The Mathieu groups

Leo Taslaman

May 26, 2009
Abstract

In the 19th century E. Mathieu discovered and studied five multiply transitive permutation groups. The groups are called the Mathieu groups and it turned out that all five are simple. In this thesis these remarkable groups are constructed, with special focus on the largest Mathieu group $M_{24}$. All maximal subgroups of $M_{24}$ will be described and classified. It is also shown that the other Mathieu groups are subgroups of $M_{24}$. Finally the simplicity of the five Mathieu groups is proved.
Acknowledgements

I wish to express my deepest respect and most sincere gratitude to my supervisor Professor Arne Meurman, for guidance, editorial support and engagement in my questions and ideas. I also wish to thank him for the choice of subject, which suited me perfectly.

Leo Taslaman, May 2009
Contents

Introduction 4

Notation 5

1 Preliminaries 6
   1.1 Basic definitions and lemmas 6
   1.2 Multiply transitive groups 8
   1.3 The finite projective groups 12

2 The Steiner System $S(5, 8, 24)$ and the Golay code 15
   2.1 Construction 15
   2.2 Basic machinery 18
   2.3 MOG 21
   2.4 Uniqueness of $S(5, 8, 24)$ and $\mathcal{C}$ 24

3 The Mathieu group $M_{24}$ 31
   3.1 Eight maximal subgroups 32
       3.1.1 The projective group $L_2(23)$ 32
       3.1.2 The Octad Stabilizer 33
       3.1.3 The Duum Stabilizer 33
       3.1.4 The Sextet Stabilizer 34
       3.1.5 The Trio Stabilizer 35
   3.2 The involutions in $M_{24}$ 37
   3.3 A further maximal subgroup 42
   3.4 Proof of maximality 45
   3.5 Generators of $M_{24}$ 58

4 Simplicity of the Mathieu groups 59
5 Uniqueness of the small Mathieu groups  62

A GAP and permutation groups  68
Introduction

The classification theorem of finite simple groups states that except for 26 groups, all finite simple groups are isomorphic to a cyclic group of prime order, an alternating group of degree at least five or a simple group of Lie type. The 26 exceptional groups are called sporadic. The five Mathieu groups were the first sporadic groups found. They were discovered and studied by Emile Mathieu in the 19th century (see [11], [12] and [13]). It took almost century before the next sporadic group was found. Mathieu found the groups when he investigated multiple transitivity and did not know that the groups were simple. This was first shown in the 1930’s by Ernst Witt, when he did researched on the Steiner System S(5, 8, 24) (see [14]). It turned out that the largest Mathieu group $M_{24}$ could be defined as the automorphism group of this system.

In Chapter 1 we will introduce the concept of multiply transitive groups and theory that is necessary for the main part of this thesis. In Chapter 2 we use Curtis [1] approach to discuss the Steiner system S(5, 8, 24), the Golay code and the link in between. We will here introduce the powerful tool MOG (Miracle Octad Generator) and find the group $M_{24}$. Chapter 3 is dedicated to the Mathieu group $M_{24}$. We will go through all maximal subgroups and on the way find the other four Mathieu groups $M_{11}$, $M_{12}$, $M_{22}$ and $M_{23}$. A major part of this chapter discuss a proof that simultaneously shows the maximality of claimed maximal groups and that there are no further maximal groups. In Chapter 4 we show simplicity of the Mathieu groups and in Chapter 5 we give a new uniqueness proof of the small Mathieu groups, i.e $M_{11}$ and $M_{12}$.
Notation

1 the identity element
\langle 1 \rangle the trivial group
\langle G_a \rangle the isotropy subgroup of \( G \) fixing \( a \)
\langle G^\rho \rangle the conjugate \( \rho G \rho^{-1} \)
\langle A,B \rangle a group \( G \) such that \( A \triangleleft G \) and \( G/A \cong B \)
\mathbb{F}_q the finite field of order \( q \)
p^k the elementary abelian group of order \( p^k \), where \( p \) is a prime
\langle L_n(q) \rangle the projective linear group \( PSL_n(\mathbb{F}_q) \)
\langle M_{X-1} \rangle the isotropy subgroup of the Mathieu group \( M_X \)
\mathbb{Z}_m cyclic group of order \( m \)
\langle S_n \rangle the symmetric group of degree \( n \)
\langle A_n \rangle the alternating group of degree \( n \)
\langle C \rangle the Golay code
\langle H \rangle the extended (8,4) Hamming code
\langle A \subseteq B \rangle \( A \) is a subset of \( B \)
\langle A \subset B \rangle \( A \) is a proper subset of \( B \)
\langle H \leq G \rangle \( H \) is a subgroup of \( G \)
\langle H < G \rangle \( H \) is a proper subgroup of \( G \)
1. Preliminaries

1.1 Basic definitions and lemmas

Lemma 1.1. If $H \leq G$ then $N_G[H]/C_G[H]$ is isomorphic to a subgroup of $\text{Aut}(H)$.

Proof. The kernel of the homomorphism

$$
\phi : N_G[H] \rightarrow \text{Aut}(H)
$$

is $C_G[H]$. So the lemma follows from the first isomorphism theorem. ■

Lemma 1.2. Let $G$ be a group and $N$ a normal subgroup of $G$. If $P$ is a Sylow $p$-subgroup of $N$ then $G = N_G[P]N$.

Proof. Sylow’s second theorem and the fact that $N$ is normal implies that $\forall g \in G \exists n \in N$ such that $P^g = P^n$. Thus $g^{-1} \in N_G[P]$, implying $g \in N_G[P]N$. ■

Lemma 1.3. If $\rho$ and $\sigma$ are two elements in a permutation group then $\sigma \rho \sigma^{-1}$ and $\rho$ has the same cycle shapes. Further if $(i_1, i_2, \ldots, i_k)$ is a cycle in $\rho$ then $(\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k))$ is a cycle in $\sigma \rho \sigma^{-1}$.

Proof. If $\rho = \rho_1 \rho_2 \ldots \rho_k$, where $\rho_i$ are disjoint cycles, then

$$
\sigma \rho \sigma^{-1} = \sigma \rho_1 \sigma^{-1} \rho_2 \sigma^{-1} \ldots \rho_k \sigma^{-1}.
$$

So it is enough to prove the lemma for one arbitrary cycle. Let $x = (i_1, i_2, \ldots, i_n)$ and $\sigma(i_m) = j_m$ for $m = 1, 2, \ldots, n$. Then it is straightforward to check that $\sigma x \sigma^{-1} = (j_1, j_2, \ldots, j_n)$. ■
Remark 1.4. If $\sigma$ centralizes $\rho$ the above lemma implies that $\sigma$ permutes the fixed points of $\rho$.

We say that a permutation group is $1/2$-transitive if all orbits have the same length and transitive if there is only one orbit. If all isotropy subgroups are trivial we say that the group is semiregular. A semiregular transitive group is called regular.

If a group $G$ is transitive on a set $A$ then there is a one to one correspondence between the cosets of an isotropy subgroup $G_a$ and the elements in $A$, namely $hG_a \leftrightarrow b$ if and only if $h(a) = b$. Thus we have the shown the for this text very important lemma.

Lemma 1.5. If $G$ is transitive on $A$ and $a \in A$ then $|A| = [G : G_a]$.

Corollary 1.6. If $G$ acts regularly on a set $A$ then $|A| = |G|$.

If $G$ is a transitive group acting on a set $A$ we say that a subset $B \subseteq A$, $|A| > |B| > 1$, is a set of imprimitivity if $\forall g \in G \ gB \cap B = B$ or $gB \cap B = \emptyset$. If we remove the condition on the size of $B$ we say that $B$ is a block. Clearly a set of imprimitivity yields a natural partition of $A$ into subsets of size $|B|$. Thus $|B|||A|$. If no set of imprimitivity exist we say that $G$ is primitive. If $|A|$ is a prime $G$ is obviously primitive.

Lemma 1.7. If $G$ is a transitive permutation group and $N \triangleleft G$ then $N$ is $1/2$-transitive. If in addition $N$ is nontrivial and $G$ is primitive then $N$ is transitive.

Proof. Let $S$ be an orbit of $N$ of minimal length. Then $\forall g \in G$ we have $N(gS) = (Ng)S = (gN)S = g(NS) = gS$ so $gS$ is a union of orbits of $N$. Since $S$ is of minimal length and $|S| = |gS|$ we see that $gS$ is exactly one orbit. Now $G$ is transitive so every orbit of $N$ has the same length (having the form $gS$). Thus $N$ is $1/2$ transitive. Finally two different orbits are disjoint so $S$ form a set of imprimitivity for $G$. So if $G$ is primitive then we have two cases. Either $|S| = 1$ implying $N$ is trivial, or $|S| = |A|$ implying $N$ is transitive.

Theorem 1.8. Let $G$ be transitive on a set $A$. If and $a \in A$ then $G$ is primitive if and only if $G_a$ is a maximal subgroup.
Proof. If \( G \) is not primitive there is a set of imprimitivity \( B \) containing \( a \). We want to show that \( G_a < G_B < G \). As \( G \) is transitive \( G \neq G_B \). Since \( G \) is transitive \( \exists g \in G \) such that \( ga \in B \setminus \{a\} \). Thus \( g \in G_B \setminus G_a \). Conversely suppose there exist \( H \) such that \( G_a < H < G \). We want to show that \( Ha = B \) is a set of imprimitivity. Since \( G_a < H \) we have \( |B| > 1 \). If \( |A| = |B| \) then \( H \) is transitive and by Lemma 1.5 \( |A| = [G : G_a] = [H : G_a] \). Contradiction. Finally suppose that \( gB \cap B \neq \emptyset \) and \( b \in gB \cap B \), then \( \exists h_1, h_2 \in H \) such that \( h_1a = gh_2a = b \) and hence \( h_1^{-1}gh_2 \in G_a \). This yields \( g \in H \) and \( gB \cap B = B \). \( \square \)

### 1.2 Multiply transitive groups

A permutation group \( G \) on set \( A \) is called \textbf{k-fold transitive} if for every two ordered subsets of \( A \), \( (a_1, a_2, \ldots, a_k) \), \( a_i \neq a_j \) and \( (b_1, b_2, \ldots, b_k) \), \( b_i \neq b_j \), there is a permutation \( \rho \in G \) such that \( \rho(a_i) = b_i \) for \( i = 1, \ldots, k \). If in addition the identity is the only permutation fixing \( k \) elements we say that \( G \) is \textbf{sharply k-fold transitive}. Note that if \( G \) is sharply \( k \)-fold transitive and \( \sigma \) is another element satisfying \( \sigma(a_i) = b_i \) for \( i = 1, \ldots, k \), then \( \rho \sigma^{-1} \) fixing \( k \) elements and thus equals the identity. Hence a permutation group is sharply transitive if and only if for each pair of ordered sets \( (a_1, a_2, \ldots, a_k) \) and \( (b_1, b_2, \ldots, b_k) \) there is exactly one permutation in \( G \) satisfying \( a_i \mapsto b_i \).

If \( G \) is a sharply \( k \)-fold transitive on a set \( A \), \( |A| = n \), and \( a_i, b_i \in A \) for \( i = 1, \ldots, n \), then there is a one to one correspondence between ordered sets \( (b_1, b_2, \ldots, b_k) \) and permutations in \( G \), namely:

\[
(b_1, b_2, \ldots, b_k) \leftrightarrow (a_1 \ a_2 \ldots \ a_k \ldots) \\
(b_1 \ b_2 \ldots \ b_k \ldots)
\]

Thus \( |G| = n(n-1) \cdots (n-k+1) \).

**Example 1.9.** It is obvious that \( S_n \) is sharply \( n \)-fold transitive. Since \( (n-1) \)-fold transitivity implies \( n \)-fold transitivity we see that \( A_n \) is \( (n-2) \)-fold transitive. There is exactly two permutations in \( S_n \) fixing \( n - 2 \) elements and only one of them is even. Thus \( A_n \) is sharply \( (n - 2) \)-fold transitive. Alternatively we can see this by considering the order of \( A_n \). \( \square \)

**Lemma 1.10.** Let \( G \) be a transitive permutation group on a set \( A \) where \( |A| \geq 2 \). Then \( G \) is \( k \)-fold transitive if and only if \( G_a \) is \((k-1)\)-transitive on \( A \setminus \{a\} \).
Proof. If \( G \) is \( k \)-fold transitive \( G_a \) obviously \((k - 1)\)-fold transitive. For the other direction pick any two ordered subsets of \( A \), \( \{a_1, a_2, \ldots, a_k\} \) and \( \{b_1, b_2, \ldots, b_k\} \). Since \( G \) is transitive we can find \( \rho \in G \) such that \( \rho(a_1) = b_1 \). Now use the \((k - 1)\)-transitivity and take \( \sigma \in G_{b_1} \) such that \( \sigma \rho(a_i) = b_i \). It follows that \( \sigma \rho \in G \) satisfies \( a_i \mapsto b_i \) for \( i = 1, \ldots, k \). \( \blacksquare \)

Lemma 1.11. If \( G \) is doubly transitive on a set \( A \) then \( G \) is primitive.

Proof. Assume \( B \subset A \) is a set of imprimitivity and pick \( a, b \in B \) and \( c \in A \setminus B \). Since \( G \) is doubly transitive we can find \( g \in G \) such that \( g(a) = a \) and \( g(b) = c \), contradicting that \( B \) is a set of imprimitivity. \( \blacksquare \)

Remark 1.12. Note that together with Lemma 1.8 this says that doubly transitivity implies that the isotropy groups are all maximal subgroup.

So far the only multiply transitive groups we have seen is the symmetric and alternating groups. We consider these groups trivial and start the work of ruling out the possibility for a nontrivial group to be more than sharply 5-fold transitive.

Lemma 1.13. Let \( G \) be a \( k \)-fold transitive group and \( H \) a subgroup fixing \( k \) points. If \( P \) is a Sylow \( p \)-subgroup of \( H \) that fixes \( m \geq k \) points then \( N_G(P) \) is \( k \)-fold transitive on the \( m \) points fixed by \( P \).

Proof. Let \( a_1, a_2, \ldots, a_k \) be the points fixed \( H \) and \( b_1, b_2, \ldots, b_k \) \( k \) arbitrary points fixed by \( P \). We want to show that there is an element in \( N_G(P) \) mapping \( a_i \mapsto b_i \) for \( i = 1, \ldots, k \). Since \( G \) is \( k \)-fold transitive there is at least one such element \( g \in G \). So we have \( g(a_i) = b_i \) for \( i = 1, \ldots, k \). Now \( P \) fixes \( b_1, b_2, \ldots, b_k \) and so \( P^g \) must fix \( a_1, a_2, \ldots, a_k \) and thus be another Sylow \( p \)-subgroup of \( H \). By the second Sylow theorem \( \exists h \in H \) such that \( P = P^{gh} \).

Finally \( gh \in N_G(P) \) and \( gh(a_i) = g(a_i) = b_i \) for \( i = 1, \ldots, k \). \( \blacksquare \)

We need the following lemma to achieve contradictions later on.

Lemma 1.14. If \( G \) is a sharply \( k \)-fold transitive group of degree \( n \) then we cannot have \((k = 4 \text{ and } n = 10)\) or \((k = 6 \text{ and } n = 13)\).

Proof. We deal with the two very similar cases separately.

Case \( k = 4 \) and \( n = 10 \)
We know that \( |G| = 10 \cdot 9 \cdot 8 \cdot 7 \) and so there is Sylow 7-subgroup \( P \). Since
P must have order seven it is generated by a 7-cycle, say \( g = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7) \). Further \( G \) is 3-transitive and \( P \) is a Sylow 7-subgroup fixing the points 8, 9 and 10. Thus Lemma 1.13 implies that \( N_G[P] \) is 3-transitive on \( \{8, 9, 10\} \) and we have a restriction homomorphism \( \varphi : N_G[P] \rightarrow S_3 \). From Lemma 1.1 we know that \( N_G[P]/C_G[P] \cong H \leq \text{Aut}(P) \cong \mathbb{Z}_6 \). As \( S_3 \) is not abelian \( \varphi[C_G[P]] \) cannot be trivial and so since it is a normal subgroup of \( S_3 \) it is isomorphic to either \( A_3 \) or \( S_3 \). In either case \( 3 | |C_G[P]| \) and we can find \( h \in C_G[P] \) of order 3. But then \( gh \) has order 21 and \( (gh)^7 \neq 1 \) fixes seven points. Contradiction.

Case \( k = 6 \) and \( n = 13 \)
Now \( |G| = 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \) so \( G \) has a Sylow 5-subgroup \( P \) of order five. Hence \( P = \langle g \rangle \) for some \( g \). If \( g \) has only one 5-cycle then it fixes eight points. \( \varphi \) does not fix any points, so \( g \) is either a product of two 5-cycles or a product of a 5-cycle and a 3-cycle. If \( g \) is a product of two 5-cycles then \( g = (1 \ 2 \ 3 \ 4 \ 5)(6 \ 7 \ 8 \ 9 \ 10) \). With the same argument as in the previous case \( C_G[P] \) contains an element \( h \) of order 3. Further the element \( gh \) has order 15 and must consist of 3-cycles and 5-cycles. Since \( (gh)^6 = g \) we see that \( gh \) has two 5-cycles and one 3-cycle. But then \( (gh)^5 \neq 1 \) fixes ten points. Contradiction.

Lemma 1.15. The involutions in \( S_4 \) that acts without fixed points form together with the identity a regular normal subgroup.

Proof. It straight forward to check that \( H = \{1, (12)(34), (13)(24), (14)(23)\} \) forms a regular subgroup. Since conjugation preserves cycle shapes and \( H \) contains all elements of cycle shape \( 2^2 \) the normality follows.

We now show that there are at most two choices for the degree of a sharply \( k \)-fold transitive group, for \( k \geq 4 \).

Theorem 1.16. If \( G \) is a nontrivial sharply \( k \)-fold transitive group of degree \( n \), where \( k \geq 4 \), then \( (k = 4 \text{ and } n = 11) \) or \( (k = 5 \text{ and } n = 12) \).

Proof. Suppose \( G \) is sharply 4-transitive. If we consider the order \( |G| = 7! / 6 = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 / (6 \cdot 5) = 7 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040 \) and \( |S_7 : G| = 6 \). Since \( S_7 \) permutes the left cosets of \( G \) transitively we have a homomorphism \( \varphi : S_7 \rightarrow S_6 \). Further \( \varphi \) cannot be injective so the kernel is nontrivial. Since the only nontrivial proper normal subgroup of \( S_7 \) is \( A_7 \) we must have \( \text{Ker}(\varphi) = A_7 \). A contradiction since \( S_7 / A_7 \cong 2 \) cannot be transitive on six elements. Thus \( n \geq 8 \).
Next we want to show that any two nonidentity involutions are conjugates. Since such an involution fixes at most three points it has at least two 2-cycles. Let \( x = (a b)(c d) \ldots \) and \( y = (e f)(g h) \ldots \). Since \( G \) is 4-transitivity we can find \( z = \left( \begin{array}{cccc} a & b & c & d \\ e & f & g & h \end{array} \right) \) and so \( zxz^{-1} \) and \( y \) agree on four points. Thus \( zxz^{-1} = y \).

Let \( g = (1)(2)(3 4) \ldots \) and \( h = (1 2)(3)(4) \ldots \) and suppose \( g, h \in G \). Since \( g^2 \) and \( h^2 \) fixes four points we have \( g^2 = h^2 = 1 \). Further \( gh \) and \( hg \) agree on four points so \( gh = hg \). Let \( k = gh = (1 2)(3 4) \ldots \). Now \( g \) might have another fixed point, say 7. To avoid writing two cases we will always when writing \( (7) \) be open for the possibility that this cycle not occur. Since \( h \) centralize \( g \) Remark 1.3 implies that also \( h \) contains \((7)\). Now since both \( g \) and \( k \) are nonidentity involutions they are conjugates and have the same cycle shape. So \( k \) fixes say 5 and 6. Using Remark 1.3 again, we get that \( g \) and \( h \) both contains \((5 6)\). Hence

\[
\begin{align*}
g &= (1)(2)(3 4)(5 6)(7) \\
h &= (1 2)(3)(4)(5 6)(7) \\
k &= (1 2)(3 4)(5)(6)(7)
\end{align*}
\]

on \( \{1, 2, \ldots, 7\} \). These generate an elementary abelian subgroup \( \langle g, h, k \rangle = H \) of order four. Assume \( x \in C_G[H] \) and \( x \neq 1 \). As above \( x \) must permute all fixed points to \( g \), \( h \) and \( k \) each, and thus looks like

\[
x = (1 2)^{\sigma_1}(3 4)^{\sigma_2}(5 6)^{\sigma_3}(7) \ldots
\]

where \( \sigma_1, \sigma_2, \sigma_3 = 0 \) or 1. Since \( x \) fixes at most three points at least two of \( \sigma_1, \sigma_2 \) and \( \sigma_3 \) equals one. If exactly two of them equals one we have \( x \in H \) and if all three equals one \( xg \neq 1 \) fixes four points. Contradiction. Hence \( H = C_G[H] \) and by Lemma 1.1 we have \( |N_G[H]/C_G[H]| \leq |\text{Aut}(H)| \). Now \( H \) is elementary abelian of order four so \( \text{Aut}(H) \cong GL_2(2) \) and \( |\text{Aut}(H)| = 6 \). Thus \( |N_G[H]| \leq 24 \). Now \( n \geq 8 \) implies that \( H \) has an orbit \( \mathcal{O} \) disjoint from \( \{1, 2, 3, 4, 5, 6, 7\} \). Since no nonidentity element in \( H \) can have more fixed points, \( H \) acts regularly on \( \mathcal{O} \). Thus Corollary 1.6 implies that \( |\mathcal{O}| = 4 \). As \( G \) is sharply 4-transitive there exist a subgroup \( W \cong S_4 \) that permutes the elements in \( \mathcal{O} \). By Lemma 1.15 \( H \triangleleft W \). Since \( |W| = 24 \) and \( N_G[H] \leq 24 \) so \( N_G[H] = W \). Let \( y \in N_G[H] \setminus H \) be an involution. If \( H \) has another orbit
\(P\) then Lemma 1.15 implies that \(y\) has two fixed points in both \(O\) and \(P\). Contradiction. Thus \(n = 10\) or \(11\) depending on whether (7) occurs or not. But Lemma 1.14 forbid the case \(k = 4\) and \(n = 10\). Thus \(n = 11\).

Let \(k \geq 5\) and suppose \(G_a\) is sharply \((k - 1)\)-fold transitive of degree \(n - 1\). If \(G_a\) is one of the trivial cases \(G_a\) has order \((n - 1)!\) or \((n - 1)!/2\), implying that \(G\) has order \(n!\) or \(n!/2\) and thus is also trivial. Assume \(G\) is nontrivial of degree \(n\). If \(k = 5\) then \(G_a\) is sharply 4-fold transitive and of degree \(n - 1 = 11\). Thus \(n = 12\). If \(k = 6\) then \(G_a\) is 5-transitive of degree \(n - 1 = 12\) from what we just proved. This yields \(k = 6\) and \(n = 13\) contradicting Lemma 1.14. Finally if \(k > 6\) we get hold of case \(k = 6\) by looking at the pointwise stabilizer of \(k - 6\) points.

\[\square\]

### 1.3 The finite projective groups

The general linear group \(GL_n(q)\) is defined as the set of invertible \(n \times n\)-matrices with entries in \(\mathbb{F}_q\). The special linear group \(SL_n(q) \subseteq GL_n(q)\) is defined as the subgroup of matrices with determinant one. Let \(V\) be the set of \(n \times 1\) vectors over \(\mathbb{F}_q\). The projective space \(\mathbb{P}^{n-1}\) is defined as the set of one-dimensional subspaces of \(V\). We call \(\mathbb{P}^1\) the projective line. If \(v \in V\) we write the respective element in \(\mathbb{P}^{n-1}\) as \(\langle v \rangle\). Clearly \(|\mathbb{P}^{n-1}| = (q^n - 1)/(q - 1)\).

Since \(GL_n(q)\) permutes the elements in \(\mathbb{P}^{n-1}\) there is an homomorphism

\[\varphi : GL_n(q) \longrightarrow S_{\mathbb{P}^{n-1}}.\]

**Lemma 1.17.** The kernel \(\text{Ker}(\varphi)\) consists of the matrices of the form \(cI\), \(c \in \mathbb{F}_q^\times\).

**Proof.** Obviously \(cI \in \text{Ker}(\varphi)\) for \(c \in \mathbb{F}_q^\times\). For the other direction let \(A \in \text{Ker}(\varphi)\). Let \(e_1, e_2, \ldots, e_n\) be the natural basis in \(\mathbb{F}_q^n\). The calculation

\[Ae_i = a_ie_i, \quad \text{for some} \quad a_i \in \mathbb{F}_q^\times\]

shows that the \(i\)th column in \(A\) equals \(a_ie_i\). As this holds \(\forall i, A\) is diagonal. Finally

\[a_ie_i + a_je_j = A(e_i + e_j) = c(e_i + e_j)\]

shows that \(c = a_i = a_j\) for all \(i\) and \(j\). Thus \(A = cI\).

\[\square\]
If we in $GL_n(q)$ and $SL_n(q)$ factor out respective kernel of $\varphi$ we get two projective groups. As permutation groups these act faithfully on $\mathbb{P}^{n-1}$. The latter group

$$L_n(q) = SL_n(q)/(SL_n(q) \cap \text{Ker}(\varphi)),$$

plays an important role in this thesis.

**Lemma 1.18.** Let $q$ be a prime power. Then

\begin{align*}
(1) \quad |GL_n(q)| &= (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) \\
(2) \quad |SL_n(q)| &= |GL_n(q)|/(q - 1) \\
(3) \quad |L_n(q)| &= |SL_n(q)|/(n, q - 1).
\end{align*}

**Proof.** Let $A \in GL_n(q)$. The first column can be chosen in $q^n - 1$ ways. Suppose we already have chosen $i$ columns. Since the columns in $A$ are linearly independent we can chose the $(i + 1)$th column in $q^n - q^i$ ways. This yields (1). Further $SL_n(q)$ is the kernel of the determinant homomorphism. As the determinant clearly is onto (2) follows. For (3) we notice that $SL_n \cap \text{Ker}(\varphi)$ consist of all matrices $cI$ where $c^n = 1$. Since $\mathbb{F}_q^\times$ form a cyclic group the number of such $c$'s is the number of solutions to $x^{(n,q-1)} = x^{n+b(q-1)} = 1$ in $\mathbb{F}_q^\times$. Thus $|SL_n(q) \cap \text{Ker}(\varphi)| = (n, q - 1)$. \hfill \blacksquare

**Theorem 1.19.** Let $n \geq 2$. As a permutation group on $\mathbb{P}^{n-1}$, $L_n(q)$ is a 2-transitive.

**Proof.** Let $e_1, e_2, \ldots, e_n$ be the natural basis in $\mathbb{F}_q^n$ and $\langle e_1 \rangle, \langle e_2 \rangle, \ldots, \langle e_n \rangle$ the respective elements in $PL$. Pick $\langle x_1 \rangle, \langle x_2 \rangle \in PL$, $\langle x_1 \rangle \neq \langle x_2 \rangle$. Clearly the representatives $x_1, x_2 \in \mathbb{F}_q^n$ are linearly independent, so we can extend them to a basis $x_1, x_2, \ldots, x_n$. Choose $A \in GL_n(q)$ such that $Ae_i = x_i$ for $i = 1, \ldots, n$. Scale the first column in $A$ with $\frac{1}{\det(A)}$ and call the new matrix $B$. Clearly $\varphi(B) \in L_n(q)$ have the action $\langle e_1 \rangle \mapsto \langle x_1 \rangle$ and $\langle e_2 \rangle \mapsto \langle x_2 \rangle$. \hfill \blacksquare

If $n = 2$ then $|\mathbb{P}^1| = q + 1$. We see that $\mathbb{P}^1$ consist $\langle (0, 1)^T \rangle$ together with $\langle (x, 1)^T \rangle$, $x \in \mathbb{F}_q$. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_n(q)$. Since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax + b \\ cx + d \end{pmatrix} \quad \text{and} \quad \langle (ax+b, cx+d)^T \rangle = \langle (\frac{ax+b}{cx+d}, 1)^T \rangle$$

13
if \( cx + d \neq 0 \) and \( \langle (1, 0)^T \rangle \) otherwise,

we see that it is convenient to rename \( \langle (1, 0)^T \rangle = \infty \) and \( \langle (x, 1)^T \rangle = x \). With the convention \( 1/0 = \infty \), \( L_2(q) \) consist of all Möbius transformations

\[
x \mapsto \frac{ax + b}{cx + d}, \quad ad - bc = 1, \quad a, b, c, d \in \mathbb{F}_q.
\]

**Lemma 1.20.** The group \( L_2(q) \) is generated by \( \alpha : x \mapsto x + 1 \) and \( \gamma : x \mapsto -\frac{1}{x} \).

**Proof.** Define \( \beta_a : x \mapsto a^2x \quad \forall a \in \mathbb{F}_q \). If \( c = 0 \) then \( d = a^{-1} \) and

\[
\frac{ax + b}{cx + d} = a^2x + ab = \alpha^{ab} \beta_a,
\]

otherwise

\[
\frac{ax + b}{cx + d} = a - \frac{1}{c^2x + cd} = \alpha^{a/c} \gamma \alpha^{cd} \beta_c.
\]

Finally

\[
\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a - 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a - a^2 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},
\]

were the matrices represent \( \alpha, \gamma \alpha^{a^{-1}} \gamma, \alpha^{-a^{-1}}, \gamma \alpha^{a-a^2} \gamma \) and \( \beta_a \) respectively, shows \( \alpha \) and \( \gamma \) generate every \( \beta_a \). Hence \( \langle \alpha, \gamma \rangle = L_2(q) \). \hspace{1cm} \blacksquare
2. The Steiner System $S(5, 8, 24)$ and the Golay code

2.1 Construction

We will in this section use Curtis approach and construct the Steiner System $S(5, 8, 24)$ and the Golay code simultaneously.

**Definition 2.1.** A Steiner System $S(i, j, k)$ is a family of $j$-element subsets of a $k$-element set, $\Omega$, with the property that any $i$ elements in $\Omega$ lie in exactly one of them.

If a Steiner System $S(i, j, k)$ exist it is of size $\binom{k}{i}/\binom{j}{i}$. It can be seen as the number of ways we can choose $i$ points divided by the number of ways each $j$-set can be represented by $i$ points. This rules out a lot of cases since the quotient has to be an integer to make sense. For example the Steiner Systems $S(2, 4, 8)$ and $S(4, 7, 14)$ cannot exist.

The equality $\frac{\binom{24}{5}}{\binom{8}{5}} = 759$ shows that there is a chance for the Steiner System $S(5, 8, 24)$ to exist and the following theorem shows that this is the case. In the remaining part of this thesis we assume that

$$\Omega = \{\infty, 0, 1, 2, 3, ..., 22\}.$$ 

Why we use these numbers will become more clear later when we come to the projective subgroup.

**Theorem 2.2.** There exists a Steiner System $S(5, 8, 24)$.  

15
**Method of Proof.** We will think of the power set $P(\Omega)$ as a 24 dimensional vector space over $\mathbb{F}_2$ in the following way. Each element in $\Omega$ represents a coordinate in the vector space. If a member of $P(\Omega)$ contains an element the corresponding coordinate is one, otherwise zero. Further the symmetric difference is used as addition. In this vector space we shall find a linear code, $C$, were all non-empty code words have weight at least eight. Clearly no pair of code words has five points in common since their sum then would have weight less than eight. Moreover $C$ will contain 759 codewords with weight exactly eight and so form a Steiner System $S(5, 8, 24)$.

**Proof.** Let $\Lambda$ be an eight element set and consider the vector space $P(\Lambda)$. To please the eye we will in an obvious manner use a matrix notation on the vectors. Define the two three dimensional subspaces

$$P = \left\{ \begin{array}{cccccccc} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{array} \right\}, \quad L = \left\{ \begin{array}{cccccccc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{array} \right\}$$

Note that for every element $l \in L \setminus 0$ there are exactly three nonzero elements in $P$ that cuts $l$ evenly. We now extend the dimension by taking three copies of $\Lambda$ and glue them together and identify

$$\Omega = \begin{array}{ccc} \Lambda_1 & \Lambda_2 & \Lambda_3 \\ \hline \hline \end{array}$$

We will call $\Lambda_1, \Lambda_2$ and $\Lambda_3$ bricks. To describe the sets in $P(\Omega)$ we use notation $[R, S, T]_t$, where $R + t$ is the intersection with $\Lambda_1$, $S + t$ with $\Lambda_2$ and $T + t$ with $\Lambda_3$. If $t = 0$ we simply write $[R, S, T]$. We now define $C$ as the image of

$$\phi : \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times P \times P \times L \rightarrow P(\Omega)$$

16
\[(\sigma_1, \sigma_2, \sigma_3, X, Y, t) \mapsto [X + \sigma_1 \Lambda_1, Y + \sigma_2 \Lambda_2, X + Y + \sigma_3 \Lambda_1, t].\]

The space above to the left has dimension 12 and \(\phi\) is obviously a linear map, so the dimension of \(\mathcal{C}\) is 12-dim(Ker(\(\phi\))) by the dimension theorem. Let \(x = (\sigma_1, \sigma_2, \sigma_3, X, Y, t) \in \text{Ker}(\phi)\). Since the image of \(x\) is zero the intersections with the three bricks all has to be zero and so the sum of the intersections, seen as members of \(P(\Lambda)\), has to be zero. This implies that \(t\) is zero and we have Ker(\(\phi\)) = \{0\}. Thus \(\mathcal{C}\) has dimension 12.

To investigate the sizes of sets in \(\mathcal{C}\) we let \(X, Y \in P \setminus \{0\}, X \neq Y\) and \(t \in L \setminus \{0\}\). Up to permutation of the three bricks and complementation modulo \(\Lambda_i\) there are eight cases. In the Table 1 we see how each case cuts the three bricks.

<table>
<thead>
<tr>
<th>Case</th>
<th>Shape</th>
<th>(\Lambda_1)</th>
<th>(\Lambda_2)</th>
<th>(\Lambda_3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>([0, 0, 0])</td>
<td>0/8</td>
<td>0/8</td>
<td>0/8</td>
</tr>
<tr>
<td>2</td>
<td>([X, X, 0])</td>
<td>4/4</td>
<td>4/4</td>
<td>0/8</td>
</tr>
<tr>
<td>3</td>
<td>([X, Y, X + Y])</td>
<td>4/4</td>
<td>4/4</td>
<td>4/4</td>
</tr>
<tr>
<td>4</td>
<td>([0, 0, 0], t)</td>
<td>4/4</td>
<td>4/4</td>
<td>4/4</td>
</tr>
<tr>
<td>5</td>
<td>([X, X, 0], t)</td>
<td>([X \cap t] \equiv 0 \text{ (mod 2)})</td>
<td>4/4</td>
<td>4/4</td>
</tr>
<tr>
<td>6</td>
<td>([X, X, 0], t)</td>
<td>([X \cap t] \equiv 1 \text{ (mod 2)})</td>
<td>2/6</td>
<td>2/6</td>
</tr>
<tr>
<td>7</td>
<td>([X, Y, X + Y], t)</td>
<td>([X \cap t] \equiv [Y \cap t] \equiv 0 \text{ (mod 2)})</td>
<td>4/4</td>
<td>4/4</td>
</tr>
<tr>
<td>8</td>
<td>([X, Y, X + Y], t)</td>
<td>([X \cap t] \equiv [Y \cap t] \equiv 1 \text{ (mod 2)})</td>
<td>2/6</td>
<td>2/6</td>
</tr>
</tbody>
</table>

Table 1

The notation \(m/n\) in column \(\Lambda_i\) means that the case cut \(\Lambda_i\) in \(m\) or \(n\) points, depending on the value of \(\sigma_i\) in the function \(\phi\) above. It is worth noting that \(m/n\) gives the same information as \(n/m\). The only nontrivial cases are 7 and 8 and especially their cut with \(\Lambda_3\). In both cases \(X + Y \in P\) imply that \(|(X + Y) \cap t|\) equals 1, 2 or 3. On the other hand \(|(X + Y) \cap t| = |(X \cap t) + (Y \cap t)|\) is easily seen even, so it must be 2. Further we have \(|X + Y + t| = |X + Y| + |t| - 2|(X + Y) \cap t| = 4\).

From Table 1 we see that \(\mathcal{C}\) contains sets of size 0, 8, 12, 16 and 24. We call the subset of octads (i.e 8-sets) \(\mathcal{C}_8\) and calculate its cardinality.
case | shape | number of elements
-----|------|-----------------
1    | [0,0,0] | 3
2    | [X,X,0] | 7 \cdot 3 \cdot 2 \cdot 2 = 84
6    | [X,X,0]_i | 7 \cdot 4 \cdot 3 \cdot 2 = 168
8    | [X,Y,X+Y]_i | 7 \cdot 4 \cdot 3 \cdot 3 \cdot 2 = 504

Table 2

Folding up this gives 759 octads. ■

**Definition 2.3.** The linear code \( C \) described in Theorem 2.2 is called The (extended) Golay code.

The code \( C \) contains \( 2^{12} = 4096 \) codewords. From the construction we see that they have weight 0, 8, 12, 16 and 24. From the equality

\[
1 + 759 + 2576 + 759 + 1 = 4096
\]

we see that the number **dodecads** (i.e. codewords of weight twelve) is 2576 and so \( C \) has weight enumerator

\[
x^{24} + 759 x^{16} y^8 + 2576 x^{12} y^{12} + 759 x^8 y^{16} + y^{24}.
\]

(2.1)

We will later see that the Golay code is the unique linear code with this weight enumerator.

### 2.2 Basic machinery

In this section we will introduce some useful lemmas for later use. Until we have proved uniqueness of the Steiner System \( S(5,8,24) \) we denote an arbitrary such system \( \mathcal{C}_8 \).

**Lemma 2.4.** If \( A, B \in \mathcal{C}_8 \) and \( |A \cap B| = 4 \) then \( A + B \in \mathcal{C}_8 \).

**Proof.** Let \( A = \{a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8\} \) and \( B = \{a_1,a_2,a_3,a_4,b_1,b_2,b_3,b_4\} \) where \( \{a_5,a_6,a_7,a_8\} \cap \{b_1,b_2,b_3,b_4\} = \emptyset \). Assume \( A + B \) is not an octad. The octad \( X \) containing \( a_5,a_6,a_7,a_8,b_1 \) cannot contain a further \( a \) and so for the intersection with \( B \) to be even it has to contain a further \( b \), say \( b_2 \). Similarly the octad \( Y \) containing \( a_5,a_6,a_7,a_8,b_3 \) must contain a further \( b \),
but this $b$ cannot be $b_1$ or $b_2$ without equal $X$ and implying $X = Y = A + B$. Assume $b_4 \in Y$. The octad containing $a_5, a_6, a_7, b_1, b_3$ must contain a further $a$. If it contains $a_8$ it will have five points in common with $X$ and $Y$ and once more $X = Y = A + B$, so assume it contains $a_1$. But now it must contain a further $b$ and equals $X$ and $Y$. Contradiction. ■

**Corollary 2.5.** For each tetrad, i.e a set of size 4, there exist an unique partition of $\Omega$ into six tetrads such that the union of any two is an octad.

**Proof.** Let $S$ be a tetrad. Then each point not in $S$ defines another tetrad $T$ such that $S + T \in \mathcal{C}_8$. Assume $T$ and $T'$ are two different such tetrads. Then they are disjoint since otherwise $S + T$ and $S + T'$ would have five points in common. Let $T_1$ and $T_2$ be to different tetrads in the partition. Then $|(S + T_1) \cap (S + T_2)| = 4$ and by Lemma 2.4 the union is an octad. ■

Such a partition will be called a **sextet**.

**Lemma 2.6.** An octad cut the tetrads of a sextet $4^2.0^4$, $3^1.1^5$ or $2^4.0^2$.

**Proof.** Octads intersect each other in 0, 2, 4 or 8 elements. We divide the problem in three cases. The largest cut with a tetrad is of size

4. For the octad to cut all other octads found in the sextet properly, it has to cut one more tetrad in four points and so be disjoint from the remaining. Thus the cut is $4^2.0^4$.

3. Again due to the intersection of the octads found in the sextet, the intersections with the other five tetrads are all of size one and we have the cut $3^1.1^5$.

2. Since the cut is even the cuts with every tetrad has to be even. Thus the cut is $2^4.0^2$.

■

**Lemma 2.7.** If $\{x_1, x_2, ..., x_8\}$ is an octad, then the number of octads intersecting $\{x_1, x_2, ..., x_i\}$ in $\{x_1, x_2, ..., x_j\}$ is the $(j + 1)$th entry in the $(i + 1)$th line in Table 3.
Table 3

\[
\begin{array}{cccccccc}
759 & 506 & 253 & 330 & 176 & 77 & 210 & 120 \\
306 & 120 & 56 & 21 & 78 & 52 & 28 & 12 \\
40 & 16 & 4 & 1 & 30 & 0 & 16 & 0 \\
77 & 253 & 210 & 130 & 46 & 32 & 20 & 8 \\
176 & 78 & 52 & 28 & 46 & 32 & 20 & 8 \\
253 & 330 & 176 & 77 & 176 & 77 & 253 & 330 \\
210 & 130 & 40 & 16 & 210 & 130 & 40 & 16 \\
120 & 78 & 52 & 28 & 120 & 78 & 52 & 28 \\
56 & 40 & 16 & 4 & 56 & 40 & 16 & 4 \\
21 & 16 & 4 & 1 & 21 & 16 & 4 & 1 \\
0 & 4 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
2 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
4 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
8 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
16 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
32 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
64 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
128 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
256 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
512 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
1024 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
2048 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
4096 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
8192 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
16384 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
32768 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
65536 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
Table 3
\]

**Proof.** The number of octads containing \( \{x_1, \ldots, x_i\} \) is \( \binom{24-i}{5-i} \binom{8-i}{5-i} \) if \( i < 5 \) and 1 otherwise. Thus the rightmost entries in the table are established. If we see the table as a tree the remaining entries can be filled with the rule:

\[
\text{parent—right child = left child.}
\]

For instance the middle entry in the third row is 253 − 77 = 176.

**Lemma 2.8.** A linear code with weight enumerator (2.1) has a purely octad basis.

**Proof.** The only nontrivial part to prove is that all dodecads are sums of octads. Let \( F_1 \) be an octad and \( a, b \in F_1 \). By Table 3 there are 16 octads cutting \( F_1 \) in exactly \( a \) and \( b \). Thus

\[
\left| \left\{ \left\{ F_i, F_j \right\} \mid F_i, F_j \in \mathcal{C}_8, \ |F_1 \cap F_2| = 2 \right\} \right| = 759 \cdot \binom{8}{2} \cdot 16 \cdot \frac{1}{2}.
\]

It is clear that all members of the above set form dodecads, but some dodecads might be represented multiple times. Since each five points in a dodecad determines a sixth point the number of ways a dodecad can be presented as a sum \( F_i + F_j \) is

\[
\binom{12}{5} \cdot \frac{1}{6} \cdot \frac{1}{2},
\]

were we divide by two since the complement to the six points defines the same sum. Thus the number of unique dodecads that is the sum of two
octads is
\[
\frac{759 \cdot \binom{8}{2} \cdot 16 \cdot \frac{1}{2}}{\binom{12}{5} \cdot \frac{1}{6} \cdot \frac{1}{2}} = 2576,
\]
i.e all dodecads.

Remark 2.9. Note that this says that each five points in a dodecad define an octad \( O_1 \) that cuts the dodecad in 6 points. Further the remaining six points are in another octad \( O_2 \) and the dodecad is the sum of \( O_1 \) and \( O_2 \).

Remark 2.10. As \( \binom{12}{5} \cdot \frac{1}{6} \cdot \frac{1}{2} = \binom{12}{2} \) each two points outside a dodecad \( D \) induce a partition of \( D \) into two sets of size six such that each half together with the two points form an octad.

Remark 2.11. Since every set of five points in a dodecad determines a unique sixth point each dodecad determines a Steiner System \( S(5, 6, 12) \).

2.3 MOG

Curtis has invented a tool, MOG ( Miracle Octad Generator ), for visualizing all octads constructed in Theorem 2.2. Figure 2.1 is a version of it generated by a simple C++ program. To find an octad (distinct from the three bricks) we start by picking one of the 35 pictures. In this picture we choose black or white in the heavy brick (i.e the left brick) and a suit in the square (i.e the two rightmost bricks). Finally we are allowed to permute the bricks.

Example 2.12. The octad in MOG[3,2] with black and heart and the two first bricks interchanged is

\[
\begin{array}{ccc}
\times & \times & \times \\
\times & \times & \times
\end{array}
\]

= \{4, 13, 10, 2, 22, 19, 12, 5\}.

MOG is constructed using the fact that each octad cuts one of the bricks in exactly four points. This would lead to 70 sextets if we draw them modulo permutations of the three bricks. But if two octads \( O_1 \) and \( O_2 \) cut the same brick in two disjoint sets of four points then they must belong to the same sextet. So the 35 sextets in Figure 2.1 describes them all. Two important observations are the following lemmas.

21
Where the underlying table of numbers is:

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

Figure 2.1: An equivalent to Curtis MOG. The sextet row \(i\) and column \(j\) will be denoted MOG\([i, j]\).

**Lemma 2.13.** Each tetrad in the square cuts the rows with the same parity and the columns with the same parity.

**Proof.** For the rows we consider an octad \(O\) that cuts \(\Lambda_i\) in four points and let \(S\) be the sextet corresponding to MOG\([2,2]\) with \(\Lambda_i\) as the heavy brick. The octad \(O\) cuts one of the tetrads in the heavy brick in one, two or four points. If the cut is of size four it is trivial. If the cut is of size two Lemma 2.6 implies that \(O\) cuts two of the square tetrads in 2 points each and are
disjoint from the remaining. Similarly if the cut is of size one Lemma 2.6 implies that \( O \) cuts each square tetrad in exactly one point. Thus the parity condition is satisfied for rows. For the columns it follows analogously using MOG[4,5].

**Lemma 2.14.** *Interchanging the two bricks in the square preserves the sextet.*

**Proof.** By Corollary 2.5 the tetrad in the heavy brick defines an unique sextet. Suppose \( \Lambda_1 \) is the heavy brick (analogously for \( \Lambda_2 \) and \( \Lambda_3 \)). Then we simply observe that if \( [X,Y,Z] \) is an octad found in the sextet defined by \( X + t \) so is \( [X,Z,Y] \).

In the remaining part of this thesis MOG will be used frequently for mainly two tasks:

- to find the octad containing five given points.
- to check whether or not an element is in \( C \).

**Example 2.15.** To find the octad containing \( \{1, 10, 13, 16, 17\} \) we start by drawing them in the MOG table and observe that \( \Lambda_2 \) is the heavy brick.

\[
\begin{array}{ccc}
\times & \times & \times \\
\times & \times & \times \\
\times & \times & \times \\
\end{array}
\quad \rightarrow \quad 
\begin{array}{ccc}
\times & \times & \times \\
\times & \times & \times \\
\times & \times & \times \\
\end{array}
= \{1, 10, 13, 16, 17, 9, \infty, 14\}.
\]

Further MOG[3,1] help us to fill in remaining points.

**Example 2.16.** A bit trickier is to find the octad containing \( \{\infty, 16, 2, 12, 5\} \). As before we start drawing the points in a table.

\[
\begin{array}{ccc}
\times & \times & \times \\
\times & \times & \times \\
\end{array}
\]

It is clear that \( \Lambda_1 \) cannot be the heavy brick since \( \{16, 2, 12, 5\} \) do not satisfy the parity condition. If \( \Lambda_3 \) is the heavy brick MOG[7,1] force us to include the point 8 to satisfy the parity condition. But then the heavy bricks do not match. Thus \( \Lambda_2 \) is the heavy brick and using the parity condition we have to include 14. Finally we find our octad using MOG[3,5].

\[
\begin{array}{ccc}
\times & \times & \times \\
\times & \times & \times \\
\times & \times & \times \\
\end{array}
= \{\infty, 14, 11, 13, 16, 2, 12, 5\}.
\]
Example 2.17. To see that
\[ \{0, 8, 20, 18, 4, 13, 16, 2, 1, 9, 12, 6\} = \begin{array}{|c|c|c|c|c|}
\hline
x & x & x & x \\
\hline
x & x & x & x \\
\hline
\end{array} \notin \mathcal{C}, \]
we simply observe that the octad containing \{0, 8, 20, 18\} cut the set in five points.

Example 2.18. By Lemma \(2.8\) \(D = \{0, 8, 20, 18, 4, 11, 16, 2, 1, 9, 12, 6\}\) form a dodecad if and only if it is the symmetric difference of two octads. Or equivalent \(D\) is a dodecad if and only if for an octad \(O\) that cuts \(D\) in six points the sum \(D + O\) is an octad. From MOC[7,1] we see that \(O = \{0, 8, 20, 18, 4, 11, 21, 5\}\) is such an octad, but
\[ D + O = \{16, 2, 1, 9, 12, 6, 21, 5\} = \begin{array}{|c|c|c|c|c|c|c|c|}
\hline
x & x & x & x & x & x & x & x \\
\hline
\end{array} \]
is obviously not an octad. Hence \(D \notin \mathcal{C}\).

Example 2.19. To see if a set is a dodecad it is often easier to go back to the construction. For instance we see directly that
\[ \begin{array}{|c|c|c|c|c|}
\hline
x & x & x & x & x \\
\hline
x & x & x & x & x \\
\hline
\end{array} = [F, F, F] \in \mathcal{C}. \]

2.4 Uniqueness of \(S(5, 8, 24)\) and \(\mathcal{C}\)

We have already found the Golay Code and its associated Steiner System \(S(5, 8, 24)\). What we mean by uniqueness of \(\mathcal{C}\) is: For an arbitrary linear code \(\mathcal{C}'\), over \(\Omega'\), with the same weight enumerator as \(\mathcal{C}\), there is a bijection \(\rho : \Omega \rightarrow \Omega'\) such that code words are mapped to code words. Uniqueness for \(S(5, 8, 24)\) is defined analogously. Since it is not relevant how we name the points in \(\Omega'\) we might as well assume \(\Omega' = \Omega\) and we characterize \(\rho\) as a permutation in \(S_\Omega\).
Lemma 2.20. \( \rho \) preserves all octads if and only if \( \rho \) preserves all the sextets.

Proof. Assume all sextets are preserved by \( \rho \). Since each octad can be found as the union of two tetrads in a sextet the image of each octad is obviously an octad. For the other direction assume there exist a sextet \( S \) such that \( \rho(S) \) is not a sextet. Then there exist two tetrads \( T_1, T_2 \subset S \) such that \( \rho(T_1) \cup \rho(T_2) \notin \mathcal{S}_8 \), but \( T_1 \cup T_2 \in \mathcal{S}_8 \).

Lemma 2.21. If every octad cutting one specific octad \( O \) in four points are known, then all octads follows by symmetric differencing.

Proof. Let \( a, b, c \) be three arbitrary distinct points in \( O \). From row four in Table 3 we see that there are 21 octads containing \( a, b, c \). For the intersection to be even any two of these must intersect in four points. By Lemma 2.4 the symmetric difference is an octad disjoint from \( a, b, c \). There are \( \binom{21}{2} = 210 \) pairs among these 21 octads. If \( A, B \) and \( C, D \) are two such pairs and \( A + B = C + D \) then two points from \( A \setminus \{a, b, c\} \) has to be in \( C \) or \( D \), say \( C \). So \( A \) and \( C \) has five points in common and \( A = C \), implying \( B = D \). Hence all 210 pairs are unique. Again using row four in Table 3 we see that these are all octads disjoint from \( a, b, c \). This shows that all octads disjoint from some \( a, b, c \) are known. Le all octads, since every octad (not \( O \)) has to differ by at least 3 points.

Theorem 2.22. The Steiner System \( \mathcal{S}_8 \) is unique.

Method of Proof. We will show that if \( \rho \) is predefined on seven points we can in one and only one way define \( \rho \) on the remaining 17 points such that seven sextets similar to seven sextets from MOG exist. To find these seven sextets we use MOG and the fact that sextets has to be mapped to sextets. By choosing suitable octads from these sextets and taking the symmetric difference we will obtain all sextets that cut a specific octad \( 4^2 \). Finally the result follows from Lemma 2.21.

Proof. Let \( \mathcal{S}_8' \) be an arbitrary Steiner System \( S(5, 8, 24), (x_1, x_2, x_3, x_4, x_5, x_6) \) an ordered set of points from \( O \in \mathcal{S}_8' \) and \( x_7 \in \Omega \setminus O \). The idea is to show that there exists exactly one permutation \( \rho \) satisfying \( \rho[\mathcal{S}_8'] = \mathcal{S}_8' \) and

25
\[ \begin{align*}
\rho(\infty) &= x_1 & \rho(0) &= x_2 & \rho(3) &= x_3 \\
\rho(15) &= x_4 & \rho(14) &= x_5 & \rho(8) &= x_6 \\
\rho(17) &= x_7
\end{align*} \]

For the rest of the proof we are going to describe \( \rho \) with a matrix \( R \) in the following way. If

\[
M = \begin{bmatrix}
\infty & 14 & 17 & 11 & 22 & 19 \\
0 & 8 & 13 & 1 & 9 \\
3 & 20 & 16 & 7 & 12 & 5 \\
15 & 18 & 10 & 2 & 21 & 6
\end{bmatrix}
\]

we define \( R[i, j] = \rho(M[i, j]) \). So we start with

\[
R = \begin{bmatrix}
x_1 & x_5 & x_7 \\
x_2 & x_6 \\
x_3 \\
x_4
\end{bmatrix}
\]

and we wish to fill in the blanks in \( R \) in such a way that the octads are preserved. From MOG[4,5] we see that the columns of \( M \) form a sextet associated with \( \mathcal{C}_8 \) and hence due to Lemma 2.20 the columns of \( R \) must form a sextet associated with \( \mathcal{C}_8' \). So in our first attempt to define \( \rho \) we fill \( R \) with the remaining 17 points such that the tetrads in the sextet defined by \( x_1, x_2, x_3, x_4 \) are columns. In what order does not matter at the moment. We write this sextet

\[
S_1 = \begin{array}{cccc}
1 & 2 & 3 & 4 \\
1 & 2 & 3 & 4 \\
1 & 2 & 3 & 4 \\
\end{array}
\]

where the corresponding entries in \( R \), to a specific number, form a tetrad. We will by \( O_{iab} \) denote octad formed by tetrads \( a \) and \( b \) from \( S_i \). Note that \( S_1 \) implies that the two first columns of \( R \) form the octad \( O \). Now MOG[2,2] implies that, for the theorem to hold, we must require

\[
S_2 = \begin{array}{cccccc}
2 & 1 & 3 & 3 & 3 & 3 \\
1 & 2 & 4 & 4 & 4 & 4 \\
1 & 2 & 5 & 5 & 5 & 5 \\
1 & 2 & 6 & 6 & 6 & 6
\end{array}
\]

to be a sextet.
To achieve this we observe that the octad containing \( x_2, x_3, x_4, x_5, x_7 \) cuts \( S_1 3.1^5 \) so we can, if necessary, permute the 17 points to obtain \( S_2 \) without destroying \( S_1 \). Similarly, MOG[7,1] implies that we must require

\[
S_3 = \begin{bmatrix}
1 & 1 & 3 & 4 & 5 & 6 \\
2 & 2 & 4 & 3 & 6 & 5 \\
1 & 2 & 5 & 6 & 3 & 4 \\
1 & 2 & 6 & 5 & 4 & 3
\end{bmatrix}
\]
to be a sextet.

To see that can be achieved we observe that the octad containing \( x_1, x_3, x_4, x_5, x_7 \) cuts both \( S_1 \) and \( S_2 3.1^5 \). By permuting the rows in the lower right \( 3 \times 4 \) submatrix of \( R \), we can start writing the sextet defined by \( x_1, x_3, x_4, x_5 \) (i.e. the sextet we want to force to be \( S_3 \)) as

\[
\begin{array}{ccc}
1 & 1 & 3 \\
2 & 2 & 3 \\
1 & 2 & 3 \\
1 & 2 & 3
\end{array}
\begin{array}{ccc}
1 & 1 & 3 \\
2 & 2 & 4 \\
1 & 2 & 3 \\
1 & 2 & 3
\end{array}
\rightarrow
\begin{array}{ccc}
1 & 1 & 3 \\
2 & 2 & 4 \\
1 & 2 & 3 \\
1 & 2 & 3
\end{array}
\begin{array}{ccc}
1 & 1 & 3 \\
2 & 2 & 4 \\
1 & 2 & 3 \\
1 & 2 & 3
\end{array}
\]

Where the 4-tetrad must be since \( O_{156} + O_{234} \) cuts the sextet \( 4^2.0^4 \). Now the second column together with one of the four last imply that there should be one 5 and one 6 in each row. Using that \( O_{145} + O_{235} \) cuts the sextet \( 2^4.0^2 \) we see that the sextet actually is \( S_3 \). It is easy to convince oneself that the group of rearrangements of the 17 un-named points that preserves \( S_1, S_2 \) and \( S_3 \) is generated by

\[
\alpha = \begin{bmatrix}
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\end{bmatrix}
\begin{bmatrix}
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\end{bmatrix}
\quad \beta = \begin{bmatrix}
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\end{bmatrix}
\quad \gamma = \begin{bmatrix}
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\end{bmatrix}
\]

where dots denote fixed points and lines cycles. Similarly MOG[3,2] require that

\[
S_4 = \begin{bmatrix}
1 & 1 & 3 & 3 & 5 & 5 \\
1 & 1 & 3 & 3 & 5 & 5 \\
2 & 2 & 4 & 4 & 6 & 6 \\
2 & 2 & 4 & 4 & 6 & 6 \\
\end{bmatrix}
\]

has to be a sextet.

The octad \( X \) containing \( x_1, x_2, x_5, x_6, x_7 \) cuts \( S_1 2^4.0^2 \) and by using \( \alpha \) we might assume it cuts the first four columns. \( X \) also cuts \( S_2 \) and \( S_3 2^4.0^2 \) so it has to be the upper left \( 2 \times 4 \) submatrix of \( R \). As \( X \) cuts the sextet defined by \( x_1, x_2, x_5, x_6 \) \( 4^2.0^4 \) the tetrads 1 and 3 above are settled. Now
$O_{112}, O_{134}, O_{234}$ all cutting this sextet $4^2.0^4$. Hence $S_4$ is a sextet. As above MOG[6,1] require that
\[
S_5 = \begin{bmatrix}
1 & 1 & 3 & 4 & 5 & 6 \\
1 & 2 & 5 & 6 & 3 & 4 \\
1 & 2 & 6 & 5 & 4 & 3 \\
2 & 2 & 4 & 3 & 6 & 5
\end{bmatrix}
\]
has to be a sextet.

The octad $Y$ containing $x_1, x_2, x_3, x_5, x_7$ cannot contain any further points from $O_{113}, O_{213}$ or $O_{313}$ since it then would have five points in common with a different octad. Using that $Y$ cuts $S_1, S_2$ and $S_3 3.1^5$ this leaves only two cases:

\[
\begin{array}{c|c|c|c|c}
\hline
\times & \times & \times & \times & \times \\
\times & \times & \times & \times & \times \\
\times & \times & \times & \times & \times \\
\hline
\end{array}
\quad \text{or} \quad
\begin{array}{c|c|c|c|c}
\hline
\times & \times & \times & \times & \times \\
\times & \times & \times & \times & \times \\
\times & \times & \times & \times & \times \\
\hline
\end{array}
\]

where the corresponding entries in $R$ form the octad. By possibly using $\beta$ to permute we might assume that the latter describes $Y$. Notice that $\beta$ preserves $S_4$. Both $Y$ and $O_{112}$ cuts the sextet defined by $x_1, x_2, x_3, x_5$ $4^2.0^4$ so the tetrads 1,2 and 3 in $S_5$ are settled. To establish the other tetrads we use the fact that $O_{113}$, $i = 1..4$ and $j = 3.6$, all cuts the sextet $3^1.1^5$. This verifies that $S_5$ is a sextet. Using the same technique, with the added case $i = 5$, on the sextet defined by $x_1, x_2, x_4, x_5$ we easily find that
\[
S_6 = \begin{bmatrix}
1 & 1 & 3 & 4 & 5 & 6 \\
1 & 2 & 6 & 5 & 4 & 3 \\
2 & 2 & 4 & 3 & 6 & 5 \\
1 & 2 & 5 & 6 & 3 & 4
\end{bmatrix}
\]
is a sextet.

Notice that $S_6$ is the image of MOG[7,3]. For our last sextet, MOG[3,2] require
\[
S_7 = \begin{bmatrix}
1 & 1 & 3 & 3 & 5 & 5 \\
2 & 2 & 4 & 4 & 6 & 6 \\
1 & 1 & 3 & 3 & 5 & 5 \\
2 & 2 & 4 & 4 & 6 & 6
\end{bmatrix}
\]
to be a sextet.

To see this we look at the octad defined by
\[
\begin{array}{c|c|c|c|c}
\hline
\times & \times & \times & \times & \times \\
\times & \times & \times & \times & \times \\
\times & \times & \times & \times & \times \\
\hline
\end{array}
\]
Since this octad cuts $S_1 2^4.0^2$ it has one more element in the second column. This implies that it also cuts $S_2$ and $S_6 2^4.0^2$. Using this we get three cases:

$$
\begin{array}{|c|c|c|}
\hline
x & x & x \\
\hline
x & x & x \\
\hline
x & x & x \\
\hline
\end{array}
\quad \text{or} \quad
\begin{array}{|c|c|c|}
\hline
x & x & x \\
\hline
x & x & x \\
\hline
x & x & x \\
\hline
\end{array}
$$

The first case fails to cut $S_4$ properly. The other two are equivalent under $\gamma$ so we might assume that the middle case describes our octad. Notice that $\gamma$ preserves all previous sextets. Since it cut $S_1 2^4.0^2$, the tetrads 1,2,3,4 above are established. Finally, the fact that $O_{214}$ and $O_{256}$ both cut the sextet $4^2.0^4$ implies that tetrads 5 and 6 are established and $S_7$ is a sextet. Since $\langle \alpha, \beta, \gamma \rangle$ was the full group of permutations preserving $S_1$, $S_2$ and $S_3$ and we used all generators in the construction of the other sextets, it is clear that no further nonidentity permutations exist that preserves all seven sextets.

To obtain the image sextets of 28 remaining sextets from MOG, we repetitively take symmetric differences of already known octads that overlap in four points. By Lemma 2.4 the symmetric difference is an octad. If we look how this new octad cuts already found sextets it is an easy task to write out the sextet. To start, using $O_{114}$ and $O_{414}$, we get

$$
\begin{array}{|c|c|c|}
\hline
x & x & x \\
\hline
x & x & x \\
\hline
x & x & x \\
\hline
\end{array}
+ \begin{array}{|c|c|c|}
\hline
x & x & x \\
\hline
x & x & x \\
\hline
x & x & x \\
\hline
\end{array}
= \begin{array}{|c|c|c|}
\hline
x & x & x \\
\hline
x & x & x \\
\hline
x & x & x \\
\hline
\end{array}
$$

$O_{112}$ cuts the sextet defined by the four points in the left brick $4^2.0^4$. Further the cut with $O_{413}$ and $O_{414}$ is $2^4.0^2$. Thus the sextet contains tetrads

$$
\begin{array}{|c|c|c|c|}
\hline
1 & 2 & 3 & 4 \\
\hline
1 & 2 & 3 & 4 \\
\hline
2 & 1 & 4 & 3 \\
\hline
2 & 1 & 4 & 3 \\
\hline
\end{array}
$$

Now $O_{535}$ cuts the sextet $4^2.0^4$. Thus

$$
S_8 = \begin{array}{|c|c|c|c|}
\hline
1 & 2 & 3 & 4 & 5 & 6 \\
\hline
1 & 2 & 3 & 4 & 5 & 6 \\
\hline
2 & 1 & 4 & 3 & 6 & 5 \\
\hline
2 & 1 & 4 & 3 & 6 & 5 \\
\hline
\end{array}
$$
Next using $O_{613}$ and $O_{714}$ gives

\[
\begin{array}{ccc}
& x & x \\
& x & x \\
& x & x \\
x & x & \\
& x & x \\
& x & x \\
\end{array}
\quad + \quad
\begin{array}{ccc}
& x & x \\
& x & x \\
& x & x \\
x & x & \\
& x & x \\
& x & x \\
\end{array}
\quad = \quad
\begin{array}{ccc}
& x & x \\
& x & x \\
& x & x \\
x & x & \\
& x & x \\
& x & x \\
\end{array}
\]

As above $O_{112}$ cuts the sextet defined by the four points in the left brick $4^2.0^4$. Further both $O_{735}$ and $O_{846}$ cut the sextet $4^2.0^4$. Thus

\[
S_9 = \begin{pmatrix}
1 & 1 & 5 & 3 & 6 & 4 \\
2 & 1 & 6 & 4 & 5 & 3 \\
2 & 2 & 3 & 5 & 4 & 6 \\
2 & 1 & 4 & 6 & 3 & 5
\end{pmatrix}
\]

By using new sextets when found we can continue this tedious process and will after a while end up with all 35 sextets defined by four points in $O_{112}$. Hence we have found all octads cutting $O_{112}$ in four points. The uniqueness now follows from Lemma 2.21.

\[\square\]

**Theorem 2.23.** The Golay code is unique.

*Proof.* Since each linear code with weight enumerator $[2.1]$ defines a Steiner system $S(5, 8, 24)$ and has a purely octad basis the assertion follows from the uniqueness of $S(5, 8, 24)$.

\[\square\]

**Corollary 2.24.** The permutations of $\Omega$ that preserves $C_8$ form a 5-fold transitive permutation group of order 244, 823, 040.

*Proof.* The permutations that preserves $C_8$ form obviously a group. To pick an element in this group we have, from the uniqueness theorem, $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20$ choices to pick $x_1, x_2, x_3, x_4, x_5$. For $x_6$ we have three choices and for $x_7$ we have 16 choices. Putting it all together we have 244, 823, 040 choices.

\[\square\]

**Definition 2.25.** The 5-fold transitive group preserving $C_8$ is called $M_{24}$.

Note that since $C$ has a purely octad basis it is also preserved by $M_{24}$.  

30
3. The Mathieu group $M_{24}$

A common problem that will haunt us for the rest of this thesis is whether or not $x \in S_{24}$ is in $M_{24}$. The proof of Theorem 2.22 gave us one solution, namely to check if $x$ maps $S_i$, $i = 1..7$, to sextets. This is however an extremely simple and tedious calculation so to increase our quality of life GAP (see Appendix) is a good option.

Lemma 3.1. In $M_{24}$ the only element in $M_{24}$ fixing seven points not in an octad is the identity.

Proof. We will later see that the octad stabilizer has form $2^4.A_8$ where $A_8$ is the restriction of the action to the octad being stabilized and $2^4$ is action on the remaining 16 points when the octad is stabilized pointwise. Further all nontrivial permutations in the $2^4$ has cycle shape $1^8.2^4$, i.e fixed point free on the points outside the octad.

Suppose $\rho \in M_{24}$ fixes $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ and the seven points are not in an octad. If $x_1, x_2, x_3, x_4, x_5, x_6$ is in an octad $O_1$, then $\rho$ is in the stabilizer of $O_1$. Now the restriction of $\rho$ to its action on $O_1$ is an even permutation so $\rho$ must fix $O_1$ pointwise. Since the $2^4$ is acting fixed point free and $\rho$ fixes a point in $\Omega \setminus O$, $\rho$ must be the identity. Let $O_2$ be the octad defined by $x_1, x_2, x_3, x_4, x_5$. If $x_6 \notin O_2$ we know from Theorem 2.22 and the octad stabilizer that $\rho$ is either the identity or has a cycle of length three, i.e the three remaining points in $O_2$. Assume the case is the latter and call the points in the three cycle $y_1, y_2, y_3$. Then $\rho^3$ fixes $O_2$ pointwise and a point in $\Omega \setminus O_2$ so $o(\rho) = 3$. Thus $\rho$ has cycle shape $1^{6+3k}.3^{6-k}$ for some $1 \leq k \leq 5$. Assume $x_6, z_1, z_2, z_3$ fixed points to $\rho$ outside $O_2$. The octad $Q$ defined by $x_5, x_6, z_1, z_2, z_3$ contains either one further point from $O_2$ being fixed by $\rho$, or three further points from $O_2$. If it contains three further points they have to be $y_1, y_2, y_3$ since $\rho$ otherwise would stabilize another octad pointwise and
have bad cycle shape. If \( y_1, y_2, y_3 \in Q \) then \( \rho \) stabilizes the octad \( O_2 + Q \) pointwise and has bad cycle shape. Hence \( Q \) contains exactly one further point from \( O_2 \) fixed by \( \rho \). But then \( \rho \) fixes six points in \( Q \) (i.e \( Q \) being fixed pointwise) and has bad cycle shape. Contradiction. \( \blacksquare \)

The following corollary will be used more frequently than the lemma itself.

**Corollary 3.2.** Only the identity fixes nine points.

### 3.1 Eight maximal subgroups

The goal in this section is to find and characterize eight natural subgroups of \( M_{24} \). We will later see that they all are maximal subgroups.

The subgroups of \( M_{24} \) fixing one, two an three points are called \( M_{23}, M_{22} \) and \( M_{21} \) respectively.

**Definition 3.3.** The groups \( M_{24}, M_{23} \) and \( M_{22} \) are Mathieu groups.

We will later see that all four groups above are simple. The group \( M_{21} \) is not a sporadic group thou. In fact \( M_{21} \cong PSL_3(4) \), a group of Lie type, but the proof of this is out of the scope for this thesis. From the 5-fold transitivity of \( M_{24} \) it follows that the stabilizers of a monad (one element set), dyad (two element set) and triad (three element set) are \( M_{23}, M_{22} \), and \( M_{21} \).\( S_3 \) respectively.

#### 3.1.1 The projective group \( L_2(23) \)

Since \( 23 \mid |M_{24}| \) there is an element \( \alpha \in M_{23} \) of order 23. The numbers in the MOG table are adapted to this element. We have \( \alpha : i \mapsto i + 1 \) or

\[
\alpha = (\infty)(0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12 \ 13 \ 14 \ 15 \ 16 \ 17 \ 18 \ 19 \ 20 \ 21 \ 22).
\]

We define another element \( \gamma : i \mapsto -1/i \), i.e

\[
\gamma = (0 \infty)(1 \ 22)(2 \ 11)(3 \ 15)(4 \ 17)(5 \ 9)(6 \ 19)(7 \ 13)(8 \ 20)(10 \ 16)(12 \ 21)(14 \ 18).
\]

To see that \( \gamma \in M_{24} \) we could check its action on sextets \( S_i, i = 1, \ldots, 7 \), and see that the images are indeed sextets. Alternatively we wait until we know more about the involutions in \( M_{24} \). Finally Lemma 1.20 implies that \( \langle \alpha, \gamma \rangle \cong L_2(23) \). By Lemma 1.20 \( L_2(23) \) is doubly transitive on \( \Omega \).
3.1.2 The Octad Stabilizer

Since $M_{24}$ clearly is transitive on octads all octad stabilizers are conjugates, so it is enough to look at one of them. Let $G$ be the stabilizer of $\Lambda_1$ and let $\varphi$ be the restriction map to $\Lambda_1$. From the proof of Theorem 2.22 we know that the $\varphi(G)$ is 6-fold transitive. Thus

$$G = K. \begin{cases} S_8 \\ A_8 \end{cases}$$

where $K$ is the kernel of $\varphi$. By Lemma 1.5 $|G| = |M_{24}|/759$. Further the permutations

\[
\begin{array}{ccc}
\begin{array}{|c|c|c|c|}
 x & x & x & x \\
 x & x & x & x \\
 x & x & x & x \\
 x & x & x & x \\
\end{array} & , & 
\begin{array}{|c|c|c|c|}
 x & x & x & x \\
 x & x & x & x \\
 x & x & x & x \\
 x & x & x & x \\
\end{array} & , & 
\begin{array}{|c|c|c|c|}
 1 & 1 & 1 & 1 \\
 1 & 1 & 1 & 1 \\
 1 & 1 & 1 & 1 \\
 1 & 1 & 1 & 1 \\
\end{array}
\end{array}
\]

are all in $M_{24}$. They generate an elementary abelian subgroup in $K$ of order 16. Finally $16 \cdot |A_8| = |G|$. Thus $K = 2^4$ and thus $G \cong 2^4.A_8$.

3.1.3 The Duum Stabilizer

The complement of a dodecad is itself a dodecad. Such a pair of complementary dodecads is called a duum. To see the structure of the duum stabilizer we need the order of the dodecad stabilizer and so we prove

**Lemma 3.4.** $M_{24}$ is transitive on dodecads.

**Proof.** The stabilizer to $\Lambda_1$ has a subgroup $H$ fixing top two points as a pair. By the last row in Table 3 there is exactly 16 octads that cuts $\Lambda_1$ in these two points. One such octad is

\[
\begin{array}{|c|c|c|}
 x & x & x \\
 x & x & x \\
 x & x & x \\
 x & x & x \\
\end{array}
\]

It is readily checked that no element in the $2^4$ fixing every point in $\Lambda_1$ fixes this octad. Thus the $2^4$ is transitive over the 16 octads cutting $\Lambda_1$ in the top two points. Finally if $D_1$ and $D_2$ are two dodecads Remark 2.9 implies that
\[ D_1 = O_1 + O_2 \text{ and } D_2 = O_3 + O_4 \] for some octads \( O_1, O_2, O_3 \) and \( O_4 \). Take \( g, h \in M_{24} \) such that \( g(O_1) = \Lambda_1 \) and \( h(O_3) = \Lambda_1 \). Then we can find \( k \in H \) such that \( kg(O_2) = h(O_4) \) and so \( h^{-1}kg(D_1) = D_2 \). □

**Lemma 3.5.** The dodecad stabilizer is sharply 5-fold transitive on its twelve points.

**Proof.** Let \( D \) be a dodecad and pick two subsets \( X = \{x_1, x_2, x_3, x_4, x_5\} \) and \( Y = \{y_1, y_2, y_3, y_4, y_5\} \) of \( D \). These sets define octads \( O_x \) and \( O_y \). From Remark 2.9 we know that \( D = O_x + R_x = O_y + R_y \) for some octads \( R_x \) and \( R_y \). Pick \( g \in M_{24} \) such that \( g(O_x) = O_y \). Since the stabilizer \( H \) of \( O_y \) acts as \( A_8 \) on \( O_y \) we can find \( h \in H \) such that \( hg(O_x \cap R_x) = O_y \cap R_y \).

If we let \( K \) be the kernel of the restriction map of \( H \) to \( O_y \) we know from the proof of Lemma 3.4 that \( K \) is transitive on the octads cutting \( O_y \) in \( O_y \cap R_y \). Especially we can choose \( k \in K \) such that \( khg(R_x) = R_y \). Then \( khg \) stabilize \( D \) and map \( X \) to \( Y \).

Finally the \( A_8 \) fixing \( O_y \) contains a \( S_6 \) acting on \( O_y \setminus R_y \) and so there must exist a permutation mapping \( x_i \) to \( y_i \) for \( i = 1, 2, 3, 4, 5 \). From Lemma 1.5 we know that the stabilizer of a dodecad has order \( |M_{24}| / 2576 = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \), so it must be sharply 5-fold transitive. □

Thus we have found the Mathieu group \( M_{12} \) and its isotropy group, i.e the Mathieu group \( M_{11} \). Finally since \( M_{24} \) is transitive on dodecads, the duum stabilizer is isomorphic to \( M_{12.2} \).

### 3.1.4 The Sextet Stabilizer

Clearly \( M_{24} \) is transitive on sextets, so it is enough to investigate one sextet stabilizer. We choose the stabilizer \( G \) to the sextet \( \text{MOG}[4,5] \) where the columns are tetrads. There are \( \binom{24}{4} \cdot \frac{1}{6} = 1771 \) sextets. By Lemma 1.5 \( G \) has order \( |M_{24}| / 1771 = 2^6 \cdot 3 \cdot 6! \).

Let \( \varphi : G \rightarrow S_6 \) be the restriction map to the action on the tetrads. Clearly \( \varphi[G] \) is doubly transitive. As the image of

\[
\begin{array}{cccc}
\cdot & \cdot & \cdot & \cdot \\
1 & 1 & 1 & 1 \\
\end{array}
\]

is a transposition, \( \varphi[G] \) contains all transpositions and \( \varphi[G] \cong S_6 \). We see that the kernel has order \( 2^6 \cdot 3 \). Further the involutions
all fixing two tetrads pointwise and preserving the others. Again due to the doubly transitivity on the tetrads, each pair of of tetrads has three such involutions. Let $X$ be the set containing these $\binom{6}{2} \cdot 3 = 45$ involutions. It is clear that all elements in $\langle X \rangle$ commute. Since $\langle X \rangle \leq \text{Ker}(\varphi)$ and $\langle X \rangle$ do not contains an element of order three we have $\langle X \rangle = 2^6$. Finally $g = \begin{pmatrix} \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \in \text{Ker}(\varphi)$ has order three and normalize all elements in $X$. Thus $g$ normalize $\langle X \rangle$ and $\text{Ker}(\varphi) \cong 2^6.3$. Hence $G \cong (2^6.3).S_6$.

### 3.1.5 The Trio Stabilizer

A partition of $\Omega$ into three octads is called a **trio**.

**Lemma 3.6.** The Mathieu group $M_{24}$ is transitive on trios.

**Proof.** From Theorem 2.22 we know that we can find a permutation $\rho \in M_{24}$ with cycle shape $5.3$ on an octad $O$ that fixes a point in $\Omega \setminus O$. Since $\rho^{15}$ fixes nine points we know that $\rho^{15} = 1$ and so $\rho$ has shape $5.3.11^i.3^j.5^k.15^l$ for some $i, j, k, l$. If $l = 0$ then $\rho^5 \neq 1$ or $\rho^3 \neq 1$ fixes at least nine points. Contradiction. Hence $\rho$ has shape $3.5.1.15$. By Table 3 there are 30 octads disjoint from $O$. Now $\rho$ has two orbits of length 15 on these 30 octads. One orbits consists of those octads containing the fixed point and the other the remaining. So the stabilizer of $O$ is transitive on the 15 trios containing $O$. Finally let $T_1$ and $T_2$ be two trios containing octads $O_1$ and $O_2$ respectively. Pick $\sigma \in M_{24}$ such that $\sigma(O_1) = O_2$ then $\sigma(T_1)$ is a trio containing $O_2$ so we can find $\pi$ the stabilizer to $O_2$ such that $\pi \sigma(T_1) = T_2$. \hfill \blacksquare

By studying the MOG table we see that there are $759 \cdot 5 = 3795$ trios. Let $G$ be the stabilizer to the MOG trio, ie the three bricks. Then due to the above lemma $|G| = |M_{24}|/3795 = 2^6 \cdot 3 \cdot 2 \cdot 168$. If $S$ is a sextet

![Diagram](image_url)
such that the tetrads can be paired to form a trio $T$, then we say that $S$ is a **refinement** of $T$. As each sextet is a refinement of $\binom{6}{2} = 15$ trios, the number of refinements to a fixed trio is $(1771 \cdot 15)/3795 = 7$. Clearly $G$ has to permute the refinements of the MOG trio. We observe that the refinements to the MOG trio is the nonzero elements in the point space $P$ from Theorem 2.2 (the corresponding sextets are MOG[2,3], MOG[3,2], MOG[4,1], MOG[4,5], MOG[5,4], MOG[6,3] and MOG[7,2]). Since these generate an elementary abelian group of order 8, using symmetric differencing as multiplication, the maximum action $G$ can have on the refinements is

$$\text{Aut}(2^3) \cong GL_3(2) \cong L_3(2) \cong L_2(7).$$

The last isomorphism will be visible inside the Octern group later. Besides the action on the refinements $G$ contains

and so the full $S_3$ bodily permuting the bricks. These actions do not interfere. Hence we can identify the restriction map to $G$’s action on bricks and the refinements with

$$\varphi : G \longrightarrow S_3 \times L_2(7).$$

Further the three elements

$$a = \begin{array}{cccccc}
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\end{array}, \quad b = \begin{array}{cccccc}
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\end{array} \quad \text{and} \quad c = \begin{array}{cccccc}
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ \\
\end{array}$$

are in $G$ and stabilize the bricks. As $o(\varphi(a)) = 3$, $o(\varphi(abc)) = 7$ and $o(\varphi(acb)) = 4$ we have $\varphi[(a, b, c)] \leq \langle 1 \rangle \times L_2(7)$ and $|\varphi[(a, b, c)]| = 84$ or 168. To eliminate the first case we need the following lemma.

**Lemma 3.7.** The projective group $L_2(7)$ is simple.

**Proof.** On the projective line $L_2(7)$ is generated by

$$\rho = (\infty)(0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6) \quad \text{and} \quad \sigma = (\infty \ 0)(1 \ 6)(2 \ 3)(4 \ 5)$$
Lemma 1.20 together with Lemma 1.11 implies that $L_2(7)$ is primitive. Assume $N \triangleleft L_2(7)$ is proper and non trivial. By Lemma 4.1 $N$ is transitive. Thus $8 \mid |N|$ and $N$ contains all Sylow 2-subgroups of $L_2(7)$. Suppose $|N| = 8$. Then as $\rho^i \sigma \rho^{-i} \in N$ for $i = 1..7$ all have order 2, i.e $N$ is elementary abelian. But $o(\rho \sigma \rho^{-1} \sigma) = 4$, contradiction. Thus $|N| = 8 \cdot 3$ or $8 \cdot 7$. If $3 \mid |N|$ then $N$ contains all Sylow 3-subgroups. Hence $\rho \sigma = (\infty 1 0)(2 4 6) \in N$. But then $(\rho \sigma) \sigma = \rho \in N$ and $N = G$. Contradiction. Similarly if 7 $\mid |N|$, then $N$ contains all Sylow 7-subgroups and $\rho \in N$. Thus $\rho \sigma \in N$ and again $N = G$. 

This shows that $\varphi[\langle a, b, c \rangle] = \langle 1 \rangle \times L_2(7)$ and $\varphi[G] \cong S_3 \times L_2(7)$. Finally $|\text{Ker}(\varphi)| = |G|/|\varphi[G]| = 2^6$. Clearly Ker$(\varphi)$ contains the subgroup fixing the first brick pointwise and preserving the bricks. By conjugating this subgroup with the $S_3$ bodily permuting the bricks we see that Ker$(\varphi)$ contains

\[
\begin{array}{c}
\begin{array}{ccc}
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
\end{array} & \\
\begin{array}{ccc}
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
\end{array} & \\
\begin{array}{ccc}
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
\end{array}
\end{array}
\]

It’s readily checked that these generate an elementary abelian group of order $2^6$. Thus

$$G \cong 2^6.(S_3 \times L_2(7)).$$

\textit{Remark} 3.8. Galois proved that the group $L_2(p)$ does not have a nontrivial permutation representation on fewer than $p + 1$ symbols for $p > 11$ ([9], p.268). This shows that the above representation of $L_2(7)$ on seven symbols is very special.

\section*{3.2 The involutions in $M_{24}$}

We have already seen one type of involution. I.e involutions fixing an octad pointwise. We will call this an involution of \textbf{type one}. Since the subgroup fixing an octad pointwise has order 16 and is transitive on the 16 points outside the octad, there is one and only one involution fixing an octad $F$ and interchanging $i, j \notin F$. Call this involution $F_{i,j}$. 

37
Lemma 3.9. Let $F$ be an octad and let $i, j, k, l \in \Omega \setminus F$ be four distinct points. Then $F_{ij} = F_{k,j}$ if and only if $\{i, j, k, l\}$ is a special tetrad of $F + \Omega$.

Proof. If $\{i, j, k, l\}$ is a special tetrad of $\Omega \setminus F$, $\exists x_1, x_2, x_3, x_4 \in F$ such that $O = \{i, j, k, l, x_1, x_2, x_3, x_4\}$ is an octad. Clearly $F_{ij}$ stabilize $O$. Thus $F_{ij} = F_{k,j}$. For the other direction we notice that $i, j$ together with three points $y_1, y_2, y_3 \in F$ defines a fourth point in $y_4 \in F$ plus two points $k, l \in \Omega \setminus F$, such that they all lie in the same octad. As this octad being stabilized $F_{ij} = F_{j,k}$. Obviously $\{i, j, k, l\}$ is a special tetrad of $\Omega \setminus F$. We can choose $\{y_1, y_2, y_3, y_4\}$ in $\frac{1}{4} \binom{8}{3} = 14$ ways. Modulo $F$ each choice defines two points in $\Omega \setminus F$. Since no two octads intersect in more than four points every two different choices modulo $F$ defines disjoint pairs in $\Omega \setminus F$. All together this gives seven pairs plus the points $i, j$, i.e all of $\Omega \setminus F$. ■

Knowing this we can easily construct any involution $F_{i,j}$. The method is

(i) Pick $x_1, x_2, x_3, x_4 \in F$

(ii) Let $a, b$ be in the octad defined by $k, l, x_1, x_2, x_3, x_4$, where the pair $k, l$ forms a known 2-cycle in $F_{i,j}$. As the octad is being stabilized we have $(a \ b) \in F_{i,j}$.

(iii) If the action on some point is unknown go to (i) and pick four new points.

Example 3.10. Suppose we want to find $(\Lambda_3)_{\infty,0}$. The unkown action on the octad

$\begin{array}{cccc}
\times & \times & \times & \\
\times & \times & \times & \\
\times & \times & \times & \\
\times & \times & \times & \\
\end{array}$

is forced to be a 2-cycle. Thus $(\Lambda_3)_{\infty,0} = \begin{array}{cccc}
| & | & | & \\
| & | & | & \\
| & | & | & \\
| & | & | & \\
\end{array}$

Similarly $\begin{array}{cccc}
\times & \times & \times & \\
\times & \times & \times & \\
\times & \times & \times & \\
\times & \times & \times & \\
\end{array}$ and $\begin{array}{cccc}
\times & \times & \times & \\
\times & \times & \times & \\
\times & \times & \times & \\
\times & \times & \times & \\
\end{array}$ imply $(\Lambda_3)_{\infty,0} = \begin{array}{cccc}
| & | & | & \\
| & | & | & \\
| & | & | & \\
| & | & | & \\
\end{array}$. Four octads later we end
up with \((\Lambda_3)_{\infty,0} = \begin{array}{ccc}
\Lambda & \Lambda & \vdots \\
\Lambda & \Lambda & \vdots \\
\Lambda & \Lambda & \vdots \\
\end{array}\).
\(\blacktriangleup\)

Multiplying \((\Lambda_3)_{\infty,0}\) and \((\Lambda_1)_{4,16}\) gives
\[
\sigma = \begin{array}{ccc}
\Lambda & \Lambda & \vdots \\
\Lambda & \Lambda & \vdots \\
\Lambda & \Lambda & \vdots \\
\end{array} \times \begin{array}{ccc}
\Lambda & \Lambda & \vdots \\
\Lambda & \Lambda & \vdots \\
\Lambda & \Lambda & \vdots \\
\end{array} = \begin{array}{ccc}
\Lambda & \Lambda & \vdots \\
\Lambda & \Lambda & \vdots \\
\Lambda & \Lambda & \vdots \\
\end{array}
\]
an involution that acts without fixed points. We notice that this involution fixes the sextet \(S_1\) tetradwise. Further the involution fixes the dodecad
\[
M = [A, B, C]_A = \begin{array}{ccc}
x & x & x \\
x & x & x \\
x & x & x \\
\end{array}
\]
cutting across the tetrads \(2^6\). We will call this an involution of type two.

**Theorem 3.11.** Let \(S\) be a sextet and \(D\) a dodecad cutting the tetrads of \(S\) \(2^6\). Then there is an involution in \(M_{24}\) fixing the tetrads of \(S\) and \(D\). Further all involutions of type two are conjugates.

**Proof.** In this proof we will by \(M_{12}\) mean the stabilizer of \(D\). Since \(M_{24}\) is transitive on dodecads \(\exists \rho \in M_{24}\) such \(\rho(M) = D\). Clearly \(D\) cuts \(\rho(S_1) 2^6\). Thus \(\rho \sigma \rho^{-1}\) fixing \(D\) and the tetrads of \(\rho(S_1)\). Were done if we can show that \(M_{12}\) fixing \(D\) is transitive on the sextets cutting \(D\) \(2^6\). Since then \(\exists \alpha \in M_{12}\) such that \(\alpha \rho \sigma \rho^{-1} \alpha^{-1}\) has the desired properties. Consider a sextet defined by four points in \(D\). Since \(D\) cannot contain an octad this sextet cuts \(D\) \(4.2^4\). Hence we have found two sextets containaing a tetrad cutting \(D\) in two points. Our goal is to show that \(M_{12}\) only has two orbits on such tetrads. Clearly one of this orbits contains all sextets cutting \(D\) \(2^6\). Note that we already know that \(M_{12}\) has at least two orbits. Let \(\{a, b, c, d\}\) and \(\{s, t, u, v\}\) be two tetrad such that \(a, b, s, t \in \Omega \setminus D\) and \(c, d, u, v \in D\). Since \(M_{12}\) is \(5\)-transitive on \(\Omega \setminus D\) there \(\exists \beta \in M_{12}\) such that
\[
\beta(s) = a \quad \text{and} \quad \beta(t) = b.
\]
By Remark 2.10 \(a, b\) induce a partition of \(D\) into two halves \(X\) and \(Y\). As \(M_{12}\) is \(5\)-transitive the subgroup \(G\) fixing \(X\) acts as \(S_6\) on \(X\) and fixing \(a, b\)
as a pair. By symmetry $G$ also acts as $S_6$ on $Y$. Consider $g \in G$ with cycle shape $1.2.3$ on $X$. No matter what cycle shape $g$ has on $Y$, $g^6$ fixes at least nine points. By Corollary 3.2 $o(g) = 6$. Thus the possible cycle shapes for $g$ on $Y$ are

$1.2.3$, $1^2.2^2$, $1^3.3$, $1^4.2$, $1^6$, $2^3$, $3^2$ and $6$

Case 1, 3, 4, 5, 6 and 7 implies that $g^3 \neq 1$ is fixing seven points not in an octad, contradicting Lemma 3.1. Similarly case 2 yields $g^2 \neq 1$ is fixing eight points not in an octad. Hence $\langle g \rangle$ acts transitively on $Y$. Further the subgroup $M_{10.2}$ fixing $a, b$ as a pair clearly preserves the partition $X$ and $Y$ as a pair. Since $M_{12}$ is sharply 5-transitive $[M_{10.2} : G] = 2$. As $G$ already contains all actions on $X$ the sharply 5-transitivity implies that there $\exists \gamma \in M_{10.2} \setminus G$ swapping $X$ and $Y$. This shows that two tetrads that cut $D$ in two points are in the same orbit if and only if they split across $X$ and $Y$ in the same way. If they do there are two cases

- If $\beta(s), \beta(t) \in A$ and $c, d \in B$ for $A, B = X$ or $Y$, then by possibly using $\gamma$ we can map so they all belong to the same half. Finally we use the $S_6$ fixes that half to map $\beta(s) \mapsto c$ and $\beta(t) \mapsto d$.

- If the pairs $\beta(s), \beta(t)$ and $c, d$ both split across $X$ and $Y$, we can use the $S_6$ stabilizing one half to map $\beta(s) \mapsto c$, say. As we can fix $c$ and stay transitive on the other half we map $\beta(t) \mapsto d$.

$\blacksquare$

Remark 3.12. As the $S_6$ acted differently (by consideration of the cycle shapes) on $X$ and $Y$ we have shown that $S_6$ is not unique up to relabeling of the points in its action on six points.

Theorem 3.13. Every involution in $M_{24}$ is of type one or two.

Proof. Let $\pi \in M_{24}$ be an involution. As the number of octads is odd, $\pi$ fixes at least one octad. Suppose $\pi$ fixes $\Lambda_1$, i.e. the left MOG brick, and let $G = 2^4.A_8$ be the stabilizer of $\Lambda_1$. Since $G$ acts as $A_8$ on $\Lambda_1$ $\pi$ fixes zero, four or eight points in $\Lambda$. If eight points are fixed $\pi$ is an involution of type 1. Suppose $\pi$ fixes zero points of $\Lambda_1$. Up to conjugation by $G$ we can assume that $\pi$ has the action

\[
\begin{array}{|c|c|}
\hline & 1 \\
\hline & 1 \\
\end{array}
\]

on $\Lambda_1$. Multiplying with $\rho = \begin{array}{|c|c|c|c|c|} \hline & 1 & 1 & 1 & 1 \\
\hline & 1 & 1 & 1 & 1 \\
\end{array}$
gives $\pi \rho = \alpha \in 2^4$. Clearly $\rho$ and $\pi$ commute. Since $\pi = \alpha \rho = \rho \alpha$ we are looking for $\alpha \in 2^4$ commuting with $\rho$. It is readily checked that the only non trivial elements in the $2^4$ commuting with $\rho$ are the seven elements fixing each brick. If we let $A$, $D$ and $E$ be the sextet defined by corresponding element in the space $P$ from from Theorem 2.2, $\pi$ has one of the following actions:

$\begin{array}{c|c|c}
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\times
\begin{array}{cccc}
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\end{array}
= \\
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\end{array}
= A_{[E,F,C]}
$

$\begin{array}{c|c|c}
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\times
\begin{array}{cccc}
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\end{array}
= \\
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\end{array}
= A_{[D,C,G]}
$

$\begin{array}{c|c|c}
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\times
\begin{array}{cccc}
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\end{array}
= \\
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\end{array}
= D_{[E,F,C]}
$

$\begin{array}{c|c|c}
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\times
\begin{array}{cccc}
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\end{array}
= \\
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\end{array}
= D_{[E,C,F]}
$

$\begin{array}{c|c|c}
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\times
\begin{array}{cccc}
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\end{array}
= \\
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\end{array}
= E_{[D,B,F]}
$

$\begin{array}{c|c|c}
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\times
\begin{array}{cccc}
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\end{array}
= \\
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{array}
\end{array}
= E_{[D,F,B]}
$

If $\pi$ fixes four points of $\Lambda_1$ we use the same idea as above. Up to conjugation by $G$, $\pi$ has the action $\begin{array}{cccc}
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots \\
1 & 1 & 1 & 1 \\
\end{array}$ on $\Lambda_1$. Multiplying by
\[ \sigma = \begin{array}{cccc}
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\end{array} \]
gives \( \pi \sigma = \beta \in 2^4 \). Clearly the only elements in

the \( 2^4 \) commuting with \( \sigma \) are the three elements fixing each tetrad. We end up with three cases. So up to conjugation \( \pi \) has one of the following actions:

\[
\begin{align*}
\sigma & \times \begin{array}{cccc}
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\end{array} = \begin{array}{cccc}
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\end{array} \\
\sigma & \times \begin{array}{cccc}
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\end{array} = \begin{array}{cccc}
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\end{array} \\
\sigma & \times \begin{array}{cccc}
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\end{array} = \begin{array}{cccc}
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\end{array}
\end{align*}
\]

Clearly all three are of type one.

\[ \blacksquare \]

### 3.3 A further maximal subgroup

All subgroups so far have been rather visible from our construction. This subgroup however is not. The subgroup was found later and did not occur on the “complete” list of maximal subgroups of \( M_{24} \) first published \([10]\). The subgroup is transitive and is called the **Octern group**. It can be defined as the stabilizer of a special “purely dodecad” four dimensional subspace \( \mathcal{C} \). The quotation marks is because we allow \( \emptyset \) and \( \Omega \) to be in the subspace. Consider the matrix

\[
\begin{array}{cccccccc}
\infty & 14 & 3 & 15 & 20 & 0 & 8 & 18 \\
17 & 16 & 10 & 7 & 4 & 13 & 2 & 11 \\
22 & 9 & 6 & 19 & 12 & 21 & 5 & 1
\end{array}
\]

42
Let \( \rho \) be the element fixing the rows and rotating the last seven columns. It can be verified that \( \rho \in M_{24} \). We now name the columns in the above matrix \( \infty, 0, 1, \ldots, 6 \). Since we only will consider elements preserving these columns there is a well defined restriction map \( \theta \) to the action on the columns. We use the notation \( \theta(x) = x \). For instance \( \rho = (0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6) \). In a natural way the subsets of \( \{ \infty, 0, \ldots, 6 \} \) corresponds to subsets of \( \Omega \). It turns out that

\[
D_1 = \{ \infty, 0, 1, 3 \}, \quad D_2 = \{ \infty, 0, 2, 6 \} \quad \text{and} \quad D_3 = \{ \infty, 1, 2, 4 \}
\]

are dodecads. Together with \( 1 = \{ \infty, 0, \ldots, 6 \} \) these generate 14 dodecads. We want to show that these are all dodecads that is union of four columns. Totally there are \( \binom{8}{4} = 70 \) possibilities. Assume there is a further such dodecad \( D_4 \). Then \( 1, D_1, D_2, D_3 \) and \( D_4 \) generate 30 such dodecads. But it turns out that none of

\[
F_1 = \{ \infty, 0, 1, 2 \}, \quad F_2 = \{ \infty, 0, 1, 4 \}, \quad F_3 = \{ \infty, 0, 1, 5 \} \\
F_4 = \{ \infty, 0, 1, 6 \}, \quad F_5 = \{ \infty, 0, 2, 4 \} \quad \text{and} \quad F_6 = \{ 0, 1, 2, 3 \}
\]

are dodecads. Its readily checked that the set

\[
\{ \rho^i F_j \mid i = 0, \ldots, 6, \; j = 1, \ldots, 6 \}
\]

contains 42 elements that is not dodecads. Since \( 70 - 42 < 30 \) a further dodecad \( D_4 \) cannot exist. Define \( \mathcal{H} \) to be the linear code spanned by \( 1, D_1, D_2, D_3 \) and define the Octern group \( G = M_{24} \cap \text{Aut}(\mathcal{H}) \). If we take \( 1, D_1, D_2, D_3 \) as a basis for \( \mathcal{H} \) we can express \( \theta[G] \) as the subgroup of \( GL_4(2) \) consisting of matrices

\[
g = \begin{pmatrix}
1 & a & b & c \\
0 & & & 0 \\
0 & A_g & & \\
0 & & &
\end{pmatrix}
\]

where \( a, b, c \in \{0, 1\} \) and \( A_g \in L_3(2) \)

We now define the restriction map

\[
\phi : \theta[\text{Aut}(\mathcal{H})] \to L_3(2)
\]

\[
\begin{array}{ccc}
\rho & \mapsto & A\rho \\
\end{array}
\]

43
and get \( \theta[G]/\text{Ker}(\varphi_G) \leq 2^3 L_3(2) \), where \( \varphi_G \) is the restriction of \( \varphi \) to \( \theta[G] \). Note that \( \text{Ker}(\varphi) \) is an elementary abelian group, containing exactly the eight elements satisfying \( D_i \mapsto D_i \) or \( D_i \mapsto D_i + 1 \) for \( i = 1, 2, 3 \). Our objectives are:

(i) Show that \( |\theta[G]| = |L_3(2)| \).

(ii) Show that \( \text{Ker}(\theta) \) is trivial.

(iii) Show that \( \text{Ker}(\varphi_G) \) is trivial.

The first step might look like magic, but it is not. GAP has been used (see Appendix).

(i) It turns out that
\[
\sigma = (02)(16)(318)(419)(513)(720)(821)(917)(1011)(1215)(14\infty)(1622) \in G.
\]
Note \( \rho \) and \( \sigma \) together implies that \( G \) is transitive. Now \( \theta[G] \) contains
\[
\rho = (0 1 2 3 4 5 6) \quad \text{and} \quad \sigma = (\infty 0)(1 6)(2 3)(4 5).
\]
By Lemma 1.20 these generate an \( L_2(7) \). Finally \( |L_2(7)| = |L_3(2)| \).

(ii) Assume \( \alpha \in M_{24} \) fixes \( \infty, 0, \ldots, 6 \) and consider the octads defined by \( \infty \) and two points from \( 0 \). That is

\[
\begin{array}{cccccccc}
\times & \times & \times & \times & \times & \times & \times & \times \\
\times & \times & \times & \times & \times & \times & \times & \times \\
\times & \times & \times & \times & \times & \times & \times & \times \\
\end{array}
\quad \text{and} \quad
\begin{array}{cccccccc}
\times & \times & \times & \times & \times & \times & \times & \times \\
\times & \times & \times & \times & \times & \times & \times & \times \\
\times & \times & \times & \times & \times & \times & \times & \times \\
\end{array}
\]

Clearly \( \alpha \) has to permute these octads among each other. On the other hand they do not cut the same columns. Thus \( \alpha \) fixes all three octads and has the following fixed points
\[
\alpha =
\begin{array}{cccccccc}
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\
\end{array}
\]
But by Corollary 3.2 only the identity can fix nine points. Hence no permutation but the identity can fix all columns.

(iii) The element \( \beta = (\infty 2)(0 6)(1 6)(3 5) \) fixes \( \mathcal{H} \). Further
\[
\beta(D_1) = D_1 + 1, \quad \beta(D_2) = D_2 \quad \text{and} \quad \beta(D_3) = D_3.
\]
So $\beta \in \text{Ker}(\varphi)$. Assume $\beta \in \varphi_G[G]$. Then

$$\gamma = \rho^2 \sigma \rho^{-2} \beta = (0 \ 5)(3 \ 6) \in \varphi_G(G).$$

Since $\gamma^2$ fix all columns $\gamma^2 = 1$. Thus $\gamma$ is an involution fixing exactly 8 points, i.e fixing two columns and two points outside these columns, pointwise. But no two columns are in an octad so seven points not in an octad being fixed, contradicting Lemma 3.1. Thus $\sigma^i \beta \sigma^{-i} \notin \varphi_G[G]$ for $i = 0, \ldots, 6$ implying that $\text{Ker}(\varphi_G)$ is trivial.

Adding it all together we get $G \cong L_3(2) \cong L_2(7)$.

Besides the exceptional isomorphism between the projective groups above there is a further remarkable bonus with this construction. If we write the generator matrix to $\mathcal{H}$

$$
\begin{pmatrix}
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
$$

we see that $\mathcal{H}$ is self dual. Hence the above matrix is also the check matrix. But the top left submatrix is recognized as check matrix to the $[7, 3]$ Hamming code when the last column is a parity check column. Thus $\mathcal{H}$ is the extended Hamming code and we have shown the following theorem.

**Theorem 3.14.** The automorphism group of the extended Hamming code is isomorphic to $2^3 \cdot L_2(7)$.

### 3.4 Proof of maximality

Even though some cases are proved in a whole new way in the following proof, the main idea comes from Curtis article [2].

Let $A \subset \Omega$ of size $n \leq 12$. We say that $A$ is of type $S_n$ if it contains or is contained in an octad. Otherwise we say that $A$ is of type $U_n$ if it is
contained in a dodecad. If $A$ is neither of type $S_n$ nor $U_n$ we say that $A$ is of type $T_n$. It turns out that all types define orbits of $M_{24}$. Using that the octad stabilizer is 6-fold transitive on the octad being stabilized we see directly that $S_n$ defines orbits for $n \leq 8$. That the remaining types define orbits might not be that obvious, but most types are irrelevant for this proof. We need the following thou.

**Lemma 3.15.** The type $U_8$ defines an orbit of $M_{24}$.

*Proof.* Suppose $X$ and $Y$ be two sets of type $U_8$ and let

$$X = D_1 + \{a, b, c, d\}, a, b, c, d \in D_1 \quad \text{and} \quad Y = D_2 + \{e, f, g, h\}, e, f, g, h \in D_2.$$  

Since $M_{24}$ is transitive on dodecads exists a mapping $D_1 \mapsto D_2$. Further the stabilizer of $D_2$ is 5-fold transitive on $D_2$. Thus $\exists g \in M_{24}$ such that $g(X) = Y$. 

**Lemma 3.16.** Let $X \subseteq \Omega$. Then $X$ is congruent an unique monad, dyad, triad or sextet (i.e any tetrad of the sextet) or $\emptyset$ modulo $\mathcal{C}$.

*Proof.* If $|X| \geq 5$ the symmetric difference with an octad having 5 points in $X$ is always a smaller set. Clearly $|X|$ is fixed modulo $\mathcal{C}$ if $|X| \leq 4$. Finally suppose $X = \Lambda + C \equiv \Lambda' + D$, where $\Lambda$ and $\Lambda'$ are monads, dyads or sextets and $C, D \in \mathcal{C}$. Then $\Lambda + \Lambda' \in \mathcal{C}$ and the result follows. 

**Lemma 3.17.** Let $G$ be a permutation group of composite order acting primitively on a set $A$. If $n_i$ is the largest orbit length of $G_a$ acting on $A$ and $n_j$ is any other orbit length such that $n_j > 1$, then $(n_i, n_j) \neq 1$.

*Proof.* The proof is out of the scope of this thesis but can be found in [4] p. 48.

**Lemma 3.18.** Let $G$ be a permutation group of composite order acting primitively on an even set $A$. Then $G_a$ cannot have an orbit of length 1 or 2 on $A \setminus a$.

*Proof.* Since $G$ is primitive Lemma [4.3] implies that $G_a$ is maximal. Suppose $G_a$ fixes a further point $b$, in other words $G_a = G_b$. Then since $G$ is transitive $\exists \pi \in G$ such that $\pi(a) = b$. Clearly $\pi \in N_G[G_a] \setminus G_a$. As $G_a$ is maximal this yields $G_a \lhd G$. Thus $G_a = G_x \forall x \in A$, i.e $G$ is regular. But $G_a$ is maximal so this can only be true if $G$ is of prime order. Contradiction.
Suppose $G_a$ has an orbit $\{b, c\}$. Then from the restriction map $\varphi : G_a \rightarrow \text{Sym}(\{b, c\})$ we see that $[G_a : G_{ab}] = 2$, and by symmetry $[G_b : G_{ab}] = 2$. Thus $N_G[G_{ab}]$ contains $G_a$ and $G_b$. Since $G_a$ is maximal $N_G[G_{ab}] = G$. Consider the factor group $G/G_{ab}$. Clearly $G_a/G_{ab}$ is contained in some 2-group $P < G/G_{ab}$. The inverse image of $P$ is strictly between $G_a$ and $G$, contradicting that $G_a$ is maximal.

**Lemma 3.19.** Any subgroup of $M_{24}$ acting primitively of degree 4, 6, 8 or 12 in its action on blocks in $\Omega$, is doubly transitive on those blocks.

**Proof.** Let $s$ be the length of an orbit in the stabilizer of a block. By Lemma 3.18 $s \geq 3$ and by Lemma 3.17 $s$ has a factor in common with the largest orbit length. This rules out all cases.

**Lemma 3.20.** If $G \leq M_{24}$ is primitive then $G \cong L_2(23)$ or $G \cong M_{24}$.

**Proof.** The proof is out of the scope for this thesis but can be found in [5] p. 30.

Before we start with the big theorem we need some elements from $M_{24}$. As usual we leave the task to show that the elements actually are in $M_{24}$ to the interested reader. We start by defining three matrices $D$, $H$ and $L$.


Not that the rows in $H$ are the MOG trio and the rows in $L$ form a duum. We use the notation $[x \times y]_A$ for the element acting with $x$ on the columns and $y$ on the rows of matrix $A$. Similarly $[G \times H]_A$ denotes the group acting with $G$ on the columns and $H$ on the rows of matrix $A$. The names of the rows and columns are adapted to the following groups:

$$[L_2(5) \times A_4]_D, \quad [L_2(7) \times S_3]_H \quad \text{and} \quad [L_2(11) \times 1]_L.$$

They all turn out to be subgroups of $M_{24}$. Further the element

$$\begin{array}{cccccccccccc}
\ast & a & b & c & e & g & i & k & l & j & h & f \\
\ast & a & b & d & f & h & j & l & k & i & g & e
\end{array} \in M_{24},$$

where elements corresponding to the same letter form transpositions.
Theorem 3.21. The following nine groups describes all maximal subgroups of $M_{24}$.

<table>
<thead>
<tr>
<th>Description</th>
<th>Group</th>
<th>Order</th>
<th>Factorized order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monad stabilizer</td>
<td>$M_{23}$</td>
<td>10,200,960</td>
<td>$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$</td>
</tr>
<tr>
<td>Dyad stabilizer</td>
<td>$M_{22.2}$</td>
<td>887,040</td>
<td>$2^8 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$</td>
</tr>
<tr>
<td>Octad stabilizer</td>
<td>$2^4.A_8$</td>
<td>322,560</td>
<td>$2^{10} \cdot 3^2 \cdot 5 \cdot 7$</td>
</tr>
<tr>
<td>Triad stabilizer</td>
<td>$M_{21}.S_3$</td>
<td>241,920</td>
<td>$2^8 \cdot 3^3 \cdot 5 \cdot 7$</td>
</tr>
<tr>
<td>Duum stabilizer</td>
<td>$M_{12.2}$</td>
<td>190,080</td>
<td>$2^7 \cdot 3^2 \cdot 5 \cdot 11$</td>
</tr>
<tr>
<td>Sextet stabilizer</td>
<td>$(2^6.3).S_6$</td>
<td>138,240</td>
<td>$2^{10} \cdot 3^3 \cdot 5$</td>
</tr>
<tr>
<td>Trio stabilizer</td>
<td>$2^6.(S_3 \times L_2(7))$</td>
<td>64,512</td>
<td>$2^{10} \cdot 3^2 \cdot 7$</td>
</tr>
<tr>
<td>Projective group</td>
<td>$L_2(23)$</td>
<td>6,072</td>
<td>$2^3 \cdot 3 \cdot 11 \cdot 23$</td>
</tr>
<tr>
<td>Octern group</td>
<td>$L_2(7)$</td>
<td>168</td>
<td>$2^3 \cdot 3 \cdot 7$</td>
</tr>
</tbody>
</table>

Method of Proof. We will see that there are no containment among the above nine groups. Then we show that all proper subgroups of $M_{24}$ are contained in one of the above groups.

Proof. By only considering the orders and the fact that a group fixing a set cannot have a subgroup moving this set, we see that the only possible containments among the nine groups are that a Trio group contains an Octern group. Assume the elements $\rho$ and $\sigma$ in the Octern group fixes a trio. Since $\rho$ has shape $1^3.7^3$ it fixes least one octad $O$. Clearly $O$ is the union of a fixed point and a 7-cycle. But then another octad being fixed, i.e all three octads in the trio being fixed. Thus the trio is a partition of three pairs (fixed point, 7-cycle), related to $\rho$. We get six possible trios but $\sigma$ fixes neither one of them. Contradiction.

If $G \in M_{24}$ is intransitive let $\Lambda$ denote one of the orbits. Either $G$ is contained in the octad or duum stabilizer or by Lemma [3.16] $\Lambda = X + C$ where $X$ is an unique monad, dyad, triad or sextet and $C \in \mathcal{C}$. But then $G$ fixes $X$ and thus is contained in corresponding stabilizer.
If $G$ is primitive Lemma 3.20 implies that $G \cong L_2(23)$ or $G \cong M_{24}$. If $G$ is imprimitive we divide six cases, namely the possible block sizes.

**Blocks of size 12.** Clearly the two blocks are congruent modulo $C$. By Lemma 3.16 they are congruent to an unique monad, dyad, triad, sextet or $\emptyset$ modulo $C$. Note that for $G$ to be transitive the only possible options are $\emptyset$ and a sextet. Thus $G$ is contained in corresponding stabilizer.

**Blocks of size 8.** Suppose $\Omega = X + Y + Z$, $|X| = |Y| = |Z| = 8$. If $X$ (and thus $Y$ and $Z$) is of type $S_8$ $G$ is in the trio stabilizer. If $X$ is of type $T_8$ it is congruent to an unique dyad modulo $C$. Thus $X$, $Y$ and $Z$ defines a set of three dyads being stabilized, contradicting that $G$ is transitive. Finally suppose $X$ is of type $U_8$. Then $X = T + D$ for some tetrad $T$ and the dododecad $D$ containing $X$. Clearly $T$ and $X$ are disjoint. Since the cut of a dododecad and an octad is 2, 4 or 6, the sextet containing $T$ has further tetrads cutting $D$ in 0 or 2 points. Thus there are exactly two tetrads disjoint from $X$, these form an octad $O_X$. Similarly $Y$ and $Z$ defines octads $O_Y$ and $O_Z$. Clearly $G$ preserves these three octads. As $G$ is transitive we have $O_X + O_Y + O_Z = \Omega$, i.e $O_X$, $O_Y$, $O_Z$ form a trio. Hence $G$ is in the trio stabilizer.

**Blocks of size 6.** Suppose the blocks are $X$, $Y$, $Z$ and $T$. By Lemma 3.19 $G$ is doubly transitive on the blocks. If the blocks are of type $S_6$, the octad containing $X$ has at least one point in $Y$, say, and zero points in $Z$. As $G$ is doubly transitive on the blocks we can fix $X$, and thus the octad containing $X$, and map $Y$ to $Z$. Contradiction. Hence all blocks are of type $U_6$. Clearly the sum of any two blocks are congruent an even set modulo $C$. As $G$ is transitive on $\Omega$ the sum cannot be a dyad. If the sum is congruent $\emptyset$ we get $X \equiv Y \equiv Z \equiv T$ mod $C$. Since each block are congruent to the same sextet $G$ is in the sextet stabilizer. If the sum is congruent a sextet there are three sextets $S_1 = X + Y$, $S_2 = X + Z$ and $S_3 = Y + Z$, with the property $S_1 + S_2 = S_3$. By Lemma 2.6 an octad cuts a sextet $4^2.0^4$, $2^4.0^2$ and $3.1^5$. Using this and the fact that all concerned tetrads must cut each other in 0, 1 or 2 points, it is easy to show that there are only two ways two sextets can intersect such that the sum is a further sextet. By permuting the rows and
columns we get the following intersection matrices

\[
\begin{bmatrix}
2 & 2 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 2 & 0 & 0 \\
0 & 0 & 2 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 2 \\
0 & 0 & 0 & 0 & 2 & 2 \\
\end{bmatrix}
\quad \text{and} \quad
\begin{bmatrix}
2 & 0 & 0 & 0 & 1 & 1 \\
0 & 2 & 0 & 0 & 1 & 1 \\
0 & 0 & 2 & 0 & 1 & 1 \\
0 & 0 & 0 & 2 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 \\
\end{bmatrix}
\]

where the rows correspond to \(S_1\), say, and columns to \(S_2\). In the first case \(S_1\) and \(S_2\) are refinements to a unique trio. Thus \(G\) is in the trio stabilizer. In the second case let \(S_1\) be the columns in following matrix (MOG is not necessarily the underlying table) and \(S_2\) the written out numbers.

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 1 & 1 \\
1 & 2 & 3 & 4 & 2 & 2 \\
5 & 5 & 5 & 5 & 3 & 3 \\
6 & 6 & 6 & 6 & 4 & 4 \\
\end{array}
\]

We note that \(S_3\) has to cut \(S_1\) in the same way. Summing the tetrads and possibly swapping the two top entries in the 4 first rows (\(S_1\) and \(S_2\) and are preserved under this action) we may assume that

\[
S_3 =
\begin{bmatrix}
5 & 5 & 5 & 1 & 1 \\
6 & 6 & 6 & 2 & 2 \\
1 & 2 & 3 & 4 & 3 & 3 \\
1 & 2 & 3 & 4 & 4 & 4 \\
\end{bmatrix}
\]

Now each sextet has a unique octad that cuts the other two sextets \(2^4.0^2\). Written out in the same table as above,

\[
\begin{array}{cccc}
B & B & B & B & C \\
B & B & B & B & C \\
\end{array}
\]

we see that they form a trio. Thus \(G\) is in the trio stabilizer.

**Blocks of size 4.** By Lemma 3.19, \(G\) is doubly transitive on the blocks. Thus \(5||G||\) and one of the Sylow 5-subgroups in \(M_{24}\) is in \(G\). Since all Sylow 5-subgroups are conjugates we may assume that the element of order 5 in \(G\), fixing one block, is \(\rho = [(\infty)(01234) \times I_D]\). Clearly the group
\[ H = \langle [I \times A_4]|_D, ([\infty](0)(1\ 2\ 4\ 3) \times (\infty\ 0)|_D \rangle \] normalize \( \rho \). Hence we can conjugate with \( H \) without budge the first column. Using \( \rho \) we see that up to conjugation by \( H \) the possible block structures are

\[
\begin{array}{cccc}
0 & 2 & 3 & 4 & 5 \\
0 & 2 & 3 & 4 & 5 \\
0 & 2 & 3 & 4 & 5 \\
0 & 2 & 3 & 4 & 5 \\
0 & 2 & 3 & 4 & 5 \\
0 & 2 & 3 & 4 & 5 \\
0 & 2 & 3 & 4 & 5 \\
0 & 2 & 3 & 4 & 5 \\
\end{array}
\]

If two blocks are of type \( S_8 \) then \( G \) is in the sextet stabilizer, due to the double transitivity on the blocks. If two blocks are of type \( T_8 \) they are congruent to a dyad modulo \( \mathcal{C} \). Totally this gives \( \binom{6}{2} = 15 \) dyads. Suppose \( a \in \Omega \) is in exactly \( n \) of the 15 dyads. Since conjugation by \( g \in G \), such that \( g(a) = b \) preserves the blocks, \( b \) is also in exactly \( n \) dyads. As this holds for \( \forall b \in \Omega \) the 15 dyads contains \( 24n \) elements, counted with repetition. Contradiction.

Clearly the sum of block 0 and \( \bullet \) is of type \( S_8 \) in case (i) and of type \( T_8 \) in case (ii). Suppose two blocks are of type \( U_8 \). We want to show that that there is a unique pairing of the points in the set such that the union of any three pairs is of type \( S_6 \). As both \( S_6 \) and \( U_8 \) defines orbits it is enough to investigate one set of type \( U_8 \). Consider the set \( \begin{array}{cccc}
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\end{array} \). Since a set of type \( S_6 \) with 5 points in \( \Lambda_1 \) has to be a subset of \( \Lambda_1 \), we immediately see that the two points not in \( \Lambda_1 \) form a pair. By gradually removing two points to see if the remaining form a set of type \( S_6 \), we easily eliminate all cases but

\[
\begin{array}{cccc}
1 & 1 & 4 & 4 \\
2 & 2 & 3 & 3 \\
\end{array}
\]. For \( G \) to be doubly transitive on the blocks this pairing has to cut the blocks in the same way. For case (iii) we have that

\[
\begin{array}{cccc}
0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 \\
\end{array}
\] induces the pairing

\[
\begin{array}{cccc}
2 & 3 & 1 & 2 \\
1 & 4 & 3 & 4 \\
\end{array}
\]
while
\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & 2 & 3 \\
1 & 2 & 1
\end{array}
\]
induces the pairing
\[
\begin{array}{ccc}
4 & 1 & 2 \\
3 & 2 & 1 \\
4 & 2 & 3
\end{array}
\]

a contradiction. We got similar contradictions in the cases (iv)-(vii). For case (viii) we write down the sextets corresponding to each block. The xes denotes the blocks defining the sextets.

\[
\begin{array}{cccc}
x & 1 & 2 & 3 \\
x & 1 & 2 & 3 \\
x & 1 & 2 & 3 \\
2 & 5 & 5 & x \\
1 & x & 2 & 2 \\
3 & 5 & 1 & 4 \\
5 & 4 & 3 & 1
\end{array}
\]

\[
\begin{array}{cccc}
2 & 4 & 2 & 1 \\
5 & 5 & 5 & 2 \\
3 & 4 & 3 & 1 \\
4 & 3 & 4 & 2 \\
1 & 2 & 2 & 1 \\
5 & x & 5 & 5 \\
4 & 3 & 4 & 3 \\
2 & x & x & 3
\end{array}
\]

\[
\begin{array}{cccc}
4 & 3 & 5 & 3 \\
1 & 1 & 2 & 5 \\
2 & 2 & 1 & 2 \\
3 & 4 & 5 & 3 \\
1 & 3 & 2 & 5 \\
2 & x & x & 3
\end{array}
\]

The tetrads that are not named x are called non-special. We now create the graph \((\Omega, E)\), where \((a, b) \in E\) if and only if \(a\) and \(b\) occur together in exactly one non-special tetrad. We draw the graph:

![Graph](image)

We see that the graph consists of two disjoint subgraphs containing the dodecads

\[
\begin{array}{ccccc}
x & x & x & x & x \\
x & x & x & x & x \\
x & x & x & x & x
\end{array}
\]

and

\[
\begin{array}{ccccc}
x & x & x & x & x \\
x & x & x & x & x \\
x & x & x & x & x
\end{array}
\]

respectively.
As the blocks are preserved by $G$, so is the graph. Hence $G$ is in the duum stabilizer.

**Blocks of size 3.** By Lemma 3.19 $G$ is doubly transitive on the blocks. Thus $7|G|$ and as in the previous case we may assume that the element of order 7 in $G$, fixing one block, is $\rho = [(\infty)(0123456) \times I]_H$. The group $H = \langle [I \times S_3]_H, [(\infty)(0124)(365)] \times I \rangle_H$ normalizes $\rho$ and up to conjugation by $H$ the possible block structures are

For case (i) we write the columns/blocks in MOG.

Clearly any pair of blocks satisfy the parity condition in the square and thus is congruent to a sextet visualized in MOG. We write down seven of the the pairs

\[
\infty + 0 \equiv \begin{array}{ccc}
\times \\
\times \\
\times \\
\times \\
\end{array}, \quad \infty + 1 \equiv \begin{array}{ccc}
\times \\
\times \\
\times \\
\times \\
\end{array}, \quad \infty + 2 \equiv \begin{array}{ccc}
\times \\
\times \\
\times \\
\times \\
\end{array}, \quad \infty + 3 \equiv \begin{array}{ccc}
\times \\
\times \\
\times \\
\times \\
\end{array}, \quad \infty + 4 \equiv \begin{array}{ccc}
\times \\
\times \\
\times \\
\times \\
\end{array}, \\
\infty + 5 \equiv \begin{array}{ccc}
\times \\
\times \\
\times \\
\times \\
\end{array} \quad \text{and} \quad \infty + 6 \equiv \begin{array}{ccc}
\times \\
\times \\
\times \\
\times \\
\end{array}.
\]
These are refinements of the MOG trio. It turns out that all further pairs also are congruent to one of the above sextets. It is easy to convince oneself that the MOG trio is unique trio having all seven sextets as refinements. As the seven sextets are preserved, as a set, \( G \) is in the trio stabilizer.

In case (ii) the sum of block 0 and \( \bullet \) is of type \( U_6 \) while the sum of block \( \bullet \) and 2 is of type \( S_6 \), contradicting that \( G \) is doubly transitive on the blocks.

Similarly in case (iii) the sum of block 0 and \( \bullet \) is of type \( S_6 \) while the sum of block 1 and 3 is of type \( U_6 \).

For case (iv) we write the blocks in MOG,

\[
\begin{array}{cccc}
0 & \bullet & 0 & 7 \\
5 & 6 & 4 & 5 \\
2 & 4 & \bullet & 3 \\
3 & 7 & 2 & 6
\end{array}
\quad \begin{array}{cccc}
6 & 3 & 4 & 3 \\
1 & 5 & 2 & 3 \\
5 & 6 & 5 & 4 \\
3 & 1 & 5 & 2
\end{array}
\]

The sum of block 0 and \( \bullet \) is congruent to the sextet \( 6 3 4 3 1 5 \) and the sum of block 2 and 3 is congruent to \( 5 5 4 3 2 5 \). These two sextets do not cut the blocks in the same way, contradicting that \( G \) is doubly transitive on the blocks.

Suppose the case is (v). Let \( \hat{G} \) be the maximal group preserving the blocks. We write out the blocks in MOG,

\[
\begin{array}{cccc}
0 & 4 & 0 & 3 \\
\bullet & 2 & 7 & \bullet \\
5 & 7 & 4 & 6 \\
6 & 3 & 5 & 2
\end{array}
\quad \begin{array}{cccc}
0 & \bullet & 0 & 6 \\
1 & 5 & 2 & 3 \\
4 & 3 & 1 & 1 \\
2 & 4 & 3 & 2
\end{array}
\]

Now any pair of blocks is of type \( U_6 \) and is congruent to a sextet modulo \( \mathcal{C} \). Let \( \mathcal{B} \) denote the set of blocks and let \( b_1, b_2 \in \mathcal{B} \). Suppose \( b_1 + b_2 \equiv S \) (mod \( \mathcal{C} \)). If \( x \in b_1 + b_2 \) and \( O \) is the octad defined by \( b_1 + b_2 + \{ x \} \), clearly \( x \) is the unique element in \( b_1 + b_2 \) that is in the tetrad \( b_1 + b_2 + O \in S \). We say that a pair \( x, y \) is special if \( x \) and \( y \) lies in different blocks. Each special pair \( x, y \in \Omega \) defines a sextet \( S \) such that \( x \in T_i \) and \( y \in T_j \) for some tetrads \( T_i, T_j \in S, \ T_i \neq T_j \). Thus there is a well defined function \( f \) on special pairs

\[
f(x, y) = \left| \{ b \in \mathcal{B} | b \cap T_i = |b \cap T_j| = 1 \} \right|, \ \text{where} \ x \in T_i, y \in T_j.
\]

We now define a relation \( \sim \) on \( \Omega \) by
\[ x \sim x, \forall x \in \Omega, \]

\[ x \sim y \text{ if } f(x, y) \geq 2, \]
in other cases \( x \not\sim y \). If \( x, y \) is a special pair lying in tetrads \( T_i \) and \( T_j \) and \( g \in \hat{G} \) we have

\[
\begin{align*}
    f(g(x), g(y)) &= \left\{ b \in \mathcal{B} \left| b \cap gT_i = |b \cap gT_j| = 1 \right\} \right. \\
    &= \left\{ b \in \mathcal{B} \left| gg^{-1}b \cap gT_i = |gg^{-1}b \cap gT_j| = 1 \right\} \right. \\
    &= \left\{ b \in \mathcal{B} \left| g(g^{-1}b \cap T_i) = |g(g^{-1}b \cap T_j)| = 1 \right\} \right. \\
    &= \left\{ b \in \mathcal{B} \left| g^{-1}b \cap T_i = |g^{-1}b \cap T_j| = 1 \right\} \right. \\
    &= \left\{ b \in \mathcal{B} \left| b \cap T_i = |b \cap T_j| = 1 \right\} \right. = f(x, y).
\]

Hence \( G \) preserves the relation \( \sim \). We will to show that \( \sim \) induce a partition of \( \Omega \) into three sets which will turn out to be the MOG trio. We start by noting that \( \rho \) preserves the MOG trio and having a 7-cycle in each brick. We see that the element \( \sigma = \begin{array}{ccc} 1 & 1 & \times \\ \times & \times & 2 \end{array} \) preserves \( \mathcal{B} \). Clearly \( \langle \rho, \sigma \rangle \) is doubly transitive on the first brick. Further the element

\[
\alpha = (\infty \ 17 \ 22)(0 \ 13 \ 19)(1 \ 8 \ 11)(2 \ 21 \ 3)(4 \ 9 \ 14)(5 \ 20 \ 7)(6 \ 15 \ 16)(10 \ 12 \ 18) \in M_{24}
\]

preserves \( \mathcal{B} \) and is transitive on the bricks. From the sextet,

\[
\begin{array}{cccccc}
4 & 5 & 6 & 6 & 3 & 2 \\
5 & 4 & 1 & 1 & 3 & 2 \\
2 & 2 & 4 & 5 & 6 & 1 \\
3 & 3 & 4 & 5 & 1 & 6
\end{array}
\]
defined by the points \( \infty \) and 0, we see that the blocks 0 and 1 both the cut the tetrads 4 (containing \( \infty \)) and 5 (containing 0). Thus \( f(\infty, 0) = 2 \) and \( \infty \sim 0 \). Since \( \hat{G} \) is doubly transitive on the first brick and preserves \( \sim \), all points in the first brick are related. Let \( x \in \Lambda_1 \) and \( y \in \Lambda_2 \) and suppose \( x \sim y \). Pick \( g \in \langle \rho, \sigma \rangle \) such that \( g(x) = \infty \). As \( \infty \) and 17 are in the same block \( \infty \sim 17 \). Thus \( g(y) \in \Lambda_2 + \{17\} \).
Multiplication with $\rho^i$ for a suitable $i$ implies that $\infty \sim 11$. But by looking at the sextet

\[
S = \begin{bmatrix}
1 & 1 & 5 & 6 & 2 & 4 \\
2 & 4 & 3 & 1 & 5 & 5 \\
2 & 4 & 1 & 3 & 6 & 6 \\
3 & 3 & 5 & 6 & 4 & 2
\end{bmatrix}
\]
defined by the points $\infty$ and 11,

we see that no block cuts the tetrad $1$ (containing $\infty$) and 6 (containing 11) in one point each. Contradiction. Thus no elements in $\Lambda_1$ are related to an element in $\Lambda_2$. Further multiplication with $\alpha$ shows that all element in one brick are related and no two element from different bricks are related. Since $G \leq \hat{G}$, $G$ stabilize the MOG trio.

Finally, we constructed the Octern group as the maximal subgroup of $M_{24}$ preserving the block structure in case (vi).

### Blocks of size 2

By Lemma 3.19 $G$ is doubly transitive on the blocks. Clearly $11| |G|$. As before we may assume that the element of order 11 is $\rho = [(\infty)(0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10) \times I]_L$. The group

\[
H = \langle [(\infty)(0 \ 1 \ 3 \ 9 \ 5 \ 4 \ 2 \ 6 \ 7 \ 10 \ 8) \times I]_L, \begin{array}{cccccccc}
a & b & c & e & g & i & k & l \\
--- & --- & --- & --- & --- & --- & --- & ---
\end{array} \rangle
\]

normalizes $\rho$. Up to conjugation of $H$ the possible block structures are

(i) \[
\begin{array}{cccccccccc}
0 & 0 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
Y & Y & 0 & 0 & 2 & 3 & 4 & 5 & 6 & 7
\end{array}_L
\]

(ii) \[
\begin{array}{cccccccccc}
0 & 0 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
Y & Y & 0 & 0 & 2 & 3 & 4 & 5 & 6 & 7
\end{array}_L
\]

(iii) \[
\begin{array}{cccccccccc}
0 & 0 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
Y & Y & 0 & 0 & 2 & 3 & 4 & 5 & 6 & 7
\end{array}_L
\]

For case (i) let $\hat{G}$ be the maximal subgroup preserving the blocks, and $\hat{G}_{\infty 2}$ the subgroup stabilizing the blocks $\infty$ and 2. We write the sextet corresponding to $\infty + 2$.

\[
\begin{array}{cccccccc}
1 & 5 & 6 & 1 & 2 & 5 & 3 & 4 \\
1 & 4 & 2 & 1 & 3 & 4 & 3 & 2
\end{array}_L
\]

Let $X$ be the octad containing 1’s and 5’s. Then $\forall g \in \hat{G}_{\infty 2}$ we have $X + gX \in G$ implying that $gX = X$ or $|X + gX| = 8$. Note that $g$ preserves
both the blocks and the sextet above. If \( gX = X \) then \( g^2 = 1 \). If \( g \) is an involution of type one, tetrad 1, 3 and 5 has to be fixed. On tetrad there are two possibilities for \( g \), plainly \( g = 1 \) or \( g = (2 \, 6) \). In the first case we see that columns 3, 6, 7, 8 has to be fixed. But \( 3 + 6 + 7 + 8 \notin \mathcal{G} \), a contradiction. In the second case no column containing a 2 or a 6 can contain a fixed point. Thus there must be an octad in the sum of the remaining columns, i.e \( \infty + 0 \, 2 \, 4 \, 5 \, 10 \) contains an octad. There are only two such octads,

\[
\begin{array}{cccc}
\times & x & x & x \\
\times & x & x & x \\
\times & x & x & x \\
\end{array}
\quad \text{and} \quad
\begin{array}{cccc}
\times & x & x & x \\
\times & x & x & x \\
\times & x & x & x \\
\end{array}
\]

Both contain the points 0, 12, 15, 19 which spread over \( \infty, 0, 2, 10 \). Thus 4 and 5 cannot contain fixed points. Especially in column 4 tetrad 4 and 5 has to be swapped. Contradiction. If \( g \) is an involution of type two, we end up with two cases.

\[
g = (\infty \, 0) (1 \, 16) (2 \, 3) (4 \, 20) (5 \, 11) (6 \, 7) (8 \, 22) (9 \, 17) (10 \, 15) (12 \, 14) (13 \, 19) (18 \, 21)
\]

or

\[
g = (\infty \, 0) (1 \, 16) (2 \, 3) (4 \, 20) (5 \, 11) (6 \, 18) (7 \, 21) (8 \, 22) (9 \, 17) (10 \, 15) (12 \, 14) (13 \, 19),
\]

but neither is in \( M_{24} \). Thus \( g = 1 \). Suppose \( |X + gX| = 8 \) and let \( X' = X + \infty + 2 \). If \( gX' = hX' \) for some \( h \in \tilde{\mathcal{G}}_{\infty 2} \) then \( h^{-1} gX' = X' \) implying that \( g = h \). Hence if \( g' \in \tilde{\mathcal{G}}_{\infty 2} \) and \( g \neq g' \) then \( gX' \) and \( g'X' \) are disjoint sets.

Thus \( |\tilde{\mathcal{G}}_{\infty 2}| \leq \frac{|\Omega + \infty + 2|}{|X'|} = 5 \), implying that \( |\tilde{\mathcal{G}}| \leq 12 \cdot 11 \cdot 5 = |L_2(11)|. \)

But \( \tilde{\mathcal{G}} \) contains \([L_2(11) \times I]_L \) so they must be isomorphic. Hence \( \tilde{\mathcal{G}} \) is in the dodecad stabilizer and so is \( \mathcal{G} \).

For doubly transitivity to hold each two blocks must be contained in the same number of sets of type \( S_6 \) which are union of blocks. In case (ii) the five tetrads that together with block 0 and \( \bullet \) form an octad are:

\[\{1, 11, 14, 16\}, \{4, 13, 20, 21\}, \{2, 8, 17, 22\}, \{10, 12, 17, 17\} \text{ and } \{3, 5, 19, 9\}.\]

There are exactly 4 blocks that are contained in one of the above sets. Thus the two blocks 0 and \( \bullet \) are contained in 4 sets of type \( S_6 \) which are unions of blocks. The five tetrads that together with block \( \bullet \) and 2 form an octad are:

\[\{\infty, 0, 10, 18\}, \{11, 13, 16, 20\}, \{5, 8, 9, 17\}, \{1, 4, 14, 21\} \text{ and } \{2, 3, 19, 22\}.\]
There are only 3 blocks that are contained in one of these sets. Hence case (ii) cannot occur. Similar reasoning rules out case (iii).

3.5 Generators of $M_{24}$

Let $\alpha$ and $\gamma$, i.e the usual generators to $L_2(23)$, be two of the generators. Since $L_2(23)$ is maximal and $5 \nmid |L_2(23)|$ any $\delta \in M_{24}$ such that $o(\delta) = 5$ works as a final generator to $M_{24}$. It turns out that $M_{24}$ is generated by

$$\alpha = (\infty)(0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22)$$
$$\gamma = (0\ \infty)(1\ 22)(2\ 11)(3\ 15)(4\ 17)(5\ 9)(6\ 19)(7\ 13)(8\ 20)(10\ 16)(12\ 21)(14\ 18)$$
$$\delta = (\infty)(0)(1)(2\ 16\ 9\ 6\ 8)(3\ 12\ 13\ 18\ 4)(5)(7\ 17\ 10\ 11\ 22)(14\ 19\ 21\ 20\ 15).$$
4. Simplicity of the Mathieu groups

Lemma 4.1. If $G$ is a transitive permutation group on a set $A$ and $N \triangleleft G$ then $N$ is $1/2$-transitive. If in addition $N$ is nontrivial and $G$ is primitive then $N$ is transitive.

Proof. Let $S$ be an orbit of $N$ of minimal length. Then $\forall g \in G$ we have $N(gS) = (Ng)S = (gN)S = g(NS) = gS$ so $gS$ is a union of orbits of $N$. Since $S$ is of minimal length and $|S| = |gS|$ we see that $gS$ is exactly one orbit. Now $G$ is transitive so every orbit of $N$ has the same length (having the form $gS$). Thus $N$ is $1/2$ transitive. Finally two different orbits are disjoint so $S$ form a set of imprimitivity for $G$. Thus if $G$ is primitive we have two cases, either $|S| = 1$ implying $N$ is trivial, or $|S| = |A|$ implying $N$ is transitive.

We will handle the small and large Mathieu groups separately. The methods on the two cases are very similar thou. The main idea, taken from [7], is to use induction and the main difference is the base cases. The key lemma used is the following.

Lemma 4.2. Let $G$ be a primitive permutation group on a set $A$. If $G_a$ is simple then $G$ is simple or every proper and nontrivial normal subgroup of $G$ is regular.

Proof. Assume $\langle 1 \rangle < N < G$. By Lemma 4.1 $N$ is transitive. Since $G_a$ is simple and $(N_a \cap G_a) \triangleleft G_a$ we must have $N_a = \langle 1 \rangle$ or $N_a = G_a$. If $N_a = \langle 1 \rangle$ then $N$ is a regular normal subgroup and If $N_a = G_a$ then $|A| = [G : G_a] = [N : G_a]$ implying that $G = N$. ■
Suppose $N$ is a regular normal subgroup of a 2-transitive group $G$. If $n, m \in N$,
\[ n(a) = b \quad \text{and} \quad m(a) = c, \]
then $\exists g \in G$ such that $gmg^{-1}(a) = b$. Since $gmg^{-1}n^{-1} \in N$ fixes $b$ it follows that all nonidentity elements in $N$ are conjugates. Hence all nonidentity elements in $N$ have the same cycle shape. As $N$ is regular this cycle shape is $p^n$ for some prime $p$.

**Lemma 4.3.** Let $G$ be a 2-transitive permutation group on a set $A$. If $G$ contains a regular normal subgroup $N$ then $|A| = |N| = p^n$ for some prime $p$.

**Proof.** Using Lemma 1.11 we see that $G$ is primitive and by Lemma 4.1 $N$ is transitive. Finally Corollary 1.6 implies that $|A| = |N|$ and the result follows from the above discussion. ■

**Theorem 4.4.** The Mathieu group $M_{11}$ is simple.

**Proof.** Assume $N \triangleleft M_{11}$ is proper and nontrivial. Since $M_{11}$ is doubly transitive it is primitive. By by Lemma 4.1 $N$ is transitive and so $11 | |N|$. Let $P$ be a Sylow 11-subgroup of $N$ and $s_{11}$ the number of Sylow 11-subgroups in $M_{11}$. From Sylow's third theorem we have that
\[ s_{11} = \frac{11 \cdot 10 \cdot 9 \cdot 8}{|N_{M_{11}}[P]|} \quad \text{and} \quad s_{11} \equiv 1 \pmod{11}, \]
implying that $s_{11} = 144$ and $|N_{M_{11}}[P]| = 55$. Now since $P < N < G$ and all Sylow 11-subgroups are conjugates, $N$ contains all 144 Sylow 11-subgroups. Using Sylow’s third theorem again we obtain $|N| = 144 \cdot N_N[P] = 11 \cdot 2 \cdot 9 \cdot 8$. Note that $N_N[P]$ contains exactly eleven elements since it contains $P$ and $N$ and is proper. Further $[N : N_N] = 11$ yields $N \cap M_{10} \neq \langle 1 \rangle$, where $M_{10} < M_{11}$ is the isotropy group fixing $a$. Now $N \cap M_{10} \triangleleft M_{10}$. As $M_{10}$ is doubly transitive and Lemma 1.11 implies that $M_{10}$ is primitive. Further Lemma 4.1 implies that $N \cap M_{10}$ is transitive on ten points. This yields $10 | |N \cap M_{10}|$ implying $10 | |N|$. Contradiction. ■

**Theorem 4.5.** The Mathieu group $M_{12}$ is simple.

**Proof.** Since $M_{11}$ is simple Lemma 4.2 implies that $M_{12}$ is simple or contains a regular normal subgroup. But 12 is not a prime power so by Lemma 1.16 $M_{12}$ cannot have a regular normal subgroup. ■
Theorem 4.6. The subgroup $M_{21}$ is simple.

Proof. We first note that $|M_{21}| = 2^6 \cdot 3^2 \cdot 5 \cdot 7$. Assume $N < M_{21}$ is nontrivial and proper. Since $M_{21}$ is 2-transitive Lemma 1.11 and Lemma 4.1 implies that $N$ is transitive. Hence $7||N|$. Let $\langle g \rangle$ be a Sylow 7-subgroup of $N$. By Lemma 1.2 $M_{21} = N_{M_{21}}[\langle g \rangle]N$. Let $H = N_{M_{21}}[\langle g \rangle]$.

We now want to show that $|H| = 21$. By Corollary 3.2 $g$ can only have cycle shape $1^3.7^3$. Thus $H$ is imprimitive with these 7-cycles as blocks. Assume $5||H|$. Then $\exists x \in H$ such that $o(x) = 5$. Define the restriction map to the three blocks $\varphi : H \rightarrow S_3$. By considering the order we get $x \in \text{Ker}(\varphi)$. But then $x$ fixes at least two points in each block plus the three points fixed by $M_{21}$, i.e nine points, contradicting Corollary 3.2. Further assume $2||H|$. Then $H$ contains an involution $y$. By Theorem 3.13 there are only two types of involutions so $y$ fixes exactly eight points, i.e the three points fixed by $M_{21}$ plus five more. For $y$ to not have more than eight fixed points this leaves two cases. Either all five points are in one block or one block contains three points and two other one point. In either case $ygy^{-1} \notin \langle g \rangle$. Contradiction. Thus $|H| = 21$ or 63. By Sylow’s third theorem the latter is impossible.

Since $N$ is proper we cannot have $H = N$ and so $H \cap N = \langle g \rangle$. By the second isomorphism theorem we have

$M_{21}/N = HN/N \cong H/(N \cap H) = H/\langle g \rangle \cong \mathbb{Z}_3$.

Hence $|N| = 2^6 \cdot 3 \cdot 5 \cdot 7$ and by Lemma 1.3 $|N_a| = 2^6 \cdot 5$. Now $N_a < G_a$. Let $\langle h \rangle$ be a Sylow 5-subgroup of $N_a$. Then Lemma 1.2 gives $G_a = N_{G_a}[\langle h \rangle]N_a$. By consideration of the order $3||N_{G_a}[\langle h \rangle]|$ and so $\exists n \in N_{G_a}[\langle h \rangle]$ such that $o(n) = 3$. As $G_a$ fixes a sextet and one tetrad pointwise in this sextet, there is a well defined restriction map to the action on the remaining tetrads $\theta : G_a \rightarrow S_5$. Clearly $\theta(h)$ is 5-cycle. If $n \in \text{Ker}(\theta)$ then $n$ fixes at least one points each of the five tetrads, i.e at least nine points, contradicting Corollary 3.2. Thus $\theta(n)$ is a 3-cycle. But in $S_5$ no 3-cycle normalize a Sylow 5-subgroup.

Theorem 4.7. The Mathieu groups $M_{22}$, $M_{23}$ and $M_{24}$ are simple.

Proof. Since $M_{21}$ is simple Lemma 4.2 implies that $M_{22}$ is simple or contains a regular normal subgroup. As 22 is not a prime power Lemma 4.3 implies that
$M_{22}$ is simple. Similarly $M_{23}$ is simple or contain a regular normal subgroup or order 23. But $M_{23}$ is 3-transitive so no subgroup of order 23 is normal. Hence $M_{23}$ is simple. Finally $M_{24}$ is simple since 24 is not a prime power. ■
5. Uniqueness of the small Mathieu groups

The goal is to show that up to isomorphism (i.e. up to relabeling of the points) $M_{11}$ is the unique nontrivial sharply 4-fold transitive group. Then using this to prove uniqueness for $M_{12}$. As a bonus we will get an explicit construction of the small Mathieu groups.

**Lemma 5.1.** All permutations of order two in $M_{11}$ are conjugates and have exactly three fixed points. Further let $g$ and $h$ be two such permutations that commute. If $(ab)$ is a cycle in $g$ then one of the following holds:

- $h$ contains $(ab)$
- $h$ contains $(a)(b)$
- $h$ contains $(ac)(bd)$ where $g$ contains $(cd)$

**Proof.** In the proof of Theorem 1.16 we saw that all such involutions were conjugates. Because of the 4-transitivity $\exists x \in M_{11}$ such that $x$ contains $(1\ 2)(3\ 4)$. Further $x^2$ fixes four points and so $x^2 = 1$. Hence $x$ is of order two. Since the degree of $M_{11}$ is odd $x$ has an odd number (less than four) of fixed points and so $x$ fixes exactly three points. Since all other permutations of order two are conjugates to $x$ all they fixes three points.

If $h(a) = a$ then $h(b) = hg(a) = gh(a) = g(a) = b$ and we got the first case. If $h(a) = b$ then $h(b) = hg(a) = gh(a) = g(b) = a$ and we got the second case. Finally let $h(a) = c$, where $c$ is neither $a$ nor $b$. Then $h(b) = hg(a) = gh(a) = g(c) = d$ for some $d$ not equal to $a$, $b$ or $c$. This is the third case. $\blacksquare$

**Theorem 5.2.** The Mathieu group $M_{11}$ is unique up to isomorphism.
Note. Even if the following proof is possible to do by hand I want to point out that it has been created using GAP (see Appendix).

Proof. Through this proof we will be using Lemma 5.1 frequently and so refer to it as “the lemma”. Up to isomorphism we can assume that the element containing \((1 \, 2)(3 \, 4)\) in \(M_{11}\) is

\[ x_1 = (1 \, 2)(3 \, 4)(5 \, 6)(7 \, 8). \]

Due to the sharply 4-fold transitivity there is an unique element \(x_2\) containing \((1 \, 2)(3 \, 4)\). Since \(x_1x_2\) and \(x_2x_1\) agree on \(\{1, 2, 3, 4\}\) they are identical so \(x_1\) and \(x_2\) commute. Since both \(x_1\) and \(x_2\) contains the cycle \((1 \, 2)\) they cannot have another common 2-cycle. Using the lemma on \((5 \, 6)\) and the fact that \(x_2\) already fixes two points we can assume that up to isomorphism

\[ x_2 = (1 \, 2)(5 \, 7)(6 \, 8)(9 \, 10) \quad \text{implying} \quad x_1x_2 = (3 \, 4)(5 \, 8)(6 \, 7)(9 \, 10). \]

Let \(x_3\) be the unique element containing \((1 \, 3)(2 \, 4)\). As above \(x_1\) and \(x_3\) commute. Using the lemma on \((5 : 6)\) and the fact that all three pairs of 2-cycles in \(\{5, 6, 7, 8\}\) are already present implies that \(x_3\) contains exactly one of \((5 \, 6)\) and \((7 \, 8)\). These are equivalent up to isomorphism so we can assume \(x_3\) contains \((5 : 6)\). Now \(x_2x_3\) contains \((1 \, 3 \, 2 \, 4)\) and have order four since \((x_2x_3)^4 = 1\). If \(x_2x_3\) do not contain \((9 \, 10)\) is also contains a 3-cycle, a contradiction. Hence

\[ x_3 = (1 \, 3)(2 \, 4)(5 \, 6)(9 \, 10) \quad \text{implying} \quad x_1x_3 = (1 \, 4)(2 \, 3)(7 \, 8)(9 \, 10). \]

Let \(x_4\) be the unique element containing \((1 \, 3)(2 \, 4)\). As above \(x_3\) and \(x_4\) commute so by lemma 5.1 \(x_4\) contains two 2-cycles from \(\{5, 6, 9, 10\}\). Since \(x_3\) and \(x_4\) already agree on 2 points \(x_4\) contains \((5 : 9)(6 : 10)\) or \((5 : 10)(6 : 9)\). These are equivalent up to isomorphism so we assume \(x_4\) contains the first. Now \(x_4\) contains a 2-cycle from \(\{7, 8, 11\}\). If this 2-cycle contains 11 then \(x_1x_4\) contains a 4-cycle and a 3-cycle, a contradiction. Thus

\[ x_4 = (1 \, 3)(5 \, 9)(6 \, 10)(7 \, 8) \quad \text{implying} \quad x_3x_4 = (2 \, 4)(5 \, 10)(6 \, 9)(7 \, 8), \]

\[ x_4x_2x_4^{-1} = (2 \, 3)(5 \, 6)(7 \, 10)(8 \, 9) \quad \text{and} \quad x_4x_1x_2x_4^{-1} = (1 \, 4)(5 \, 6)(7 \, 9)(8 \, 10). \]

Let \(x_5\) be the unique element containing \((7 \, 8)(9 \, 11)\). By the lemma the fixed points are \(\{1, 2, 10\}, \{3, 4, 10\}\) or \(\{5, 6, 10\}\). Now all permutations having a
2-cycles in \{1, 2, 3, 4\} are already present so by the lemma there are only four cases for \(x_5\) namely:

\[(1\ 5)(2\ 6)(7\ 8)(9\ 11),\quad (1\ 6)(2\ 5)(7\ 8)(9\ 11),\]
\[(3\ 5)(4\ 6)(7\ 8)(9\ 11)\quad \text{and}\quad (3\ 6)(4\ 6)(7\ 8)(9\ 11)\]

Case one and three multiplied by \(x_4\) yields a 4-cycle and a 3-cycle. Contradiction. Further if \(g = (1\ 3)(2\ 4)(7\ 8)\) then \(\langle x_1, x_2, x_3, x_4, x_5 \rangle^g = \langle x_1, x_1 x_2, x_3, x_4 \rangle = \langle x_1, x_2, x_3, x_4 \rangle\) so case two and four are equivalent under isomorphism so we can assume that

\[x_5 = (1\ 6)(2\ 5)(7\ 8)(9\ 11)\].

We have now shown that \(\langle x_1, x_2, x_3, x_4, x_5 \rangle \leq M_{11}\) is unique up to isomorphism. Finally we want to show equality. The idea is to use Lagrange theorem to push up the order. We find the elements:

\[y_1 = x_5 x_2 x_3 = (1 3 5 7 2 4 6 8)(9 11)\]
\[y_2 = x_1 x_2 x_4 x_5 = (1 9 11 8 5 2 10 7 6 4 3)\]
\[y_3 = x_2 x_4 x_5 = (1 9 11 7 5)(2 10 8 6 3)\]
\[a_1 = x_4 x_2 x_1 = (1 3 4)(5 7 10)(6 8 9)\]
\[s = x_5 x_4 x_5^{-1} = (1 10)(2 11)(3 6)(7 8)\]
\[a_2 = s a_1 s^{-1} = (1 5 8)(3 7 9)(4 10 6)\].

Now \(o(y_1) = 8\), \(o(y_2) = 11\), \(o(y_3) = 5\) and \(|\langle a_1, a_2 \rangle| = 9\) yields

\[|\langle x_1, x_2, x_3, x_4, x_5 \rangle| \geq 11 \cdot 5 \cdot 9 \cdot 8 = \frac{|M_{11}|}{2}\]

As \(M_{11}\) is simple it cannot contain a subgroup of index two. Hence

\[M_{11} = \langle x_1, x_2, x_3, x_4, x_5 \rangle\].

\[\blacksquare\]

**Lemma 5.3.** Let \(G\) be a sharply doubly transitive group of degree nine. Then \(G = H \rtimes G_a\) where \(H \cong \mathbb{Z}_3 \times \mathbb{Z}_3\). Further \(G_a\) acts transitively on \(H \setminus \{1\}\) by conjugation.
Proof. Suppose $G$ is acting on $\{1, 2, \ldots, 9\}$ and let $g \in G$ be an element of order three. Let $X_i = \{g \in G | g(1) = i\}$. Then $G = X_1 \cup \cdots \cup X_9$. Since $G$ is sharply doubly transitive $|X_i| = 8$ for $i = 1, \ldots, 9$. For all $i \neq 1$ the seven isotropy subgroups not fixing 1 and $i$ is transitive and each containing an element in $X_i$. Because of the doubly transitivity we can conjugate $g$ with some $\alpha_i$ such that $g^{\alpha_i} \in X_i$. Hence there are exactly eight element of order three and none of order nine. These eight element together with the identity form a normal Sylow 3-subgroup $H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Finally pick two nonidentity elements $k \in G_\alpha$ and $h \in H$ and assume $h^k = h \iff hk = kh$. Suppose $h(a) = b$. Then $k(b) = kh(a) = hk(a) = h(a) = b$, a contradiction since $k$ cannot fix two points. Hence $G_\alpha$ acts transitively on $H$ by conjugation.

Theorem 5.4. The Mathieu group $M_{12}$ is unique up to isomorphism.

Method of Proof. Let $H$ be the sharply 4-fold transitive group constructed above and embed it in $S_{12}$. Further let $G < S_{12}$ be an arbitrary sharply 5-fold transitive group such that $G_{12} = H$. We will show that there exist an unique element $\sigma \in G \setminus H$ having five special properties. Moreover we will see that $\sigma$ do not depend on the choice of $G$. Finally as $H$ is maximal in $G$ it follows that $H \langle \sigma \rangle = G$. The uniqueness of $G$ now follows from the uniqueness of $H$ and $\sigma$.

Proof. From above we have $H = \langle x_1, x_2, x_3, x_4, x_5 \rangle$ where

$$
\begin{align*}
x_1 &= (1 2)(3 4)(5 6)(7 8) \\
x_2 &= (1 2)(5 7)(6 8)(9 10) \\
x_3 &= (1 3)(2 4)(5 6)(9 10) \\
x_4 &= (1 3)(5 9)(6 10)(7 8) \\
x_5 &= (1 6)(2 5)(7 8)(9 11)
\end{align*}
$$

Since $|H| = 11 \cdot 10 \cdot 9 \cdot 8$ and $|G| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ we see that the Sylow 3-subgroups in $H$ and $G$ have order 9 and 27 respectively. Our aim is to find $\sigma$ in a Sylow 3-subgroup. Let $A = \langle a_1, a_2 \rangle$ be the subgroup of order nine in Theorem 5.2. Clearly $A < H_{2, 11}$.

Next we want to show that there is an element $\sigma \in G$ satisfying properties (1)-(5):

66
Let $P$ be a Sylow 3-subgroup of $G$ such that $A < P$. If we consider the orbits of the point 10 we get

$$A(1) = \{1, 3, 4, 5, 6, 7, 8, 9, 10\} \subseteq P(1) \subseteq \{1, 2, \ldots, 12\} \implies 9 \leq |P(10)| \leq 12.$$  

But $|P(10)| = |P : P_{10}| |P| = 27$ so $|P(10)| = 9$. Thus $|P_{10}| = 3$ and we can find $\sigma$, $o(\sigma) = 3$, such that $P_{10} = \langle \sigma \rangle$. It is clear that $\sigma$ satisfies properties (2) and (3) above. Since no nonidentity element in $A$ fixes the point 10 we have $|\langle \sigma \rangle \cap A| = 1$ and $|A\langle \sigma \rangle| = |P|$. Hence $P = A\langle \sigma \rangle$. If $\sigma(12) = 12$ this implies that $P \leq H$, a contradiction since $|P| \nmid |H|$. So $\sigma$ satisfies property (1) above. Next we want to investigate $Z(P)$. Since $P$ is a 3-group we know that $|Z(P)| = 3, 9$ or 27. Assume the latter, i.e $P$ is abelian. Then $\forall i \in A(1)$ we can find $a \in A$ such that $a(10) = i$. Hence $\forall i \in A(1)$ we have

$$\sigma i = \sigma a(10) = a\sigma(10) = a(10) = i.$$  

A contradiction since the only element in $G$ fixing five points is the identity. Hence $P$ is non abelian. If $|Z(P)| = 9$ then $P/Z(P)$ is cyclic, implying $P$ is abelian. Contradiction. Thus $|Z(P)| = 3$. Suppose $|Z(P) \cap A| = 1$. Then since $|AZ(P)| = |P|$ and both $A$ and $Z(P)$ are normal subgroups we get $P \cong A \times Z(P)$, i.e again abelian. Contradiction. Thus $Z(P) < A$ and $Z(P) = \langle a \rangle$ for some $a \in A$. By Lemma 5.3, the group $H_{2,11,10}$ acting transitively on $A$ by conjugation and fixing $A$ as a set. So we can find $h \in H_{2,11,10}$ such that $hah^{-1} = a_1$. We set

$$\bar{P} = P^h, \quad \bar{\sigma} = h\sigma h^{-1}.$$  

Now $Z(\bar{P}) = Z(P)^h = \langle hah^{-1} \rangle = \langle a_1 \rangle$. Clearly $o(\bar{\sigma}) = 3$, $\bar{\sigma}(10) = 10$ and $\bar{\sigma}(12) \neq 12$. Further the same arguments that implied $P = A\langle a \rangle$ yields $\bar{P} = A\langle \bar{a} \rangle$. Hence $\bar{\sigma}$ also satisfy properties (1), (2) and (3) above. So if we swap the names $P, \sigma$ and $\bar{P}, \bar{\sigma}$ we have achieved

$$Z(P) = \langle a_1 \rangle.$$  

67
Since $a_1 \in Z(P)$ we have $a_1 \sigma = \sigma a_1$ and $\sigma$ satisfies property (4). To obtain property (5) consider the commutator subgroup of $P$. As $P$ is non abelian we have $[P,P] \neq \{1\}$. Further $P/Z(P)$ is abelian (prime square order) yields $[P,P] \leq Z(P)$. Thus $[P,P] = Z(P)$. In particular

$$[\sigma, a_2] = 1, a_1 \text{ or } a_1^2$$

If $[\sigma, a_2] = 1$ then $\sigma, a_1$ and $a_2$ all would commute. As $P = A(\sigma)$ this yields that $P$ is abelian. Contradiction. Thus $[\sigma, a_2] = a_1$ or $[\sigma, a_2] = a_1^2$. Now $\sigma^{-1}$ also satisfies properties (1)-(4), so by replacing $\sigma$ with $\sigma^{-1}$ if necessary we might assume

$$[\sigma, a_2] = a_1 \iff \sigma a_2 = a_1 a_2 \sigma$$

Let property (5). Knowing that $\sigma$ satisfies properties (1)-(5) we now explicit find the action on each point in $\{1, \ldots, 12\}$.

\[
\begin{align*}
\sigma(5) &= \sigma a_1(10) = a_1 \sigma(10) = a_1(10) = 5 \\
\sigma(7) &= \sigma a_1(5) = a_1 \sigma(5) = a_1(5) = 7 \\
\sigma(6) &= \sigma a_2(10) = a_1 a_2 \sigma(10) = a_1 a_2(10) = a_1(6) = 8 \\
\sigma(8) &= \sigma a_1(6) = a_1 \sigma(6) = a_1(8) = 9 \\
\sigma(9) &= \sigma a_1(8) = a_1 \sigma(8) = a_1(9) = 6 \\
\sigma(1) &= \sigma a_2(8) = a_1 a_2 \sigma(8) = a_1 a_2(9) = a_1(3) = 4 \\
\sigma(3) &= \sigma a_1(1) = a_1 \sigma(1) = a_1(4) = 1 \\
\sigma(4) &= \sigma a_1(3) = a_1 \sigma(3) = a_1(1) = 3
\end{align*}
\]

It remains to find the action on $\{2, 11, 12\}$. Since $\sigma$ already fixes three points $\{2, 11, 12\}$ is in a three cycle. Hence

$$\sigma = (1\ 4\ 3)(6\ 8\ 9)(2\ 11\ 12) \quad \text{or} \quad \sigma = (1\ 4\ 3)(6\ 8\ 9)(2\ 12\ 11)$$

Consider the second case. Then since $H < G$ is a maximal subgroup $H(\sigma) = G$. But the element

$$x_5 x_3 \sigma = (1\ 5)(2\ 9)(4\ 6\ 7\ 8\ 10\ 11\ 12)$$

has order $14 \nmid |G|$. Contradiction. Thus $\sigma = (1\ 4\ 3)(6\ 8\ 9)(2\ 11\ 12)$ is the only possibility. \hfill \blacksquare
A. GAP and permutation groups

GAP (Groups, Algorithms, Programming) is a system for computational discrete algebra. It is free and can be found at [http://www.gap-system.org](http://www.gap-system.org). GAP is a very good tool for tedious calculations. Even if it is a computer program the outcome often is verifiable by hand. The web page contains a detailed manual, but to get started here is short list of for this thesis useful commands.

```gap
gap> x:=(1,2)(3,4,5);
Defines the permutation $x = (1\ 2)(3\ 4\ 5)$. All permutations in GAP acts on a set of positive integers.

gap> S:=[1,2,5];
Formally this defines a list, but if the numbers are written in ascending order we can see this as the definition $S = \{1, 2, 5\}$.

gap> OnPoints(5,x);
Determine $x(5)$.

gap> OnSets(S,x);
Assuming $S$ is an ordered list this command returns the image of $S$ under $x$ as an ordered list.

gap> G:=Group(x,y,z);
Defines the Group $G = \langle x, y, z \rangle$.

gap> MathieuGroup(24);
Returns $M_{24}$ with the same generators used in thesis thesis. The non infinity elements $x \in \Omega$ are relabeled as $x + 1$ and $\infty$ as 24.
```
gap> Order(G);
Determine the order of the group $G$.

gap> x in S;
If $S$ is any set this command returns true if $x \in S$ and false otherwise.

gap> S:=Filter(T,x->P(x));
Defines $S$ as the set of elements in $T$ satisfying $P$, where $P$ is a predicate on $T$.

**Example A.1.** Suppose we want to find $\sigma$ in the Octern group. We look for an involution in $M_{24}$ having the action $(1\ 2)(3\ 8)(4\ 5)(6\ 7)$ on the columns in

\[
\begin{array}{cccccccc}
\infty & 14 & 3 & 15 & 20 & 0 & 8 & 18 \\
17 & 16 & 10 & 7 & 4 & 13 & 2 & 11 \\
22 & 9 & 6 & 19 & 12 & 21 & 5 & 1
\end{array}
\]

Since GAP is relatively slow we start by filtering out all involutions.

gap> I:=Filtered(MathieuGroup(24),x->x*x=());

```gap
gap> P:=function(x)
> if OnSets([18,23,24],x)=[10,15,17] and
> OnSets([4,7,11],x)=[2,12,19] and
> OnSets([8,16,20],x)=[5,13,21] and
> OnSets([1,14,22],x)=[3,6,9] then
> return true;
> else
> return false;
> fi;
> end;;
gap> Filtered(I,x->P(x));
[ (1,3)(2,7)(4,19)(5,20)(6,14)(8,21)(9,22)(10,18)(11,12)
(13,16)(15,24)(17,23) ]
```

**Remark A.2.** It is worth noting that GAP, unlike us, uses left to right multiplication. To show that this is irrelevant let $\cdot$ denote left to right
multiplication and $\ast$ right to left multiplication. Let $G$ be the set of all permutations in the group GAP calculated on. Then $\varphi : (G, \cdot) \rightarrow (G, \ast)$ defined by $\varphi(x) = x^{-1}$ is obviously a bijection. Further

$$\varphi(x \cdot y) = (x \cdot y)^{-1} = (y \ast x)^{-1} = x^{-1} \ast y^{-1} = \varphi(x) \ast \varphi(y).$$

So $\varphi$ is an isomorphism.
Bibliography


