_G(x))$ is then either A_3 or S_3 so $3||\phi(C_G(x))|$ which implies $3||C_G(x)|$ (proposition 2.38). By Cauchy's theorem. we can choose $y \in C_G(x)$ such that $|y| = 3$. Now the order of a permutation is the $l.c.m$ of the lengths of the cycles in its cycle decomposition so $|xy| = l.c.m(|x|, |y|) = 7 \cdot 3 = 21$ and since x and y has prime order, they consist of a 7-cycle and a 3-cycle, respectively. Since $x, y \in C_G(x)$, we have $(xy)^7 = y \neq 1$ which fixes 7 points, a contradiction since G is sharply 4-transitive so only the identity fixes 4 points.

Now suppose that $k = 6, n = 13$. Then $|G| = 13 \cdot 12 \cdots 8$ and G has a sylow 5-subgroup so there exists an element $x \in G$ of order 5 which generates the Sylow 5-subgroup $< x >$. Also, x is either an 8-cycle or a 5-cycles since G is sharply 6-transitive. But an 8-cycle would fix more than eight points, contradiction. Let $x = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)$. Since G is $3 - transitive$, the same argument as above shows that there exists $y \in C_G(x)$ with $|y| = 3$. The element xy has order 15 and must consist of 3-cycles and 5-cycles since it cannot contain a 15-cycle due to the degree of G . Finally, $(xy)^6 = x$ so xy must have two 5-cycles and one 3-cycle. But then $(xy)^5 = 1$ which fixes 10 points, contradiction and the lemma is proved. □

Lemma 2.69. *The symmetric group S_4 contains three elements of order 2 which acts without fixed points. These elements are $(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$ and forms a regular normal subgroup together with the identity. All other elements of order 2 in S_4 are transpositions which has two fixed points.*

In the following result the symmetric group and the alternating group are considered trivial.

Theorem 2.70. *Let G be a nontrivial sharply k-transitive group of degree n. If $k \geq 4$, then we have either $k = 4, n = 11$ or $k = 5, n = 12$.*

Proof. We proceed in a series of steps.
Step 1. Suppose that $k = 4$. We show that $n \geq 8$ and all elements of G of order 2 are conjugate in G .
By the definition of k-transitive groups we must have $n \geq 4$. If $n = 4$ or $n = 5$ by proposition 2.65 $|G| = n!$ so $G = S_n$, contradiction. If $n = 6$ then $|G| = \frac{n!}{2}$ so $G = A_n$, again a contradiction. Now let $n = 7$ so $|G| = \frac{7!}{6}$. Further, we note that G is a subgroup of S_7 (since it is a permutation group of degree 7) and $|S_7 : G| = 6$ so the number of left cosets of G in S_7 is 6. By proposition 2.51 S_7 acts transitively on S_7/G which induce a homomorphism $\phi : S_7 \to S_{S_7/G} \cong S_6$. Furthermore, we can define the map $\psi : S_7 \to \phi(S_6)$ which also is a homomorphism. By the first isomorphism theorem, $S_7/ker\ \phi \cong \phi(S_6)$ and the only normal subgroups of S_7 is $\{e\}$, A_7 and S_7. If $ker\ \phi = \{e\}$ then $S_7/ker\ \phi \cong S_7$, a contradiction since $|S_7| > |S_6|$. With the same argument, ker ϕ cannot be equal to S_7, so we must have $ker\ \phi = A_7$. By this, we can write ψ as $\psi : S_7 \to S_7/A_7 \cong C_2$. But this is a contradiction since C_2 cannot be transitive on 6 elements. Thus $n \geq 8$.

We now show that all elements of G of order 2 are conjugate in G . Let $x, y \in G$ be such elements. Since x and y fixes at most three points (by the fact that G is sharply k-transitive) and $n \geq 8$ we must have $x = (1\ 2)(3\ 4)...$ and $y = (a\ b)(c\ d)...$, that is at least two transpositions must occur in each element. If we choose $g \in G$ with

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & . & . & . \\ a & b & c & d & . & . & . \end{pmatrix}$$

we get

$$gxg^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & . & . & . \\ a & b & c & d & . & . & . \end{pmatrix} (1\ 2)(3\ 4)... \begin{pmatrix} a & b & c & d & . & . & . \\ 1 & 2 & 3 & 4 & . & . & . \end{pmatrix} = (a\ b)(c\ d)...$$

Since $gxg^{-1}y^{-1}$ fixes four points this must equal the identity so

$$gxg^{-1}y^{-1} = 1 \Leftrightarrow gxg^{-1} = y.$$

Hence we have found an element $g \in G$ such that $gxg^{-1} = y$ for all $x, y \in G$ with order 2 and the fact follows.

step 2. We show that if $k = 4$ then $n = 11$.
Let $x = (1)(2)(3\ 4)...$ and $y = (1\ 2)(3)(4)...$ be elements of G. Note that these elements exist since G is 4-transitive. Then x^2 and y^2 fixes four points so $x^2 = y^2 = 1$ since only the identity fixes four points. Also, $(xy)(yx)^{-1}$ fixes four points so it follows that $xy = yx$. Set $z = xy$ so that $z = (1\ 2)(3\ 4)...$. Now, we know that x has at most three fixed points. If it has a third fixed point we denote this by 7. In the following whenever we write (7) we will allow for the possibility that this term does not occur. Since y commutes with x, we can show that y permutes the fixed points of x. Let s be a fixed point of x so

$$x(y(s)) = y(x(s)) = y(s)$$

which shows that $y(s)$ is also a fixed point of x. Thus y fixes 7. Hence $x = (1)(2)(3\ 4)(7)...$, $y = (1\ 2)(3)(4)(7)...$ and $z = xy = (1\ 2)(3\ 4)(7)...$. Since x and z both have order 2 they are conjugate by step 1, so it follows that x and z has the same cycle structure, hence z has two or three fixed points. We know that z must have two fixed points other than 7, say it fixes 5 and 6. The elements x and y commutes with z so they must permute the fixed points of z. Since we have already accounted for all fixed points of x and y, each must interchange 5 and 6. Thus we have

$$\begin{aligned} x &= (1)(2)(3\ 4)(5\ 6)(7)... \\ y &= (1\ 2)(3)(4)(5\ 6)(7)... \\ z &= (1\ 2)(3\ 4)(5)(6)(7)... \end{aligned} \tag{1}$$

and $< x, y, z >= H$ is the klein four-group, the elementary abelian group of order 4. Suppose that $w \in G$ centralizes H, i.e., $w \in C_G(H)$. Then w must fix the common fixed point 7 by the same argument as before. The element w commutes with x, y, and z so it permutes their fixed points and hence

$$w = (1\ 2)^{\alpha}(3\ 4)^{\beta}(5\ 6)^{\gamma}(7)...$$

with $\alpha, \beta, \gamma = 0, 1$. If w is not the identity, then w fixes at most three points so at least two of α, β, γ are equal to 1. Hence the possibilities are x, y, z or $w = (1\ 2)(3\ 4)(5\ 6)(7)...$. In the latter case, note that

$$xw = (1)(2)(3\ 4)(5\ 6)(7)... \circ (1\ 2)(3\ 4)(5\ 6)(7)... = (1\ 2)(3)(4)(5)(7)... \neq 1$$

fixes four points, a contradiction and w must be one of the other elements hence H is self-centralizing, i.e., $H = C_G(H)$. Now $|Aut\ H| = 6$ since there are 6 different ways to map the non identity elements in the set $\{e, x, y, z\}$ to itself while letting the identity be fixed. These maps indeed preserve the group structure of H. By Corollary 2.44 , $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$ and since H is self-centralizing we have that

$$|N_G(H) : C_G(H)| = \frac{|N_G(H)|}{|C_G(H)|} = \frac{|N_G(H)|}{4} \leq 6$$

so $|N_G(H)| \leq 24$. Now $\{1, 2, 3, 4, 5, 6, 7\}$ is a union of orbits of H which contains the fixed points of all elements of $H \setminus \{e\}$ since no element in $H \setminus \{e\}$ can fix four points. The action on further orbits is regular, since the only points that can be fixed by some non identity element under the action of H is in $\{1, 2, 3, 4, 5, 6, 7\}$ and the stabilizer is trivial. There is at least one more orbit since $n \geq 8$. By the orbit-stabilizer theorem, the size of the orbits induced by the regular action is equal to the order of H. Let $\{a, b, c, d\}$ be such an orbit and let W be the set of elements of G which permutes this set. Clearly $W \cong S_4$ since G is sharply 4-transitive. By lemma 2.69, H is a normal subgroup of W which is equivalent to $W \leq N_G(H)$ and since $|N| \leq 24$ and $|W| = 24$ we have $N = W \cong S_4$. Let g be an element of $N \setminus H$ of order 2. By the previous lemma, g has two fixed points in $\{a, b, c, d\}$. If H has two such orbits then g fixes two points in each so g fixes four points, a contradiction since G is sharply 4-transitive. Thus there are precisely four more points being permuted other than $\{1,2,3,4,5,6,7\}$. This yields $n = 10$ or $n = 11$ since we must allow for the possibility that the point 7 does not occur. However, by lemma 2.68 we cannot have $k = 4$ and $n = 10$. Thus $n = 11$.

step 3. We show that if If $k \geq 5$ and G is nontrivial then $n = 12$.
Suppose that G is sharply k-transitive of degree n. Then by proposition 2.64, G_x is sharply $(k-1)$-transitive of degree $n-1$. If G_a is trivial, then $|G_a| = (n-1)!$ or $\frac{(n-1)!}{2}$ which implies $|G| = n!$ or $|G| = \frac{n!}{2}$. This shows that G is also trivial. Equivalently, if $|G|$ is nontrivial then G_a is nontrivial so let us suppose that G is nontrivial. If $k = 5$ then G_a is a nontrivial sharply 4-transitive group of degree $n-1$. It was shown in step 2 that the only nontrivial sharply 4-transitive group is of degree 11. Hence $n-1 = 11$ which implies $n = 12$. In this same way, $k = 6$ yields $n = 13$. However, it was shown in lemma 2.68 that this group does not exist. It now follows easily by induction that no trivial groups exist for $k \geq 6$ and the theorem is proved. □

3 Construction

We are now prepared to begin the detailed construction of the Mathieu groups. As stated before, we will use the construction due to Witt.

Lemma 3.1. *Let G be k-transitive $(k \geq 2)$ on a set M. Let $y \in G$ and $b \in M$ with $yb \neq b$ and let $x \in S_{M\cup\{a\}}$ with $xa \neq a$. Let H be the group generated by the elements of G and x, i.e., $H =< G, x >$ and suppose that $x^2 = y^2 = (xy)^3 = 1$ and $xG_bx = G_b$. Then H is $(k+1)-transitive$ on $M \cup \{a\}$ with $H_a = G$*

Proof. Define $GxG = \{g_1xg_2 | g_1, g_2 \in G\}$ and let $K = G \cup GxG$. Then K is clearly nonempty. Take some $g_1xg_2 \in GxG$ and since

$$x^2 = 1 \Leftrightarrow x = x^{-1}$$

we see that $(g_1xg_2)^{-1} = g_2^{-1}x^{-1}g_1^{-1} \in GxG$ so K is closed under inverses. We need to show that K is closed under multiplication to conclude that it is a group. Given an element $g \in G$, we see that

$$gg_1xg_2 \in GxG$$

and also that

$$g_1xg_2g \in GxG$$

so multiplication by an element of G with an element of GxG is also in K. Take two element $g_1xg_2, g_3xg_4 \in GxG$. The product of these can be written as

$$(g_1xg_2)(g_3xg_4) = g_1(xg_2g_3x)g_4$$

which is in the set $G(xGx)G$. Since have shown that K is closed by multiplication by G , it is sufficient to show that xGx is in K to conclude that K is closed under multiplication. From $x^2 = y^2 = 1$ and $(xy)^3 = 1$ we obtain

$$(xy)^3 = 1 \Leftrightarrow (xy)^2 = (xy)^{-1} = y^{-1}x^{-1} = yx \Leftrightarrow$$
$$\Leftrightarrow xy = yx(xy)^{-1} = yxy^{-1}x^{-1} = yxyx \Leftrightarrow xyx^{-1} = yxyxx^{-1} \Leftrightarrow xyx = yxy.$$

Now G is 2-transitive so by proposition 2.66, $G = G_b \cup G_b y G_b$. Hence

$$xGx = x(G_b \cup G_b y G_b)x = xG_bx \cup (xG_bx)xyx(xG_bx) = G_b \cup G_b xyx G_b =$$
$$= G_b \cup G_b yxy G_b \subseteq G \cup GxG = K$$

so K is closed under multiplication. In fact, K is equal to H since $GxG \subset K$ and $xGx \subset K$. It is clear that G fixes a. Take some $g_1 x g_2 \in H = G \cup GxG$. Clearly

$$g_1xg_2(a) = g_1(x(g_2))(a) = a$$

and hence $H_a = G$. Finally H_a is k-transitive so H is (k+1)-transitive by proposition 2.64. □

Lemma 3.2. *Let G be 2-transitive on M. Let $y \in G$, $a \in M$ with $ya \neq a$ and let $x_1, x_2, x_3 \in S_{M \cup \{1,2,3\}}$. Suppose that*

$$x_1 = (1\ a)(2)(3)...$$
$$x_2 = (1\ 2)(3)(a)...$$
$$x_3 = (2\ 3)(1)(a)...$$
$$y^2 = x_1^2 = x_2^2 = x_3^2 = 1$$
$$(x_1y)^3 = (x_2x_1)^3 = (x_3x_2)^3 = 1$$
$$(yx_2)^2 = (yx_3)^2 = (x_1x_3)^2 = 1$$
$$x_1G_ax_1 = x_2G_ax_2 = x_3G_ax_3 = G_a.$$

Then $H =< G, x_1, x_2, x_3 >$ is 5-transitive on $M \cup \{1,2,3\}$ and $H_{1,2,3} = G$.

Proof. By lemma 3.1, $K =< G, x_1 >$ is 3-transitive on $M \cup \{1\}$ with $K_1 = G$. Since $y^2 = (yx_2)^2 = 1$ and $x_2^2 = 1$ we have

$$(yx_2)^2 = 1 \Rightarrow yx_2 = (yx_2)^{-1} = x_2^{-1}y^{-1} \Rightarrow yx_2 = x_2y$$

so x_2 and y commutes. We show that $x_2 < G_a, y > x_2 =< G_a, y >$. In particular, given that $g \in< G_a, y >$, we want to show that $x_2gx_2 \in< G_a, y >$. Write $g = g_1g_2g_3g_4$. If $g_i \in G_a$ $(i = 1,2,3,4)$ we get that $x_2g_ix_2 \in G_a \subset<G_a, y >$ due to conditions. If $g_i = y = y^{-1}$, we get $x_2g_ix_2 = x_2yx_2 = y \in< G_a, y >$ since x_2 and y commute. Now define the map

$$< G_a, y > \rightarrow x_2 < G_a, y > x_2$$

$$g \mapsto x_2gx_2.$$

This is clearly a group homomorphism since

$$x_2(g_1g_2g_3g_4)x_2 = (x_2g_1x_2)(g_2x_2g_2)(g_3x_2g_3)(g_4x_2g_4)$$

so $x_2 g x_2$ is a product of elements in G_a, y and y^{-1}. Thus $x_2 < G_a, y > x_2 =< G_a, y >$. Using this, we obtain

$$x_2 K_1 x_2 = x_2 G x_2 = x_2 < G_a, y > x_2 =< G_a, y >= G = K_1.$$

By lemma 3.1 $L =< K, x_2 >$ is 4-transitive on $M \cup \{1, 2\}$ with $L_2 = K$. Again we see that x_3 commutes with x_1 and y so with the same argument as above we get that $x_3 L_2 x_3 = L_2$ so $H =< L, x_3 >$ is 5-transitive on $M \cup \{1, 2, 3\}$ and $H_3 = L$. We conclude that $H_{1,2,3} = L_{1,2} = K_1 = G$. □

It is time to state the theorem that is central in this thesis. Note how the generators of the two groups are choosen in such a way that it will obey the condition in the two previous lemmas.

Theorem 3.3. *Given the following permutations*

$$s = (4\ 5\ 6)(7\ 8\ 9)(10\ 11\ 12)$$

$$t = (4\ 7\ 10)(5\ 8\ 11)(6\ 9\ 12)$$

$$u = (5\ 7\ 6\ 10)(8\ 9\ 12\ 11)$$

$$v = (5\ 8\ 6\ 12)(7\ 11\ 10\ 9)$$

$$w = (5\ 11\ 6\ 9)(7\ 12\ 10\ 8)$$

$$x_1 = (1\ 4)(7\ 8)(9\ 11)(10\ 12)$$

$$x_2 = (1\ 2)(7\ 10)(8\ 11)(9\ 12)$$

$$x_3 = (2\ 3)(7\ 12)(8\ 10)(9\ 11)$$

then $M_{11} =< s, t, u, v, w, x_1, x_2 >$ is a sharply 4-transitive of degree 11 and $M_{12} =< M_{11}, x_3 >$ is a sharply 5-transitive of degree 12. This yields that $|M_{11}| = 7920$ and $|M_{12}| = 95040$

Proof. Let $H =< s, t >$. Since the set of generators of H commutes, H is abelian so an element of H is of the form $s^x t^y$. Clearly, the map

$$H \to C_3 \times C_3$$

$$s^x t^y \mapsto (x, y)$$

is an isomorphism so H is an elementary group of degree 9. It is easy to check that H is transitive, hence regular by proposition 2.52. Now let $Q =< u, v, w >$. The conjugates of the generators of H by the generators of Q are elements of H, so H is normalized by Q. We claim that Q is isomorphic to the quaternion group Q_8, a regular group of degree 8. By calculation, we see that Q has 8 elements. The quaternion group has the following presentation

$$Q_8 =< i, j, k \mid i^2 = j^2 = k^2 = ijk > .$$

It is then enough to show that u, v, w satisfies the relations in Q_8 with the following maps

$$u \mapsto i$$
$$v \mapsto j$$
$$w \mapsto k$$

to conclude that $Q \cong Q_8$. We have

$$\begin{aligned} u^2 &= (5\ 7\ 6\ 10)(8\ 9\ 12\ 11)(5\ 7\ 6\ 10)(8\ 9\ 12\ 11) = (5\ 6)(7\ 10)(8\ 12)(9\ 11) \\ v^2 &= (5\ 8\ 6\ 12)(7\ 11\ 10\ 9)(5\ 8\ 6\ 12)(7\ 11\ 10\ 9) = (5\ 6)(7\ 10)(8\ 12)(9\ 11) \\ w^2 &= (5\ 11\ 6\ 9)(7\ 12\ 10\ 8)(5\ 11\ 6\ 9)(7\ 12\ 10\ 8) = (5\ 6)(7\ 10)(8\ 12)(9\ 11) \end{aligned}$$

and

$$\begin{aligned} uvw = (5\ 7\ 6\ 10)(8\ 9\ 12\ 11)(5\ 8\ 6\ 12)(7\ 11\ 10\ 9)(5\ 11\ 6\ 9)(7\ 12\ 10\ 8) = \\ = (5\ 6)(7\ 10)(8\ 12)(9\ 11) \end{aligned}$$

so the relations are indeed satisfied. Now let $G =< s, t, u, v, w >$, so G is generated by the elements in H and Q . Thus every element in G is of the form

$$h_1 q_1 h_2 q_2 \cdots h_{r-1} q_{r-1} h_r q_r$$

for some positive integer r. Since Q normalizes H, for all $h \in H$ and $q \in Q$ we have $qh = h'q$ for some $h' \in H$. It now follows by induction that $G = HQ$ and G is a sharply 2-transitive group of degree 9, and $G_4 = Q$. If we let $a = 4$ in the preceding lemma, we see that x_1, x_2 and x_3 normalize Q so that

$$x_1 G_4 x_1 = x_2 G_4 x_2 = x_3 G_4 x_3 = G_4.$$

Moreover, if

$$y = s^{-1} u^2 s = (4\ 6)(7\ 12)(8\ 11)(9\ 10)$$

we see that the condition for y, x_1, x_2 and x_3 in the previous lemma are satisfied. Thus by lemma 3.2 we have that M_{12} is is 5-transitive of degree 12. Furthermore, M_{11} is a subgroup of M_{12} fixing 3, i.e $(M_{12})_3 = M_{11}$ thus proposition 2.64 implies that M_{11} is 4-transitive of degree 11. Lemma 3.2 ensures that M_{12} is sharply 5-transitive and it also follows that M_{11} is sharply 4-transitive. Finally, the last statement follows by proposition 2.65. □

We have successfully constructed M_{11} and M_{12}, and we have already completed enough preparatory work to a detailed construction to the remaining Mathieu groups. However, we decided to leave that task for future readers.

4 Simplicity

It is time to show that the Mathieu groups M_{11} and M_{12} are indeed simple.

Theorem 4.1. *M_{11} is simple.*

Proof. Set $G = M_{11}$ and we know that $|G| = 11 \cdot 10 \cdot 9 \cdot 8$. By Sylow's theorem, there exists a subgroup P of order 11. Let $P =< x >$ be the subgroup generated by x. Moreover, x must be an $11 - cycle$ which acts transitively on a set of 11 elements. If $A \geq P$ then A is clearly transitive and if A is abelian then by proposition 2.52, A is regular. This means that A must have order 11 because otherwise it would contradict the fact that it is sharply $1 - transitive$ and we get that $A = P$. Thus P is self-centralizing by proposition 2.28. Since $Aut\ P$ is isomorphic to $(\mathbb{Z}/11\mathbb{Z})^{\times}$ we have that $|Aut\ P| = 10$. Furthermore, $N_G(P)/C_G(P)$ is isomorphic to a subgroup of $Aut\ P$ so by Lagrange's theorem, $|N_G(P) : C_G(P)| = |N_G(P) : P|$ must divide 10. Suppose $2 \mid |N_G(P) \mid$ so $N_G(P)$ has an element y of order 2 by Cauchy's theorem. Since the degree 11 is odd, y must fix a point, say 1. Now $y \in N_G(P)$ so $yxy^{-1} = yxy = x^{-1}$ and

$$y(x^r(1)) = x^{-r}(y(1)) = x^{-r}(1)$$

. This shows that y is a product of five transposition and hence $y \notin A_{11}$, which is a contradiction since all generators of M_{11} given in Theorem 3.3 are even permutations and finite products of even permutation cannot give an odd permutation. Thus we have $|N_G(P) : P| = 1$ or 5.

Now suppose that H is a nontrivial normal subgroup of G. Since G has prime degree, it is primitive, and since H transitive (see proposition 2.9), the given action has exactly one orbit. The Orbit-Stabilizer theorem gives

$$\frac{|H|}{|H_x|} = |Hx| \implies |H| = 11|H_x|$$

and hence $11 \mid |H|$. By Cauchy's theorem there is an element that generates a cyclic subgroup P with $|P| = 11$ such that $P \subset H$. Now $N_G(P)$ acts on P by conjugation so it will equal the stabilizer of an element in the set being acted on. Thus by proposition 2.53, $G = HN_G(P)$ and hence $N_G(P) \not\subseteq H$ since otherwise G would equal to H. By the above this implies that $N_H(P) = P$ and since P is abelian, $Z(P) = P$ so $P = Z(N_H(P))$ and which shows that P is in the center of its normalizer. Thus Theorem 2.56 implies that H has a normal $11 - complement$ K. Then $k \trianglelefteq G$ and $11 \nmid |K|$ yields $K = \{e\}$. The orbit stabilizer theorem forces $|H| = 11$ since $|Hx| = |H||H_x|$ with $|H| = 11^n$ for some $n \geq 1$ implies $|H_x| = \frac{11}{11^n}$ and n must be equal to 1. Finally we have $H = P$ and $G = PN_G(P) = N_G(P)$ with the result we obtained above $|N_G(P) : P| = |G : P| \neq 1$ or 5, contradiction and M_{11} is simple.

□

Before showing that M_{12} is simple, we state the two following crucial facts. However, we choose to show only the latter.

Proposition 4.2. *Let G be an m-transitive permutation group of degree n which has a regular normal subgroup N.*

i) If $m = 2$, then $n = |N| = p^k$ for some prime p.

ii) If $m = 3$, then either $n = 3$ or $n = 2^k$.

iii) If $m = 4$, then $n = 4$

iv) We cannot have $m \geq 5$.

Proposition 4.3. *Let G be a primitive permutation group acting on a set A, and suppose that G has no regular normal subgroups. Let $a \in A$. If G_a is simple, then G is simple.*

Proof. Let $N \trianglelefteq G$ with $N \neq \{e\}$. Since G is primitive, N is transitive by proposition 2.9. Now G_a is simple and $N_a \trianglelefteq G_a$ so $N_a = \{e\}$ or G_a. Suppose that $N_a = \{e\}$. But this means that N_a is a regular normal subgroup of G, contradiction. Thus $N_a = G_a$ and since N is transitive, its action on A possess only one orbit that is equal to $|A|$. Thus the orbit stabilizer theorem yields

$$|N : N_a| = |G : G_a| = |A|.$$

Hence $N = G$ is simple. $\square$

Theorem 4.4. *M_{12} is simple.*

Proof. This Follows from the simplicity of M_{11}. We stated in the proof of theorem 3.3 that $(M_{12})_3 = M_{11}$, i.e., M_{11} being the stabilizer subgroup of M_{12} with respect to 3. We have shown earlier that there are no nontrivial sharply 4-transitive groups of degree 11 other than M_{11} except for (possibly) the trivial ones, which shows that M_{11} is a maximal subgroup of M_{12}. Thus M_{12} is primitive. By theorem 4.2, M_{12} has no regular subgroups. It finally follows by the previous proposition that M_{12} is simple. $\square$

References

[1] Donald L. Passman. *Permutation Groups*. 1968.

[2] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 2004.

[3] Wikipedia contributors. *Group Action*. 2023. URL: `https://en.wikipedia.org/wiki/Group_action`.

[4] Wikipedia contributors. *Mathieu Group*. 2023. URL: `https://en.wikipedia.org/wiki/Mathieu_group`.

[5] Rikard Bögvad. *Personal Communication*. 2023. Stockholm University.