Imperial College London

Doctoral Thesis

Majorana Representations and the Coxeter Groups $G^{(m,n,p)}$

Sophie C. E. Decelle

A thesis submitted in fulfilment of the requirements
for the degree of Doctor of Philosophy

under the supervision of

Prof. Alexander A. Ivanov

in the

Algebra and Algebraic Combinatorics Group
Department of Mathematics

February 2014

Declaration of Authorship

I, Sophie C. E Decelle, declare that the work presented in this thesis is my own except that which is referenced.

Copyright Declaration

The copyright of this thesis rests with the author and is made available under a Creative Commons Attribution Non-Commercial No Derivatives licence. Researchers are free to copy, distribute or transmit the thesis on the condition that they attribute it, that they do not use it for commercial purposes and that they do not alter, transform or build upon it. For any reuse or redistribution, researchers must make clear to others the licence terms of this work.

La Nature est un temple où de vivants piliers
Laissent parfois sortir de confuses paroles;
L'homme y passe à travers des forêts de symboles
Qui l'observent avec des regards familiers.

Charles Baudelaire, 1857
Extract from the poem 'Correspondances'

Nature is a temple in which living pillars
Sometimes give voice to confused words;
Man passes there through forests of symbols
Which look at him with understanding eyes.

Translation from William Aggeler, 1954

IMPERIAL COLLEGE LONDON

Abstract

Majorana Representations and the Coxeter Groups $G^{(m,n,p)}$

by Sophie C. E. Decelle

The work presented in this thesis is a contribution to Majorana theory as introduced by A. A. Ivanov in [Iva09]. Inspired by a theorem of S. Sakuma [Sak07], Majorana theory is an axiomatisation of seven properties of the Monster algebra $V_{\mathbb{M}}$, invariant under the Monster group $\mathbb{M}$, and of some of its idempotents. For a finite group G generated by a G-invariant set T of involutions one can define what it means for G to have a *Majorana representation* with respect to T. It yields a G-invariant *Majorana algebra* X generated by a set A of idempotents called *Majorana axes*. To each axis a in A an automorphism $\tau(a)$ of X called *Majorana involution* is associated, so that $X,\ A$ and $\tau(A)$ satisfy the Majorana axioms. In this thesis we give a review of the Majorana algebras already obtained and we motivate the following objective: the classification of all Majorana algebras V generated by three Majorana axes $a_1,\ a_2$ and a_3 such that V also contains a Majorana axis $a_{1,2}$ with associated automorphism $\tau(a_{1,2}) = \tau(a_1)\tau(a_2)$. This objective requires the classification of all subgroups $G = \langle \tau(a_i) \mid i \in [1,3] \rangle$ of $GL(V)$, which are necessarily quotients of the Coxeter groups $G^{(m,n,p)} := \langle x, y, z \mid x^2,\ y^2,\ z^2,\ (xy)^2,\ (xz)^m,\ (yz)^n,\ (xyz)^p \rangle$ such that $m,\ n,\ p \in [1,6]$ and the set of conjugates of $x,\ y,\ xy$ and z is 6-transposition. We prove that all such groups are quotients of only eleven finite groups. Comparing with S. P. Norton's list of 'triangle-point' configurations of $2A$ involutions in $\mathbb{M}$ [Nor85], we observe that nine of them *2A-embed* in $\mathbb{M}$. The next step is to answer which of those eleven groups can be generated by Majorana involutions. Using partial results already known, we manage to answer this question completely for one of the eleven groups isomorphic to $L_2(11)$. For the remaining ten groups we give technical restrictions on the structure of their possible Majorana algebras, thus laying the foundations for further progress.

Acknowledgements

I would like to thank my supervisor, Prof. Alexander A. Ivanov, for introducing me to the Monster algebra and Majorana representations and for his patience and genuine enthusiasm during all our meetings which led to this thesis. On a more personal note, I thank Sasha for taking me on this mathematical journey and for sharing with me his views on life and human nature.

I gratefully acknowledge the EPSRC for financially supporting my research, and the Mathematics department of Imperial college for providing an agreeable atmosphere in which to work and socialise. My thanks also go to some of the administrators of the department and to the ICT for their unfaltering helpfulness.

I thank Matthew for his patient support and advice. To a great bunch of fellow Maths PhD students, some now doctors: Cristina, Florencia, Lisa, Matthew R. and Senja, I say: well-done and carry on. I thank Pauline, Nathan, Jeremy and Daniel for their generosity. Last but not least a thankful thought goes to my parents for supporting me and not asking too many questions.

Sophie Decelle,

July 2013

Contents

Declaration of Authorship 2

Copyright Declaration 3

Abstract 5

Acknowledgements 6

List of Tables 10

Notations 11

1 Preliminaries 13
- 1.1 Introduction . . . 13
- 1.2 Notes on Chapter 3 . . . 18
  - 1.2.1 Frobenius groups . . . 18
  - 1.2.2 Frobenius reciprocity . . . 19
  - 1.2.3 Structure class constants and p-powers . . . 20
    - Structure constants . . . 21
    - p-powers of conjugacy classes . . . 21
- 1.3 Notes on Chapter 4 . . . 21
  - Group theoretic results . . . 21
  - The use of Magma . . . 22

2 Majorana representations 24
- 2.1 Introduction to the Monster algebra $V_{\mathbb{M}}$ . . . 24
  - 2.1.1 The dihedral subalgebras of $V_{\mathbb{M}}$ generated by pairs of $2A$-axes . . . 25
  - 2.1.2 Partial associativity in $V_{\mathbb{M}}$ . . . 28
- 2.2 Axioms of Majorana theory and Majorana calculus . . . 30
- 2.3 Internal Majorana representations and Sakuma's Theorem . . . 33
  - Proof of Sakuma's Theorem . . . 34
  - Vectors invariant under cyclic groups in dihedral Majorana algebras 37
  - Inclusions between dihedral Majorana algebras . . . 37
- 2.4 Majorana representations . . . 37
  - 2.4.1 Definition . . . 38

2.4.2 Dimension and shape . . . 39
2.4.3 The known Majorana representations . . . 41
2.4.4 Eigenvectors . . . 43
2.4.5 Tri-generated Majorana Algebras . . . 45

3 The 6-transposition Coxeter groups $G^{(m,n,p)}$ 49
3.1 Motivation and Main Theorem . . . 49
3.1.1 Tri-generated Majorana algebras and property (σ) . . . 49
3.1.2 Main theorem . . . 50
3.1.3 The tri-generated $2A$ subgroups of $\mathbb{M}$ . . . 52
3.2 The 6-transposition quotients of the $G^{(m,n,p)}$ groups . . . 55
3.2.1 Introduction . . . 55
3.2.2 The finite 6-transposition $G^{(m,n,p)}$ groups . . . 56
3.2.3 The infinite 6-transposition quotients of the $G^{(m,n,p)}$ groups for $(m,n,p) \neq (6,\ 6,\ 6)$ . . . 60
3.3 The 6-transposition quotients of the group $G^{(6,6,6)}$ . . . 71
3.3.1 Introduction and main result . . . 71
3.3.2 The largest 6-transposition quotient of $G^{(6,6,6;\ 5,5,5)}$ . . . 76
On a quotient of $G^{(6,6,6:\ 5,5,5)}$ isomorphic to $2^5 : S_5$ . . . 77
Lifting Ω_H to Q . . . 79
3.3.3 The largest 6-transposition quotient of $G^{(6,6,6;\ 6,6,6)}$ . . . 83
3.3.4 Two remarks on Burnside groups . . . 87
3.4 Shapes of the Majorana representations . . . 89

4 The $L_2(11)$-subalgebra of the Monster algebra $V_{\mathbb{M}}$ 92
4.1 Motivation and Main result . . . 92
4.2 Properties and subgroup structure of $L_2(11)$ . . . 93
4.3 The $L_2(11)$ subalgebra of $V_{\mathbb{M}}$ . . . 95
4.3.1 S. P. Norton's observations . . . 95
4.4 Inner products . . . 100
4.4.1 Dihedral subalgebras of V and spanning set . . . 101
Dihedral subalgebras . . . 101
Spanning set . . . 101
4.4.2 A_5 subalgebras of V . . . 102
4.4.3 Inner product values . . . 105
4.4.3.1 Inner products of type $(2,2)$ . . . 105
4.4.3.2 Inner products of type $(2,3)$ . . . 106
4.4.3.3 Inner products of type $(2,5)$ . . . 107
4.4.3.4 Inner products of type $(3,3)$ . . . 108
4.4.3.5 Inner products of type $(3,5)$ . . . 109
4.4.3.6 Inner products of type $(5,5)$ . . . 111
4.4.4 Dependence relations in the algebra . . . 112
4.5 The Majorana representation of $L_2(11)$ . . . 114

Bibliography 116

A Magma functions **119**
A.1 The function 'Triangle' . . . 119
A.2 The semidirect product $G_{11} \cong (3^4 : 2) : (3_+^{1+2} : 2^2)$ . . . 120

B Appendix B **123**
B.1 Shapes for the representations $\mathcal{R}_1$ of G_1 . . . 123
B.2 Shapes for the representations $\mathcal{R}_2$ of G_2 . . . 125
B.3 Shapes for the representations $\mathcal{R}_3$ of G_3 . . . 127
B.4 Shapes for the representations $\mathcal{R}_4$ of G_4 . . . 128
B.5 Shapes for the representations $\mathcal{R}_6$ of G_6 . . . 130
B.6 Shapes for the representations $\mathcal{R}_7$ of G_7 . . . 132
B.7 Shapes for the representations $\mathcal{R}_8$ of G_8 . . . 134
B.8 Shapes for the representations $\mathcal{R}_{10}$ of G_{10} . . . 135
Fusion of G_{10} in $\mathbb{M}$ . . . 137

List of Tables

1.1 The groups G . . . 16
1.2 The groups G as quotients of $G^{(m,n,p)}$ groups . . . 17

2.1 Dihedral subalgebras of $V_{\mathbb{M}}$ generated by two $2A$-axes . . . 27
2.2 The Fusion rules . . . 32
2.3 Majorana representations of dihedral groups . . . 36
2.4 Known Majorana representations . . . 43
2.5 Eigenvectors of Majorana axis a . . . 45

3.1 The groups satisfying $(\boldsymbol{\sigma})$ . . . 51
3.2 The $G^{(m,n,p)}$ quotients embedding in $\mathbb{M}$ with $a,\ b,\ ab,\ c \in 2A$ . . . 54
3.3 Orders of the finite $G^{(m,n,p)}$ groups satisfying $(\boldsymbol{\sigma})$ . . . 56
3.4 The finite non-abelian and non-dihedral $G^{(m,n,p)}$ groups . . . 57
3.5 The $G^{(m,n,p;\ r_1)}$ groups for $(m,n,p) \in \mathcal{F}$ and $r_1 \in [1,6]$ . . . 62
3.6 The largest quotients of $G^{(6,6,6)}$ satisfying $(\boldsymbol{\sigma})$ . . . 71
3.7 Number of shapes of the Majorana representations of the groups satisfying $(\boldsymbol{\sigma})$ . . . 90

4.1 Fusion of K in $\mathbb{M}$ . . . 97
4.2 Fusion of A in $\mathbb{M}$ . . . 97
4.3 Inner Products of type $(2,2)$, with $t, s \in G^{(2)}$ . . . 105
4.4 Inner Products of type $(2,3)$, with $t \in G^{(2)}$ and $h \in G^{(3)}$ . . . 106
4.5 Inner Products of type $(2,5)$, with $t \in G^{(2)}$ and $f \in G^{(5)}$ . . . 107
4.6 Inner Products of type $(3,3)$, with $h, k \in G^{(3)}$ . . . 108
4.7 Inner Products of type $(3,5)$, with $h \in G^{(3)}$ and $f \in G^{(5)}$ . . . 109
4.8 Inner Products of type $(5,5)$, with $f, g \in G^{(5)}$ . . . 111

Notations

$\mathbb{M}$	the Monster simple group
$V_{\mathbb{M}}$	the Monster algebra
$\mathbb{Z}_p$	the ring of integers modulo p where p is a prime number
$\mathbb{Z}_p^*$	the multiplicative group $\mathbb{Z}_p \setminus \{0\}$
C_m	the cyclic group of order m
m^n	the elementary abelian group of order m^n
D_{2n}	the dihedral group of order $2n$
A_n	the alternating group of degree n
S_n	the symmetric group of degree n
$L_n(p^k)$	the projective special linear group of dimension n
	over the finite field of order p^k and characteristic p
$GL(V)$	the general linear group of a vector space V

For a group G:

$\|G\|$	the order of G
$Z(G)$	the centre of G
$\langle g \rangle$	the subgroup of G generated by $g \in G$
$N_G(H)$	the normaliser in G of a subgroup $H \subset G$
$C_G(g)$	the centraliser in G of $g \in G$
g^G	the conjugacy class in G of $g \in G$

For two groups G and H:

$G \times H$	the direct product of G and H
$G : H$	a semidirect product of G and H
$G\ wr\ H$	the wreath product of G and H

To friendships, old and new

Chapter 1

Preliminaries

1.1 Introduction

In this section we explain the content of this thesis. The remainder of this chapter contains background material for Chapters 3 and 4.

We first introduce the Monster algebra in Chapter 2 which was first constructed by R. L. Griess in his monumental paper [Gri82]. We denote by $\mathbb{M}$ the Monster simple group and we let $V_{\mathbb{M}}$ be the Monster algebra, a commutative non-associative algebra of dimension $196,884$ over $\mathbb{R}$ with identity $\iota_{\mathbb{M}}$ and automorphism group $\mathbb{M}$, as described by J. H. Conway in [Con85]. The group $\mathbb{M}$ has two conjugacy classes of involutions which we call $2A$ and $2B$ where $2A$ is the smallest of the two classes. It is known that $\mathbb{M}$ is a 6-transposition group in the sense that it is generated by its $2A$ involutions which are 6-transpositions; the product of any two has order at most 6 and belongs to either of the nine $\mathbb{M}$ conjugacy classes: $1A, 2A, 2B, 3A, 3C, 4A, 4B, 5A, 6A$.

For a long time it has been desirable to describe the subalgebra structure of $V_{\mathbb{M}}$. The $2A$ involutions of $\mathbb{M}$ play an important part in that description. From [Con85] there exists a bijection, which we name *Conway's bijection* $\mathcal{C}$, sending each $2A$ involution t to a unique non-trivial idempotent $a_t := \mathcal{C}(t)$ of $V_{\mathbb{M}} \backslash \{0\}$ called a *2A-axis*. For a set A of $2A$-axes of $V_{\mathbb{M}}$ we denote by $\langle\langle A \rangle\rangle$ the subalgebra of $V_{\mathbb{M}}$ generated by A. In [Con85] J. H. Conway describes, with the help of S. P. Norton, all the *dihedral* subalgebras $\langle\langle a_t, a_s \rangle\rangle$ of $V_{\mathbb{M}}$ for two $2A$ involutions t and s. There are nine distinct isomorphism types of subalgebras $\langle\langle a_t, a_s \rangle\rangle$ each uniquely determined by the

conjugacy class of the product ts.

Within the framework of Vertex Operator Algebras (VOAs) the Monster group $\mathbb{M}$ can be realised as the automorphism group of the Moonshine VOA as constructed in [FLM88] and [Miy04]. In [Sak07] S. Sakuma accomplishes the characterisation of the dihedral subalgebras of $V_{\mathbb{M}}$ as subalgebras U generated by two Ising vectors in the Griess algebra of a VOA. To do so he follows M. Miyamoto by associating to each Ising vector u of U a *Miyamoto involution* $\tau(u)$ which is an involutory automorphism of U, and shows that the product of any two Miyamoto involutions has order at most 6.

Inspired by the work of S. Sakuma, A. A. Ivanov introduced Majorana theory in his book [Iva09]. Majorana theory is an axiomatisation of seven of the properties of $V_{\mathbb{M}}$ and its $2A$-axes. The Majorana axioms are denoted (M1) to (M7) and can be read in Chapter 2, section 2.2. They define for a real commutative non-associative algebra V with a well-defined symmetric bilinear form $(\ ,\ )$ a set A of non-trivial idempotents of $V\backslash\{0\}$ called *Majorana axes*. To each Majorana axis $a \in A$ A. A. Ivanov associates an involutory automorphism $\tau(a)$ of V called a *Majorana involution*. An algebra V generated by a set of Majorana axes and which satisfies all the Majorana axioms is called a *Majorana algebra*. In [IPSS10] A. A. Ivanov *et al* prove a result which they refer to as 'Sakuma's Theorem' (Theorem 2.14); a Majorana algebra generated by two Majorana axes a_1 and a_2 is isomorphic to one of the dihedral subalgebras of $V_{\mathbb{M}}$. In particular they show that the product of the two Majorana involutions $\tau(a_1)$ and $\tau(a_2)$ has order no greater than 6.

One of the main goals of Majorana theory is to describe subalgebras of $V_{\mathbb{M}}$ in a more transparent way than in [Sak07] and [Con85]. Majorana theory is outside of the VOA framework and does not rely on the need to calculate with Leech vectors. However, the Majorana axioms may not necessarily define subalgebras of $V_{\mathbb{M}}$ but in fact one of the motivations behind Majorana theory is also to describe a class of subalgebras independently of $\mathbb{M}$.

The main objective of this thesis is to contribute to the classification of Majorana algebras V generated by three Majorana axes a_1, a_2 and a_3 such that V also contains a Majorana axis $a_{1,2}$ with associated Majorana involution $\tau(a_{1,2}) := \tau(a_1)\tau(a_2)$, and determine which of those algebras are subalgebras of $V_{\mathbb{M}}$. To achieve this classification one first needs to find all possible

groups G generated by the involutions $\tau(a_1)$, $\tau(a_2)$ and $\tau(a_3)$ where $\tau(a_1)$ and $\tau(a_2)$ commute. An important motivation is to observe how close the Majorana axioms bring the list of the possible groups G to S. P. Norton's list in [Nor85] of subgroups of $\mathbb{M}$ generated by a triple of $2A$ involutions two of which commute such that their product is also in class $2A$. We say that a group generated by three involutions x, y, z, two of which commute $xy = yx$, *2A-embeds* in $\mathbb{M}$ if it embeds in $\mathbb{M}$ such that the involutions x, y, z and xy are mapped to $2A$ involutions. We now present the results of this thesis into one Main Theorem.

Main Theorem. *Let V be a Majorana algebra generated by three Majorana axes a_1, a_2 and a_3 such that V also contains a Majorana axis $a_{1,2}$ with associated Majorana involution $\tau(a_{1,2}) := \tau(a_1)\tau(a_2)$. Let G be the subgroup $\langle \tau(a_1), \tau(a_2), \tau(a_3) \rangle$ of $GL(V)$. Then the following hold:*

1) *G is finite and is a quotient of at least one of the eleven groups G_i, $i \in [1, 11]$, from Table 1.1 below;*

2) *for all eleven groups the possible shapes for the algebra V are as given in Chapter 3, section 3.4;*

3) *for $G_5 \cong L_2(11)$ the algebra V is **based on an embedding into** $\mathbb{M}$ (in the sense of Definition 2.21) so that V is isomorphic to a subalgebra of $V_{\mathbb{M}}$ which is described in Chapter 4.*

Name	Isomorphism Type	$2A$-embeds in $\mathbb{M}$	Largest $2A$-embedded quotient	Centre Order	Subgroups
G_1	$2\ wr\ 2^2$	Y		2	
G_2	$(S_3 \times S_3) : 2^2$	Y		2	
G_3	$2^4 : D_{10}$	Y		1	
G_4	$2 \times S_5$	Y		2	
G_5	$L_2(11)$	Y		1	
G_6	$(2^4 :_{\phi_1} D_{12}) \times 2$	Y		2	
G_7	$2^4 :_{\lambda_2} A_5$	Y		1	G_3
G_8	$2 \times S_6$	Y		2	$G_2,\ G_4$
G_9	$\big(2^4 : (S_3 \times S_3)\big) \times 2$	N	$2^4 : (S_3 \times S_3)$	2	
G_{10}	$2^5 :_{\phi} S_5$	Y		2	$G_3,\ G_4,\ G_6$
G_{11}	$(3^4 : 2) : (3_+^{1+2} : 2^2)$	N	$3_+^{1+2} : 2^2$	1	

TABLE 1.1: The groups G

The result in part 1) of the Main Theorem is proved in Chapter 3 using purely group theoretic arguments. Indeed, to find all groups $\langle \tau(a_1), \tau(a_2), \tau(a_3) \rangle$ we can classify all groups satisfying the following property:

Property $(\boldsymbol{\sigma})$. *A group G has property $(\boldsymbol{\sigma})$ if it satisfies each of the following two conditions:*

(i) *G is generated by three elements $a,\ b,\ c$ of order dividing 2, two of which commute, say $ab = ba$;*

(ii) *for any two elements $t,\ s$ in $T := a^G \cup b^G \cup (ab)^G \cup c^G$ the product ts has order at most 6.*

All the groups having property $(\boldsymbol{\sigma})$ are necessarily quotients of the Coxeter groups $G^{(m,n,p)} := \langle x, y, z \mid x^2,\ y^2,\ z^2,\ (xy)^2,\ (xz)^m,\ (yz)^n,\ (xyz)^p \rangle$ for $m,\ n,\ p \in [1, 6]$ and such that the conjugates of $x,\ y,\ z$ and xy are 6-transpositions. The exact result proved in Chapter 3 is the following.

Theorem. *A group has property $(\boldsymbol{\sigma})$ if and only if it is a quotient of at least one of the eleven groups in Table 1.1 which are quotients of the $G^{(m,n,p)}$ groups given in Table 1.2.*

Name	Isomorphism Type	Quotient of $G^{(m,n,p)}$ for (m,n,p) equal to	Number of Added Relations
G_1	$2\ wr\ 2^2$	$(4,4,4)$	0
G_2	$(S_3 \times S_3) : 2^2$	$(4,4,6)$	0
G_3	$2^4 : D_{10}$	$(4,5,5)$	0
G_4	$2 \times S_5$	$(4,5,6)$	0
G_5	$L_2(11)$	$(5,5,5)$	0
G_6	$(2^4 :_{\phi_1} D_{12}) \times 2$	$(4,6,6)$	1
G_7	$2^4 :_{\lambda_2} A_5$	$(6,5,5)$	1
G_8	$2 \times S_6$	$(6,6,5)$	1
G_9	$\big(2^4 : (S_3 \times S_3)\big) \times 2$	$(6,6,6)$	1
G_{10}	$2^5 :_{\phi} S_5$	$(6,6,6)$	4
G_{11}	$(3^4 : 2) : (3^{1+2}_{+} : 2^2)$	$(6,6,6)$	4

TABLE 1.2: The groups G as quotients of $G^{(m,n,p)}$ groups

Part 2) of the Main Theorem is proved in the last section of Chapter 3 using *Majorana representations* of the eleven groups G_i for $i \in [1,11]$. The definition of a Majorana representation was introduced by A. A. Ivanov in [Iva09] and can be read in Definition 2.17 of Chapter 2. The definition is for a finite group generated by a union of conjugacy classes of involutions which act on a prescribed Majorana algebra. One obvious benefit of the definition is that it allows us to describe subalgebras of $V_{\mathbb{M}}$ from subgroups of $\mathbb{M}$ in which calculations are easier to perform than in the whole of $\mathbb{M}$. We will see that not all Majorana algebras are subalgebras of $V_{\mathbb{M}}$. Part of the definition of a Majorana representation for a finite group K generated by a K-invariant set of involutions T, is a map sending each involution $t \in T$ to a Majorana axis a_t such that the Majorana algebra X generated by the axes $\{a_t\}_{t\in T}$ is acted on by K via conjugation of the indices. The *shape*, Definition 2.23, of a Majorana representation of K gives the types of all the dihedral Majorana subalgebras of X. At the end of Chapter 3 we find all the possible shapes for the Majorana representations of the eleven groups G_i for $i \in [1,11]$ such that for each group, the set of involutions T, forming part of the definition of a Majorana representation, consists of

the conjugates of the generating involutions $a,\ b,\ c$ and of ab.

Finally, part 3) of the Main Theorem is a consequence of the main result of Chapter 4 describing all possible Majorana representations for the group $G_5 \cong L_2(11)$. The group $L_2(11)$ is generated by its unique class of involutions T of size 55 and from [Nor98] it $2A$-embeds in $\mathbb{M}$. We denote by L the corresponding $L_2(11)$ subgroup of $\mathbb{M}$ generated by $2A$ involutions.

Theorem. *Let V be a Majorana algebra associated with a Majorana representation of $L_2(11)$. Then V is generated by the set of 55 Majorana axes $\{a_t \mid t \in T\}$ and is isomorphic to a unique subalgebra of $V_{\mathbb{M}}$. Moreover, V satisfies:*

1) $dim(V) = 101$;

2) *V is linearly spanned by the set $\{a_t \cdot a_s \mid t,\ s\ \in T\}$;*

3) *if $K = C_{\mathbb{M}}(L)$ then $C_{V_{\mathbb{M}}}(K) \cong V \oplus \iota_{\mathbb{M}}$.*

In Chapter 4 we also give a basis for the Majorana algebra V of $L_2(11)$ for which we recover all the pairwise inner product values.

1.2 Notes on Chapter 3

1.2.1 Frobenius groups

In Chapter 3 we mention a subgroup F_{55} of the projective special linear group $L_2(11)$, where F_{55} is a Frobenius group of order 55.

Definition 1.1. A finite Frobenius group G is a group containing a non-trivial proper subgroup H such that $H \cap H^g = 1$ for all $g \in G \setminus H$.

In the language of permutation groups, Frobenius groups are a class of transitive permutation groups where only the identity fixes more than one point and the stabiliser of a point is non-trivial. The next two results on Frobenius groups are taken from p.140 and p.38 of [Gor68].

Theorem 1.2. *(Frobenius' Theorem) Let G be a Frobenius group acting on a set X and let H be a subgroup stabilising a point $x \in X$. Then the following subset K of G is a normal subgroup of G of order $[G : H]$:*

$$K := \left(G \setminus \bigcup_{g \in G} H^g\right) \cup \{1\}. \qquad \square$$

The subgroup K is called the Frobenius kernel of G and H is called the Frobenius complement. A consequence of Frobenius' Theorem is the following result.

Theorem 1.3. *Let G be a Frobenius group with kernel K and complement H. Then the following hold true:*

1) *G is the semidirect product of K by H;*

2) *$|H|$ divides $|K| - 1$;*

3) *Every element of $H \setminus \{1\}$ induces a conjugation automorphism of K which fixes only the identity element of K;*

4) *$C_G(k) \subseteq K$ for every $k \in K \setminus \{1\}$.* $\square$

A subclass of the Frobenius groups are the $F_{p,q}$ groups.

Definition 1.4. For two primes $p \neq q$ such that q divides $p - 1$, we let $F_{p,q}$ be the group of order pq with the following presentation: $F_{p,q} := \langle\ k,\ h \mid k^p,\ h^q,\ k^h(k^{-1})^u\ \rangle$, where u is an element of order q in $\mathbb{Z}_p*$.

The isomorphism type of $F_{p,q}$ does not depend on the choice of the integer u of order q since all such integers generate the group $\mathbb{Z}_p*$. From Sylow's theorems it can be deduced that the only non-abelian groups of order pq for two primes $p,\ q$ are the $F_{p,q}$ groups.

Proposition 1.5. *Let G be a non-abelian group of order pq where $p,\ q$ are two primes with $p \geq q$. Then q divides $p - 1$ and $G \cong F_{p,q}$.* $\square$

Example 1.6. *In Chapter 3, we denote by F_{55} the Frobenius group $F_{11,5} = K : H \cong C_{11} : C_5$ with Frobenius kernel $K := \langle k \rangle \cong C_{11}$ and Frobenius complement $H := \langle h \rangle \cong C_5$. The group H acts on K by sending $k \to k^u$ where $u \in \{3,\ 4,\ 5,\ 9\}$ is an element of order 5 in $\mathbb{Z}_{11}$. From Definition 1.4 the group F_{55} satisfies the presentation $\langle\ k,\ h \mid k^{11},\ h^5,\ k^h \cdot (k^{-1})^3\ \rangle$.*

1.2.2 Frobenius reciprocity

We let k be an arbitrary field, G be an arbitrary group and H be a subgroup of G. We denote by kG the group algebra of G over k and by $\mathbb{1}_G$ the trivial kG-module.
We let V be a kG-module and W be a kH-module and we denote by $V\downarrow_H$ the restriction of V

to H and by $W\uparrow^G$ the induced module $kG\otimes_{kH}W$. Lastly we denote by $\langle V, V'\rangle_{kG}$ the dimension of the Hom-space $Hom_{kG}(V, V')$ for two kG-modules V and V'.

Proposition 1.7. *Let $C_V(H)$ be the subspace of V fixed by H. Then $C_V(H)$ has dimension*

$$\langle V,\ \mathbb{1}_H\uparrow^G\rangle_{kG}. \qquad \square$$

Next we state a general form of Frobenius reciprocity (see [Wei03] for example).

Theorem 1.8. *(Frobenius reciprocity) Let $H \subseteq G$ be finite groups and k a field. For V a finite-dimensional kG-module, and W a finite-dimensional kH-module we have that*

$$\langle V, W\uparrow^G\rangle_{kG} = \langle V\downarrow_H, W\rangle_{kH}. \qquad \square$$

For the next result we assume the reader is familiar with elementary character theory. The computation of the dimensions $\langle V, W\uparrow^G\rangle_{kG}$ and $\langle V\downarrow_H, W\rangle_{kH}$ is possible using an inner product of group characters.

For the rest of this subsection we fix G a finite group and k a field with characteristic 0 or coprime to the order of G.

Definition 1.9. Let V and V' be two kG-modules with characters χ_V and $\chi_{V'}$ respectively. We define the inner product of characters as:

$$\langle \chi_V, \chi_{V'}\rangle_{kG} := \frac{1}{|G|}\sum_{g\in G}\chi_V(g)\overline{\chi_{V'}(g)}$$

As a corollary to Frobenius reciprocity we can now derive the next result.

Corollary 1.10. *Let $H \subseteq G$, let V be a kG-module with character χ_V and let W be a kH-module with character χ_W, then:*

$$\langle \chi_V, \chi_{W\uparrow^G}\rangle_{kG} = \langle \chi_{V\downarrow_H}, \chi_W\rangle_{kH}. \qquad \square.$$

Proposition 1.7 together with Corollary 1.10 gives $dim\big(C_V(H)\big) = \big\langle \chi_{V\downarrow_H},\ \mathbb{1}_H\big\rangle_{kH}$ which is often easier to calculate than $\langle \chi_V, \mathbb{1}_{H\uparrow^G}\rangle_{kG}$ and will be used in Chapter 2.

1.2.3 Structure class constants and p-powers

Throughout all the subsequent chapters we use structure class constants and p-powers to determine for a subgroup H of $\mathbb{M}$ the fusion of the conjugacy classes of H into those of $\mathbb{M}$.

Structure constants

Let G be a finite group and let C_1, C_2 and C_3 be conjugacy classes of G. For $g_3 \in C_3$, the number of pairs $(g_1, g_2) \in C_1 \times C_2$ such that $g_1 g_2 = g_3$ is equal to the structure class constant s_{C_1,C_2,C_3}. We let k be an arbitrary algebraically closed field and we denote by $Irr(G)$ the set of distinct irreducible characters of G.

Proposition 1.11. *For G and s_{C_1,C_2,C_3} as above we have:*

$$s_{C_1,C_2,C_3} = \frac{|G|}{|C_1| \cdot |C_2|} \sum_{\chi \in Irr(G)} \frac{\chi(g_1)\chi(g_2)\overline{\chi(g_3)}}{\chi(1)}.$$

□

p-powers of conjugacy classes

For a finite group G, the p-power line in the character table of G, which was first introduced in the character tables in the Atlas of finite simple groups [CCN+85], records for each conjugacy class C of G, and for each prime p dividing the order of an element $g \in C$, to which conjugacy class the p^{th}-power of g belongs to.

Example 1.12. *The conjugacy classes of S_4 are C_1, C_2, C_3, C_4, C_5 with representatives 1, $(1,2)$, $(1,2)(3,4)$, $(1,2,3)$, $(1,2,3,4)$ where clearly the elements in C_5 square to elements in C_3.*

1.3 Notes on Chapter 4

Group theoretic results

When finding the group structure of the groups discussed in Chapter 4 we make use of two well-know results of group theory: Burnside's $p^a \cdot q^b$ Theorem, and the Schur-Zassenhaus Theorem (p.187 and p.70 of [Asc00]). The reference for this subsection is [Asc00]. We assume the reader is familiar with elementary group theory and in particular with the notions of solvability of a group and of the splitting of a group over one of its normal subgroups.

Theorem 1.13. *(Feit and Thompson's Odd Order Theorem)*
Any group of odd order is solvable. □

Theorem 1.14. *(Burnside's $p^a \cdot q^b$ Theorem)*
Let p, q be two distinct primes and a, $b \in \mathbb{N}$. Any group of order $p^a \cdot q^b$ is solvable. □

Theorem 1.15. *(Schur-Zassenhaus Theorem)*
Let G be a finite group, let $N \trianglelefteq G$ and assume:

1) $(|N|, |G/N|) = 1$, *and*

2) *either N or G/N is solvable.*

Then

(i) *G splits over N, and*

(ii) *G acts transitively on the complements to N in G.* □

Remark 1.16. By the Feit and Thompson's Odd Order Theorem condition 2) of the Schur-Zassenhaus Theorem is implied by condition 1).

The use of Magma

In Chapter 4 we describe all the quotients of the Coxeter groups $G^{(m,n,p)}$ satisfying property $(\boldsymbol{\sigma})$. We do so by introducing a finite number of extra relations to the presentation of $G^{(m,n,p)}$ and so the groups considered are finitely presented groups. From subsection 3.2.3 onwards the orders of the groups considered were all computed with the software package Magma [BCP97]. Magma has a group category called GrpFP to deal with finitely presented groups. It also provides the user with a finitely presented group constructor that contructs a finitely presented group in a single step.

Example 1.17. *From the Atlas [CCN+85] the alternating group A_5 can be defined by the presentation $\langle a, b \mid a^2,\ b^3,\ (ab)^5 \rangle$. The Magma input would be:*

$$\mathsf{A}\langle \mathsf{a}, \mathsf{b} \rangle := \mathsf{Group}\langle \mathsf{a}, \mathsf{b} \mid \mathsf{a}^2,\ \mathsf{b}^3,\ (\mathsf{ab})^5 \rangle;$$

The orders of the groups from Chapter 4 were all checked (for those already known) or computed with the Magma function Order which takes a finitely presented group as its argument and returns either the size of the group as a positive integer, or the object Infinity if the group can be shown to be infinite, or the value 0 if the order of the group cannot be computed and the

group cannot be shown to be infinite. The function is based on the Todd-Coxeter algorithm [CT36] solving the coset enumeration problem for a finitely presented group G and one of its subgroup H. The Todd-Coxeter procedure installed in Magma is based on the coset enumeration programme *ACE3* developed by G. Havas [Hav] and C. Ramsay [Ram].

Chapter 2

Majorana representations

2.1 Introduction to the Monster algebra $V_{\mathbb{M}}$

We introduce the Monster algebra and give some of its properties. The main reference for this section is the article [Con85] written by J. H. Conway with significant contributions from S. P. Norton.

We let $\mathbb{M}$ be the Monster simple group and we let $\left(V_{\mathbb{M}}, \ \cdot \ , (\ ,\ )\right)$ be the Monster algebra, a commutative non-associative algebra of dimension $196,884$ over $\mathbb{R}$ with identity $\iota_{\mathbb{M}}$ and automorphism group $\mathbb{M}$, as described in [Con85]. As an $\mathbb{R}\mathbb{M}$-module $V_{\mathbb{M}}$ decomposes as the direct sum $V'_{\mathbb{M}} \oplus \mathbb{1}_{\mathbb{M}}$ where $\mathbb{1}_{\mathbb{M}}$ is the trivial $\mathbb{R}\mathbb{M}$-module equal to the $\mathbb{R}$-span of the identity $\iota_{\mathbb{M}}$ and $V'_{\mathbb{M}}$ is the minimal faithful irreducible $\mathbb{R}\mathbb{M}$-module of dimension $196,883$.

The group $\mathbb{M}$ has two conjugacy classes of involutions which we denote $2A$ and $2B$, following the notation used in the Atlas of Finite Simple Groups [CCN+85], where $2A$ is the smallest of the two classes. We call $2A$ involutions and $2B$ involutions the elements of $2A$ and $2B$ respectively. For a $2A$ involution t its centraliser $C_{\mathbb{M}}(t) \cong 2.\mathbb{B}\mathbb{M}$ is a double cover of the Baby Monster group, and for a $2B$ involution z its centraliser $C_{\mathbb{M}}(z) \cong 2^{1+24}.Co_1$ is an extension of the extraspecial group 2^{1+24} by the first Conway group Co_1.

Character calculations in the character table of $\mathbb{M}$ in [Con85] show that for each $2A$ involution t of $\mathbb{M}$, the centraliser $C_{\mathbb{M}}(t)$ fixes a unique 1-space of $V'_{\mathbb{M}}$, so that $C_{\mathbb{M}}(t)$ stabilises a 2-subspace W of $V_{\mathbb{M}}$. In [Con85] J. H. Conway shows that W has two non-trivial idempotents a_t and $\iota_{\mathbb{M}} - a_t$ where $a_t \cdot a_t = a_t$ and $(a_t, a_t) = 1$ (we note that a different scaling is used in [Con85]).

We call this bijection between the conjugacy class $2A$ and the idempotents a_t of $V_{\mathbb{M}}$ **Conway's bijection** $\mathcal{C}$:

$$\begin{aligned} \mathcal{C}: \ 2A &\to V_{\mathbb{M}} \\ t &\mapsto a_t \end{aligned} \tag{2.1}$$

and we call the non-trivial vector a_t fixed by $C_{\mathbb{M}}(t)$ a **2A-axis**.

2.1.1 The dihedral subalgebras of $V_{\mathbb{M}}$ generated by pairs of $2A$-axes

As in [CCN+85] we denote by NA, NB, ... the conjugacy classes of elements of order N in $\mathbb{M}$ in descending order of their centraliser order.

In [Con85] J. H. Conway describes with the help of S. P. Norton the subalgebras of $V_{\mathbb{M}}$ generated by two $2A$-axes a_t and a_s, which we call **dihedral subalgebras** of $V_{\mathbb{M}}$. The corresponding $2A$ involutions t and s generate a dihedral subgroup of $\mathbb{M}$. Calculations in the character table of $\mathbb{M}$ of the structure class constants $s_{2A,2A,X}$ (see Definition 1.11) for X any conjugacy class of $\mathbb{M}$ give that the product ts lies in either of the nine conjugacy classes: $1A$, $2A$, $2B$, $3A$, $3C$, $4A$, $4B$, $5A$, $6A$. This shows that the $2A$ involutions of $\mathbb{M}$ are 6-transpositions, which is such an essential property used in this thesis that we write the following proposition.

Proposition 2.1. *(The 6-transposition Property)*
Let t, s be two $2A$ involutions in $\mathbb{M}$, then their product ts has order less or equal to 6. □

In the next theorem we denote by Fi_{24} the 3-transposition automorphism group of the Fisher simple group Fi'_{24}, which contains Fi'_{24} with index 2, we denote by Co_3 the third Conway simple group, and we denote by HN the Harada-Norton simple group. These notations follow those of the Atlas [CCN+85].

Theorem 2.2. *Let t and s be $2A$ involutions with corresponding $2A$-axes a_t and a_s and let $\rho := ts$. Let U be the dihedral subalgebra of $V_{\mathbb{M}}$ generated by the $2A$-axes a_t and a_s. Then there are nine isomorphism types for U determined by the conjugacy class in $\mathbb{M}$ of ρ. Furthermore the nine dihedral algebras have bases, algebra and inner product values as described in Table 2.1 where:*

1) *for* $\rho \in 3A$*: the* 1*-subspace of* U *spanned by* u_ρ *is invariant under* $N_{\mathbb{M}}(\langle\rho\rangle) \cong 3.Fi_{24}$ *and* $u_\rho = u_{\rho^{-1}}$*;*

2) *for* $\rho \in 4A$*: the* 1*-subspace of* U *spanned by* v_ρ *is invariant under* $N_{\mathbb{M}}(\langle\rho\rangle) \cong 2_+^{1+24}.Co_3$ *and* $v_\rho = v_{\rho^{-1}}$*;*

3) *for* $\rho \in 5A$*: the* 1*-subspace of* U *spanned by* w_ρ *is invariant under* $N_{\mathbb{M}}(\langle\rho\rangle) \cong (D_{10} \times HN).2$ *and* $w_\rho = -w_{\rho^2} = -w_{\rho^3} = w_{\rho^4}$*.* □

We explain the notation of Table 2.1. As in the above theorem we let $\rho := ts$, we let U be the dihedral subalgebra of $V_{\mathbb{M}}$ generated by the $2A$-axes a_t and a_s and we write that U is of **type NX** if ρ is in the conjugacy class NX of $\mathbb{M}$. Since $\rho = ts$, then for all integers i the involution $t\rho^i$ is also a $2A$ involution, since it can be written as a conjugate of either t or s, and so $\mathcal{C}(t\rho^i)$ is a $2A$-axis of U. We denote by a_i the $2A$-axis $\mathcal{C}(t\rho^i)$ and so $a_0 := a_t$ and $a_1 := a_s$.
If $\rho \in 2A$ then a_ρ is a $2A$-axis of U distinct from a_0 and a_1 and the dihedral subalgebra of type $2A$ has basis $\{a_0,\ a_1,\ a_\rho\}$. If $\rho \in 3A$ then $a_{-1} = a_2$ is a $2A$-axis of U distinct from a_0 and a_1 but the algebra product is not closed on the $\mathbb{R}$-linear span of $\{a_0,\ a_1,\ a_{-1}\}$. The element $u_\rho := \frac{2^6}{3^3.5}(2a_0 + 2a_1 + a_{-1}) - \frac{2^{11}}{3^3.5}a_0 \cdot a_1$ is introduced to close the algebra product and is chosen so that u_ρ is invariant under $N_{\mathbb{M}}(\langle\rho\rangle)$ with respect to the action of $\mathbb{M}$ on $V_{\mathbb{M}}$ (see [Con85]). We call u_ρ a **3A-axis**. Similarly in the dihedral subalgebras of types $4A$ and $5A$ the algebra product is not closed on the $\mathbb{R}$ linear span of the $2A$-axes $\{a_i\}$ so the vectors v_ρ and w_ρ are introduced in Table 2.1, and we call them **4A-axis** and **5A-axis** respectively. As for $3A$-axes the $4A$ and $5A$-axes are chosen to be invariant under $N_{\mathbb{M}}(\langle\rho\rangle)$ for $\rho \in 4A$ and $5A$.
Lastly from the p-powers of the conjugacy classes $4B$, $4A$ and $6A$ in $\mathbb{M}$ we have the following inclusions of dihedral subalgebras:

$$2A \hookrightarrow 4B,\ 2B \hookrightarrow 4A,\ 2A \hookrightarrow 6A, \text{ and } 3A \hookrightarrow 6A.$$

Type (subalgebras)	Basis	Algebra and inner products
1A	a_0	$a_0 \cdot a_0 = a_0,\ (a_0, a_0) = 1$
2A ($1A$)	$a_0,\ a_1,\ a_\rho$	$a_0 \cdot a_1 = \frac{1}{2^3}(a_0 + a_1 - a_\rho),\ a_0 \cdot a_\rho = \frac{1}{2^3}(a_0 + a_\rho - a_1)$ $(a_0, a_1) = (a_0, a_\rho) = (a_1, a_\rho) = \frac{1}{2^3}$
2B ($1A$)	$a_0,\ a_1$	$a_0 \cdot a_1 = 0,\ (a_0, a_1) = 0$
3A ($1A$)	$a_{-1},\ a_0,\ a_1,$ u_ρ	$a_0 \cdot a_1 = \frac{1}{2^5}(2a_0 + 2a_1 + a_{-1}) - \frac{3^3 \cdot 5}{2^{11}} u_\rho$ $a_0 \cdot u_\rho = \frac{1}{3^2}(2a_0 - a_1 - a_{-1}) + \frac{5}{2^5} u_\rho$ $u_\rho \cdot u_\rho = u_\rho$ $(a_0, a_1) = \frac{13}{2^8},\ (a_0, u_\rho) = \frac{1}{2^2},\ (u_\rho, u_\rho) = \frac{2^3}{5}$
3C ($1A$)	$a_{-1},\ a_0,\ a_1$	$a_0 \cdot a_1 = \frac{1}{2^6}(a_0 + a_1 - a_{-1}),\ (a_0, a_1) = \frac{1}{2^6}$
4A ($1A$,$2B$)	$a_{-1},\ a_0,\ a_1,$ $a_2,\ v_\rho$	$a_0 \cdot a_1 = \frac{1}{2^6}(3a_0 + 3a_1 + a_2 + a_{-1} - 3v_\rho)$ $a_0 \cdot v_\rho = \frac{1}{2^4}(5a_0 - 2a_1 - a_2 - 2a_{-1} + 3v_\rho)$ $v_\rho \cdot v_\rho = v_\rho,\ \ a_0 \cdot a_2 = 0$ $(a_0, a_1) = \frac{1}{2^5},\ (a_0, a_2) = 0,\ (a_0, v_\rho) = \frac{3}{2^3},\ (v_\rho, v_\rho) = 2$
4B ($1A$,$2A$)	$a_{-1},\ a_0,\ a_1,$ $a_2,\ a_{\rho^2}$	$a_0 \cdot a_1 = \frac{1}{2^6}(a_0 + a_1 - a_{-1} - a_2 + a_{\rho^2})$ $a_0 \cdot a_2 = \frac{1}{2^3}(a_0 + a_2 - a_{\rho^2})$ $(a_0, a_1) = \frac{1}{2^6},\ (a_0, a_2) = (a_0, a_{\rho^2}) = \frac{1}{2^3}$
5A ($1A$)	$a_{-2},\ a_{-1},\ a_0,$ $a_1,\ a_2,\ w_\rho$	$a_0 \cdot a_1 = \frac{1}{2^7}(3a_0 + 3a_1 - a_2 - a_{-1} - a_{-2}) + w_\rho$ $a_0 \cdot a_2 = \frac{1}{2^7}(3a_0 + 3a_2 - a_1 - a_{-1} - a_{-2}) - w_\rho$ $a_0 \cdot w_\rho = \frac{7}{2^{12}}(a_1 + a_{-1} - a_2 - a_{-2}) + \frac{7}{2^5} w_\rho$ $w_\rho \cdot w_\rho = \frac{5^2 \cdot 7}{2^{19}}(a_{-2} + a_{-1} + a_0 + a_1 + a_2)$ $(a_0, a_1) = \frac{3}{2^7},\ (a_0, w_\rho) = 0,\ (w_\rho, w_\rho) = \frac{5^3 \cdot 7}{2^{19}}$
6A ($1A$,$2A$,$3A$)	$a_{-2},\ a_{-1},\ a_0,$ $a_1,\ a_2,\ a_3$ $a_{\rho^3},\ u_{\rho^2}$	$a_0 \cdot a_1 = \frac{1}{2^6}(a_0 + a_1 - a_{-2} - a_{-1} - a_2 - a_3 + a_{\rho^3}) + \frac{3^2 \cdot 5}{2^{11}} u_{\rho^2}$ $a_0 \cdot a_2 = \frac{1}{2^5}(2a_0 + 2a_2 + a_{-2}) - \frac{3^3 \cdot 5}{2^{11}} u_{\rho^2}$ $a_0 \cdot u_{\rho^2} = \frac{1}{3^2}(2a_0 - a_2 - a_{-2}) + \frac{5}{2^5} u_{\rho^2}$ $a_0 \cdot a_3 = \frac{1}{2^3}(a_0 + a_3 - a_{\rho^3}),\ a_{\rho^3} \cdot u_{\rho^2} = 0,\ (a_{\rho^3}, u_{\rho^2}) = 0$ $(a_0, a_1) = \frac{5}{2^8},\ (a_0, a_2) = \frac{13}{2^8},\ (a_0, a_3) = \frac{1}{2^3}$

TABLE 2.1: Dihedral subalgebras of $V_{\mathbb{M}}$ generated by two $2A$-axes

Next we state a property of the $2A$-axes that will form one of the axioms of Majorana theory. For all $v \in V_{\mathbb{M}}$ we denote by $ad(v)$ the adjoint transformation in $End(V_{\mathbb{M}})$:

$$\begin{aligned} ad(v) : V_{\mathbb{M}} &\to V_{\mathbb{M}} \\ w &\mapsto v \cdot w \end{aligned}$$

By rescaling appropriately the values in section 16 and appendix 6 of [Con85] we obtain the next proposition.

Proposition 2.3. *For a $2A$-axis a the eigenvalues of $ad(a)$ are $1,\ 0,\ \frac{1}{4}$ and $\frac{1}{32}$ so that $V_{\mathbb{M}} \cong V_1^{(a)} \oplus V_0^{(a)} \oplus V_{\frac{1}{4}}^{(a)} \oplus V_{\frac{1}{32}}^{(a)}$, where $V_\lambda^{(a)}$ denotes the eigenspace of a with eigenvalue λ.* □

2.1.2 Partial associativity in $V_{\mathbb{M}}$

In section 16 of [Con85] J. H. Conway defines a bilinear alternating function Δ on the exterior square of $V_{\mathbb{M}}$:

$$\begin{aligned} \Delta : \wedge^2 V_{\mathbb{M}} &\to End(V_{\mathbb{M}}) \\ u \wedge v &\mapsto ad(u)ad(v) - ad(v)ad(u) \end{aligned}$$

where clearly $\Delta(u \wedge v) = \Delta(-v \wedge u)$, and for $a \wedge b \in \wedge^2 V_{\mathbb{M}}$ we have $(a \wedge b)^{\Delta(u \wedge v)} = a^{\Delta(u \wedge v)} \wedge b^{\Delta(u \wedge v)}$. Then J. H. Conway proves the following proposition.

Proposition 2.4. *Let $u \wedge v \in \wedge^2 V_{\mathbb{M}}$. Then the algebra $\wedge^2 V_{\mathbb{M}}$ can be decomposed as:*

$$\wedge^2 V_{\mathbb{M}} = Ker(\Delta(u \wedge v)) \oplus Im(\Delta(u \wedge v)) \cong V'_{\mathbb{M}} \oplus V_2 \oplus V_3$$

and

$$Ker(\Delta(u \wedge v)) \cong V'_{\mathbb{M}} \oplus V_3, \quad Im(\Delta(u \wedge v)) \cong V_2$$

where $V'_{\mathbb{M}}$ is the minimal irreducible $\mathbb{RM}$-module of dimension $196,883$, and V_2 and V_3 are irreducible $\mathbb{RM}$-modules of dimension $21,296,876$ and $19,360,062,527$ respectively. □

Next we state a property of $V_{\mathbb{M}}$ introduced by S. P. Norton. Let us define a symmetric bilinear function $\langle\ ,\ \rangle$ on the set $\wedge^2 V_{\mathbb{M}} \times \wedge^2 V_{\mathbb{M}}$:

$$\begin{aligned} \langle\ ,\ \rangle :\ \wedge^2 V_{\mathbb{M}} \times \wedge^2 V_{\mathbb{M}} &\to \mathbb{R} \\ u \wedge v,\ x \wedge y &\mapsto (u^{\Delta(x \wedge y)}, v) \end{aligned}$$

where $(u^{\Delta(x\wedge y)}, v) = (u\cdot x, y\cdot v) - (u\cdot y, x\cdot v) = (x^{\Delta(u\wedge v)}, y)$. Since $Im(\Delta)$ is irreducible and there exist vectors $u,\ v,\ x$ and y in $V_{\mathbb{M}}$ where $\langle u\wedge v, x\wedge y\rangle$ is positive, for example for $a_0,\ a_1$ in row $2A$ of Table 2.1 we get $(a_0^{\Delta(a_0\wedge a_1)}, a_1) = \frac{41}{8^3}$, S. P. Norton deduced the next proposition.

Proposition 2.5. *(Norton Inequality)*
For any u and v in $V_{\mathbb{M}}$ the following inequality holds:

$$(u\cdot u, v\cdot v) - (u\cdot v, u\cdot v) \geq 0$$

□

When equality holds in the expression above for two elements $u,\ v \in V_{\mathbb{M}}$ then they associate with every element $x \in V_{\mathbb{M}}$: $(u\cdot x)\cdot v = (v\cdot x)\cdot u$. Clearly a subalgebra of $V_{\mathbb{M}}$ generated by a set $\{a_i\}_{i\in I}$ of $2A$-axes, such that for any two axes $a_i,\ a_j$ we get the equality $(a_i\cdot a_i, a_j\cdot a_j) - (a_i\cdot a_j, a_i\cdot a_j) = 0$, is associative. In fact associative subalgebras of $V_{\mathbb{M}}$ generated by $2A$-axes have been completely described by W. Meyer and W. Neutsch in Theorem 4 of [MN93] which we reproduce below.

Theorem 2.6. *Let V be a k-dimensional associative subalgebra of $V_{\mathbb{M}}$, then:*

1) *V is isomorphic to the direct sum of k copies of $\mathbb{R}$:*

$$V \cong \mathbb{R}^k;$$

2) *$k \leq 48$;*

3) *V contains a basis of k mutually annihilating idempotents, $\{a_{t_1}, \ldots, a_{t_k}\}$, where $\forall i\ \ t_i \in 2A$, which are orthogonal to each other, such that for all $i \neq j \in [1, \ldots, k]$:*

$$a_{t_i}\cdot a_{t_j} = 0$$
$$(a_{t_i}, a_{t_j}) = 0;$$

4) *The idempotents of V are the partial sums of a_{t_i}s so there are 2^k idempotents, including 0, and among them $\{a_{t_1}, \ldots, a_{t_k}\}$ is the only orthonormal basis;*

5) *The corresponding set of involutions $\{t_1, \ldots, t_k\} \subseteq 2A$ generates a group $E := \langle t_1, \ldots, t_k\rangle$ which is an elementary abelian 2-subgroup of $\mathbb{M}$, with*

$$t_i t_j\ \in 2B \text{ for all } i \neq j \in [1, \ldots, k].$$

□

2.2 Axioms of Majorana theory and Majorana calculus

The main reference for this section is the foundational article of Majorana theory [IPSS10].

Within the framework of Vertex Operator Algebras (VOAs) the Monster group $\mathbb{M}$ can be realised as the automorphism group of the Moonshine VOA as constructed in [FLM88] and [Miy04]. In [Sak07] S. Sakuma studies subalgebras U generated by two Ising vectors in the Griess algebra of a VOA by associating to each Ising vector u an involutory automorphism $\tau(u)$ of U called a *Miyamoto involution* after M. Miyamoto who first studied them. S. Sakuma proves, independently of $\mathbb{M}$, that the structure of U is uniquely determined by some inner products of Ising vectors and that the order of the product of any two Miyamoto involutions is less than or equal to 6. Moreover each algebra U is isomorphic to one of the nine dihedral subalgebras of $V_{\mathbb{M}}$.

Inspired by S. Sakuma, A. A. Ivanov introduced Majorana theory in his book [Iva09]. It is an axiomatisation of seven of the properties of $\big(V_{\mathbb{M}},\ \cdot\ ,(\ ,\ )\big)$ and its $2A$-axes $\{a_t\}_{t\in 2A}$, outside of the VOA framework. We now give below the axioms of Majorana theory (M1) to (M7).

We let $\big(V,\cdot,(\ ,\ )\big)$ be a real commutative non-associative algebra such that:

(M1) $(\ ,\ )$ is a symmetric positive definite bilinear form on V that associates with $\cdot$ in the sense that $(u, v\cdot w) = (u\cdot v, w)$ for all $u, v, w \in V$, and $\cdot$ is a bilinear commutative non-associative algebra product on V;

(M2) the Norton inequality (Proposition 2.5) holds, so that $(u\cdot u, v\cdot v) \geq (u\cdot v, u\cdot v)$ for all $u, v \in V$.

Let A be a subset of $V\backslash\{0\}$ whose elements a satisfy the conditions (M3) to (M7):

(M3) $(a, a) = 1$ and $a\cdot a = a$;

(M4) $V = V_1^{(a)} \oplus V_0^{(a)} \oplus V_{\frac{1}{2^2}}^{(a)} \oplus V_{\frac{1}{2^5}}^{(a)}$, where $V_\mu^{(a)} = \{v \mid v \in V, a\cdot v = \mu v\}$ is the μ-eigenspace of the adjoint action of a on V;

(M5) $V_1^{(a)} = \{\lambda a \mid \lambda \in \mathbb{R}\}$;

(M6) the linear transformation $\tau(a)$ of V, called a **Majorana involution**, is defined via

$$\tau(a) : u \mapsto (-1)^{2^5\mu} u$$

for $u \in V_\mu^{(a)}$ with $\mu = 1, 0, \frac{1}{2^2}, \frac{1}{2^5}$, and preserves the algebra product (*i.e.* $u^{\tau(a)} \cdot v^{\tau(a)} = (u \cdot v)^{\tau(a)}$ for all $u, v \in V$);

(M7) if $V_+^{(a)}$ is the centralizer of $\tau(a)$ in V, so that $V_+^{(a)} = V_1^{(a)} \oplus V_0^{(a)} \oplus V_{\frac{1}{2^2}}^{(a)}$, then the linear transformation $\sigma(a)$ of $V_+^{(a)}$ defined via

$$\sigma(a) : u \mapsto (-1)^{2^2\mu} u$$

for $u \in V_\mu^{(a)}$ with $\mu = 1, 0, \frac{1}{2^2}$ preserves the algebra product on $V_+^{(a)}$ (*i.e.* $u^{\sigma(a)} \cdot v^{\sigma(a)} = (u \cdot v)^{\sigma(a)}$ for all $u, v \in V_+^{(a)}$).

Definition 2.7. Let $\big(V, \cdot, (\ ,\ )\big)$ be a real commutative non-associative algebra satisfying axioms (M1) and (M2) and containing a set A of non-trivial idempotents satisfying axioms (M3) to (M7). We call the elements of A **Majorana axes**.

Definition 2.8. A real commutative non-associative algebra $\big(V, \cdot, (\ ,\ )\big)$ is called a **Majorana algebra** if it satisfies axioms (M1) and (M2) and is generated by a set of Majorana axes.

A few interesting properties can be deduced from the axioms of Majorana theory. We state two lemmas which are direct consequences of the axioms (M1) to (M5).

Lemma 2.9. *The eigenspace decomposition in (M4) is orthogonal with respect to the inner product* $(\ ,\ )$. □

Lemma 2.10. *Let V be an $\mathbb{R}$-vector space satisfying the axioms (M1) to (M5), and let a be a Majorana axis of V. Then for all $v \in V$, the projection of v onto the eigenspace $V_1^{(a)}$ is $(a, v)a$.* □

An important consequence of the latter lemma are the 'Fusion rules'.

Lemma 2.11. *For a fixed Majorana axis a, the product of any two eigenvectors of a lies in the direct sum of the eigenspace(s) of the spectrum given by Table 2.2.*

Sp	1	0	$\frac{1}{2^2}$	$\frac{1}{2^5}$
1	1	0	$\frac{1}{2^2}$	$\frac{1}{2^5}$
0	0	0	$\frac{1}{2^2}$	$\frac{1}{2^5}$
$\frac{1}{2^2}$	$\frac{1}{2^2}$	$\frac{1}{2^2}$	$1, 0$	$\frac{1}{2^5}$
$\frac{1}{2^5}$	$\frac{1}{2^5}$	$\frac{1}{2^5}$	$\frac{1}{2^5}$	$1, 0, \frac{1}{2^2}$

TABLE 2.2: The Fusion rules

To give an example, let us prove the inclusion $V_0^{(a)}.V_0^{(a)} \subseteq V_0^{(a)}$. We let $u \neq v \in V_0^{(a)}$. By axiom (M6), $(u.v)^{\tau(a)} = u^{\tau(a)}.v^{\tau(a)} = u.v$ so that the projection of $u.v$ onto $V_{\frac{1}{2^5}}^{(a)}$ is 0, and by axiom (M7), $(u.v)^{\sigma(a)} = u^{\sigma(a)}.v^{\sigma(a)} = u.v$ so that the projection of $u.v$ onto $V_{\frac{1}{2^2}}^{(a)}$ is 0. Hence we can write $u \cdot v = \lambda a + \alpha$ where $\lambda \in \mathbb{R}$ and $\alpha \in V_0^{(a)}$. Now using axiom (M1) we have $(a, u \cdot v) = (a \cdot u, v) = (0, v) = 0$ and $(a, u \cdot v) = (a \cdot a, \lambda a + \alpha) = (a, a \cdot (\lambda a + \alpha)) = (a, \lambda a) = \lambda$. Hence $\lambda = 0$ and so $u \cdot v \in V_0^{(a)}$.

Lastly we introduce the *Resurrection principle* which was formulated by S. Shpectorov and can be read in [IPSS10]. It is believed that S. Sakuma used a similar idea in his paper [Sak07] but no such result is mentioned explicitly. This principle is a consequence of the Fusion rules involving 0 and $\frac{1}{4}$-eigenvectors of a Majorana axis a. It is a crucial tool used to close the algebra product on a generating set for a Majorana algebra.

Proposition 2.12. *(The Resurrection principle)*
Let V be a Majorana algebra, let a be a Majorana axis of V, and let W be an a-stable subspace of V. For $v \in V$ suppose that

$$\alpha_v = v + w_\alpha \text{ and } \beta_v = v + w_\beta$$

are 0 and $\frac{1}{2^2}$-eigenvectors of a, respectively, for some $w_\alpha, w_\beta \in W$. Then

$$v = -\left[4a \cdot (w_\alpha - w_\beta) + w_\beta\right],$$

in particular $v \in W$. □

2.3 Internal Majorana representations and Sakuma's Theorem

As mentioned in the introduction, S. Sakuma classified all subalgebras generated by two Ising vectors in the Griess algebra of a VOA using classical results on VOAs. In a comparable way, A. A. Ivanov *et al* classified all dihedral Majorana algebras, by which we mean Majorana algebras generated by two Majorana axes, using Majorana calculus. They called their result 'Sakuma's Theorem' in his honour.

A Majorana algebra U generated by a set A of Majorana axes is invariant under the group of automorphisms G generated by the set of Majorana involutions $\tau(A)$. A. A. Ivanov axiomatised, and extended, the G-invariance of U by defining a *Majorana representation* for G, which we define in Definition 2.17 in the next section ([IPSS10]). For a dihedral Majorana algebra invariant under a dihedral group, the weaker definition of an *internal Majorana representation* suffices [IPSS10].

Definition 2.13. Let $\big(V, \cdot, (\ ,\ )\big)$ be a real commutative non-associative algebra satisfying axioms (M1) and (M2) with a set $A \subseteq V$ of Majorana axes satisfying axioms (M3) to (M7). We let B be any subset of A and G be the subgroup of $GL(V)$ generated by the set of Majorana involutions $\{\tau(a)\}_{a\in B}$. We also let U be the subalgebra of V generated by B and denote by $\cdot|_U$ and $(\ ,\ )|_U$ the restriction of $\cdot$ and $(\ ,\ )$ to U. The quintet

$$(G, U, B, (\ ,\ )|_U, \cdot|_U)$$

is called an **internal Majorana representation** of G.

For example $(\mathbb{M}, V_{\mathbb{M}}, \mathcal{C}(2A), (\ ,\ ), \cdot)$ is an internal Majorana representation of $\mathbb{M}$ where $\mathcal{C}$ is Conway's bijection 2.1.

In [IPSS10] Majorana calculus was used to find all the internal Majorana representations of the dihedral groups, and thus all the dihedral Majorana algebras. We remark that the set of dihedral Majorana algebras must contain all the dihedral subalgebras of $V_{\mathbb{M}}$ described in subsection 2.1.1. In fact from Sakuma's Theorem, these are exactly the Majorana dihedral subalgebras.

Theorem 2.14. *(Sakuma's Theorem)*
Let $\big(V, A, (\ ,\ ), \cdot\big)$ be a quadruple satisfying (M1) to (M7). Let a_0, a_1 be a pair of Majorana axes and let τ_0, τ_1 be their corresponding Majorana involutions. Let D be the dihedral subgroup $\langle \tau_0,\ \tau_1 \rangle$ of $GL(V)$, and let U be the subalgebra $\langle\langle a_0,\ a_1\rangle\rangle$ of V such that $(D, U, \{a_0, a_1\}, (\ ,\ )|_U, \cdot|_U)$ is an internal Majorana representation of D. Then the following hold:

1) *$dim(U) \leq 8$;*

2) *the isomorphism type of the algebra $\big(U, (\ ,\ )|_U, \cdot|_U\big)$ is uniquely determined by the two inner products values $\lambda_1 := (a_0, a_1)$ and $\lambda_2 := (a_0, a_1^{\tau_0})$;*

3) *the existing representations have parameters as given in Table 2.3 and the algebras U are equal to the dihedral subalgebras of $V_{\mathbb{M}}$ as described in Table 2.1.* □

Proof of Sakuma's Theorem

We sketch the argument, given in [IPSS10], proving Sakuma's Theorem and we refer the reader to [IPSS10] for a full version.

The proof of parts 1) and 2) of the theorem relies on constructing a D-invariant set of Majorana axes for U. We let $\rho := \tau_0\tau_1$ and we let $a_{2i+\epsilon} := (a_\epsilon)^{\rho^i}$ for $\epsilon \in \{0, 1\}$ and $i \in \mathbb{Z}$, where $a_{2i+\epsilon}$ is the Majorana axis corresponding to the Majorana involution $\tau_\epsilon^{\rho^i}$. We let $B_0 := \{a_{2i} | i \in \mathbb{Z}\}$, $B_1 := \{a_{2i+1} | i \in \mathbb{Z}\}$ and $B := B_0 \cup B_1$.

Claim 1: The set B is D-invariant and B is contained in U.

The D-invariance is clear. To prove the second part of Claim 1, one can write $a_1 = \lambda_1 a_0 + \alpha_1 + \beta_1 + \gamma_1$ where $\lambda_1 = (a_0, a_1)$, $\alpha_1 \in V_0^{(a_0)}$, $\beta_1 \in V_{\frac{1}{2^2}}^{(a_0)}$ and $\gamma_1 \in V_{\frac{1}{2^5}}^{(a_0)}$. The vectors α_1, β_1, γ_1 can be expressed as linear combinations of the elements a_0, a_1, $a_0 \cdot a_1$, $a_0 \cdot (a_0 \cdot a_1)$ so all belong to U. By applying τ_0 to a_1 we obtain $a_{-1} = \lambda_1 a_0 + \alpha_1 + \beta_1 - \gamma_1$, so $a_{-1} \in U$ and by induction it follows that $B \subseteq U$.

Claim 2: The vectors σ_1, $\sigma_{2,1}$, $\sigma_{2,0}$ below are D-invariant:

$$\sigma_1 := a_0 \cdot a_1 - \frac{1}{2^5}(a_0 + a_1)$$
$$\sigma_{2,1} := a_1 \cdot a_{-1} - \frac{1}{2^5}(a_{-1} + a_1)$$
$$\sigma_{2,0} := a_0 \cdot a_2 - \frac{1}{2^5}(a_0 + a_2)$$

and the following equality holds true for all $j \in \mathbb{Z}$:

$$a_j \cdot \sigma_1 = \frac{7}{2^5}\sigma_1 + \big(\frac{3\lambda_1}{2^2} - \frac{25}{2^{10}}\big)a_j + \frac{7}{2^{11}}\big(a_{j-1} + a_{j+1}\big) \tag{2.2}$$

.

Since we can write $a_1 = \lambda_1 a_0 + \alpha_1 + \beta_1 + \gamma_1$ as in the proof of the previous claim, we have $a_0 \cdot a_1 = \lambda_1 a_0 + \frac{1}{2^2}\beta_1 + \frac{1}{2^5}\gamma_1$ and so the difference $a_0 \cdot a_1 - \frac{1}{2^5}a_1$ is in $V_+^{(a_0)}$ which means it is centralised by τ_0. Hence σ_1 is centralised by τ_0 and similarly we can show that σ_1 is centralised by τ_1 so we have that σ_1 is invariant under $D = \langle \tau_0, \tau_1 \rangle$. The other assertions of Claim 2 can be checked quite easily by D-invariance of σ_1.

Next we define $\lambda_j^{(\epsilon)} := (a_\epsilon, a_{j+\epsilon})$ for $\epsilon \in \{0, 1\}$ and $j \in \mathbb{Z}$.

Claim 3: For any $i, j \in \mathbb{Z}$ the value of (a_i, a_{i+j}) is uniquely determined by j so that $\lambda_j^{(\epsilon)}$ does not depend on ϵ.

Claim 3 is proved using the fact that D acts transitively on B_0 and B_1. By transitivity of D we have $\lambda_j^{(0)} = \lambda_j^{(1)}$ for all odd j so it remains to prove that $\lambda_j^{(0)} = \lambda_j^{(1)}$ for all even j. Taking the inner products of a_j and a_{j+1} with both sides of the equality 2.2 for $j = 0$ and $j = 1$, along with axiom (M1), we get that $\lambda_i^{(0)} = \lambda_i^{(1)}$ for all i by D-invariance of the inner product.

Claim 4: The following equalities hold true for all $i \in \mathbb{Z}$:

$$a_{2i} \cdot \sigma_{2,0} = \frac{7}{2^5}\sigma_{2,0} + \big(\frac{3\lambda_2}{2^2} - \frac{25}{2^{10}}\big)a_{2i} + \frac{7}{2^{11}}(a_{2i-2} + a_{2i+2})$$
$$a_{2i+1} \cdot \sigma_{2,1} = \frac{7}{2^5}\sigma_{2,1} + \big(\frac{3\lambda_1}{2^2} - \frac{25}{2^{10}}\big)a_{2i+1} + \frac{7}{2^{11}}\big(a_{2i-1} + a_{2i+3}\big)$$

A proof of Claim 4 can be obtained by generalising equation 2.2 and using D-invariance and the equality $\lambda_2^{(0)} = \lambda_2^{(1)}$ from Claim 3.

Next we define W to be the subspace of U spanned by the set $\mathcal{L}$:

$$\mathcal{L} := \{a_0,\ a_1,\ a_{-1},\ a_2,\ a_{-2},\ \sigma_1,\ \sigma_{2,0},\ \sigma_{2,1}\}.$$

Claim 5: W is D-invariant and closed under the algebra product.

The first part of Claim 5 can be proved using Claims 3 and 4, whilst the second part can be proved using the Resurrection principle 2.12.

Claim 6: The set B contains at most 6 Majorana axes.

The proof of Claim 6 follows from computing the determinant $det(\mathcal{G})$ of the Gram matrix $\mathcal{G}$ for the inner products (a_i, a_j) for all $a_i, a_j \in B$. For $|B| \geq 7$, $det(\mathcal{G}) = 0$. In particular the dihedral group D cannot be larger than D_{12}.

For $|B| = 1$ the group D is trivial and U is the $\mathbb{R}$-span of a_0. For each value of $2 \leq |B| \leq 6$ one obtains quadratic equations (with rational coefficients) to solve for λ_1 and the value of λ_2 follows. The dimension of U is found by computing the rank of the Gram matrix of $\mathcal{L}$. We find nine possibilities for the pair (λ_1, λ_2) so there are at most nine distinct Majorana representations of the dihedral group D. Since all the dihedral subalgebras of $V_{\mathbb{M}}$ generated by two $2A$-axes must appear as Majorana algebras, there are in fact exactly nine Majorana representations of the dihedral groups whose Majorana algebras are all equal to subalgebras of $V_{\mathbb{M}}$. Hence if the algebra U from a Majorana representation of a dihedral group corresponds to the dihedral subalgebra NX of $V_{\mathbb{M}}$ we write that U has **type NX**. We summarise in Table 2.3 the parameters found for all Majorana representations of dihedral groups.

Type:	$1A$	$2A$	$2B$	$3A$	$3C$	$4A$	$4B$	$5A$	$6A$
$\|B\|$	1	2	2	3	3	4	4	5	6
λ_1	1	$\frac{1}{2^3}$	0	$\frac{13}{2^8}$	$\frac{1}{2^6}$	$\frac{1}{2^5}$	$\frac{1}{2^6}$	$\frac{3}{2^7}$	$\frac{5}{2^8}$
λ_2	1	1	1	$\frac{13}{2^8}$	$\frac{1}{2^6}$	0	$\frac{1}{2^3}$	$\frac{3}{2^7}$	$\frac{13}{2^8}$
$dim(U)$	1	3	2	4	3	5	5	6	8
D	1	D_4	D_4	D_6	D_6	D_8	D_8	D_{10}	D_{12}

TABLE 2.3: Majorana representations of dihedral groups

Not all of the algebra products for the dihedral Majorana algebras were computed from first principles using the axioms (M1) to (M7). Instead part 3) of Sakuma's Theorem was partially obtained from the information on the dihedral subalgebras of $V_{\mathbb{M}}$ in Table 2.1.

Remark 2.15. Sakuma's Theorem proves the 6-transposition property of the Majorana involutions, thus reproving the 6-transposition property of the $2A$ involutions of $\mathbb{M}$ rather than relying on it.

Vectors invariant under cyclic groups in dihedral Majorana algebras

In the dihedral Majorana subalgebras of types $3A$ and $4A$, we observe that swapping the roles of a_0 and a_1 as well as choosing different generators for the algebras implies that the basis elements u_ρ in $3A$ and v_ρ in $4A$ depend on the cyclic group $\langle\rho\rangle$ of order 3 and 4 respectively, but not on the element ρ. Hence:

$$u_\rho = u_{\rho^2} \text{ and } v_\rho = v_{\rho^3}.$$

We call u_ρ a **3A-axial vector** and we call v_ρ a **4A-axial vector**. In the dihedral Majorana algebra of type $5A$ the expressions for the products $a_0 \cdot a_1$ and $a_0 \cdot a_2$ given in Table 2.1 are almost symmetrical except for a sign difference in front of the basis element w_ρ. This yields the following equalities :

$$w_\rho = -w_{\rho^2} = -w_{\rho^3} = w_{\rho^4}.$$

We call the element w_ρ a **5A-axial vector**.

Inclusions between dihedral Majorana algebras

Since each of the dihedral Majorana algebras is equal to one of the subalgebras of $V_\mathbb{M}$ from Table 2.1, we can deduce the following inclusions of dihedral Majorana algebras.

Corollary 2.16. *The dihedral Majorana algebra of type $6A$ contains dihedral subalgebras of types $2A$ and $3A$, the dihedral Majorana algebra of type $4B$ contains subalgebras of type $2A$, and the algebra of type $4A$ contains subalgebras of type $2B$.* □

2.4 Majorana representations

The definition of a Majorana representation for a finite group G aims at describing Majorana algebras invariant under G. One of the motivations behind it is the description of subalgebras

of $V_{\mathbb{M}}$ invariant under the relevant subgroup of $\mathbb{M}$, allowing for calculations to be performed in that subgroup instead of the whole of $\mathbb{M}$. But Majorana theory also aims at describing a class of algebras independently of $\mathbb{M}$, and indeed some Majorana algebras generated by more than two Majorana axes may not necessarily be subalgebras of $V_{\mathbb{M}}$, as will be seen in the next section. In that case, defining a group action on a Majorana algebra via a Majorana representation provides an even more useful tool to characterise the algebra.

2.4.1 Definition

Definition 2.17. A **Majorana representation** of a finite group G is a tuple

$$\mathcal{R} = \big(G,\ T,\ X,\ (\ ,\ ),\ \cdot,\ \varphi,\ \psi\big),$$

where T is a union of conjugacy classes of involutions generating G, and $\big(X,\ \cdot,\ (\ ,\ )\big)$ is a commutative non-associative $\mathbb{R}$-algebra satisfying the Majorana axioms (M1) and (M2) and which is generated by a set A of Majorana axes. The map ψ is a bijection sending each involution t of T to a Majorana axis a_t of X. The map $\varphi : G \to GL(X)$ is a homomorphism with kernel $Z(G)$ such that $Im(\varphi)$ is a group of automorphisms of $\big(X,\ \cdot\ ,\ (\ ,\ )\big)$ where $\varphi(t) = \tau(t)$ for all $t \in T$, and φ and ψ commute in the sense that :

$$\forall g \in G,\quad a_{g^{-1}tg} = (a_t)^{\varphi(g)},$$

so that G acts on X by permuting the elements $\psi(T)$. Lastly we require that the algebra X satisfies conditions $(2A)$ and $(3A)$ below.

Let $t_0,\ t_1,\ t_2,\ t_3 \in T$ with corresponding axes $a_{t_i} := \psi(t_i)$.

(2A) We define ρ to be the product t_0t_1. Then

(i) if $\rho \in T$ and the vectors a_{t_0}, a_{t_1} generate a dihedral subalgebra of type $2A$ then $a_\rho = \psi(\rho)$,

(ii) if $\rho^i \in T$ for ρ of order 4 or 6 and the axes a_{t_0} and a_{t_1} generate a subalgebra of type $4B$ or $6A$, then $\psi(\rho^i)$ coincides with the axis a_{ρ^i}.

(3A) If $\langle t_0, t_1\rangle \cong \langle t_2, t_3\rangle \cong D_6$ so that $\rho_1 := t_0t_1$ and $\rho_2 := t_2t_3$ have order 3, and if the following two conditions are satisfied:

(i) $\rho_1 = \rho_2$ or ρ_2^{-1}, and

(ii) the dihedral subalgebras generated by $\{a_{t_0}, a_{t_1}\}$ and $\{a_{t_2}, a_{t_3}\}$ have type $3A$,

then the corresponding $3A$-axial vectors u_{ρ_1} and u_{ρ_2} in the above subalgebras are equal in X.

The algebra X in the definition of a Majorana representation is clearly a Majorana algebra and we write $\langle\langle \psi(T) \rangle\rangle$ to mean X is generated by $\psi(T)$.

Remark 2.18. (i) In this thesis we assume conditions (2A) and (3A) to ensure a Majorana axis only depends on the cyclic subgroup $\langle\rho\rangle$ in the dihedral subalgebras of types $2A$ and $3A$, and not on the element ρ. Also any three involutions in T have their corresponding Majorana axes either generating the same dihedral algebra of type $2A$ or each pair of axes generates a dihedral algebra of type $2B$.

(ii) In [Ser12] and in other works on Majorana representations, some extra conditions akin to conditions (2A) and (3A), which are satisfied by $V_{\mathbb{M}}$, are also assumed in the definition of a Majorana representation (in addition to (2A) and (3A)).

(iii) In the above definition the elements of T must necessarily be 6-transpositions by Sakuma's Theorem 2.14.

We will often denote by $\mathcal{R} = (G, T, X)$ or simply $\mathcal{R} = (G, X)$ a Majorana representation $\mathcal{R}$ of G when the context is clear.

Definition 2.19. Let $\mathcal{R}_\mathcal{G} = (G, T_G, X)$ be a Majorana representation of G and let $H \subseteq G$ be a subgroup. Let $T_H \subset T_G$ such that T_H is a union of conjugacy classes of H and $\langle T_H \rangle = H$. Let $\mathcal{R}_\mathcal{H} = (H, T_H, Y)$ be a Majorana representation of H with Majorana algebra Y generated by the Majorana axes $\psi(T_H)$ such that $Y \subseteq X$. The Majorana representation $\mathcal{R}_\mathcal{H} = (H, T_H, Y)$ of H is called a **Majorana subrepresentation** of $\mathcal{R}_\mathcal{G}$.

2.4.2 Dimension and shape

Definition 2.20. Let $\mathcal{R} = (G, T, X)$ be a Majorana representation of G. The **dimension** of $\mathcal{R}$ is $dim(X)$ the dimension of X over $\mathbb{R}$.

Definition 2.21. We say that $\mathcal{R} = (G, T, X)$ is **based on an embedding** into $\mathbb{M}$ if there exists a monomorphism $\iota : G \hookrightarrow \mathbb{M}$ with $\iota(T) \subseteq 2A$ and such that X is isomorphic to the subalgebra of $V_{\mathbb{M}}$ generated by the $2A$-axes $\mathcal{C}(\iota(T))$.

If a Majorana representation $\mathcal{R} = (G, T, X)$ is based on an embedding into $\mathbb{M}$ then X is isomorphic to a subalgebra of $V_{\mathbb{M}}$ so we can easily bound above the dimension of $\mathcal{R}$.

Lemma 2.22. *Let $\mathcal{R} = (G,\ X)$ be a Majorana representation of G based on an embedding $\iota : G \hookrightarrow \mathbb{M}$ and let K be the centraliser $K := C_{\mathbb{M}}(\iota(G))$. Then $X \subseteq C_{V_{\mathbb{M}}}(K)$ so that*

$$dim(X) \leq dim(C_{V_{\mathbb{M}}}(K)).$$

Proof. From the definition of a Majorana representation the algebra X is generated by vectors indexed by elements of G and each $g \in G$ acts on X by conjugation of the indices. In particular X is an $\mathbb{R}G$-module. We can let K act on X in a similar way. Any $x \in X$ can be written $x := x_g$ for some $g \in \iota(G)$, and for any $k \in K$ we have $x_g^k = x_{g^k} = x_g$ since $K = C_{\mathbb{M}}(\iota(G))$, so that we have the inclusion of $\mathbb{R}K$-modules $X \subseteq C_{V_{\mathbb{M}}}(K)$. □

Is it important to note that for an arbitrary finite group G we cannot bound the number of Majorana representations of G, since we cannot assume that the map ψ describes the corresponding Majorana algebras uniquely, but the possible *shapes* of a Majorana representation of G can be enumerated.

Definition 2.23. The **shape** of a Majorana representation $\mathcal{R} = (G, T, X)$ is the tuple $(\Psi(d_1), \ldots, \Psi(d_n))$, where $\{d_i\}$ is the set of G-orbits representatives from the products $\{t_{1,i}t_{2,i}\}$ where $t_{1,i} \neq t_{2,i} \in T$ and the map Ψ maps each $d_i = t_{1,i}t_{2,i}$, to the type of the dihedral Majorana algebra generated by the axes $a_{t_{1,i}}$ and $a_{t_{2,i}}$. Also, because there is only one type of dihedral algebra associated with D_{10} and D_{12} respectively, we do not give the multiplicity of the types $5A$ and $6A$ in the shape.

Example 2.24. *Let $\mathcal{R} := (S_4, T, X)$ be a Majorana representation of the symmetric group S_4 where we take T to be the conjugacy class of the (2)-cycles and X be the Majorana algebra generated by the Majorana axes $\psi(T)$. Pairs of elements of T will generate dihedral subgroups conjugate to either $\langle (1,2),\ (3,4)\rangle \cong C_2 \times C_2$ or to $\langle (1,2),\ (2,3)\rangle \cong D_6$. Hence when constructing the algebra X we need to decide whether the subalgebra generated by $a_{(1,2)}$ and $a_{(3,4)}$ is of type $2A$ or $2B$, and whether the subalgebra generated by $a_{(1,2)}$ and $a_{(2,3)}$ is of type $3A$ or $3C$. Hence the possible shapes of $\mathcal{R}$ are $(2A, 3A)$, $(2B, 3A)$, $(2A, 3C)$ and $(2B, 3C)$.*
We note that if conditions (2A) and (3A) are dropped in the definition of a Majorana representation, then more shapes are possible.

2.4.3 The known Majorana representations

The first Majorana representations that were described are all based on embeddings into the Monster group. The existence of some embeddings is easy to prove by calculating with structure class constants, Definition 1.11, in the character table of $\mathbb{M}$. For example S_4 is a $(2,3,4)$ group which means it can be presented as $\langle\ g,\ h \mid g^2,\ h^3,\ (gh)^4\rangle$, so the existence of an embedding of S_4 into $\mathbb{M}$ is proved if there exist non-zero structure class constants S_{C_1,C_2,C_3} where C_1 is a conjugacy class of involutions of $\mathbb{M}$ and C_2 and C_3 are conjugacy classes of elements of order 3 and 4 respectively. Some other embeddings' existence is far less trivial. Fortunately invaluable information on embeddings into $\mathbb{M}$ can be read from [Nor98].

The classification of Majorana representations started with that of all Majorana representations of S_4 based on an embedding into $\mathbb{M}$ in [IPSS10]. Then followed the description of all Majorana representations of $L_3(2)$ and A_5 based on an embedding into $\mathbb{M}$, in [IS12b] and [IS12a] respectively. In [IPSS10], [IS12b] and [IS12a] the dimension of the representations considered are given, along with a basis $\mathcal{B}$ for the corresponding algebra, as well as inner product values on $\mathcal{B}$ and explicit expressions of the algebra products between elements of $\mathcal{B}$. In these early articles the emphasis was on developing Majorana calculus and calculations were performed using the subgroup structure and various combinatorial descriptions of the groups considered. In particular the use of a computer was kept to a minimum. This proved increasingly difficult as the size of the groups considered grew.
The hardest task is to find a generating set for the algebra of a Majorana representation, and prove that the algebra product is closed on that set. Indeed in [Iva11b] A. A. Ivanov describes a Majorana representation based on an embedding into $\mathbb{M}$ of A_6 and A_7 respectively; their dimensions are only given within 1 of the correct answer and explicit expressions for the algebra products on the chosen generating set for the algebra are not all given. The exact dimensions were eventually found by Á. Seress in [Ser12], along with expressions for the algebra products. Similarly the main result of [Dec14] together with information from [Ser12] gives the dimension and inner product values of a Majorana representation of $L_2(11)$ based on an embedding into $\mathbb{M}$, but the expression for the algebra products on a basis $\mathcal{B}$ for the corresponding algebra are not given in [Dec14].

A turning point in Majorana theory was reached when in [Ser12], Á. Seress described a generic theoretical procedure to construct 2-*closed* Majorana representation of a given finite group,

along with a *GAP* ([GAP08]) computer program implementing the procedure. A Majorana representation is defined as '2-closed' if the algebra product on the corresponding Majorana algebra is closed on the linear span of the set $\{a_t \cdot a_s \mid t, s \in T\}$, subject to two extra conditions called (4A) and (5A), which are akin to conditions (2A) and (3A), and require that any two dihedral subgroups of order 8 or 10 generated by involutions in T which intersect in a cyclic subgroup of order 4 or 5 have their corresponding dihedral subalgebras intersecting in a basis element. These conditions can be read on p.4 of [Ser12].

Not only did the *GAP* program confirm the information on the Majorana representations already classified but it also described new Majorana representations for the groups A_5, S_5, A_6, $3.A_6$, S_6, A_7 and the Mathieu group M_{11}, some of which are not based on an embedding into $\mathbb{M}$. When the procedure is successful for a particular representation, the program is able to give the algebra products with respect to a basis of the corresponding algebra, along with the dimension and inner product values. We note that the procedure makes repeated use of the Resurrection principle, 2.12, to find unknown inner product values and close the algebra product. The full potential of the procedure was sadly halted by the premature passing away of Á. Seress on the 13th of February 2013.

A final note on representations not based on an embedding in $\mathbb{M}$: in [Iva11a] A. A. Ivanov describes a potential Majorana representation of A_6 of dimension 70 which is not based on an embedding in $\mathbb{M}$. The existence of this representation was verified by Á. Seress in [Ser12].

Let us now summarise in Table 2.4 what is known of the Majorana representations of the groups S_4, A_5, S_5, A_6, $3.A_6$, S_6, A_7, $L_2(11)$ and M_{11}. It should be noted that for the groups S_4 and $L_2(11)$ all possible shapes for their Majorana representations, subject to conditions $(2A)$ and $(3A)$, have been classified. For the remaining groups this is not necessarily true; as far as the author is aware a Majorana representation of shape $(2B, 3A)$ of the group A_5 has not yet been investigated.

Remark 2.25. We explain the shape of the Majorana representation of S_6 given in row 15 of Table 2.4. The set T consists of the (2)-cycles and $(2,2)$-cycles. Products of two elements of T are in all possible conjugacy classes of S_6 but that of the (6)-cycles. Let $t,\ s \in T$; if the product ts is a (2)-cycle or a $(2,2)$-cycle then the Majorana algebra generated by a_t and a_s is of type $2A$, if ts is a $(2,2,2)$-cycle the algebra has type $2B$, if ts has order 3 the algebra has type $3A$, and if ts has order 4 the algebra has type $4B$.

No.	Group	$\lvert T\rvert$	Shape	Dimension	Embedding into $\mathbb{M}$	Reference(s)
1	S_4	$6+3$	$(2A^2, 3A, 4B)$	13	Y	[IPSS10]
2	S_4	$6+3$	$(2A^2, 3C, 4B)$	9	Y	[IPSS10]
3	S_4	6	$(2B, 3A)$	13	Y	[IPSS10]
4	S_4	6	$(2B, 3C)$	6	Y	[IPSS10]
5	S_4	$6+3$	$(2A, 2B, 3C, 4A)$	12	N	[Ser12]
6	S_4	6	$(2A, 3C)$	6	N	[Ser12]
7	A_5	15	$(2A, 3A, 5A)$	26	Y	[IS12a]
8	A_5	15	$(2A, 3C, 5A)$	20	Y	[IS12a]
9	A_5	15	$(2B, 3C, 5A)$	21	N	[Ser12]
10	S_5	$10+15$	$(2A^2, 3A, 4B, 5A, 6A)$	36	Y	[Ser12]
11	$L_3(2)$	21	$(2A, 3A, 4B)$	49	Y	[IS12b]
12	$L_3(2)$	21	$(2A, 3C, 4B)$	21	Y	[IS12b]
13	A_6	45	$(2A, 3A, 4B, 5A)$	76	Y	[Iva11b],[Ser12]
14	A_6	45	$(2A, 3C, 4B, 5A)$	70	N	[Iva11a],[Ser12]
15	S_6	$15+45$	$(2A^2, 2B, 3A^2, 4B^2, 5A, 6A)$	91	Y	[Ser12]
16	A_7	21	$(2A, 3A^3, 4B, 5A, 6A)$	196	Y	[Iva11b],[Ser12]
17	$L_2(11)$	55	$(2A, 3A, 5A, 6A)$	101	Y	[Dec14],[Ser12]
18	M_{11}	165	$(2A, 3A, 4B)$	286	Y	[Ser12]

TABLE 2.4: Known Majorana representations

2.4.4 Eigenvectors

In Table 2.5 presented on the next page, we give the expressions of some of the eigenvectors of a Majorana axis a belonging to one of the Majorana representations mentioned in the previous

section.

For space reasons we omitted the full expression for the eigenvector α_t^+ appearing in the last row of Table 2.5 but we explicate it here. The vector α_t^+ is a 0-eigenvector for a Majorana axis a_t belonging to the Majorana representation of shape $(2A, 3A, 5A)$ for the group A_5 [IS12a]. Let $H \cong A_5$, let T consists of the involutions of H, and let $\mathcal{R} = (H, T)$ be a Majorana representation of H of shape $(2A, 3A, 5A)$. We define $H^{(r)}$ to be a set of elements of order r in H containing one representative from every subgroup of order r, so that $|H^{(2)}| = 15$, $|H^{(3)}| = 10$, $|H^{(5)}| = 6$, where $H^{(5)}$ is contained in a single conjugacy class. For $g \in H$ we define $H_s^{(r)}(g) := \{h \mid h \in H^{(r)},\ o(gh) = s\}$.

Proposition 2.26. *Let $t \in T$ and let $H_2^{(2)}(t) = \{s_1, s_2\}$, $H_5^{(3)}(t) \cap H_2^{(3)}(s_1) = \{g_1, g_2\}$, and $H_5^{(3)}(t) \cap H_2^{(3)}(s_2) = \{g_3, g_4\}$. Then the element*

$$\alpha_t^+ := -\frac{19}{3^3 \cdot 5} a_t - \frac{2^3}{3 \cdot 5} a_{s_1} + \frac{2^6}{3^3 \cdot 5} \sum_{q \in H_3^{(2)}(t)} a_q + \frac{2^4}{3^2 \cdot 5}(a_{s_1 g_1} + a_{s_1 g_1^{-1}} + a_{s_1 g_2} + a_{s_1 g_2^{-1}})$$
$$- \frac{2^4}{3^2 \cdot 5}(a_{s_2 g_3} + a_{s_2 g_3^{-1}} + a_{s_2 g_4} + a_{s_2 g_4^{-1}}) + (u_{g_1} + u_{g_2}) + \sigma_{t,g_1} \frac{2^{12}}{3^3 \cdot 5} x_t.$$

is a 0-eigenvector of a_t, where σ_{t,g_1} is $+1$ or -1 depending on whether or not t and g_1 are conjugate in H. □

Group	Type/ Shape	0-eigenvector	$\frac{1}{2^2}$-eigenvector	$\frac{1}{2^5}$-eigenvector
D_4	2A	$a_0 + a_{-1} - \frac{1}{2^2}a_1$	$a_1 - a_{-1}$	
D_4	2B	a_t		
D_6	3C	$a_1 + a_{-1} - \frac{1}{2^5}a_0$		$a_1 - a_{-1}$
D_6	3A	$u_\rho - \frac{2\cdot5}{3^3}a_0 + \frac{2^5}{3^3}(a_1 + a_{-1})$	$u_\rho - \frac{2^3}{3^2\cdot5}a_0 - \frac{2^5}{3^2\cdot5}(a_1 + a_{-1})$	$a_1 - a_{-1}$
D_8	4B	$a_2 + a_{\rho^2} - \frac{1}{2^2}a_0$	$a_2 - a_{\rho^2}$	$a_1 - a_{-1}$
		$a_1 + a_{-1} - \frac{1}{2^2}a_{\rho^2}$		
D_8	4A	$v_\rho - \frac{1}{2}a_0 + 2(a_1 + a_{-1}) + a_2$, a_2	$v_\rho - \frac{1}{3}a_0 - \frac{2}{3}(a_1 + a_{-1}) - \frac{1}{3}a_2$	$a_1 - a_{-1}$
D_{10}	5A	$-\frac{3}{2^5}a_0 + a_1 + a_{-1} + a_2 + a_{-2}$	$w_\rho + \frac{1}{2^7}(a_1 + a_{-1} - a_2 - a_{-2})$	$a_1 - a_{-1}$
		$w_\rho - \frac{3\cdot7}{2^{12}}a_0 + \frac{7}{2^6}(a_2 + a_{-2})$		$a_2 - a_{-2}$
D_{12}	6A	$u_{\rho^2} + \frac{2}{3^2\cdot5}a_0 - \frac{2^8}{3^2\cdot5}(a_1 + a_{-1})$ $-\frac{2^5}{3^2\cdot5}(a_2 + a_{-2} + a_3 - a_{\rho^3})$	$u_{\rho^2} - \frac{2^3}{3^2\cdot5}a_0$ $-\frac{2^5}{3^2\cdot5}(a_2 + a_{-2} + a_3 - a_{\rho^3})$	$a_1 - a_{-1}$
A_4	(2A,3A)	$-\frac{2^2}{3^2}a_t + (u_h + u_{tht} + u_{th} + u_{th^2})$	$u_h + u_{tht} - u_{th} - u_{th^2}$	$a_2 - a_{-2}$
A_5	(2A,3A,5A)	α_t^+		

TABLE 2.5: Eigenvectors of Majorana axis a

2.4.5 Tri-generated Majorana Algebras

We let X be a Majorana algebra with set of Majorana axes A and we let $B \subseteq A$. We denote by $\langle\langle B\rangle\rangle$ the subalgebra of X generated by the set B. In this subsection we will prove the following.

Proposition 2.27. *All the Majorana algebras described in Table 2.4 are generated by three Majorana axes. Moreover for the groups S_4, A_5, S_5, S_6, $L_2(11)$ the Majorana algebras are generated by a dihedral Majorana algebra $\langle\langle a_t,\ a_s\rangle\rangle$ of type $2A$ or $2B$ together with another Majorana axis $a_r \notin \langle\langle a_t,\ a_s\rangle\rangle$.*

The remainder of this subsection is a proof of Proposition 2.27. We start by remarking that all of the aformentioned groups can be generated by three involutions by a result of G. Malle, J. Saxl and T. Weigel [MSW94]. We now state two well-known results telling us which of the aforementioned groups can be generated by three involutions, two of which commute. The first result was proved by M. Cherkassoff and D. Sjerve in [CS94], and the second one by V. D. Mazurov in [Maz03].

Theorem 2.28. *The following groups can be generated by three involutions, two of which commute:*

1) *the alternating groups A_n if and only if $n = 5$ or $n \geq 9$;*

2) *the symmetric groups S_n if and only if $n \geq 4$;*

3) *the projective special linear groups $L_2(q)$ if and only if $q \neq 2, 3, 7, 9$;*

4) *the projective general linear groups $PGL_2(q)$ if and only if $q \neq 2$.* □

Theorem 2.29. *Every sporadic finite simple group except the Mathieu groups M_{11}, M_{22}, M_{23} and the McLaughlin group McL can be generated by three involutions, two of which commute.* □

By the above two theorems the groups S_4, A_5, S_5, and $L_2(11)$ are generated by three involutions two of which commute, whereas A_6, S_6, A_7, $L_3(2)$, and M_{11} are not. Moreover from [Cox39] we have the presentations:

$$S_4 = \left\langle a, b, c \;\middle|\; a^2, b^2, c^2, (ab)^2, (ac)^3, (bc)^3, (abc)^4 \right\rangle,$$
$$A_5 = \left\langle a, b, c \;\middle|\; a^2, b^2, c^2, (ab)^2, (ac)^5, (bc)^5, (abc)^3 \right\rangle,$$
$$L_2(11) = \left\langle a, b, c \;\middle|\; a^2,\ b^2,\ (ab)^2,\ c^2,\ (ac)^5,\ (bc)^5,\ (abc)^5 \right\rangle.$$

Lemma 2.30. *The groups A_6, S_6, A_7, $L_3(2)$, $3.A_6$ and M_{11} can be generated by three involutions, and the groups A_6, S_6, A_7, and $L_3(2)$ afford the following presentations:*

$$\begin{aligned}
A_6 &= \left\langle a,b,c \;\middle|\; a^2, b^2, c^2, (ab)^4, (ac)^5, (bc)^5, (abc)^5, (a^cb)^4, ((ab)^cb)^4 \right\rangle,\\
S_6 &= \left\langle a,b,c \;\middle|\; a^2, b^2, c^2, (ab)^2, (ac)^6, (bc)^6, (abc)^5, (a^cb)^4, c^{acbc}\big((bc)^3\big)^{acbc}\big((bc)^3\big)^{acbcac} \right\rangle,\\
A_7 &= \left\langle a,b,c \;\middle|\; a^2, b^2, c^2, (ab)^3, (ac)^6, (bc)^4, (abc)^7, (b^ac)^5, (b^ca)^3 \right\rangle,\\
L_3(2) &= \left\langle a,b,c \;\middle|\; a^2, b^2, c^2, (ab)^4, (ac)^3, (bc)^3, (abc)^7 \right\rangle.
\end{aligned}$$

Proof. The presentations given for A_6, A_7, and $L_3(2)$ were derived from the presentations given in [CCN+85] which are:

$$\begin{aligned}
L_3(2) &= \left\langle d,e \;\middle|\; d^2, e^3, (de)^7, [d,e]^4 \right\rangle,\\
A_6 &= \left\langle d,e \;\middle|\; d^2, e^4, (de)^5, (de^2)^5 \right\rangle,\\
A_7 &= \left\langle d,e \;\middle|\; d^3, e^5, (de)^7, (dd^e)^2, (de^{-2}de^2)^2 \right\rangle.
\end{aligned}$$

For each of those presentations we find triples of generating involutions $\{a,\ b,\ c\}$ such that there exists two short words in $a,\ b,\ c$ satisfying the presentation of the [CCN+85]. We used Magma [BCP97] to find the order of the groups defined by those new presentations. For example for A_6 we can take $d = (2,6)(1,3)$ and $e = (1,4,6,3)(2,5)$ which satisfy the presentation given above. We rename c the involution d and we find that $e = ab$ where $a = (1,6)(2,5)$, $b = (1,4)(3,6)$, and clearly $(ab)^4 = 1$, and $(abc)^5 = ((ab)^2c)^5 = 1$. The relations $a^2 = b^2 = c^2 = (ab)^4 = (abc)^5 = ((ab)^2c)^5 = 1$ are not yet enough for Magma to compute the order of the group so we consider the four extra relations $(ac)^5 = (bc)^5 = (a^cb)^4 = ((ab)^cb)^4 = 1$ and Magma gives that the group thus presented has order $360 = |A_6|$.

From Lemma 3.22 of Chapter 3, the presentation for S_6 can easily be obtained from the presentation for $2 \times S_6$ and the expression given for its central element in terms of the generators. For $3.A_6$ we used a pair of generators as permutations in S_{18} from the online Atlas of finite groups representations [ABL+99]. We note that one way to embed $3.A_6$ in S_{18} is through the faithful action of $3.A_6$ on the 18 codewords of length 6 from the hexacode [CS88]. We wrote a short function 'Triangle' (see Appendix A) with Magma to find a triple of generating involutions for $3.A_6$:

$$(1,10)(2,18)(3,12)(4,5)(8,15)(9,17),\ (1,16)(3,11)(4,6)(5,14)(7,12)(10,13),$$

$$\text{and } (4,7)(6,10)(11,17)(12,13)(14,18)(15,16).$$

Similarly for M_{11} we found the triple:

$$(1,4)(2,8)(3,7)(9,10),\ (1,3)(2,11)(6,7)(8,10), \text{ and } (2,5)(3,10)(6,7)(9,11).$$

□

The next lemma finishes the proof of Proposition 2.27.

Lemma 2.31. *The groups S_4, A_5, S_5, A_6, $3.A_6$, S_6, A_7, $L_3(2)$, $L_2(11)$ and M_{11} can be generated by three involutions whose conjugacy classes are included in the set T for the Majorana representations described in Table 2.4.*

Proof. The lemma is trivially true for all the groups, except S_4, S_5 and S_6, since they possess a single conjugacy class of involutions. The group S_4 can be generated by three (2)-cycles; $(1,2)$, $(2,3)$ and $(3,4)$, which must be contained in T. Similarly for S_5 one can observe that $(1,2)(3,4)$, $(1,3)(2,4)$ and $(4,5)$ generate S_5 (taking the products of two or three of the generators we get a group whose order is divisible by 30 and contains (2)-cycles as well as $(2,2)$-cycles so it must be S_5), and must be included in T for the Majorana representation described in Table 2.4. Similarly for S_6 can be generated by the involutions $(1,3)(4,6)$, $(1,2)(3,6)$ and $(4,5)$, all of which are clearly contained in T. □

Remark 2.32. From Corollary 3.47 of Chapter 3 the group S_5 can be presented as:

$$S_5 = \left\langle a,b,c \;\middle|\; a^2, b^2, c^2, (ab)^2, (ac)^6, (bc)^6, (abc)^6, (ab^c)^5, (aba^c)^5, (abb^c)^5, (cb^{ca})^4, (c^a c^{bc})^2 \right\rangle.$$

Chapter 3

The 6-transposition Coxeter groups $G^{(m,n,p)}$

3.1 Motivation and Main Theorem

3.1.1 Tri-generated Majorana algebras and property (σ)

If at all possible, the classification of all Majorana representations generated by three Majorana axes is a gigantic task. Indeed, just the number of subalgebras of $V_{\mathbb{M}}$ generated by three $2A$-axes is very large since the number of different conjugacy classes of subgroups of $\mathbb{M}$ generated by three $2A$ involutions is huge. This can be gauged from the work of S. P. Norton in [Nor13]; he classifies all nets in the Monster, which are triples of $2A$ involutions $t,\ s,\ r$ in $\mathbb{M}$ up to *braiding*, and up to the product rst having order less or equal to 7. There are over 230 such nets in $\mathbb{M}$, and so over 230 conjugacy classes of subgroups of $\mathbb{M}$ generated by a triple of $2A$ involutions.

As mentioned in the introduction, this thesis investigates Majorana algebras U generated by three Majorana axes $a_1,\ a_2,\ a_3$ such that U also contains a Majorana axis $a_{1,2}$ with associated Majorana involution $\tau(a_{1,2}) = \tau(a_1)\tau(a_2)$. These tri-generated algebras can also be described as Majorana algebras generated by a dihedral Majorana algebra $\langle\langle a_1,\ a_2\rangle\rangle$ of type $2A$ and another Majorana axis a_3 not necessarily contained in $\langle\langle a_1,\ a_2\rangle\rangle$.
The algebras U are invariant under the group G generated by the Majorana involutions $\tau(a_1)$, $\tau(a_2)$ and $\tau(a_3)$ where $\tau(a_1)$ and $\tau(a_2)$ commute, and by remark 2.15 the product of any two involutions each conjugate to either of $\tau(a_1),\ \tau(a_2),\ \tau(a_1)\tau(a_2)$, or $\tau(a_3)$ has order no greater

than 6. Hence the classification of the Majorana algebras U can be derived from the description of the Majorana representations of all the groups satisfying the following property.

Property (σ). *A group G has property (σ) if it satisfies each of the following two conditions:*

(i) *G is generated by three elements $a,\ b,\ c$ of order dividing 2, two of which commute, say $ab = ba$;*

(ii) *for any two elements $t,\ s$ in $T := a^G \cup b^G \cup (ab)^G \cup c^G$ the product ts has order at most 6.*

Hence to start the classification of tri-generated Majorana algebras we tried and succeeded in classifying all groups G which have property (σ).

Remark 3.1. In the above definition we do not insist that the three elements are involutions, nor that they are distinct.

3.1.2 Main theorem

A priori we did not expect to find explicitly all groups having (σ) and we certainly did not expect all of them to be finite.

In order to classify all groups satisfying (σ) we can classify all quotients of the Coxeter groups $G^{(m,n,p)}$ for $2 \leq m,\ n,\ p \leq 6$, where $G^{(m,n,p)}$ is defined by the presentation;

$$G^{(m,n,p)} := \langle a, b, c \mid a^2,\ b^2,\ c^2,\ (ab)^2,\ (ac)^m,\ (bc)^n,\ (abc)^p \rangle,$$

and such that the product of any two elements each conjugate to either of $a,\ b,\ ab,\ c$ has order no greater than 6. For $2 \leq m,\ n,\ p \leq 6$ it is known which $G^{(m,n,p)}$ groups are finite or infinite. We give a complete summary in the next section 3.2 and we observe that all the finite $G^{(m,n,p)}$ groups satisfy property (σ). To tackle the infinite cases, we introduce five relations $R_1^{r_1} = 1,\ R_2^{r_2} = 1,\ R_3^{r_3} = 1,\ R_4^{r_4} = 1$ and $R_5^{r_5} = 1$, where;

$$R_1 := a \cdot b^c,\quad R_2 := ab \cdot b^c,\quad R_3 := ab \cdot a^c,\quad R_4 := c \cdot b^{ca}, \text{ and } R_5 := c^a \cdot c^{bc}.$$

For all i we must have that $r_i \in [1, 6]$ otherwise the quotient of $G^{(m,n,p)}$ by a relation $R_i^{r_i} = 1$ would not satisfy (σ). In sections 3.2 and 3.3, we quotient each infinite $G^{(m,n,p)}$ group by some or all of the five relations $R_i^{r_i} = 1$, and we obtain a list of finite $G^{(m,n,p)}$ quotients for all $r_i \in [1, 6]$ and we show which of them satisfy (σ).

Our original wish was to classify all Majorana algebras U generated by three Majorana axes

$a_1,\ a_2,\ a_3$ such that U also contains a Majorana axis $a_{1,2}$ with associated Majorana involution $\tau(a_{1,2}) = \tau(a_1)\tau(a_2)$. Eventually we would like to determine which of those Majorana algebras U are based on an embedding in $\mathbb{M}$ as in Definition 2.21. For this reason we would like to know for which of the $G^{(m,n,p)}$ quotients Q satisfying $(\boldsymbol{\sigma})$ there exists an embedding $\iota : Q \hookrightarrow \mathbb{M}$ such that the $\mathbb{M}$-conjugacy class of $\iota(a),\ \iota(b),\ \iota(c)$ and $\iota(ab)$ is $2A$. This prompts the following definition.

Definition 3.2. We say that a quotient Q of a $G^{(m,n,p)}$ group **$2A$-embeds** in $\mathbb{M}$ if there exists a monomorphism $\iota : Q \hookrightarrow \mathbb{M}$ such that $\iota(a),\ \iota(b),\ \iota(c)$ and $\iota(ab)$ are in the conjugacy class $2A$ of $\mathbb{M}$.

In Table 3 of [Nor85] S. P. Norton lists all $G^{(m,n,p)}$ quotients that can be $2A$-embedded into $\mathbb{M}$ up to conjugacy in $\mathbb{M}$, so we can easily deduce which groups satisfying $(\boldsymbol{\sigma})$ $2A$-embed in $\mathbb{M}$. In the next subsection we will explain his table and reproduce it in Table 3.2. The following theorem is the main result of this chapter. It will be proved in sections 3.2 and 3.3.

Theorem 3.3. *A group has property* $(\boldsymbol{\sigma})$ *if and only if it is a quotient of at least one of the following* 11 *groups:*

Name	Isomorphism Type	$G^{(m,n,p)}$ (m,n,p)	Added relations $R_i^{r_i} = 1$ $(r_1, r_2, r_3, r_4, r_5)$	$2A$-embeds in $\mathbb{M}$	Largest $2A$-embedded quotient	Centre Order	Subgroups
G_1	$2\ wr\ 2^2$	$(4,4,4)$		Y$(18,25)$		2	
G_2	$(S_3 \times S_3) : 2^2$	$(4,4,6)$		Y(19)		2	
G_3	$2^4 : D_{10}$	$(4,5,5)$		Y$(21,27)$		1	
G_4	$2 \times S_5$	$(4,5,6)$		Y(22)		2	
G_5	$L_2(11)$	$(5,5,5)$		Y(33)		1	
G_6	$(2^4 :_{\phi_1} D_{12}) \times 2$	$(4,6,6)$	$(4,-,-,-,-)$	Y(30)		2	
G_7	$2^4 :_{\lambda_2} A_5$	$(6,5,5)$	$(5,-,-,-,-)$	Y(32)		1	G_3
G_8	$2 \times S_6$	$(6,6,5)$	$(4,-,-,-,-)$	Y(34)		2	G_2, G_4
G_9	$\big(2^4 : (S_3 \times S_3)\big) \times 2$	$(6,6,6)$	$(4,-,-,-,-)$	N	$2^4 : (S_3 \times S_3)$, (36)	2	
G_{10}	$2^5 :_{\phi} S_5$	$(6,6,6)$	$(5,\ 5,\ 5,\ 4,-)$	Y(37)		2	G_3, G_4, G_6
G_{11}	$(3^4 : 2) : (3_+^{1+2} : 2^2)$	$(6,6,6)$	$(6,\ 6,\ 6,-,\ 3)$	N	$3_+^{1+2} : 2^2$, (16)	1	

TABLE 3.1: The groups satisfying $(\boldsymbol{\sigma})$

We give a brief example of how to read Table 3.1. The group G_6 is a quotient of $G^{(4,6,6)}$ by the relation $R_1^4 = (acbc)^4 = 1$. It $2A$-embeds in $\mathbb{M}$ as described in row 30 of Norton's Table 3.2, and its centre has order 2.

Remark 3.4. We present now some precisions on the split extensions in Table 3.1 which will be proved in the next sections:

for G_3 : there is a unique non-trivial split extension $2^4 : D_{10}$;

for G_6 : there are two conjugacy classes of non-trivial split extensions $2^4 :_{\phi_i} D_{12}$, $i = 1, 2$, where ϕ_1 comes from the inclusion $E_1 := \langle (1,2)(3,4), (3,5)(7,8) \rangle \subset A_8 \cong GL_4(2)$ and ϕ_2 from $E_2 := \langle (1,2)(3,4)(5,6)(7,8), (3,5)(6,8) \rangle \subset A_8 \cong GL_4(2)$;

for G_7 : there are two conjugacy classes of non-trivial split extensions $2^4 :_{\lambda_i} A_5$, $i = 1, 2$, where λ_1 arises from the isomorphism $A_5 \cong SL_2(4)$ whereas λ_2 arises from the isomorphism $A_5 \cong P\Omega_4^-(2)$;

for G_{10} : modulo the centre of the group, the action ϕ arises from the isomorphism $A_5 \cong SL_2(4)$.

Remark 3.5. (i) In Theorem 3.3 we write each of the groups listed as a quotient of a $G^{(m,n,p)}$ group, but not necessarily uniquely. For example $L_2(11)$ can also be written as a quotient of $G^{(6,6,5)}$ from Theorem 3.15 of the next section.

(ii) A very helpful first step when attempting to find the Majorana representations of the groups G_1 to G_{11} above, is to first describe any Majorana subrepresentations they might have, Definition 2.19, so the 'Subgroups' column of Table 3.1 is particularly useful.

3.1.3 The tri-generated $2A$ subgroups of $\mathbb{M}$

In [Nor85] S. P. Norton produced a list of all 'triangle-point' configurations in the graph Γ of commuting $2A$ involutions of $\mathbb{M}$, where two $2A$ involutions are joined by an edge if they commute. If a, b and ab are three commuting $2A$ involutions, so that they form a triangle in Γ, and if $c \in 2A$ then S. P. Norton found all possible triples of conjugacy classes in $\mathbb{M}$ in which the products ac, bc, abc can lie. The subgroups of $\mathbb{M}$ generated by these triples (a, b, c) necessarily satisfy $(\boldsymbol{\sigma})$ by the 6-transposition property of the $2A$ involutions (2.1). In Table 3 of [Nor85] S. P. Norton gives the 37 different orbits representatives of triples (a, b, c) of $2A$ involutions and for each representative one can read the isomorphism type of the group generated by (a, b, c) and

the conjugacy classes in $\mathbb{M}$ of ac, bc and abc, along with other useful information. We reproduce part of his table in Table 3.2 on the next page.

We explain the meaning of column 5 of Table 3.2 called 'Ancestors'. In [Nor85] S. P. Norton defines for each representative triple (a, b, c), the following three subgroups of $\langle a, b, c\rangle$:

$$A_1 := \langle a,\ b,\ a^c\rangle,\ A_2 := \langle a,\ b,\ b^c\rangle \text{ and } A_3 := \langle a,\ b,\ (ab)^c\rangle,$$

which are called the *ancestors subgroups*. Column 5 gives the three rows of Table 3.2 which contain a subgroup of $\mathbb{M}$ conjugate to A_1, A_2 and A_3 respectively.

No.	Order	Iso. Type	Classes of $ac,\ bc,\ abc$	Ancestors	No.	Order	Iso. Type	Classes of $ac,\ bc,\ abc$	Ancestors
1	4	2^2	$(1A\ 2A\ 2A)$	$(1,1,1)$	20	32	$2^4.2$	$(4A\ 4B\ 4B)$	$(8,2,2)$
2	8	2^3	$(2A\ 2A\ 2B)$	$(1,1,1)$	21	160	$2^4.D_{10}$	$(4A\ 5A\ 5A)$	$(8,27,27)$
3	12	$2\times S_3$	$(2A\ 3A\ 6A)$	$(1,3,3)$	22	240	$2\times S_5$	$(4A\ 5A\ 6A)$	$(9,22,11)$
4	16	$2\times D_8$	$(2A\ 4A\ 4A)$	$(1,2,2)$	23	96	$2^2\times S_4$	$(4A\ 6A\ 6A)$	$(7,11,11)$
5	8	D_8	$(2A\ 4B\ 4B)$	$(1,1,1)$	24	192	$2^4.D_{12}$	$(4A\ 6A\ 6A)$	$(8,10,10)$
6	8	2^3	$(2B\ 2B\ 2B)$	$(1,1,1)$	25	64	$2^4.2^2$	$(4B\ 4B\ 4B)$	$(4,4,4)$
7	16	$2\times D_8$	$(2B\ 4A\ 4A)$	$(1,2,2)$	26	72	$3^2.D_8$	$(4B\ 4B\ 6A)$	$(3,3,13)$
8	16	$2\times D_8$	$(2B\ 4B\ 4B)$	$(1,2,2)$	27	160	$2^4.D_{10}$	$(4B\ 5A\ 5A)$	$(4,21,21)$
9	24	$2^2\times S_3$	$(2B\ 6A\ 6A)$	$(1,3,3)$	28	120	S_5	$(4B\ 5A\ 6A)$	$(3,28,10)$
10	24	S_4	$(3A\ 3A\ 4B)$	$(10,10,5)$	29	48	$2\times S_4$	$(4B\ 6A\ 6A)$	$(5,10,10)$
11	48	$2\times S_4$	$(3A\ 4A\ 6A)$	$(11,7,11)$	30	384	$2^5.D_{12}$	$(4B\ 6A\ 6A)$	$(4,11,11)$
12	60	A_5	$(3A\ 5A\ 5A)$	$(12,12,12)$	31	660	$L_2(11)$	$(5A\ 5A\ 5A)$	$(33,33,33)$
13	36	$S_3\times S_3$	$(3A\ 6A\ 6A)$	$(13,3,3)$	32	960	$2^4.A_5$	$(5A\ 5A\ 6A)$	$(32,32,12)$
14	24	S_4	$(3C\ 3C\ 4B)$	$(14,14,5)$	33	660	$L_2(11)$	$(5A\ 6A\ 6A)$	$(31,12,12)$
15	60	A_5	$(3C\ 5A\ 5A)$	$(15,15,15)$	34	1440	$2\times S_6$	$(5A\ 6A\ 6A)$	$(34,11,11)$
16	108	$3^{1+2}.2^2$	$(3C\ 6A\ 6A)$	$(16,3,3)$	35	120	S_5	$(6A\ 6A\ 6A)$	$(12,12,12)$
17	32	$2^2\ wr\ 2$	$(4A\ 4A\ 4A)$	$(6,6,6)$	36	576	$\frac{1}{2}.S_4\ wr\ 2$	$(6A\ 6A\ 6A)$	$(13,11,11)$
18	64	$2^3.2^3$	$(4A\ 4A\ 4B)$	$(7,7,4)$	37	3840	2^5S_5	$(6A\ 6A\ 6A)$	$(12,12,12)$
19	144	$2\times 3^2.D_8$	$(4A\ 4A\ 6A)$	$(9,9,13)$					

TABLE 3.2: The $G^{(m,n,p)}$ quotients embedding in $\mathbb{M}$ with $a,\ b,\ ab,\ c\in 2A$

3.2 The 6-transposition quotients of the $G^{(m,n,p)}$ groups

3.2.1 Introduction

The groups $G^{(m,n,p)}$ are one of the three families of groups studied by H. S. M. Coxeter in [Cox39]. By symmetry of the presentation for $G^{(m,n,p)}$, any permutation of $\{m,n,p\}$ does not change the isomorphism type of $G^{(m,n,p)}$, so we can assume that $m \leq n \leq p$ without loss of generality. In [Cox39] H. S. M. Coxeter noted the following relationship between the groups $G^{(m,n,p)}$ and another family of groups.

Proposition 3.6. *The group* $G^{(2,m,n;q)}$ *defined by the presentation:*

$$\langle r,\ s \mid r^2,\ s^m,\ (rs)^n,\ [r,\ s]^q \rangle$$

has index 2 *in the group* $G^{(m,n,2q)}$ *under the mapping* $r \to ab,\ s \to ac.$ □

Using Tietze transformations, the above proposition, and a criterion for the group $G^{(m,n,p)}$ to be finite or infinite, H. S. M. Coxeter computed the orders of some of the $G^{(m,n,p)}$ groups. We state below this criteria called 'Theorem E' in [Cox39].

Proposition 3.7. *Suppose that* $m,\ n,\ p$ *satisfy the following two conditions:*

(i) $m > 2,\ n > 3,$

(ii) $m,\ n,\ p$ *are either all even or one even and the other two equal.*

Then the group $G^{(m,n,p)}$ *is finite if and only if* $cos(\frac{2\pi}{m}) + cos(\frac{2\pi}{n}) + cos(\frac{2\pi}{p}) < 1.$ □

We define $\mathcal{S}$ to be the set of triples $\mathcal{S} := \{(4\ ,6\ ,6\ ),\ (5,\ 5,\ 6),\ (6,\ 6,\ 6)\}$ and we let $2 \leq m \leq n \leq p \leq 6$. From Proposition 3.7 if $(m,n,p) \in \mathcal{S}$ then the group $G^{(m,n,p)}$ is infinite and if $(m,n,p) \notin \mathcal{S} \cup \{(5,\ 6,\ 6)\}$ then the group is finite. The only case not dealt with by Proposition 3.7 is $(m,n,p) = (5,\ 6,\ 6)$. The group $G^{(5,6,6)}$ was proved to be infinite by M. Edjvet as a consequence of his 'Main Theorem' in [Edj94]. His result relies on the method of 'pictures' for a finitely presented group and arguments from topology and cohomology. More exactly the result in [Edj94] is that $G^{(2,5,6;3)}$ is infinite, which by Proposition 3.6 proves that $G^{(5,6,6)}$ is infinite. His proof relies on two lemmas; firstly Lemma 3.2 part (iv) states that the picture for the presentation of $G^{(2,5,6;3)}$ is 'quasi-aspherical' over $C_2 * C_5$, then Lemma 5.1 part (ii) uses cohomological arguments to show that given a quasi-aspherical picture for $G^{(2,5,6;3)}$

we can deduce the group is infinite. We refer the reader to [Edj94] or [HT93] for a detailed explanation of the definition and use of pictures. We can now state the following more precise result.

Proposition 3.8. *Let* $2 \leq m \leq n \leq p \leq 6$. *The group* $G^{(m,n,p)}$ *is finite if and only if* $(m,n,p) \notin \{(4\ ,6\ ,6\ ),\ (5,\ 5,\ 6),\ (5,\ 6,\ 6),\ (6,\ 6,\ 6)\}$. □

3.2.2 The finite 6-transposition $G^{(m,n,p)}$ groups

The orders of the finite groups $G^{(m,n,p)}$ where $2 \leq m \leq n \leq p \leq 6$ are all known. The table in the proposition below, and the following proposition, are based on Table 1 of [EJ08] which content relies on the work of H. S. M. Coxeter [Cox39].

Proposition 3.9. *For* $2 \leq m \leq n \leq p \leq 6$ *the groups* $G^{(m,n,p)}$ *which are finite have orders as presented in Table 3.3.* □

(m,n)	p	Order	(m,n)	p	Order	(m,n)	p	Order
(2, 2)	2, 4, 6	8	(2, 5)	5	10	(3, 5)	5	60
(2, 2)	3, 5	4	(2, 5)	6	4	(3, 5)	6	2
(2, 3)	3	6	(2, 6)	6	24	(3, 6)	6	108
(2, 3)	4	4	(3, 3)	3, 5	1	(4, 4)	4	64
(2, 3)	5	2	(3, 3)	4	24	(4, 4)	5	4
(2, 3)	6	12	(3, 3)	6	6	(4, 4)	6	144
(2, 4)	4	16	(3, 4)	4	4	(4, 5)	5	160
(2, 4)	5	4	(3, 4)	5	2	(4, 5)	6	240
(2, 4)	6	8	(3, 4)	6	48	(5, 5)	5	660

TABLE 3.3: Orders of the finite $G^{(m,n,p)}$ groups satisfying $(\boldsymbol{\sigma})$

Proposition 3.10. *If* p *is even the group* $G^{(2,n,p)}$ *has order* $2 \cdot gcd(n, 2p)$, *otherwise it has order* $4 \cdot gcd(n,p)$. □

We now give in Proposition 3.11 the less obvious isomorphism types of the finite $G^{(m,n,p)}$ groups from Proposition 3.9 and in Proposition 3.12 we prove that they all satisfy property $(\boldsymbol{\sigma})$.

Proposition 3.11. *The isomorphism types for the finite* $G^{(m,n,p)}$ *groups which are not dihedral or abelian groups are as in Table 3.4.*

(m,n,p)	Order	Isomorphism Type	Generators $a,\ b,\ c$	In Norton's list (Orbit no.)	Classes in $\mathbb{M}$
$(2,4,4)$	16	$D_8 \times 2$	$(2,3),\ (1,4)(5,6),\ (1,2)(3,4)$	Y(4) Y(7) Y(8)	$(2A,4A,4A)$ $(2B,4A,4A)$ $(2B,4B,4B)$
$(2,6,6)$	24	$D_{12} \times 2$	$(2,3),\ (2,3)(6,7),\ (1,2)(4,5)$	Y(9)	$(2B,6A,6A)$
$(3,3,4)$	24	S_4	$(1,2),\ (3,4),\ (1,3)$	Y(10)	$(3A,3A,4B)$
$(3,4,6)$	48	$S_4 \times 2$	$(3,4)(5,6),\ (1,2)(3,4)(5,6),$ $(1,3)(5,6)$	Y(11)	$(3A,4A,6A)$
$(3,5,5)$	60	A_5	$(1,2)(3,4),\ (1,3)(2,4),$ $(1,5)(3,4)$	Y(12) Y(15)	$(3A,5A,5A)$ $(3C,5A,5A)$
$(3,6,6)$	108	$3^{1+2}_{+} : 2^2$	$(x_1,\ \phi),\ (x_1^2x_2,\ \psi),$ $(x_1x_2, \phi\psi)$	Y(16)	$(3C,6A,6A)$
$(4,4,4)$	64	$2\ wr\ 2^2$	$s,\ t,\ v_1$	Y(18) Y(25)	$(4A,4A,4B)$ $(4B,4B,4B)$
$(4,4,6)$	144	$(S_3 \times S_3) : 2^2$	$\alpha,\ \alpha\beta,\ (2,3)$	Y(19)	$(4A,4A,6A)$
$(4,5,5)$	160	$2^4 : D_{10}$	$e_3(1,2)(3,4),\ e_1+e_4,\ (1,3)(4,5)$	Y(21) Y(27)	$(4A,5A,5A)$ $(4B,5A,5A)$
$(4,5,6)$	240	$S_5 \times 2$	$(1,2),\ (3,4)(6,7),$ $(1,3)(2,5)(6,7)$	Y(22)	$(4A,5A,6A)$
$(5,5,5)$	660	$L_2(11)$	$(1,4)(5,9)(7,8)(10,11),$ $(3,6)(5,8)(7,9)(10,11),$ $(1,5)(2,7)(3,9)(8,10)$	Y(31)	$(5A,5A,5A)$

TABLE 3.4: The finite non-abelian and non-dihedral $G^{(m,n,p)}$ groups

We explain the content of Table 3.4 of Proposition 3.11. Column 4 gives a set of generators $a,\ b,\ c$ for $G^{(m,n,p)}$, which are either elements of a permutation group or which notation can be read from the proof of 3.11. Column 5 answers whether the group $G^{(m,n,p)}$ in that row is isomorphic to one of the groups in Norton's Table 3.2, which means the group $2A$-embeds in $\mathbb{M}$. If the group $2A$-embeds in $\mathbb{M}$ then column 6 gives the conjugacy classes in $\mathbb{M}$ of the products $ac,\ bc$ and abc.

Proof. In this proof we show the isomorphism types of the groups which were not described explicitly by H. S. M. Coxeter or by M. Edjvet. They are the four cases:

$$(m,n,p) \in \{(3,6,6),\ (4,4,4),\ (4,4,6),\ (4,5,5)\}.$$

Case $(m,n,p) = (3,6,6)$

The group $G^{(3,6,6)}$ is of the form $3_+^{1+2} : 2^2$, which we prove by construction. We start by letting $\{x_1,\ x_2\}$ be a generating set for $N := 3_+^{1+2}$, an extraspecial group of order 27, exponent 3 (called '+' type) so that its centre is $Z(N) = \Phi(N) \cong 3$ and $N/Z(N) \cong 3^2$. We let $z := [x_1, x_2]$ where $\langle z \rangle = Z(N)$. It is a well-known fact that $Aut(N) = (Inn(N) : Sp_2(3)) : \langle \theta \rangle$, where:

$$Inn(N) \cong N/Z(N),$$
$$Sp_2(3) \cong SL_2(3) \cong Q_8 : 3,$$
$$Sp_2(3).\langle \theta \rangle \cong GL_2(3)$$

and θ is an automorphism of order 2 sending one of the generators of N to its square, and centralising the other generator. Hence without loss of generality we let $\theta : x_1 \to x_1^2,\ x_2 \to x_2$, and we let $K := \langle \phi,\ \psi \rangle \cong 2^2$ be a subgroup of $Aut(N)$ not containing θ where:

$$\phi :\ x_1 \to x_1^2 \qquad\qquad \psi :\ x_1 \to x_2$$
$$x_2 \to x_2^2 \qquad\qquad x_2 \to x_1$$

If we let $a,\ b,\ c$ be equal to $(x_1,\ \phi),\ (x_1^2 x_2,\ \psi),\ (x_1 x_2,\ \phi\psi)$ respectively, then the group generated by $a,\ b,\ c$ satisfies the same presentation as $G^{(6,6,3)} \cong G^{(3,6,6)}$ so by order comparison they must be isomorphic. We also remark that $\langle (ac)^2, (bc)^2 \rangle \cong 3_+^{1+2}$ and $\langle a, b \rangle \cong 2^2$.

Case $(m,n,p) = (4,4,4)$

The group $G^{(4,4,4)}$ is isomorphic to the wreath product $2\ wr\ 2^2$ where the action is given by the regular representation of 2^2 on the direct product of four copies of 2. This group can be constructed as the semidirect product of a group $N \cong 2^4$ by a group $K \cong 2^2$. We take K to be generated by two involutions s and t and we write N additively over the field $GF(2)$. We let $\{v_1,\ v_s,\ v_t,\ v_{st}\}$ be a basis for N and we let K act on N by left multiplication on the indices of the v_i's. Hence one can then take the generators $a,\ b,\ c$ of $G^{(4,4,4)}$ to be $s,\ t$ and v_1. Lastly one should note that we can let K be equal to $\langle a, b \rangle$ and N be the normal closure of c in $G^{(4,4,4)}$ so that $N = \langle c \rangle \times \langle c^a \rangle \times \langle c^b \rangle \times \langle c^{ab} \rangle$.

Case $(m,n,p) = (4,4,6)$

We prove by construction that the group $G^{(4,4,6)}$ is isomorphic to $(S_3 \times S_3) : 2^2$. We let $G := N : K$ where $N \cong S_3 \times S_3$ and $K \cong 2^2$. We define $N := N_1 \times N_2 \cong S_3 \times S_3$ where we take $N_1 := \langle (1,2),\ (2,3) \rangle$ and $N_2 := \langle (4,5),\ (5,6) \rangle$. There are five conjugacy classes of S_3 subgroups in N with representatives $N_1,\ N_2,\ N_3 := \langle (1,2)(4,5),\ (1,2,3) \rangle,\ N_4 := \langle (1,2)(4,5),\ (4,5,6) \rangle,\ N_5 := \langle (1,2)(4,5),\ (1,2,3)(4,6,5) \rangle$ of sizes 1, 1, 3, 3 and 6 respectively. Clearly $Inn(N_1 \times N_2) \cong S_3 \times S_3$ and an outer automorphism would send $\{1,2,3\}$ to $\{4,5,6\}$, for example one can define an involution α which sends $1 \leftrightarrow 4,\ 2 \leftrightarrow 5,\ 3 \leftrightarrow 6$ so that $\alpha : N_1 \leftrightarrow N_2,\ N_3^G \leftrightarrow N_4^G,\ N_5^G \leftrightarrow N_5^G$. From the sizes of the conjugacy classes of S_3 subgroups, there are clearly no other outer automorphisms than α modulo the inner automorphism group. Hence we can deduce $Aut(S_3 \times S_3) \cong (S_3 \times S_3) : 2$. We define $K := \langle \alpha,\ \beta \rangle$ where β is conjugation by $(1,2)(4,5)$ and α is as above. We can take as the generators $a,\ b,\ c$ of $G^{(4,4,6)}$ the elements $\alpha,\ \alpha\beta$ and $(2,3)$, so by order comparison $G \cong G^{(4,4,6)}$.

Case $(m,n,p) = (4,5,5)$

The group $G^{(4,5,5)}$ is isomorphic to $2^4 : D_{10}$. We give a direct argument. First we let N be the normal closure of the involution a in $G^{(4,5,5)}$ and we notice that $G^{(4,5,5)}/N \cong \langle b,\ c \rangle \cong D_{10}$ so that $|N| = 16$ since $|G^{(4,5,5)}| = 160$. The subgroup N must contain the elements $\{a, a^c, a^{cb}, a^{cbc}\}$, where a commutes with a^c, since ac has order 4, and with a^{cb}, since $a \cdot a^{cb} = ((ac)^2)^b$. The order of $a \cdot a^{cbc} = (a \cdot b^c)^2$ is a power of 2 since $|N|$ is. Hence the element $a \cdot b^c$ must have order greater than 2, otherwise $|N| = 4$, and it must be less or equal to 8 to avoid $|N| > 16$. We let $K := \langle a, b, a^c \rangle$ which is a quotient of a group $G^{(2,n,p)}$ since $(ac)^2$ has order 2, where n and p are the orders of $b \cdot a^c$ and $ab \cdot a^c$ respectively, so that $n \in \{4,8\}$ by our previous remark, and $p \in \{1,2,4,5,8,10\}$ since $|G^{(4,5,5)}| = 160$. From Proposition 3.9 the integer p cannot be equal to 1 otherwise $|G^{(4,5,5)}| < 160$ and p cannot be equal to 2 otherwise K is a quotient of 2^3 which would imply ac has order 2 so that $G^{(4,5,5)}$ is a quotient of $G^{(2,5,5)} \cong D_{10}$, a contradiction. Similarly from Proposition 3.10 we cannot have $p \in \{5,10\}$ otherwise K is quotient of 2^3. Hence $n,p \in \{4,8\}$. If $n = p = 8$ then by Proposition 3.10 the order $|K|$ is divisible by 32 which is impossible. If $\{n,p\} = \{4,8\}$ then $K \cong G^{(2,4,8)} \cong G^{(2,8,4)}$ which has the same order as $G^{(2,4,4)}$ by 3.10, so actually $n = p = 4$ and so $a \cdot a^{cbc}$ has order 2. Hence $N = \langle a,\ a^c,\ a^{cb},\ a^{cbc} \rangle \cong 2^4$. We let $H := \langle b,\ c \rangle \cong D_{10}$ which satisfies $H \cap N = 1$ and $|NH| = |G^{(4,5,5)}|$ hence we can write $G^{(4,5,5)} \cong N : H \cong 2^4 : D_{10}$. Lastly we remark that there is a unique conjugacy class of D_{10} subgroups in $GL_4(2)$. Let F be the exceptional isomorphism $A_8 \cong_F GL(4,2)$. Clearly there is a unique conjugacy class of dihedral groups of order 10 in A_8 all conjugate

to $D := \langle (1,2)(3,4), (1,3)(4,5) \rangle$ and using Magma we can write the action of $F\big((1,2)(3,4)\big)$, $F\big((1,3)(4,5)\big)$ on $V \cong N$ a vector space of dimension 4 over $GF(2)$ with elementary basis $e_1,\ e_2,\ e_3,\ e_4$. The element $F\big((1,2)(3,4)\big)$ acts as $e_1 \to e_4,\ e_2 \to e_1+e_2+e_3+e_4,\ e_3 \to e_3,\ e_4 \to e_1$, and $F\big((1,3)(4,5)\big)$ acts as $e_1 \to e_3,\ e_2 \to e_1+e_4,\ e_3 \to e_1,\ e_4 \to e_2+e_3$. We can take as generators for $G^{(4,5,5)}$ the following elements:

$$a := e_3(1,2)(3,4),\ b := e_1+e_4,\ c := (1,3)(4,5).$$

□

Proposition 3.12. *All the groups in Table 3.4 satisfy property* $(\boldsymbol{\sigma})$.

Proof. For all the groups in Table 3.4 but for $G^{(4,5,6)} \cong S_5 \times 2$ it is clear from their structure that no product of two involutions has order greater than 6 so $(\boldsymbol{\sigma})$ is automatically satisfied. In the group $S_5 \times 2$ some products of two involutions have order 10. Using the same notation as above there are 5 conjugacy classes of involutions in $S_5 \times 2$ with representatives $z := (6,7)$ the central element is in its own class, and the other representatives are $(1,2),\ (1,2)(3,4),\ (1,2)z$ and $(1,2)(3,4)z$. A pair of involutions in $S_5 \times 2$ has product of order 10 if it is conjugate to a pair of involutions $(1,2)(3,4),\ (1,4)(2,5)z$. Let $(a,\ b,\ c)$ be a generating triple of involutions in a presentation as that of $G^{(4,5,6)}$, then the set $\{a,\ b,\ ab,\ c\}$ contains elements conjugate only to the involutions $(1,2),\ (1,2)z,\ (1,2)(3,4)z$. In particular no element of $\{a,\ b,\ ab,\ c\}$ is conjugate to a $(2,2)$-cycle and so property $(\boldsymbol{\sigma})$ is satisfied by $G^{(4,5,6)}$. □

Remark 3.13. As a guideline for the above proposition we remark that it can be deduced from Norton's Table 3.2. Indeed one can readily check that all groups in Table 3.4 can also be found in Table 3.2, hence they $2A$-embed in $\mathbb{M}$ and so satisfy $(\boldsymbol{\sigma})$ by the 6-transposition property of the $2A$ involutions. We kept this observation out of the above proof in order to keep the description as self-contained as possible.

3.2.3 The infinite 6-transposition quotients of the $G^{(m,n,p)}$ groups for $(m,n,p) \neq (6,\ 6,\ 6)$

Let us now find the largest quotients of the infinite $G^{(m,n,p)}$ groups satisfying $(\boldsymbol{\sigma})$ for (m,n,p) in the set $\{(4,\ 6,\ 6),\ (5,\ 5,\ 6),\ (5,\ 6,\ 6)\}$. The case $(m,n,p) = (6,\ 6,\ 6)$ will be treated separately in the next section.

We recall that R_1 is the word $a \cdot b^c = acbc$, and we denote the quotient of $G^{(m,n,p)}$ by the relation $R_1^{r_1} = 1$ by:

$$G^{(m,n,p;\ r_1)} := \langle a, b, c \mid a^2,\ b^2,\ c^2,\ (ab)^2,\ (ac)^m,\ (bc)^n,\ (abc)^p,\ (ab^c)^{r_1} \rangle,$$

where we let $r_1 \in [1, 6]$ to avoid contradicting $\boldsymbol{(\sigma)}$. The presentation for $G^{(m,n,p;\ r_1)}$ is not symmetric in $a,\ b$, and ab but we can swap the roles of a and b. Hence we need to consider the quotients $G^{(m,n,p;\ r_1)}$ with $r_1 \in [1, 6]$ and $(m, n, p) \in \mathcal{F}$, where

$$\mathcal{F} := \{(4,\ 6,\ 6),\ (6,\ 6,\ 4),\ (5,\ 5,\ 6),\ (6,\ 5,\ 5),\ (5,\ 6,\ 6),\ (6,\ 6,\ 5)\}.$$

Definition 3.14. We say that a quotient Q of $G^{(m,n,p)}$ does not **shrink** if the orders $ac,\ bc$ and abc in Q are not smaller than $m,\ n$ and p respectively.

The next theorem is the main result of this section. It is a complete classification of the groups $G^{(m,n,p;\ r_1)}$ for $(m, n, p) \in \mathcal{F}$, which satisfy $\boldsymbol{(\sigma)}$ and do not shrink. All such groups are finite and their orders were obtained with Magma as mentioned in paragraph 1.3. The dashes $-$ in Table 3.5 mean the parameter sought is not applicable to that group.

Theorem 3.15. *The groups* $G^{(m,n,p;\ r_1)}$ *which do not shrink for* $(m, n, p) \in \mathcal{F}$ *and* $r_1 \in [1, 6]$ *are as given in Table 3.5.*

$(m,n,p;\ r_1)$	Iso. Type	$(\boldsymbol{\sigma})$	$2A$-embeds in $\mathbb{M}$	Element contradicting $(\boldsymbol{\sigma})$
$(4,6,6;\ 4)$	$2\times(2^4:_{\phi_1} D_{12})$	**Y**	**Y**	–
$(6,6,4;\ 3)$	$2^4:_{\phi_1} D_{12}$	**Y**	**Y**	–
$(6,6,4;\ 6)$	$2^2.\big(2\times(2^4:_{\phi_1} D_{12})\big)$	N	N	$ab\cdot a^c$ has order 8
$(6,5,5;\ 5)$	$2^4:_{\lambda_2} A_5$	**Y**	**Y**	–
$(5,5,6;\ 3)\cong(3,5,10)$	$2\times A_5$	N	N	$ab\cdot a^c$ has order 10
$(5,5,6;\ 6)$	$2.(2^4:_{\lambda_2} A_5)$	N	N	$ab\cdot a^c$ has order 10
$(6,6,5;\ 4)$	$2\times S_6$	**Y**	**Y**	–
$(6,6,5;\ 5)$	$2\times L_2(11)$	N	N	$ab\cdot a^c$ has order 10
$(5,6,6;\ 5)$	$2\times L_2(11)$	N	N	$ab\cdot a^c$ has order 10
$(5,6,6;\ 6)$	$(2^3:3):(2\times S_6)$	N	N	$ab\cdot a^c$ has order 12

TABLE 3.5: The $G^{(m,n,p;\ r_1)}$ groups for $(m,n,p)\in\mathcal{F}$ and $r_1\in[1,6]$

We will prove Theorem 3.15 in a series of lemmas treating each case $(m,n,p)\in\mathcal{F}$ separately. In the proof of these lemmas we will make use of some quotients of $G^{(m,n,p;\ r_1)}$ whose presentations are symmetric in $a,\ b,\ ab$. We let R_2 and R_3 be the words:

$$R_2 := ab\cdot a^c,\quad R_3 := ab\cdot b^c,$$

and we denote the quotient of $G^{(m,n,p;\ r_1)}$ by the normal closure of $R_2^{r_2}$ and $R_3^{r_3}$ by:

$$G^{(m,n,p;\ r_1,r_2,r_3)} := \langle a,b,c \mid a^2,\ b^2,\ c^2,\ (ab)^2,\ (ac)^m,\ (bc)^n,\ (abc)^p,\ (ab^c)^{r_1},\ (aba^c)^{r_2},\ (abb^c)^{r_3}\rangle,$$

where $r_2,\ r_3 \in [1,6]$ to avoid contradicting $(\boldsymbol{\sigma})$. By symmetry in $\{a,\ b,\ ab\}$ of the presentation for $G^{(m,n,p;\ r_1,r_2,r_3)}$ we deduce the following easy lemma.

Lemma 3.16. *Any permutation α of $\{a,\ b,\ ab\}$ permutes $\{m,\ n,\ p\}$ and $\{r_1,\ r_2,\ r_3\}$ respectively and so induces the isomorphism $G^{(m,n,p;\ r_1,r_2,r_3)} \cong (G)^{(\alpha(m),\alpha(n),\alpha(p);\ \alpha(r_1),\alpha(r_2),\alpha(r_3))}$.* □

Example 3.17. *The permutation $(a,\ b)$ permutes ac with bc and R_2 with R_3 and so induces the isomorphism $G^{(m,n,p:\ r_1,r_2,r_3)} \cong G^{(n,m,p:\ r_1,r_3,r_2)}$.*

For each $(m,n,p) \in \mathcal{F}$ we give a lemma summarising which groups $G^{(m,n,p;\ r_1)}$ were obtained for all $r_1 \in [1,6]$. The information is presented in tables, where column 1 gives the value of r_1 in the relation $R_1^{r_1} = 1$ satisfied by $G^{(m,n,p;\ r_1)}$, column 2 gives the order of the group computed with Magma, and column 3 gives the isomorphism type of the group. Column 4 answers whether or not the group satisfies property $(\boldsymbol{\sigma})$, column 5 answers whether the group can be $2A$-embedded in $\mathbb{M}$, and if so in which row of Table 3.2 it can be found. If the group $2A$-embeds in $\mathbb{M}$, column 6 gives the conjugacy classes in $\mathbb{M}$ of the products ac, bc and abc. Finally column 7 gives the orders of ac, bc, and abc.
The meaning of a dash $-$ in some of the tables' entries is that either the parameter sought is not applicable to the group in that row, or that the group does not contain two distinct commuting involutions.

Lemma 3.18. *For $r_1 \in [1,6]$ the groups $G^{(4,6,6;\ r_1)} \cong G^{(6,4,6;\ r_1)}$ are all finite with order and isomorphism type given in the following table.*

r_1	Order	Isomorphism Type	$(\boldsymbol{\sigma})$	$2A$-embeds in $\mathbb{M}$	Classes in $\mathbb{M}$	Minimal $G^{(m,n,p)}$
1, 3, 5	4	2^2	Y	Y (1)	$(1A, 2A, 2A)$	$G^{(1,2,2)}$
2, 6	24	$D_{12} \times 2$	Y	Y(9)	$(2B, 6A, 6A)$	$G^{(2,6,6)}$
4	384	$2 \times (2^4 :_{\phi_1} D_{12})$	Y	Y (30)	$(4B, 6A, 6A)$	$G^{(4,6,6)}$

Proof. Let $r_1 = 4$ and we denote G the group $G^{(4,6,6;\ 4)}$ in this proof only. We let N be the normal closure of a so that $G/N \cong \langle b,c\rangle \cong D_{12}$, hence $|N| = 2^5$ since $|G| = 384$. Clearly N must contain the set of involutions $\{a, a^c, a^{cb}, a^{cbc}, a^{cbcb}\}$. All involutions in $\{a, a^c, a^{cb}, a^{cbc}, a^{cbcb}\}$

pairwise commute since the product of any two is conjugate to either $(ac)^2$ or R_1^2 which have order 2. For example $[a, a^c] = (ac)^4 = 1$ and $[a, a^{cb}] = ((ac)^4)^b = 1$, $[a, a^{cbc}] = R_1^4 = 1$, $[a, a^{cbcb}] = (R_1^4)^b = 1$. Also it is easy to check all involutions are distinct, otherwise we would get a smaller group G. Hence $N = \langle a,\ a^c,\ a^{cb},\ a^{cbc},\ a^{cbcb}\rangle \cong 2^5$. We let $H := \langle b,\ c\rangle$ so that $G^{(4,6,6;\ 4)} \cong NH$ and $H \cap N = 1$. Hence G is isomorphic to a split extension $2^5 : D_{12}$. We rename the elements $a,\ a^c,\ a^{cb},\ a^{cbc},\ a^{cbcb}$ by $v_1,\ v_2,\ v_3,\ v_4,\ v_5$. It is trivial to see that b acts on N as $v_1 \to v_1,\ v_2 \to v_3,\ v_3 \to v_2,\ v_4 \to v_5,\ v_5 \to v_4$ and c acts as $v_1 \to v_2,\ v_2 \to v_1,\ v_3 \to v_4,\ v_4 \to v_3,\ v_5 \to v_1 + v_2 + v_3 + v_4 + v_5$. From this action we can determine that $\langle b, c\rangle = H$ has one fixed point on N which is $z := v_1 + v_4 + v_5$, so that $Z(G) = \langle z\rangle \cong 2$. The orbits of H are easy to compute, and have sizes $1, 1, 3, 3, 6, 6, 6, 6$. We call M the quotient of N by $Z(G)$, so $M \cong 2^4$, and when viewed as a $GF(2)H$-module H has orbits on M of sizes $1, 3, 6, 6$. In $A_8 \cong GL_4(2)$ there are two conjugacy classes of D_{12} subgroups with representatives $E_1 := \langle (1,2)(3,4), (3,5)(7,8)\rangle$ and $E_2 := \langle (1,2)(3,4)(5,6)(7,8), (3,5)(6,8)\rangle$ respectively. The actions ϕ_1, and ϕ_3 of E_1 and E_2 on the vector space V of dimension 4 over $GF(2)$ have orbits sizes $1, 3, 6, 6$ and $1, 1, 2, 3, 3, 6$ respectively. Hence $V :_{\phi_1} E_1 \cong G/Z(G)$. Lastly we observe that G has $G^{(4,6,6;\ 2)} \cong G^{(2,6,6)} \cong 2 \times D_{12}$ as a quotient group; if we let Y be the normal closure of the involution $y := (ac)^2$ we can show $Y = \langle y, y^b, y^{bc}, y^{bcb}\rangle \cong 2^4$ where $G/Y \cong 2 \times D_{12}$. Hence we can write $G \cong 2 \times (2^4 :_{\phi_1} D_{12})$. □

Lemma 3.19. *For* $r_1 \in [1, 6]$ *the groups* $G^{(6,6,4;\ r_1)}$ *are all finite with order and isomorphism type given in the following table :*

r_1	Order	Isomorphism Type	$(\boldsymbol{\sigma})$	$2A$-embeds in $\mathbb{M}$	Classes in $\mathbb{M}$	Minimal $G^{(m,n,p)}$
1, 5	4	2^2	Y	Y (1)	$(1A, 2A, 2A)$	$G^{(1,2,2)}$
2, 4	8	2^3	Y	Y (2)	$(2A, 2A, 2B)$	$G^{(2,2,2)}$
3	192	$2^4 :_{\phi_1} D_{12}$	Y	Y(24)	$(6A, 6A, 4A)$	$G^{(6,6,4)}$
6	1536	$2^2.\big(2 \times (2^4 :_{\phi_1} D_{12})\big)$	N	N	–	$G^{(6,6,4)}$
			$ab \cdot a^c$ has order 8			

Proof. In this proof, and this proof only, we write G_{r_1} for $G^{(6,6,4;\ r_1)}$ to ease the reading. This notation should not be confused with that of Theorem 3.3.

For $r_1 = 3$ we proceed in a similar fashion as in the proof of the previous lemma. First we find the normal closure N in G_3 of the involution ab;

$$N := \langle ab,\ (ab)^c,\ (ab)^{ca},\ (ab)^{cac} \rangle \cong 2^4, \text{ where } (ab)^{ca} = (ab)^{cb}.$$

We let H be the dihedral group $\langle a,\ c \rangle$ which has order 12, and we notice that $G_3 = NH$ and $H \cap N = 1$. Hence the group G_3 is isomorphic to a split extension $2^4 : D_{12}$. From the above proof there are only two such split extensions. Relabelling the involutions ab, $(ab)^c$, $(ab)^{ca}$, $(ab)^{cac}$ by v_1, v_2, v_3, v_4 and writing the group operation on N to be addition, we can clearly see that a acts on N as $v_1 \to v_1$, $v_2 \to v_3$, $v_3 \to v_2$, $v_4 \to v_1 + v_4$ since:

$$v_4^a = (ab)^{caca} = cacab(bcac)^2a = cacab(cacb)^2a = (ab)^{cac} \cdot ab = v_4 + v_1.$$

And c acts as $v_1 \to v_2$, $v_2 \to v_1$, $v_3 \to v_4$, $v_4 \to v_3$. Hence H has orbits of sizes $1, 3, 6, 6$ so that its action is equivalent to that of E_1 on V, hence can write $G_3 \cong 2^4 :_{\phi_1} D_{12} \cong G^{(4,6,6;\ 4)}/Z\big(G^{(4,6,6;\ 4)}\big)$.

For $r_1 = 6$ the elements $ab \cdot a^c$ and $ab \cdot b^c$ have order 8 so that G_6 does not satisfy property $(\boldsymbol{\sigma})$. Let x be the involution $(ab \cdot b^c)^4$. The normal closure of $\langle x \rangle$ in G_6 is $N := \langle x,\ x^a,\ x^c \rangle \cong 2^2$ since the equalities $x^a = x^b$ and $x^{ca} = x^{ac}$ follow from $(abc)^2 = (cba)^2$. We call Q the quotient group G_6/N. The group G_6 is a quotient of $G^{(6,6,4;\ 6,8,8)}$ and the group Q is a quotient of $G^{(6,6,4;\ 6,4,4)}$. By Lemma 3.16 there is an isomorphism $G^{(6,6,4;\ 6,4,4)} \cong G^{(4,6,6;\ 4,4,6)}$ swapping the roles of a and ab. From Lemma 3.18 we know $G^{(4,6,6;\ 4)} \cong 2^5 : D_{12}$ and it is easy to check that the element $ab \cdot a^c$ has order 4 and the element $ab \cdot a^c$ has order 6 in $G^{(4,6,6;\ 4)}$ so $G^{(4,6,6;\ 4)} = G^{(4,6,6;\ 4,4,6)}$. Hence by order considerations $Q \cong 2 \times (2^4 :_{\phi_1} D_{12})$ so that $G_6 \cong 2^2.\big(2 \times (2^4 :_{\phi_1} D_{12})\big)$. □

Lemma 3.20. *For $r_1 \in [1, 6]$ the groups $G^{(6,5,5;\ r_1)} \cong G^{(5,6,5;\ r_1)}$ are all finite with order and isomorphism type given in the following table :*

r_1	Order	Isomorphism Type	(σ)	$2A$-embeds in $\mathbb{M}$	Classes in $\mathbb{M}$	Minimal $G^{(m,n,p)}$
1, 3	1	1	–	–	–	$G^{(1,1,1)}$
2, 4, 6	10	D_{10}	Y	–	–	$G^{(2,5,5)}$
5	960	$2^4 :_{\lambda_2} A_5$	Y	Y(32)	$(6A, 5A, 5A)$	$G^{(6,5,5)}$

Proof. Let $r_1 = 5$ and we denote in this proof only the group $G^{(6,5,5;\ 5)}$ by G which has order 960. We use similar techniques as in the proofs of the previous two lemmas. We let N be the normal closure of the involution $y := (ac)^3$. Clearly $G/N \cong G^{(3,5,5;\ 5)} \cong G^{(3,5,5)} \cong A_5$ from Proposition 3.11 (one can easily check that the generators of $G^{(3,5,5)}$ satisfy the relation $R_1^5 = 1$). Hence $|N| = 16$. The subgroup N must contain the elements in $\{y, y^b, y^{bc}, y^{bcb}\}$, since $y^a = y = y^c$ and ab has order 2. One can show that in fact $N = \langle y, y^b, y^{bc}, y^{bcb}\rangle \cong 2^4$. We now consider the subgroup $A := \langle a,\ b,\ a^c\rangle$ which is a quotient of A_5 since its three generating involutions satisfy the same presentation as $G^{(3,5,5)} \cong A_5$, so by simplicity of A_5 we have $A \cong A_5$. Also we observe that $A \cap N = 1$, hence $G = N : A$ is isomorphic to a split extension $2^4 : A_5$. There are two conjugacy classes of A_5 subgroups in $A_8 \cong GL_4(2)$ with representatives $A^{(1)} := \langle (1,2)(3,4), (1,3,5)\rangle$ and $A^{(2)} := \langle (1,2)(3,4), (1,2,3)(4,5,6)\rangle$ respectively. The action λ_1 of $A^{(1)}$ on the 4-dimensional vector space V over $GF(2)$ has orbits sizes 1 and 15 and arises from the isomorphism $SL_2(4) \cong A_5$ (a transitive action on V), whilst the action λ_2 of $A^{(2)}$ on V has orbits sizes 1, 5 and 10 and arises from the isomorphism $SL_2(4) \cong P\Omega_4^-(2)$. Both aforementioned isomorphisms can be read from [ABL+99]. With Magma one can construct the semidirect product $N : A$ explicitly and check that A does not act transitively on N, so that $G \cong 2^4 :_{\lambda_2} A_5$. □

Lemma 3.21. *For $r_1 \in [1, 6]$ the groups $G^{(5,5,6;\ r_1)}$ are all finite with order and isomorphism type given in the following table :*

r_1	Order	Isomorphism Type	$(\boldsymbol{\sigma})$	$2A$-embeds in $\mathbb{M}$	Classes in $\mathbb{M}$	Minimal $G^{(m,n,p)}$
1, 2, 4	2	2	–	–	–	$G^{(1,1,2)}$
3	120	$A_5 \times 2$	N $a^c.ab$ has order 10	N	–	$G^{(5,5,6)}$
5	10	D_{10}	Y	–	–	$G^{(2,5,5)}$
6	1920	$2.(2^4 :_{\lambda_2} A_5)$	N $a^c.ab$ has order 10	N	–	$G^{(5,5,6)}$

Proof. In this proof we write G_{r_1} for $G^{(5,5,6;\ r_1)}$ to ease the reading.

For $r_1 = 3$ the order of G_3 is 120. We notice that the subgroup $H := \langle a,\ b,\ a^c \rangle$ is a quotient of $G^{(3,5,10)}$, which from [Cox39] is a group isomorphic to $A_5 \times 2$ of order 120, hence $G_3 \cong G^{(3,5,10)}$. Clearly G_3 does not satisfy property $(\boldsymbol{\sigma})$ since there exists products of pair of involutions, such as $ab \cdot a^c$ or $ab \cdot b^c$, which have order 10.

For $r_1 = 6$ the elements $ab \cdot a^c$ and $ab \cdot b^c$ have order 10 in G_6, so that G_6 does not satisfy property $(\boldsymbol{\sigma})$. We let x be the involution $(ab \cdot a^c)^5$ and we let N be the normal closure of x in G_6. We call Q the quotient G_6/N. The group G_6 is a quotient of the group $G^{(5,5,6:\ 6,10,10)}$ and the group Q is a quotient of $G^{(5,5,6;\ 6,5,5)}$. By Lemma 3.16 there is an isomorphism $G^{(5,5,6;\ 6,5,5)} \cong G^{(6,5,5;\ 5,5,6)}$ swapping the roles of a and ab. By Lemma 3.20 we have $G^{(6,5,5;\ 5)} \cong 2^4 :_{\lambda_2} A_5$, and in this group the element $ab \cdot a^c$ has order 5 and the element $ab \cdot a^c$ has order 6 so that $Q \cong 2^4 :_{\lambda_2} A_5$ by order comparison. Hence $|N| = 2$ so that $\langle x \rangle$ is normal in G_6. Hence $G_6 \cong 2.(2^4 :_{\lambda_2} A_5)$. □

Lemma 3.22. *For $r_1 \in [1, 6]$ the groups $G^{(6,6,5;\ r_1)}$ are all finite with order and isomorphism type given in the following table :*

r_1	Order	Isomorphism Type	$(\boldsymbol{\sigma})$	$2A$-embeds in $\mathbb{M}$	Classes in $\mathbb{M}$	Minimal $G^{(m,n,p)}$
1, 3	2	2	–	–	–	$G^{(1,1,2)}$
2, 6	4	2^2	Y	Y(1)	–	$G^{(1,2,2)}$
4	1440	$2 \times S_6$	Y	Y(34)	–	$G^{(6,6,5)}$
5	1320	$2 \times L_2(11)$	N $a^c.ab$ has order 10	N	–	$G^{(6,6,5)}$

Proof. In this proof, and this proof only, we write G_{r_1} for $G^{(6,6,5;\ r_1)}$ to ease the reading.

For $r_1 = 4$ the group G_4 has order 1440. Comparing with Norton's Table 3.2 we conjecture that G_4 is isomorphic to $2 \times S_6$ and we prove it below. It is easy to find a triple of involutions in $2 \times S_6$ which satisfies the same presentation as $G^{(6,6,5;\ 4)}$, for example take $a,\ b,\ c$ to be:

$$(1,4)(2,6)(3,5),\ (1,4)(7,8),\ (2,5)(3,4)(7,8),$$

so by order consideration $G_4 \cong 2 \times S_6$. It now remains to show that G_4 satisfies property $(\boldsymbol{\sigma})$. A subgroup S_6 of G_4 satisfies property $(\boldsymbol{\sigma})$ as the product of two involutions has order 1, 2, 3, 4, 5 or 6, whereas in G_4 the product of two involutions can also have order 10. Let us show that such pairs of involutions cannot be individually conjugate to elements in $\{a,\ b,\ ab,\ c\}$. In S_6 the representatives of the 3 conjugacy classes of involutions are $s := (1,2),\ t := (1,2)(3,4)$ and $u := (1,2)(3,4)(5,6)$. Hence in G_4 the representatives of conjugacy classes of involutions are $s,\ t,\ u,\ z,\ sz,\ tz$, and uz, where $z := (7,8)$ is the unique central element. In G_4 two involutions have product of order 10 if and only if they are each conjugate to the involutions $(1,2)(3,4)$ and $(1,4)(2,5)z$ respectively. The latter two involutions are conjugate to t and tz respectively. None of the elements $a,\ b,\ ab$ and c are conjugate to t, so G_4 satisfies $(\boldsymbol{\sigma})$. Let $x := (bc)^3 = (2,5)$ then $x^{acbc} = (1,6)$ and $x^{acbcac} = (3,5)$. We notice that $c^{acbc} = (1,6)(3,5)(7,8)$ so an expression for the central involution z in terms of the generators is $z = c^{acbc}x^{acbc}x^{acbcac}$.

For $r_1 = 5$, the order of the group G_5 is 1320. We let $H := \langle a^c, b^c, ab\rangle$ and we notice that $G_5 = H$ since $a,\ b,\ c$ are in H:

$$(abc)^2 \in H \quad \Rightarrow\ (abc)^4 = cba \in H \quad \Rightarrow\ c \in H \quad \Rightarrow\ ca^c = a \in H \quad \Rightarrow b \in H.$$

We let $s := ab \cdot a^c$ and $t := ab \cdot b^c$. Since the presentation for G_5 is symmetric in $\{a, b\}$ we have that the elements s and t must have the same order, which we denote n. Hence the generators $a^c,\ b^c,\ ab$ for H satisfy the same presentation as the group $G^{(n,n,5:\ 6)}$ since the word R_1 for the generators of H is $a^c(ab)b^c(ab) = (bc)^{acab}$ which has order 6. Now $|G_5| = 1320$ so we cannot have $n \in \{1, 2, 3, 4, 5\}$ by comparison with the groups described in Propositions 3.9 and 3.11. If $n = 6$ then G_5 is a quotient of $G^{(6,5,5;\ 6)} \cong 2^2$, a contradiction. Hence both s and t have order greater than 6 so that property $(\boldsymbol{\sigma})$ does not hold in G_5. Next we notice that both s and t have order 10 since their squares are conjugate to $cacb = R_1$ of order 5. The calculation for s^2 is:

$$s^2 = b(ac)^3cbcac = bcacacacbcac = bcacab(bcac)^2 = bcacab(cacb)^3 = (acacbcac)^{bcacb} =$$
$$((ca)^4bcac)^{bcacb} = (acacab)^{cacbcacb} = (cacb)^{acacbcacb}$$

We can also show that the involutions s^5 and t^5 are equal. It follows that s^5 is a central involution of G, indeed we clearly have that the two elements ab and a^c commute with s^5 and that the elements ab and b^c commute with t^5, and since $s^5 = t^5$ we get that the generators $a^c,\ b^c,\ ab$ of $H = G_5$ centralises $N := \langle s^5\rangle \cong 2$. Next we form the quotient H/N and we observe that it satisfies the same presentation as $G^{(5,5,5)} \cong L_2(11)$, so by order comparison $H/N \cong L_2(11)$. We let K be the subgroup $\langle ab,\ c,\ c^a\rangle$ where $|K| = 660$ and $s^5 \notin K$ so that $G_5 \cong 2 \times L_2(11)$. □

Lemma 3.23. *For* $r_1 \in [1, 6]$ *the groups* $G^{(5,6,6;\ r_1)} \cong G^{(6,5,6;\ r_1)}$ *are all finite with order and isomorphism type given in the following table :*

r_1	Order	Isomorphism Type	$(\boldsymbol{\sigma})$	$2A$-embeds in $\mathbb{M}$	Classes in $\mathbb{M}$	Minimal $G^{(m,n,p)}$
1, 3	2	2	–	–	–	$G^{(1,1,2)}$
2, 4	4	2^2	Y	Y(1)	–	$G^{(1,2,2)}$
5	1320	$2 \times L_2(11)$	N $a^c.ab$ has order 10	N	–	$G^{(5,6,6)}$
6	69120	$(2^3 \times 3).(2 \times S_6)$	N $a^c.ab$ has order 12	N	–	$G^{(5,6,6)}$

Proof. For $r_1 = 5$ we can use a similar argument as for $G^{(6,5,5;\ 5)}$.

For $r_1 = 6$ we let $G := G^{(5,6,6:\ 6)}$. We find that $ab \cdot a^c$ has order 12 and $ab \cdot b^c$ has order 24, so G does not satisfy property $(\boldsymbol{\sigma})$, and we can write $G = G^{(5,6,6;\ 6,12,24)}$ by Lemma 3.16. We let $x := (ab \cdot b^c)^{12}$ be an involution and we find the normal closure in G of $\langle x \rangle$ which is:

$$N := \langle x,\ x^a,\ x^c, x^{ca}, (ab \cdot b^c)^8 \rangle \cong 2^3 \times 3$$

Now the element $(ab \cdot a^c)N$ has order 4 and the element $(ab \cdot a^c)N$ has order 6, hence the quotient $Q := G/N$ is a quotient of $G^{(5,6,6;\ 6,6,4)}$ and so by Lemma 3.16 there is an isomorphism $Q \cong G^{(6,6,5;\ 4,6,6)}$ swapping the roles of a and ab. We notice that in the quotient $G^{(6,6,5;\ 4)} \cong 2 \times S_6$ from the above proposition the element $ab \cdot a^c$ has order 4 and the element $ab \cdot a^c$ has order 6 so that $G^{(6,6,5;\ 4,6,6)} \cong 2 \times S_6$. Hence $G \cong (2^3 \times 3).(2 \times S_6)$. □

Comparing the $G^{(m,n,p)}$ quotients obtained in this section with the groups listed in Norton's Table 3.2, we deduce the following.

Corollary 3.24. *All the quotients of the groups* $G^{(m,n,p)}$ *satisfying property* $(\boldsymbol{\sigma})$ *for* $(m,n,p) \neq (6,6,6)$ $2A$*-embed into the Monster group* $\mathbb{M}$. □

3.3 The 6-transposition quotients of the group $G^{(6,6,6)}$

3.3.1 Introduction and main result

We fix $(m,n,p) = (6,6,6)$ and we recall that;

$$G^{(6,6,6;\ r_1,r_2,r_3)} := \langle a,b,c \mid a^2,\ b^2,\ c^2,\ (ab)^2,\ (ac)^6,\ (bc)^6,\ (abc)^6,\ (ab^c)^{r_1},\ (abb^c)^{r_2},\ (aba^c)^{r_3}\rangle.$$

We will only consider the cases $r_1,\ r_2,\ r_3 \in [1,6]$ to avoid contradicting $\boldsymbol{(\sigma)}$. The main result of this section is the following theorem, whose proof will form the remainder of this chapter.

Theorem 3.25. *The largest quotients of the group* $G^{(6,6,6)}$ *which do not shrink and satisfy* $\boldsymbol{(\sigma)}$ *are given in Table 3.6 as quotients of the* $G^{(6,6,6;\ r_1,r_2,r_3)}$ *groups for* $r_1,\ r_2,\ r_3 \in [1,6]$.

(r_1,r_2,r_3)	Added relation	Order	Isomophism Type	$\boldsymbol{(\sigma)}$	$2A$-embeds in $\mathbb{M}$	Largest $2A$-embedded quotient
(4, 6, 6) (6, 4, 6) (6, 6, 4)	–	1152	$\left(2^4 : (S_3 \times S_3)\right) \times 2$	Y	N	$2^4 : (S_3 \times S_3)$
(5, 5, 5)	$(c \cdot b^{ca})^4 = 1$	3840	$2^5 :_\phi S_5$	Y	Y(37)	$2^5 :_\phi S_5$
(6, 6, 6)	$(c^a \cdot c^{bc})^3 = 1$	17496	$(3^4 : 2) : (3^{1+2}_+ : 2^2)$	Y	N	$3^{1+2}_+ : 2^2$

TABLE 3.6: The largest quotients of $G^{(6,6,6)}$ satisfying $\boldsymbol{(\sigma)}$

In this subsection we let $G := G^{(6,6,6;\ r_1,\ r_2,\ r_3)}$.

Proposition 3.26. (i) *If* $1 \in \{r_1,\ r_2,\ r_3\}$ *then* G *is a quotient of the group* 2^2*;*

(ii) *If* $2 \in \{r_1,\ r_2,\ r_3\}$ *then* G *is a quotient of the group* $S_3 \times S_3 \times 2$*;*

(iii) *If* $3 \in \{r_1,\ r_2,\ r_3\}$ *then* G *is a quotient of the group* D_{12}*;*

(iv) *If* $4 \in \{r_1,\ r_2,\ r_3\}$ *then* G *is a quotient of the group* $\left(2^4 : (S_3 \times S_3)\right) \times 2$*;*

(v) *If* $\{5,\ 6\} \subseteq \{r_1,\ r_2,\ r_3\}$ *then* G *is a quotient of the group* 2^2*.*

The orders of the groups in (ii), (iii) and (iv) were computed with Magma. We now prove statements (i) – (v).

Lemma 3.27. *If one of* $\{r_1,\ r_2,\ r_3\}$ *is equal to* 1 *then* G *is a quotient of a group isomorphic to* 2^2.

Proof. If $r_1 = 1$ then $a = cbc$ so that $(ab)^2 = (bc)^2 = 1$ so that $(bc)^3 = ab = 1$ and hence a presentation for G is $\langle b,\ c \mid b^2,\ c^2,\ (bc)^2\rangle \cong 2 \times 2$. The proof is similar for the cases $r_2 = 1$ and $r_3 = 1$. □

Lemma 3.28. *Let* $G := G^{(6,6,6;\ r_i)}$ *for* $i = 1,\ 2$ *or* 3. *If* $r_i = 2$ *then* G *is a quotient of a group isomorphic to* $S_3 \times S_3 \times 2$.

Proof. Let $G := G^{(6,6,6;\ r_1)}$. If $r_1 = 2$ the order of G is $72 = 2^3 \cdot 3^2$ hence G is a soluble group by Burnside's $p^a \cdot q^b$ Theorem 1.14. By inspection we find a Sylow 3-subgroup $N = \langle (ac)^2\rangle \times \langle (bc)^2\rangle$. Using the relation $R_1^2 = 1$ (equivalently $acbc = cbca$) the commutator $[b, (ac)^2]$ is trivial and $[a, (ac)^2] = [c, (ac)^2] = (ac)^2$, so $N \lhd G$. Hence G satisfies the hypotheses of the Schur-Zassenhaus Theorem, 1.15, so that $G \cong N \rtimes K$ where $|K| = 2^3$ and all complements to K in G are G-conjugates. By inspection again we find a Sylow 2-subgroup $K = \langle a\rangle \times \langle b\rangle \times \langle c^{abc}\rangle$ since $[a, c^{abc}] = [b, c^{abc}] = 1$. From the group structure of G it is clear that no elements of G has order greater than 6 so that G satisfies $(\boldsymbol{\sigma})$.

There is another way of looking at G. If $r_1 = 2$ then $r_2 = r_3 = 6$ since $R_2^2 = (a \cdot (ab)^c)^2 = (ca)^2$ and $R_3^2 = (b \cdot (ab)^c)^2 = (cb)^2$. Hence the generators of the subgroup $H := \langle a,\ b,\ (ab)^c\rangle$ satisfy the same presentation as $G^{(6,6,3)} \cong G^{(3,6,6)} \cong 3_+^{1+2} : 2^2$, and since 3^2 divides $|G|$ but 3^3 does not, then H is a proper quotient of $G^{(3,6,6)}$ of order dividing 36. Clearly H has order 36 since both $(bc)^2$ and $(ac)^2$ are distinct elements in H and from the relation ${R_1}^2 = 1$ we can compute easily $[(ac)^2, (bc)^2] = 1$. Hence $H \cong \frac{3_+^{1+2}.2^2}{Z(3_+^{1+2})}$ and so $H \cong 3^2 : 2^2 \cong S_3 \times S_3$. We notice that the involution $(abc)^3$ is not in H, otherwise $c = ab(ab)^c ab(abc)^3 \in H$ so that $H = \langle a, b, c\rangle = G$, a contradiction. The involution $(abc)^3$ commutes with all the generators of H, for example using $(acbc)^2 = 1$ and $(ac)^6 = (abc)^6 = 1$ we notice that $[a, (abc)^3] = 1$:

$$a(abc)^3a = (acb)^3 = (acbc)cacbacb = (cbca)cacbacb = cb(cacaca)bcb = cb(ac)^3bcb =$$
$$cbacac(acbc)b = cbacac(cbca)b = (cba)^3 = (abc)^3,$$

and similar calculations give $[b, (abc)^3] = [(ab)^c, (abc)^3] = 1$. Hence $G = H \times \langle (abc)^3\rangle \cong S_3 \times S_3 \times 2$ and the centre of G is $\langle (abc)^3\rangle$. Comparing with Norton's Table 3.2 the group G

does not embed in $\mathbb{M}$, but $G/Z(G) \cong G^{(3,6,6)}$ does. The proof for G equal to $G^{(6,6,6;\ r_2)}$ with $r_2 = 2$ or $G^{(6,6,6;\ r_3)}$ with $r_3 = 2$ is similar. □

Lemma 3.29. *Let* $G := G^{(6,6,6;\ r_i)}$ *for* $i = 1,\ 2$ *or* 3. *If* $r_i = 3$ *then* G *is a quotient of a group isomorphic to* D_{12}.

Proof. If $r_1 = 3$ then the order of G is 12. Hence the cyclic subgroups $\langle ac\rangle$, $\langle bc\rangle$, $\langle abc\rangle$ cannot all be distinct and have order 6. If any two of those subgroups have order 6 they must be equal. We cannot have $\langle bc\rangle = \langle abc\rangle$ or $\langle ac\rangle = \langle abc\rangle$ as this gives $acbc$ has order dividing 2, and since $r_1 = 3$ the order must be 1 so that G has order dividing 4 by Lemma 3.27, a contradiction. So if two of the cyclic subgroups have order 6 we must have $\langle ac\rangle = \langle bc\rangle$ hence either $ac = bc$ or $ac = cb$ so that either $a = b$ or $a = b^c$. The latter is impossible as it implies $acbc$ has order 1. If $ac = bc$ then $G = \langle a,\ c\rangle \cong D_{12}$ by order comparison. If only one of the cyclic subgroups above has order 6, then G must be a quotient of a group isomorphic to $G^{(2,3,6)} \cong D_{12}$ by comparing with the orders of the groups in Proposition 3.9, but if any of $\langle ac\rangle$, $\langle bc\rangle$ has order 2 or 3 then $acbc$ has order 2, a contradiction. Finally if none of $\langle ac\rangle$, $\langle bc\rangle$, $\langle abc\rangle$ has order 6 then G is a quotient of a group $G^{(m,n,p)}$ where $\{m,n,p\} \subseteq \{1,2,3\}$ but from Proposition 3.9 the order of G would be at most 8, a contradiction. Hence $a = b$ and $G \cong D_{12}$. Similarly for $r_2 = 3$ or $r_3 = 3$ we eventually find that $b = 1$ or $a = 1$ and in both cases $G \cong D_{12}$. □

Lemma 3.30. *Let* $G := G^{(6,6,6;\ r_i)}$ *for* $i = 1,\ 2$ *or* 3. *If* $r_i = 4$ *then* G *is a quotient of a group isomorphic to* $\left(2^4 : (S_3 \times S_3)\right) \times 2$.

Proof. Without loss of generality we let $r_1 = 4$. The group G has order $1152 = 2^4 \cdot 72$ and from Lemma 3.28 it has a quotient $Q := G^{(6,6,6;\ 2)} \cong S_3 \times S_3 \times 2$ of order 72. We call N the normal closure of $\langle x\rangle$ in G where x is the involution $R_1^2 = (acbc)^2$. Since $G/N \cong S_3 \times S_3 \times 2$ then N must have order 16. We observe that $x^a = x$ and $x^{cbc} = x$ since from $R_1^4 = 1$ we have that $(acbc)^2 = (cbca)^2$. Hence the normaliser $N_G(\langle x\rangle)$ contains $\langle a, cbc\rangle \cong D_8$ as a subgroup. We claim that $x,\ x^b,\ x^c,\ x^{bc}$ are pairwise distinct elements of N. Indeed if $x^b = x$ then $N_G(\langle x\rangle)$ contains $\langle a,b,c\rangle = G$ as a subgroup so that $N = \langle x\rangle \subseteq Z(G)$ contradicting $|N| = 16$, and similarly if $x^c = x$ or $x^b = x^c$ then $\langle a,b,c\rangle \subseteq N_G(\langle x\rangle)$. By the same argument it is easy to see that we cannot have $x^{bc} = x$ or $x^{bc} = x^c$. Also to avoid $|N| = 8$ we must have $x^{bc} \neq x^b$. Similarly there cannot be an element of $\{x, x^b, x^c, x^{bc}\}$ equal to a product of other elements in the set. It can be shown that the elements in $\{x, x^b, x^c, x^{bc}\}$ commute with each other. Let us

compute the order of $[x, x^b]$:

$$\begin{aligned}
(xb)^2 &= (acbc)^2 b (cbca)^2 b && \text{since } x = (acbc)^2 \text{ has order 2}\\
&= acbca(cb)^3 cacbcba\\
&= a(cbcabcbcbacbcba) && \text{since } (bc)^3 \text{ has order 2}\\
&= a(cbcab)^3\\
&= a(abcbc)^3 && \text{since } (b^c \cdot ab)^3 \text{ has order 2}\\
&= (bc)^2(abcbca)(bc)^2 && \text{using } (bc)^2 = (cb)^4, \text{ as } bc \text{ has order 6}\\
&= (abcbcacbcb)^{(cb)^2}\\
&= (acbcacbc)^{b(cb)^2}\\
&= (x)^{b(cb)^2}
\end{aligned}$$

The orders of the other commutators can be found in a similar way. We can check whether we can write G as a semidirect product of N by a group isomorphic to $G^{(6,6,6;2)} \cong S_3 \times S_3 \times 2$. It is easy to check that there exists no subgroups in $A_8 \cong GL_4(2) \cong Aut(N)$ isomorphic to $S_3 \times S_3 \times 2$ but there exists two conjugacy classes of subgroups isomorphic to $S_3 \times S_3$ with representatives $S_1 := \langle (1,2)(7,8), (1,2,3), (4,5)(7,8), (4,5,6)\rangle$ and $S_2 := \langle (1,2)(3,4), (3,4,6), (1,6)(2,4)(3,5)(7,8), (1,2,5)\rangle$, which have orbits on V (the 4-dimensional vector space over $GF(2)$), of sizes $1, 6, 9$ and $1, 3, 3, 9$ respectively. We refer to the two actions on V as f_1 and f_2 respectively. We now define a subgroup H of G to be $H := \langle a,\ b,\ (ab)^c\rangle$, which is a quotient of $G^{(3,6,6)}$ and it is easy to check that $H \cong S_3 \times S_3$ using a similar argument as in the proof of Lemma 3.28. We can also check that the action of H on N is equivalent to f_1, whereas the action of $H^c = \langle a^c, b^c, ab\rangle$ on N is equivalent to f_2. Clearly $N \cap H = 1$ and NH is a subgroup of index 2 in G. Since G has a quotient group $G^{(6,6,6;\ 2)} \cong S_3 \times S_3 \times 2$ and there is no subgroup isomorphic to $S_3 \times S_3 \times 2$ in $Aut(N)$ then we can write G as a the semidirect product of $N : H$ by an involution z, where z commutes with elements of N and H. Hence $z \in Z(G)$, and we found by inspection an expression for the central involution in the generators $a,\ b,\ c$;

$$z = \left((ab)^{cacbc} \cdot c^a\right)^3.$$

□

Proposition 3.31. *If one of* $r_1,\ r_2,\ r_3$ *is equal to* 5 *then each of the three elements* $R_1,\ R_2,\ R_3$ *must have order dividing* 5.

Proof. Without loss of generality we let $r_1 = 5$ so that $R_1^5 = (acbc)^5 = 1$ and we derive the following:

$$\begin{aligned}
R_2^2 &= aca(bcac)abc \\
&= aca(cacb)^4abc && \text{since } bcac = (R_1^{-1})^c \text{ has order 5} \\
&= (ac)^3b(cacb)^2cacbbac \\
&= (ca)^3b(cacb)^2cacac && \text{since } ac \text{ has order 6} \\
&= (cacacb)a(cacb)cac(bcacac) && \text{since } a,\ b \text{ commute} \\
&= (acacbcac)^{bcacac} \\
&= y^{bcacac}
\end{aligned}$$

where:

$$\begin{aligned}
y &= (ac)^2bcac \\
&= (ca)^4bcac \\
&= (cac)(acacab)(cac) \\
&= (cacb)^{acac} \\
&= R_1^{cacac}
\end{aligned}$$

Hence $R_2^2 = (R_1)^{b^{c(ac)^2}}$ so that R_2 has order dividing 5. Similarly we derive:

$$\begin{aligned}
R_3^2 &= bcab(cbca)bc \\
&= bcab(acbc)^4bc && \text{since } cbca = R_1^{-1} \text{ has order 5} \\
&= bcabacbc(acbc)^2acbcbc \\
&= (bc)^3(acbc)^2acbcbc && \text{since } a,\ b \text{ commute} \\
&= (cb)^3(acbc)^2a(cbcbc) && \text{since } bc \text{ has order 6} \\
&= (cbcbca)bcbc(acbc)(acbcbc) && \text{since } a,\ b \text{ commute} \\
&= w^{acbcbc}
\end{aligned}$$

where:

$$\begin{aligned} w &= bcbc(acbc) \\ &= (cb)^4 acbc \\ &= (bcbcba)^{cbc} \\ &= (cbca)^{bcbc} \\ &= ((R_1)^{-1})^{cacac} \end{aligned}$$

Hence $R_3 = (R_1^{-1})^{a^{(cb)^2 c}}$ so that R_3 has order dividing 5. □

Corollary 3.32. *If* $\{5,6\} \subseteq \{r_1, r_2, r_3\}$ *then* G *is a quotient of* 2^2.

Proof. By the above Proposition 3.31 if $5 \in \{r_1, r_2, r_3\}$ then the elements $R_1,\ R_2,\ R_3$ have order dividing 5 so that if $6 \in \{r_1, r_2, r_3\}$ then at least one of $R_1,\ R_2,\ R_3$ is the identity and so by Lemma 3.27 the group G is isomorphic to a quotient of 2^2. □

The corollary above tells us the only remaining quotients $G := G^{(6,6,6;\ r_1,r_2,r_3)}$ to consider are the ones where $\{r_1, r_2, r_3\}$ is equal to $\{5\}$ or $\{6\}$. We first deal with $\{r_1, r_2, r_3\} = \{5\}$ in the next subsection, and then finish this chapter with the case $\{r_1, r_2, r_3\} = \{6\}$.

3.3.2 The largest 6-transposition quotient of $G^{(6,6,6;\ 5,5,5)}$

We could not determine with Magma the order of the group $G^{(6,6,6;5,5,5)}$ so we introduced an extra relation $R_4^{r_4} = 1$ where:

$$R_4 = c \cdot b^{ca}, \quad r_4 \in [1,6],$$

and we denote by $G^{(6,6,6;\ 5,5,5;\ r_4)}$ the group with presentation:

$$G^{(6,6,6;\ 5,5,5;\ r_4)} :=$$
$$\langle a,b,c \mid a^2,\ b^2,\ c^2,\ (ab)^2,\ (ac)^m,\ (bc)^n,\ (abc)^p,\ (ab^c)^5,\ (abb^c)^5,\ (aba^c)^5,\ (cb^{ca})^{r_4} \rangle.$$

For any word R in the generators $a,\ b,\ c$ and an integer $r \in [1,6]$ we denote by $G^{(6,6,6;\ 5,5,5;\ r_4)}/\{R^r\}$ the quotient of $G^{(6,6,6;\ 5,5,5;\ r_4)}$ by the normal closure of R^r.

The following proposition was obtained by finding the order of the groups $G := G^{(6,6,6;\ 5,5,5;\ r_4)}$ for $r_4 \in [1,6]$ with the Magma function Order (as discussed in paragraph 1.3 of Chapter 1).

Proposition 3.33. *Let* $r_4 \in [1,6]$*, then the group* $G := G^{(6,6,6;\ 5,5,5;\ r_4)}$ *does not shrink if and only if* $r_4 = 4$*.*

Proof. If $r_4 \in \{1,\ 3,\ 5\}$ then G is trivial. If $r_4 \in \{2,\ 6\}$ then G is a quotient of the cyclic group of order 2. Lastly if $r_4 = 4$ then Magma gives $|G| = 3840$. □

In the remainder of this subsection we will prove the following theorem.

Theorem 3.34. *The largest quotient* Q *of* $G^{(6,6,6;\ 5,5,5;\ 4)}$ *satisfying property* $(\boldsymbol{\sigma})$ *is equal to* $G^{(6,6,6;\ 5,5,5;\ 4)}$ *and* Q *is isomorphic to* $N :_\phi S_5$ *where* $N \cong 2^5$ *and* S_5 *centralises an involution* $z \in N$ *such that the action* S_5 *on* $N/\langle z\rangle \cong 2^4$ *stems from the isomorphism* $A_5 \cong SL_2(4)$*.*

On a quotient of $G^{(6,6,6:\ 5,5,5)}$ **isomorphic to** $2^5 : S_5$

We let $Q := G^{(6,6,6;\ 5,5,5;\ 4)}$. We notice that Q contains A_5 as a subgroup, for example $\langle a,\ b,\ a^c\rangle \cong G^{(3,5,5)} \cong A_5$. By comparing the presentation of Q with the group in row 37 of Norton's Table 3.2 we conjecture that $Q \cong 2^5 : S_5$.

Let us now construct a group G which is the split extension of an elementary abelian group $N \cong 2^5$ by a group $H \cong S_5$. We will give the action ϕ of H on N by writing N as a $GF(2)S_5$-module. First we remark the following.

Lemma 3.35. *The group* S_5 *is a quotient of* Q *and satisfies property* $(\boldsymbol{\sigma})$*.*

Proof. The only possible triples of involutions in S_5 that satisfy the same presentation as Q are those where $a,\ b$ are $(2,2)$-cycles forming a Klein-4-group and c is a (2)-cycle, so that if $a = (i,j)(k,l)$ then $c = (m,n)$ where $n \in \{i,j,k,l\}$ and $\Omega = \{1,2,3,4,5\} = \{i,j,k,l,m\}$. For example if we take $b = (i,k)(j,l)$ and $c = (m,i)$ then $ac = (i,m,j)(k,l)$, $bc = (i,m,k)(j,l)$ and $abc = (i,m,l)(j,k)$ have order 6, and $a \cdot b^c = (i,j,k,m,l)$, $(ab) \cdot a^c = (i,l,j,m,k)$ and $(ab) \cdot b^c = (i,l,k,m,j)$ have order 5 and lastly $c \cdot b^{ca} = (i,k,m,l)$ has order 4. The group S_5 clearly satisfies $(\boldsymbol{\sigma})$ since it has no element of order greater than 6. □

Example 3.36. *The elements* $a = (1,2)(3,4)$*,* $b = (1,3)(2,4)$ *and* $c = (4,5)$ *generate* H *and satisfy the same presentation as* Q*.*

We denote by Ω_H the set of ordered triples of involutions $(a,\ b,\ c)$ in H, which generate H as a quotient of Q.

Lemma 3.37. *The set* Ω_H *has size* 120.

Proof. There are 5 Klein-4-subgroups $\langle a,\ b,\ ab\rangle$ of H and by the above proof for each such subgroup there are 4 choices for c such that $(a,\ b,\ c)$ generates a quotient of $G^{(6,6,6)}$. Hence the number of elements of Ω_H is $5 \cdot 4 \cdot 3! = 120$. □

Let us now construct N as a $GF(2)H$-module. I am indebted to my supervisor A. A. Ivanov for suggesting the following construction.

Let S be the set of even subsets of elements of the set of Sylow 5-subgroups of H where $Syl_5(H) = \{S_1,\ S_2,\ S_3,\ S_4,\ S_5,\ S_6\}$, and where $S_1 = \langle(1,2,3,4,5)\rangle$, $S_2 = \langle(1,3,4,5,2)\rangle$, $S_3 = \langle(1,4,5,2,3)\rangle$, $S_4 = \langle(1,5,2,3,4)\rangle$, $S_5 = \langle(1,2,5,3,4)\rangle$, and $S_6 = \langle(1,3,4,2,5)\rangle$. We define addition on S to be the symmetric difference of two sets. We turn S into a $GF(2)H$-module, which we denote N, by letting H act on S by conjugation. We call this action ϕ. For simplicity the action of H on S is given as permutation of the indices of the S_i's and the set S can be written $S = \{\emptyset,\ \{1,2\},\ldots,\ \{5,6\},\ \{1,2,3,4\},\ldots,\ \{3,4,5,6\},\ z\}$, where $z = \{1,2,3,4,5,6\}$. The orbits of H on S are $\emptyset$, $\{z\}$, $\big\{\{i,\ j\}\big\}_{i\neq j}$ and $\big\{\{i_1,\ i_2,\ i_3,\ i_4\}\big\}_{i_1\neq i_2\neq i_3\neq i_4}$ of sizes 1, 1, 15, 15 respectively.
We denote by G the semidirect product $N :_\phi H \cong 2^5 :_\phi S_5$ of order $2^8 \cdot 3 \cdot 5 = 3840$. Also, for all $h \in H$, we denote by $Fix_N(h)$ the set of elements of N fixed by h.

Proposition 3.38. *The conjugacy classes of the G are as follows :*

Class in G	$1a$	$2a$	$2b$	$2c$	$2d$	$2e$	$2f$	$2g$	$3a$	$4a$	$4b$	$4c$
p-powers	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	b	b	b
Size	1	1	15	15	40	40	60	60	320	60	60	120
Class in G	$4d$	$4e$	$4f$	$4g$	$5a$	$6a$	$6b$	$6c$	$8a$	$8b$	$10a$	
p-powers	b	g	g	c	$-$	ae	ad	aa	ab	aa	aa	
Size	120	240	240	240	384	320	320	320	240	240	384	

where the representatives of the conjugacy classes of involutions are:

$2a$: $(z,1)$, *the central element*

$2b$: $(\{1,2\},1)$, *the size* 2 *subsets,*

$2c$: $(\{1,2,3,4\}\ ,\ 1)$, *the size* 4 *subsets,*

$2d$: $(\emptyset,c)$, *or generically* (n,h) *where* $n \in Fix_N(h)$, $|n| = 0$ *mod* 4 *and* h *is a* (2)*-cycle,*

$2e$: (z,c), *or generically* (n,h) *where* $n \in Fix_N(h)$, $|n| = 2$ *mod* 4 *and* h *is a* (2)*-cycle,*

$2f$: (z,a), *or generically* (n,h) *where* $n \in Fix_N(h)$, n *contains exactly* 2 *fixed Sylow-*5*-subgroups, and* h *is a* $(2,2)$*-cycle,*

$2g$: $(\emptyset,a)$, *or generically* (n,h) *where* $n \in Fix_N(h)$, n *contains no fixed Sylow-*5*-subgroups, and* h *is a* $(2,2)$*-cycle.*

□

We now define $S_C(x)$ to be the subset of $Fix_N(x)$ which is contained in the conjugacy class C of G so that $S_C(x) := \{n \in N \mid n^x = n,\ n \in C\}$.

Example 3.39. *(continued)*
For $a,\ b,\ c$ *as in our previous example 3.36, the elements* $a,\ b,\ ab,\ c$ *of* H *act on the indices of the* S_i*'s as* $(1,5)(2,3)$, $(1,5)(4,6)$, $(2,3)(4,6)$, *and* $(1,6)(2,4)(3,5)$ *respectively. Their fixed points are:*

$$\begin{aligned}
Fix_N(a) = S_{2g}(a) \cup S_{2f}(a) &= \{\emptyset,\ \{1,5\},\ \{2,3\},\ \{1,5,2,3\}\} \cup \{z,\ \{1,5,4,6\},\ \{2,3,4,6\},\ \{4,6\}\},\\
Fix_N(b) = S_{2g}(b) \cup S_{2f}(b) &= \{\emptyset,\ \{1,5\},\ \{4,6\},\ \{1,5,4,6\}\} \cup \{z,\ \{1,5,2,3\},\ \{4,6,2,3\},\ \{2,3\}\},\\
Fix_N(ab) = S_{2g}(ab) \cup S_{2f}(ab) &= \{\emptyset,\ \{4,6\},\ \{2,3\},\ \{4,6,2,3\}\} \cup \{z,\ \{4,6,1,5\},\ \{2,3,1,5\},\ \{1,5\}\},\\
Fix_N(c) = S_{2d}(c) \cup S_{2e}(c) &= \{\emptyset,\ \{1,6,2,4\},\ \{1,6,3,5\},\ \{2,4,3,5\}\} \cup \{z,\ \{1,6\},\ \{2,4\},\ \{3,5\}\}.
\end{aligned}$$

Lifting Ω_H to Q

We let Ω_G be the set of ordered triples of involutions $(a',\ b',\ c')$ in G such that :

(1) $\{a',\ b',\ c'\}$ generates G,

(2) $(a',\ b',\ c')$ satisfies the same presentation as the generators of $Q = G^{(6,6,6;\ 5,5,5;\ 4)}$,

(3) Products of pairs of elements from the conjugacy classes of $a',\ b',\ a'b',\ c'$ have order at most 6.

Proposition 3.40. *The triples* $(a',\ b',\ c')$ *in* Ω_G *must satisfy:*

(i) $\{a',\ b',\ a'b'\}$ *is contained in either* $2f$ *or* $2g$,

(ii) the involution c' *is in* $2d \cup 2e$.

Proof. The conjugacy classes $2a,\ 2b,\ 2c$ correspond to elements of N so they cannot contain either of $a',\ b',\ c'$. The conjugacy classes $2d,\ 2e$ contain the odd involutions of H, and the conjugacy classes $2f,\ 2g$ contain the even involutions so a' and b' must belong to either $2f$ or $2g$ and c' must be in $2d \cup 2e$. There exist $t \in 2f$ and $s \in 2g$ such that the product st has order 10; for example if $s = (\{4,6\}, (1,5)(2,3)(4)(6))$ and $t = (\{3,5\}, (2,6)(3,5)(1)(4))$ then $st = (\{3,4,5,6\}, (1,5,2,6,3))$. Hence $a',\ b'$ and $a'b'$ need to be from the same conjugacy class to satisfy $(\boldsymbol{\sigma})$. □

We would like to lift a triple $(a,\ b,\ c)$ of Ω_H, from an S_5-complement H of G, to a triple $(a',\ b',\ c')$ of Ω_G such that $a' = (n_a\ ,\ a)$, $b' = (n_b\ ,\ b)$ and $c' = (n_c\ ,\ c)$, where $n_a,\ n_b,\ n_c \in N$.

Lemma 3.41. *(i) The vectors* $n_a,\ n_b,\ n_c$ *must be fixed by* $a,\ b,\ c$ *respectively.*

(ii) There are only 8 *possible pairs* (n_a, n_b) *such that* $a',\ b',\ a'b'$ *are all in class* $2f$ *and* 8 *other pairs such that* $a',\ b',\ a'b'$ *are all in class* $2g$.

Proof. The proof of (i) is obvious since $a',\ b',\ c'$ are involutions, for example $a'^2 = (\emptyset, 1) = (n_a + n_a^a, 1)$ so that $n_a \in Fix_N(a)$. For (ii) we can look, without loss of generality, at our previous example 3.36 for a triple on Ω_H: $a = (1,2)(3,4),\ b = (1,3)(2,4),\ c = (4,5)$ of H acting on S as $(1,5)(2,3)$, $(1,5)(4,6)$, $(2,3)(4,6)$, and $(1,6)(2,4)(3,5)$ respectively, with the fixed points of each element being as described on the previous page. For each $n_a \in S_{2f}(a)$ there are exactly two elements $n_b \in S_{2f}(b)$ such that $n_{ab} := n_a + n_b$ is in $S_{2f}(ab)$. For example if we let $n_a = \{1,5\}$ then we must take $n_b = \{1,5\}$ or $n_b = \{1,5,4,6\}$, so that $n_{ab} = \emptyset$ or $\{4,6\}$ is in $S_{2f}(ab)$, in order to have $a',\ b',\ a'b'$ all conjugate in $2f$. An identical argument holds for $n_a \in S_{2g}(a)$. □

Proposition 3.42. *The only subgroups of* G *containing an* S_5 *complement* H *of* N *are; H itself,* $Z(G) \times H \cong 2 \times S_5$ *and* G.

Proof. The orbits of a complement H on N are $\emptyset$, $\{z\}$, $\big\{\{i,\ j\}\big\}_{i \neq j}$ and $\big\{\{i_1,\ i_2,\ i_3,\ i_4\}\big\}_{i_1 \neq i_2 \neq i_3 \neq i_4}$, where $z' = (z, 1)$ is the central element of G. From the action of H on N we can form the subgroups H, $\langle z' \rangle \times H$, and G and no other. □

Lemma 3.43. *A triple* $(a,\ b,\ c)$ *from* Ω_H *cannot be lifted to a triple* $(a',\ b',\ c')$ *generating a group isomorphic to* $2 \times S_5$*, where all the following conditions are satisfied:*

(i) $a' = (n_a, a),\ b' = (n_b, b),\ c' = (n_c, c)$*, for* $n_a,\ n_b,\ n_c \in N$*,*

(ii) $(a',\ b',\ c')$ *satisfies the same presentation as* Q*,*

(iii) *Products of pairs of elements from the conjugacy classes of* $a',\ b',\ a'b',\ c'$ *have order no greater than* 6*.*

Proof. Condition (iii) fails as we need $n_a,\ n_b,\ n_{ab}$ to be either $\emptyset$ or $\{z\}$, and all conjugate by Proposition 3.40 part (i), which is impossible by Proposition 3.38. Indeed if $n_a,\ n_b,\ n_{ab}$ are all equal to $\emptyset$ then they generate H, and if all are equal to $\{z\}$ we get $a'b' = (z, ab)$ which contradicts $a'b' = (z, a) \cdot (z, b) = (\emptyset, ab)$. Similarly if one, or two, of $n_a,\ n_b,\ n_{ab}$ is, or are, equal to $\{z\}$ then $a',\ b',\ a'b'$ cannot all be conjugate by Proposition 3.38. □

Proposition 3.44. *There are* 2^6 *liftings of a triple* $(a,\ b,\ c)$ *of* Ω_H *to a triple* $(a',\ b',\ c')$ *of* Ω_G *and* 2^6 *liftings of* $(a,\ b,\ c)$ *to a triple* $(a',\ b',\ c')$ *of* $\Omega_{H'}$*, where* H' *is another* S_5 *complement in* G*.*

Proof. From Lemma 3.43, we can only lift $(a,\ b,\ c)$ of Ω_H to a triple $(a',\ b',\ c')$ of Ω_G or a triple $(a',\ b',\ c')$ of $\Omega_{H'}$ for $H' \neq H$ another S_5 complement of N in G. From Lemma 3.41 there are 8 possibilities for the pairs (n_a, n_b) giving $a',\ b',\ c'$ conjugate in $2g$, and 8 pairs giving conjugates in $2f$. For n_c we can take any of the 8 fixed points of c. The key to see whether the group generated by $\{a',\ b',\ c'\}$ is an S_5 complement of G is to express (2)-cycles of H, which are conjugates of c, in the generators $a,\ b,\ c$, so that $(2,2)$-cycles can be expressed as products of two conjugates of c. Taking $a,\ b,\ c$ as in example 3.36 we let ϵ be the $(2,2)$-cycle $\epsilon := (2,4)(3,5)$. It can be written as $\epsilon = c^{bc} \cdot c^a$ and we call $\epsilon' := n_\epsilon \epsilon$ the lift of ϵ obtained from the lift of $a,\ b,\ c$ to $a',\ b',\ c'$. One can easily check that for 4 of the fixed points of c we get $n_\epsilon \notin Fix_N(\epsilon)$ so that ϵ' has order 4, so $\epsilon'^2 \in N$ and hence $a',\ b',\ c'$ generate G. For the 4 other fixed points of c we have $n_\epsilon \in Fix_N(c)$ so that $a',\ b',\ c'$ generate an S_5 complement H' of N in G. □

Corollary 3.45. *There are four classes of* S_5*-complements in* G*.*

Proof. For H an S_5-complement to N in G it is clear that $N_G(H) = \langle z \rangle \times H \cong 2 \times S_5$. Hence the conjugacy class H^G of H has size 2^4 by the Orbit-Stabiliser Theorem. Since there are 2^6

possible liftings of a triple $(a,\ b,\ c)$ of Ω_H to a triple $(a',\ b',\ c')$ of $\Omega_{H'}$, where H' is another S_5 subgroup of G, then there must be $2^6/2^4 = 4$ conjugacy classes of S_5-complements. □

Remark 3.46. We saw $H \cong S_5$ had one fixed point z in N so that $H^0(N,H) \cong \mathbb{Z}/2\mathbb{Z}$. From the above corollary $H^1(N,H) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Lastly with Magma we computed $H^2(N,H) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; there are four equivalence classes of extensions of 2^5 by S_5 with respect to the action ϕ.

We give now a brief example of the two different liftings.
First we look at a lifting to another complement. We let $n_a = \{2,3\},\ n_b = \emptyset, n_c = \emptyset$, so that $n_{ab} = \{2,3\}$, where $a,\ b,\ c$ are as in our previous examples 3.36 and 3.39. The lift of $(2,4)(3,5)$ in G is $\epsilon := c'^{b'c'} \cdot c'^{a'} = (\{2,4,5,6\}, c^{bc} \cdot c^a)$, where $c^{bc} \cdot c^a$ acts as $(2,4)(5,6)$ on S. Hence $\{2,4,5,6\} \in Fix_N(c^{bc} \cdot c^a)$ and so ϵ has order 2 and is in class $2g$. From the above proof we have lifted the set of generators of a complement to a set generating another complement.
Secondly we give an example to a lifting of a generating set to one generating the whole of G. We let $n_a = \{4,6\},\ n_b = \{z\},\ n_c = \emptyset$, so that $n_{ab} = \{1,2,3,5\}$. The lift of $(2,4)(3,5)$ in G is equal to $\epsilon := c'^{b'c'} \cdot c'^{a'} = (\{1,2,3,5\}, c^{bc} \cdot c^a)$ where $\{1,2,3,5\} \notin Fix_S(c^{bc} \cdot c^a)$. Hence $\epsilon^2 = (\{2,4,5,6\}, 1) \in N$.

From the proof of Proposition 3.44 we can deduce the following corollary.

Corollary 3.47. *The following assertions hold:*

1) S_5 *is isomorphic to the quotient of* $G^{(6,6,6;\ 5,5,5;\ 4)}$ *by the relation* $(c^a \cdot c^{bc})^2 = 1$.

2) *Let* $\{a',\ b',\ c'\} \in \Omega_G$. *Then the central element* $(z,1)$ *of* G *can be written as* $(z,1) = x^{a'}x^{b'}x^{c'}x^{c'a'}$ *where* $x = (c'^{a'} \cdot c'^{b'c'})^2$. □

Next the following lemma is readily checked by direct calculations on a given triple of Ω_G.

Lemma 3.48. *Let* $\{a',\ b',\ c'\} \in \Omega_G$. *Then the elements* $a' \cdot b'^{c'}$ *and* $a' \cdot (a'b')^{c'}$ *have order* 5 *and the element* $c' \cdot b'^{c'a'}$ *has order* 4. □

We recall that we defined $Q := G^{(6,6,6;\ 5,5,5;\ 4)}$ and from Proposition 3.33 $|Q| = 3840$. Hence from Lemmas 3.48 and 3.43 part (3), we can deduce the following.

Corollary 3.49. *The group* G *is isomorphic to* $Q \cong G^{(6,6,6;\ 5,5,5;\ 4)} \cong 2^5 :_\phi S_5$. □

3.3.3 The largest 6-transposition quotient of $G^{(6,6,6;\ 6,6,6)}$

Throughout this subsection we let $G := G^{(6,6,6;\ 6,6,6)}$. We will prove the following theorem.

Theorem 3.50. *The largest quotient of G satisfying* $(\boldsymbol{\sigma})$ *is $Q := G/\langle (c^a \cdot c^{bc})^3 \rangle$ which is isomorphic to $(3^4 : 2) : (3_+^{1+2} : 2^2)$.*

We start by finding the isomorphism type of G, which is $(3^5 : 2) : (3_+^{1+2} : 2^2)$ and we show that $(\boldsymbol{\sigma})$ is not satisfied by G as there exists pairs of conjugates of c whose product has order 9; for example $c^a \cdot c^{bc}$. We then prove that quotienting G by the relation $(c^a \cdot c^{bc})^3 = 1$ gives a group isomorphic to $(3^4 : 2) : (3_+^{1+2} : 2^2)$ where $(\boldsymbol{\sigma})$ holds true.

We denote by $G^{(6,6,6;\ 6,6,6;\ r_4)}$ the group with presentation:

$$G^{(6,6,6;\ r_1,r_2,r_3;\ r_4)} := \langle a, b, c \mid a^2,\ b^2,\ c^2,\ (ab)^2,\ (ac)^m,\ (bc)^n,\ (abc)^p,\ (ab^c)^6,\ (abb^c)^6,\ (aba^c)^6,\ (cb^{ca})^{r_4} \rangle.$$

The next lemma was obtained with Magma.

Lemma 3.51. *The group G coincides with $G^{(6,6,6;\ 6,6,6;\ 6)}$ and has order $52488 = 2^3 \cdot 3^8$.* □

By the above lemma, the element $R_4 = c \cdot b^{ca}$ has order 6 in G and we use this to find useful quotients of G.

Proposition 3.52. *Let $K := G^{(6,6,6;\ 6,6,6;\ r_4)}$ where $r_4 \in [1, 6]$ then:*

(i) *if $r_4 \in \{1, 5\}$ then $K \cong D_{12}$,*

(ii) *if $r_4 \in \{3\}$ then $K \cong G^{(3,6,6)} \cong 3_+^{1+2} : 2^2$,*

(iii) *if $r_4 \in \{2, 4\}$ then $K \cong 2 \times G^{(3,6,6)} \cong 2 \times (3_+^{1+2} : 2^2)$.*

Proof. (i) If $r_4 = 1$ then $b = c^{ac}$ so that $K = \langle a,\ c \rangle \cong D_{12}$ and a similar argument follows for $r_4 = 5$ since the element R_4 has order 6 in G.
(ii) If $r_4 = 3$ then $(c \cdot b^{ca})^3 = 1$ so that $bcacacbc = cacacbcaca$. The left hand side is equal to:

$$b(ca)^3bac = b(ac)^3bac = (abc)acacbac = (cba)^5acacba = (cba)^4cbcb(bacbac) = ((cb)^2)^{(abc)^2},$$

and the right hand side is equal to:

$$(ca)^3bacaca = (ac)^3bacaca = (cb)^{acaca},$$

hence bc and its square $(bc)^2$ must have the same order and since we require bc to have order dividing 6 this forces bc to have order 3. Hence K is a quotient of $G^{(6,3,6)} \cong G^{(3,6,6)} \cong 3^{1+2}_{+} : 2^2$. It is easy to find a set of generators for $G^{(3,6,6)}$ that satisfy the same presentation as K so that $K \cong 3^{1+2}_{+} : 2^2$.

(iii) For $r_4 = 2$ we obtain a commutator relation $[b, (ac)^3] = 1$ and since a and c also commute with the involution $(ac)^3$ we can rewrite K as $\langle (ac)^3 \rangle \times \langle a,\ a^c,\ b \rangle$. The generators of the subgroup $\langle a,\ a^c,\ b \rangle$ of G satisfy the same presentation as $G^{(3,6,6)}$ hence K is a quotient of $2 \times (3^{1+2}_{+} : 2^2)$. To prove the isomorphism we define a group $H := \langle z \rangle \times G^{(3,6,6)}$ where z is a central involution of H, and lift a set of generators $\{a',\ b',\ c'\}$ for the group $G^{(3,6,6)}$ to a new triple of generators $a = za',\ b = zb',\ c = c'$. It is now trivial to check that the generators $\{a,\ b,\ c\}$ satisfy the same presentation as the generators of K. □

Similarly to the proof of Proposition 3.11, we can prove that G has a subgroup H where:

$$H := \langle a,\ b,\ b^c \rangle = \langle (a \cdot b^c)^2, (bc)^2 \rangle \times \langle a, b \rangle \cong G^{(6,3,6)} \cong 3^{1+2}_{+} : 2^2.$$

We let y be the involution:

$$y := R_4^3 = (c \cdot b^{ca})^3$$

and we define $M := \langle y \rangle^G$ to be the closure of $\langle y \rangle$ in G.

By part (ii) of Proposition 3.52 we have $G/M \cong 3^{1+2}_{+} : 2^2$ where $|M| = 3^5 \cdot 2$. Clearly $R_4 \notin H$ and in fact $y \notin H$ so that $G = M : H$.

Next we let x be the following element:

$$x := (c \cdot a^{cb})^2,$$

which has order 3 since $c \cdot a^{cb}$ must have the same order in G as $R_4 = c \cdot b^{ca}$ by symmetry in a and b of the presentation for G. We denote by N the closure $\langle x \rangle^G$ of $\langle x \rangle$ in G and by part (iii) of Proposition 3.52 we have $G/N \cong 2 \times (3^{1+2}_{+} : 2^2)$.

Proposition 3.53. *In G we have the inclusion of subgroups $N \subseteq M$.*

Proof. Within this proof we let $s := c \cdot b^{ca}$ and $t := c \cdot a^{cb}$. It is easy to show that $st = t^{-1}s^{-1}$, $ts = s^{-1}t^{-1}$ and $s^{-1}t = t^{-1}s$. Let us prove the former equality: $st = cacbcacbcacb = \big((acbc)^3\big)^c$ so st is an involution since $acbc$ has order 6. Using these equalities we get that:

$$x^y = (t^2)^{s^3} = t^{-2} = x^2 \quad \Rightarrow \; x = y^x y \quad \Rightarrow \; \langle x \rangle^G \subseteq \langle y \rangle^G \quad \Rightarrow \; N \subseteq M.$$

□

Proposition 3.54. *The group N is elementary abelian of order $3^5 = 243$ and $\{x,\ x^a,\ x^b,\ x^{ab}, x^{bc}\}$ generates N.*

Proof. The proof is similar to that of Lemmas 3.18 and 3.30, and the calculations of the commutators $[x_1, x_2] = 1$ for all $x_1, x_2 \in \{x,\ x^a,\ x^b,\ x^{ab}, x^{bc}\}$ were checked with Magma. □

Proposition 3.55. *The subgroup M can be written as a semidirect product $N : \langle y \rangle \cong 3^5 : 2$ where y inverts every element of N.*

Proof. The only thing to check is the action of y on N. Define a set $\mathcal{S} := \{y,\ yy^a,\ yy^b,\ yy^{ab},\ yy^{bc}\}$.

Claim 1: The set $\mathcal{S}$ generates a subgroup of M isomorphic to $3^4 : 2$.

By Proposition 3.54 the set $\{x,\ x^a,\ x^b,\ x^{ab}, x^{bc}\}$ generates N so that for all $v \in \{a,\ b,\ ab,\ bc\}$ we have that $x^v \neq x$ and $x^v \neq x^2$. This implies $c \cdot a^{cb} \neq (c \cdot a^{cb})^v$ and $(c \cdot a^{cb})^2 \neq (c \cdot a^{cb})^v$ for all $v \in \{a,\ b,\ ab,\ bc\}$. The permutation $(a,\ b)$ clearly does not change the isomorphism type of G and it sends $x = (c \cdot a^{cb})^2$ to $(c \cdot b^{ca})^2 = y(c \cdot b^{ca})^{-1}$ and we can conclude $c \cdot b^{ca} \neq (c \cdot b^{ca})^v$ and $(c \cdot b^{ca})^2 \neq (c \cdot b^{ca})^v$ for all $v \in \{a,\ b,\ ab,\ bc\}$. Thus the involutions $\{y,\ y^a,\ y^b,\ y^{ab},\ y^{bc}\}$ are pairwise distinct, and none is equal to a product of the other ones. Now consider the set of elements $\mathcal{S}_y := \{yy^a,\ yy^b,\ yy^{ab},\ yy^{bc}\}$, which are all non-trivial elements of N, since $M \lhd G$ and $M \cong 3^5 : \langle y \rangle$. Clearly the subgroup $\langle \mathcal{S}_y \rangle$ has order 3^4 to avoid contradicting Proposition 3.54, and hence $\langle \mathcal{S} \rangle \cong 3^4 : \langle y \rangle$.

Claim 2: The element y sends each element of $\mathcal{S}' := \{x,\ yy^a,\ yy^b,\ yy^{ab},\ yy^{bc}\}$ to its square.

From the proof of Proposition 3.53 we had $x^y = x^2$. For $v \in \{a,\ b,\ ab,\ bc\}$ the element yy^v is in N so without loss of generality it can be written $yy^v = \chi^\epsilon$ where $\chi = (x)^{\epsilon_1}(x^a)^{\epsilon_2}(x^b)^{\epsilon_3}(x^{ab})^{\epsilon_4}(x^{bc})^{\epsilon_5}$ where $\epsilon_i \in \{0, 1, 2\}$ for all i and such that $\epsilon := (\epsilon_1, \ldots, \epsilon_5)$. We notice the following:

$$(yy^v)^y = (\chi^\epsilon)^y = y^v y = (yy^v)^2 = (\chi^\epsilon)^2.$$

Claim 3: The set $\mathcal{S}' := \{x,\ yy^a,\ yy^b,\ yy^{ab},\ yy^{bc}\}$ generates N.

We want to show that $x \notin \{yy^a,\ yy^b,\ yy^{ab},\ yy^{bc}\}$. If $x \in \langle yy^a,\ yy^b,\ yy^{ab},\ yy^{bc}\rangle$ then there exists v as above so that $yy^v = x\chi'$ where $\chi' = (x^a)^{\epsilon_1}(x^b)^{\epsilon_2}(x^{ab})^{\epsilon_3}(x^{bc})^{\epsilon_4}$ and $\epsilon_i \in \{0,1,2\}$ for all i. This implies $x^v\chi'^v = x^2\chi'^2$ so that either $x^2 = x^v$ and $\chi'^2 = \chi'^v$ or $x^2 = \chi'$ or $x = \chi'$ which are all impossible.

We have shown $\langle \mathcal{S}' \rangle = N$ and y sends each element of N to its square. We remark that the latter implies y can be represented as the central involution of $GL_5(3)$. □

Corollary 3.56. *The group G can be written as $M : H \cong (3^5 : 2) : (3^{1+2}_+ : 2^2)$.* □

Proposition 3.57. *The group G does not satisfy* $(\boldsymbol{\sigma})$.

Proof. We prove that the element $\eta := c^a \cdot c^{bc}$ has order 9. First we notice that $c^a \cdot c^{bc} = (ac)^2(bc)^2$ where $(ac)^2$ is an element of order 3 in H and $(bc)^2$ is another element of order 3 that is in neither M nor H. Let us write $h := (ac)^2$ and $mk := (bc)^2$ where $k \in H$ has order 3 and $m \in M$ must satisfy $m \cdot m^{h^2} \cdot m^h = 1$ in M, so that m has order 3. Hence the product $(ac)^2(bc)^2 = hmk = m^h(hk)$ where clearly hk is an element of order 3 since $H \cong 3^{1+2}_+ : 2^2$ so either η has order 3 if it satisfies the equality $m \cdot m^{(hk)^2} \cdot m^{hk} = 1$ in M, otherwise it has order 9. In particular the element η^3 is either the identity in G or an element of N.

Claim: the element η cannot have order 3.

We write η as an expression containing elements of N. In fact we notice:

$$\eta^3 = acacbcbcacacbcbcacacbcbc = abcb(x^b(x^2)^{cbc})cbcbcba \text{ so that } (\eta^3)^{abcb} = x^b(x^2)^{cbc} \cdot b^c.$$

Hence if η had order 3 we would have that an element of order 3 in N is equal to an element of order 2 in G;

$$x^b(x^2)^{cbc} = b^c$$

which is a contradiction. Hence η has order 9 and so G does not satisfy property $(\boldsymbol{\sigma})$. □

We now let Q be the quotient of G by the relation $\eta^3 = 1$ where $\eta^3 = (c^a \cdot c^{bc})^3$.

Proposition 3.58. *The subgroup $\langle \eta^3 \rangle$ is normal in G and $Q \cong G/\langle \eta^3 \rangle \cong (3^4 : 2) : (3^{1+2}_+ : 2^2)$ has order* 17496 *and satisfies property* $(\boldsymbol{\sigma})$.

Proof. From the proof of Proposition 3.57 the element $\eta^3 = \left((ac)^2(bc)^2\right)^3$ is in N and has order 3, so that $(\eta^3)^{-1} = \eta^6 = \left((cb)^2(ca)^2\right)^3$. It is easy to calculate the following:

$$(\eta^3)^a = (\eta^6)^{ac} \text{ and } (\eta^6)^a = (\eta^6)^{cac}$$
$$(\eta^3)^b = (\eta^6)^{cb} \text{ and } (\eta^6)^b = (\eta^6)^{cbc}$$

so clearly $(\eta^3)^c = \eta^6$ and $(\eta^3)^{(ac)^2} = \eta^3$ and $(\eta^3)^{(bc)^2} = \eta^3$. The latter two equalities hold true if $(\eta^3)^a = \eta^3 = (\eta^3)^b$. Hence the subgroup $\langle\eta\rangle \cong 3$ is normal in G so that $Q = G/\langle\eta\rangle$. Therefore Q is a group isomorphic to $(3^4 : 2) : (3^{1+2}_{+} : 2^2)$ of order 17496.

We now prove that Q satisfies $(\boldsymbol{\sigma})$. Since G is soluble by Burnside $p^a \cdot q^b$ Theorem, 1.14, it was possible to write a short Magma program to find the orbits of H on N. The only actions of elements of H on N that would lead to products of involutions having order greater than 6 is that of elements of order 3 or 6 in H which could give elements of order 9 or 18 in G. We first checked the sizes of the orbits of all conjugacy class representatives for elements of order 6 and 3 in H. For the representatives of order 6 their orbits' sizes are either $1, 2, 3$ or 6, and when the size of the orbit is 3 or 6 the elements in the orbit sum up to 0 *mod* 3, so that there are no elements of order 18 in G.

For the representatives of order 3 their orbits' sizes are all 1 or 3. Now there are four conjugacy classes of elements of order 3 in H and for three of them the representatives have their orbits of size 3 whose elements sum up to 0 *mod* 3. The other conjugacy class of elements of order 3 contain the conjugates of the element $(ac)^2$ and it has orbits of size 3 on N whose elements do not sum up to 0 *mod* 3. Hence there exist elements of order 9 arising from the action of H-conjugates of $(ac)^2$ on N. Using Magma we can compute that there are three conjugacy classes of order 9 in G, and moreover the H-part of their representatives is conjugate to $a \cdot a^c$, so that the cubes of the representatives of the conjugacy classes of order 9 are conjugate and all belong to N. Hence $Q := G/\langle\eta^3\rangle$ contains no elements of order 9. It can be easily shown that Q contains no elements of order 4; this can be reduced to showing that no product of involutions yh where h is an involution H can have order 4. Hence Q has exponent 6 and so satisfies $(\boldsymbol{\sigma})$. □

3.3.4 Two remarks on Burnside groups

In September 2013 J. I. Hall remarked to the author that the groups $G^{(3,6,6)}$ and $G_{11} := G^{(6,6,6;\ 6,6,6)}/\{(c^a \cdot c^{bc})^3 = 1\}$ contain Burnside groups as subgroups.

Definition 3.59. The **free Burnside group** $B(n, m)$ is the free group of rank n and exponent m.

Clearly the group $B(1,m)$ is the cyclic group of order m. For any finite n and $k = 2, 3, 4$ or 6 it is known that $B(n,k)$ is finite from results of W. Burnside for the cases $k = 2$ and $k = 3$, I. N. Sanov for the case $k = 4$ and M. Hall for the case $k = 6$.
The first two statements in the theorem below were proved by W. Burnside in [Bur02] and the order of $B(n,3)$ was found by F. Levi and B. L. Van der Waerden in [LdW30].

Theorem 3.60. *The group $B(n,2)$ is an elementary abelian 2-group of order 2^n. The group $B(n,3)$ is finite and its order is equal to 3^k where $k := n + \binom{n}{2} + \binom{n}{3}$.* □

Proposition 3.61. *The group $G^{(3,6,6)}$ is isomorphic to $B(2,3) : A$ where $A \cong 2^2$.*

Proof. From the proof of Proposition 3.11 it is clear that the extraspecial group 3^{1+2}_+ is isomorphic to $B(2,3)$, and so $G^{(3,6,6)} \cong B(2,3) : A$ where $A := \langle \psi,\ \phi \rangle \cong 2^2$ such that if $B(2,3)$ is generated by $x_1,\ x_2$ then ψ inverts x_1 and fixes x_2 whilst ϕ inverts x_2 and fixes x_1. □

Proposition 3.62. *The group G_{11} is isomorphic to a semidirect product $B(3,3) : A$ where $A \cong 2^2$.*

Proof. Let $a,\ b,\ c$ be three involutions generating the group:

$$G_{11} := G^{(6,6,6;\ 6,6,6)}/\{(c^a \cdot c^{bc})^3 = 1\} \cong (3^4 : 2) : (3^{1+2}_+ : 2^2).$$

From the previous subsection the group G_{11} can be written as a semidirect product $M : H$ where $H = \langle a, b, b^c \rangle \cong 3^{1+2}_+ : 2^2$ and $M = N : \langle y \rangle \cong 3^4 : 2$ where $y = (c \cdot b^{ca})^3$ and N is the normal closure of $x = (c \cdot a^{cb})^2$ in G_{11}. From the proof of Proposition 3.11 $\langle (bc)^2, (a \cdot b^c)^2 \rangle \cong 3^{1+2}_+$. Define $R := \langle N, (bc)^2, (a \cdot b^c)^2 \rangle \cong 3^4 : 3^{1+2}_+$ and define $S := \langle a, b, y^{ac} \rangle$, then $G_{11} = R : S$ where $S \cong 2^3$ since a and b commute and G_{11} has exponent 6 from the proof of Proposition 3.58. The group R can be generated by the three elements: $x,\ (bc)^2$ and $(a \cdot b^c)^2$ and since R has exponent 3 the proposition is proved. □

In the next theorem the finiteness was proved by M. Hall in [Hal58] and the order was proved by P. Hall and G. Higman in [HH56].

Theorem 3.63. *Let $n \in \mathbb{N}$, then the group $B(n,6)$ is finite of order $2^a \cdot 3^b$ where $a = 1 + (r-1)3^c$, $b = 1 + (r-1)2^r$ and $c = r + \binom{r}{2} + \binom{r}{3}$.* □

Proposition 3.64. *The group G_{11} is a homomorphic image of the group $B(3,6)$ of order $2^{4375} \cdot 3^{17}$.* □

3.4 Shapes of the Majorana representations

In the last section of Chapter 4 we show that the group $G_5 \cong L_2(11)$ affords a unique Majorana representation whose Majorana algebra is equal to a subalgebra of $V_{\mathbb{M}}$. For the other groups G_i, $i \in [1, 11]$, from Theorem 3.3, the task of describing their possible Majorana representations requires significantly more computations due to the larger number of conjugacy classes of involutions involved, and therefore it should be attempted with the help of a computer program.

In September 2012 the author of this thesis communicated to Á. Seress three triples of involutions generating the groups G_{11}, G_{10} and G_9 respectively as quotients of a $G^{(m,n,p)}$ group, in the hope that his *GAP* computer program implementing the procedure from [Ser12] (as discussed in subsection 2.4.3) would give the dimension and inner product values of the Majorana algebras obtained from the Majorana representations of G_9, G_{10} and G_{11}. These groups were chosen because they contain most of the other groups G_i as subgroups. Unfortunately the procedure was not successful, so instead one would want to look at the Majorana representations of proper subgroups, thus defining Majorana subrepresentations. Generators of the following four quotients of the groups G_i, which are all isomorphic to subgroups of the groups G_i, were also fed to Á. Seress's *GAP* program:

$$\begin{aligned} G_9/N_9 &\cong S_3 \times S_3 \times 2 \quad \text{where} \quad N_9 \cong 2^4, \\ G_9/Z(G_9) &\cong 2^4 : (S_3 \times S_3), \\ G_{10}/N_{10} &\cong S_5 \quad \text{where} \quad N_{10} \cong 2^5, \\ G_{10}/Z(G_{10}) &\cong 2^4 : S_5, \\ G_{11}/N_{11} &\cong 2 : (3_+^{1+2} : 2^2) \quad \text{where} \quad N_{11} \cong 3^4. \end{aligned}$$

Unfortunately for those subgroups too, the *GAP* program was unsuccessful. The passing away of Á. Seress in February 2013 prevented further trials of his *GAP* program on the smallest of the groups G_i. The time scale for this thesis did not permit the search for an algorithm able to surpass the difficulties encountered by Á. Seress's program.

In this section we complete the preliminary task of finding all possible shapes, defined in Definition 2.23, of the Majorana representations $\mathcal{R}_i = (G_i, T_i, X_i)$ of the groups G_i for all $i \in [1, 11]$, such that T_i is the union of the conjugacy classes of a, b, ab and c, where a, b, c are three involutions, two of which commute $ab = ba$, which generate G_i as a quotient of a $G^{(m,n,p)}$ group

as indicated in Table 3.1 of Theorem 3.3.

For each representation $\mathcal{R}_i$ we give the number of its possible shapes and for all except $\mathcal{R}_9$ and $\mathcal{R}_{11}$ we give the conjugacy classes involved in each shape in Appendix B. Each shape of $\mathcal{R}_i$ dictates which types of dihedral Majorana subalgebras are contained in the Majorana algebra X_i. Using Norton's Table 3.2 we can find which shapes are allowed if X_i were a subalgebra of $V_{\mathbb{M}}$.

Theorem 3.65. *Let G_i, for $i \in [1,11]$, be the groups listed in Theorem 3.3. For each $i \in [1,11]$ we let $\mathcal{R}_i = (G_i, T_i, X_i)$ be a Majorana representation of G_i where T_i is the union of the conjugacy classes of a, b, ab and c, for a, b, c three involutions generating G_i as a quotient of a $G^{(m,n,p)}$ group as in Table 3.1. Then the total number of shapes of $\mathcal{R}_i$ and the number of shapes allowed in $V_{\mathbb{M}}$ is as in Table 3.7 below.*

Name	Isomorphism Type	$G^{(m,n,p)}$ (m,n,p)	Added relations $R_i^{r_i} = 1$ $(r_1, r_2, r_3, r_4, r_5)$	Total number of possible shapes	Number of shapes allowed in $V_{\mathbb{M}}$
G_1	$2\ wr\ 2^2$	$(4,4,4)$		2^5	2
G_2	$(S_3 \times S_3) : 2^2$	$(4,4,6)$		2	1
G_3	$2^4 : D_{10}$	$(4,5,5)$		2^2	2
G_4	$2 \times S_5$	$(4,5,6)$		1	1
G_5	$L_2(11)$	$(5,5,5)$		1	1
G_6	$(2^4 :_{\phi_1} D_{12}) \times 2$	$(4,6,6)$	$(4,-,-,-,-)$	2^5	1
G_7	$2^4 :_{\lambda_2} A_5$	$(6,5,5)$	$(5,-,-,-,-)$	2	1
G_8	$2 \times S_6$	$(6,6,5)$	$(4,-,-,-,-)$	1	1
G_9	$\left(2^4 : (S_3 \times S_3)\right) \times 2$	$(6,6,6)$	$(4,-,-,-,-)$	2^2	0
G_{10}	$2^5 :_{\phi} S_5$	$(6,6,6)$	$(5,\ 5,\ 5,\ 4,-)$	2^2	1
G_{11}	$(3^4 : 2) : (3_+^{1+2} : 2^2)$	$(6,6,6)$	$(6,\ 6,\ 6,-,\ 3)$	2^4	0

TABLE 3.7: Number of shapes of the Majorana representations of the groups satisfying $(\boldsymbol{\sigma})$

Proof. The number of possible shapes for the Majorana representations $\mathcal{R}_9 = (G_9, T_9, X_9)$ and $\mathcal{R}_{11} = (G_{11}, T_{11}, X_{11})$ were calculated with Magma. The code written in Magma is rather elementary since the groups G_9 and G_{11} are both soluble and of exponent 6. We do not give a full description of the shapes of $\mathcal{R}_9$ and $\mathcal{R}_{11}$ due to the large number of conjugacy classes involved in them. From Norton's Table 3.2 the groups G_9 and G_{11} cannot be $2A$-embedded in

$\mathbb{M}$ so that for none of the shapes of $\mathcal{R}_9$ and $\mathcal{R}_{11}$ could the Majorana algebras X_9 and X_{11} be subalgebras of $V_{\mathbb{M}}$.

The fact that $\mathcal{R}_5$ has a unique possible shape and that this shape is allowed in $V_{\mathbb{M}}$ can be deduced from Propositions 4.1 and 4.21 of Chapter 4.

A full description of the shapes of the representations $\mathcal{R}_i$ for $i \in [1, 11]$, $i \neq 5, 9, 11$, can be found in Appendix B. □

Chapter 4

The $L_2(11)$-subalgebra of the Monster algebra $V_{\mathbb{M}}$

4.1 Motivation and Main result

The main reference for this chapter is the article [Dec14] written by the author of this thesis.

In this chapter, we investigate a subalgebra $V = \langle\langle a_x, a_y, a_z\rangle\rangle$ of the Monster algebra $V_{\mathbb{M}}$ such that the dihedral subalgebra $\langle\langle a_x, a_y\rangle\rangle$ has type $2A$ and each of the dihedral subalgebras $\langle\langle a_x, a_z\rangle\rangle$, $\langle\langle a_y, a_z\rangle\rangle$ and $\langle\langle a_{xy}, a_z\rangle\rangle$ has type $5A$. The vector a_{xy} is the $2A$-axis corresponding to the $2A$ involution xy (since a dihedral subalgebra $\langle\langle a_s, a_t\rangle\rangle$ of type $2A$ contains the axis a_{st}). Keeping in mind Conway's bijection $\mathcal{C}$ (2.1), we might ask whether there exists a subgroup of $\mathbb{M}$ generated by a triple of $2A$ involutions $\{x,\ y,\ z\}$ satisfying the relations:

$$x^2 = \ y^2 = \ z^2 = \ (xy)^2 = \ (xz)^5 = \ (yz)^5 = \ (xyz)^5 = 1.$$

A group affording the presentation

$$\langle x,\ y,\ z \mid x^2,\ y^2,\ (xy)^2,\ z^2,\ (xz)^5,\ (yz)^5,\ (xyz)^5\rangle$$

defines the Coxeter group $G^{(5,5,5)}$ and from [Cox39] it is isomorphic to the projective special linear group $L_2(11)$. From classical results on $L_n(p^k)$, [Dor72], $L_2(11)$ is a simple group of order $660 = 2^2 \cdot 3 \cdot 5 \cdot 11$ and it has a single conjugacy class of involutions which we denote by T, and whose size is 55.

Proposition 4.1. *There exists a monomorphism $\iota : L_2(11) \hookrightarrow \mathbb{M}$ such that $\iota(T) \subseteq 2A$ and ι is unique up to conjugacy in $\mathbb{M}$.*

Proof. In Table 5 of [Nor98] S. Norton gives the list of simple subgroups of $\mathbb{M}$ having their elements of order 5 in the $\mathbb{M}$-conjugacy class $5A$. From Norton's list there is only one conjugacy class of groups isomorphic to $L_2(11)$ containing $5A$ elements and their involutions belong to class $2A$. □

Throughout this chapter ι denotes the monomorphism as in Proposition 4.1, $G \cong L_2(11)$ denotes the image of ι, and T denotes the conjugacy class of involutions in G.

We can restate our aim to be the study of the subalgebra V of $V_{\mathbb{M}}$ generated by the set of 55 $2A$-axes $\{a_t \mid t \in T\}$. We determine the dimension of V and then find a spanning set for V. In the next section we prove the following theorem. We recall that $\iota_{\mathbb{M}}$ is the identity of the Monster algebra $V_{\mathbb{M}}$.

Theorem 4.2. *Let V be the subalgebra of $V_{\mathbb{M}}$ generated by the set of 55 $2A$-axes $\{a_t \mid t \in T\}$ where T is the class of involutions of the unique $2A$-generated $L_2(11)$-subgroup G of $\mathbb{M}$. Then*

1) *$dim(V) = 101$,*

2) *V is linearly spanned by the set $\{a_t \cdot a_s \mid t, \ s \ \in T\}$.*

3) *If $K = C_{\mathbb{M}}(G)$ then $C_{V_{\mathbb{M}}}(K) = V \oplus \iota_{\mathbb{M}}$.*

At the end of this chapter we will state a recent result of Á. Seress proving that V is isomorphic to the Majorana algebra of the unique Majorana representation of $L_2(11)$.

4.2 Properties and subgroup structure of $L_2(11)$

We present some of the standard properties of $G \cong L_2(11)$ used when calculating inner product values for V.

The group G is the automorphism group of the $(11, 5, 2)$-biplane, which we denote $\mathcal{B}$ (see [Tod33]).
$\mathcal{B}$ is a 2-symmetric design with 11 points, $\{p_1, \ldots, p_{11}\}$, and 11 lines, $\{l_1, \ldots, l_{11}\}$, such that

each line contains 5 points, each point lies on 5 lines, two lines intersect in exactly 2 points, and two points share exactly 2 lines. We call the incidence relation $p_i \in l_j$ a flag, which we denote $\alpha_{i,j}$, and the relation $p_i \notin l_j$ an anti-flag, which we denote by $w_{i,j}$.

From [Kan69], the lines of $\mathcal{B}$ can be obtained by finding a difference set l_1 of size 5, with elements from $\mathbb{Z}_{11}$, such that every integer modulo 11 appears exactly twice as a difference $i - j \bmod 11$ for i and j in l_1. We have that $l_1 = \{1, 3, 4, 5, 9\}$, which is the set of non-zero perfect squares in $\mathbb{Z}_{11}$, and all other lines l_k can be defined by $l_k = \{1 + k,\ 3 + k,\ 4 + k,\ 5 + k,\ 9 + k\}$, where $k \in \mathbb{Z}_{11}^*$ and addition is modulo 11.
The incidence matrix $\mathcal{N}$ of $\mathcal{B}$ is given below with the rows indexed by the points of $\mathcal{B}$, the columns indexed by the lines, and each flag is represented by a '1' and each anti-flag by a '0'.

1	0	1	1	1	0	0	0	1	0	0
0	1	0	1	1	1	0	0	0	1	0
0	0	1	0	1	1	1	0	0	0	1
1	0	0	1	0	1	1	1	0	0	0
0	1	0	0	1	0	1	1	1	0	0
0	0	1	0	0	1	0	1	1	1	0
0	0	0	1	0	0	1	0	1	1	1
1	0	0	0	1	0	0	1	0	1	1
1	1	0	0	0	1	0	0	1	0	1
1	1	1	0	0	0	1	0	0	1	0
0	1	1	1	0	0	0	1	0	0	1

We can represent G as a permutation group on 11 letters, so that $G \subset Sym(11)$, by letting G act on the indices of the points or lines such that the incidence structure of $\mathcal{B}$ is preserved.

The stabiliser $G(\alpha_{i,j})$ of a flag $\alpha_{i,j}$ is isomorphic to A_4, the stabiliser $G(w_{k,l})$ of an anti-flag $w_{k,l}$ is isomorphic to D_{10}, and the stabiliser of a line (or a point) is isomorphic to A_5. We can associate to a flag $\alpha_{i,j}$ a unique subgroup $S(\alpha_{i,j}) \cong C_2 \times C_2$ and to an anti-flag $w_{k,l}$ a unique subgroup $S(w_{k,l}) \cong C_5$ such that $N_G\big(S(\alpha_{i,j})\big) = G(\alpha_{i,j})$ and $N_G\big(S(w_{k,l})\big) = G(w_{k,l})$. It is easy to see that each involution t stabilises 3 flags and to deduce that $C_G(t) \cong D_{12}$. Similarly for $\langle h \rangle$ a subgroup of order 3 we can deduce $N_G(\langle h \rangle) \cong D_{12}$. There are only one class of involutions and one class of elements of order 3 in G, so we can let d be the G-invariant bijection between subgroups of

order 2 and 3 sending each involution t to the unique subgroup of order 3 commuting with t:

$$\begin{aligned} d: \ G^{(2)} &\to G^{(3)} \\ \langle t \rangle &\mapsto \langle h \rangle \end{aligned} \tag{4.1}$$

Furthermore, by [Kan69], G contains one class of subgroups isomorphic to the Frobenius group of order 55, see example 1.6, which we denote F_{55}. These are the four conjugacy classes of maximal subgroups of G; two non-conjugate classes of subgroups isomorphic to A_5 each of size 11 and each stabilising a point and a line, respectively, one class of subgroups isomorphic to D_{12}, and one class of subgroups isomorphic to the Frobenius group F_{55}.

4.3 The $L_2(11)$ subalgebra of $V_{\mathbb{M}}$

We start this section by finding an upper bound for $dim(V)$ based on the work of S. P. Norton ([Nor85], [Nor96], and [Nor98]). We then calculate the Gram matrix of a particular subset of V which provides a lower bound for $dim(V)$.

4.3.1 S. P. Norton's observations

The upper bound on $dim(V)$ stems from the following inclusion (see 1.7).

Lemma 4.3. $V \subseteq C_{V_{\mathbb{M}}}\big(C_{\mathbb{M}}(G)\big)$

Proof. By the definition of a $2A$-axis, a_t is fixed by $C_{\mathbb{M}}(t) \cong 2.BM$. Therefore $C_{\mathbb{M}}(G) = C_{\mathbb{M}}\big(\langle x, y, z\rangle\big) = \bigcap_{t=x,y,z} C_{\mathbb{M}}(t)$ fixes $V = \langle\langle a_x, a_y, a_z\rangle\rangle$ by $\mathbb{M}$-invariance of the algebra $V_{\mathbb{M}}$. □

We denote by K the group $C_{\mathbb{M}}(G)$. From Corollary 1.10 the dimension of the fixed space of K in $V_{\mathbb{M}}$ is equal to the inner product of characters $\langle \chi_{V_{\mathbb{M}}}\downarrow_K, \mathbb{1}_K\rangle_{\mathbb{R}K}$, where $\mathbb{1}_K$ is the trivial character of K, and $\chi_{V_{\mathbb{M}}}\downarrow_K$ is the character of $V_{\mathbb{M}}$ restricted to K.

We call an A_5-subgroup H of $\mathbb{M}$ an **$\mathbf{A_5}$ of type (2A, 3A, 5A)** if the elements of order 2, 3 and 5 of H are in the $\mathbb{M}$-conjugacy classes $2A$, $3A$ and $5A$ respectively.

Proposition 4.4. (i) *For K as above, $K \cong M_{12}$.*

(ii) *The conjugacy classes of G fuse into those $\mathbb{M}$ as follows:*

Class in G	$1a$	$2a = T$	$3a$	$5a$	$5b$	$6a$	$11a$	$11b$
Class in $\mathbb{M}$	$1A$	$2A$	$3A$	$5A$	$5A$	$6A$	$11A$	$11A$

(iii) *All A_5-subgroups of G are of type $(2A, 3A, 5A)$. Further, all A_5-subgroups H of type $(2A, 3A, 5A)$ are conjugate in $\mathbb{M}$ with $C_{\mathbb{M}}(H) \cong A_{12}$.*

Proof. The result from part (i) can be read from the entry 31 of Table 3 of [Nor85]. To prove (ii) we carry on from the proof of Proposition 4.1. From Table 5 of [Nor98] we deduce the inclusion $3a \subset 3A$. In the character table of $\mathbb{M}$, given in the Atlas [CCN+85], the information on p-powers (see 1.2.3) of elements $g \in 6A$ gives $g^2 \in 3A$ and $g^3 \in 2A$, and $6A$ is the unique conjugacy class of elements of order 6 with those p-powers, hence to avoid a contradiction we must have $6a \subset 6A$. Since $\mathbb{M}$ has a unique class $11A$ of elements of order 11 the classes $11a$ and $11b$ are subsets of $11A$. Part (iii) follows from part (ii) and Lemma 4 of [Nor85]. □

We let $A := C_{\mathbb{M}}(H) \cong A_{12}$ be the centraliser in $\mathbb{M}$ of H, an A_5 subgroup of type $(2A, 3A, 5A)$.

In the proof of Proposition 4.5 below find the fusion of the conjugacy classes of K and A into those of $\mathbb{M}$. We first determine the fusion of all but two conjugacy classes of K. This is then enough to determine the fusion of A, which in turn gives the fusion of the two remaining classes in K. We use the character tables of the Atlas and we follow its notation, by denoting the conjugacy classes of elements of order n in $\mathbb{M}$ by nA, $nB, \ldots$ (*etc*) in decreasing centralisers' orders. Similarly for K and A we use the notations nA_K, $nB_K, \cdots$, and nA_A, $nB_A, \cdots$, respectively.

Proposition 4.5. *For $K \cong M_{12}$ and $A \cong A_{12}$ as above, the fusion of their conjugacy classes into those of $\mathbb{M}$ is as described in the Tables 4.1 and 4.2 below. It yields:*

$$dim\ \left(C_{V_{\mathbb{M}}}(K)\right) = \langle \chi_{V_{\mathbb{M}}} \downarrow_K, \mathbb{1}_K \rangle_{\mathbb{R}K} = 102$$

Class in K	$1A_K$	$2A_K$	$2B_K$	$3A_K$	$3B_K$	$4A_K$	$4B_K$
p-powers						B	B
Class in $\mathbb{M}$	$1A$	$2A$	$2B$	$3B$	$3A$	$4A$	$4A$
Value of $\chi_{V_{\mathbb{M}}}$	$196,883$	4371	275	53	782	275	275
Class in K	$5A_K$	$6A_K$	$6B_K$	$8A_K$	$8B_K$	$10A_K$	$11A_K$
p-powers		BA	AB	A	B	AA	
Class in $\mathbb{M}$	$5A$	$6B$	$6A$	$8B$	$8B$	$10A$	$11A$
Value of $\chi_{V_{\mathbb{M}}}$	133	77	78	11	11	21	16

TABLE 4.1: Fusion of K in $\mathbb{M}$

Class in A	$1A_A$	$2A_A$	$2B_A$	$2C_A$	$3A_A$	$3B_A$	$3C_A$	$3D_A$	$4A_A$	$4B_A$	$4C_A$
p-powers									A	C	A
Class in $\mathbb{M}$	$1A$	$2A$	$2A$	$2B$	$3A$	$3A$	$3A$	$3B$	$4B$	$4A$	$4B$
Value of $\chi_{V_{\mathbb{M}}}$	$196,883$	4371	4371	275	782	782	782	53	51	275	51
Class in A	$4D_A$	$5A_A$	$5B_A$	$6A_A$	$6B_A$	$6C_A$	$6D_A$	$6E_A$	$6F_A$	$6G_A$	$7A_A$
p-powers	C			AA	AC	BB	BC	BA	CB	DC	
Class in $\mathbb{M}$	$4A$	$5A$	$5A$	$6A$	$6C$	$6A$	$6C$	$6A$	$6A$	$6B$	$7A$
Value of $\chi_{V_{\mathbb{M}}}$	275	133	133	78	14	78	14	78	78	77	50
Class in A	$8A_A$	$8B_A$	$9A_A$	$9B_A$	$9C_A$	$10A_A$	$10B_A$	$11A_A$	$11B_A$	$12A_A$	$12B_A$
p-powers	D	B	D	D	D	AA	BB			EA	AA
Class in $\mathbb{M}$	$8B$	$8B$	$9A$	$9A$	$9A$	$10A$	$10A$	$11A$	$11A$	$12C$	$12C$
Value of $\chi_{V_{\mathbb{M}}}$	11	11	26	26	26	21	21	16	16	6	6
Class in A	$12C_A$	$12D_A$	$14A_A$	$15A_A$	$15B_A$	$20A_A$	$21A_A$	$30A_A$	$35A_A$	$35B_A$	–
p-powers	BB	EC	AA	AA	AB	AA	AA	AAA	AA	AA	–
Class in $\mathbb{M}$	$12A$	$12C$	$14A$	$15A$	$15A$	$20B$	$21A$	$30B$	$35A$	$35A$	–
Value of $\chi_{V_{\mathbb{M}}}$	14	6	10	7	7	1	5	3	0	0	

TABLE 4.2: Fusion of A in $\mathbb{M}$

Proof. By part (i) of the previous proposition we have the inclusion of groups $H \subset G$, which implies $K \subset A \cong A_{12}$. In A, the elements with cycle decompositions $2^2 1^8$, $2^4 1^4$, and 2^6 have 8, 4, and no fixed points respectively in the natural action of A_{12} on 12 points, and so by Lemma 6 of [Nor85] they are mapped to the $\mathbb{M}$-conjugacy classes $2A$, $2B$ and $2A$ respectively. There is a doubly transitive action of M_{12} on 12 points with character $\mathbb{1}_K + \chi^K_{11a}$ where $\mathbb{1}_K$ is the trivial character of K and χ^K_{11a} is the first irreducible character of degree 11 (as in the Atlas). This character takes the value 0 for the elements in the class $2A_K$, and the value 4 for the elements in the class $2B_K$, hence $2A_K \subset 2A$ and $2B_K \subset 2B$.

The structure class constants for any pair of $2A$ involutions in $\mathbb{M}$ give the number of elements in each conjugacy class of $\mathbb{M}$ expressible as a product of two $2A$ involutions. For $\mathbb{M}$ the product of two $2A$ involutions lies in either of the $\mathbb{M}$ classes : $1A$, $2A$, $2B$, $3A$, $3C$, $4A$, $4B$, $5A$ or $6A$ (see 2.1). Similarly for $K \cong M_{12}$ we obtain that the product of two $2A_K$ involutions lies in either of the K classes $1A_K$, $2A_K$, $2B_K$, $3B_K$, $4A_K$, $4B_K$, $5A_K$ or $6A_K$. To avoid a contradiction on the monomorphism ι we have $5A_K \subset 5A$, and $6A_K \subset 6A$ and $3A_K$ is a subset of either $3A$ or $3C$. The class $6A_K$ has p-powers $3B_K$, $2A_K$ in K which must be subsets of the p-powers $3A$, $2A$ of $6A$ in $\mathbb{M}$. Hence $3B_K \subset 3A$. From lemma 6 of [Nor85] no elements of order 3 in A belongs to class $3C$ of $\mathbb{M}$. Hence $3A_K$ belongs to either $3A$ or $3B$. If $3A_K \subset 3A$ then $6B_K \subset 6C$ and if $3B_K \subset 3B$ then $6B_K$ is in either $6B$ or $6E$ according to the relevant p-powers in K and $\mathbb{M}$. We determine the fusion in $\mathbb{M}$ of $3A_K$ and $6B_K$ later in the proof. The classes $4A_K$, $4B_K$ contain products of $2A$ involutions and their squares lie in class $2B_K \subset 2B$ hence $4A_K$, $4B_K \subset 4A$ as $4A$ is the unique class in $\mathbb{M}$ squaring to $2B$. The classes $8A_K$, $8B_K$ square to $4A$ in $\mathbb{M}$ hence $8A_K$, $8B_K \subset 8B$, the unique class in $\mathbb{M}$ squaring to $4A$. Similarly $10A_K \subset 10A$ as $10A_K$ has p-powers $5A$, $2A$ in $\mathbb{M}$ and $10A$ is the unique class in $\mathbb{M}$ with such p-powers. There is a unique class of elements of order 11 in $\mathbb{M}$ so $11A_K$, $11B_K \subset 11A$. If $3A_K \subset 3A$ then $6B_K \subset 6C$ and the completed fusion of conjugacy classes of K in those of $\mathbb{M}$ gives a value of $\langle \chi_{V_{\mathbb{M}}} \downarrow_K, \mathbb{1}_K \rangle_{\mathbb{R}K}$ which is not integral, a contradiction. Hence $3A_K \subset 3B$ and $6B_K$ is in $6B$ or $6E$. To determine which, we look at the fusion of the conjugacy classes of $A = C_{\mathbb{M}}(H) \cong A_{12}$ in $\mathbb{M}$.

From lemma 6 of [Nor85] $2A_A$, $2B_A \subset 2A$ and $2C_A \subset 2B$. Also the elements of order 3 are in either $3A$ or $3B$ but not $3C$. From the structure constants, the product of any two involutions in the union $2A_A \cup 2B_A$ is in either of the A classes:

$$1A_A,\ 2A_A,\ 2B_A,\ 2C_A,\ 3A_A,\ 3B_A,\ 3C_A,\ 4A_A,\ 4B_A,\ 4C_A,\ 4D_A,\ 5A_A,\ 5B_A,\ 6A_A,$$
$$6C_A,\ 6E_A \text{ and } 6F_A.$$

Comparing with the constants for two $2A$ involutions in $\mathbb{M}$ we have

$$5A_A,\ 5B_A \subset 5A,$$
$$6A_A,\ 6C_A,\ 6E_A,\ 6F_A \subset 6A,$$
$$\text{and } 4A_A,\ 4B_A,\ 4C_A,\ 4D_A \text{ are in either } 4A \text{ or } 4B.$$

The class $6A$ of $\mathbb{M}$ has p-powers $3A$ and $2A$ so that the p-powers in A of $6A_A,\ 6C_A,\ 6E_A,\ 6F_A$ must be subsets of $3A$ and $2A$. Hence $3A_A,\ 3B_A,\ 3C_A \subset 3A$ and we cannot yet determine if $3D_A$ lies in $3A$ or $3B$. Comparing the value of the characters $\mathbb{1}_A + \chi_{11}^A$ of A and $\mathbb{1}_K + \chi_{11a}^K$ of K for the permutation actions of A and K on 12 points, we get that $3A_K \subset 3D_A$, $6B_K \subset 6G_A$ and $3B_K \subset 3A$. Since $3A_K \subset 3B$ then $3D_A \subset 3B$, and since $6B_K$ lies in either $6B$ or $6E$ then so does $6G_A$. The classes $8A_A,\ 8B_A$ square to $4B_A,\ 4D_A$ respectively where both are subsets of $4A$ in $\mathbb{M}$. Hence $8A_A,\ 8B_A \subset 8B$, the unique class in $\mathbb{M}$ squaring to $4A$. The classes $10A_A,\ 10B_A$ have p-powers in classes $5A,\ 2A$ of $\mathbb{M}$ so they are subsets of $10A$ the unique class in $\mathbb{M}$ with these p-powers. We have $11A_A,\ 11B_A \subset 11A$ the unique class of elements of order 11 in $\mathbb{M}$. Using p-powers we find $12A_A,\ 12B_A,\ 12D_A \subset 12C$ the unique class in $\mathbb{M}$ with p-powers $6A,\ 4B$, and $12C_A \subset 12C$ the unique class of $\mathbb{M}$ with p-powers $6C,\ 4A$. The class $14A_A$ is in $14A$, the unique class of elements of order 14 with 7^{th}-powers in $2A$. This implies $7A_A \subset 7A$. Using p-powers similarly as above we find

$$15A_A,\ 15B_A \subset 15A, \text{ the unique class in } \mathbb{M} \text{ with } p\text{-powers } 5A,\ 3A,$$
$$20A_A \subset 20B, \text{ the unique class in } \mathbb{M} \text{ with } p\text{-powers } 10A,\ 4B$$
$$21A_A \subset 21A, \text{ the unique class in } \mathbb{M} \text{ with } p\text{-powers } 7A,\ 3A$$
$$30A_A \subset 30B, \text{ the unique class in } \mathbb{M} \text{ with } p\text{-powers } 15A,\ 10A,\ 6A$$
$$\text{and } 35A_A,\ 35B_A \subset 35A, \text{ the unique class in } \mathbb{M} \text{ with } p\text{-powers } 7A,\ 5A.$$

The only classes in A left to fuse in those of $\mathbb{M}$ are $6G_A$ which is in either of $6B$ or $6E$, and the classes $9A_A,\ 9B_A,\ 9C_A$ of elements of order 9 which are in either $9A$ or $9B$ of $\mathbb{M}$. From a calculation of S. Shpectorov in [IS12a] we know the value $\langle \chi_{V_{\mathbb{M}}} \downarrow_A, \mathbb{1}_A \rangle_{\mathbb{R}A} = 26$. This can only happen if $6G_A \subset 6B$ and $9A_A,\ 9B_A,\ 9C_A \subset 9A$. In particular $6B_K \subset 6B$ since $6B_K \subset 6G_A$. □

The following useful observation was made by S. P. Norton (in a more general context).

Lemma 4.6. *The identity $\iota_{\mathbb{M}}$ of $V_{\mathbb{M}}$ cannot be contained in V.*

Proof. The groups G and K centralise each other in $\mathbb{M}$ and $G \times K$ is a subgroup of $\mathbb{M}$. The unique conjugacy class of involutions T of G is in class $2A$ of $\mathbb{M}$, and we have proved that the classes $2A_K$ and $2B_K$ are in $2A$ and $2B$ respectively.

Claim : there exist elements $s \in T$ and $t \in 2A_K$ such that the element ts of $G \times K$ is in class $2B$ of $\mathbb{M}$.

From Proposition 4.4, part (iii), the element s can be taken from a A_5-subgroup X of G of type $(2A, 3A, 5A)$. From the proof of Proposition 4.5, the elements of $2A_K$ act fixed-point freely on 12 points, and the centraliser in $\mathbb{M}$ of an A_5-subgroup of type $(2A, 3A, 5A)$ is isomorphic to A_{12}. From line 7 in Table 4 of [Nor98], there exists a subgroup $Y \subseteq A_{12}$, $Y \cong A_5$, that acts transitively on 12 points. Let $t \in Y$. Then, by line 8 in Table 3 of [Nor98], the involutions in the diagonal subgroups of $X \times Y$ are in $2B$. In particular $ts \in 2B$ and the claim is proved.
Since $ts \in 2B$, the axes a_t and a_s generate a dihedral algebra of type $2B$ and $a_t \cdot a_s = 0$ (see Table 2.1). For all $z \in T$ there is an element $g \in G$ such that $z = s^g$, so by invariance of the algebra product $(a_t \cdot a_s)^g = 0 = a_t \cdot a_z$ since G normalises K. Now, V is generated by the 55 $2A$-axes a_z for $z \in T$ and the 0-eigenspace of a_t is closed under the algebra product, so if the identity $\iota_{\mathbb{M}}$ were in V we would get the contradiction $a_t \cdot \iota_{\mathbb{M}} = 0$. □

The identity of a commutative algebra being unique and therefore stable under the automorphism group we have $\iota_{\mathbb{M}} \in C_{V_{\mathbb{M}}}(K)$. And since $\iota_{\mathbb{M}}$ is not in V we obtain the main result of this subsection.

Proposition 4.7. *For the algebra V we have $dim(V) \leq 101$.* □

4.4 Inner products

In the following two subsections we calculate all inner products on a well-chosen subset of V and compute the rank of the corresponding Gram matrix to bound below the dimension of V. We do so using the information on some subalgebras of V which have already been classified, whilst inner product values which are not inherited from subalgebras of V are obtained by describing intersections of subgroups of G.

4.4.1 Dihedral subalgebras of V and spanning set

We will use the information on dihedral subalgebras of V to choose a spanning set for V. The algebra V contains the dihedral subalgebras of type $2A$, $3A$, $5A$, and $6A$ which are equal to the Majorana representations of D_4 of type $2A$, D_6 of type $3A$, D_{10} and D_{12} respectively.

Dihedral subalgebras

We recall that each dihedral subalgebra corresponds to a dihedral subgroup D of $\mathbb{M}$ generated by two $2A$ involutions t and s, whose product we denote by $\rho := ts$. We denote by a_0, a_1 and a_i the $2A$-axes a_t, a_s and $a_{t\rho^i}$ as in Chapter 2. Lastly we recall that $\mathcal{C}$ denotes Conway's bijection 2.1, which is a map sending each $2A$ involution to a unique $2A$-axis.
In the subalgebra of type $2A$, we have $a_\rho = \mathcal{C}(\rho)$ which is also a $2A$-axis, and in the types $3A$ and $5A$ the vectors u_ρ and w_ρ are introduced to close the algebra product. They correspond to cyclic subgroups of order 3 or 5 in D respectively. We also recall that the 1-dimensional subspace linearly spanned by the vector u_ρ or w_ρ is invariant under the normaliser $N_{\mathbb{M}}(\langle\rho\rangle)$ which is isomorphic to $3.Fi_{24}$ or $(D_{10} \times HN).2$ respectively. Also, in the type $3A$ the vector itself is stable under $N_{\mathbb{M}}(\langle\rho\rangle)$, so that $u_\rho = u_{\rho^{-1}}$, and in the type $5A$ the vector is stabilised up to negation $w_\rho = -w_{\rho^2} = -w_{\rho^3} = w_{\rho^4}$.

Spanning set

Any element of order 3 or 5 in G can be expressed as a product of two involutions, and any two involutions correspond to a dihedral subalgebra of V. Hence to study the algebra V we can consider the span of the vectors contained in the dihedral subalgebras of types $2A$, $3A$ and $5A$.

Throughout this chapter we let $G^{(i)}$ be a set of non-trivial representatives of each cyclic subgroup of order i for $i = 2, 3, 5$, of size 55, 55 and 66 respectively, where for $i = 5$ the representatives are taken from the same conjugacy class of G.

We also use the notations:

$$A := \{a_t \mid t \in G^{(2)}\},$$
$$U := \{u_h \mid h \in G^{(3)}\},$$
$$W := \{w_f \mid f \in G^{(5)}\},$$

and we define $S := A \cup U \cup W$, which we will take as a spanning set for V as an $\mathbb{R}$-vector space.

4.4.2 A_5 subalgebras of V

For H an A_5-subgroup of $\mathbb{M}$ of type $(2A, 3A, 5A)$, the structure of a subalgebra $V_H \subseteq V_{\mathbb{M}}$ generated by the $2A$-axes indexed by the involutions of H follows from a result in [IS12a]; there exists a unique Majorana representation of shape $(2A, 3A, 5A)$ for the group A_5 which is based on an embedding into $\mathbb{M}$, hence the corresponding Majorana algebra is equal to a subalgebra of $V_{\mathbb{M}}$.
Since G contains two conjugacy classes of A_5-subgroups of type $(2A, 3A, 5A)$, of size 11 each, then the algebra V contains 22 A_5-subalgebras of type $(2A, 3A, 5A)$. We reformulate the result from [IS12a] so as to present V_H as a subalgebra of $V_{\mathbb{M}}$ generated by a triple of $2A$-axes.

Proposition 4.8. *Let $V_H = \langle\langle a_x, a_y, a_z\rangle\rangle$ be a subalgebra of $V_{\mathbb{M}}$ where the dihedral subalgebra $\langle\langle a_x, a_y\rangle\rangle$ has type $2A$ and where the dihedral subalgebras $\langle\langle a_x, a_z\rangle\rangle$, $\langle\langle a_y, a_z\rangle\rangle$, and $\langle\langle a_{xy}, a_z\rangle\rangle$ have types $5A$, $5A$ and $3A$ respectively. Then V_H has dimension 26 and it is linearly spanned by the products of all pairs of $2A$-axes indexed by the involutions of an A_5 group H of type $(2A, 3A, 5A)$.* □

For explicit formulas for the algebra product in V_H or a list of all inner product values, we refer the reader to [IS12a]. In the rest of the chapter we will simply refer to an A_5-subgroup H to mean an A_5-subgroup of type $(2A, 3A, 5A)$.

For an A_5-subgroup H, we denote by $H^{(2)}$, $H^{(3)}$ and $H^{(5)}$ the sets of non-trivial conjugate representatives of cyclic subgroups of order 2, 3 and 5 and in the corresponding algebra V_H we denote by A_H, U_H and W_H the sets of vectors $\{a_t \mid t \in H^{(2)}\}$, $\{u_h \mid h \in H^{(3)}\}$, and $\{w_f \mid f \in H^{(5)}\}$.
We also let w_H be the sum of all vectors in W_H. By [IS12a], the set $S_H := A_H \cup U_H \cup W_H$ is a spanning set of size 31 for V_H, and V_H is 26-dimensional with a basis $A_H \cup U_H \cup \{w_H\}$. The

five independent linear relations on S_H, which can be found in [IS12a] or [Nor96], are called the Norton Relations.

Proposition 4.9. ***The Norton Relations***

In the algebra V_H corresponding to an A_5-subgroup H of type $(2A, 3A, 5A)$, all vectors $w_f \in W_H$ satisfy:

$$w_f = \frac{1}{6}w_H + \frac{1}{2^7}\left(\sum_{t\in H_5^{(2)}(f)} a_t - \sum_{t\in H_3^{(2)}(f)} a_t\right) + \frac{3^2.5}{2^{12}}\left(\sum_{\substack{h\in H^{(3)},\\ o([h,f])=3}} u_h - \sum_{\substack{h\in H^{(3)},\\ o([h,f])=5}} u_h\right)$$

where

$$H_5^{(2)}(f) := \{t \in H^{(2)} \mid o(tf) = 5\},$$
$$H_3^{(2)}(f) := \{t \in H^{(2)} \mid o(tf) = 3\}.$$ □

We denote by $\mathcal{H}_1 = \{H_1, \ldots, H_{11}\}$ and $\mathcal{H}_2 = \{H'_1, \ldots, H'_{11}\}$ the two classes of A_5-subgroups in G. One class corresponds to the rows of the incidence matrix $\mathcal{N}$ (see subsection 4.2), and the other class corresponds to the columns, so the intersection between A_5's taken from different classes can be read directly from the entries of $\mathcal{N}$.

For a given A_5-subgroup H_i in G let W^i be the sum of all vectors in W_{H_i}. For a vector $w_f \in W_{H_i}$ we rewrite a **simplified Norton relation for** w_f as

$$w_f = \frac{1}{6}W^i + \lambda\ A_i(f) + \mu\ U_i(f) \tag{4.2}$$

where the meaning of $\lambda,\ \mu,\ A_i(f)$ and $U_i(f)$ is clear from Proposition 4.9:

$$\lambda := \frac{1}{2^7}, \quad \mu := \frac{3^2.5}{2^{12}}, \quad A_i(f) := \sum_{t\in H_i^{(2)}{}_5(f)} a_t - \sum_{t\in H_i^{(2)}{}_3(f)} a_t, \quad U_i(f) := \sum_{\substack{h\in H_i^{(3)},\\ o([h,f])=3}} u_h - \sum_{\substack{h\in H_i^{(3)},\\ o([h,f])=5}} u_h.$$

Corollary 4.10. *Let w be the sum of all vectors w_f in $W \subseteq V$. Then $S' := A \cup U \cup \{w\}$ is a spanning set of size 111 for V.*

Proof. Consider an A_5-subgroup $H_1 \in \mathcal{H}_1$. From $\mathcal{N}$, any subgroup $H_{i'} \in \mathcal{H}_2$ intersect H_1 in a D_{10} or an A_4. If $H_1 \cap H_{i'} \cong D_{10}$ there exists a representative f of $H_1^{(5)}$ in $H_1 \cap H_{i'}$ for which the simplified Norton relations 4.2 give

$$w_f = \begin{cases} \frac{1}{6}W^1 + \lambda\ A_1(f) + \mu\ U_1(f) \\ \\ \frac{1}{6}W^{i'} + \lambda\ A_{i'}(f) + \mu\ U_{i'}(f) \end{cases}$$

and so $W^{i'}$ is in $Sp(A \cup U \cup \{W^1\})$, the $\mathbb{R}$-linear span of $A \cup U \cup \{W^1\}$.

If $H_1 \cap H_{i'} \cong A_4$ then the situation can be visualized as the following submatrix of $\mathcal{N}$, where each anti-flag has been replaced by the unique element of $G^{(5)}$ stabilising it, and the rows and columns are indexed with the copy of A_5 stabilising the corresponding line or point of $\mathcal{B}$.

$$\begin{array}{c} \\ H_i' \\ H_j' \end{array} \begin{array}{c} \begin{array}{cc} H_1 & H_i \end{array} \\ \begin{pmatrix} 1 & w_g \\ w_f & w_k \end{pmatrix} \end{array}$$

From the Norton relations of the elements $g \in H_i \cap H_{i'}$, $k \in H_i \cap H_{j'}$ and $f \in H_1 \cap H_{j'}$, we find $W^{i'} \in Sp\big(A \cup U \cup \{W^1\}\big)$. From $\mathcal{N}$, for any subgroup $H_i \in \mathcal{H}_1$ there are 3 elements of $\mathcal{H}_2$ intersecting both H_1 and H_i in a D_{10}, with say $H_{l'}$ being one of them:

$$\begin{array}{c} \\ H_{l'} \end{array} \begin{array}{c} \begin{array}{cc} H_1 & H_i \end{array} \\ \begin{pmatrix} w_f & w_l \end{pmatrix} \end{array}$$

so the Norton relations for f and l give $W^i \in Sp\big(A \cup U \cup \{W^1\}\big)$. Hence there exists $v \in Sp(A \cup U)$ such that

$$22\ W^1 = \textstyle\sum_{H_i \in \mathcal{H}_1} W^i + \sum_{H_{i'} \in \mathcal{H}_2} W^{i'} + v,$$

and from $\mathcal{N}$ every element of $G^{(5)}$ is contained in exactly one element of $\mathcal{H}_1$ and one of $\mathcal{H}_2$ so that

$$\textstyle\sum_{H_i \in \mathcal{H}_1} W^i + \sum_{H_{i'} \in \mathcal{H}_2} W^{i'} = 2\ w,$$

where w is the sum of all vectors w_f in W, and hence

$$W^1 = \tfrac{1}{11}w + v' \quad \text{for some } v' \in Sp(A \cup U).$$

□

4.4.3 Inner product values

Definition 4.11. For each pair $(G^{(i)}, G^{(j)})$ with $i,\ j \in \{2,3,5\}$ we call the inner product values on $G^{(i)} \times G^{(j)}$ inner products of **type (i, j)**.

If we let $E^{(i)}$ be the equivalence class of elements of order i in G belonging to the same cyclic subgroup, then the orbits of G acting by conjugation on $E^{(i)} \times E^{(j)}$ form a subpartition of the distinct inner products values of type (i, j) (these orbits were calculated using Magma).

We will only explain the inner products values (u_k, v_l) for which the subgroup $\langle k, l\rangle$ is isomorphic to F_{55} or to the whole of G (in other cases the inner products have already been found). They arise as the solutions of equations of intersecting subalgebras inside V, or equivalently as particular configurations of subgroups inside G. These intersections of subgroups can be read from the incidence matrix $\mathcal{N}$ or found using code written in Magma.

4.4.3.1 Inner products of type $(2,2)$

From the dihedral subalgebras of V we know all possible inner product values of any two Majorana axes in V from Table 2.1.

Case	$o(ts)$	$\langle\langle a_t, a_s\rangle\rangle$	$\langle t, s\rangle$	(a_t, a_s)
1	1	$1A$	1	1
2	2	$2A$	D_4	$\frac{1}{2^3}$
3	3	$3A$	D_6	$\frac{13}{2^8}$
4	5	$5A$	D_{10}	$\frac{3}{2^7}$
5	6	$6A$	D_{12}	$\frac{5}{2^8}$

TABLE 4.3: Inner Products of type $(2,2)$, with $t, s \in G^{(2)}$

4.4.3.2 Inner products of type $(2,3)$

Case	$o(ht)$	$\langle t,h\rangle$	(a_t,u_h)
1	2	D_6	$\frac{1}{2^2}$
2	3	A_4	$\frac{1}{3^2}$
3	5	A_5	$\frac{1}{2.3^2}$
4	6	C_6	0
5	11	$L_2(11)$	$\frac{1}{2.3.5}$

TABLE 4.4: Inner Products of type $(2,3)$, with $t \in G^{(2)}$ and $h \in G^{(3)}$

The value for case 5) of the inner product of type $(2,3)$ was computed using the following lemma.

Lemma 4.12. *For $t \in G^{(2)}$ and $h \in G^{(3)}$ such that $\langle t,h\rangle \cong L_2(11)$ we have*

$$(a_t,u_h) = \tfrac{1}{2.3.5}.$$

Proof. We fix an element $h \in G^{(3)}$ and we let $t \in G^{(2)}$ such that $\langle t,h\rangle = G$. Since $N_G\big(\langle h\rangle\big) \cong D_{12}$ then $\langle h\rangle$ is contained in exactly two distinct dihedral groups of order 6. Let S_h be one of the two sets of 3 involutions, $S_h := \{s, sh, sh^2\}$, such that $\langle S_h, h\rangle \cong D_6$, and up to permutation of the set S_h we have

$$\begin{aligned}\langle t,\ s\rangle &\cong D_6,\\ \langle t,\ sh\rangle &\cong D_{12},\\ \langle t,\ sh^2\rangle &\cong D_{10}.\end{aligned}$$

In the $3A$-dihedral subalgebra $\langle\langle a_s, u_h\rangle\rangle$ we have the equality

$$u_h = -\tfrac{2^{11}}{3^3.5}\Big[a_s \cdot a_{sh} - \tfrac{1}{2^5}(2a_s + 2a_{sh} - a_{sh^2})\Big],$$

so taking the inner product with a_t gives

$$(a_t, u_h) = -\frac{2^{11}}{3^3.5}\Big[(a_t\ ,\ a_s \cdot a_{sh}) - \frac{1}{2^5}(a_t\ ,\ 2a_s + 2a_{sh} - a_{sh^2})\Big],$$

and by associativity of the algebra product with the inner product

$$(a_t,\ a_s \cdot a_{sh}) = (a_s,\ a_t \cdot a_{sh}).$$

Since $\langle t, sh\rangle \cong D_{12}$, the element $\rho = tsh$ has order 6 so the algebra product $a_t \cdot a_{sh}$ is contained in the dihedral algebra $\langle\langle a_t, a_{sh}\rangle\rangle$ of type $6A$, and so

$$(a_s,\ a_t \cdot a_{sh}) = \frac{1}{2^6}(a_s,\ a_t + a_{sh} - a_{t\rho^2} - a_{t\rho^3} - a_{t\rho^4} - a_{t\rho^5} + a_{\rho^3}) + \frac{3^2.5}{2^{11}}(a_s, u_{\rho^2}),$$

where $\langle s, \rho^2\rangle \cong A_4$, so the value of (a_s, u_{ρ^3}) is known to be $\frac{1}{9}$ from [IPSS10]. Since all the required inner products are now known, one can compute $(a_t, u_h) = \frac{1}{2.3.5}$. □

4.4.3.3 Inner products of type $(2, 5)$

Case	$o(tf) = o(tf^{-1})$	$o([t, f])$	$\langle t, f\rangle$	(a_t, w_f)
1	2	5	D_{10}	0
2	3	5	A_5	$-\frac{7^2}{2^{14}}$
3	5	3	A_5	$\frac{7^2}{2^{14}}$
4	5	5	$L_2(11)$	$-\frac{1}{2^{14}}$
5	6	6	$L_2(11)$	$-\frac{3}{2^{12}}$
6	11	5	$L_2(11)$	$\frac{19}{2^{14}}$

TABLE 4.5: Inner Products of type $(2, 5)$, with $t \in G^{(2)}$ and $f \in G^{(5)}$

The next lemma justifies the values found in cases 4), 5) and 6). We omit its proof which is similar to the proof of Lemma 4.12.

Lemma 4.13. *Let $t \in G^{(2)}$ and $f \in G^{(5)}$ such that $\langle t,\ f\rangle \cong L_2(11)$. Then exactly one of the following holds.*

(i) *There exists $s \in G^{(2)}$ commuting with t and inverting f, and*

$$(a_t, w_f) = -\tfrac{1}{2^{11}} + \tfrac{1}{2^6}p - \tfrac{1}{2^3}q, \quad \textit{where}$$

$$p = 7(a_t, a_{sf}) + (a_t, a_{sf^2}) \quad \textit{and} \quad q = (a_{ts}, a_{sf}).$$

(ii) *There exists $s \in G^{(2)}$ inverting f and generating with t a dihedral group of order 6, and*

$$(a_t, w_f) = \tfrac{3^2}{2^{14}} + \tfrac{1}{2^7}p - \tfrac{3^3.5}{2^{11}}q, \quad \textit{where}$$

$$p = (a_t,\ 5a_{sf} + a_{sf^2} + a_{sf^3} + a_{sf^4}) \quad \textit{and} \quad q = (u_{st}, a_{sf}).$$

(iii) *There exists $s \in G^{(2)}$ inverting f and generating with t a dihedral group of order 12, and*

$$(a_t, w_f) = -\tfrac{3}{2^{15}} + \tfrac{1}{2^6}p + \tfrac{1}{2^7}q - \tfrac{3^2.5}{2^{11}}r, \quad \textit{where}$$

$$p = (a_{sf},\ a_{\rho^3} - 2a_t - a_{t\rho^2} - a_{t\rho^3} - a_{t\rho^4} - a_{t\rho^5}), \quad q = (a_t,\ a_{sf^2} + a_{sf^3} + a_{sf^4}) \quad \textit{and}$$
$$r = (u_{\rho^2}, a_{sf}),$$

for $\rho := ts$ of order 6 in $\langle t,\ s\rangle \cong D_{12}$.

□

4.4.3.4 Inner products of type $(3,3)$

Case	$\{o(hk), o(hk^{-1})\}$	$\langle h, k\rangle$	(u_h, u_k)
1	$\{1,3\}$	C_3	$\frac{2^3}{5}$
2	$\{2,3\}$	A_4	$\frac{2^3.17}{3^4.5}$
3	$\{5,5\}$	A_5	$\frac{2^4}{3^4.5}$
4	$\{5,6\}$	$L_2(11)$	$\frac{2^3}{3.5^2}$
5	$\{5,11\}$	$L_2(11)$	$\frac{2^3.7}{3^3.5^2}$
6	$\{6,6\}$	$L_2(11)$	$\frac{2^5}{3^4.5}$

TABLE 4.6: Inner Products of type $(3,3)$, with $h, k \in G^{(3)}$

In the next lemma part (i) addresses cases 4) and 6) and part (ii) addresses case 5). The lemma assumes all products of type $(2,3)$ are known.

Lemma 4.14. *Let $h,\ k \in G^{(3)}$ with $\langle h,k\rangle \cong L_2(11)$. Then exactly one of the following holds.*

(i) *There exists an involution t inverting both h and k, and*

$$(u_h,u_k) = \tfrac{2^4}{3^5.5}(5 - 2^3.3^2p + 2^6q), \quad \textit{where}$$

$$p = (u_h, a_{tk^2}) = (u_k, a_{th^2}) \quad \textit{and} \quad q = (a_{th}, a_{tk^2}) + (a_{th}, a_{tk}) + (a_{th^2}, a_{tk}) + (a_{th^2}, a_{tk^2}).$$

(ii) *There exists an involution t inverting h and generating with k an alternating group A_4, and*

$$(u_h,u_k) = \tfrac{2^5}{3^3.5}(\tfrac{1}{2^2.3} - p - 2q - r), \quad \textit{where}$$

$$p = (a_{th},\ 3u_{tk} - 4u_{tk} - 4u_{tk^2}), \quad q = (a_{th^2}, u_k) \quad \textit{and} \quad r = (a_{th}, u_k).$$

□

4.4.3.5 Inner products of type $(3,5)$

Case	$o(hf)$	$o(hf^{-1})$	$\langle h,f\rangle$	(u_h, w_f)
1	2	5	A_5	$\frac{-5.7}{2^9.3^2}$
2	3	5	A_5	$\frac{5.7}{2^9.3^2}$
3	3	6	$L_2(11)$	$\frac{-67}{2^9.3^2.5}$
4	5	5	$L_2(11)$	$\frac{-1}{2^8.3^2.5}$
5	6	11	$L_2(11)$	$\frac{7}{2^6.3^2.5}$
6	11	11	$L_2(11)$	$\frac{-7}{2^7.3^2.5}$

TABLE 4.7: Inner Products of type $(3,5)$, with $h \in G^{(3)}$ and $f \in G^{(5)}$

Part (i) of the next lemma addresses case 3), and part (ii) addresses cases 5) and 6).

Lemma 4.15. *Let $h \in G^{(3)}$ and $f \in G^{(5)}$ such that $\langle h,\ f\rangle \cong L_2(11)$. Then exactly one of the following holds.*

(i) *There exists an involution t inverting f and h, and*

$$(u_h, w_f) = -\tfrac{2^{11}}{3^3.5}(p - \tfrac{1}{2^5}q), \quad \textit{where}$$

$$p = \tfrac{7}{2^{12}}(a_{tf} + a_{tf^4} - a_{tf^2} - a_{tf^3},\ a_{th}) + \tfrac{7}{2^5}(w_f, a_{th}) \quad \textit{and} \quad q = (2a_t + 2a_{th} + a_{th^2},\ w_f).$$

(ii) *There exists an involution t inverting f and generating with h a subgroup isomorphic to A_5, and*

$$(u_h, w_f) = \tfrac{7}{2^7}p + \tfrac{1}{2^7}q - \tfrac{1}{2^4}r, \quad \textit{where}$$

$$p = (a_{sf} + a_{sf^4},\ u_h), \quad q = (a_{sf^2} + a_{sf^3},\ u_h) \quad \textit{and} \quad r = (a_{sf},\ u_{sh} + u_{sh^2}).$$

□

The inner product value for case 4) of the inner product of type $(3, 5)$ can be found using the Norton relations 4.9 inside some A_5-subalgebras of V. The proof of the following lemma uses similar arguments to the proof of Corollary 4.10. We use the notation of the simplified Norton relations (see equation 4.2).

Lemma 4.16. *Let $f \in G^{(5)}$ and $h \in G^{(3)}$. If there exists an element $g \in G^{(5)}$ such that $A_1 := \langle f, g\rangle$ and $A_2 := \langle h, g\rangle$ are two non-conjugate A_5-subgroups of G, then*

$$(u_h, w_f) = \tfrac{1}{6}\big(u_h\ , W^2\big) + \tfrac{1}{2^7}\big(u_h\ , l_a\big) + \tfrac{3^2.5}{2^{12}}\big(u_h, l_u\big), \quad \textit{where}$$

$$l_a = A_1(g) + A_1(f) - A_2(g) \quad \textit{and} \quad l_u = U_1(g) + U_1(f) - U_2(g).$$

□

4.4.3.6 Inner products of type $(5,5)$

Case	$\{o(fg), o(fg^{-1})\}$	$o([f,g])$	$\langle f,g\rangle$	(u_h, w_f)
1	$\{1,5\}$	1	C_5	$\frac{5^3.7}{2^{19}}$
2	$\{3,5\}$	5	A_5	$\frac{7.29}{2^{19}}$
3	$\{5,11\}$	11	F_{55}	$\frac{-11}{2^{19}}$
4	$\{3,6\}$	5	$L_2(11)$	$\frac{3.151}{2^{21}}$
5	$\{2,6\}$	5	$L_2(11)$	$\frac{157}{2^{20}}$
6	$\{5,11\}$	2	$L_2(11)$	$\frac{59}{2^{20}}$
7	$\{5,5\}$	3	$L_2(11)$	$\frac{-3.41}{2^{20}}$

TABLE 4.8: Inner Products of type $(5,5)$, with $f, g \in G^{(5)}$

In the next lemma, part (i) justifies the values of the inner product of type $(5,5)$ for the cases 2), 3) and 4), and part (ii) justifies case 6). The proof is similar to that of Corollary 4.10 and again we use the notation of the simplified Norton relations 4.2.

Lemma 4.17. *Let $f,\ g \in G^{(5)}$ not contained in a common A_5-subgroup, with f and g belonging to the pairs $\{H_i,\ H_{i'}\}$ and $\{H_j,\ H_{j'}\}$ respectively, of distinct non-conjugate A_5-subgroups of G. Then exactly one of the following holds.*

(i) *$H_i \cap H_{j'} \cong D_{10}$, or $H_j \cap H_{i'} \cong D_{10}$, with k an element of order 5 in $H_i \cap H_{j'}$, say, then*

$$(w_f, w_g) = \frac{1}{6^2}(W^j, W^j) + \frac{1}{2^8.3}(l_a\ , W^j) + \frac{3.5}{2^{13}}(l_u,\ W^j) + \frac{1}{2^{14}}(l_a\ , A_j(g)) + \frac{3^2.5}{2^{19}}(l_a\ ,\ U_j(g)) + \frac{3^2.5}{2^{19}}(l_u\ , A_j(g)) + \frac{3^4.5^2}{2^{24}}(l_u\ , U_j(g)),$$

where $l_a = A_j(k) - A_{i'}(k) + A_{i'}(f)$ and $l_u = U_j(k) - U_{i'}(k) + U_{i'}(f)$.

(ii) *$H_i \cap H_{j'} \cong H_j \cap H_{i'} \cong A_4$, and there exist two elements $k \neq l \in G^{(5)}$ such that k belongs to H_i and $H_{m'}$ and l belongs to H_j and $H_{m'}$, so that*

$$(w_f, w_g) = \frac{1}{6^2}(W^j, W^j) + \frac{1}{2^8.3}(l_a\ , W^j) + \frac{3.5}{2^{13}}(l_u\ , W^j) + \frac{1}{2^{14}}(l_a\ , A_j(g)) + \frac{3^2.5}{2^{19}}(l_a\ , U_j(g)) + \frac{3^2.5}{2^{19}}(l_u\ , A_j(g)) + \frac{3^4.5^2}{2^{24}}(l_u\ , U_j(g)),$$

$$\text{where}\quad l_a = A_j(l) - A_{m'}(l) - A_i(k) + A_{m'}(k) + A_i(f),$$
$$\text{and}\quad l_u = U_j(l) - U_{m'}(l) - U_i(k) + U_{m'}(k) + U_i(f).$$

□

Corollary 4.18. *The inner product values between the vector w, and the vectors $a_t \in A$, $u_h \in U$, $w_f \in W$ and w itself are as follows:*

1) $(a_t, w) = \frac{3^2}{2^{11}}$;

2) $(u_h, w) = -\frac{3^2}{2^7.5}$;

3) $(w_f, w) = \frac{3^3.5.17}{2^{18}}$;

4) $(w, w) = \frac{3^4.5.11.17}{2^{17}}$. □

4.4.4 Dependence relations in the algebra

We let $V_{S'}$ be the $\mathbb{R}$-vector space with basis $\{v_s :\ s \in S'\}$ where $S' = A \cup U \cup \{w\}$ is a subset of V. We turn $V_{S'}$ into a G-module by the natural action of G on S', and we let π be the natural projection

$$\pi : V_{S'} \to V$$
$$\sum \lambda_s v_s \to \sum \lambda_s s$$

where $\lambda_s \in \mathbb{R}$ for all $s \in S'$. We let $\mathcal{G} := \big((v_{s_1}, v_{s_2})\big)_{s_1,s_2 \in V_{S'}} = \big((s_1, s_2)\big)_{s_1,s_2 \in V_{S'}}$ be the Gram matrix of $V_{S'}$ where the inner product values are those calculated in the previous subsection. The inner product is real and symmetric hence the Gram matrix $\mathcal{G}$ can be used to determine the linear independence over $\mathbb{R}$ of the vectors in $\{v_s :\ s \in S'\}$. Using Magma we find the rank of the matrix $\mathcal{G}$ and give a description of the kernel of π in Proposition 4.19. Before we state Proposition 4.19 we explain some of the notations used in the proposition.

For a fixed involution $t \in G^{(2)}$ its normaliser $N_G(t) \cong D_{12}$ has the following orbits on $G^{(2)}$ (the action is conjugation):

$$O_1,\ O_3^1,\ O_3^2,\ O_6^1,\ O_6^2,\ O_6^3,\ O_6^4,\ O_{12}^1 \text{ and } O_{12}^2,$$

where the subscript indicates the size of the orbit. If we write $N_G(t) = \langle \rho \rangle \rtimes \langle s \rangle$ then $\rho^3 = t$, so $O_1 = \{\rho^3\}$, $O_3^1 = \{s,\ s\rho^2,\ s\rho^4\}$ and $O_3^2 = \{s\rho,\ s\rho^3,\ s\rho^5\}$ without loss of generality. Further we can describe the orbits as follows:

$$\begin{aligned} O_3^1 \cup O_3^2 &= \{s \in G^{(2)} \mid \langle s,\ t \rangle \cong 2^2\} \\ O_6^1 \cup O_6^2 &= \{s \in G^{(2)} \mid \langle s,\ t \rangle \cong D_{12}\} \\ O_6^3 \cup O_6^4 &= \{s \in G^{(2)} \mid \langle s,\ t \rangle \cong D_6\} \\ O_{12}^1 \cup O_{12}^2 &= \{s \in G^{(2)} \mid \langle s,\ t \rangle \cong D_{10}\}. \end{aligned}$$

For $(t_1,\ t_2)$ in $O_3^1 \times O_6^2$ or $O_3^2 \times O_6^1$ the subgroup $\langle t_1,\ t_2 \rangle$ in G is isomorphic to either 2^2 or D_{10}. For $(t_1,\ t_2)$ in $O_3^1 \times O_6^1$ or $O_3^2 \times O_6^2$ the subgroup $\langle t_1,\ t_2 \rangle$ is isomorphic to either D_6 or D_{12}.

Lastly we recall that d is the bijection 4.1 introduced in section 4.2, between subgroups of order 2 and 3 in G : for each involution $t \in G^{(2)}$ there is a unique subgroup $\langle h \rangle$ of order 3, $h \in G^{(3)}$, whose elements commute with t.

Proposition 4.19. (i) *The rank of the Gram matrix $\mathcal{G}$ is* 101.

(ii) *The kernel of π is* 10*-dimensional and consists of* 10 *linearly independent relations, between the vectors of $A \cup U$, taken from a set of* 55 *G-invariant relations $R(t)$ indexed by the involutions of G.*

For a fixed involution t in $G^{(2)}$, $R(t)$ defines the following $N_G(t)$-invariant relation:

$$R(t) := \sum_{r \in T_1} a_r - \sum_{s \in T_2} a_s + \frac{3^2.5}{2^5}\Big(\sum_{h \in d(T_1)} u_h - \sum_{k \in d(T_2)} u_k \Big) = 0,$$

where T_1 and T_2 can taken to be $O_3^1 \cup O_6^1$ and $O_3^2 \cup O_6^2$ respectively (or vice versa).

□

By the rank-nullity Theorem we have that $Im(\pi) \subseteq V$ has dimension 101 , proving the following proposition.

Proposition 4.20. *For the algebra V we have $dim(V) \geq 101$.* □

The above, together with Proposition 4.7, proves that $dim(V) = 101$. Hence the set S' spans V, so that $\{a_t \cdot a_s \mid t,\ s \in T\}$ also spans V. From Lemma 4.6, the identity $\iota_{\mathbb{M}}$ of $V_{\mathbb{M}}$ is not in V. The space $C_{V_{\mathbb{M}}}(K)$ is 102-dimensional, containing $\iota_{\mathbb{M}}$ and having V as a subspace. Hence $C_{V_{\mathbb{M}}}(K)$ decomposes as $V \oplus \iota_{\mathbb{M}}$, and we have proved Theorem 4.2.

4.5 The Majorana representation of $L_2(11)$

We let L be a group isomorphic to $L_2(11)$ with conjugacy classes denoted $1a,\ 2a,\ 3a,\ 5a,\ 5b,\ 11a$ and $11b$ and we let $\mathcal{R} = (L, 2a, X)$ be a Majorana representation of L with Majorana algebra X.

Proposition 4.21. *A Majorana representation $\mathcal{R} = (L, 2a, X)$ of L must have shape $(2A, 3A, 5A, 6A)$.*

Proof. The group $L_2(11)$ has a single conjugacy class of involutions, $2a$, and a single class $3a$ of elements of order 3. From the structure class constants the product of any two $2a$ involutions is in either of the $L_2(11)$ classes $1a,\ 2a,\ 3a,\ 5a,\ 5b$ or $6a$. Hence X contains dihedral subalgebras of type $5A$ and $6A$ since they are the only dihedral subalgebras associated with dihedral groups of order 10 and 12. By the inclusion of the dihedral subalgebras $3A \hookrightarrow 6A$ and $2A \hookrightarrow 6A$ the classes $3a$ and $2a$ are mapped to $3A$ and $2A$ under ψ. Hence X also contains dihedral subalgebras of type $3A$ and $2A$ and we have accounted for all possible dihedral subalgebras in X. □

We remark that since $\mathcal{R}$ has shape $(2A, 3A, 5A, 6A)$, the algebra X contains the set of Majorana axes $A' := \{\psi(t) \mid t \in 2a\}$, the set of $3A$-vectors $U' := \{u'_h \mid h \in 3a\}$, and the set of $5A$-vectors $W' := \{w'_f \mid f \in 5a\}$ which are in bijection with the subsets A, U and W respectively of the algebra V. Next we remark that the descriptions of the inner product values and the algebra products in V given in the previous section were achieved using only properties of $V_{\mathbb{M}}$ that are included in the Majorana axioms; for example Proposition 4.19 can also be applied to X so $dim(X) \geq 101$.
In [Ser12] Àkos Seress describes an algorithm with which he closed the algebra product on the set $A' \cup U' \cup W'$ of X and proves the following:

Proposition 4.22. *Let $\mathcal{R} = (L, 2a, X)$ be a Majorana representation of L of shape $(2A, 3A, 5A, 6A)$. Then $dim(X) = 101$.*

The above proposition shows that the Majorana axioms define X uniquely. We recall that from Proposition 4.1 there exists a monomorphism $\iota : L_2(11) \hookrightarrow \mathbb{M}$ such that $\iota(T) \subseteq 2A$. Hence from Àkos Seress's result we can conclude the following.

Theorem 4.23. *There is a unique Majorana representation $\mathcal{R} = (L, 2a, X)$ of $L_2(11)$. This representation is based on an embedding in $\mathbb{M}$ so that X is isomorphic to V the $L_2(11)$-subalgebra of $V_{\mathbb{M}}$.* □

Bibliography

[ABL+99] Rachel Abbott, John Bray, Steve Linton, Simon Nickerson, Simon Norton, Richard Parker, Stephen Rogers, Ibrahim Suleiman, Jonathan Tripp, Peter Walsh, and Robert Wilson, *Online atlas of finite group representations*, May 1999, http://web.mat.bham.ac.uk/atlas/v2.0/.

[Asc00] M. Aschbacher, *Finite group theory*, CUP, Cambridge, 2000.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The magma algebra system. i. the user language*, J. Symbolic Comput. **24** (1997), 235–265, http://magma.maths.usyd.edu.au/magma/.

[Bur02] W. Burnside, *On an unsettled question in the theory of discontinuous groups*, Quart. J. Pure Appl. Math. **33** (1902), 230–238.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *The atlas of finite simple groups*, Clarendon Press, Oxford, 1985.

[Con85] J. H. Conway, *A simple construction for the Fischer-Griess monster group*, Invent. Mat. **79** (1985), 513–540.

[Cox39] H. S. M. Coxeter, *The abstract groups* $G^{m,n,p}$, Trans. Amer. Math. Soc. **45** (1939), 73–150.

[CS88] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices, and groups*, Springer-Verlag, New York, 1988.

[CS94] M. Cherkassoff and D. Sjerve, *On groups generated by three involutions, two of which commute*, The Hilton Symposium, CRM Proc. Lecture Notes **6** (1994), 169–185.

[CT36] H. S. M. Coxeter and J. A. Todd, *A practical method for enumerating cosets of a finite abstract group*, Proc. of the Edinburgh Math. Soc.(Series 2) **5** (1936), 26–34.

[Dec14] S. Decelle, *The $L_2(11)$-subalgebra of the Monster algebra*, Ars Mathematica Contemporanea **7** (2014), http://amc-journal.eu/index.php/amc/article/view/259.

[Dor72] L. L. Dornhoff, *Group representations theory*, M. Dekker, New York, 1971-72.

[Edj94] M. Edjvet, *On certain quotients of the triangle groups*, J. Algebra **169** (1994), 367–391.

[EJ08] M. Edjvet and A. Juhász, *The groups $G^{m,n,p}$*, J. Algebra **319** (2008), 248–266.

[FLM88] I. B. Frenkel, J. Lepowsky, and A. Meurman, *Vertex Operator Algebras and the Monster*, Pure and Applied Mathematics, vol. 134, Academic Press, New York, 1988.

[GAP08] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008, http://www.gap-system.org).

[Gor68] D. Gorenstein, *Finite groups*, Harper & Row, New York, London, 1968.

[Gri82] R. L. Griess, *The Friendly Giant*, Invent. Mat. **69** (1982), 1–102.

[Hal58] M. Hall, *Solution of the Burnside problem for exponent six*, Illinois J. Math. **2** (1958), 764–786.

[Hav] G. Havas, *Coset enumeration strategies*.

[HH56] P. Hall and G. Higman, *On the p-length of p-soluble groups and reduction theorems for Burnside's problem*, Proc. London Math. Soc.. **3** (1956), 1–42.

[HT93] J. Howie and R. M. Thomas, *The groups $(2,\ 3,\ p;\ q)$; asphericity and a conjecture of Coxeter*, J. Algebra **154** (1993), 289–309.

[IPSS10] A. A. Ivanov, D. V. Pasechnik, Á. Seress, and S. Shpectorov, *Majorana representations of the symmetric group of degree* 4, J. Algebra **324** (2010), 2432–2463.

[IS12a] A. A. Ivanov and Á. Seress, *Majorana representations of A_5*, Math. Z. **272** (2012), 269–295.

[IS12b] A. A. Ivanov and S. Shpectorov, *Majorana representations of $L_3(2)$*, Adv. Geom. **14** (2012), 717–738.

[Iva09] A. A. Ivanov, *The monster group and Majorana involutions*, CUP, Cambridge, 2009.

[Iva11a] ———, *Majorana representation of A_6 involving $3C$-algebras*, Bull. Math. Sci. **1** (2011), 365–378.

[Iva11b] ———, *On Majorana representations of A_6 and A_7*, Comm. Math. Phys. **307** (2011), 1–16.

[Kan69] W. M. Kantor, *Automorphism groups of designs*, Math. Z. **109** (1969), 246–252.

[LdW30] F. Levi and B. L. Van der Waerden, *Über eine besonderen klasse von gruppen*, Math. Zeit. **32** (1930), 315–318.

[Maz03] V. D. Mazurov, *On generation of sporadic simple groups by three involutions two of which commute*, Sibirsk. Mat. Zh. **44:1** (2003), 193–198.

[Miy04] M. Miyamoto, *A new construction of the moonshine vertex operator algebras over the real number field*, Annals of Mathematics **159** (2004), 535–596.

[MN93] W. Meyer and W. Neutsch, *Associative subalgabras of the Griess algebra*, J. Algebra **158** (1993), 1–17.

[MSW94] G. Malle, J. Saxl, and T. Weigel, *Generation of classical groups*, Geometriae Dedicata **49** (1994), 85–116.

[Nor85] S. P. Norton, *The uniqueness of the Fischer-Griess Monster*, Contemp. Math. **45** (1985), 271–285.

[Nor96] ———, *The Monster algebra: some new formulae*, Contemp. Math. **193** (1996), 297–306.

[Nor98] ———, *Anatomy of the Monster I*, LMS Lect. Notes Ser. **249** (1998), 198–214.

[Nor13] ———, *The string of nets*, Proc. of the Edinburgh Math. Soc.(Series 2) **56** (2013), 223–262.

[Ram] C. Ramsay, *Ace*, http://www.csee.uq.edu.au/~cram/.

[Sak07] S. Sakuma, 6-*transposition property of τ-involutions of vertex operator algebras*, International Math. Research Notes (2007).

[Ser12] Á. Seress, *Construction of 2-closed M-representations*, Proc. International Symposium on Symbolic and Algebraic Computation (ISSAC '12) (2012), 311–318.

[Tod33] J. A. Todd, *A combinatorial problem*, J. Math, and Phys. **12** (1933), 321–333.

[Wei03] S. H. Weintraub, *Representation theory of finite groups: Algebra and arithmetic*, American Mathematical Society, Providence, RI, 2003.

Appendix A

Magma functions

A.1 The function 'Triangle'

The Magma function 'Triangle' was written to find a triple of generating involutions for the groups $3.A_6$ and M_{11} (see Lemma 2.30). The first argument G of the function is a group given as a permutation group, a linear group or a polycyclic group. The second argument T is the union of some conjugacy classes of involutions in G. The function returns two values; *answer* and *triple*. If there exists a triple of generating involutions in $T \subset G$ then *answer* has the value 1 and *triple* is a triple of involutions generating G; otherwise *answer* takes the value 0 and *triple* gives the identity of G (thrice).

```
function Triangle(G,T)

answer:=0;
triple:=[Id(G),Id(G),Id(G)];
T:=SetToSequence(T);

for i:=1 to #T do
        for j:=i+1 to #T do
                for k:=j+1 to #T do
                H:=sub<G|T[i],T[j],T[k]>;
                        if H eq G then
                        answer:=1;
                        triple:=[T[i],T[j],T[k]];
                        break k; break j; break i;
                        end if;
                end for;
        end for;
end for;
```

```
return answer, triple;

end function;
```

A.2 The semidirect product $G_{11} \cong (3^4 : 2) : (3^{1+2}_{+} : 2^2)$

In subsection 3.3.3 we described the quotient Q of the group $G := G^{(6,6,6;\ 6,6,6)}$, where

$$G^{(6,6,6;\ 6,6,6)} := \langle a, b, c \mid a^2,\ b^2,\ c^2,\ (ab)^2,\ (ac)^6,\ (bc)^6,\ (abc)^6,\ (ab^c)^6,\ (abb^c)^6,\ (aba^c)^6 \rangle,$$

and

$$Q := G/\langle (c^a \cdot c^{bc})^3 \rangle \cong (3^4 : 2) : (3^{1+2}_{+} : 2^2).$$

We recall that we can write $G = (N : \langle y \rangle) : H$ where $H = \langle a,\ b,\ a^c \rangle \cong 3^{1+2}_{+} : 2^2$, $N = \langle x,\ x^a,\ x^b,\ x^{ab}, x^{bc} \rangle \cong 3^5$ for $x := (c \cdot a^{cb})^2$, and y is an involution inverting every element of N by Proposition 3.55.

The short Magma program below gives the action of H on the elementary abelian group N.

```
L:=[6,6,6,6,6,6,6,6,6];
k:=L[1];l:=L[2];m:=L[3];
n:=L[4];p:=L[5];q:=L[6];
r:=L[7];s:=L[8];t:=L[9];

K<a,b,c>:= Group< a, b, c  | a^2, b^2, c ^2, (a*b)^2, (a*c)^k, (b*c)^l, (a*b*c)^m,
 (a*c*b*c)^n, (a*c*a*b*c)^p, (b*c*a*b*c)^q, (c*a*c*b*c*a)^r,
 (c*a*c*a*b*c*a)^s, (c*b*a*c*a*c*a*b)^t >;

Order(K);

G:=PCGroup(K);Order(G);

trio:=[ G.2*G.3, G.2*G.4^2*G.9*G.10*G.11^2, G.1*G.5*G.6*G.9^2*G.11^2 ];

a:=trio[1];b:=trio[2];c:=trio[3];
gensH:=[a,b,a^c];
H:=sub<G|gensH>;Order(H);

x:=(c*b^(c*a))^2;Order(x);N:=sub<G|x>;

list:=[x,x^a,x^b,x^(a*b),x^(b*c)];

function Action(t,list)
        vec:=[0,0,0,0,0];
        l:=list;
```

```
                for i1:=0 to 2 do
                vec[1]:=i1;
                        for i2:=1 to 3 do
                        vec[2]:=i2-1;
                                for i3:=1 to 3 do
                                vec[3]:=i3-1;
                                        for i4:=1 to 3 do
                                        vec[4]:=i4-1;
                                                for i5:=1 to 3 do
                                                vec[5]:=i5-1;
                                                u:=l[1]^(vec[1])*l[2]^(vec[2])*
                                                l[3]^(vec[3])*l[4]^(vec[4])*l[5]^(vec[5]);
                                                        if t eq u then
                                                        return vec;
                                                        break i5;break i4;break i3;
                                                        break i2;break i1;
                                                        end if;
                                                end for;
                                        end for;
                                end for;
                        end for;
                        end for;
end function;

for j:=1 to #gens do
u:=gensH[j];
for i:=1 to #list do
Action(list[i]^u,list);
end for;
end for;

a:=GL(5,3)![[ 0, 1, 0, 0, 0 ],
[ 1, 0, 0, 0, 0 ],
[ 0, 0, 0, 1, 0 ],
[ 0, 0, 1, 0, 0 ],
[ 1, 2, 2, 1, 1 ]];


b:=GL(5,3)![[ 0, 0, 1, 0, 0 ],
[ 0, 0, 0, 1, 0 ],
[ 1, 0, 0, 0, 0 ],
[ 0, 1, 0, 0, 0 ],
[ 2, 0, 1, 0, 1 ]];


cac:=GL(5,3)![[ 1, 1, 2, 2, 0 ],
[ 0, 1, 0, 0, 0 ],
[ 1, 1, 1, 0, 1 ],
[ 2, 1, 1, 2, 2 ],
```

```
[ 1, 0, 1, 1, 2 ]];

U:=sub<GL(5,3)|a,b,cac>;IsIsomorphic(U,H);

J:=Orbits(sub<U|cac>);
for i:=1 to #J do
print #J[i];
end for;
```

Appendix B

Appendix B

B.1 Shapes for the representations $\mathcal{R}_1$ of G_1

From the proof of Proposition 3.11 the group $G_1 = G^{(4,4,4)}$ is isomorphic to the semidirect product $N : K$ where $K := \langle a,\ b\rangle \cong 2^2$ acts by conjugation on $N := \langle c\rangle \times \langle c^a\rangle \times \langle c^b\rangle \times \langle c^{ab}\rangle \cong 2^4$ which is the normal closure of $\langle c\rangle$ in G_1. The group G_1 has centre $Z(G_1) = \langle z\rangle \cong 2$ where $z := c \cdot c^a \cdot c^b \cdot c^{ab} \in N$. We denote by 1_N the identity of N. The orbits of K on N have sizes $1,\ 1,\ 2,\ 2,\ 2,\ 4$ and 4:

$$\{1_N\},\ \{z\},\ O_1 := \{c \cdot c^a,\ c^b \cdot c^{ab}\},\ O_2 := \{c \cdot c^b,\ c^a \cdot c^{ab}\},\ O_3 := \{c^b \cdot c^a,\ c^b \cdot c^{ab}\},$$
$$O_4 := \{c \cdot c^b \cdot c^a,\ c \cdot c^a \cdot c^{ab},\ c \cdot c^b \cdot c^{ab},\ c^a \cdot c^b \cdot c^{ab}\} \text{ and } O_5 := \{c,\ c^a,\ c^b,\ c^{ab}\}.$$

Proposition B.1. *The conjugacy classes of G_1 are as follows :*

Class in G_1	$1a$	$2a$	$2b$	$2c$	$2d$	$2e$	$2f$	$2g$	$2h$	$2i$	$4a$	$4b$	$4c$	$4d$	$4e$	$4f$
p-powers	–	–	–	–	–	–	–	–	–	–	a	a	a	b	c	d
Size	1	1	2	2	2	4	4	4	4	4	4	4	4	8	8	8

where the representatives of the conjugacy classes are:

$2a$ *: the central element z,*

$2b$ *: the elements in the orbit O_1 of K,*

$2c$ *: the elements in the orbit O_2 of K,*

$2d$: *the elements in the orbit* O_3 *of* K,

$2e$: *the elements in the orbit* O_4 *of* K,

$2f$: $(n,\ b)$ *where* $n \in Fix_N(b) = \{1,\ z,\ c \cdot c^b,\ c^a \cdot c^{ab}\}$,

$2g$: $(n,\ ab)$ *where* $n \in Fix_N(ab) = \{1,\ z,\ c \cdot c^{ab},\ c^a \cdot c^b\}$,

$2h$: $(n,\ a)$ *where* $n \in Fix_N(a) = \{1,\ z,\ c \cdot c^a,\ c^b \cdot c^{ab}\}$,

$2i$: *the elements in the orbit* O_4 *of* K *which contains* c,

$4a$: $(n,\ a)$ *where* $n \in N \backslash Fix_N(a)$ *such that* $n \cdot n^a = z$,

$4b$: $(n,\ b)$ *where* $n \in N \backslash Fix_N(b)$ *such that* $n \cdot n^b = z$,

$4c$: $(n,\ ab)$ *where* $n \in N \backslash Fix_N(ab)$ *such that* $n \cdot n^{ab} = z$,

$4d$: $(n,\ a)$ *where* $n \in N \backslash Fix_N(a)$ *such that* $n \cdot n^a \neq z$,

$4e$: $(n,\ b)$ *where* $n \in N \backslash Fix_N(b)$ *such that* $n \cdot n^b \neq z$,

$4f$: $(n,\ ab)$ *where* $n \in N \backslash Fix_N(ab)$ *such that* $n \cdot n^{ab} \neq z$.

□

From the above proposition the next lemma is immediate.

Lemma B.2. *The three involutions* a, b, c *generating* G_1 *are in conjugacy classes* $2h,\ 2f,\ 2i$ *respectively, and the involution* ab *is in conjugacy class* $2g$. □

Proposition B.3. *Let* $T_1 = 2f \cup 2g \cup 2h \cup 2i$ *and let* $\mathcal{R}_1 := (G_1, T_1, X_1)$ *be a Majorana representation of* G_1. *Then there are* 2^5 *possible shapes for* $\mathcal{R}_1$ *of which only two are allowed in* $V_{\mathbb{M}}$.

Proof. Elements in the product set T_1^2 are in all conjugacy classes of G_1 except $2e$. The types of the classes of elements of order 4 are determined by types of their squares from the inclusions of the dihedral Majorana algebras $2A \hookrightarrow 4B$ and $2B \hookrightarrow 4A$. So only the types of the conjugacy classes of involutions involved in T_1^2 need to be determined. From the definition of a Majorana representation the type of the conjugacy classes involved in T_1 is $2A$. For the other classes of involutions involved in T_1^2 which are $2a,\ 2b,\ 2c,\ 2d$ they can either be of type $2A$ or $2B$. If any of the classes $2a,\ 2b,\ 2c,\ 2d$ is of type $2A$, then by condition (2A) of the definition of a Majorana representation we include them in a set S_1 also containing T_1. Then in order to find

the full shape of $\mathcal{R}_1$ we need to find in which conjugacy classes the elements of S_1^2 lie. Using structure class constants we find that the set S_1^2 contains, in addition of T_1^2, elements from the conjugacy class $2e$ which can be of type $2A$ or $2B$ so there are $1 + (2^4 - 1) \times 2 = 31$ possible shapes for $\mathcal{R}_1$ so far. We can also join to T_1 the class $2e$, hence there are in total 2^5 possible shapes for $\mathcal{R}_1$. From Norton's Table 3.2, there are two conjugacy classes of $2A$-embedded G_1 subgroups in $\mathbb{M}$ and hence only two possible shapes for $\mathcal{R}_1$ for which X_1 could be a subalgebra of $V_{\mathbb{M}}$. □

B.2 Shapes for the representations $\mathcal{R}_2$ of G_2

From the proof of Proposition 3.11 the group $G_2 = G^{(4,4,6)}$ is isomorphic to the semidirect product $(N_1 \times N_2) : K$ where $K := \langle a,\ b\rangle \cong 2^2$ acts by conjugation on $N_1 \times N_2 := \langle r_1,\ s_1\rangle \times \langle r_2,\ s_2\rangle \cong S_3 \times S_3$ where we let $r_1 := (1,2) = c^{abc}$, $s_1 := (2,3) = c$, $r_2 := (4,5) = c^{abca}$ and $s_2 := (5,6) = c^a$. The group G_2 has centre $Z(G_2) = \langle z\rangle \cong 2$ where $z := r_1 r_2 \beta = c^{abc} c^{abca} ab$. The orbits of K on the 15 involutions of $N_1 \times N_2$ have sizes $1, 2, 2, 2, 4, 4$ and 4 where the size 1 orbit contains $r_1 r_2$.

Proposition B.4. *The conjugacy classes of G_2 are as follows :*

Class in G_2	$1a$	$2a$	$2b$	$2c$	$2d$	$2e$	$2f$	$2g$	$3a$	$3b$	$4a$	$4b$	$6a$	$6b$	$6c$	$6d$	$6e$	$6f$
p-powers	–	–	–	–	–	–	–	–	–	–	g	g	aa	ba	ac	ad	bb	be
Size	1	1	6	6	6	6	9	9	4	4	18	18	4	4	12	12	12	12

where the representatives of the conjugacy classes are:

$2a$: *the central element z,*

$2b$: *the elements $n\alpha$ where $n \in N_1 \times N_2$ such that $n^\alpha = n^{-1}$,*

$2c$: *the orbit O_1 of size 6 of the actions of $N_1 \times N_2$ and K on the involutions of $N_1 \times N_2$, where $O_1 := \{r_1,\ s_1,\ r_2,\ s_2,\ s_1^{r_1},\ s_2^{r_2}\}$,*

$2d$: *the elements nz where $n \in 2c$,*

$2e$: *the elements $n\alpha\beta$ where $n \in N_1 \times N_2$ such that $n^{\alpha\beta} = n^{-1}$,*

$2f$: *the elements $n\beta$ where $n \in N_1 \times N_2$ such that $n^\beta = n^{-1}$,*

$2g$: *the other orbit* O_2 *of size* 9 *of the actions of* $N_1 \times N_2$ *and* K *on the involutions of* $N_1 \times N_2$, *where* $O_2 := \{r_1r_2,\ s_1r_2,\ r_1s_2,\ s_1^{r_1}r_2,\ r_1s_2^{r_2},\ s_1s_2^{r_2},\ s_1^{r_1}s_2\}$,

$3a$: *the orbit* L_1 *of size* 4 *of the actions of* $N_1 \times N_2$ *and* K *on the elements of order* 3 *of* $N_1 \times N_2$, *where* $L_1 := \{r_1s_1,\ r_2s_2,\ s_1r_1,\ s_2r_2\}$,

$3b$: *the orbit* L_2 *of size* 4 *of the actions of* $N_1 \times N_2$ *and* K *on the elements of order* 3 *of* $N_1 \times N_2$, *where* $L_2 := \{r_1s_1r_2s_2,\ r_1s_1s_2r_2,\ s_1r_1s_2r_2,\ s_1r_1r_2s_2\}$,

$4a$: *the conjugates of* $r_1s_1\alpha = ca$,

$4b$: *the conjugates of* $zr_1s_1\alpha$,

$6a$: *the elements* zh *where* $h \in 3a$,

$6b$: *the elements* zh *where* $h \in 3b$,

$6c$: *the elements of order* 6 *in* $N_1 \times N_2$,

$6d$: *the elements* zl *where* $l \in 6c$,

$6e$: *the elements* $n\alpha$ *where* $n \in N_1 \times N_2$ *such that* $n^\alpha \neq n^{-1}$,

$6f$: *the elements* $n\alpha\beta$ *where* $n \in N_1 \times N_2$ *such that* $n^{\alpha\beta} \neq n^{-1}$.

□

From the above proposition the next lemma is immediate.

Lemma B.5. *The three involutions* a, b, c *generating* G_2 *are in conjugacy classes* $2b,\ 2e,\ 2d$ *respectively, and the involution* ab *is in conjugacy class* $2f$. □

Proposition B.6. *Let* $T_2 = 2b \cup 2d \cup 2e \cup 2f$ *and let* $\mathcal{R}_2 := (G_2, T_2, X_2)$ *be a Majorana representation of* G_2. *Then there are two possible shapes for* $\mathcal{R}_2$ *of which only one is allowed in* $V_{\mathbb{M}}$.

Proof. The proof is similar to that of Proposition B.3. We find which conjugacy classes are involved in the shape of $\mathcal{R}_2$ by determining in which conjugacy classes the products of any two involutions from the set T_2 lie. If any element of T_2^2 has order 6 and squares to an involution not conjugate to any element of T_2 then we include its conjugacy class in T_2. We find that all the conjugacy classes of G_2 are involved in the shape of $\mathcal{R}_2$ and all their types are determined except for the type of $2g$ which can either be $2A$ or $2B$ and hence the elements in $4a$ and $4b$ are

either of type $4B$ or $4A$. By the classification of dihedral Majorana representations, products of two Majorana involutions of order 6 have type $6A$ so the classes of the elements of order 6 must be of type $6A$. Then by the inclusions of dihedral Majorana subalgebras $2A, 3A \hookrightarrow 6A$, the squares of the elements of order 6 must of type $3A$ and their cubes must of type $2A$ so the other conjugacy classes of involutions are all of type $2A$ and the conjugacy classes of elements of order 3 are all of type $3A$. Hence there are two possible shapes for $\mathcal{R}_2$. From Norton's Table 3.2, there is a unique conjugacy class of $2A$-embedded G_2 subgroups in $\mathbb{M}$ and hence a unique possible shape for $\mathcal{R}_2$ for which X_2 could be a subalgebra of $V_{\mathbb{M}}$, which is when $2g$ is of type $2B$. □

B.3 Shapes for the representations $\mathcal{R}_3$ of G_3

From the proof of Proposition 3.11 the group $G_3 = G^{(4,5,5)}$ is isomorphic to the semidirect product $N : D \cong 2^4 : D_{10}$ where $D := \langle b,\ c\rangle \cong D_{10}$ acts on $D := \langle a\rangle \times \langle a^c\rangle \times \langle a^{cb}\rangle \times \langle a^{cbc}\rangle \cong 2^4$ which is the normal closure of $\langle a\rangle$ in G_3. We rename $v_1,\ v_2,\ v_3$ and v_4 respectively the generators $a,\ a^c,\ a^{cb}$ and a^{cbc} of N. We use the additive notation for elements of N and we denote its identity by 0. The orbits of D on N have sizes 1, 5, 5 and 5:

$$\{0\},\ N1 := \{v_1,\ v_2,\ v_3,\ v_4,\ v_1+v_2+v_3+v_4\},$$
$$N_2 := \{v_1+v_2,\ v_1+v_3,\ v_2+v_4,\ v_1+v_2+v_4,\ v_1+v_2+v_3\} \text{ and}$$
$$N_3 := \{v_2+v_3,\ v_1+v_4,\ v_3+v_4,\ v_1+v_3+v_4,\ v_2+v_3+v_4\}.$$

Proposition B.7. *The conjugacy classes of G_3 are as follows :*

Class in G_3	$1a$	$2a$	$2b$	$2c$	$2d$	$4a$	$4b$	$4c$	$5a$	$5b$
p-powers	–	–	–	–	–	a	b	c	–	–
Size	1	5	5	5	20	20	20	20	32	32

where the representatives of the conjugacy classes are:

$2a$ *: the elements in the orbit N_1 of D,*

$2b$ *: the elements in the orbit N_2 of D,*

$2c$ *: the elements in the orbit N_3 of D,*

$2d$: (n,t) *where* t *is an involution of* D *and* $n \in Fix_N(t)$,

$4a$: (n,t) *where* t *is an involution of* D *and* $n \neq 0$ *and* $\in N_1 \backslash Fix_{N_1}(t)\}$,

$4b$: (n,t) *where* t *is an involution of* D *and* $n \in N$ *such that* $n^t n \in N_2$,

$5a$: (n,f) *where* $f \in \{bc, (bc)^4\}$ *is an element of order* 5 *in* D *and* n *is any element of* N,

$5b$: (n,f^2) *where* $f \in \{bc, (bc)^4\}$ *and* n *is any element of* N.

□

From the above proposition the next lemma is immediate.

Lemma B.8. *The three involutions* a, b, c *generating* G_3 *are in conjugacy classes* $2a$, $2d$, $2d$ *respectively and* ab *is in* $2a$. □

Proposition B.9. *Let* $T_3 = 2a \cup 2d$ *and let* $\mathcal{R}_3 := (G_3, T_3, X_3)$ *be a Majorana representation of* G_3. *Then there are four possible shapes for* $\mathcal{R}_3$ *of which only two are allowed in* $V_{\mathbb{M}}$.

Proof. We proceed as in the proof of Proposition B.3. From the definition of a Majorana representation the elements in the classes $2a$ and $2d$ must be of type $2A$. We find that the set T_3^2 contains elements from all conjugacy classes of G_3. By the classification of dihedral Majorana representations, products of two Majorana involutions of order 5 have type $5A$ so the classes $5a$ and $5b$ are of type $5A$. Elements in the class $4a$ must be of type $4B$ since their squares are of type $2A$, by the inclusion of dihedral Majorana algebras $2A \hookrightarrow 4B$. The elements in the classes $2b$ and $2c$ can either be of type $2A$ or $2B$ and they determine the types of the classes $4b$ and $4c$. Hence there are four different shapes for $\mathcal{R}_3$. From Norton's Table 3.2, there are two conjugacy class of $2A$-embedded G_3 subgroups in $\mathbb{M}$ and hence two possible shapes for $\mathcal{R}_3$ for which X_3 could be a subalgebra of $V_{\mathbb{M}}$. From rows 2 and 6 of Norton's Table 3.2 an elementary abelian subgroup of order 8 in $\mathbb{M}$ which is generated by three $2A$ involutions a, b, c has its elements ac, bc, abc in conjugacy classes $2A, 2A, 2B$ or $2B, 2B, 2B$ of $\mathbb{M}$ respectively. From this fact we deduce that the two possible shapes for $\mathcal{R}_3$ that are allowed in $V_{\mathbb{M}}$ are when $2b$ and $2c$ are of different types; either $2b$ is $2A$ and $2c$ is $2B$, or $2b$ is $2A$ and $2c$ is $2A$. □

B.4 Shapes for the representations $\mathcal{R}_4$ of G_4

From the proof of Proposition 3.11 the group $G_4 = G^{(4,5,6)}$ is isomorphic to the direct product $\langle z \rangle \times H \cong 2 \times S_5$ so we can take the generators a, b, c of G_4 to be equal to $(1,2)$, $(3,4)(6,7)$,

$(1,3)(2,5)(6,7)$ where the centre of G_4 consists of the involution $z := (6,7) = (b \cdot a^c)^3$ and the group H is generated by $a,\ bz,\ cz$.

Proposition B.10. *The conjugacy classes of G_4 are as follows :*

Class in G_4	$1a$	$2a$	$2b$	$2c$	$2d$	$2e$	$3a$	$4a$	$4b$	$5a$	$6a$	$6b$	$6c$	$10a$
p-powers	$-$	$-$	$-$	$-$	$-$	$-$	$-$	e	e	$-$	ac	ab	aa	aa
Size	1	1	10	10	15	15	20	30	30	24	20	20	20	24

where the representatives of the conjugacy classes are:

$2a$ *: the central element z,*

$2b$ *: the elements zt where t is a transposition of $H \cong S_5$,*

$2c$ *: the transpositions of H,*

$2d$ *: the elements zs where s is a $(2,2)$-cycle of H,*

$2e$ *: the $(2,2)$-cycles of H,*

$3a$ *: the (3)-cycles of H,*

$4a$ *: the elements zq where q is a (4)-cycle of H,*

$4b$ *: the (4)-cycles of H,*

$5a$ *: the (5)-cycles of H,*

$6a$ *: the $(2,3)$-cycles of H,*

$6b$ *: the elements zr where r is a $(2,3)$-cycle of H,*

$6c$ *: the elements zh where h is a (3)-cycle of H,*

$10a$ *: the elements zf where f is a (5)-cycle of H.*

□

From the above proposition the next lemma is immediate.

Lemma B.11. *The three involutions a, b, c and ab of G_4 are in conjugacy classes $2c,\ 2b,\ 2d$ and $2d$ respectively.* □

Proposition B.12. *Let $T_4 = 2b \cup 2c \cup 2d$ and let $\mathcal{R}_4 := (G_4, T_4, X_4)$ be a Majorana representation of G_4. Then there is a unique shape for $\mathcal{R}_4$ and that shape is allowed in $V_{\mathbb{M}}$.*

Proof. Elements in the product set T_4^2 are in all conjugacy classes of G_4 except $10a$. The conjugacy classes $6a,\ 6b,\ 6c$ are necessarily of type $6A$ and $5a$ is of type $5A$. From the definition of a Majorana representation the type of the conjugacy classes involved in T_4 is $2A$. The type of the conjugacy class $2e$ must be $2B$ because the product of two Majorana involutions cannot have order 10. By the inclusion of the dihedral Majorana algebras $2A \hookrightarrow 6A,\ 3A \hookrightarrow 6A$, the squares and cubes of elements in $6a,\ 6b,\ 6c$, which are in classes $3a$ and $2a,\ 2b,\ 2c$, have types $3A$ and $2A$ respectively. From the inclusions of dihedral Majorana algebras $2A \hookrightarrow 4B$ and $2B \hookrightarrow 4A$ the classes $4a$ and $4b$ are of type $4A$, and so the shape of $\mathcal{R}_4$ is uniquely determined. From Norton's Table 3.2, there is a unique conjugacy class of $2A$-embedded G_4 subgroups in $\mathbb{M}$ and hence the unique shape of $\mathcal{R}_4$ is allowed in $V_{\mathbb{M}}$.

□

B.5 Shapes for the representations $\mathcal{R}_6$ of G_6

From the proof of Lemma 3.18 the group G_6 is equal to $G^{(4,6,6;\ 4)}$ where we recall that $G^{(m,n,p;\ r_1)} := \langle a, b, c \mid a^2,\ b^2,\ c^2,\ (ab)^2,\ (ac)^m,\ (bc)^n,\ (abc)^p,\ (ab^c)^{r_1}\rangle$. The group G_6 is isomorphic to the semidirect product $N : D \cong 2^5 : D_{12}$ where $D := \langle b,\ c\rangle \cong D_{12}$ acts on $N := \langle a\rangle \times \langle a^c\rangle \times \langle a^{cb}\rangle \times \langle a^{cbc}\rangle \times \langle a^{cbcb}\rangle \cong 2^5$ which is the normal closure of $\langle a\rangle$ in G_6. We rename $v_1,\ v_2,\ v_3,\ v_4$ and v_5 the generators $a,\ a^c,\ a^{cb},\ a^{cbc}$ and a^{cbcb} of N, respectively. We use the additive notation for products of elements of N and we denote its identity by 0. The centre $Z(G_6)$ is equal to $\langle z\rangle \cong 2$ where z is the involution $z := v_1 + v_4 + v_5 = aa^{cbc}a^{cbcb} \in N$. The orbits of D on N have sizes $1,\ 1,\ 3,\ 3,\ 6,\ 6,\ 6$ and 6 where we let $U_1,\ U_2$ be the orbits of sizes 3 and $O_1,\ O_2,\ O_3,\ O_4$ be the orbits of size 6 such that:

$$U_1 := \{v_2 + v_5,\ v_3 + v_4,\ v_2 + v_3 + v_4 + v_5\},\ U_2 := \{zu_1 \mid u_1 \in U_1\},$$
$$O_1 := \{v_1,\ v_2,\ v_3,\ v_4,\ v_5,\ v_1 + v_2 + v_3 + v_4 + v_5\},\ O_2 := \{zo_1 \mid o_1 \in O_1\},$$
$$O_3 := \{v_1+v_2,\ v_1+v_3,\ v_2+v_4,\ v_3+v_5,\ v_1+v_2+v_3+v_5,\ v_1+v_2+v_3+v_4\},\ O_4 := \{zo_3 \mid o_3 \in O_3\}.$$

Proposition B.13. *The conjugacy classes of G_6 are as follows :*

Class in G_6	$1a$	$2a$	$2b$	$2c$	$2d$	$2e$	$2f$	$2g$	$2h$	$2i$	$2j$	$2k$	$2l$	$2m$
p-powers	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Size	1	1	3	3	4	4	6	6	6	6	12	12	12	12

Class in G_6	$3a$	$4a$	$4b$	$4c$	$4d$	$4e$	$4f$	$4g$	$4h$	$4i$	$4j$	$6a$	$6b$	$6c$
p-powers	–	b	b	b	b	b	b	g	h	h	g	ad	ad	aa
Size	32	12	12	12	12	12	12	24	24	24	24	32	32	32

where the representatives of the conjugacy classes of involutions are:

$2a$ *: the central element* z,

$2b$ *: the elements in the orbit* U_1 *of* D,

$2c$ *: the elements in the orbit* U_2 *of* D,

$2d$ *:* $n(bc)^3$ *where* $(bc)^3$ *is the central involution of* D *and* $n \in Fix_N((bc)^3)$,

$2e$ *:* $zn(bc)^3$ *where* $(bc)^3$ *is the central involution of* D *and* $n \in Fix_N((bc)^3)$,

$2f$ *: the elements in the orbit* O_1 *of* D,

$2g$ *: the elements in the orbit* O_2 *of* D,

$2h$ *: the elements in the orbit* O_3 *of* D,

$2i$ *: the elements in the orbit* O_4 *of* D,

$2j$ *:* nt *where* $t \in \{b,\ b^c,\ b^{cb}\} \subset D$ *and* $n \in Fix_N(t)$,

$2k$ *:* znt *where* $t \in \{b,\ b^c,\ b^{cb}\} \subset D$ *and* $n \in Fix_N(t)$,

$2l$ *:* ns *where* $s \in \{c,\ c^b,\ c^{bc}\} \subset D$ *and* $n \in Fix_N(s)$,

$2m$ *:* zns *where* $s \in \{c,\ c^b,\ c^{bc}\} \subset D$ *and* $n \in Fix_N(s)$.

□

From the above proposition the next lemma is immediate.

Lemma B.14. *The three involutions a, b, c generating G_6 are in conjugacy classes $2f,\ 2j,\ l$ respectively and ab is in class $2k$.* □

Proposition B.15. *Let $T_6 = 2f\ \cup\ 2j\ \cup\ 2k\ \cup\ 2l$ and let $\mathcal{R}_6 := (G_6, T_6, X_6)$ be a Majorana representation of G_6. Then there are 2^5 possible shapes for $\mathcal{R}_6$ of which only one is allowed in $V_{\mathbb{M}}$.*

Proof. The proof is similar to the proof of Proposition B.9 for the group G_3. We find that all conjugacy classes of G_6 are involved in the shape of $\mathcal{R}_6$ so that the elements of order 6 are of type $6A$ and the types of the elements of order 4 are determined by the types of their squares. From the definition of a Majorana representation and the inclusions between dihedral Majorana algebras we obtain that the involutions in the classes $2a,\ 2d,\ 2e,\ 2f,\ 2j,\ 2k,\ 2m$ are of type $2A$ and the elements in $3a$ are of type $3A$. The only types left to determine are those of the classes $2b,\ 2c,\ 2g,\ 2h,\ 2i$ which can either be $2A$ or $2B$ so there are 2^5 possible shapes for $\mathcal{R}_6$. From Norton's Table 3.2, there is only one conjugacy class of $2A$-embedded G_6 subgroups in $\mathbb{M}$ which can be found in row 30 of Table 3.2. Hence there is only one shape for $\mathcal{R}_6$ for which X_6 could be a subalgebra of $V_{\mathbb{M}}$. □

B.6 Shapes for the representations $\mathcal{R}_7$ of G_7

From the proof of Lemma 3.20 the group $G_7 = G^{(6,5,5;5)}$ is isomorphic to the semidirect product $N : A$ where $A := \langle a,\ b,\ a^c \rangle \cong A_5$ acts on $N \cong 2^4$ which is the normal closure of the involution $y := (ac)^3$. The subgroup N can be generated by the four elements $y,\ y^b,\ y^{bc}$ and y^{bcb} which we rename $v_1,\ v_2,\ v_3$ and v_4 respectively. We use the additive notation for elements of N and we denote its identity by 0. The action of A on N is intransitive and stems from the isomorphism $SL_2(4) \cong P\Omega_4^-(2)$. The orbits of A on N have sizes 1, 5 and 10:

$$\{0\},\ N1 := \{v_1 + v_2,\ v_1 + v_3,\ v_2 + v_4,\ v_1 + v_2 + v_3,\ v_1 + v_2 + v_4\},$$
$$N_2 := \{v_1,\ v_2,\ v_3,\ v_4,\ v_1 + v_4,\ v_2 + v_3,\ v_3 + v_4,\ v_1 + v_3 + v_4,\ v_2 + v_3 + v_4,\ v_1 + v_2 + v_3 + v_4\}.$$

Proposition B.16. *The conjugacy classes of G_7 are as follows :*

Class in G_7	$1a$	$2a$	$2b$	$2c$	$3a$	$4a$	$4b$	$5a$	$5b$	$6a$	$6b$	$6c$
p-powers	–	–	–	–	–	a	b	–	–	aa	aa	ab
Size	1	5	10	60	80	60	120	192	192	80	80	80

where the representatives of the conjugacy classes are:

$2a$: *the elements in the orbit* N_1 *of* A,

$2b$: *the elements in the orbit* N_2 *of* A,

$2c$: (n_t, t) *where* t *is a* $(2,2)$*-cycle of* A *and* $n_t \in Fix_N(t)$, *for example* (n_a, a) *where* $n_a \in \{0,\ v_1,\ v_2,\ v_1+v_2\}$,

$3a$: (n_h, h) *where* h *is a* (3)*-cycle of* A *and* $n_h \in N$ *such that* $n_h + n_h^h + n_h^{h^2} = 0$, *for example* $(n, (ac)^2)$ *where* $n \in \{0,\ v_2,\ v_3,\ v_2+v_3\}$,

$4a$: (n_t, t) *where* t *is a* $(2,2)$*-cycle of* A *and* $n_t \in N_1 \backslash Fix_{N_1}(t)$,

$4b$: (n_t, t) *where* t *is a* $(2,2)$*-cycle of* A *and* $n_t \in N_2 \backslash Fix_{N_2}(t)$,

$5a$: (n, f) *where* f *is a* (5)*-cycle of* A *and* $n \in N$,

$5b$: (n, f^2) *where* f *is a* (5)*-cycle of* A *non-conjugate to a* (5)*-cycle in class* $5b$ *and* $n \in N$,

$6a$: (n_h, h) *where* h *is a* (3)*-cycle of* A *and* $n_h \in N$ *such that* $n_h + n_h^h + n_h^{h^2} \in N_1$,

$6b$: (n_h, h) *where* h *is a* (3)*-cycle of* A *and* $n_h \in N$ *such that* $n_h + n_h^h + n_h^{h^2} \in N_1$, *and where* (n_h, h) *is non-conjugate to an element of class* $6a$,

$6c$: (n_h, h) *where* h *is a* (3)*-cycle of* A *and* $n_h + n_h^h + n_h^{h^2} \in N_2$.

□

From the above proposition the next lemma is immediate.

Lemma B.17. *The three involutions* a, b, c *generating* G_7 *are all in conjugacy class* $2c$. □

Proposition B.18. *Let* $T_7 = 2c$ *and let* $\mathcal{R}_7 := (G_7, T_7)$ *be a Majorana representation of* G_7. *Then there are two possible shapes for* $\mathcal{R}_7$ *of which only one is allowed in* $V_{\mathbb{M}}$.

Proof. Elements in the product set T_7^2 are in either of the G_7 conjugacy classes $1a,\ 2a,\ 2b,\ 2c, 3a,\ 4a, 5a,\ 5b$ or $6c$. From the definition of a Majorana representation, products of involutions in the class $2c$ have type $2A$. Elements in the conjugacy classes $5a$ and $5b$ have type $5A$ and elements in $6c$ have type $6A$. By the inclusion of dihedral Majorana algebras $2A \hookrightarrow 6A,\ 3A \hookrightarrow 6A$, the squares and cubes of elements in $6a$, which are in classes $3a$ and $2b$, have types $3A$ and $2A$ respectively. By condition (2A) in the definition of a Majorana representation, products of

involutions from the union $S := T_7 \cup \{2c\}$ are involved in the shape of $\mathcal{R}_7$. Elements in the set S^2 are conjugate to either elements of T_7^2 or to $4b$. Only the types of the elements in classes $2a,\ 4a,\ 4b$ are left to be determined. The elements in $4a$ and $4b$ square to elements in $2a$, so by the inclusions of dihedral Majorana algebras $2A \hookrightarrow 4B,\ 2B \hookrightarrow 4A$ there are two possibilities for the shape of $\mathcal{R}_7$ determined by the type of $2a$ which can be either $2A$ or $2B$. From Norton's Table 3.2, there is only one conjugacy class of $2A$-embedded G_7 subgroups in $\mathbb{M}$ which can be found in row 32 of Table 3.2. Hence the only shape of $\mathcal{R}_7$ for which X_7 could be a subalgebra of $V_{\mathbb{M}}$ is when $2a$ has type $2B$, by a similar argument to the one found at the end of the proof of Proposition B.9. □

B.7 Shapes for the representations $\mathcal{R}_8$ of G_8

From the proof of Lemma 3.22 the group $G_8 = G^{(6,6,5:4)}$ is isomorphic to the direct product $\langle z \rangle \times H \cong 2 \times S_6$ so we can take the generators $a,\ b,\ c$ to be equal to $(1,4)(2,6)(3,5),\ (1,4)(7,8),$ $(2,5)(3,4)(7,8)$ where the centre of G_8 consists of the involution $z := (7,8) = (b \cdot a^c)^3$ and the group H is generated by $a,\ bz,\ cz$.

Proposition B.19. *The conjugacy classes of G_8 are as follows :*

Class in G_8	$1a$	$2a$	$2b$	$2c$	$2d$	$2e$	$2f$	$2g$	$3a$	$3b$	$4a$
p-powers	–	–	–	–	–	–	–	–	–	–	g
Size	1	1	15	15	15	15	45	45	40	40	90

Class in G_8	$4b$	$4c$	$4d$	$5a$	$6a$	$6b$	$6c$	$6d$	$6e$	$6f$	$10a$
p-powers	g	g	g	–	aa	ba	ac	be	bd	ab	aa
Size	90	90	90	144	40	40	120	120	120	120	144

where the representatives of the conjugacy classes of involutions are:

$2a$ *: the central element* $z = (7,8)$,

$2b$ *: the* $(2,2,2)$*-cycles of* H*, for example* a,

$2c$ *: the elements* zt *where* $t \in 2b$,

$2d$: *the elements zs where s is a transposition of H, for example b,*

$2e$: *the elements s where s is a transposition of H, for example zb,*

$2f$: *the elements zr where r is a $(2,2)$-cycle of H, for example c,*

$2g$: *the elements r where r is a $(2,2)$-cycle of H, for example zc.*

□

From the above proposition the next lemma is immediate.

Lemma B.20. *The three involutions a, b, c generating G_8 are in conjugacy classes $2b$, $2d$, $2f$ respectively, and the involution ab is in class $2f$.* □

Proposition B.21. *Let $T_8 = 2b \cup 2d \cup 2f$ and let $\mathcal{R}_8 := (G_8, T_8, X_8)$ be a Majorana representation of G_8. Then there is a unique possible shape for $\mathcal{R}_8$ and this shape is allowed in $V_{\mathbb{M}}$.*

Proof. The proof is very similar to the proof of Proposition B.12 so we do not include all the details here. We find that all the conjugacy classes of G_8 are involved in the shape of $\mathcal{R}_8$ and from the definition of a Majorana representation and the inclusions between the dihedral Majorana algebras there is a unique possible shape for $\mathcal{R}_8$; all classes of involutions but $2g$ are of type $2A$ and $2g$ is of type $2B$ and the types of the other conjugacy classes are then completely determined by their p-powers. From Norton's Table 3.2, there exists a unique conjugacy class of $2A$-embedded G_8 subgroups in $\mathbb{M}$ and so the unique shape of $\mathcal{R}_8$ is allowed in $V_{\mathbb{M}}$. □

B.8 Shapes for the representations $\mathcal{R}_{10}$ of G_{10}

The group $G_{10} = G^{(6,6,6;\ 5,5,5;\ 4)} \cong 2^5 :_\phi S_5$ is the largest group that satisfies $(\boldsymbol{\sigma})$ and $2A$-embeds in $\mathbb{M}$. We let $a,\ b,\ c$ be the generators of G_{10} such that a and b commute. We recall that the conjugacy classes of G_{10} described in Proposition 3.38 of the previous section are as follows.

Class in G_{10}	$1a$	$2a$	$2b$	$2c$	$2d$	$2e$	$2f$	$2g$	$3a$	$4a$	$4b$	$4c$
p-powers	–	–	–	–	–	–	–	–	–	b	b	b
Size	1	1	15	15	40	40	60	60	320	60	60	120
Class in G_{10}	$4d$	$4e$	$4f$	$4g$	$5a$	$6a$	$6b$	$6c$	$8a$	$8b$	$10a$	
p-powers	b	g	g	c	–	ae	ad	aa	ab	aa	aa	
Size	120	240	240	240	384	320	320	320	240	240	384	

From Lemma 3.41 and the proof of Proposition 3.44 we can let the elements a, b and ab be in conjugacy class $2f$ and c be in conjugacy class $2d$.

Proposition B.22. *Let $T_{10} := 2d \cup 2f$ and let $\mathcal{R}_{10} := (G_{10}, T_{10}, X_{10})$ be a Majorana representation of G_{10}. Then there are four possible shapes for $\mathcal{R}_{10}$ of which only one is allowed in $V_{\mathbb{M}}$.*

Proof. The proof is similar to the proof of Propositions B.12 and B.18 and so some of the details are omitted. The conjugacy classes involved in the shape of $\mathcal{R}_{10}$ are all the conjugacy classes of involutions, all the conjugacy classes of elements of order 4 except $4g$, and the classes $3a$, $5a$, $6a$, $6b$, $6c$. The types of the elements of order 4 are determined by that of the types of their squares. By definition of T_{10} the classes $2d$, $2f$ have type $2A$. The classes $6a$, $6b$, $6c$ are of type $6A$ so that the class $3a$ has type $3A$ and the classes $2a$ and $2e$ have type $2A$. Because the product of two Majorana involutions cannot have order equal to 10 the class $2g$ must be of type $2B$. The only types left to be determined are those of $2b$ and $2c$ which can be either $2A$ or $2B$ so there are four possible shapes for $\mathcal{R}_{10}$. From Norton's Table 3.2, there is only one conjugacy class of $2A$-embedded G_{10} subgroups in $\mathbb{M}$ which can be found in row 37 of Table 3.2 so there is only one shape of $\mathcal{R}_{10}$ allowed in $V_{\mathbb{M}}$. From the proposition below the shape for which X_{10} could be a subalgebra of $V_{\mathbb{M}}$ is when $2b$ has type $2B$ and $2c$ has type $2A$. □

Fusion of G_{10} in $\mathbb{M}$

Now we let $\eta : G_{10} \hookrightarrow \mathbb{M}$ be the embedding such that $\eta(G_{10})$ corresponds to the group in row 37 of Norton's Table 3.2. We abuse notation and denote G_{10} the image $\eta(G_{10})$. We obtained the fusion of the classes of G_{10} into those of $\mathbb{M}$.

Proposition B.23. *Let G_{10} be a subgroup of the Monster $\mathbb{M}$ isomorphic to $2^5.S_5$ as in row 37 of Norton's Table 3.2. Then the fusion of the conjugacy classes of G_{10} in those of $\mathbb{M}$ is as follows:*

Fusion of G_{10} in $\mathbb{M}$

Class in G_{10}	$1a$	$2a$	$2b$	$2c$	$2d$	$2e$	$2f$	$2g$	$3a$	$4a$	$4b$	$4c$
p-powers in G_{10}	–	–	–	–	–	–	–	–	–	b	b	b
Size	1	1	15	15	40	40	60	60	320	60	60	120
Class in $\mathbb{M}$	$1A$	$2A$	$2B$	$2A$	$2A$	$2A$	$2A$	$2B$	$3A$	$4A$	$4A$	$4A$
p-powers in $\mathbb{M}$	–	–	–	–	–	–	–	–	–	B	B	B

Class in G_{10}	$4d$	$4e$	$4f$	$4g$	$5a$	$6a$	$6b$	$6c$	$8a$	$8b$	$10a$
p-powers in G_{10}	b	g	g	c	–	ae	ad	aa	ab	aa	aa
Size	120	240	240	240	384	320	320	320	240	240	384
Class in $\mathbb{M}$	$4A$	$4A$	$4A$	$4B$	$5A$	$6A$	$6A$	$6A$	$8B$	$8B$	$10A$
p-powers in $\mathbb{M}$	B	B	B	A	–	AA	AA	AA	A	A	AA

Proof. In [Nor85] S. P. Norton gives the elements a, b, c as elements of A_{12}. From Lemma 6 of [Nor85] the permutation types 2^2, 2^6 in A_{12} are $2A$ involutions in $\mathbb{M}$, and the type 2^4 are $2B$. Hence the classes $2a$, $2c$, $2d$, $2e$, $2f$ are in $2A$ and the classes $2b$, $2g$ are in $2B$. From the 6-transposition property of the $2A$ involutions and the information on p-powers in G_{10} and $\mathbb{M}$ the rest of the fusion easily follows. □